StorageGRID 11.6 文档

StorageGRID

NetApp
November 07, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-116/index.html on November 07, 2024. Always check docs.netapp.com for the latest.

目录

StorageGRID 11.6 文档 1
发行说明 2
入门 3
网格入门 3
网络连接准则 66
安装和维护设备硬件 93
SG100 和 SG1000 服务设备 93
SG6000 存储设备 198
SG5700 存储设备 370
SG5600 存储设备 495
安装和升级软件 606
升级 StorageGRID 软件 606
安装 Red Hat Enterprise Linux 或 CentOS 637
安装 Ubuntu 或 Debian 697
安装 VMware 757
执行系统管理 803
管理 StorageGRID 803
使用 ILM 管理对象 1081
系统强化 1231
配置 FabricPool 1238
使用 StorageGRID 1257
使用租户帐户 1257
使用 S3 1353
使用 Swift 1469
监控和维护 StorageGRID 1499
监控和故障排除 1499
扩展网格 1808
恢复和维护 1856
查看审核日志 2081
如何在您的环境中启用StorageGRID 2157
其他版本的NetApp StorageGRID 文档 2158
法律声明 2159
版权 2159
商标 2159
专利 2159
隐私政策 2159
开放源代码 2159

StorageGRID 11.6 文档

发行说明

获取有关新功能，已删除或已弃用功能，已修复问题和已知问题的特定版本信息。

登录到 NetApp 支持站点 "查看或下载 PDF 文件" 包含 StorageGRID 11.6 发行说明。

入门

网格入门

网格入门：概述

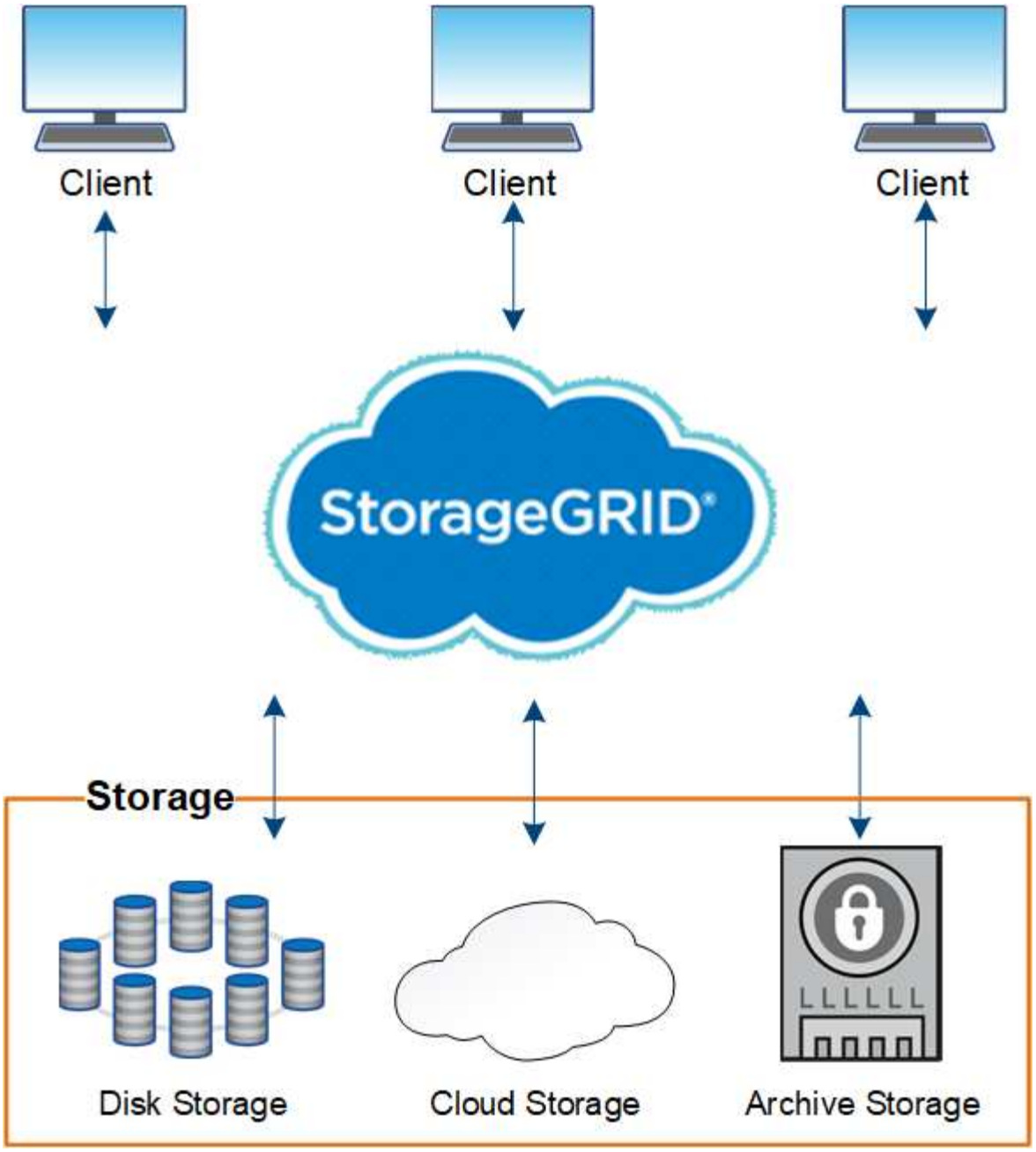
使用这些简介可简要了解 StorageGRID 系统，并了解 StorageGRID 架构和网络拓扑，数据管理功能以及用户界面。

什么是 **StorageGRID** ？

NetApp®StorageGRID®是一款软件定义的对象存储套件，支持公共、私有和混合多云环境中的各种用例。StorageGRID 为Amazon S3 API提供本机支持、并提供行业领先的创新技术、例如自动化生命周期管理、以便长期经济高效地存储、保护和保留非结构化数据。

StorageGRID 可为大规模非结构化数据提供安全，持久的存储。元数据驱动的集成生命周期管理策略可优化数据在整个生命周期中的位置。将内容放置在合适的位置，合适的时间和合适的存储层上，以降低成本。

StorageGRID 由分布在不同地理位置的冗余异构节点组成，这些节点可以与现有客户端应用程序和下一代客户端应用程序集成在一起。



StorageGRID 系统的优势包括：

- 一个地理位置分散的非结构化数据存储库，具有大规模可扩展性和易用性。
- 标准对象存储协议：
  - Amazon Web Services Simple Storage Service （ S3 ）
  - OpenStack Swift
- 已启用混合云。基于策略的信息生命周期管理（ ILM ）可将对象存储到公有 云，包括 Amazon Web Services （ AWS ）和 Microsoft Azure 。StorageGRID 平台服务支持对存储到公有 云的对象进行内容复制，事件通知和元数据搜索。
- 灵活的数据保护，可确保持久性和可用性。可以使用复制和分层纠删编码来保护数据。空闲和正在运行的数据验证可确保完整性，确保长期保留。
- 动态数据生命周期管理，有助于管理存储成本。您可以创建在对象级别管理数据生命周期的 ILM 规则，并自

定义数据位置，持久性，性能，成本和保留时间。磁带可用作集成归档层。

- 数据存储和某些管理功能的高可用性，以及集成的负载平衡功能，可优化 StorageGRID 资源中的数据负载。
- 支持多个存储租户帐户，以便按不同实体隔离系统上存储的对象。
- 用于监控 StorageGRID 系统运行状况的众多工具，包括全面的警报系统，图形信息板以及所有节点和站点的详细状态。
- 支持基于软件或硬件的部署。您可以在以下任意位置部署 StorageGRID ：
  - 在 VMware 中运行的虚拟机。
  - Linux 主机上的容器引擎。
  - StorageGRID 工程设备。
    - 存储设备提供对象存储。
    - 服务设备可提供网格管理和负载平衡服务。
- 符合以下法规的相关存储要求：
  - 《证券和交易委员会（ SEC ）》，采用 17 § 240.17a-4 （ f ），用于监管交易所成员，代理或交易商。
  - 金融行业监管局（ FINRA ）规则 4511 （ c ），该规则符合 SEC 规则 17a-4 （ f ）的格式和介质要求。
  - 商品期货交易委员会（ CFTC ）在监管商品期货交易的第 17 条 CFR § 1.31 （ c ） - （ d ）条中进行了规定。
- 无中断升级和维护操作。在升级，扩展，停用和维护过程中保持对内容的访问。
- 联合身份管理。与 Active Directory ， OpenLDAP 或 Oracle Directory Service 集成以进行用户身份验证。支持使用安全断言标记语言 2.0 （ SAML 2.0 ）标准的单点登录（ SSO ），以便在 StorageGRID 和 Active Directory 联合身份验证服务（ AD FS ）之间交换身份验证和授权数据。

采用 **StorageGRID** 的混合云

您可以在混合云配置中使用 StorageGRID ，方法包括实施策略驱动型数据管理将对象存储在云存储池中，利用 StorageGRID 平台服务以及使用 NetApp FabricPool 将数据迁移到 StorageGRID 。

云存储池

通过云存储池，您可以将对象存储在 StorageGRID 系统之外。例如，您可能希望将不常访问的对象移至成本较低的云存储，例如 Amazon S3 Glacier ， S3 Glacier Deep Archive 或 Microsoft Azure Blob 存储中的归档访问层。或者，您可能希望维护 StorageGRID 对象的云备份，该备份可用于恢复因存储卷或存储节点故障而丢失的数据。

不支持将云存储池与 FabricPool 结合使用，因为从云存储池目标检索对象会增加延迟。

S3 平台服务

通过 S3 平台服务，您可以将远程服务用作对象复制，事件通知或搜索集成的端点。平台服务独立于网格的 ILM 规则运行，并可为各个 S3 存储分段启用。支持以下服务：

- CloudMirror 复制服务会自动将指定对象镜像到目标 S3 存储分段，该存储分段可以位于 Amazon S3 或第二个 StorageGRID 系统上。
- 事件通知服务会将有关指定操作的消息发送到支持接收简单通知服务（ SNS ）事件的外部端点。
- 搜索集成服务会将对象元数据发送到外部 Elasticsearch 服务，从而可以使用第三方工具搜索，可视化和分析元数据。

例如，您可以使用 CloudMirror 复制将特定客户记录镜像到 Amazon S3 ，然后利用 AWS 服务对数据执行分析。

使用 **StorageGRID** 进行 **ONTAP** 数据分层

您可以使用 FabricPool 将数据分层到 StorageGRID ，从而降低 ONTAP 存储的成本。FabricPool 是一项 NetApp Data Fabric 技术，可将数据自动分层到内部或外部的低成本对象存储层。

与手动分层解决方案不同， FabricPool 可通过自动化数据分层来降低存储成本，从而降低总拥有成本。它通过分层到公有 和包括 StorageGRID 在内的私有云，提供云经济的优势。

相关信息

- 管理 StorageGRID
- 使用租户帐户
- 使用 ILM 管理对象
- 为 FabricPool 配置 StorageGRID

StorageGRID 架构和网络拓扑

StorageGRID 系统由一个或多个数据中心站点上的多种类型的网格节点组成。

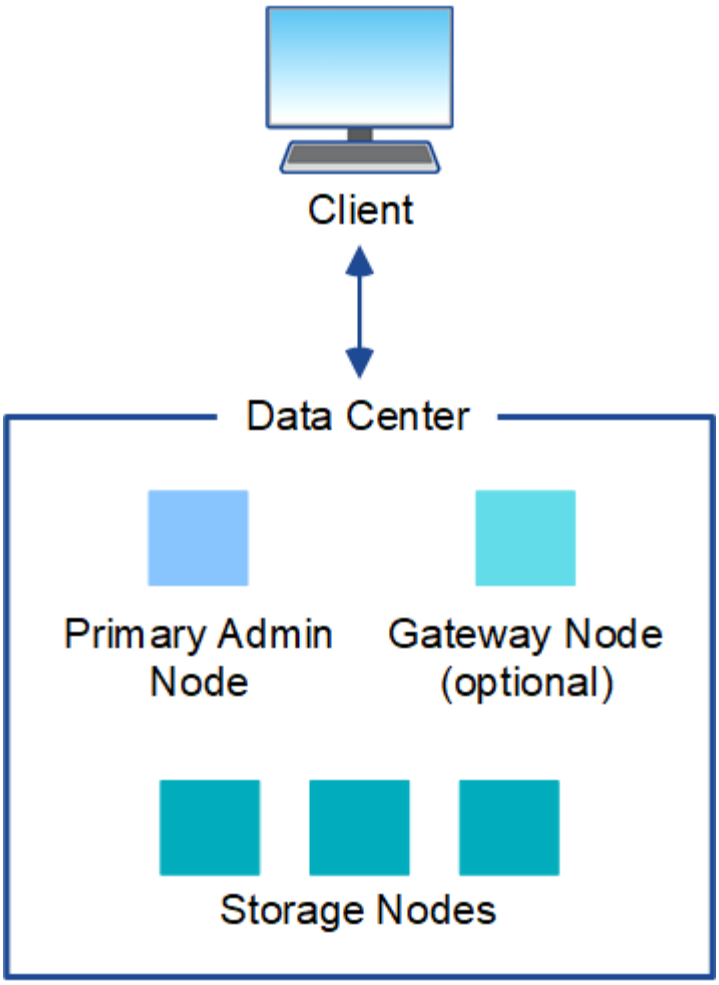
有关追加信息 关于 StorageGRID 网络拓扑，要求和网格通信的信息，请参见 网络连接准则。

部署拓扑

StorageGRID 系统可以部署到一个数据中心站点或多个数据中心站点。

单个站点

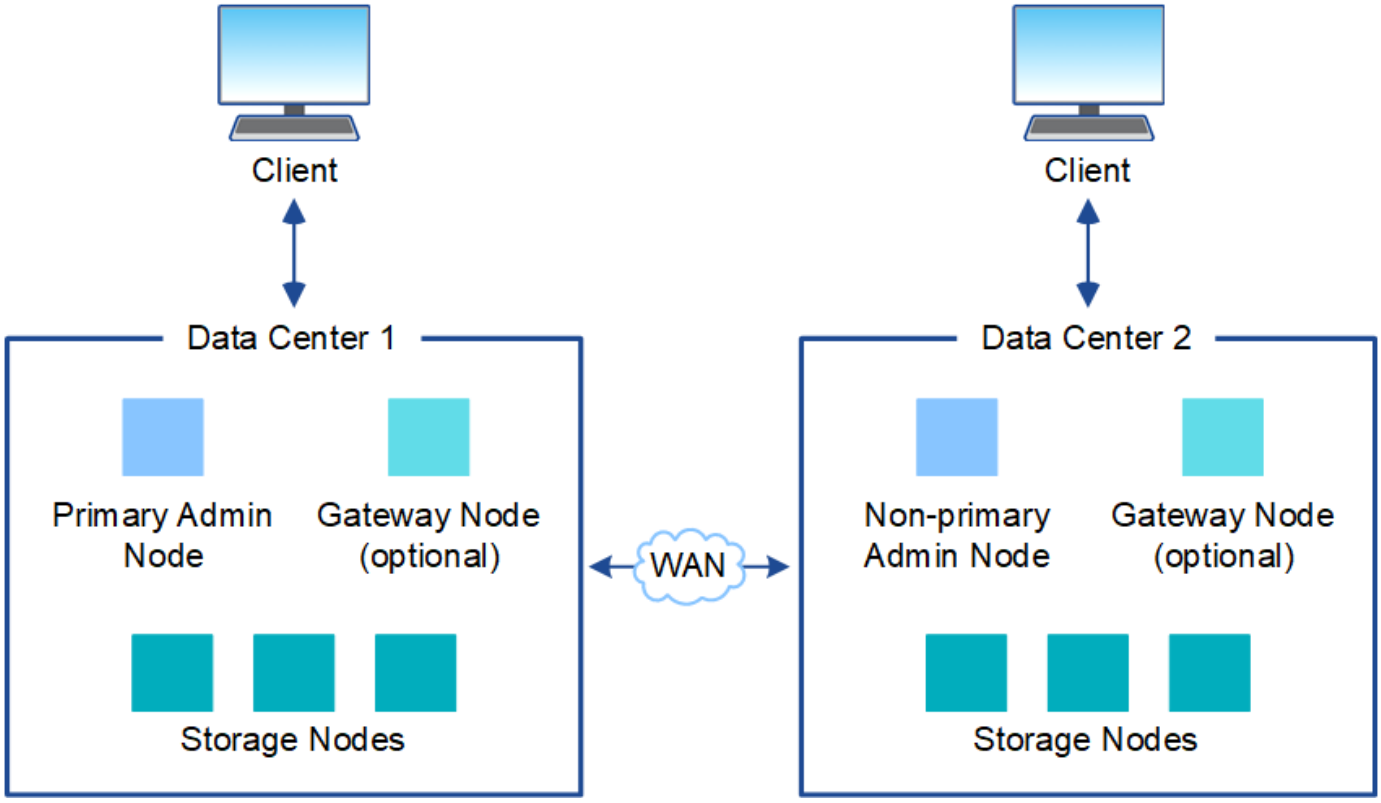
在使用单个站点的部署中， StorageGRID 系统的基础架构和操作会集中进行。



多个站点

在包含多个站点的部署中，可以在每个站点安装不同类型和数量的 StorageGRID 资源。例如，一个数据中心可能需要比另一个数据中心更多的存储。

不同站点通常位于不同故障域中不同地理位置的不同位置，例如地震故障线或泛洪。数据共享和灾难恢复可通过自动将数据分发到其他站点来实现。



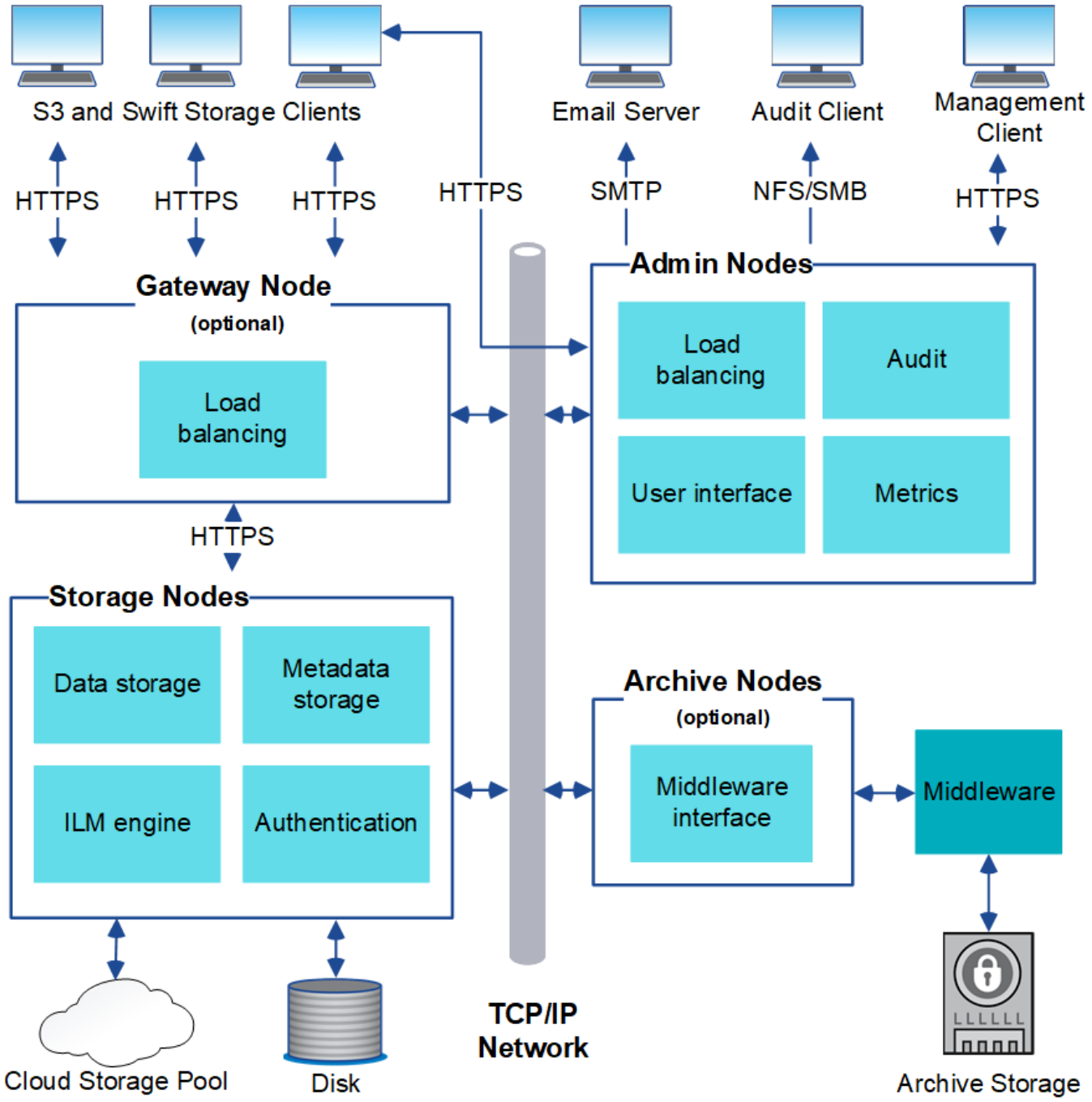
一个数据中心中也可以存在多个逻辑站点，以便使用分布式复制和纠删编码来提高可用性和故障恢复能力。

网格节点冗余

在单站点或多站点部署中，您可以选择包含多个管理节点或网关节点以实现冗余。例如，您可以在一个站点或多个站点上安装多个管理节点。但是，每个 StorageGRID 系统只能有一个主管理节点。

系统架构

此图显示了网格节点在 StorageGRID 系统中的排列方式。



S3 和 Swift 客户端在 StorageGRID 中存储和检索对象。其他客户端用于发送电子邮件通知，访问 StorageGRID 管理界面以及访问审核共享（可选）。

S3 和 Swift 客户端可以连接到网关节点或管理节点，以使用存储节点的负载平衡接口。或者， S3 和 Swift 客户端也可以使用 HTTPS 直接连接到存储节点。

对象可以存储在 StorageGRID 中的软件或基于硬件的存储节点上，外部归档介质（如磁带）上或云存储池中（由外部 S3 存储分段或 Azure Blob 存储容器组成）。

网格节点和服务

StorageGRID 系统的基本组件是网格节点。节点包含服务，这些服务是为网格节点提供一组功能的软件模块。

StorageGRID 系统使用四种类型的网格节点：

- * 管理节点 * 提供系统配置，监控和日志记录等管理服务。登录到网格管理器后，您将连接到管理节点。每个网格都必须有一个主管理节点，并且可能有额外的非主管理节点，以实现冗余。您可以连接到任何管理节点，每个管理节点都会显示一个类似的 StorageGRID 系统视图。但是，必须使用主管理节点执行维护过程。

  管理节点还可用于对 S3 和 Swift 客户端流量进行负载平衡。

- * 存储节点 * 用于管理和存储对象数据和元数据。每个 StorageGRID 系统必须至少具有三个存储节点。如果您有多个站点，则 StorageGRID 系统中的每个站点也必须有三个存储节点。
- * 网关节点（可选） * 提供了一个负载平衡接口，客户端应用程序可以使用该接口连接到 StorageGRID 。负载平衡器可将客户端无缝定向到最佳存储节点，以便节点甚至整个站点的故障是透明的。您可以组合使用网关节点和管理节点进行负载平衡，也可以实施第三方 HTTP 负载平衡器。
- * 归档节点（可选） * 提供了一个接口，可通过该接口将对象数据归档到磁带。

要了解更多信息，请参见 管理 StorageGRID。

基于软件的节点

基于软件的网格节点可以通过以下方式进行部署：

- 作为 VMware vSphere 中的虚拟机（ VM ）
- 在 Linux 主机上的容器引擎中。支持以下操作系统：
  - Red Hat Enterprise Linux
  - CentOS
  - Ubuntu
  - Debian

有关详细信息，请参见以下内容：

- 安装 VMware
- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian

使用 "NetApp 互操作性表工具" 以获取支持的版本列表。

StorageGRID 设备节点

StorageGRID 硬件设备经过专门设计，可在 StorageGRID 系统中使用。某些设备可用作存储节点。其他设备可以用作管理节点或网关节点。您可以将设备节点与基于软件的节点结合使用，也可以部署完全设计的全设备网格，这些网格不依赖于外部虚拟机管理程序，存储或计算硬件。

有四种类型的 StorageGRID 设备可用：

- * SG100 和 SG1000 服务设备 * 是一个单机架单元（ 1U ）服务器，每个服务器均可作为主管理节点，非主管理节点或网关节点运行。这两个设备可以同时作为网关节点和管理节点（主节点和非主节点）运行。
- * SG6000 存储设备 * 作为存储节点运行，并将 1U SG6000-CN 计算控制器与 2U 或 4U 存储控制器架相结

合。SG6000有三种型号：

  - * SGF6024* ： 将 SG6000-CN 计算控制器与 2U 存储控制器架相结合，该存储控制器架包含 24 个固态驱动器（ SSD ）和冗余存储控制器。
  - * SG6060和SG6060X*：将SG6000-CN计算控制器与4U机箱相结合、其中包括58个NL-SAS驱动器、2个SSD和冗余存储控制器。SG6060和SG6060X各自支持一个或两个60驱动器扩展架、最多可提供178个专用于对象存储的驱动器。

- * SG5700 存储设备 * 是一个作为存储节点运行的集成存储和计算平台。SG5700有四种型号：
  - * SG5712和SG5712X*：一个2U机箱、包含12个NL-SAS驱动器以及集成的存储和计算控制器。
  - * SG5760和SG5760X*：一个4U机箱、包含60个NL-SAS驱动器以及集成的存储和计算控制器。
- * SG5600 存储设备 * 是一个作为存储节点运行的集成存储和计算平台。SG5600 有两种型号：
  - * SG5612* ： 一个 2U 机箱，包含 12 个 NL-SAS 驱动器以及集成存储和计算控制器。
  - * SG5660* ： 一个 4U 机箱，包含 60 个 NL-SAS 驱动器以及集成存储和计算控制器。

有关详细信息，请参见以下内容：

- "NetApp Hardware Universe"
- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

管理节点的主服务

下表显示了管理节点的主服务；但是，此表并未列出所有节点服务。

服务	关键功能
审核管理系统（ AMS ）	跟踪系统活动。
配置管理节点（ CMN ）	管理系统范围的配置。仅限主管理节点。
管理应用程序程序接口（ mgmt-API ）	处理来自网格管理 API 和租户管理 API 的请求。
高可用性	管理管理节点和网关节点组的高可用性虚拟 IP 地址。 • 注： * 此服务也可在网关节点上找到。
负载平衡器	为从客户端到存储节点的 S3 和 Swift 流量提供负载平衡。 • 注： * 此服务也可在网关节点上找到。
网络管理系统（ NMS ）	提供网格管理器的功能。

服务	关键功能
Prometheus	收集和存储指标。
服务器状态监控器（ SSM ）	监控操作系统和底层硬件。

存储节点的主服务

下表显示了存储节点的主服务；但是，此表并未列出所有节点服务。

某些服务（例如，模块转换服务和 RSM 服务）通常仅存在于每个站点的三个存储节点上。

服务	关键功能
帐户（访问）	管理租户帐户。
管理域控制器（ ADC-A ）	维护拓扑和网格范围的配置。
Cassandra	存储和保护对象元数据。
Cassandra Reaper	自动修复对象元数据。
区块	管理经过擦除编码的数据和奇偶校验片段。
数据移动器（ DMV ）	将数据移动到云存储池。
分布式数据存储（ DDS ）	监控对象元数据存储。
身份（ idnt ）	从 LDAP 和 Active Directory 联合用户身份。
本地分发路由器（ LDR ）	处理对象存储协议请求并管理磁盘上的对象数据。
复制状态机（ RSM ）	确保 S3 平台服务请求发送到其各自的端点。
服务器状态监控器（ SSM ）	监控操作系统和底层硬件。

网关节点的主要服务

下表显示了网关节点的主服务；但是，此表并未列出所有节点服务。

服务	关键功能
连接负载平衡器（ CLB ）	为从客户端到存储节点的 S3 和 Swift 流量提供第 3 层和第 4 层负载平衡。传统负载平衡机制。 • 注： * CLB 服务已弃用。
高可用性	管理管理节点和网关节点组的高可用性虚拟 IP 地址。 • 注： * 此服务也可在管理节点上找到。
负载平衡器	为从客户端到存储节点的 S3 和 Swift 流量提供第 7 层负载平衡。这是建议的负载平衡机制。 • 注： * 此服务也可在管理节点上找到。
服务器状态监控器（ SSM ）	监控操作系统和底层硬件。

归档节点的主服务

下表显示了归档节点的主服务；但是，此表并未列出所有节点服务。

服务	关键功能
归档（ ARC-）	与 Tivoli Storage Manager （ TSM ）外部磁带存储系统通信。
服务器状态监控器（ SSM ）	监控操作系统和底层硬件。

StorageGRID 服务

以下是 StorageGRID 服务的完整列表。

- * 客户服务转发器 *

  为负载平衡器服务提供一个界面，用于查询远程主机上的帐户服务，并提供有关负载平衡器端点配置更改的通知。管理节点和网关节点上存在负载平衡器服务。

- * ADA 服务（管理域控制器） *

  维护拓扑信息，提供身份验证服务，并响应 LDR 和 CMN 服务的查询。在一个站点上安装的前三个存储节点中的每个节点上都存在此 ADC-Service 。

- * AMS 服务（审核管理系统） *

  监控所有已审核的系统事件和事务并将其记录到文本日志文件中。管理节点上存在 AMS 服务。

- * 应用程序中心服务（归档） *

  提供一个管理界面，用于配置与外部归档存储的连接，例如通过 S3 接口连接到云，或者通过 TSM 中间件

连接到磁带。归档节点上存在此 ARC-Service 。

- * Cassandra Reaper 服务 *

  自动修复对象元数据。所有存储节点上都存在 Cassandra Reaper 服务。

- * 区块服务 *

  管理经过擦除编码的数据和奇偶校验片段。存储节点上存在区块服务。

- * CLB 服务（连接负载平衡器） *

  为通过 HTTP 连接的客户端应用程序提供 StorageGRID 网关的已弃用服务。网关节点上存在 CLB 服务。CLB 服务已弃用，将在未来的 StorageGRID 版本中删除。

- * CMN 服务（配置管理节点） *

  管理系统范围的配置和网格任务。每个网格都有一个 CMN 服务，该服务位于主管理节点上。

- * DDS 服务（分布式数据存储） *

  与 Cassandra 数据库连接以管理对象元数据。存储节点上存在 DDS 服务。

- * DMV 服务（数据移动） *

  将数据移动到云端点。存储节点上存在 DMV 服务。

- * 动态 IP 服务 *

  监控网格中的动态 IP 更改并更新本地配置。所有节点上都存在动态 IP （ dynip ）服务。

- * Grafana 服务 *

  用于在网格管理器中可视化指标。管理节点上存在 Grafana 服务。

- * 高可用性服务 *

  管理在高可用性组页面上配置的节点上的高可用性虚拟 IP 。管理节点和网关节点上存在高可用性服务。此服务也称为 keepalived 服务。

- * 身份（ idnt ）服务 *

  从 LDAP 和 Active Directory 联合用户身份。身份服务（ idnt ）位于每个站点的三个存储节点上。

- * Lambda 仲裁服务 *

  管理 S3 Select SelectObjectContent 请求。

- * 负载平衡器服务 *

  为从客户端到存储节点的 S3 和 Swift 流量提供负载平衡。可以通过负载平衡器端点配置页面配置负载平衡器服务。管理节点和网关节点上存在负载平衡器服务。此服务也称为 nginx 网关服务。

- * LDR 服务（本地分发路由器） *

  管理网格中内容的存储和传输。存储节点上存在 LDR 服务。

- * MIFSCd 信息服务控制守护进程服务 *

  提供一个界面，用于查询和管理其他节点上的服务以及管理节点上的环境配置，例如查询其他节点上运行的服务的状态。所有节点上都存在 MIFSCd 服务。

- * nginx 服务 *

  充当各种网格服务（例如 Prometheus 和动态 IP ）的身份验证和安全通信机制，以便能够通过 HTTPS API 与其他节点上的服务进行通信。所有节点上都存在 nginx 服务。

- * nginx 网关服务 *

  为负载平衡器服务供电。管理节点和网关节点上存在 nginx 网关服务。

- * NMS 服务（网络管理系统） *

  为通过网格管理器显示的监控，报告和配置选项提供电源。管理节点上存在 NMS 服务。

- * 持久性服务 *

  管理根磁盘上需要在重新启动后持续存在的文件。所有节点上都存在持久性服务。

- * Prometheus 服务 *

  从所有节点上的服务收集时间序列指标。管理节点上存在 Prometheus 服务。

- * RSM 服务（复制状态计算机服务） *

  确保平台服务请求发送到其各自的端点。RSM 服务位于使用此 ADC 服务的存储节点上。

- * SSM 服务（服务器状态监控器） *

  监控硬件状况并向 NMS 服务报告。每个网格节点上都存在一个 SSM 服务实例。

- * 跟踪收集器服务 *

  执行跟踪收集以收集信息以供技术支持使用。跟踪收集器服务使用开源 Jaeger 软件，并位于管理节点上。

对象管理

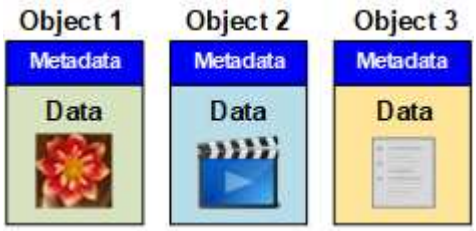
StorageGRID 如何管理数据

在开始使用 StorageGRID 系统时，了解 StorageGRID 系统如何管理数据非常有用。

什么是对象

对于对象存储，存储单元是对象，而不是文件或块。与文件系统或块存储的树状层次结构不同，对象存储以非结构化的平面布局对数据进行组织。对象存储可将数据的物理位置与用于存储和检索数据的方法分离。

基于对象的存储系统中的每个对象都有两部分：对象数据和对象元数据。



对象数据

对象数据可以是任何内容；例如，照片，电影或病历。

对象元数据

对象元数据是指描述对象的任何信息。StorageGRID 使用对象元数据跟踪网格中所有对象的位置，并管理每个对象的生命周期。

对象元数据包括以下信息：

- 系统元数据，包括每个对象的唯一 ID （ UUID ），对象名称， S3 存储分段或 Swift 容器的名称，租户帐户名称或 ID ，对象的逻辑大小，首次创建对象的日期和时间， 以及上次修改对象的日期和时间。
- 每个对象副本或纠删编码片段的当前存储位置。
- 与对象关联的任何用户元数据。

对象元数据可自定义并可扩展，因此应用程序可以灵活地使用。

有关 StorageGRID 如何以及在何处存储对象元数据的详细信息，请转到 管理对象元数据存储。

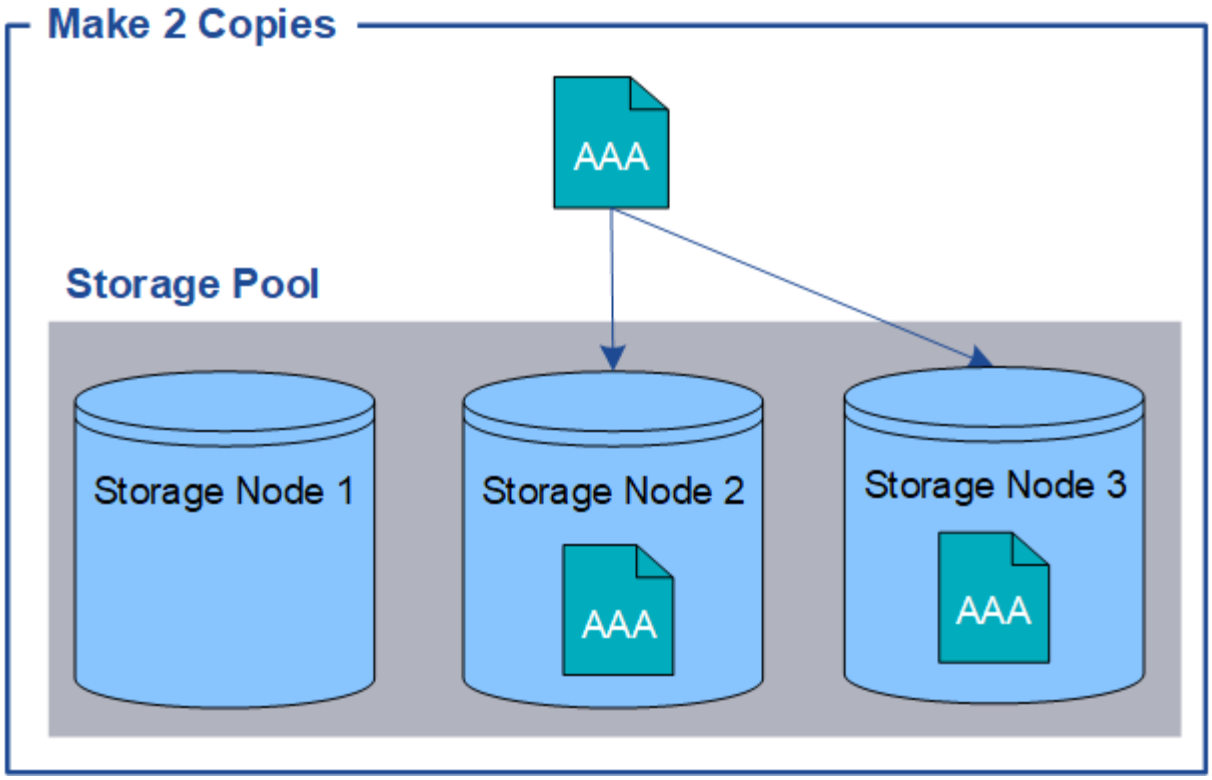
如何保护对象数据

StorageGRID 系统提供了两种机制来防止对象数据丢失：复制和纠删编码。

Replication

如果 StorageGRID 将对象与配置为创建复制副本的信息生命周期管理（ ILM ）规则匹配，则系统会创建对象数据的精确副本，并将其存储在存储节点，归档节点或云存储池中。ILM 规则规定了创建的副本数量，这些副本的存储位置以及系统保留这些副本的时间长度。例如，如果由于存储节点丢失而导致副本丢失，则如果 StorageGRID 系统中的其他位置存在该对象的副本，则该对象仍可用。

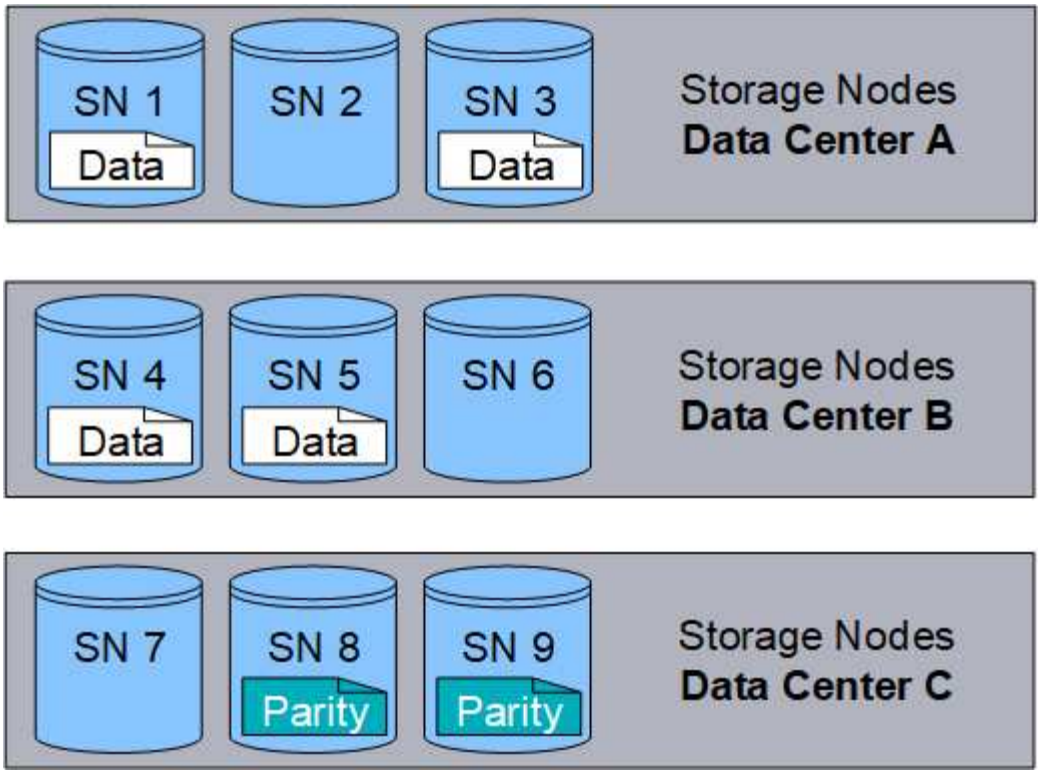
在以下示例中， make 2 copies 规则指定将每个对象的两个复制副本放置在包含三个存储节点的存储池中。



纠删编码

如果 StorageGRID 将对象与配置为创建纠删编码副本的 ILM 规则匹配，则会将对象数据分段为数据片段，计算额外的奇偶校验片段，并将每个片段存储在不同的存储节点上。访问某个对象时，系统会使用存储的片段重新组合该对象。如果数据或奇偶校验片段损坏或丢失，纠删编码算法可以使用剩余数据和奇偶校验片段的子集重新创建该片段。ILM 规则和纠删编码配置文件决定了所使用的纠删编码方案。

以下示例说明了如何对对象数据使用纠删编码。在此示例中， ILM 规则使用 4+2 纠删编码方案。每个对象都会被划分为四个相等的数据片段，并根据对象数据计算两个奇偶校验片段。六个片段中的每个片段都存储在三个数据中心的不同存储节点上，以便为节点故障或站点丢失提供数据保护。



相关信息

- 使用 ILM 管理对象
- 使用信息生命周期管理

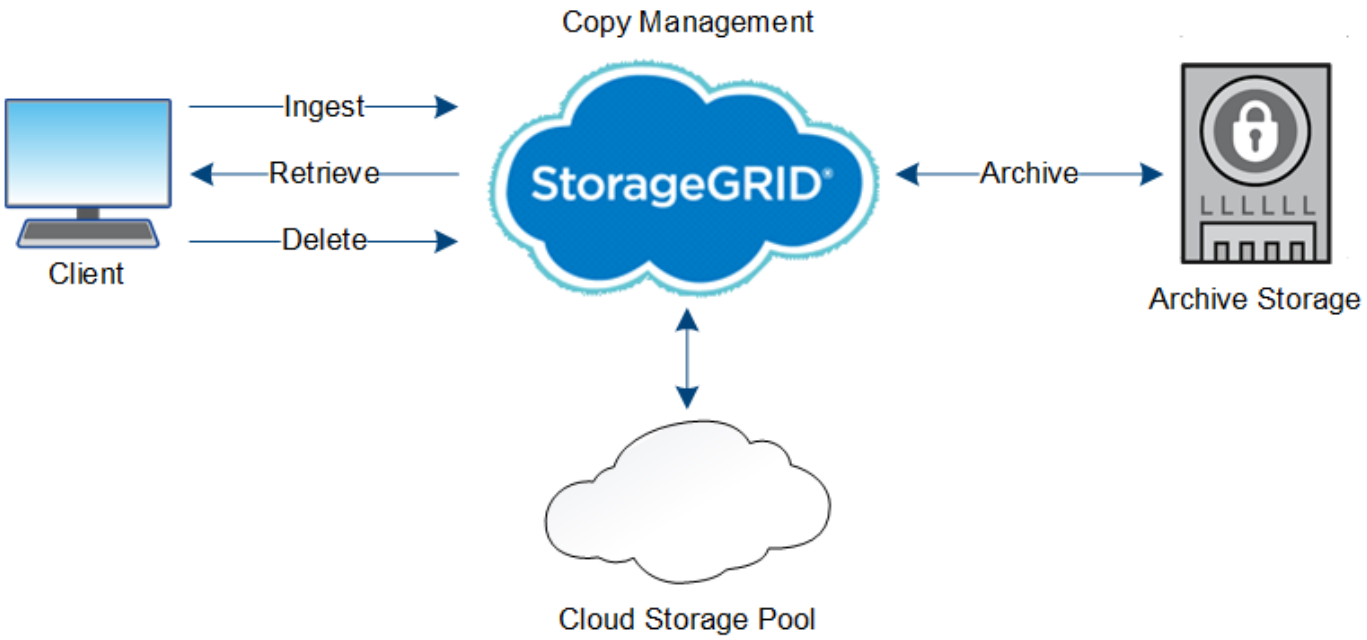
对象生命周期

对象的生命周期

对象的生命周期由多个阶段组成。每个阶段都表示对象发生的操作。

对象的生命周期包括载入，副本管理，检索和删除操作。

- * 载入 * ： S3 或 Swift 客户端应用程序通过 HTTP 将对象保存到 StorageGRID 系统的过程。在此阶段，StorageGRID 系统将开始管理此对象。
- * 副本管理 * ：在 StorageGRID 中管理复制的副本和经过纠删编码的副本的过程，如活动 ILM 策略中的 ILM 规则所述。在副本管理阶段， StorageGRID 通过在存储节点，云存储池或归档节点上创建和维护指定数量和类型的对象副本来保护对象数据不会丢失。
- * 检索 * ：客户端应用程序访问 StorageGRID 系统存储的对象的过程。客户端读取从存储节点，云存储池或归档节点检索到的对象。
- * 删除 * ：从网格中删除所有对象副本的过程。如果客户端应用程序向 StorageGRID 系统发送删除请求，或者由于 StorageGRID 在对象的生命周期到期时自动执行过程，则可以删除对象。



相关信息

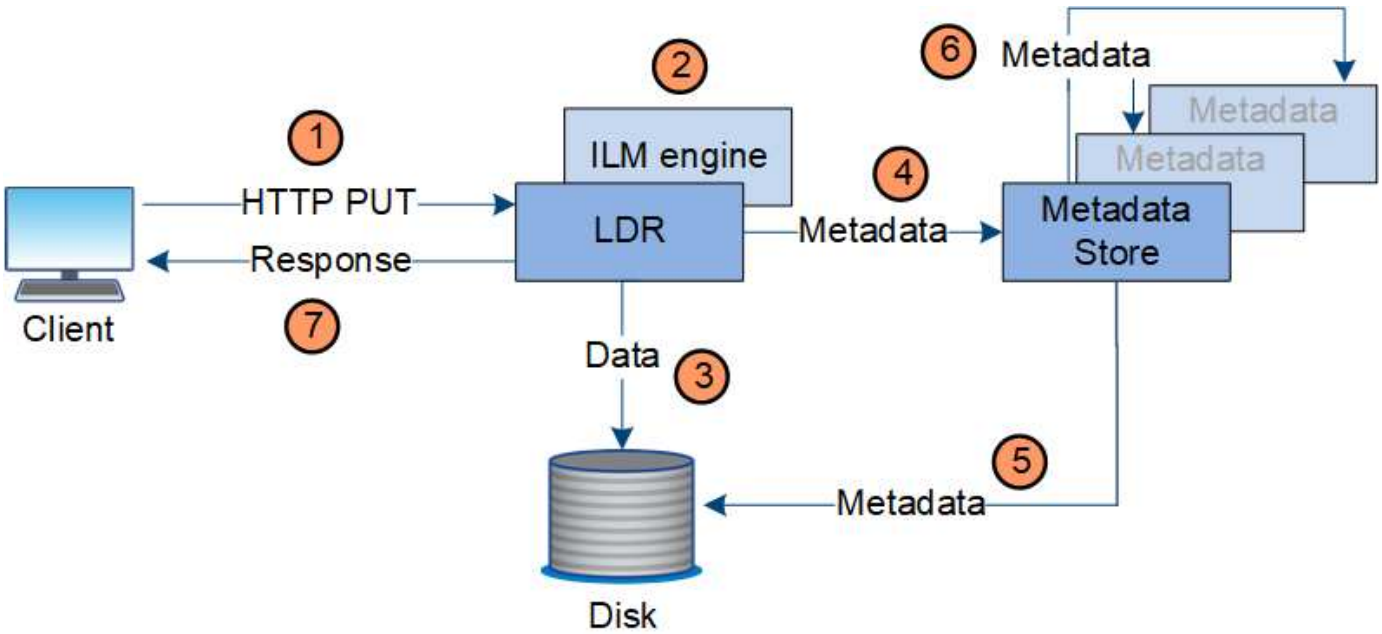
- 使用 ILM 管理对象
- 使用信息生命周期管理

载入数据流

载入或保存操作由客户端和 StorageGRID 系统之间定义的数据流组成。

数据流

当客户端将对象载入 StorageGRID 系统时，存储节点上的 LDR 服务将处理此请求并将元数据和数据存储到磁盘。



1. 客户端应用程序将创建此对象，并通过 HTTP PUT 请求将其发送到 StorageGRID 系统。
2. 将根据系统的 ILM 策略评估对象。
3. LDR 服务将对象数据保存为复制副本或纠删编码副本。（图中显示了将复制副本存储到磁盘的简化版本。）
4. LDR 服务将对象元数据发送到元数据存储。
5. 元数据存储将对象元数据保存到磁盘。
6. 元数据存储会将对象元数据的副本传播到其他存储节点。这些副本也会保存到磁盘中。
7. LDR 服务向客户端返回 HTTP 200 OK 响应，以确认已载入对象。

副本管理

对象数据由活动 ILM 策略及其 ILM 规则管理。ILM 规则可创建复制的或经过纠删编码的副本，以防止对象数据丢失。

在对象生命周期的不同时间，可能需要不同类型或位置的对象副本。系统会定期评估 ILM 规则，以确保根据需要放置对象。

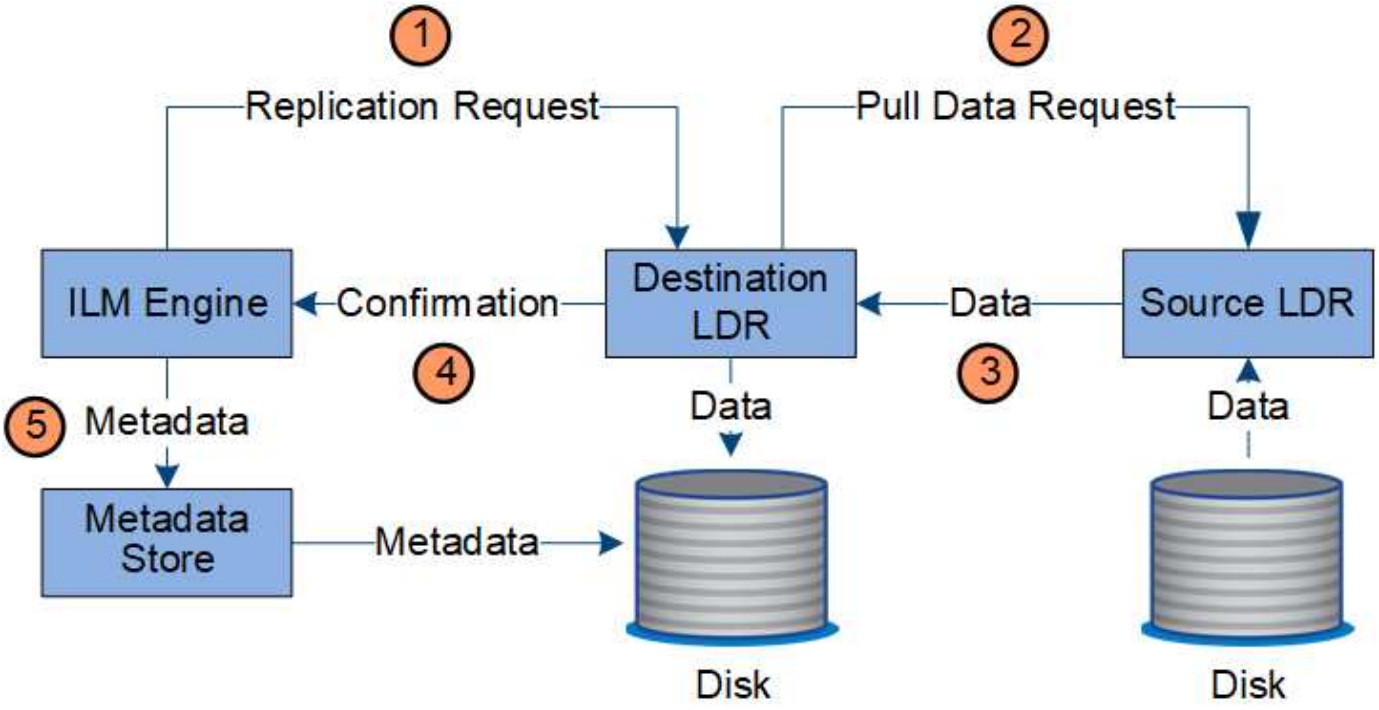
对象数据由 LDR 服务管理。

内容保护：复制

如果 ILM 规则的内容放置说明要求复制对象数据的副本，则构成已配置存储池的存储节点会创建副本并将其存储到磁盘中。

数据流

LDR 服务中的 ILM 引擎可控制复制，并确保将正确数量的副本存储在正确的位置和正确的时间内。



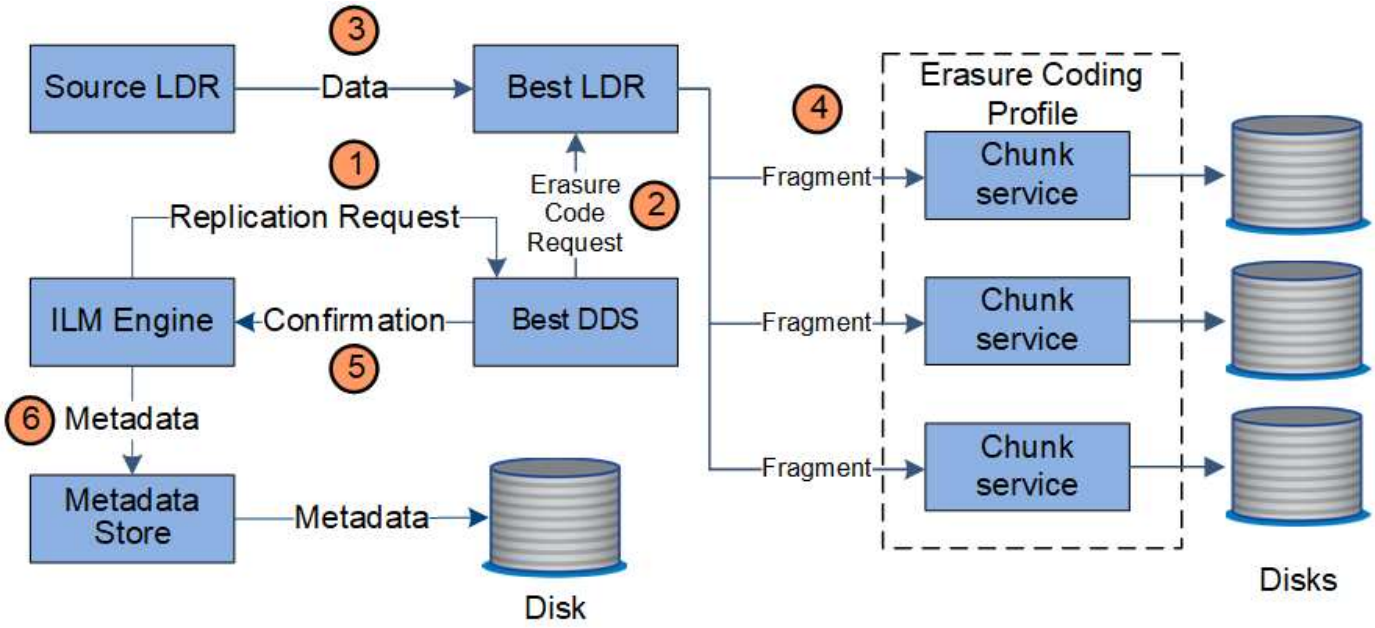
1. ILM 引擎会查询此 ADC-LDR 服务，以确定 ILM 规则指定的存储池中的最佳目标 LDR 服务。然后，它会向该 LDR 服务发送一个命令以启动复制。
2. 目标 LDR 服务会向此 ADC-Service 查询最佳源位置。然后，它会向源 LDR 服务发送复制请求。
3. 源 LDR 服务会向目标 LDR 服务发送一份副本。
4. 目标 LDR 服务通知 ILM 引擎已存储对象数据。
5. ILM 引擎使用对象位置元数据更新元数据存储。

内容保护：纠删编码

如果 ILM 规则包含为对象数据创建纠删编码副本的说明，则适用的纠删编码方案会将对象数据拆分为数据和奇偶校验片段，并将这些片段分布在 Erasure Coding 配置文件中配置的存储节点上。

数据流

ILM 引擎是 LDR 服务的一个组件，用于控制纠删编码，并确保将纠删编码配置文件应用于对象数据。



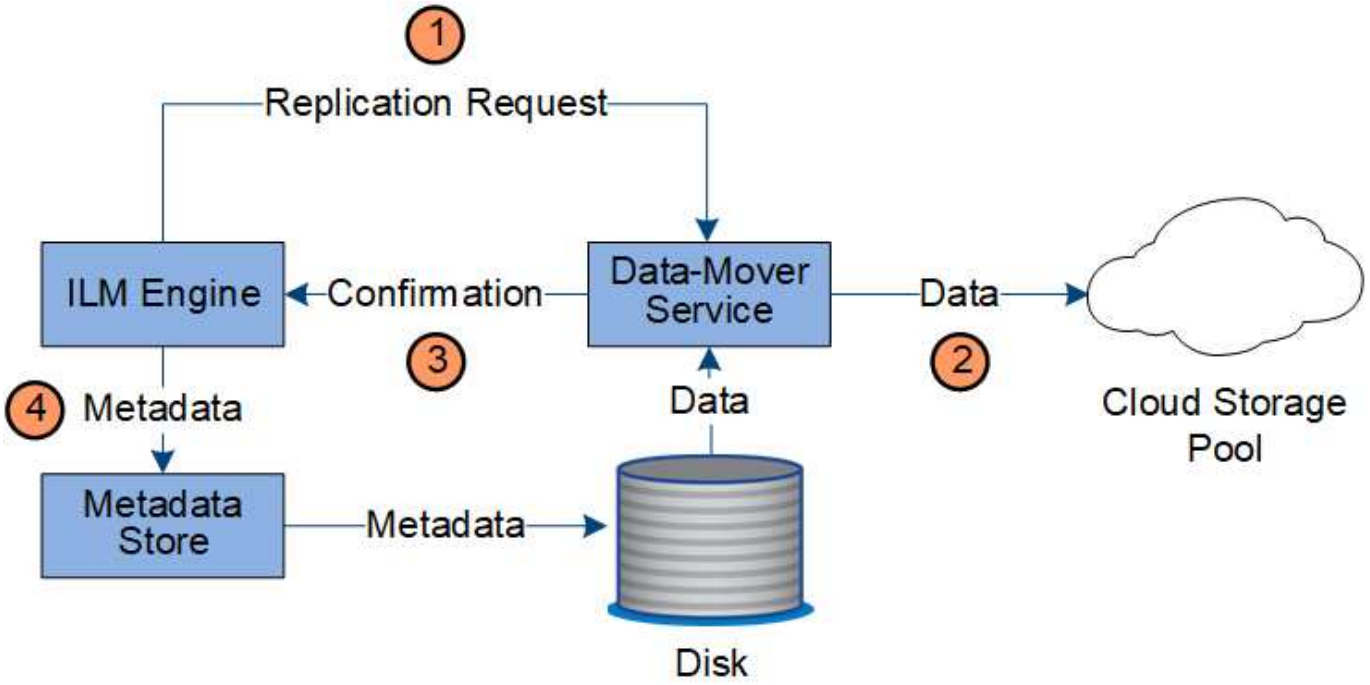
1. ILM 引擎会查询此 ADC-Service ，以确定哪种 DDS 服务能够以最佳方式执行纠删编码操作。一旦确定，ILM 引擎就会向该服务发送 " 启动 " 请求。
2. DDS 服务指示 LDR 对对象数据进行纠删编码。
3. 源 LDR 服务会向选定用于纠删编码的 LDR 服务发送一份副本。
4. 一旦细分为适当数量的奇偶校验和数据片段， LDR 服务会将这些片段分布在构成 Erasure 编码配置文件存储池的存储节点（区块服务）中。
5. LDR 服务通知 ILM 引擎，确认对象数据已成功分发。
6. ILM 引擎使用对象位置元数据更新元数据存储。

内容保护：云存储池

如果 ILM 规则的内容放置说明要求将对象数据的复制副本存储在云存储池中，则对象数据将复制到为云存储池指定的外部 S3 存储分段或 Azure Blob 存储容器。

数据流

ILM 引擎是 LDR 服务的一个组件， Data Mover 服务可控制对象到云存储池的移动。

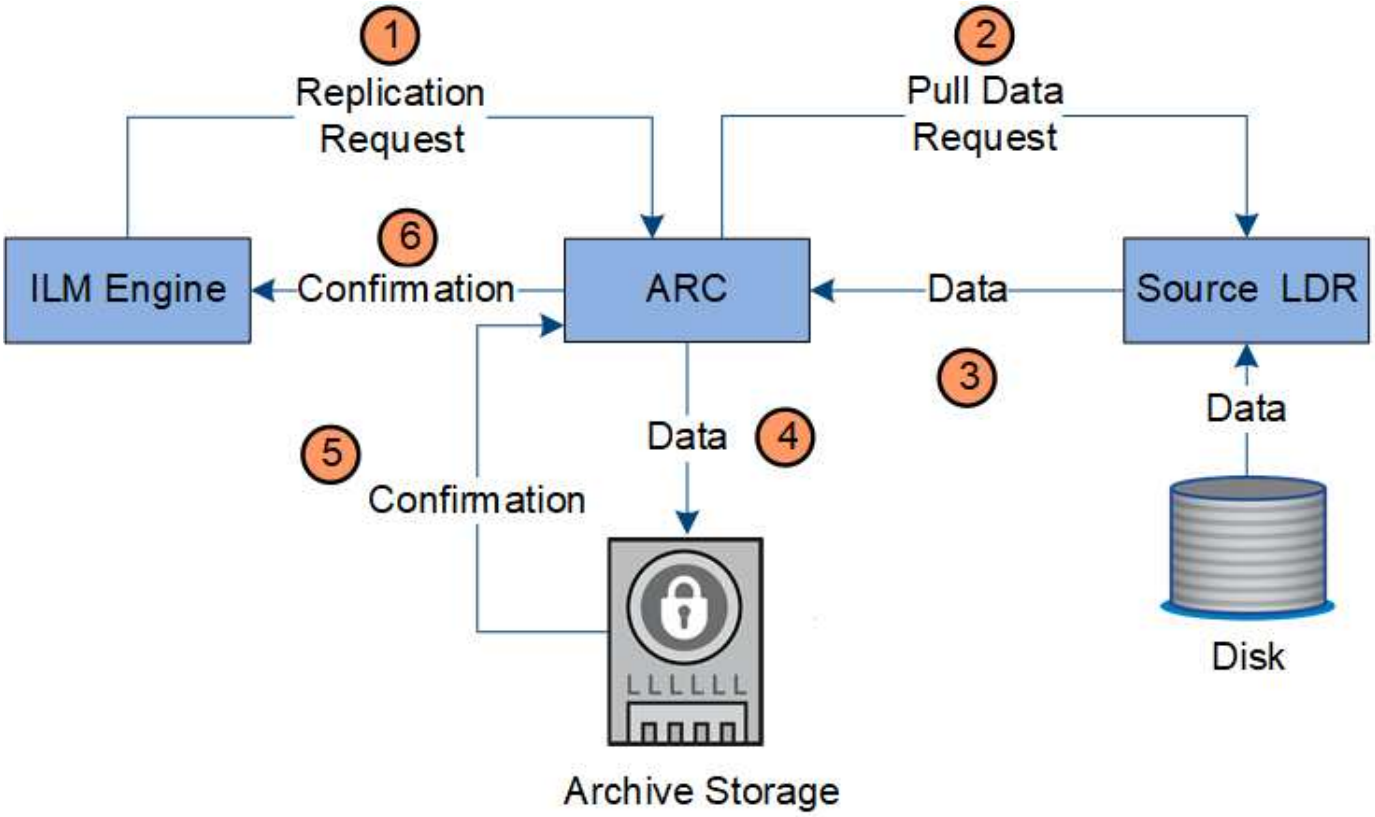


1. ILM 引擎选择要复制到云存储池的数据转换服务。
2. Data Mover 服务会将对象数据发送到云存储池。
3. Data Mover 服务会通知 ILM 引擎已存储对象数据。
4. ILM 引擎使用对象位置元数据更新元数据存储。

内容保护：归档

归档操作由 StorageGRID 系统与客户端之间定义的数据流组成。

如果 ILM 策略要求归档对象数据的副本，则作为 LDR 服务的组件的 ILM 引擎会向归档节点发送请求，归档节点进而向目标归档存储系统发送对象数据的副本。



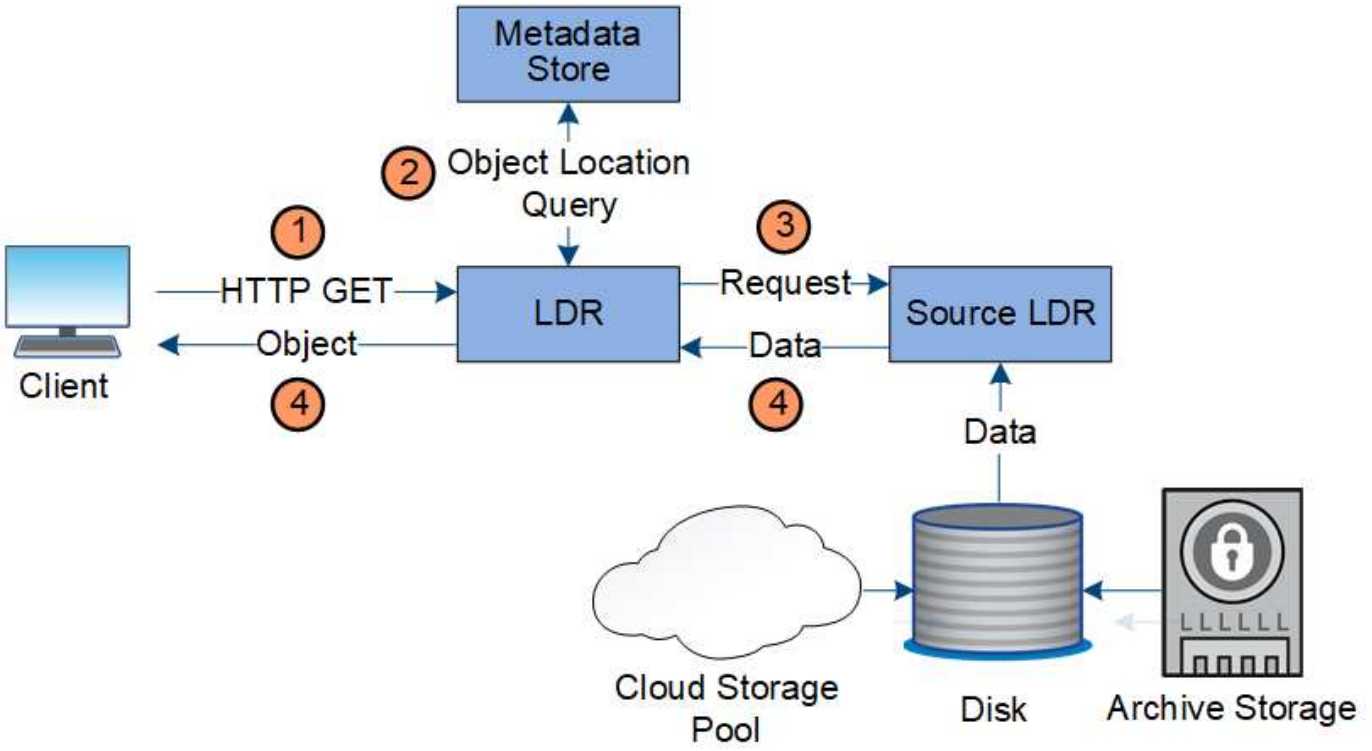
1. ILM 引擎会向 ARC-Service 发送一个请求，要求将副本存储在归档介质上。
2. 此 ARR 服务会向此 ADC/ 服务查询最佳源位置，并向源 LDR 服务发送请求。
3. ARR 服务从 LDR 服务检索对象数据。
4. 此应用程序服务会将对象数据发送到归档介质目标。
5. 归档介质会通知 ARC-Service 对象数据已存储。
6. ARC-Service 会通知 ILM 引擎已存储对象数据。

检索数据流

检索操作由 StorageGRID 系统与客户端之间定义的数据流组成。系统使用属性跟踪从存储节点或云存储池或归档节点检索对象的情况（如有必要）。

存储节点的 LDR 服务会在元数据存储中查询对象数据的位置，并从源 LDR 服务中检索这些数据。首选情况下，从存储节点检索。如果对象在存储节点上不可用，则检索请求将定向到云存储池或归档节点。

如果唯一的对象副本位于 AWS Glacier 存储或 Azure 归档层上，则客户端应用程序必须对 S3 后对象还原请求进行问题描述 ，才能将可检索的副本还原到云存储池。



1. LDR 服务从客户端应用程序接收检索请求。
2. LDR 服务会在元数据存储库中查询对象数据位置和元数据。
3. LDR 服务将检索请求转发到源 LDR 服务。
4. 源 LDR 服务从查询的 LDR 服务返回对象数据，系统将对象返回给客户端应用程序。

删除数据流

当客户端执行删除操作或对象的生命周期到期时，所有对象副本都会从 StorageGRID 系统中删除，从而触发自动删除。已定义用于删除对象的数据流。

删除层次结构

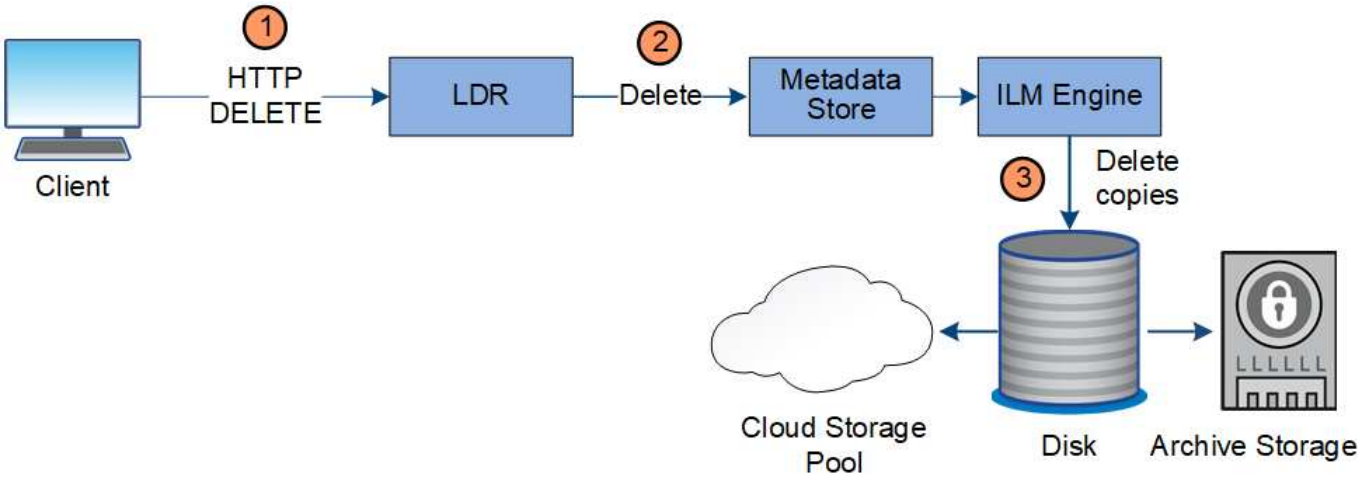
StorageGRID 提供了多种方法来控制何时保留或删除对象。可以根据客户端请求删除对象，也可以自动删除对象。StorageGRID 始终将任何 S3 对象锁定设置优先于客户端删除请求，而客户端删除请求优先于 S3 存储分段生命周期和 ILM 放置说明。

- * S3 对象锁定 *：如果为网格启用了全局 S3 对象锁定设置，则 S3 客户端可以在启用了 S3 对象锁定的情况下创建存储分段，然后使用 S3 REST API 为添加到存储分段的每个对象版本指定保留日期和合法保留设置。
  - 任何方法都不能删除处于合法保留状态的对象版本。
  - 在达到对象版本的保留截止日期之前，无法通过任何方法删除该版本。
  - 启用了 S3 对象锁定的存储分段中的对象由 ILM "`Forever` " 保留。但是，在达到保留截止日期后，可以通过客户端请求或存储分段生命周期到期来删除对象版本。
  - 如果 S3 客户端对存储分段应用默认的 retain-until 日期，则无需为每个对象指定 retain-until 日期。
- * 客户端删除请求 *： S3 或 Swift 客户端可以问题描述 删除对象请求。当客户端删除某个对象时，该对象的所有副本都会从 StorageGRID 系统中删除。

- * S3 存储分段生命周期 * ： S3 客户端可以将生命周期配置添加到指定到期操作的存储分段中。如果存储分段生命周期存在，则在满足到期操作中指定的日期或天数时， StorageGRID 会自动删除对象的所有副本，除非客户端先删除该对象。
- * ILM 放置说明 * ：假设存储分段未启用 S3 对象锁定，并且没有存储分段生命周期，则 StorageGRID 会在 ILM 规则中的最后一个时间段结束且没有为此对象指定其他放置时自动删除对象。

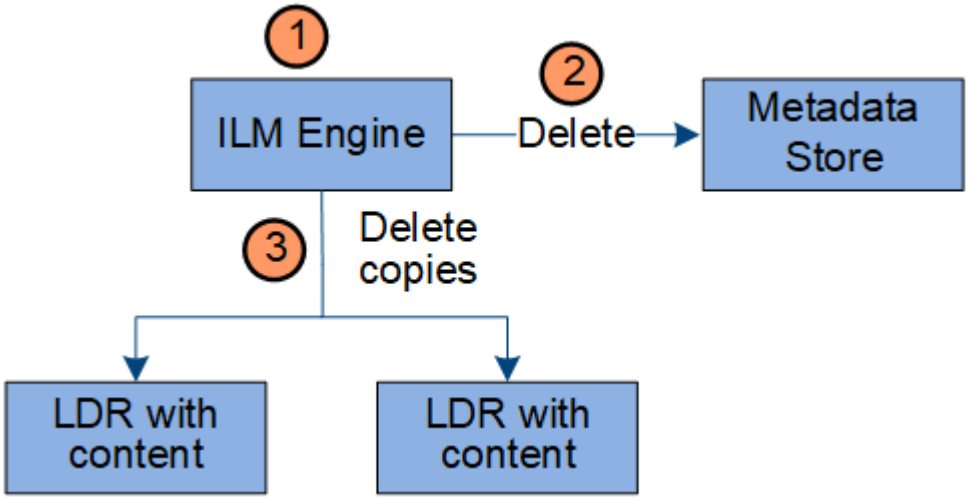
> S3 存储分段生命周期中的到期操作始终会覆盖 ILM 设置。因此，即使有关放置对象的任何 ILM 指令已失效，该对象也可能会保留在网格中。

用于客户端删除的数据流



1. LDR 服务从客户端应用程序接收删除请求。
2. LDR 服务会更新元数据存储，使对象在客户端请求时看起来已被删除，并指示 ILM 引擎删除对象数据的所有副本。
3. 对象将从系统中删除。元数据存储已更新，以删除对象元数据。

用于 **ILM** 删除的数据流



1. ILM 引擎确定需要删除此对象。

2. ILM 引擎会通知元数据存储。元数据存储可更新对象元数据，以便在客户端请求中删除此对象。
3. ILM 引擎会删除对象的所有副本。元数据存储已更新，以删除对象元数据。

如何使用 StorageGRID

了解网格管理器

网格管理器是一个基于浏览器的图形界面，可用于配置，管理和监控 StorageGRID 系统。

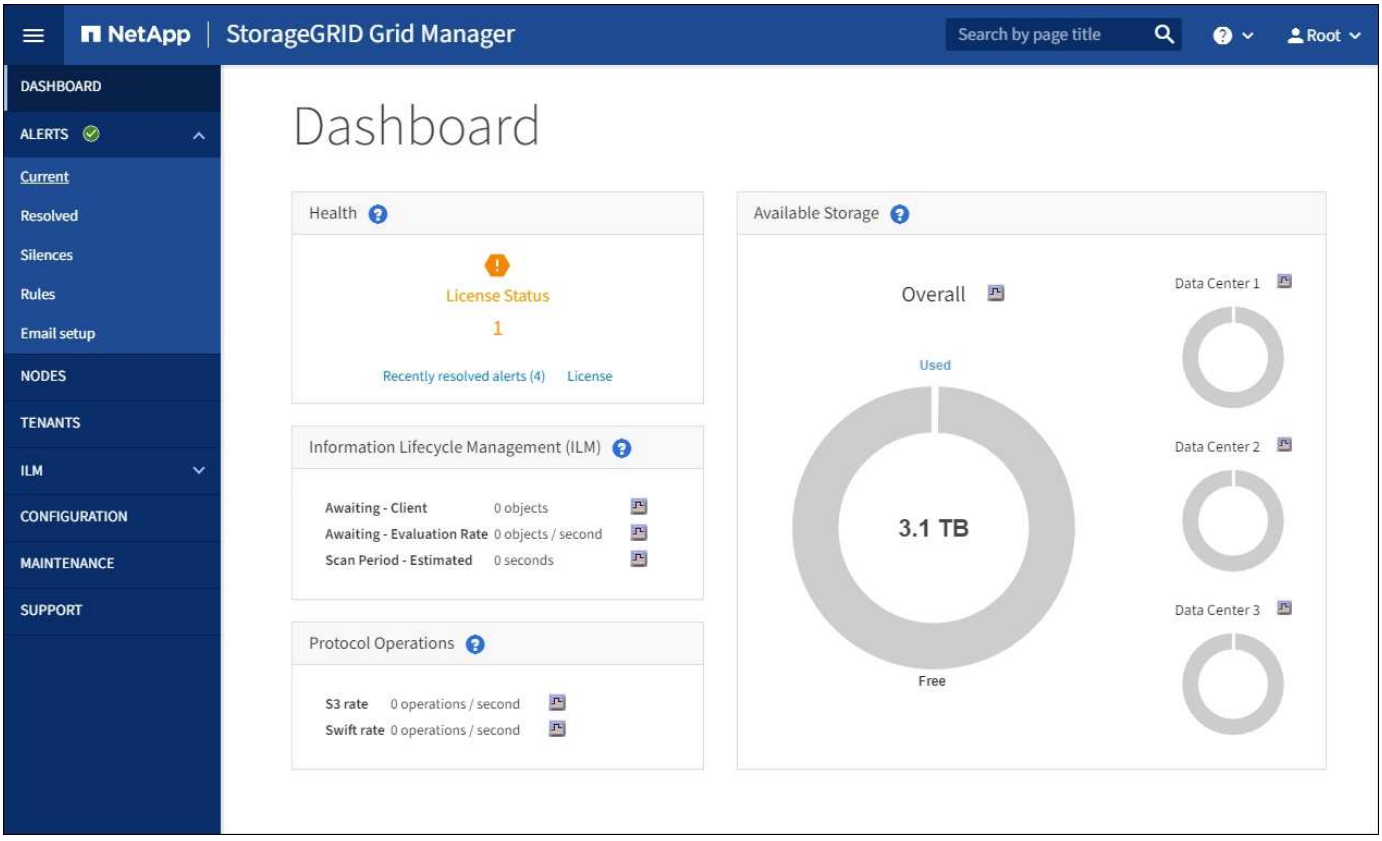
登录到网格管理器后，您将连接到管理节点。每个 StorageGRID 系统都包括一个主管理节点和任意数量的非主管理节点。您可以连接到任何管理节点，每个管理节点都会显示一个类似的 StorageGRID 系统视图。

您可以使用访问网格管理器 支持的 Web 浏览器。

网格管理器信息板

首次登录到网格管理器时，您可以使用信息板一目了然地监控系统活动。

信息板包含有关系统运行状况，存储使用情况， ILM 进程以及 S3 和 Swift 操作的摘要信息。



有关每个面板上信息的说明，请单击帮助图标 。

了解更多信息。

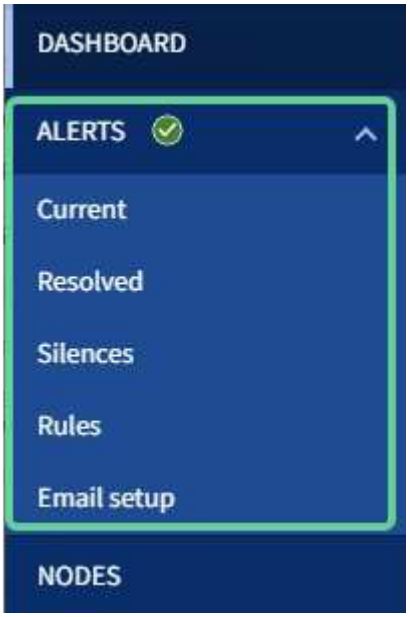
- 监控和故障排除

搜索字段

标题栏中的 * 搜索 * 字段可用于快速导航到网格管理器中的特定页面。例如，您可以输入 * 公里 * 以访问密钥管理服务器（ KMS ）页面。您可以使用 * 搜索 * 在网格管理器的边栏以及配置，维护和支持菜单中查找条目。

警报菜单

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



在警报菜单中，您可以执行以下操作：

- 查看当前警报
- 查看已解决的警报
- 配置静音以禁止警报通知
- 为触发警报的条件定义警报规则
- 为警报通知配置电子邮件服务器

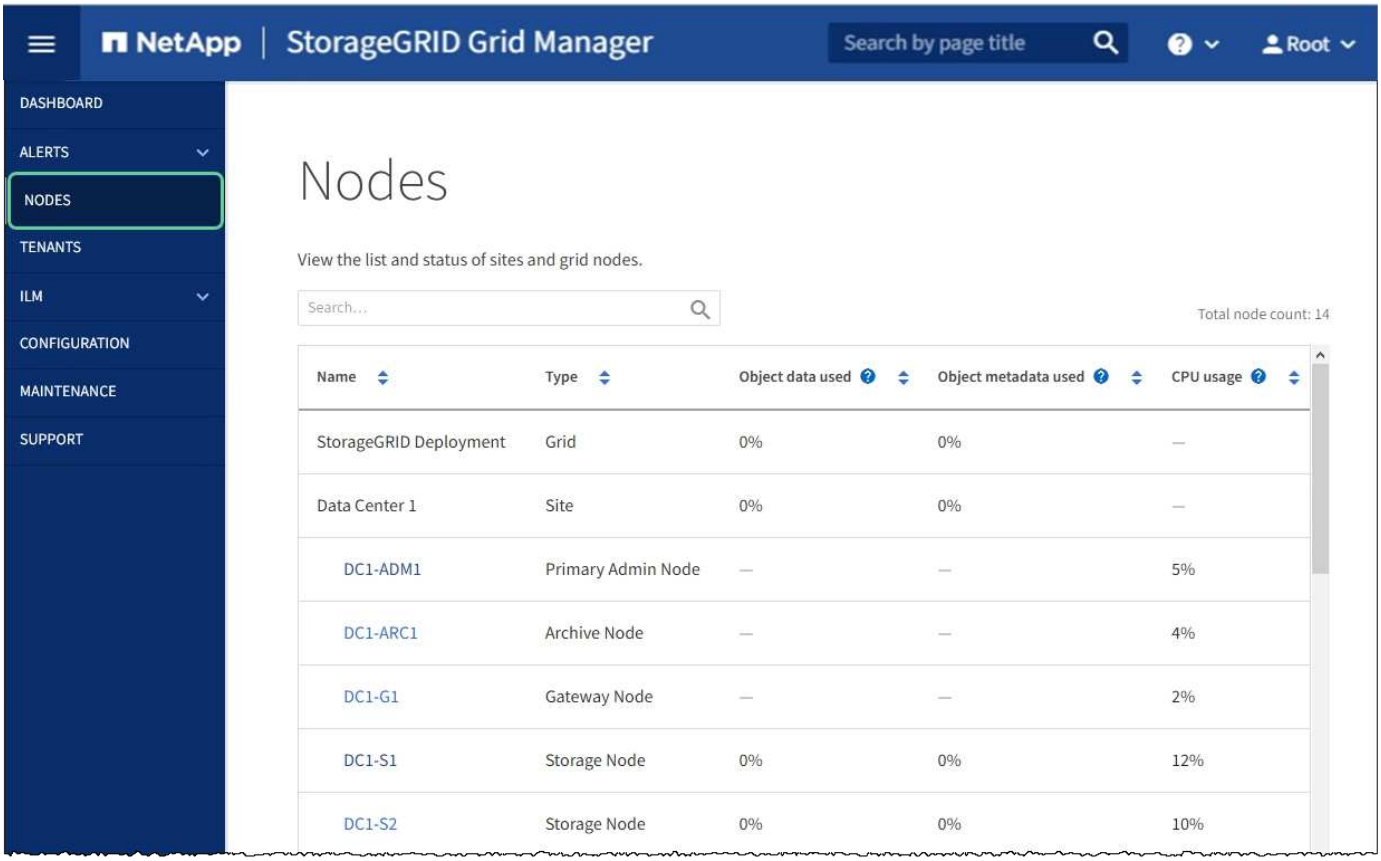
了解更多信息。

- 监控和管理警报
- 监控和故障排除

节点页面

节点页面显示有关整个网格，网格中的每个站点以及站点上的每个节点的信息。

节点主页显示整个网格的组合指标。要查看特定站点或节点的信息，请选择站点或节点。



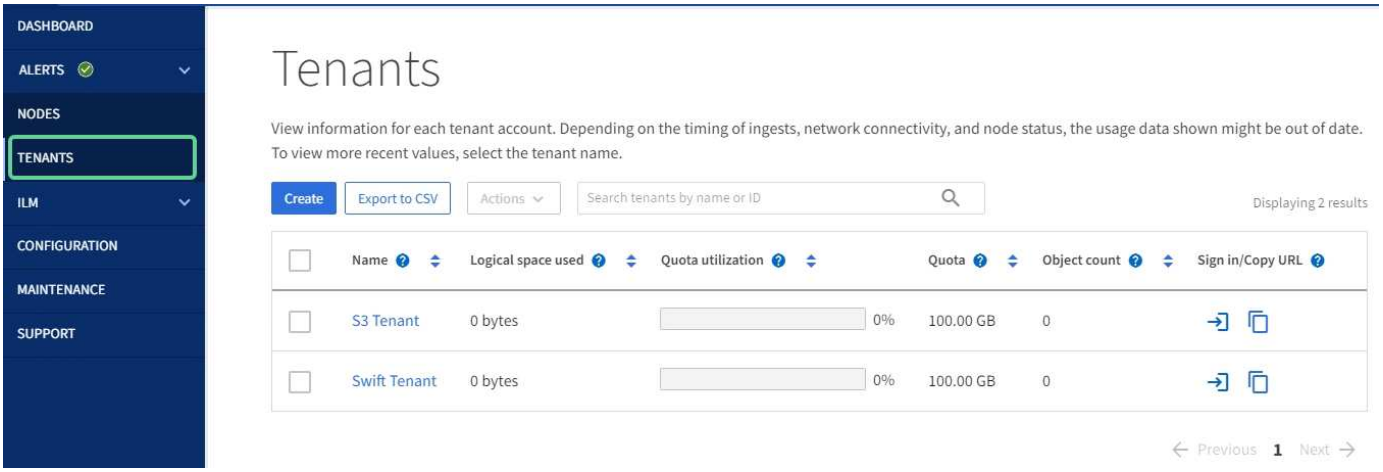
了解更多信息。

- 查看节点页面
- 监控和故障排除

租户页面

通过租户页面，您可以为 StorageGRID 系统创建和监控存储租户帐户。您必须至少创建一个租户帐户，以指定谁可以存储和检索对象以及这些对象可以使用哪些功能。

" 租户 " 页面还提供每个租户的使用情况详细信息，包括已用存储容量和对象数量。如果在创建租户时设置了配额，则可以查看已使用的配额量。



了解更多信息。

- 管理租户和客户端连接
- 管理 StorageGRID
- 使用租户帐户

ILM 菜单

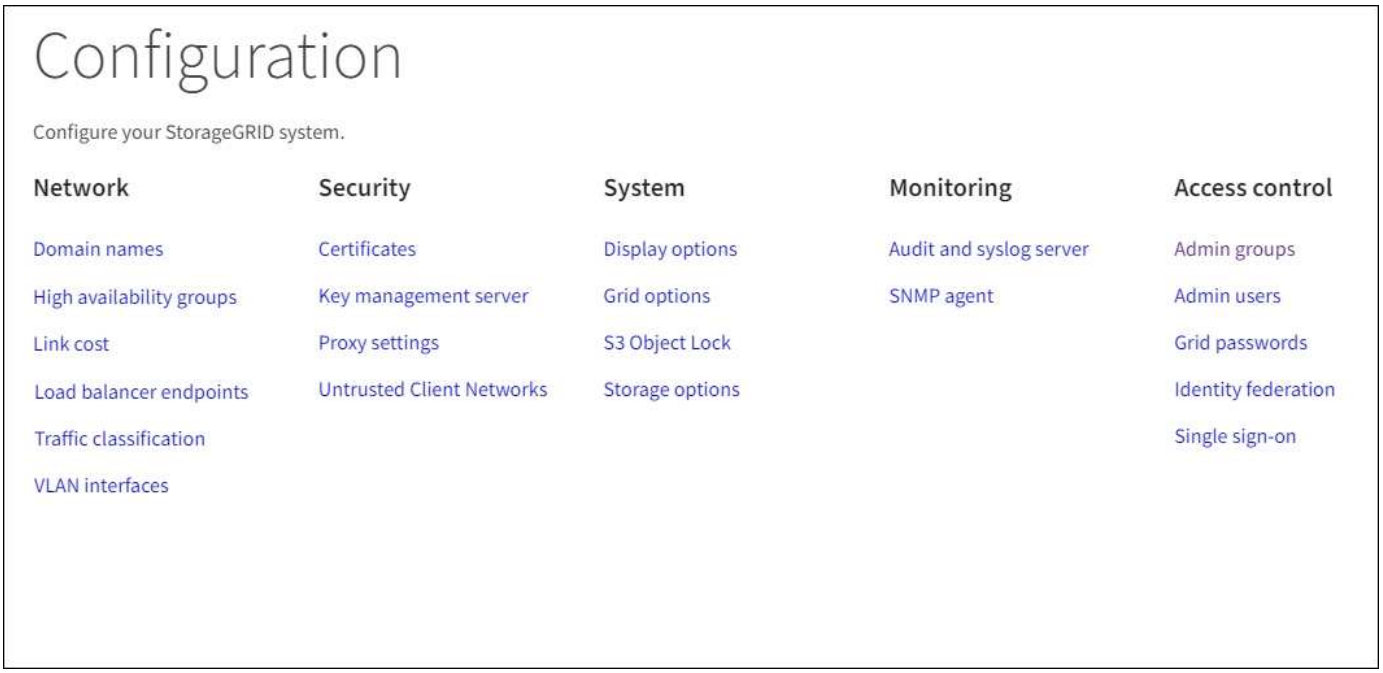
您可以通过 ILM 菜单配置信息生命周期管理（ ILM ）规则和策略，以控制数据的持久性和可用性。您还可以输入对象标识符以查看该对象的元数据。

了解更多信息。

- 使用信息生命周期管理
- 使用 ILM 管理对象

配置菜单

通过配置菜单，您可以指定网络设置，安全设置，系统设置，监控选项和访问控制选项。

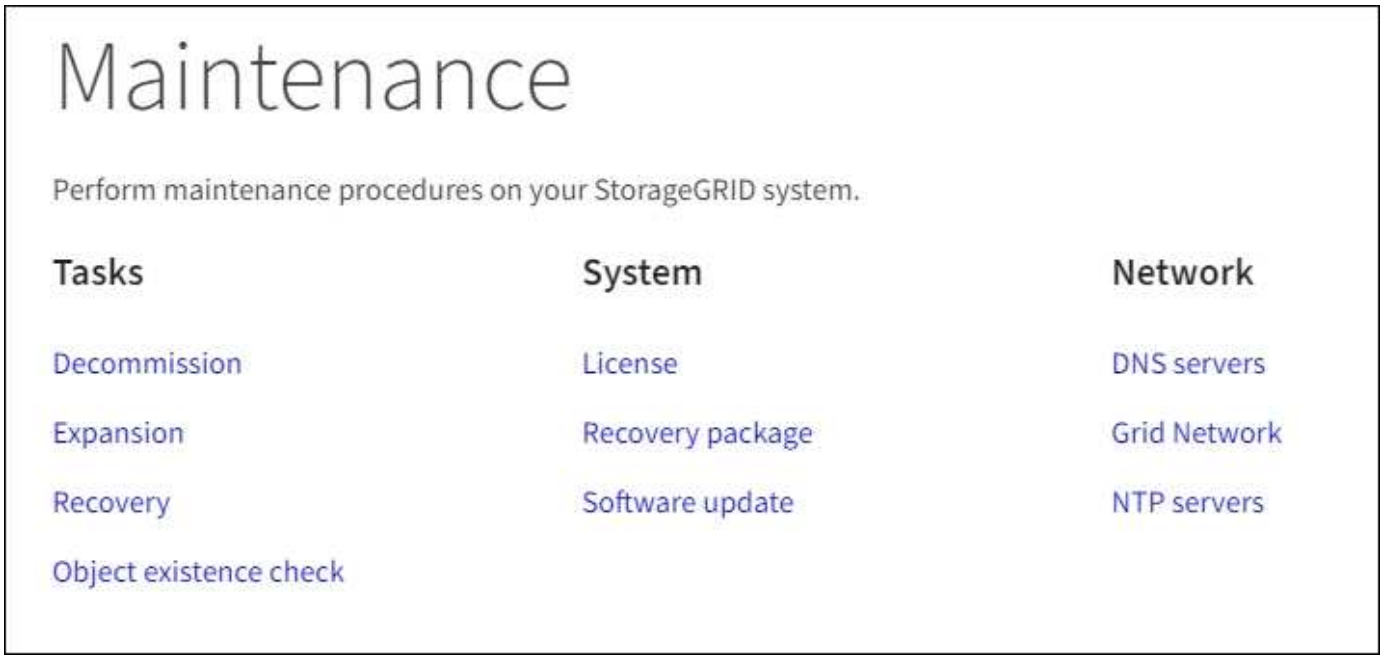


了解更多信息。

- 配置网络设置
- 管理租户和客户端连接
- 查看审核消息
- 控制 StorageGRID 访问
- 管理 StorageGRID
- 监控和故障排除
- 查看审核日志

维护菜单

通过维护菜单，您可以执行维护任务，系统维护和网络维护。



任务

维护任务包括：

- 执行停用操作以删除未使用的网格节点和站点。
- 用于添加新网格节点和站点的扩展操作。
- 用于更换故障节点和还原数据的恢复操作。
- 对象存在检查以验证对象数据是否存在（尽管不是正确）。

系统

您可以执行的系统维护任务包括：

- 查看当前 StorageGRID 许可证的详细信息或上传新许可证。
- 生成恢复包。
- 在选定设备上执行 StorageGRID 软件更新，包括软件升级，修补程序和 SANtricity OS 软件更新。

网络

您可以执行的网络维护任务包括：

- 编辑有关 DNS 服务器的信息。
- 配置网格网络上使用的子网。
- 编辑有关 NTP 服务器的信息。

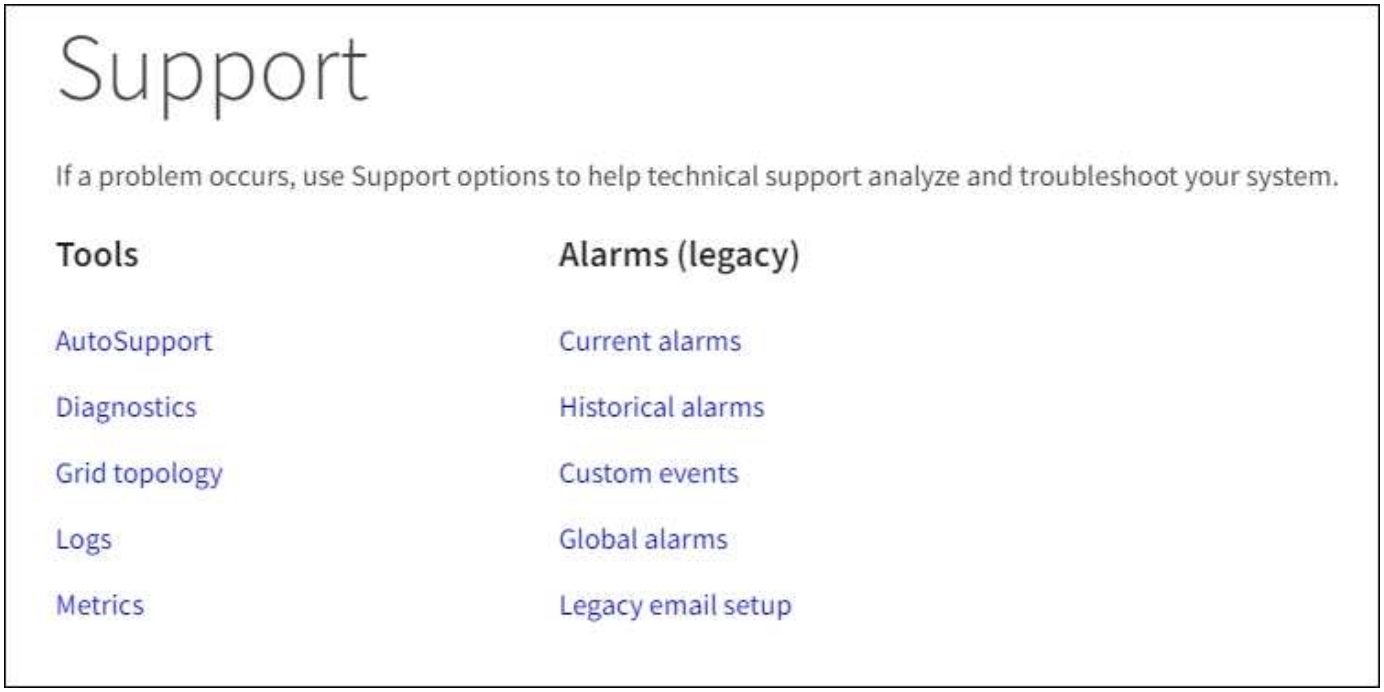
了解更多信息。

- 执行维护
- 下载恢复包

- 扩展网格
- 升级软件
- 恢复和维护
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

支持菜单

" 支持 " 菜单提供了一些选项，可帮助技术支持分析您的系统并对其进行故障排除。支持菜单分为两部分：工具和警报（旧版）。



工具

从支持菜单的工具部分，您可以：

- 启用 AutoSupport 。
- 对网格的当前状态执行一组诊断检查。
- 访问网格拓扑树以查看有关网格节点，服务和属性的详细信息。
- 检索日志文件和系统数据。
- 查看详细指标和图表。

> * 指标 * 选项中提供的工具供技术支持使用。这些工具中的某些功能和菜单项会有意失效。

警报（原有）

从支持菜单的警报（旧）部分，您可以查看当前，历史和全局警报，设置自定义事件以及为旧警报和 AutoSupport 设置电子邮件通知。

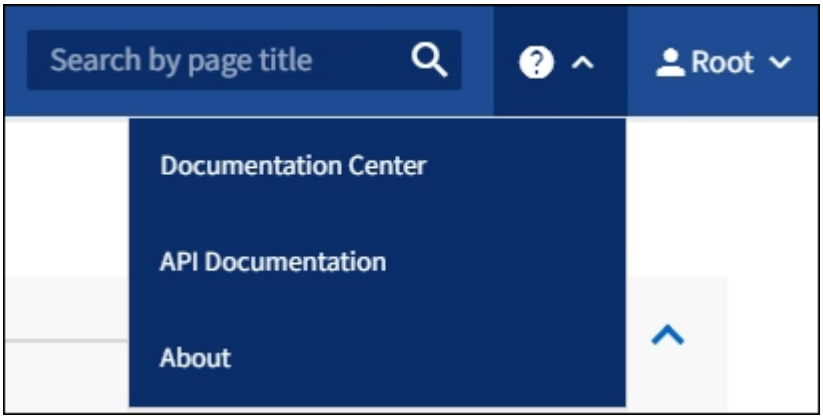
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

了解更多信息。

- StorageGRID 架构和网络拓扑
- StorageGRID 属性
- 使用 StorageGRID 支持选项
- 管理 StorageGRID
- 监控和故障排除

帮助菜单

通过 "Help" 选项，您可以访问当前版本的 StorageGRID 文档中心以及 API 文档。您还可以确定当前安装的 StorageGRID 版本。



了解更多信息。

- 管理 StorageGRID

浏览租户管理器

租户管理器是一个基于浏览器的图形界面，租户用户可以访问它来配置，管理和监控其存储帐户。

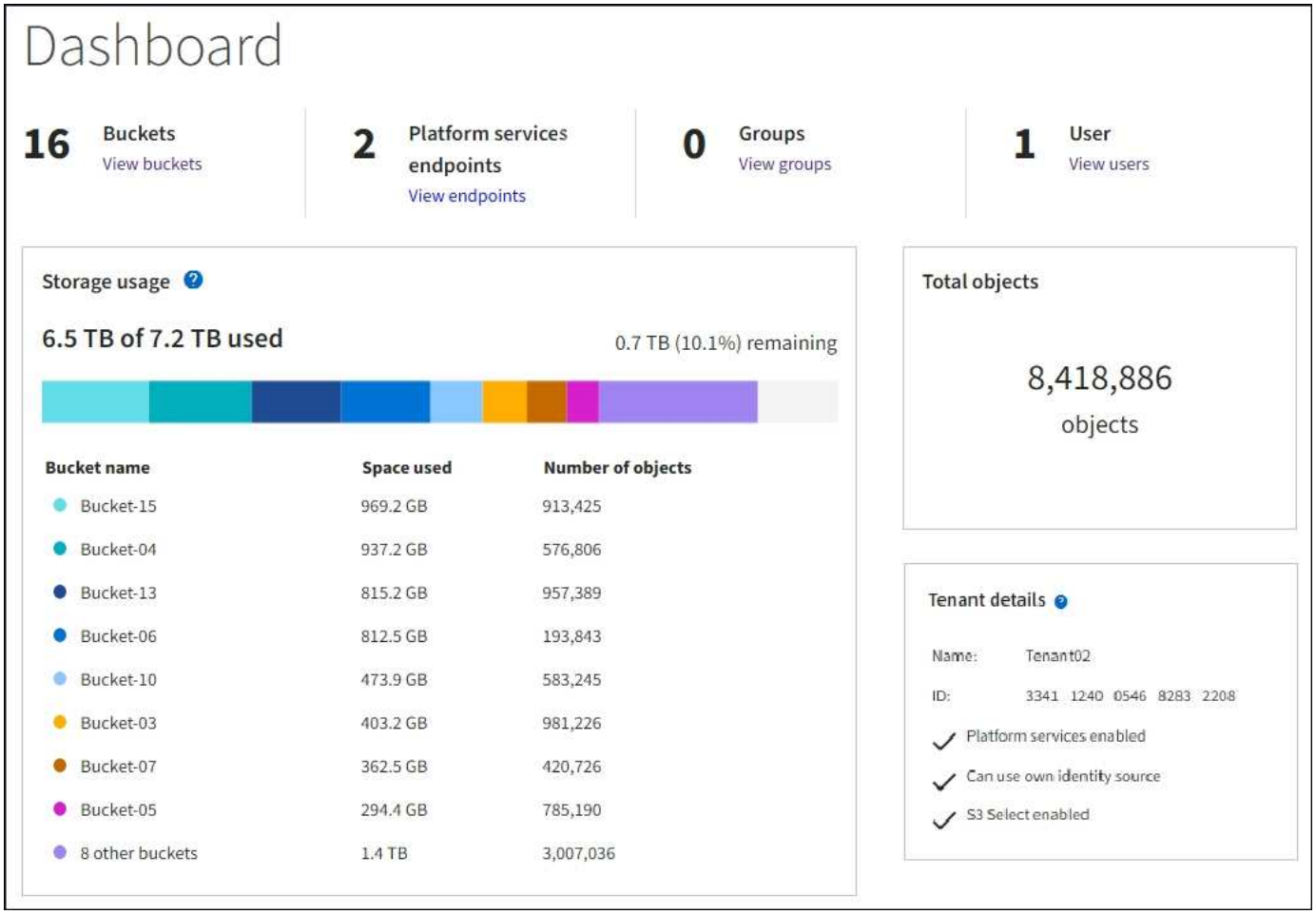
当租户用户登录到租户管理器时，他们将连接到管理节点。

租户管理器信息板

网格管理员使用网格管理器或网格管理 API 创建租户帐户后，租户用户可以登录到租户管理器。

租户管理器信息板允许租户用户一目了然地监控存储使用情况。存储使用情况面板包含租户最大的分段（ S3 ）或容器（ Swift ）列表。已用空间值是分段或容器中的对象数据总量。条形图表示这些分段或容器的相对大小。

条形图上方显示的值是租户的所有分段或容器所用空间的总和。如果在创建帐户时指定了租户可用的最大 GB ，TB 或 PB 数，则还会显示已用配额量和剩余配额量。



存储菜单（仅限 **S3** 租户）

存储菜单仅适用于 S3 租户帐户。此菜单允许 S3 用户管理访问密钥，创建和删除存储分段以及管理平台服务端点。

我的访问密钥

S3 租户用户可以按如下方式管理访问密钥：

- 拥有 " 管理自己的 S3 凭据 " 权限的用户可以创建或删除自己的 S3 访问密钥。

- 具有 root 访问权限的用户可以管理 S3 root 帐户，自己的帐户以及所有其他用户的访问密钥。根访问密钥还可以提供对租户的分段和对象的完全访问权限，除非分段策略明确禁用此功能。

> 可以从 " 访问管理 " 菜单管理其他用户的访问密钥。

存储分段

具有相应权限的 S3 租户用户可以执行以下与存储分段相关的任务：

- 创建存储分段
- 为新存储分段启用 S3 对象锁定（假设已为 StorageGRID 系统启用 S3 对象锁定）
- 更新一致性级别设置
- 应用默认保留设置
- 配置跨源资源共享（ CORS ）
- 为属于租户的分段启用和禁用上次访问时间更新设置
- 删除空分段
- 使用管理存储分段中的对象 S3 控制台处于实验阶段

如果网格管理员为租户帐户启用了平台服务，则具有适当权限的 S3 租户用户也可以执行以下任务：

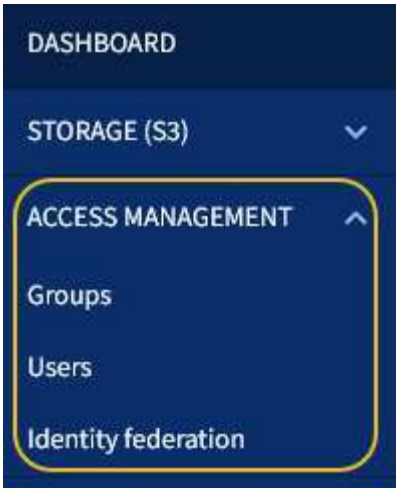
- 配置 S3 事件通知，可将其发送到支持 AWS Simple Notification Service （ SNS ）的目标服务。
- 配置 CloudMirror 复制，从而使租户能够自动将对象复制到外部 S3 存储分段。
- 配置搜索集成，每当创建，删除对象或更新其元数据或标记时，此集成都会将对象元数据发送到目标搜索索引。

平台服务端点

如果网格管理员为租户帐户启用了平台服务，则具有管理端点权限的 S3 租户用户可以为每个平台服务配置目标端点。

访问管理菜单

通过访问管理菜单， StorageGRID 租户可以从联合身份源导入用户组并分配管理权限。租户还可以管理本地租户组和用户，除非对整个 StorageGRID 系统实施单点登录（ Single Sign-On ， SSO ）。



相关信息

- 了解网格管理器
- 使用租户帐户

控制 **StorageGRID** 访问

您可以通过创建或导入组和用户并为每个组分配权限来控制谁可以访问 StorageGRID 以及用户可以执行哪些任务。您也可以选择启用单点登录（ SSO ），创建客户端证书和更改网格密码。

控制对网格管理器的访问

您可以通过从身份联合服务导入组和用户或设置本地组和本地用户来确定谁可以访问网格管理器和网格管理 API 。

使用身份联合可以加快设置组和用户的速度，并允许用户使用熟悉的凭据登录到 StorageGRID 。如果使用 Active Directory ， OpenLDAP 或 Oracle Directory Server ，则可以配置身份联合。

如果要使用其他 LDAP v3 服务，请联系技术支持。

您可以通过为每个组分配不同的权限来确定每个用户可以执行的任务。例如，您可能希望一个组中的用户能够管理 ILM 规则，而另一个组中的用户可以执行维护任务。用户必须至少属于一个组才能访问系统。

您也可以将组配置为只读。只读组中的用户只能查看设置和功能。他们不能在网格管理器或网格管理 API 中进行任何更改或执行任何操作。

启用单点登录

StorageGRID 系统支持使用安全断言标记语言 2.0 （ SAML 2.0 ）标准的单点登录（ SSO ）。启用 SSO 后，所有用户都必须经过外部身份提供程序的身份验证，然后才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用户无法登录到 StorageGRID 。

启用 SSO 后，如果用户登录到 StorageGRID ，则会重定向到您组织的 SSO 页面以验证其凭据。当用户从一个管理节点注销时，他们将自动从所有管理节点中注销。

更改网格密码

许多安装和维护过程以及下载 StorageGRID 恢复软件包都需要配置密码短语。下载 StorageGRID 系统的网格拓扑信息和加密密钥备份时，也需要使用密码短语。您可以根据需要更改此密码短语。

相关信息

- 管理 StorageGRID
- 使用租户帐户

管理租户和客户端连接

作为网格管理员，您可以创建和管理 S3 和 Swift 客户端用于存储和检索对象的租户帐户，并管理控制客户端连接到 StorageGRID 系统的方式的配置选项。

租户帐户

租户帐户允许您指定谁可以使用 StorageGRID 系统存储和检索对象，以及他们可以使用哪些功能。租户帐户允许支持 S3 REST API 或 Swift REST API 的客户端应用程序在 StorageGRID 上存储和检索对象。每个租户帐户都使用 S3 客户端协议或 Swift 客户端协议。

您必须为要用于在 StorageGRID 系统上存储对象的每个客户端协议至少创建一个租户帐户。或者，如果要将系统上存储的对象隔离为不同的实体，则可以创建其他租户帐户。每个租户帐户都有自己的联合或本地组和用户，以及自己的分段（用于 Swift 的容器）和对象。

您可以使用网格管理器或网格管理 API 创建租户帐户。创建租户帐户时，您可以指定以下信息：

- 租户的显示名称（租户的帐户 ID 会自动分配，不能更改）。
- 租户帐户是使用 S3 还是 Swift 。
- 对于 S3 租户帐户：是否允许租户帐户使用平台服务。如果允许使用平台服务，则必须对网格进行配置，以支持使用这些服务。
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。
- 如果为 StorageGRID 系统启用了身份联合，则哪个联合组具有 " 根访问 " 权限来配置租户帐户。
- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。

如果 S3 租户帐户需要符合法规要求，网格管理员可以为 StorageGRID 系统启用全局 S3 对象锁定设置。如果为系统启用了 S3 对象锁定，则所有 S3 租户帐户都可以在启用了 S3 对象锁定的情况下创建存储分段，然后为该存储分段中的对象版本指定保留和合法保留设置。

创建租户帐户后，租户用户可以登录到租户管理器。

客户端与 **StorageGRID** 节点的连接

租户用户必须先确定这些客户端如何连接到 StorageGRID 节点，然后才能使用 S3 或 Swift 客户端在 StorageGRID 中存储和检索数据。

客户端应用程序可以通过连接到以下任一项来存储或检索对象：

- 管理节点或网关节点上的负载平衡器服务。建议使用此连接。
- 网关节点上的 CLB 服务。

  CLB 服务已弃用。

- 存储节点，具有或不具有外部负载平衡器。

在配置 StorageGRID 以使客户端能够使用负载平衡器服务时，您需要执行以下步骤：

1. 也可以配置高可用性（ HA ）组。如果创建 HA 组，则多个管理节点和网关节点的接口将置于主动备份配置中。客户端连接使用 HA 组的虚拟 IP 地址进行。
2. 为负载平衡器服务配置端点。管理节点或网关节点上的负载平衡器服务会将传入的网络连接从客户端应用程序分发到存储节点。创建负载平衡器端点时，您可以指定端口号，端点是否接受 HTTP 或 HTTPS 连接，将使用此端点的客户端类型（ S3 或 Swift ）以及用于 HTTPS 连接的证书（如果适用）。
3. （可选）指定节点的客户端网络不可信，以确保与节点的客户端网络的所有连接都发生在负载平衡器端点上。

相关信息

- 管理 StorageGRID
- 使用租户帐户
- 使用 S3
- 使用 Swift
- 浏览租户管理器
- 配置网络设置

配置网络设置

您可以从网格管理器配置各种网络设置，以微调 StorageGRID 系统的运行。

域名

如果您计划支持 S3 虚拟托管模式请求，则必须配置 S3 客户端连接到的端点域名列表。例如，`s3.example.com` ， `s3.example.co.uk` 和 `s3-east.example.com` 。

配置的服务器证书必须与端点域名匹配。

高可用性组

您可以使用高可用性（ High Availability ， HA ）组为 S3 和 Swift 客户端提供高可用性数据连接，或者为 Grid Manager 和租户管理器提供高可用性连接。

创建 HA 组时，您可以为一个或多个节点选择网络接口。每个 HA 组均可访问选定节点上的共享服务。

- 包括网关节点，管理节点或两者上的接口的 HA 组可为 S3 和 Swift 客户端提供高可用性数据连接。
- 管理节点上包含接口的 HA 组仅提供与网格管理器和租户管理器的高可用性连接。

这些接口可以属于网格网络（ eth0 ），客户端网络（ eth2 ）或 VLAN 网络。

您最多可以为每个 HA 组分配 10 个虚拟 IP （ VIP ）地址。您可以将一个接口指定为主接口，并按优先级顺序对任何其他接口进行排名。主接口是活动接口，除非发生故障。如果活动接口发生故障， VIP 地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。

链路成本

您可以调整链路成本以反映站点之间的延迟。如果存在两个或更多数据中心站点，则链路成本会优先考虑应由哪个数据中心站点提供请求的服务。

负载平衡器端点

您可以使用负载平衡器处理从 S3 和 Swift 客户端载入和检索工作负载。负载平衡通过在多个存储节点之间分布工作负载和连接来最大限度地提高速度和连接容量。

如果要使用管理节点和网关节点上包含的 StorageGRID 负载平衡器服务，则必须配置一个或多个负载平衡器端点。每个端点都为 S3 和 Swift 向存储节点发出的请求定义了一个网关节点或管理节点端口。

流量分类

您可以创建流量分类策略来识别和处理不同类型的网络流量，包括与特定分段，租户，客户端子网或负载平衡器端点相关的流量。这些策略有助于限制和监控流量。

VLAN 接口

您可以创建虚拟 LAN （ VLAN ）接口来隔离流量并对流量进行分区，以提高安全性，灵活性和性能。每个 VLAN 接口都与管理节点和网关节点上的一个或多个父接口相关联。您可以在 HA 组和负载平衡器端点中使用 VLAN 接口，按应用程序或租户隔离客户端或管理流量。

例如，您的网络可能使用 VLAN 100 传输 FabricPool 流量，而使用 VLAN 200 传输归档应用程序。

相关信息

- 管理 StorageGRID
- 管理租户和客户端连接

配置安全设置

您可以从网格管理器配置各种安全设置，以帮助保护 StorageGRID 系统。

证书

StorageGRID 使用两种类型的安全证书：

- 使用 HTTPS 连接时需要服务器证书。服务器证书用于在客户端和服务器之间建立安全连接，向客户端验证服务器的身份并为数据提供安全通信路径。服务器和客户端都有一个证书副本。
- 客户端证书用于向服务器验证客户端或用户身份，从而提供比单独使用密码更安全的身份验证。客户端证书不会对数据进行加密。

您可以在 * 配置 * > * 安全性 * > * 证书 * 页面上查看所有 StorageGRID 证书。

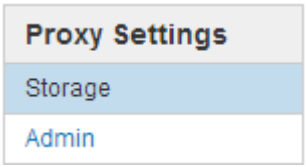
密钥管理服务器

您可以配置一个或多个外部密钥管理服务器（ KMS ），以便为 StorageGRID 服务和存储设备提供加密密钥。每个 KMS 或 KMS 集群都使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为关联 StorageGRID 站点上的设备节点提供一个加密密钥。使用密钥管理服务器可以保护 StorageGRID 数据，即使设备已从数据中心中删除也是如此。对设备卷进行加密后，除非节点可以与 KMS 通信，否则无法访问设备上的任何数据。

要使用加密密钥管理，必须在安装期间为每个设备启用 * 节点加密 * 设置，然后才能将该设备添加到网格中。

代理设置

如果您使用的是 S3 平台服务或云存储池，则可以在存储节点和外部 S3 端点之间配置非透明代理服务器。如果使用 HTTPS 或 HTTP 发送 AutoSupport 消息，则可以在管理节点和技术支持之间配置非透明代理服务器。



不可信的客户端网络

如果您使用的是客户端网络，则可以通过指定每个节点上的客户端网络不可信来帮助保护 StorageGRID 免受恶意攻击。如果节点的客户端网络不可信，则节点仅接受显式配置为负载平衡器端点的端口上的入站连接。

例如，您可能希望网关节点拒绝客户端网络上除 HTTPS S3 请求之外的所有入站流量。或者，您可能希望启用来自存储节点的出站 S3 平台服务流量，同时防止客户端网络上与该存储节点的任何入站连接。

相关信息

- 管理 StorageGRID
- 管理租户和客户端连接

配置系统设置

您可以从网格管理器配置各种系统设置，以微调 StorageGRID 系统的运行。

显示选项

通过显示选项，您可以指定用户会话的超时期限，并禁止对原有警报和事件触发的 AutoSupport 消息发送电子邮件通知。

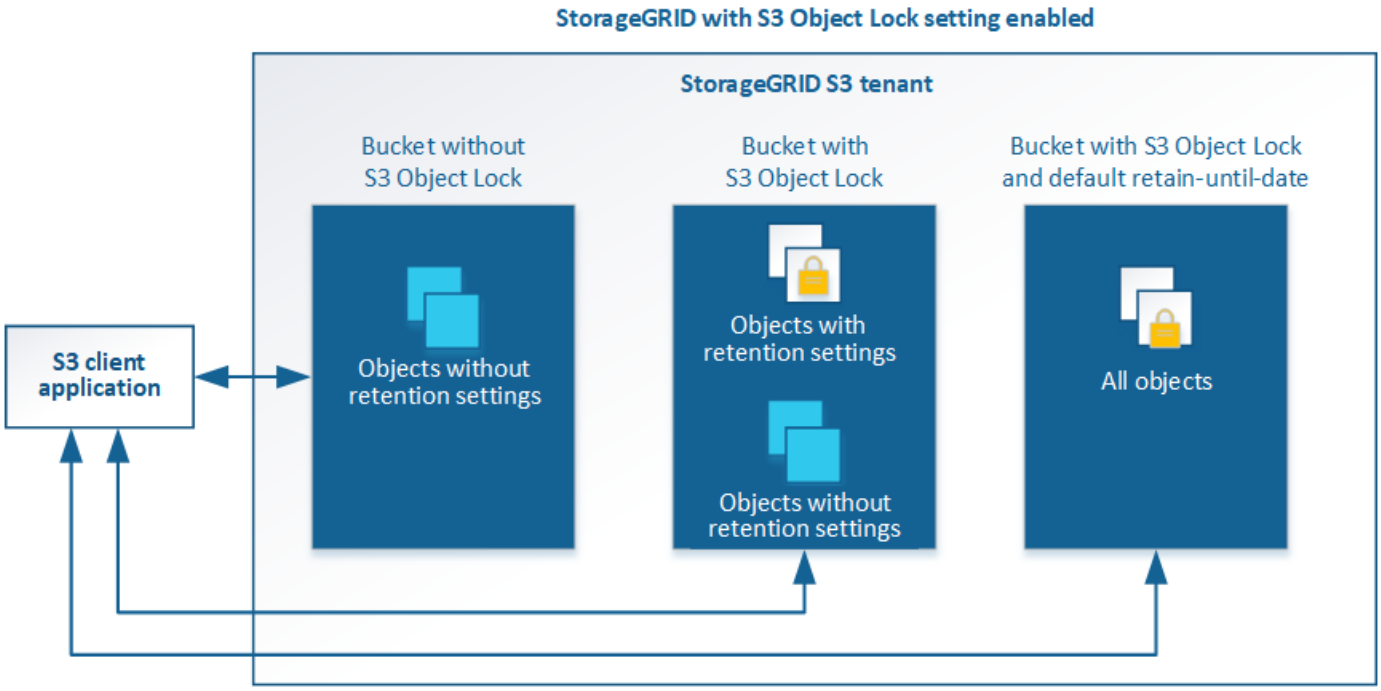
网格选项

您可以使用网格选项为存储在 StorageGRID 系统中的所有对象配置设置，包括存储的对象压缩和存储的对象加密。和存储的对象哈希。

您还可以使用这些选项为 S3 和 Swift 客户端操作指定全局设置。

S3 对象锁定

StorageGRID S3 对象锁定功能是一种对象保护解决方案，相当于 Amazon Simple Storage Service （ Amazon S3 ）中的 S3 对象锁定。您可以为 StorageGRID 系统启用全局 S3 对象锁定设置，以允许 S3 租户帐户在启用了 S3 对象锁定的情况下创建分段。然后，租户可以使用 S3 客户端应用程序为这些分段中的对象指定保留设置（保留到日期，合法保留或同时指定这两者）。此外，启用了 S3 对象锁定的每个存储分段也可以选择具有默认保留模式和保留期限，如果在没有自身保留设置的情况下将对象添加到存储分段，则此模式和保留期限适用。



存储选项

通过存储选项，您可以控制对象分段并覆盖存储卷水印设置，以管理存储节点的可用存储空间。

使用信息生命周期管理

您可以使用信息生命周期管理（ ILM ）来控制 StorageGRID 系统中所有对象的放置，持续时间和数据保护。ILM 规则可确定 StorageGRID 在一段时间内如何存储对象。您可以配置一个或多个 ILM 规则，然后将其添加到 ILM 策略中。

ILM 规则定义：

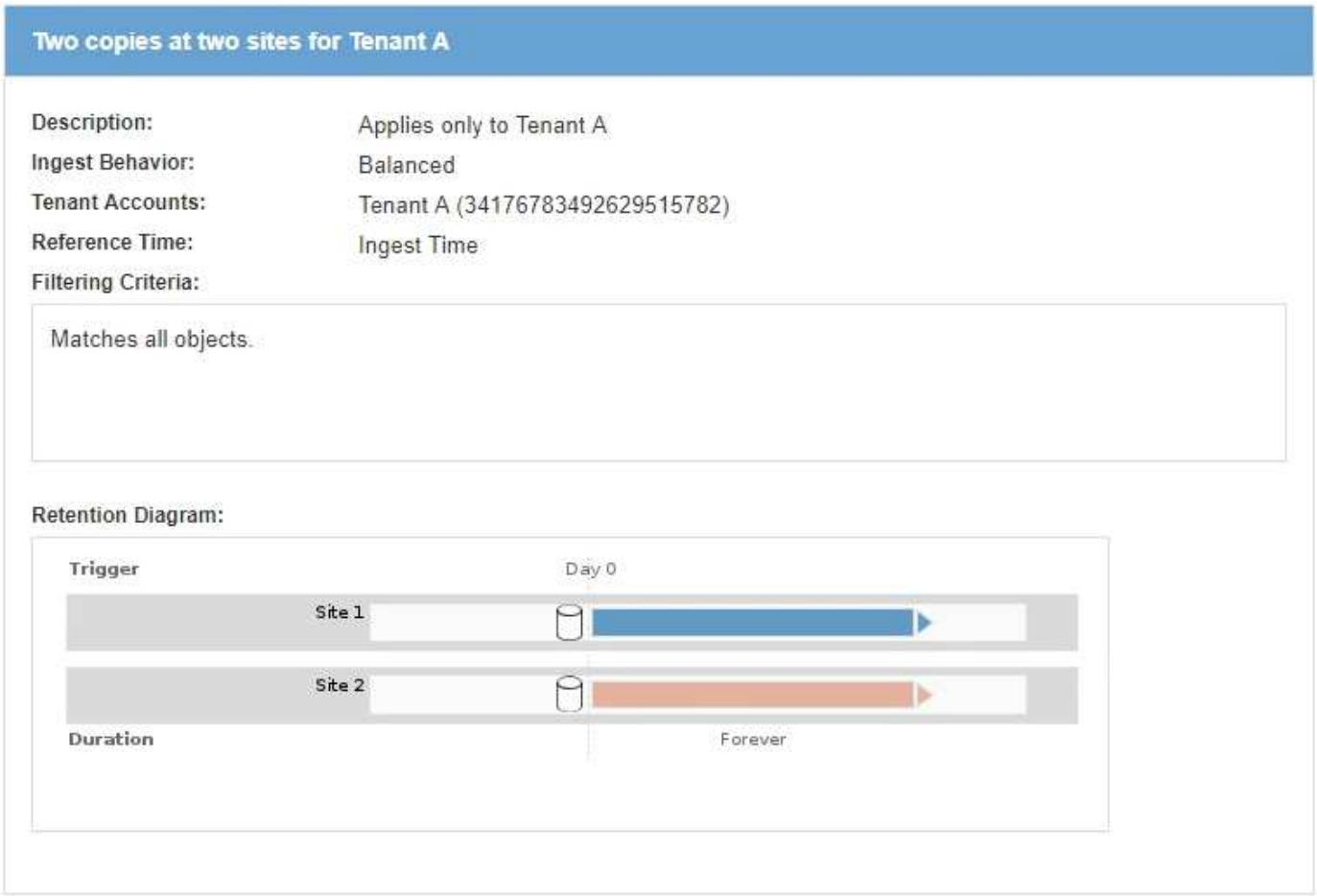
- 应存储哪些对象。规则可以应用于所有对象，也可以指定筛选器来标识规则适用场景 中的对象。例如，规则只能应用于与特定租户帐户，特定 S3 分段或 Swift 容器或特定元数据值关联的对象。
- 存储类型和位置。对象可以存储在存储节点，云存储池或归档节点上。
- 创建的对象副本的类型。可以复制副本或对副本进行纠删编码。
- 对于复制的副本，为创建的副本数。
- 对于纠删编码副本，使用纠删编码方案。
- 对象的存储位置和副本类型会随时间发生变化。
- 在将对象载入网格时如何保护对象数据（同步放置或双提交）。

请注意，对象元数据不受 ILM 规则管理。而是将对象元数据存储在 Cassandra 数据库中，该数据库称为元数据存储。每个站点会自动维护三个对象元数据副本，以防止数据丢失。这些副本会均匀分布在所有存储节点上。

ILM 规则示例

此示例 ILM 规则适用场景 属于租户 A 的对象它会为这些对象创建两个复制副本，并将每个副本存储在不同的站点上。这两个副本会保留 "`Forever ，` " ，这意味着 StorageGRID 不会自动删除它们。相反， StorageGRID 将保留这些对象，直到客户端删除请求或存储分段生命周期到期时将其删除为止。

此规则对载入行为使用平衡选项：租户 A 将对象保存到 StorageGRID 后，系统会立即应用双站点放置指令，除非无法立即创建所需的两个副本。例如，如果租户 A 保存对象时无法访问站点 2 ，则 StorageGRID 将在站点 1 的存储节点上创建两个临时副本。一旦站点 2 可用， StorageGRID 就会在该站点创建所需的副本。



ILM 策略如何评估对象

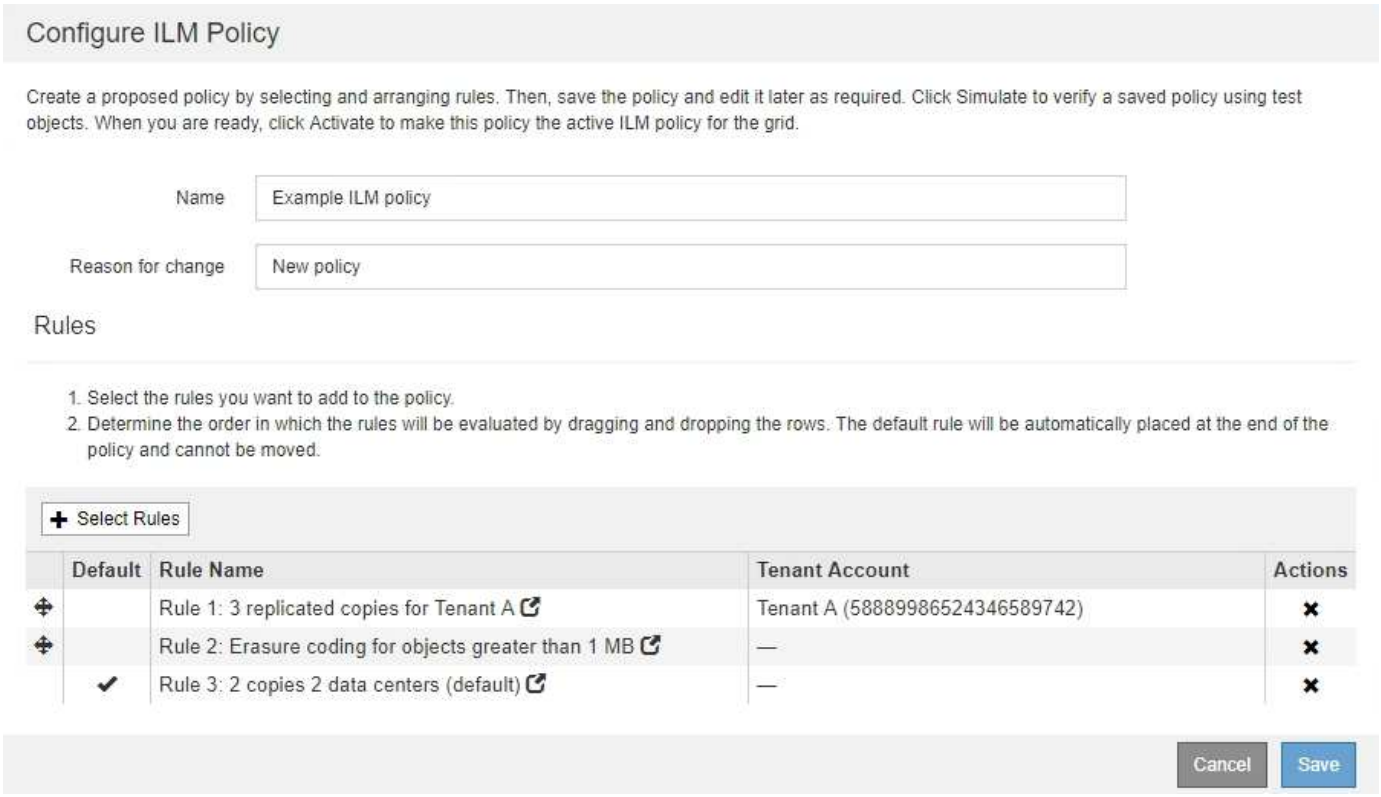
StorageGRID 系统的活动 ILM 策略控制所有对象的放置，持续时间和数据保护。

当客户端将对象保存到 StorageGRID 时，系统会根据活动策略中按顺序排列的一组 ILM 规则对这些对象进行评估，如下所示：

1. 如果策略中第一个规则的筛选器与某个对象匹配，则会根据该规则的载入行为载入该对象，并根据该规则的放置说明进行存储。
2. 如果第一个规则的筛选器与对象不匹配，则会根据策略中的每个后续规则对对象进行评估，直到匹配为止。
3. 如果没有与对象匹配的规则，则会应用策略中默认规则的载入行为和放置说明。默认规则是策略中的最后一条规则，不能使用任何筛选器。它必须应用于所有租户，所有分段和所有对象版本。

ILM 策略示例

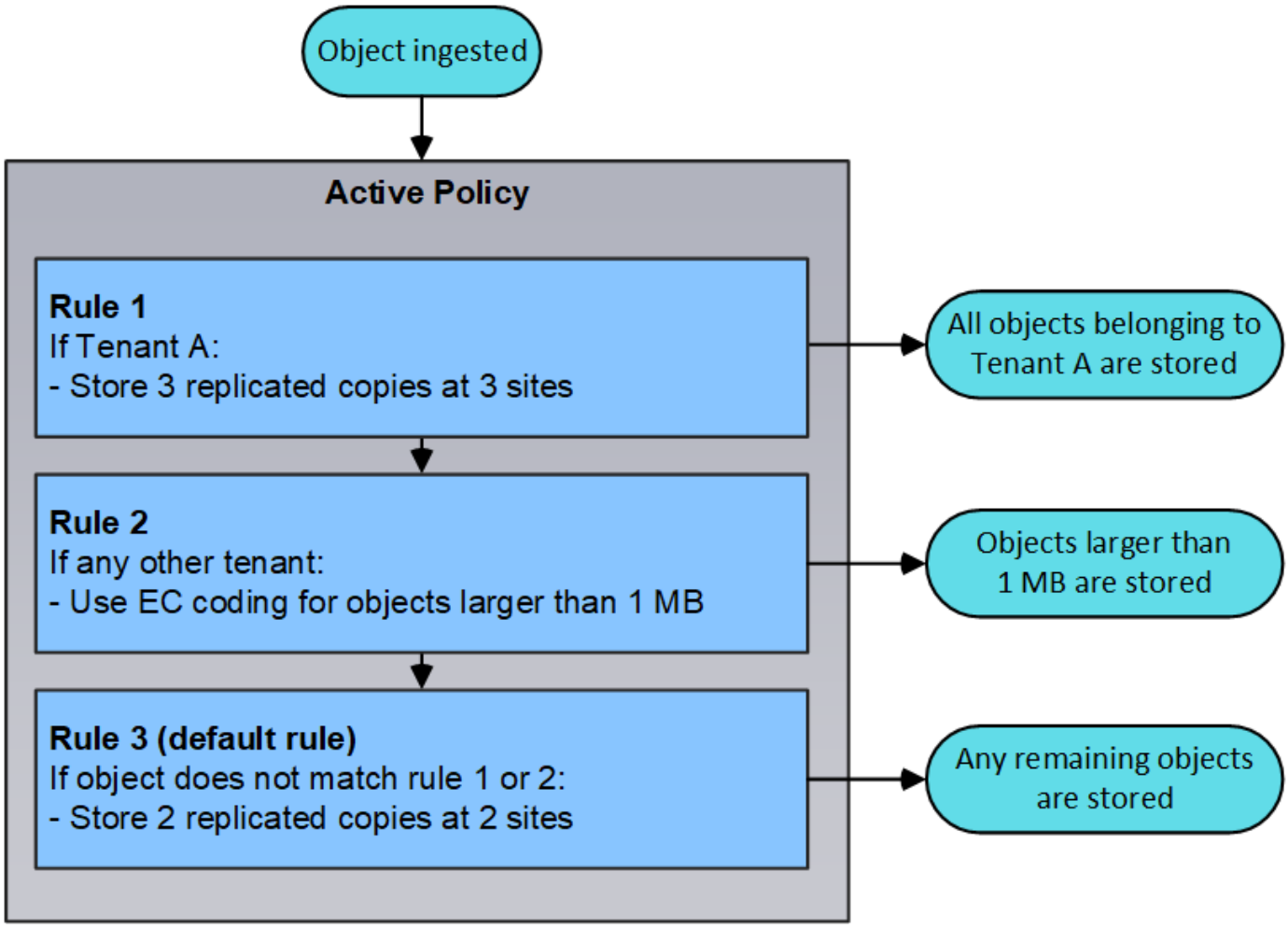
此示例 ILM 策略使用三个 ILM 规则。



在此示例中，规则 1 匹配属于租户 A 的所有对象这些对象会在三个站点上存储为三个复制副本。规则 1 不匹配属于其他租户的对象，因此会根据规则 2 对其进行评估。

规则 2 匹配其他租户的所有对象，但前提是它们大于 1 MB 。这些较大的对象在三个站点上使用 6+3 纠删编码进行存储。规则 2 与 1 MB 或更小的对象不匹配，因此会根据规则 3 评估这些对象。

规则 3 是策略中的最后一条规则和默认规则，不使用筛选器。规则 3 为规则 1 或规则 2 不匹配的所有对象（不属于租户 A 且小于 1 MB 的对象）创建两个复制副本。

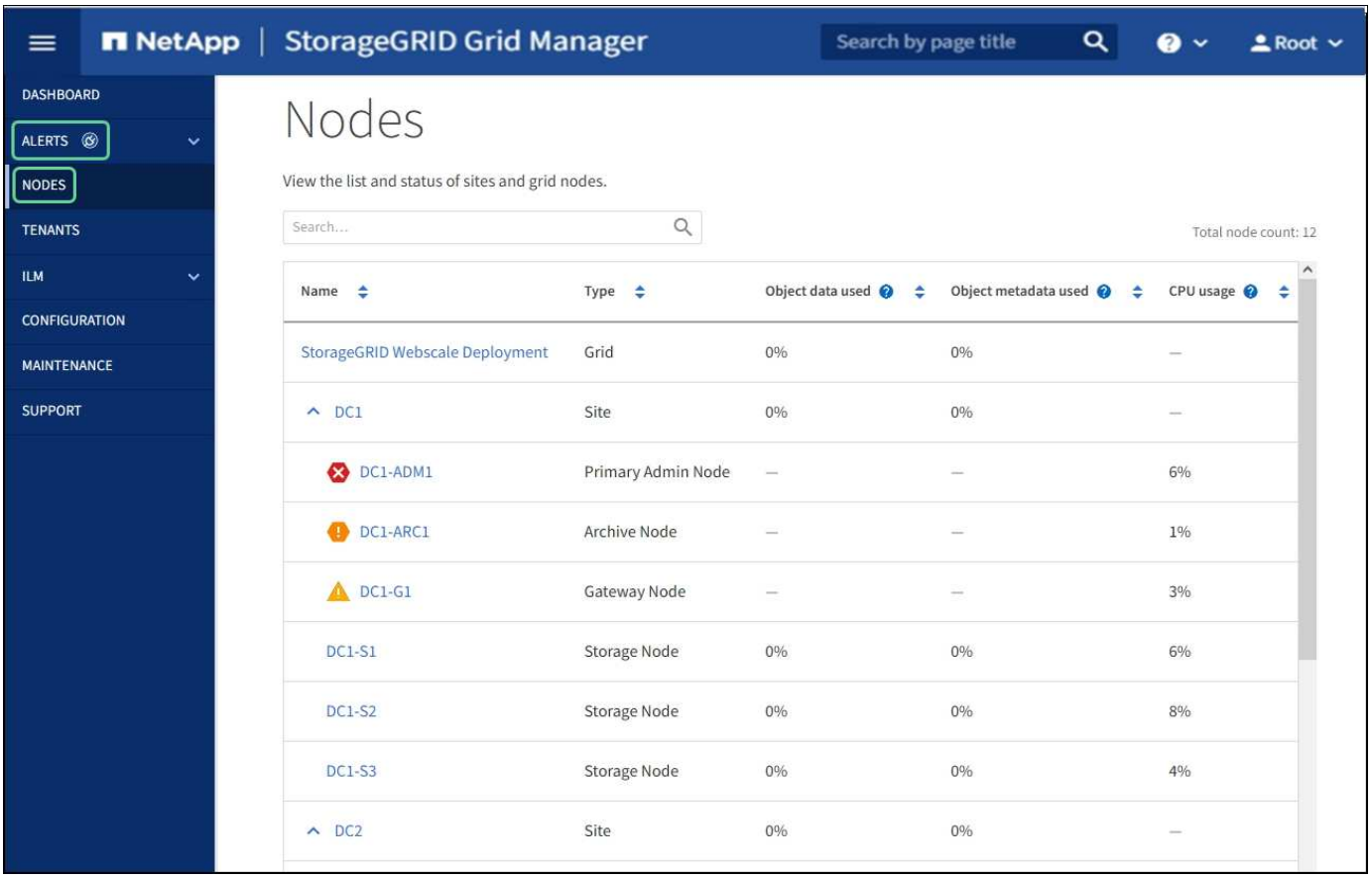


- 相关信息 *
- 使用 ILM 管理对象

监控操作

查看节点页面

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



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

连接状态图标

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

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

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

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

警报图标

如果节点存在活动警报，则节点名称旁边会显示以下图标之一：

- * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。

- * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，

以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。

- * 次要 * ⚠：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运行能力。您应监控和解决自身未清除的小警报，以确保它们不会导致更严重的问题。

系统，站点或节点的详细信息

要查看可用信息，请按如下所示选择网格，站点或节点的名称：

- 选择网格名称可查看整个 StorageGRID 系统统计信息的聚合摘要。（屏幕截图显示了一个名为 StorageGRID 部署的系统。）
- 选择一个特定的数据中心站点，以查看该站点上所有节点的统计信息的聚合摘要。
- 选择一个特定节点以查看该节点的详细信息。

节点页面的选项卡

节点页面顶部的选项卡取决于您从左侧树中选择的内容。

选项卡名称	**Description**	包括的
概述	• 提供有关每个节点的基本信息。 • 显示影响节点的所有活动警报。	所有节点
硬件	• 显示每个节点的 CPU 利用率和内存使用情况 • 对于设备节点，提供了其他硬件信息。	所有节点
网络	显示一个图形，其中显示了通过网络接口接收和发送的网络流量。单个节点的视图显示该节点的追加信息。	所有节点，每个站点和整个网格
存储	• 提供每个节点上的磁盘设备和卷的详细信息。 • 对于存储节点，每个站点和整个网格，均包含显示一段时间内使用的对象数据存储和元数据存储的图形。	所有节点，每个站点和整个网格
对象	• 提供有关 S3 和 Swift 载入和检索速率的信息。 • 对于存储节点，提供对象计数以及有关元数据存储查询和后台验证的信息。	存储节点，每个站点和整个网格

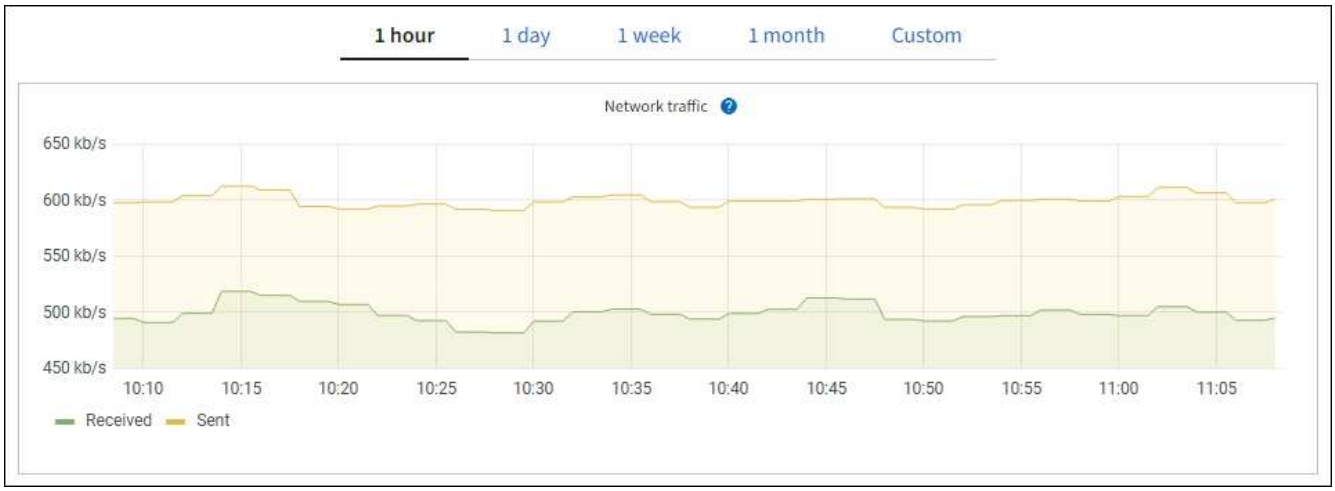
选项卡名称	**Description**	包括的
ILM	提供有关信息生命周期管理（ ILM ）操作的信息。 • 对于存储节点，提供有关纠删编码对象的 ILM 评估和后台验证的详细信息。 • 对于每个站点和整个网格，显示一个 ILM 队列随时间变化的图形。 • 对于整个网格，提供完成对所有对象的完整 ILM 扫描的估计时间。	存储节点，每个站点和整个网格
负载平衡器	包括与负载平衡器服务相关的性能和诊断图。 • 对于每个站点，提供该站点上所有节点的统计信息的聚合摘要。 • 对于整个网格，提供所有站点的统计信息的聚合摘要。	管理节点和网关节点，每个站点和整个网格
平台服务	提供有关站点上任何 S3 平台服务操作的信息。	每个站点
SANtricity 系统管理器	提供对 SANtricity System Manager 的访问权限。在 SANtricity System Manager 中，您可以查看存储控制器的硬件诊断和环境信息以及与驱动器相关的问题。	存储设备节点 注：如果存储设备上的控制器固件早于8.70 (11.70)、则不会显示SANtricity 系统管理器选项卡。

Prometheus 指标

管理节点上的 Prometheus 服务从所有节点上的服务收集时间序列指标。

Prometheus 收集的指标会在网格管理器的许多位置使用：

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



- * 警报 * ： 如果使用 Prometheus 指标的警报规则条件评估为 true ，则会在特定严重性级别触发警报。
- * 网格管理 APi* ： 您可以在自定义警报规则中使用 Prometheus 指标，也可以使用外部自动化工具来监控 StorageGRID 系统。有关完整的 Prometheus 指标列表，请访问网格管理 API 。（从网格管理器的顶部，选择帮助图标并选择 * API Documentation* > * 指标 * 。） 虽然有 1000 多个指标可用，但监控最关键的 StorageGRID 操作只需要相对较少的指标。

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

- * 支持 * > * 工具 * > * 诊断 * 页面和 * 支持 * > * 工具 * > * 指标 * 页面：这些页面主要供技术支持使用，提供了许多工具和图表，这些工具和图表使用了 Prometheus 指标的值。

> 指标页面中的某些功能和菜单项有意不起作用，可能会发生更改。

StorageGRID 属性

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

StorageGRID 属性在网格管理器中的许多位置使用：

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

属性值

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

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

相关信息

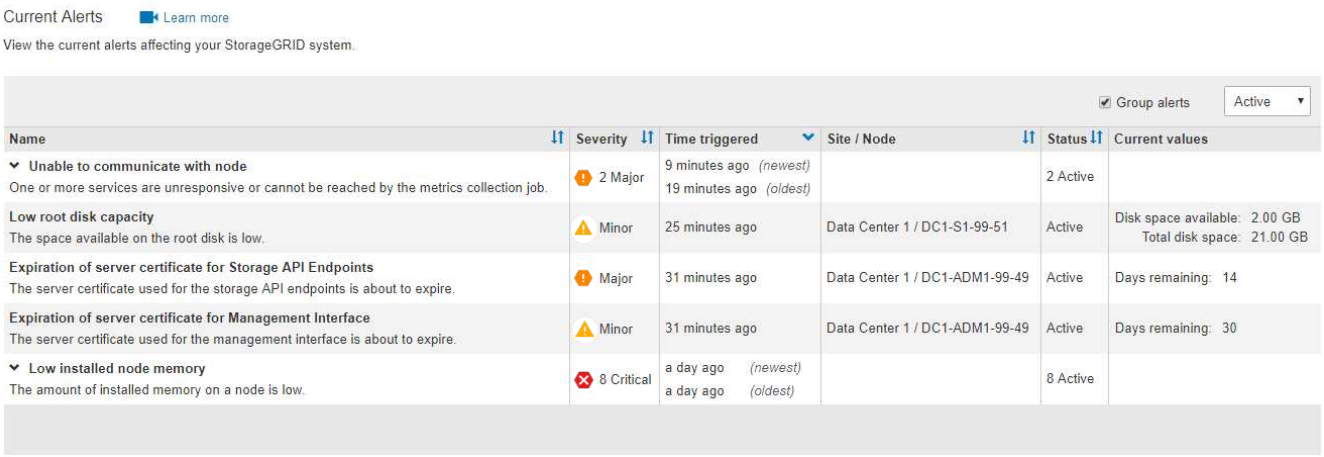
- 监控和故障排除
- 监控和管理警报
- 使用 StorageGRID 支持选项

监控和管理警报

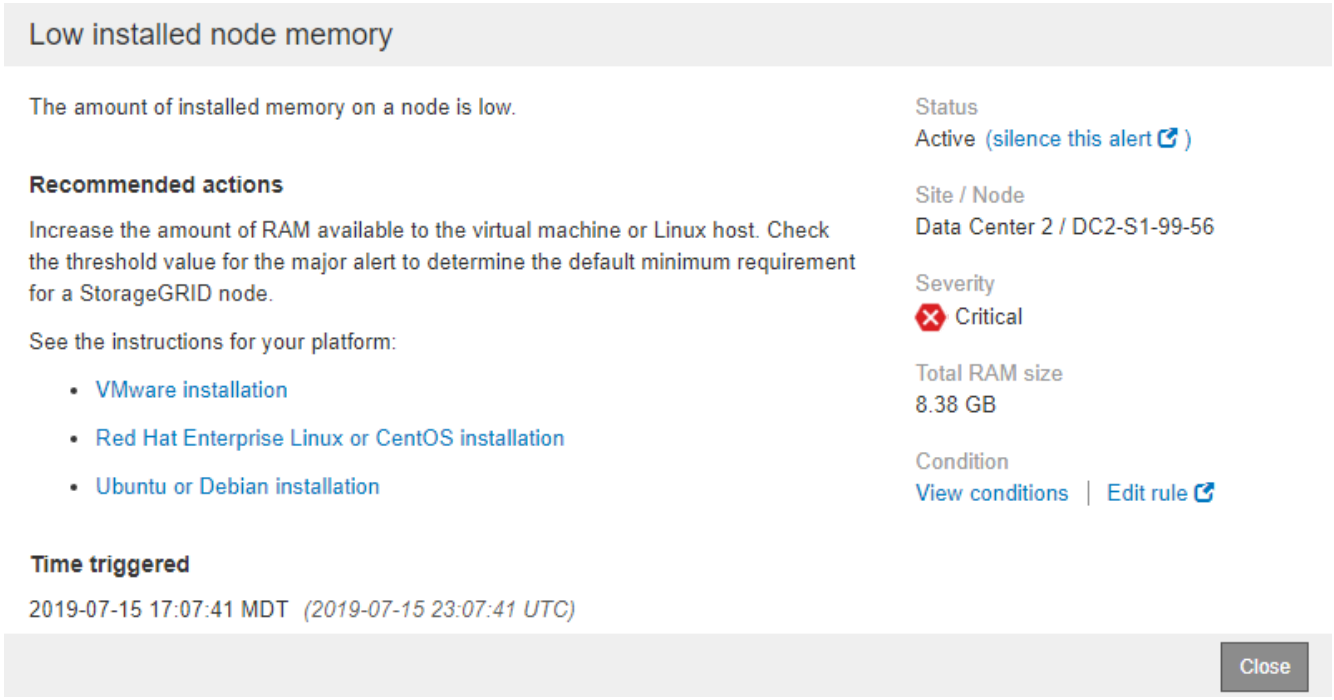
警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

警报系统是用于监控 StorageGRID 系统中可能发生的任何问题的主要工具。

- 警报系统侧重于系统中可操作的问题。对于需要您立即关注的事件，系统会触发警报，而对于可以安全忽略的事件，则不会触发警报。
- " 当前警报 " 和 " 已解决警报 " 页面提供了一个便于用户查看当前和历史问题的界面。您可以按各个警报和警报组对列表进行排序。例如，您可能希望按节点 / 站点对所有警报进行排序，以查看哪些警报正在影响特定节点。或者，您可能希望按触发时间对组中的警报进行排序，以查找特定警报的最新实例。
- 同一类型的多个警报会分组到一个电子邮件中，以减少通知数量。此外，在 " 当前警报 " 和 " 已解决警报 " 页面上，多个相同类型的警报将显示为一个组。您可以展开和折叠警报组以显示或隐藏各个警报。例如，如果多个节点报告 "* 无法与节点 * 通信 " 警报，则只会发送一封电子邮件，并且警报将在 " 当前警报 " 页面上显示为一个组。



- 警报使用直观的名称和说明来帮助您更快地了解问题所在。警报通知包括有关受影响节点和站点的详细信息，警报严重性，触发警报规则的时间以及与警报相关的指标的当前值。
- 警报电子邮件通知以及 " 当前警报 " 和 " 已解决警报 " 页面上的警报列表提供了解决警报的建议操作。这些建议操作通常包括指向 StorageGRID 文档的直接链接，以便于查找和访问更详细的故障排除过程。



旧警报系统已弃用。旧警报系统的用户界面和 API 将在未来版本中删除。警报系统具有显著优势，并且易于使用。

管理警报

所有 StorageGRID 用户均可查看警报。如果您具有 root 访问权限或管理警报权限，则还可以按如下所示管理警报：

- 如果您需要在一个或多个严重性级别临时禁止警报通知，则可以轻松地在指定持续时间内将特定警报规则静默。您可以对整个网格，单个站点或单个节点静默警报规则。
- 您可以根据需要编辑默认警报规则。您可以完全禁用警报规则，也可以更改其触发条件和持续时间。
- 您可以创建自定义警报规则，以确定与您的情况相关的特定条件，并提供您自己的建议操作。要定义自定义警报的条件，请使用网格管理 API 的 " 指标 " 部分提供的 Prometheus 指标创建表达式。

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

```
node_memory_MemTotal < 24000000000
```

相关信息

监控和故障排除

使用 **SNMP** 监控

如果要使用简单网络管理协议（ Simple Network Management Protocol ， SNMP ）监控 StorageGRID ，可以使用网格管理器配置 SNMP 代理。

每个 StorageGRID 节点都运行一个 SNMP 代理或守护进程，该代理或守护进程可提供一个管理信息库（ Management Information Base ， MIB ）。StorageGRID MIB 包含警报和警报的表和通知定义。每个 StorageGRID 节点还支持一组 MIB-II 对象。

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

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

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

在以下情况下会发送陷阱和通知通知通知：

- 默认或自定义警报将在任何严重性级别触发。要禁止警报的 SNMP 通知，您必须为此警报配置静默。警报通知由配置为首选发送方的任何管理节点发送。
- 某些警报（旧系统）会在指定的严重性级别或更高级别触发。

> 不会针对每个警报或每个警报严重性发送 SNMP 通知。

- 相关信息 *
- 监控和故障排除

查看审核消息

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

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

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

每个管理节点都会将审核消息存储在文本文件中。审核共享包含活动文件（ audit.log ）以及前几天压缩的审核日志。此外，网格中的每个节点都会在本地日志文件（ localaudit.log ）中存储有限数量的审核消息。

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

您也可以将存储在管理节点和本地节点上的审核信息发送到外部系统日志服务器。使用外部系统日志服务器可以更轻松地管理审核信息并减少网络流量。请参见 配置审核消息和日志目标 有关详细信息 …

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

相关信息

- 查看审核日志
- 管理 StorageGRID

执行维护

您可以执行各种维护过程来使 StorageGRID 系统保持最新并确保其高效运行。网格管理器提供了一些工具和选项，可帮助您加快执行维护任务的过程。

软件更新

您可以从网格管理器的软件更新页面执行三种类型的软件更新：

- StorageGRID 软件升级
- StorageGRID 热修补程序
- SANtricity 操作系统升级

StorageGRID 软件升级

如果有新的 StorageGRID 功能版本，软件升级页面将指导您完成上传所需文件和升级 StorageGRID 系统的过程。您必须从主管理节点升级所有数据中心站点的所有网格节点。

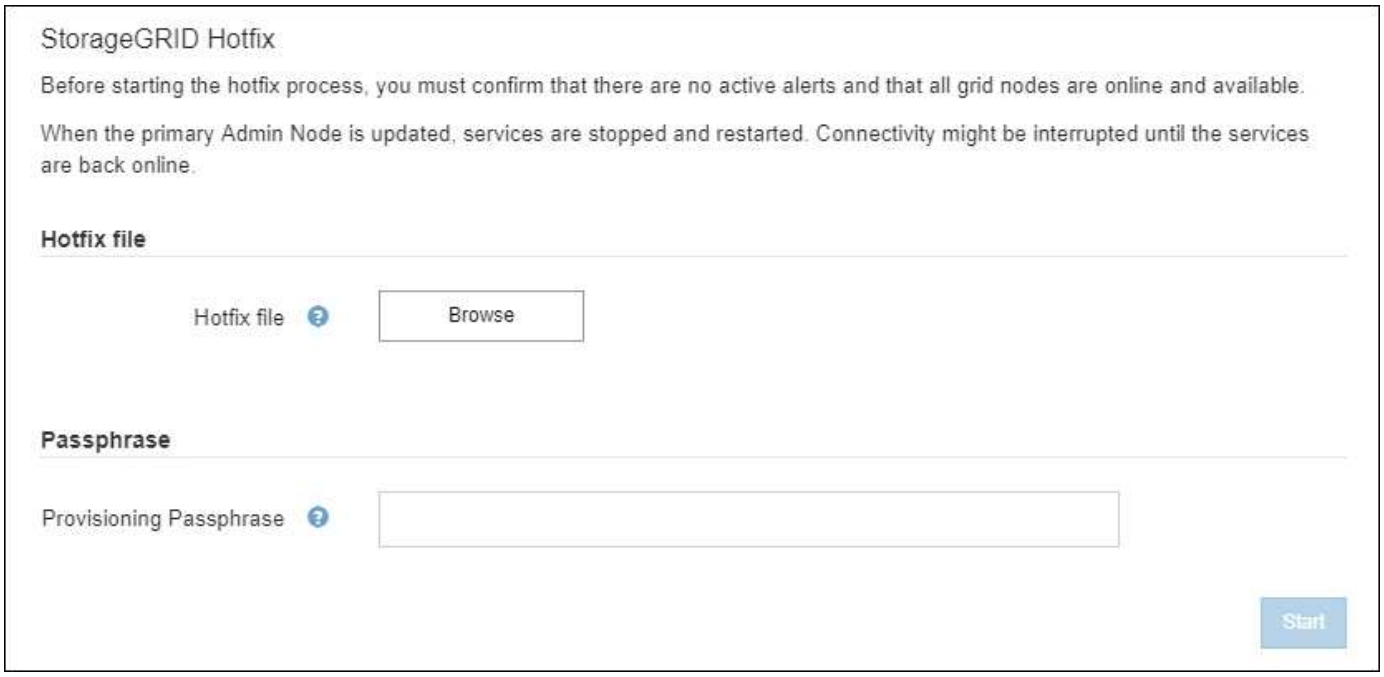
在 StorageGRID 软件升级期间，客户端应用程序可以继续载入和检索对象数据。

修补程序

如果在功能版本之间检测到并解决了软件问题，您可能需要在 StorageGRID 系统中应用修补程序。

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

您可以通过下面所示的 StorageGRID 修复程序页面上传修复程序文件。



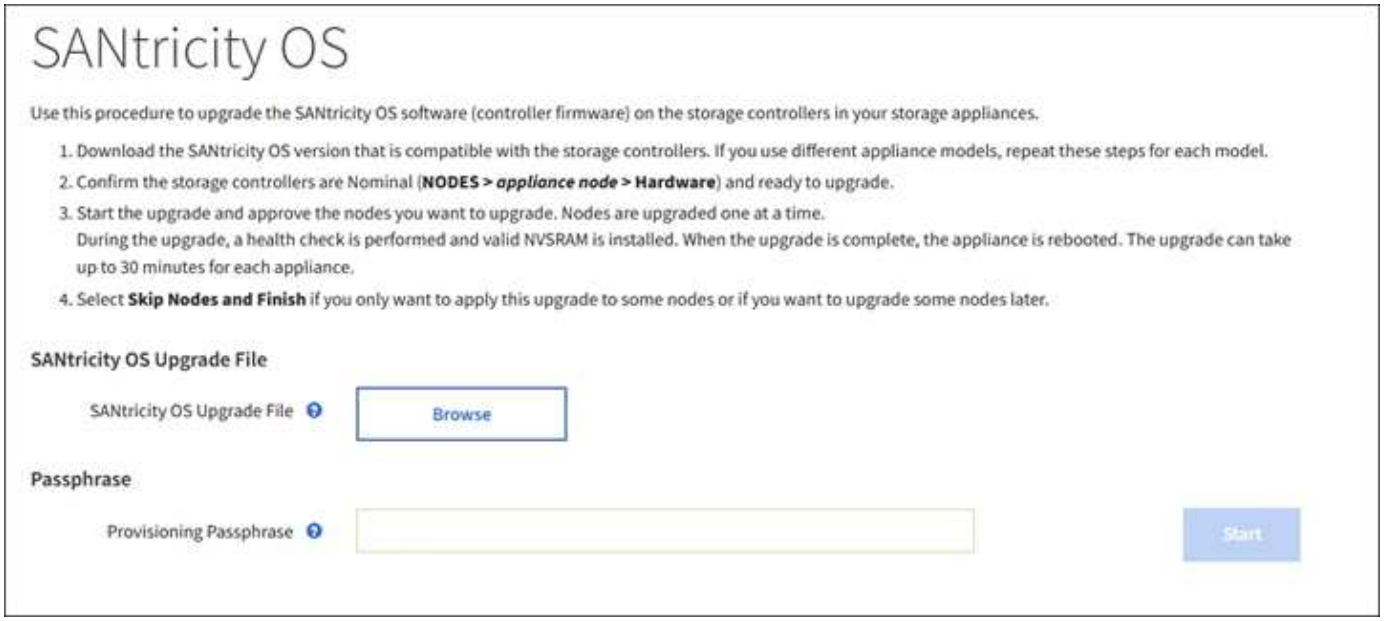
此修补程序会首先应用于主管理节点。然后，您必须批准将此修补程序应用于其他网格节点，直到 StorageGRID 系统中的所有节点运行相同的软件版本为止。您可以通过选择批准单个网格节点，网格节点组或所有网格节点来自定义批准顺序。

虽然所有网格节点都会使用新的修补程序版本进行更新，但修补程序中的实际更改可能仅影响特定类型节点上的特定服务。例如，某个修补程序可能只会影响存储节点上的 LDR 服务。

SANtricity 操作系统升级

如果存储设备的存储控制器运行不正常，您可能需要升级 SANtricity 操作系统软件。您可以将 SANtricity OS 文件上传到 StorageGRID 系统中的主管理节点，并从网格管理器应用升级。

您可以通过下面显示的 SANtricity 页面上传 SANtricity 操作系统升级文件。

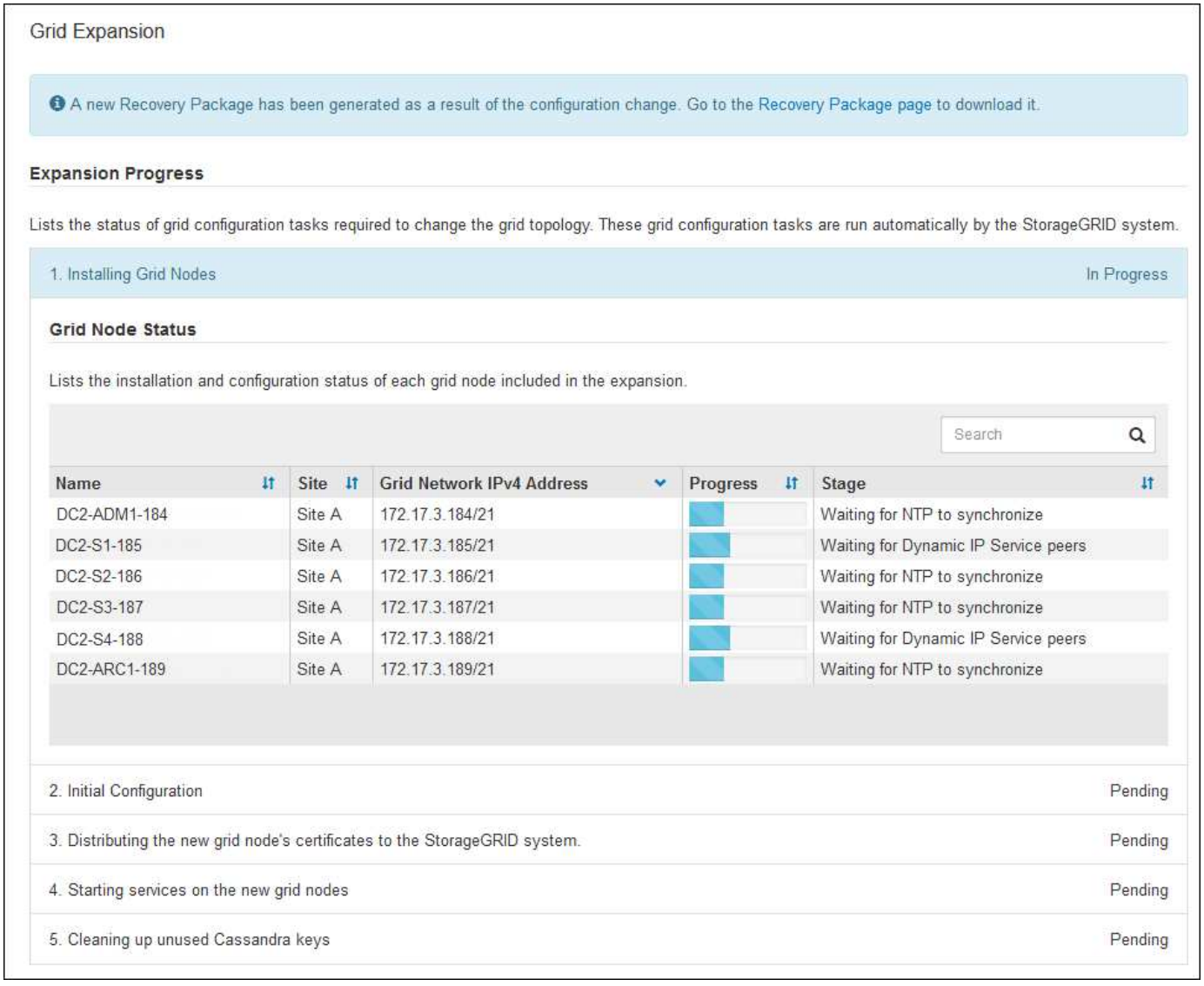


上传文件后，您可以在单个存储节点或所有节点上批准升级。通过有选择地批准节点，您可以更轻松地计划升级。批准升级某个节点后，系统将执行运行状况检查，如果此升级适用于此节点，则会安装此升级。

扩展过程

您可以通过以下方式扩展 StorageGRID 系统：向存储节点添加存储卷，向现有站点添加新的网格节点或添加新的数据中心站点。如果您的存储节点使用SG6060或SG6060X存储设备、则可以添加一个或两个扩展架、使此节点的存储容量增加一倍或三倍。

您可以在不中断当前系统运行的情况下执行扩展。添加节点或站点时，首先部署新节点，然后从网格扩展页面执行扩展操作步骤 。

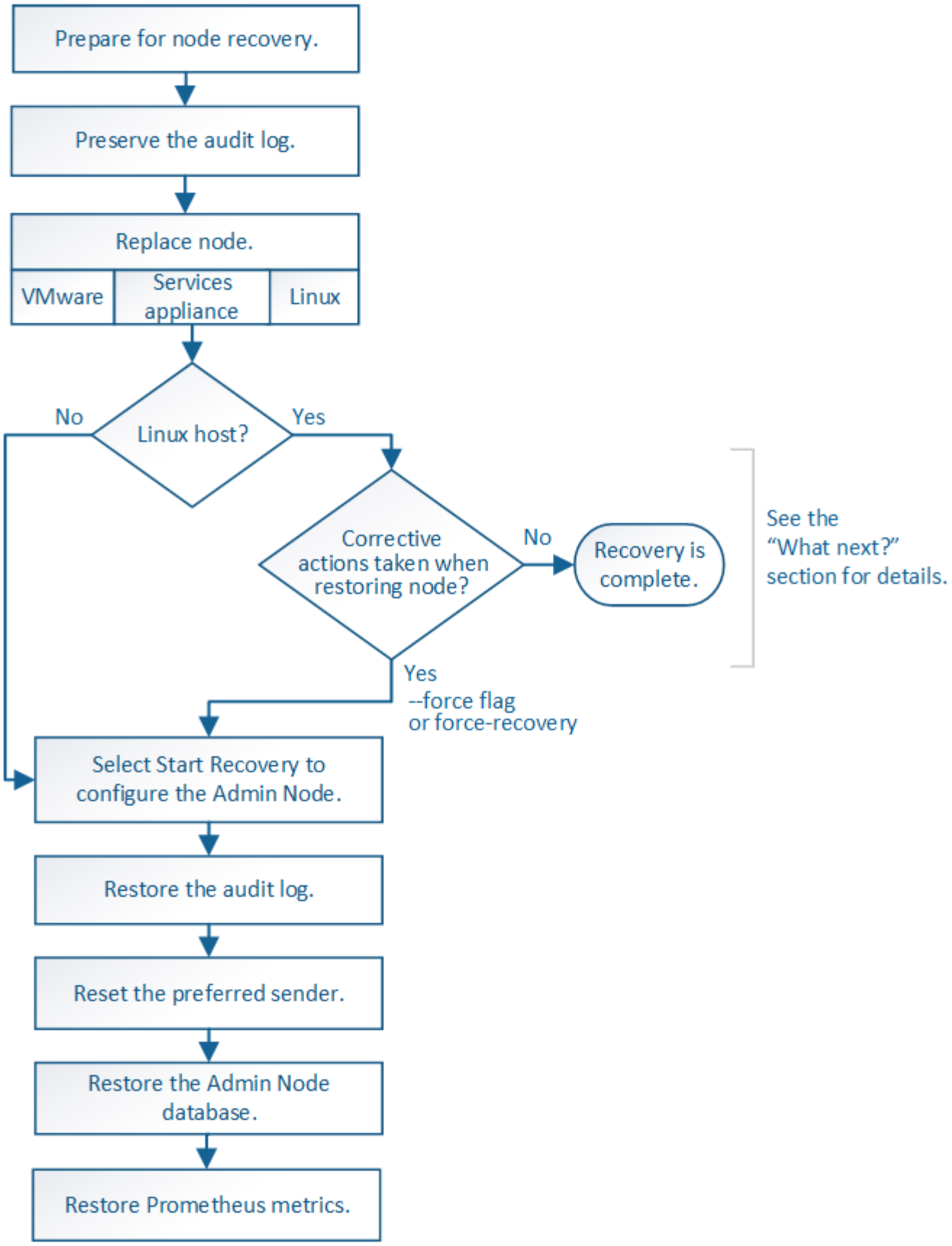


节点恢复过程

如果硬件，虚拟化，操作系统或软件故障导致节点无法运行或不可靠，则网格节点可能会发生故障。

恢复网格节点的步骤取决于托管网格节点的平台以及网格节点的类型。每种类型的网格节点都有一个特定的恢复操作步骤 ，您必须严格遵循该恢复。通常，您会尝试尽可能保留故障网格节点中的数据，修复或更换故障节点，使用 " 恢复 " 页面配置替代节点并还原节点的数据。

例如，此流程图显示管理节点出现故障时的恢复操作步骤 。



停用过程

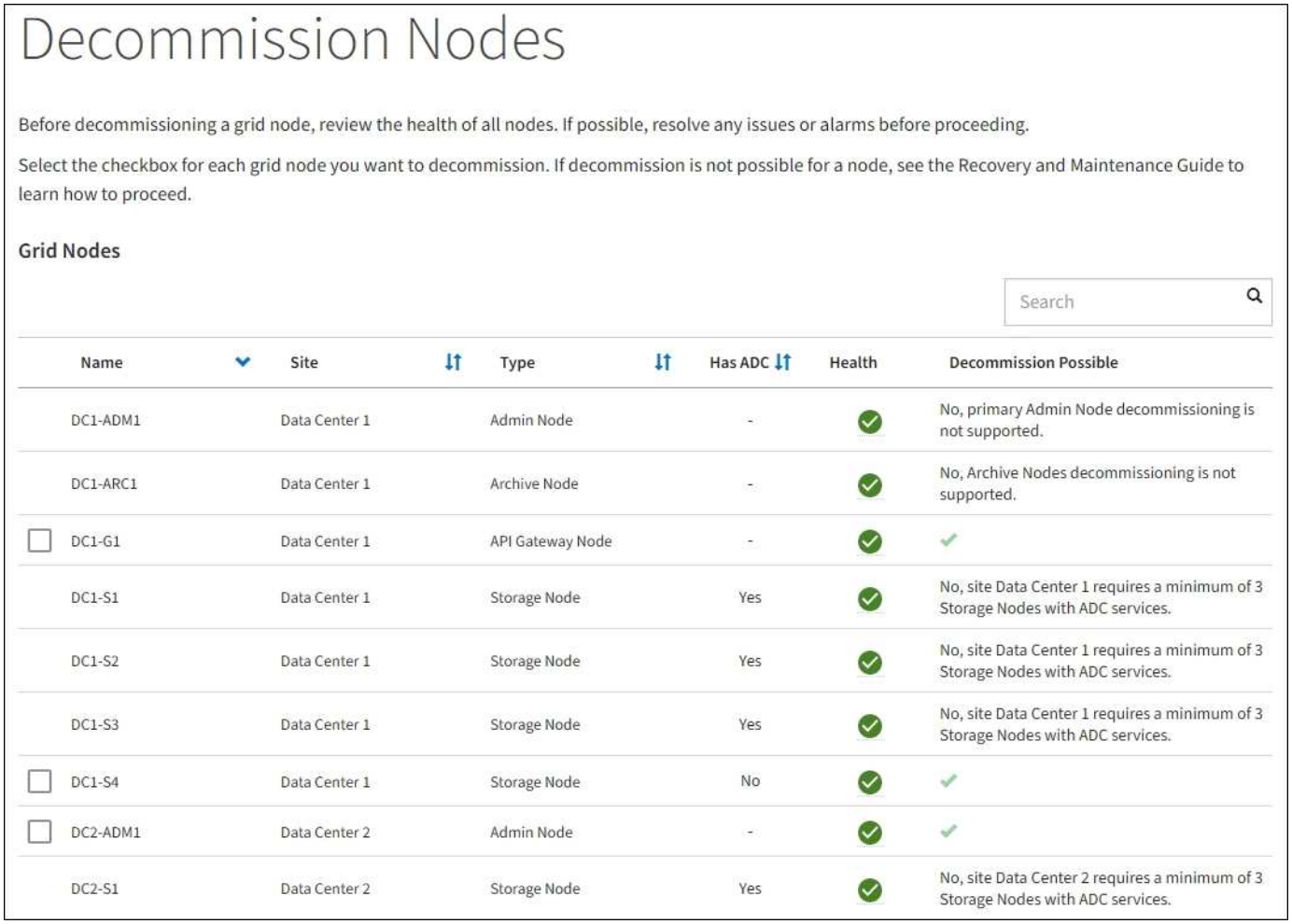
您可能需要从 StorageGRID 系统中永久删除网格节点或整个数据中心站点。

例如，在以下情况下，您可能需要停用一个或多个网格节点：

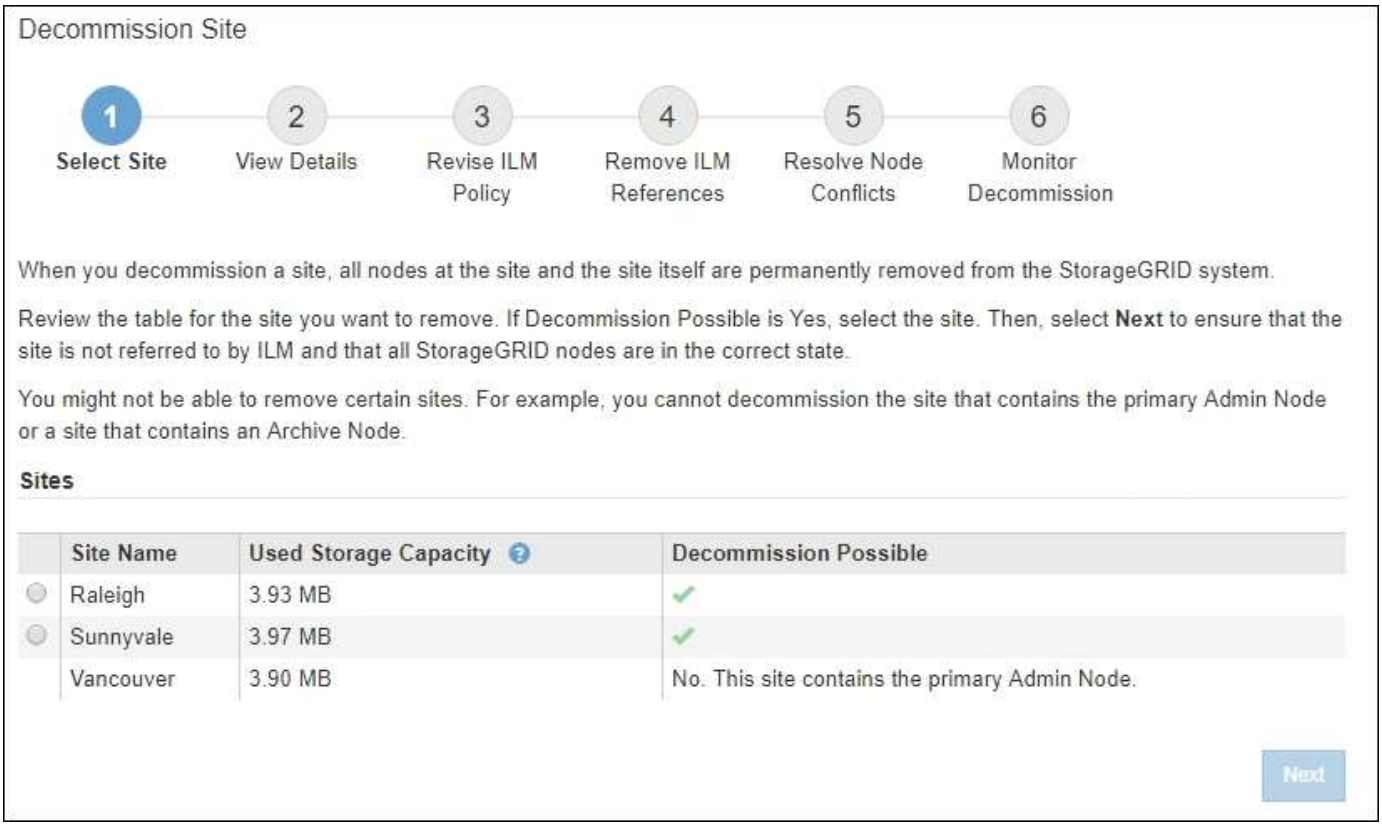
- 您已向系统中添加较大的存储节点，并希望删除一个或多个较小的存储节点，同时保留对象。
- 您所需的总存储较少。
- 您不再需要网关节点或非主管理节点。
- 您的网格包含一个断开连接的节点，您无法恢复此节点或使其恢复联机。

您可以使用网格管理器中的 " 取消配置节点 " 页面删除以下类型的网格节点：

- 存储节点，除非站点上保留的节点不足以满足某些要求
- 网关节点
- 非主管理节点



您可以使用网格管理器中的 " 弃用站点 " 页面删除站点。已连接站点停用会删除操作站点并保留数据。断开连接的站点停用会删除故障站点，但不会保留数据。" 取消配置站点 " 向导将指导您完成选择站点，查看站点详细信息，修改 ILM 策略，从 ILM 规则中删除站点引用以及解决任何节点冲突的过程。



网络维护过程

您可能需要执行的一些网络维护过程包括：

- 更新网格网络上的子网
- 使用更改 IP 工具更改网格部署期间最初设置的网络配置
- 添加，删除或更新域名系统（ DNS ）服务器
- 添加，删除或更新网络时间协议（ NTP ）服务器，以确保在网格节点之间准确同步数据
- 还原与可能已与网格其余部分隔离的节点的网络连接

主机级别和中间件过程

某些维护过程特定于在 Linux 或 VMware 上部署的 StorageGRID 节点，或者特定于 StorageGRID 解决方案 的其他组件。例如，您可能希望将网格节点迁移到其他 Linux 主机，或者对连接到 Tivoli Storage Manager （ TSM ）的归档节点执行维护。

设备节点克隆

通过设备节点克隆，您可以轻松地将网格中的现有设备节点替换为同一逻辑 StorageGRID 站点中具有较新设计或增强功能的设备。此过程会将所有数据传输到新设备，从而使其投入使用以更换旧设备节点，并使旧设备处于预安装状态。克隆提供了一个易于执行的硬件升级过程，并提供了替代设备的方法。

网格节点过程

您可能需要在特定网格节点上执行某些过程。例如，您可能需要重新启动网格节点或手动停止并重新启动特定网格节点服务。某些网格节点过程可以从网格管理器执行；另一些过程则要求您登录到网格节点并使用该节点的命令行。

相关信息

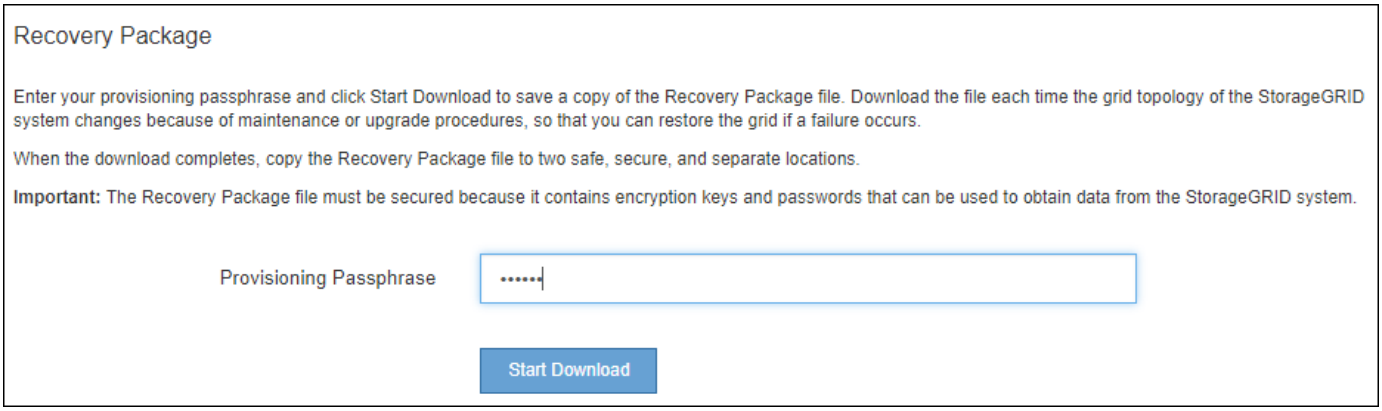
- 管理 StorageGRID
- 升级软件
- 扩展网格
- 恢复和维护

下载恢复包

恢复包是一个可下载的 .zip 文件，其中包含安装，扩展，升级和维护 StorageGRID 系统所需的部署专用文件和软件。

恢复软件包文件还包含系统专用的配置和集成信息，包括服务器主机名和 IP 地址以及系统维护，升级和扩展期间所需的高度机密的密码。要从主管理节点的故障中恢复，需要使用恢复包。

安装 StorageGRID 系统时，您需要下载恢复软件包文件并确认可以成功访问此文件的内容。每次由于维护或升级过程而更改 StorageGRID 系统的网格拓扑时，您还应下载此文件。



下载恢复软件包文件并确认可以提取其内容后，将恢复软件包文件复制到两个安全，安全和独立的位置。

恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

相关信息

- 升级软件
- 扩展网格
- 恢复和维护

使用 **StorageGRID** 支持选项

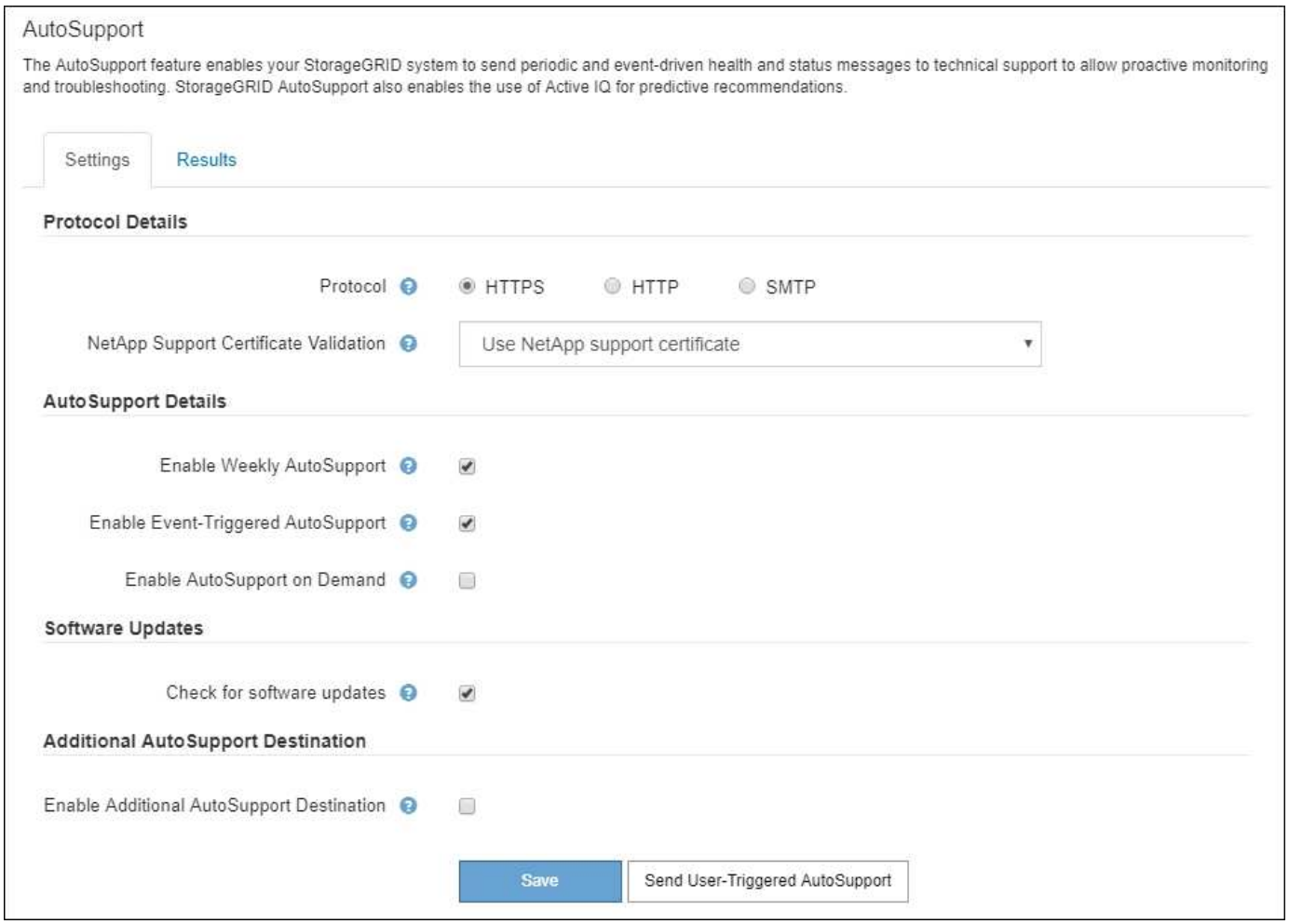
网格管理器提供了一些选项，可帮助您在 StorageGRID 系统出现问题描述 时与技术支持联系。

配置 **AutoSupport**

通过 AutoSupport 功能， StorageGRID 系统可以向技术支持发送运行状况和状态消息。使用 AutoSupport 可以显著加快问题的确定和解决速度。技术支持还可以监控系统的存储需求，并帮助您确定是否需要添加新节点或站

点。您也可以将 AutoSupport 消息配置为发送到另一个目标。

您可以使用网格管理器配置 AutoSupport （ * 支持 * > * 工具 * > * AutoSupport * ）。* AutoSupport * 页面有两个选项卡： * 设置 * 和 * 结果 * 。



AutoSupport 消息中包含的信息

AutoSupport 消息包含如下信息：

- StorageGRID 软件版本
- 操作系统版本
- 系统级别和位置级别属性信息
- 近期警报和警报（旧系统）
- 所有网格任务的当前状态，包括历史数据
- 管理节点数据库使用情况
- 丢失或缺失对象的数量
- 网格配置设置
- NMS 实体
- 活动 ILM 策略

- 已配置网格规范文件
- 诊断指标

您可以在首次安装 StorageGRID 时启用 AutoSupport 功能和各个 AutoSupport 选项，也可以稍后启用它们。如果未启用 AutoSupport ，网格管理器信息板上将显示一条消息。此消息包含指向 AutoSupport 配置页面的链接。

如果关闭此消息，则此消息将不会再次显示，直到清除浏览器缓存为止，即使 AutoSupport 仍处于禁用状态。

使用 **Active IQ**

Active IQ 是一名基于云的数字顾问，利用 NetApp 客户群的预测性分析和社区智慧。其持续风险评估，预测性警报，规范化指导和自动化操作可帮助您在问题发生之前防患于未然，从而改善系统运行状况并提高系统可用性。

如果要使用 NetApp 支持站点上的 Active IQ 信息板和功能，则必须启用 AutoSupport 。

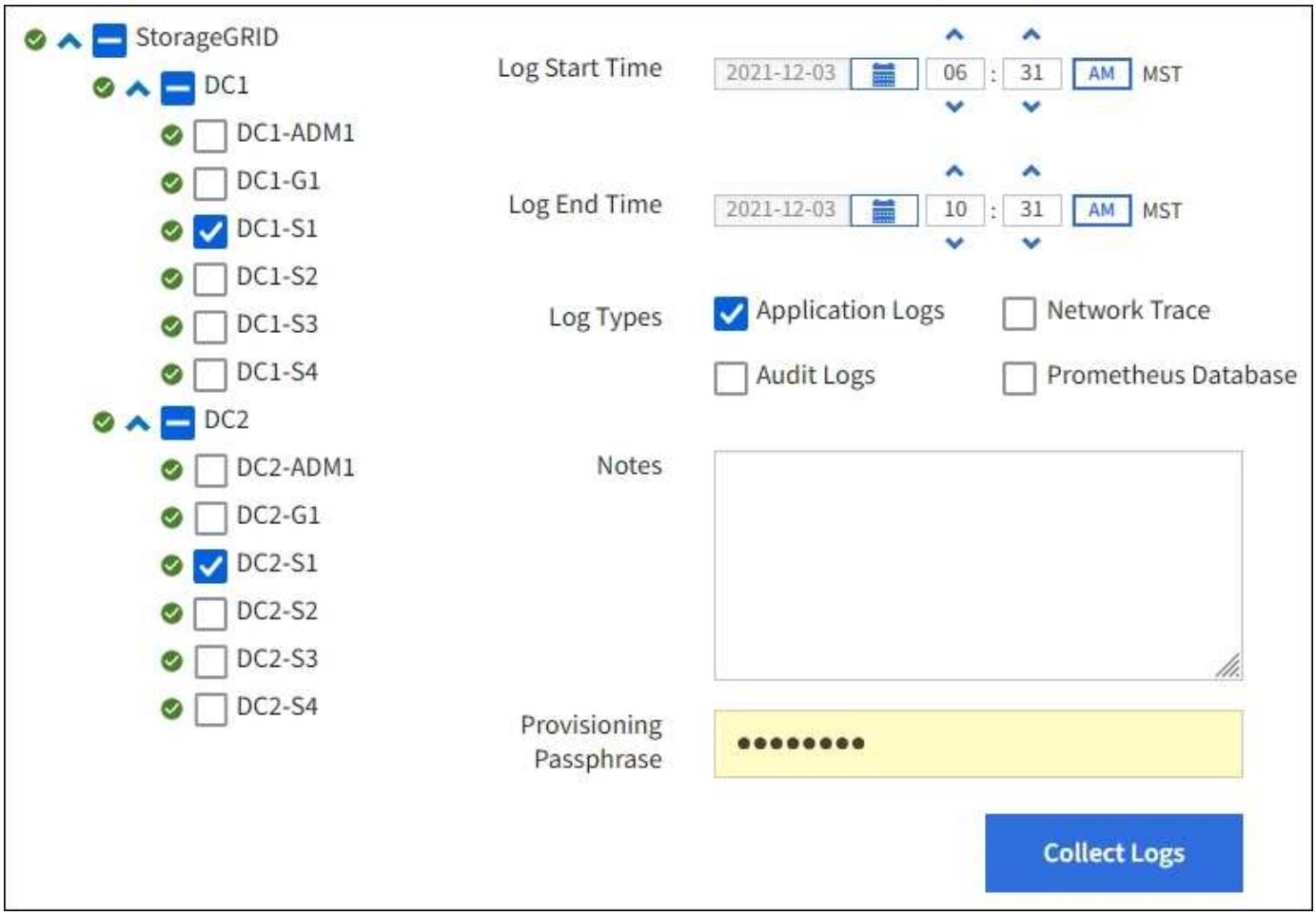
"Active IQ 数字顾问文档"

收集 **StorageGRID** 日志

为了帮助解决问题，您可能需要收集日志文件并将其转发给技术支持。

StorageGRID 使用日志文件捕获事件，诊断消息和错误情况。每个网格节点都会维护 bycast.log 文件，它是主要的故障排除文件。StorageGRID 还会为各个 StorageGRID 服务创建日志文件，与部署和维护活动相关的日志文件以及与第三方应用程序相关的日志文件。

拥有适当权限且知道 StorageGRID 系统配置密码短语的用户可以使用网格管理器中的日志页面收集日志文件，系统数据和配置数据。收集日志时，您可以选择一个或多个节点并指定时间段。数据会收集并归档在 ` .tar.gz` 文件中，您可以将该文件下载到本地计算机。在此文件中，每个网格节点都有一个日志文件归档。



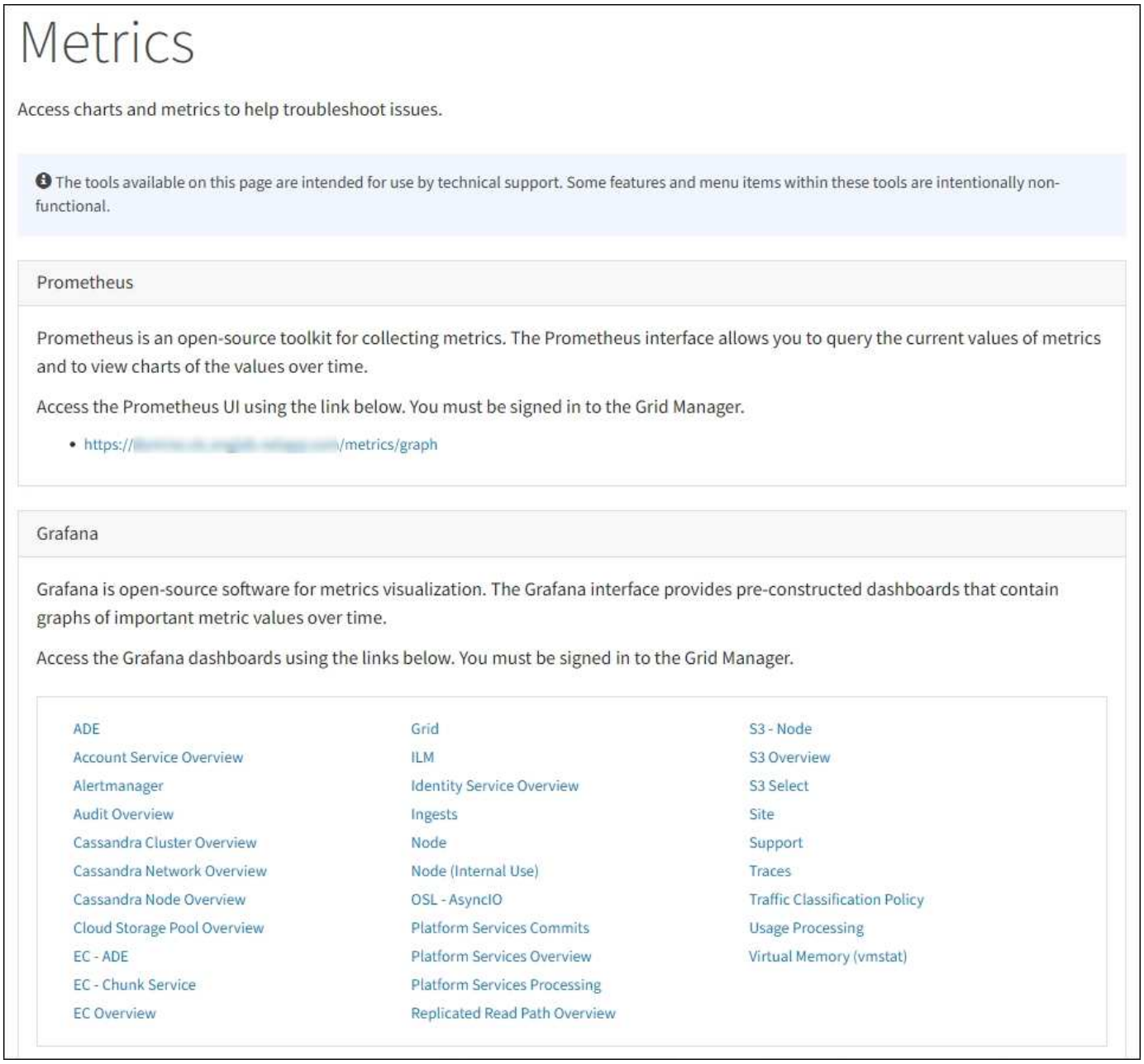
使用指标并运行诊断

对问题描述 进行故障排除时，您可以与技术支持人员一起查看 StorageGRID 系统的详细指标和图表。您还可以运行预构建的诊断查询，主动评估 StorageGRID 系统的关键值。

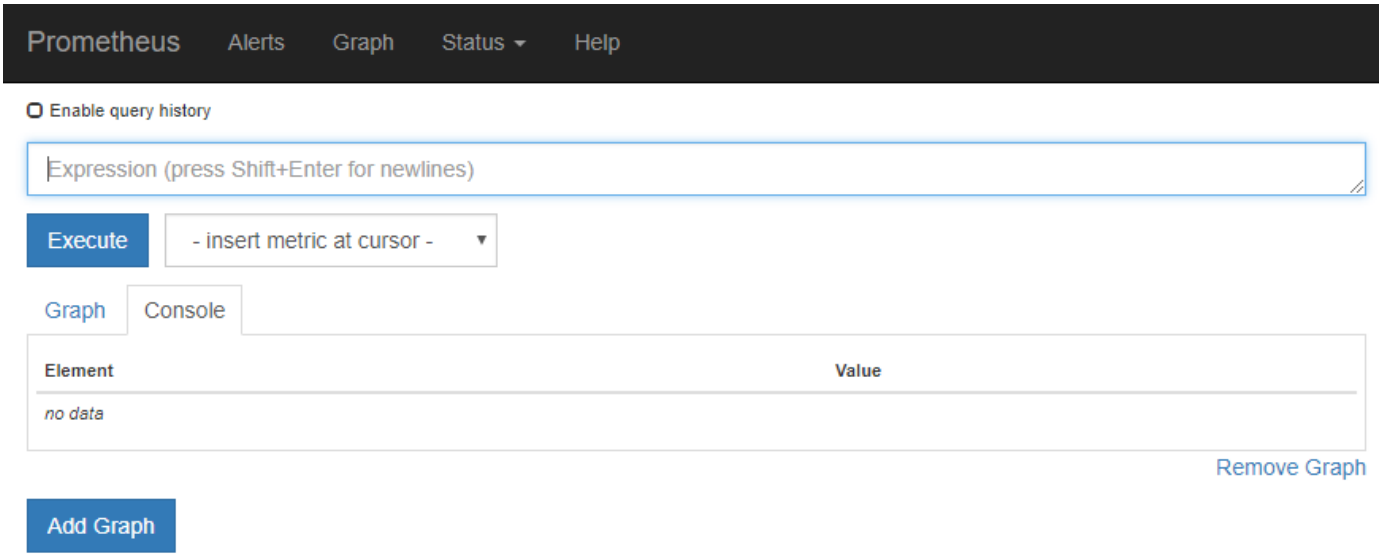
指标页面

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

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



您可以通过指标页面的 Prometheus 部分中的链接查询 StorageGRID 指标的当前值，并查看这些值随时间变化的图形。

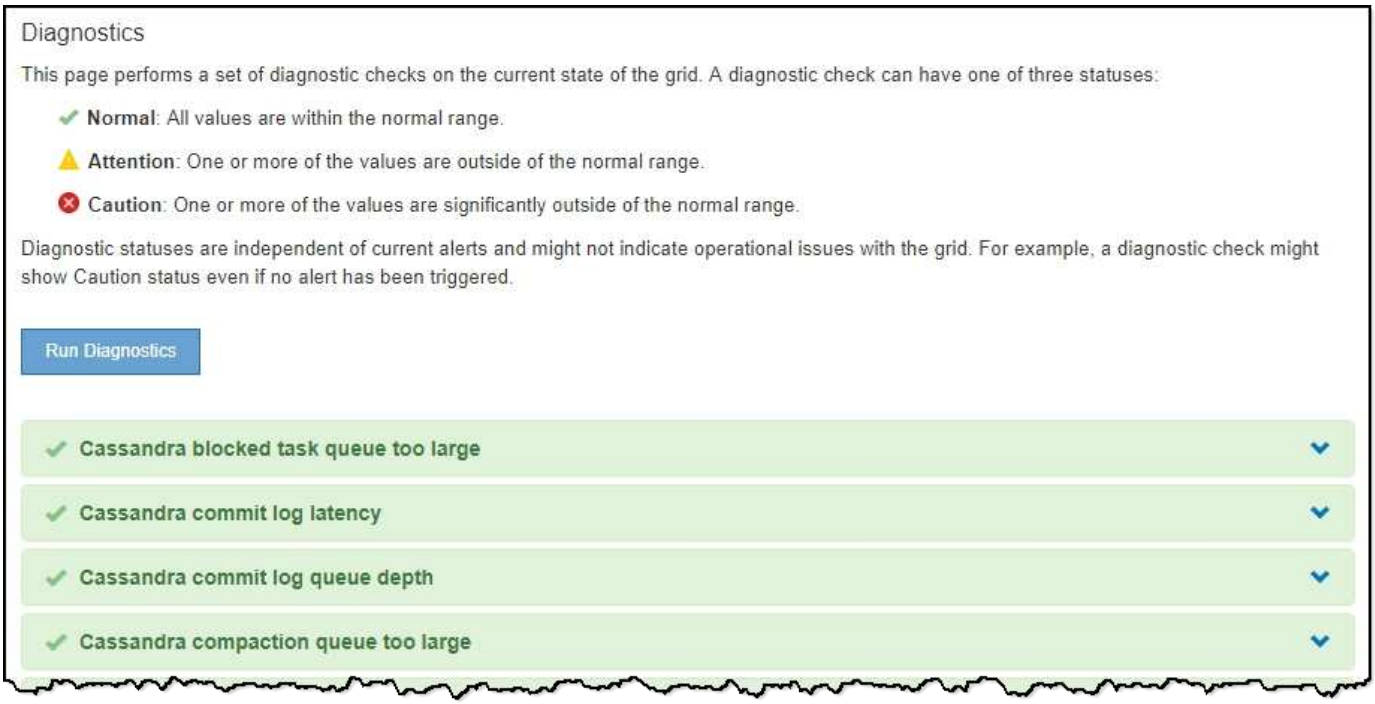


名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间可能会发生更改，恕不另行通知。

您可以通过指标页面的 Grafana 部分中的链接访问预构建的信息板，其中包含一段时间内的 StorageGRID 指标图形。

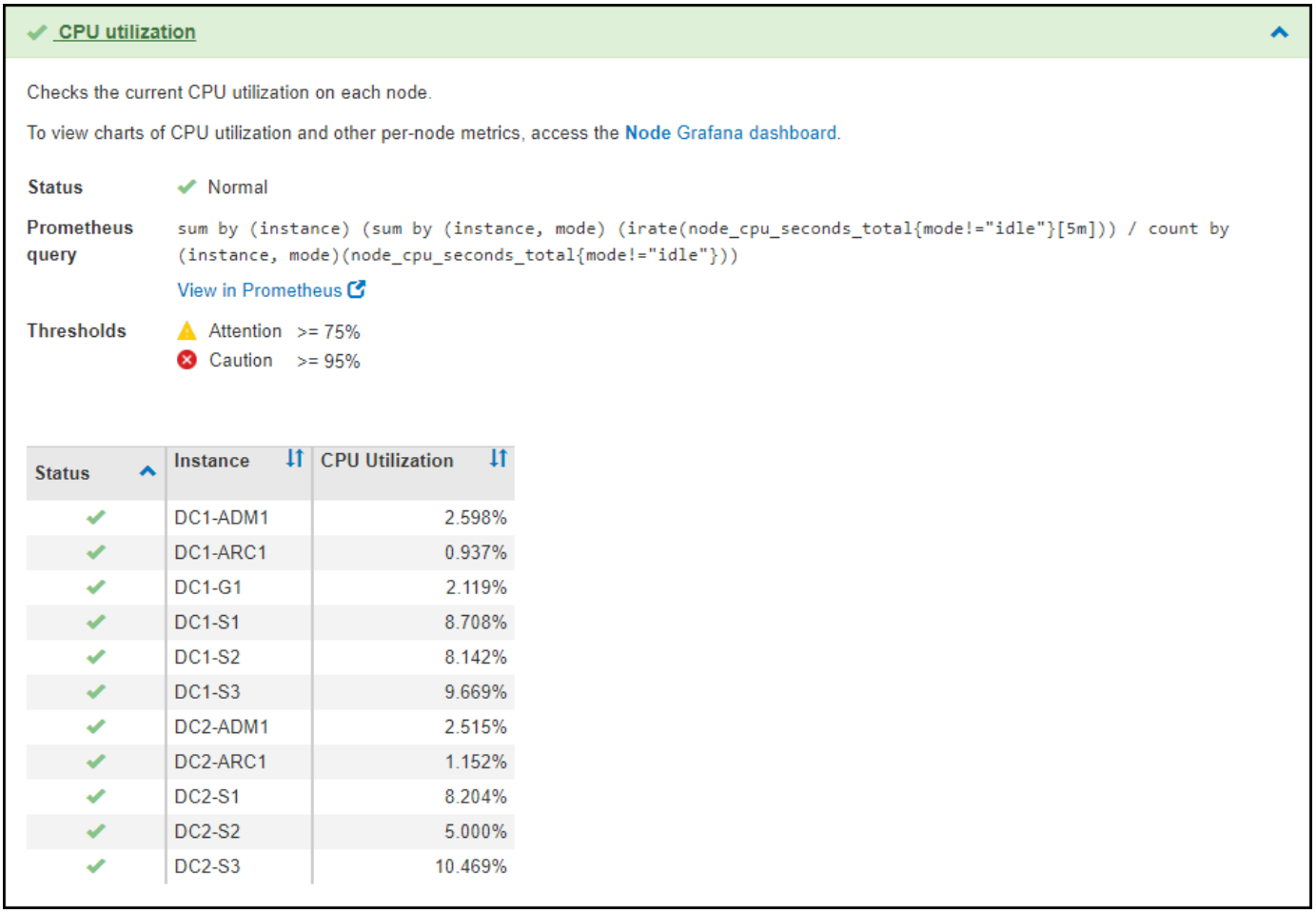
诊断页面

" 诊断 " 页面会对网格的当前状态执行一组预先构建的诊断检查。在此示例中，所有诊断均处于正常状态。



单击特定诊断可以查看有关诊断及其当前结果的详细信息。

在此示例中，显示了 StorageGRID 系统中每个节点的当前 CPU 利用率。所有节点值均低于警示和警示阈值，因此诊断的整体状态为正常。



相关信息

- 管理 StorageGRID
- 配置网络设置

网络连接准则

网络连接准则：概述

使用以下准则了解 StorageGRID 架构和网络拓扑，并了解网络配置和配置的要求。

关于这些说明

这些准则提供了在部署和配置 StorageGRID 节点之前可用于创建 StorageGRID 网络基础架构的信息。使用这些准则有助于确保网格中的所有节点之间以及网格与外部客户端和服务之间可以进行通信。

外部客户端和外部服务需要连接到 StorageGRID 网络才能执行如下功能：

- 存储和检索对象数据
- 接收电子邮件通知
- 访问 StorageGRID 管理界面（网格管理器和租户管理器）
- 访问审核共享（可选）
- 提供以下服务：
  - 网络时间协议（ NTP ）
  - 域名系统（ DNS ）
  - 密钥管理服务器（ KMS ）

必须正确配置 StorageGRID 网络，才能处理这些功能等的流量。

开始之前

为 StorageGRID 系统配置网络需要在以太网交换， TCP/IP 网络，子网，网络路由和防火墙方面具有丰富的经验。

在配置网络之前，请熟悉 StorageGRID 架构，如中所述 网格入门。

确定要使用的 StorageGRID 网络以及这些网络的配置方式后，您可以按照相应的说明安装和配置 StorageGRID 节点。

安装基于软件的节点

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian
- 安装 VMware

安装设备节点

- SG100 和 SG1000 服务设备

- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

配置和管理 **StorageGRID** 软件

- 管理 StorageGRID
- 发行说明

StorageGRID 网络类型

StorageGRID 系统中的网格节点处理 _grid traffic ， _admin traffic _ 和 _client traffic 。您必须正确配置网络，以管理这三种类型的流量并提供控制和安全性。

流量类型

流量类型	**Description**	网络类型
网格流量	网格中所有节点之间传输的内部 StorageGRID 流量。所有网格节点都必须能够通过此网络与所有其他网格节点进行通信。	网格网络（必需）
管理流量	用于系统管理和维护的流量。	管理网络（可选）， VLAN 网络（可选）
客户端流量	在外部客户端应用程序和网格之间传输的流量，包括来自 S3 和 Swift 客户端的所有对象存储请求。	客户端网络（可选）， VLAN 网络（可选）

您可以通过以下方式配置网络：

- 仅限网格网络
- 网格和管理网络
- 网格和客户端网络
- 网格网络，管理网络和客户端网络

网格网络是必需的，可以管理所有网格流量。管理员和客户端网络可以在安装时包括在内，也可以稍后添加，以适应需求的变化。尽管管理网络和客户端网络是可选的，但在使用这些网络处理管理和客户端流量时，网格网络可以实现隔离和安全。

内部端口只能通过网格网络访问。可以从所有网络类型访问外部端口。这种灵活性为设计 StorageGRID 部署以及在交换机和防火墙中设置外部 IP 和端口筛选提供了多种选项。请参见 内部网格节点通信 和 外部通信。

网络接口

StorageGRID 节点使用以下特定接口连接到每个网络：

网络	接口名称
网格网络（必需）	eth0
管理网络（可选）	Eth1
客户端网络（可选）	Eth2

有关将虚拟或物理端口映射到节点网络接口的详细信息，请参见安装说明：

基于软件的节点

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian
- 安装 VMware

设备节点

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

每个节点的网络信息

您必须为节点上启用的每个网络配置以下内容：

- IP 地址
- 子网掩码
- 网关 IP 地址

您只能为每个网格节点上的三个网络中的每个网络配置一个 IP 地址 / 掩码 / 网关组合。如果不想为网络配置网关，应使用 IP 地址作为网关地址。

高可用性组

通过高可用性（ High Availability ， HA ）组，可以向网格或客户端网络接口添加虚拟 IP （ VIP ）地址。有关详细信息，请参见 管理高可用性组。

网格网络

网格网络为必填项。它用于所有内部 StorageGRID 流量。网格网络可在网格中的所有节点之间以及所有站点和子网之间建立连接。网格网络上的所有节点必须能够与所有其他节点进行通信。网格网络可以包含多个子网。包含 NTP 等关键网格服务的网络也可以添加为网格子网。

StorageGRID 不支持节点之间的网络地址转换（ Network Address Translation ， NAT ）。

网格网络可用于所有管理流量和所有客户端流量，即使已配置管理网络和客户端网络也是如此。除非节点配置了

客户端网络，否则网格网络网关是节点的默认网关。

> 在配置网格网络时，您必须确保网络不受不可信客户端的保护，例如在开放式 Internet 上的客户端。

请注意网格网络网关的以下要求和详细信息：

- 如果存在多个网格子网，则必须配置网格网络网关。
- 网格网络网关是节点默认网关，直到网格配置完成为止。
- 系统会自动为所有节点生成静态路由，并发送到全局网格网络子网列表中配置的所有子网。
- 如果添加了客户端网络，则在网格配置完成后，默认网关将从网格网络网关切换到客户端网络网关。

管理网络

管理网络是可选的。配置后，它可用于系统管理和维护流量。管理网络通常是一个专用网络，不需要在节点之间进行路由。

您可以选择应在哪些网格节点上启用管理网络。

使用管理网络时，管理和维护流量无需通过网格网络传输。管理网络的典型用途包括：

- 访问 Grid Manager 和租户管理器用户界面。
- 访问关键服务，例如 NTP 服务器， DNS 服务器，外部密钥管理服务器（ KMS ）和轻型目录访问协议（ LDAP ）服务器。
- 访问管理节点上的审核日志。
- 安全 Shell 协议（ SSH ）访问以进行维护和支持。

管理网络决不用于内部网格流量。提供了一个管理网络网关，允许管理网络与多个外部子网进行通信。但是，管理网络网关绝不会用作节点默认网关。

请注意管理网络网关的以下要求和详细信息：

- 如果要从管理网络子网外部进行连接或配置了多个管理网络子网，则需要使用管理网络网关。
- 系统会为节点的管理网络子网列表中配置的每个子网创建静态路由。

客户端网络

客户端网络是可选的。配置后，它可用于为 S3 和 Swift 等客户端应用程序提供对网格服务的访问。如果您计划使外部资源（例如云存储池或 StorageGRID CloudMirror 复制服务）可以访问 StorageGRID 数据，则外部资源也可以使用客户端网络。网格节点可以与可通过客户端网络网关访问的任何子网进行通信。

您可以选择应在哪些网格节点上启用客户端网络。所有节点不必位于同一客户端网络上，并且节点永远不会通过客户端网络彼此通信。网格安装完成后，客户端网络才会运行。

为了提高安全性，您可以指定节点的客户端网络接口不可信，以便客户端网络在允许的连接方面更具限制性。如果节点的客户端网络接口不可信，则该接口会接受出站连接，例如 CloudMirror 复制使用的连接，但仅接受已明确配置为负载平衡器端点的端口上的入站连接。请参见 管理不可信的客户端网络 和 配置负载平衡器端点。

使用客户端网络时，客户端流量不需要通过网格网络传输。网格网络流量可以分隔到安全的不可路由网络上。以

下节点类型通常配置有客户端网络：

- 网关节点，因为这些节点可提供对 StorageGRID 负载平衡器服务的访问以及 S3 和 Swift 客户端对网格的访问。
- 存储节点，因为这些节点提供对 S3 和 Swift 协议以及云存储池和 CloudMirror 复制服务的访问。
- 管理节点，以确保租户用户无需使用管理网络即可连接到租户管理器。

对于客户端网络网关，请注意以下事项：

- 如果配置了客户端网络，则需要客户端网络网关。
- 网格配置完成后，客户端网络网关将成为网格节点的默认路由。

可选 **VLAN** 网络

根据需要，您可以选择使用虚拟 LAN （ VLAN ）网络来处理客户端流量和某些类型的管理流量。但是，网格流量不能使用 VLAN 接口。节点之间的内部 StorageGRID 流量必须始终使用 eth0 上的网格网络。

要支持使用 VLAN ，您必须将节点上的一个或多个接口配置为交换机上的中继接口。您可以将网格网络接口（ eth0 ）或客户端网络接口（ eth2 ）配置为中继，也可以为节点添加其他中继接口。

如果将 eth0 配置为中继，网格网络流量将按交换机上的配置流经中继原生 接口。同样，如果 eth2 配置为中继，并且客户端网络也配置在同一节点上，则客户端网络将使用交换机上配置的中继端口的原生 VLAN 。

VLAN 网络仅支持入站管理流量，例如用于 SSH ， Grid Manager 或租户管理器流量。VLAN 网络不支持出站流量，例如用于 NTP ， DNS ， LDAP ， KMS 和云存储池的流量。

> 只能将 VLAN 接口添加到管理节点和网关节点。您不能使用 VLAN 接口对存储节点或归档节点进行客户端或管理员访问。

请参见 配置 VLAN 接口 有关说明和准则，请参见。

VLAN 接口仅用于 HA 组，并在活动节点上分配 VIP 地址。请参见 管理高可用性组 有关说明和准则，请参见。

相关信息

- 网络要求

网络拓扑示例

网格网络拓扑

最简单的网络拓扑只能通过配置网格网络来创建。

配置网格网络时，您需要为每个网格节点的 eth0 接口建立主机 IP 地址，子网掩码和网关 IP 地址。

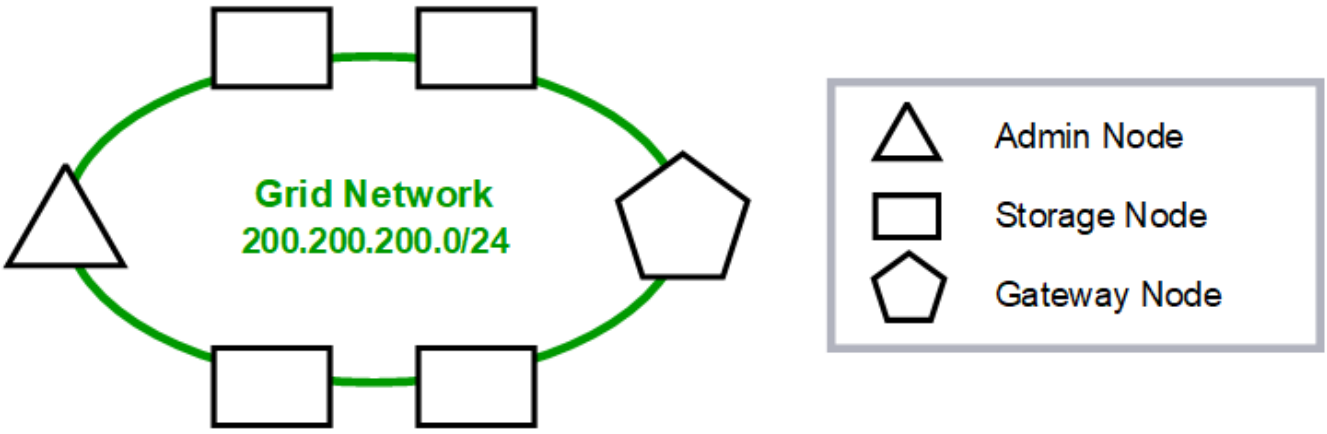
在配置期间，必须将所有网格网络子网添加到网格网络子网列表（ GSLL ）中。此列表包括所有站点的所有子网，并且可能还包括外部子网，这些子网可提供对 NTP ， DNS 或 LDAP 等关键服务的访问权限。

在安装时，网格网络接口会对 GNSL 中的所有子网应用静态路由，如果配置了网格网络网关，则会将节点的默认路由设置为网格网络网关。如果没有客户端网络，并且网格网络网关是节点的默认路由，则不需要使用 GNSL 。此外，还会生成到网格中所有其他节点的主机路由。

在此示例中，所有流量共享同一网络，包括与 S3 和 Swift 客户端请求以及管理和维护功能相关的流量。

此拓扑适用于外部不可用的单站点部署，概念验证或测试部署，或者当第三方负载平衡器充当客户端访问边界时。如果可能，网格网络应专门用于内部流量。管理网络和客户端网络都具有其他防火墙限制，可阻止外部向内部服务发送流量。支持对外部客户端流量使用网格网络，但这种使用可提供更少的保护层。

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

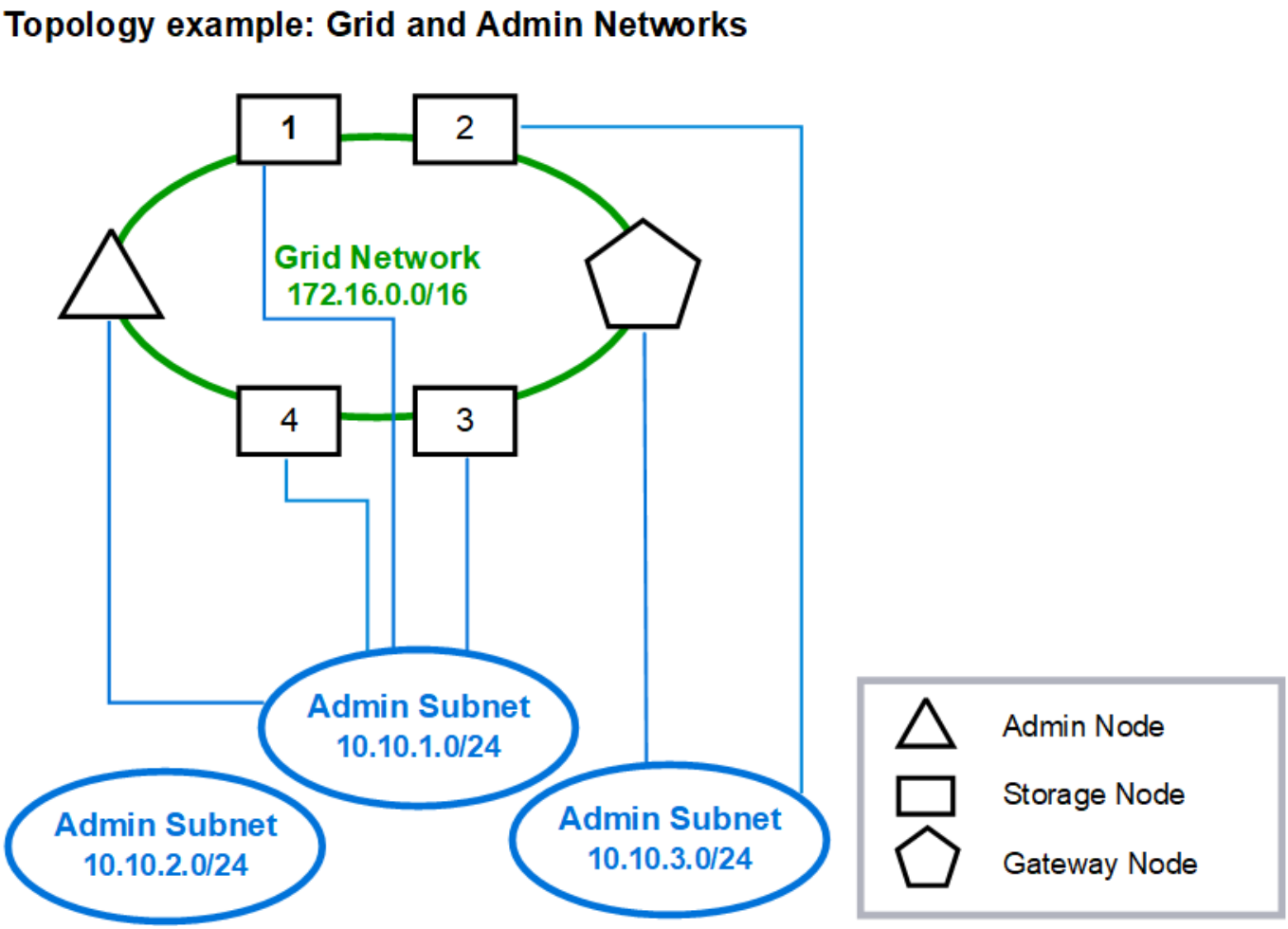
管理网络拓扑

可以选择使用管理网络。使用管理网络和网格网络的一种方法是，为每个节点配置可路由的网格网络和有限制的管理网络。

配置管理网络时，您需要为每个网格节点的 eth1 接口建立主机 IP 地址，子网掩码和网关 IP 地址。

管理网络对于每个节点都是唯一的，并且可以包含多个子网。可以为每个节点配置一个管理外部子网列表（ Admin External Subnet List ， AESL ）。AESL 列出了每个节点可通过管理网络访问的子网。AESL 还必须包括网格通过管理网络访问的任何服务的子网，例如 NTP ， DNS ， KMS 和 LDAP 。AESL 中的每个子网都应用静态路由。

在此示例中，网格网络用于处理与 S3 和 Swift 客户端请求以及对象管理相关的流量。而管理网络则用于管理功能。



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	**Routes**			**Type**	**From**
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

客户端网络拓扑

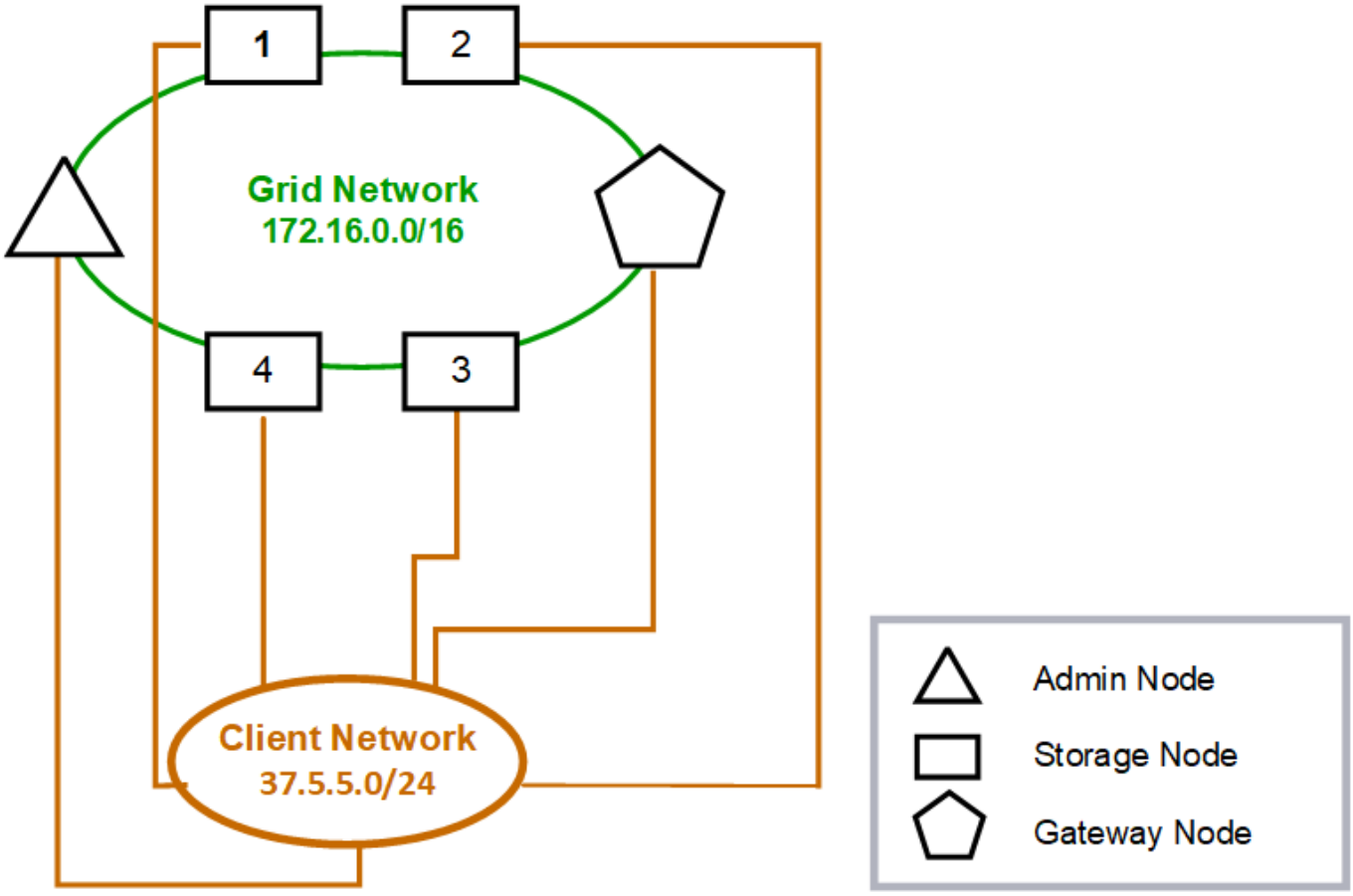
可以选择使用客户端网络。使用客户端网络可以将客户端网络流量（例如 S3 和 Swift ）与网格内部流量分隔开，从而提高网格网络连接的安全性。如果未配置管理网络，则可通过客户端网络或网格网络处理管理流量。

配置客户端网络时，您需要为所配置节点的 eth2 接口建立主机 IP 地址，子网掩码和网关 IP 地址。每个节点的客户端网络可以独立于任何其他节点上的客户端网络。

如果在安装期间为节点配置客户端网络，则在安装完成后，节点的默认网关将从网格网络网关切换到客户端网络网关。如果稍后添加客户端网络，则节点的默认网关将以相同方式进行切换。

在此示例中，客户端网络用于处理 S3 和 Swift 客户端请求以及管理功能，而网格网络则专用于内部对象管理操作。

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

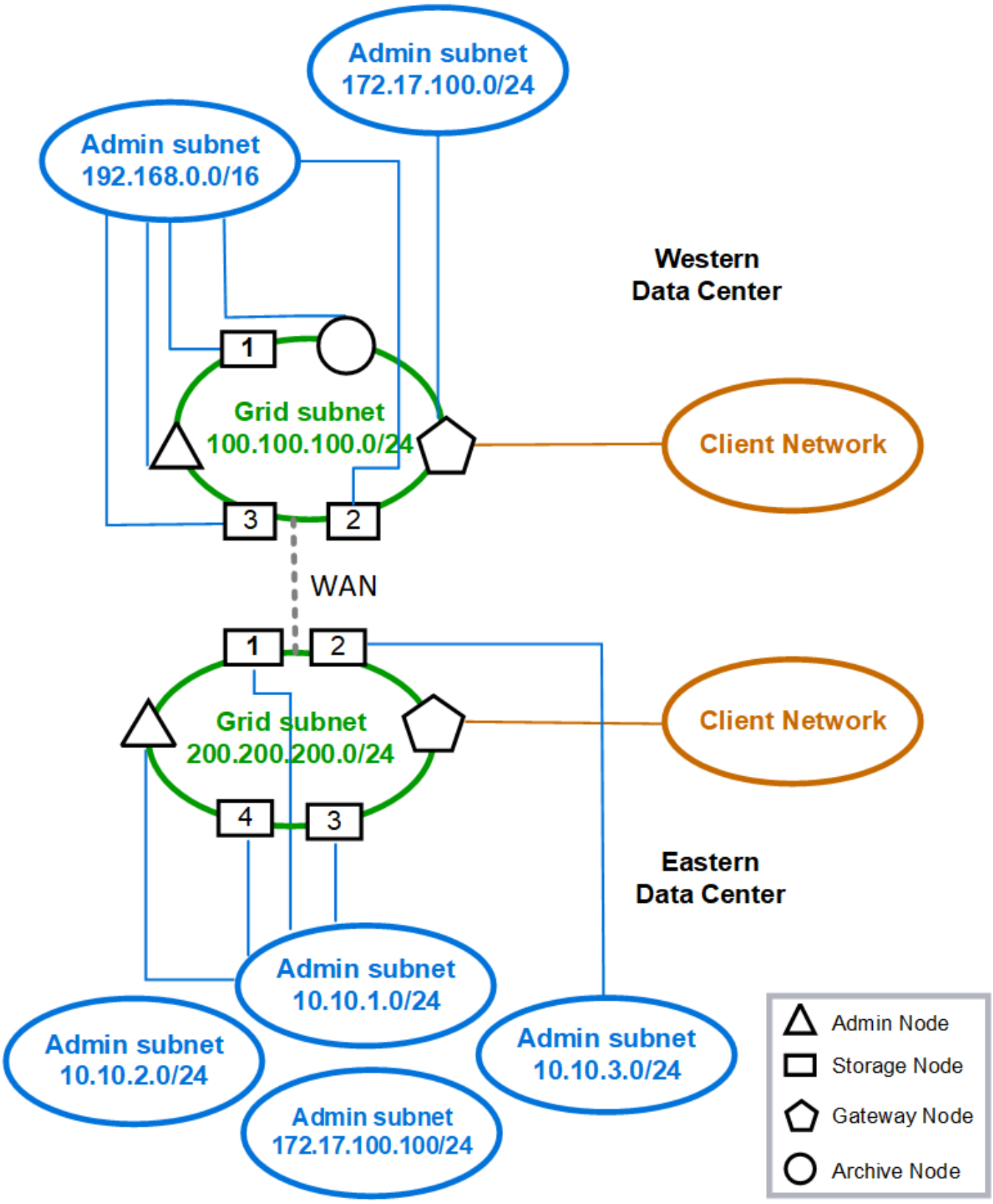
所有这三个网络的拓扑结构

您可以将所有这三个网络配置为一个网络拓扑，其中包括专用网格网络，特定于特定于站点的受限制管理网络和开放式客户端网络。如果需要，使用负载平衡器端点和不可信的客户端网络可以提供额外的安全性。

在此示例中：

- 网格网络用于处理与内部对象管理操作相关的网络流量。
- 管理网络用于处理与管理功能相关的流量。
- 客户端网络用于处理与 S3 和 Swift 客户端请求相关的流量。

Topology example: Grid, Admin, and Client Networks



网络要求

您必须验证当前的网络基础架构和配置是否可以支持计划的 StorageGRID 网络设计。

一般网络连接要求

所有 StorageGRID 部署都必须能够支持以下连接。

这些连接可以通过网格网络，管理网络或客户端网络进行，也可以通过这些网络的组合进行，如网络拓扑示例所示。

- * 管理连接 * ： 管理员到节点的入站连接，通常通过 SSH 。通过 Web 浏览器访问网格管理器，租户管理器和 StorageGRID 设备安装程序。
- * NTP 服务器连接 * ： 接收入站 UDP 响应的出站 UDP 连接。

  主管理节点必须至少可访问一个 NTP 服务器。

- * DNS 服务器连接 * ： 接收入站 UDP 响应的出站 UDP 连接。
- * LDAP/Active Directory 服务器连接 * ： 从存储节点上的身份服务发出的出站 TCP 连接。
- * AutoSupport ： 从管理节点到 `support.netapp.com` 或客户配置的代理的出站 TCP 连接。
- * 外部密钥管理服务器 * ： 启用节点加密的每个设备节点的出站 TCP 连接。
- 来自 S3 和 Swift 客户端的入站 TCP 连接。
- 来自 StorageGRID 平台服务（例如 CloudMirror 复制）或云存储池的出站请求。

如果 StorageGRID 无法使用默认路由规则与任何已配置的 NTP 或 DNS 服务器建立联系，则只要指定了 DNS 和 NTP 服务器的 IP 地址，它就会自动尝试在所有网络（网格，管理员和客户端）上进行联系。如果可以在任何网络上访问 NTP 或 DNS 服务器， StorageGRID 将自动创建其他路由规则，以确保将来尝试连接到该网络时都使用该网络。

> 虽然您可以使用这些自动发现的主机路由，但通常应手动配置 DNS 和 NTP 路由，以确保在自动发现失败时连接。

如果您尚未准备好在部署期间配置可选的管理和客户端网络，则可以在配置步骤期间批准网格节点时配置这些网络。此外，您还可以在安装后使用更改 IP 工具配置这些网络（请参见 配置 IP 地址）。

VLAN 接口仅支持 S3 和 Swift 客户端连接以及 SSH ， Grid Manager 和租户管理连接。出站连接，例如与 NTP ， DNS ， LDAP ， AutoSupport 和 KMS 服务器的连接， 必须直接通过客户端，管理员或网格网络接口。如果将接口配置为支持 VLAN 接口的中继，则此流量将按交换机上的配置通过接口的原生 VLAN 进行传输。

适用于多个站点的广域网（ **WAN** ）

在为 StorageGRID 系统配置多个站点时，在计算客户端流量之前，站点之间的 WAN 连接的每个方向的最小带宽必须为 25 Mbit/ 秒。站点之间，节点或站点扩展，节点恢复以及其他操作或配置之间的数据复制或纠删编码需要额外的带宽。

管理节点和网关节点的连接

管理节点必须始终受到不可信客户端的保护，例如在开放式 Internet 上的客户端。您必须确保任何不可信的客户端都不能访问网格网络，管理网络或客户端网络上的任何管理节点。

要添加到高可用性组的管理节点和网关节点必须使用静态 IP 地址进行配置。有关详细信息，请参见 管理高可用性组。

使用网络地址转换（ **Network Address Translation** ， **NAT** ）

请勿在网格节点之间或 StorageGRID 站点之间的网格网络上使用网络地址转换（ Network Address Translation ， NAT ）。如果您对网格网络使用专用 IPv4 地址，则这些地址必须可从每个站点的每个网格节点直接路由。但是，您可以根据需要在外部客户端和网格节点之间使用 NAT ，例如为网关节点提供公有 IP 地址。只有在使用对网格中的所有节点都透明的通道应用程序时，才支持使用 NAT 桥接公有 网段，这意味着网格节点不需要了解公有 IP 地址。

网络特定要求

请按照每种 StorageGRID 网络类型的要求进行操作。

网络网关和路由器

- 如果设置了此值，则给定网络的网关必须位于特定网络的子网内。
- 如果使用静态寻址配置接口，则必须指定 0.0.0.0 以外的网关地址。
- 如果您没有网关，则最佳做法是将网关地址设置为网络接口的 IP 地址。

Subnets

每个网络都必须连接到其自身的子网，而该子网不会与节点上的任何其他网络重叠。

网格管理器会在部署期间强制实施以下限制。此处提供这些配置文件，用于协助进行部署前网络规划。

- 任何网络 IP 地址的子网掩码不能为 255.255.255.254 或 255.255.255.255 （ CIDR 表示法为 /31 或 /32 ）。
- 网络接口 IP 地址和子网掩码（ CIDR ）定义的子网不能与同一节点上配置的任何其他接口的子网重叠。
- 每个节点的网格网络子网必须包含在 GNSL 中。
- 管理网络子网不能与网格网络子网，客户端网络子网或 GNSL 中的任何子网重叠。
- AESL 中的子网不能与 GNSL 中的任何子网重叠。
- 客户端网络子网不能与网格网络子网，管理网络子网， GNSL 中的任何子网或 AESL 中的任何子网重叠。

网格网络

- 在部署时，每个网格节点都必须连接到网格网络，并且必须能够使用部署节点时指定的网络配置与主管理节点进行通信。
- 在正常网格操作期间，每个网格节点都必须能够通过网格网络与所有其他网格节点进行通信。

网格网络必须在每个节点之间直接可路由。不支持节点之间的网络地址转换（ Network Address Translation ， NAT ）。

- 如果网格网络包含多个子网，请将其添加到网格网络子网列表（ GSLL ）中。在 GNSL 中的每个子网的所有节点上创建静态路由。

- 如果将网格网络接口配置为支持 VLAN 接口的中继，则中继原生 VLAN 必须是用于网格网络流量的 VLAN 。所有网格节点都必须可通过中继原生 VLAN 进行访问。

管理网络

管理网络是可选的。如果您计划配置管理网络，请遵循以下要求和准则。

管理网络的典型用途包括管理连接， AutoSupport ， KMS 以及与 NTP ， DNS 和 LDAP 等关键服务器的连接（如果这些连接不是通过网格网络或客户端网络提供的）。

只要所需的网络服务和客户端可访问，管理网络和 AESL 就可以对每个节点唯一。

要从外部子网启用入站连接，必须在管理网络上至少定义一个子网。AESL 中的每个子网都会在每个节点上自动生成静态路由。

客户端网络

客户端网络是可选的。如果您计划配置客户端网络，请注意以下事项。

- 客户端网络用于支持来自 S3 和 Swift 客户端的流量。如果已配置，客户端网络网关将成为节点的默认网关。
- 如果您使用客户端网络，则可以通过仅接受显式配置的负载平衡器端点上的入站客户端流量来帮助保护 StorageGRID 免受恶意攻击。请参见 配置负载平衡器端点。
- 如果客户端网络接口配置为中继以支持 VLAN 接口，请考虑是否需要配置客户端网络接口（ eth2 ）。如果已配置，则客户端网络流量将按交换机中的配置流经中继原生 VLAN 。

部署特定的网络注意事项

Linux 部署

为了提高效率，可靠性和安全性， StorageGRID 系统在 Linux 上作为一组容器引擎运行。StorageGRID 系统不需要与容器引擎相关的网络配置。

使用非绑定设备作为容器网络接口，例如 VLAN 或虚拟以太网（ Veth ）对。在节点配置文件中指定此设备作为网络接口。

请勿直接使用绑定或网桥设备作为容器网络接口。这样做可能会由于内核问题描述 在容器命名空间中对绑定和网桥设备使用 macvlan 而阻止节点启动。

请参见的安装说明 Red Hat Enterprise Linux 或 CentOS 或 Ubuntu 或 Debian 部署。

用于容器引擎部署的主机网络配置

在容器引擎平台上开始 StorageGRID 部署之前，请确定每个节点要使用的网络（网格，管理，客户端）。您必须确保在正确的虚拟或物理主机接口上配置每个节点的网络接口，并且每个网络都有足够的带宽。

物理主机

如果使用物理主机支持网格节点：

- 确保所有主机对每个节点接口使用相同的主机接口。此策略可简化主机配置，并支持将来的节点迁移。
- 获取物理主机本身的 IP 地址。

> 主机本身以及主机上运行的一个或多个节点均可使用主机上的物理接口。分配给使用此接口的主机或节点的任何 IP 地址都必须是唯一的。主机和节点不能共享 IP 地址。

- 打开主机所需的端口。
- 如果要在 StorageGRID 中使用 VLAN 接口，则主机必须具有一个或多个中继接口，以提供对所需 VLAN 的访问。这些接口可以作为 eth0 ， eth2 或其他接口传递到节点容器中。要添加中继或访问接口，请参见以下内容：
  - * RHEL 或 CentOS （安装节点之前） *： 创建节点配置文件
  - * Ubuntu 或 Debian （安装节点之前） *： 创建节点配置文件
  - * RHEL ， CentOS ， Ubuntu 或 Debian （安装节点后） *： Linux ：向节点添加中继或访问接口

最小带宽建议

下表提供了每种类型的 StorageGRID 节点和每种网络的最小带宽建议。您必须为每个物理或虚拟主机配置足够的网络带宽，以满足计划在该主机上运行的 StorageGRID 节点总数和类型的聚合最小带宽要求。

节点类型	网络类型		
	网格	管理员	客户端
管理员	10 Gbps	1 Gbps	1 Gbps
网关	10 Gbps	1 Gbps	10 Gbps
存储	10 Gbps	1 Gbps	10 Gbps
归档	10 Gbps	1 Gbps	10 Gbps

> 此表不包括访问共享存储所需的 SAN 带宽。如果您使用的是通过以太网（ iSCSI 或 FCoE ）访问的共享存储，则应在每个主机上配置单独的物理接口，以提供足够的 SAN 带宽。为了避免出现瓶颈，给定主机的 SAN 带宽应大致与该主机上运行的所有存储节点的聚合存储节点网络带宽匹配。

使用下表根据计划在每个主机上运行的 StorageGRID 节点的数量和类型确定要在该主机上配置的最小网络接口数。

例如，要在单个主机上运行一个管理节点，一个网关节点和一个存储节点，请执行以下操作：

- 连接管理节点上的网格和管理网络（需要 10 + 1 = 11 Gbps ）
- 连接网关节点上的网格和客户端网络（需要 10 + 10 = 20 Gbps ）
- 在存储节点上连接网格网络（需要 10 Gbps ）

在这种情况下，您应至少提供 11 + 20 + 10 = 41 Gbps 的网络带宽， 可通过两个 40 Gbps 接口或五个 10 Gbps

接口来满足，这些接口可能聚合为中继，然后由三个或更多 VLAN 共享，这些 VLAN 承载主机所在物理数据中心的本地网格，管理和客户端子网。

有关在 StorageGRID 集群中的主机上配置物理和网络资源以准备 StorageGRID 部署的一些建议方法，请参见以下内容：

- 配置主机网络（ Red Hat Enterprise Linux 或 CentOS ）
- 配置主机网络（ Ubuntu 或 Debian ）

用于平台服务和云存储池的网络和端口

如果您计划使用 StorageGRID 平台服务或云存储池，则必须配置网格网络和防火墙以确保可以访问目标端点。

平台服务的网络连接

如中所述 管理租户的平台服务 和 什么是平台服务，平台服务包括提供搜索集成，事件通知和 CloudMirror 复制的外部服务。

平台服务需要从托管 StorageGRID ADA 服务的存储节点访问外部服务端点。提供访问权限的示例包括：

- 在具有 ADE 服务的存储节点上，使用路由到目标端点的 AESL 条目配置唯一管理网络。
- 依靠客户端网络提供的默认路由。如果使用默认路由，则可以使用 不可信客户端网络功能 限制入站连接。

云存储池网络连接

云存储池还需要从存储节点访问所使用的外部服务提供的端点，例如 Amazon S3 Glacier 或 Microsoft Azure Blob 存储。有关信息，请参见 什么是云存储池。

用于平台服务和云存储池的端口

默认情况下，平台服务和云存储池通信使用以下端口：

- * 80* ： 对于以 `http` 开头的端点 URI
- * 443 ： 对于以 `https` 开头的端点 URI

创建或编辑端点时，可以指定其他端口。请参见 网络端口参考。

如果使用非透明代理服务器，则还必须使用 配置存储代理设置 允许将消息发送到外部端点，例如 Internet 上的端点。

VLAN 和平台服务以及云存储池

您不能将 VLAN 网络用于平台服务或云存储池。目标端点必须可通过网格，管理员或客户端网络访问。

设备节点

您可以将 StorageGRID 设备上的网络端口配置为使用符合吞吐量，冗余和故障转移要求的端口绑定模式。

可以在固定或聚合绑定模式下配置 StorageGRID 设备上的 10/225-GbE 端口，以便连接到网格网络和客户端网络。

可以在独立或主动备份模式下配置 1-GbE 管理网络端口，以便连接到管理网络。

请参见设备安装和维护说明中有关端口绑定模式的信息：

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

网络安装和配置

您必须了解在节点部署和网格配置期间如何使用网格网络以及可选的管理和客户端网络。

节点的初始部署

首次部署节点时，必须将节点连接到网格网络，并确保其能够访问主管理节点。如果网格网络已隔离，则可以在主管理节点上配置管理网络，以便从网格网络外部进行配置和安装访问。

配置了网关的网格网络将在部署期间成为节点的默认网关。默认网关允许不同子网上的网格节点在配置网格之前与主管理节点进行通信。

如有必要，还可以将包含 NTP 服务器或需要访问网格管理器或 API 的子网配置为网格子网。

自动向主管理节点注册节点

部署节点后，它们会使用网格网络向主管理节点注册自己。然后，您可以使用网格管理器， `configure-storagegrid.py` Python 脚本或安装 API 来配置网格并批准注册的节点。在网格配置期间，您可以配置多个网格子网。完成网格配置后，系统将在每个节点上创建通过网格网络网关到这些子网的静态路由。

禁用管理网络或客户端网络

如果要禁用管理网络或客户端网络，您可以在节点批准过程中从其中删除配置，也可以在安装完成后使用更改 IP 工具（请参见 配置 IP 地址）。

安装后准则

完成网格节点部署和配置后，请按照以下准则更改 DHCP 地址和网络配置。

- 如果使用 DHCP 分配 IP 地址，请为所使用网络上的每个 IP 地址配置 DHCP 预留。

  您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。

  > 当节点的 IP 地址发生更改时，节点会重新启动，如果 DHCP 地址更改同时影响多个节点，则发生原因 可能会中断。

- 如果要更改网格节点的 IP 地址，子网掩码和默认网关，必须使用更改 IP 过程。请参见 配置 IP 地址。

- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改，您可能需要重新建立这些连接。

网络端口参考

您必须确保网络基础架构能够在网格内的节点之间以及与外部客户端和服务之间提供内部和外部通信。您可能需要跨内部和外部防火墙，交换系统和路由系统进行访问。

请使用为提供的详细信息 内部网格节点通信 和 外部通信 以确定如何配置所需的每个端口。

内部网格节点通信

StorageGRID 内部防火墙仅允许传入网格网络上的特定端口，但端口 22 ， 80 ， 123 和 443 除外（请参见有关外部通信的信息）。负载平衡器端点定义的端口也接受连接。

> NetApp 建议您在网格节点之间启用 Internet 控制消息协议（ Internet Control Message Protocol ， ICMP ）流量。如果无法访问网格节点，则允许 ICMP 流量可以提高故障转移性能。

除了 ICMP 和表中列出的端口之外， StorageGRID 还使用虚拟路由器冗余协议（ VRRP ）。VRRP 是一种使用 IP 协议编号 112 的 Internet 协议。StorageGRID 仅在单播模式下使用 VRRP 。只有在满足条件时才需要 VRRP 高可用性组 已配置。

基于 **Linux** 的节点的准则

如果企业网络策略限制对其中任何端口的访问，则可以在部署时使用部署配置参数重新映射端口。有关端口重新映射和部署配置参数的详细信息，请参见：

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian

基于 **VMware** 的节点的准则

只有在需要定义 VMware 网络外部的防火墙限制时，才配置以下端口。

如果企业网络策略限制对其中任何端口的访问，则可以在使用 VMware vSphere Web Client 部署节点时重新映射端口，也可以在自动部署网格节点时使用配置文件设置重新映射端口。有关端口重新映射和部署配置参数的详细信息，请参见安装 VMware。

设备节点准则

如果企业网络策略限制对其中任何端口的访问，则可以使用 StorageGRID 设备安装程序重新映射端口。有关设备端口重新映射的详细信息，请参见：

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

StorageGRID 内部端口

Port	TCP 或 UDP	from	收件人：	详细信息
22.	TCP	主管理节点	所有节点	在维护过程中，主管理节点必须能够通过端口 22 上的 SSH 与所有其他节点进行通信。允许来自其他节点的 SSH 流量是可选的。
80	TCP	设备	主管理节点	StorageGRID 设备使用此节点与主管理节点进行通信以启动安装。
123.	UDP	所有节点	所有节点	网络时间协议服务。每个节点都使用 NTP 与其他节点同步其时间。
443.	TCP	所有节点	主管理节点	用于在安装和其他维护过程中与主管理节点进行状态通信。
1139.	TCP	存储节点	存储节点	存储节点之间的内部流量。
1501	TCP	所有节点	具有模块转换器的存储节点	报告，审核和配置内部流量。
1502	TCP	所有节点	存储节点	与 S3 和 Swift 相关的内部流量。
1504	TCP	所有节点	管理节点	NMS 服务报告和配置内部流量。
1505.	TCP	所有节点	管理节点	AMS 服务内部流量。
1506.	TCP	所有节点	所有节点	服务器状态内部流量。
1507.	TCP	所有节点	网关节点	负载平衡器内部流量。
1508.	TCP	所有节点	主管理节点	配置管理内部流量。

1509.	TCP	所有节点	归档节点	归档节点内部流量。
1511	TCP	所有节点	存储节点	元数据内部流量。
5353	UDP	所有节点	所有节点	也可用于在安装，扩展和恢复期间进行全网格 IP 更改以及主管理节点发现。
7001	TCP	存储节点	存储节点	Cassandra TLS 节点间集群通信。
7443	TCP	所有节点	管理节点	维护过程和错误报告的内部流量。
8443	TCP	主管理节点	设备节点	与维护模式操作步骤相关的内部流量。
9042	TCP	存储节点	存储节点	Cassandra 客户端端口。
9999	TCP	所有节点	所有节点	多个服务的内部流量。包括维护过程，指标和网络更新。
10226	TCP	存储节点	主管理节点	由 StorageGRID 设备使用，用于将 AutoSupport 消息从 E 系列 SANtricity 系统管理器转发到主管理节点。
11139.	TCP	归档 / 存储节点	归档 / 存储节点	存储节点和归档节点之间的内部流量。
18000	TCP	管理 / 存储节点	具有模块转换器的存储节点	帐户服务内部流量。
18001	TCP	管理 / 存储节点	具有模块转换器的存储节点	身份联合内部流量。
18002	TCP	管理 / 存储节点	存储节点	与对象协议相关的内部 API 流量。
18003	TCP	管理 / 存储节点	具有模块转换器的存储节点	平台为内部流量提供服务。

18017	TCP	管理 / 存储节点	存储节点	数据移动服务为云存储池提供内部流量。
18019	TCP	存储节点	存储节点	用于纠删编码的区块服务内部流量。
18082	TCP	管理 / 存储节点	存储节点	与 S3 相关的内部流量。
18083.	TCP	所有节点	存储节点	与 Swift 相关的内部流量。
18200 年	TCP	管理 / 存储节点	存储节点	有关客户端请求的其他统计信息。
19000	TCP	管理 / 存储节点	具有模块转换器的存储节点	Keystone 服务内部流量。

- 相关信息 *

外部通信

外部通信

客户端需要与网格节点进行通信才能载入和检索内容。使用的端口取决于所选的对象存储协议。这些端口需要可供客户端访问。

对端口的访问受限

如果企业网络策略限制对任何端口的访问，您可以使用 负载平衡器端点 允许对用户定义的端口进行访问。然后，您可以使用 不可信的客户端网络 仅允许对负载平衡器端点端口进行访问。

端口重新映射

要使用 SMTP ， DNS ， SSH 或 DHCP 等系统和协议，您必须在部署节点时重新映射端口。但是，您不应重新映射负载平衡器端点。有关端口重新映射的信息，请参见适用于您的平台的安装说明：

基于软件的节点

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian
- 安装 VMware

设备节点

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备

- SG5600 存储设备

用于外部通信的端口

下表显示了用于向节点进行流量的端口。

此列表不包括可能配置为的端口 负载平衡器端点 或用于 "系统日志服务器"。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
22.	TCP	SSH	服务笔记本电脑	所有节点	要执行控制台步骤，需要 SSH 或控制台访问。您也可以选择使用端口 2022 ，而不是 22 。
25.	TCP	SMTP	管理节点	电子邮件服务器	用于警报和基于电子邮件的 AutoSupport 。您可以使用电子邮件服务器页面覆盖默认端口设置 25 。
53.	TCP/UDP	DNS	所有节点	DNS 服务器	用于域名系统。
67	UDP	DHCP	所有节点	DHCP 服务	也可用于支持基于 DHCP 的网络配置。dhclient 服务不会对静态配置的网格运行。
68	UDP	DHCP	DHCP 服务	所有节点	也可用于支持基于 DHCP 的网络配置。对于使用静态 IP 地址的网格，不会运行 dhclient 服务。
80	TCP	HTTP	浏览器	管理节点	端口 80 重定向到管理节点用户界面的端口 443 。
80	TCP	HTTP	浏览器	设备	端口 80 重定向到 StorageGRID 设备安装程序的端口 8443 。
80	TCP	HTTP	具有模块转换器的存储节点	AWS	用于发送到 AWS 或其他使用 HTTP 的外部服务的平台服务消息。创建端点时，租户可以覆盖默认的 HTTP 端口设置 80 。
80	TCP	HTTP	存储节点	AWS	发送到使用 HTTP 的 AWS 目标的云存储池请求。配置云存储池时，网格管理员可以覆盖默认的 HTTP 端口设置 80 。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
111.	TCP/UDP	rpcbind	NFS 客户端	管理节点	由基于 NFS 的审核导出（ portmap ）使用。 • 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。
123.	UDP	NTP	主要 NTP 节点	外部 NTP	网络时间协议服务。选择为主 NTP 源的节点还会将时钟时间与外部 NTP 时间源同步。
137.	UDP	NetBIOS	SMB 客户端	管理节点	由基于 SMB 的审核导出用于需要 NetBIOS 支持的客户端。 • 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。
138.	UDP	NetBIOS	SMB 客户端	管理节点	由基于 SMB 的审核导出用于需要 NetBIOS 支持的客户端。 • 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。
139.	TCP	SMB	SMB 客户端	管理节点	由基于 SMB 的审核导出用于需要 NetBIOS 支持的客户端。 • 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
161.	TCP/UDP	SNMP	SNMP 客户端	所有节点	用于 SNMP 轮询。所有节点均提供基本信息；管理节点还提供警报和警报数据。配置后，默认为 UDP 端口 161 。 • 注： * 仅需要此端口，只有在配置了 SNMP 的情况下，才会在节点防火墙上打开此端口。如果您计划使用 SNMP ，则可以配置备用端口。 • 注： * 有关将 SNMP 与 StorageGRID 结合使用的信息，请联系您的 NetApp 客户代表。
162.	TCP/UDP	SNMP 通知	所有节点	通知目标	出站 SNMP 通知和陷阱默认为 UDP 端口 162 。 • 注： * 只有在启用 SNMP 并配置通知目标时，才需要此端口。如果您计划使用 SNMP ，则可以配置备用端口。 • 注： * 有关将 SNMP 与 StorageGRID 结合使用的信息，请联系您的 NetApp 客户代表。
389.	TCP/UDP	LDAP	具有模块转换器的存储节点	Active Directory/LDAP	用于连接到 Active Directory 或 LDAP 服务器以实现身份联合。
443.	TCP	HTTPS	浏览器	管理节点	供 Web 浏览器和管理 API 客户端用于访问 Grid Manager 和租户管理器。
443.	TCP	HTTPS	管理节点	Active Directory	如果启用了单点登录（ SSO ），则由连接到 Active Directory 的管理节点使用。
443.	TCP	HTTPS	归档节点	Amazon S3	用于从归档节点访问 Amazon S3 。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
443.	TCP	HTTPS	具有模块转换器的存储节点	AWS	用于发送到 AWS 或其他使用 HTTPS 的外部服务的平台服务消息。创建端点时，租户可以覆盖默认的 HTTP 端口设置 443 。
443.	TCP	HTTPS	存储节点	AWS	发送到使用 HTTPS 的 AWS 目标的云存储池请求。配置云存储池时，网格管理员可以覆盖默认 HTTPS 端口设置 443 。
445	TCP	SMB	SMB 客户端	管理节点	由基于 SMB 的审核导出使用。 • 注： * 只有在启用了基于 SMB 的审核导出时，才需要此端口。
903	TCP	NFS	NFS 客户端	管理节点	由基于 NFS 的审核导出使用（ `rpc.mountd` ）。 • 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。
2022 年	TCP	SSH	服务笔记本电脑	所有节点	要执行控制台步骤，需要 SSH 或控制台访问。您也可以选择使用端口 22 ，而不是 2022 。
2049.	TCP	NFS	NFS 客户端	管理节点	由基于 NFS 的审核导出（ NFS ）使用。 • 注： * 只有在启用了基于 NFS 的审核导出时，才需要此端口。
5696	TCP	KMIP	设备	公里	从配置了节点加密的设备到密钥管理服务器（ KMS ）的密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）外部流量，除非在 StorageGRID 设备安装程序的 KMS 配置页面上指定了其他端口。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
8022	TCP	SSH	服务笔记本电脑	所有节点	端口 8022 上的 SSH 允许访问设备和虚拟节点平台上的基本操作系统，以便进行支持和故障排除。此端口不用于基于 Linux 的（裸机）节点，并且不需要在网格节点之间或在正常操作期间访问。
8082	TCP	HTTPS	S3 客户端	网关节点	通过网关节点（ HTTPS ）发送到已弃用的 CLB 服务的 S3 客户端流量。
8083.	TCP	HTTPS	Swift 客户端	网关节点	在网关节点（ HTTPS ）上发送到已弃用的 CLB 服务的 Swift 客户端流量。
8084	TCP	HTTP	S3 客户端	网关节点	通过网关节点（ HTTP ）发送到已弃用的 CLB 服务的 S3 客户端流量。
8085	TCP	HTTP	Swift 客户端	网关节点	在网关节点（ HTTP ）上传输到已弃用的 CLB 服务的 Swift 客户端流量。
8443	TCP	HTTPS	浏览器	管理节点	可选。供 Web 浏览器和管理 API 客户端用于访问网格管理器。可用于分隔网格管理器和租户管理器通信。
9022	TCP	SSH	服务笔记本电脑	设备	在预配置模式下授予对 StorageGRID 设备的访问权限，以便提供支持和进行故障排除。在网格节点之间或正常操作期间，不需要访问此端口。
9091.	TCP	HTTPS	外部 Grafana 服务	管理节点	由外部 Grafana 服务使用，用于安全访问 StorageGRID Prometheus 服务。 • 注： * 只有在启用了基于证书的 Prometheus 访问时，才需要此端口。
9443	TCP	HTTPS	浏览器	管理节点	可选。供 Web 浏览器和管理 API 客户端用于访问租户管理器。可用于分隔网格管理器和租户管理器通信。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
18082	TCP	HTTPS	S3 客户端	存储节点	直接发送到存储节点（ HTTPS ）的 S3 客户端流量。
18083.	TCP	HTTPS	Swift 客户端	存储节点	Swift 客户端流量直接发送到存储节点（ HTTPS ）。
18084	TCP	HTTP	S3 客户端	存储节点	直接发送到存储节点（ HTTP ）的 S3 客户端流量。
18085	TCP	HTTP	Swift 客户端	存储节点	Swift 客户端流量直接发送到存储节点（ HTTP ）。

安装和维护设备硬件

SG100 和 SG1000 服务设备

SG100 和 SG1000 设备：概述

StorageGRID SG100 服务设备和 SG1000 服务设备可以作为网关节点和管理节点运行，以便在 StorageGRID 系统中提供高可用性负载平衡服务。这两个设备可以同时作为网关节点和管理节点（主节点或非主节点）运行。

设备功能

这两种型号的服务设备均可提供以下功能：

- StorageGRID 系统的网关节点或管理节点功能。
- StorageGRID 设备安装程序，用于简化节点部署和配置。
- 部署后，可以从现有管理节点或从下载到本地驱动器的软件访问 StorageGRID 软件。为了进一步简化部署过程，在制造过程中，设备会预加载最新版本的软件。
- 用于监控和诊断某些设备硬件的基板管理控制器（ BMC ）。
- 能够连接到所有三个 StorageGRID 网络，包括网格网络，管理网络和客户端网络：
  - SG100 最多支持四个 10 GbE 或 25 GbE 网格网络和客户端网络连接。
  - SG1000 最多支持四个 10 GbE ， 25 GbE ， 40 GbE 或 100 GbE 网格网络和客户端网络连接。

SG100 和 **SG1000** 图表

此图显示了 SG100 和 SG1000 的正面，其中已卸下挡板。

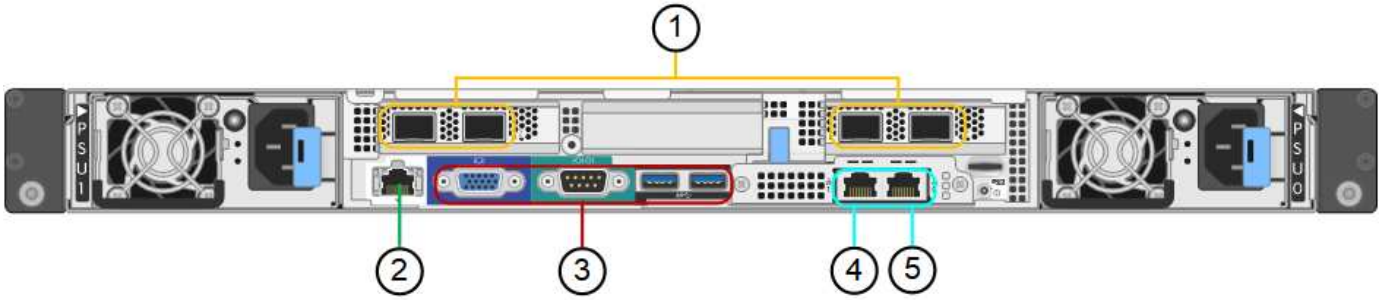
> 从正面看，除了挡板上的产品名称之外，这两个设备是相同的。

橙色轮廓所示的两个固态驱动器（ SSD ）用于存储 StorageGRID 操作系统，并使用 RAID1 进行镜像以实现冗余。将 SG100 或 SG1000 服务设备配置为管理节点时，这些驱动器用于存储审核日志，指标和数据库表。

其余驱动器插槽为空。

SG100 背面的连接器

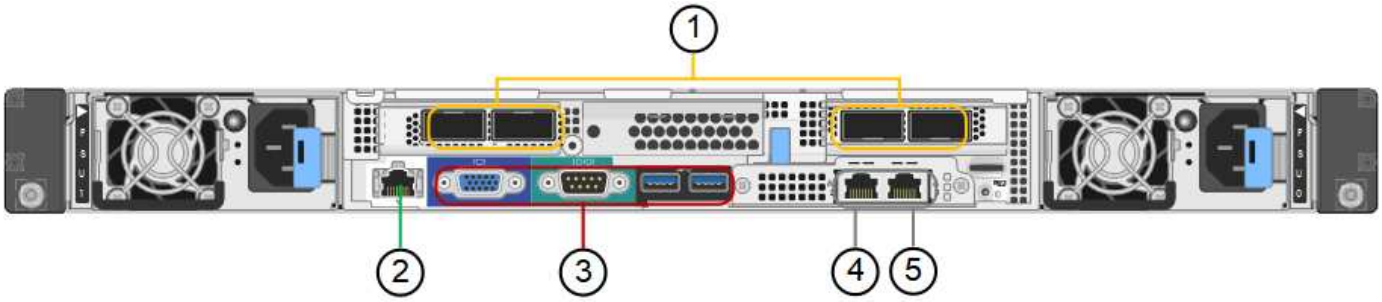
此图显示了 SG100 背面的连接器。



	Port	Type	使用 ...
1.	网络端口 1-4	10/225-GbE ，根据缆线或 SFP 收发器类型（支持 SFP28 和 SFP+ 模块），交换机速度和已配置的链路速度	连接到网格网络和 StorageGRID 客户端网络。
2.	BMC 管理端口	1-GbE （ RJ-45 ）	连接到设备基板管理控制器。
3.	诊断和支持端口	• VGA • 串行， 115200 8-N-1 • USB	保留供技术支持使用。
4.	管理网络端口 1	1-GbE （ RJ-45 ）	将设备连接到 StorageGRID 的管理网络。
5.	管理网络端口 2	1-GbE （ RJ-45 ）	选项： • 与管理端口 1 绑定，以便与 StorageGRID 的管理网络建立冗余连接。 • 保持断开连接并可用于临时本地访问（ IP 169.254.0.1 ）。 • 安装期间，如果 DHCP 分配的 IP 地址不可用，请使用端口 2 进行 IP 配置。

SG1000 背面的连接器

此图显示了 SG1000 背面的连接器。



	Port	Type	使用 ...
1.	网络端口 1-4	10/25/40/100-GbE ，基于缆线或收发器类型，交换机速度和已配置的链路速度。本机支持 QSFP28 和 QSFP+ （ 40/100GbE ） ， SFP28/SFP+ 收发器可与 QSA （单独销售）结合使用，以使用 10/25GbE 速度。	连接到网格网络和 StorageGRID 客户端网络。
2.	BMC 管理端口	1-GbE （ RJ-45 ）	连接到设备基板管理控制器。
3.	诊断和支持端口	• VGA • 串行， 115200 8-N-1 • USB	保留供技术支持使用。
4.	管理网络端口 1	1-GbE （ RJ-45 ）	将设备连接到 StorageGRID 的管理网络。
5.	管理网络端口 2	1-GbE （ RJ-45 ）	选项： • 与管理端口 1 绑定，以便与 StorageGRID 的管理网络建立冗余连接。 • 保持断开连接并可用于临时本地访问（ IP 169.254.0.1 ）。 • 安装期间，如果 DHCP 分配的 IP 地址不可用，请使用端口 2 进行 IP 配置。

SG100 和 SG1000 应用程序

您可以通过各种方式配置 StorageGRID 服务设备，以提供网关服务以及某些网格管理服务的冗余。

可以通过以下方式部署设备：

- 作为网关节点添加到新网格或现有网格中
- 作为主管理节点或非主管理节点添加到新网格中，或者作为非主管理节点添加到现有网格中
- 同时作为网关节点和管理节点（主节点或非主节点）运行

该设备有助于在 S3 或 Swift 数据路径连接中使用高可用性（ HA ）组和智能负载平衡。

以下示例介绍了如何最大限度地提高设备的功能：

- 使用两个 SG100 或两个 SG1000 设备通过将其配置为网关节点来提供网关服务。

  不要在同一站点中部署 SG100 和 SG1000 服务设备。可能会导致性能不可预测。

- 使用两个 SG100 或两个 SG1000 设备为某些网格管理服务提供冗余。为此，请将每个设备配置为管理节点。
- 使用两个 SG100 或两个 SG1000 设备提供通过一个或多个虚拟 IP 地址访问的高可用性负载平衡和流量调整服务。为此，请将设备配置为管理节点或网关节点的任意组合，并将这两个节点添加到同一 HA 组。

  如果在同一 HA 组中使用管理节点和网关节点，则 CLB （连接负载平衡器）端口和仅管理节点端口不会进行故障转移。有关配置 HA 组的说明，请参见有关管理 StorageGRID 的说明。

  CLB 服务已弃用。

在与 StorageGRID 存储设备结合使用时， SG100 和 SG1000 服务设备均支持部署纯设备网格，而不依赖于外部虚拟机管理程序或计算硬件。

相关信息

管理 StorageGRID

安装和部署概述

您可以在首次部署 StorageGRID 时安装一个或多个 StorageGRID 服务设备，也可以稍后在扩展过程中添加服务设备节点。

您需要的内容

您的 StorageGRID 系统正在使用所需版本的 StorageGRID 软件。

设备	所需的 **StorageGRID** 版本
SG100	11.4 或更高版本（建议使用最新的修补程序）

设备	所需的 **StorageGRID** 版本
SG1000	11.3 或更高版本（建议使用最新的修补程序）

安装和部署任务

准备 StorageGRID 设备并将其添加到网格包括四个主要步骤：

1. 准备安装：
   - 正在准备安装站点
   - 打开包装箱的包装并检查包装箱中的物品
   - 获取其他设备和工具
   - 验证网络配置
   - 可选：如果您计划对所有设备数据进行加密，请配置外部密钥管理服务器（ KMS ）。有关外部密钥管理的详细信息，请参见 StorageGRID 管理说明。
2. 安装硬件：
   - 注册硬件
   - 将设备安装到机柜或机架中
   - 为设备布线
   - 连接电源线并接通电源
   - 查看启动状态代码
3. 配置硬件：
   - 访问 StorageGRID 设备安装程序并配置连接到 StorageGRID 网络所需的链路和网络 IP 设置
   - 访问设备上的基板管理控制器（ BMC ）接口。
   - 可选：如果您计划使用外部 KMS 对设备数据进行加密，请启用节点加密。
4. 部署设备网关或管理节点

   安装并配置设备硬件后，您可以将此设备部署为 StorageGRID 系统中的网关节点和管理节点。SG100 和 SG1000 设备可以同时作为网关节点和管理节点（主节点和非主节点）运行。

任务	说明
在新的 StorageGRID 系统中部署设备网关或管理节点	部署服务设备节点
将设备网关或管理节点添加到现有 StorageGRID 系统	展开StorageGRID 系统
在节点恢复操作中部署设备网关或管理节点	恢复和维护StorageGRID 系统

相关信息

扩展网格

恢复和维护您的网格

管理 StorageGRID

准备安装（ SG100 和 SG1000 ）

准备安装 StorageGRID 设备需要准备站点并获取所有必需的硬件，缆线和工具。您还应收集 IP 地址和网络信息。

相关信息

Web 浏览器要求

准备站点（ SG100 和 SG1000 ）

在安装设备之前，您必须确保要使用的站点和机柜或机架符合 StorageGRID 设备的规格。

步骤

1. 确认站点满足温度，湿度，海拔范围，气流，散热， 布线，电源和接地。有关详细信息，请参见 NetApp Hardware Universe 。
2. 确认您所在位置的交流电源电压正确（介于 120 到 240 伏之间）。
3. 获取一个 19 英寸（ 48.3 厘米）的机柜或机架，以适合此大小的磁盘架（不带缆线）：

高度	宽度	深度	最大重量
1.70 英寸 （ 4.32 厘米）	17.32 英寸 （ 44.0 厘米）	32.0 英寸 （ 81.3 厘米）	39 磅 （ 17.7 千克）

4. 确定要在何处安装设备。

相关信息

"NetApp Hardware Universe"

"NetApp 互操作性表工具"

打开包装箱（ SG100 和 SG1000 ）

安装 StorageGRID 设备之前，请打开所有包装箱的包装，并将包装箱上的物品与包装清单上的物品进行比较。

设备硬件

- * SG100 或 SG1000*

- * 导轨套件及说明 *

电源线

StorageGRID 设备的发货包括以下电源线：

- * 您所在国家或地区有两条电源线 *

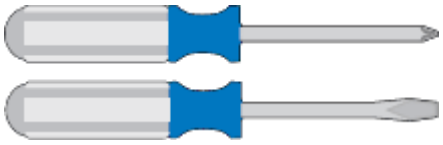
  您的机柜可能使用专用电源线，而不是设备随附的电源线。

获取其他设备和工具（ **SG100** 和 **SG1000** ）

在安装 StorageGRID 设备之前，请确认您拥有所需的所有附加设备和工具。

要安装和配置硬件，您需要使用以下附加设备：

- * 螺丝刀 *

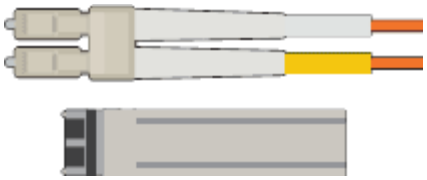


  十字线编号2 把螺丝刀

  中型平口螺丝刀

- * ESD 腕带 *

- * 光缆和收发器 *



- 缆线
  - 双轴电缆 / 铜缆（ 1 到 4 ）

    或

  - 光纤 / 光纤（ 1 到 4 ）
- 根据链路速度，每个收发器 / 适配器 1 到 4 个（不支持混合速度）
  - SG100 ：

链路速度（ **GbE** ）	所需设备
10	SFP+ 收发器
25.	SFP28 收发器

  - SG1000 ：

链路速度（ **GbE** ）	所需设备
10	QSFP-SFP 适配器（ QSA ）和 SFP+ 收发器
25.	QSFP-SFP 适配器（ QSA ）和 SFP28 收发器
40	QSFP + 收发器
100	QSP28 收发器

- * RJ-45 （ Cat5/Cat5e/Cat6/Cat6a ）以太网缆线 *

- * 服务笔记本电脑 *

支持的 Web 浏览器

1 GbE （ RJ-45 ）端口

某些端口可能不支持 10/100 以太网速度。

- * 可选工具 *

带十字头的电钻

Flashlight

查看设备网络连接（ **SG100** 和 **SG1000** ）

在安装 StorageGRID 设备之前，您应了解可以将哪些网络连接到此设备。

将 StorageGRID 设备部署为 StorageGRID 系统中的节点时，您可以将其连接到以下网络：

- * 适用于 StorageGRID 的网格网络 * ： 网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。网格网络为必填项。
- * 适用于 StorageGRID 的管理网络 * ： 管理网络是一个用于系统管理和维护的封闭网络。管理网络通常是一个专用网络，不需要在站点之间进行路由。管理网络是可选的。
- * 适用于 StorageGRID 的客户端网络： * 客户端网络是一种开放网络，用于访问包括 S3 和 Swift 在内的客户端应用程序。客户端网络可提供对网格的客户端协议访问，从而可以隔离和保护网格网络。您可以配置客户端网络，以便仅使用您选择打开的端口通过此网络访问设备。客户端网络是可选的。
- 服务设备的 * BMC 管理网络 * （可选）： 通过此网络，您可以访问 SG100 和 SG1000 中的基板管理控制器，这些设备可用于监控和管理设备中的硬件组件。此管理网络可以与 StorageGRID 的管理网络相同，也可以是一个独立的管理网络。

  如果未连接可选的 BMC 管理网络，则某些支持和维护过程将更难执行。除非出于支持目的需要，否则您可以使 BMC 管理网络保持未连接状态。

相关信息

收集安装信息（ SG100 和 SG1000 ）

缆线设备 SG100 和 SG1000

网络连接准则

网格入门

SG100 和 **SG1000** 设备的端口绑定模式

在为 SG100 和 SG1000 设备配置网络链路时，您可以对连接到网格网络和可选客户端网络的端口以及连接到可选管理网络的 1-GbE 管理端口使用端口绑定。端口绑定可在 StorageGRID 网络和设备之间提供冗余路径，从而有助于保护数据。

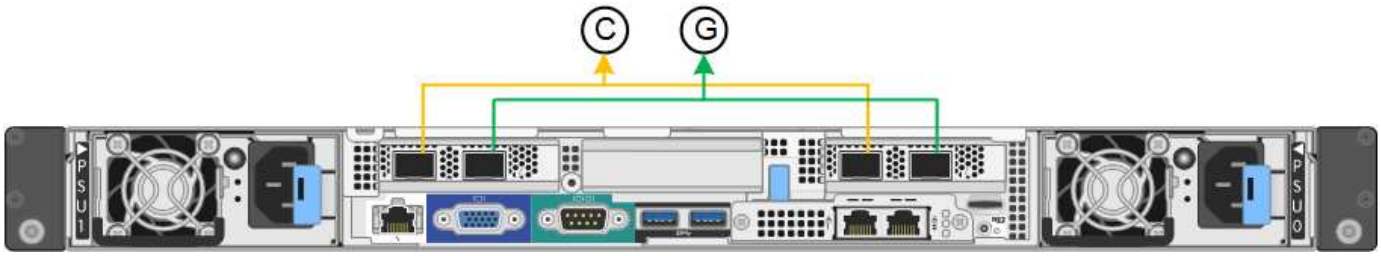
网络绑定模式

服务设备上的网络端口支持网格网络和客户端网络连接的固定端口绑定模式或聚合端口绑定模式。

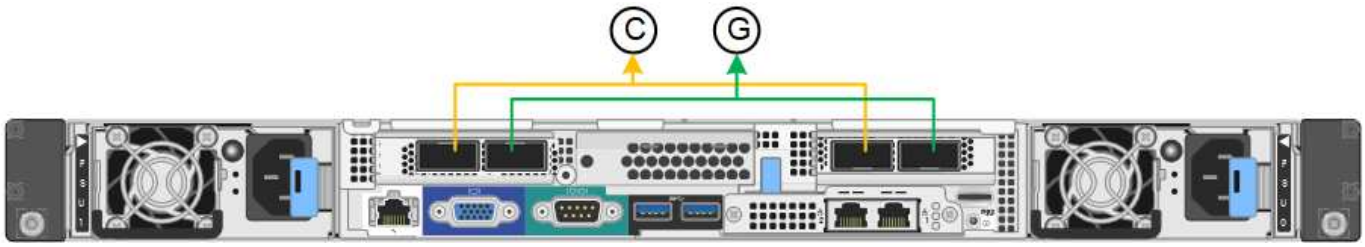
固定端口绑定模式

固定端口绑定模式是网络端口的默认配置。

- SG100 固定端口绑定模式 *



- SG1000 固定端口绑定模式 *



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

使用固定端口绑定模式时，可以使用主动备份模式或链路聚合控制协议模式（ LACP 802.3ad ）绑定端口。

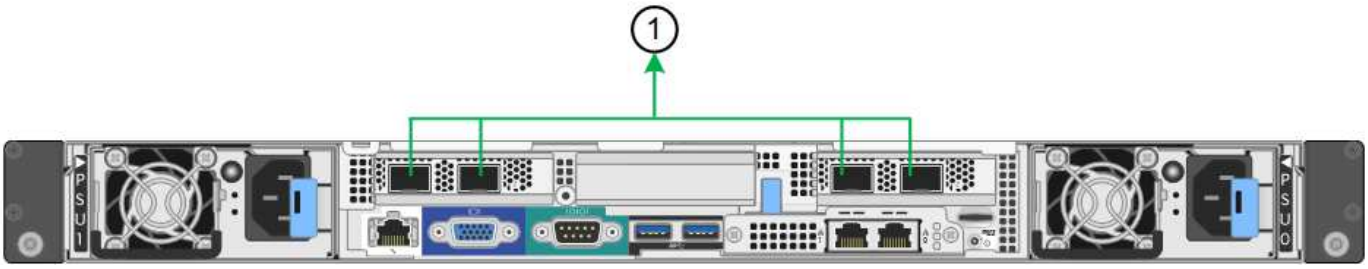
- 在主动备份模式（默认）下，一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。端口 4 为端口 2 （网格网络）提供备份路径，端口 3 为端口 1 （客户端网络）提供备份路径。
- 在 LACP 模式下，每对端口在服务设备和网络之间形成一个逻辑通道，从而提高吞吐量。如果一个端口发生故障，另一个端口将继续提供通道。吞吐量会降低，但连接不会受到影响。

> 如果不需要冗余连接，则每个网络只能使用一个端口。但是，请注意，安装 StorageGRID 后，可能会在网格管理器中触发 * 服务设备链路已关闭 * 警报，指示已拔下缆线。您可以安全地禁用此警报规则。

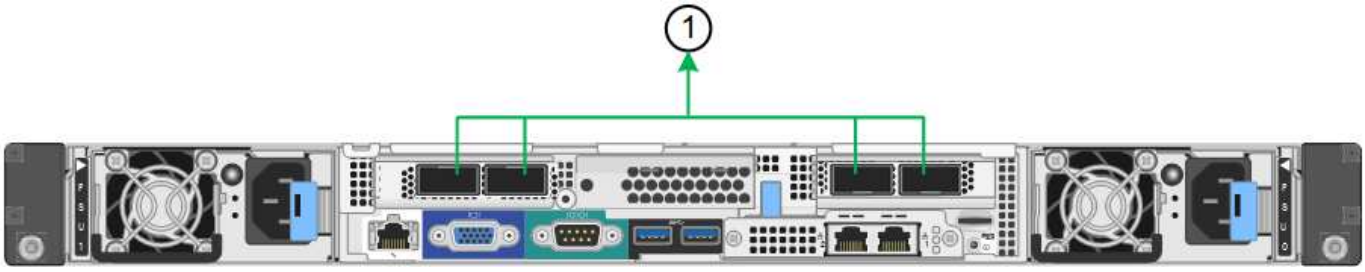
聚合端口绑定模式

聚合端口绑定模式可显著提高每个 StorageGRID 网络的吞吐量，并提供额外的故障转移路径。

- SG100 聚合端口绑定模式 *



- SG1000 聚合端口绑定模式 *



Callout	哪些端口已绑定
1.	所有连接的端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

如果您计划使用聚合端口绑定模式：

- 您必须使用 LACP 网络绑定模式。
- 您必须为每个网络指定唯一的 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。
- 这些端口必须连接到可支持 VLAN 和 LACP 的交换机。如果多个交换机参与 LACP 绑定，则这些交换机必须支持多机箱链路聚合组（ MLAG ）或等效项。

- 您必须了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。

如果不想使用全部四个端口，可以使用一个，两个或三个端口。使用多个端口可以最大程度地提高在其中一个端口出现故障时某些网络连接仍可用的可能性。

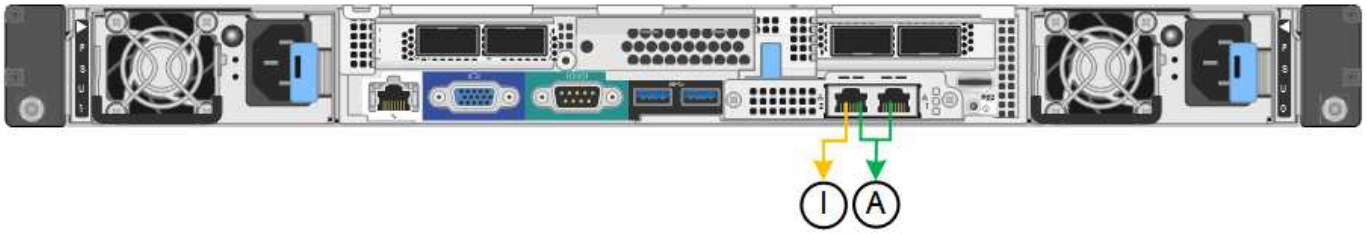
> 如果您选择使用的端口少于四个、请注意、在安装设备节点后、可能会在网格管理器中触发*服务设备链路已关闭*警报、指示已拔下电缆。您可以安全地为触发的警报禁用此警报规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。

管理端口的网络绑定模式

对于服务设备上的两个 1-GbE 管理端口，您可以选择独立网络绑定模式或主动备份网络绑定模式来连接到可选的管理网络。

- SG100 网络管理端口 *

- SG1000 网络管理端口 *



在独立模式下，只有左侧的管理端口连接到管理网络。此模式不提供冗余路径。右侧的管理端口未连接，可用于临时本地连接（使用 IP 地址 169.254.0.1 ）

在主动备份模式下，两个管理端口均连接到管理网络。一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。将这两个物理端口绑定到一个逻辑管理端口可提供指向管理网络的冗余路径。

> 如果在将 1-GbE 管理端口配置为主动备份模式后需要临时本地连接到服务设备，请从两个管理端口拔下缆线，将临时缆线插入右侧的管理端口，然后使用 IP 地址 169.254.0.1 访问此设备。

Callout	网络绑定模式
答	主动备份模式。这两个管理端口都绑定到一个连接到管理网络的逻辑管理端口。

Callout	网络绑定模式
I	独立模式。左侧端口连接到管理网络。右侧端口可用于临时本地连接（ IP 地址 169.254.0.1 ）。

收集安装信息（ **SG100** 和 **SG1000** ）

在安装和配置 StorageGRID 设备时，您必须做出决策并收集有关以太网交换机端口， IP 地址以及端口和网络绑定模式的信息。记下连接到设备的每个网络所需的信息。安装和配置硬件需要这些值。

管理和维护端口

StorageGRID 管理网络是一个可选网络，用于系统管理和维护。此设备使用设备上的以下 1-GbE 管理端口连接到管理网络。

- SG100 RJ-45 端口 *

- SG1000 RJ-45 端口 *

- 管理和维护连接 *

所需信息	您的价值
已启用管理网络	选择一项： • 否 • 是（默认）
网络绑定模式	选择一项： • 独立（默认） • 主动备份
图中圈出的左侧端口的交换机端口（独立网络绑定模式的默认活动端口）	
图中圈出的右侧端口的交换机端口（仅限主动备份网络绑定模式）	

所需信息	您的价值
管理网络端口的 MAC 地址 • 注： * 设备正面的 MAC 地址标签列出了 BMC 管理端口的 MAC 地址。要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 * 。 2 例如，如果标签上的 **MAC** 地址以 ***09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 * （ *y* ） FF* 结尾，则管理端口的 MAC 地址将以 * （ *y*+1 ） 01* 结尾。您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 * + 2 =* 来轻松进行计算。	
DHCP 为管理网络端口分配的 IP 地址（如果在启动后可用） • 注： * 您可以使用 MAC 地址查找已分配的 IP 来确定 DHCP 分配的 IP 地址。	• IPv4 地址（ CIDR ）： • 网关
您计划在管理网络上用于设备节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
管理网络子网（ CIDR ）	

网络端口

设备上的四个网络端口连接到 StorageGRID 网格网络和可选客户端网络。

• 网络连接 *

所需信息	您的价值
链路速度	对于 SG100 ，请选择以下选项之一： • 自动（默认） • 10 GbE • 25 GbE 对于 SG1000 ，请选择以下选项之一： • 自动（默认） • 10 GbE • 25 GbE • 40 GbE • 100 GbE • 注： * 对于 SG1000 ， 10-GbE 和 25-GbE 速度要求使用 QSA 适配器。
端口绑定模式	选择一项： • FIXED （默认） • 聚合
端口 1 的交换机端口（固定模式的客户端网络）	
端口 2 的交换机端口（固定模式的网格网络）	
端口 3 的交换机端口（固定模式的客户端网络）	
端口 4 的交换机端口（固定模式的网格网络）	

网格网络端口

适用于 StorageGRID 的网格网络是一个必需的网络，用于所有内部 StorageGRID 流量。此设备使用四个网络端口连接到网格网络。

- 网格网络连接 *

所需信息	您的价值
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）

所需信息	您的价值
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为网格网络分配的 IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划用于网格网络上设备节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
网格网络子网（ GRID ）	
最大传输单元（ Maximum Transmission Unit ， MTU ）设置（可选）您可以使用默认值 1500 ，也可以将 MTU 设置为适合巨型帧的值，例如 9000 。	

客户端网络端口

适用于 StorageGRID 的客户端网络是一个可选网络，通常用于提供对网格的客户端协议访问。此设备使用四个网络端口连接到客户端网络。

- 客户端网络连接 *

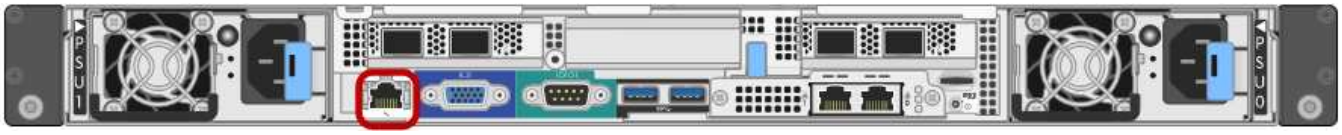
所需信息	您的价值
已启用客户端网络	选择一项： • 否（默认） • 是的。
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）

所需信息	您的价值
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为客户端网络分配的 IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划在客户端网络上用于设备节点的静态 IP 地址 • 注意： * 如果启用了客户端网络，则设备上的默认路由将使用此处指定的网关。	• IPv4 地址（ CIDR ）： • 网关

BMC 管理网络端口

您可以使用图中圈出的 1-GbE 管理端口访问服务设备上的 BMC 接口。此端口支持使用智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）标准通过以太网远程管理控制器硬件。

- SG100 BMC 管理端口 *



- SG1000 BMC 管理端口 *

- BMC 管理网络连接 *

所需信息	您的价值
要连接到 BMC 管理端口的以太网交换机端口（在图中圈出）	
为 BMC 管理网络分配的 DHCP IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划用于 BMC 管理端口的静态 IP 地址	• IPv4 地址（ CIDR ）： • 网关

相关信息

SG100 和 SG1000 设备概述

缆线设备 SG100 和 SG1000

配置 StorageGRID IP 地址

安装硬件（SG100 和 SG1000）

注册硬件

注册设备硬件具有支持优势。

步骤

1. 找到设备的机箱序列号。

   您可以在装箱单上，确认电子邮件中或打开设备包装后在设备上找到此编号。

2. 访问 NetApp 支持站点，网址为 "mysupport.netapp.com"。
3. 确定是否需要注册硬件：

如果您是 ...	请按照以下步骤操作 ...
现有 NetApp 客户	a. 使用您的用户名和密码登录。 b. 选择 * 产品 * > * 我的产品 * 。 c. 确认新序列号已列出。 d. 如果不是，请按照适用于新 NetApp 客户的说明进行操作。
NetApp 新客户	a. 单击 * 立即注册 * ，然后创建帐户。 b. 选择 * 产品 * > * 注册产品 * 。 c. 输入产品序列号和请求的详细信息。 注册获得批准后，您可以下载所需的任何软件。审批过程可能需要长达 24 小时。

将设备安装到机柜或机架中（SG100 和 SG1000）

您必须在机柜或机架中为设备安装一组导轨，然后将设备滑入导轨。

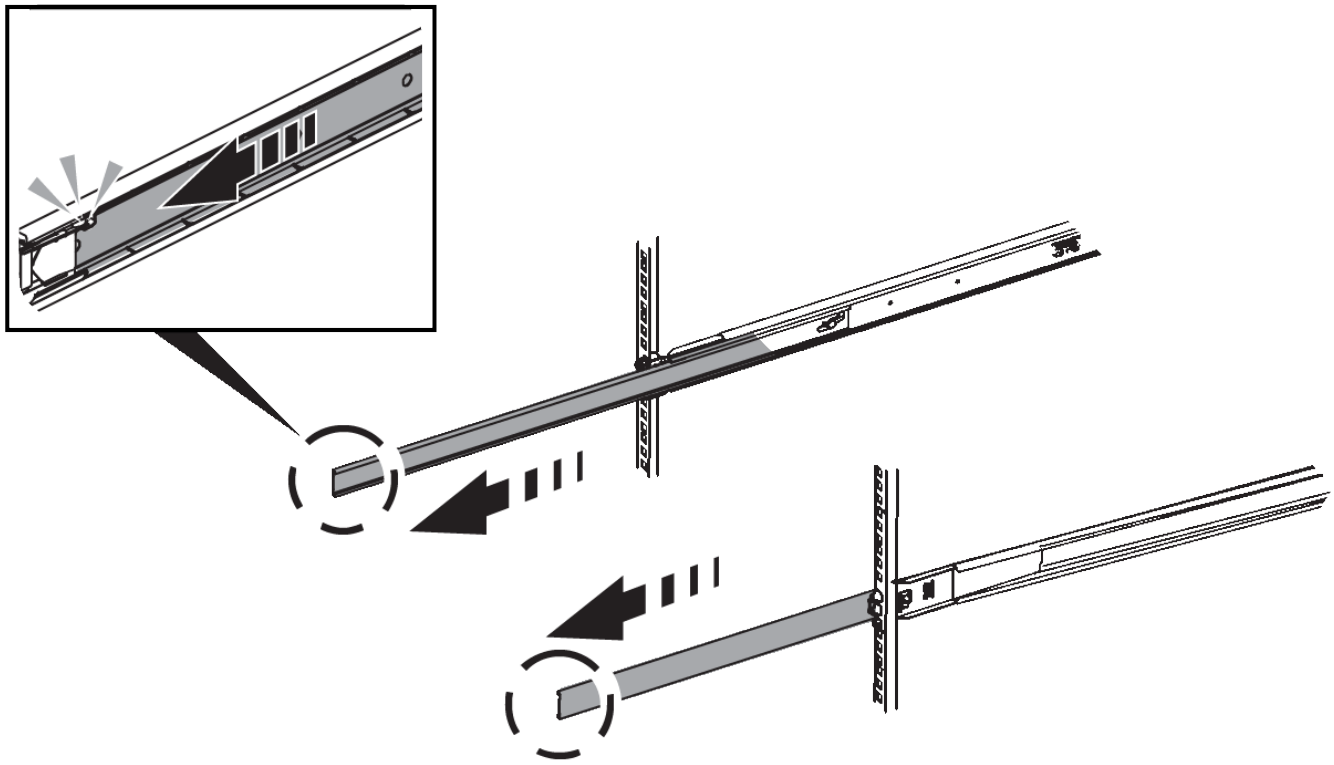
您需要的内容

- 您已查看包装盒中的安全通知文档，并了解移动和安装硬件的预防措施。

- 导轨套件随附了相关说明。

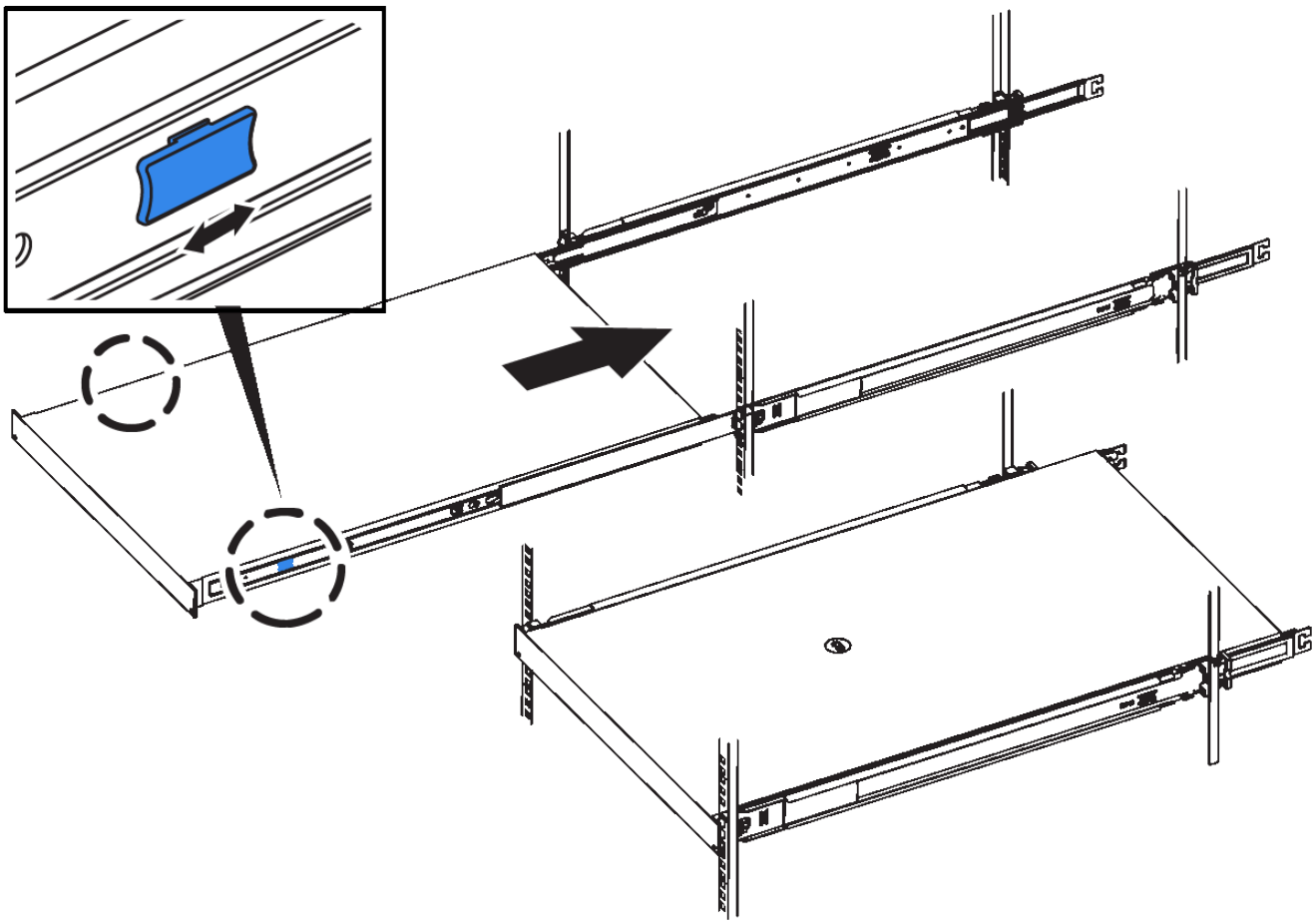
步骤

1. 请仔细按照导轨套件的说明在机柜或机架中安装导轨。
2. 在机柜或机架中安装的两个导轨上，展开导轨的可移动部分，直到听到卡嗒声为止。



3. 将设备插入导轨。
4. 将设备滑入机柜或机架。

   如果无法再移动设备，请拉动机箱两侧的蓝色闩锁，将设备滑入原处。



在打开设备电源之前，请勿连接前挡板。

缆线设备 **SG100** 和 **SG1000**

您必须将设备上的管理端口连接到服务笔记本电脑，并将设备上的网络端口连接到网格网络和适用于 StorageGRID 的可选客户端网络。

您需要的内容

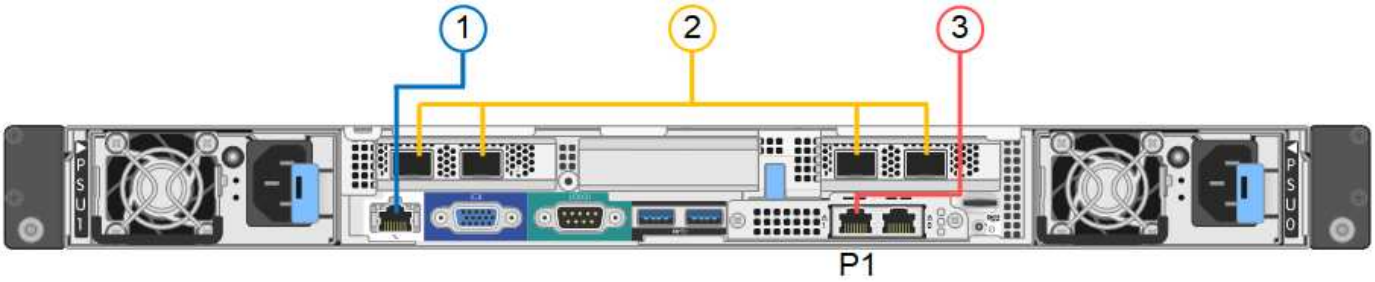
- 您有一根 RJ-45 以太网缆线用于连接管理端口。
- 您可以选择以下网络端口之一。这些项目不随设备提供。
  - 一到四根双轴缆线，用于连接四个网络端口。
  - 对于 SG100 ，如果您计划使用光缆连接端口，则需要一到四个 SFP+ 或 SFP28 收发器。
  - 对于 SG1000 ，如果您计划使用光缆连接端口，则需要一到四个 QSFP+ 或 QSFP28 收发器。

* 受到激光辐射的风险 * —请勿拆卸或卸下 SFP 或 QSFP 收发器的任何部件。您可能受到激光辐射的影响。

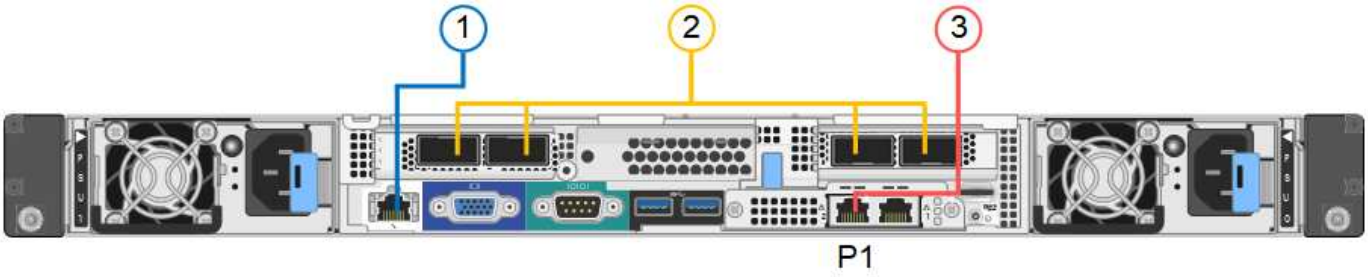
关于此任务

下图显示了设备背面的端口。

- SG100 端口连接 *



- SG1000 端口连接 *



	Port	端口类型	功能
1.	设备上的 BMC 管理端口	1-GbE （RJ-45）	连接到访问 BMC 接口的网络。
2.	设备上有四个网络端口	• 对于 SG100：10/225-GbE • 对于 SG1000：10/25/40/100-GbE	连接到网格网络和 StorageGRID 客户端网络。
3.	设备上的管理网络端口（图中标记为 P1）	1-GbE （RJ-45） • 重要信息： * 此端口仅以 1000 BASE/ 全满运行，不支持 10 或 100 MB 速度。	将设备连接到 StorageGRID 的管理网络。
	设备上最右侧的 RJ-45 端口	1-GbE （RJ-45） • 重要信息： * 此端口仅以 1000 BASE/ 全满运行，不支持 10 或 100 MB 速度。	• 如果要与管理网络建立冗余连接，则可以与管理端口 1 绑定。 • 可以保持断开连接，并可用于临时本地访问（IP 169.254.0.1）。 • 在安装期间，如果 DHCP 分配的 IP 地址不可用，则可以使用将设备连接到服务笔记本电脑。

步骤

1. 使用以太网缆线将设备上的 BMC 管理端口连接到管理网络。

虽然此连接是可选的，但建议便于支持。

2. 使用双轴缆线或光缆和收发器将设备上的网络端口连接到相应的网络交换机。

   这四个网络端口必须使用相同的链路速度。请参见下表，了解根据您的硬件和链路速度所需的设备。

SG100 链路速度（ **GbE** ）	所需设备
10	SFP+ 收发器
25.	SFP28 收发器
SG1000 链路速度（ GbE ）	所需设备
10	QSA 和 SFP+ 收发器
25.	QSA 和 SFP28 收发器
40	QSFP + 收发器
100	QSP28 收发器

   - 如果您计划使用固定端口绑定模式（默认），请将端口连接到 StorageGRID 网格和客户端网络，如表所示。

Port	连接到 ...
端口 1	客户端网络（可选）
端口 2	网格网络
端口 3	客户端网络（可选）
端口 4	网格网络

   - 如果您计划使用聚合端口绑定模式，请将一个或多个网络端口连接到一个或多个交换机。您应至少连接四个端口中的两个，以避免发生单点故障。如果在一个 LACP 绑定中使用多个交换机，则这些交换机必须支持 MLAG 或等效项。

3. 如果您计划使用 StorageGRID 管理网络，请使用以太网缆线将设备上的管理网络端口连接到管理网络。

连接电源线并接通电源（ **SG100** 和 **SG1000** ）

连接网络缆线后，您可以为设备接通电源。

步骤

1. 将电源线分别连接到设备中的两个电源设备。
2. 将这两条电源线连接到机柜或机架中的两个不同配电单元（ PDU ）。
3. 如果设备正面的电源按钮当前未呈蓝色亮起，请按此按钮打开设备电源。

   在启动过程中，请勿再次按电源按钮。

4. 如果发生错误，请更正任何问题。
5. 如果已卸下前挡板，请将其连接到设备。

相关信息

查看 SG100 和 SG1000 设备上的状态指示符

查看 **SG100** 和 **SG1000** 设备上的状态指示符

设备中的指示灯可帮助您确定设备控制器和两个 SSD 的状态。

设备指示灯和按钮

	显示	**State**
1.	电源按钮	• 蓝色：设备已启动。 • off ： 设备已关闭。
2.	重置按钮	使用此按钮可对控制器执行硬重置。
3.	识别按钮	此按钮可以设置为闪烁，打开（稳定）或关闭。 • 蓝色，闪烁：表示机柜或机架中的设备。 • 蓝色，实心：表示机柜或机架中的设备。 • off ： 无法在机柜或机架中直观地识别设备。
4.	警报 LED	• 琥珀色，稳定亮起：发生错误。 • 注： * 要查看启动和错误代码，您必须访问 BMC 界面。 • off ： 不存在任何错误。

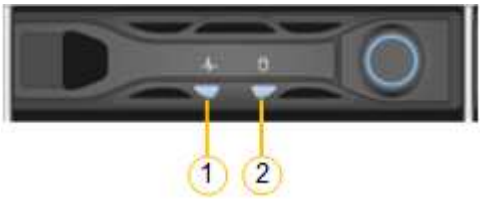
常规启动代码

在启动期间或设备硬重置后，将发生以下情况：

1. 基板管理控制器（ BMC ）会记录启动顺序的代码，包括发生的任何错误。
2. 电源按钮将亮起。
3. 如果在启动期间发生任何错误，警报 LED 将亮起。

   要查看启动和错误代码，您必须访问 BMC 界面。

SSD 指示灯



LED	显示	State
1.	驱动器状态 / 故障	• 蓝色（实心）：驱动器已联机 • 琥珀色（闪烁）：驱动器故障 • off ： 插槽为空
2.	驱动器处于活动状态	蓝色（闪烁）：正在访问驱动器

相关信息

硬件安装故障排除（ SG100 和 SG1000 ）

配置 BMC 接口（ SG100 和 SG1000 ）

配置 **StorageGRID** 连接（ **SG100** 和 **SG1000** ）

在将服务设备部署为 StorageGRID 系统中的节点之前，您必须配置设备与计划使用的网络之间的连接。您可以通过浏览到服务设备上预安装的 StorageGRID 设备安装程序来配置网络连接。

访问 **StorageGRID** 设备安装程序

您必须访问 StorageGRID 设备安装程序来配置设备与三个 StorageGRID 网络之间的连接：网格网络，管理网络（可选）和客户端网络（可选）。

您需要的内容

- 您正在使用可连接到 StorageGRID 管理网络的任何管理客户端。
- 客户端具有 支持的 Web 浏览器。

- 服务设备已连接到您计划使用的所有 StorageGRID 网络。
- 您知道这些网络上服务设备的 IP 地址，网关和子网。
- 您已配置计划使用的网络交换机。

关于此任务

要首次访问 StorageGRID 设备安装程序，您可以使用 DHCP 为服务设备上的管理网络端口分配的 IP 地址（假设它已连接到管理网络），也可以将服务笔记本电脑直接连接到服务设备。

步骤

1. 如果可能，请使用服务设备上管理网络端口的 DHCP 地址来访问 StorageGRID 设备安装程序。

   ◦ SG100 管理网络端口 *

   ◦ SG1000 管理网络端口 *

   a. 找到服务器设备正面的 MAC 地址标签，然后确定管理网络端口的 MAC 地址。

      MAC 地址标签列出了 BMC 管理端口的 MAC 地址。

   要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 * 。 2 例如，如果标签上的 **MAC** 地址以 ***09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 * （ *y* ） FF* 结尾，则管理端口的 MAC 地址将以 * （ *y*+1 ） 01* 结尾。您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 * + 2 =* 来轻松进行计算。

   a. 向网络管理员提供 MAC 地址，以便他们可以在管理网络上查找设备的 DHCP 地址。

   b. 在客户端中，输入 StorageGRID 设备安装程序的以下 URL： + ` * https://*services-appliance_IP*:8443*`

      对于 ` service-appliation_ip_` ，请使用 DHCP 地址。

   c. 如果系统提示您显示安全警报，请使用浏览器的安装向导查看并安装证书。

      下次访问此 URL 时，不会显示此警报。

   此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。

2. 或者，如果无法使用 DHCP 获取 IP 地址，请使用链路本地连接访问 StorageGRID 设备安装程序。

   a. 使用以太网缆线将服务笔记本电脑直接连接到服务设备上最右侧的 RJ-45 端口。

- SG100 链路本地连接 *

- SG1000 链路本地连接 *

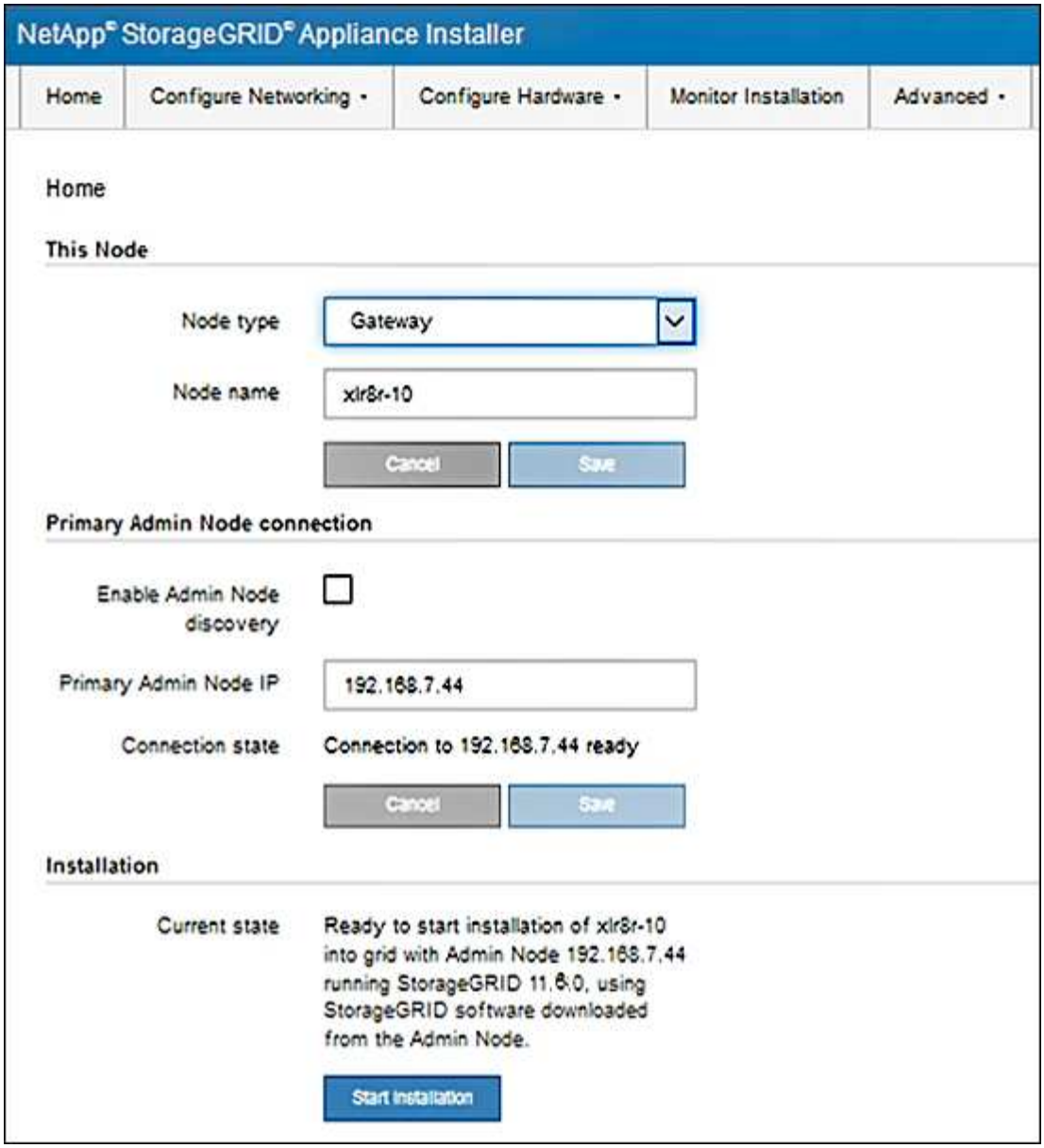
b. 打开 Web 浏览器。

c. 输入 StorageGRID 设备安装程序的 URL： + ` * https://169.254.0.1:8443*`

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。

> 如果无法通过链路本地连接访问主页，请将服务笔记本电脑 IP 地址配置为 `169.254.0.2` ，然后重试。

3. 查看主页页面上显示的所有消息，并根据需要配置链路配置和 IP 配置。



验证并升级 **StorageGRID** 设备安装程序版本

设备上的 StorageGRID 设备安装程序版本必须与 StorageGRID 系统上安装的软件版本匹配，以确保所有 StorageGRID 功能均受支持。

您需要的内容

您已访问 StorageGRID 设备安装程序。

关于此任务

StorageGRID 设备出厂时预安装了 StorageGRID 设备安装程序。如果要将设备添加到最近升级的 StorageGRID 系统，则可能需要先手动升级 StorageGRID 设备安装程序，然后再将设备安装为新节点。

升级到新的 StorageGRID 版本时， StorageGRID 设备安装程序会自动升级。您无需升级已安装设备节点上的 StorageGRID 设备安装程序。只有在安装包含早期版本的 StorageGRID 设备安装程序的设备时，才需要此操作步骤 。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 升级固件 * 。
2. 将当前固件版本与 StorageGRID 系统上安装的软件版本进行比较。（从网格管理器的顶部，选择帮助图标并选择 * 关于 * 。）

   两个版本中的第二位数字应匹配。例如，如果您的 StorageGRID 系统运行的是 11.* 6* 。 *x.y* ，则 StorageGRID 设备安装程序版本应为 3.* 6* 。 *z* 。

3. 如果设备安装了StorageGRID 设备安装程序的低级版本、请转到 "NetApp下载：StorageGRID 设备"。

   使用您的 NetApp 帐户的用户名和密码登录。

4. 下载适当版本的 * StorageGRID Appliances * 支持文件以及相应的校验和文件。

   StorageGRID 设备的支持文件是一个 ` .zip` 归档文件，其中包含所有 StorageGRID 设备型号的当前和先前固件版本，位于每种控制器类型的子目录中。

   下载 StorageGRID 设备的支持文件后，解压缩 ` .zip` 归档并查看 README 文件，以了解有关安装 StorageGRID 设备安装程序的重要信息。

5. 按照 StorageGRID 设备安装程序的 " 升级固件 " 页面上的说明执行以下步骤：
   a. 上传适用于您的控制器类型的相应支持文件（固件映像）和校验和文件。
   b. 升级非活动分区。
   c. 重新启动和交换分区。
   d. 升级第二个（非活动）分区。

相关信息

访问 StorageGRID 设备安装程序

配置网络链路（ **SG100** 和 **SG1000** ）

您可以为用于将设备连接到网格网络，客户端网络和管理网络的端口配置网络链路。您可以设置链路速度以及端口和网络绑定模式。

您需要的内容

- 您已获得所需的额外设备来满足您的缆线类型和链路速度要求。
- 您已将网络端口连接到支持所选速度的交换机。

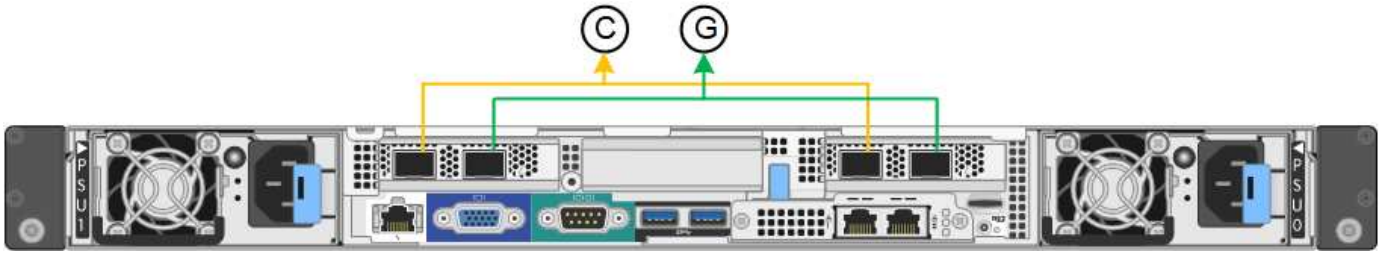
如果您计划使用聚合端口绑定模式， LACP 网络绑定模式或 VLAN 标记：

- 您已将设备上的网络端口连接到可支持 VLAN 和 LACP 的交换机。
- 如果多个交换机参与 LACP 绑定，则这些交换机支持多机箱链路聚合组（ MLAG ）或等效项。
- 您了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。
- 您知道要用于每个网络的唯一 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。

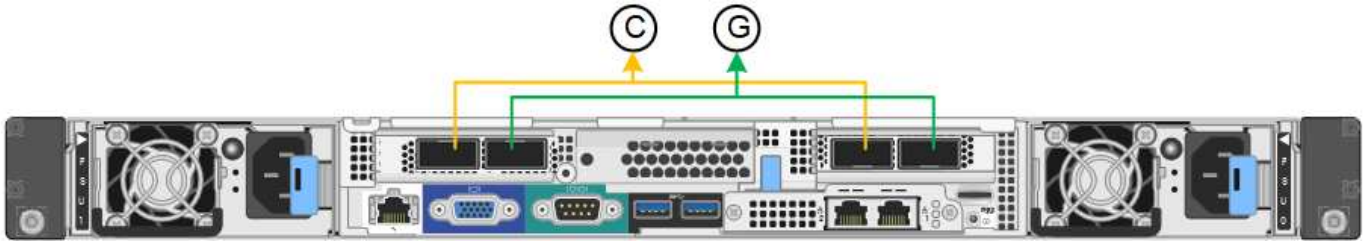
关于此任务

图中显示了四个网络端口在固定端口绑定模式下的绑定方式（默认配置）。

- SG100 固定端口绑定模式 *



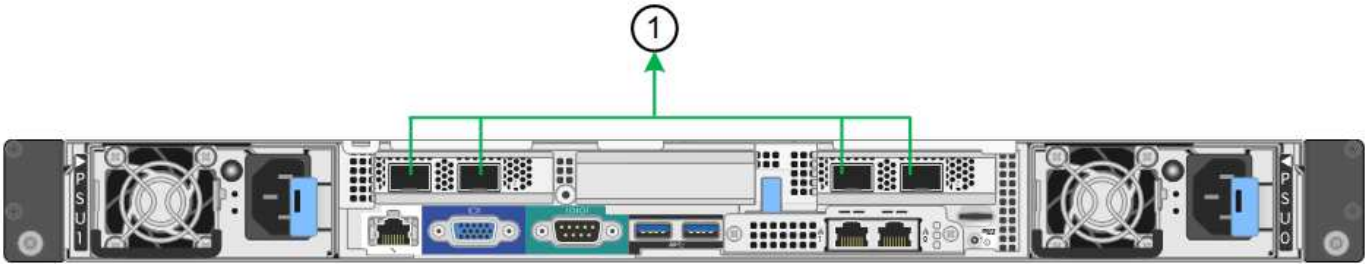
- SG1000 固定端口绑定模式 *



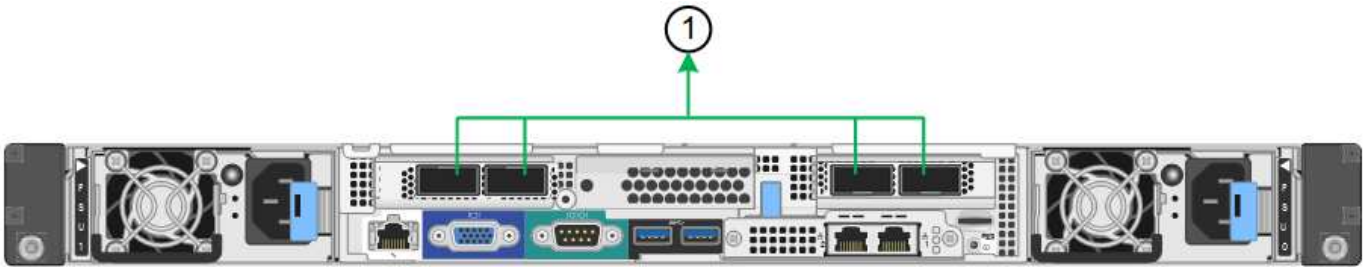
Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

此图显示了四个网络端口在聚合端口绑定模式下的绑定方式。

- SG100 聚合端口绑定模式 *



- SG1000 聚合端口绑定模式 *



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表总结了用于配置四个网络端口的选项。默认设置以粗体显示。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

> LACP 传输哈希策略默认为 layer2+3 模式。如有必要，您可以使用网格管理 API 将其更改为 layer3+4 模式。

- * 固定（默认）端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 端口 1 和 3 对客户端网络使用主动备份绑定。 • 可以为两个网络指定VLAN标记。
LACP （ 802.3ad ）	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 端口 1 和 3 对客户端网络使用 LACP 绑定。 • 可以为两个网络指定VLAN标记。

- * 聚合端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （ 802.3ad ）	• 端口 1-4 对网格网络使用一个 LACP 绑定。 • 一个 VLAN 标记用于标识网格网络数据包。	• 端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。 • 通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

有关其他详细信息，请参见有关服务设备的 GbE 端口连接的文章。

此图显示了 SG100 上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。

这些图显示了设备上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。

- 绑定 SG100 管理网络端口 *

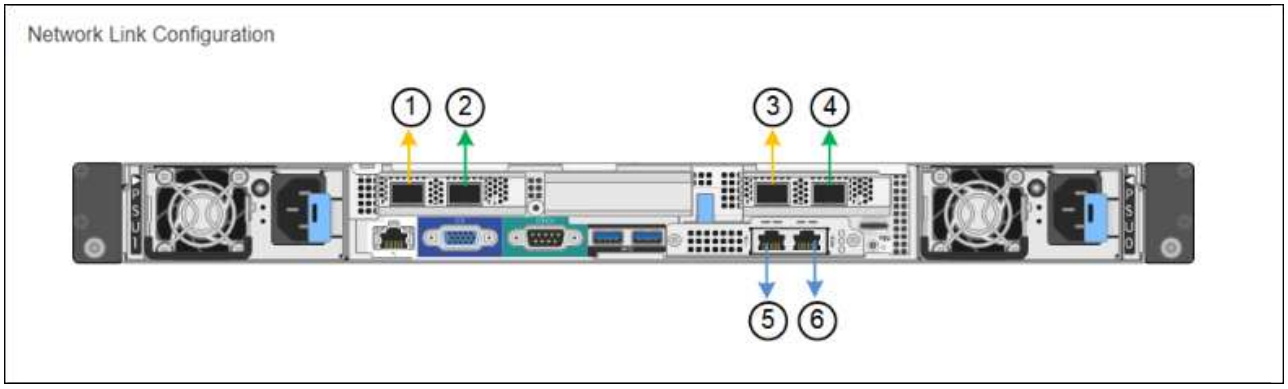
- 绑定 SG1000 管理网络端口 *

步骤

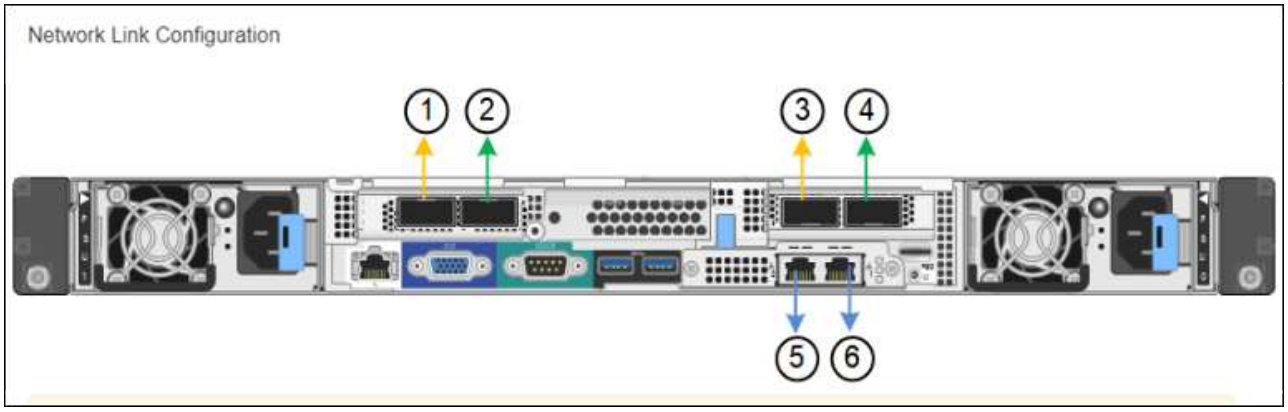
1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * 链接配置 * 。

   " 网络链路配置 " 页面显示设备示意图，其中包含编号为的网络和管理端口。

   ◦ SG100 端口 *



   ◦ SG1000 端口 *



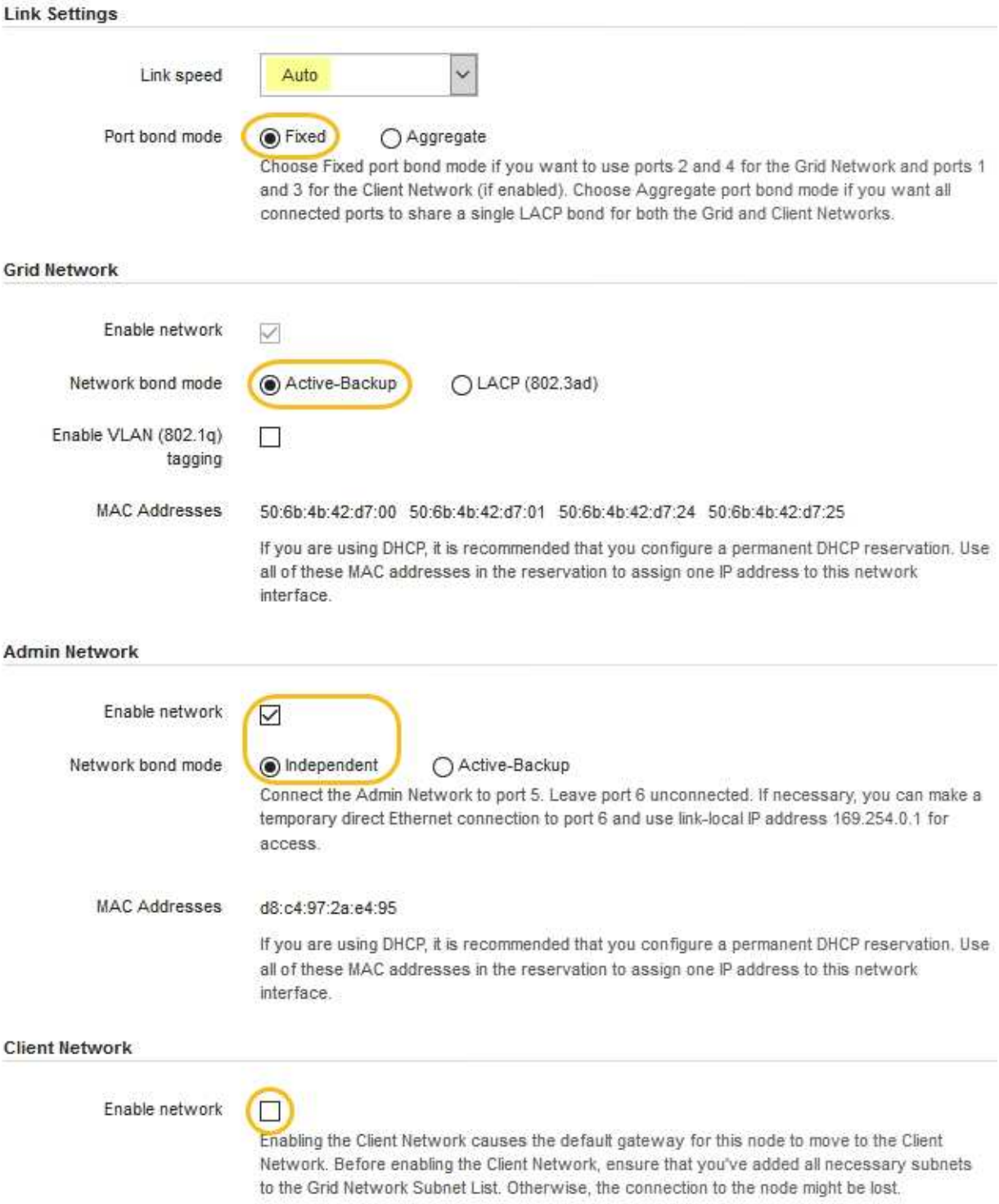
   " 链路状态 " 表列出了已编号端口的链路状态和速度（所示为 SG1000 ）。

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Down	N/A
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

首次访问此页面时：

- * 链路速度 * 设置为 * 自动 * 。
- * 端口绑定模式 * 设置为 * 固定 * 。
- 对于网格网络， * 网络绑定模式 * 设置为 * 主动备份 * 。
- 此时将启用 * 管理网络 * ，并将网络绑定模式设置为 * 独立 * 。
- 已禁用 * 客户端网络 * 。



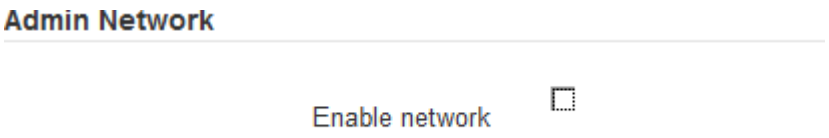
2. 从 * 链路速度 * 下拉列表中选择网络端口的链路速度。

   您用于网格网络和客户端网络的网络交换机也必须支持此速度并为此速度进行配置。您必须使用适当的适配器或收发器来设置所配置的链路速度。请尽可能使用自动链路速度，因为此选项会与链路配对节点协商链路速度和正向错误更正（ FEC ）模式。

3. 启用或禁用计划使用的 StorageGRID 网络。

   网格网络为必填项。您不能禁用此网络。

a. 如果设备未连接到管理网络，请取消选中管理网络的 * 启用网络 * 复选框。



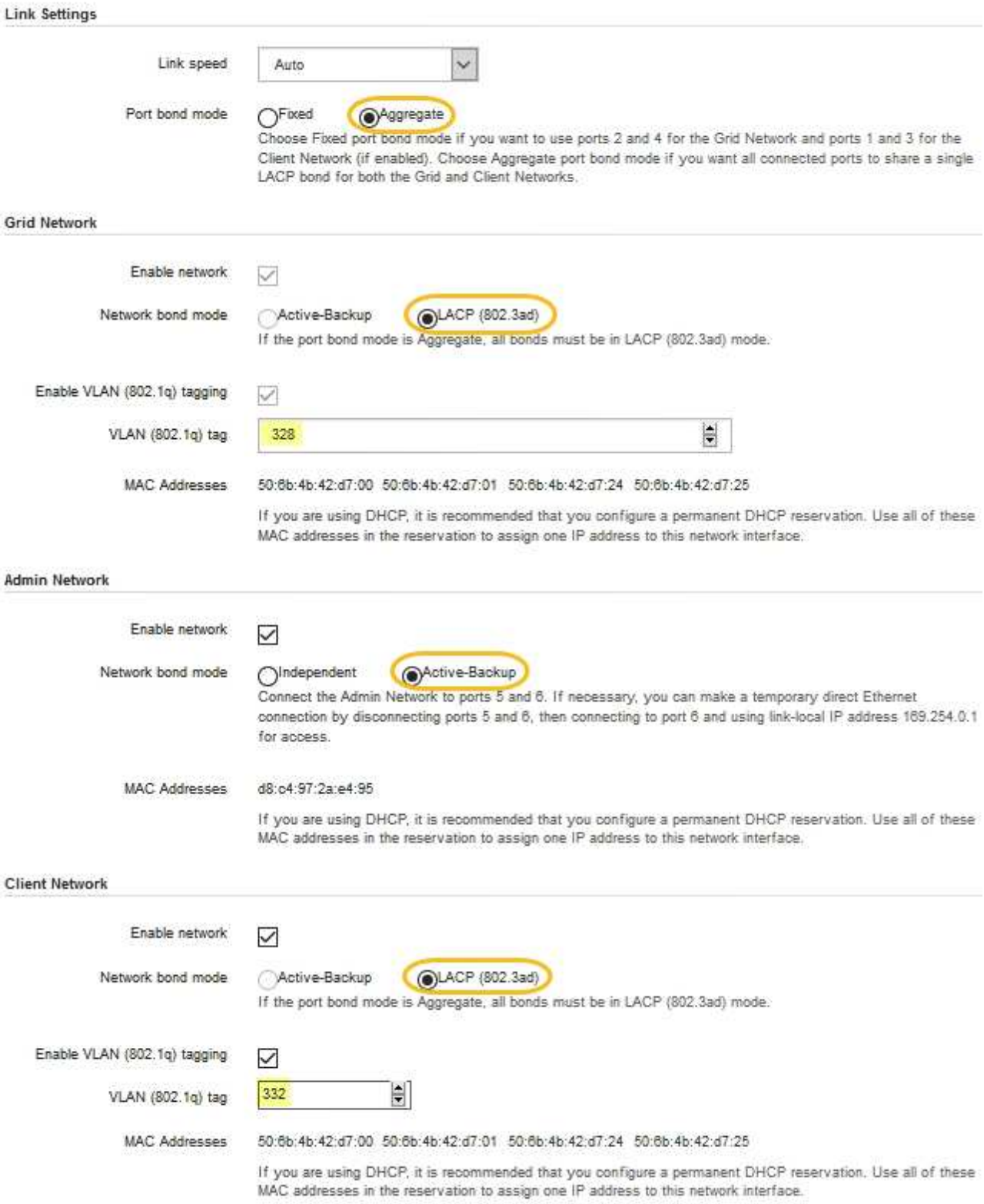
b. 如果设备已连接到客户端网络，请选中客户端网络的 * 启用网络 * 复选框。

此时将显示数据 NIC 端口的客户端网络设置。

4. 请参见表，并配置端口绑定模式和网络绑定模式。

此示例显示：

- 为网格和客户端网络选择了 * 聚合 * 和 * LACP * 。您必须为每个网络指定唯一的 VLAN 标记。您可以选择 0 到 4095 之间的值。
- 已为管理网络选择 * 主动备份 * 。



5. 对所做的选择感到满意后，单击 * 保存 * 。

如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*services_appliance_IP*:8443*`

相关信息

获取其他设备和工具（ SG100 和 SG1000 ）

配置 **StorageGRID IP** 地址

您可以使用 StorageGRID 设备安装程序在 StorageGRID 网格，管理和客户端网络上配置服务设备所使用的 IP 地址和路由信息。

关于此任务

您必须为每个已连接网络上的设备分配一个静态 IP ，或者为 DHCP 服务器上的地址分配一个永久租约。

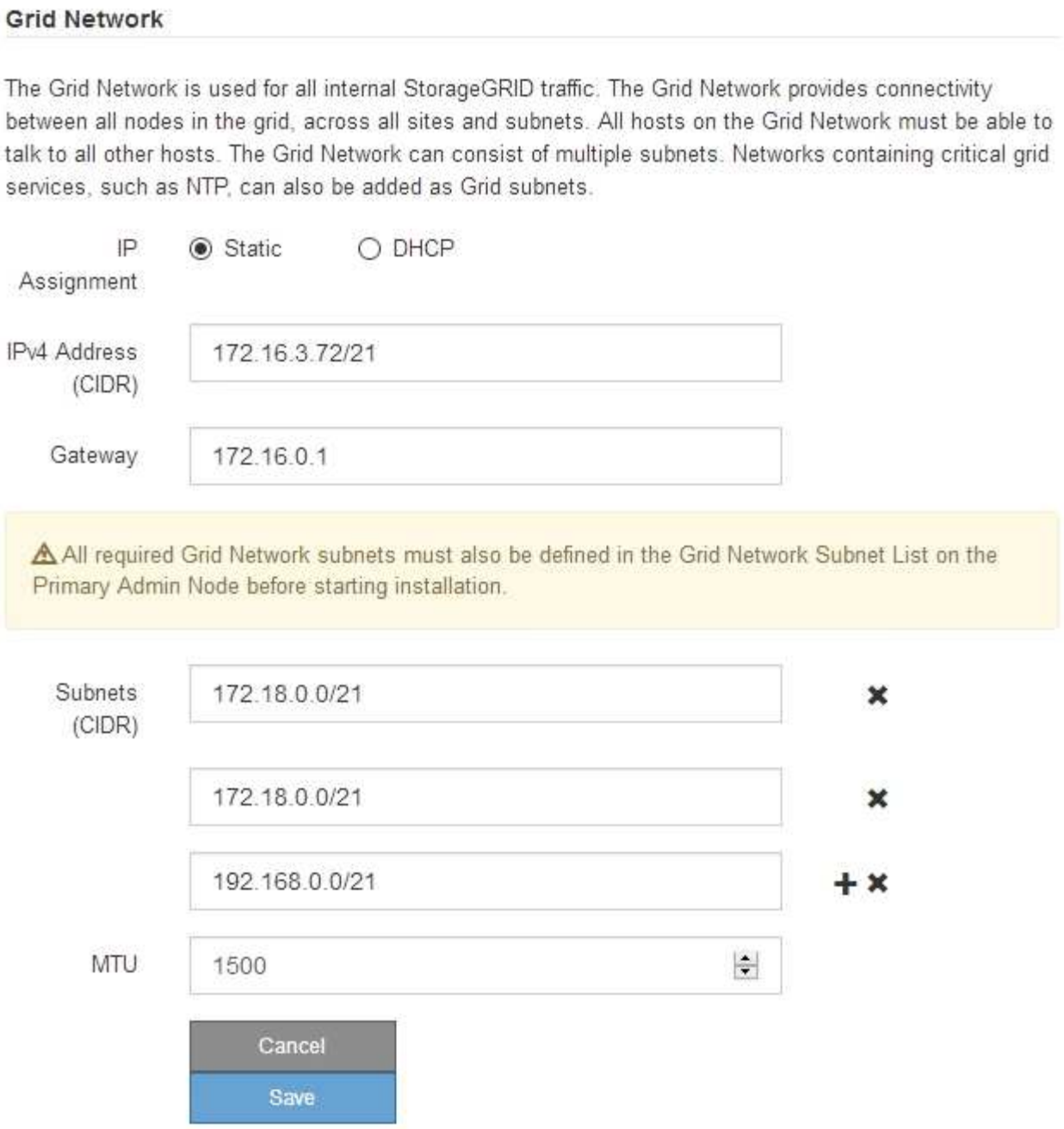
如果要更改链路配置，请参见有关更改服务设备的链路配置的说明。

步骤

1. 在 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。

   此时将显示 "IP Configuration" 页面。

2. 要配置网格网络，请在页面的 * 网格网络 * 部分中选择 * 静态 * 或 * DHCP * 。



3. 如果选择 * 静态 * ，请按照以下步骤配置网格网络：
   a. 使用 CIDR 表示法输入静态 IPv4 地址。
   b. 输入网关。

      如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

   c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

      网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

d. 单击 * 保存 * 。

更改 IP 地址时，网关和子网列表可能也会发生更改。

如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance_IP*:8443*`

e. 确认网格网络子网列表正确无误。

如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

4. 如果选择了 * DHCP * ，请按照以下步骤配置网格网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认网格网络子网列表正确无误。

如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

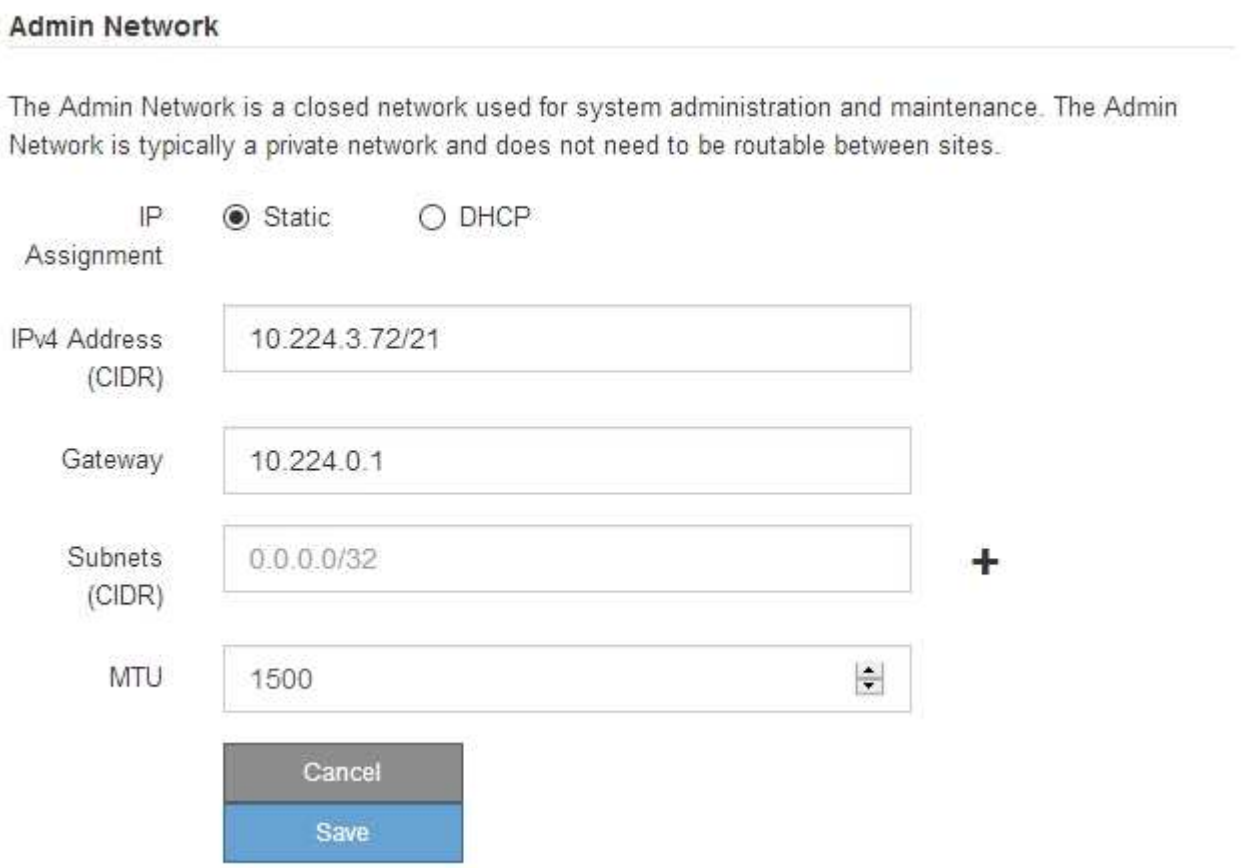
网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

a. 单击 * 保存 * 。

5. 要配置管理网络，请在页面的管理网络部分中选择 * 静态 * 或 * DHCP * 。

要配置管理网络，必须在链路配置页面上启用管理网络。



6. 如果选择 * 静态 * ，请按照以下步骤配置管理网络：

a. 使用 CIDR 表示法为设备上的管理端口 1 输入静态 IPv4 地址。

管理端口 1 位于设备右端的两个 1-GbE RJ45 端口的左侧。

b. 输入网关。

如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

更改 IP 地址时，网关和子网列表可能也会发生更改。

如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance*:8443*`

e. 确认管理网络子网列表正确无误。

您必须验证是否可以使用提供的网关访问所有子网。

无法使用默认路由来使用管理网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

7. 如果选择了 * DHCP * ，请按照以下步骤配置管理网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认管理网络子网列表正确无误。

您必须验证是否可以使用提供的网关访问所有子网。

无法使用默认路由来使用管理网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

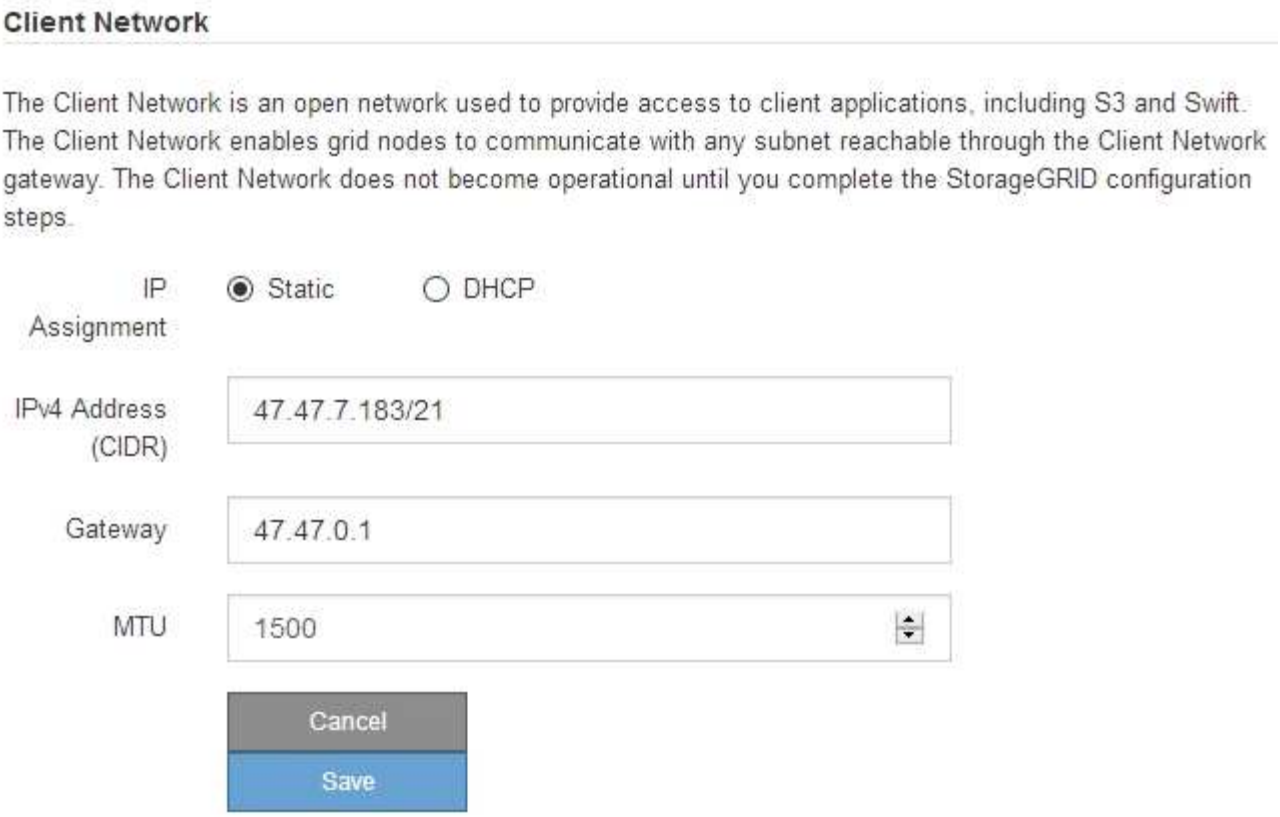
c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

8. 要配置客户端网络，请在页面的 * 客户端网络 * 部分中选择 * 静态 * 或 * DHCP * 。

要配置客户端网络，必须在链路配置页面上启用客户端网络。



9. 如果选择 * 静态 * ，请按照以下步骤配置客户端网络：
   a. 使用 CIDR 表示法输入静态 IPv4 地址。
   b. 单击 * 保存 * 。
   c. 确认客户端网络网关的 IP 地址正确无误。

      如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

   d. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

      网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

   e. 单击 * 保存 * 。
10. 如果选择了 * DHCP * ，请按照以下步骤配置客户端网络：
    a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

       系统会自动填充 * IPv4 地址 * 和 * 网关 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

a. 确认网关是否正确。

> 如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

b. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

相关信息

更改服务设备的链路配置

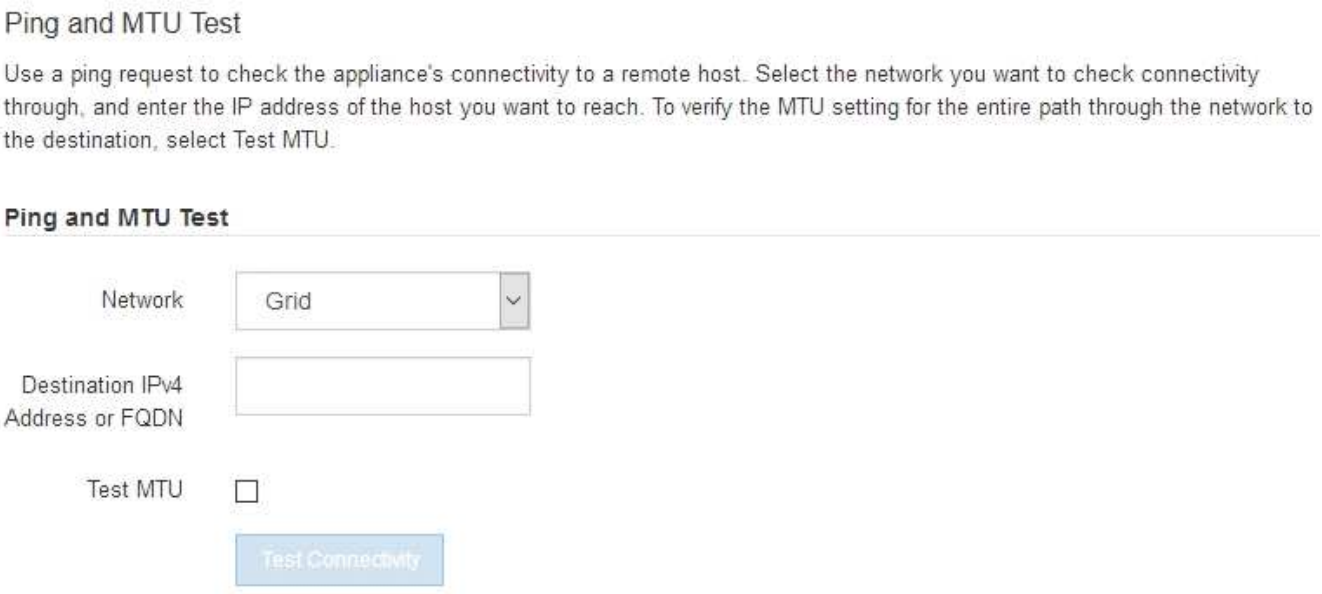
验证网络连接

您应确认可以从设备访问所使用的 StorageGRID 网络。要验证通过网络网关的路由，您应测试 StorageGRID 设备安装程序与不同子网上的 IP 地址之间的连接。您还可以验证 MTU 设置。

步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * Ping 和 MTU 测试 * 。

   此时将显示 Ping 和 MTU 测试页面。



2. 从 * 网络 * 下拉框中，选择要测试的网络：网格，管理员或客户端。
3. 输入该网络上某个主机的 IPv4 地址或完全限定域名（ FQDN ）。

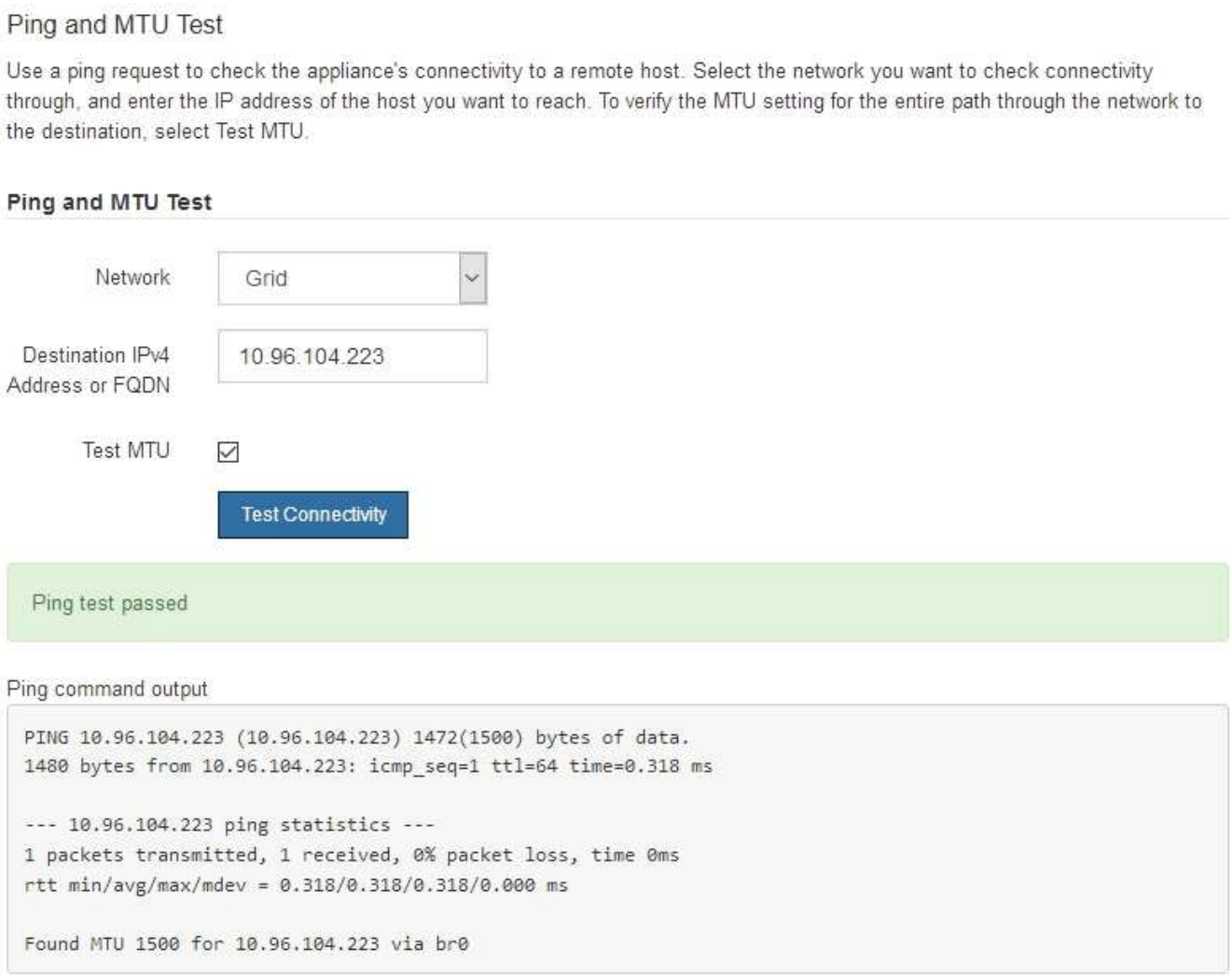
   例如，您可能需要对网络或主管理节点上的网关执行 ping 操作。

4. 或者，选中 * 测试 MTU* 复选框以验证通过网络到目标的整个路径的 MTU 设置。

例如，您可以测试设备节点与其他站点的节点之间的路径。

5. 单击 * 测试连接 * 。

   如果网络连接有效，则会显示 "Ping test passed" 消息，并列出 ping 命令输出。



相关信息

配置网络链路（ SG100 和 SG1000 ）

更改 MTU 设置

验证端口级别的网络连接

要确保 StorageGRID 设备安装程序与其他节点之间的访问不会受到防火墙的阻碍，请确认 StorageGRID 设备安装程序可以连接到指定 IP 地址或地址范围内的特定 TCP 端口或端口集。

关于此任务

使用 StorageGRID 设备安装程序中提供的端口列表，您可以测试设备与网格网络中其他节点之间的连接。

此外，您还可以在管理和客户端网络以及 UDP 端口上测试连接，例如用于外部 NFS 或 DNS 服务器的端口。有关这些端口的列表，请参见 StorageGRID 网络连接准则中的端口参考。

端口连接表中列出的网格网络端口仅适用于 StorageGRID 11.6.0 版。要验证每种节点类型的端口是否正确，您应始终参考适用于您的 StorageGRID 版本的网络连接准则。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 端口连接测试（ nmap ） * 。

   此时将显示端口连接测试页面。

   端口连接表列出了网格网络上需要 TCP 连接的节点类型。对于每种节点类型，此表列出了设备应可访问的网格网络端口。

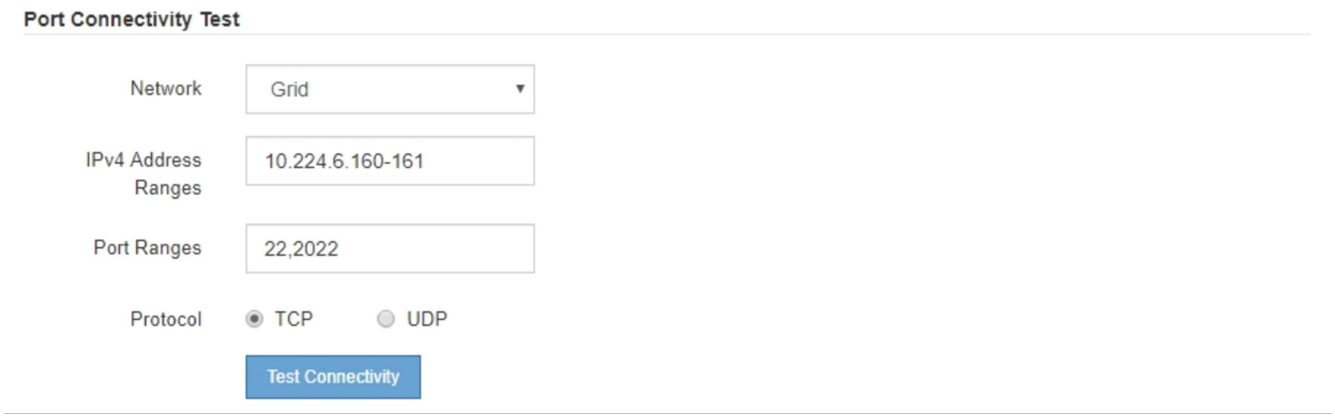
   您可以测试表中列出的设备端口与网格网络中的其他节点之间的连接。

2. 从 * 网络 * 下拉列表中，选择要测试的网络： * 网格 * ， * 管理 * 或 * 客户端 * 。
3. 为该网络上的主机指定一个 IPv4 地址范围。

   例如，您可能需要探测网络或主管理节点上的网关。

   使用连字符指定一个范围，如示例所示。

4. 输入 TCP 端口号，以逗号分隔的端口列表或端口范围。



5. 单击 * 测试连接 * 。

   ◦ 如果选定的端口级别网络连接有效，则绿色横幅中会显示 "`Port connectivity test passed` " 消息。nmap 命令输出列在横幅下方。

- 如果与远程主机建立了端口级网络连接，但主机未侦听一个或多个选定端口，则黄色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  主机未侦听的任何远程端口的状态为 "`closed" 。` 例如，当您尝试连接的节点处于预安装状态且 StorageGRID NMS 服务尚未在该节点上运行时，您可能会看到此黄色横幅。

- 如果无法为一个或多个选定端口建立端口级别网络连接，则红色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  红色横幅表示已尝试通过 TCP 连接到远程主机上的某个端口，但未向发送方返回任何内容。如果未返回任何响应，则此端口的状态为 " 已筛选 " ，并且可能会被防火墙阻止。

  此外，还会列出带有 "`closed` " 的端口。

相关信息

网络连接准则

配置 BMC 接口（ SG100 和 SG1000 ）

服务设备上的基板管理控制器（ BMC ）的用户界面可提供有关硬件的状态信息，并可用于为服务设备配置 SNMP 设置和其他选项。

更改 BMC 接口的根密码

为了安全起见，您必须更改 BMC root 用户的密码。

您需要的内容

管理客户端正在使用 支持的 Web 浏览器。

关于此任务

首次安装设备时， BMC 会使用 root 用户的默认密码（`root/calvin`）。您必须更改 root 用户的密码以保护您的系统。

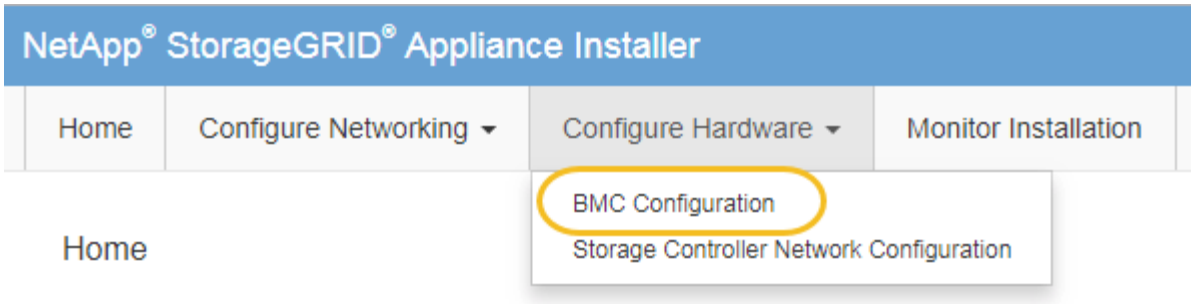
步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*services_appliance_IP*:8443*`

   对于 `services _appliation_ip` ，请在任何 StorageGRID 网络上使用此设备的 IP 地址。

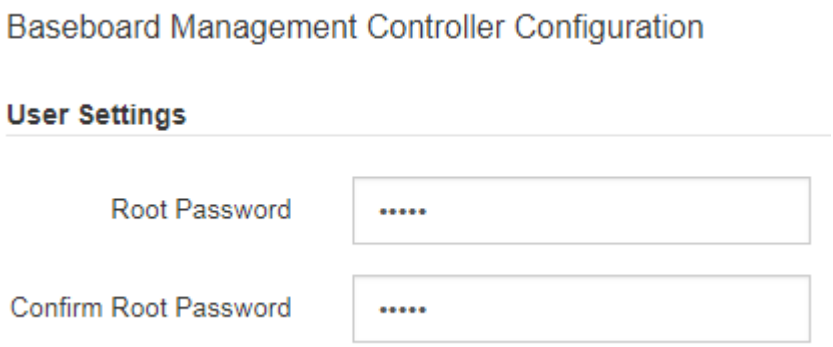
   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * BMC 配置 * 。



此时将显示 Baseboard Management Controller Configuration 页面。

3. 在提供的两个字段中输入 root 帐户的新密码。



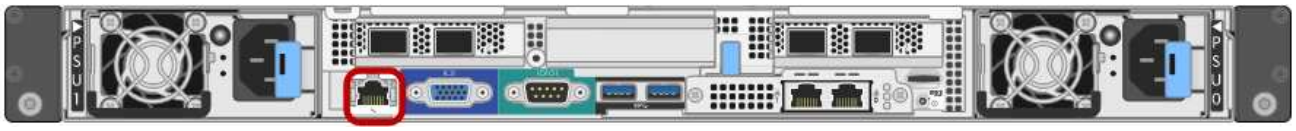
4. 单击 * 保存 * 。

设置 **BMC** 管理端口的 **IP** 地址

在访问 BMC 接口之前，必须为服务设备上的 BMC 管理端口配置 IP 地址。

您需要的内容

- 管理客户端正在使用 支持的 Web 浏览器。
- 您正在使用可连接到 StorageGRID 网络的任何管理客户端。
- BMC 管理端口将连接到您计划使用的管理网络。
- SG100 BMC 管理端口 *



- SG1000 BMC 管理端口 *

关于此任务

出于支持目的， BMC 管理端口允许进行低级硬件访问。您只能将此端口连接到安全，可信的内部管理网络。如果没有此类网络可用，请保持 BMC 端口未连接或被阻止，除非技术支持请求 BMC 连接。

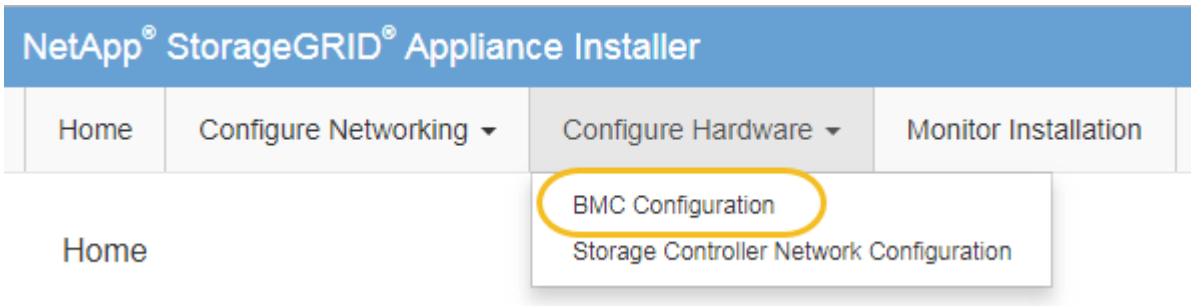
步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*services_appliance_IP*:8443*`

   对于 ` services_appliation_ip_` ，请在任何 StorageGRID 网络上使用此设备的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * BMC 配置 * 。

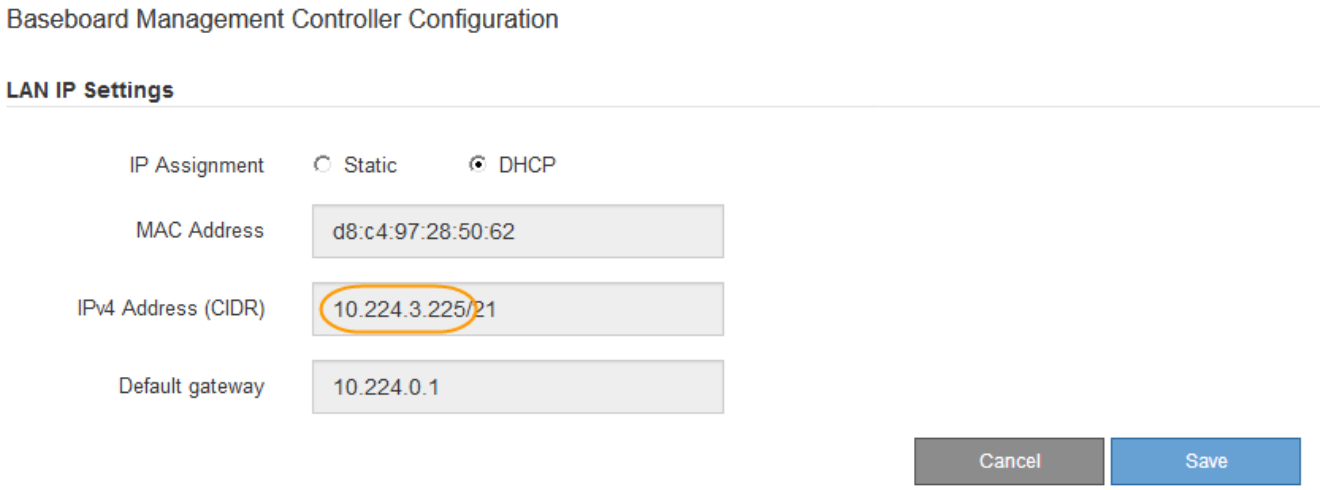


   此时将显示 Baseboard Management Controller Configuration 页面。

3. 记下自动显示的 IPv4 地址。

   DHCP 是为该端口分配 IP 地址的默认方法。

   显示 DHCP 值可能需要几分钟的时间。



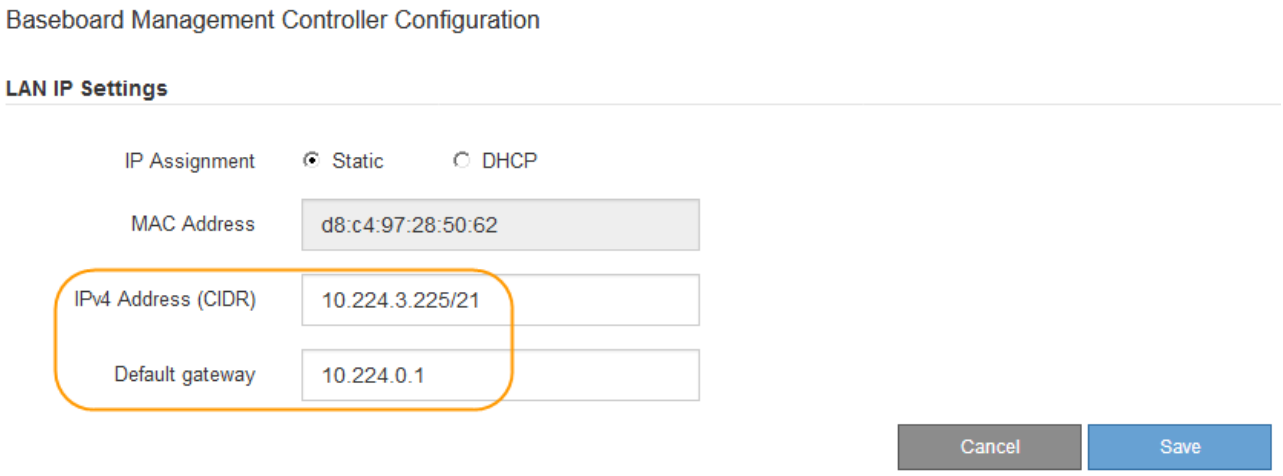
4. 也可以为 BMC 管理端口设置静态 IP 地址。

   您应该为 BMC 管理端口分配静态 IP ，或者为 DHCP 服务器上的地址分配永久租约。

a. 选择 * 静态 * 。

b. 使用 CIDR 表示法输入 IPv4 地址。

c. 输入默认网关。



d. 单击 * 保存 * 。

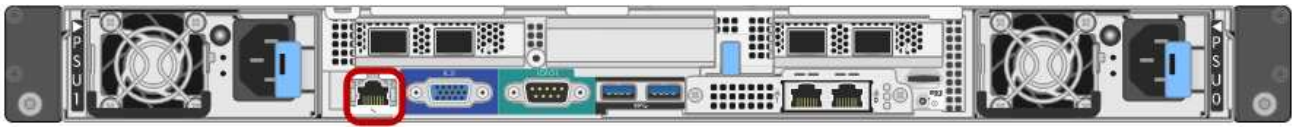
应用所做的更改可能需要几分钟的时间。

访问 **BMC** 界面

您可以使用 BMC 管理端口的 DHCP 或静态 IP 地址访问服务设备上的 BMC 接口。

您需要的内容

- 管理客户端正在使用 支持的 Web 浏览器。
- 服务设备上的 BMC 管理端口已连接到您计划使用的管理网络。
- SG100 BMC 管理端口 *



- SG1000 BMC 管理端口 *

步骤

1. 输入 BMC 接口的 URL： + ` * https://*BMC_Port_IP*`

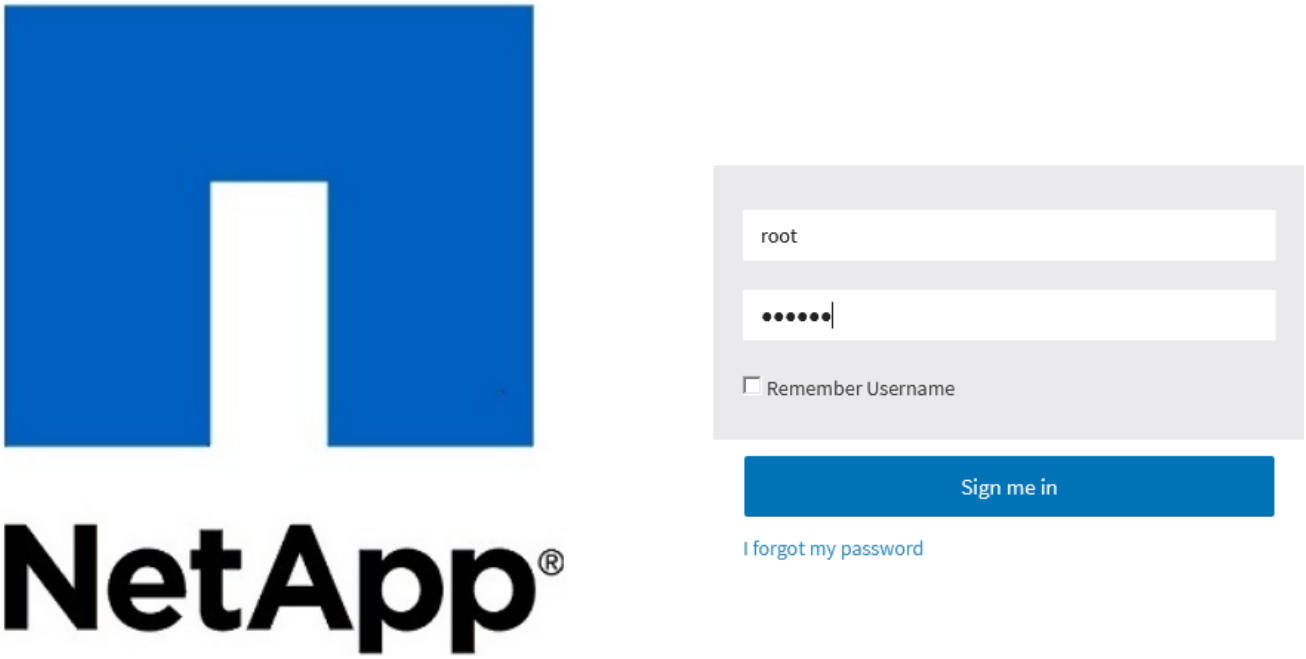
   对于 ` BMC_Port_IP_` ，请使用 DHCP 或静态 IP 地址作为 BMC 管理端口。

   此时将显示 BMC 登录页面。

如果尚未配置 `BMC_Port_IP` ，请按照中的说明进行操作 配置 BMC 接口（ SG100/SG1000 ）。如果由于硬件问题而无法遵循此操作步骤，并且尚未配置 BMC IP 地址，则仍可访问此 BMC 。默认情况下， BMC 使用 DHCP 获取 IP 地址。如果在 BMC 网络上启用了 DHCP ，则网络管理员可以提供分配给 BMC MAC 的 IP 地址，该地址印在 SG6000-CN 控制器正面的标签上。如果 BMC 网络上未启用 DHCP ， BMC 将在几分钟后不会做出响应，并为自己分配默认静态 IP `192.168.0.120` 。您可能需要将笔记本电脑直接连接到 BMC 端口，并更改网络设置以为笔记本电脑分配 IP ，例如 `192.168.0.200/24` ，以便浏览到 `192.168.0.120` 。

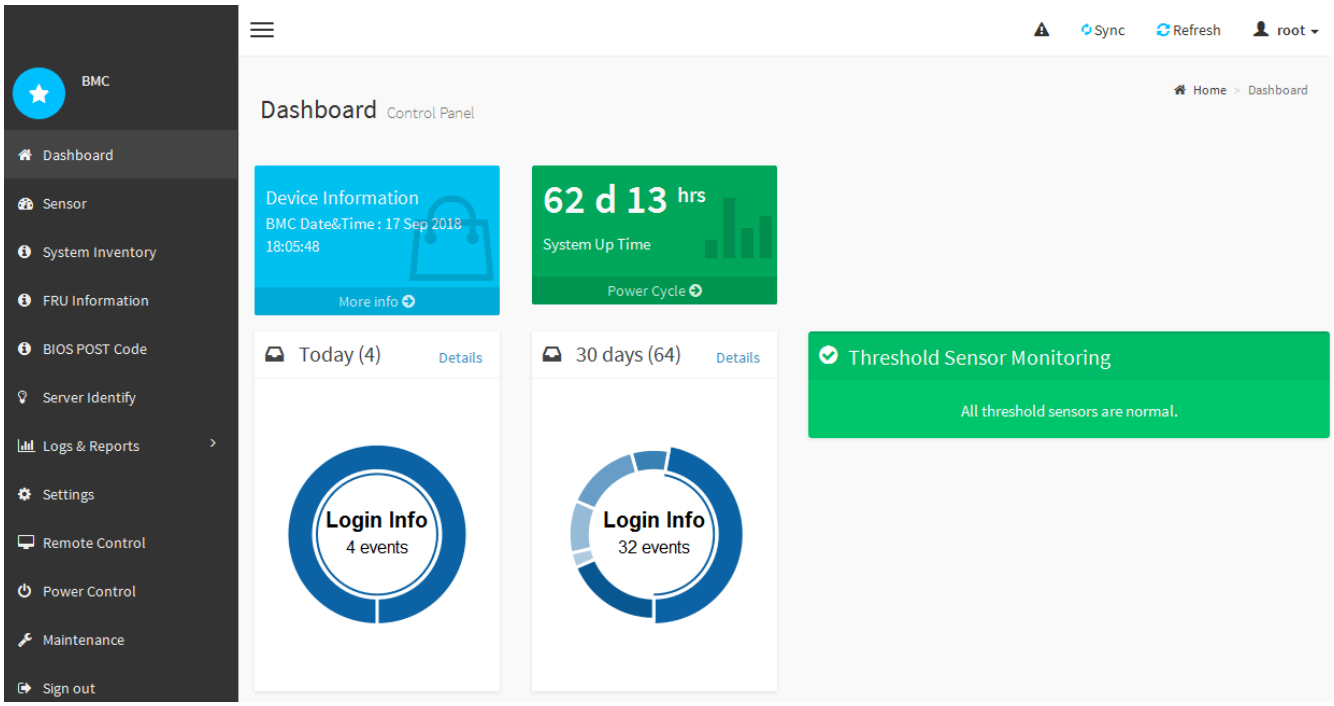
2. 使用您在更改默认 root 密码时设置的密码输入 root 用户名和密码： + ` * root*`

   ` * *password*`



3. 单击 * 登录 *

   此时将显示 BMC 信息板。



4. 或者，也可以选择 * 设置 * > * 用户管理 * 并单击任何 " 已 d " 用户来创建其他用户。

当用户首次登录时，系统可能会提示他们更改密码以提高安全性。

相关信息

更改 BMC 接口的根密码

配置服务设备的 SNMP 设置

如果您熟悉为硬件配置 SNMP ，则可以使用 BMC 界面为服务设备配置 SNMP 设置。您可以提供安全社区字符串，启用 SNMP 陷阱并最多指定五个 SNMP 目标。

您需要的内容

- 您知道如何访问 BMC 信息板。
- 您在为 SNMPv1-v2c 设备配置 SNMP 设置方面具有经验。

如果此设备发生故障且需要更换，则此操作步骤 所做的 BMC 设置可能不会保留下来。请确保您已应用所有设置，以便在更换硬件后根据需要轻松重新应用这些设置。

步骤

1. 从 BMC 信息板中，选择 * 设置 * > * SNMP 设置 * 。
2. 在 SNMP 设置页面上，选择 * 启用 SNMP V1/V2 * ，然后提供只读社区字符串和读写社区字符串。

   只读社区字符串类似于用户 ID 或密码。您应更改此值，以防止入侵者获取有关网络设置的信息。读写社区字符串可保护设备免受未经授权的更改。

3. （可选）选择 * 启用陷阱 * ，然后输入所需信息。

使用 IP 地址输入每个 SNMP 陷阱的目标 IP 。不支持完全限定域名。

如果您希望服务设备在 SNMP 控制台处于异常状态时立即向其发送通知，请启用陷阱。陷阱可能指示链路启动 / 关闭状况，温度超过特定阈值或流量较高。

4. 或者，也可以单击 * 发送测试陷阱 * 来测试您的设置。
5. 如果设置正确，请单击 * 保存 * 。

为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，则必须使用 BMC 界面配置 SMTP 设置，用户， LAN 目标，警报策略和事件筛选器。

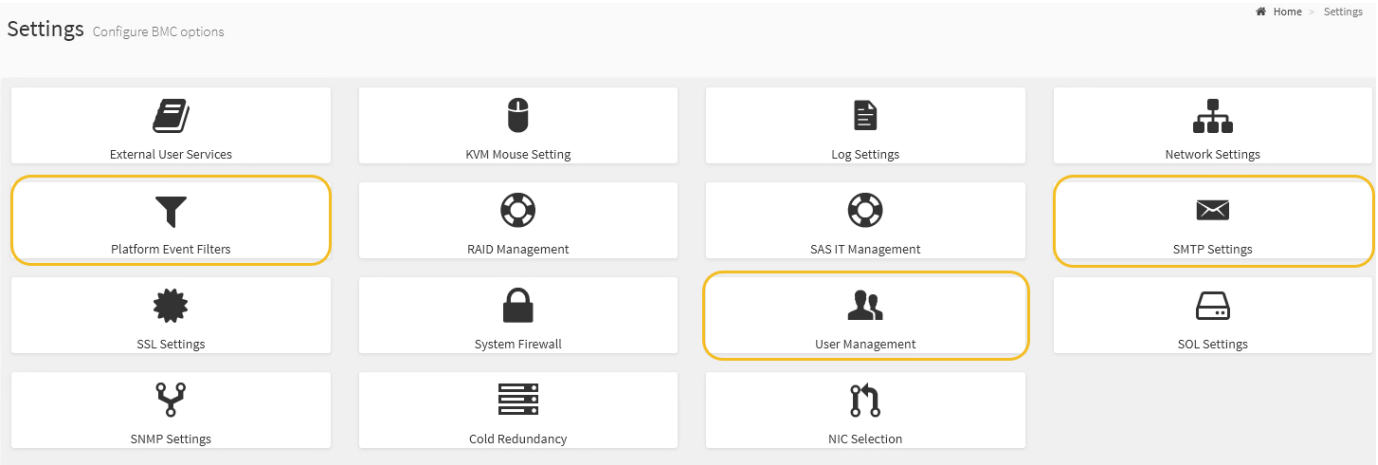
如果此设备发生故障且需要更换，则此操作步骤 所做的 BMC 设置可能不会保留下来。请确保您已应用所有设置，以便在更换硬件后根据需要轻松重新应用这些设置。

您需要的内容

您知道如何访问 BMC 信息板。

关于此任务

在 BMC 界面中，您可以使用设置页面上的 * SMTP 设置 * ， * 用户管理 * 和 * 平台事件筛选器 * 选项来配置电子邮件通知。



步骤

1. 配置 SMTP 设置。
   a. 选择 * 设置 * > * SMTP 设置 * 。
   b. 对于发件人电子邮件 ID ，请输入有效的电子邮件地址。

      此电子邮件地址在 BMC 发送电子邮件时作为发件人地址提供。
2. 设置用户以接收警报。
   a. 从 BMC 信息板中，选择 * 设置 * > * 用户管理 * 。
   b. 至少添加一个用户以接收警报通知。

您为用户配置的电子邮件地址是 BMC 向其发送警报通知的地址。例如，您可以添加一个通用用户，例如 "`notification -user ，` " ，并使用技术支持团队 Email发送名单 的电子邮件地址。

3. 配置警报的 LAN 目标。
   a. 选择 * 设置 * > * 平台事件筛选器 * > * LAN 目标 * 。
   b. 至少配置一个 LAN 目标。
      - 选择 * 电子邮件 * 作为目标类型。
      - 对于 BMC 用户名，请选择先前添加的用户名。
      - 如果您添加了多个用户并希望所有用户都接收通知电子邮件，则必须为每个用户添加一个 LAN 目标。
   c. 发送测试警报。
4. 配置警报策略，以便定义 BMC 发送警报的时间和位置。
   a. 选择 * 设置 * > * 平台事件筛选器 * > * 警报策略 * 。
   b. 为每个 LAN 目标至少配置一个警报策略。
      - 对于策略组编号，请选择 * 。 1
      - 对于策略操作，选择 * 始终向此目标发送警报 * 。
      - 对于 LAN 通道，选择 * 1 * 。
      - 在目标选择器中，选择策略的 LAN 目标。
5. 配置事件筛选器以将不同事件类型的警报定向到相应的用户。
   a. 选择 * 设置 * > * 平台事件筛选器 * > * 事件筛选器 * 。
   b. 对于警报策略组编号，输入 * 1 * 。
   c. 为要通知警报策略组的每个事件创建筛选器。
      - 您可以为电源操作，特定传感器事件或所有事件创建事件筛选器。
      - 如果不确定要监控哪些事件，请选择 "Sensor Type" （传感器类型）为 "All 传感器 " （所有传感器） * ，并选择 "Event Options" （事件选项）为 "All Events" （所有事件）。如果收到不需要的通知，您可以稍后更改所做的选择。

可选：启用节点加密

如果启用了节点加密，则可以通过安全密钥管理服务器（ KMS ）加密来保护设备中的磁盘，防止物理丢失或从站点中删除。您必须在设备安装期间选择并启用节点加密，并且在 KMS 加密过程开始后，不能取消选择节点加密。

您需要的内容

查看有关管理 StorageGRID 的说明中有关 KMS 的信息。

关于此任务

启用了节点加密的设备将连接到为 StorageGRID 站点配置的外部密钥管理服务器（ KMS ）。每个 KMS （或 KMS 集群）负责管理站点上所有设备节点的加密密钥。这些密钥对启用了节点加密的设备中每个磁盘上的数据进行加密和解密。

可以在 StorageGRID 中安装 KMS 之前或之后在网格管理器中设置此设备。有关更多详细信息，请参见管理 StorageGRID 的说明中有关 KMS 和设备配置的信息。

- 如果在安装设备之前设置了 KMS ，则在设备上启用节点加密并将其添加到配置了 KMS 的 StorageGRID 站点时， KMS 控制的加密将开始。
- 如果在安装此设备之前未设置 KMS ，则在为包含此设备节点的站点配置了 KMS 并可使用此 KMS 后，将对启用了节点加密的每个设备执行 KMS 控制的加密。

> 在连接到启用了节点加密的设备上的 KMS 之前存在的数据将使用不安全的临时密钥进行加密。除非将密钥设置为 KMS 提供的值，否则设备不会受到删除或被盗的保护。

如果没有对磁盘进行解密所需的 KMS 密钥，则无法检索设备上的数据，并且数据实际上会丢失。如果无法从 KMS 中检索到解密密钥，则会出现这种情况。如果清除KMS配置、KMS密钥过期、与KMS的连接断开或从安装了KMS密钥的StorageGRID 系统中删除设备、则无法访问此密钥。

步骤

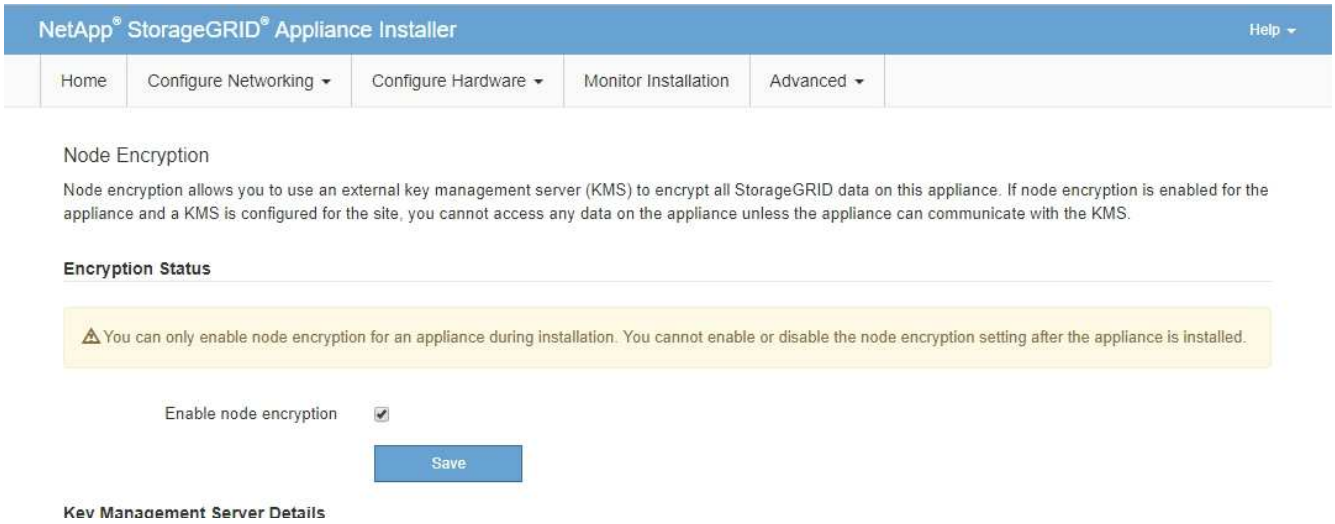
1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

   > 使用 KMS 密钥对设备加密后，如果不使用相同的 KMS 密钥，则无法对设备磁盘进行解密。

2. 选择 * 配置硬件 * > * 节点加密 * 。



3. 选择 * 启用节点加密 * 。

   在安装设备之前，您可以取消选择 * 启用节点加密 * ，而不会有数据丢失的风险。安装开始后，设备节点将访问 StorageGRID 系统中的 KMS 加密密钥并开始磁盘加密。安装设备后，您无法禁用节点加密。

   > 将启用了节点加密的设备添加到具有 KMS 的 StorageGRID 站点后，您无法停止对此节点使用 KMS 加密。

4. 选择 * 保存 * 。
5. 将设备部署为 StorageGRID 系统中的节点。

   当设备访问为 StorageGRID 站点配置的 KMS 密钥时，便会开始使用由 KMS 控制的加密。安装程序会在 KMS 加密过程中显示进度消息，此过程可能需要几分钟时间，具体取决于设备中的磁盘卷数。

   > 设备最初会配置一个随机的非 KMS 加密密钥，该密钥会分配给每个磁盘卷。磁盘会使用此临时加密密钥进行加密，这种加密密钥不安全，直到启用了节点加密的设备访问为 StorageGRID 站点配置的 KMS 密钥为止。

完成后

您可以查看节点加密状态， KMS 详细信息以及设备节点处于维护模式时正在使用的证书。

相关信息

管理 StorageGRID

监控维护模式下的节点加密（ SG100 和 SG1000 ）

部署服务设备节点

您可以将服务设备部署为主管理节点，非主管理节点或网关节点。SG100 和 SG1000 设备可以同时作为网关节点和管理节点（主节点或非主节点）运行。

将服务设备部署为主管理节点

在将服务设备部署为主管理节点时，您可以使用设备上提供的 StorageGRID 设备安装程序安装 StorageGRID 软件，或者上传要安装的软件版本。在安装任何其他设备节点类型之前，您必须先安装并配置主管理节点。主管理节点可以连接到网格网络以及可选的管理网络和客户端网络（如果配置了其中一个或两者）。

您需要的内容

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路， IP 地址和端口重新映射（如果需要）。

  > 如果已重新映射任何端口，则不能使用相同的端口配置负载平衡器端点。您可以使用重新映射的端口创建端点，但这些端点将重新映射到原始 CLB 端口和服务，而不是负载平衡器服务。按照中的步骤进行操作 删除端口重新映射。

  请参见 负载平衡的工作原理— CLB 服务（已弃用） 有关 CLB 服务的详细信息。

  > CLB 服务已弃用。

- 您的服务笔记本电脑具有 支持的 Web 浏览器。
- 您知道分配给设备的 IP 地址之一。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。

关于此任务

要在设备主管理节点上安装 StorageGRID ，请执行以下操作：

- 您可以使用 StorageGRID 设备安装程序安装 StorageGRID 软件。如果要安装其他版本的软件，请先使用 StorageGRID 设备安装程序上传。
- 软件安装完毕后，请稍候。
- 安装软件后，设备将自动重新启动。

步骤

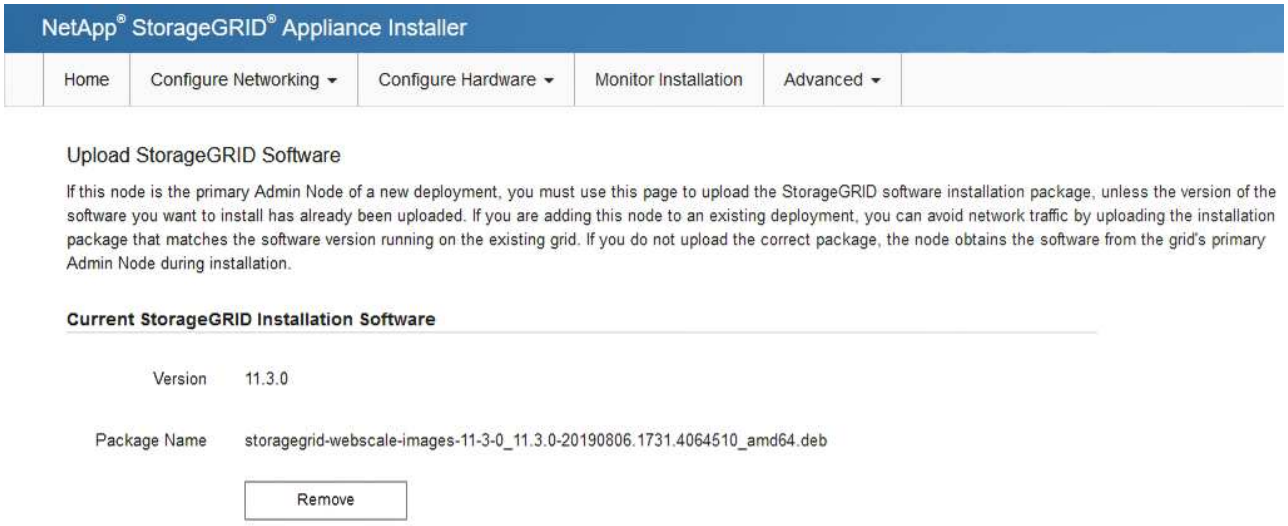
1. 打开浏览器，然后输入设备的 IP 地址。+ ` * https://*services_appliance_IP*:8443*`

   此时将显示 StorageGRID 设备安装程序主页页面。

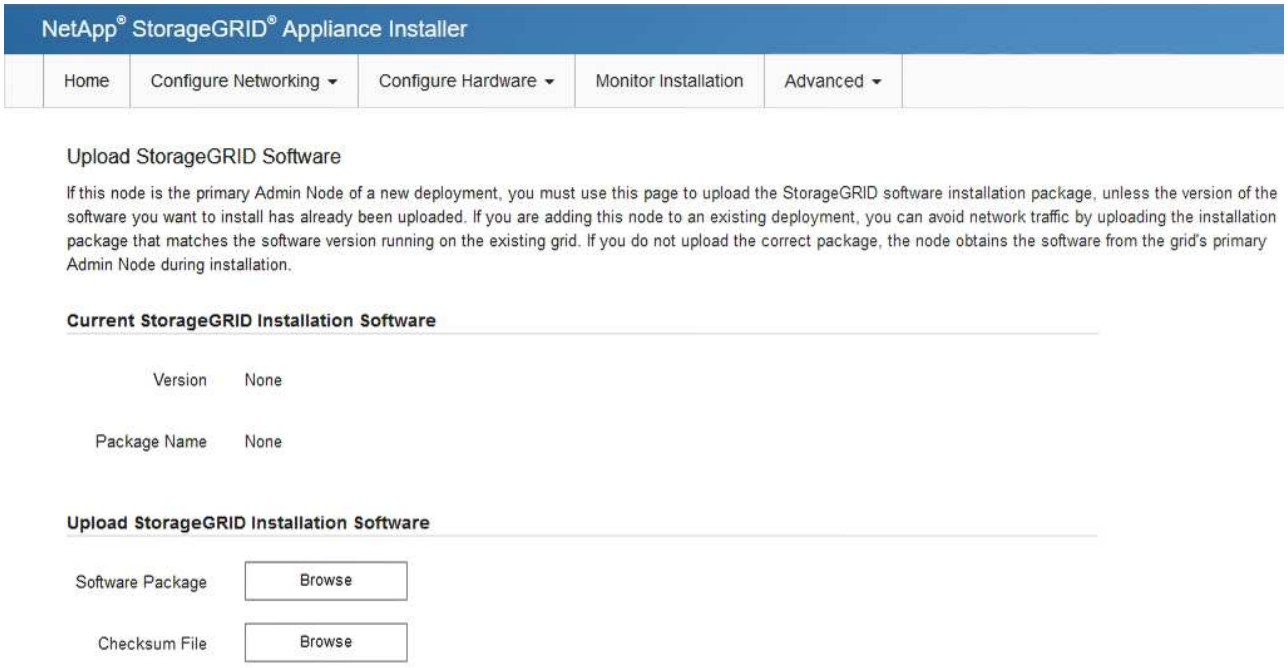
2. 在 * 此节点 * 部分中，选择 * 主管理 * 。
3. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后单击 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的网格节点页面上。

4. 或者，要安装其他版本的 StorageGRID 软件，请执行以下步骤：
   a. 下载安装归档：https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["NetApp下载：StorageGRID 设备"^]。
   b. 提取归档。
   c. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 上传 StorageGRID 软件 * 。
   d. 单击 * 删除 * 以删除当前软件包。



   e. 单击 * 浏览 * 下载并提取的软件包，然后单击 * 浏览 * 获取校验和文件。

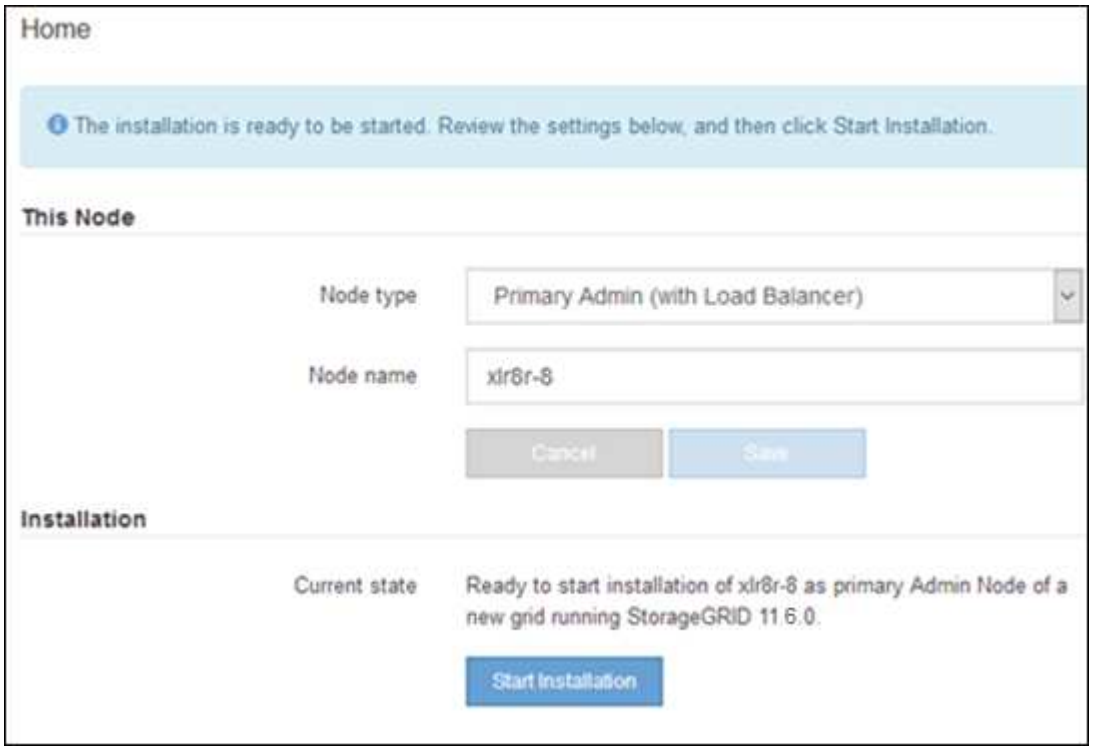


f. 选择 * 主页 * 以返回到主页页面。

5. 确认当前状态为 "`Ready to start installation of primary Admin Node name with software version x.y` "，并且已启用 * 开始安装 * 按钮。

> 如果要将管理节点设备部署为节点克隆目标，请在此停止部署过程，然后按照继续执行节点克隆操作步骤 恢复和维护 说明。

6. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。



当前状态将更改为 "`Installation is in progress，` "，此时将显示监控器安装页面。

如果需要手动访问监控器安装页面，请单击菜单栏中的 * 监控器安装 * 。

将服务设备部署为网关或非主管理节点

在将服务设备部署为网关节点或非主管理节点时，您可以使用该设备上随附的 StorageGRID 设备安装程序。

您需要的内容

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路， IP 地址和端口重新映射（如果需要）。

如果已重新映射任何端口，则不能使用相同的端口配置负载平衡器端点。您可以使用重新映射的端口创建端点，但这些端点将重新映射到原始 CLB 端口和服务，而不是负载平衡器服务。按照中的步骤进行操作 删除端口重新映射。

CLB 服务已弃用。

- 已部署 StorageGRID 系统的主管理节点。
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 您的服务笔记本电脑具有 支持的 Web 浏览器。
- 您知道分配给设备的 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。

关于此任务

要在服务设备节点上安装 StorageGRID ，请执行以下操作：

- 您可以指定或确认主管理节点的 IP 地址以及设备节点的名称。
- 您开始安装，并等待软件安装完成。

  在完成设备网关节点安装任务后，安装将暂停。要恢复安装，请登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装过程。安装非主管理节点不需要您的批准。

不要在同一站点中部署 SG100 和 SG1000 服务设备。可能会导致性能不可预测。

如果您需要一次部署多个设备节点，则可以使用 `configure-sGa.py` Appliance Installation 脚本自动执行安装过程。您也可以使用设备安装程序上传包含配置信息的 JSON 文件。请参见 自动化设备安装和配置（ SG100 和 SG1000 ） 有关自动安装的详细信息，请参见。

步骤

1. 打开浏览器，然后输入设备的 IP 地址。

   ` * https://*Controller_IP*:8443*`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

   如果先前已在此数据中心中安装了其他节点，则 StorageGRID 设备安装程序可以自动发现此 IP 地址，前提是主管理节点或至少一个配置了 admin_IP 的其他网格节点位于同一子网上。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 等待连接状态，使新 IP 地址准备就绪。
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 等待显示发现的 IP 地址列表。 c. 为要部署此设备存储节点的网格选择主管理节点。 d. 单击 * 保存 * 。 e. 等待连接状态，使新 IP 地址准备就绪。

4. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后单击 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的节点页面（概述选项卡）上。如果需要，您可以在批准节点时更改名称。

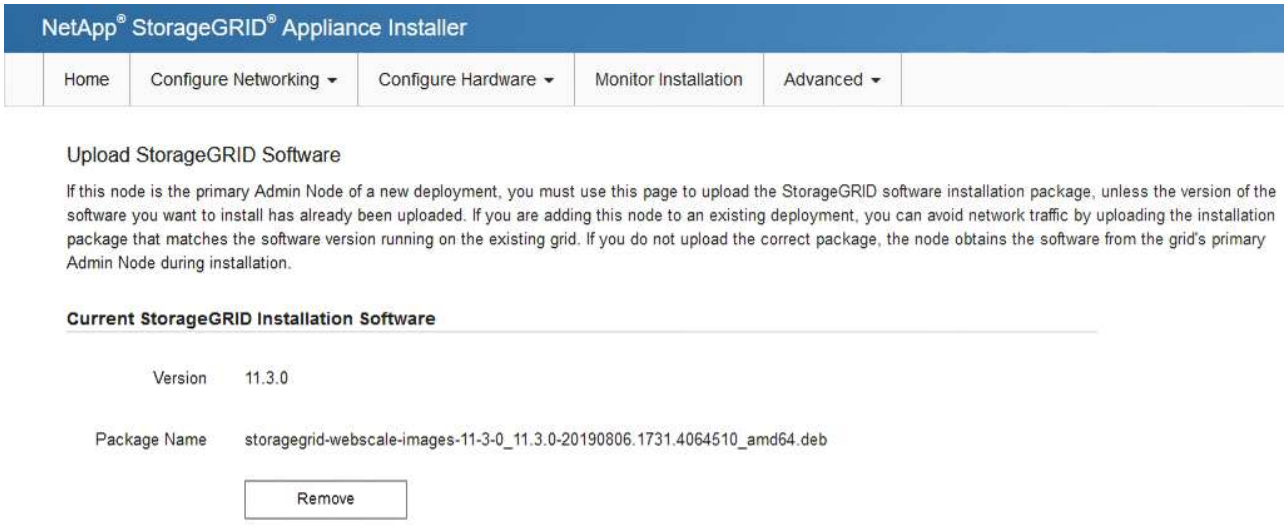
5. 或者，要安装其他版本的 StorageGRID 软件，请执行以下步骤：

   a. 下载安装归档：https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["NetApp下载：StorageGRID 设备"^]。

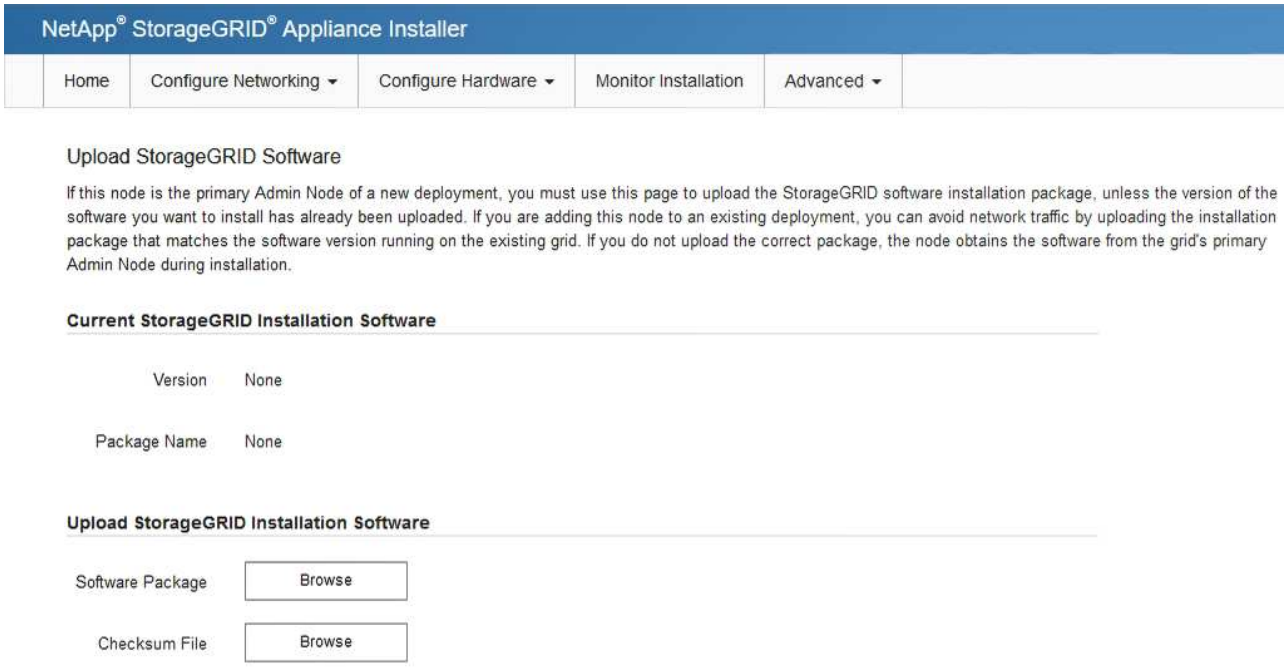
   b. 提取归档。

   c. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 上传 StorageGRID 软件 * 。

   d. 单击 * 删除 * 以删除当前软件包。



e. 单击 * 浏览 * 下载并提取的软件包，然后单击 * 浏览 * 获取校验和文件。

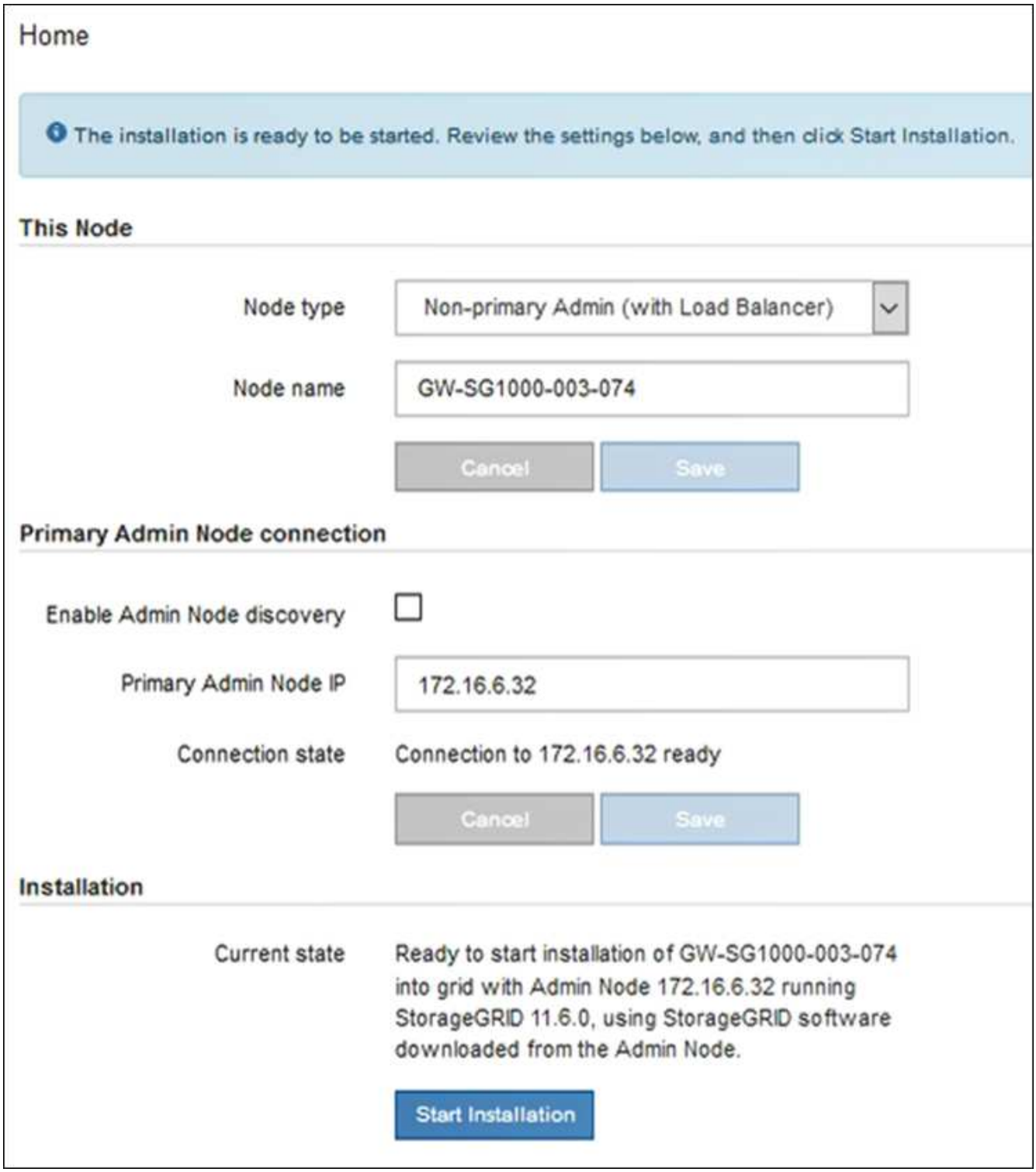


f. 选择 * 主页 * 以返回到主页页面。

6. 在 Installation 部分中，确认当前状态为 "Ready to start installation of ` node_node name_` into grid with primary Admin Node ` *admin_IP*` " ，并且 * 开始安装 * 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

7. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。



当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

如果需要手动访问监控器安装页面，请单击菜单栏中的 * 监控器安装 * 。

8. 如果网格包含多个设备节点，请对每个设备重复上述步骤。

监控服务设备安装

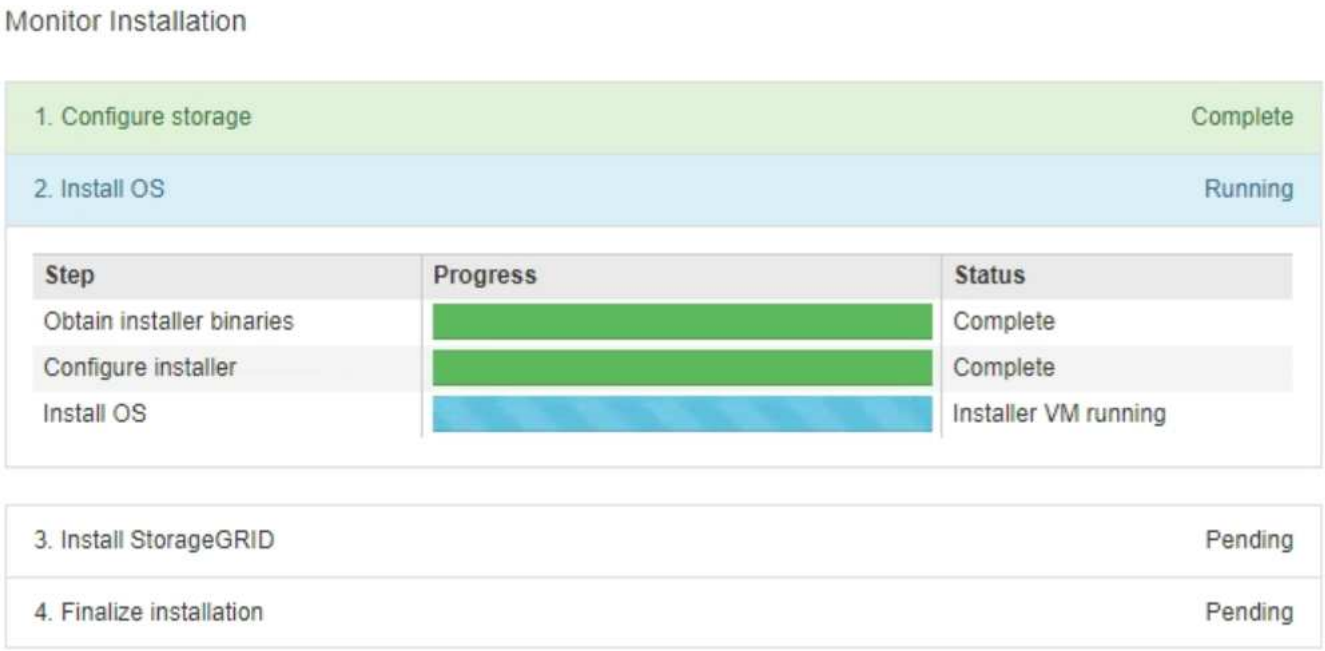
在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新

启动。

步骤

1. 要监控安装进度，请单击菜单栏中的 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

2. 查看前两个安装阶段的进度。

   ◦ * 。配置存储 *

   在此阶段，安装程序将从设备中的驱动器中清除任何现有配置，并配置主机设置。

   ◦ * 。安装 OS*

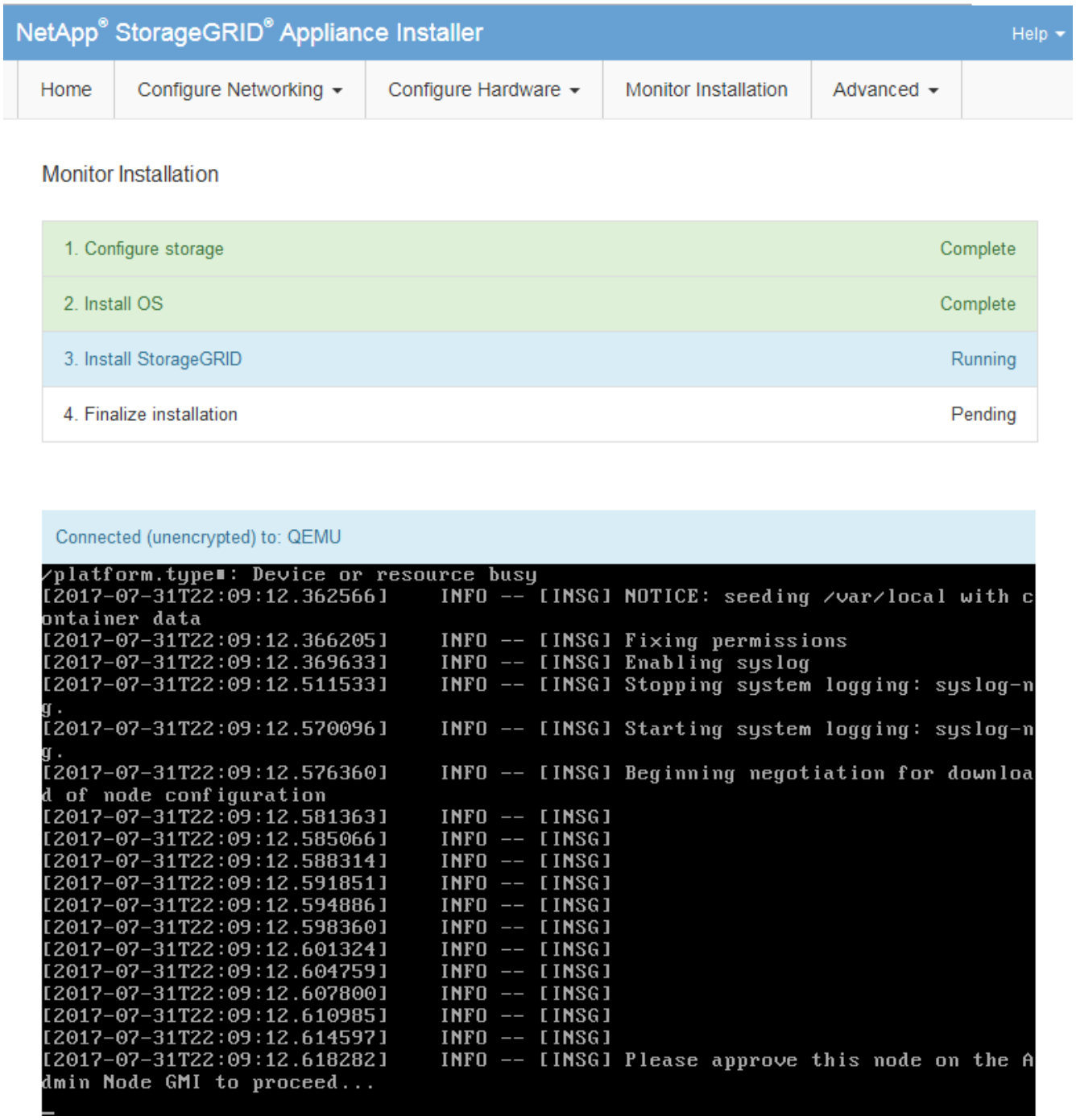
   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

3. 继续监控安装进度，直到出现以下过程之一：

   ◦ 对于除主管理节点之外的所有设备节点，安装 StorageGRID 阶段将暂停，嵌入式控制台上会显示一条消息，提示您使用网格管理器在管理节点上批准此节点。继续执行下一步。

   ◦ 对于设备主管理节点安装，您无需批准该节点。设备将重新启动。您可以跳过下一步。

   > 在安装设备主管理节点期间，将显示第五个阶段（请参见显示四个阶段的示例屏幕截图）。如果第五阶段的进度超过 10 分钟，请手动刷新网页。



4. 转至主管理节点的网格管理器，批准待定网格节点，然后完成 StorageGRID 安装过程。

   在网格管理器中单击 * 安装 * 后，第 3 阶段完成，第 4 阶段 * 完成安装 * 开始。阶段 4 完成后，设备将重新启动。

自动化设备安装和配置（ **SG100** 和 **SG1000** ）

您可以自动安装和配置设备以及配置整个 StorageGRID 系统。

关于此任务

自动化安装和配置对于部署多个 StorageGRID 实例或一个大型复杂的 StorageGRID 实例非常有用。

要自动执行安装和配置，请使用以下一个或多个选项：

- 创建一个 JSON 文件，用于指定设备的配置设置。使用 StorageGRID 设备安装程序上传 JSON 文件。

  您可以使用同一文件配置多个设备。

- 使用 StorageGRID`configure-sGa.py` Python 脚本自动配置设备。
- 使用其他 Python 脚本配置整个 StorageGRID 系统的其他组件（ " 网格 " ）。

您可以直接使用 StorageGRID 自动化 Python 脚本，也可以使用它们作为示例，说明如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。请参见的说明 下载并提取 StorageGRID 安装文件。

使用 **StorageGRID** 设备安装程序自动配置设备

您可以使用包含配置信息的 JSON 文件自动配置设备。您可以使用 StorageGRID 设备安装程序上传文件。

您需要的内容

- 您的设备必须使用与 StorageGRID 11.5 或更高版本兼容的最新固件。
- 您必须连接到要使用配置的设备上的 StorageGRID 设备安装程序 支持的 Web 浏览器。

关于此任务

您可以自动执行设备配置任务，例如配置以下内容：

- 网格网络，管理网络和客户端网络 IP 地址
- BMC 接口
- 网络链路
  - 端口绑定模式
  - 网络绑定模式
  - 链路速度

使用上传的 JSON 文件配置设备通常比在 StorageGRID 设备安装程序中使用多个页面手动执行配置效率更高，尤其是在需要配置多个节点时。您必须一次应用一个节点的配置文件。

希望自动安装和配置设备的经验丰富的用户可以 使用 configure-sga.py 脚本。

步骤

1. 使用以下方法之一生成 JSON 文件：
   - 。 "ConfigBuilder 应用程序"。
   - 。 configure-sga.py设备配置脚本。您可以从StorageGRID 设备安装程序(帮助*设备配置脚本)下载此脚本。

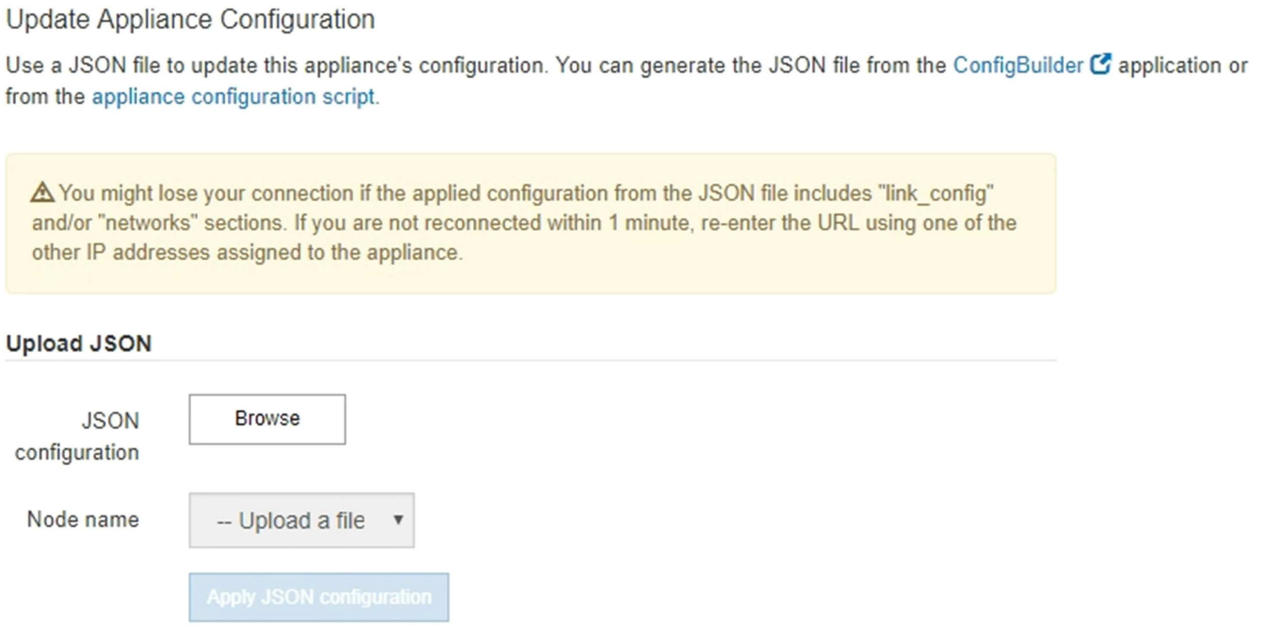
     JSON 文件中的节点名称必须符合以下要求：

- 必须是一个有效的主机名，至少包含 1 个字符，并且不超过 32 个字符
- 可以使用字母，数字和连字符
- 不能以连字符开头或结尾
- 不能仅包含数字

> 请确保 JSON 文件中的节点名称（顶级名称）是唯一的，否则您将无法使用 JSON 文件配置多个节点。

2. 选择 * 高级 * > * 更新设备配置 * 。

   此时将显示更新设备配置页面。

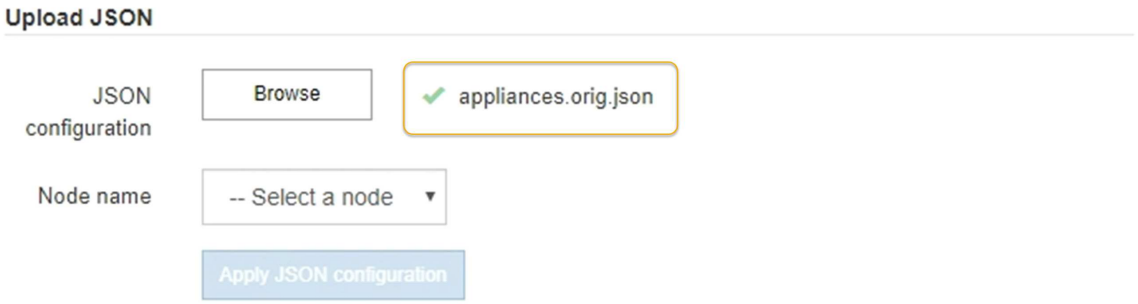


3. 选择包含要上传的配置的 JSON 文件。

   a. 选择 * 浏览 * 。
   b. 找到并选择文件。
   c. 选择 * 打开 * 。

   已上传并验证此文件。验证过程完成后，文件名会显示在绿色复选标记旁边。

> 如果 JSON 文件中的配置包含 "link_config" ， "networks" 或这两者的部分，则可能会断开与设备的连接。如果 1 分钟内未重新连接，请使用分配给设备的其他 IP 地址之一重新输入设备 URL 。

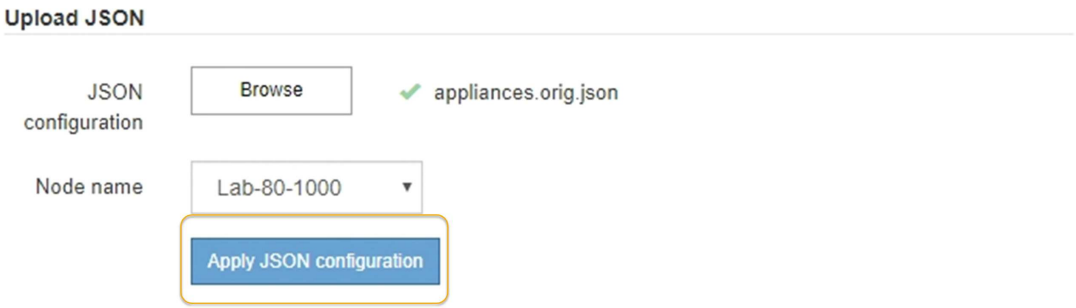


此时将使用 JSON 文件中定义的顶级节点名称填充 * 节点名称 * 下拉列表。

如果文件无效，则文件名将显示为红色，并在黄色横幅中显示一条错误消息。此无效文件不会应用于此设备。您可以使用 ConfigBuilder 来确保具有有效的 JSON 文件。

4. 从 * 节点名称 * 下拉列表中选择一个节点。

   此时将启用 * 应用 JSON 配置 * 按钮。



5. 选择 * 应用 JSON 配置 * 。

   此配置将应用于选定节点。

使用 **configure-sga.py** 脚本自动安装和配置设备节点

您可以使用 `configure-sGa.py` 脚本自动执行 StorageGRID 设备节点的许多安装和配置任务，包括安装和配置主管理节点。如果要配置大量设备，此脚本可能会很有用。您也可以使用此脚本生成包含设备配置信息的 JSON 文件。

您需要的内容

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为主管理节点配置网络链路和 IP 地址。
- 如果要安装主管理节点，则您知道其 IP 地址。
- 如果要安装和配置其他节点，则已部署主管理节点，并且您知道其 IP 地址。
- 对于主管理节点以外的所有节点，已在主管理节点上的网格网络子网列表中定义 StorageGRID 设备安装程

序的 IP 配置页面上列出的所有网格网络子网。

- 您已下载 `configure-sGA .py` 文件。该文件包含在安装归档中，您也可以通过单击 StorageGRID 设备安装程序中的 * 帮助 * > * 设备安装脚本 * 来访问该文件。

> 此操作步骤 适用于在使用命令行界面方面具有一定经验的高级用户。或者，您也可以 使用 StorageGRID 设备安装程序自动执行配置。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 要获得有关脚本语法的一般帮助以及查看可用参数列表，请输入以下内容：

```
configure-sga.py --help
```

`configure-sGa.py` 脚本使用五个子命令：

- **高级** 用于高级 StorageGRID 设备交互，包括 BMC 配置和创建包含设备当前配置的 JSON 文件
- `configure` 用于配置 RAID 模式，节点名称和网络参数
- `install` 用于开始 StorageGRID 安装
- `m` 监控 StorageGRID 安装
- `reboot` 用于重新启动设备

  如果输入子命令（ advanced ， configure ， install ， monitor 或 reboot ）参数，然后输入 ` -help` 选项，则会收到其他帮助文本，其中提供了有关该子命令中可用选项的更多详细信息： + `configure-sga.py` *`subcommand`* `-help`

3. 要确认设备节点的当前配置，请输入以下内容，其中 ` *SGA-install-IP*` 是设备节点的任一 IP 地址： + `configure-sga.py configure` *`SGA-install-IP`*

结果将显示设备的当前 IP 信息，包括主管理节点的 IP 地址以及有关管理，网格和客户端网络的信息。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
```

```
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
  MTU:       1500
```

```
  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

########################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
########################################################################
```

4. 如果需要更改当前配置中的任何值，请使用 `configure` 子命令对其进行更新。例如，如果要将设备用于连接到主管理节点的 IP 地址更改为 `172.16.2.99` ，请输入以下内容： + `configure-sga.py configure -admin-IP 172.16.2.99 sGA-install-ip`
5. 如果要将设备配置备份到 JSON 文件，请使用 advanced 和 `backup-file` 子命令。例如，如果要将 IP 地址为 ` SGA-install-ip_` 的设备配置备份到名为 `appliance-SG1000.json` 的文件中，请输入以下命令： + `configure-sga.py advanced -backup-file appliance-SG1000.json SGA-install-IP`

   包含配置信息的 JSON 文件将写入执行脚本的同一目录。

   > 检查生成的 JSON 文件中的顶级节点名称是否与设备名称匹配。请勿对此文件进行任何更改，除非您是经验丰富的用户并全面了解 StorageGRID API 。

6. 如果对设备配置满意，请使用 `install` 和 `monitor` 子命令安装此设备： + `configure-sga.py install -monitor sGA-install-ip`
7. 如果要重新启动设备，请输入以下内容： + `configure-sga.py reboot sGA-install-ip`

自动配置 **StorageGRID**

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	**Description**
configure-storagegrid.py	用于自动配置的 Python 脚本

文件名	Description
configure-storaggrid.sample.json	用于脚本的示例配置文件
configure-storaggrid.blank.json	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

关于此任务

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

> 您也可以使用配置系统 网格管理器 或 安装 API。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如： + `cd StorageGRID-Webscale -version/platform`

   其中，` *platform*` 是 `dEBS` ， `rpms` 或 `vSphere` 。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完成后

在配置过程中会生成一个恢复包 ` .zip` 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 `passwords.txt` 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

安装 **REST API** 概述

StorageGRID 提供了两个用于执行安装任务的 REST API： StorageGRID 安装 API 和 StorageGRID 设备安装程序 API 。

这两个 API 都使用 Swagger 开源 API 平台来提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 API

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。
- **recovery-package** —下载恢复软件包的操作。
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

StorageGRID 设备安装程序 API

StorageGRID 设备安装程序 API 可通过 HTTPS 从 ` Controller_IP_ ： 8443` 访问。

要访问 API 文档，请转到设备上的 StorageGRID 设备安装程序，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 设备安装程序 API 包括以下部分：

- * 克隆 * —用于配置和控制节点克隆的操作。
- * 加密 * —用于管理加密和查看加密状态的操作。
- * 硬件配置 * —用于在连接的硬件上配置系统设置的操作。
- * 安装 * —用于开始设备安装和监控安装状态的操作。
- * 网络连接 * - 与 StorageGRID 设备的网格，管理和客户端网络配置以及设备端口设置相关的操作。
- * 设置 * —用于帮助初始设备安装设置的操作，包括请求获取有关系统的信息并更新主管理节点 IP 。
- * 支持 * —用于重新启动控制器和获取日志的操作。
- * 升级 * —与升级设备固件相关的操作。
- **uploadsg** —用于上传 StorageGRID 安装文件的操作。

硬件安装故障排除（ SG100 和 SG1000 ）

如果您在安装期间遇到问题，查看与硬件设置和连接问题相关的故障排除信息可能会很有帮助。

查看设备的启动代码

在为设备接通电源时， BMC 会记录一系列启动代码。您可以在连接到 BMC 管理端口的图形控制台上查看这些代码。

您需要的内容

- 您知道如何访问 BMC 信息板。
- 如果您要使用 LAN 上串行（ Serial Over LAN ，故障转移），则具有使用 IPMI 故障转移控制台应用程序的经验。

步骤

1. 选择以下方法之一以查看设备控制器的启动代码，并收集所需的设备。

方法	所需设备
VGA 控制台	• 支持 VGA 的显示器 • VGA 缆线
KVM	• RJ-45 缆线

方法	所需设备
串行端口	• DB-9 串行缆线 • 虚拟串行终端
解决	• 虚拟串行终端

2. 如果您使用的是 VGA 控制台，请执行以下步骤：
   a. 将支持 VGA 的显示器连接到设备背面的 VGA 端口。
   b. 查看监控器上显示的代码。
3. 如果您使用的是 BMC KVM ，请执行以下步骤：
   a. 连接到 BMC 管理端口并登录到 BMC Web 界面。
   b. 选择 * 远程控制 * 。
   c. 启动 KVM 。
   d. 在虚拟监控器上查看代码。
4. 如果您使用的是串行端口和终端，请执行以下步骤：
   a. 连接到设备背面的 DB-9 串行端口。
   b. 使用设置 `115200 8-N-1` 。
   c. 查看通过串行终端打印的代码。
5. 如果您使用的是 SOL ，请执行以下步骤：
   a. 使用 BMC IP 地址和登录凭据连接到 IPMI SOL 。

      如果未更改 BMC root 帐户密码，则出厂默认值可能为 "calvin" 。

      ```
      ipmitool -i lanplus -H BMC_Port_IP -U root -P Password sole activate
      ```

   b. 查看虚拟串行终端上的代码。
6. 使用下表查找您的设备的代码。

代码	表示
您好	主启动脚本已启动。
HP	系统正在检查是否需要更新网络接口卡（ Network Interface Card ， NIC ）固件。
RB	应用固件更新后，系统正在重新启动。
FP	硬件子系统固件更新检查已完成。控制器间通信服务正在启动。

代码	表示
HC	系统正在检查现有 StorageGRID 安装数据。
好的	StorageGRID 设备正在运行。
HA	StorageGRID 正在运行。

相关信息

访问 BMC 界面

查看设备的错误代码

如果在设备启动时发生硬件错误， BMC 将记录一个错误代码。您可以根据需要使用 BMC 界面查看这些错误代码，然后与技术支持联系以解决此问题描述 。

您需要的内容

- 您知道如何访问 BMC 信息板。

步骤

1. 从 BMC 信息板中，选择 * BIOS POST Code* 。
2. 查看为当前代码和先前代码显示的信息。

   如果显示以下任一错误代码，请与技术支持联系以解决此问题描述 。

代码	表示
0x0E	未找到微代码
0x0F	未加载微代码
0x50	内存初始化错误。内存类型无效或内存速度不兼容。
0x51	内存初始化错误。SPD 读取失败。
0x52	内存初始化错误。内存大小无效或内存模块不匹配。
0x53	内存初始化错误。未检测到可用内存。
0x54	未指定的内存初始化错误
0x55	未安装内存
0x56	CPU 类型或速度无效

代码	表示
0x57	CPU 不匹配
0x58	CPU 自检失败或可能出现 CPU 缓存错误
0x59	未找到 CPU 微代码或微代码更新失败
0x5A	内部 CPU 错误
0x5B	重置 PPI 不可用
0x5C	PEI 阶段 BMC 自检失败
0xD0	CPU 初始化错误
0xD1	北网桥初始化错误
0xD2	南桥初始化错误
0xD3	某些架构协议不可用
0xd4	PCI 资源分配错误。资源不足。
0xD5	原有选项 ROM 没有空间
0xD6	未找到控制台输出设备
0xD7	未找到控制台输入设备
0xD8	密码无效
0xD9	加载启动选项时出错（ LoadImage 返回错误）
0xDA	启动选项失败（ StartImage 返回错误）
0xDB	闪存更新失败
0xDC	重置协议不可用
0xDD	Dxe 阶段 BMC 自检失败
0xE8	MRC： err_no_memory

代码	表示
0xE9	MRC： err_lt_lock
0xEA	MRC： err_DDR_init
0xEB	MRC： ERR_MEM_TEST
0xEC	MRC： err_vendor_specific
0xED	MRC： ERR_DIMM_COMPAT
0xEE	MRC： err_MRC_compatibility
0xEF	MRC： err_MRC_struct
0xF0	MRC： ERR_SET_VDD
0xF1	MRC： ERR_IOT_MEM_buffer
0xF2	MRC： err_rc_internal
0xF	MRC： err_invalid_REG_access
0xf4	MRC： ERR_SET_MC_FRQ
0xf5	MRC： err_read_mc_fREQ
0x70	MRC： err_DIMM_channel
0x74	MRC： err_smix_check
0xf6	MRC： err_SMBUS
0xF7	MRC： ERR_PCU
0xf8.	MRC： err_NGN
0xf9	MRC： err_interlef_failure

硬件设置似乎挂起（ **SG100** 和 **SG1000** ）

如果硬件故障或布线错误阻止 StorageGRID 设备完成启动处理，则此设备安装程序可能不

可用。

步骤

1. 查看设备上的 LED 以及 BMC 中显示的启动和错误代码。
2. 如果您需要有关解决问题描述 的帮助，请联系技术支持。

相关信息

查看设备的启动代码

查看设备的错误代码

对连接问题（ **SG100** 和 **SG1000** ）进行故障排除

如果您在 StorageGRID 设备安装期间遇到连接问题，应执行列出的更正操作步骤。

无法连接到设备

如果无法连接到服务设备，则可能存在网络问题描述 ，或者硬件安装可能未成功完成。

步骤

1. 尝试使用设备的 IP 地址对设备执行 ping 操作： + ` * ping *services_appliation_ip**`
2. 如果 ping 未收到任何响应，请确认您使用的 IP 地址正确无误。

   您可以使用网格网络，管理网络或客户端网络上设备的 IP 地址。

3. 如果 IP 地址正确，请检查设备布线， QSFP 或 SFP 收发器以及网络设置。
4. 如果可以对设备进行物理访问，则可以使用与永久链路本地 IP `169.254.0.1` 的直接连接来检查控制器网络配置，并在必要时进行更新。有关详细说明，请参见中的步骤 2 访问 StorageGRID 设备安装程序。

   如果无法解决问题描述 问题，请联系技术支持。

5. 如果 ping 成功，请打开 Web 浏览器。
6. 输入 StorageGRID 设备安装程序的 URL： + ` * https://*appliances_controller_IP*:8443**`

   此时将显示主页页面。

在 **StorageGRID** 设备安装程序运行期间重新启动服务设备

在 StorageGRID 设备安装程序运行期间，您可能需要重新启动服务设备。例如，如果安装失败，您可能需要重新启动服务设备。

关于此任务

只有在服务设备运行 StorageGRID 设备安装程序时，此操作步骤 才适用。安装完成后，此步骤将不再起作用，因为 StorageGRID 设备安装程序不再可用。

步骤

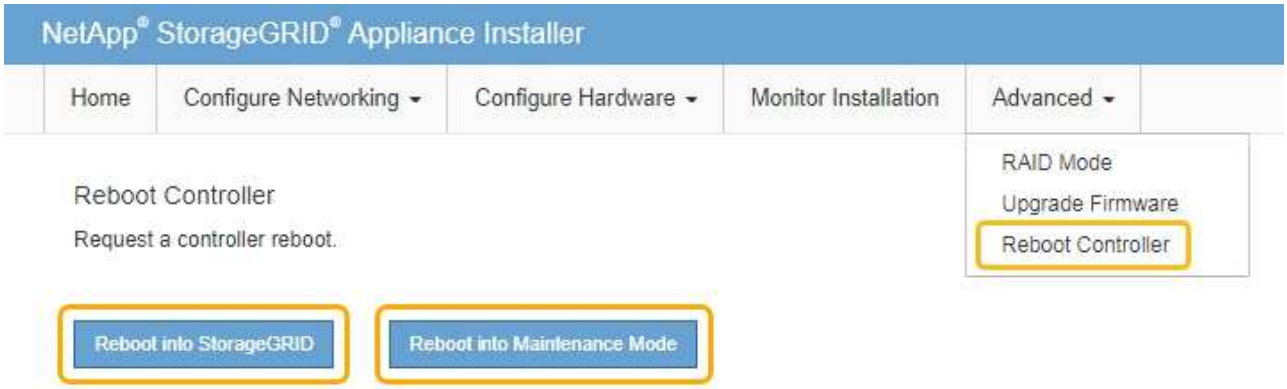
1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 高级 * > * 重新启动控制器 * 。

此时将显示重新启动控制器页面。

2. 在 StorageGRID 设备安装程序中，单击 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   ◦ 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。

   ◦ 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



服务设备将重新启动。

维护设备

您可能需要对设备执行维护过程。本节中的过程假定设备已部署为 StorageGRID 系统中的网关节点或管理节点。

将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

关于此任务

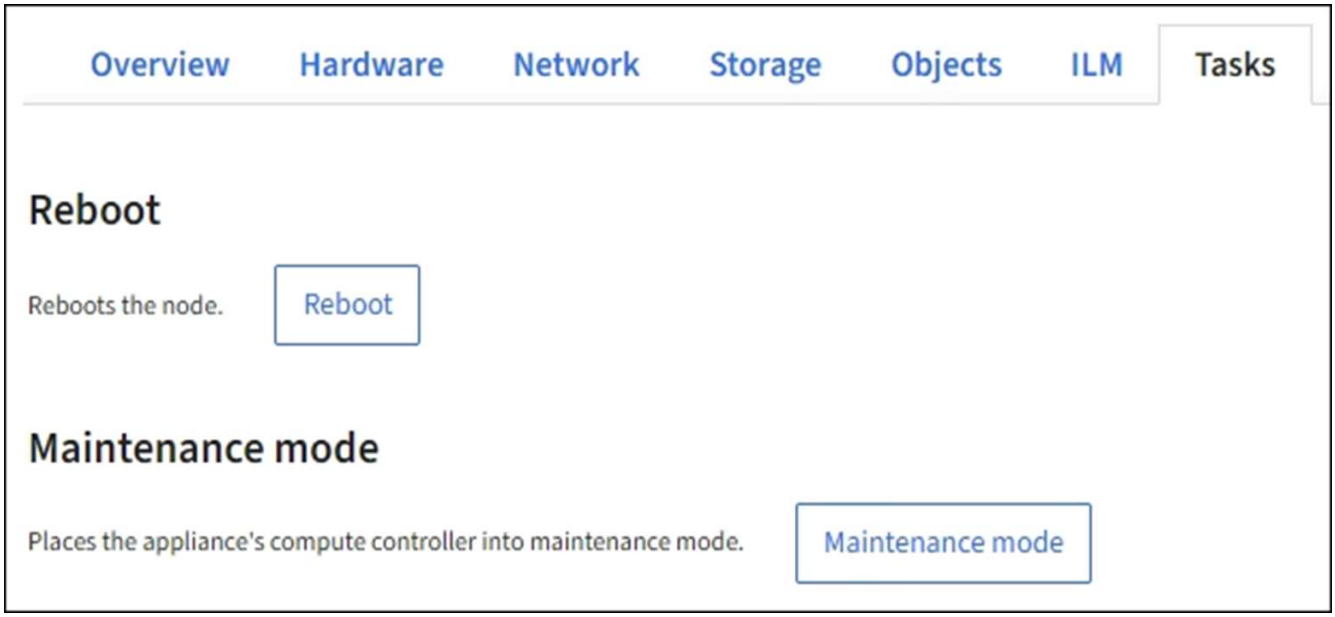
在极少数情况下，将 StorageGRID 设备置于维护模式可能会使该设备无法进行远程访问。

> 处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

步骤

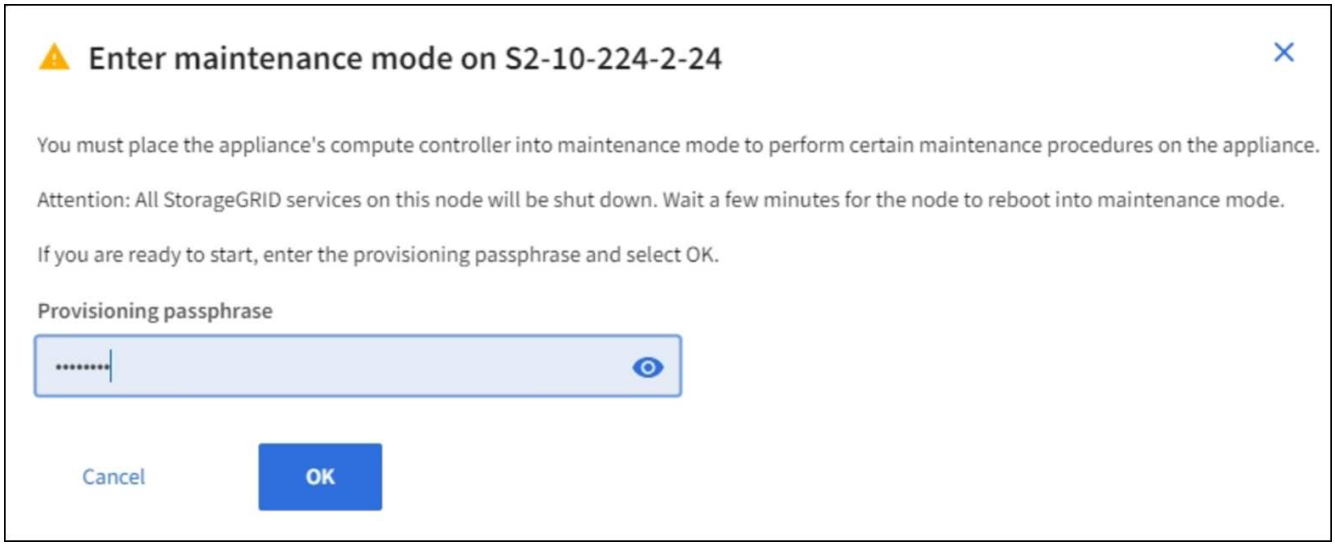
1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面的树视图中，选择设备存储节点。

3. 选择 * 任务 * 选项卡。



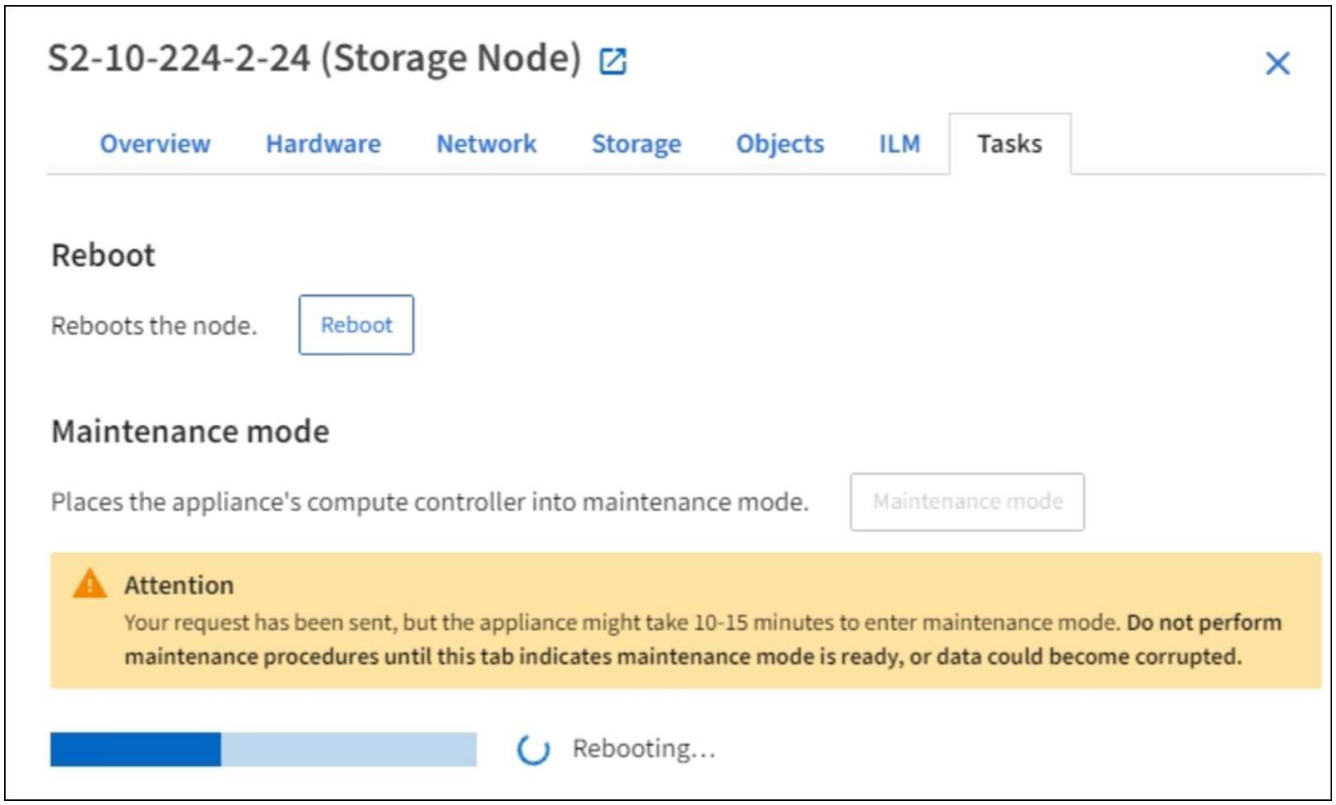
4. 选择 * 维护模式 * 。

   此时将显示确认对话框。

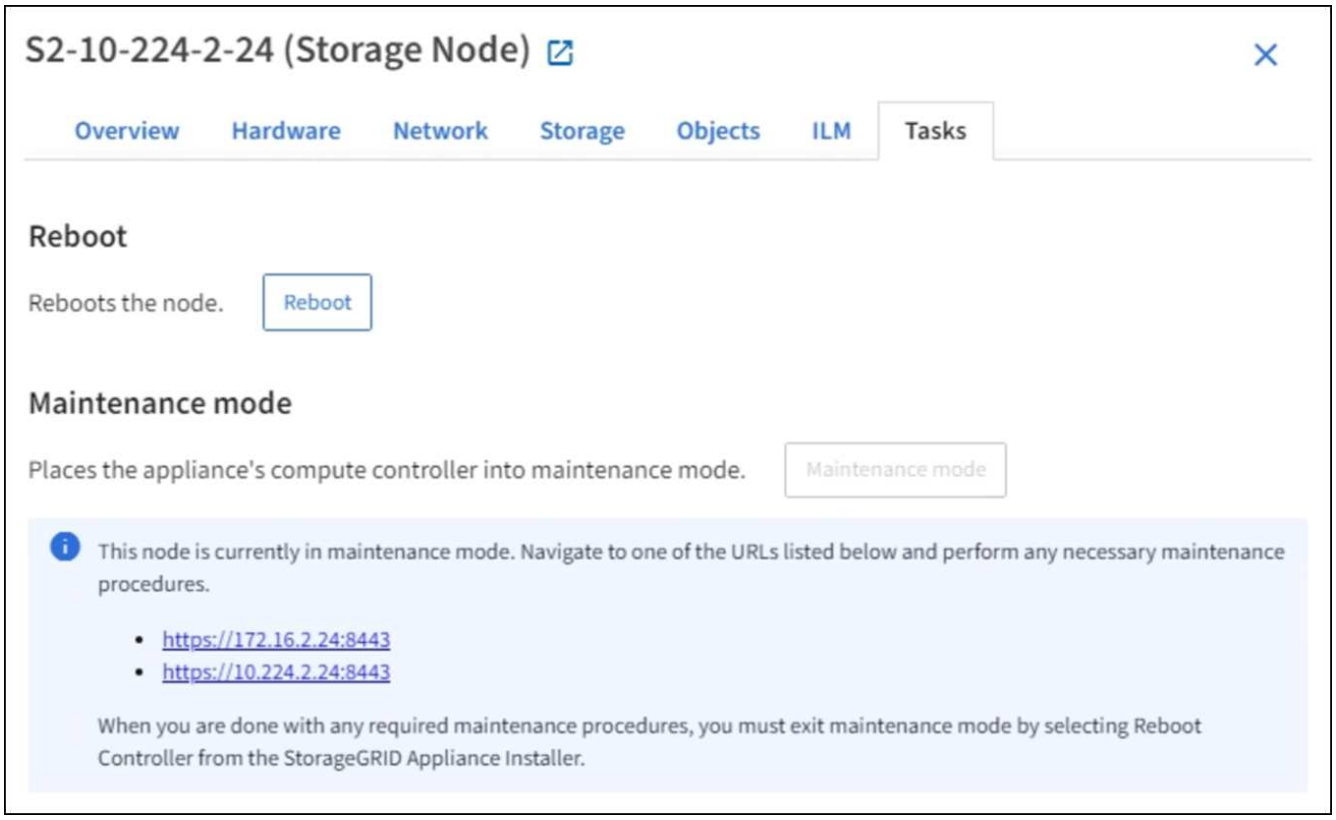


5. 输入配置密码短语，然后选择 * 确定 * 。

   进度条和一系列消息（包括 " 已发送请求 " ， " 正在停止 StorageGRID " 和 " 正在重新启动 " ）表示设备正在完成进入维护模式的步骤。



设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL 。



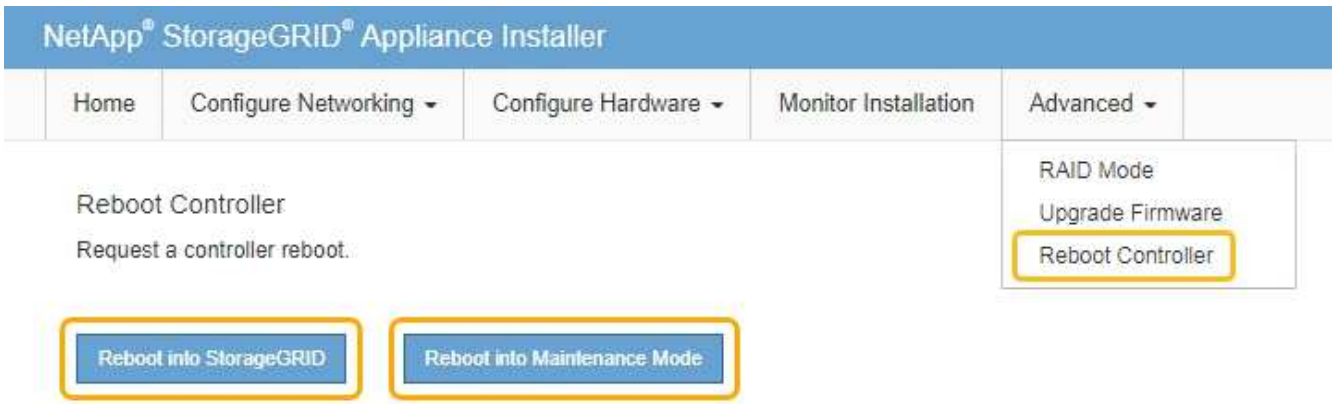
6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL 。

   如果可能，请使用包含设备管理网络端口 IP 地址的 URL 。

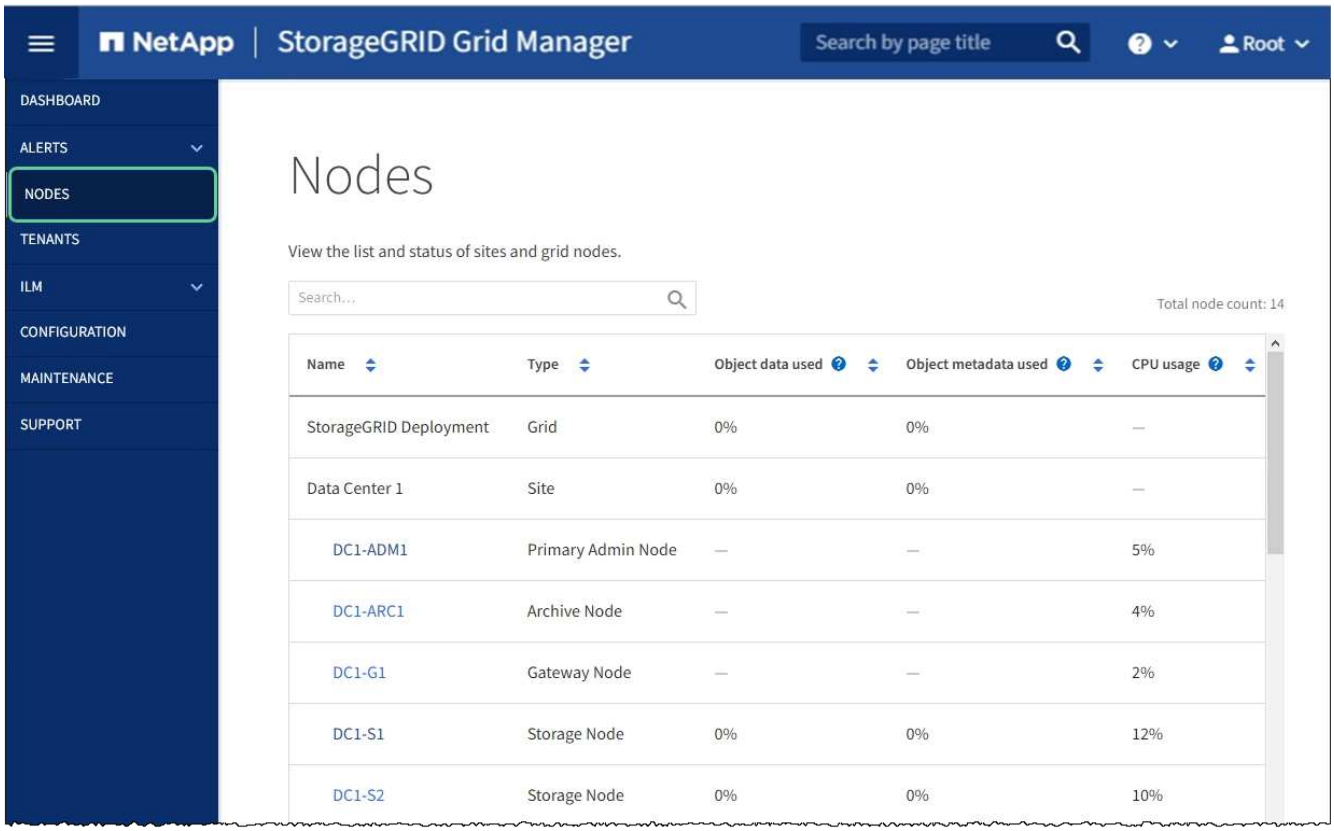
如果您直接连接到设备的管理端口，请使用 ` https://169.254.0.1:8443` 访问 StorageGRID 设备安装程序页面。

7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。

8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



打开和关闭控制器标识 **LED**

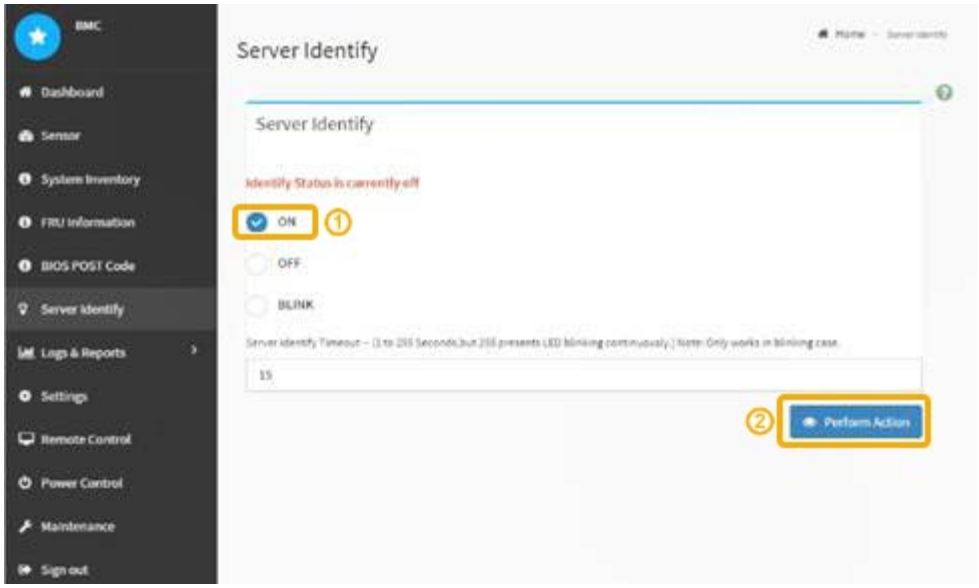
可以打开控制器正面和背面的蓝色标识 LED ，以帮助在数据中心中找到设备。

您需要的内容

您必须具有要标识的控制器的 BMC IP 地址。

步骤

1. 访问控制器 BMC 界面。
2. 选择 * 服务器标识 * 。
3. 选择 * 开 * ，然后选择 * 执行操作 * 。



结果

控制器正面（如图所示）和背面的蓝色标识 LED 亮起。

如果控制器上安装了挡板，则可能很难看到正面的识别 LED 。

完成后

要关闭控制器识别 LED ，请执行以下操作：

- 按下控制器前面板上的识别 LED 开关。
- 从控制器 BMC 界面中，选择 * 服务器标识 * ，选择 * 关闭 * ，然后选择 * 执行操作 * 。

控制器正面和背面的蓝色标识 LED 熄灭。

相关信息

在数据中心中找到控制器

访问 BMC 界面

在数据中心中找到控制器

找到控制器，以便执行硬件维护或升级。

您需要的内容

- 您已确定哪个控制器需要维护。
- （可选）为了帮助您查找数据中心中的控制器， 打开蓝色标识 LED。

步骤

1. 在数据中心中查找需要维护的控制器。
   - 查看控制器正面或背面的蓝色标识 LED 是否亮起。

     正面识别 LED 位于控制器前挡板后面，如果已安装挡板，可能很难查看。

   - 检查每个控制器正面附加的标签，以获取匹配的部件号。
2. 卸下控制器前挡板（如果已安装），以访问前面板控件和指示灯。
3. 可选：如果您使用蓝色标识 LED 来查找控制器，请将其关闭。

- 按下控制器前面板上的识别 LED 开关。
- 使用控制器 BMC 界面。

关闭服务设备

关闭服务设备以执行硬件维护。

您需要的内容

- 您已将需要维护的服务设备物理定位在数据中心。

  在数据中心中查找控制器

- 此设备已运行 置于维护模式。

关于此任务

为了防止服务中断，请在计划维护时段关闭服务设备，此时通常会发生服务中断。

步骤

1. 将设备置于维护模式后，关闭设备：

   您必须输入以下指定的命令，以有控制的方式关闭设备。使用电源开关关闭设备将导致数据丢失。

   a. 使用 PuTTY 或其他 ssh 客户端登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

   b. 关闭服务设备： + ` * shutdown -h now*`

      此命令可能需要长达 10 分钟才能完成。

2. 使用以下方法之一验证设备是否已关闭：
   - 查看设备正面的电源 LED ，确认其已关闭。
   - 检查 BMC 界面的电源控制页面，确认设备已关闭。

更换服务设备

如果设备运行不正常或出现故障，您可能需要更换设备。

您需要的内容

- 您的更换设备的部件号与要更换的设备相同。

- 您可以通过标签来识别连接到设备的每个缆线。
- 您已拥有 已物理定位设备。
- 此设备已运行 已置于维护模式。

关于此任务

更换设备时，无法访问 StorageGRID 节点。如果设备运行正常，您可以在此操作步骤 开始时执行受控关闭。

> 如果在安装 StorageGRID 软件之前更换设备，则在完成此操作步骤 后，您可能无法立即访问 StorageGRID 设备安装程序。虽然您可以从与设备位于同一子网上的其他主机访问 StorageGRID 设备安装程序，但不能从其他子网上的主机访问它。此情况应在 15 分钟内自行解决（当原始设备的任何 ARP 缓存条目超时），或者您也可以通过手动从本地路由器或网关清除任何旧的 ARP 缓存条目来立即清除此情况。

步骤

1. 将设备置于维护模式后，关闭设备。
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 关闭设备： + ` * shutdown -h now*`
2. 使用以下两种方法之一验证设备电源是否已关闭：
   - 设备正面的电源指示灯 LED 熄灭。
   - BMC 界面的电源控制页面指示设备已关闭。
3. 如果连接到设备的 StorageGRID 网络使用 DHCP 服务器，请更新 DNS/network 和 IP 地址设置。
   a. 找到设备正面的 MAC 地址标签，然后确定管理网络端口的 MAC 地址。

      > MAC 地址标签列出了 BMC 管理端口的 MAC 地址。

      要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 * 。 2 例如，如果标签上的 **MAC** 地址以 ***09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 * （ *y* ） FF* 结尾，则管理端口的 MAC 地址将以 * （ *y*+1 ） 01* 结尾。您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 * + 2 =* 来轻松进行计算。
   b. 请网络管理员将您删除的设备的 DNS/network 和 IP 地址与替换设备的 MAC 地址关联起来。

      > 在为替代设备接通电源之前，您必须确保原始设备的所有 IP 地址均已更新。否则，设备将在启动时获取新的 DHCP IP 地址，并且可能无法重新连接到 StorageGRID 。此步骤将对连接到设备的所有 StorageGRID 网络执行适用场景 。

如果原始设备使用静态 IP 地址，新设备将自动采用您删除的设备的 IP 地址。

4. 卸下并更换设备：
   a. 为缆线贴上标签，然后断开缆线和任何网络收发器的连接。

      To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

   b. 从机柜或机架中取出故障设备。
   c. 将故障设备中的两个电源，八个散热风扇和两个 SSD 传输到更换设备。

      按照提供的说明更换这些组件。

   d. 将替代设备安装到机柜或机架中。
   e. 更换缆线和任何光纤收发器。
   f. 打开设备电源并监控设备 LED 和启动代码。

      使用 BMC 界面监控启动状态。

5. 确认设备节点显示在网格管理器中且未显示任何警报。

相关信息

将设备安装到机柜或机架中（ SG100 和 SG1000 ）

查看 SG100 和 SG1000 设备上的状态指示灯

查看设备的启动代码

更换服务设备中的一个或两个电源

此服务设备具有两个电源以实现冗余。如果其中一个电源发生故障，您必须尽快更换，以确保计算控制器具有冗余电源。在控制器中运行的两个电源必须具有相同的型号和功率。

您需要的内容

- 您已拥有 已物理定位控制器 更换电源。
- 如果仅更换一个电源：
  - 您已卸载更换用的电源设备，并确保其型号和功率与要更换的电源设备相同。
  - 您已确认另一个电源已安装且正在运行。
- 如果要同时更换两个电源：
  - 您已卸载替代电源设备，并确保其型号和功率相同。

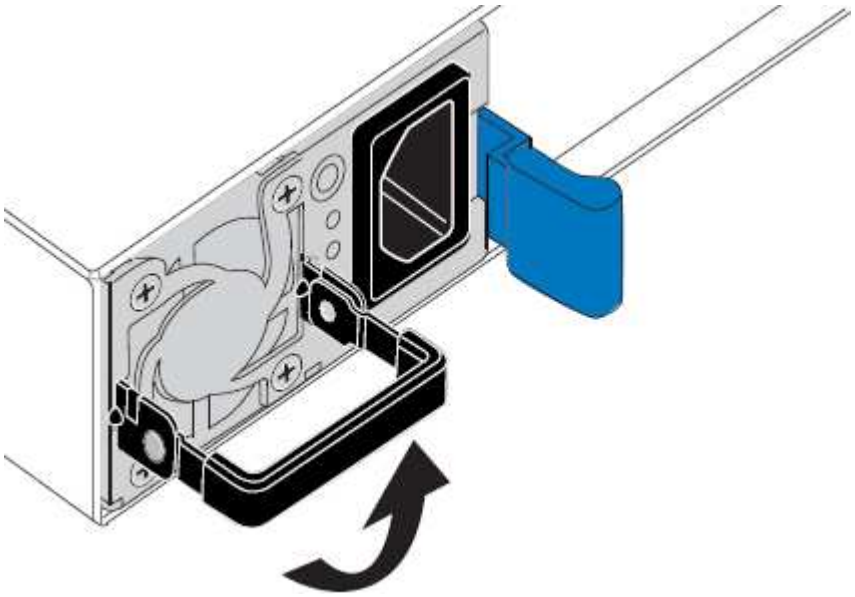
关于此任务

此图显示了 SG100 的两个电源设备，这些设备可从设备背面访问。

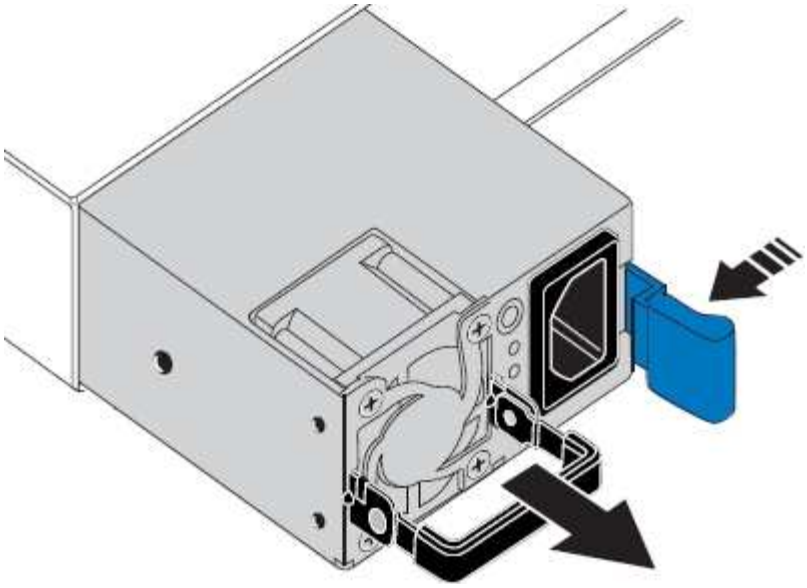
SG1000 的电源相同。

步骤

1. 如果您只更换一个电源，则无需关闭设备。转至 拔下电源线 步骤。如果要同时更换两个电源，请在拔下电源线之前执行以下操作：
   a. 将设备置于维护模式。
   b. 关闭设备。
2. 【拔掉电源线， start=2]] 从要更换的每个电源中拔下电源线。
3. 提起要更换的第一个电源上的凸轮把手。



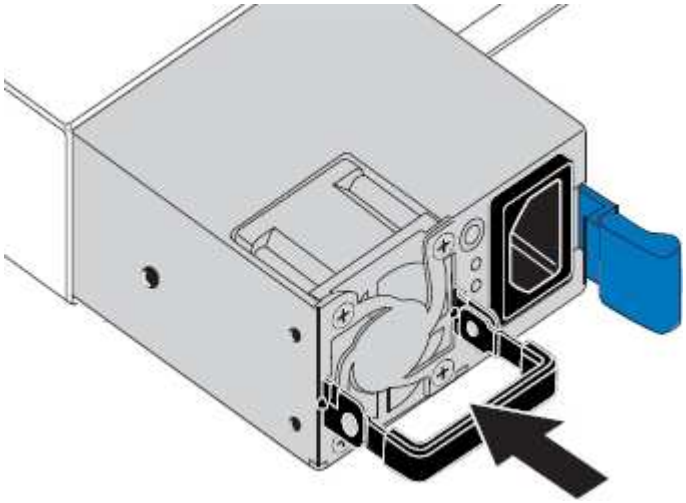
4. 按下蓝色闩锁并拉出电源。



5. 使蓝色闩锁位于右侧，将替代电源滑入机箱。

   两个电源的型号和功率必须相同。

   在中滑动更换部件时，请确保蓝色闩锁位于右侧。



6. 向下推凸轮把手以固定更换用的电源。
7. 如果要更换这两个电源，请重复步骤 2 到 6 以更换第二个电源。
8. 将电源线连接到更换的设备并接通电源。
9. 如果您将设备置于维护模式，请退出维护模式。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。

更换服务设备中的风扇

此服务设备具有八个散热风扇。如果其中一个风扇发生故障，您必须尽快更换，以确保设备具有适当的散热效果。

您需要的内容

- 您已卸载替代风扇。
- 您已拥有 已物理定位设备。
- 您已确认其他风扇已安装并正在运行。
- 您已拥有 已将设备置于维护模式。

关于此任务

更换风扇时，无法访问设备节点。

图中显示了服务设备的风扇。将顶盖从设备上取下后，即可访问散热风扇。

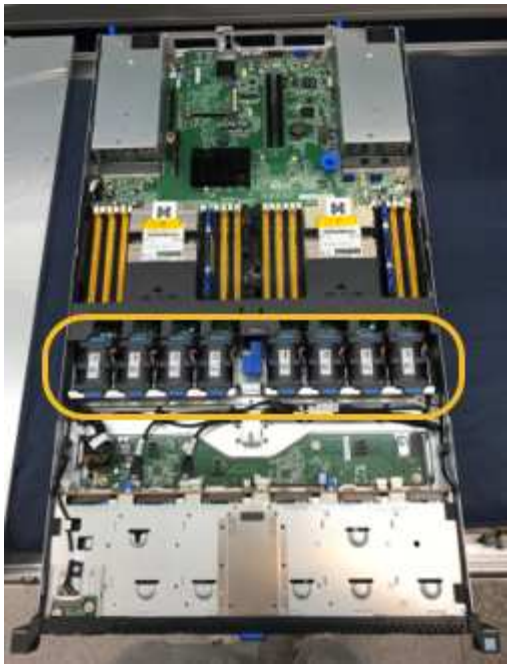
两个电源设备中的每个设备都包含一个风扇。此操作步骤 不包括这些风扇。

步骤

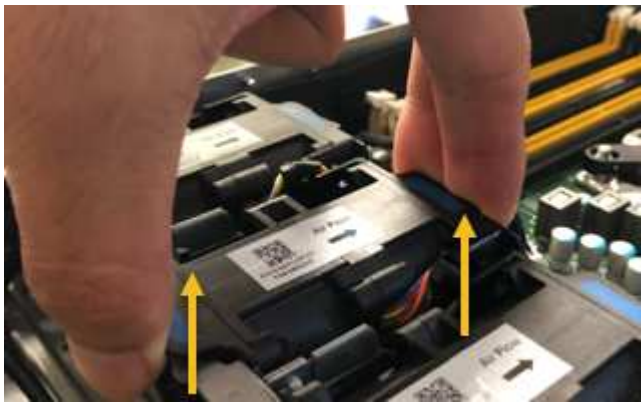
1. 将设备置于维护模式后，关闭设备。
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

   b. 关闭服务设备： + ` * shutdown -h now*`
2. 使用以下两种方法之一验证服务设备的电源是否已关闭：
   - 设备正面的电源指示灯 LED 熄灭。
   - BMC 界面的电源控制页面指示设备已关闭。
3. 将设备从机架中拉出。
4. 提起顶盖上的闩锁，然后从设备中卸下此盖板。
5. 找到出现故障的风扇。

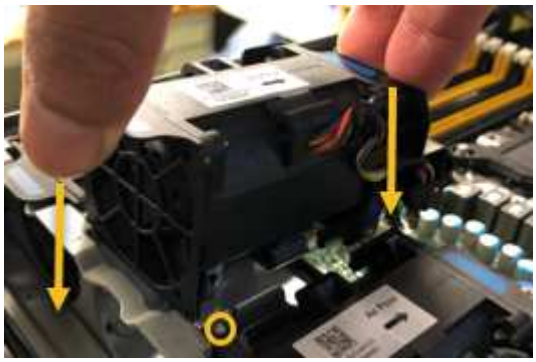


6. 将故障风扇从机箱中提出。

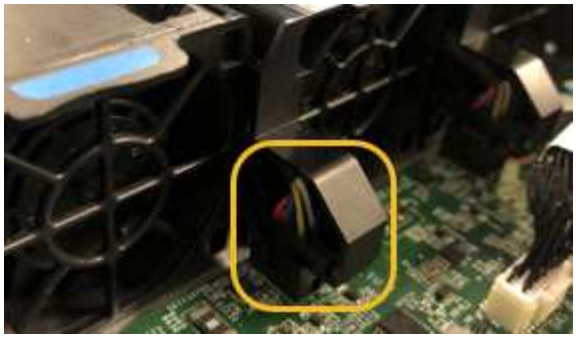


7. 将替代风扇滑入机箱中的打开插槽。

   将风扇边缘与导销对中。此销在照片中圈出。



8. 将风扇连接器稳固地按入电路板。



9. 将顶盖重新放在设备上，然后向下按压闩锁以将盖固定到位。
10. 打开设备电源并监控控制器 LED 和启动代码。

    使用 BMC 界面监控启动状态。

11. 确认设备节点显示在网格管理器中且未显示任何警报。

更换服务设备中的驱动器

服务设备中的 SSD 包含 StorageGRID 操作系统。此外，如果将设备配置为管理节点，则 SSD 还包含审核日志，指标和数据库表。驱动器使用 RAID1 进行镜像以实现冗余。如果其中一个驱动器发生故障，您必须尽快更换它以确保冗余。

您需要的内容

- 您已拥有 已物理定位设备。
- 您已通过注意到左侧 LED 呈琥珀色闪烁来验证哪个驱动器出现故障。

  如果您删除工作正常的驱动器，则会关闭设备节点。请参见有关查看状态指示器的信息以验证故障。

- 您已获得替代驱动器。
- 您已获得适当的 ESD 保护。

步骤

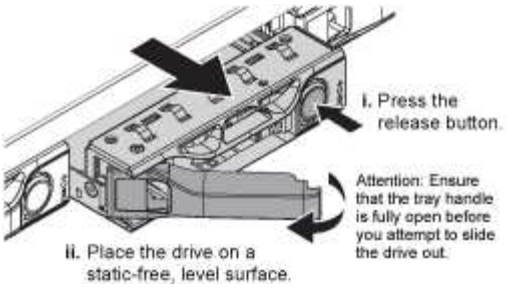
1. 验证驱动器的左侧 LED 是否呈琥珀色闪烁。

   您还可以使用网格管理器监控 SSD 的状态。选择 * 节点 * 。然后选择 ` * 设备节点 *` > * 硬件 * 。如果某个驱动器发生故障，则存储 RAID 模式字段会显示一条消息，指出哪个驱动器发生故障。

2. 将 ESD 腕带的腕带一端绕在腕带上，并将扣具一端固定到金属接地，以防止静电放电。
3. 拆开备用驱动器的包装，并将其放在设备附近的无静电水平表面上。

   节省所有包装材料。

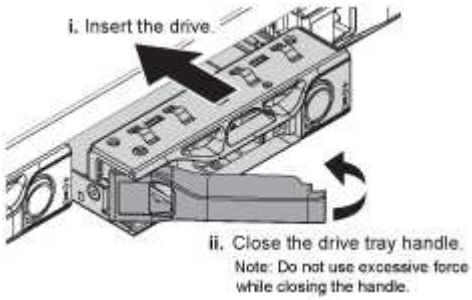
4. 按下故障驱动器上的释放按钮。



驱动器弹出器上的手柄部分打开，驱动器从插槽中释放。

5. 打开手柄，滑出驱动器，然后将其放在无静电的水平表面上。
6. 在将替代驱动器插入驱动器插槽之前，请按此驱动器上的释放按钮。

   闩锁会弹开。



7. 将替代驱动器插入插槽，然后合上驱动器手柄。

   合上手柄时，请勿用力过大。

   驱动器完全插入后，您会听到卡嗒声。

   驱动器会使用工作驱动器中的镜像数据自动重建。您可以使用网格管理器检查重建的状态。选择 * 节点 * 。然后选择 ` * 设备节点 *` > * 硬件 * 。存储 RAID 模式字段包含一条消息 `re`构建 ，直到驱动器完全重建为止。

8. 有关驱动器更换的信息，请联系技术支持。

   技术支持将提供有关退回故障驱动器的说明。

更改服务设备的链路配置

您可以更改服务设备的以太网链路配置。您可以更改端口绑定模式，网络绑定模式和链路速度。

您需要的内容

- 您已拥有 已将设备置于维护模式。

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

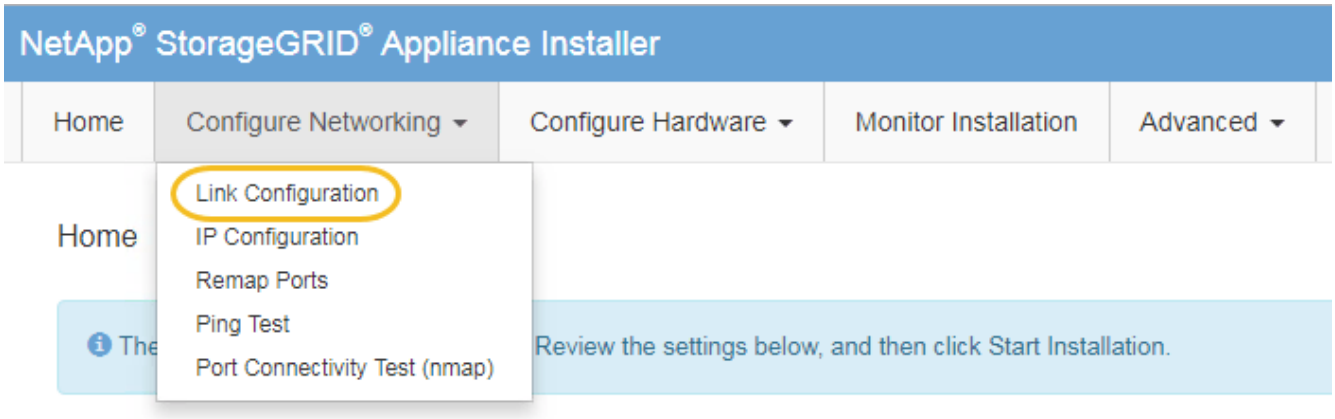
关于此任务

用于更改服务设备的以太网链路配置的选项包括：

- 将 * 端口绑定模式 * 从 " 固定 " 更改为 " 聚合 " 或从 " 聚合 " 更改为 " 固定 "
- 将 * 网络绑定模式 * 从主动备份更改为 LACP 或从 LACP 更改为主动备份
- 启用或禁用 VLAN 标记，或者更改 VLAN 标记的值
- 更改链路速度

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * 链路配置 * 。



2. 对链路配置进行所需的更改。

   有关选项的详细信息，请参见 配置网络链路。

3. 对所做的选择感到满意后，单击 * 保存 * 。

   如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*services_appliance_IP*:8443*`

4. 对设备的 IP 地址进行任何必要的更改。

   如果更改了 VLAN 设置，则设备的子网可能已更改。如果需要更改设备的 IP 地址，请参见 配置 StorageGRID IP 地址。

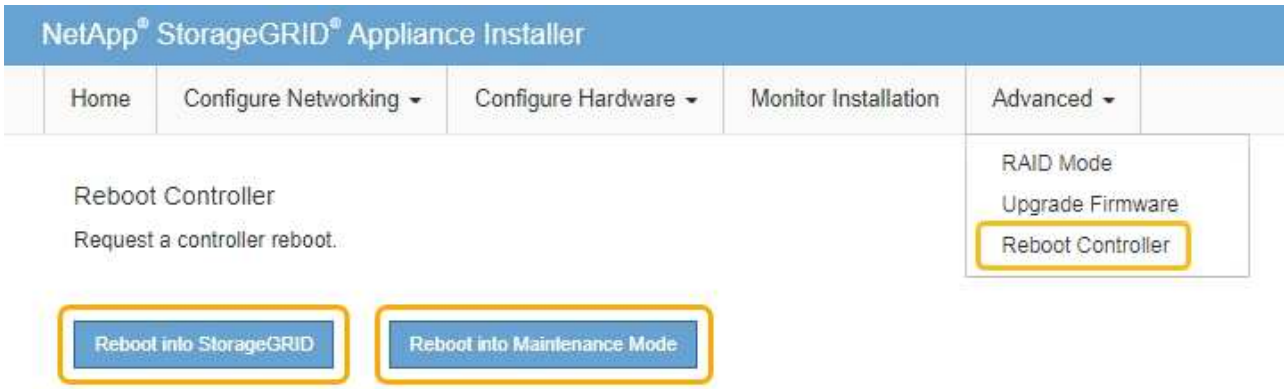
5. 从菜单中选择 * 配置网络连接 * > * Ping 测试 * 。
6. 使用 Ping 测试工具检查与任何网络上的 IP 地址的连接，这些网络可能已受到您在配置设备时所做的链路配置更改的影响。

   除了您选择执行的任何其他测试之外，请确认您可以对主管理节点的网格网络 IP 地址以及至少一个其他节点的网格网络 IP 地址执行 ping 操作。如有必要，请返回到有关配置网络链路的说明，并更正任何问题。

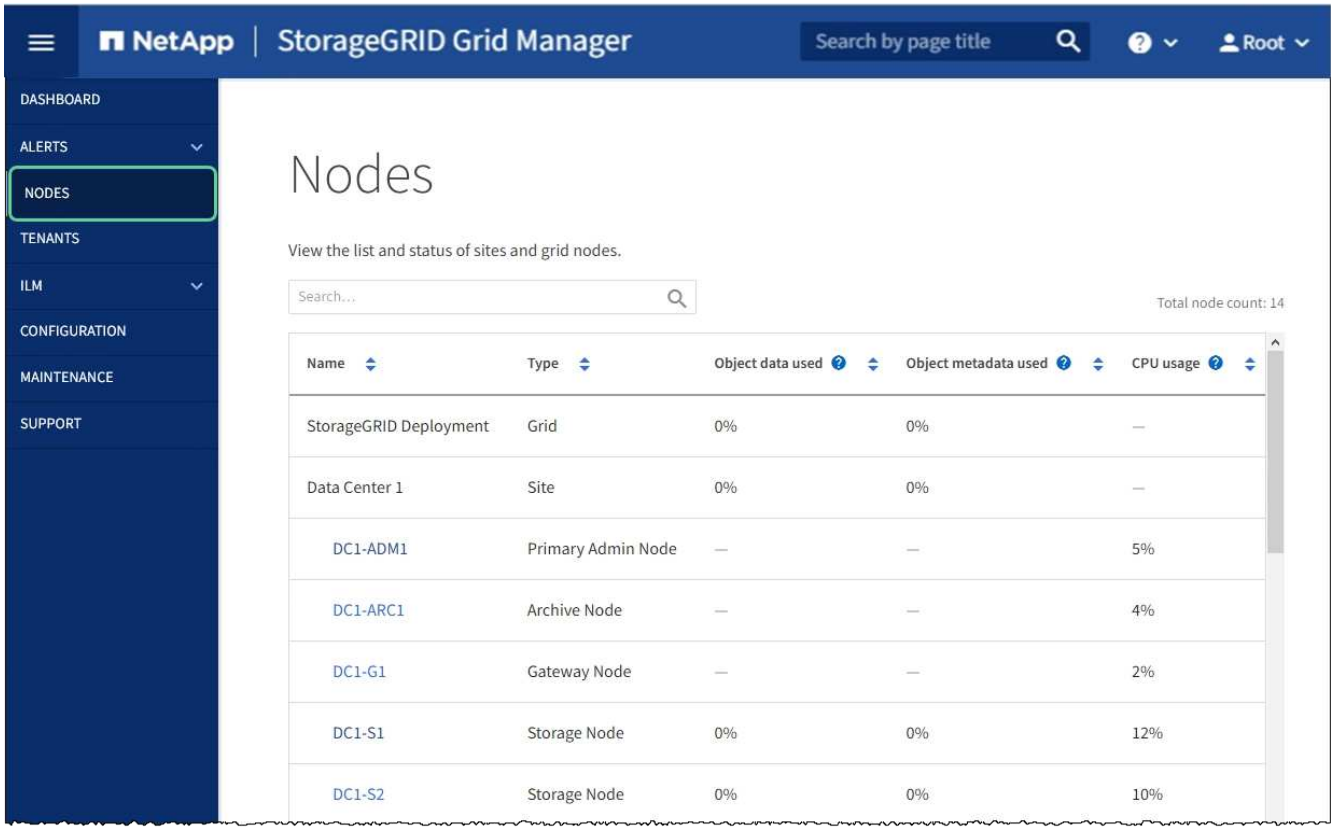
7. 在您确信链路配置更改正常运行后，请重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。

◦ 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



更改 **MTU** 设置

您可以更改在为设备节点配置 IP 地址时分配的 MTU 设置。

关于此任务

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

要在不重新启动设备节点的情况下更改 MTU 设置， 使用更改 IP 工具。

如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络， 使用维护模式更改 MTU 设置。

使用更改 **IP** 工具更改 **MTU** 设置

您需要的内容

- 您有 `passwords.txt` 文件可用于更改 IP 工具。

步骤

访问更改 IP 工具并按中所述更新 MTU 设置 更改节点网络配置。

使用维护模式更改 **MTU** 设置

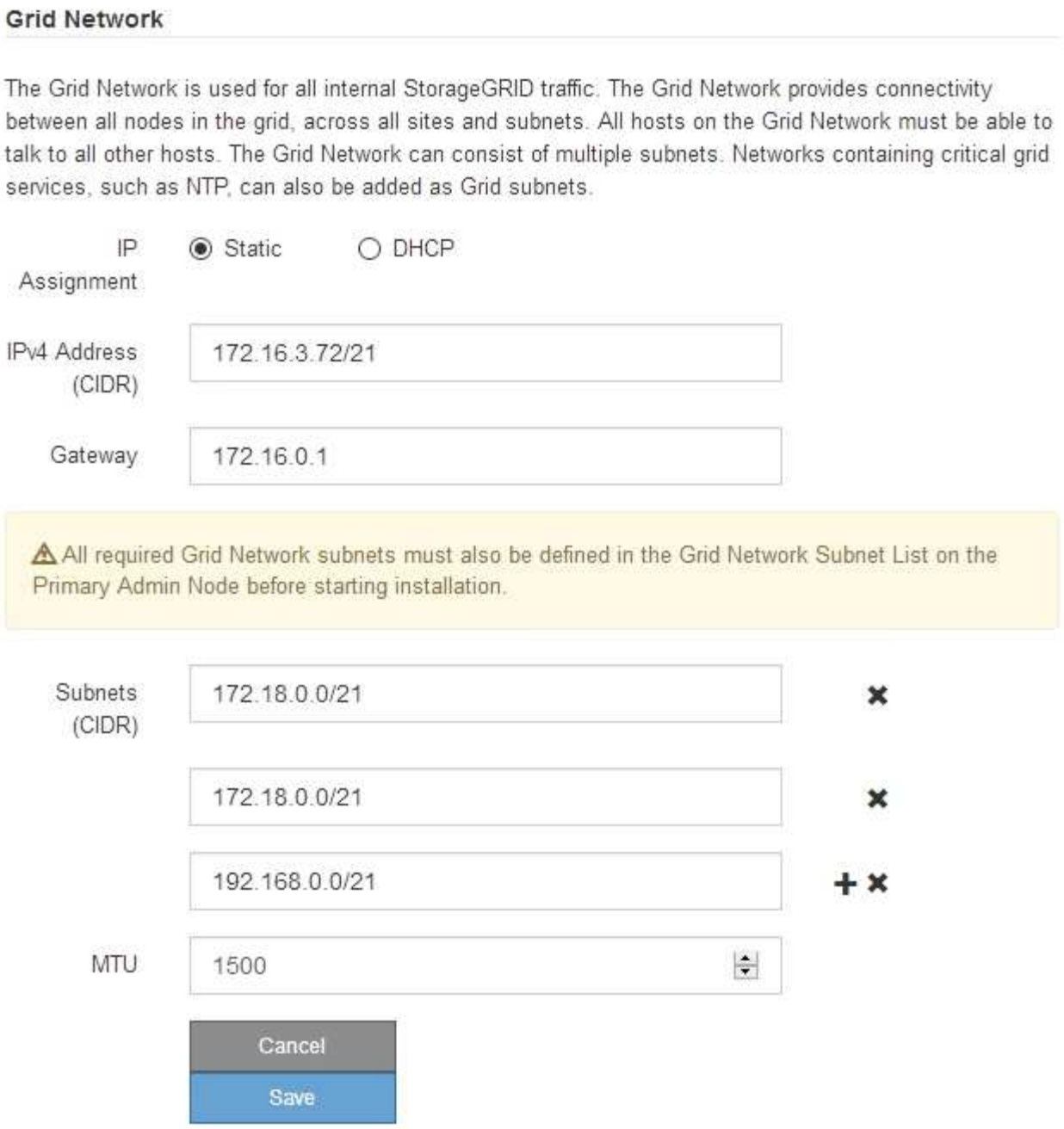
如果无法使用更改 IP 工具访问这些设置，请使用维护模式更改 MTU 设置。

您需要的内容

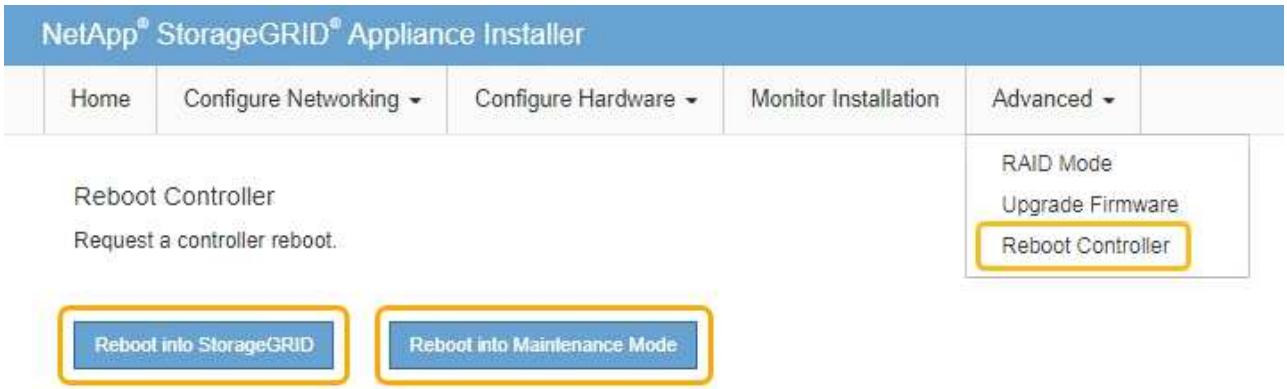
- 您已拥有 已将设备置于维护模式。

步骤

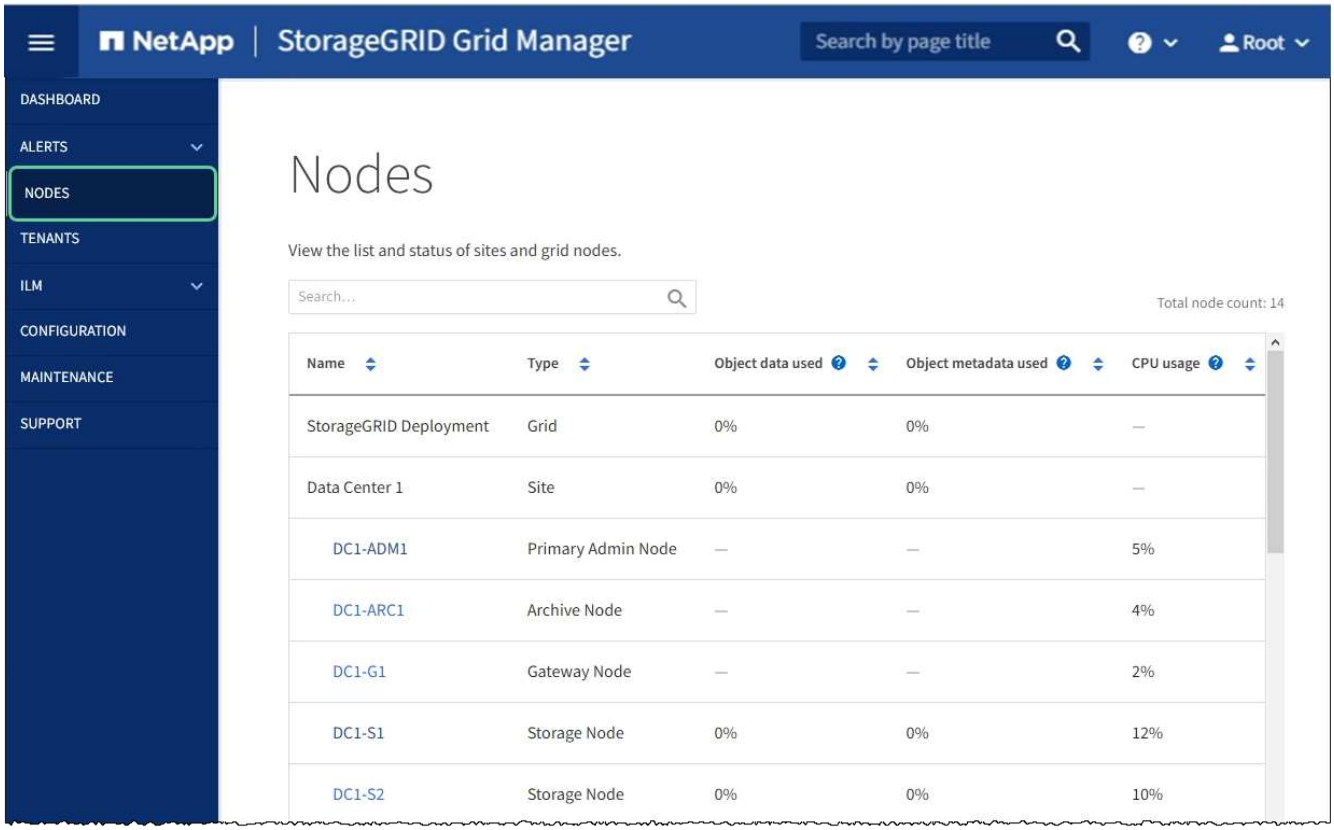
1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。
2. 对网格网络，管理网络和客户端网络的 MTU 设置进行所需的更改。



3. 如果对设置感到满意，请选择 * 保存 * 。
4. 重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：
   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

检查 **DNS** 服务器配置

您可以检查并临时更改此设备节点当前正在使用的域名系统（ DNS ）服务器。

您需要的内容

- 您已拥有 已将设备置于维护模式。

关于此任务

如果加密设备无法连接到密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群，则可能需要更改 DNS 服务器设置，因为 KMS 的主机名指定为域名，而不是 IP 地址。对设备的 DNS 设置所做的任何更改都是临时的，在退出维护模式时将丢失。要使这些更改永久生效，请在网格管理器中指定 DNS 服务器（ * 维护 * > * 网络 * > * DNS 服务器 * ）。

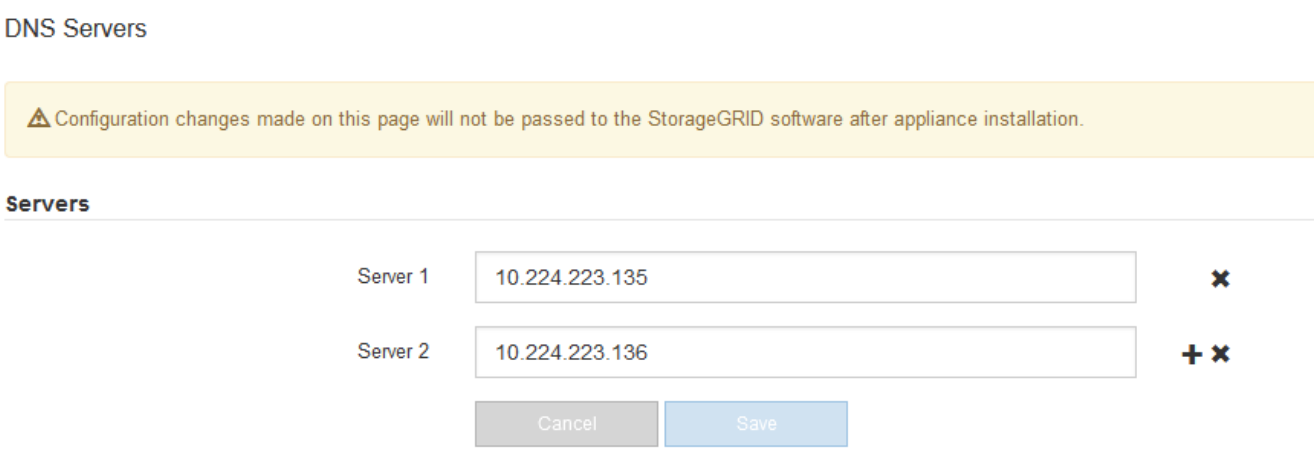
- 只有在节点加密的设备中，使用完全限定域名（而不是 IP 地址）为主机名定义 KMS 服务器时，才需要临时更改 DNS 配置。
- 当节点加密设备使用域名连接到 KMS 时，它必须连接到为网格定义的一个 DNS 服务器。然后，其中一个 DNS 服务器会将域名转换为 IP 地址。
- 如果节点无法访问网格的 DNS 服务器，或者您在节点加密设备节点脱机时更改了网格范围的 DNS 设置，则节点将无法连接到 KMS 。在解析 DNS 问题描述 之前，无法解密设备上的加密数据。

要解决 DNS 问题描述 阻止 KMS 连接的问题，请在 StorageGRID 设备安装程序中指定一个或多个 DNS 服务器的 IP 地址。通过这些临时 DNS 设置，设备可以连接到 KMS 并对节点上的数据进行解密。

例如，如果在加密节点脱机时网格的 DNS 服务器发生更改，则该节点将无法在重新联机时访问 KMS ，因为它仍在使用先前的 DNS 值。在 StorageGRID 设备安装程序中输入新的 DNS 服务器 IP 地址后，可以通过临时 KMS 连接对节点数据进行解密。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * DNS 配置 * 。
2. 验证指定的 DNS 服务器是否正确。



3. 如果需要，请更改 DNS 服务器。

   对 DNS 设置所做的更改是临时的，当您退出维护模式时，这些更改将丢失。

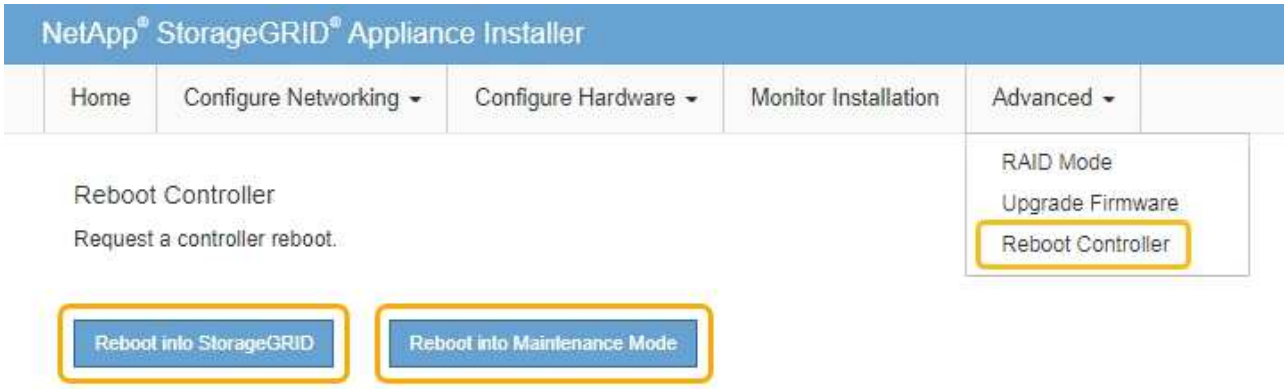
4. 对临时 DNS 设置感到满意后，请选择 * 保存 * 。

   节点使用此页面上指定的 DNS 服务器设置重新连接到 KMS ，从而可以解密节点上的数据。

5. 解密节点数据后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，

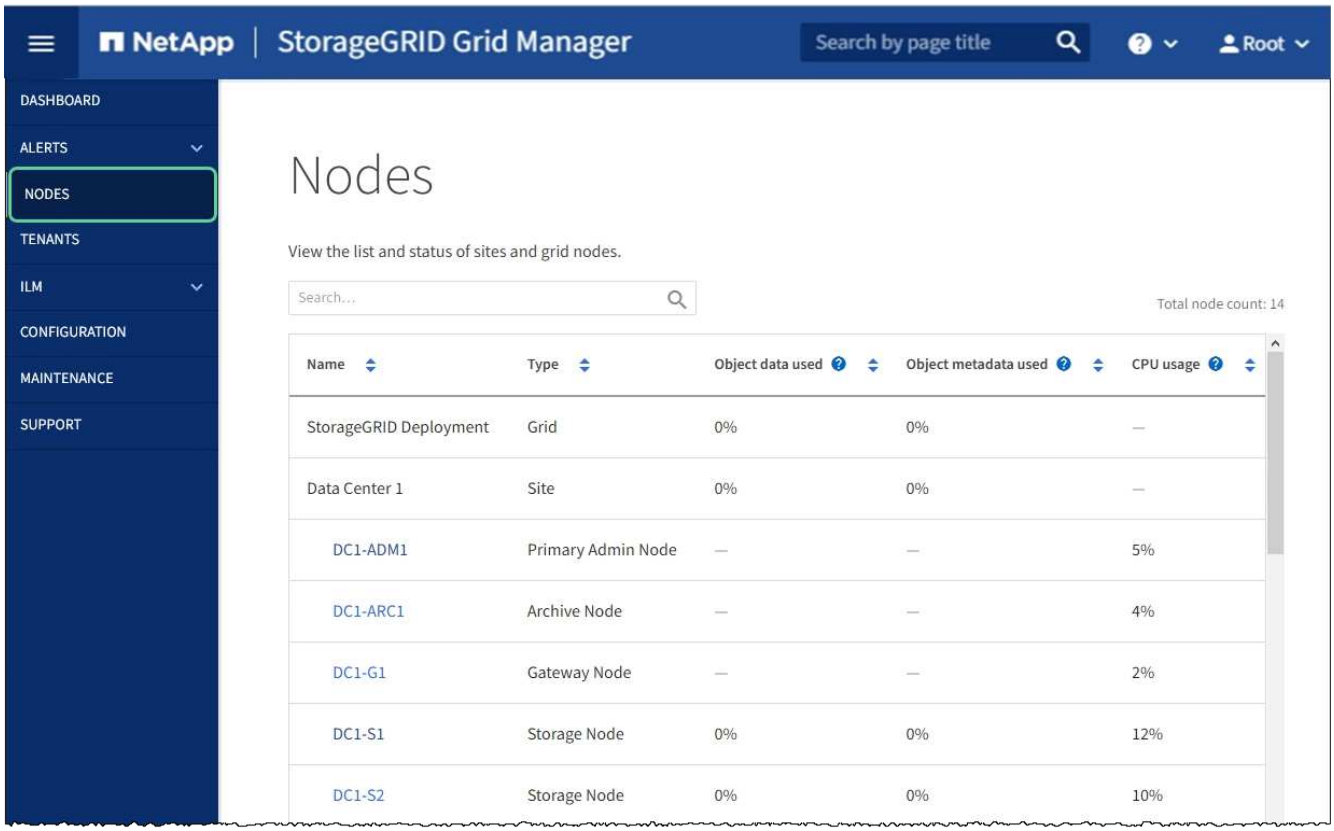
然后选择以下选项之一：

- 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
- 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



当节点重新启动并重新加入网格时，它将使用网格管理器中列出的系统范围的 DNS 服务器。重新加入网格后，在设备处于维护模式时，设备将不再使用 StorageGRID 设备安装程序中指定的临时 DNS 服务器。

设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



监控维护模式下的节点加密（ **SG100** 和 **SG1000** ）

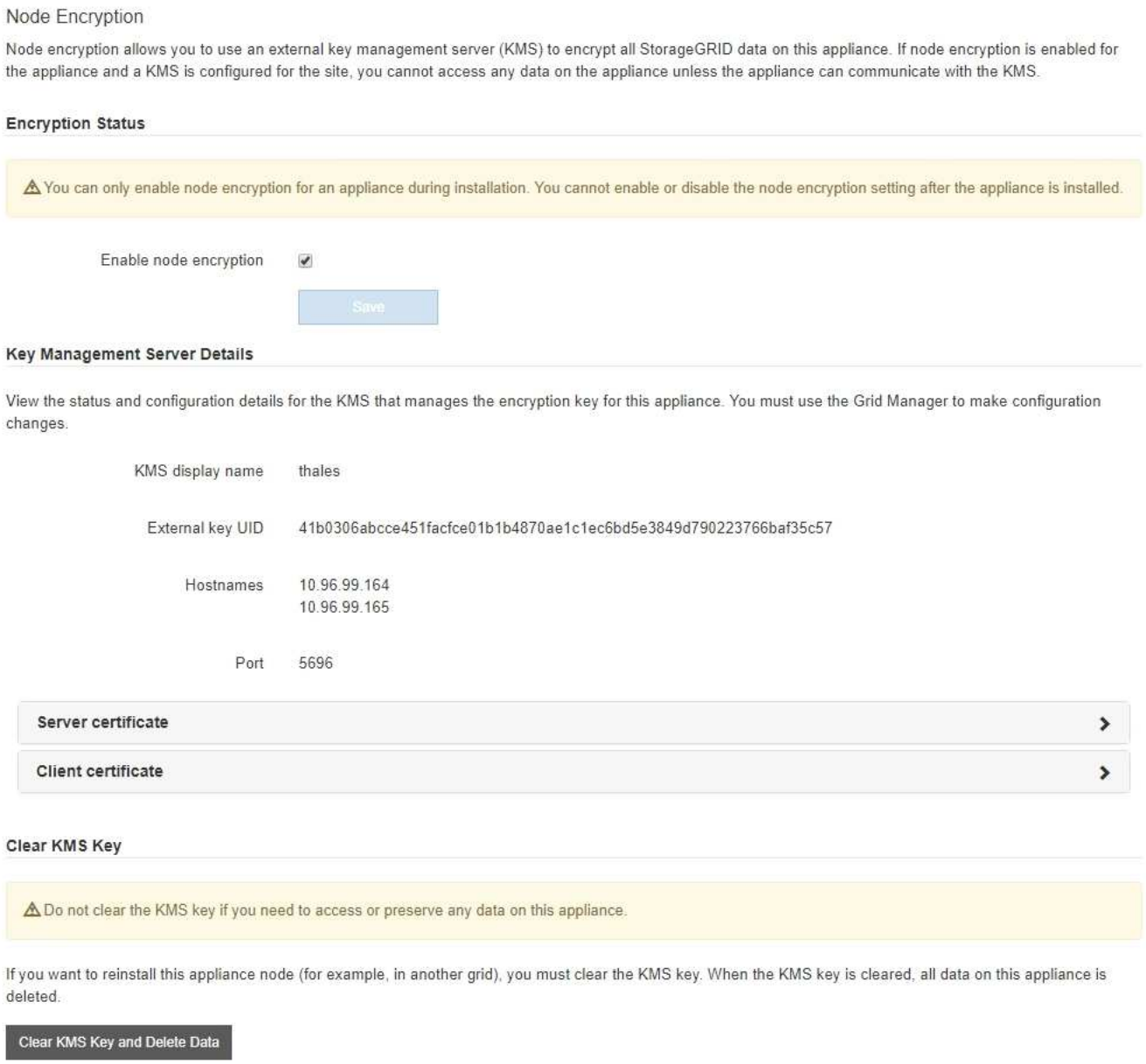
如果您在安装期间为设备启用了节点加密，则可以监控每个设备节点的节点加密状态，包括节点加密状态和密钥管理服务器（ KMS ）详细信息。

您需要的内容

- 您在安装期间为设备启用了节点加密。安装设备后，您无法启用节点加密。
- 您已拥有 已将设备置于维护模式。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置硬件 * > * 节点加密 * 。



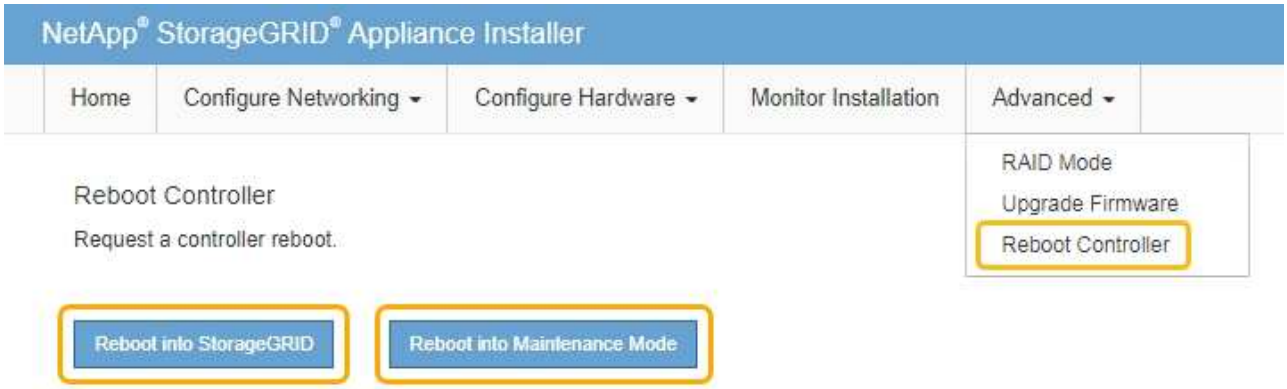
节点加密页面包括三个部分：

- " 加密状态 " 显示设备是启用还是禁用了节点加密。
- 密钥管理服务器详细信息显示了有关用于对设备进行加密的 KMS 的信息。您可以展开服务器和客户端证书部分以查看证书详细信息和状态。
  - 要解决证书本身的问题，例如续订已过期的证书，请参见 有关配置 KMS 的说明。
  - 如果连接到 KMS 主机时出现意外问题，请验证 域名系统（ DNS ）服务器正确无误 这样 已正确配置设备网络。
  - 如果无法解决证书问题，请联系技术支持。
- 清除 KMS 密钥会禁用设备的节点加密，删除设备与为 StorageGRID 站点配置的密钥管理服务器之间的关联，并删除设备中的所有数据。您必须 清除 KMS 密钥 在将设备安装到另一个 StorageGRID 系统之前。

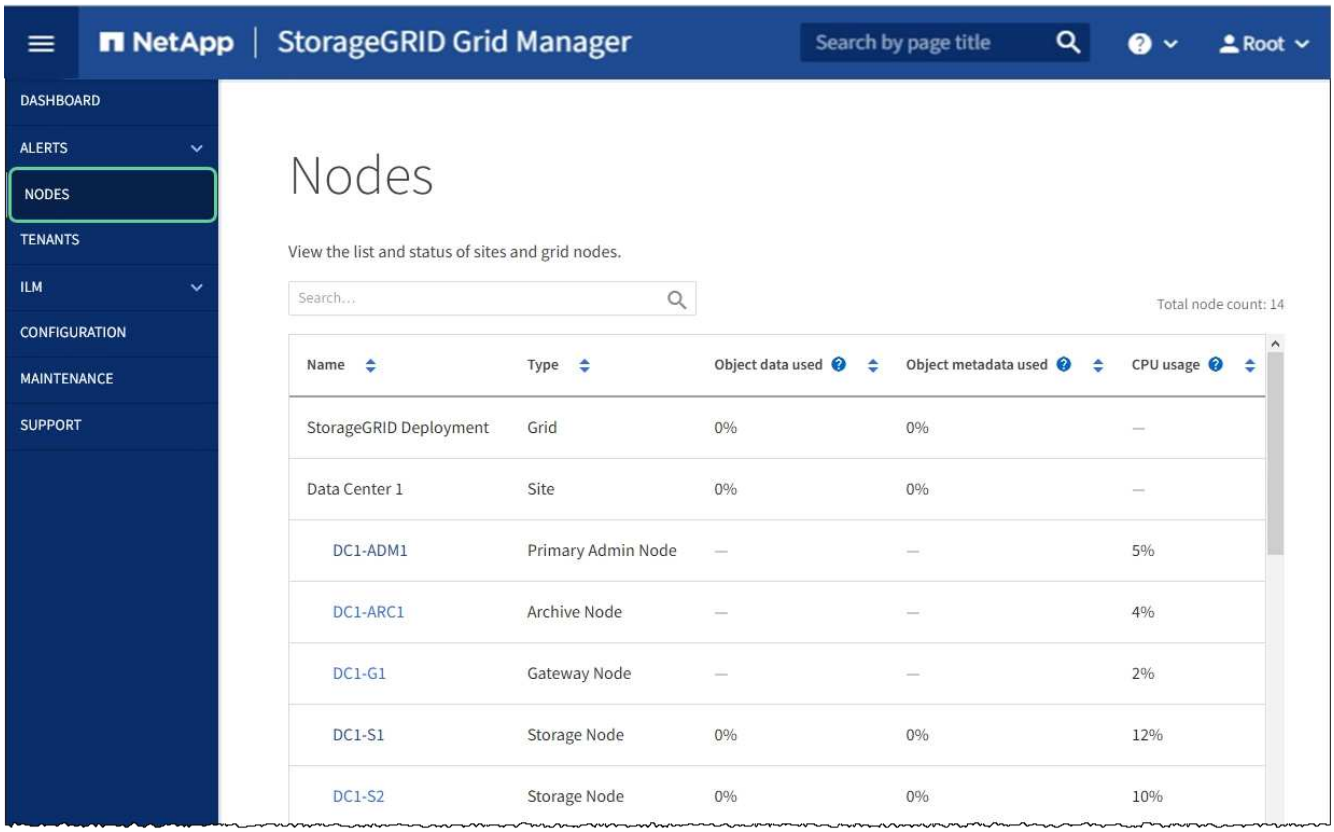
> 清除 KMS 配置将从设备中删除数据，从而使其永远无法访问。此数据不可恢复。

2. 检查完节点加密状态后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果需要在节点重新加入网格之前对其执行其他维护操作，请选择此选项。



   设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

清除密钥管理服务器配置

清除密钥管理服务器（ KMS ）配置将禁用设备上的节点加密。清除 KMS 配置后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

您需要的内容

如果需要保留设备上的数据，则必须先执行节点停用操作步骤 或克隆节点，然后才能清除 KMS 配置。

清除 KMS 后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

停用节点 将其包含的任何数据移动到网格中的其他节点。

关于此任务

清除设备 KMS 配置将禁用节点加密，从而删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。然后，设备上的数据将被删除，并且设备将保持预安装状态。此过程不能逆转。

必须清除 KMS 配置：

- 在将设备安装到不使用 KMS 或使用其他 KMS 的其他 StorageGRID 系统之前，请先安装此设备。

  如果您计划在使用相同 KMS 密钥的 StorageGRID 系统中重新安装设备节点，请勿清除 KMS 配置。

- 在恢复和重新安装 KMS 配置丢失且 KMS 密钥不可恢复的节点之前。
- 在退回您的站点上先前使用的任何设备之前。
- 停用已启用节点加密的设备后。

在清除 KMS 以将其数据移动到 StorageGRID 系统中的其他节点之前，请停用此设备。在停用设备之前清除 KMS 将导致数据丢失，并可能导致设备无法运行。

步骤

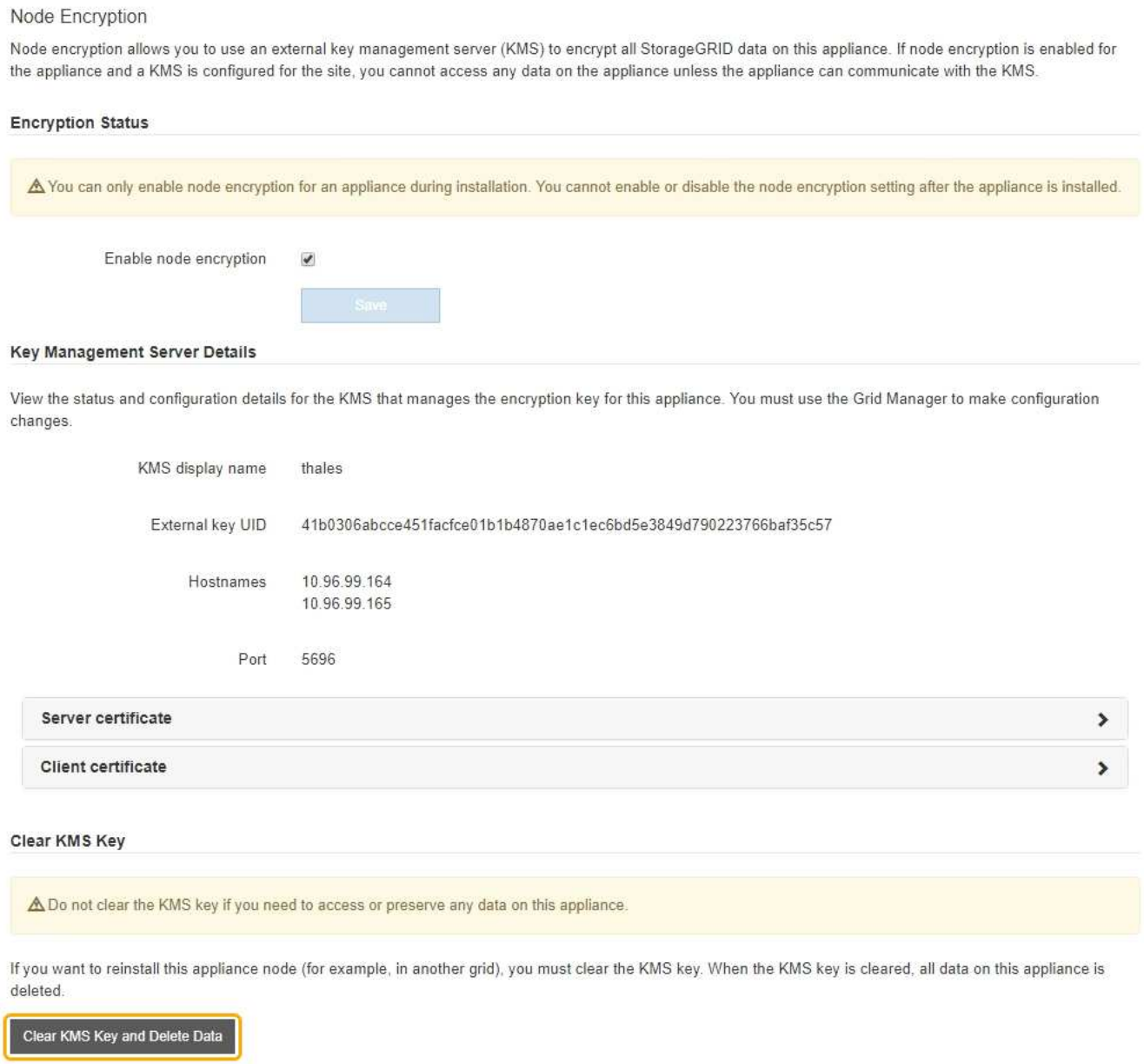
1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

   ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

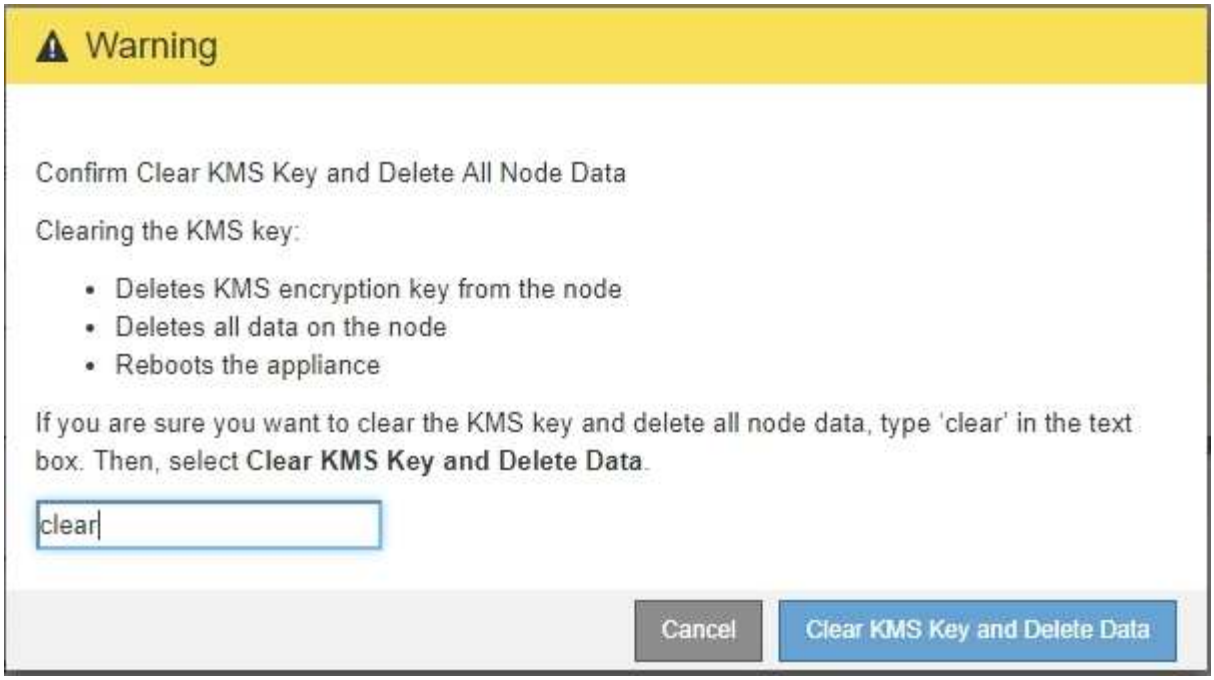
   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 节点加密 * 。



如果清除了 KMS 配置，则设备上的数据将被永久删除。此数据不可恢复。

3. 在窗口底部，选择 * 清除 KMS 密钥和删除数据 * 。
4. 如果确实要清除 KMS 配置，请键入 + ` * clear*` + 并选择 * 清除 KMS 密钥和删除数据 * 。



KMS 加密密钥和所有数据将从节点中删除，设备将重新启动。这可能需要长达 20 分钟。

5. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

6. 选择 * 配置硬件 * > * 节点加密 * 。
7. 验证是否已禁用节点加密，以及是否已从窗口中删除 * 密钥管理服务器详细信息 * 和 * 清除 KMS 密钥和删除数据 * 控件中的密钥和证书信息。

   在将设备重新安装到网格中之前，无法在设备上重新启用节点加密。

完成后

在设备重新启动并确认 KMS 已清除且设备处于预安装状态后，您可以从 StorageGRID 系统中物理删除此设备。请参见 有关准备重新安装设备的说明。

相关信息

管理 StorageGRID

SG6000 存储设备

SG6000 设备：概述

StorageGRID SG6000 设备是一种集成的存储和计算平台，可作为 StorageGRID 系统中的存储节点运行。这些设备可以在混合网格环境中使用，该环境将设备存储节点和虚拟（基于软件的）存储节点结合在一起。

SG6000 设备提供以下功能：

- 提供三种型号：
  - SG6060包含60个驱动器、支持扩展架并使用E2800A控制器。
  - SG6060X包含60个驱动器、支持扩展架并使用E2800B控制器。

    SG6060和SG6060X的规格和功能相同、但互连端口在存储控制器上的位置除外。

  - SGF6024 ，提供 24 个固态驱动器（ SSD ）。
- 集成 StorageGRID 存储节点的存储和计算要素。
- 包括 StorageGRID 设备安装程序，以简化存储节点的部署和配置。
- 包括 SANtricity System Manager ，用于管理和监控存储控制器和驱动器。
- 包括一个基板管理控制器（ BMC ），用于监控和诊断计算控制器中的硬件。
- 最多支持四个连接到 StorageGRID 网格网络和客户端网络的 10-GbE 或 25-GbE 连接。
- 支持联邦信息处理标准（ FIPS ）驱动器。如果将这些驱动器与 SANtricity 系统管理器中的驱动器安全功能结合使用，则会阻止未经授权的数据访问。

SG6060和**SG6060X**设备

StorageGRID SG6060和SG60X设备各包含一个计算控制器和一个存储控制器架、其中包含两个存储控制器和60个驱动器。也可以在这两个设备中添加60个驱动器的扩展架。除了存储控制器上互连端口的位置之外、SG6060和SG6060X之间在规格或功能上没有区别。

SG6060和**SG6060X**组件

SG6060和SG660X设备包括以下组件：

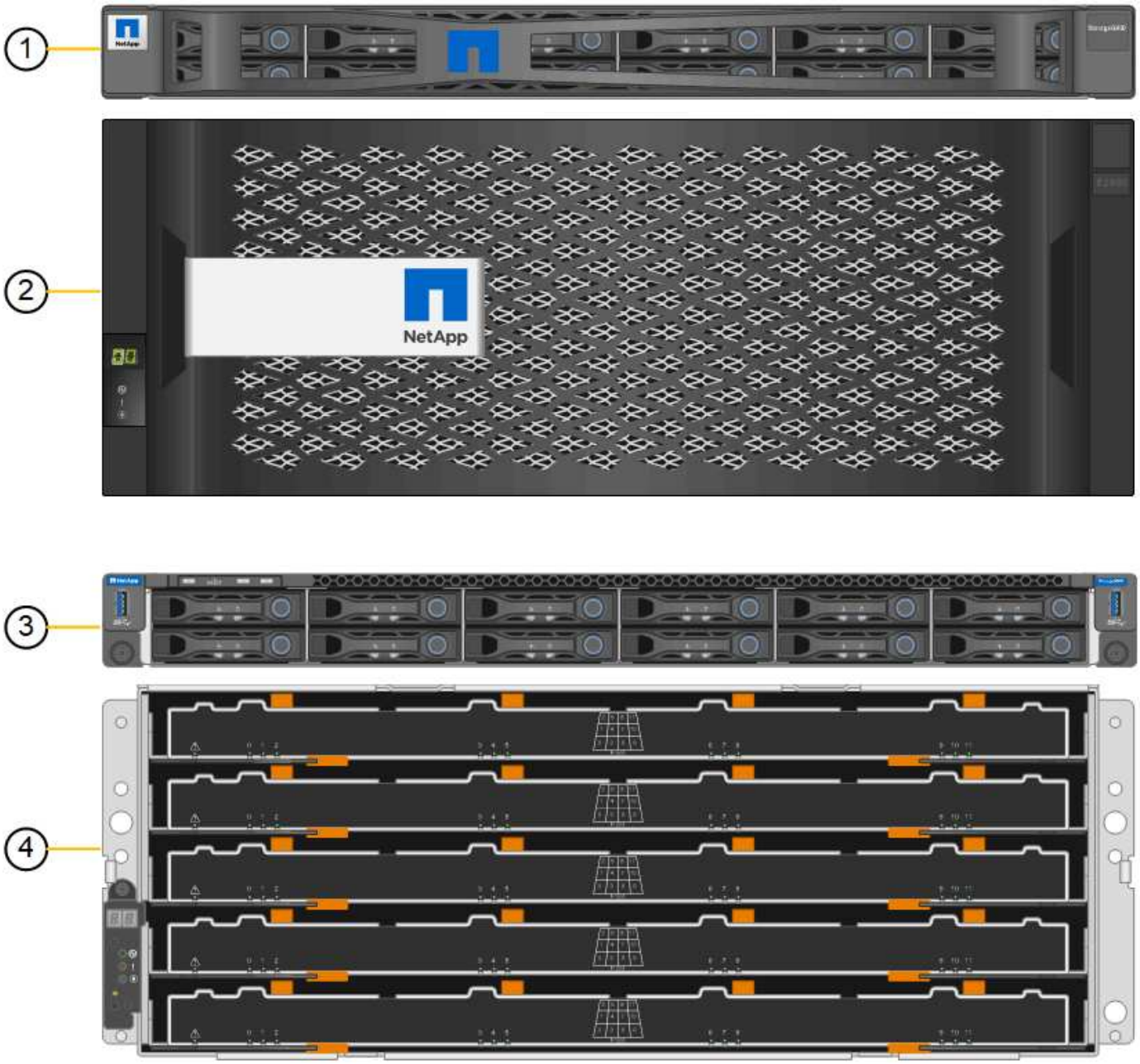
组件	**Description**
计算控制器	SG6000-CN 控制器，一种单机架单元（ 1U ）服务器，其中包括： • 40 个核心（ 80 个线程） • 192 GB RAM • 高达 4 × 25 Gbps 聚合以太网带宽 • 4 × 16 Gbps 光纤通道（ FC ）互连 • 可简化硬件管理的基板管理控制器（ BMC ） • 冗余电源

组件	Description
存储控制器架	E 系列 E2860 控制器架（存储阵列），一个 4U 架，其中包括： • 两个E2800系列控制器(双工配置)、用于提供存储控制器故障转移支持 ◦ SG6060包含E2800A存储控制器 ◦ SG6060X包含E2800B存储控制器 • 五抽屉驱动器架，可容纳 60 个 3.5 英寸驱动器（ 2 个固态驱动器或 SSD 以及 58 个 NL-SAS 驱动器） • 冗余电源和风扇
可选：存储扩展架 • 注： * 扩展架可以在初始部署期间安装，也可以稍后添加。	E 系列 DE460C 机箱，一个 4U 磁盘架，其中包括： • 两个输入 / 输出模块（ IOM ） • 五个抽盒，每个抽盒容纳 12 个 NL-SAS 驱动器，总共 60 个驱动器 • 冗余电源和风扇 每个SG6060和SG60X设备都可以有一个或两个扩展架、总共可容纳180个驱动器。

SG6060和**6060X**示意图

SG6060和SG60X的正面是相同的。下图显示了SG6060的正面、其中包括一个1U计算控制器和一个4U磁盘架、其中包含两个存储控制器和五个驱动器抽盒中的60个驱动器。

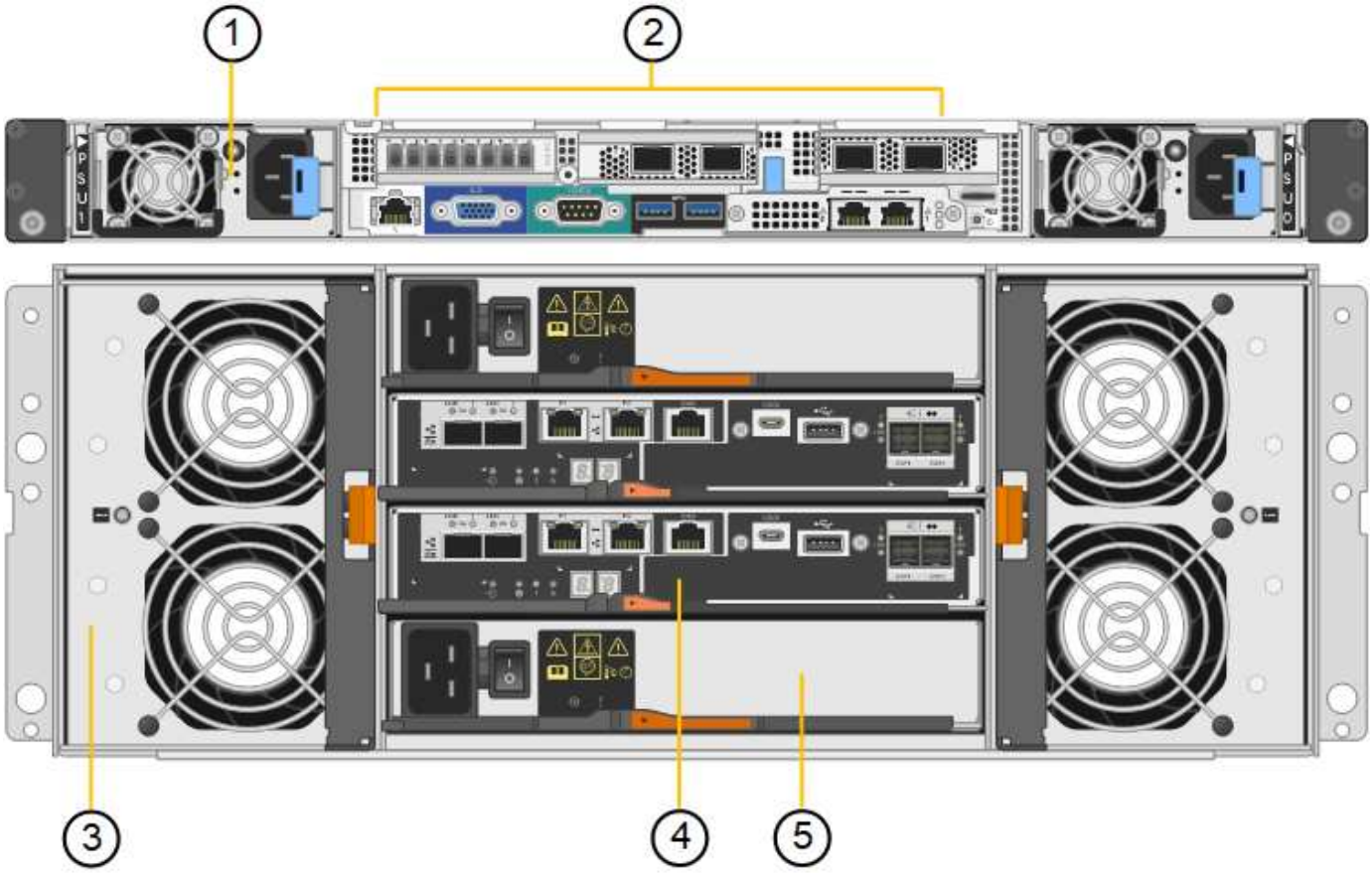
• SG6060正面图*



Callout	Description
1.	带有前挡板的 SG6000-CN 计算控制器
2.	带前挡板的 E2860 控制器架（可选扩展架看起来相同）
3.	SG6000-CN 计算控制器，已卸下前挡板
4.	已卸下前挡板的 E2860 控制器架（可选扩展架看起来相同）

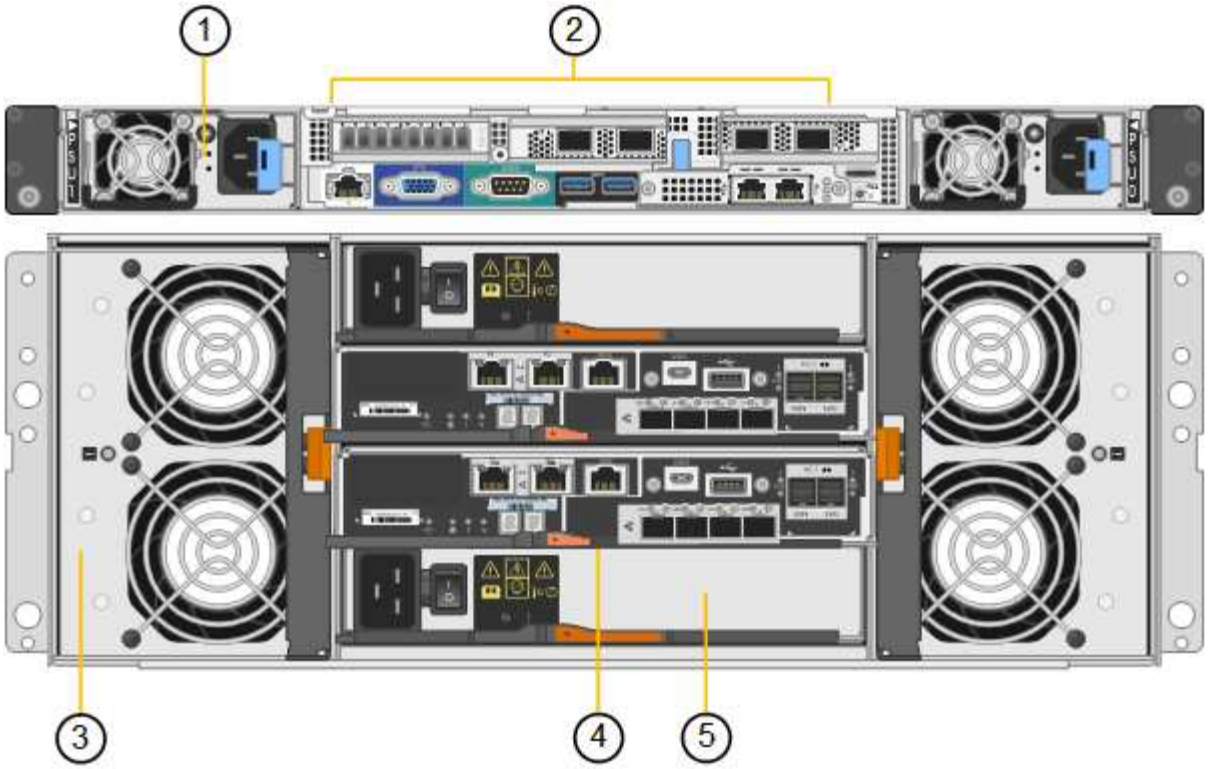
下图显示了SG6060和SG6060X的背面、包括计算和存储控制器、风扇和电源。

- SG6060背面图*



Callout	Description
1.	SG6000-CN 计算控制器的电源（第 1 页，共 2 页）
2.	用于 SG6000-CN 计算控制器的连接器
3.	E2860 控制器架的风扇（图 1 ）
4.	E系列E2800A存储控制器(图1)和连接器
5.	E2860 控制器架的电源（图 1 ）

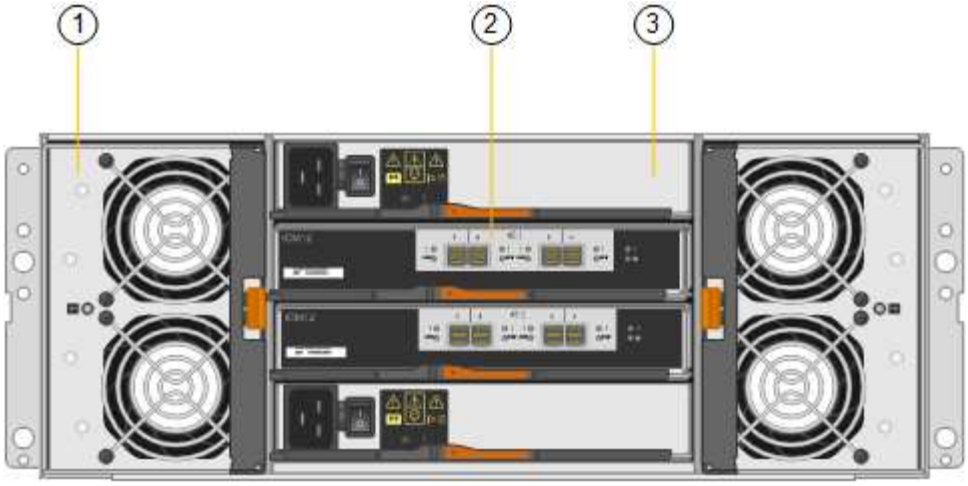
- SG6060X背面图*



Callout	Description
1.	SG6000-CN 计算控制器的电源（第 1 页，共 2 页）
2.	用于 SG6000-CN 计算控制器的连接器
3.	E2860 控制器架的风扇（图 1 ）
4.	E系列E2800B存储控制器(图1)和连接器
5.	E2860 控制器架的电源（图 1 ）

- SG6060和SG60X扩展架*

此图显示了SG6060和SG6060X的可选扩展架的背面、包括输入/输出模块(IOM)、风扇和电源。每个SG6060和SG6060X都可以安装一个或两个扩展架、这些扩展架可以包含在初始安装中、也可以稍后添加。



Callout	Description
1.	扩展架的风扇（第 1 张，共 2 张）
2.	扩展架的 IOM （第 1 张，共 2 张）
3.	扩展架的电源（图 1 ）

SGF6024 概述

StorageGRIDSGF6024 包括一个计算控制器和一个存储控制器架，可容纳 24 个固态驱动器。

SGF6024 组件

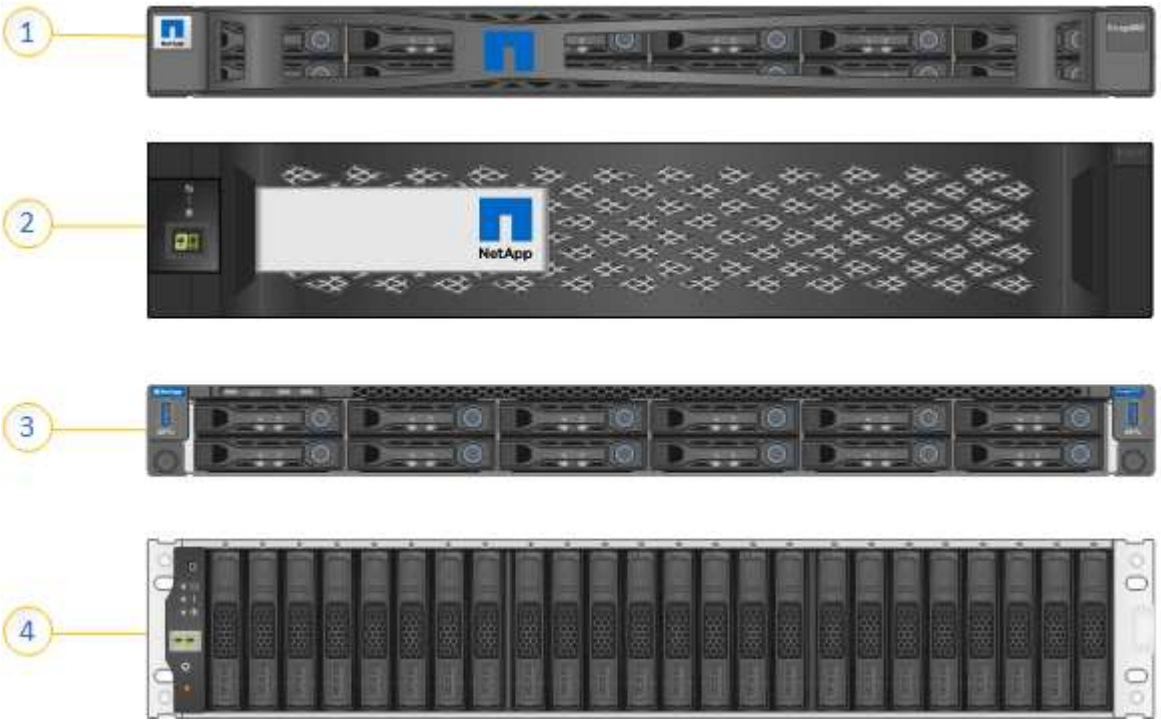
SGF6024 设备包括以下组件：

组件	Description
计算控制器	SG6000-CN 控制器，一种单机架单元（ 1U ）服务器，其中包括： • 40 个核心（ 80 个线程） • 192 GB RAM • 高达 4 × 25 Gbps 聚合以太网带宽 • 4 × 16 Gbps 光纤通道（ FC ）互连 • 可简化硬件管理的基板管理控制器（ BMC ） • 冗余电源

组件	Description
闪存阵列（控制器架）	E 系列 EF570 闪存阵列（也称为控制器架），一个 2U 磁盘架，其中包括： • 两个 E 系列 EF570 控制器（双工配置），用于提供存储控制器故障转移支持 • 24 个固态驱动器（也称为 SSD 或闪存驱动器） • 冗余电源和风扇

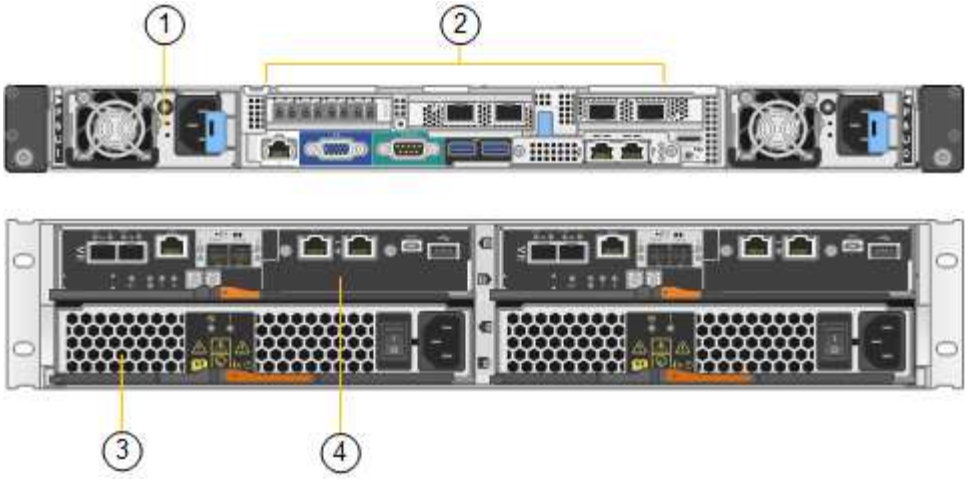
SGF6024 图表

此图显示了 SGF6024 的正面，其中包括一个 1U 计算控制器和一个 2U 机箱，其中包含两个存储控制器和 24 个闪存驱动器。



Callout	Description
1.	带有前挡板的 SG6000-CN 计算控制器
2.	EF570 闪存阵列，带前挡板
3.	SG6000-CN 计算控制器，已卸下前挡板
4.	已卸下前挡板的 EF570 闪存阵列

此图显示了 SGF6024 的背面，包括计算和存储控制器，风扇和电源。



Callout	Description
1.	SG6000-CN 计算控制器的电源（第 1 页，共 2 页）
2.	用于 SG6000-CN 计算控制器的连接器
3.	EF570 闪存阵列的电源（第 1 页，共 2 页）
4.	E 系列 EF570 存储控制器（图 1 ）和连接器

SG6000 设备中的控制器

每个型号的 StorageGRID SG6000 设备都在 1U 机箱中包含一个 SG6000-CN 计算控制器，并在 2U 或 4U 机箱中包含双工 E 系列存储控制器，具体取决于型号。查看图表，了解有关每种控制器类型的更多信息。

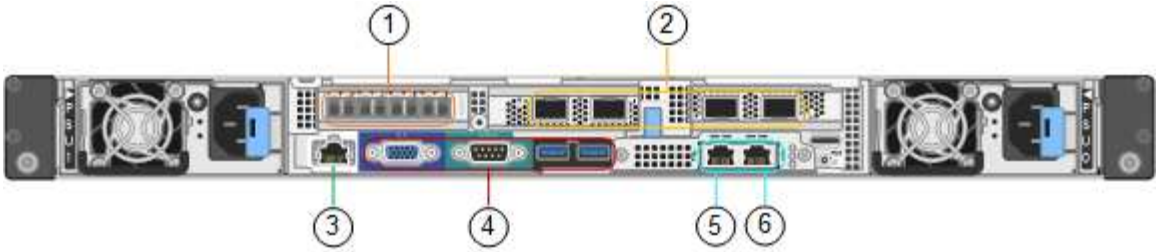
所有设备： **SG6000-CN** 计算控制器

- 为设备提供计算资源。
- 包括 StorageGRID 设备安装程序。

> 设备上未预安装 StorageGRID 软件。部署设备时，系统会从管理节点检索此软件。

- 可以连接到所有三个 StorageGRID 网络，包括网格网络，管理网络和客户端网络。
- 连接到 E 系列存储控制器并作为启动程序运行。

此图显示了 SG6000-CN 背面的连接器。



	Port	Type	使用 …
1.	互连端口 1-4	16 Gb/ 秒光纤通道（ FC ），具有集成光纤	将 SG6000-CN 控制器连接到 E2800 控制器（每个 E2800 有两个连接）。
2.	网络端口 1-4	10-GbE 或 25-GbE ，取决于缆线或 SFP 收发器类型，交换机速度和已配置的链路速度	连接到网格网络和 StorageGRID 客户端网络。
3.	BMC 管理端口	1-GbE （ RJ-45 ）	连接到 SG6000-CN 基板管理控制器。
4.	诊断和支持端口	• VGA • 串行， 115200 8-N-1 • USB	保留供技术支持使用。
5.	管理网络端口 1	1-GbE （ RJ-45 ）	将 SG6000-CN 连接到 StorageGRID 管理网络。
6.	管理网络端口 2	1-GbE （ RJ-45 ）	选项： • 与管理端口 1 绑定，以便与 StorageGRID 的管理网络建立冗余连接。 • 保持未连接状态，并可用于临时本地访问（ IP 169.254.0.1 ）。 • 安装期间，如果 DHCP 分配的 IP 地址不可用，请使用端口 2 进行 IP 配置。

SG6060和**SG6060X**：**E2800**系列存储控制器

- 两个控制器，用于提供故障转移支持。

- 管理驱动器上的数据存储。
- 在双工配置中用作标准 E 系列控制器。
- 包括 SANtricity 操作系统软件（控制器固件）。
- 包括用于监控存储硬件和管理警报的 SANtricity System Manager ， AutoSupport 功能和驱动器安全功能。
- 连接到 SG6000-CN 控制器并提供对存储的访问权限。

SG6060和SG6060X使用E2800系列存储控制器。

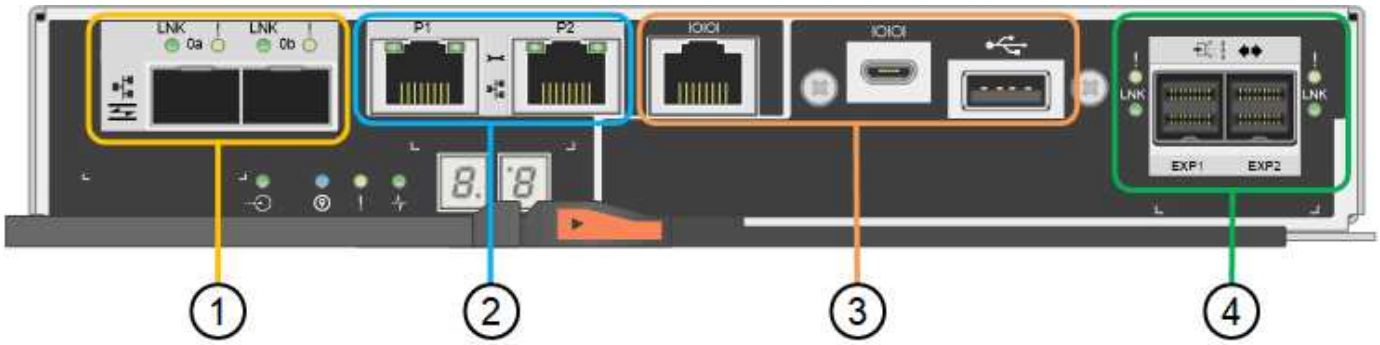
设备	控制器
SG6060	两个E2800A存储控制器
SG6060X	两个E2800B存储控制器

E2800A没有HIC、E2800B有四端口HIC。E2800A和E2800B存储控制器的规格和功能相同、但互连端口的位置除外。

请勿在同一设备中使用E2800A和E2800B。

下图显示了每个E2800系列控制器背面的连接器。

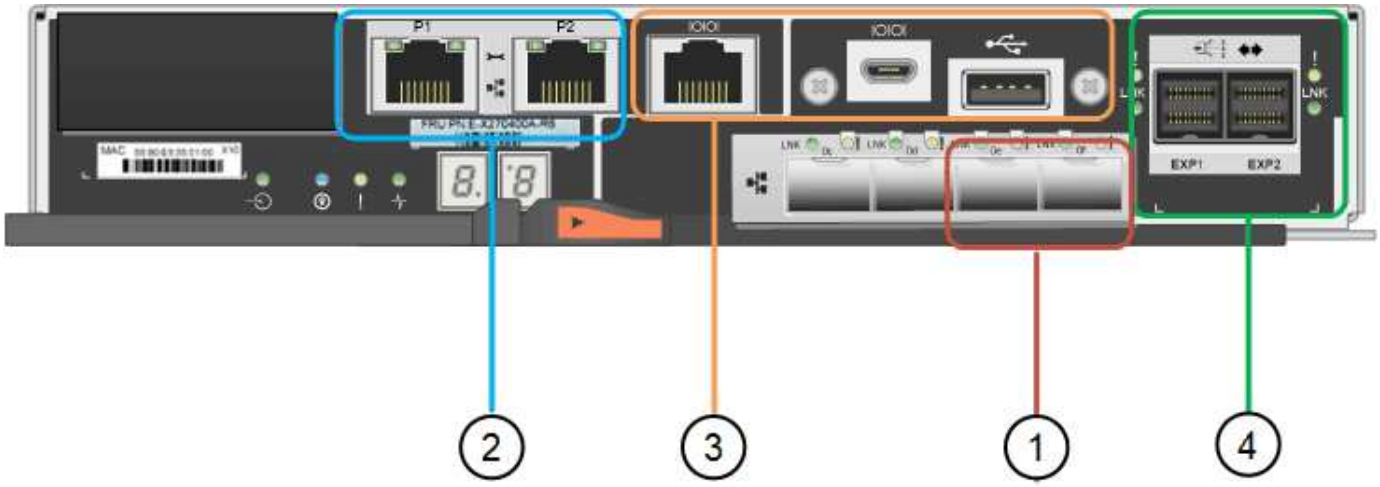
- E2800A存储控制器*



	Port	Type	使用 …
1.	互连端口 1 和 2	16 Gb/ 秒 FC 光纤 SFPa	将每个E2800A控制器连接到SG6000-CN控制器。SG6000-CN控制器有四个连接(每个E2800A两个)。

	Port	Type	使用 ...
2.	管理端口 1 和 2	1 Gb （ RJ-45 ） 以太网	• 端口 1 选项： ◦ 连接到管理网络以启用对 SANtricity 系统管理器的直接 TCP/IP 访问 ◦ 保持未连接状态以保存交换机端口和 IP 地址。使用网格管理器或存储网格设备安装程序 UI 访问 SANtricity System Manager 。 • 注 * ： 如果您选择使端口 1 保持未连接状态，则某些可选的 SANtricity 功能（例如 NTP 同步以获得准确的日志时间戳）将不可用。 • 注 * ： 如果不对端口 1 布线，则需要 StorageGRID 11.5 或更高版本以及 SANtricity 11.70 或更高版本。 • 端口 2 预留用于技术支持。
3.	诊断和支持端口	• RJ-45 串行端口 • 微型 USB 串行端口 • USB 端口	保留供技术支持使用。
4.	驱动器扩展端口 1 和 2	12 Gb/ 秒 SAS	将端口连接到扩展架中 IOM 上的驱动器扩展端口。

• E2800B存储控制器*



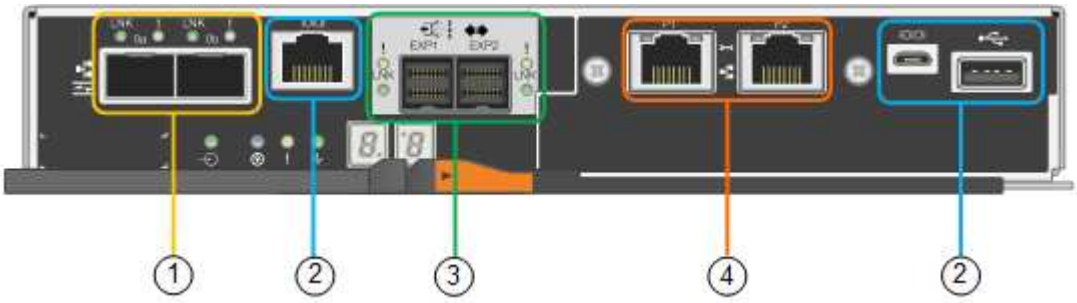
	Port	Type	使用 ...
1.	互连端口 1 和 2	16 Gb/ 秒 FC 光纤 SFPa	将每个E2800B控制器连接到SG6000-CN控制器。SG6000-CN控制器有四个连接(每个E2800B两个)。
2.	管理端口 1 和 2	1 Gb （ RJ-45 ）以太网	• 端口 1 选项： ◦ 连接到管理网络以启用对 SANtricity 系统管理器的直接 TCP/IP 访问 ◦ 保持未连接状态以保存交换机端口和 IP 地址。使用网格管理器或存储网格设备安装程序 UI 访问 SANtricity System Manager 。 • 注 * ： 如果您选择使端口 1 保持未连接状态，则某些可选的 SANtricity 功能（例如 NTP 同步以获得准确的日志时间戳）将不可用。 • 注 * ： 如果不对端口 1 布线，则需要 StorageGRID 11.5 或更高版本以及 SANtricity 11.70 或更高版本。 • 端口 2 预留用于技术支持。

	Port	Type	使用 ...
3.	诊断和支持端口	• RJ-45 串行端口 • 微型 USB 串行端口 • USB 端口	保留供技术支持使用。
4.	驱动器扩展端口 1 和 2	12 Gb/ 秒 SAS	将端口连接到扩展架中 IOM 上的驱动器扩展端口。

SGF6024： EF570 存储控制器

- 两个控制器，用于提供故障转移支持。
- 管理驱动器上的数据存储。
- 在双工配置中用作标准 E 系列控制器。
- 包括 SANtricity 操作系统软件（控制器固件）。
- 包括用于监控存储硬件和管理警报的 SANtricity System Manager ， AutoSupport 功能和驱动器安全功能。
- 连接到 SG6000-CN 控制器并提供对闪存存储的访问权限。

此图显示了每个 EF570 控制器背面的连接器。

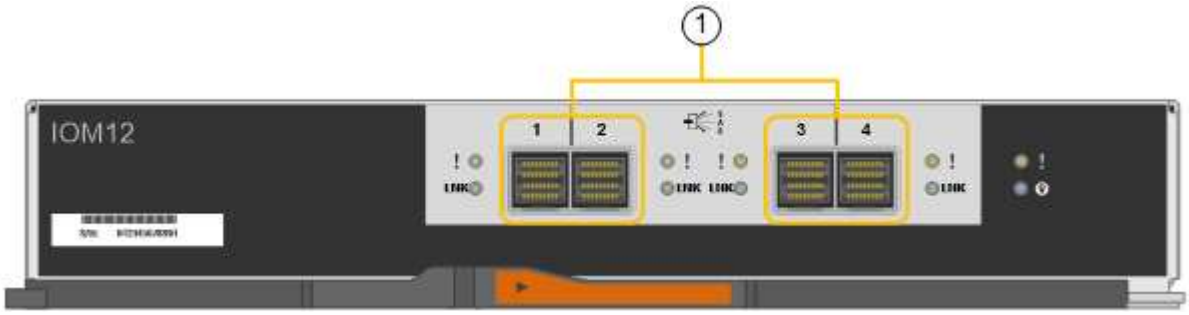


	Port	Type	使用 ...
1.	互连端口 1 和 2	16 Gb/ 秒 FC 光纤 SFPa	将每个 EF570 控制器连接到 SG6000-CN 控制器。SG6000-CN 控制器有四个连接（每个 EF570 有两个连接）。
2.	诊断和支持端口	• RJ-45 串行端口 • 微型 USB 串行端口 • USB 端口	保留供技术支持使用。
3.	驱动器扩展端口	12 Gb/ 秒 SAS	未使用。SGF6024 设备不支持扩展驱动器架。

	Port	Type	使用 ...
4.	管理端口 1 和 2	1 Gb （ RJ-45 ） 以太网	• 端口 1 连接到通过浏览器访问 SANtricity 系统管理器的网络。 • 端口 2 预留用于技术支持。

SG6060和**SG6060X**：用于可选扩展架的输入/输出模块

扩展架包含两个输入 / 输出模块（ IOM ），这些模块连接到存储控制器或其他扩展架。



	Port	Type	使用 ...
1.	驱动器扩展端口 1-4	12 Gb/ 秒 SAS	将每个端口连接到存储控制器或其他扩展架（如果有）。

安装和部署概述

您可以在首次部署 StorageGRID 时安装一个或多个 StorageGRID 存储设备，也可以稍后在扩展过程中添加设备存储节点。在恢复操作中，您可能还需要安装设备存储节点。

您需要的内容

您的 StorageGRID 系统正在使用所需版本的 StorageGRID 软件。

设备	所需的 **StorageGRID** 版本
SG6060和SG60X、无扩展架	11.1.1 或更高版本
带有扩展架(一个或两个)的SG6060和SG60X	11.3 或更高版本 • 注意： * 如果在初始部署后添加扩展架，则必须使用 11.4 或更高版本。
SGF6024	11.3 或更高版本

安装和部署任务

将 StorageGRID 存储设备添加到 StorageGRID 系统包括四个主要步骤：

1. 准备安装：
   - 正在准备安装站点
   - 打开包装箱的包装并检查包装箱中的物品
   - 获取其他设备和工具
   - 收集 IP 地址和网络信息
   - 可选：如果您计划对所有设备数据进行加密，请配置外部密钥管理服务器（ KMS ）。有关外部密钥管理的详细信息，请参见 StorageGRID 管理说明。
2. 安装硬件：
   - 注册硬件
   - 将设备安装到机柜或机架中
   - 安装驱动器
   - 安装可选扩展架(仅限SG6060和SG6060X型号；最多两个扩展架)
   - 为设备布线
   - 连接电源线并接通电源
   - 查看启动状态代码
3. 配置硬件：
   - 访问 SANtricity 系统管理器以配置 SANtricity 系统管理器设置
   - 访问 StorageGRID 设备安装程序，为存储控制器上的管理端口 1 设置静态 IP 地址，以及配置连接到 StorageGRID 网络所需的链路和网络 IP 设置
   - 访问 SG6000-CN 控制器上的基板管理控制器（ BMC ）接口
   - 可选：如果您计划使用外部 KMS 对设备数据进行加密，请启用节点加密。
   - 可选：更改 RAID 模式。
4. 将设备部署为存储节点：

任务	说明
在新的 StorageGRID 系统中部署设备存储节点	部署设备存储节点
将设备存储节点添加到现有 StorageGRID 系统	有关扩展 StorageGRID 系统的说明
在存储节点恢复操作中部署设备存储节点	恢复和维护说明

相关信息

准备安装（ SG6000 ）

安装硬件（ SG6000 ）

配置硬件（ SG6000 ）

扩展网格

恢复和维护

管理 StorageGRID

准备安装（ **SG6000** ）

准备安装 StorageGRID 设备需要准备站点并获取所有必需的硬件，缆线和工具。您还应收集 IP 地址和网络信息。

相关信息

Web 浏览器要求

准备站点（ **SG6000** ）

在安装设备之前，您必须确保要使用的站点和机柜或机架符合 StorageGRID 设备的规格。

步骤

1. 确认站点满足温度，湿度，海拔范围，气流，散热， 布线，电源和接地。有关详细信息，请参见 NetApp Hardware Universe 。
2. 确认您所在位置为 SG6060 提供 240 伏交流电源，为 SGF6024 提供 120 伏交流电源。
3. 获取一个 19 英寸（ 48.3 厘米）的机柜或机架，以适合此大小的磁盘架（不带缆线）：

磁盘架类型	高度	宽度	深度	最大重量
• 用于 SG6060 的 E2860 控制器架 *	6.87 英寸（ 17.46 厘米）	17.66 英寸（ 44.86 厘米）	38.25 英寸（ 97.16 厘米）	250 磅（ 113 千克）
• 用于 SG6060 （一个或两个）的可选扩展架 *	6.87 英寸（ 17.46 厘米）	17.66 英寸（ 44.86 厘米）	38.25 英寸（ 97.16 厘米）	250 磅（ 113 千克）
用于 SGF6024 的 * EF570 控制器架 *	3.35 英寸（ 8.50 厘米）	17.66 英寸（ 44.86 厘米）	19.00 英寸（ 48.26 厘米）	51.74 磅（ 23.47 千克）
每个设备的 * SG6000-CN 控制器 *	1.70 英寸（ 4.32 厘米）	17.32 英寸（ 44.0 厘米）	32.0 英寸（ 81.3 厘米）	39 磅（ 17.7 千克）

4. 确定要在何处安装设备。

安装 E2860 控制器架或可选扩展架时，请从机架或机柜的底部到顶部安装硬件，以防止设备发生倾翻。要确保最重的设备位于机柜或机架的底部，请在 E2860 控制器架和扩展架上方安装 SG6000-CN 控制器。

在提交安装之前，请确认设备随附的 0.5 米光缆或您提供的缆线长度足以满足计划的布局要求。

相关信息

"NetApp Hardware Universe"

"NetApp 互操作性表工具"

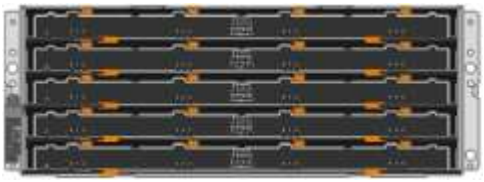
打开包装箱（ **SG6000** ）

安装 StorageGRID 设备之前，请打开所有包装箱的包装，并将包装箱上的物品与包装清单上的物品进行比较。

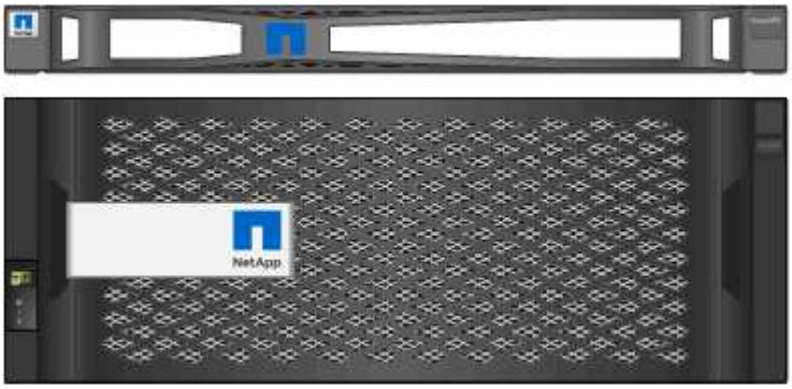
SG6060和SG6060X

- * SG6000-CN 控制器 *

- * 未安装驱动器的 E2860 控制器架 *

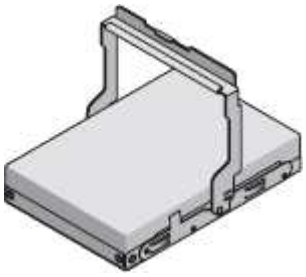


- * 两个前挡板 *

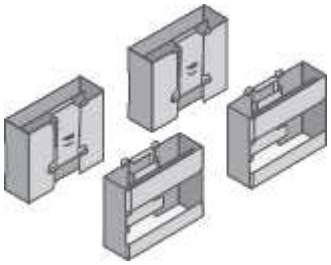


- * 两个导轨套件，含说明 *

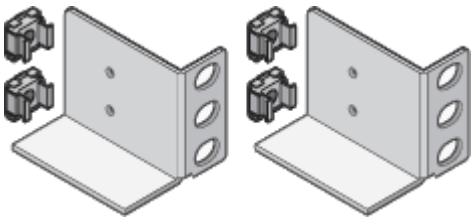
- * 60 个驱动器（ 2 个 SSD 和 58 个 NL-SAS ） *



- * 四个句柄 *

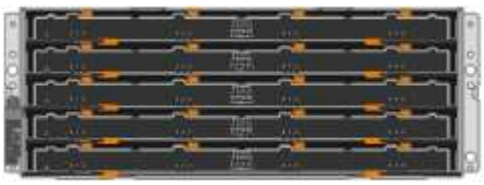


- * 用于方孔机架安装的背面支架和固定框架螺母 *



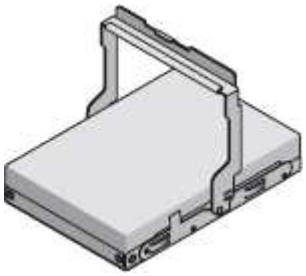
SG6060和**SG6060X**扩展架

- * 未安装驱动器的扩展架 *



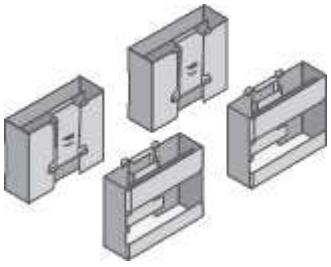
- * 前挡板 *

- * 60 个 NL-SAS 驱动器 *

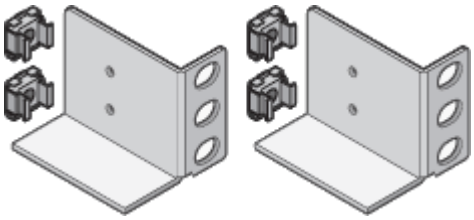


- * 一个导轨套件，含说明 *

- * 四个句柄 *



- * 用于方孔机架安装的背面支架和固定框架螺母 *



SGF6024

- * SG6000-CN 控制器 *

- * 已安装 24 个固态（闪存）驱动器的 EF570 闪存阵列 *

- * 两个前挡板 *

- * 两个导轨套件，含说明 *

- * 磁盘架端盖 *

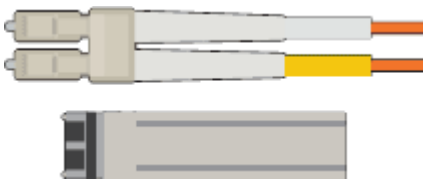
缆线和连接器

StorageGRID 设备的发货包括以下缆线和连接器：

- * 您所在国家或地区的四根电源线 *

  您的机柜可能使用专用电源线，而不是设备随附的电源线。

- * 光缆和 SFP 收发器 *



  用于 FC 互连端口的四根光缆

  四个 SFP+ 收发器，支持 16 Gb/ 秒 FC

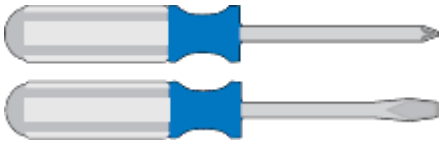
- 可选：两根**SAS**缆线用于连接每个**SG6060**或**SG60X**扩展架

获取其他设备和工具（ **SG6000** ）

在安装 StorageGRID 设备之前，请确认您拥有所需的所有附加设备和工具。

要安装和配置硬件，您需要使用以下附加设备：

- * 螺丝刀 *

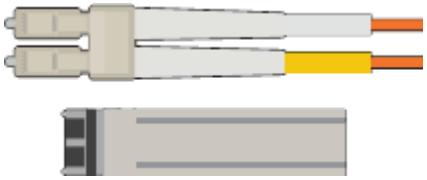


十字线编号2 把螺丝刀

中型平口螺丝刀

- * ESD 腕带 *

- * 光缆和 SFP 收发器 *



您需要以下选项之一：

  - 一到四根双轴缆线或光缆，用于您计划在 SG6000-CN 控制器上使用的 10/225-GbE 端口
  - 如果要使用光缆和 10-GbE 链路速度，则为 10/225-GbE 端口提供一到四个 SFP+ 收发器
  - 如果要使用光缆和 25 GbE 链路速度，则为 10/225-GbE 端口提供一到四个 SFP28 收发器

- * RJ-45 （ Cat5/Cat5e/Cat6 ）以太网缆线 *

- * 服务笔记本电脑 *

支持的 Web 浏览器

1 GbE （ RJ-45 ）端口

- * 可选工具 *

带十字头的电钻

Flashlight

适用于 60 个驱动器磁盘架的机械升降机

查看设备网络连接（ **SG6000** ）

在安装 StorageGRID 设备之前，您应了解可以将哪些网络连接到此设备。

在 StorageGRID 系统中将 StorageGRID 设备部署为存储节点时，您可以将其连接到以下网络：

- * 适用于 StorageGRID 的网格网络 * ： 网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。网格网络为必填项。
- * 适用于 StorageGRID 的管理网络 * ： 管理网络是一个用于系统管理和维护的封闭网络。管理网络通常是一个专用网络，不需要在站点之间进行路由。管理网络是可选的。
- * 适用于 StorageGRID 的客户端网络： * 客户端网络是一种开放网络，用于访问包括 S3 和 Swift 在内的客户端应用程序。客户端网络可提供对网格的客户端协议访问，从而可以隔离和保护网格网络。客户端网络是可选的。
- * 适用于 SANtricity System Manager* 的管理网络（可选）： 通过此网络，您可以访问存储控制器上的 SANtricity System Manager ，从而监控和管理存储控制器架中的硬件组件。此管理网络可以与 StorageGRID 的管理网络相同，也可以是一个独立的管理网络。

如果未连接可选的 SANtricity System Manager 网络，则可能无法使用某些 SANtricity 功能。

- SG6000-CN 控制器的 * BMC 管理网络 * （可选）：通过此网络可以访问 SG6000-CN 中的基板管理控制器，从而可以监控和管理 SG6000-CN 控制器中的硬件组件。此管理网络可以与 StorageGRID 的管理网络相同，也可以是一个独立的管理网络。

  如果未连接可选的 BMC 管理网络，则某些支持和维护过程将更难执行。除非出于支持目的需要，否则您可以使 BMC 管理网络保持未连接状态。

有关 StorageGRID 网络的详细信息，请参见 *Grid Primer* 。

相关信息

收集安装信息（ SG6000 ）

缆线设备（ SG6000 ）

SG6000-CN 控制器的端口绑定模式

网络准则

SG6000-CN 控制器的端口绑定模式

在为 SG6000-CN 配置网络链路时，您可以对连接到网格网络和可选客户端网络的 10/25GbE 端口以及连接到可选管理网络的 1-GbE 管理端口使用端口绑定。端口绑定可在 StorageGRID 网络和设备之间提供冗余路径，从而有助于保护数据。

相关信息

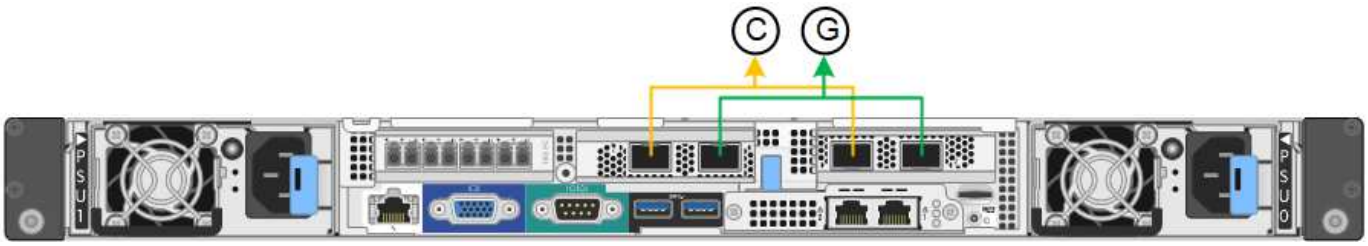
配置网络链路（ SG6000 ）

10/225-GbE 端口的网络绑定模式

SG6000-CN 控制器上的 10/225-GbE 网络端口支持网格网络和客户端网络连接的固定端口绑定模式或聚合端口绑定模式。

固定端口绑定模式

固定模式是 10/225-GbE 网络端口的默认配置。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

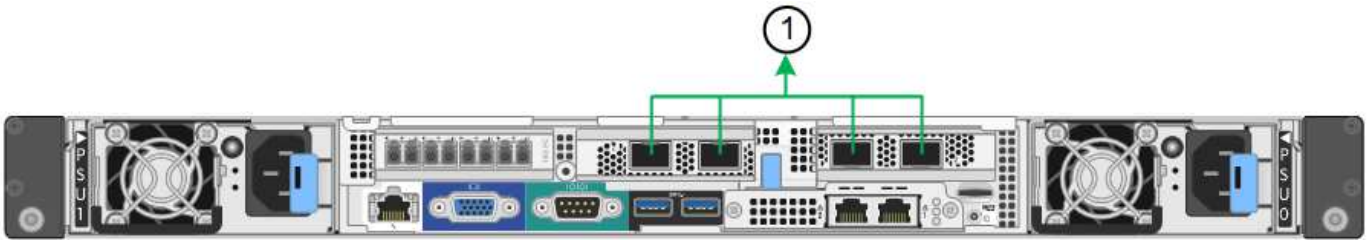
使用固定端口绑定模式时，可以使用主动备份模式或链路聚合控制协议模式（ LACP 802.3ad ）绑定端口。

- 在主动备份模式（默认）下，一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。端口 4 为端口 2 （网格网络）提供备份路径，端口 3 为端口 1 （客户端网络）提供备份路径。
- 在 LACP 模式下，每对端口在控制器和网络之间形成一个逻辑通道，从而提高吞吐量。如果一个端口发生故障，另一个端口将继续提供通道。吞吐量会降低，但连接不会受到影响。

> 如果不需要冗余连接，则每个网络只能使用一个端口。但是，请注意，安装 StorageGRID 后，网格管理器中将触发警报，指示链路已关闭。由于此端口会有目的断开连接，因此您可以安全地禁用此警报。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。

聚合端口绑定模式

聚合端口绑定模式可显著提高每个 StorageGRID 网络的吞吐量，并提供额外的故障转移路径。



Callout	哪些端口已绑定
1.	所有连接的端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

如果您计划使用聚合端口绑定模式：

- 您必须使用 LACP 网络绑定模式。
- 您必须为每个网络指定唯一的 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。
- 这些端口必须连接到可支持 VLAN 和 LACP 的交换机。如果多个交换机参与 LACP 绑定，则这些交换机必须支持多机箱链路聚合组（ MLAG ）或等效项。
- 您必须了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。

如果您不想使用全部四个 10/225-GbE 端口，则可以使用一个，两个或三个端口。如果使用多个端口，则在一个 10/225-GbE 端口出现故障时，某些网络连接将保持可用的可能性最大。

如果您选择使用的端口少于四个、请注意、在安装设备节点后、可能会在网格管理器中触发*服务设备链路已关闭*警报、指示已拔下电缆。您可以安全地为触发的警报禁用此警报规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。

1-GbE 管理端口的网络绑定模式

对于 SG6000-CN 控制器上的两个 1-GbE 管理端口，您可以选择独立网络绑定模式或主动备份网络绑定模式来连接到可选的管理网络。

在独立模式下，只有左侧的管理端口连接到管理网络。此模式不提供冗余路径。右侧的管理端口未连接，可用于临时本地连接（使用 IP 地址 169.254.0.1 ）

在主动备份模式下，两个管理端口均连接到管理网络。一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。将这两个物理端口绑定到一个逻辑管理端口可提供指向管理网络的冗余路径。

如果在将 1-GbE 管理端口配置为主动备份模式后需要临时本地连接到 SG6000-CN 控制器，请从两个管理端口拔下缆线，将临时缆线插入右侧的管理端口，然后使用 IP 地址 169.254.0.1 访问此设备。

Callout	网络绑定模式
答	这两个管理端口都绑定到一个连接到管理网络的逻辑管理端口。
I	左侧端口连接到管理网络。右侧端口可用于临时本地连接（ IP 地址 169.254.0.1 ）。

收集安装信息（ **SG6000** ）

在安装和配置 StorageGRID 设备时，您必须做出决策并收集有关以太网交换机端口， IP 地址以及端口和网络绑定模式的信息。

关于此任务

您可以使用下表记录连接到设备的每个网络的所需信息。安装和配置硬件需要这些值。

连接到存储控制器上的 **SANtricity System Manager** 所需的信息

您必须将设备中的两个存储控制器(E2800系列控制器或EF570控制器)连接到要用于SANtricity System Manager的管理网络。控制器位于每个设备中，如下所示：

- SG6060和SG6060X：控制器A位于顶部、控制器B位于底部。
- SGF6024 ： 控制器 A 位于左侧，控制器 B 位于右侧。

所需信息	控制器 **A** 的值	控制器 **B** 的值
要连接到管理端口1的以太网交换机端口(在E2800A控制器上标记为P1、在E2800B控制器上标记为0a)		
管理端口1的MAC地址(印在E2800A控制器上端口P1附近的标签上、E2800B控制器上的端口0a上)		
DHCP 为管理端口 1 分配的 IP 地址（如果在启动后可用） • 注： * 如果要连接到存储控制器的网络包含 DHCP 服务器，则网络管理员可以使用 MAC 地址确定 DHCP 服务器分配的 IP 地址。		
您计划在管理网络上用于设备的静态 IP 地址	对于 IPv4 ： • IPv4 地址： • 子网掩码： • 网关 对于 IPv6 ： • IPv6 地址： • 可路由的 IP 地址： • 存储控制器路由器 IP 地址：	对于 IPv4 ： • IPv4 地址： • 子网掩码： • 网关 对于 IPv6 ： • IPv6 地址： • 可路由的 IP 地址： • 存储控制器路由器 IP 地址：
IP 地址格式	选择一项： • IPv4 • IPv6	选择一项： • IPv4 • IPv6
速度和双工模式 • 注： * 您必须确保 SANtricity System Manager 管理网络的以太网交换机设置为自动协商。	必须为： • 自动协商（默认）	必须为： • 自动协商（默认）

StorageGRID 管理网络是一个可选网络，用于系统管理和维护。此设备使用 SG6000-CN 控制器上的以下 1-GbE 管理端口连接到管理网络。

所需信息	您的价值
已启用管理网络	选择一项： • 否 • 是（默认）
网络绑定模式	选择一项： • 独立（默认） • 主动备份
图中红色圆圈中左侧端口的交换机端口（独立网络绑定模式的默认活动端口）	
图中红色圆圈中右侧端口的交换机端口（仅限主动备份网络绑定模式）	
管理网络端口的 MAC 地址 • 注： * SG6000-CN 控制器正面的 MAC 地址标签列出了 BMC 管理端口的 MAC 地址。要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 * 。 2 例如，如果标签上的 **MAC** 地址以 ***09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 * （ *y* ） FF* 结尾，则管理端口的 MAC 地址将以 * （ *y*+1 ） 01* 结尾。您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 * + 2 =* 来轻松进行计算。	
DHCP 为管理网络端口分配的 IP 地址（如果在启动后可用） • 注： * 您可以使用 MAC 地址查找已分配的 IP 来确定 DHCP 分配的 IP 地址。	• IPv4 地址（ CIDR ）： • 网关

所需信息	您的价值
您计划在管理网络上用于设备存储节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
管理网络子网（ CIDR ）	

在 **SG6000-CN** 控制器上连接和配置 **10/225-GbE** 端口所需的信息

SG6000-CN 控制器上的四个 10/225-GbE 端口连接到 StorageGRID 网格网络和可选客户端网络。

所需信息	您的价值
链路速度	选择一项： • 自动（默认） • 10 GbE • 25 GbE
端口绑定模式	选择一项： • FIXED （默认） • 聚合
端口 1 的交换机端口（固定模式的客户端网络）	
端口 2 的交换机端口（固定模式的网格网络）	
端口 3 的交换机端口（固定模式的客户端网络）	
端口 4 的交换机端口（固定模式的网格网络）	

将 **SG6000-CN** 控制器连接到网格网络所需的信息

适用于 StorageGRID 的网格网络是一个必需的网络，用于所有内部 StorageGRID 流量。此设备使用 SG6000-CN 控制器上的 10/225-GbE 端口连接到网格网络。

所需信息	您的价值
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）

所需信息	您的价值
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为网格网络分配的 IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划用于网格网络上设备存储节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
网格网络子网（ GRID ）	

将 **SG6000-CN** 控制器连接到客户端网络所需的信息

适用于 StorageGRID 的客户端网络是一个可选网络，通常用于提供对网格的客户端协议访问。设备使用 SG6000-CN 控制器上的 10/225-GbE 端口连接到客户端网络。

所需信息	您的价值
已启用客户端网络	选择一项： • 否（默认） • 是的。
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：

所需信息	您的价值
DHCP 为客户端网络分配的 IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划在客户端网络上用于设备存储节点的静态 IP 地址 • 注： * 如果启用了客户端网络，则控制器上的默认路由将使用此处指定的网关。	• IPv4 地址（ CIDR ）： • 网关

将 **SG6000-CN** 控制器连接到 **BMC** 管理网络所需的信息

您可以使用以下 1-GbE 管理端口访问 SG6000-CN 控制器上的 BMC 接口。此端口支持使用智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）标准通过以太网远程管理控制器硬件。

所需信息	您的价值
要连接到 BMC 管理端口的以太网交换机端口（在图中圈出）	
为 BMC 管理网络分配的 DHCP IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划用于 BMC 管理端口的静态 IP 地址	• IPv4 地址（ CIDR ）： • 网关

相关信息

SG6000 设备中的控制器

查看设备网络连接（ SG6000 ）

SG6000-CN 控制器的端口绑定模式

缆线设备（ SG6000 ）

配置 StorageGRID IP 地址

安装硬件（ **SG6000** ）

硬件安装需要将 SG6000-CN 控制器和存储控制器架安装到机柜或机架中，连接缆线并接通电源。

注册硬件

注册设备硬件具有支持优势。

步骤

1. 找到存储控制器架的机箱序列号。

   您可以在装箱单上，确认电子邮件中或打开设备包装后在设备上找到此编号。

   存储设备上有多个序列号。存储控制器架上的序列号是您在设备上请求服务或支持时必须注册和使用的序列号。

2. 访问 NetApp 支持站点，网址为 "mysupport.netapp.com"。

3. 确定是否需要注册硬件：

如果您是 ...	请按照以下步骤操作 ...
现有 NetApp 客户	a. 使用您的用户名和密码登录。 b. 选择 * 产品 * > * 我的产品 * 。 c. 确认新序列号已列出。 d. 如果不是，请按照适用于新 NetApp 客户的说明进行操作。
NetApp 新客户	a. 单击 * 立即注册 * ，然后创建帐户。 b. 选择 * 产品 * > * 注册产品 * 。 c. 输入产品序列号和请求的详细信息。 注册获得批准后，您可以下载所需的任何软件。审批过程可能需要长达 24 小时。

SG6060和**SG6060X**：将**60**个驱动器磁盘架安装到机柜或机架中

您必须在机柜或机架中为 E2860 控制器架安装一组导轨，然后将控制器架滑入导轨。如果您要安装 60 个驱动器扩展架，则需要使用相同的操作步骤 。

您需要的内容

- 您已查看包装盒中的安全通知文档，并了解移动和安装硬件的预防措施。
- 导轨套件随附了相关说明。

每个 60 个驱动器架的重量约为 132 磅（ 60 千克），而未安装驱动器。要安全移动磁盘架，需要四个人或一台机械升降机。

为避免损坏硬件，如果安装了驱动器，请勿移动磁盘架。移动磁盘架之前，必须先卸下所有驱动器。

安装 E2860 控制器架或可选扩展架时，请从机架或机柜的底部到顶部安装硬件，以防止设备发生倾翻。要确保最重的设备位于机柜或机架的底部，请在 E2860 控制器架和扩展架上方安装 SG6000-CN 控制器。

在提交安装之前，请确认设备随附的 0.5 米光缆或您提供的缆线长度足以满足计划的布局要求。

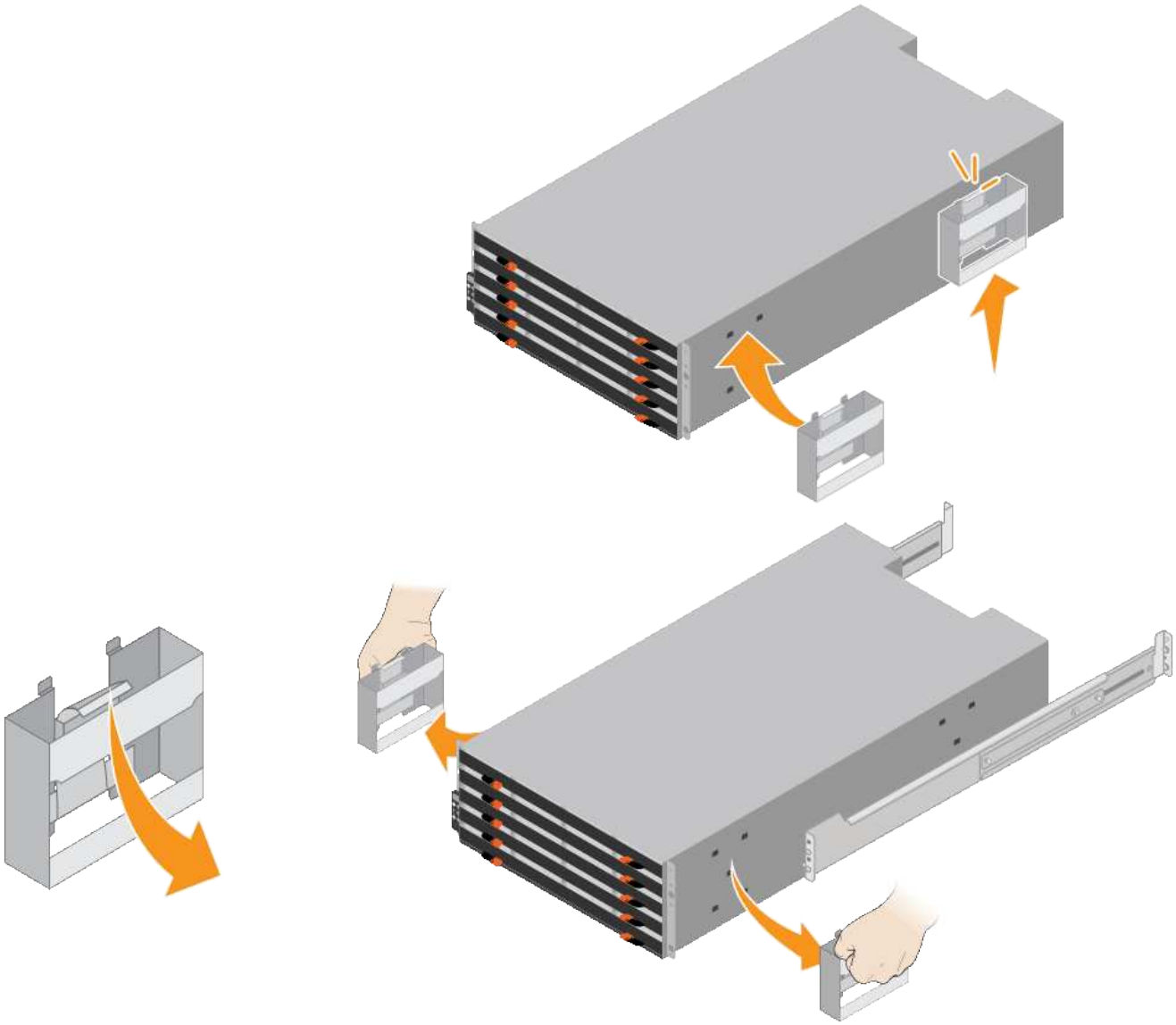
步骤

1. 请仔细按照导轨套件的说明在机柜或机架中安装导轨。

   对于方孔机柜，您必须先安装提供的锁紧螺母，以使用螺钉固定磁盘架的前后。

2. 卸下设备的外包装箱。然后，向下折叠内箱上的挡板。
3. 如果您要用手提设备，请将四个手柄连接到机箱两侧。

   向上推每个手柄，直到其卡入到位。



4. 将磁盘架的背面（带有连接器的一端）放在导轨上。
5. 从底部支撑好磁盘架，将其滑入机柜。如果使用的是手柄，请在滑入磁盘架时使用拇指闩锁一次分离一个手柄。

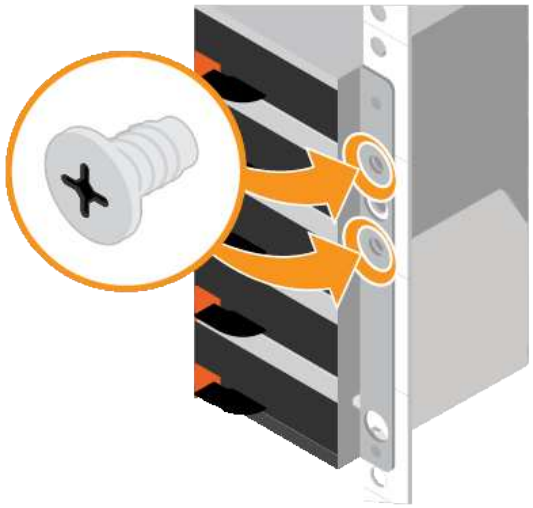
   要卸下手柄，请向后拉释放闩锁，向下推，然后从磁盘架中拉出。

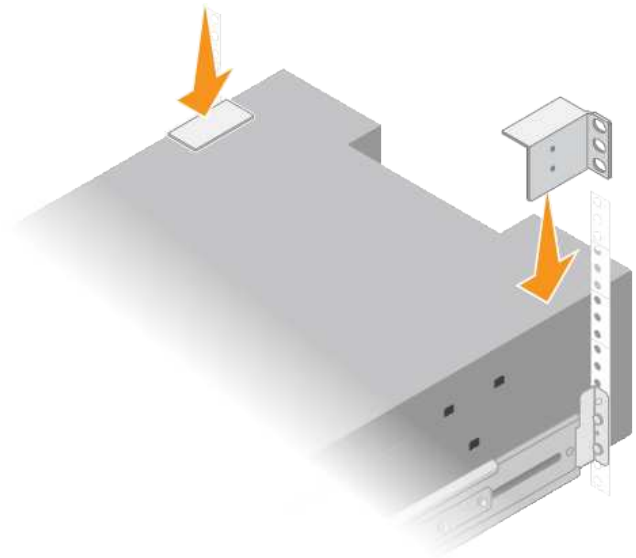
6. 将磁盘架固定到机柜正面。

   将螺钉插入两侧磁盘架顶部的第一个和第三个孔中。

7. 将磁盘架固定到机柜后部。

   将两个后支架放在磁盘架后上部分的每一侧。将螺钉插入每个支架的第一个和第三个孔中。





8. 对任何扩展架重复上述步骤。

SG6060和**SG6060X**：安装驱动器

将 60 个驱动器的磁盘架安装到机柜或机架中后，必须将所有 60 个驱动器安装到该磁盘架中。E2860 控制器架的发货包含两个 SSD 驱动器，您应将其安装在控制器架的顶部抽屉中。每个可选扩展架都包含 60 个 HDD 驱动器，而不包含 SSD 驱动器。

您需要的内容

您已在机柜或机架中安装 E2860 控制器架或可选扩展架（一个或两个）。

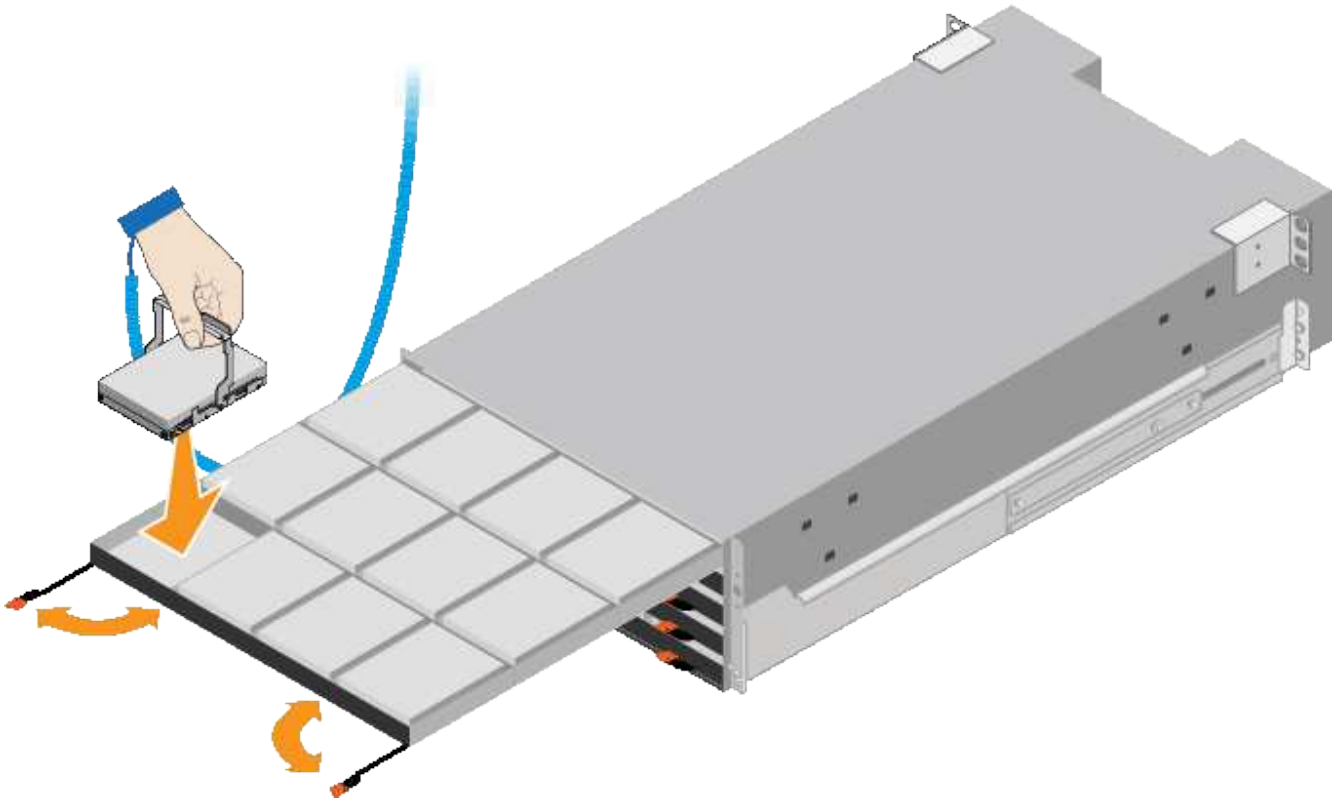
为避免损坏硬件，如果安装了驱动器，请勿移动磁盘架。移动磁盘架之前，必须先卸下所有驱动器。

步骤

1. 将 ESD 腕带的腕带一端绕在腕带上，并将扣具一端固定到金属接地，以防止静电放电。
2. 将驱动器从其包装中取出。
3. 释放顶部驱动器抽盒上的拉杆，然后使用拉杆将抽盒滑出。
4. 找到两个 SSD 驱动器。

   扩展架不使用 SSD 驱动器。

5. 将每个驱动器把手提起至垂直位置。
6. 将两个 SSD 驱动器安装在插槽 0 和 1 中（前两个插槽沿抽盒左侧）。
7. 将每个驱动器轻轻放入其插槽中，然后放低凸起的驱动器把手，直到其卡入到位。



8. 将 10 个 HDD 驱动器安装到顶部抽盒中。
9. 推中间并轻轻合上两个拉杆，将抽盒滑回原位。

> 如果您感到绑定，请停止推动抽盒。Use the release levers at the front of the drawer to slide the drawer back out.然后，小心地将抽盒重新插入插槽。

10. 重复上述步骤，将 HDD 驱动器安装到其他四个抽盒中。

> 您必须安装全部 60 个驱动器，以确保正常运行。

11. 将前挡板连接到磁盘架。
12. 如果您有扩展架，请重复上述步骤，在每个扩展架的每个抽盒中安装 12 个 HDD 驱动器。
13. 按照说明将 SG6000-CN 安装到机柜或机架中。

SGF6024： 将 **24** 个驱动器磁盘架安装到机柜或机架中

您必须在机柜或机架中为 EF570 控制器架安装一组导轨，然后将阵列滑入导轨。

您需要的内容

- 您已查看包装盒中的安全通知文档，并了解移动和安装硬件的预防措施。
- 导轨套件随附了相关说明。

步骤

1. 请仔细按照导轨套件的说明在机柜或机架中安装导轨。

对于方孔机柜，您必须先安装提供的锁紧螺母，以使用螺钉固定磁盘架的前后。

2. 卸下设备的外包装箱。然后，向下折叠内箱上的挡板。
3. 将磁盘架的背面（带有连接器的一端）放在导轨上。

   满载的磁盘架重约 52 磅（ 24 千克）。需要两个人才能安全移动机箱。

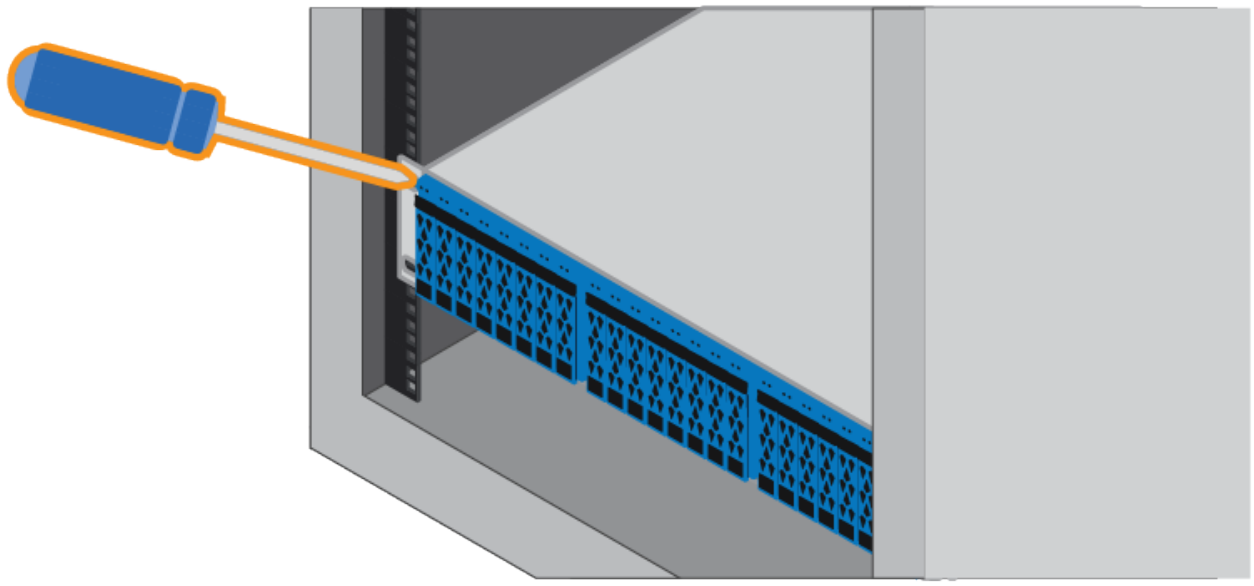
4. 小心地将机箱完全滑入导轨上。

   您可能需要调整导轨，以确保机箱一直滑入导轨。

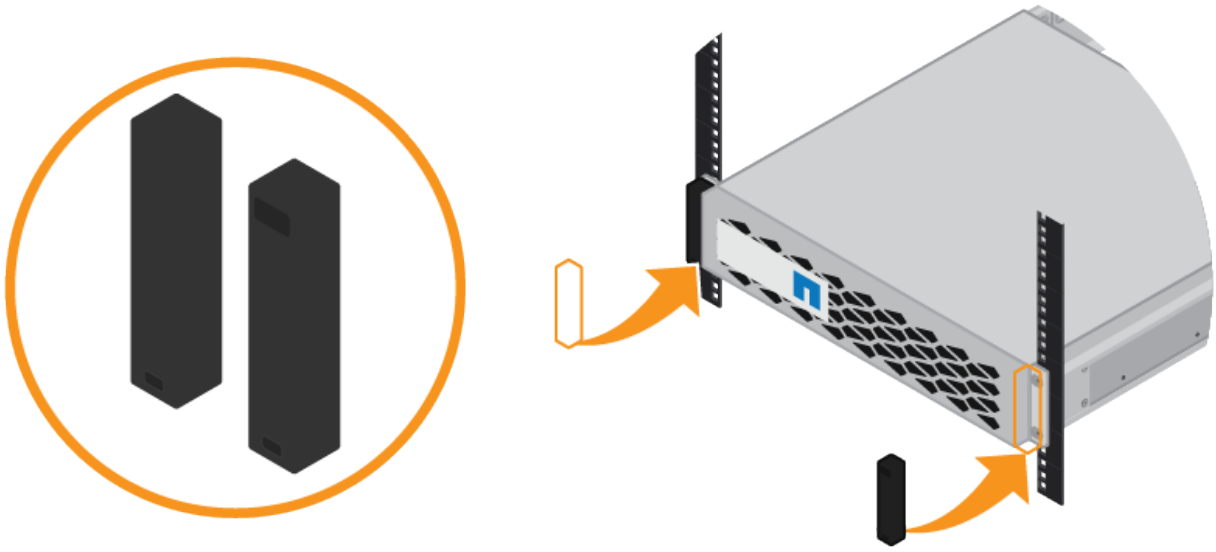
   安装完机箱后，请勿在导轨上放置其他设备。导轨的设计不会增加重量。

   如果适用，您可能需要卸下磁盘架端盖或系统挡板，以将机箱固定到机架柱上；如果需要，则需要在完成操作后更换端盖或挡板。

5. 通过安装支架（预装在机箱正面的任意一侧），机架或系统机柜上的孔以及导轨正面的孔插入两个 M5 螺钉，将机箱固定到机箱或机架和导轨的正面。



6. 通过将两个 M5 螺钉插入机箱支架和导轨套件支架，将机箱固定到导轨背面。
7. 如果适用，请更换磁盘架端盖或系统挡板。



SG6000-CN： 安装到机柜或机架中

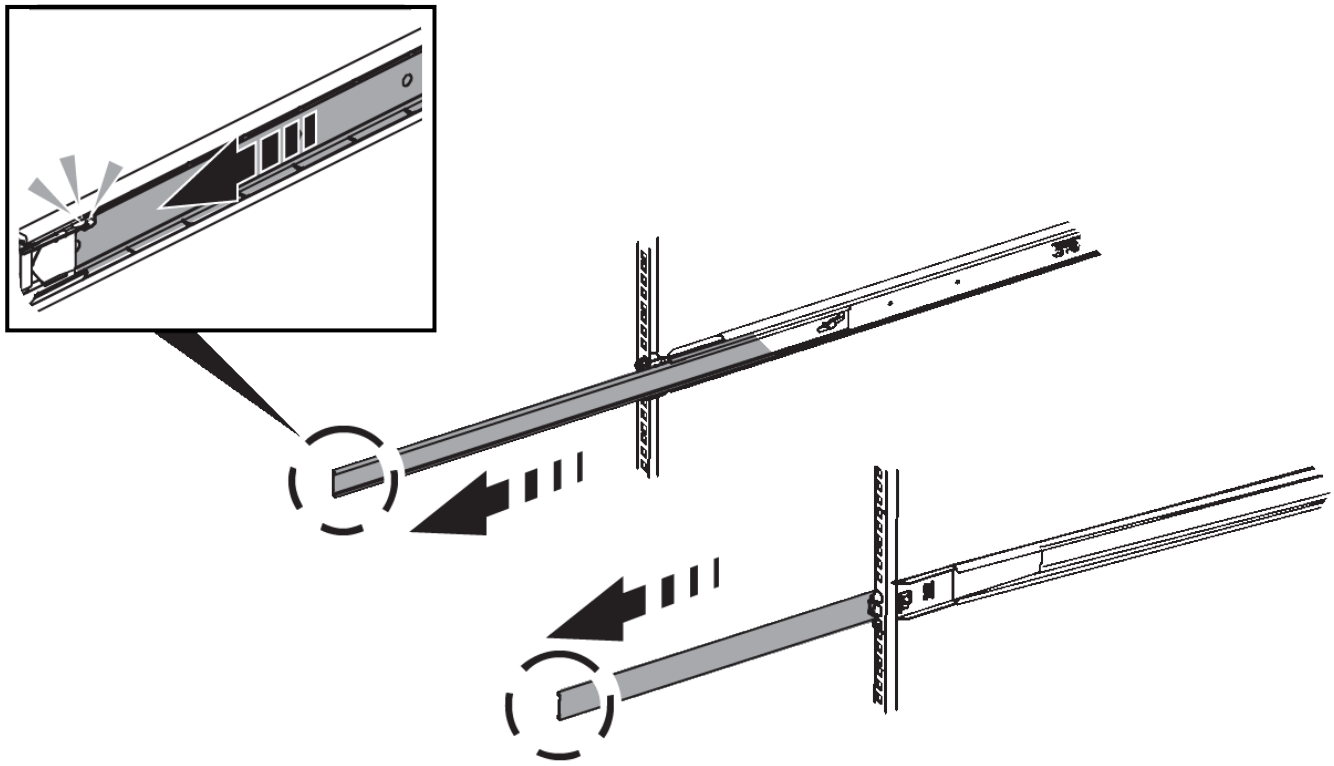
您必须在机柜或机架中为 SG6000-CN 控制器安装一组导轨，然后将控制器滑入导轨。

您需要的内容

- 您已查看包装盒中的安全通知文档，并了解移动和安装硬件的预防措施。
- 导轨套件随附了相关说明。
- 您已安装 E2860 控制器架和驱动器或 EF570 控制器架。

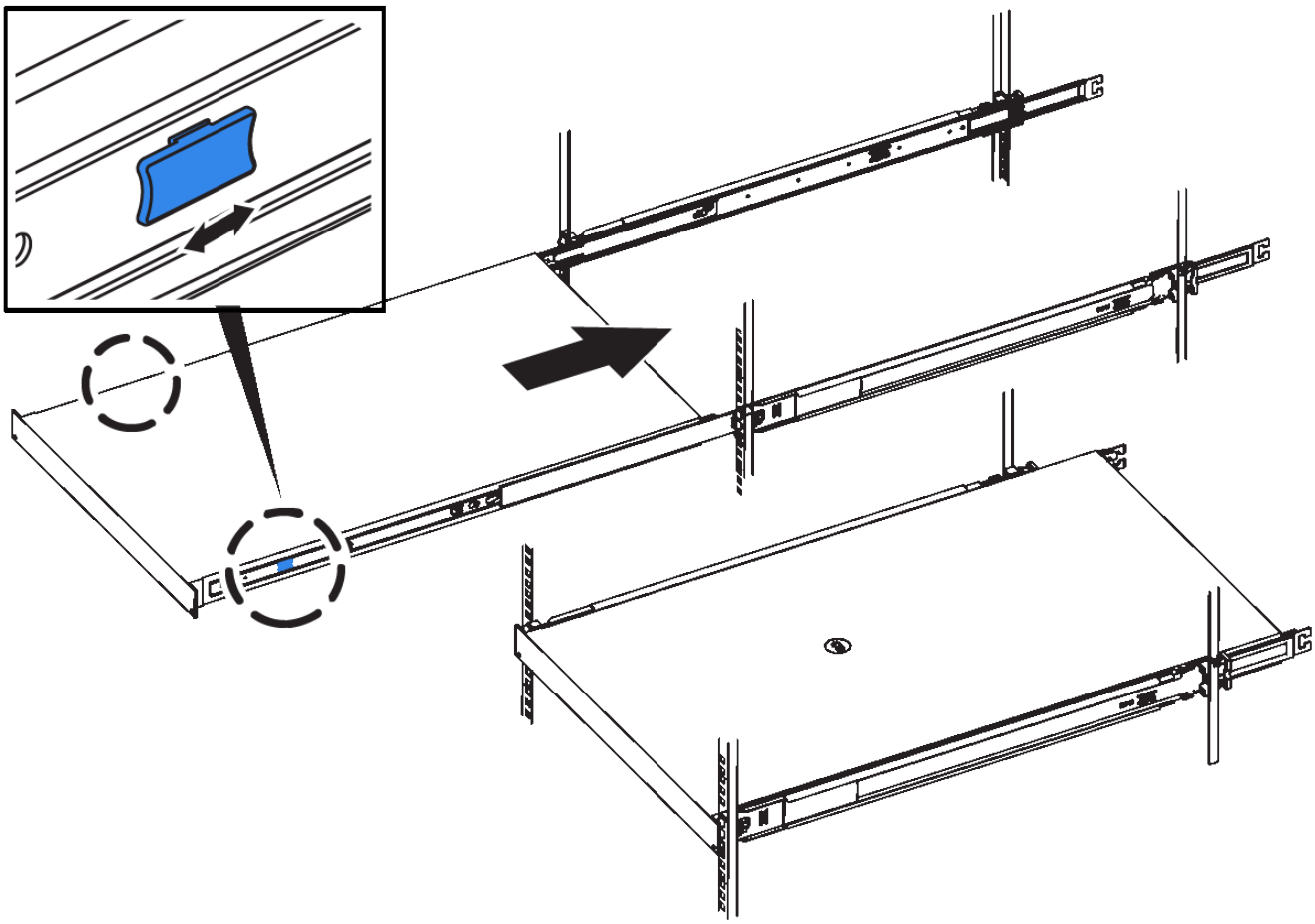
步骤

1. 请仔细按照导轨套件的说明在机柜或机架中安装导轨。
2. 在机柜或机架中安装的两个导轨上，展开导轨的可移动部分，直到听到卡嗒声为止。



3. 将 SG6000-CN 控制器插入导轨。
4. 将控制器滑入机柜或机架。

   如果无法再移动控制器，请拉动机箱两侧的蓝色闩锁，将控制器完全滑入。



在打开控制器电源之前，请勿连接前挡板。

5. 拧紧控制器前面板上的固定螺钉，将控制器固定在机架中。

缆线设备（ **SG6000** ）

您必须将存储控制器连接到 SG6000-CN 控制器，连接所有三个控制器上的管理端口，并将 SG6000-CN 控制器上的网络端口连接到网格网络和适用于 StorageGRID 的可选客户端网络。

您需要的内容

- 设备附带有四根光缆，用于将两个存储控制器连接到 SG6000-CN 控制器。
- 您可以使用 RJ-45 以太网缆线（至少四根）连接管理端口。
- 您可以选择以下网络端口之一。这些项目不随设备提供。
  - 一到四根双轴缆线，用于连接四个网络端口。
  - 如果您计划使用光缆连接端口，则需要一到四个 SFP+ 或 SFP28 收发器。

* 受到激光辐射的风险 * —请勿拆卸或卸下 SFP 收发器的任何部件。您可能受到激光辐射的影响。

关于此任务

本节提供了为以下设备布线的说明：

- SG6060和SG6060X
- SGF6024

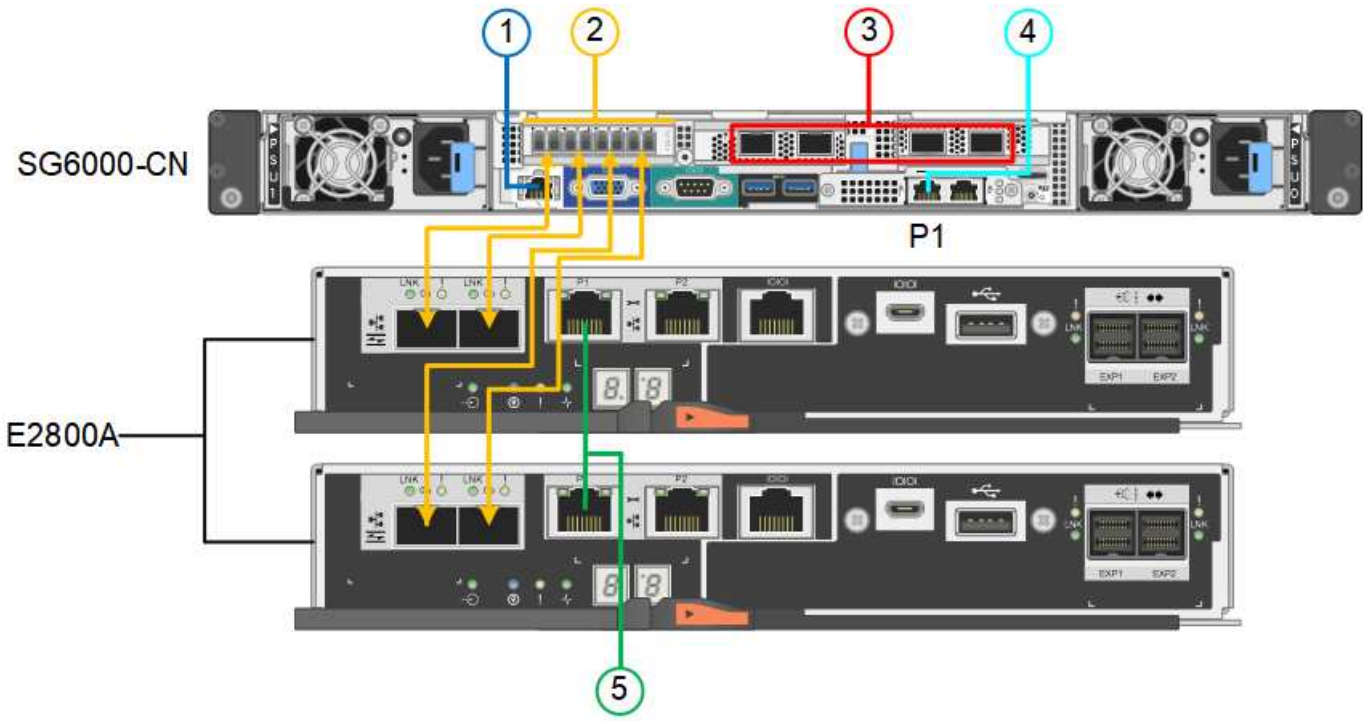
为**SG6060**或**SG6060X**布线

下图显示了SG6060和SG6060X设备中的三个控制器、其中SG6000-CN计算控制器位于顶部、而两个E2800存储控制器位于底部。

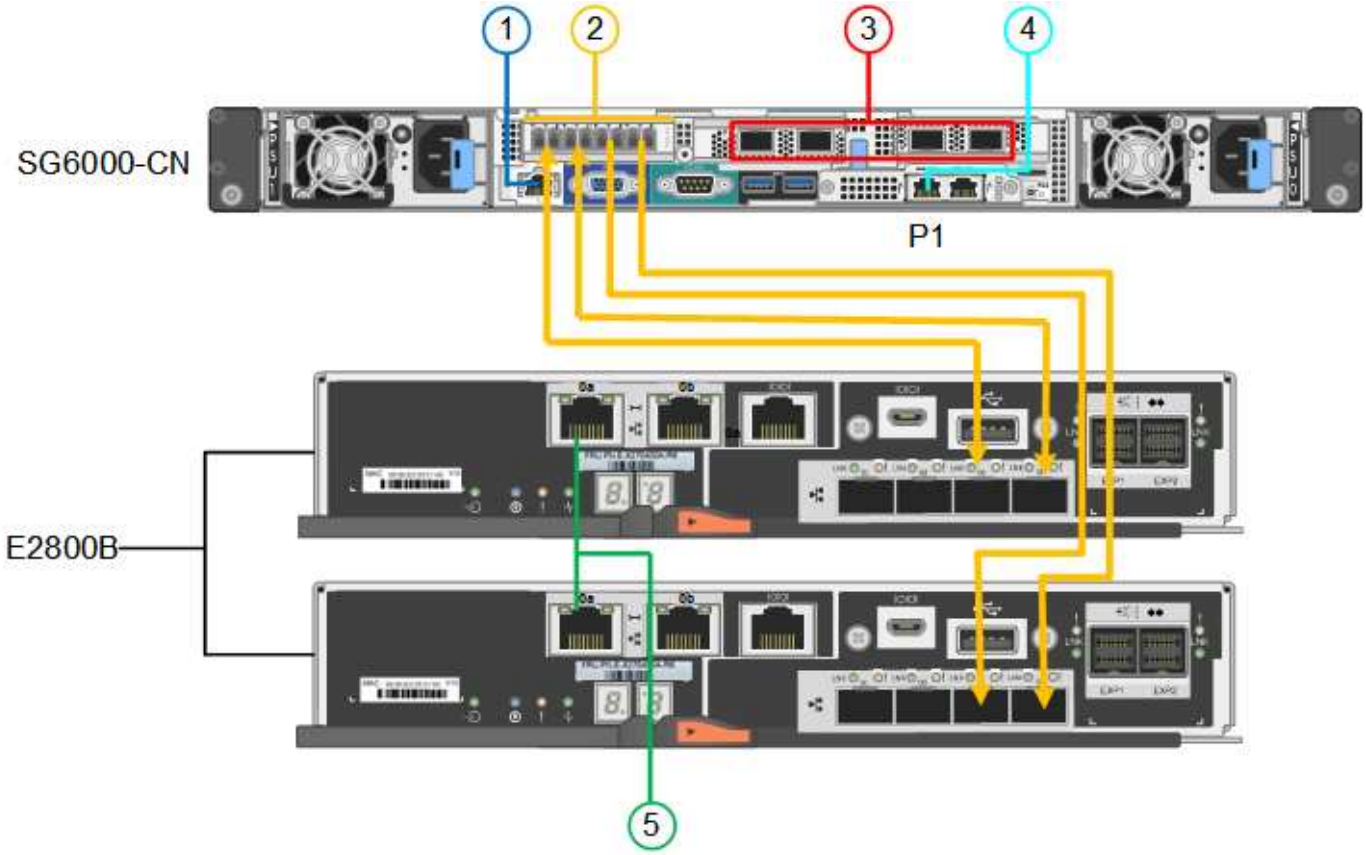
SG6060具有E2800A控制器、SG60X具有E2800B控制器。除了互连端口的位置之外、两个版本的E2800控制器的规格和功能都相同。

请勿在同一设备中使用E2800A和E2800B控制器。

- SG6060到E2800A连接*

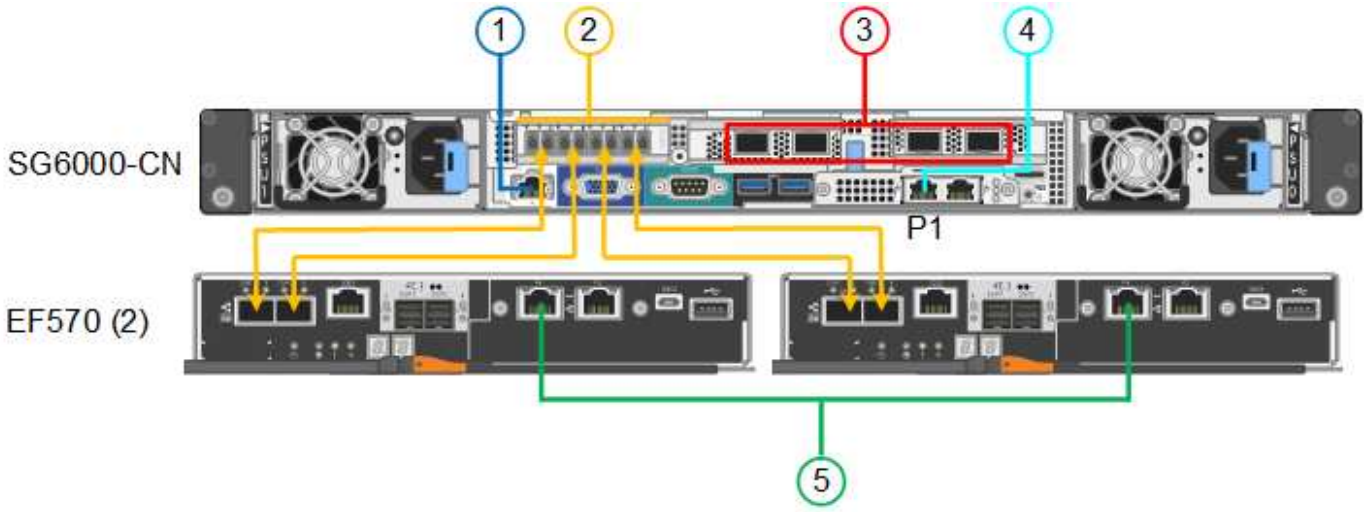


- SG60X到E2800B连接*



为**SGF6024**布线

下图显示了 SG6024 设备中的三个控制器，其中 SG6000-CN 计算控制器位于顶部，两个 EF570 存储控制器并排位于计算控制器下方。



	Port	端口类型	功能
1.	SG6000-CN 控制器上的 BMC 管理端口	1-GbE （RJ-45）	连接到访问 BMC 接口的网络。

	Port	端口类型	功能
2.	FC 连接端口： • 4 个用于 SG6000-CN 控制器 • 每个存储控制器上 2 个	16 Gb/ 秒 FC 光纤 SFP+	将每个存储控制器连接到 SG6000-CN 控制器。
3.	SG6000-CN 控制器上的四个网络端口	10/225-GbE	连接到网格网络和 StorageGRID 客户端网络。
4.	SG6000-CN 控制器上的管理网络端口（图中标记为 P1 ）	1-GbE （ RJ-45 ） • 重要信息： * 此端口仅以 1000 BASE/ 全满运行，不支持 10 或 100 MB 速度。	将 SG6000-CN 控制器连接到 StorageGRID 管理网络。
	SG6000-CN 控制器上最右侧的 RJ-45 端口	1-GbE （ RJ-45 ） • 重要信息： * 此端口仅以 1000 BASE/ 全满运行，不支持 10 或 100 MB 速度。	• 如果要与管理网络建立冗余连接，则可以与管理端口 1 绑定。 • 可以保持未连接状态，并可用于临时本地访问（ IP 169.254.0.1 ）。 • 在安装期间，如果 DHCP 分配的 IP 地址不可用，则可以使用将 SG6000-CN 控制器连接到服务笔记本电脑。
5.	每个存储控制器上的管理端口 1	1-GbE （ RJ-45 ）	连接到访问 SANtricity System Manager 的网络。
	每个存储控制器上的管理端口 2	1-GbE （ RJ-45 ）	为技术支持预留。

步骤

1. 使用以太网缆线将 SG6000-CN 控制器上的 BMC 管理端口连接到管理网络。

   虽然此连接是可选的，但建议便于支持。

2. 使用四根光缆和四个 SFP+ 收发器将每个存储控制器上的两个 FC 端口连接到 SG6000-CN 控制器上的 FC 端口。
3. 使用双轴缆线或光缆以及 SFP+ 或 SFP28 收发器将 SG6000-CN 控制器上的网络端口连接到相应的网络交换机。

   这四个网络端口必须使用相同的链路速度。如果您计划使用 10-GbE 链路速度，请安装 SFP+ 收发器。如果您计划使用 25 GbE 链路速度，请安装 SFP28 收发器。

- 如果您计划使用固定端口绑定模式（默认），请将端口连接到 StorageGRID 网格和客户端网络，如表所示。

Port	连接到 ...
端口 1	客户端网络（可选）
端口 2	网格网络
端口 3	客户端网络（可选）
端口 4	网格网络

- 如果您计划使用聚合端口绑定模式，请将一个或多个网络端口连接到一个或多个交换机。您应至少连接四个端口中的两个，以避免发生单点故障。如果在一个 LACP 绑定中使用多个交换机，则这些交换机必须支持 MLAG 或等效项。

4. 如果您计划使用 StorageGRID 管理网络，请使用以太网缆线将 SG6000-CN 控制器上的管理网络端口连接到管理网络。
5. 如果您计划使用SANtricity System Manager的管理网络、请使用以太网缆线将每个存储控制器上的管理端口1 (E2800A上的P1和E2800B上的0A)(左侧的RJ-45端口)连接到SANtricity System Manager的管理网络。

   请勿使用存储控制器上的管理端口2 (E2800A上的P2和E2800B上的0b)(右侧的RJ-45端口)。此端口是为技术支持预留的。

相关信息

SG6000-CN 控制器的端口绑定模式

将 SG6000-CN 控制器重新安装到机柜或机架中

SG6060和**SG6060X**：为可选扩展架布线

如果您使用的是扩展架，则必须将其连接到 E2860 控制器架。每个SG6060或SG60X设备最多可以有两个扩展架。

您需要的内容

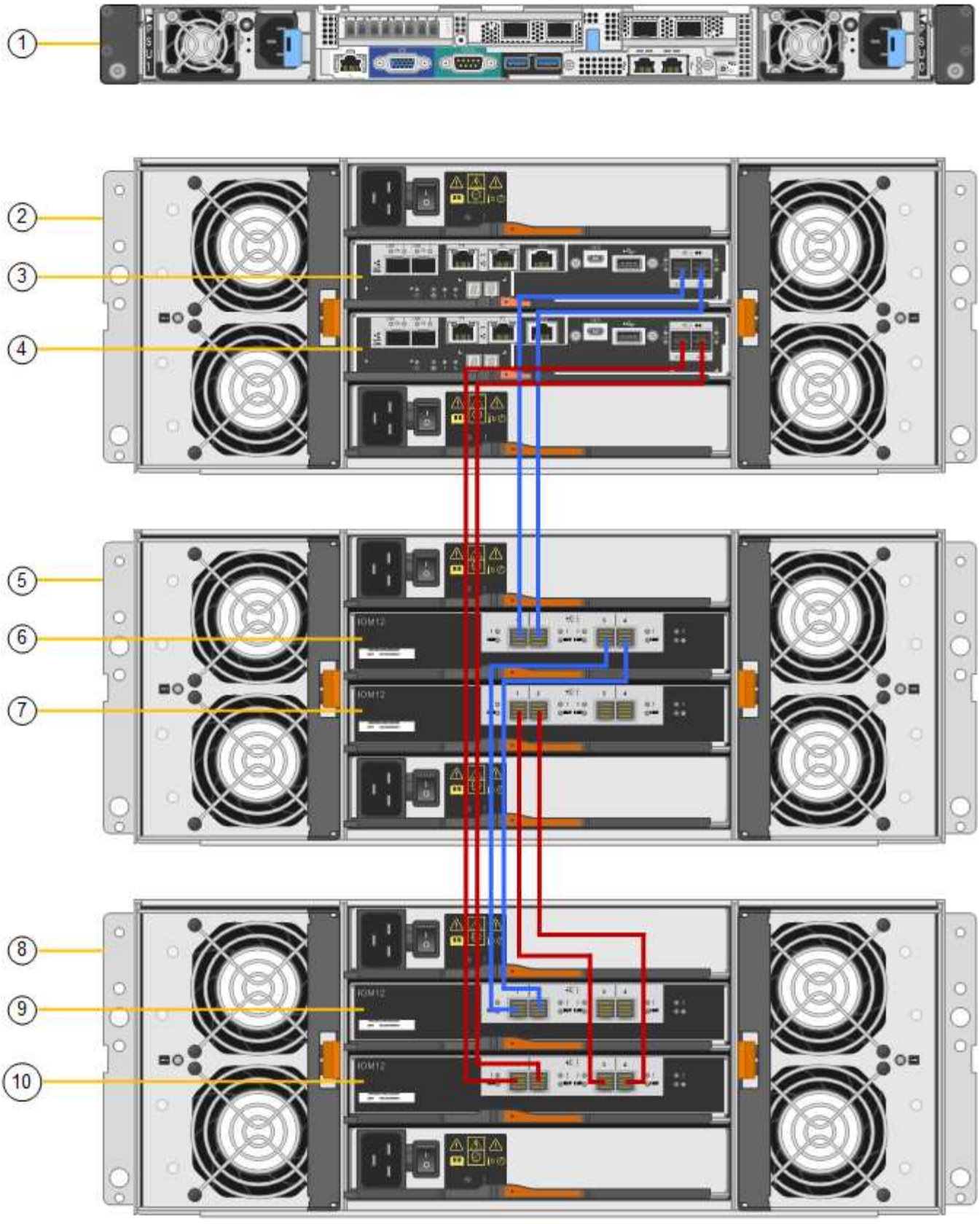
- 每个扩展架附带两根 SAS 缆线。
- 您已将扩展架安装在包含 E2860 控制器架的机柜或机架中。

  SG6060和SG6060X：将60个驱动器磁盘架安装到机柜或机架中

步骤

将每个扩展架连接到 E2860 控制器架，如图所示。

此图显示了SG6060中两个扩展架的布线情况(SG60X的扩展布线相同)。如果只有一个扩展架、请将IOM A连接到控制器A、并将IOM B连接到控制器B



Callout	Description
1.	SG6000-CN

Callout	Description
2.	E2860 控制器架
3.	控制器 A
4.	控制器 B
5.	扩展架 1
6.	扩展架 1 的 IOM A
7.	扩展架 1 的 IOM B
8.	扩展架 2.
9	扩展架 2 的 IOM A
10	扩展架 2 的 IOM B

连接电源线并接通电源（ **SG6000** ）

连接网络缆线后，您可以为 SG6000-CN 控制器以及两个存储控制器或可选扩展架供电。

步骤

1. 确认存储控制器架中的两个控制器均已关闭。

   * 电击风险 * —在连接电源线之前，请确保两个存储控制器中每个控制器的电源开关均已关闭。

2. 如果您有扩展架，请确认两个 IOM 电源开关均已关闭。

   * 电击风险 * —在连接电源线之前，请确保每个扩展架的两个电源开关均已关闭。

3. 将电源线连接到 SG6000-CN 控制器中的两个电源设备中的每个设备。
4. 将这两条电源线连接到机柜或机架中的两个不同配电单元（ PDU ）。
5. 将电源线连接到存储控制器架中的两个电源设备中的每个设备。
6. 如果您有扩展架，请分别为每个扩展架中的两个电源设备连接一根电源线。
7. 将每个存储架（包括可选扩展架）中的两条电源线连接到机柜或机架中的两个不同 PDU 。
8. 如果 SG6000-CN 控制器正面的电源按钮当前未呈蓝色亮起，请按此按钮打开控制器的电源。

   在启动过程中，请勿再次按电源按钮。

9. 打开存储控制器架背面的两个电源开关。如果您有扩展架，请打开每个架的两个电源开关。

- 请勿在启动过程中关闭电源开关。
- 首次启动时，存储控制器架和可选扩展架中的风扇可能会发出很大的声音。启动期间发出较大的噪音是正常的。

10. 组件启动后，请检查其状态。
    - 检查每个存储控制器背面的七段显示。有关详细信息，请参见有关查看启动状态代码的文章。
    - 验证 SG6000-CN 控制器正面的电源按钮是否亮起。
11. 如果发生错误，请更正任何问题。
12. 如果已卸下 SG6000-CN 控制器，请将前挡板连接到该控制器。

相关信息

查看 SG6000 存储控制器的启动状态代码

查看 SG6000-CN 控制器上的状态指示灯和按钮

将 SG6000-CN 控制器重新安装到机柜或机架中

查看 **SG6000-CN** 控制器上的状态指示灯和按钮

SG6000-CN 控制器包含一些指示灯，可帮助您确定控制器的状态，其中包括以下指示灯和按钮。

	显示	**Description**
1.	电源按钮	• 蓝色：控制器已启动。 • off ： 控制器已关闭。
2.	重置按钮	无指示符 _ 使用此按钮可对控制器执行硬重置。
3.	识别按钮	• 闪烁或稳定蓝色：标识机柜或机架中的控制器。 • off ： 无法在机柜或机架中直观地识别控制器。 此按钮可以设置为闪烁，打开（稳定）或关闭。
4.	警报 LED	• 琥珀色：发生错误。 • 注： * 要查看启动和错误代码，您必须访问 BMC 界面。 • off ： 不存在任何错误。

常规启动代码

在启动期间或在对 SG6000-CN 控制器进行硬重置后，将发生以下情况：

1. 基板管理控制器（ BMC ）会记录启动顺序的代码，包括发生的任何错误。
2. 电源按钮将亮起。
3. 如果在启动期间发生任何错误，警报 LED 将亮起。

   要查看启动和错误代码，您必须访问 BMC 界面。

相关信息

硬件安装故障排除（ SG6000 ）

配置 BMC 接口（ SG6000 ）

打开 SG6000-CN 控制器的电源并验证其运行情况

查看 **SG6000** 存储控制器的启动状态代码

每个存储控制器都有一个七段显示器，可在控制器启动时提供状态代码。E2800 控制器和 EF570 控制器的状态代码相同。

关于此任务

有关这些代码的说明，请参见适用于您的存储控制器类型的 E 系列系统监控信息。

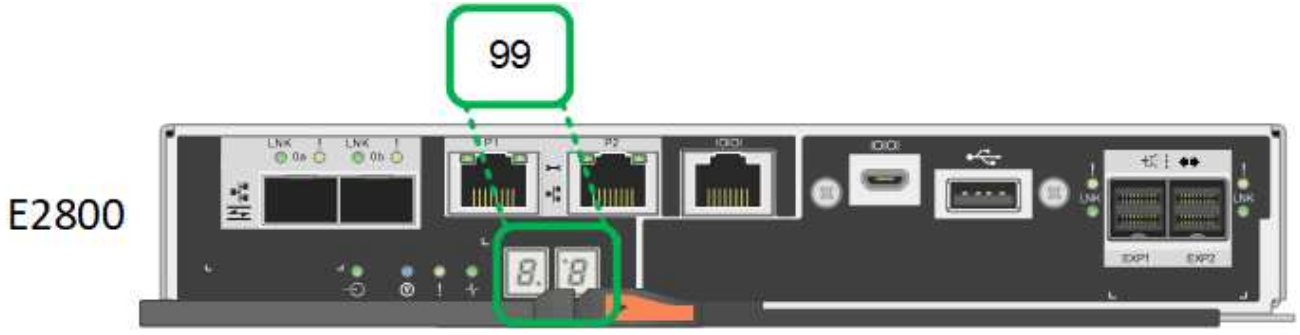
步骤

1. 在启动期间，通过查看每个存储控制器的七段显示器上显示的代码来监控进度。

   每个存储控制器上的七段显示会显示重复序列 * 操作系统 * ， * 可持续发展 * ， `* 空白 _*` ，以指示控制器正在执行每日开始处理。

2. 控制器启动后，确认每个存储控制器显示 99 ，这是 E 系列控制器架的默认 ID 。

   确保此值显示在两个存储控制器上，如本示例 E2800 控制器所示。



3. 如果一个或两个控制器显示其他值，请参见 硬件安装故障排除（ SG6000 ） 并确认您已正确完成安装步骤。如果无法解决此问题，请联系技术支持。

相关信息

"《 E5700 和 E2800 系统监控指南》"

"NetApp 支持"

打开 SG6000-CN 控制器的电源并验证其运行情况

配置硬件（ **SG6000** ）

为设备接通电源后，您必须配置 StorageGRID 要使用的网络连接。您必须配置 SANtricity 系统管理器，该软件将用于监控控制器架中的存储控制器和其他硬件。此外，还必须确保可以访问 SG6000-CN 控制器的 BMC 接口。

配置 **StorageGRID** 连接（ **SG6000** ）

在将 StorageGRID 设备部署为 StorageGRID 系统中的存储节点之前，您必须配置设备与计划使用的网络之间的连接。您可以通过浏览到 StorageGRID 设备安装程序来配置网络连接，该安装程序预安装在 SG6000-CN 控制器（计算控制器）上。

访问 **StorageGRID** 设备安装程序

您必须访问 StorageGRID 设备安装程序以验证安装程序版本，并配置设备与三个 StorageGRID 网络之间的连接：网格网络，管理网络（可选）和客户端网络（可选）。

您需要的内容

- 您正在使用可以连接到 StorageGRID 管理网络的任何管理客户端，或者您使用的是服务笔记本电脑。
- 客户端或服务笔记本电脑具有受支持的 Web 浏览器。
- SG6000-CN 控制器连接到您计划使用的所有 StorageGRID 网络。
- 您知道这些网络上 SG6000-CN 控制器的 IP 地址，网关和子网。
- 您已配置计划使用的网络交换机。

关于此任务

要首次访问 StorageGRID 设备安装程序，您可以使用为 SG6000-CN 控制器上的管理网络端口分配的 DHCP IP 地址（假设控制器已连接到管理网络），也可以将服务笔记本电脑直接连接到 SG6000-CN 控制器。

步骤

1. 如果可能，请使用 SG6000-CN 控制器上管理网络端口的 DHCP 地址来访问 StorageGRID 设备安装程序。

   a. 找到 SG6000-CN 控制器正面的 MAC 地址标签，并确定管理网络端口的 MAC 地址。

      MAC 地址标签列出了 BMC 管理端口的 MAC 地址。

      要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 * 。 2 例如，如果标签上的 **MAC** 地址以 ***09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 * （ *y* ） FF* 结尾，则管理端口的 MAC 地址将以 * （ *y*+1 ） 01* 结尾。您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 * + 2 =* 来轻松进行计算。

b. 向网络管理员提供 MAC 地址，以便他们可以在管理网络上查找设备的 DHCP 地址。

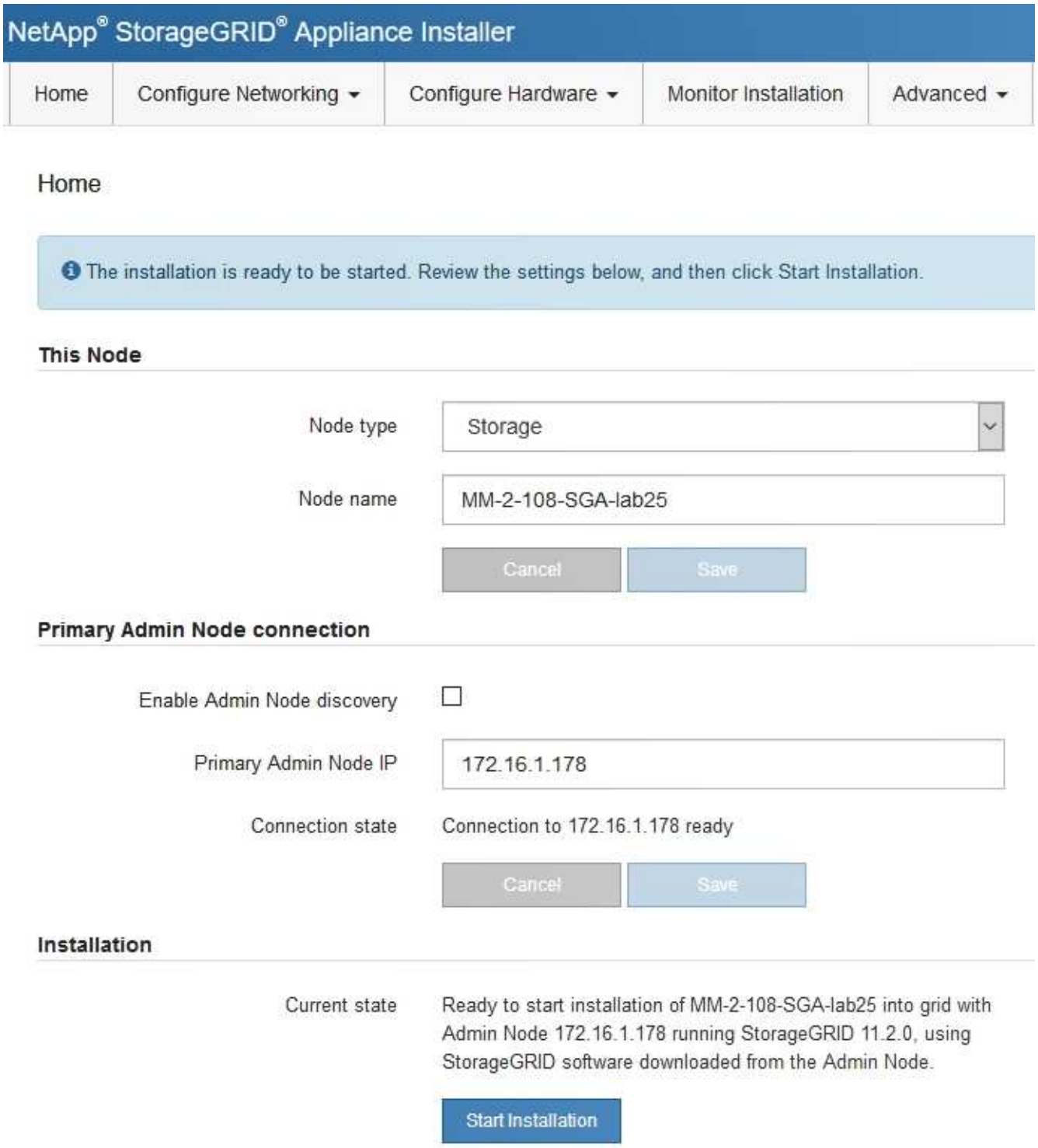
c. 在客户端中，输入 StorageGRID 设备安装程序的以下 URL： + ` * https://*Appliance_Controller_IP*:8443*`

   对于 ` SG6000-CN_Controller_IP_` ，请使用 DHCP 地址。

d. 如果系统提示您显示安全警报，请使用浏览器的安装向导查看并安装证书。

   下次访问此 URL 时，不会显示此警报。

   此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。



2. 如果无法使用 DHCP 获取 IP 地址，则可以使用链路本地连接。

   a. 使用以太网缆线将服务笔记本电脑直接连接到 SG6000-CN 控制器上最右侧的 RJ-45 端口。

   b. 在服务笔记本电脑上打开 Web 浏览器。

c. 输入 StorageGRID 设备安装程序的 URL： + ` * https://169.254.0.1:8443*`

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前的连接方式。

如果无法通过链路本地连接访问主页，请将服务笔记本电脑 IP 地址配置为 `169.254.0.2` ，然后重试。

完成后

访问 StorageGRID 设备安装程序后：

- 验证设备上的 StorageGRID 设备安装程序版本是否与 StorageGRID 系统上安装的软件版本匹配。如有必要，请升级 StorageGRID 设备安装程序。

  验证并升级 StorageGRID 设备安装程序版本

- 查看 StorageGRID 设备安装程序主页页面上显示的所有消息，并根据需要配置链路配置和 IP 配置。

相关信息

Web 浏览器要求

验证并升级 **StorageGRID** 设备安装程序版本

设备上的 StorageGRID 设备安装程序版本必须与 StorageGRID 系统上安装的软件版本匹配，以确保所有 StorageGRID 功能均受支持。

您需要的内容

您已访问 StorageGRID 设备安装程序。

关于此任务

StorageGRID 设备出厂时预安装了 StorageGRID 设备安装程序。如果要将设备添加到最近升级的 StorageGRID 系统，则可能需要先手动升级 StorageGRID 设备安装程序，然后再将设备安装为新节点。

升级到新的 StorageGRID 版本时， StorageGRID 设备安装程序会自动升级。您无需升级已安装设备节点上的 StorageGRID 设备安装程序。只有在安装包含早期版本的 StorageGRID 设备安装程序的设备时，才需要此操作步骤 。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 升级固件 * 。
2. 将当前固件版本与 StorageGRID 系统上安装的软件版本进行比较。（从网格管理器的顶部，选择帮助图标并选择 * 关于 * 。）

   两个版本中的第二位数字应匹配。例如，如果您的 StorageGRID 系统运行的是 11.* 6* 。 *x.y* ，则 StorageGRID 设备安装程序版本应为 3.* 6* 。 *z* 。

3. 如果设备安装了StorageGRID 设备安装程序的低级版本、请转到 "NetApp下载：StorageGRID 设备"。

   使用您的 NetApp 帐户的用户名和密码登录。

4. 下载适当版本的 * StorageGRID Appliances * 支持文件以及相应的校验和文件。

   StorageGRID 设备的支持文件是一个 ` .zip` 归档文件，其中包含所有 StorageGRID 设备型号的当前和先前固件版本，位于每种控制器类型的子目录中。

   下载 StorageGRID 设备的支持文件后，解压缩 ` .zip` 归档并查看 README 文件，以了解有关安装 StorageGRID 设备安装程序的重要信息。

5. 按照的升级固件页面上的说明进行操作 StorageGRID 设备安装程序 要执行以下步骤：

   a. 上传适用于您的控制器类型的相应支持文件（固件映像）和校验和文件。

   b. 升级非活动分区。

   c. 重新启动和交换分区。

   d. 升级第二个（非活动）分区。

配置网络链路(SG6000系列)

您可以为用于将设备连接到网格网络，客户端网络和管理网络的端口配置网络链路。您可以设置链路速度以及端口和网络绑定模式。

您需要的内容

如果要克隆设备节点，请为源设备节点使用的所有链路配置目标设备的网络链路。

如果您计划使用 25 GbE 链路速度：

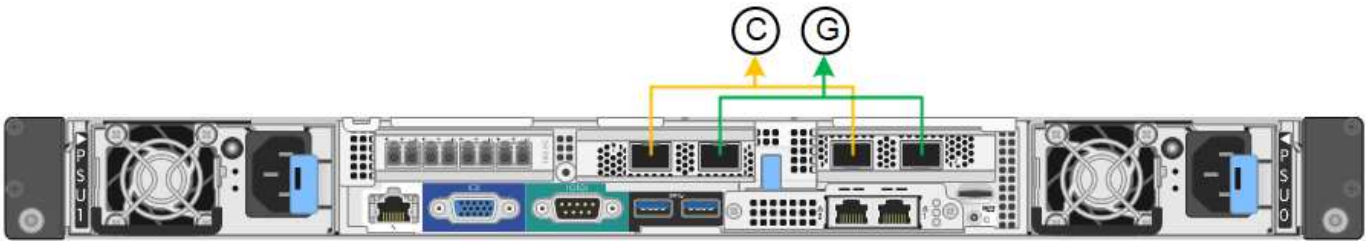
- 您正在使用 SFP28 双轴缆线，或者已在计划使用的网络端口中安装 SFP28 收发器。
- 您已将网络端口连接到可支持这些功能的交换机。
- 您了解如何配置交换机以使用此较高的速度。

如果您计划使用聚合端口绑定模式， LACP 网络绑定模式或 VLAN 标记：

- 您已将设备上的网络端口连接到可支持 VLAN 和 LACP 的交换机。
- 如果多个交换机参与 LACP 绑定，则这些交换机支持多机箱链路聚合组（ MLAG ）或等效项。
- 您了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。
- 您知道要用于每个网络的唯一 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。

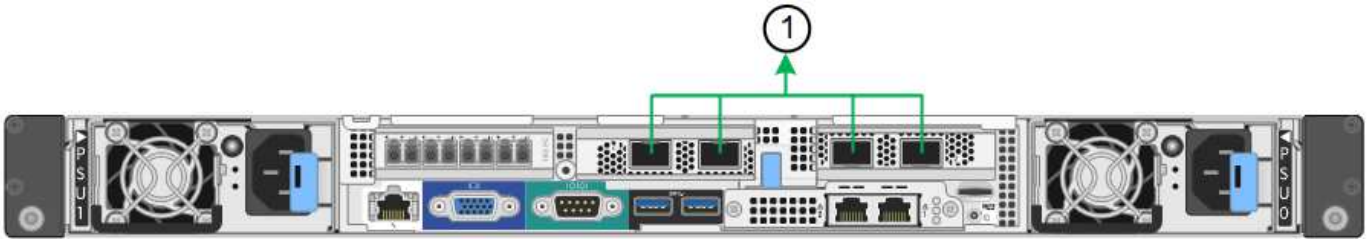
关于此任务

此图显示了四个网络端口在固定端口绑定模式下的绑定方式（默认配置）。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

此图显示了四个网络端口在聚合端口绑定模式下的绑定方式。



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表汇总了用于配置四个网络端口的选项。默认设置以粗体显示。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

- * 固定（默认）端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 端口 1 和 3 对客户端网络使用主动备份绑定。 • 可以为两个网络指定VLAN标记。
LACP （ 802.3ad ）	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 端口 1 和 3 对客户端网络使用 LACP 绑定。 • 可以为两个网络指定VLAN标记。

- * 聚合端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （ 802.3ad ）	• 端口 1-4 对网格网络使用一个 LACP 绑定。 • 一个 VLAN 标记用于标识网格网络数据包。	• 端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。 • 通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

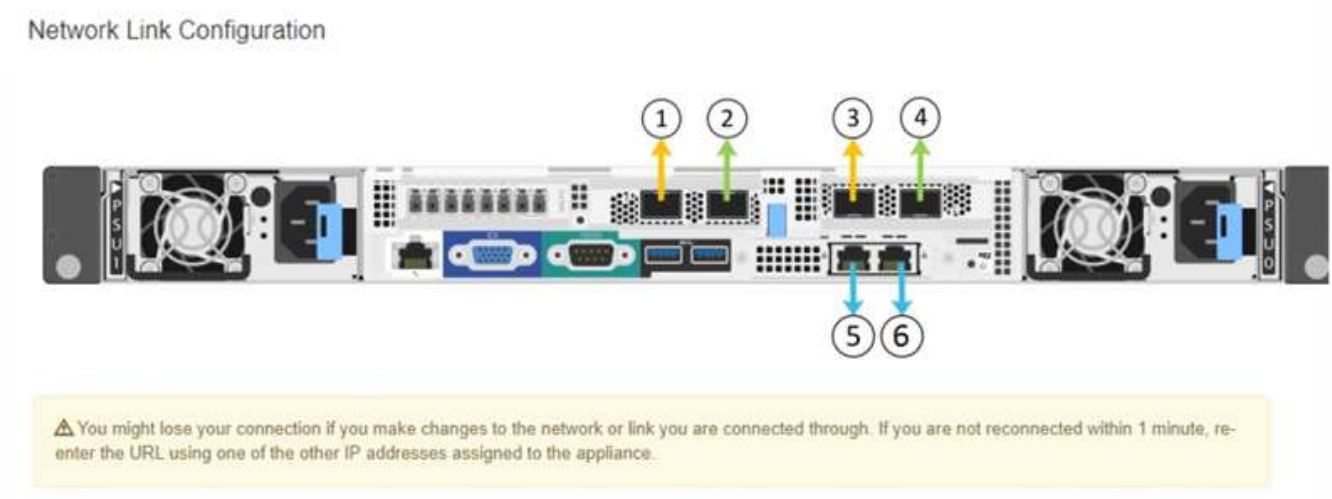
请参见 SG6000-CN 控制器的端口绑定模式 有关端口绑定和网络绑定模式的详细信息。

此图显示了 SG6000-CN 控制器上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。

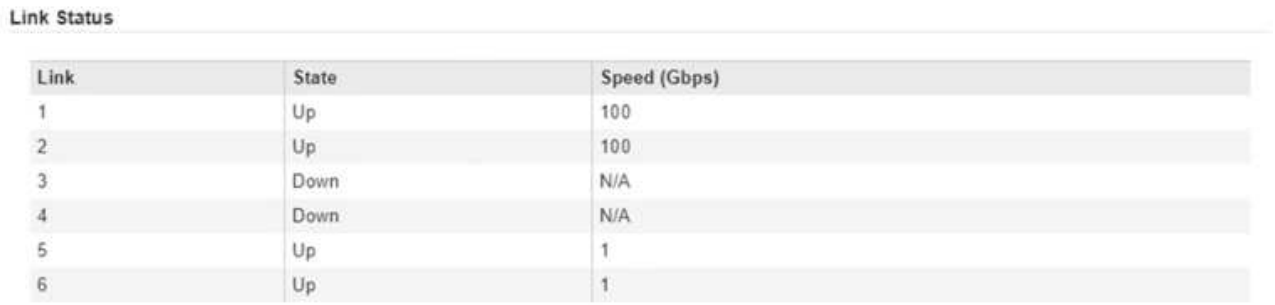
步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 链路配置 * 。

   " 网络链路配置 " 页面显示设备示意图，其中包含编号为的网络和管理端口。



   链路状态表列出了已编号端口的链路状态（启动 / 关闭）和速度（ 1/25/40/100 Gbps ）。

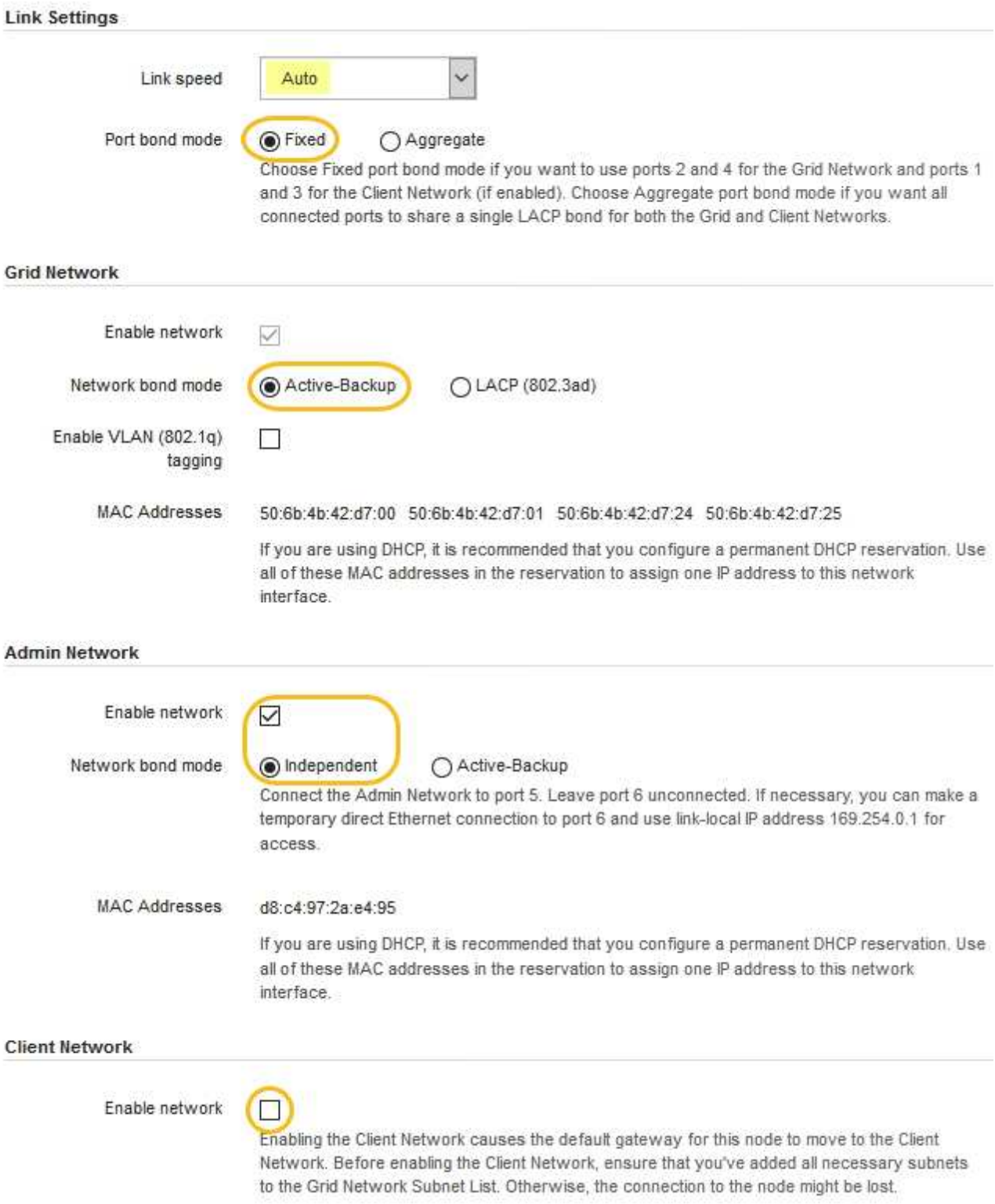


Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Up	100
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

   首次访问此页面时：

- * 链路速度 * 设置为 * 自动 * 。
- * 端口绑定模式 * 设置为 * 固定 * 。
- 对于网格网络， * 网络绑定模式 * 设置为 * 主动备份 * 。
- 此时将启用 * 管理网络 * ，并将网络绑定模式设置为 * 独立 * 。
- 已禁用 * 客户端网络 * 。



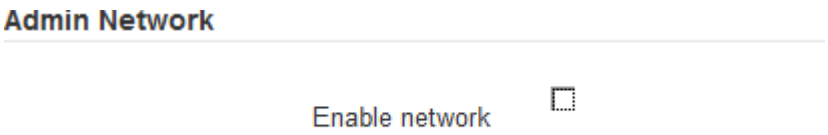
2. 如果您计划对网络端口使用 25 GbE 链路速度，请从链路速度下拉列表中选择 * 自动 * 。

   您用于网格网络和客户端网络的网络交换机也必须支持此速度并为此速度进行配置。您必须使用 SFP28 双轴缆线或光缆和 SFP28 收发器。

3. 启用或禁用计划使用的 StorageGRID 网络。

   网格网络为必填项。您不能禁用此网络。

   a. 如果设备未连接到管理网络，请取消选中管理网络的 * 启用网络 * 复选框。

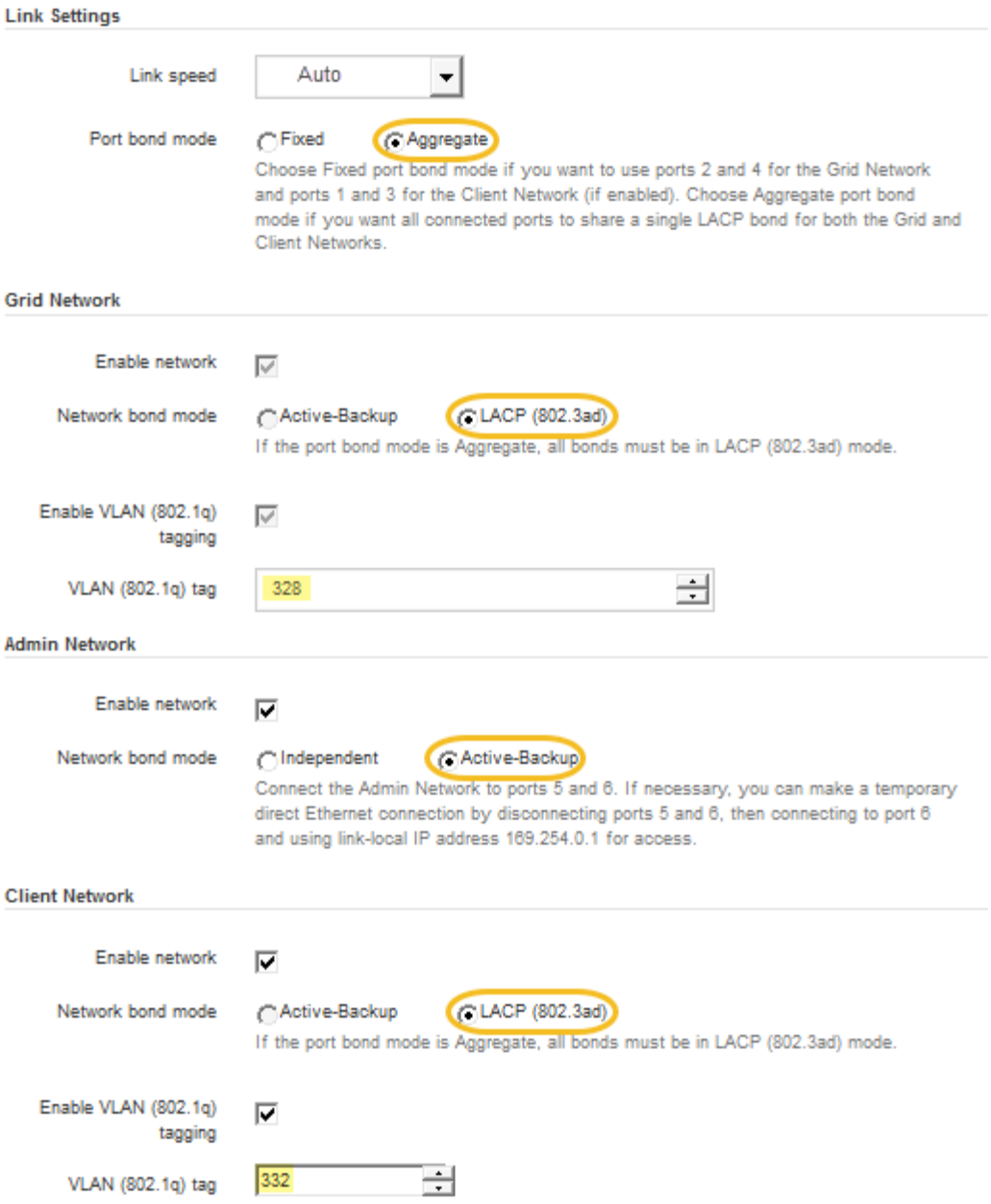
   b. 如果设备已连接到客户端网络，请选中客户端网络的 * 启用网络 * 复选框。

      此时将显示网络端口的客户端网络设置。

4. 请参见表，并配置端口绑定模式和网络绑定模式。

   此示例显示：

   - 为网格和客户端网络选择了 * 聚合 * 和 * LACP * 。您必须为每个网络指定唯一的 VLAN 标记。您可以选择 0 到 4095 之间的值。
   - 已为管理网络选择 * 主动备份 * 。



5. 对所做的选择感到满意后，单击 * 保存 * 。

> 如果更改了所连接的网络或链路，则可能会断开连接。如果您未在 1 分钟内重新连接，请使用其他 URL 之一重新输入 StorageGRID 设备安装程序的 URL IP 地址 已分配给设备： `* https://*SG6000-CN_Controller_IP*:8443*`

配置 **StorageGRID IP** 地址

您可以使用 StorageGRID 设备安装程序在 StorageGRID 网格，管理和客户端网络上配置设备存储节点所使用的 IP 地址和路由信息。

关于此任务

您必须为每个已连接网络上的设备分配一个静态 IP ，或者为 DHCP 服务器上的地址分配一个永久租约。

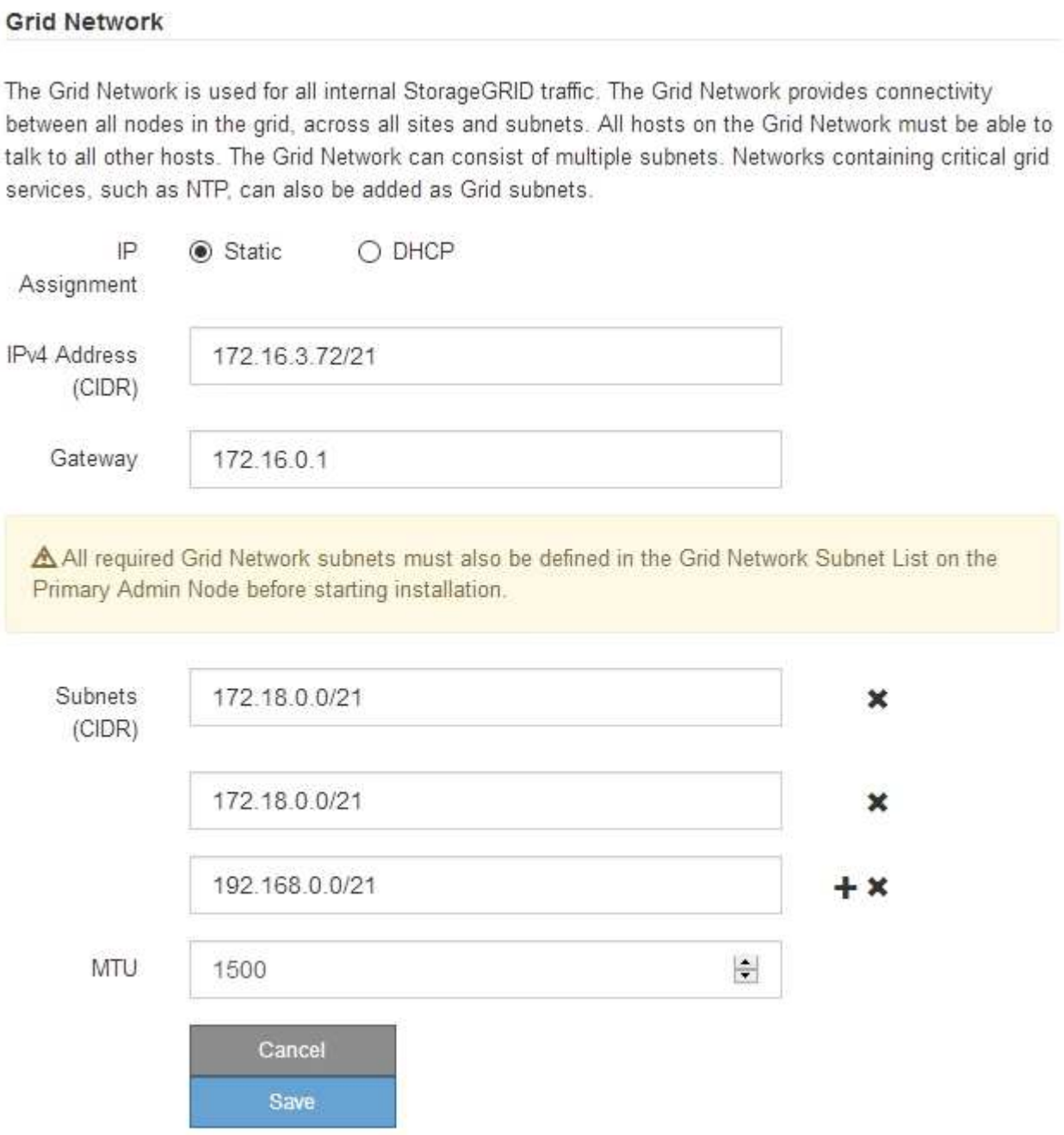
如果要更改链路配置，请参见 有关更改 SG6000-CN 控制器的链路配置的说明。

步骤

1. 在 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。

   此时将显示 "IP Configuration" 页面。

2. 要配置网格网络，请在页面的 * 网格网络 * 部分中选择 * 静态 * 或 * DHCP * 。



3. 如果选择 * 静态 * ，请按照以下步骤配置网格网络：

   a. 使用 CIDR 表示法输入静态 IPv4 地址。

   b. 输入网关。

如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

> 为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

d. 单击 * 保存 * 。

更改 IP 地址时，网关和子网列表可能也会发生更改。

如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance_IP*:8443*`

e. 确认网格网络子网列表正确无误。

如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

> 未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

4. 如果选择了 * DHCP * ，请按照以下步骤配置网格网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认网格网络子网列表正确无误。

如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

> 未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500

。

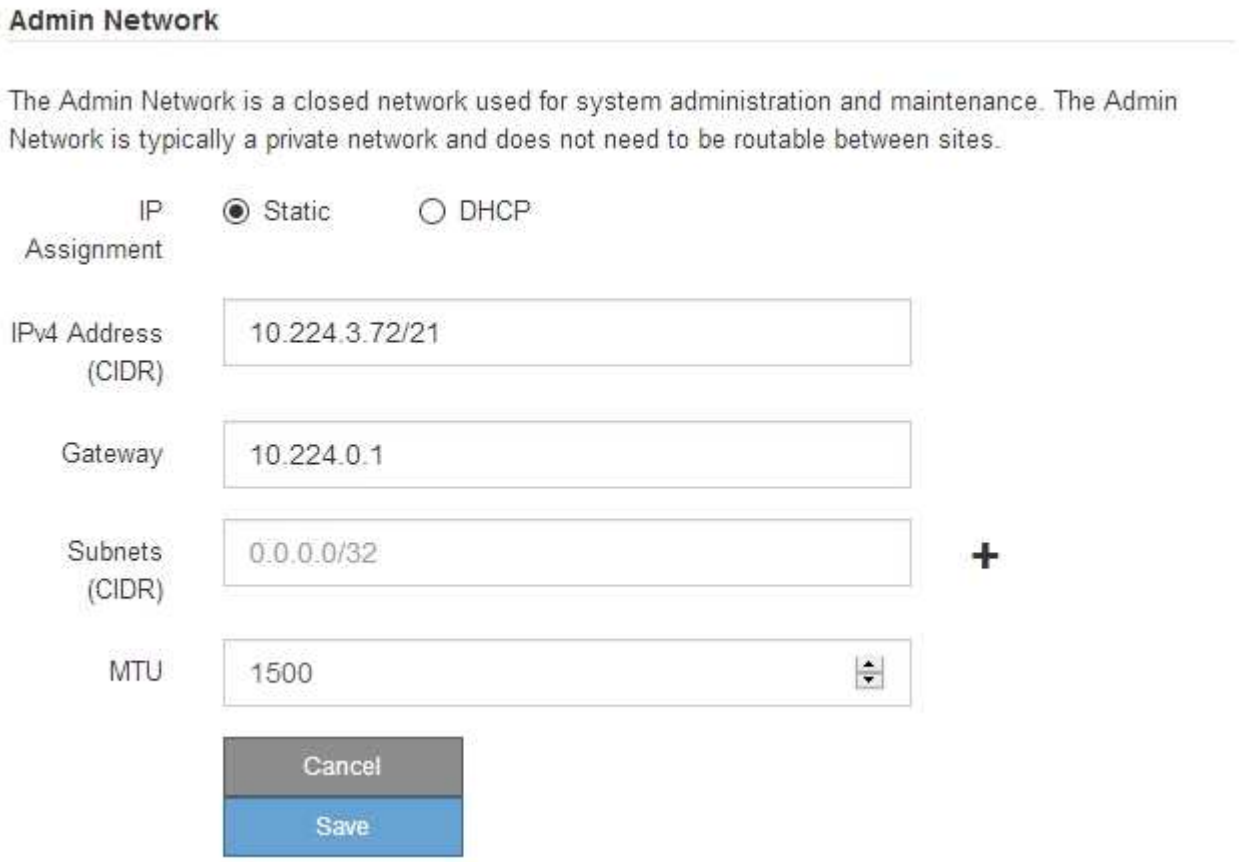
网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

a. 单击 * 保存 * 。

5. 要配置管理网络，请在页面的 * 管理网络 * 部分中选择 * 静态 * 或 * DHCP * 。

要配置管理网络，必须在链路配置页面上启用管理网络。



6. 如果选择 * 静态 * ，请按照以下步骤配置管理网络：

a. 使用 CIDR 表示法为设备上的管理端口 1 输入静态 IPv4 地址。

管理端口 1 位于设备右端的两个 1-GbE RJ45 端口的左侧。

b. 输入网关。

如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

更改 IP 地址时，网关和子网列表可能也会发生更改。

如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance*:8443*`

e. 确认管理网络子网列表正确无误。

您必须验证是否可以使用提供的网关访问所有子网。

> 无法使用默认路由来使用管理网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

7. 如果选择了 * DHCP * ，请按照以下步骤配置管理网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认管理网络子网列表正确无误。

您必须验证是否可以使用提供的网关访问所有子网。

> 无法使用默认路由来使用管理网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

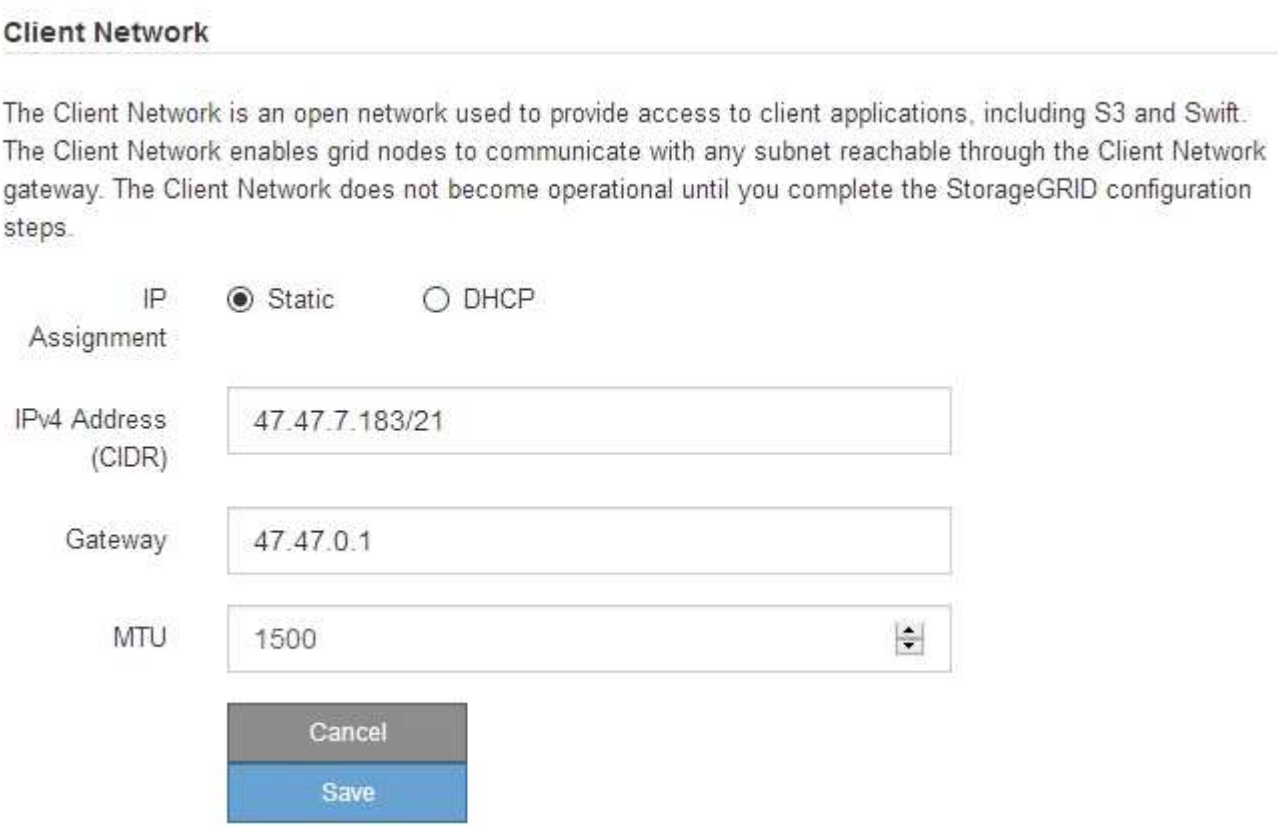
c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

8. 要配置客户端网络，请在页面的 * 客户端网络 * 部分中选择 * 静态 * 或 * DHCP * 。

要配置客户端网络，必须在链路配置页面上启用客户端网络。



9. 如果选择 * 静态 * ，请按照以下步骤配置客户端网络：
   a. 使用 CIDR 表示法输入静态 IPv4 地址。
   b. 单击 * 保存 * 。
   c. 确认客户端网络网关的 IP 地址正确无误。

      如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

   d. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

      网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

   e. 单击 * 保存 * 。
10. 如果选择了 * DHCP * ，请按照以下步骤配置客户端网络：
    a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

       系统会自动填充 * IPv4 地址 * 和 * 网关 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

a. 确认网关是否正确。

> 如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

b. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

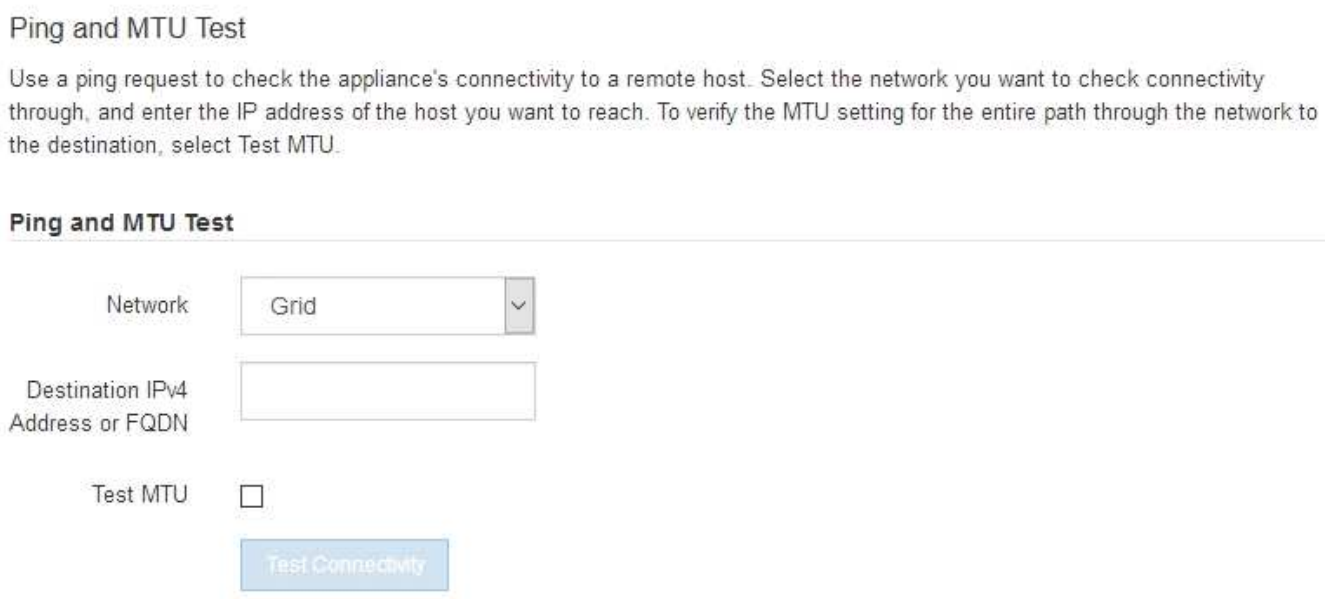
验证网络连接

您应确认可以从设备访问所使用的 StorageGRID 网络。要验证通过网络网关的路由，您应测试 StorageGRID 设备安装程序与不同子网上的 IP 地址之间的连接。您还可以验证 MTU 设置。

步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * Ping 和 MTU 测试 * 。

   此时将显示 Ping 和 MTU 测试页面。



2. 从 * 网络 * 下拉框中，选择要测试的网络：网格，管理员或客户端。
3. 输入该网络上某个主机的 IPv4 地址或完全限定域名（ FQDN ）。

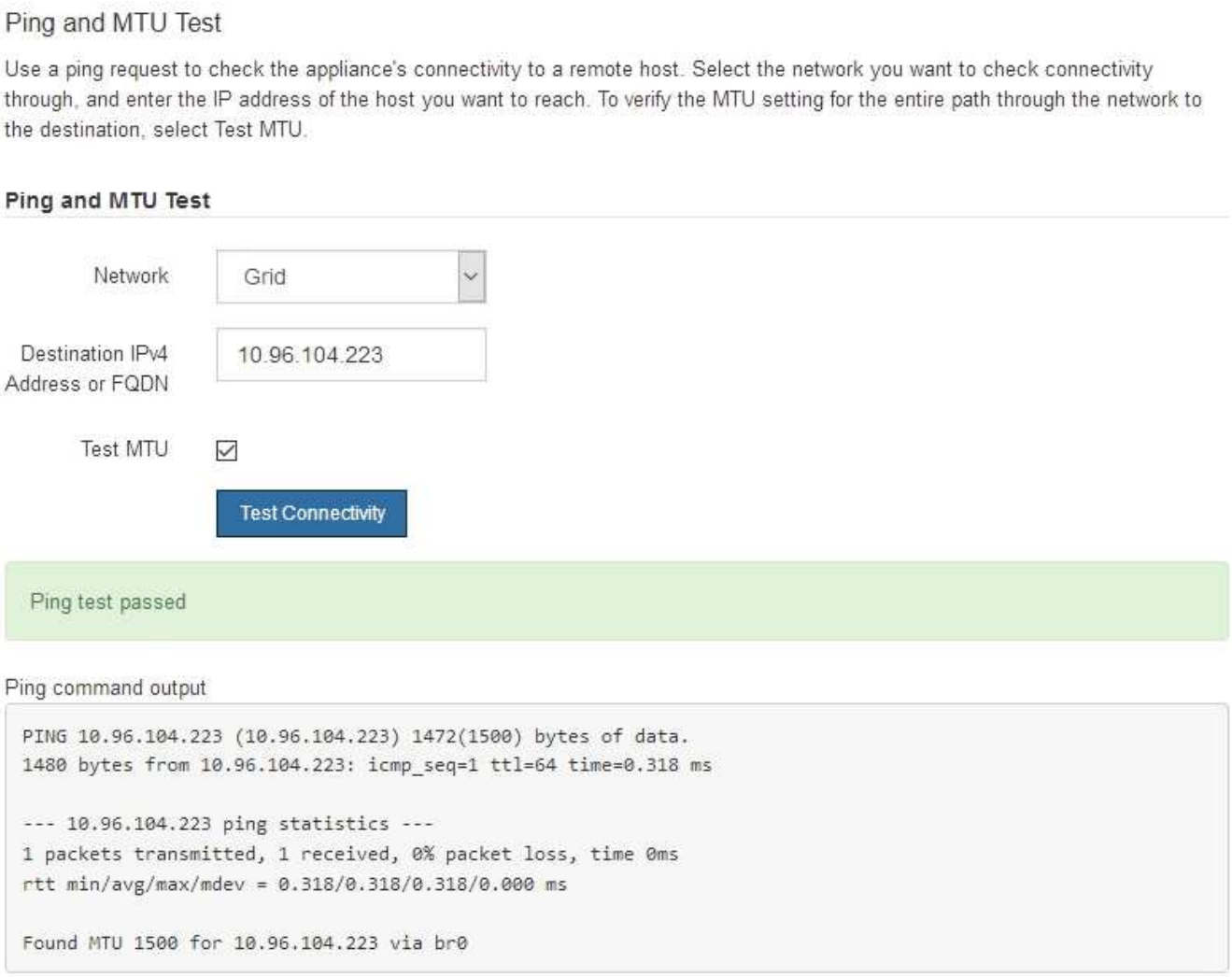
   例如，您可能需要对网络或主管理节点上的网关执行 ping 操作。

4. 或者，选中 * 测试 MTU* 复选框以验证通过网络到目标的整个路径的 MTU 设置。

   例如，您可以测试设备节点与其他站点的节点之间的路径。

5. 单击 * 测试连接 * 。

   如果网络连接有效，则会显示 "Ping test passed" 消息，并列出 ping 命令输出。



相关信息

配置网络链路（ SG6000 ）

更改 MTU 设置

验证端口级别的网络连接

要确保 StorageGRID 设备安装程序与其他节点之间的访问不会受到防火墙的阻碍，请确认 StorageGRID 设备安装程序可以连接到指定 IP 地址或地址范围内的特定 TCP 端口或端口集。

关于此任务

使用 StorageGRID 设备安装程序中提供的端口列表，您可以测试设备与网格网络中其他节点之间的连接。

此外，您还可以在管理和客户端网络以及 UDP 端口上测试连接，例如用于外部 NFS 或 DNS 服务器的端口。有关这些端口的列表，请参见 StorageGRID 网络连接准则中的端口参考。

端口连接表中列出的网格网络端口仅适用于 StorageGRID 11.6.0 版。要验证每种节点类型的端口是否正确，您应始终参考适用于您的 StorageGRID 版本的网络连接准则。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 端口连接测试（ nmap ） * 。

   此时将显示端口连接测试页面。

   端口连接表列出了网格网络上需要 TCP 连接的节点类型。对于每种节点类型，此表列出了设备应可访问的网格网络端口。

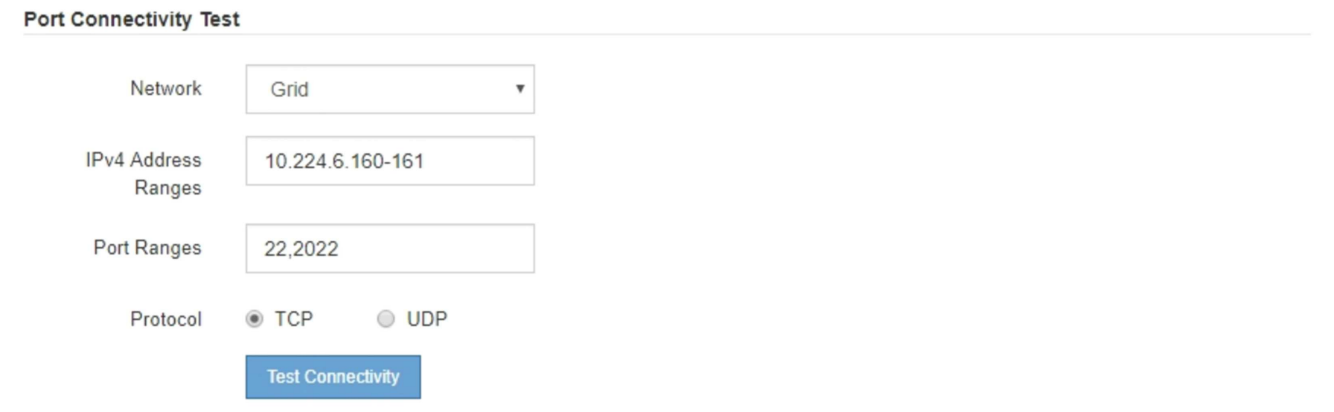
   您可以测试表中列出的设备端口与网格网络中的其他节点之间的连接。

2. 从 * 网络 * 下拉列表中，选择要测试的网络： * 网格 * ， * 管理 * 或 * 客户端 * 。
3. 为该网络上的主机指定一个 IPv4 地址范围。

   例如，您可能需要探测网络或主管理节点上的网关。

   使用连字符指定一个范围，如示例所示。

4. 输入 TCP 端口号，以逗号分隔的端口列表或端口范围。



5. 单击 * 测试连接 * 。

   ◦ 如果选定的端口级别网络连接有效，则绿色横幅中会显示 "`Port connectivity test passed` " 消息。nmap 命令输出列在横幅下方。

- 如果与远程主机建立了端口级网络连接，但主机未侦听一个或多个选定端口，则黄色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  主机未侦听的任何远程端口的状态为 "`closed" 。` 例如，当您尝试连接的节点处于预安装状态且 StorageGRID NMS 服务尚未在该节点上运行时，您可能会看到此黄色横幅。

- 如果无法为一个或多个选定端口建立端口级别网络连接，则红色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  红色横幅表示已尝试通过 TCP 连接到远程主机上的某个端口，但未向发送方返回任何内容。如果未返回任何响应，则此端口的状态为 " 已筛选 " ，并且可能会被防火墙阻止。

  此外，还会列出带有 "`closed` " 的端口。

相关信息

网络连接准则

访问和配置 **SANtricity System Manager** （ **SG6000** ）

您可以使用 SANtricity 系统管理器监控存储控制器，存储磁盘和存储控制器架中其他硬件组件的状态。此外，您还可以为 E 系列 AutoSupport 配置代理，使您能够在不使用管理端口的情况下从设备发送 AutoSupport 消息。

设置并访问 **SANtricity** 系统管理器

您可能需要访问存储控制器上的 SANtricity 系统管理器来监控存储控制器架中的硬件或配置 E 系列 AutoSupport 。

您需要的内容

- 您正在使用 支持的 Web 浏览器。
- 要通过网格管理器访问 SANtricity 系统管理器，您必须已安装 StorageGRID ，并且必须具有存储设备管理员权限或根访问权限。
- 要使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器，您必须具有 SANtricity 系统管理器管理员用户名和密码。
- 要使用 Web 浏览器直接访问 SANtricity System Manager ，您必须具有 SANtricity System Manager 管理员用户名和密码。

> 您必须具有SANtricity 固件8.70 (11.70)或更高版本、才能使用网格管理器或StorageGRID 设备安装程序访问SANtricity 系统管理器。您可以使用 StorageGRID 设备安装程序并选择 * 帮助 * > * 关于 * 来检查固件版本。

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

关于此任务

根据您所处的安装和配置过程的阶段，有三种方法可以访问 SANtricity System Manager ：

- 如果此设备尚未部署为 StorageGRID 系统中的节点，则应使用 StorageGRID 设备安装程序中的高级选项卡。

  部署节点后，您将无法再使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器。

- 如果此设备已部署为 StorageGRID 系统中的节点，请使用网格管理器中节点页面上的 SANtricity 系统管理器选项卡。
- 如果无法使用 StorageGRID 设备安装程序或网格管理器，则可以使用连接到管理端口的 Web 浏览器直接访问 SANtricity 系统管理器。

此操作步骤 包含首次访问 SANtricity System Manager 的步骤。如果您已设置 SANtricity 系统管理器，请转到配置硬件警报步骤。

使用网格管理器或 StorageGRID 设备安装程序，您可以访问 SANtricity 系统管理器，而无需配置或连接设备的管理端口。

您可以使用 SANtricity 系统管理器监控以下内容：

- 存储阵列级别性能， I/O 延迟， CPU 利用率和吞吐量等性能数据
- 硬件组件状态
- 支持的功能包括查看诊断数据

您可以使用 SANtricity 系统管理器配置以下设置：

- 存储控制器架中组件的电子邮件警报， SNMP 警报或系统日志警报
- 存储控制器架中组件的 E 系列 AutoSupport 设置。

  有关 E 系列 AutoSupport 的更多详细信息，请参见 "NetApp E 系列系统文档站点"。

- 驱动器安全密钥，用于解锁安全驱动器（如果启用了驱动器安全功能，则需要执行此步骤）
- 用于访问 SANtricity 系统管理器的管理员密码

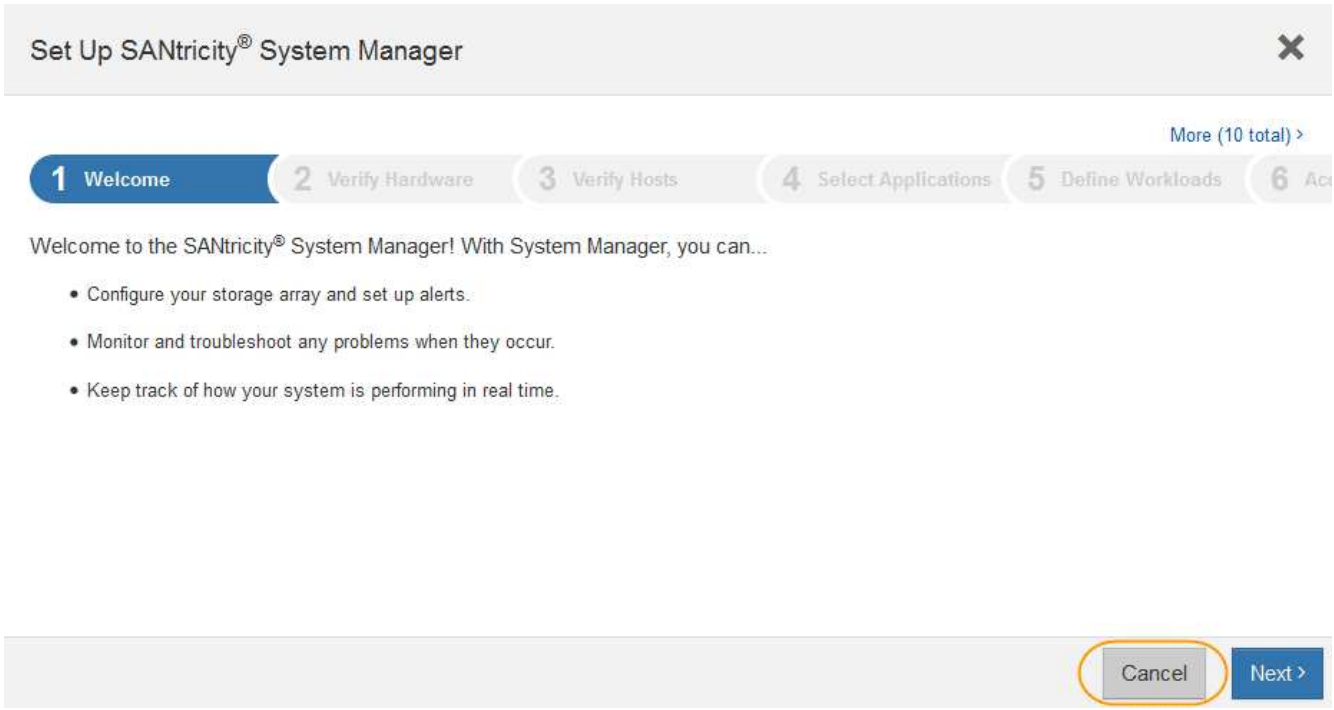
步骤

1. 使用 StorageGRID 设备安装程序并选择 * 高级 * > * SANtricity 系统管理器 *

   如果StorageGRID 设备安装程序不可用或未显示登录页面、则必须使用 存储控制器的 IP 地址。浏览到存储控制器 IP 以访问 SANtricity System Manager 。

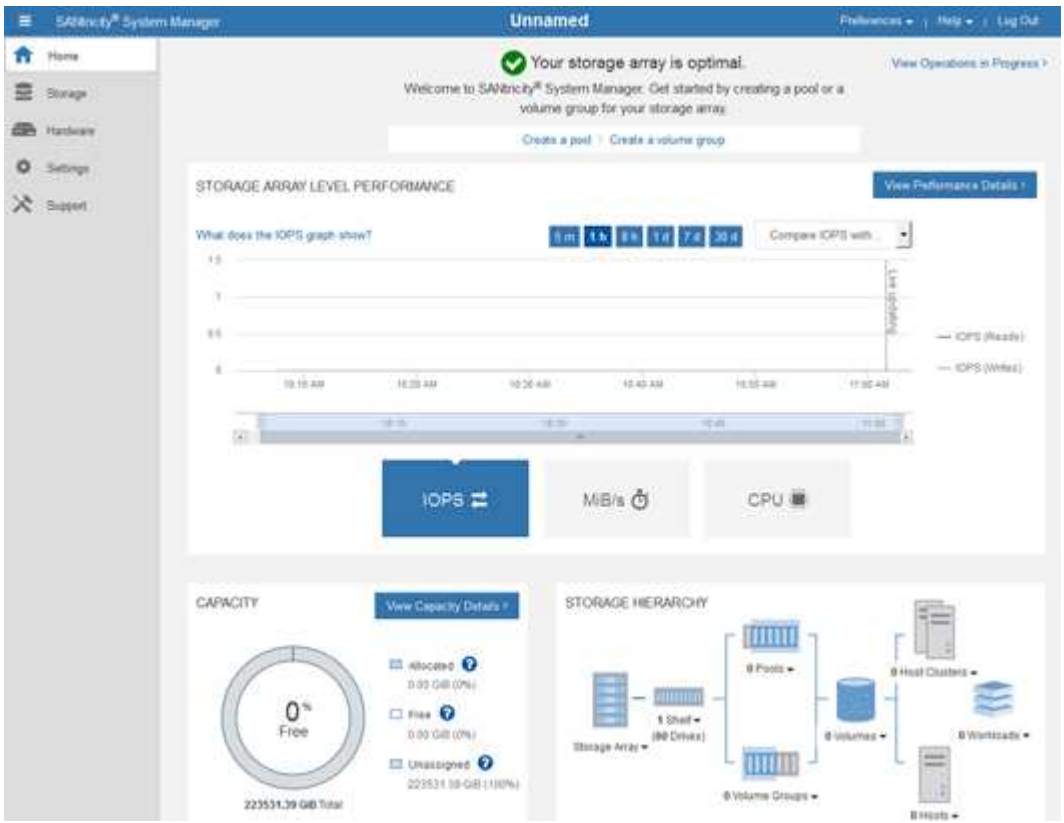
2. 设置或输入管理员密码。

SANtricity 系统管理器使用一个管理员密码，该密码在所有用户之间共享。



3. 选择 * 取消 * 以关闭向导。

请勿完成 StorageGRID 设备的设置向导。



4. 【 config_hardware_alerts_sg6000 ， start=4]] 配置硬件警报。

a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
b. 使用联机帮助的 * 设置 * > * 警报 * 部分了解警报。
c. 按照 "`如何` " 说明设置电子邮件警报， SNMP 警报或系统日志警报。

5. 管理存储控制器架中组件的 AutoSupport 。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 支持 * > * 支持中心 * 部分了解 AutoSupport 功能。
   c. 按照 "`如何` " 说明管理 AutoSupport 。

      有关配置 StorageGRID 代理以在不使用管理端口的情况下发送 E 系列 AutoSupport 消息的具体说明，请转至 有关配置存储代理设置的说明。

6. 如果为设备启用了驱动器安全功能，请创建并管理安全密钥。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 设置 * > * 系统 * > * 安全密钥管理 * 部分了解驱动器安全性。
   c. 按照 "`如何` " 说明创建和管理安全密钥。
7. 也可以更改管理员密码。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 主页 * > * 存储阵列管理 * 部分了解管理员密码。
   c. 按照 "`如何` " 说明更改密码。

在 **SANtricity System Manager** 中查看硬件状态

您可以使用 SANtricity 系统管理器监控和管理存储控制器架中的各个硬件组件，并查看硬件诊断和环境信息，例如组件温度以及与驱动器相关的问题。

您需要的内容

- 您正在使用 支持的 Web 浏览器。
- 要通过网格管理器访问 SANtricity 系统管理器，您必须具有存储设备管理员权限或 root 访问权限。
- 要使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器，您必须具有 SANtricity 系统管理器管理员用户名和密码。
- 要使用 Web 浏览器直接访问 SANtricity System Manager ，您必须具有 SANtricity System Manager 管理员用户名和密码。

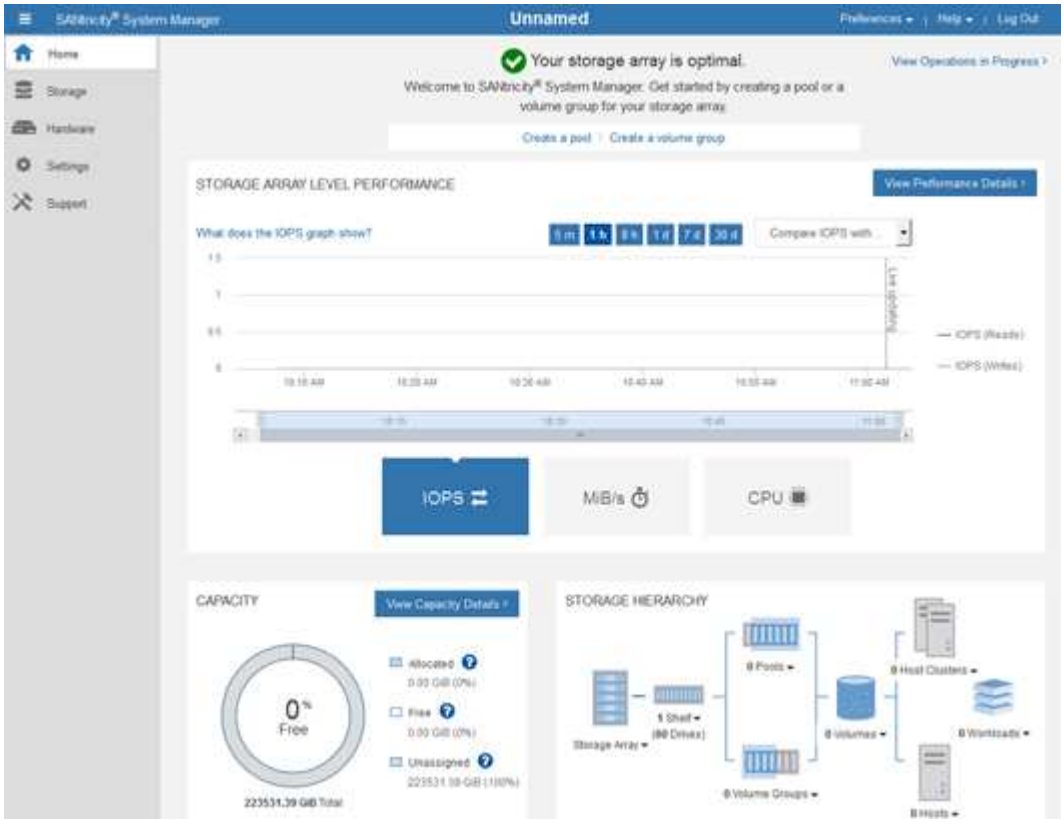
> 您必须具有SANtricity 固件8.70 (11.70)或更高版本、才能使用网格管理器或StorageGRID 设备安装程序访问SANtricity 系统管理器。

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

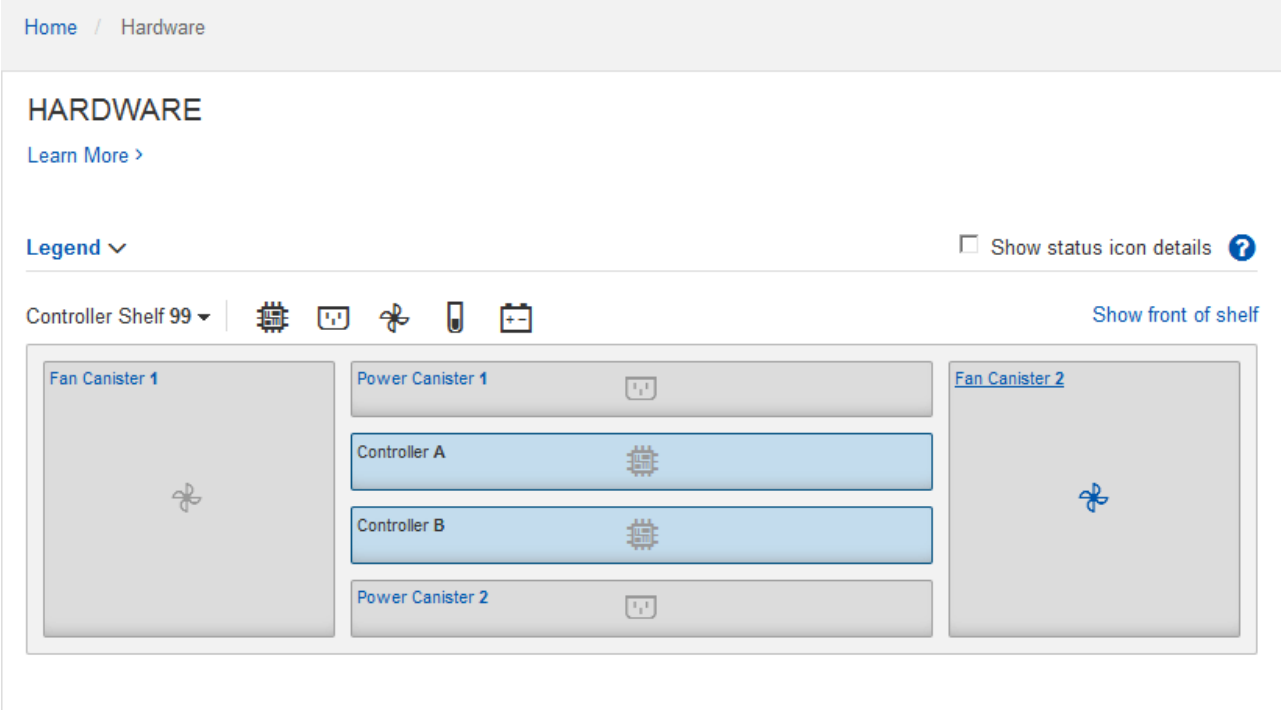
步骤

1. 访问 SANtricity 系统管理器。
2. 如果需要，请输入管理员用户名和密码。
3. 单击 * 取消 * 以关闭设置向导并显示 SANtricity 系统管理器主页。

   此时将显示 SANtricity System Manager 主页。在 SANtricity 系统管理器中，控制器架称为存储阵列。



4. 查看显示的设备硬件信息，并确认所有硬件组件的状态均为最佳。
   a. 单击 * 硬件 * 选项卡。
   b. 单击 * 显示磁盘架的背面 * 。



从磁盘架背面，您可以查看两个存储控制器，每个存储控制器中的电池，两个电源箱，两个风扇箱和扩展架（如果有）。您还可以查看组件温度。

a. 要查看每个存储控制器的设置，请选择控制器，然后从上下文菜单中选择 * 查看设置 * 。
b. 要查看磁盘架背面其他组件的设置，请选择要查看的组件。
c. 单击 * 显示磁盘架正面 * ，然后选择要查看的组件。

   从磁盘架正面，您可以查看存储控制器磁盘架或扩展磁盘架（如果有）的驱动器和驱动器抽盒。

如果需要关注任何组件的状态，请按照 Recovery Guru 中的步骤解决问题描述 或联系技术支持。

使用 **StorageGRID** 设备安装程序设置存储控制器的 **IP** 地址

每个存储控制器上的管理端口 1 用于将设备连接到 SANtricity System Manager 的管理网络。如果无法从StorageGRID 设备安装程序访问SANtricity 系统管理器、则必须为每个存储控制器设置一个静态IP地址、以确保不会丢失与控制器架中的硬件和控制器固件的管理连接。

您需要的内容

- 您正在使用可以连接到 StorageGRID 管理网络的任何管理客户端，或者您使用的是服务笔记本电脑。
- 客户端或服务笔记本电脑具有受支持的 Web 浏览器。

关于此任务

DHCP 分配的地址可以随时更改。为控制器分配静态 IP 地址，以确保一致的可访问性。

只有当您无法从 StorageGRID 设备安装程序（ * 高级 * > * SANtricity 系统管理器 * ）或网格管理器（ * 节点 * > * SANtricity 系统管理器 * ）访问 SANtricity 系统管理器时，才应遵循此操作步骤。

步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*Appliance_Controller_IP*:8443*`

   对于 ` 设备控制器 IP` ，请在任何 StorageGRID 网络上使用设备的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 存储控制器网络配置 * 。

   此时将显示存储控制器网络配置页面。

3. 根据您的网络配置，对于 IPv4 ， IPv6 或这两者，请选择 * 已启用 * 。
4. 记下自动显示的 IPv4 地址。

   DHCP 是为存储控制器管理端口分配 IP 地址的默认方法。

   显示 DHCP 值可能需要几分钟的时间。

5. （可选）设置存储控制器管理端口的静态 IP 地址。

   您应该为管理端口分配静态 IP ，或者为 DHCP 服务器上的地址分配永久租约。

   a. 选择 * 静态 * 。
   b. 使用 CIDR 表示法输入 IPv4 地址。
   c. 输入默认网关。

   d. 单击 * 保存 * 。

      应用所做的更改可能需要几分钟的时间。

连接到 SANtricity 系统管理器时，您将使用新的静态 IP 地址作为 URL： + ` * https://*Storage_Controller_IP*`

配置 **BMC** 接口（ **SG6000** ）

SG6000-CN 控制器上的基板管理控制器（ Baseboard Management Controller ， BMC ）的用户界面提供了有关硬件的状态信息，并允许您为 SG6000-CN 控制器配置 SNMP 设置和其他选项。

更改 **BMC** 接口的根密码

为了安全起见，您必须更改 BMC root 用户的密码。

您需要的内容

- 管理客户端正在使用 支持的 Web 浏览器。

关于此任务

首次安装设备时， BMC 会使用 root 用户的默认密码（`root/calvin`）。您必须更改 root 用户的密码以保护您的系统。

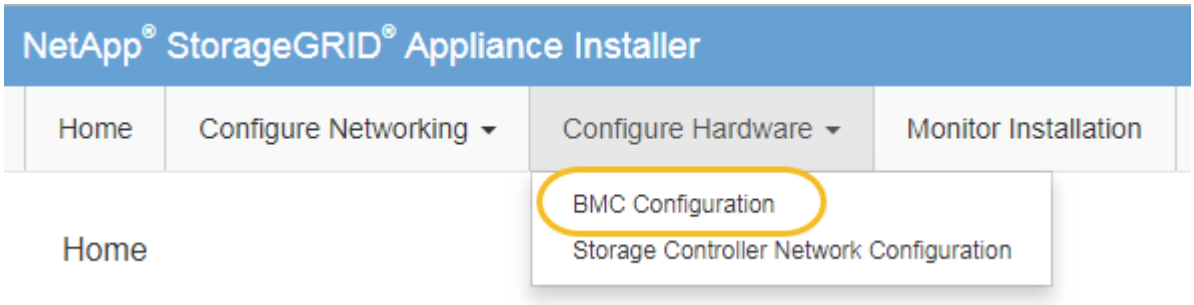
步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*Appliance_Controller_IP*:8443*`

   对于 ` 设备控制器 IP` ，请在任何 StorageGRID 网络上使用设备的 IP 地址。

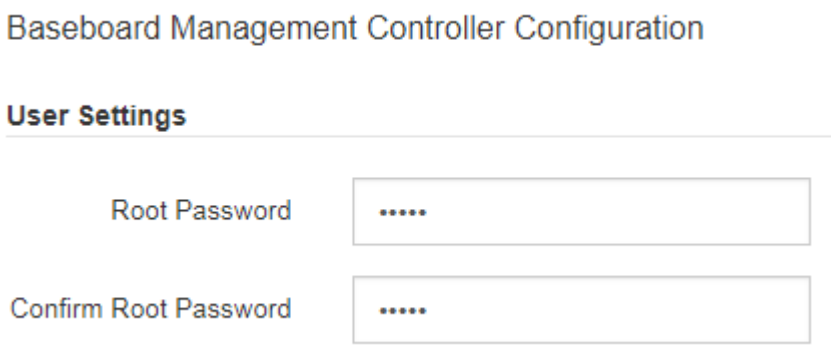
   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * BMC 配置 * 。



   此时将显示 Baseboard Management Controller Configuration 页面。

3. 在提供的两个字段中输入 root 帐户的新密码。



4. 单击 * 保存 * 。

设置 **BMC** 管理端口的 **IP** 地址

在访问 BMC 接口之前，您必须为 SG6000-CN 控制器上的 BMC 管理端口配置 IP 地址。

您需要的内容

- 管理客户端正在使用 支持的 Web 浏览器。
- 您正在使用可连接到 StorageGRID 网络的任何管理客户端。
- BMC 管理端口将连接到您计划使用的管理网络。

关于此任务

出于支持目的， BMC 管理端口允许进行低级硬件访问。

您只能将此端口连接到安全，可信的内部管理网络。如果没有此类网络可用，请保持 BMC 端口未连接或被阻止，除非技术支持请求 BMC 连接。

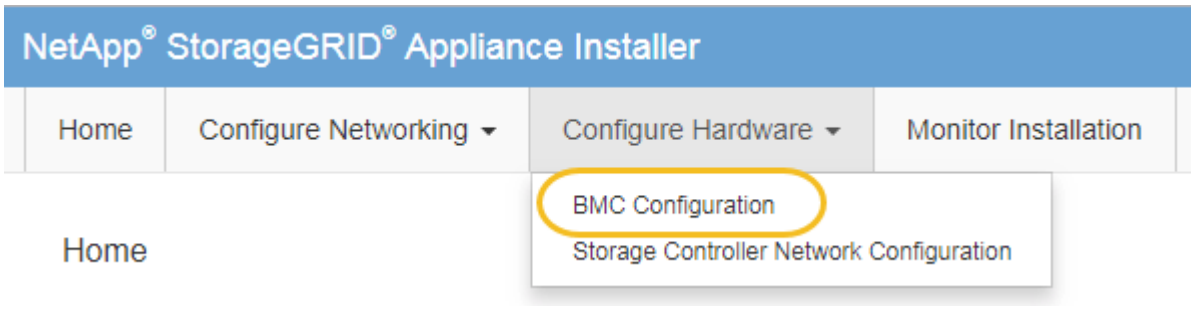
步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*SG6000-CN_Controller_IP*:8443*`

   对于 `s 6000-CN_Controller_IP` ，请在任何 StorageGRID 网络上使用设备的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * BMC 配置 * 。

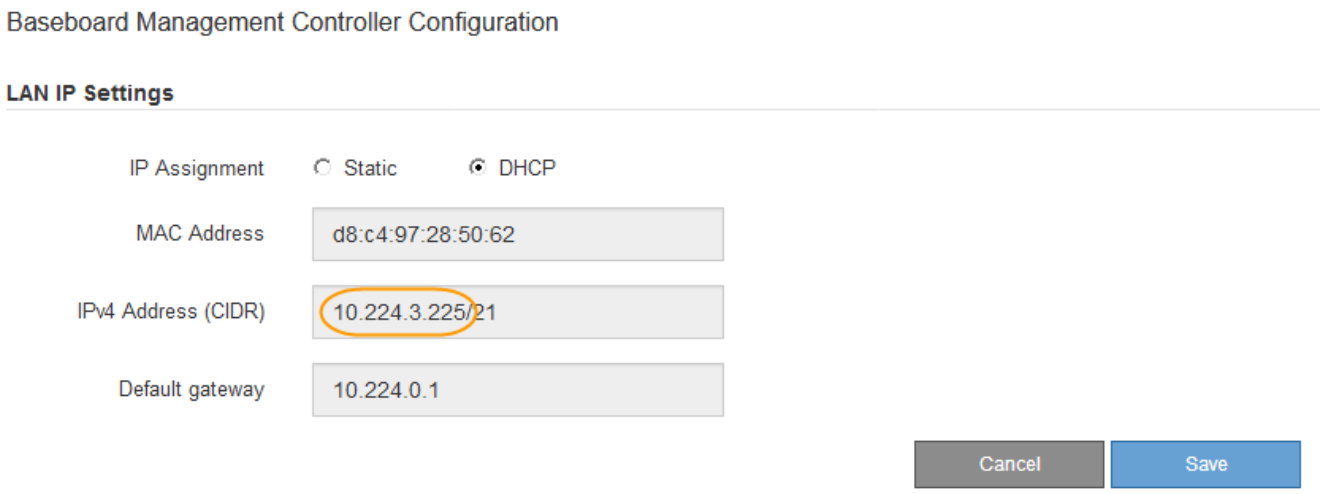


   此时将显示 Baseboard Management Controller Configuration 页面。

3. 记下自动显示的 IPv4 地址。

   DHCP 是为该端口分配 IP 地址的默认方法。

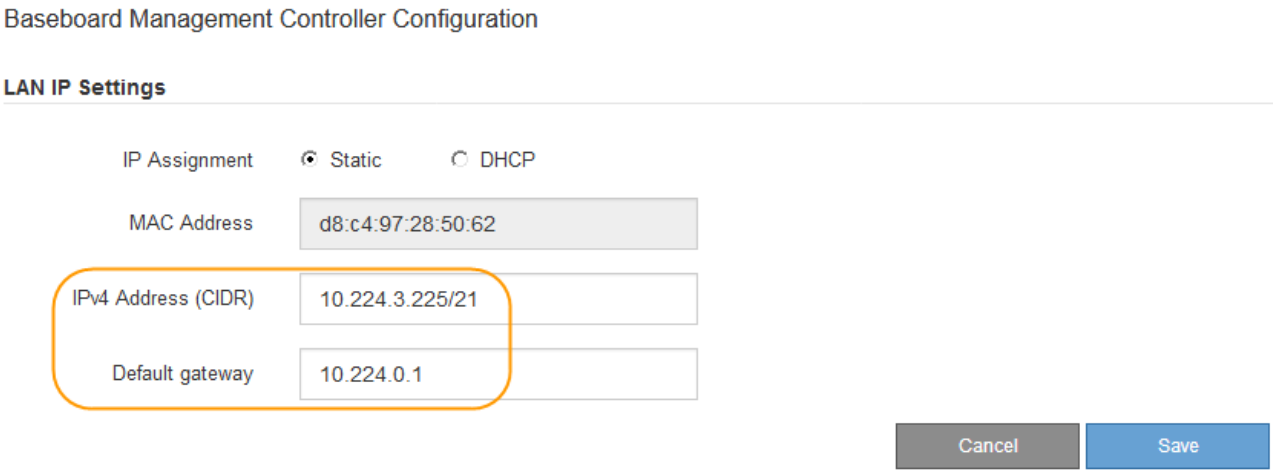
   显示 DHCP 值可能需要几分钟的时间。



4. 也可以为 BMC 管理端口设置静态 IP 地址。

   您应该为 BMC 管理端口分配静态 IP ，或者为 DHCP 服务器上的地址分配永久租约。

   a. 选择 * 静态 * 。
   b. 使用 CIDR 表示法输入 IPv4 地址。
   c. 输入默认网关。



   d. 单击 * 保存 * 。

      应用所做的更改可能需要几分钟的时间。

访问 **BMC** 界面

您可以使用 BMC 管理端口的 DHCP 或静态 IP 地址访问 SG6000-CN 控制器上的 BMC 接口。

您需要的内容

- SG6000-CN 控制器上的 BMC 管理端口将连接到您计划使用的管理网络。

- 管理客户端正在使用 支持的 Web 浏览器。

步骤

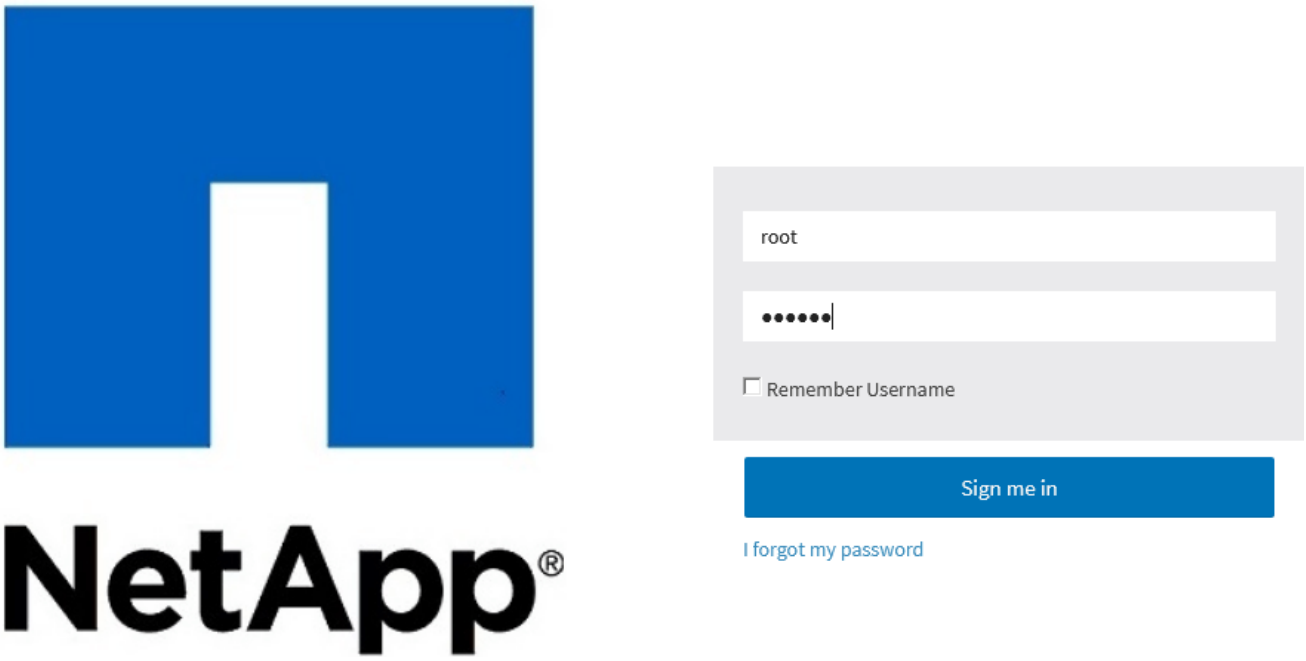
1. 输入 BMC 接口的 URL： + ` * https://*BMC_Port_IP*`*

   对于 ` BMC_Port_IP_` ，请使用 DHCP 或静态 IP 地址作为 BMC 管理端口。

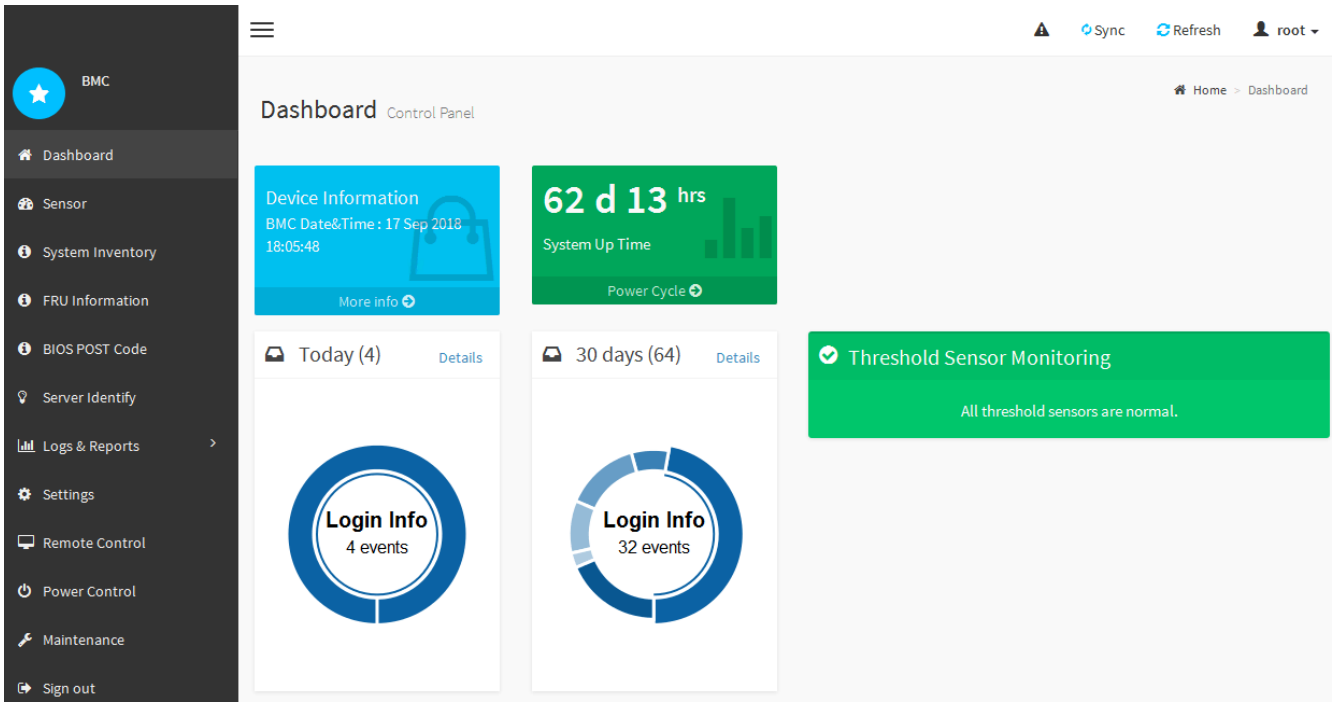
   此时将显示 BMC 登录页面。

   > 如果尚未配置 `BMC_Port_IP` ，请按照中的说明进行操作 配置 BMC 接口（ SG6000 ）。如果由于硬件问题而无法遵循此操作步骤，并且尚未配置 BMC IP 地址，则仍可访问此 BMC 。默认情况下， BMC 使用 DHCP 获取 IP 地址。如果在 BMC 网络上启用了 DHCP ，则网络管理员可以提供分配给 BMC MAC 的 IP 地址，该地址印在 SG6000-CN 控制器正面的标签上。如果 BMC 网络上未启用 DHCP ， BMC 将在几分钟后不会做出响应，并为自己分配默认静态 IP `192.168.0.120` 。您可能需要将笔记本电脑直接连接到 BMC 端口，并更改网络设置以为笔记本电脑分配 IP ，例如 `192.168.0.200/24` ，以便浏览到 `192.168.0.120` 。

2. 使用您在时设置的密码输入 root 用户名和密码 已更改默认根密码：



3. 选择 * 登录 * 。



4. 或者，也可以选择 * 设置 * > * 用户管理 * 并单击任何 " 已 d " 用户来创建其他用户。

当用户首次登录时，系统可能会提示他们更改密码以提高安全性。

为 **SG6000-CN** 控制器配置 **SNMP** 设置

如果您熟悉为硬件配置 SNMP ，则可以使用 BMC 界面为 SG6000-CN 控制器配置 SNMP 设置。您可以提供安全社区字符串，启用 SNMP 陷阱并最多指定五个 SNMP 目标。

您需要的内容

- 您知道如何访问 BMC 信息板。
- 您在为 SNMPv1-v2c 设备配置 SNMP 设置方面具有经验。

如果 SG6000-CN 发生故障且需要更换，则可能无法保留此操作步骤 所做的 BMC 设置。请确保您已应用所有设置，以便在更换硬件后根据需要轻松重新应用这些设置。

步骤

1. 从 BMC 信息板中，选择 * 设置 * > * SNMP 设置 * 。
2. 在 SNMP 设置页面上，选择 * 启用 SNMP V1/V2 * ，然后提供只读社区字符串和读写社区字符串。

   只读社区字符串类似于用户 ID 或密码。您应更改此值，以防止入侵者获取有关网络设置的信息。读写社区字符串可保护设备免受未经授权的更改。

3. （可选）选择 * 启用陷阱 * ，然后输入所需信息。

使用 IP 地址输入每个 SNMP 陷阱的目标 IP 。不支持完全限定域名。

如果希望 SG6000-CN 控制器在 SNMP 控制台处于异常状态时立即向其发送通知，请启用陷阱。陷阱可能

指示各种组件的硬件故障或超出温度阈值。

4. 或者，也可以单击 * 发送测试陷阱 * 来测试您的设置。
5. 如果设置正确，请单击 * 保存 * 。

为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，则必须使用 BMC 界面配置 SMTP 设置，用户， LAN 目标，警报策略和事件筛选器。

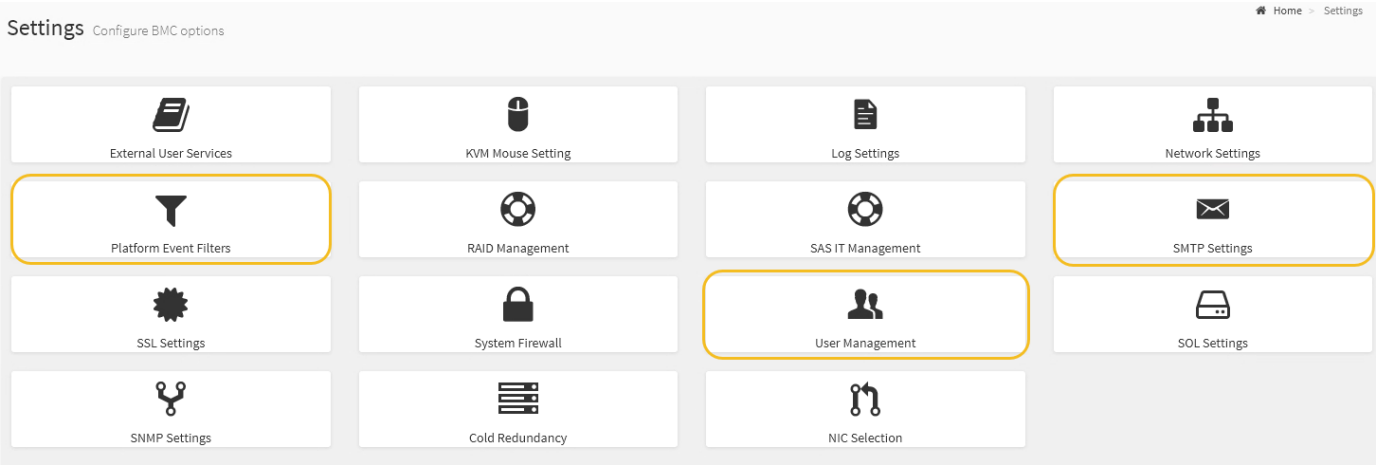
如果 SG6000-CN 发生故障且需要更换，则可能无法保留此操作步骤 所做的 BMC 设置。请确保您已应用所有设置，以便在更换硬件后根据需要轻松重新应用这些设置。

您需要的内容

您知道如何访问 BMC 信息板。

关于此任务

在 BMC 界面中，您可以使用设置页面上的 * SMTP 设置 * ， * 用户管理 * 和 * 平台事件筛选器 * 选项来配置电子邮件通知。



步骤

1. 配置 SMTP 设置。
   a. 选择 * 设置 * > * SMTP 设置 * 。
   b. 对于发件人电子邮件 ID ，请输入有效的电子邮件地址。

      此电子邮件地址在 BMC 发送电子邮件时作为发件人地址提供。
2. 设置用户以接收警报。
   a. 从 BMC 信息板中，选择 * 设置 * > * 用户管理 * 。
   b. 至少添加一个用户以接收警报通知。

      您为用户配置的电子邮件地址是 BMC 向其发送警报通知的地址。例如，您可以添加一个通用用户，例如 "`notification -user ，` " ，并使用技术支持团队 Email发送名单 的电子邮件地址。

3. 配置警报的 LAN 目标。
   a. 选择 * 设置 * > * 平台事件筛选器 * > * LAN 目标 * 。
   b. 至少配置一个 LAN 目标。
      - 选择 * 电子邮件 * 作为目标类型。
      - 对于 BMC 用户名，请选择先前添加的用户名。
      - 如果您添加了多个用户并希望所有用户都接收通知电子邮件，则必须为每个用户添加一个 LAN 目标。
   c. 发送测试警报。
4. 配置警报策略，以便定义 BMC 发送警报的时间和位置。
   a. 选择 * 设置 * > * 平台事件筛选器 * > * 警报策略 * 。
   b. 为每个 LAN 目标至少配置一个警报策略。
      - 对于策略组编号，请选择 * 。 1
      - 对于策略操作，选择 * 始终向此目标发送警报 * 。
      - 对于 LAN 通道，选择 * 1 * 。
      - 在目标选择器中，选择策略的 LAN 目标。
5. 配置事件筛选器以将不同事件类型的警报定向到相应的用户。
   a. 选择 * 设置 * > * 平台事件筛选器 * > * 事件筛选器 * 。
   b. 对于警报策略组编号，输入 * 1 * 。
   c. 为要通知警报策略组的每个事件创建筛选器。
      - 您可以为电源操作，特定传感器事件或所有事件创建事件筛选器。
      - 如果不确定要监控哪些事件，请选择 "Sensor Type" （传感器类型）为 "All 传感器 " （所有传感器） * ，并选择 "Event Options" （事件选项）为 "All Events" （所有事件）。如果收到不需要的通知，您可以稍后更改所做的选择。

可选：启用节点加密

如果启用了节点加密，则可以通过安全密钥管理服务器（ KMS ）加密来保护设备中的磁盘，防止物理丢失或从站点中删除。您必须在设备安装期间选择并启用节点加密，并且在 KMS 加密过程开始后，不能取消选择节点加密。

您需要的内容

查看有关管理 StorageGRID 的说明中有关 KMS 的信息。

关于此任务

启用了节点加密的设备将连接到为 StorageGRID 站点配置的外部密钥管理服务器（ KMS ）。每个 KMS （或 KMS 集群）负责管理站点上所有设备节点的加密密钥。这些密钥对启用了节点加密的设备中每个磁盘上的数据进行加密和解密。

可以在 StorageGRID 中安装 KMS 之前或之后在网格管理器中设置此设备。有关更多详细信息，请参见管理 StorageGRID 的说明中有关 KMS 和设备配置的信息。

- 如果在安装设备之前设置了 KMS ，则在设备上启用节点加密并将其添加到配置了 KMS 的 StorageGRID 站点时， KMS 控制的加密将开始。
- 如果在安装此设备之前未设置 KMS ，则在为包含此设备节点的站点配置了 KMS 并可使用此 KMS 后，将对启用了节点加密的每个设备执行 KMS 控制的加密。

> 在连接到启用了节点加密的设备上的 KMS 之前存在的数据将使用不安全的临时密钥进行加密。除非将密钥设置为 KMS 提供的值，否则设备不会受到删除或被盗的保护。

如果没有对磁盘进行解密所需的 KMS 密钥，则无法检索设备上的数据，并且数据实际上会丢失。如果无法从 KMS 中检索到解密密钥，则会出现这种情况。如果清除KMS配置、KMS密钥过期、与KMS的连接断开或从安装了KMS密钥的StorageGRID 系统中删除设备、则无法访问此密钥。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

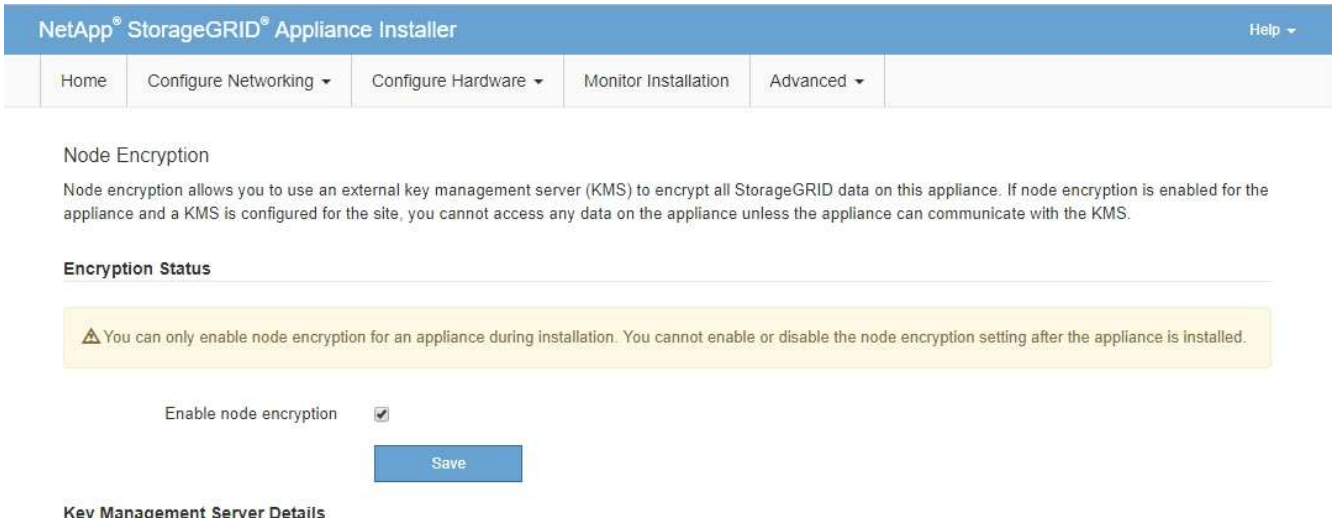
   ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

   > 使用 KMS 密钥对设备加密后，如果不使用相同的 KMS 密钥，则无法对设备磁盘进行解密。

2. 选择 * 配置硬件 * > * 节点加密 * 。



3. 选择 * 启用节点加密 * 。

   在安装设备之前，您可以取消选择 * 启用节点加密 * ，而不会有数据丢失的风险。安装开始后，设备节点将访问 StorageGRID 系统中的 KMS 加密密钥并开始磁盘加密。安装设备后，您无法禁用节点加密。

   > 将启用了节点加密的设备添加到具有 KMS 的 StorageGRID 站点后，您无法停止对此节点使用 KMS 加密。

4. 选择 * 保存 * 。

5. 将设备部署为 StorageGRID 系统中的节点。

   当设备访问为 StorageGRID 站点配置的 KMS 密钥时，便会开始使用由 KMS 控制的加密。安装程序会在 KMS 加密过程中显示进度消息，此过程可能需要几分钟时间，具体取决于设备中的磁盘卷数。

   > 设备最初会配置一个随机的非 KMS 加密密钥，该密钥会分配给每个磁盘卷。磁盘会使用此临时加密密钥进行加密，这种加密密钥不安全，直到启用了节点加密的设备访问为 StorageGRID 站点配置的 KMS 密钥为止。

完成后

您可以查看节点加密状态， KMS 详细信息以及设备节点处于维护模式时正在使用的证书。

相关信息

管理 StorageGRID

在维护模式下监控节点加密（ SG6000 ）

可选：更改 **RAID** 模式（仅限 **SG6000** ）

您可以在设备上更改为其他 RAID 模式，以满足存储和恢复要求。您只能在部署设备存储节点之前更改此模式。

您需要的内容

- 您正在使用可以连接到 StorageGRID 的任何客户端。
- 客户端具有 支持的 Web 浏览器。

关于此任务

在将设备部署为存储节点之前，您可以选择以下卷配置选项之一：

- * DDP * ： 此模式每八个数据驱动器使用两个奇偶校验驱动器。这是所有设备的默认和建议模式。与 RAID6 相比， DDP 可提高系统性能，缩短驱动器发生故障后的重建时间，并简化管理。

  > 由于有两个SSD、DDP不会在SG6060设备中提供抽盒丢失保护。对于添加到SG6060中的任何扩展架、抽屉丢失保护功能均有效。

- * DDP16* ： 此模式每 16 个数据驱动器使用两个奇偶校验驱动器，因此与 DDP 相比，存储效率更高。与 RAID6 相比， DDP16 可提高系统性能，缩短驱动器故障后的重建时间，简化管理并提供同等的存储效率。要使用 DDP16 模式，您的配置必须至少包含 20 个驱动器。DDP16 不提供抽盒丢失保护。
- * RAID6* ： 此模式每 16 个或更多数据驱动器使用两个奇偶校验驱动器。要使用 RAID 6 模式，您的配置必须至少包含 20 个驱动器。虽然与 DDP 相比， RAID6 可以提高设备的存储效率，但不建议在大多数 StorageGRID 环境中使用。

> 如果已配置任何卷或先前已安装 StorageGRID ，则更改 RAID 模式会删除和更换这些卷。这些卷上的所有数据都将丢失。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

` * https://*Controller_IP*:8443*`

` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 高级 * > * RAID 模式 * 。
3. 在 * 配置 RAID 模式 * 页面上，从模式下拉列表中选择所需的 RAID 模式。
4. 单击 * 保存 * 。

相关信息

"NetApp E 系列系统文档站点"

可选：重新映射设备的网络端口

您可能需要将设备存储节点上的内部端口重新映射到不同的外部端口。例如，由于使用了防火墙问题描述 ，您可能需要重新映射端口。

您需要的内容

- 您先前已访问 StorageGRID 设备安装程序。
- 您尚未配置，也不打算配置负载平衡器端点。

> 如果重新映射任何端口，则不能使用相同的端口来配置负载平衡器端点。如果要配置负载平衡器端点且已重新映射端口，请按照中的步骤进行操作 删除端口重新映射。

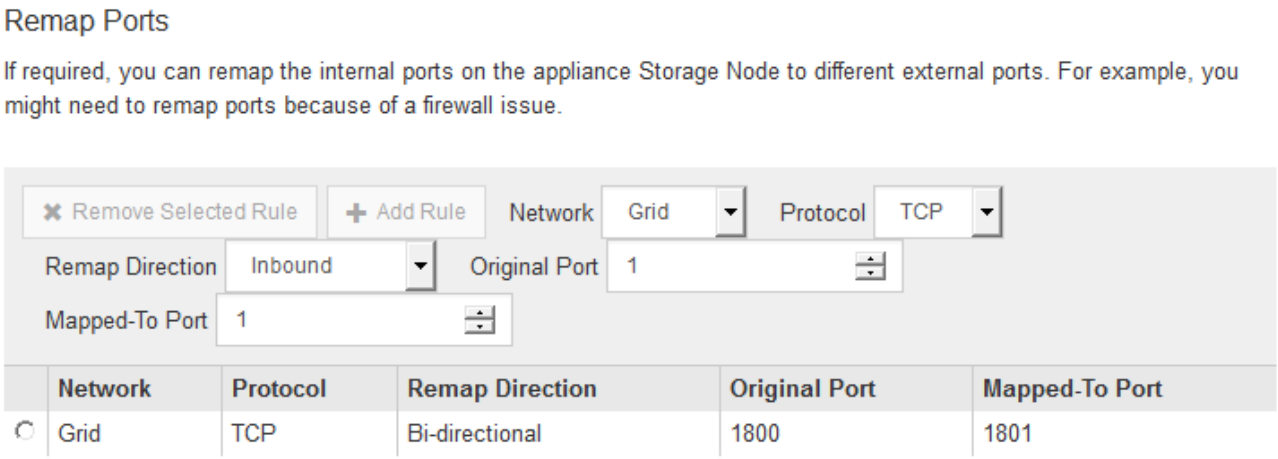
步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 删除端口 * 。

   此时将显示 Remap Port 页面。

2. 从 * 网络 * 下拉框中，为要重新映射的端口选择网络：网格，管理员或客户端。
3. 从 * 协议 * 下拉框中，选择 IP 协议： TCP 或 UDP 。
4. 从 * 映射方向 * 下拉框中，选择要为此端口重新映射的流量方向：入站，出站或双向。
5. 对于 * 原始端口 * ，输入要重新映射的端口的编号。
6. 对于 * 映射到端口 * ，请输入要使用的端口编号。
7. 单击 * 添加规则 * 。

   此时，新端口映射将添加到表中，重新映射将立即生效。



8. 要删除端口映射，请选择要删除的规则对应的单选按钮，然后单击 * 删除选定规则 * 。

部署设备存储节点

安装和配置存储设备后，您可以将其部署为 StorageGRID 系统中的存储节点。将设备部署为存储节点时，您可以使用设备上随附的 StorageGRID 设备安装程序。

您需要的内容

- 如果要克隆设备节点，请继续执行恢复和维护过程。

  恢复和维护

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路， IP 地址和端口重新映射（如果需要）。
- 您知道分配给设备计算控制器的一个 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。
- 已部署 StorageGRID 系统的主管理节点。
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 您的服务笔记本电脑具有受支持的 Web 浏览器。

关于此任务

每个存储设备都用作一个存储节点。任何设备都可以连接到网格网络，管理网络和客户端网络

要在 StorageGRID 系统中部署设备存储节点，请访问 StorageGRID 设备安装程序并执行以下步骤：

- 您可以指定或确认主管理节点的 IP 地址以及存储节点的名称。
- 您可以开始部署，并等待卷配置完毕并安装软件。
- 当安装暂停完成设备安装任务后，您可以通过登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装和部署过程来恢复安装。

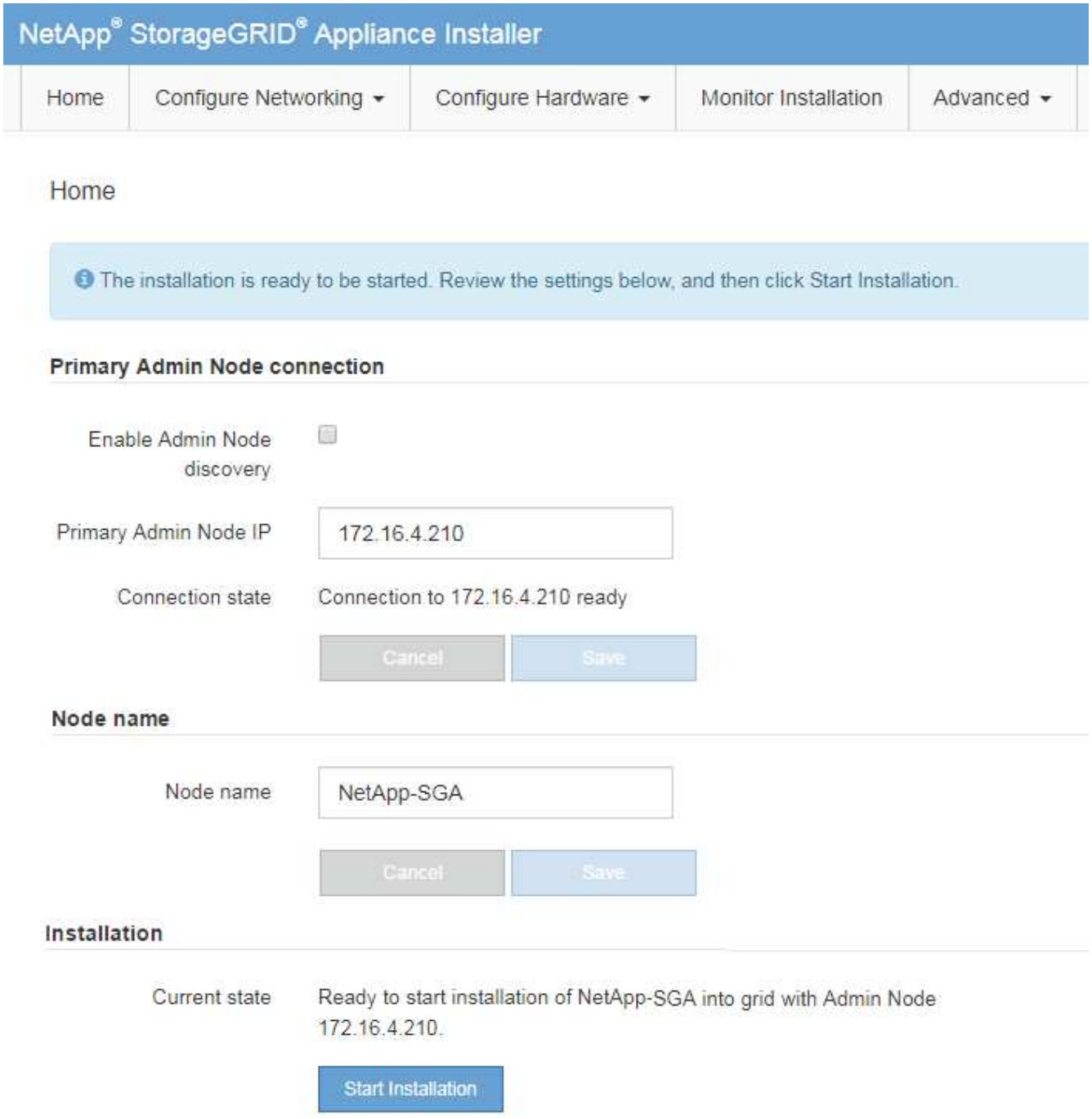
> 如果您需要一次部署多个设备节点，则可以使用 `configure-sGa.py` Appliance Installation 脚本自动执行安装过程。

- 如果要执行扩展或恢复操作，请按照相应说明进行操作：
  - 要将设备存储节点添加到现有 StorageGRID 系统，请参见有关扩展 StorageGRID 系统的说明。
  - 要在恢复操作中部署设备存储节点，请参见有关恢复和维护的说明。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   此时将显示 StorageGRID 设备安装程序主页页面。



2. 在 * 主管理节点连接 * 部分中，确定是否需要指定主管理节点的 IP 地址。

   如果先前已在此数据中心中安装了其他节点，则 StorageGRID 设备安装程序可以自动发现此 IP 地址，前提

是主管理节点或至少一个配置了 admin_IP 的其他网格节点位于同一子网上。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 等待连接状态，使新 IP 地址准备就绪。
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 等待显示发现的 IP 地址列表。 c. 为要部署此设备存储节点的网格选择主管理节点。 d. 单击 * 保存 * 。 e. 等待连接状态，使新 IP 地址准备就绪。

4. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后单击 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的节点页面（概述选项卡）上。如果需要，您可以在批准节点时更改名称。

5. 在 * 安装 * 部分中，确认当前状态为 "Ready to start installation of ` node_node name_` into grid with primary Admin Node ` *admin_IP*` " ，并且 * 开始安装 * 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

   如果要将存储节点设备部署为节点克隆目标，请在此停止部署过程，然后继续执行节点克隆操作步骤 的恢复和维护。+恢复和维护

6. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。

   当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

   如果需要手动访问监控器安装页面，请单击 * 监控安装 * 。

7. 如果网格包含多个设备存储节点，请对每个设备重复这些步骤。

   如果您需要一次部署多个设备存储节点，则可以使用 `configure-sGa.py` Appliance Installation 脚本自动执行安装过程。

相关信息

扩展网格

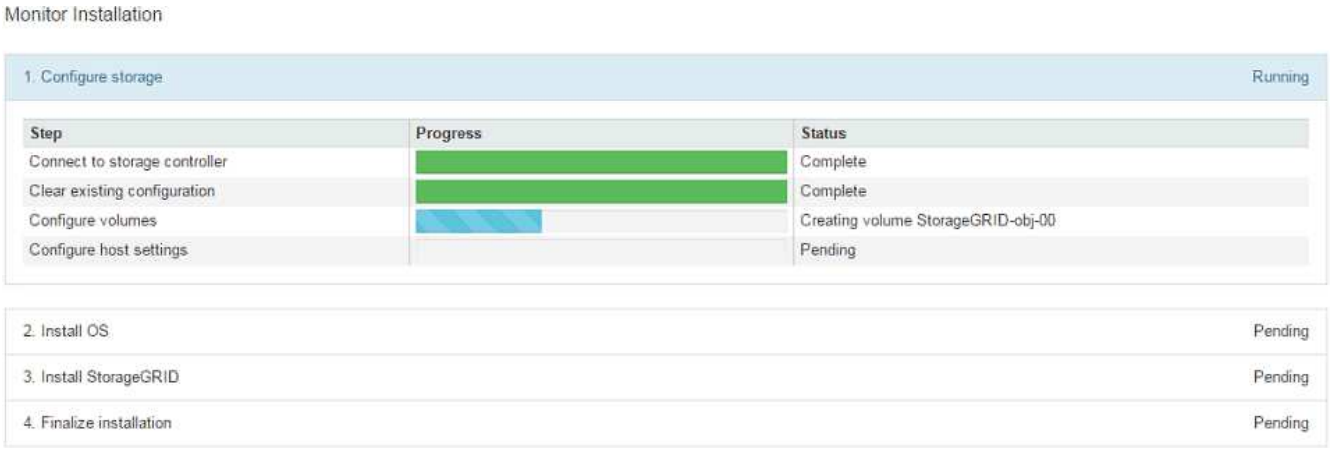
监控存储设备安装

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

步骤

1. 要监控安装进度，请单击 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

2. 查看前两个安装阶段的进度。

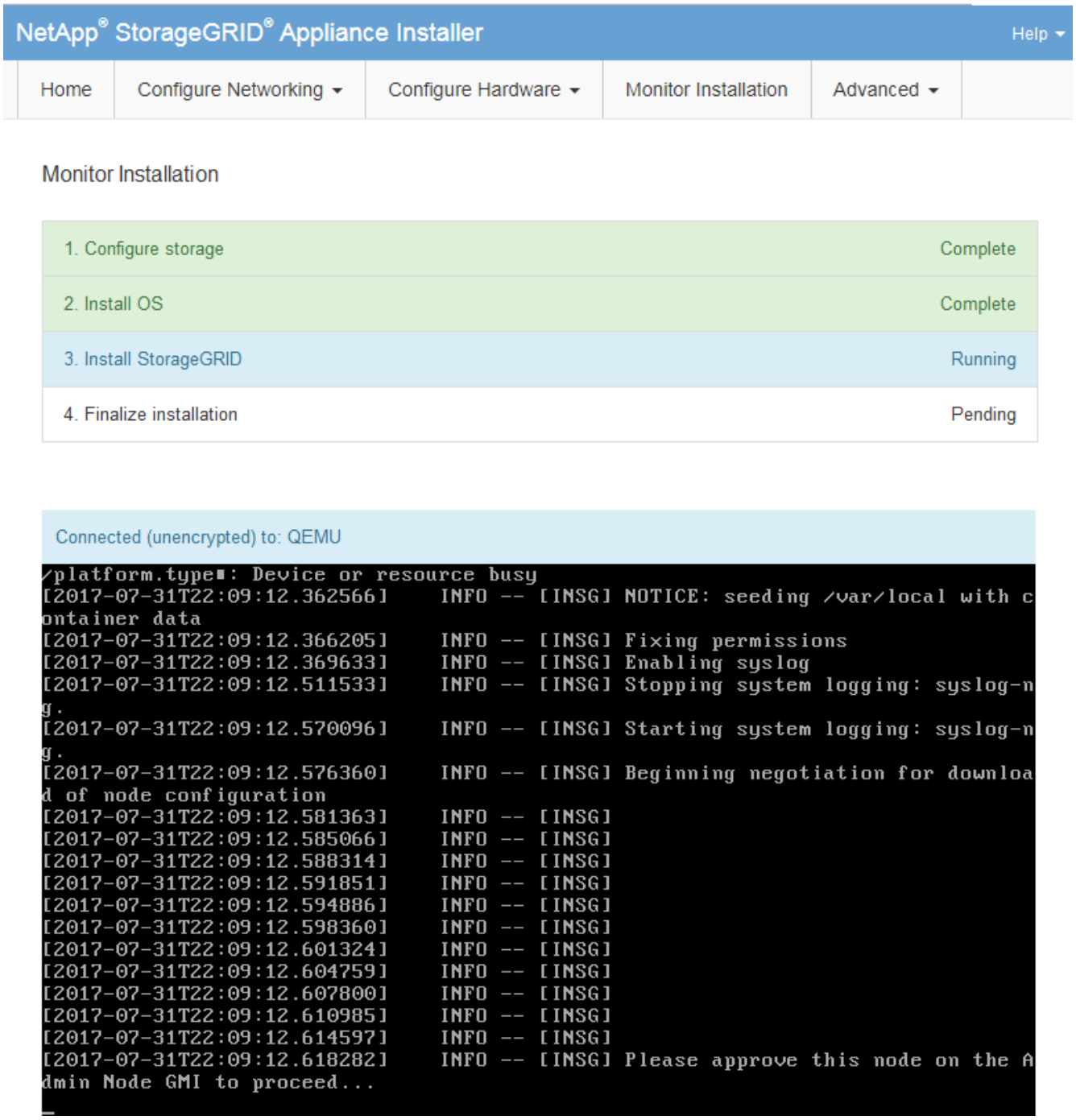
   ◦ 。配置存储 *

   在此阶段，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。

   ◦ 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

3. 继续监控安装进度，直到 * 安装 StorageGRID 网格管理器 * 阶段暂停，并且嵌入式控制台上显示一条消息，提示您使用网格管理器在管理节点上批准此节点。继续执行下一步。



4. 转至主管理节点的网格管理器，批准待定存储节点并完成 StorageGRID 安装过程。

   在网格管理器中单击 * 安装 * 后，第 3 阶段完成，第 4 阶段 * 完成安装 * 开始。阶段 4 完成后，控制器将重新启动。

自动化设备安装和配置（ **SG6000** ）

您可以自动安装和配置设备以及配置整个 StorageGRID 系统。

关于此任务

自动化安装和配置对于部署多个 StorageGRID 实例或一个大型复杂的 StorageGRID 实例非常有用。

要自动执行安装和配置，请使用以下一个或多个选项：

- 创建一个 JSON 文件，用于指定设备的配置设置。使用 StorageGRID 设备安装程序上传 JSON 文件。

  您可以使用同一文件配置多个设备。

- 使用 StorageGRID`configure-sGa.py` Python 脚本自动配置设备。
- 使用其他 Python 脚本配置整个 StorageGRID 系统的其他组件（ " 网格 " ）。

您可以直接使用 StorageGRID 自动化 Python 脚本，也可以使用它们作为示例，说明如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。请参见有关的信息 下载并提取 StorageGRID 安装文件。

使用 **StorageGRID** 设备安装程序自动配置设备

您可以使用包含配置信息的 JSON 文件自动配置设备。您可以使用 StorageGRID 设备安装程序上传文件。

您需要的内容

- 您的设备必须使用与 StorageGRID 11.5 或更高版本兼容的最新固件。
- 您必须连接到要使用配置的设备上的 StorageGRID 设备安装程序 支持的 Web 浏览器。

关于此任务

您可以自动执行设备配置任务，例如配置以下内容：

- 网格网络，管理网络和客户端网络 IP 地址
- BMC 接口
- 网络链路
  - 端口绑定模式
  - 网络绑定模式
  - 链路速度

使用上传的 JSON 文件配置设备通常比在 StorageGRID 设备安装程序中使用多个页面手动执行配置效率更高，尤其是在需要配置多个节点时。您必须一次应用一个节点的配置文件。

有经验的用户如果希望自动安装和配置其设备，可以使用 `configure-sGA .py` 脚本。+使用 configure-sga.py 脚本自动安装和配置设备节点

步骤

1. 使用以下方法之一生成 JSON 文件：
   - ConfigBuilder 应用程序

     "ConfigBuilder.netapp.com"

   - `configure-sGa.py` 设备配置脚本。您可以从 StorageGRID 设备安装程序（ * 帮助 * > * 设备配置脚

本 * ）下载此脚本。请参见有关使用 configure-sga.py 脚本自动配置的说明。

使用 configure-sga.py 脚本自动安装和配置设备节点

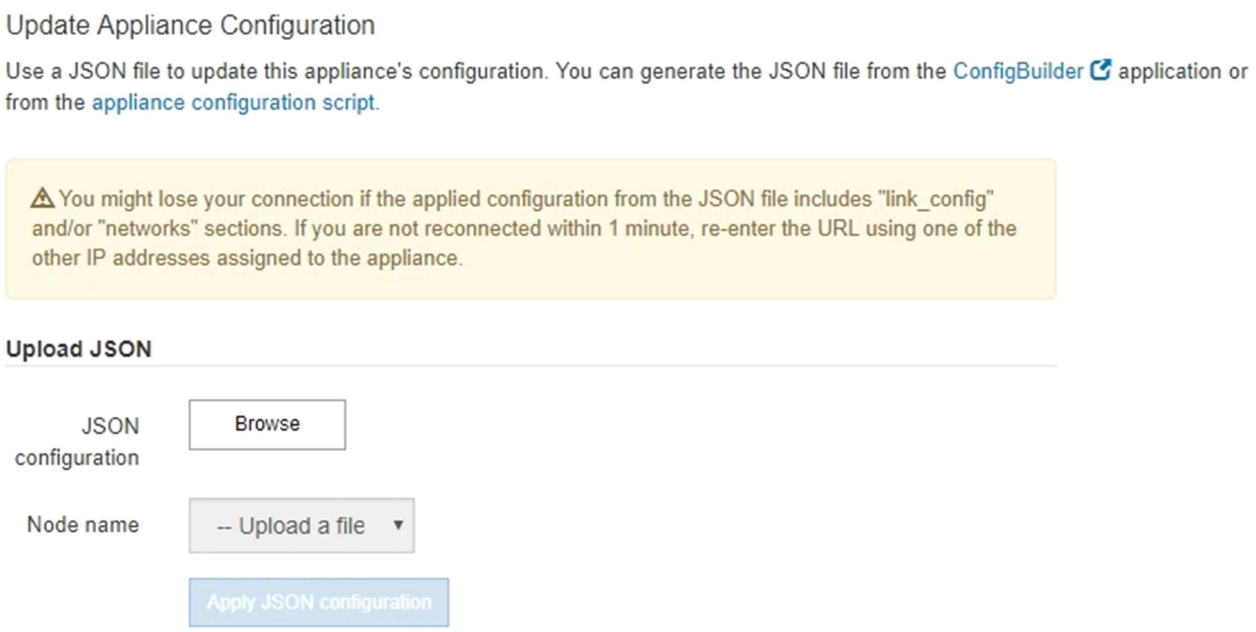
JSON 文件中的节点名称必须符合以下要求：

- 必须是一个有效的主机名，至少包含 1 个字符，并且不超过 32 个字符
- 可以使用字母，数字和连字符
- 不能以连字符开头或结尾
- 不能仅包含数字

> 请确保 JSON 文件中的节点名称（顶级名称）是唯一的，否则您将无法使用 JSON 文件配置多个节点。

2. 选择 * 高级 * > * 更新设备配置 * 。

此时将显示更新设备配置页面。

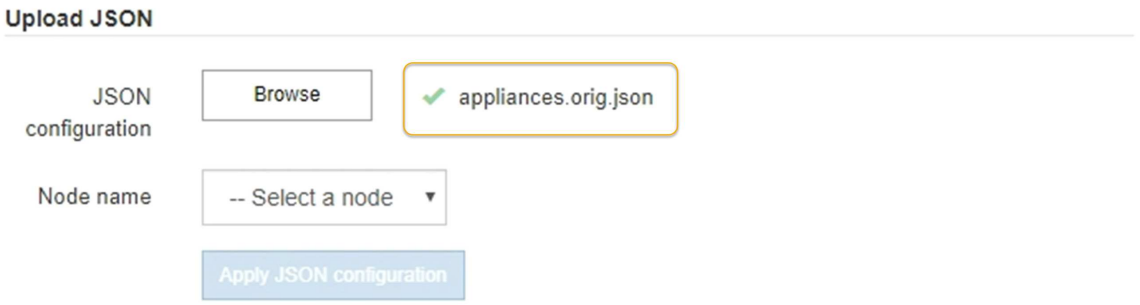


3. 选择包含要上传的配置的 JSON 文件。

a. 选择 * 浏览 * 。
b. 找到并选择文件。
c. 选择 * 打开 * 。

已上传并验证此文件。验证过程完成后，文件名会显示在绿色复选标记旁边。

如果 JSON 文件中的配置包含 "link_config" ， "networks" 或这两者的部分，则可能会断开与设备的连接。如果 1 分钟内未重新连接，请使用分配给设备的其他 IP 地址之一重新输入设备 URL 。

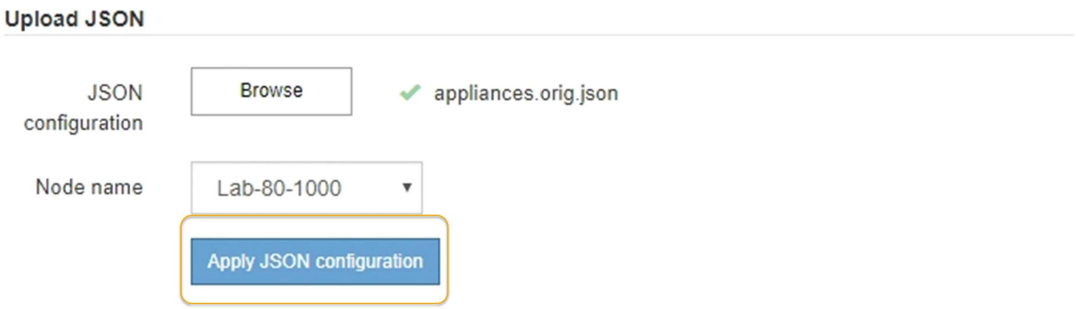


此时将使用 JSON 文件中定义的顶级节点名称填充 * 节点名称 * 下拉列表。

如果文件无效，则文件名将显示为红色，并在黄色横幅中显示一条错误消息。此无效文件不会应用于此设备。您可以使用 ConfigBuilder 来确保具有有效的 JSON 文件。

4. 从 * 节点名称 * 下拉列表中选择一个节点。

   此时将启用 * 应用 JSON 配置 * 按钮。



5. 选择 * 应用 JSON 配置 * 。

   此配置将应用于选定节点。

使用 **configure-sga.py** 脚本自动安装和配置设备节点

您可以使用 `configure-sGa.py` 脚本自动执行 StorageGRID 设备节点的许多安装和配置任务，包括安装和配置主管理节点。如果要配置大量设备，此脚本可能会很有用。您也可以使用此脚本生成包含设备配置信息的 JSON 文件。

您需要的内容

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为主管理节点配置网络链路和 IP 地址。

- 如果要安装主管理节点，则您知道其 IP 地址。
- 如果要安装和配置其他节点，则已部署主管理节点，并且您知道其 IP 地址。
- 对于主管理节点以外的所有节点，已在主管理节点上的网格网络子网列表中定义 StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网。
- 您已下载 `configure-sGA .py` 文件。该文件包含在安装归档中，您也可以通过单击 StorageGRID 设备安装程序中的 * 帮助 * > * 设备安装脚本 * 来访问该文件。

> 此操作步骤 适用于在使用命令行界面方面具有一定经验的高级用户。或者，您也可以使用 StorageGRID 设备安装程序自动执行配置。+使用 StorageGRID 设备安装程序自动配置设备

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 要获得有关脚本语法的一般帮助以及查看可用参数列表，请输入以下内容：

```
configure-sga.py --help
```

`configure-sGa.py` 脚本使用五个子命令：

- **高级** 用于高级 StorageGRID 设备交互，包括 BMC 配置和创建包含设备当前配置的 JSON 文件
- `configure` 用于配置 RAID 模式，节点名称和网络参数
- `install` 用于开始 StorageGRID 安装
- `m` 监控 StorageGRID 安装
- `reboot` 用于重新启动设备

如果输入子命令（ advanced ， configure ， install ， monitor 或 reboot ）参数，然后输入 ` -help` 选项，则会收到其他帮助文本，其中提供了有关该子命令中可用选项的更多详细信息： + `configure-sga.py` *`subcommand`* `-help`

3. 要确认设备节点的当前配置，请输入以下内容，其中 ` *SGA-install-IP*` 是设备节点的任一 IP 地址： + `configure-sga.py configure` *`SGA-install-IP`*

结果将显示设备的当前 IP 信息，包括主管理节点的 IP 地址以及有关管理，网格和客户端网络的信息。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
```

```
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4

        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
```

```
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#####################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#####################################################################
```

4. 如果需要更改当前配置中的任何值，请使用 `configure` 子命令对其进行更新。例如，如果要将设备用于连接到主管理节点的 IP 地址更改为 `172.16.2.99` ，请输入以下内容： + `configure-sga.py configure -admin-IP 172.16.2.99 sGA-install-ip`
5. 如果要将设备配置备份到 JSON 文件，请使用 `advanced` 和 `backup-file` 子命令。例如，如果要将 IP 地址为 ` SGA-install-ip_` 的设备配置备份到名为 `appliance-SG1000.json` 的文件中，请输入以下命令： + `configure-sga.py advanced -backup-file appliance-SG1000.json SGA-install-IP`

   包含配置信息的 JSON 文件将写入执行脚本的同一目录。

   > 检查生成的 JSON 文件中的顶级节点名称是否与设备名称匹配。请勿对此文件进行任何更改，除非您是经验丰富的用户并全面了解 StorageGRID API 。

6. 如果对设备配置满意，请使用 `install` 和 `monitor` 子命令安装此设备： + `configure-sga.py install -monitor sGA-install-ip`
7. 如果要重新启动设备，请输入以下内容： + `configure-sga.py reboot sGA-install-ip`

自动配置 **StorageGRID**

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	Description
`configure-storaggrid.py`	用于自动配置的 Python 脚本
`configure-storaggrid.sample.json`	用于脚本的示例配置文件
`configure-storaggrid.blank.json`	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

关于此任务

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

> 您也可以使用网格管理器或安装 API 配置系统。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如： + `cd StorageGRID-Webscale -version/platform`

   其中，`platform` 是 `dEBS`， `rpms` 或 `vSphere`。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完成后

在配置过程中会生成一个恢复包 `.zip` 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 `passwords.txt` 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

安装 **REST API** 概述

StorageGRID 提供了两个用于执行安装任务的 REST API： StorageGRID 安装 API 和 StorageGRID 设备安装程序 API 。

这两个 API 都使用 Swagger 开源 API 平台来提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 **API**

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。
- **recovery-package** —下载恢复软件包的操作。
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

StorageGRID 设备安装程序 API

StorageGRID 设备安装程序 API 可通过 HTTPS 从 ` Controller_IP_ ： 8443` 访问。

要访问 API 文档，请转到设备上的 StorageGRID 设备安装程序，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 设备安装程序 API 包括以下部分：

- * 克隆 * —用于配置和控制节点克隆的操作。
- * 加密 * —用于管理加密和查看加密状态的操作。
- * 硬件配置 * —用于在连接的硬件上配置系统设置的操作。
- * 安装 * —用于开始设备安装和监控安装状态的操作。
- * 网络连接 * - 与 StorageGRID 设备的网格，管理和客户端网络配置以及设备端口设置相关的操作。
- * 设置 * —用于帮助初始设备安装设置的操作，包括请求获取有关系统的信息并更新主管理节点 IP 。
- * 支持 * —用于重新启动控制器和获取日志的操作。
- * 升级 * —与升级设备固件相关的操作。
- **uploadsg** —用于上传 StorageGRID 安装文件的操作。

硬件安装故障排除（ SG6000 ）

如果您在安装期间遇到问题，查看与硬件设置和连接问题相关的故障排除信息可能会很有帮助。

查看 SG6000-CN 控制器的启动代码

在为设备接通电源时， BMC 会为 SG6000-CN 控制器记录一系列启动代码。您可以通过多种方式查看这些代码。

您需要的内容

- 您知道如何访问 BMC 信息板。
- 如果您要使用 LAN 上串行（ Serial Over LAN ，故障转移），则具有使用 IPMI 故障转移控制台应用程序的经验。

步骤

1. 选择以下方法之一以查看设备控制器的启动代码，并收集所需的设备。

方法	所需设备
VGA 控制台	• 支持 VGA 的显示器 • VGA 缆线
KVM	• RJ-45 缆线

方法	所需设备
串行端口	• DB-9 串行缆线 • 虚拟串行终端
解决	• 虚拟串行终端

2. 如果您使用的是 VGA 控制台，请执行以下步骤：
   a. 将支持 VGA 的显示器连接到设备背面的 VGA 端口。
   b. 查看监控器上显示的代码。
3. 如果您使用的是 BMC KVM ，请执行以下步骤：
   a. 连接到 BMC 管理端口并登录到 BMC Web 界面。
   b. 选择 * 远程控制 * 。
   c. 启动 KVM 。
   d. 在虚拟监控器上查看代码。
4. 如果您使用的是串行端口和终端，请执行以下步骤：
   a. 连接到设备背面的 DB-9 串行端口。
   b. 使用设置 `115200 8-N-1` 。
   c. 查看通过串行终端打印的代码。
5. 如果您使用的是 SOL ，请执行以下步骤：
   a. 使用 BMC IP 地址和登录凭据连接到 IPMI SOL 。

      如果未更改 BMC root 帐户密码，则出厂默认值可能为 "calvin" 。

      ```
      ipmitool -i lanplus -H BMC_Port_IP -U root -P Password sole activate
      ```

   b. 查看虚拟串行终端上的代码。
6. 使用下表查找您的设备的代码。

代码	表示
您好	主启动脚本已启动。
HP	系统正在检查是否需要更新网络接口卡（ Network Interface Card ， NIC ）固件。
RB	应用固件更新后，系统正在重新启动。
FP	硬件子系统固件更新检查已完成。控制器间通信服务正在启动。

代码	表示
他	仅适用于设备存储节点： 系统正在等待与存储控制器建立连接并与 SANtricity 操作系统同步。 • 注： * 如果启动操作步骤 在此阶段未进展，请执行以下步骤： a. 确认 SG6000-CN 控制器与两个存储控制器之间的四根互连缆线已牢固连接。 b. 根据需要更换一根或多根缆线，然后重试。 c. 如果无法解决问题描述 问题，请联系技术支持。
HC	系统正在检查现有 StorageGRID 安装数据。
好的	StorageGRID 设备安装程序正在运行。
HA	StorageGRID 正在运行。

查看 **SG6000-CN** 控制器的错误代码

如果在 SG6000-CN 控制器启动时发生硬件错误，则 BMC 会记录一个错误代码。您可以根据需要使用 BMC 界面查看这些错误代码，然后与技术支持联系以解决此问题描述 。

您需要的内容

- 您知道如何访问 BMC 信息板。

步骤

1. 从 BMC 信息板中，选择 * BIOS POST Code* 。
2. 查看为当前代码和先前代码显示的信息。

   如果显示以下任一错误代码，请与技术支持联系以解决此问题描述 。

代码	表示
0x0E	未找到微代码
0x0F	未加载微代码
0x50	内存初始化错误。内存类型无效或内存速度不兼容。
0x51	内存初始化错误。SPD 读取失败。

代码	表示
0x52	内存初始化错误。内存大小无效或内存模块不匹配。
0x53	内存初始化错误。未检测到可用内存。
0x54	未指定的内存初始化错误
0x55	未安装内存
0x56	CPU 类型或速度无效
0x57	CPU 不匹配
0x58	CPU 自检失败或可能出现 CPU 缓存错误
0x59	未找到 CPU 微代码或微代码更新失败
0x5A	内部 CPU 错误
0x5B	重置 PPI 不可用
0x5C	PEI 阶段 BMC 自检失败
0xD0	CPU 初始化错误
0xD1	北网桥初始化错误
0xD2	南桥初始化错误
0xD3	某些架构协议不可用
0xd4	PCI 资源分配错误。资源不足。
0xD5	原有选项 ROM 没有空间
0xD6	未找到控制台输出设备
0xD7	未找到控制台输入设备
0xD8	密码无效
0xD9	加载启动选项时出错（ LoadImage 返回错误）

代码	表示
0xDA	启动选项失败（ StartImage 返回错误）
0xDB	闪存更新失败
0xDC	重置协议不可用
0xDD	Dxe 阶段 BMC 自检失败
0xE8	MRC： err_no_memory
0xE9	MRC： err_lt_lock
0xEA	MRC： err_DDR_init
0xEB	MRC： ERR_MEM_TEST
0xEC	MRC： err_vendor_specific
0xED	MRC： ERR_DIMM_COMPAT
0xEE	MRC： err_MRC_compatibility
0xEF	MRC： err_MRC_struct
0xF0	MRC： ERR_SET_VDD
0xF1	MRC： ERR_IOT_MEM_buffer
0xF2	MRC： err_rc_internal
0xF	MRC： err_invalid_REG_access
0xf4	MRC： ERR_SET_MC_FRQ
0xf5	MRC： err_read_mc_fREQ
0x70	MRC： err_DIMM_channel
0x74	MRC： err_smix_check
0xf6	MRC： err_SMBUS

代码	表示
0xF7	MRC： ERR_PCU
0xf8.	MRC： err_NGN
0xf9	MRC： err_interlef_failure

硬件设置似乎挂起（**SG6000**）

如果硬件故障或布线错误导致存储控制器或 SG6000-CN 控制器无法完成启动处理，则 StorageGRID 设备安装程序可能不可用。

步骤

1. 对于存储控制器，请查看七段显示器上的代码。

   在启动期间初始化硬件时，两个七段显示一系列代码。硬件成功启动后，这两个七段显示 `99` 。

2. 查看 SG6000-CN 控制器上的 LED 以及 BMC 中显示的启动和错误代码。
3. 如果您需要有关解决问题描述 的帮助，请联系技术支持。

相关信息

查看 SG6000 存储控制器的启动状态代码

"《 E5700 和 E2800 系统监控指南》"

查看 SG6000-CN 控制器上的状态指示灯和按钮

查看 SG6000-CN 控制器的启动代码

查看 SG6000-CN 控制器的错误代码

对连接问题进行故障排除（**SG6000**）

如果您在 StorageGRID 设备安装期间遇到连接问题，应执行列出的更正操作步骤。

无法连接到设备

如果无法连接到设备，则可能存在网络问题描述 ，或者硬件安装可能未成功完成。

步骤

1. 如果无法连接到 SANtricity 系统管理器：
   a. 尝试使用管理网络上任一存储控制器的 IP 地址对设备执行 ping 操作，以查看 SANtricity System Manager： + ` * ping *Storage_Controller_IP**`
   b. 如果 ping 未收到任何响应，请确认您使用的 IP 地址正确无误。

      使用任一存储控制器上的管理端口 1 的 IP 地址。

c. 如果 IP 地址正确，请检查设备布线和网络设置。

   如果无法解决问题描述 问题，请联系技术支持。

d. 如果 ping 成功，请打开 Web 浏览器。

e. 输入 SANtricity 系统管理器的 URL： + ` * https://*Storage_Controller_IP*`

   此时将显示 SANtricity 系统管理器的登录页面。

2. 如果无法连接到 SG6000-CN 控制器：

   a. 尝试使用 SG6000-CN 控制器的 IP 地址对设备执行 ping 操作： + ` * ping *SG6000-CN_Controller_IP*`

   b. 如果 ping 未收到任何响应，请确认您使用的 IP 地址正确无误。

      您可以使用网格网络，管理网络或客户端网络上设备的 IP 地址。

   c. 如果 IP 地址正确，请检查设备布线， SFP 收发器和网络设置。

   d. 如果可以物理访问 SG6000-CN ，则可以使用与永久链路本地 IP `169.254.0.1` 的直接连接来检查控制器网络配置，并在必要时进行更新。有关详细说明，请参见中的步骤 2 访问 StorageGRID 设备安装程序。

      如果无法解决问题描述 问题，请联系技术支持。

   e. 如果 ping 成功，请打开 Web 浏览器。

   f. 输入 StorageGRID 设备安装程序的 URL： + ` * https://*SG6000-CN_Controller_IP*:8443*`

      此时将显示主页页面。

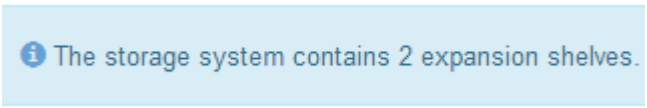
扩展架未显示在设备安装程序中

如果您为SG6060或SG6060X安装了扩展架、但这些扩展架未显示在StorageGRID 设备安装程序中、则应验证这些磁盘架是否已完全安装并打开电源。

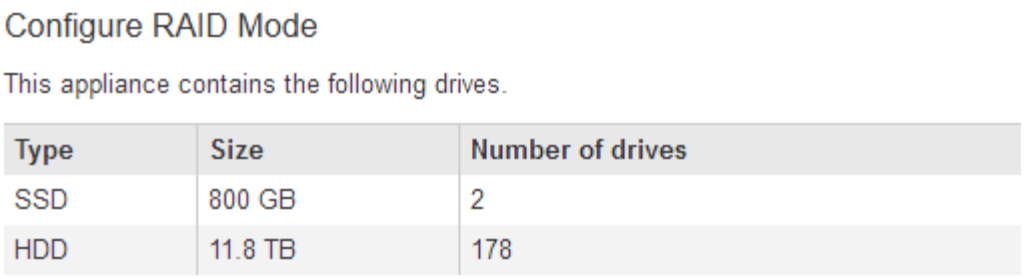
关于此任务

您可以通过在 StorageGRID 设备安装程序中查看以下信息来验证扩展架是否已连接到设备：

- 主页 * 页面包含一条有关扩展架的消息。

- * 高级 * > * RAID 模式 * 页面可通过驱动器数量指示设备是否包含扩展架。例如，在以下屏幕截图中，显示了两个 SSD 和 178 个 HDD 。包含两个扩展架的 SG6060 总共包含 180 个驱动器。



如果 StorageGRID 设备安装程序页面未指示存在扩展架，请遵循此操作步骤 。

步骤

1. 请验证 所有必需的缆线均已牢固连接。
2. 验证您是否已安装 已打开扩展架电源。
3. 如果您需要有关解决问题描述 的帮助，请联系技术支持。

在 **StorageGRID** 设备安装程序运行期间重新启动 **SG6000-CN** 控制器

在 StorageGRID 设备安装程序运行期间，您可能需要重新启动 SG6000-CN 控制器。例如，如果安装失败，您可能需要重新启动控制器。

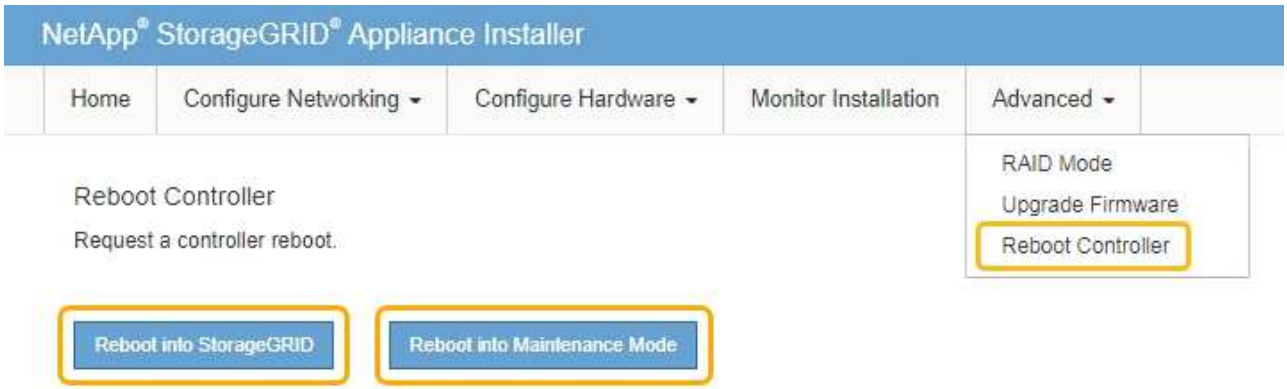
关于此任务

只有在 SG6000-CN 控制器运行 StorageGRID 设备安装程序时，此操作步骤 才适用。安装完成后，此步骤将不再起作用，因为 StorageGRID 设备安装程序不再可用。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



SG6000-CN 控制器将重新启动。

维护 SG6000 设备

您可能需要对 SG6000 设备执行维护过程。本节中的过程假定设备已部署为 StorageGRID 系统中的存储节点。

要防止服务中断，请在关闭设备之前确认所有其他存储节点均已连接到网格，或者在可接受服务中断期间的计划维护窗口期间关闭设备。请参见有关的信息 监控节点连接状态。

> 如果您使用的 ILM 规则只创建一个对象的一个副本，则必须在计划维护时段关闭设备。否则，在任何维护操作步骤 导致存储节点停止服务期间，您可能暂时无法访问这些对象。请参见有关的信息 通过信息生命周期管理管理对象。

将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

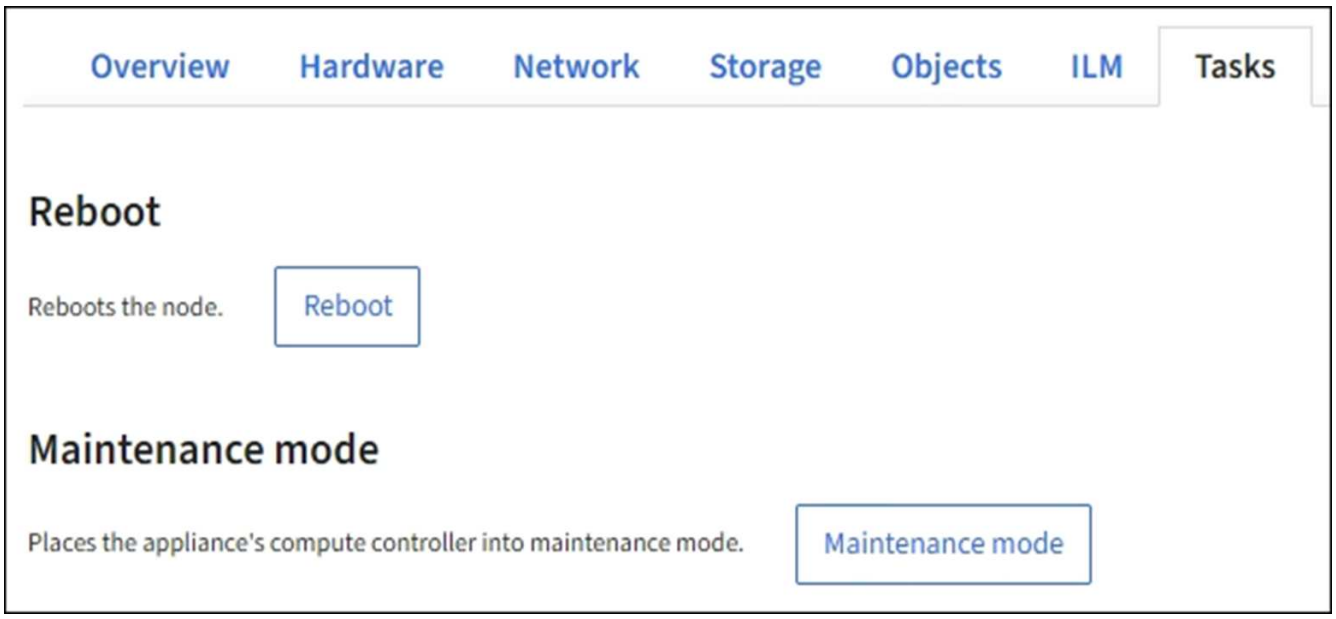
关于此任务

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

> 处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

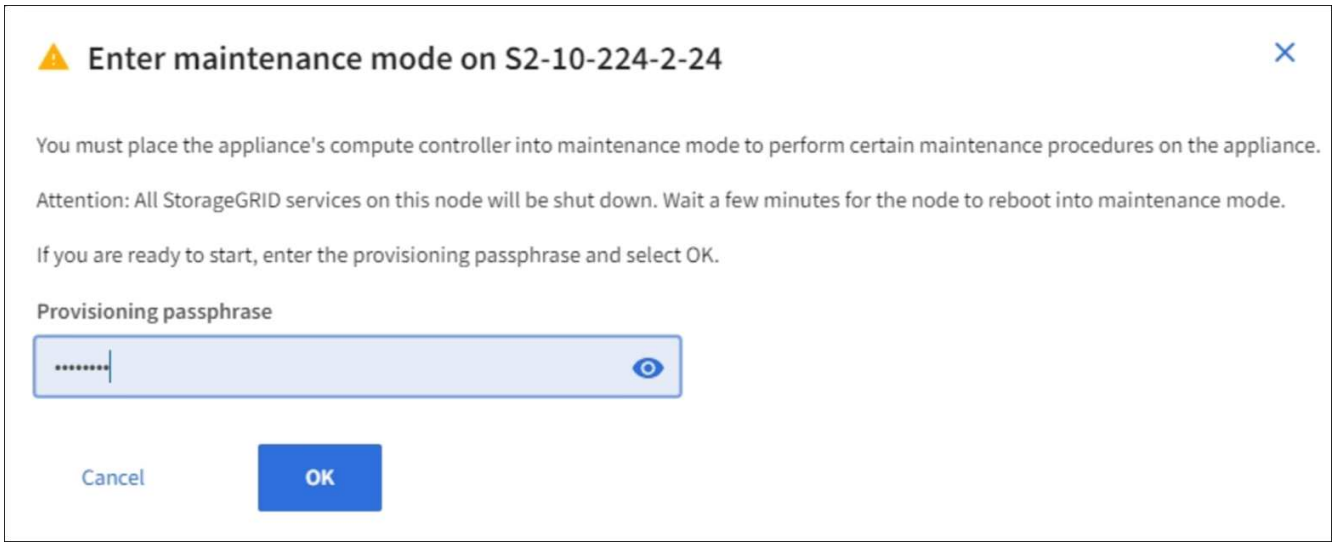
步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面的树视图中，选择设备存储节点。
3. 选择 * 任务 * 。



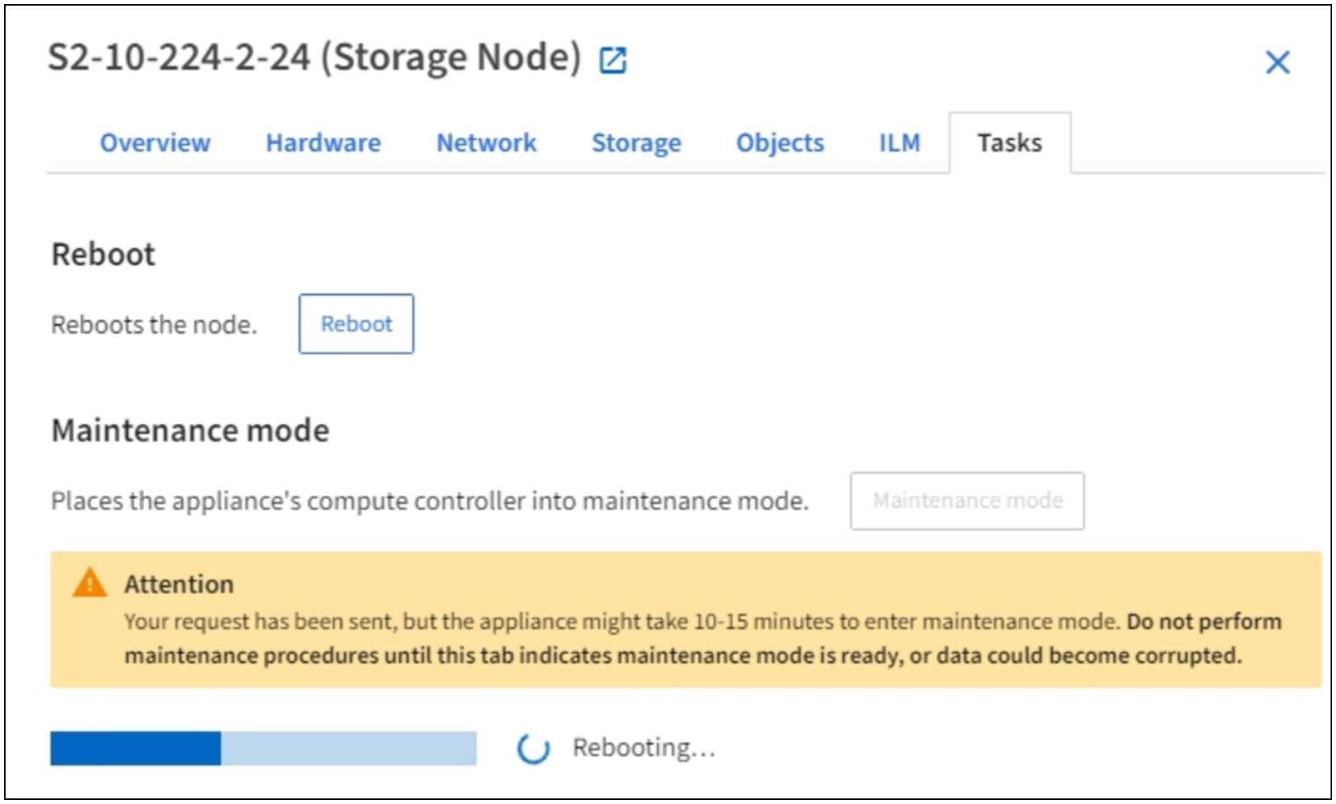
4. 选择 * 维护模式 * 。

   此时将显示确认对话框。

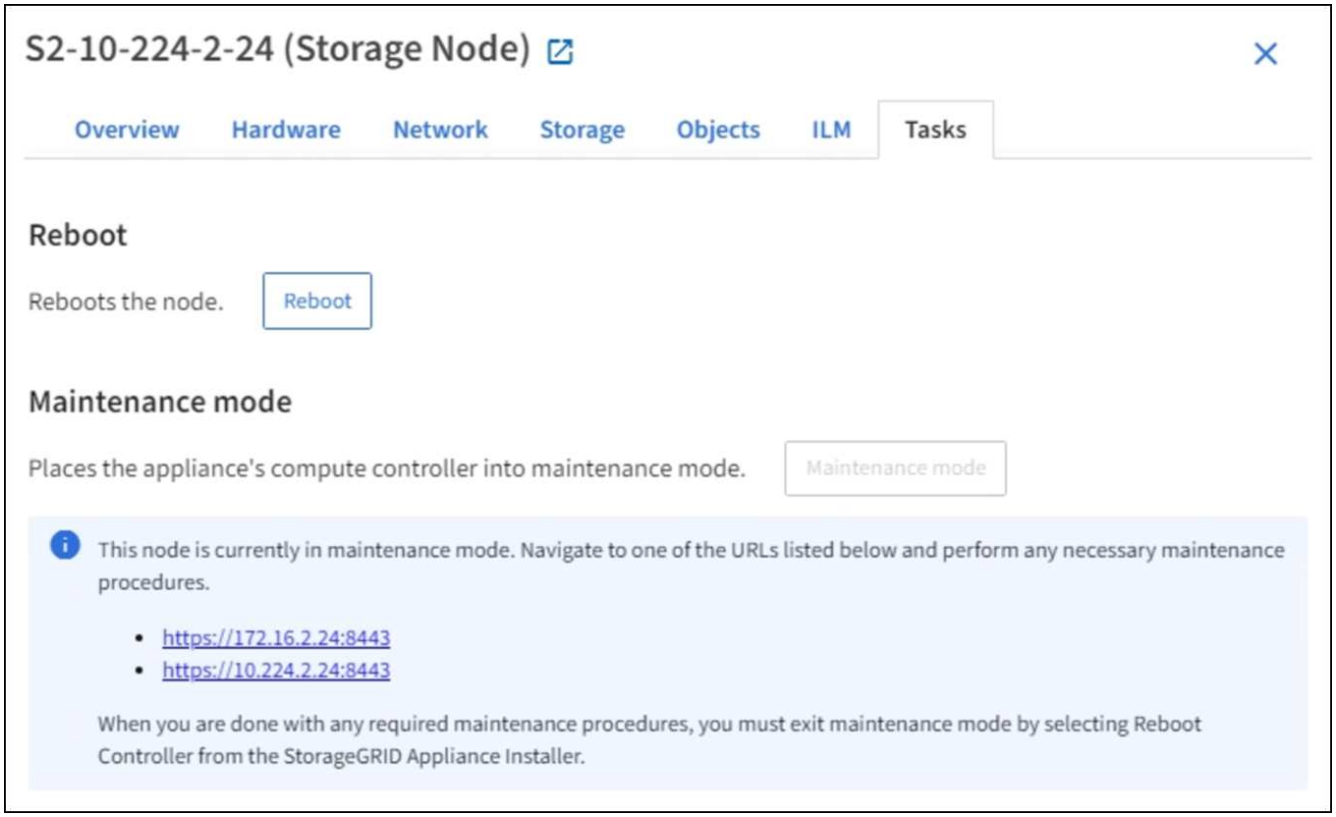


5. 输入配置密码短语，然后选择 * 确定 * 。

   进度条和一系列消息（包括 " 已发送请求 " ， " 正在停止 StorageGRID " 和 " 正在重新启动 " ）表示设备正在完成进入维护模式的步骤。



   设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL 。



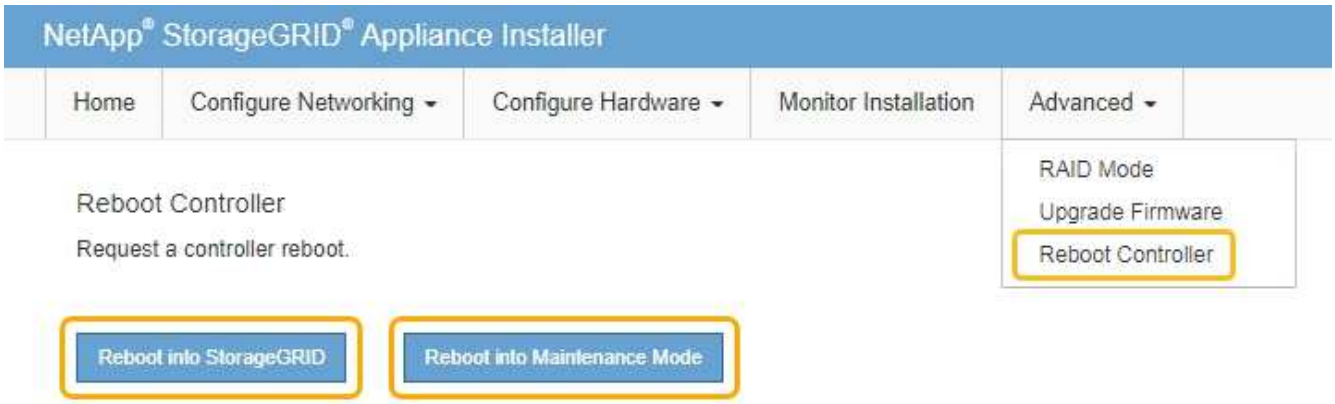
6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL 。

   如果可能，请使用包含设备管理网络端口 IP 地址的 URL 。

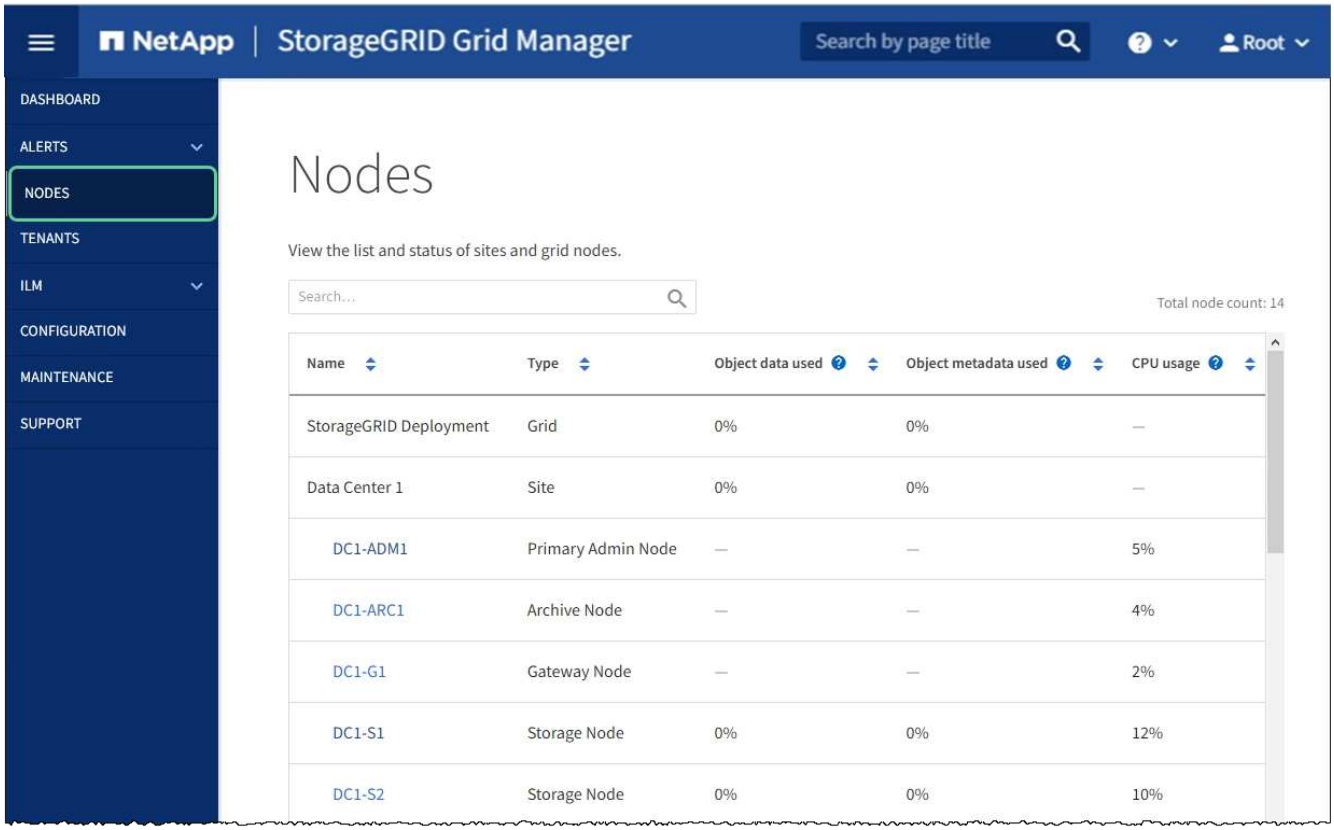
   > 如果您直接连接到设备的管理端口，请使用 ` https://169.254.0.1:8443` 访问 StorageGRID 设备安装程序页面。

7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。

8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



升级存储控制器上的 **SANtricity** 操作系统

为了确保存储控制器能够以最佳方式运行，您必须升级到适用于您的 StorageGRID 设备的最新 SANtricity 操作系统维护版本。请参考 NetApp 互操作性表工具（ IMT ）来确定应使用的版本。如果需要帮助，请联系技术支持。

根据当前安装的 SANtricity OS 版本，使用以下过程之一：

- 如果存储控制器使用的是 SANtricity OS 08.42.20.00 （ 11.42 ）或更高版本，请使用网格管理器执行升级。

  使用网格管理器升级存储控制器上的 SANtricity 操作系统

- 如果存储控制器使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ），请使用维护模式执行升级。

  使用维护模式升级存储控制器上的 SANtricity 操作系统

> 升级存储设备的 SANtricity 操作系统时，必须按照 StorageGRID 文档中的说明进行操作。如果您使用任何其他说明，则设备可能无法运行。

相关信息

"NetApp 互操作性表工具"

"NetApp下载：StorageGRID 设备"

监控和故障排除

使用网格管理器升级存储控制器上的 **SANtricity** 操作系统

对于当前使用 SANtricity OS 08.42.20.00 （ 11.42 ）或更高版本的存储控制器，您必须使用网格管理器应用升级。

您需要的内容

- 您已查阅 NetApp 互操作性表工具（ IMT ）以确认用于升级的 SANtricity 操作系统版本与您的设备兼容。
- 您具有维护或 root 访问权限。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有配置密码短语。
- 您可以访问 SANtricity 操作系统的 NetApp 下载页面。

关于此任务

在完成 SANtricity 操作系统升级过程之前，您无法执行其他软件更新（ StorageGRID 软件升级或修补程序）。如果您尝试在 SANtricity 操作系统升级过程完成之前启动修补程序或 StorageGRID 软件升级，则系统会重定向到 SANtricity 操作系统升级页面。

只有在 SANtricity 操作系统升级成功应用于已选择进行升级的所有适用节点之后，操作步骤 才会完成。在每个节点上（按顺序）加载 SANtricity 操作系统可能需要 30 分钟以上的时间，并且最多需要 90 分钟来重新启动每个 StorageGRID 存储设备。

> 只有在使用网格管理器执行升级时，以下步骤才适用。如果设备中的存储控制器使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ），则无法使用网格管理器进行升级。

> 此操作步骤 会自动将 NVSRAM 升级到与 SANtricity 操作系统升级相关的最新版本。您无需应用单独的 NVSRAM 升级文件。

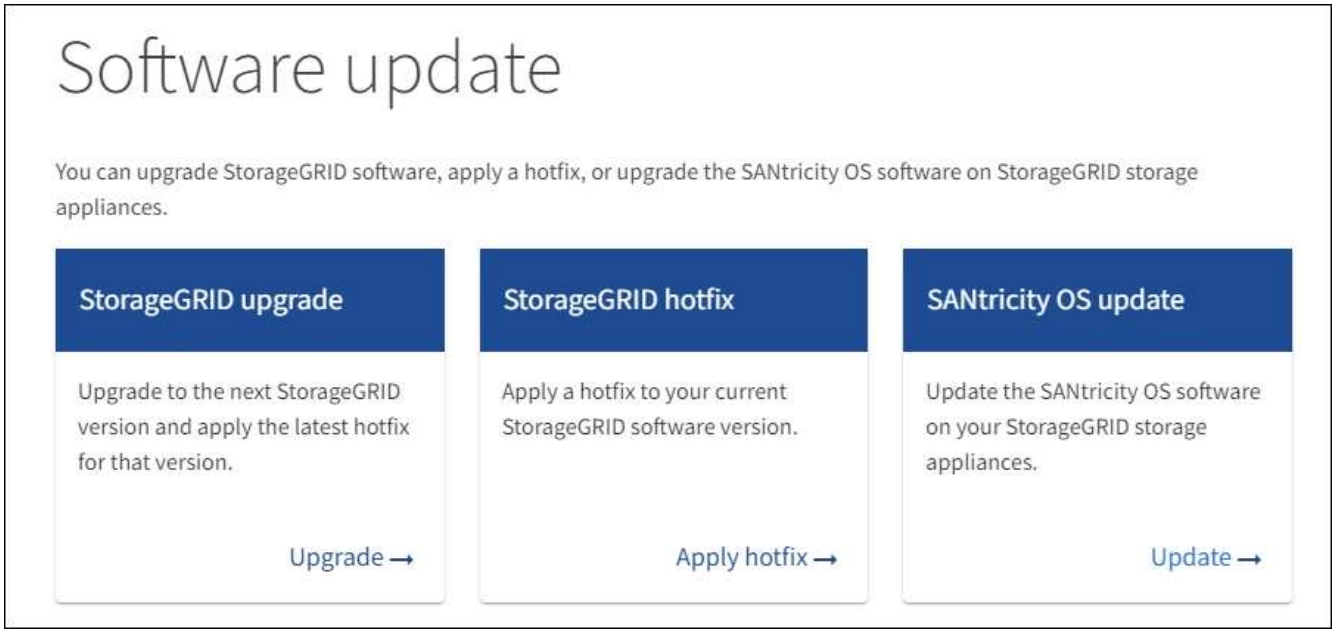
步骤

1. 【下载 _SANtricity 操作系统】从 NetApp 支持站点下载新的 SANtricity 操作系统软件文件。

请务必为存储控制器选择 SANtricity 操作系统版本。

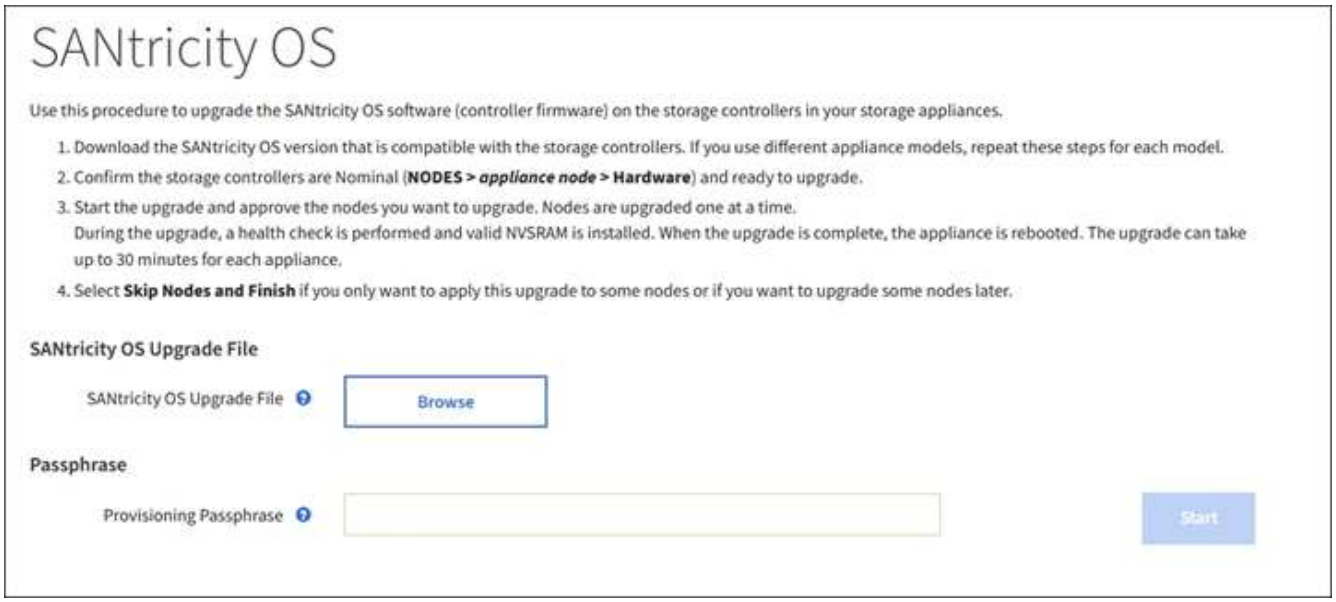
"NetApp下载：StorageGRID 设备"

2. 选择 * 维护 * > * 系统 * > * 软件更新 * 。



3. 在 SANtricity OS update 部分中，选择 * 更新 * 。

此时将显示 SANtricity OS 升级页面。



4. 选择从 NetApp 支持站点下载的 SANtricity OS 升级文件。

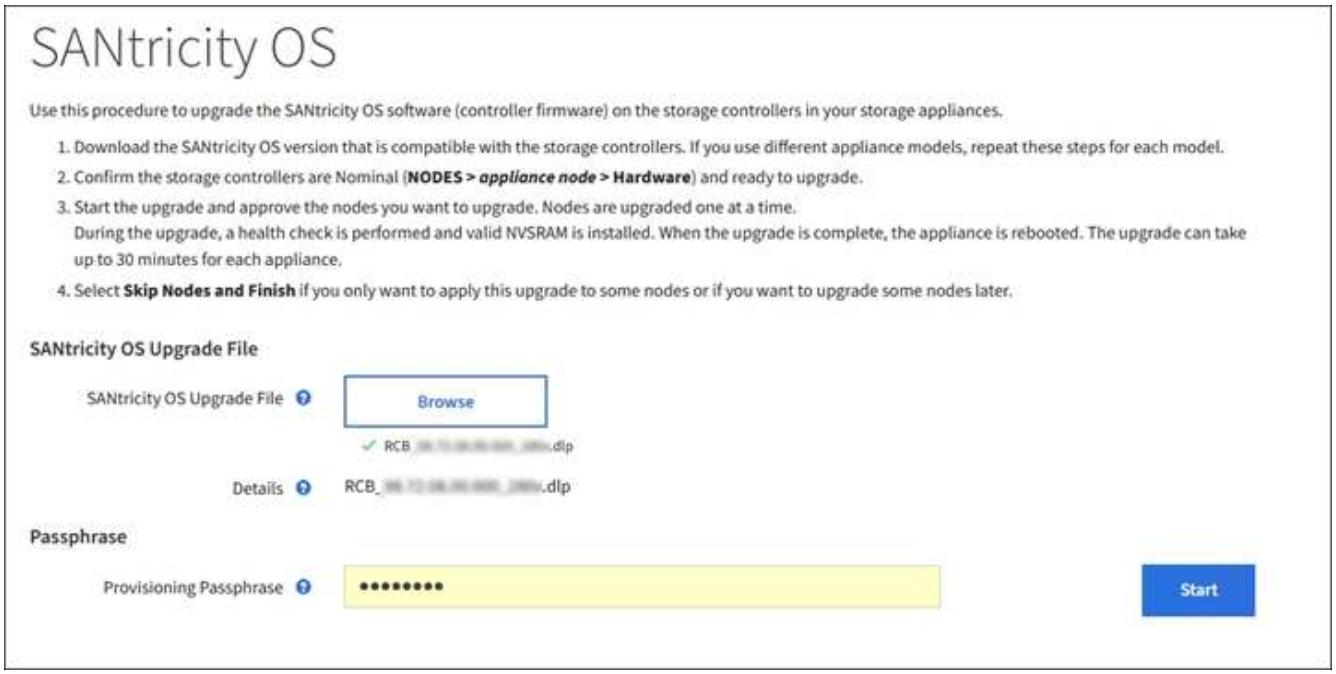
   a. 选择 * 浏览 * 。
   b. 找到并选择文件。
   c. 选择 * 打开 * 。

已上传并验证此文件。验证过程完成后，文件名会显示在 * 浏览 * 按钮旁边。

请勿更改文件名，因为它是验证过程的一部分。

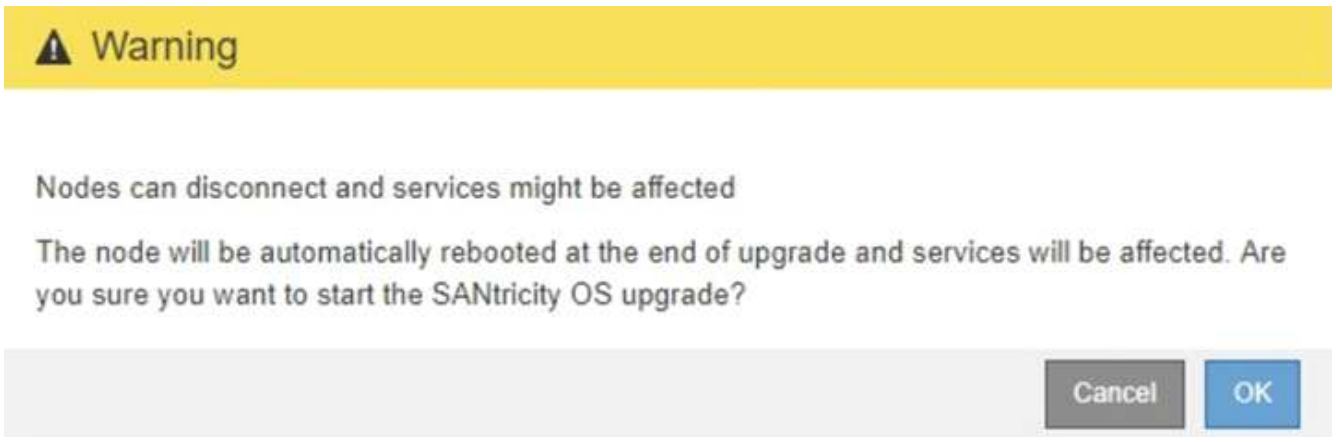
5. 输入配置密码短语。

已启用 * 开始 * 按钮。



6. 选择 * 开始 * 。

此时将显示一个警告框，指出在重新启动已升级的节点上的服务时，浏览器的连接可能会暂时断开。



7. 选择 * 确定 * 将 SANtricity 操作系统升级文件暂存到主管理节点。

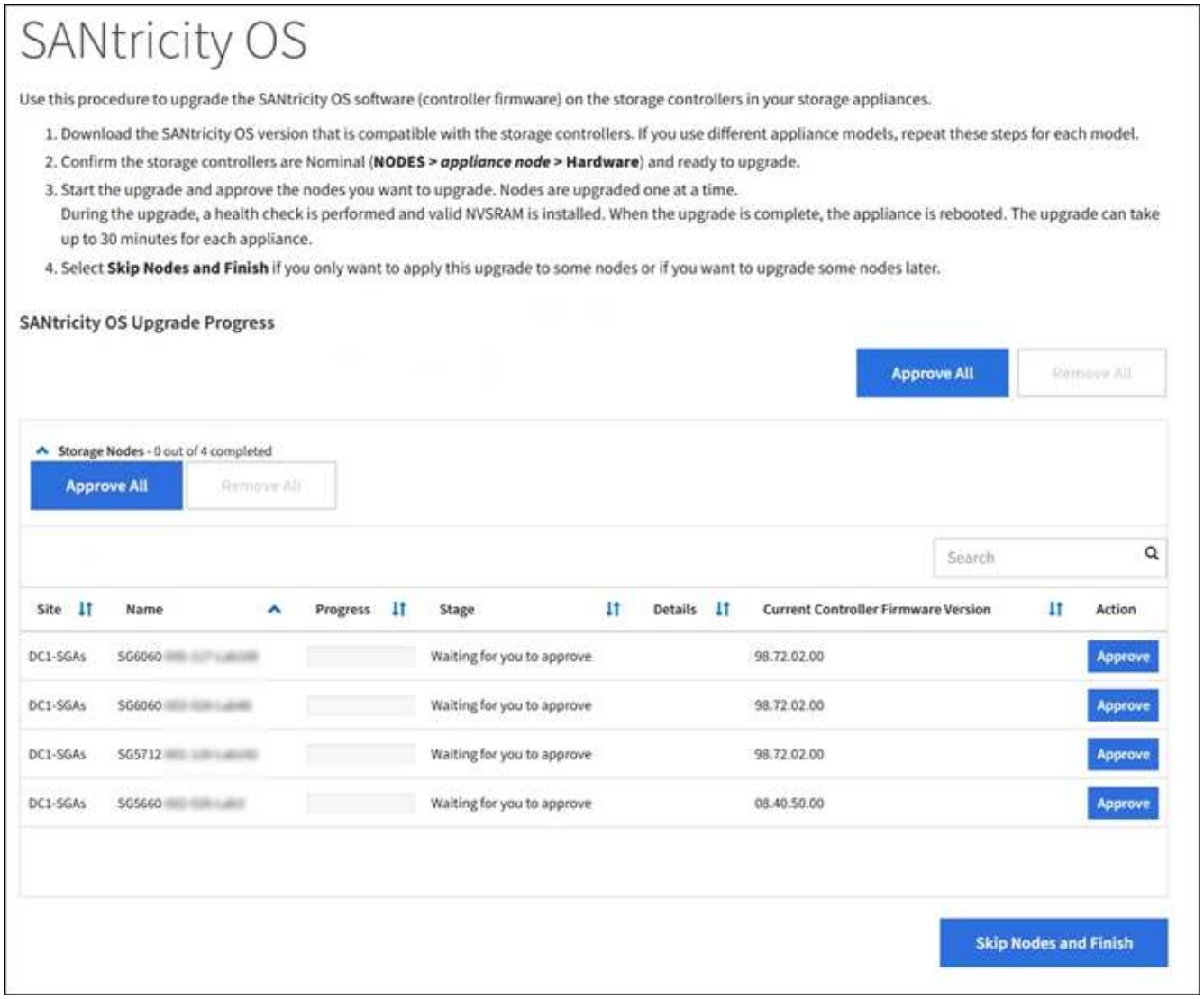
SANtricity 操作系统升级开始时：

a. 运行状况检查已运行。此过程会检查是否没有节点的状态为 "Needs Attention （需要注意） " 。

如果报告了任何错误，请解决这些错误并再次选择 * 启动 * 。

b. 此时将显示 SANtricity 操作系统升级进度表。此表显示了网格中的所有存储节点以及每个节点的当前升级阶段。

此表显示了所有设备存储节点。不会显示基于软件的存储节点。对于需要升级的所有节点，请选择 * 批准 * 。



8. 或者，也可以按 * 站点 * ， * 名称 * ， * 进度 * ， * 阶段 * ， * 详细信息 * 按升序或降序对节点列表进行排序。 或 * 当前控制器固件版本 * 。或者，在 * 搜索 * 框中输入一个术语以搜索特定节点。

   您可以使用此部分右下角的左箭头和右箭头滚动浏览节点列表。

9. 批准已准备好添加到升级队列的网格节点。相同类型的已批准节点将一次升级一个。

   请勿批准设备存储节点的 SANtricity 操作系统升级，除非您确定该节点已做好停止和重新启动的准备。在某个节点上批准 SANtricity 操作系统升级后，该节点上的服务将停止，升级过程将开始。稍后，当节点完成升级后，设备节点将重新启动。对于与节点通信的客户端，这些操作可能会导致发生原因 服务中断。

   ◦ 选择 * 全部批准 * 按钮之一，将所有存储节点添加到 SANtricity 操作系统升级队列。

如果节点升级顺序非常重要，请一次批准一个节点或一组节点，并等待每个节点完成升级，然后再批准下一个节点。

- 选择一个或多个 * 批准 * 按钮将一个或多个节点添加到 SANtricity OS 升级队列。

  选择 * 批准 * 后，升级过程将确定是否可以升级此节点。如果某个节点可以升级，则会将其添加到升级队列中。

对于某些节点，不会有意应用选定的升级文件，您可以在不升级这些特定节点的情况下完成升级过程。有意未升级的节点会显示完成阶段（已尝试升级），并在详细信息列中列出未升级此节点的原因。

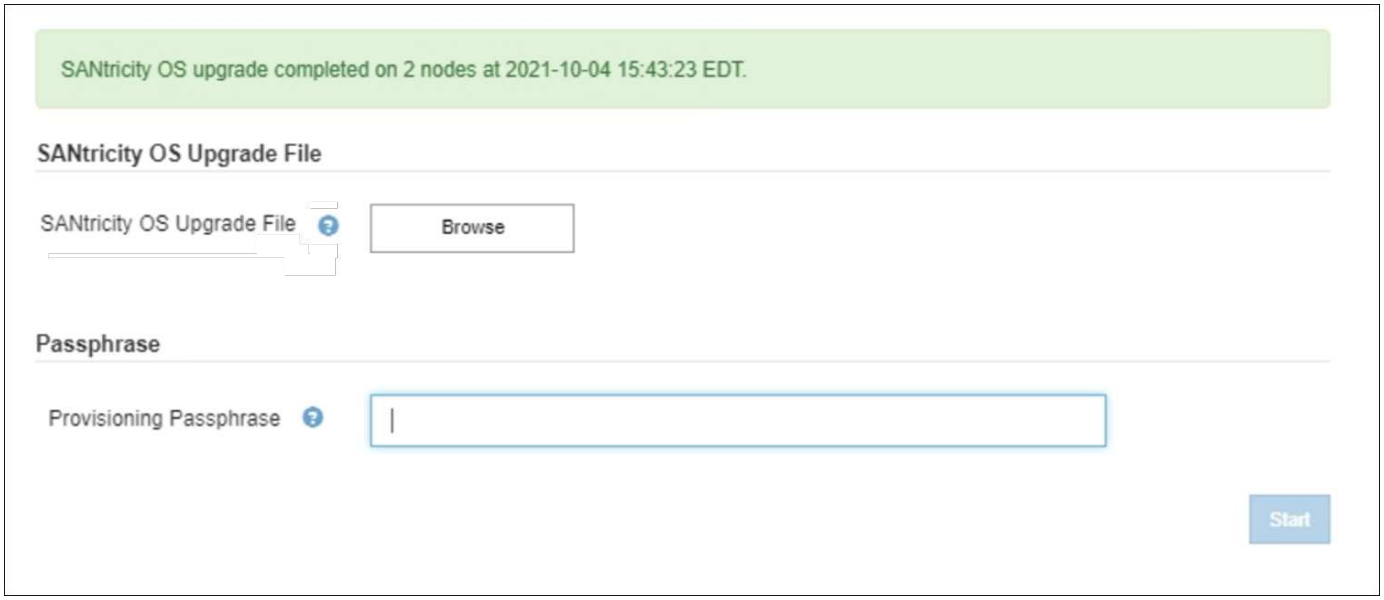
10. 如果需要从 SANtricity 操作系统升级队列中删除一个或所有节点，请选择 * 删除 * 或 * 全部删除 * 。

    当此阶段超过已排队时， * 删除 * 按钮将处于隐藏状态，您无法再从 SANtricity 操作系统升级过程中删除此节点。

11. 等待 SANtricity 操作系统升级应用于每个批准的网格节点。

    - 如果在应用 SANtricity 操作系统升级期间任何节点显示错误阶段，则此节点的升级将失败。在技术支持的协助下，您可能需要将设备置于维护模式才能进行恢复。
    - 如果节点上的固件版本太旧，无法使用网格管理器进行升级，则节点将显示错误阶段并提供详细信息："`您必须使用维护模式升级此节点上的 SANtricity OS 。请参见适用于您的设备的安装和维护说明。升级后，您可以使用此实用程序进行将来的升级。` 要解决此错误，请执行以下操作：
      i. 使用维护模式升级显示 " 错误 " 阶段的节点上的 SANtricity OS 。
      ii. 使用网格管理器重新启动并完成 SANtricity 操作系统升级。

    在所有已批准的节点上完成 SANtricity 操作系统升级后， SANtricity 操作系统升级进度表将关闭，绿色横幅将显示 SANtricity 操作系统升级完成的日期和时间。



1. 如果节点无法升级，请记下 "Details" 列中显示的原因并采取相应的措施：
   - " s存储节点已升级。 " 无需执行进一步操作。
   - "`SANtricity 操作系统升级不适用于此节点。` " 此节点没有可由 StorageGRID 系统管理的存储控制器。

完成升级过程，而不升级显示此消息的节点。

- "`SANtricity OS 文件与此节点不兼容。` " 节点所需的 SANtricity 操作系统文件与您选择的文件不同。完成当前升级后，下载适用于此节点的正确 SANtricity OS 文件，然后重复升级过程。

> 只有在所有列出的存储节点上批准 SANtricity 操作系统升级后， SANtricity 操作系统升级过程才会完成。

1. 如果要结束节点批准并返回到 SANtricity OS 页面以允许上传新的 SANtricity OS 文件，请执行以下操作：

   a. 选择 * 跳过节点并完成 * 。

      此时将显示一条警告，询问您是否确实要在不升级所有节点的情况下完成升级过程。

   b. 选择 * 确定 * 返回到 * SANtricity OS* 页面。

   c. 准备好继续批准节点后，请转至 下载 SANtricity 操作系统 重新启动升级过程。

   > 已批准并升级的节点仍保持升级状态，而不会出现错误。

2. 对处于完成阶段且需要其他 SANtricity 操作系统升级文件的所有节点重复此升级操作步骤 。

   > 对于状态为 "Needs Attenance" 的任何节点，请使用维护模式执行升级。

   > 重复升级操作步骤 时，您必须批准先前升级的节点。

相关信息

"NetApp 互操作性表工具"

使用维护模式升级存储控制器上的 SANtricity 操作系统

使用维护模式升级存储控制器上的 **SANtricity** 操作系统

对于当前使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ）的存储控制器，您必须使用维护模式操作步骤 来应用升级。

您需要的内容

- 您已查阅 NetApp 互操作性表工具（ IMT ）以确认用于升级的 SANtricity 操作系统版本与您的设备兼容。
- 如果StorageGRID 设备在StorageGRID 系统中运行、则表示SG6000-CN控制器已运行 置于维护模式。

> 维护模式会中断与存储控制器的连接。

关于此任务

请勿一次在多个 StorageGRID 设备上升级 E 系列控制器中的 SANtricity 操作系统或 NVSRAM 。

> 一次升级多个 StorageGRID 设备可能会导致发生原因 数据不可用，具体取决于您的部署模式和 ILM 策略。

步骤

1. 确认设备已进入 维护模式。
2. 从服务笔记本电脑访问 SANtricity 系统管理器并登录。
3. 将新的 SANtricity OS 软件文件和 NVSRAM 文件下载到管理客户端。

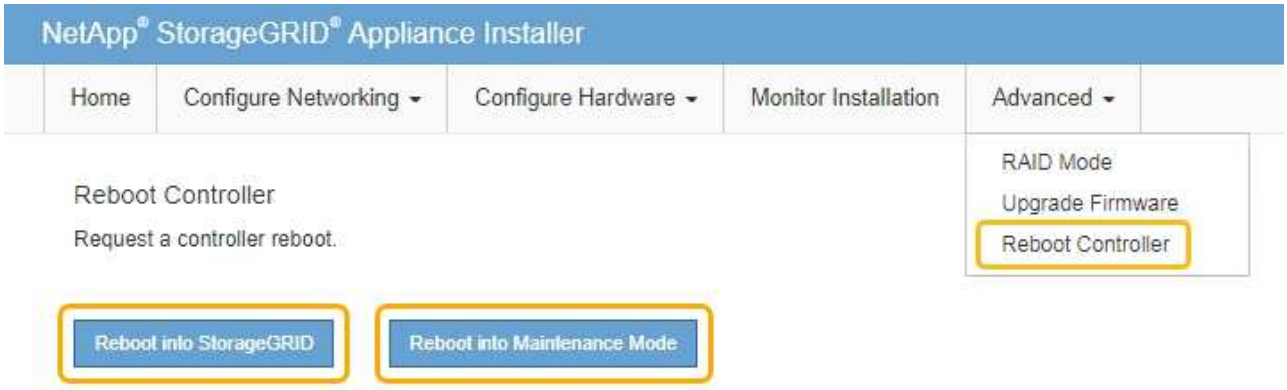
   NVSRAM 是特定于 StorageGRID 设备的。请勿使用标准 NVSRAM 下载。

4. 按照 *upgrading SANtricity OS* 指南或 SANtricity 系统管理器联机帮助中的说明升级固件和 NVSRAM 。

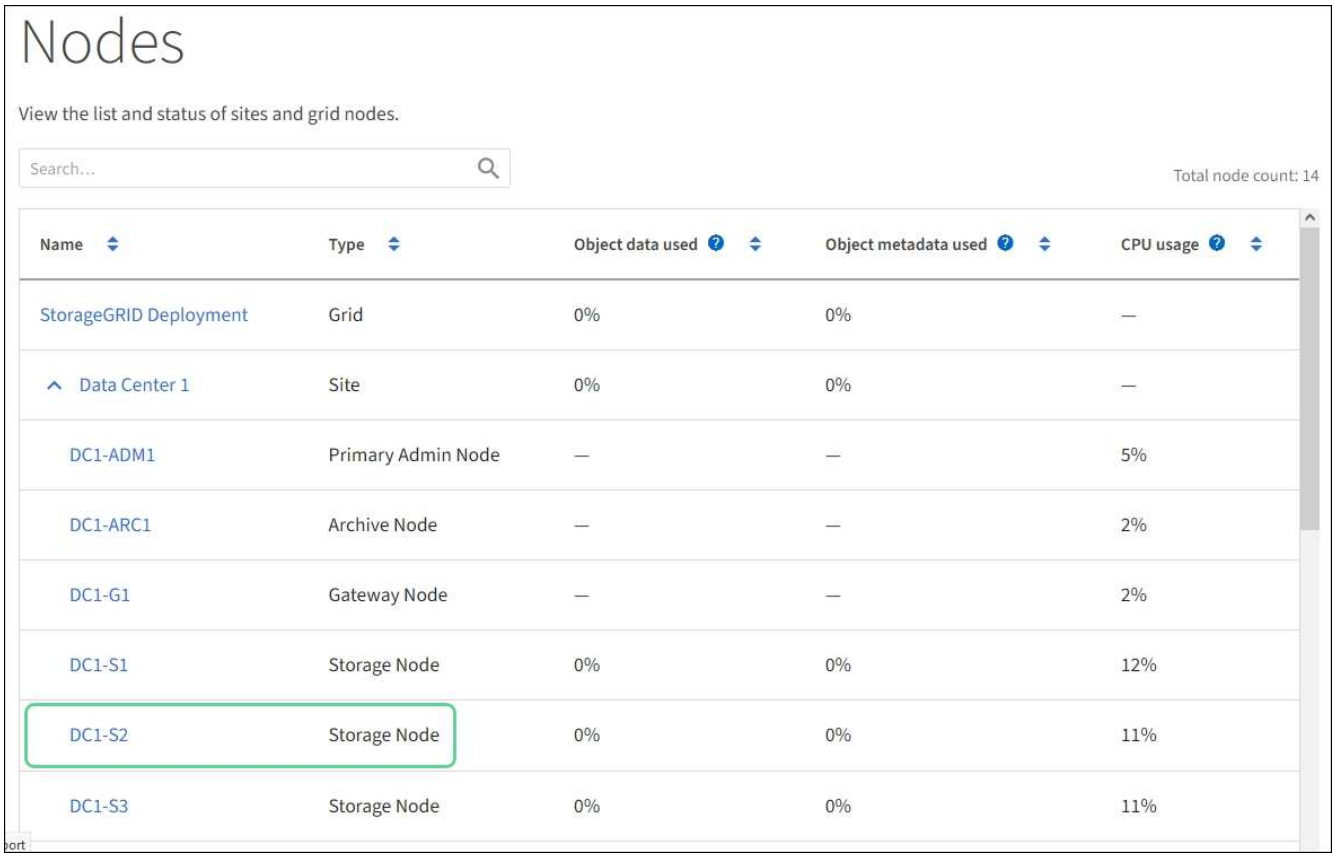
   立即激活升级文件。请勿延迟激活。

5. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。节点页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

"NetApp 互操作性表工具"

使用网格管理器升级存储控制器上的 SANtricity 操作系统

使用 **SANtricity** 系统管理器升级驱动器固件

您可以升级驱动器固件，以确保具有所有最新功能和错误修复。

您需要的内容

- 存储设备处于最佳状态。
- 所有驱动器均处于最佳状态。
- 您已安装与您的 SANtricity 版本兼容的最新版本 StorageGRID System Manager 。
- 您已拥有 已将 StorageGRID 设备置于维护模式。

> 维护模式会中断与存储控制器的连接，停止所有 I/O 活动并使所有驱动器脱机。

> 请勿一次升级多个 StorageGRID 设备上的驱动器固件。这样做可能会导致发生原因 数据不可用，具体取决于您的部署模式和 ILM 策略。

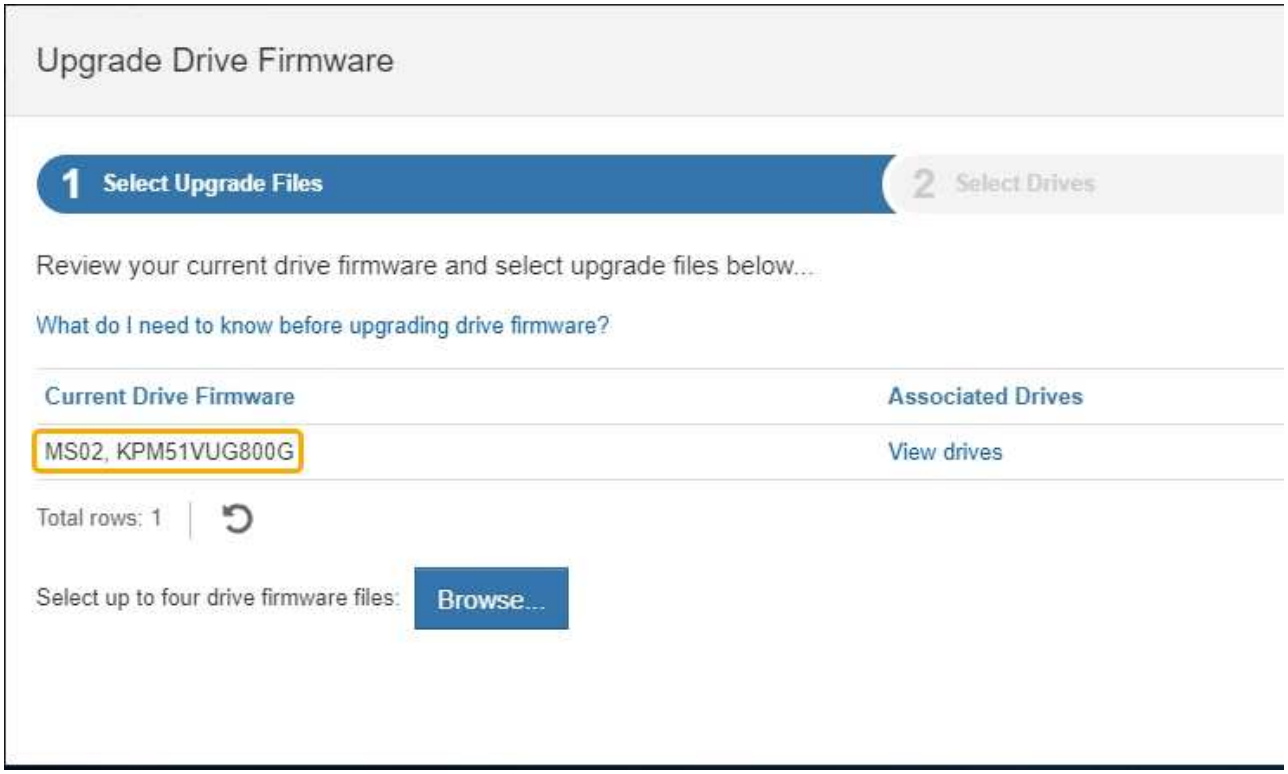
步骤

1. 确认此设备已位于中 维护模式。

2. 使用以下方法之一访问 SANtricity System Manager：
   - 使用 StorageGRID 设备安装程序并选择 * 高级 * > * SANtricity 系统管理器 *
   - 通过浏览到存储控制器 IP： + ` * https://*Storage_Controller_IP*` 来使用 SANtricity 系统管理器
3. 如果需要，输入 SANtricity System Manager 管理员用户名和密码。
4. 验证存储设备中当前安装的驱动器固件版本：
   a. 在 SANtricity 系统管理器中，选择 * 支持 * > * 升级中心 * 。
   b. 在驱动器固件升级下，选择 * 开始升级 * 。

      升级驱动器固件将显示当前安装的驱动器固件文件。

   c. 请在当前驱动器固件列中记下当前驱动器固件版本和驱动器标识符。



      在此示例中：

      - 驱动器固件修订版为 * 。 MS02* 。
      - 驱动器标识符为 * 。 KPM51 VVG800G* 。

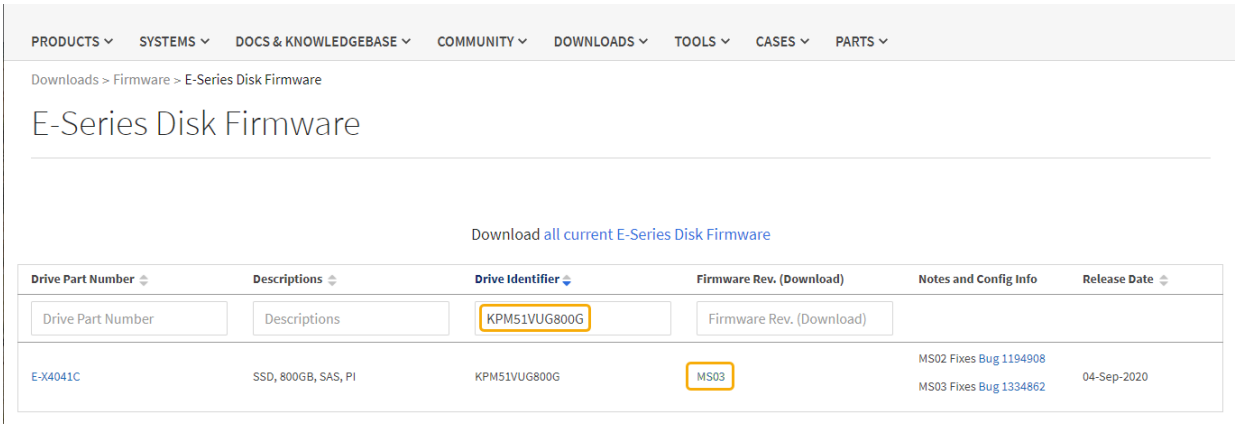
   在关联驱动器列中选择 * 查看驱动器 * ，以显示这些驱动器在存储设备中的安装位置。

   a. 关闭升级驱动器固件窗口。
5. 下载并准备可用的驱动器固件升级：
   a. 在驱动器固件升级下，选择 * NetApp 支持 * 。
   b. 在 NetApp 支持网站上，选择 * 下载 * 选项卡，然后选择 * E 系列磁盘驱动器固件 * 。

      此时将显示 E 系列磁盘固件页面。

c. 搜索存储设备中安装的每个 * 驱动器标识符 * ，并验证每个驱动器标识符是否具有最新的固件版本。

- 如果固件版本不是链接，则此驱动器标识符的固件版本为最新。
- 如果为驱动器标识符列出了一个或多个驱动器部件号，则可以对这些驱动器进行固件升级。您可以选择任何链接来下载固件文件。



d. 如果列出了更高版本的固件，请选择固件修订版中的链接（ download ）列以下载包含固件文件的 ` .zip` 归档。

e. 提取（解压缩）从支持站点下载的驱动器固件归档文件。

6. 安装驱动器固件升级：

a. 在 SANtricity 系统管理器的驱动器固件升级下，选择 * 开始升级 * 。

b. 选择 * 浏览 * ，然后选择从支持站点下载的新驱动器固件文件。

驱动器固件文件的文件名类似于 + `D HUC101212CS600_30602291_MS01_2800_0002.DLP` 。

您最多可以选择四个驱动器固件文件，一次一个。如果多个驱动器固件文件与同一驱动器兼容，则会收到文件冲突错误。确定要用于升级的驱动器固件文件，然后删除另一个驱动器固件文件。

c. 选择 * 下一步 * 。

- 选择驱动器 * 列出了可使用选定固件文件进行升级的驱动器。

  仅显示兼容的驱动器。

为驱动器选择的固件将显示在 * 建议的固件 * 中。如果必须更改此固件，请选择 * 返回 * 。

d. 选择 * 脱机（并行） * 升级。

您可以使用脱机升级方法，因为设备处于维护模式，此时所有驱动器和所有卷的 I/O 活动都将停止。

> 除非您确定设备处于维护模式，否则请勿继续。如果在启动脱机驱动器固件更新之前未将设备置于维护模式，则可能会丢失发生原因 数据。

e. 在表的第一列中，选择要升级的一个或多个驱动器。

最佳实践是，将所有相同型号的驱动器升级到相同的固件修订版。

f. 选择 * 开始 * ，然后确认要执行升级。

如果需要停止升级，请选择 * 停止 * 。当前正在进行的所有固件下载均已完成。已取消所有尚未启动的固件下载。

停止驱动器固件升级可能会导致数据丢失或驱动器不可用。

g. （可选）要查看已升级内容的列表，请选择 * 保存日志 * 。

此日志文件将保存在浏览器的下载文件夹中，名称为 `latest-upgrade-log-timestamp.txt` 。

如果在升级操作步骤期间出现以下任何错误，请采取适当的建议操作。

- * 已分配的驱动器出现故障 *

  出现此故障的一个原因可能是驱动器没有相应的签名。确保受影响的驱动器为授权驱动器。有关详细信息，请联系技术支持。

更换驱动器时，请确保更换驱动器的容量等于或大于要更换的故障驱动器。

您可以在存储阵列接收 I/O 时更换故障驱动器

- * 检查存储阵列 *
  - 确保已为每个控制器分配 IP 地址。
  - 确保连接到控制器的所有缆线均未损坏。
  - 确保所有缆线均已紧密连接。
- * 集成热备用驱动器 *

  必须先更正此错误情况，然后才能升级固件。

- * 卷组不完整 *

  如果一个或多个卷组或磁盘池不完整，则必须更正此错误情况，然后才能升级固件。

- * 当前正在任何卷组上运行的独占操作（后台介质 / 奇偶校验扫描除外） *

  如果正在执行一个或多个独占操作，则必须先完成这些操作，然后才能升级固件。使用 System Manager 监控操作进度。

- * 缺少卷 *

  您必须先更正缺少的卷情况，然后才能升级固件。

- * 任一控制器处于非最佳状态 *

  其中一个存储阵列控制器需要注意。必须先更正此情况，然后才能升级固件。

- 控制器对象图形之间的存储分区信息不匹配 *

  验证控制器上的数据时出错。请联系技术支持以解决此问题描述。

- * SPM 验证数据库控制器检查失败 *

  控制器上发生存储分区映射数据库错误。请联系技术支持以解决此问题描述。

- * 配置数据库验证（如果存储阵列的控制器版本支持） *

  控制器上发生配置数据库错误。请联系技术支持以解决此问题描述。

- * 与 MEL 相关的检查 *

  请联系技术支持以解决此问题描述。

- * 在过去 7 天内报告了 10 个以上的 DDN 信息性或严重 MEL 事件 *

  请联系技术支持以解决此问题描述。

- * 过去 7 天报告了 2 页以上的 2C 严重 MEL 事件 *

  请联系技术支持以解决此问题描述。

- * 过去 7 天报告了 2 个以上的 " 降级驱动器通道 " 严重 MEL 事件 *

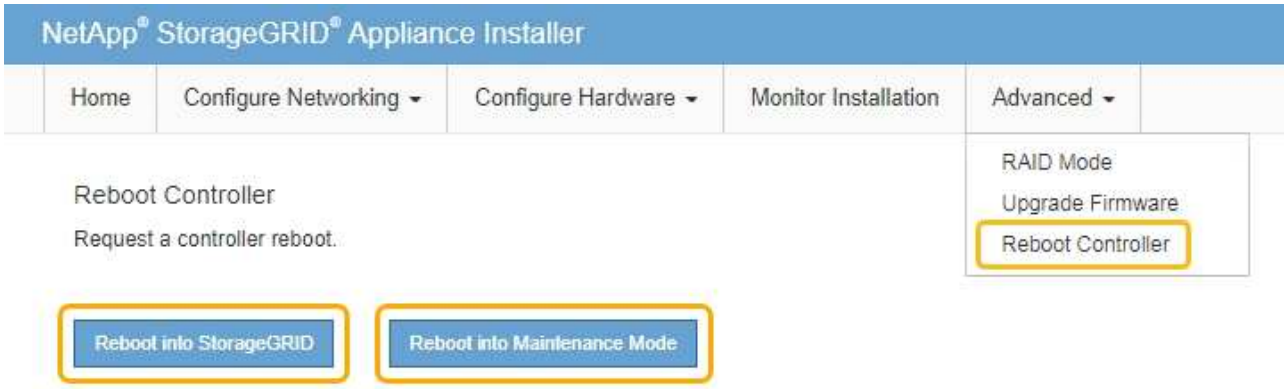
  请联系技术支持以解决此问题描述。

- * 过去 7 天内 4 个以上的关键 MEL 条目 *

  请联系技术支持以解决此问题描述。

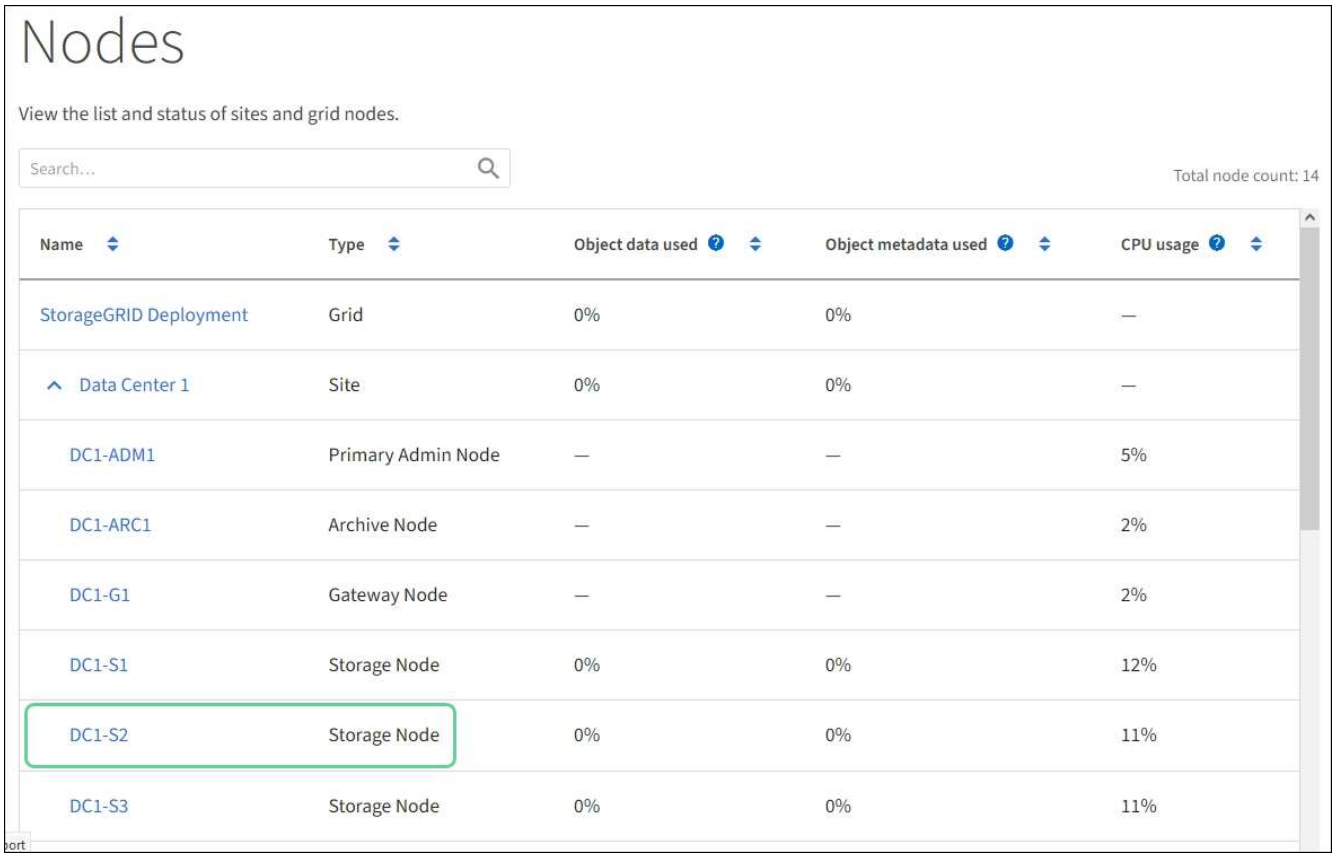
7. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。节点页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处

于活动状态的警报，并且节点已连接到网格。



相关信息

升级存储控制器上的 SANtricity 操作系统

将扩展架添加到已部署的 **SG6060**

要增加存储容量、您可以向StorageGRID 系统中已部署的SG6060或SG6060X添加一个或两个扩展架。

您需要的内容

- 您必须具有配置密码短语。
- 您必须运行 StorageGRID 11.4 或更高版本。
- 每个扩展架都有扩展架和两根 SAS 缆线。
- 您已将要在数据中心中添加扩展架的存储设备物理定位。

  在数据中心中找到控制器

关于此任务

要添加扩展架，请执行以下高级步骤：

- 在机柜或机架中安装硬件。
- 将SG6060或SG6060X置于维护模式。

- 将扩展架连接到 E2860 控制器架或其他扩展架。
- 使用 StorageGRID 设备安装程序启动扩展
- 请稍候，直到配置完新卷为止。

每个设备节点为一个或两个扩展架完成操作步骤 所需时间应至少为一小时。为了最大限度地减少停机时间、以下步骤将指导您在将SG6060或SG6060X置于维护模式之前安装新的扩展架和驱动器。每个设备节点的其余步骤大约需要 20 到 30 分钟。

步骤

1. 按照说明将 60 个驱动器磁盘架安装到机柜或机架中。

   SG6060和SG6060X：将60个驱动器磁盘架安装到机柜或机架中

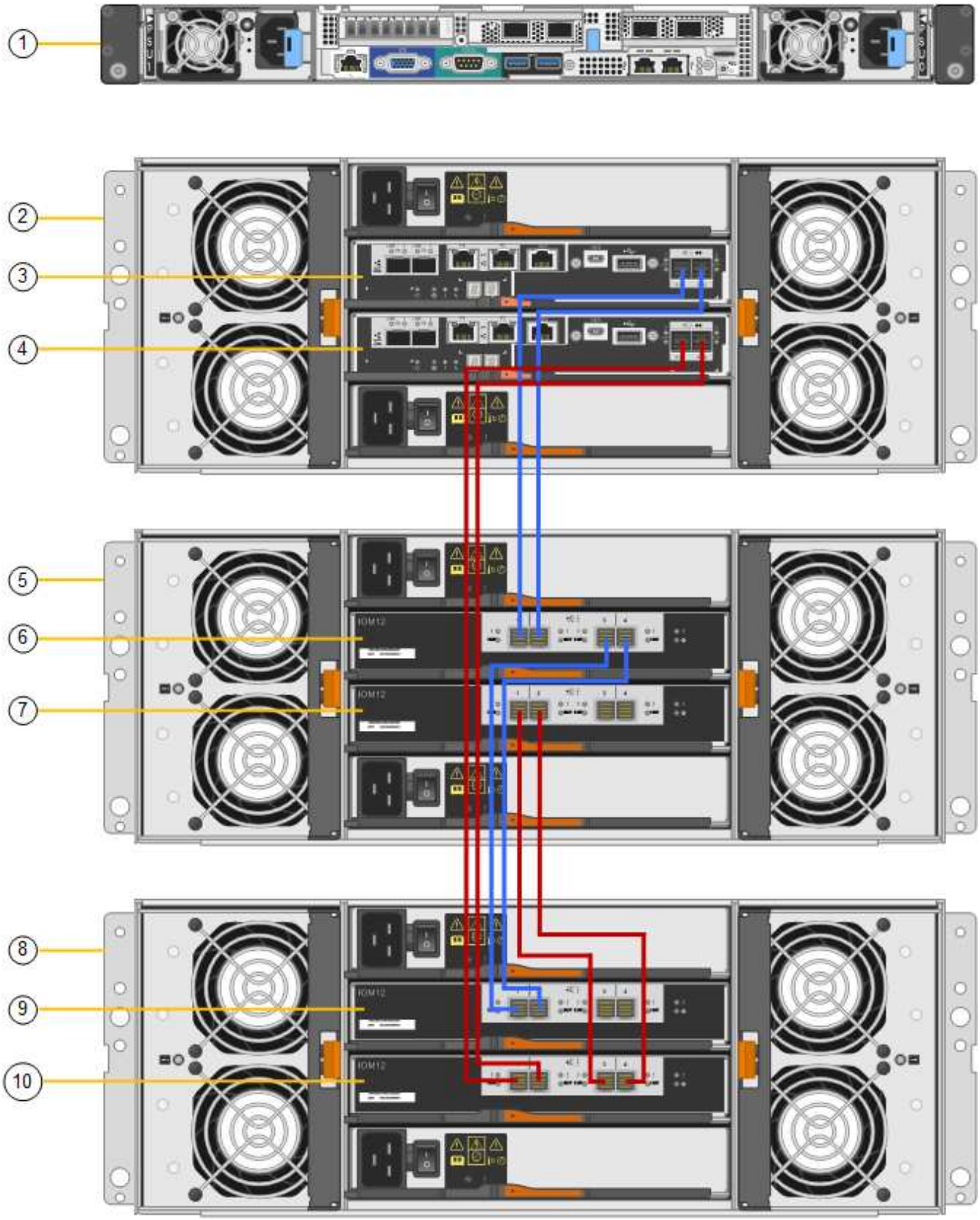
2. 按照说明安装驱动器。

   SG6060和SG6060X：安装驱动器

3. 在网格管理器中， 将 SG6000-CN 控制器置于维护模式。
4. 将每个扩展架连接到 E2860 控制器架，如图所示。

   此图显示了两个扩展架。如果只有一个，请将 IOM A 连接到控制器 A ，并将 IOM B 连接到控制器 B

   图中显示了SG6060。SG6060X的扩展布线相同。



Callout	Description
1.	SG6000-CN

Callout	Description
2.	E2860 控制器架
3.	控制器 A
4.	控制器 B
5.	扩展架 1
6.	扩展架 1 的 IOM A
7.	扩展架 1 的 IOM B
8.	扩展架 2.
9	扩展架 2 的 IOM A
10	扩展架 2 的 IOM B

5. 连接电源线并为扩展架通电。
   a. 将电源线连接到每个扩展架中的两个电源设备中的每个设备。
   b. 将每个扩展架中的两条电源线连接到机柜或机架中的两个不同 PDU 。
   c. 打开每个扩展架的两个电源开关。
      - 请勿在启动过程中关闭电源开关。
      - 首次启动时，扩展架中的风扇可能会发出很大的声音。启动期间发出较大的噪音是正常的。
6. 监控 StorageGRID 设备安装程序的主页页面。

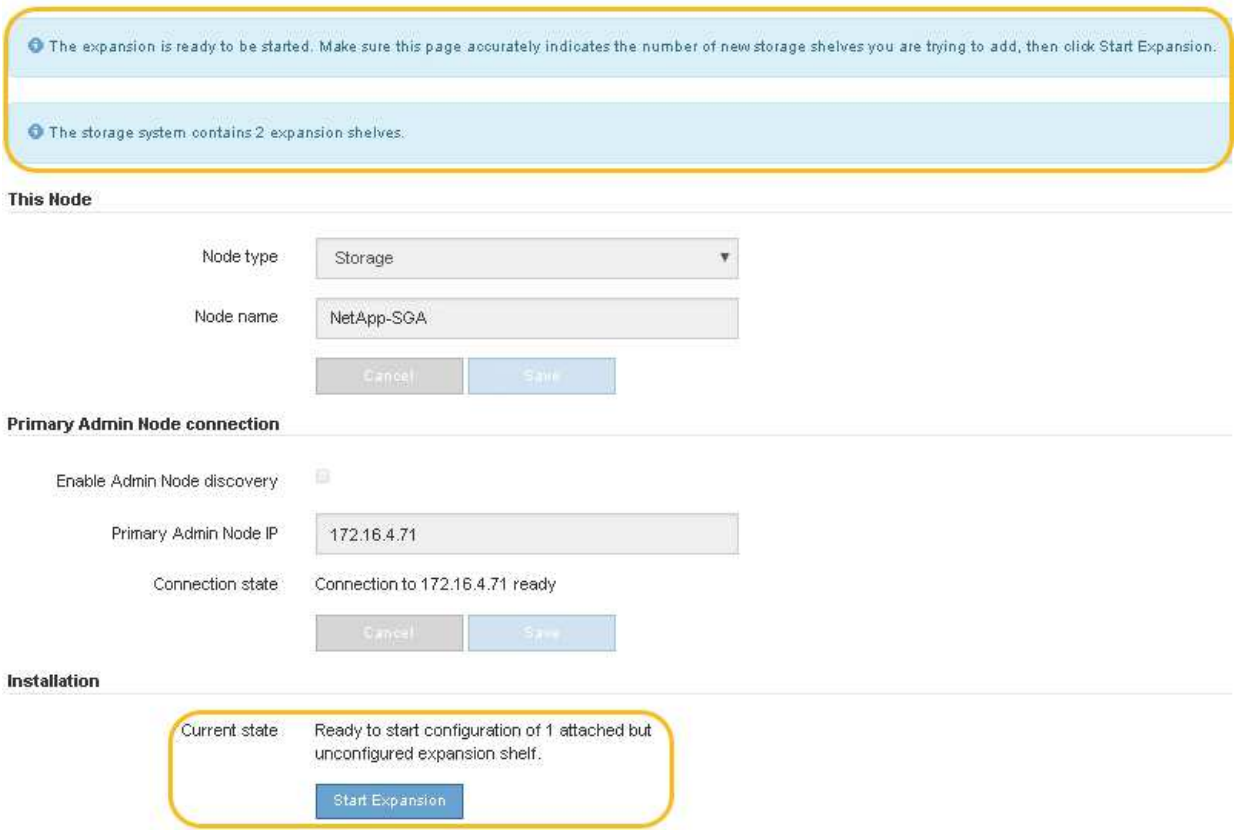
   大约五分钟后，扩展架将完成启动，系统会检测到这些扩展架。主页页面将显示检测到的新扩展架数量，并且已启用开始扩展按钮。

   屏幕截图显示了主页上可能显示的消息示例，具体取决于现有或新扩展架的数量，如下所示：

   - 此页面顶部圈出的横幅指示检测到的扩展架总数。
     - 此横幅将指示扩展架的总数，无论是已配置和部署磁盘架，还是新磁盘架和未配置磁盘架。
     - 如果未检测到扩展架，则不会显示横幅。
   - 页面底部圆圈内的消息表示扩展已准备就绪，可以启动。
     - 此消息指示 StorageGRID 检测到的新扩展架数量。"`Attached` " 表示检测到磁盘架。"`Unconfigured` " 表示磁盘架为新磁盘架，尚未使用 StorageGRID 设备安装程序进行配置。

     此消息不包含已部署的扩展架。它们包含在页面顶部横幅的计数中。

- 如果未检测到新的扩展架，则不会显示此消息。



7. 如有必要，请解决主页上的消息中所述的任何问题。

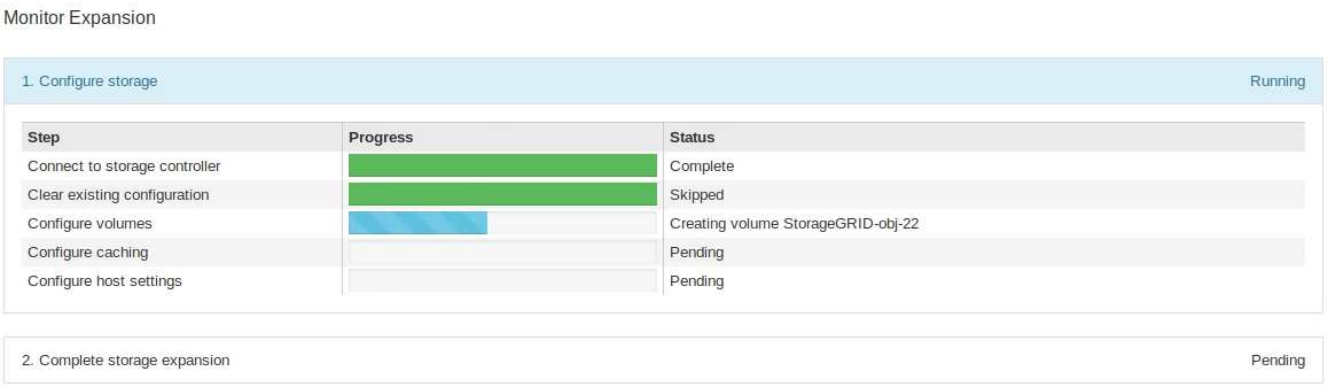
   例如，使用 SANtricity 系统管理器解决任何存储硬件问题。

8. 验证主页上显示的扩展架数量是否与要添加的扩展架数量匹配。

   如果未检测到新的扩展架，请验证它们是否已正确布线并已启动。

9. [start_expand]] 单击 * 启动扩展 * 以配置扩展架并使其可用于对象存储。
10. 监控扩展架配置的进度。

    进度条会显示在网页上，就像在初始安装期间一样。



配置完成后，设备将自动重新启动以退出维护模式并重新加入网格。此过程可能需要长达 20 分钟。

> 要在扩展架配置失败时重试此配置，请转到 StorageGRID 设备安装程序，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至维护模式 * 。节点重新启动后，重试 扩展架配置。

重新启动完成后， * 任务 * 选项卡将显示以下屏幕截图：

11. 验证设备存储节点和新扩展架的状态。
    a. 在网格管理器中，选择 * 节点 * 并验证设备存储节点是否具有绿色复选标记图标。

       绿色复选标记图标表示没有处于活动状态的警报，并且节点已连接到网格。有关节点图标的问题描述，请参见有关 StorageGRID 监控和故障排除的说明。

    b. 选择 * 存储 * 选项卡，然后确认添加的每个扩展架的对象存储表中显示了 16 个新的对象存储。
    c. 验证每个新扩展架的磁盘架状态是否为标称，配置状态是否为已配置。

相关信息

打开包装箱(SG6000和SG6060X)

SG6060和SG6060X：将60个驱动器磁盘架安装到机柜或机架中

SG6060和SG6060X：安装驱动器

监控和故障排除

打开和关闭控制器标识 **LED**

可以打开控制器正面和背面的蓝色标识 LED ，以帮助在数据中心中找到设备。

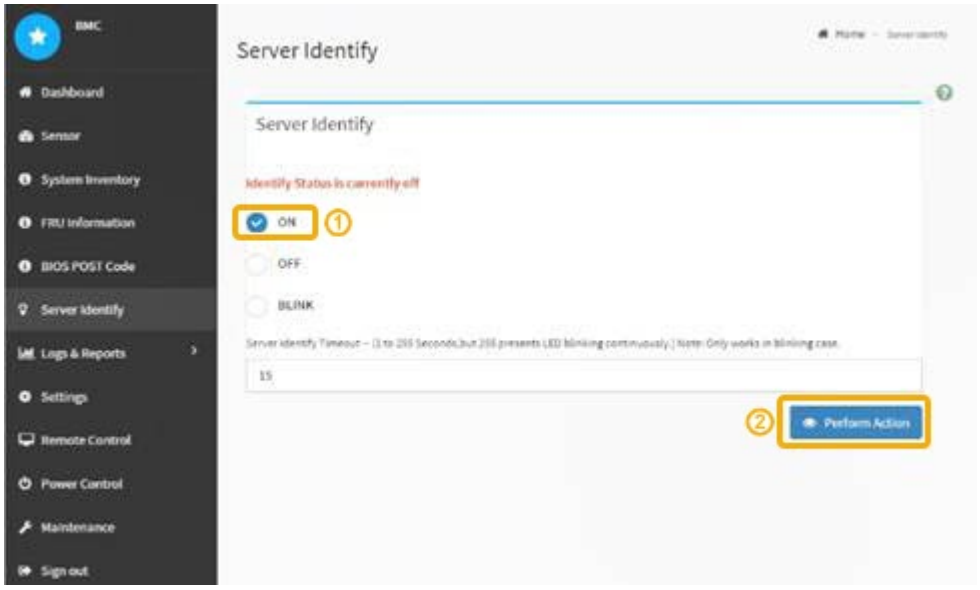
您需要的内容

您必须具有要标识的控制器的 BMC IP 地址。

步骤

1. 访问控制器 BMC 界面。

2. 选择 * 服务器标识 * 。
3. 选择 * 开 * ，然后选择 * 执行操作 * 。



结果

控制器正面（如图所示）和背面的蓝色标识 LED 亮起。

如果控制器上安装了挡板，则可能很难看到正面的识别 LED 。

完成后

要关闭控制器识别 LED ，请执行以下操作：

- 按下控制器前面板上的识别 LED 开关。
- 从控制器 BMC 界面中，选择 * 服务器标识 * ，选择 * 关闭 * ，然后选择 * 执行操作 * 。

控制器正面和背面的蓝色标识 LED 熄灭。

相关信息

确认要更换的光纤通道 HBA

在数据中心中找到控制器

访问 BMC 界面

在数据中心中找到控制器

找到控制器，以便执行硬件维护或升级。

您需要的内容

- 您已确定哪个控制器需要维护。

  （可选）要帮助查找数据中心中的控制器，请打开蓝色的 "Identify" LED 。

  打开和关闭控制器标识 LED

步骤

1. 在数据中心中查找需要维护的控制器。

   - 查看控制器正面或背面的蓝色标识 LED 是否亮起。

     正面识别 LED 位于控制器前挡板后面，如果已安装挡板，可能很难查看。

- 检查每个控制器正面附加的标签，以获取匹配的部件号。

2. 卸下控制器前挡板（如果已安装），以访问前面板控件和指示灯。
3. 可选：如果您使用蓝色标识 LED 来查找控制器，请将其关闭。
   - 按下控制器前面板上的识别 LED 开关。
   - 使用控制器 BMC 界面。

     打开和关闭控制器标识 LED

相关信息

删除光纤通道 HBA

从机柜或机架中卸下 SG6000-CN 控制器

关闭 SG6000-CN 控制器

更换**SG6000**中的存储控制器

如果E2800系列控制器或EF570控制器运行不正常或出现故障、您可能需要更换该控制器。

您需要的内容

- 您的更换控制器的部件号与要更换的控制器相同。
- 您可以通过标签来识别连接到控制器的每个缆线。
- 您已安装 ESD 腕带，或者已采取其他防静电预防措施。
- 您有一个 1 号十字螺丝刀。
- 您可以按照 E 系列说明更换双工配置中的控制器。

  请勿依赖 E 系列说明来更换 StorageGRID 设备中的控制器，因为这些过程是不同的。

- 您已在数据中心中找到要更换控制器的物理存储设备。

  在数据中心中找到控制器

关于此任务

您可以通过以下两种方式确定控制器是否出现故障：

- SANtricity System Manager 中的恢复 Guru 可指示您更换控制器。
- 控制器上的琥珀色警示 LED 亮起，表示控制器出现故障。

  如果磁盘架中的两个控制器的警示 LED 均亮起，请联系技术支持以获得帮助。

如果您的设备包含两个存储控制器、则只要满足以下条件、您就可以在设备启动并执行读/写操作时更换其中一个控制器：

- 磁盘架中的第二个控制器处于最佳状态。
- SANtricity System Manager 中 Recovery Guru 的详细信息区域中的 "`确定删除` " 字段显示是，表示可以安全删除此组件。

> 如果可能，请将设备置于此替代操作步骤 的维护模式，以最大限度地减少意外错误或故障的潜在影响。

> 如果磁盘架中的第二个控制器状态不是最佳、或者Recovery Guru指示无法删除此控制器、请联系技术支持。

更换控制器时，您必须从原始控制器中取出电池，然后将其安装到替代控制器中。在某些情况下，您可能还需要从原始控制器中卸下主机接口卡，并将其安装在替代控制器中。

> 大多数设备型号中的存储控制器不包括主机接口卡（ HIC ）。

此任务包含以下部分：

1. 准备
2. 使控制器脱机
3. 删除控制器
4. 将电池移至新控制器
5. 如果需要、将HIC移至新控制器
6. 更换控制器

准备

步骤

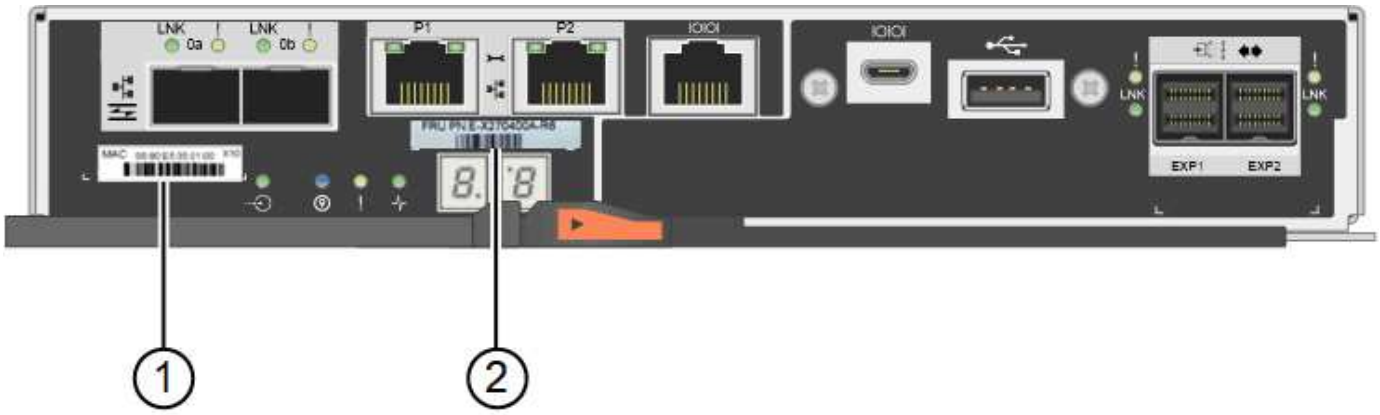
1. 拆开新控制器的包装，将其放在无静电的平面上。

   请保存包装材料，以便在运输故障控制器时使用。

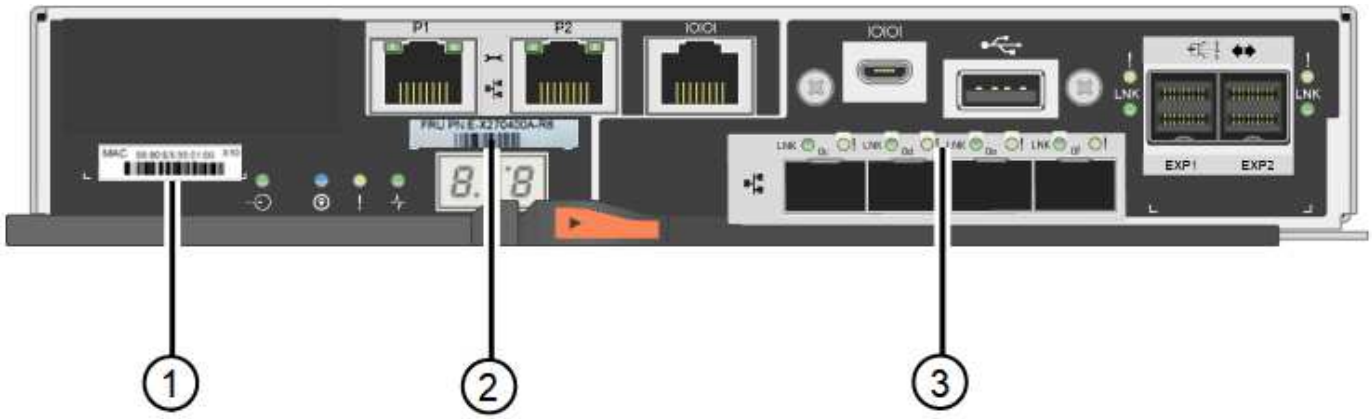
2. 在替代控制器的背面找到 MAC 地址和 FRU 部件号标签。

这些图显示了E2800A控制器和E2800B控制器。用于更换E2800系列控制器和EF570控制器的操作步骤 是相同的。

- E2800A存储控制器*



- E2800B存储控制器*



Label	组件	Description
1.	MAC 地址	管理端口1的MAC地址(E2800A上的"`P1"和E2800B`上的0a)。如果您使用 DHCP 获取原始控制器的 IP 地址，则需要使用此地址连接到新控制器。
2.	FRU 部件号	FRU 部件号。此编号必须与当前安装的控制器的更换部件号匹配。
3.	4端口HIC	4端口主机接口卡(HIC)。在执行更换时、必须将此卡移至新控制器。 注：E2800A控制器没有HIC。

使控制器脱机

步骤

1. 准备删除控制器。您可以使用 SANtricity 系统管理器执行这些步骤。

   a. 确认故障控制器的更换部件号与更换控制器的 FRU 部件号相同。

      如果控制器出现故障并需要更换，则更换部件号将显示在 Recovery Guru 的 Details 区域中。如果需要手动查找此数字，可以在 * 基础 * 选项卡上查看控制器。

*可能会丢失数据访问和#8212；*如果两个部件号不同、请勿尝试使用此操作步骤。

a. 备份配置数据库。

   如果删除控制器时出现问题，您可以使用保存的文件还原配置。

b. 收集设备的支持数据。

   在更换组件之前和之后收集支持数据可确保在更换组件无法解决问题时，您可以向技术支持发送一整套日志。

c. 使计划更换的控制器脱机。

卸下控制器

步骤

1. 从设备中删除控制器：
   a. 戴上 ESD 腕带或采取其他防静电预防措施。
   b. 为缆线贴上标签，然后断开缆线和 SFP 的连接。

      To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

   c. 通过挤压凸轮把手上的闩锁，直到其释放，然后打开右侧的凸轮把手，将控制器从设备中释放。
   d. 用两只手和凸轮把手将控制器滑出设备。

      请始终用双手支撑控制器的重量。

   e. 将控制器放在无静电的平面上，可拆卸盖朝上。
   f. 向下按按钮并滑动外盖，以卸下外盖。

将电池移至新控制器

步骤

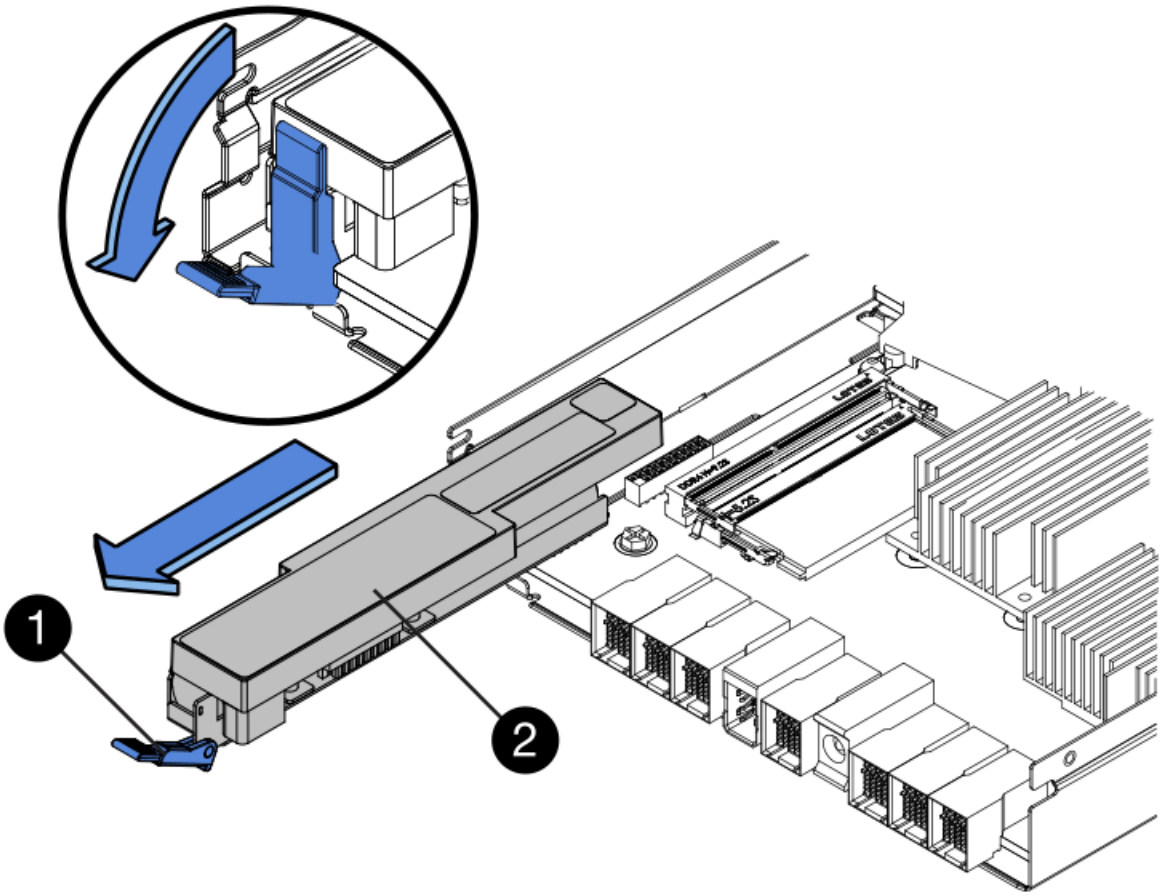
1. 从发生故障的控制器中取出电池，然后将其安装到替代控制器中：
   a. 确认控制器（电池和 DIMM 之间）中的绿色 LED 熄灭。

      如果此绿色 LED 亮起，则表示控制器仍在使用电池电源。您必须等待此 LED 熄灭，然后才能卸下任何组件。

项目	Description
1.	内部缓存活动 LED
2.	电池

b. 找到电池的蓝色释放闩锁。

c. 向下推动释放闩锁并将其从控制器中移出，以解锁电池。



项目	Description
1.	电池释放闩锁
2.	电池

d. 抬起电池，将其滑出控制器。

e. 从更换用的控制器上卸下盖板。

f. 调整更换控制器的方向，使电池插槽面向您。

g. 将电池略微向下插入控制器。

   您必须将电池前部的金属法兰插入控制器底部的插槽中，然后将电池顶部滑入控制器左侧的小对齐销下。

h. 向上移动电池闩锁以固定电池。

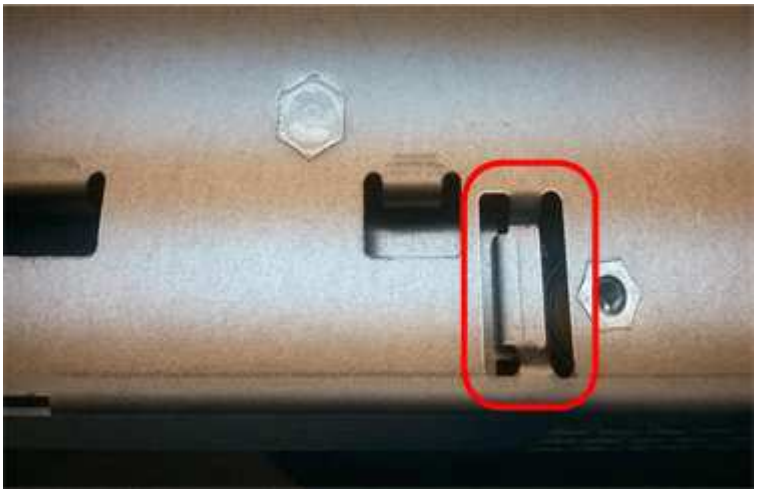
   当闩锁卡入到位时，闩锁的底部会挂到机箱上的金属插槽中。

i. 将控制器翻转，以确认电池安装正确。

* 可能的硬件损坏 * —电池正面的金属法兰必须完全插入控制器上的插槽（如第一图所示）。如果电池安装不正确（如图 2 所示），则金属法兰可能会接触控制器板，从而导致损坏。

- 正确—电池的金属法兰已完全插入控制器上的插槽：

- * 不正确 - 电池的金属法兰未插入控制器上的插槽： *



2. 更换控制器盖板。

如果需要、将**HIC**移至新控制器

步骤

1. 如果故障控制器包含主机接口卡(HIC)、请将HIC从故障控制器移至更换控制器。

   单独的HIC仅用于E2800B控制器。HIC安装在主控制器板上、并包含两个SPF连接器。

   此操作步骤 中的插图显示了一个双端口HIC。控制器中的HIC可能具有不同数量的端口。

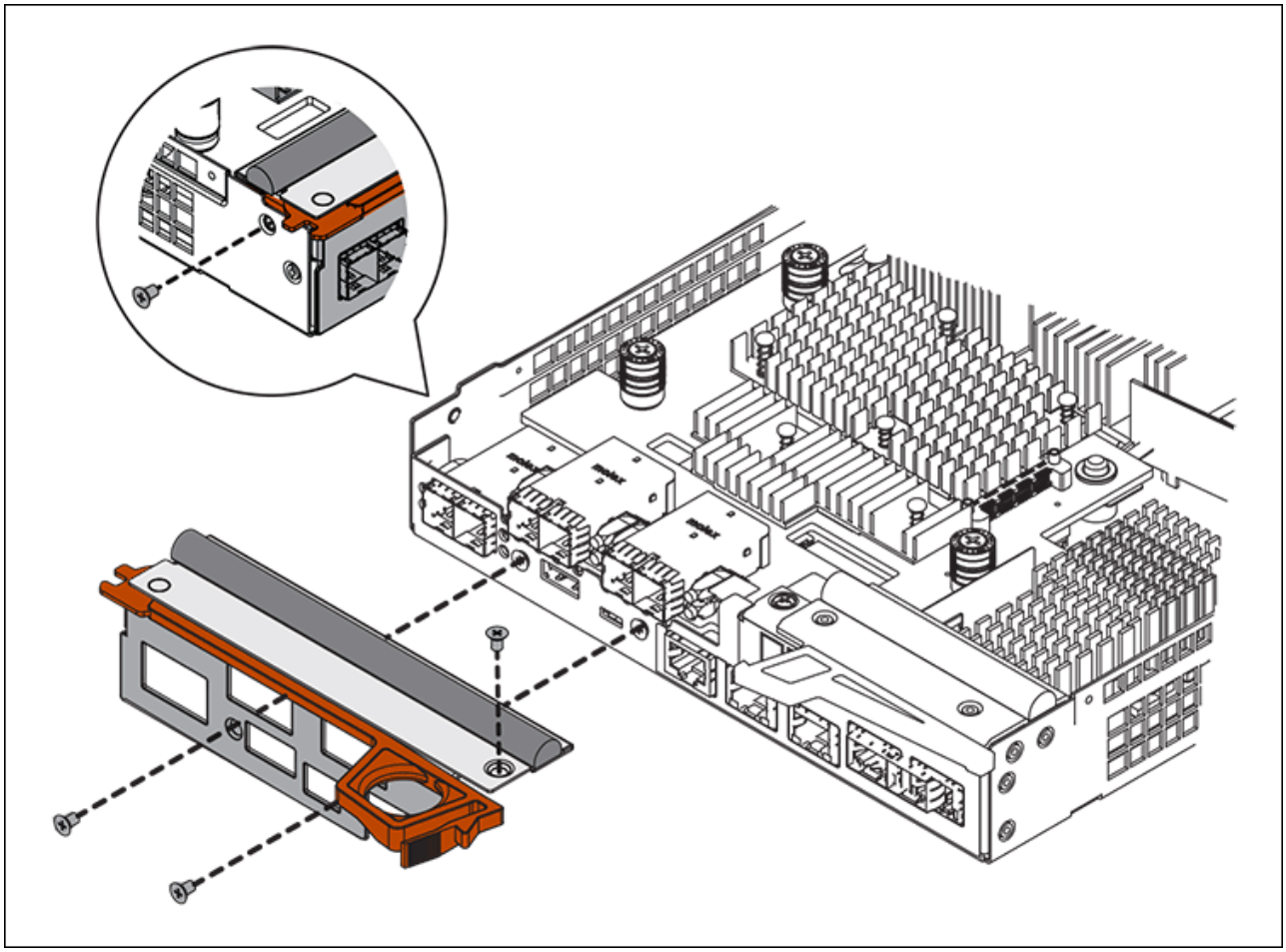
2. 如果控制器没有HIC (E2800A)、请更换控制器盖板。如果控制器确实具有HIC (E2800B)、请继续执行将HIC从故障控制器移至替代控制器。

a. 如果配有HIC、请将HIC从故障控制器移至更换控制器。

b. 从HIC中删除所有SFP。

c. 使用1号十字螺丝刀卸下将HIC面板连接到控制器的螺钉。

有四个螺钉：一个在顶部，一个在侧面，两个在正面。

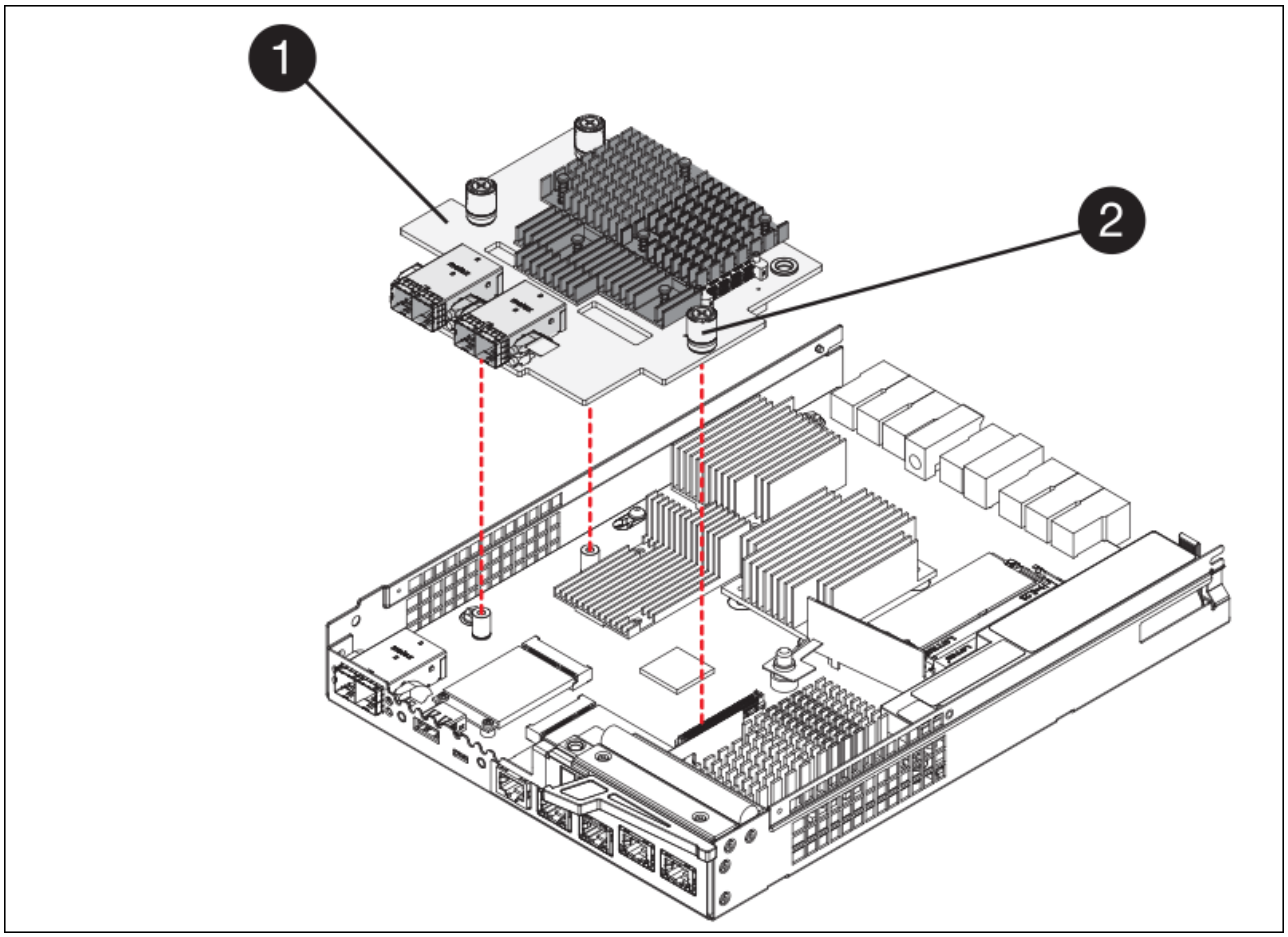


d. 卸下 HIC 面板。

e. 使用您的手指或十字螺丝刀松开将 HIC 固定到控制器卡的三个翼形螺钉。

f. 小心地将 HIC 从控制器卡上卸下，方法是将该卡抬起并滑回。

请注意，不要擦除或撞击 HIC 底部或控制器卡顶部的组件。



Label	Description
1.	主机接口卡
2.	翼形螺钉

g. 将 HIC 放置在无静电表面上。

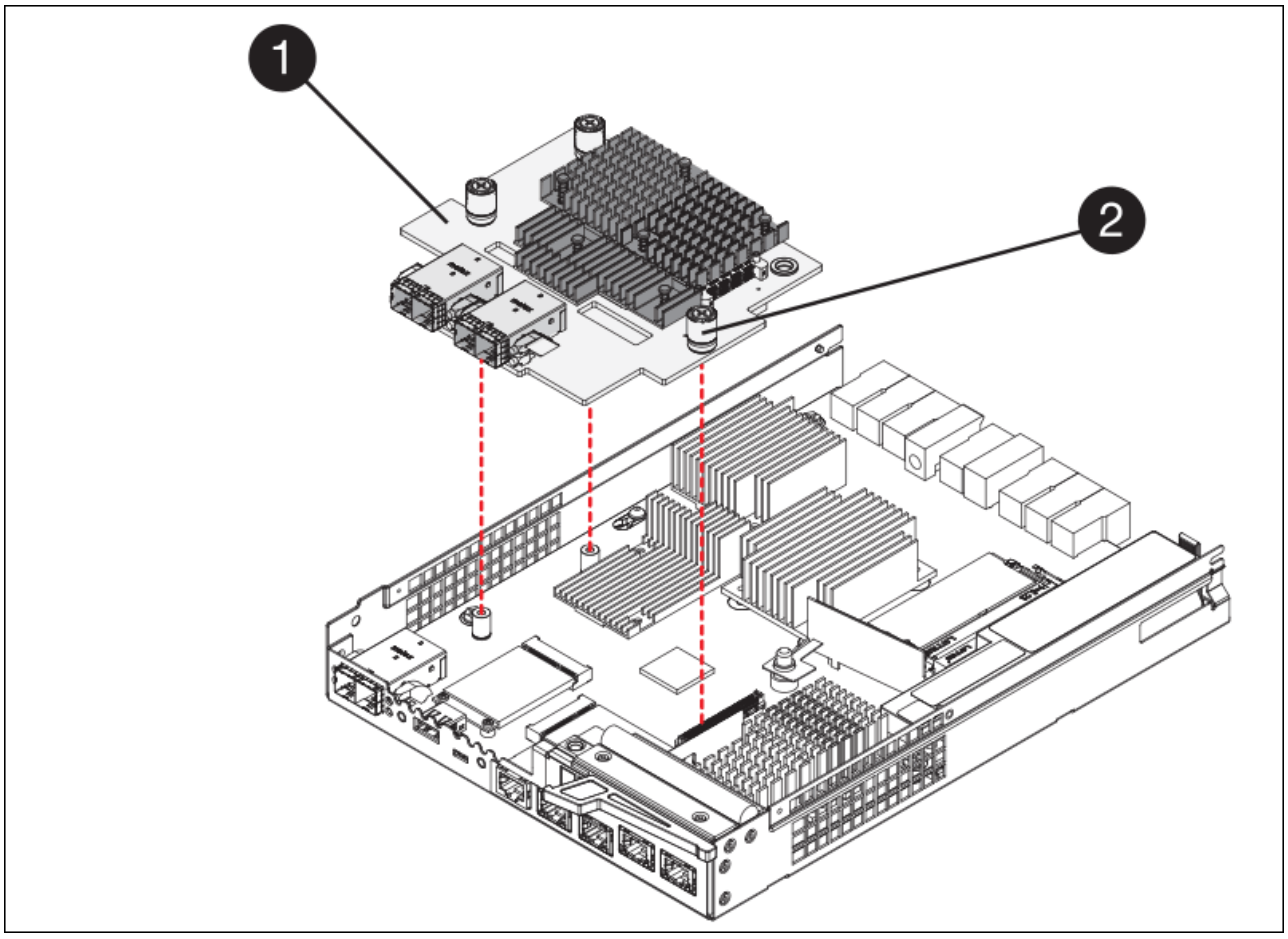
h. 使用1号十字螺丝刀卸下将空白面板连接到更换用控制器的四个螺钉、然后卸下面板。

i. 将HIC上的三个翼形螺钉与更换用的控制器上的相应孔对齐、并将HIC底部的连接器与控制器卡上的HIC接口连接器对齐。

   请注意，不要擦除或撞击 HIC 底部或控制器卡顶部的组件。

j. 小心地将 HIC 放低到位，然后轻按 HIC 以固定 HIC 连接器。

* 可能的设备损坏 * —请务必小心，不要挤压 HIC 和翼形螺钉之间控制器 LED 的金带连接器。

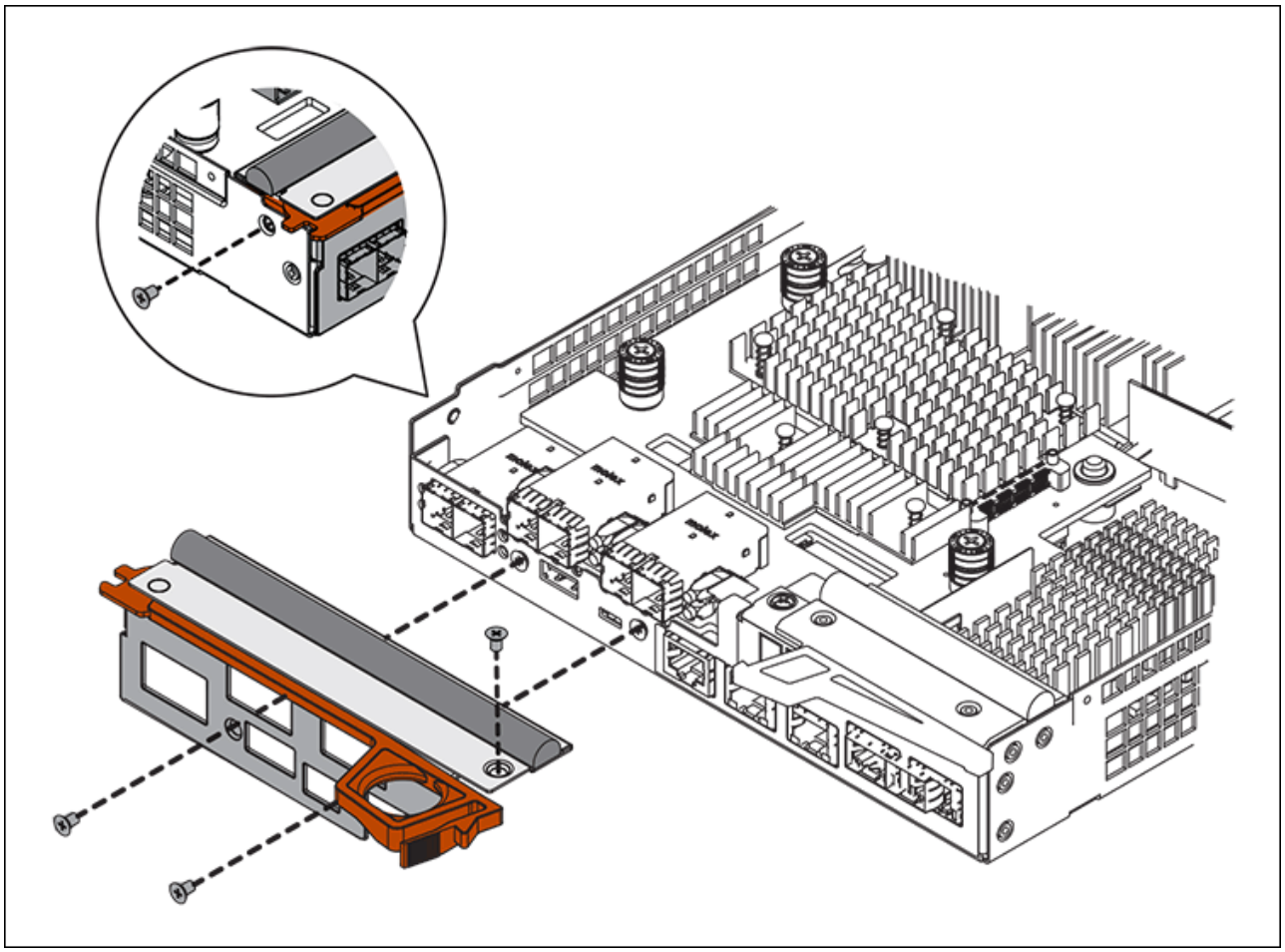


Label	Description
1.	主机接口卡
2.	翼形螺钉

a. 手动拧紧 HIC 翼形螺钉。

请勿使用螺丝刀，否则可能会过度拧紧螺钉。

b. 使用1号十字螺丝刀、使用四个螺钉将从原始控制器上卸下的HIC面板连接到新控制器。



c. 将所有已删除的SFP重新安装到HIC中。

更换控制器

步骤

1. 将替代控制器安装到设备中。
   a. 将控制器翻转，使可拆卸盖朝下。
   b. 在凸轮把手处于打开位置的情况下，将控制器完全滑入设备中。
   c. 将凸轮把手移至左侧，将控制器锁定到位。
   d. 更换缆线和 SFP 。
   e. 如果原始控制器使用 DHCP 作为 IP 地址，请在替代控制器背面的标签上找到 MAC 地址。请您的网络管理员将您删除的控制器的 DNS/network 和 IP 地址与替代控制器的 MAC 地址相关联。

   如果原始控制器未使用 DHCP 作为 IP 地址，则新控制器将采用您删除的控制器的 IP 地址。

2. 使用 SANtricity 系统管理器使控制器联机：
   a. 选择 * 硬件 * 。
   b. 如果图形显示了驱动器，请选择 * 显示磁盘架背面 * 。
   c. 选择要置于联机状态的控制器。

d. 从上下文菜单中选择 * 置于联机状态 * ，然后确认要执行此操作。

e. 验证七段显示屏是否显示状态 `99` 。

3. 确认新控制器处于最佳状态，并收集支持数据。

更换部件后，按照套件随附的 RMA 说明将故障部件退回 NetApp 。请参见 "部件退回和放大器；更换" 第页，了解更多信息。

相关信息

"NetApp E 系列系统文档站点"

更换存储控制器架中的硬件组件

如果发生硬件问题，您可能需要更换存储控制器架中的组件。

您需要的内容

- 您已安装 E 系列硬件更换操作步骤 。
- 您已在物理上找到要在数据中心中更换存储架硬件组件的存储设备。

  在数据中心中找到控制器

关于此任务

要更换存储控制器中的电池，请参见这些说明中有关更换存储控制器的说明。这些说明介绍了如何从设备中卸下控制器，从控制器中取出电池，安装电池以及更换控制器。

有关控制器架中其他现场可更换单元（ FRU ）的说明，请访问 E 系列系统维护流程。

FRU	请参见说明
电池	StorageGRID （以下说明）：更换存储控制器
驱动器	E 系列： • 更换驱动器（ 60 个驱动器） • 更换驱动器（ 12 个或 24 个驱动器）
动力箱	E 系列 • 更换电源箱（ 60 个驱动器） • 更换电源（ 12 个或 24 个驱动器）
风扇箱（仅限 60 驱动器架）	E 系列：更换风扇箱（ 60 个驱动器）
驱动器抽盒（仅限 60 驱动器磁盘架）	E 系列：更换驱动器抽盒（ 60 个驱动器）

相关信息

"NetApp E 系列系统文档站点"

更换存储控制器

更换可选 **60** 驱动器扩展架中的硬件组件

您可能需要更换扩展架中的输入 / 输出模块，电源或风扇。

您需要的内容

- 您已安装 E 系列硬件更换操作步骤 。
- 您已在物理上找到要在数据中心更换扩展架硬件组件的存储设备。

  在数据中心中找到控制器

关于此任务

要更换 60 驱动器扩展架中的输入 / 输出模块（ IOM ），请参见这些说明中有关更换存储控制器的说明。

要更换 60 驱动器扩展架中的电源或风扇，请访问 E 系列维护 60 驱动器硬件的过程。

FRU	请参见 **E** 系列说明
输入 / 输出模块（ IOM ）	更换 IOM
动力箱	更换电源箱（ 60 个驱动器）
风扇箱	更换风扇箱（ 60 个驱动器）

关闭 **SG6000-CN** 控制器

关闭 SG6000-CN 控制器以执行硬件维护。

您需要的内容

您已将需要维护的 SG6000-CN 控制器物理定位在数据中心。请参见 在数据中心中找到控制器。

关于此任务

要防止服务中断，请在可以接受服务中断期间的计划维护窗口期间关闭控制器或关闭控制器之前，确认所有其他存储节点均已连接到网格。请参见有关的信息 监控节点连接状态。

> 如果您使用的 ILM 规则只创建一个对象的一个副本，则必须在计划的维护窗口期间关闭控制器。否则，在此操作步骤 期间，您可能暂时无法访问这些对象。请参见 "通过信息生命周期管理来管理对象"。

步骤

1. 关闭SG6000-CN控制器：

> 您必须通过输入以下指定的命令来控制控制器的关闭。最佳做法是、尽可能执行可控关闭、以避免不必要的警报、确保完整日志可用并避免服务中断。

a. 如果尚未登录到网格节点、请使用PuTTY或其他ssh客户端登录：

   i. 输入以下命令： `ssh admin@ grid_node_ip_`

   ii. 输入 `passwords.txt` 文件中列出的密码。

   iii. 输入以下命令切换到 root： `su -`

   iv. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

b. 关闭SG6000-CN控制器：

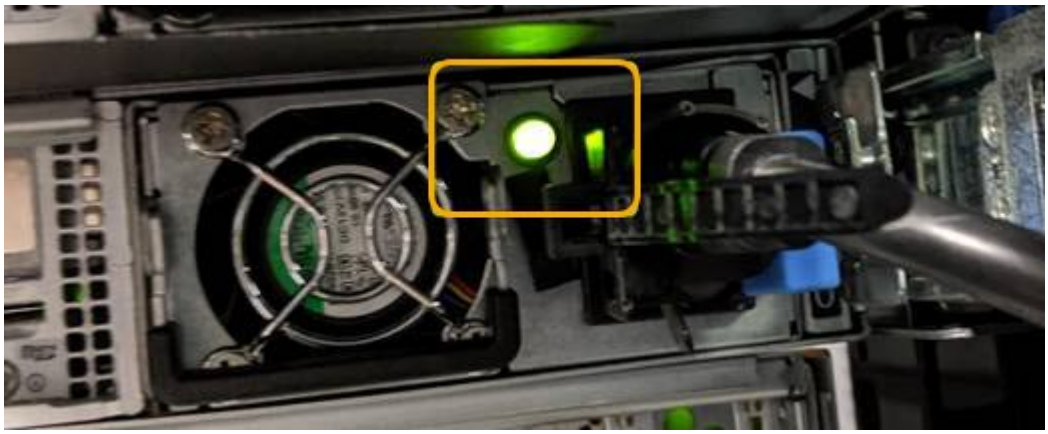
```
shutdown -h now
```

此命令可能需要长达 10 分钟才能完成。

2. 使用以下方法之一验证 SG6000-CN 控制器是否已关闭：

   ◦ 查看控制器正面的蓝色电源 LED ，确认其已关闭。

   ◦ 查看控制器背面两个电源上的绿色 LED ，确认它们以正常速率闪烁（大约每秒闪烁一次）。



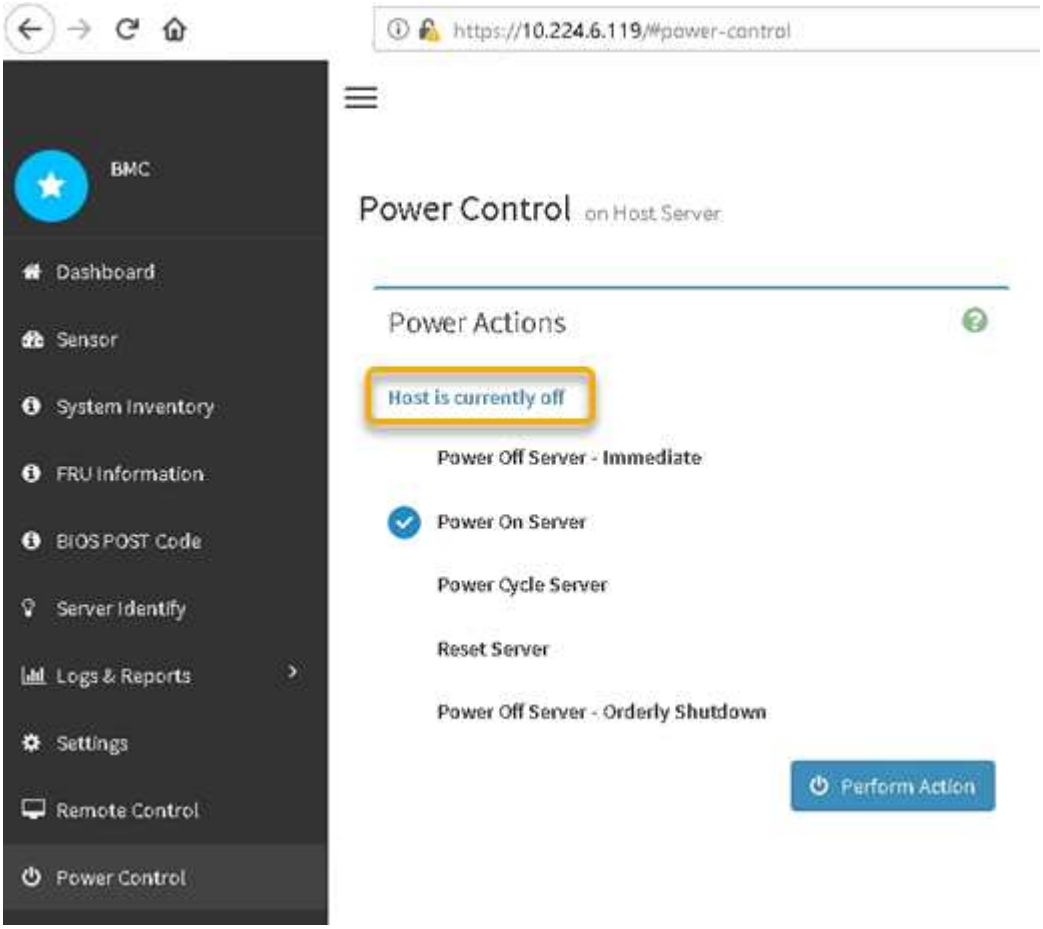
   ◦ 使用控制器 BMC 界面：

      i. 访问控制器 BMC 界面。

      访问 BMC 界面

ii. 选择 * 电源控制 * 。

iii. 验证电源操作是否指示主机当前已关闭。



相关信息

从机柜或机架中卸下 SG6000-CN 控制器

打开 **SG6000-CN** 控制器的电源并验证其运行情况

完成维护后，打开控制器电源。

您需要的内容

- 您已将控制器安装在机柜或机架中并连接了数据和电源线。

  将 SG6000-CN 控制器重新安装到机柜或机架中

- 您已将控制器物理定位在数据中心中。

  在数据中心中找到控制器

步骤

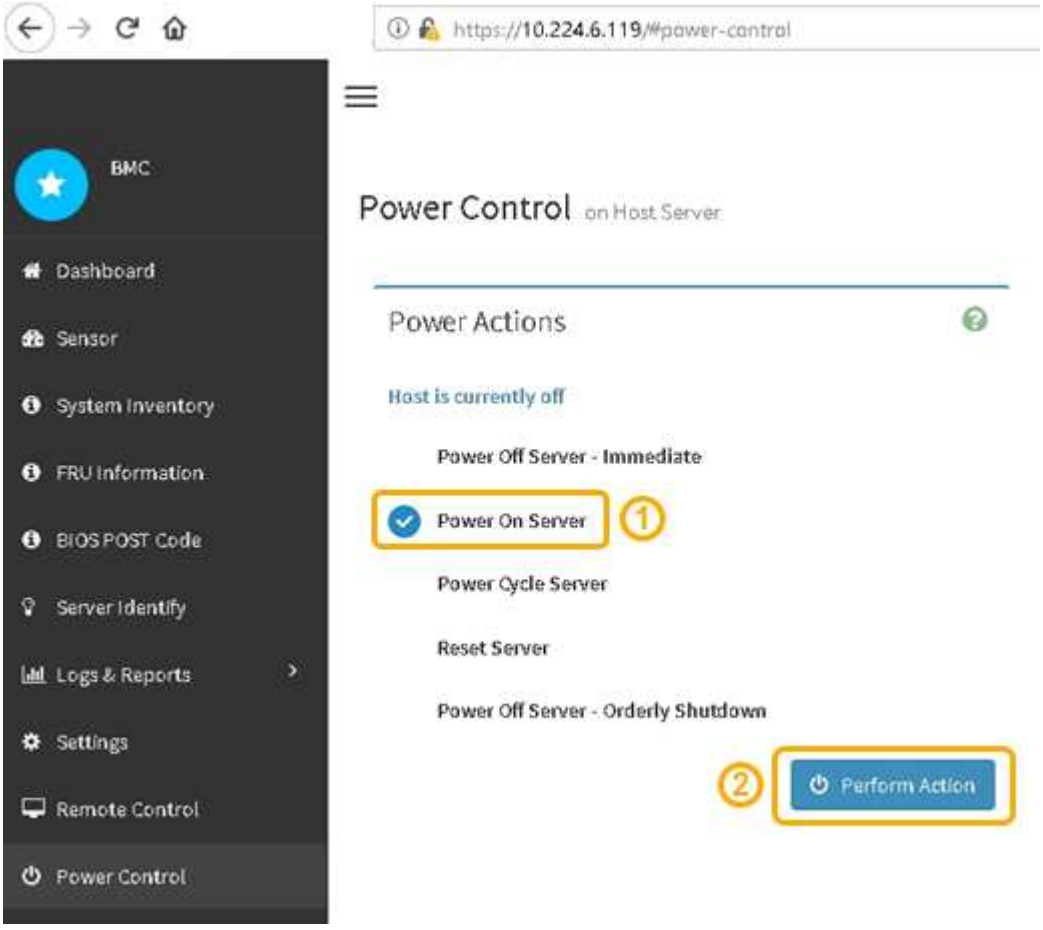
1. 启动 SG6000-CN 控制器，并使用以下方法之一监控控制器 LED 和启动代码：

   ◦ 按下控制器正面的电源开关。

- 使用控制器 BMC 界面：
  i. 访问控制器 BMC 界面。

     访问 BMC 界面

  ii. 选择 * 电源控制 * 。
  iii. 选择 * 启动服务器 * ，然后选择 * 执行操作 * 。



使用 BMC 界面监控启动状态。

2. 确认设备控制器显示在网格管理器中且未显示任何警报。

控制器可能需要长达 20 分钟才能显示在网格管理器中。

3. 确认新的 SG6000-CN 控制器已完全正常运行：

   a. 使用 PuTTY 或其他 ssh 客户端登录到网格节点：

      i. 输入以下命令： `ssh admin@ grid_node_ip_`

      ii. 输入 `passwords.txt` 文件中列出的密码。

      iii. 输入以下命令切换到 root： `su -`

      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

   b. 输入以下命令并验证其是否返回预期输出： `+ cat /sys/class/fc_host/* / port_state`

      预期输出：

      ```
      Online
      Online
      Online
      Online
      ```

      如果未返回预期输出，请联系技术支持。

   c. 输入以下命令并验证其是否返回预期输出： `+ cat /sys/class/fc_host/*/speed`

      预期输出：

      ```
      16 Gbit
      16 Gbit
      16 Gbit
      16 Gbit
      ```

      +
      如果未返回预期输出，请联系技术支持。

   a. 在网格管理器的节点页面中，确保设备节点已连接到网格，并且没有任何警报。

      请勿使其他设备节点脱机，除非此设备具有绿色图标。

4. 可选：如果已卸下前挡板，请安装前挡板。

相关信息

查看 SG6000-CN 控制器上的状态指示灯和按钮

查看 SG6000 存储控制器的启动状态代码

如果 SG6000-CN 控制器运行不正常或出现故障，您可能需要更换该控制器。

您需要的内容

- 您的更换控制器的部件号与要更换的控制器相同。
- 您可以通过标签来识别连接到控制器的每个缆线。
- 您已在数据中心中找到要更换的控制器。

  在数据中心中找到控制器

关于此任务

更换 SG6000-CN 控制器后，无法访问设备存储节点。如果 SG6000-CN 控制器运行正常，则可以在此操作步骤开始时执行受控关闭。

> 如果在安装 StorageGRID 软件之前更换控制器，则在完成此操作步骤 后，您可能无法立即访问 StorageGRID 设备安装程序。虽然您可以从与设备位于同一子网上的其他主机访问 StorageGRID 设备安装程序，但不能从其他子网上的主机访问它。此情况应在 15 分钟内自行解决（当原始控制器的任何 ARP 缓存条目超时），或者您也可以通过手动从本地路由器或网关清除任何旧的 ARP 缓存条目来立即清除此情况。

步骤

1. 显示并记录设备的当前配置。
   a. 登录到要更换的设备：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 输入 … **`run-host-command ipmitool lan print`** 以显示设备的当前BMC配置。
2. 如果 SG6000-CN 控制器运行充分，可以进行可控的关闭，请关闭 SG6000-CN 控制器。

   关闭 SG6000-CN 控制器
3. 如果此StorageGRID 设备上的任何网络接口配置了DHCP、则可能需要更新DHCP服务器上的永久DHCP租约分配、以引用替代设备的MAC地址。此更新可确保为设备分配预期的IP地址。
   a. 找到 SG6000-CN 控制器正面的 MAC 地址标签，并确定管理网络端口的 MAC 地址。

MAC 地址标签列出了 BMC 管理端口的 MAC 地址。

要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 * 。 2 例如，如果标签上的 **MAC** 地址以 ***09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 * （ *y* ） FF* 结尾，则管理端口的 MAC 地址将以 * （ *y*+1 ） 01* 结尾。您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 * + 2 =* 来轻松进行计算。

b. 请您的网络管理员将您删除的控制器的 DNS/network 和 IP 地址与替代控制器的 MAC 地址相关联。

在为替代控制器接通电源之前，您必须确保原始控制器的所有 IP 地址均已更新。否则，控制器将在启动时获取新的 DHCP IP 地址，并且可能无法重新连接到 StorageGRID 。此步骤将对连接到控制器的所有 StorageGRID 网络执行适用场景 。

如果原始控制器使用静态 IP 地址，则新控制器将自动采用您删除的控制器的 IP 地址。

4. 卸下并更换 SG6000-CN 控制器：
   a. 为缆线贴上标签，然后断开缆线以及任何 SFP+ 或 SFP28 收发器。

      To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

   b. 从机柜或机架中卸下故障控制器。
   c. 将替代控制器安装到机柜或机架中。
   d. 更换缆线以及任何 SFP+ 或 SFP28 收发器。
   e. 打开控制器电源并监控控制器 LED 和启动代码。
5. 如果更换控制器的设备使用密钥管理服务器(KMS)对数据进行加密、则可能需要进行其他配置、节点才能加入网格。如果节点未自动加入网格、请确保这些配置设置已传输到新控制器、并手动配置任何不具有预期配置的设置：
   - "配置StorageGRID 连接"
   - "为此设备配置节点加密"
6. 使用更换的控制器登录到设备：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
7. 还原设备的BMC网络连接。有两个选项：
   - 使用静态IP、网络掩码和网关
   - 使用DHCP获取IP、网络掩码和网关
     i. 要还原BMC配置以使用静态IP、网络掩码和网关、请输入以下命令：

```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP

run-host-command ipmitool lan set 1 netmask Netmask_IP

run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

i. 要还原BMC配置以使用DHCP获取IP、网络掩码和网关、请输入以下命令：

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

8. 还原BMC网络连接后、连接到BMC界面以审核和还原可能已应用的任何其他自定义BMC配置。例如、您应确认SNMP陷阱目标和电子邮件通知的设置。请参见 "配置BMC接口"。
9. 确认设备节点显示在网格管理器中且未显示任何警报。

相关信息

SG6000-CN ： 安装到机柜或机架中

查看 SG6000-CN 控制器上的状态指示灯和按钮

查看 SG6000-CN 控制器的启动代码

更换 **SG6000-CN** 控制器中的一个或两个电源

SG6000-CN 控制器具有两个电源以实现冗余。如果其中一个电源发生故障，您必须尽快更换，以确保计算控制器具有冗余电源。在控制器中运行的两个电源必须具有相同的型号和功率。

您需要的内容

- 您已确定要更换电源的控制器数据中心的物理位置。

  在数据中心中查找控制器

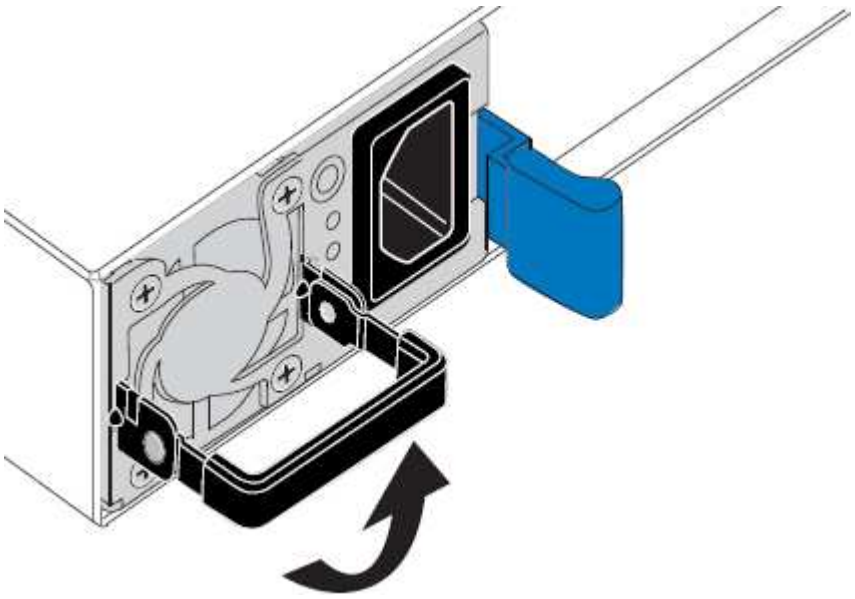
- 如果仅更换一个电源：
  - 您已卸载更换用的电源设备，并确保其型号和功率与要更换的电源设备相同。
  - 您已确认另一个电源已安装且正在运行。
- 如果要同时更换两个电源：
  - 您已卸载替代电源设备，并确保其型号和功率相同。

关于此任务

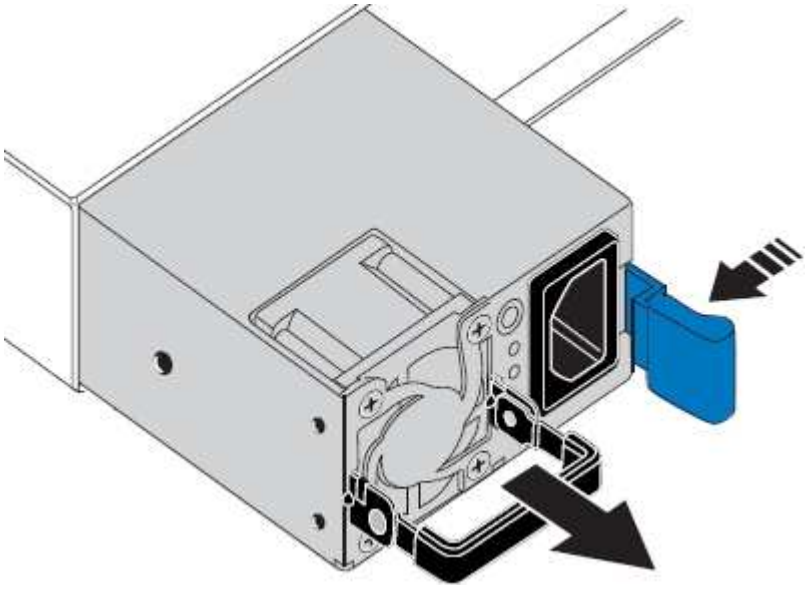
此图显示了 SG6000-CN 控制器的两个电源设备，可从控制器背面访问这些设备。使用此操作步骤 更换一个或两个电源。如果要更换这两个电源，则必须先对设备执行有控制的关闭。

步骤

1. 如果您只更换一个电源，则无需关闭设备。转至 拔下电源线 步骤。如果要同时更换两个电源，请在拔下电源线之前执行以下操作：
   a. 将设备置于维护模式。
   b. 关闭设备。
2. 【拔掉电源线， start=2]] 从要更换的每个电源中拔下电源线。
3. 提起要更换的第一个电源上的凸轮把手。



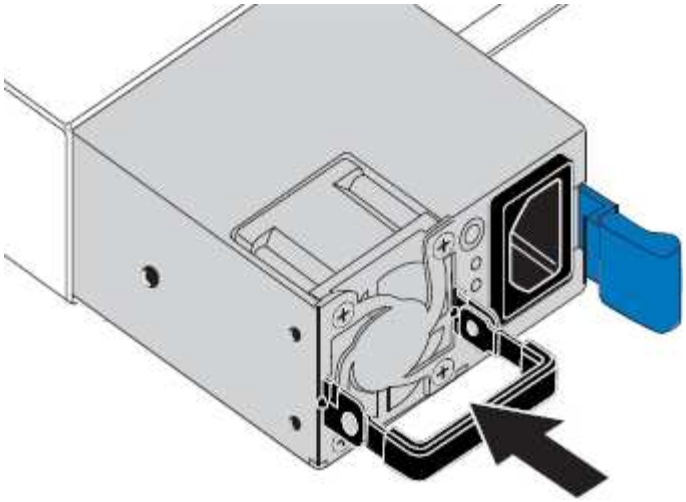
4. 按下蓝色闩锁并拉出电源。



5. 使蓝色闩锁位于右侧，将替代电源滑入机箱。

   两个电源的型号和功率必须相同。

   在中滑动更换部件时，请确保蓝色闩锁位于右侧。



6. 向下推凸轮把手以固定更换用的电源。
7. 如果要更换这两个电源，请重复步骤 2 到 6 以更换第二个电源。
8. 将电源线连接到更换的设备并接通电源。
9. 如果您将设备置于维护模式，请退出维护模式。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。

从机柜或机架中卸下 **SG6000-CN** 控制器

从机柜或机架中卸下 SG6000-CN 控制器，以便检修顶盖或将控制器移至其他位置。

您需要的内容

- 您可以通过标签来标识连接到 SG6000-CN 控制器的每个缆线。
- 您已实际找到要在数据中心中执行维护的 SG6000-CN 控制器。

  在数据中心中找到控制器

- 您已关闭 SG6000-CN 控制器。

  关闭 SG6000-CN 控制器

  请勿使用电源开关关闭控制器。

步骤

1. 标记并断开控制器电源线。
2. 将 ESD 腕带的腕带一端绕在腕带上，并将扣具一端固定到金属接地，以防止静电放电。
3. 标记并断开控制器数据缆线以及任何 SFP+ 或 SFP28 收发器的连接。

   To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

4. 松开控制器前面板上的两个固定螺钉。

5. 将 SG6000-CN 控制器向前滑出机架，直到安装导轨完全展开，并且您可以听到两侧的闩锁卡嗒声。

   可以访问控制器顶盖。

6. 可选：如果要从机柜或机架中完全卸下控制器，请按照导轨套件的说明从导轨中卸下控制器。

相关信息

拆下 SG6000-CN 控制器盖板

将 **SG6000-CN** 控制器重新安装到机柜或机架中

硬件维护完成后，将控制器重新安装到机柜或机架中。

您需要的内容

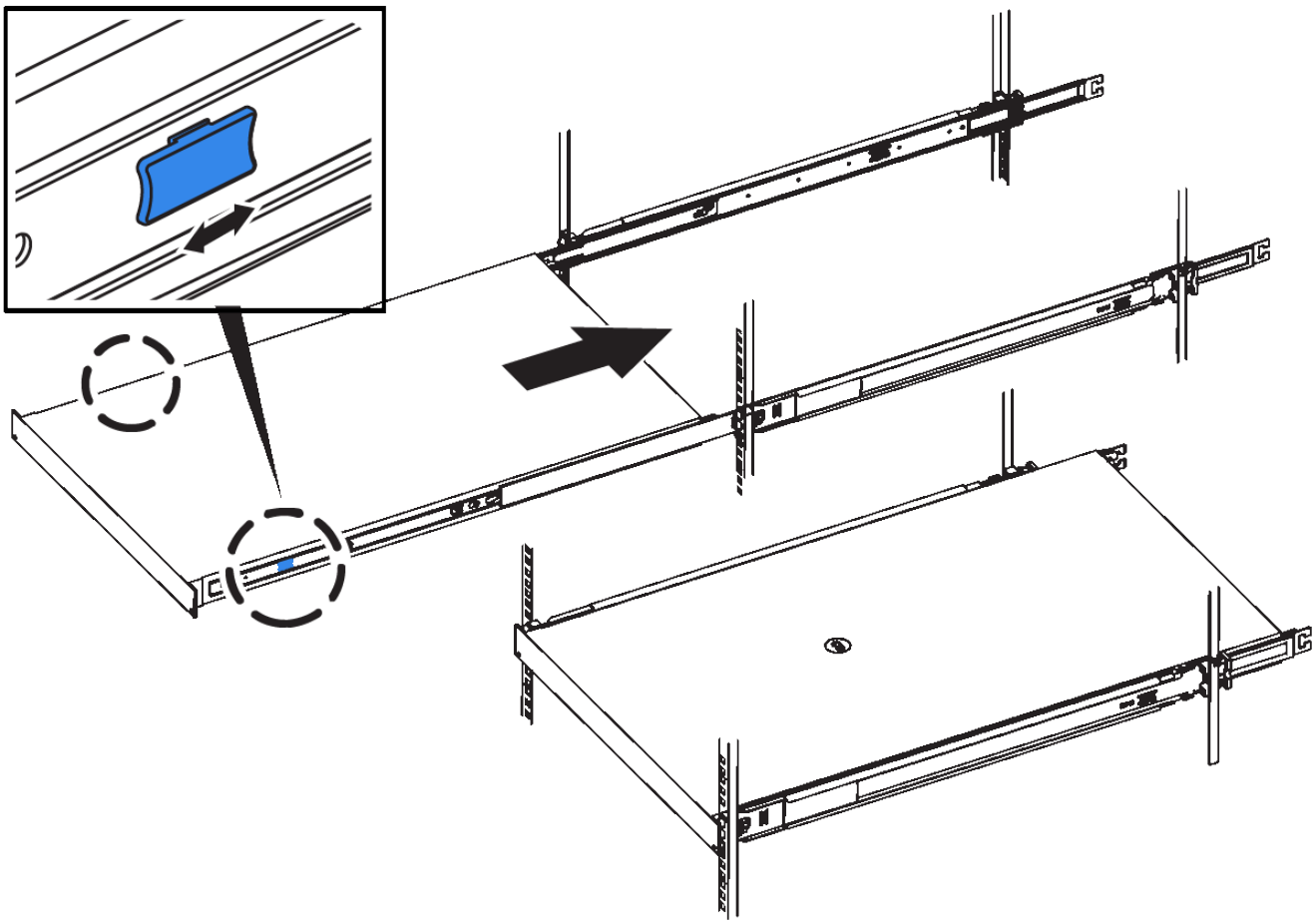
您已重新安装控制器盖板。

重新安装 SG6000-CN 控制器盖板

步骤

1. 按下蓝色导轨可同时释放两个机架导轨，并将 SG6000-CN 控制器滑入机架，直到其完全就位。

   如果无法再移动控制器，请拉动机箱两侧的蓝色闩锁，将控制器完全滑入。



在打开控制器电源之前，请勿连接前挡板。

2. 拧紧控制器前面板上的固定螺钉，将控制器固定在机架中。

3. 将 ESD 腕带的腕带一端绕在腕带上，并将扣具一端固定到金属接地，以防止静电放电。
4. 重新连接控制器数据缆线以及任何 SFP+ 或 SFP28 收发器。

To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

缆线设备（ SG6000 ）

5. 重新连接控制器电源线。

连接电源线并接通电源（ SG6000 ）

完成后

可以重新启动控制器。

[打开 SG6000-CN 控制器的电源并验证其运行情况]

拆下 **SG6000-CN** 控制器盖板

拆下控制器盖板，以便检修内部组件以进行维护。

您需要的内容

从机柜或机架中卸下控制器，以便检修顶盖。

[从机柜或机架中卸下 SG6000-CN 控制器]

步骤

1. 确保 SG6000-CN 控制器盖板闩锁未锁定。如有必要，将蓝色塑料闩锁按解锁方向转动四分之一圈，如闩锁上所示。
2. 将闩锁向 SG6000-CN 控制器机箱的后部来回旋转，直到其停止为止；然后，小心地将机箱盖从机箱中提起并放在一旁。

将 ESD 腕带的腕带一端绑在腕带周围，并将扣具一端固定到金属接地，以防止在 SG6000-CN 控制器内部工作时发生静电放电。

相关信息

[删除光纤通道 HBA]

重新安装 **SG6000-CN** 控制器盖板

内部硬件维护完成后，重新安装控制器盖板。

您需要的内容

您已完成控制器内部的所有维护过程。

步骤

1. 打开主机盖闩锁后，握住机箱上方的主机盖，并将顶部主机盖闩锁中的孔与机箱中的销对齐。对齐后，将其放低到机箱上。

2. 向前和向下旋转机箱盖闩锁，直到其停止，并且机箱盖完全就位到机箱中。确认外盖前边缘没有间隙。

   如果外盖未完全就位，则可能无法将 SG6000-CN 控制器滑入机架。

3. 可选：将蓝色塑料闩锁按锁定方向转动四分之一圈，如闩锁上所示，以将其锁定。

完成后

在机柜或机架中重新安装控制器。

将 SG6000-CN 控制器重新安装到机柜或机架中

更换 **SG6000-CN** 控制器中的光纤通道 **HBA**

如果 SG6000-CN 控制器运行不正常或发生故障，您可能需要更换该控制器中的光纤通道主机总线适配器（ HBA ）。

确认要更换的光纤通道 **HBA**

如果您不确定要更换哪个光纤通道主机总线适配器（ HBA ），请完成此操作步骤 以进行识别。

您需要的内容

- 您拥有需要更换光纤通道 HBA 的存储设备或 SG6000-CN 控制器的序列号。

> 如果包含要更换的光纤通道 HBA 的存储设备的序列号以字母 Q 开头，则它不会在网格管理器中列出。您必须检查附加到数据中心中每个 SG6000-CN 控制器正面的标签，直到找到匹配项为止。

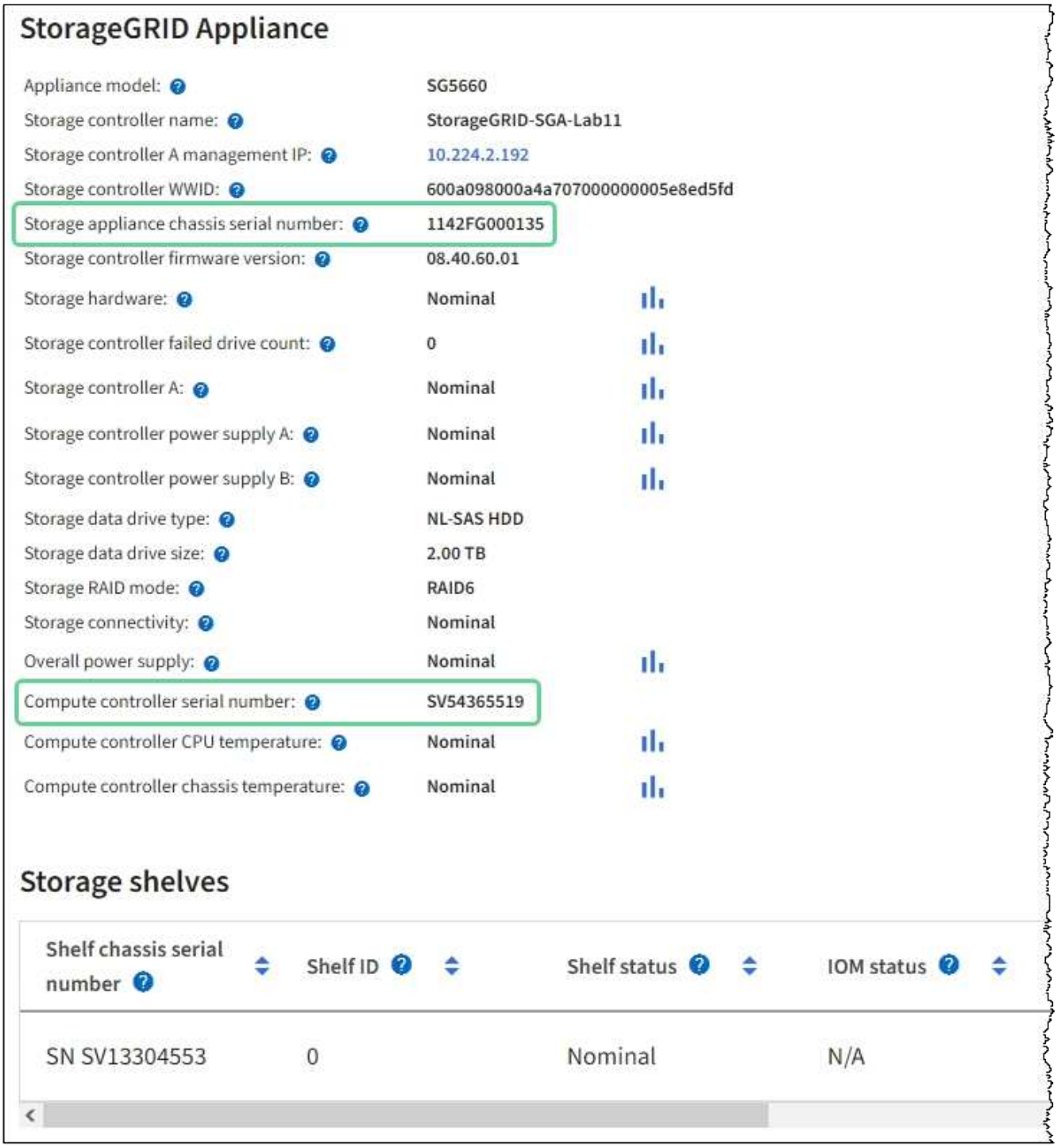
- 您将使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面上的表中，选择设备存储节点。

3. 选择 * 硬件 * 选项卡。

   检查 StorageGRID 设备部分中的 * 存储设备机箱序列号 * 和 * 计算控制器序列号 * 。查看其中一个序列号是否与要更换光纤通道 HBA 的存储设备的序列号匹配。如果任一序列号匹配，则表明您找到了正确的设备。



   - 如果未显示 StorageGRID 设备部分，则选定节点不是 StorageGRID 设备。从树视图中选择其他节点。
   - 如果设备型号不是SG6060或SG6060X、请从树视图中选择其他节点。
   - 如果序列号不匹配，请从树视图中选择其他节点。

4. 找到需要更换光纤通道 HBA 的节点后，记下 StorageGRID 设备部分列出的计算控制器 BMC IP 地址。

您可以使用此 IP 地址打开计算控制器识别 LED ，以帮助您在数据中心中找到设备。

打开和关闭控制器识别 LED

相关信息

删除光纤通道 HBA

删除光纤通道 **HBA**

如果 SG6000-CN 控制器运行不正常或发生故障，您可能需要更换该控制器中的光纤通道主机总线适配器（ HBA ）。

您需要的内容

- 您拥有正确的替代光纤通道 HBA 。
- 您已拥有 "已确定哪个SG6000-CN控制器包含要更换的光纤通道HBA"。
- 您已拥有 "以物理方式定位SG6000-CN控制器" 在数据中心。
- 您已拥有 "关闭SG6000-CN控制器"。

> 从机架中卸下控制器之前、需要进行有控制的关闭。

- 您已拥有 "已从机柜或机架中卸下控制器"。
- 您已拥有 "已卸下控制器盖板"。

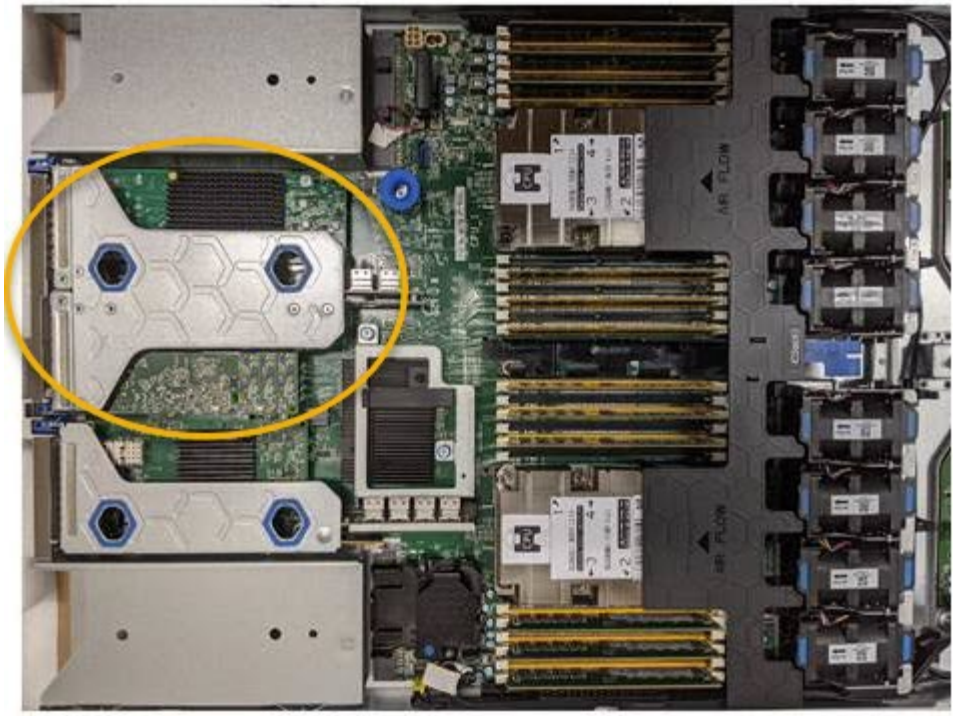
关于此任务

为了防止服务中断，请在开始更换光纤通道 HBA 之前确认所有其他存储节点均已连接到网格，或者在计划的维护时段内更换适配器，此时通常会发生服务中断。请参见有关的信息 "监控节点连接状态"。

> 如果您使用的 ILM 规则只创建一个对象的一个副本，则必须在计划的维护窗口期间更换光纤通道 HBA 。否则，在此操作步骤 期间，您可能暂时无法访问这些对象。请参见有关的信息 "为什么不应使用单副本复制"。

步骤

1. 将 ESD 腕带的腕带一端绕在腕带上，并将扣具一端固定到金属接地，以防止静电放电。
2. 找到包含光纤通道 HBA 的控制器背面的提升板部件。



3. 抓住竖板部件并穿过蓝色标记的孔，然后小心地将其向上提起。提起提升板部件时，将其向机箱前部移动，以使其已安装适配器中的外部连接器能够脱离机箱。
4. 将提升板卡放在平坦的防静电表面上，并使金属机架朝下，以便接触适配器。

提升板部件中有两个适配器：一个光纤通道 HBA 和一个以太网网络适配器。图中显示了光纤通道 HBA 。

5. 打开蓝色适配器闩锁（带圆圈），然后小心地从提升板部件中卸下光纤通道 HBA 。稍微摇晃适配器，以便从其连接器中卸下适配器。请勿用力过大。
6. 将适配器放在平坦的防静电表面上。

完成后

安装替代光纤通道 HBA 。

重新安装光纤通道 HBA

替代光纤通道 HBA 安装在与已删除的光纤通道 HBA 相同的位置。

您需要的内容

- 您拥有正确的替代光纤通道 HBA 。
- 您已删除现有光纤通道 HBA 。

  删除光纤通道 HBA

步骤

1. 将 ESD 腕带的腕带一端绕在腕带上，并将扣具一端固定到金属接地，以防止静电放电。
2. 从包装中取出更换用的光纤通道 HBA 。
3. 在蓝色适配器闩锁处于打开位置的情况下，将光纤通道 HBA 与其在提升板部件上的连接器对齐；然后，小心地将适配器按入连接器中，直到其完全就位。

   提升板部件中有两个适配器：一个光纤通道 HBA 和一个以太网网络适配器。图中显示了光纤通道 HBA 。
4. 找到与系统板上的导销对齐的竖板部件上的对齐孔（带圆圈），以确保竖板部件正确定位。

5. 将提升板部件置于机箱中，确保其与系统板上的连接器和导销对齐；然后，插入提升板部件。
6. 小心地将竖板部件沿着其中心线，蓝色标记的孔旁边按到位，直到其完全就位。
7. 从要重新安装缆线的光纤通道 HBA 端口上取下保护盖。

完成后

如果控制器中没有其他要执行的维护过程，请重新安装控制器盖板。

重新安装 SG6000-CN 控制器盖板

更改 **SG6000-CN** 控制器的链路配置

您可以更改 SG6000-CN 控制器的以太网链路配置。您可以更改端口绑定模式，网络绑定模式和链路速度。

您需要的内容

此设备已运行 已置于维护模式。

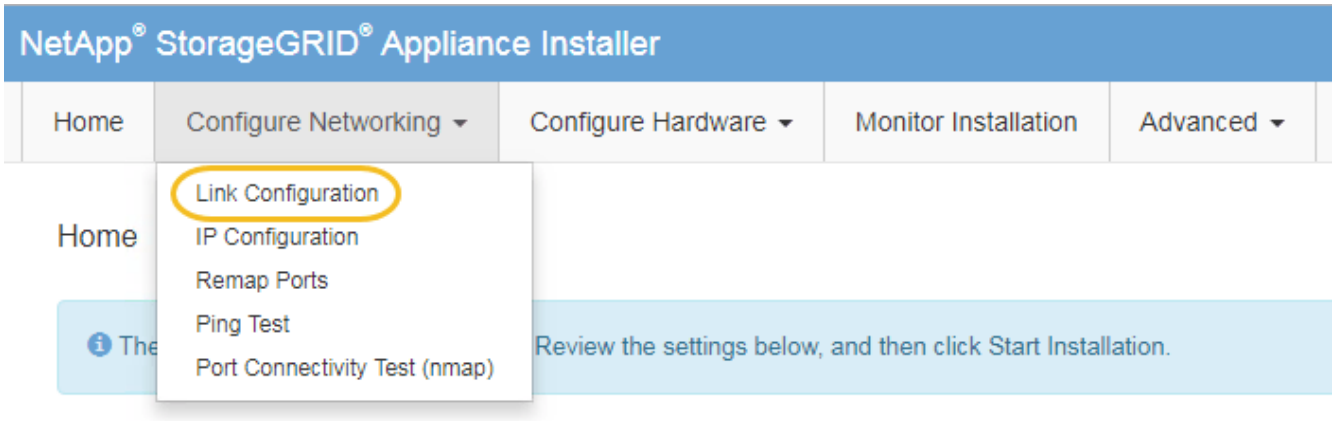
关于此任务

更改 SG6000-CN 控制器的以太网链路配置的选项包括：

- 将 * 端口绑定模式 * 从 " 固定 " 更改为 " 聚合 " 或从 " 聚合 " 更改为 " 固定 "
- 将 * 网络绑定模式 * 从主动备份更改为 LACP 或从 LACP 更改为主动备份
- 启用或禁用 VLAN 标记，或者更改 VLAN 标记的值
- 更改链路速度。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * 链路配置 * 。



2. 【 link_config_changes ， start=2]] 对链路配置进行所需的更改。

   有关选项的详细信息，请参见 配置网络链路（ SG6000 ）。

3. 对所做的选择感到满意后，单击 * 保存 * 。

   如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*Appliance_Controller_IP*:8443*`

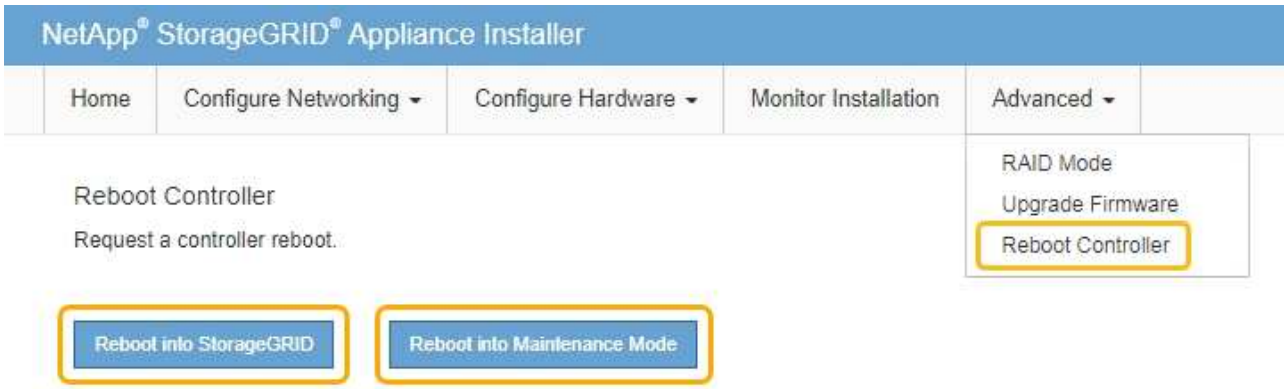
   如果更改了 VLAN 设置，则设备的子网可能已更改。如果需要更改设备的 IP 地址，请按照执行操作 配置 IP 地址 说明。

4. 从菜单中选择 * 配置网络连接 * > * Ping 测试 * 。
5. 使用 Ping 测试工具检查可能受中所做链路配置更改影响的任何网络上的 IP 地址连接 链路配置更改 步骤。

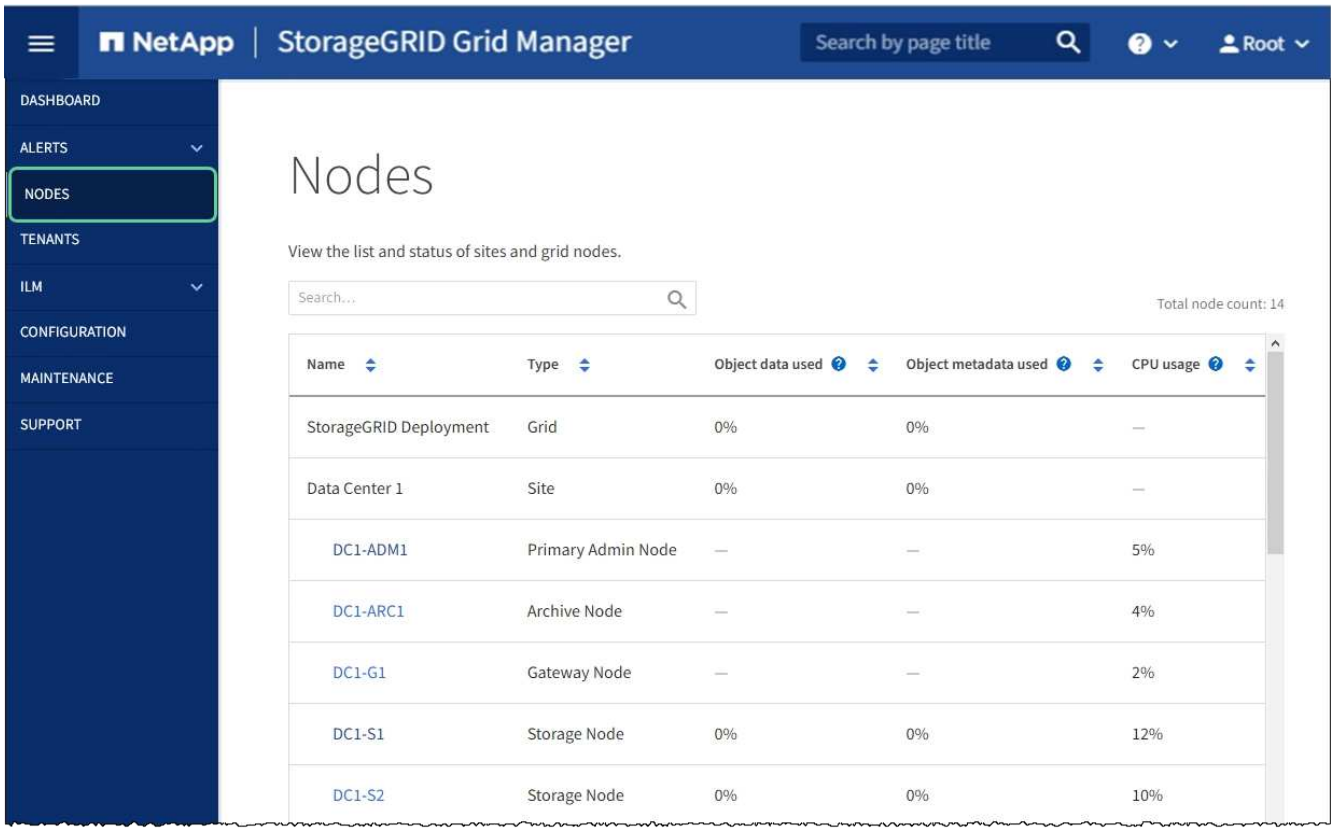
   除了您选择执行的任何其他测试之外，请确认您可以对主管理节点的网格网络 IP 地址以及至少一个其他存储节点的网格网络 IP 地址执行 ping 操作。如有必要，请返回到 链路配置更改 执行步骤并更正任何链路配置问题。

6. 如果您对链路配置更改是否正常工作感到满意，并且在节点处于维护模式时还需要执行其他步骤，请立即执行这些操作。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



更改 **MTU** 设置

您可以更改在为设备节点配置 IP 地址时分配的 MTU 设置。

关于此任务

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

要在不重新启动设备节点的情况下更改 MTU 设置， 使用更改 IP 工具。

如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络， 使用维护模式更改 MTU 设置。

使用更改 **IP** 工具更改 **MTU** 设置

您需要的内容

您有 `passwords.txt` 文件可用于更改 IP 工具。

步骤

访问更改 IP 工具并按中所述更新 MTU 设置 更改节点网络配置。

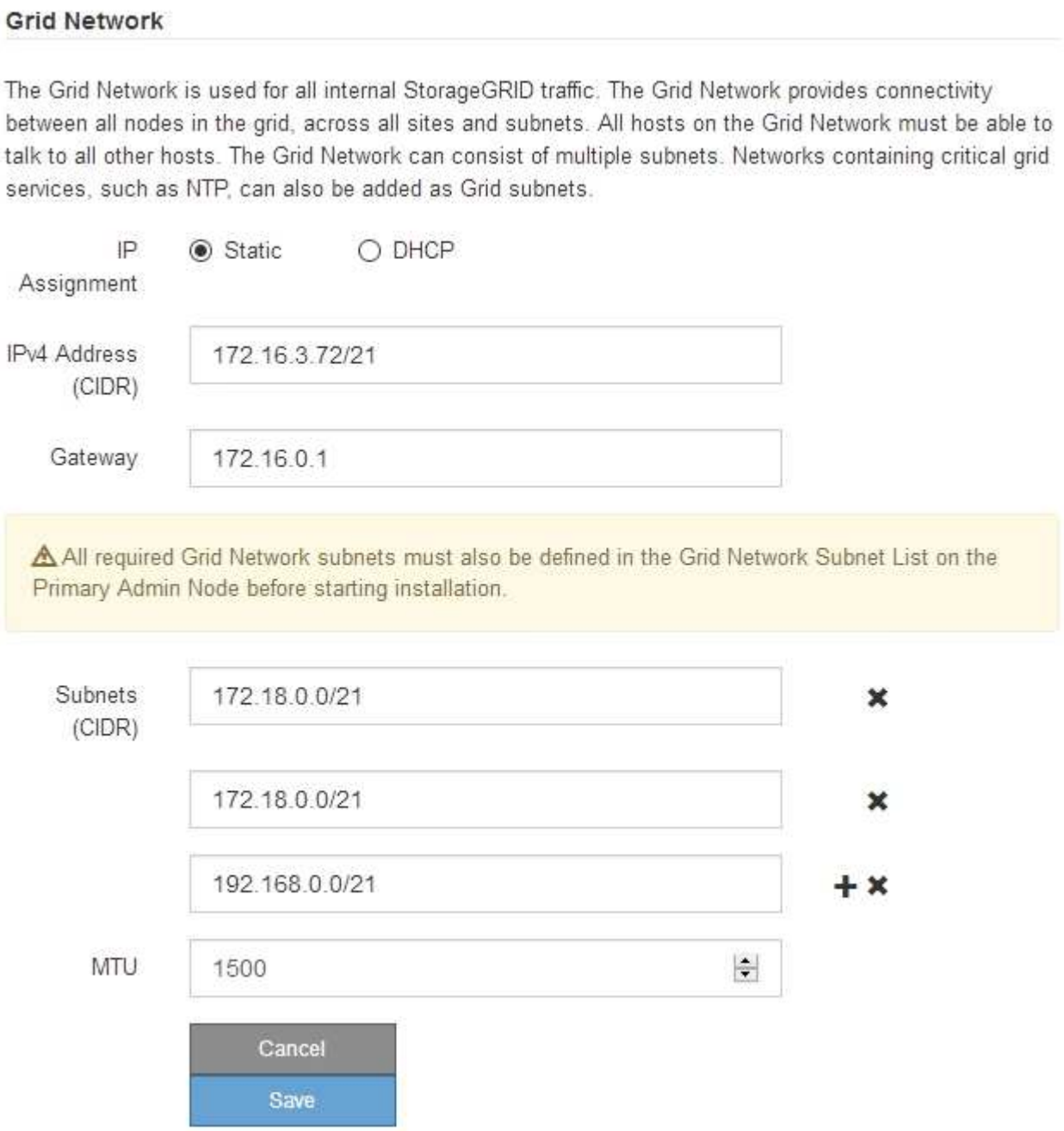
如果无法使用更改 IP 工具访问这些设置，请使用维护模式更改 MTU 设置。

您需要的内容

此设备已运行 已置于维护模式。

步骤

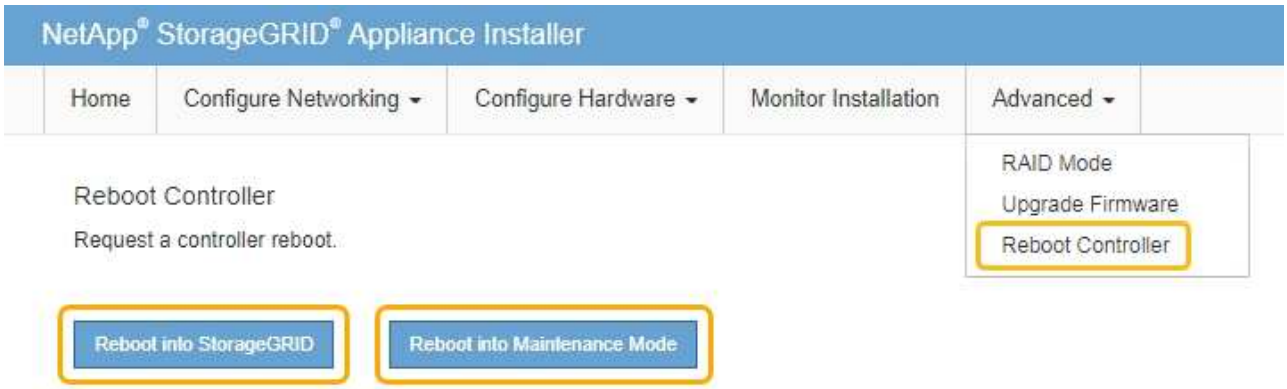
1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。
2. 对网格网络，管理网络和客户端网络的 MTU 设置进行所需的更改。



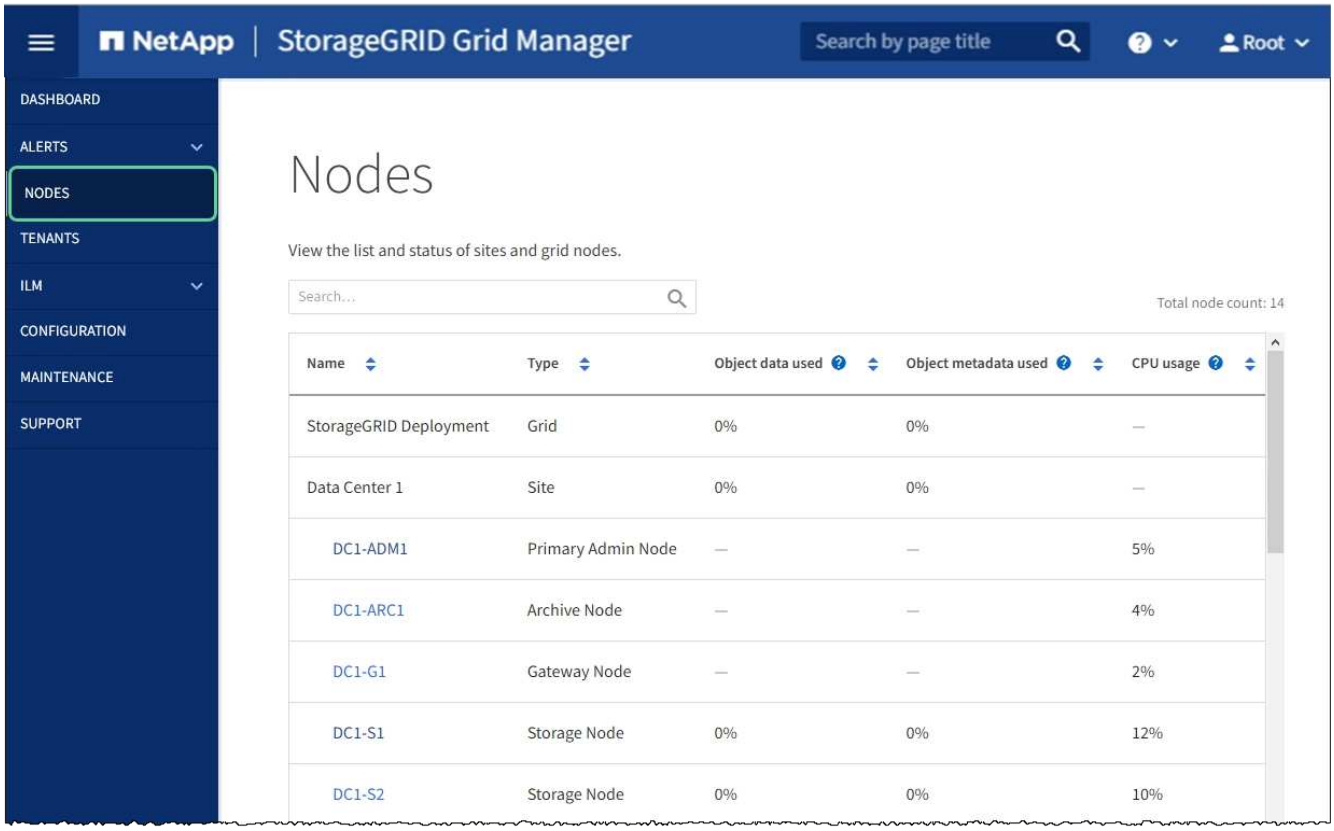
3. 如果对设置感到满意，请选择 * 保存 * 。

4. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

检查 **DNS** 服务器配置

您可以检查并临时更改此设备节点当前正在使用的域名系统（ DNS ）服务器。

您需要的内容

此设备已运行 已置于维护模式。

关于此任务

如果加密设备无法连接到密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群，则可能需要更改 DNS 服务器设置，因为 KMS 的主机名指定为域名，而不是 IP 地址。对设备的 DNS 设置所做的任何更改都是临时的，在退出维护模式时将丢失。要使这些更改永久生效，请在网格管理器中指定 DNS 服务器（ * 维护 * > * 网络 * > * DNS 服务器 * ）。

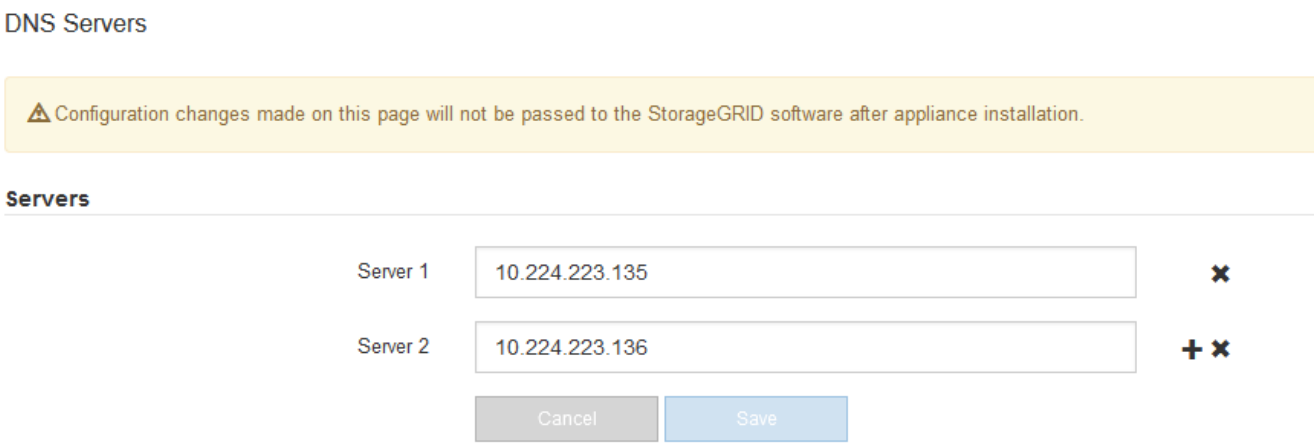
- 只有在节点加密的设备中，使用完全限定域名（而不是 IP 地址）为主机名定义 KMS 服务器时，才需要临时更改 DNS 配置。
- 当节点加密设备使用域名连接到 KMS 时，它必须连接到为网格定义的一个 DNS 服务器。然后，其中一个 DNS 服务器会将域名转换为 IP 地址。
- 如果节点无法访问网格的 DNS 服务器，或者您在节点加密设备节点脱机时更改了网格范围的 DNS 设置，则节点将无法连接到 KMS 。在解析 DNS 问题描述 之前，无法解密设备上的加密数据。

要解决 DNS 问题描述 阻止 KMS 连接的问题，请在 StorageGRID 设备安装程序中指定一个或多个 DNS 服务器的 IP 地址。通过这些临时 DNS 设置，设备可以连接到 KMS 并对节点上的数据进行解密。

例如，如果在加密节点脱机时网格的 DNS 服务器发生更改，则该节点将无法在重新联机时访问 KMS ，因为它仍在使用先前的 DNS 值。在 StorageGRID 设备安装程序中输入新的 DNS 服务器 IP 地址后，可以通过临时 KMS 连接对节点数据进行解密。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * DNS 配置 * 。
2. 验证指定的 DNS 服务器是否正确。



3. 如果需要，请更改 DNS 服务器。

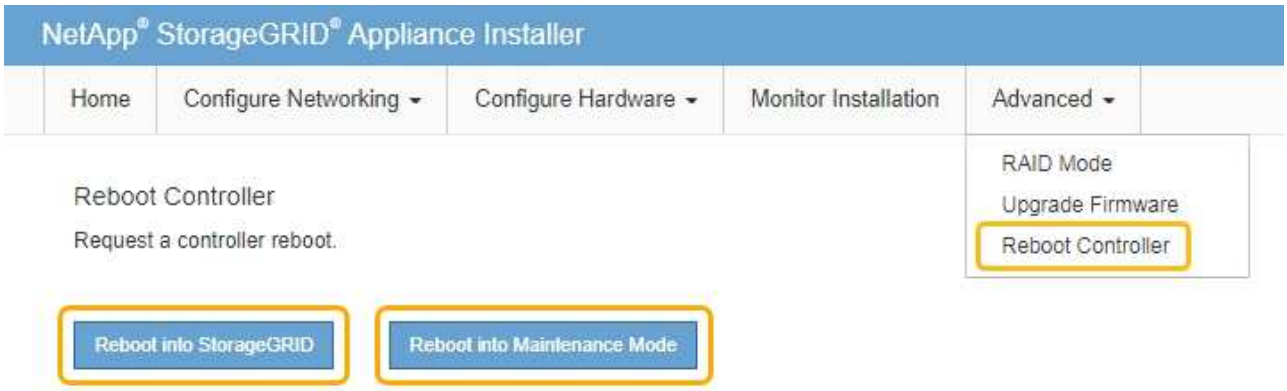
对 DNS 设置所做的更改是临时的，当您退出维护模式时，这些更改将丢失。

4. 对临时 DNS 设置感到满意后，请选择 * 保存 * 。

   节点使用此页面上指定的 DNS 服务器设置重新连接到 KMS ，从而可以解密节点上的数据。

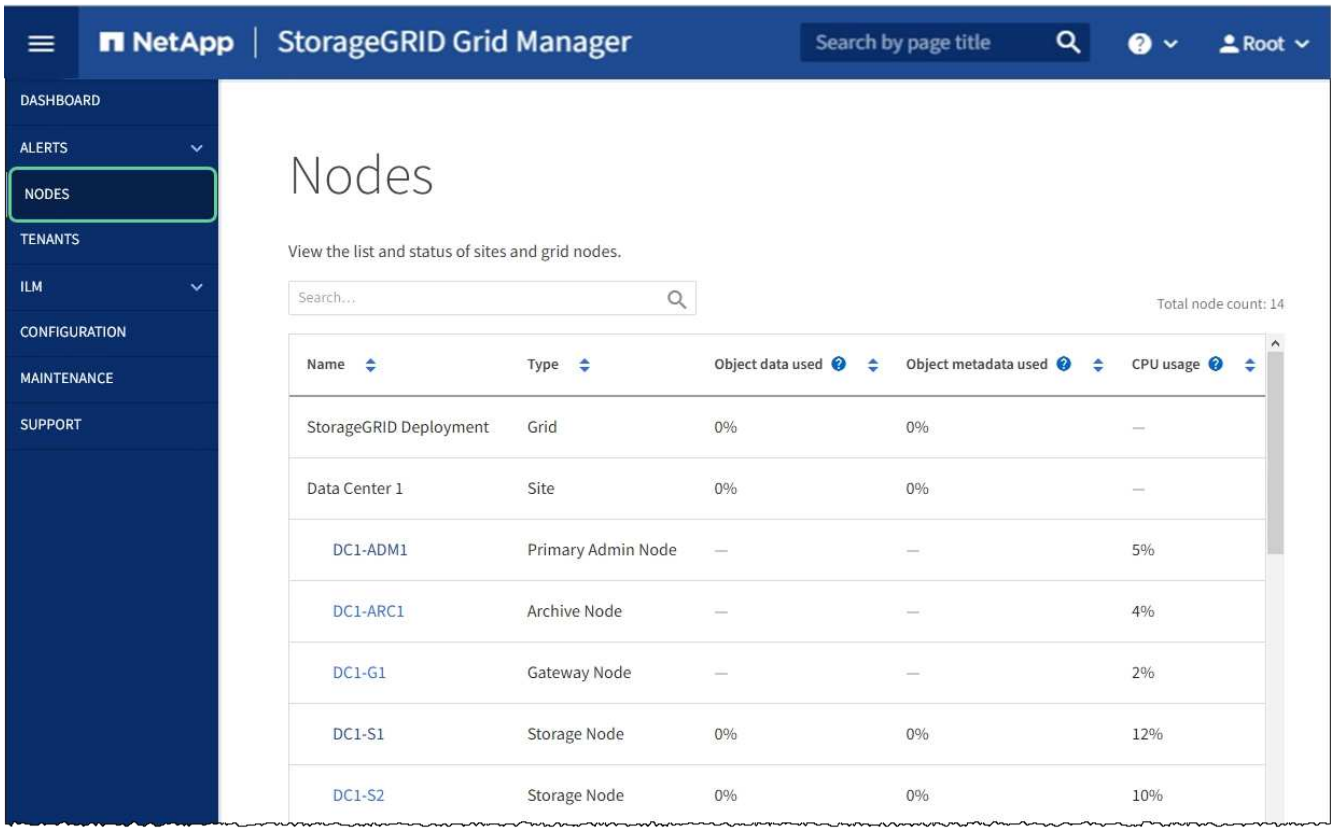
5. 解密节点数据后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



当节点重新启动并重新加入网格时，它将使用网格管理器中列出的系统范围的 DNS 服务器。重新加入网格后，在设备处于维护模式时，设备将不再使用 StorageGRID 设备安装程序中指定的临时 DNS 服务器。

设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



在维护模式下监控节点加密（ **SG6000** ）

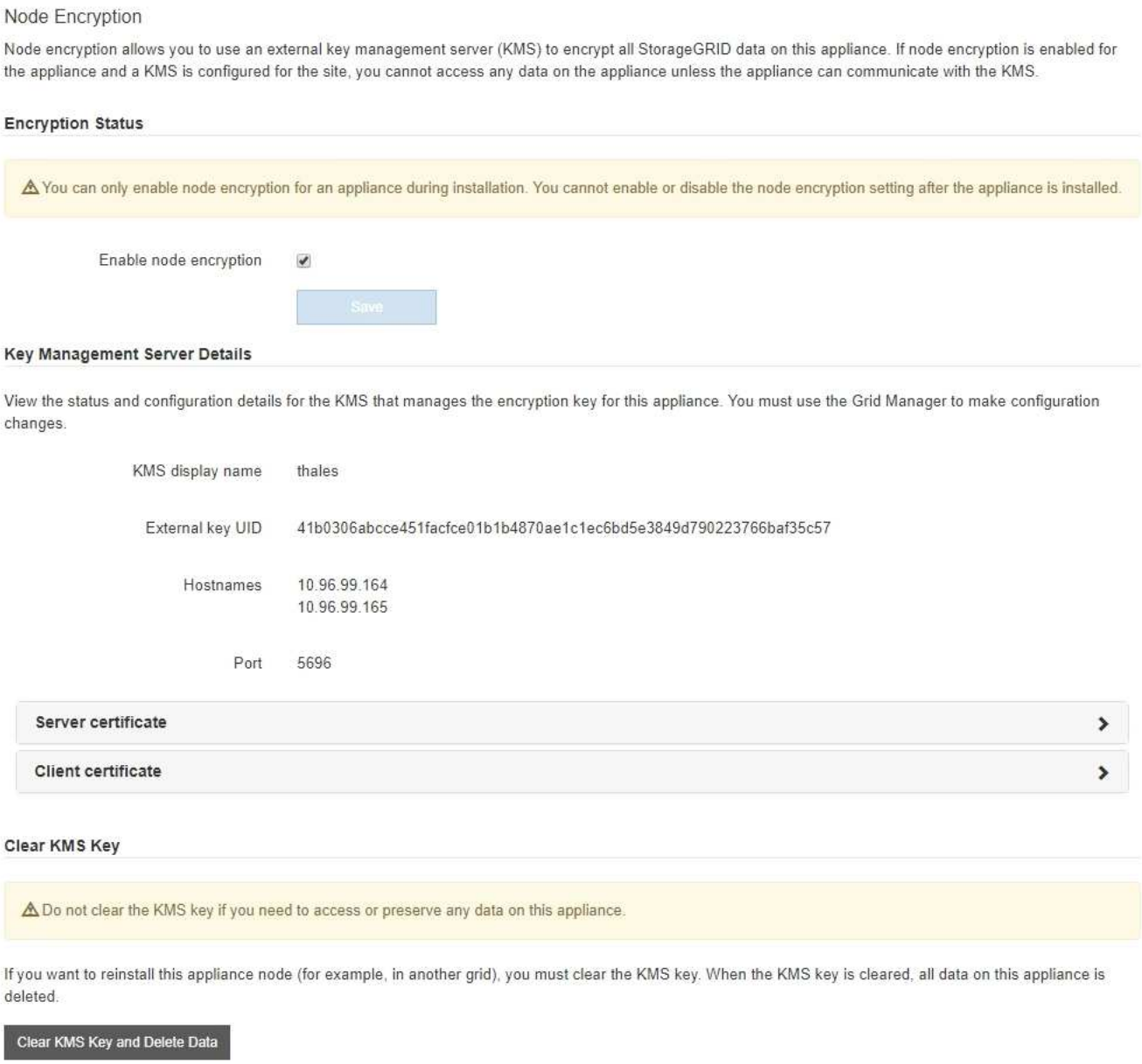
如果您在安装期间为设备启用了节点加密，则可以监控每个设备节点的节点加密状态，包括节点加密状态和密钥管理服务器（ KMS ）详细信息。

您需要的内容

- 必须在安装期间为设备启用节点加密。安装设备后，您无法启用节点加密。
- 您已拥有 已将设备置于维护模式。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置硬件 * > * 节点加密 * 。



节点加密页面包括以下三个部分：

- " 加密状态 " 显示设备是启用还是禁用了节点加密。
- 密钥管理服务器详细信息显示了有关用于对设备进行加密的 KMS 的信息。您可以展开服务器和客户端证书部分以查看证书详细信息和状态。
  - 要解决证书本身的问题，例如续订已过期的证书，请参见管理 StorageGRID 的说明中有关 KMS 的信息。
  - 如果连接到 KMS 主机时出现意外问题，请验证域名系统（ DNS ）服务器是否正确以及设备网络连接是否配置正确。

    检查 DNS 服务器配置

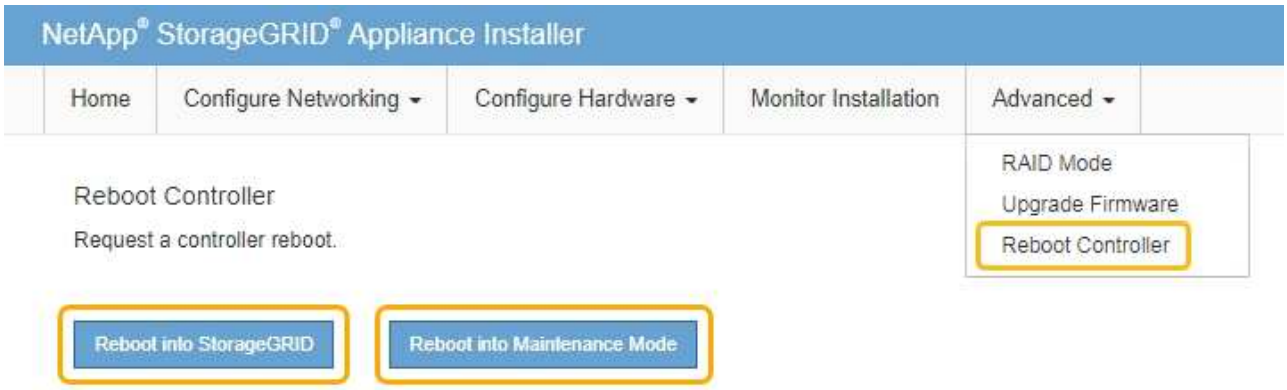
  - 如果无法解决证书问题，请联系技术支持。
- 清除 KMS 密钥会禁用设备的节点加密，删除设备与为 StorageGRID 站点配置的密钥管理服务器之间的关联，并删除设备中的所有数据。您必须 清除 KMS 密钥 在将设备安装到另一个 StorageGRID 系统之

前。

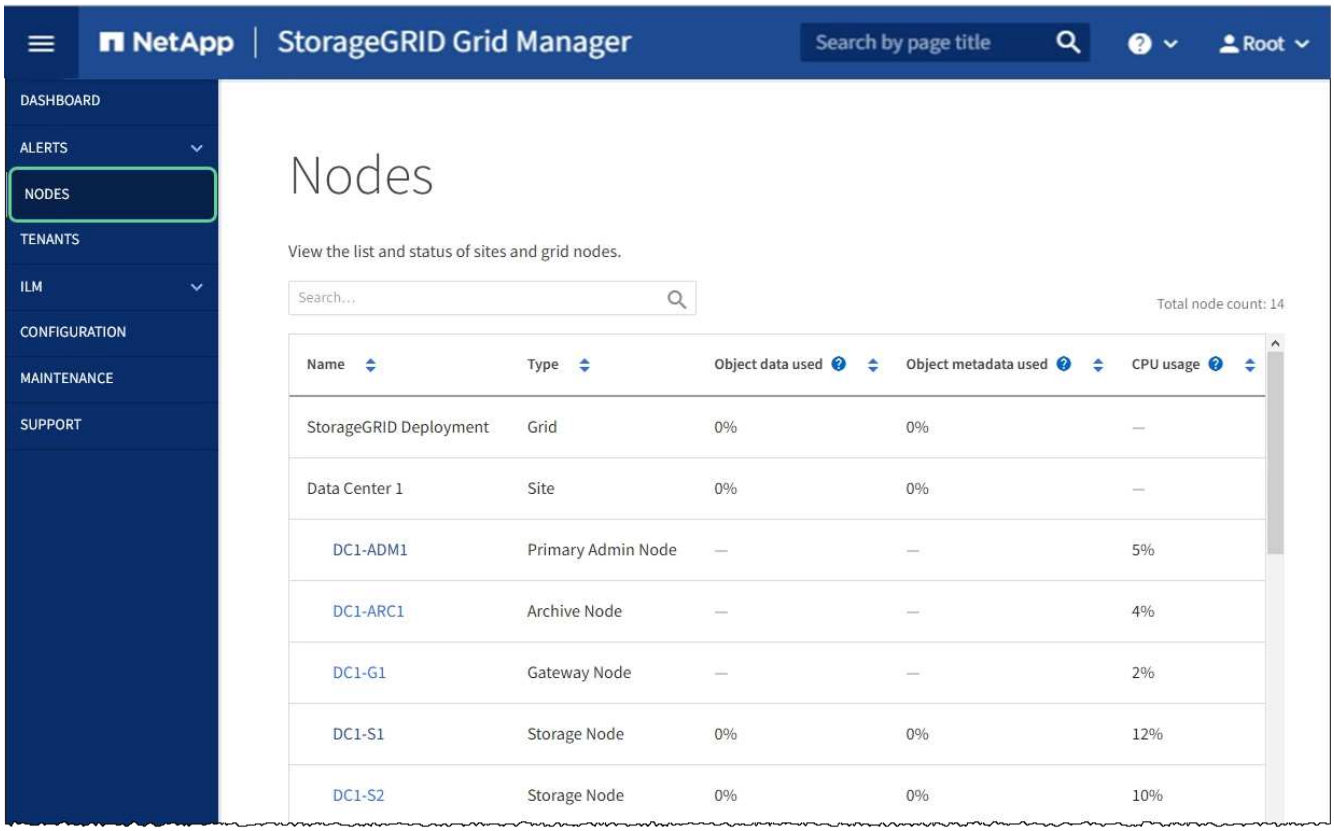
清除 KMS 配置将从设备中删除数据，从而使其永远无法访问。此数据不可恢复。

2. 检查完节点加密状态后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

清除密钥管理服务器配置

清除密钥管理服务器（ KMS ）配置将禁用设备上的节点加密。清除 KMS 配置后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

您需要的内容

如果需要保留设备上的数据，则必须先执行节点停用操作步骤 或克隆节点，然后才能清除 KMS 配置。

清除 KMS 后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

停用节点 将其包含的任何数据移动到 StorageGRID 中的其他节点。

关于此任务

清除设备 KMS 配置将禁用节点加密，从而删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。然后，设备上的数据将被删除，并且设备将保持预安装状态。此过程不能逆转。

必须清除 KMS 配置：

- 在将设备安装到不使用 KMS 或使用其他 KMS 的其他 StorageGRID 系统之前，请先安装此设备。

如果您计划在使用相同 KMS 密钥的 StorageGRID 系统中重新安装设备节点，请勿清除 KMS 配置。

- 在恢复和重新安装 KMS 配置丢失且 KMS 密钥不可恢复的节点之前。
- 在退回您的站点上先前使用的任何设备之前。
- 停用已启用节点加密的设备后。

> 在清除 KMS 以将其数据移动到 StorageGRID 系统中的其他节点之前，请停用此设备。在停用设备之前清除 KMS 将导致数据丢失，并可能导致设备无法运行。

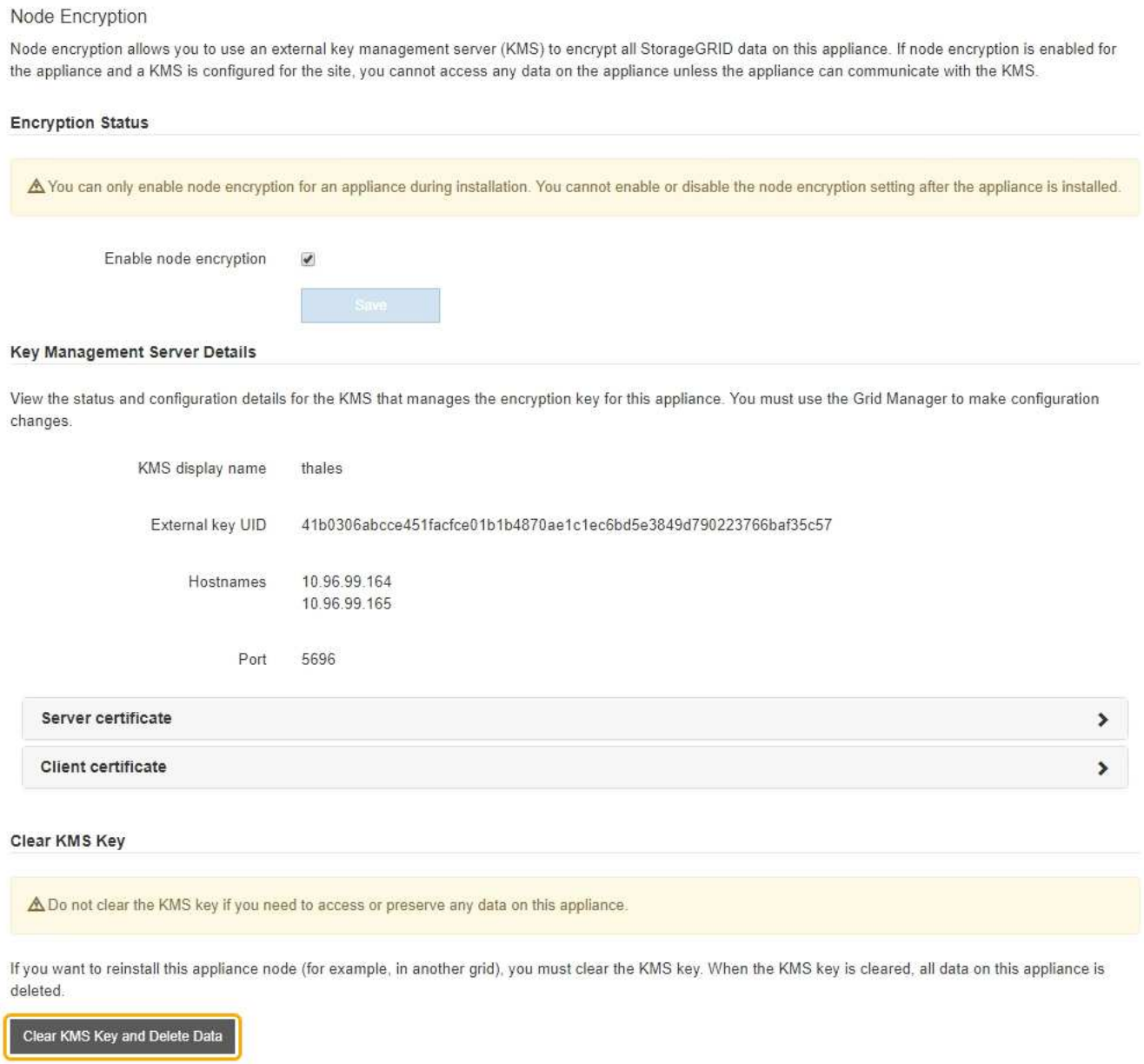
步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

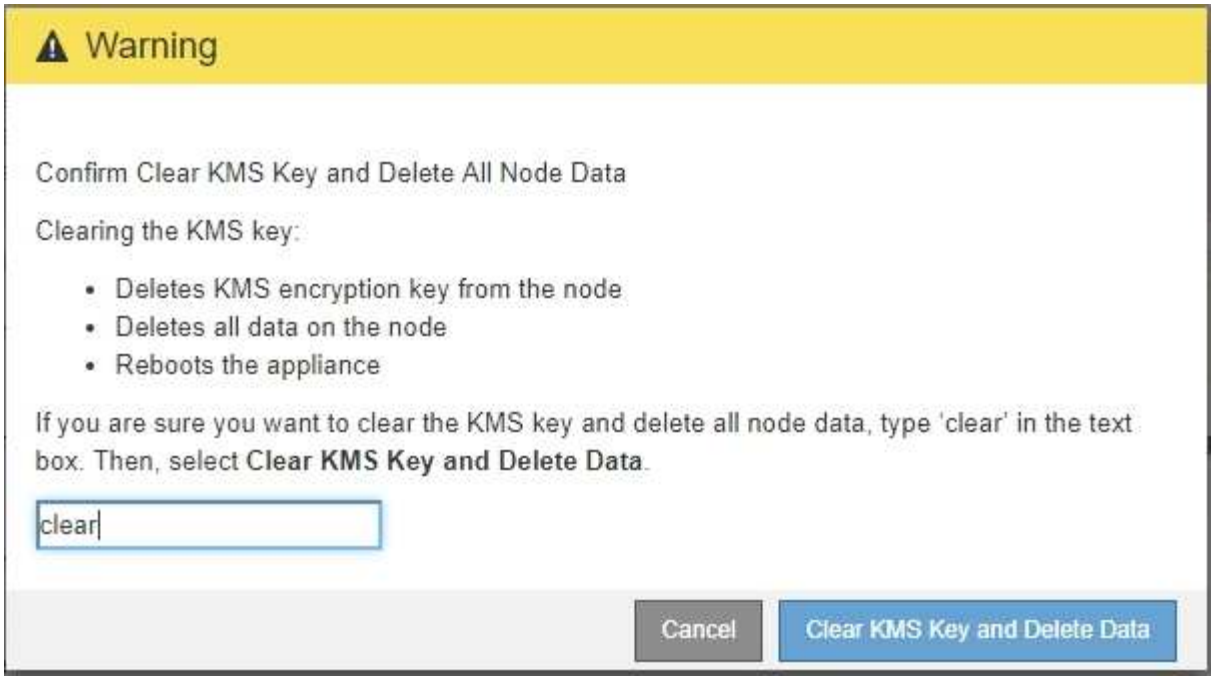
   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 节点加密 * 。



如果清除了 KMS 配置，则设备上的数据将被永久删除。此数据不可恢复。

3. 在窗口底部，选择 * 清除 KMS 密钥和删除数据 * 。
4. 如果确实要清除 KMS 配置，请键入 + ` * clear*` + 并选择 * 清除 KMS 密钥和删除数据 * 。



KMS 加密密钥和所有数据将从节点中删除，设备将重新启动。这可能需要长达 20 分钟。

5. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

6. 选择 * 配置硬件 * > * 节点加密 * 。
7. 验证是否已禁用节点加密，以及是否已从窗口中删除 * 密钥管理服务器详细信息 * 和 * 清除 KMS 密钥和删除数据 * 控件中的密钥和证书信息。

   在将设备重新安装到网格中之前，无法在设备上重新启用节点加密。

完成后

在设备重新启动并确认 KMS 已清除且设备处于预安装状态后，您可以从 StorageGRID 系统中物理删除此设备。请参见 有关准备重新安装设备的说明。

相关信息

管理 StorageGRID

SG5700 存储设备

StorageGRID SG5700 设备概述

SG5700 StorageGRID 设备是一个集成的存储和计算平台，作为 StorageGRID 网格中的存储节点运行。此设备可在混合网格环境中使用，该环境将设备存储节点与虚拟（基于软件的）存储节点相结合。

StorageGRID SG5700系列设备具有以下功能：

- 集成 StorageGRID 存储节点的存储和计算要素。
- 包括 StorageGRID 设备安装程序，以简化存储节点的部署和配置。
- 包括用于硬件管理和监控的 E 系列 SANtricity System Manager 。
- 最多支持四个连接到 StorageGRID 网格网络和客户端网络的 10-GbE 或 25-GbE 连接。
- 支持全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。如果将这些驱动器与 SANtricity 系统管理器中的驱动器安全功能结合使用，则会阻止未经授权的数据访问。

SG5700设备有四种型号：SG5712和SG5712X以及SG5760和SG5760X。除了存储控制器上互连端口的位置之外、SG5712和SG5712X之间在规格或功能上没有区别。同样、除了存储控制器上互连端口的位置之外、SG5760和SG5760X在规格或功能上没有任何区别。

这些型号包括以下组件：

组件	**SG5712**	**SG5712X**	**SG5760**	**SG5760X**
计算控制器	E5700SG 控制器	E5700SG 控制器	E5700SG 控制器	E5700SG 控制器
存储控制器	E2800A控制器	E2800B控制器	E2800A控制器	E2800B控制器
机箱	E 系列 DE212C 机箱，一个双机架单元（ 2U ）机箱	E 系列 DE212C 机箱，一个双机架单元（ 2U ）机箱	E 系列 DE460C 机箱，一个四机架单元（ 4U ）机箱	E 系列 DE460C 机箱，一个四机架单元（ 4U ）机箱
驱动器	12 个 NL-SAS 驱动器（ 3.5 英寸）	12 个 NL-SAS 驱动器（ 3.5 英寸）	60 个 NL-SAS 驱动器（ 3.5 英寸）	60 个 NL-SAS 驱动器（ 3.5 英寸）
冗余电源和风扇	两个电源风扇箱	两个电源风扇箱	两个电源箱和两个风扇箱	两个电源箱和两个风扇箱

根据每个机箱中的驱动器数量， StorageGRID 设备中可用的最大原始存储空间是固定的。您不能通过添加具有额外驱动器的磁盘架来扩展可用存储。

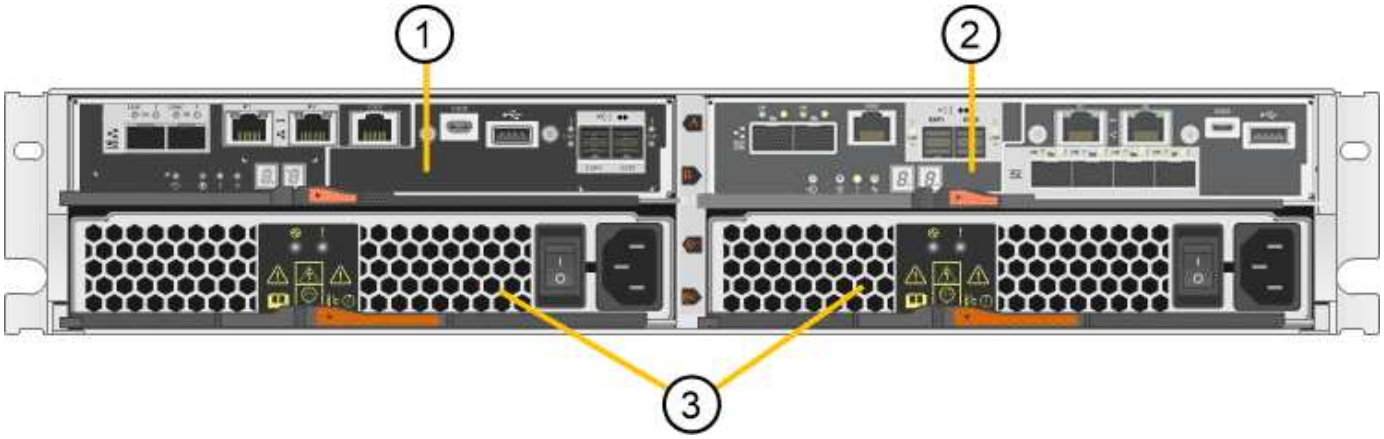
型号**SG5712**和**5712X**

图中显示了SG5712和SG5712X型号的正面和背面、这是一个2U机箱、可容纳12个驱动器。

- SG5712前视图和后视图*

SG5712 包括两个控制器和两个电源风扇箱。

- SG5712组件*



Callout	Description
1.	E2800A控制器(存储控制器)
2.	E5700SG 控制器（计算控制器）
3.	电源风扇箱

- SG5712X前视图和后视图*

SG5712X包括两个控制器和两个电源风扇箱。

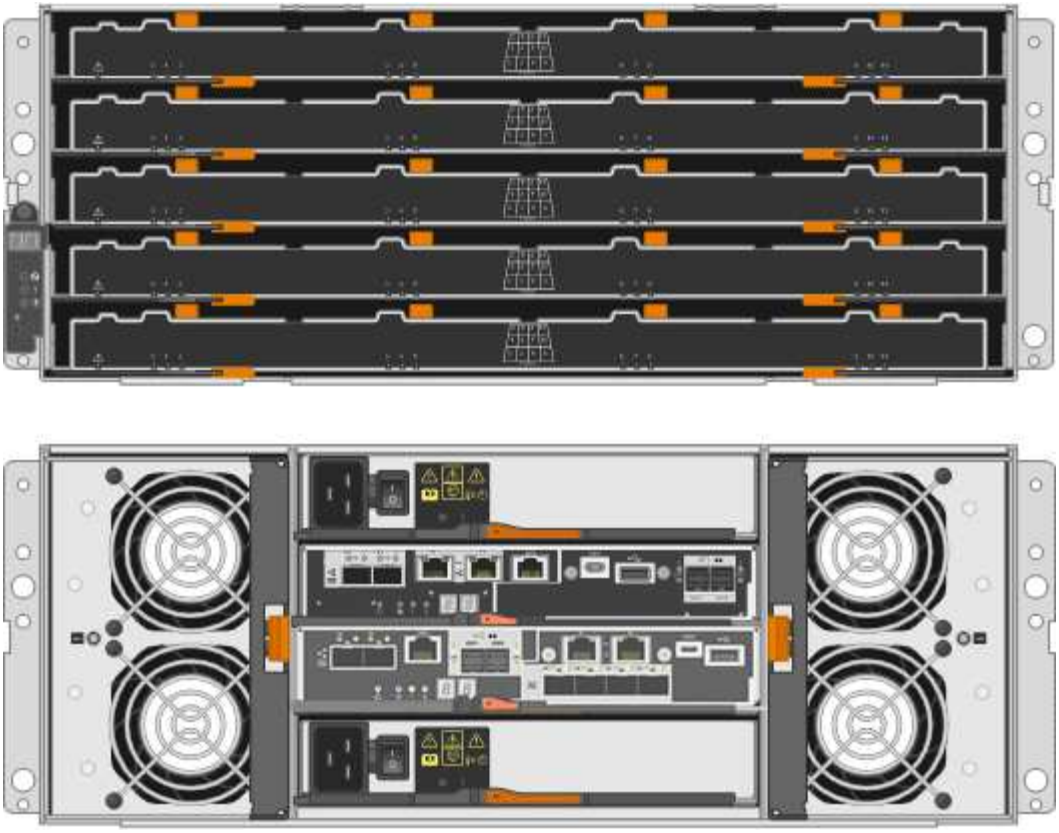
- SG5712X组件*

Callout	Description
1.	E2800B控制器(存储控制器)
2.	E5700SG 控制器（计算控制器）
3.	电源风扇箱

型号**SG5760**和**SG5760X**

图中显示了SG5760和SG5760X型号的正面和背面、这是一个4U机箱、可在5个驱动器抽盒中容纳60个驱动器。

- SG5760前视图和后视图*

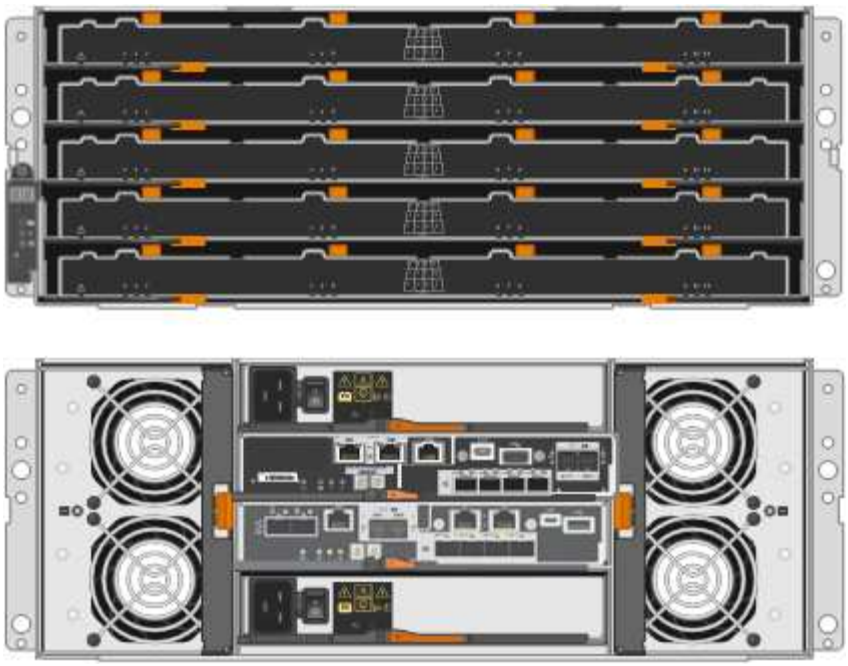


SG5760 包括两个控制器，两个风扇箱和两个电源箱。

- SG5760组件*

Callout	Description
1.	E2800A控制器(存储控制器)
2.	E5700SG 控制器（计算控制器）
3.	风扇箱（第 1 页，共 2 页）
4.	电源箱（第 1 页，共 2 页）

- SG5760X前视图和后视图*



SG5760S包括两个控制器、两个风扇箱和两个电源箱。

- SG5760X组件*

Callout	Description
1.	E2800B控制器(存储控制器)
2.	E5700SG 控制器（计算控制器）
3.	风扇箱（第 1 页，共 2 页）
4.	电源箱（第 1 页，共 2 页）

相关信息

"NetApp E 系列系统文档站点"

StorageGRID 5700设备中的控制器

StorageGRID 设备的12驱动器SG5712和SG5712X以及60驱动器SG5760和SG5760X型号都包括一个E5700SG计算控制器和一个E系列E2800存储控制器。

- SG5712和SG5760使用E2800A控制器。
- SG5712X和SG5760X使用E2800B控制器。

```
The E2800A and E2800B controllers are identical in specification and
function except for the location of the interconnect ports.
```

您应查看这些图表以了解控制器之间的差异。

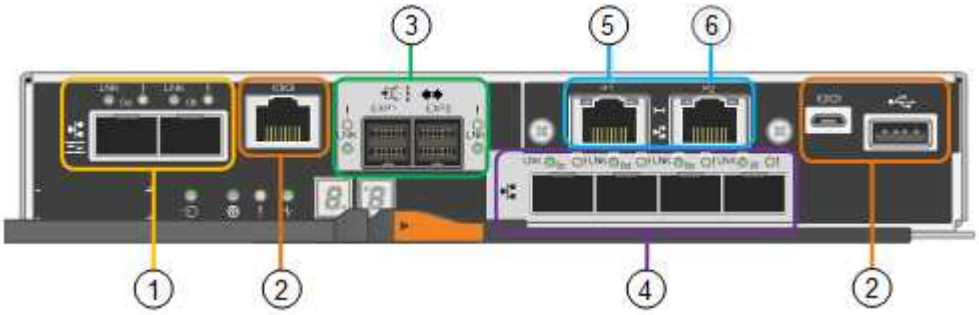
E5700SG 控制器

- 用作设备的计算服务器。
- 包括 StorageGRID 设备安装程序。

> 设备上未预安装 StorageGRID 软件。部署设备时，可从管理节点访问此软件。

- 可以连接到所有三个 StorageGRID 网络，包括网格网络，管理网络和客户端网络。
- 连接到 E2800 控制器并作为启动程序运行。

此图显示了 E5700SG 控制器背面的连接器。



	Port	Type	使用 ...
1.	互连端口 1 和 2	16GB/s 光纤通道（ FC ），光纤 SFPa	将 E5700SG 控制器连接到 E2800 控制器。
2.	诊断和支持端口	• RJ-45 串行端口 • 微型 USB 串行端口 • USB 端口	为技术支持预留。
3.	驱动器扩展端口	12 Gb/ 秒 SAS	未使用。StorageGRID 设备不支持扩展驱动器架。
4.	网络端口 1-4	10-GbE 或 25-GbE ，取决于 SFP 收发器类型，交换机速度和已配置的链路速度	连接到网格网络和 StorageGRID 客户端网络。
5.	管理端口 1	1 Gb （ RJ-45 ）以太网	连接到 StorageGRID 的管理网络。

	Port	Type	使用 ...
6.	管理端口 2	1 Gb （ RJ-45 ）以太网	选项： • 与管理端口 1 绑定，以便与 StorageGRID 的管理网络建立冗余连接。 • 保持未连接状态，并可用于临时本地访问（ IP 169.254.0.1 ）。 • 安装期间，如果 DHCP 分配的 IP 地址不可用，请使用端口 2 进行 IP 配置。

E2800系列存储控制器

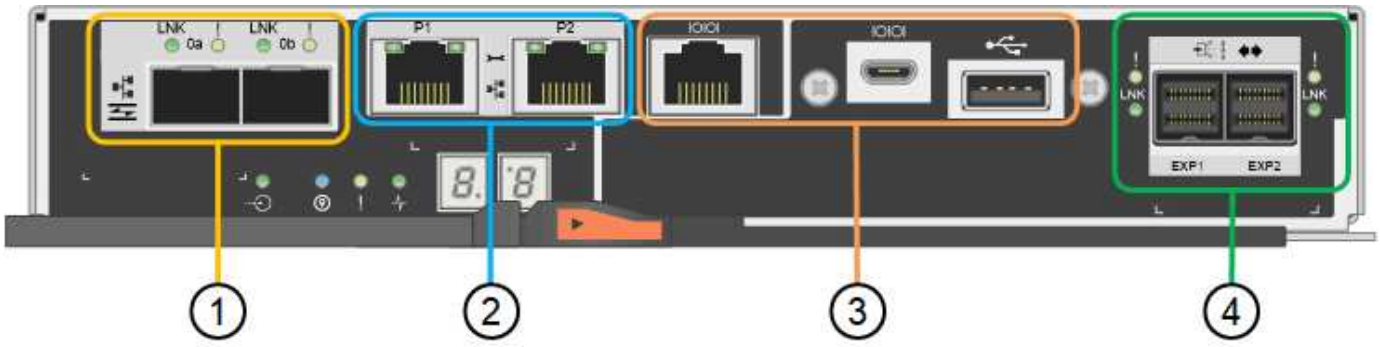
SG5700设备中使用了两个版本的E2800存储控制器：E2800A和E2800B。E2800A没有HIC、E2800B有四端口HIC。这两个控制器版本的规格和功能相同、但互连端口的位置除外。

E2800系列存储控制器具有以下规格：

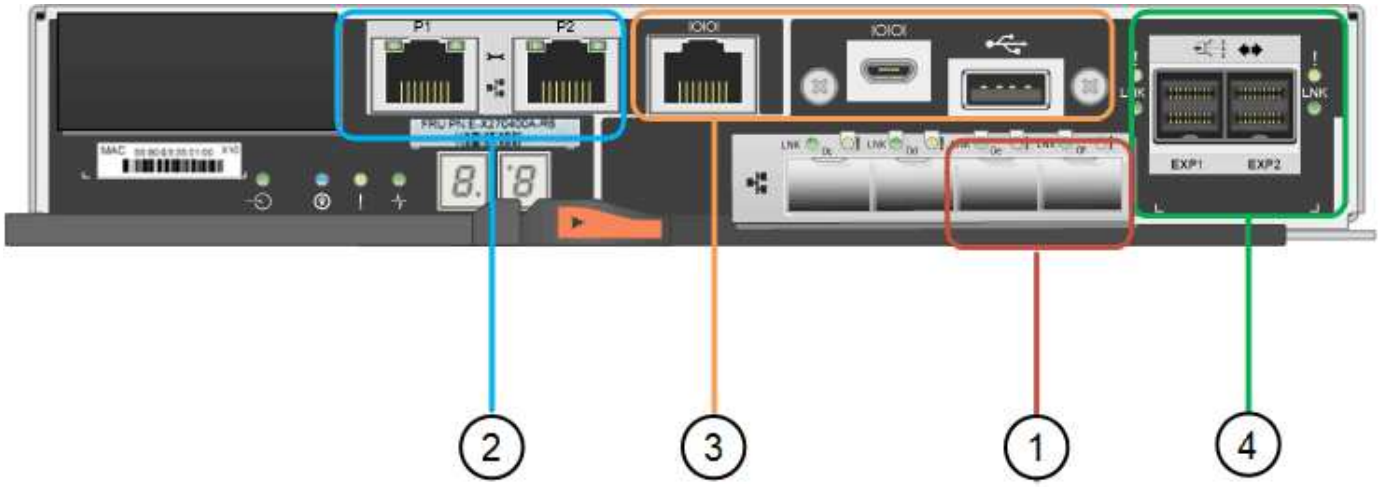
- 用作设备的存储控制器。
- 管理驱动器上的数据存储。
- 在单工模式下用作标准 E 系列控制器。
- 包括 SANtricity 操作系统软件（控制器固件）。
- 包括用于监控设备硬件和管理警报的 SANtricity System Manager ， AutoSupport 功能和驱动器安全功能。
- 连接到 E5700SG 控制器并作为目标运行。

下图显示了E2800A和E2800B控制器背面的连接器。

- E2800A*背面的连接器



- E2800B*背面的连接器



	Port	Type	使用 ...
1.	互连端口 1 和 2	16 GB/s FC 光纤 SFPa	将 E2800 控制器连接到 E5700SG 控制器。
2.	管理端口 1 和 2	1 Gb （ RJ-45 ） 以太网	• 端口 1 选项： ◦ 连接到管理网络以启用对 SANtricity 系统管理器的直接 TCP/IP 访问 ◦ 保持未连接状态以保存交换机端口和 IP 地址。使用网格管理器或存储网格设备安装程序 UI 访问 SANtricity System Manager 。 • 注 * ： 如果您选择使端口 1 保持未连接状态，则某些可选的 SANtricity 功能（例如 NTP 同步以获得准确的日志时间戳）将不可用。 • 注 * ： 如果不对端口 1 布线，则需要 StorageGRID 11.5 或更高版本以及 SANtricity 11.70 或更高版本。 • 端口 2 预留用于技术支持。

	Port	Type	使用 ...
3.	诊断和支持端口	• RJ-45 串行端口 • 微型 USB 串行端口 • USB 端口	保留供技术支持使用。
4.	驱动器扩展端口。	12 Gb/ 秒 SAS	未使用。

安装和部署概述

您可以在首次部署 StorageGRID 时安装一个或多个 StorageGRID 设备，也可以稍后在扩展过程中添加设备存储节点。在恢复操作中，您可能还需要安装设备存储节点。

将 StorageGRID 存储设备添加到 StorageGRID 系统包括四个主要步骤：

1. 准备安装：
   - 正在准备安装站点
   - 打开包装箱的包装并检查包装箱中的物品
   - 获取其他设备和工具
   - 收集 IP 地址和网络信息
   - 可选：如果您计划对所有设备数据进行加密，请配置外部密钥管理服务器（ KMS ）。有关外部密钥管理的详细信息，请参见 StorageGRID 管理说明。
2. 安装硬件：
   - 注册硬件
   - 将设备安装到机柜或机架中
   - 安装驱动器（仅限 SG5760 ）
   - 为设备布线
   - 连接电源线并接通电源
   - 查看启动状态代码
3. 配置硬件：
   - 访问 SANtricity 系统管理器，为 E2800 控制器上的管理端口 1 设置静态 IP 地址以及配置 SANtricity 系统管理器设置
   - 访问 StorageGRID 设备安装程序并配置连接到 StorageGRID 网络所需的链路和网络 IP 设置
   - 可选：如果您计划使用外部 KMS 对设备数据进行加密，请启用节点加密。
   - 可选：更改 RAID 模式。
4. 将设备部署为存储节点：

任务	说明
在新的 StorageGRID 系统中部署设备存储节点	部署设备存储节点
将设备存储节点添加到现有 StorageGRID 系统	有关扩展 StorageGRID 系统的说明
在存储节点恢复操作中部署设备存储节点	恢复和维护说明

相关信息

准备安装（ SG5700 ）

安装硬件

配置硬件（ SG5700 ）

安装 VMware

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

SG100 和 SG1000 服务设备

扩展网格

恢复和维护

管理 StorageGRID

准备安装（ **SG5700** ）

准备安装 StorageGRID 设备需要准备站点并获取所有必需的硬件，缆线和工具。您还应收集 IP 地址和网络信息。

相关信息

Web 浏览器要求

准备站点（ **SG5700** ）

在安装设备之前，您必须确保要使用的站点和机柜或机架符合 StorageGRID 设备的规格。

步骤

1. 确认站点满足温度，湿度，海拔范围，气流，散热， 布线，电源和接地。有关详细信息，请参见 NetApp Hardware Universe 。
2. 如果要安装 SG5760 型号，请确认您所在位置提供 240 伏交流电源。
3. 获取一个 19 英寸（ 48.3 厘米）的机柜或机架，以适合此大小的磁盘架（不带缆线）：

设备型号	高度	宽度	深度	最大重量
SG5712 （ 12 个驱动器）	3.41 英寸 （ 8.68 厘米）	17.6 英寸 （ 44.7 厘米）	21.1 英寸 （ 53.6 厘米）	63.9 磅 （ 29.0 千克）
SG5760 （ 60 个驱动器）	6.87 英寸 （ 17.46 厘米）	17.66 英寸 （ 44.86 厘米）	38.25 英寸 （ 97.16 厘米）	250 磅 （ 113 千克）

4. 安装所需的任何网络交换机。有关兼容性信息，请参见 NetApp 互操作性表工具。

相关信息

"NetApp Hardware Universe"

"NetApp 互操作性表工具"

打开包装箱（ **SG5700** ）

安装 StorageGRID 设备之前，请打开所有包装箱的包装，并将包装箱上的物品与包装清单上的物品进行比较。

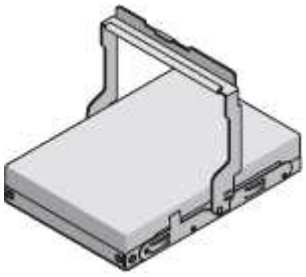
- * 已安装 12 个驱动器的 SG5712 设备 *

- * 未安装驱动器的 SG5760 设备 *

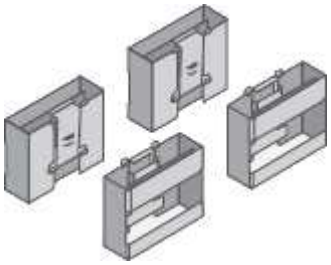
- * 设备前挡板 *

- * 导轨套件及说明 *

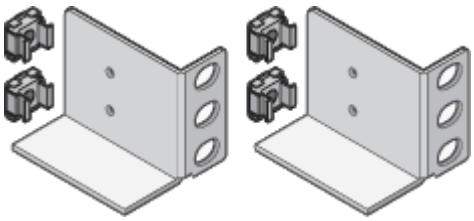
- * SG5760： 60 个驱动器 *



- * SG5760： 句柄 *



- * SG5760： 用于方孔机架安装的背面支架和固定框架螺母 *



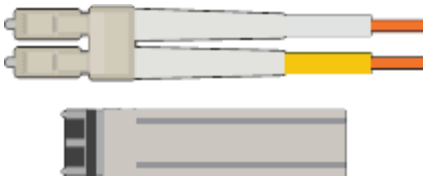
缆线和连接器

StorageGRID 设备的发货包括以下缆线和连接器：

- * 您所在国家或地区有两条电源线 *

  您的机柜可能使用专用电源线，而不是设备随附的电源线。

- * 光缆和 SFP 收发器 *



用于 FC 互连端口的两根光缆

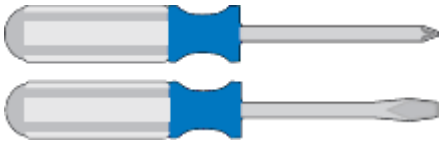
八个 SFP+ 收发器，与四个 16Gb/s FC 互连端口和四个 10-GbE 网络端口兼容

获取其他设备和工具（ **SG5700** ）

在安装 StorageGRID 设备之前，请确认您拥有所需的所有附加设备和工具。

要安装和配置硬件，您需要使用以下附加设备：

- * 螺丝刀 *

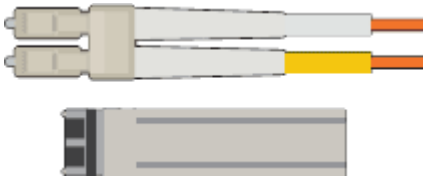


十字线编号2 把螺丝刀

中型平口螺丝刀

- * ESD 腕带 *

- * 光缆和 SFP 收发器 *



您计划使用的 10/25/GbE 端口的光缆

可选：如果要使用 25 GbE 链路速度，请使用 SFP28 收发器

- * 以太网缆线 *

- * 服务笔记本电脑 *

支持的 Web 浏览器

SSH 客户端，例如 PuTTY

1 Gb （ RJ-45 ）以太网端口

- * 可选工具 *

带十字头的电钻

Flashlight

SG5760 的机械升降机

查看设备网络连接（ **SG5700** ）

在安装 StorageGRID 设备之前，您应了解可以将哪些网络连接到设备，以及如何使用每个控制器上的端口。

StorageGRID 设备网络

将 StorageGRID 设备部署为 StorageGRID 网格中的存储节点时，您可以将其连接到以下网络：

- * 适用于 StorageGRID 的网格网络 * ： 网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。网格网络为必填项。
- * 适用于 StorageGRID 的管理网络 * ： 管理网络是一个用于系统管理和维护的封闭网络。管理网络通常是一

个专用网络，不需要在站点之间进行路由。管理网络是可选的。

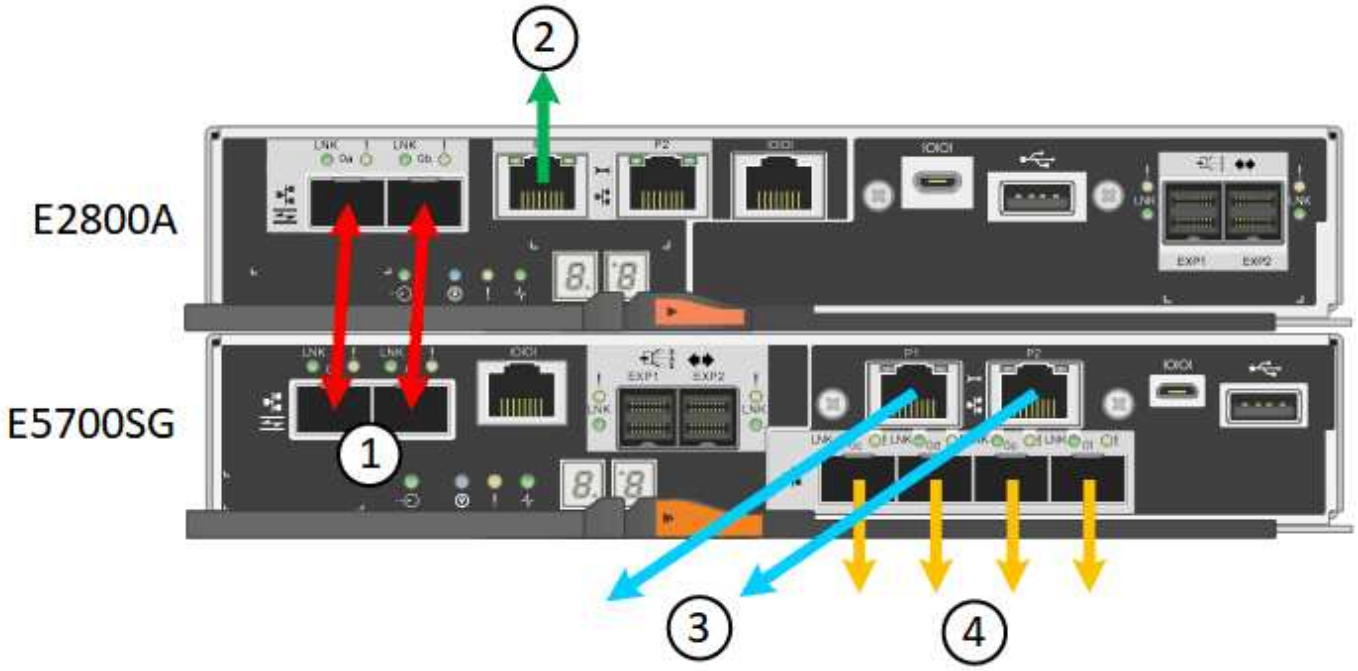
- * 适用于 StorageGRID 的客户端网络： * 客户端网络是一种开放网络，用于访问包括 S3 和 Swift 在内的客户端应用程序。客户端网络可提供对网格的客户端协议访问，从而可以隔离和保护网格网络。客户端网络是可选的。
- * 适用于 SANtricity System Manager* 的管理网络（可选）：通过此网络，您可以访问 E2800 控制器上的 SANtricity System Manager ，从而监控和管理设备中的硬件组件。此管理网络可以与 StorageGRID 的管理网络相同，也可以是一个独立的管理网络。

  如果未连接可选的 SANtricity System Manager 网络，则可能无法使用某些 SANtricity 功能。

有关 StorageGRID 网络的详细信息，请参见 *Grid Primer* 。

StorageGRID 设备连接

安装 StorageGRID 设备时，必须将两个控制器彼此连接并连接到所需的网络。此图显示了 SG5760 中的两个控制器，其中 E2800 控制器位于顶部， E5700SG 控制器位于底部。在 SG5712 中， E2800 控制器位于 E5700SG 控制器的左侧。



	Port	端口类型	功能
1.	每个控制器上两个互连端口	16 GB/s FC 光纤 SFP+	将两个控制器彼此连接。
2.	E2800 控制器上的管理端口 1	1-GbE （ RJ-45 ）	连接到访问 SANtricity System Manager 的网络。您可以使用适用于 StorageGRID 的管理网络或独立的管理网络。

	Port	端口类型	功能
2.	E2800 控制器上的管理端口 2	1-GbE （RJ-45）	为技术支持预留。
3.	E5700SG 控制器上的管理端口 1	1-GbE （RJ-45）	将 E5700SG 控制器连接到 StorageGRID 管理网络。
3.	E5700SG 控制器上的管理端口 2	1-GbE （RJ-45）	• 如果要与管理网络建立冗余连接，则可以与管理端口 1 绑定。 • 可以保持未连接状态，并可用于临时本地访问（IP 169.254.0.1）。 • 在安装期间，如果 DHCP 分配的 IP 地址不可用，则可以使用将 E5700SG 控制器连接到服务笔记本电脑。
4.	E5700SG 控制器上的 10/225-GbE 端口 1-4	10-GbE 或 25-GbE • 注： * 设备附带的 SFP+ 收发器支持 10-GbE 链路速度。如果要对四个网络端口使用 25 GbE 链路速度，则必须提供 SFP28 收发器。	连接到网格网络和 StorageGRID 客户端网络。请参见 " E5700SG 控制器的`10/225-GbE 端口连接 " 。`

相关信息

收集安装信息（SG5700）

缆线设备（SG5700）

E5700SG 控制器端口的端口绑定模式

网络连接准则

安装 VMware

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

E5700SG 控制器端口的端口绑定模式

在为 E5700SG 控制器端口配置网络链路时，您可以对连接到网格网络和可选客户端网络的 10/25/GbE 端口以及连接到可选管理网络的 1-GbE 管理端口使用端口绑定。端口绑定可在 StorageGRID 网络和设备之间提供冗余路径，从而有助于保护数据。

相关信息

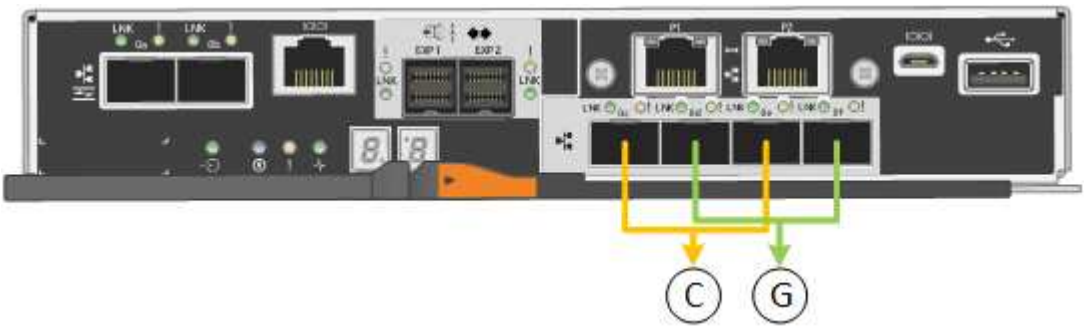
配置网络链路（ SG5700 ）

10/225-GbE 端口的网络绑定模式

E5700SG 控制器上的 10/225-GbE 网络端口支持网格网络和客户端网络连接的固定端口绑定模式或聚合端口绑定模式。

固定端口绑定模式

固定模式是 10/225-GbE 网络端口的默认配置。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

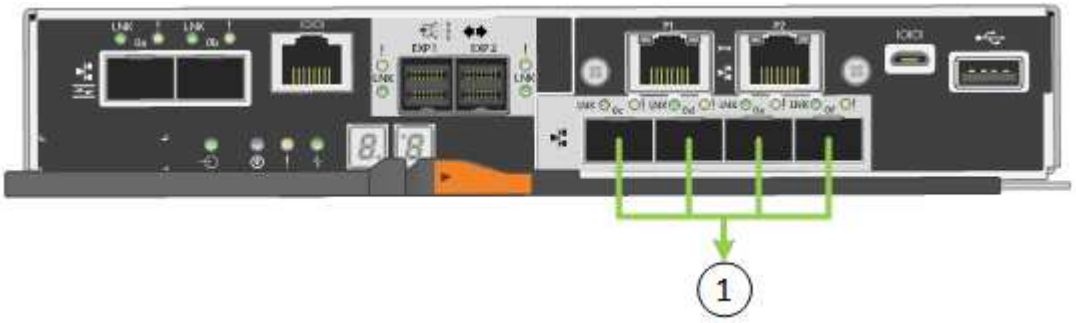
使用固定端口绑定模式时，您可以使用两种网络绑定模式之一：主动备份或链路聚合控制协议（ LACP ）。

- 在主动备份模式（默认）下，一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。端口 4 为端口 2 （网格网络）提供备份路径，端口 3 为端口 1 （客户端网络）提供备份路径。
- 在 LACP 模式下，每对端口在控制器和网络之间形成一个逻辑通道，从而提高吞吐量。如果一个端口发生故障，另一个端口将继续提供通道。吞吐量会降低，但连接不会受到影响。

如果不需要冗余连接，则每个网络只能使用一个端口。但是，请注意，安装 StorageGRID 后，网格管理器中将发出警报，指示已拔下缆线。您可以安全地确认此警报以将其清除。

聚合端口绑定模式

聚合端口绑定模式可显著提高每个 StorageGRID 网络的吞吐量，并提供额外的故障转移路径。



Callout	哪些端口已绑定
1.	所有连接的端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

如果您计划使用聚合端口绑定模式：

- 您必须使用 LACP 网络绑定模式。
- 您必须为每个网络指定唯一的 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。
- 这些端口必须连接到可支持 VLAN 和 LACP 的交换机。如果多个交换机参与 LACP 绑定，则这些交换机必须支持多机箱链路聚合组（ MLAG ）或等效项。
- 您必须了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。

如果您不想使用全部四个 10/225-GbE 端口，则可以使用一个，两个或三个端口。如果使用多个端口，则在一个 10/225-GbE 端口出现故障时，某些网络连接将保持可用的可能性最大。

如果您选择使用的端口少于四个、请注意、在安装设备节点后、可能会在网格管理器中触发*服务设备链路已关闭*警报、指示已拔下电缆。您可以安全地为触发的警报禁用此警报规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。

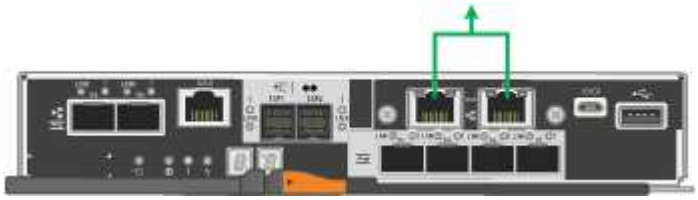
1-GbE 管理端口的网络绑定模式

对于 E5700SG 控制器上的两个 1-GbE 管理端口，您可以选择独立网络绑定模式或主动备份网络绑定模式来连接到可选的管理网络。

在独立模式下，只有管理端口 1 连接到管理网络。此模式不提供冗余路径。管理端口 2 未连接，可用于临时本地连接（使用 IP 地址 169.254.0.1 ）

在主动备份模式下，管理端口 1 和 2 均连接到管理网络。一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。将这两个物理端口绑定到一个逻辑管理端口可提供指向管理网络的冗余路径。

如果在将 1-GbE 管理端口配置为主动备份模式后需要临时本地连接到 E5700SG 控制器，请从两个管理端口拔下缆线，将临时缆线插入管理端口 2 ，然后使用 IP 地址 169.254.0.1 访问此设备。



收集安装信息（ **SG5700** ）

在安装和配置 StorageGRID 设备时，您必须做出决策并收集有关以太网交换机端口， IP 地址以及端口和网络绑定模式的信息。

关于此任务

您可以使用下表记录连接到设备的每个网络的所需信息。安装和配置硬件需要这些值。

连接到 **E2800** 控制器上的 **SANtricity System Manager** 所需的信息

您必须将 E2800 控制器连接到要用于 SANtricity System Manager 的管理网络。

所需信息	您的价值
要连接到管理端口 1 的以太网交换机端口	
管理端口1的MAC地址(印在E2800A控制器端口P1附近的标签上、E2800B控制器端口P1旁边的标签上)	
DHCP 为管理端口 1 分配的 IP 地址（如果在启动后可用） • 注： * 如果要连接到 E2800 控制器的网络包含 DHCP 服务器，则网络管理员可以使用 MAC 地址确定 DHCP 服务器分配的 IP 地址。	
速度和双工模式 • 注： * 您必须确保 SANtricity System Manager 管理网络的以太网交换机设置为自动协商。	必须为： • 自动协商（默认）
IP 地址格式	选择一项： • IPv4 • IPv6

所需信息	您的价值
您计划在管理网络上用于设备的静态 IP 地址	对于 IPv4 ： • IPv4 地址： • 子网掩码： • 网关 对于 IPv6 ： • IPv6 地址： • 可路由的 IP 地址： • E2800 控制器路由器 IP 地址：

将 **E5700SG** 控制器连接到管理网络所需的信息

StorageGRID 管理网络是一个可选网络，用于系统管理和维护。此设备使用 E5700SG 控制器上的 1-GbE 管理端口连接到管理网络。

所需信息	您的价值
已启用管理网络	选择一项： • 否 • 是（默认）
网络绑定模式	选择一项： • 独立 • 主动备份
端口 1 的交换机端口	
端口 2 的交换机端口（仅限主动备份网络绑定模式）	
DHCP 为管理端口 1 分配的 IP 地址（如果在启动后可用） • 注： * 如果管理网络包含 DHCP 服务器，则 E5700SG 控制器会在启动后在其七段显示器上显示 DHCP 分配的 IP 地址。您还可以使用 MAC 地址查找分配的 IP ，从而确定 DHCP 分配的 IP 地址。	• IPv4 地址（ CIDR ）： • 网关

所需信息	您的价值
您计划在管理网络上用于设备存储节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
管理网络子网（ CIDR ）	

在 **E5700SG** 控制器上连接和配置 **10/25/GbE** 端口所需的信息

E5700SG 控制器上的四个 10/225-GbE 端口连接到 StorageGRID 网格网络和客户端网络。

有关这些端口选项的详细信息，请参见 "E5700SG 控制器的 10/225-GbE 端口连接 " 。

所需信息	您的价值
链路速度 • 注： * 如果选择 25 GbE ，则必须安装 SPF28 收发器。不支持自动协商，因此您还必须为 25GbE 配置端口和连接的交换机。	选择一项： • 10 GbE （默认） • 25 GbE
端口绑定模式	选择一项： • FIXED （默认） • 聚合
端口 1 的交换机端口（客户端网络）	
端口 2 的交换机端口（网格网络）	
端口 3 的交换机端口（客户端网络）	
端口 4 的交换机端口（网格网络）	

将 **E5700SG** 控制器连接到网格网络所需的信息

适用于 StorageGRID 的网格网络是一个必需的网络，用于所有内部 StorageGRID 流量。此设备使用 E5700SG 控制器上的 10/225-GbE 端口连接到网格网络。

有关这些端口选项的详细信息，请参见 "E5700SG 控制器的 10/225-GbE 端口连接 " 。

所需信息	您的价值
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为网格网络分配的 IP 地址（如果在启动后可用） • 注： * 如果网格网络包含 DHCP 服务器，则 E5700SG 控制器会在启动后在其七段显示中显示为网格网络分配的 DHCP IP 地址。	• IPv4 地址（ CIDR ）： • 网关
您计划用于网格网络上设备存储节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
网格网络子网（ CIDR ） • 注： * 如果未启用客户端网络，则控制器上的默认路由将使用此处指定的网关。	

将 **E5700SG** 控制器连接到客户端网络所需的信息

适用于 StorageGRID 的客户端网络是一个可选网络，通常用于提供对网格的客户端协议访问。设备使用 E5700SG 控制器上的 10/225-GbE 端口连接到客户端网络。

有关这些端口选项的详细信息，请参见 "E5700SG 控制器的 10/225-GbE 端口连接 " 。

所需信息	您的价值
已启用客户端网络	选择一项： • 否（默认） • 是的。

所需信息	您的价值
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记 （如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为客户端网络分配的 IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划在客户端网络上用于设备存储节点的静态 IP 地址 • 注： * 如果启用了客户端网络，则控制器上的默认路由将使用此处指定的网关。	• IPv4 地址（ CIDR ）： • 网关

相关信息

查看设备网络连接（ SG5700 ）

E5700SG 控制器端口的端口绑定模式

配置硬件（ SG5700 ）

安装硬件（ SG5700 ）

硬件安装需要将设备安装到机柜或机架中，连接缆线并接通电源。

注册硬件

注册设备硬件具有支持优势。

步骤

1. 找到机箱序列号。

   您可以在装箱单上，确认电子邮件中或打开设备包装后在设备上找到此编号。

2. 访问 NetApp 支持站点，网址为 "mysupport.netapp.com"。
3. 确定是否需要注册硬件：

如果您是 ...	请按照以下步骤操作 ...
现有 NetApp 客户	a. 使用您的用户名和密码登录。 b. 选择 * 产品 * > * 我的产品 * 。 c. 确认新序列号已列出。 d. 如果不是，请按照适用于新 NetApp 客户的说明进行操作。
NetApp 新客户	a. 单击 * 立即注册 * ，然后创建帐户。 b. 选择 * 产品 * > * 注册产品 * 。 c. 输入产品序列号和请求的详细信息。 注册获得批准后，您可以下载所需的任何软件。审批过程可能需要长达 24 小时。

在机柜或机架中安装设备（ **SG5700** ）

您必须在机柜或机架中安装导轨，然后将设备滑入导轨。如果您使用的是 SG5760 ，则还必须在安装设备后安装驱动器。

您需要的内容

- 您已查看包装盒中的安全通知文档，并了解移动和安装硬件的预防措施。
- 导轨套件随附了相关说明。
- 您已获得此设备的 *Installation and Setup Instructions*。

从机架，机柜或机架的底部安装硬件，以防止设备发生倾翻。

在装满驱动器后， SG5712 的重约为 64 磅（ 29 千克）。要安全移动 SG5712 ，需要两个人或一台机械升降机。

SG5760 重约 132 磅（ 60 千克），未安装驱动器。要安全移动空 SG5760 ，需要四个人或一台机械升降机。

为避免损坏硬件，如果安装了驱动器，请勿移动 SG5760 。移动磁盘架之前，必须先卸下所有驱动器。

步骤

1. 请仔细按照导轨套件的说明在机柜或机架中安装导轨。
2. 如果您使用的是 SG5760 ，请按照以下步骤准备移动设备。

a. 拆下外包装箱。然后，向下折叠内箱上的挡板。

b. 如果您要用手提起 SG5760 ，请将四个手柄连接到机箱两侧。

将设备滑入导轨时，请取下这些手柄。

3. 请参见 *Installation and Setup Instructions*、 并将设备滑入机柜或机架中。
4. 请参见 *Installation and Setup Instructions*、 并将设备固定到机柜或机架上。

如果您使用的是 SG5760 ，请使用后支架将设备固定到机架或机柜的背面。如果机架或机柜有方形孔，请使用固定框架螺母。

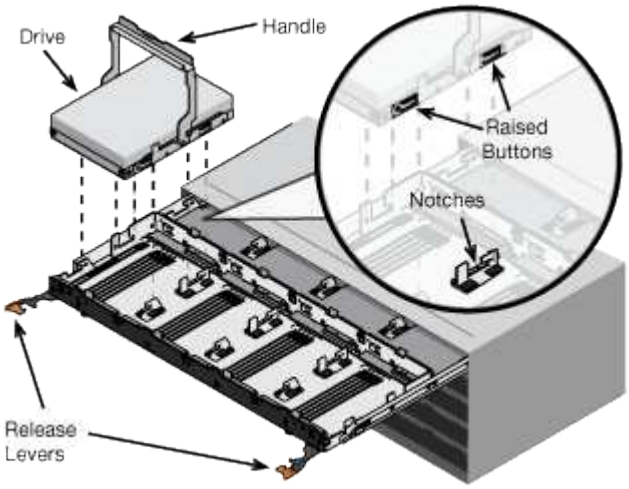
5. 如果您使用的是 SG5760 ，请在 5 个驱动器抽盒中的每个抽盒中安装 12 个驱动器。

您必须安装全部 60 个驱动器，以确保正常运行。

a. 戴上 ESD 腕带，然后将驱动器从其包装中取出。

b. 释放顶部驱动器抽盒上的拉杆，然后使用拉杆将抽盒滑出。

c. 将驱动器把手提起至垂直位置，并将驱动器上的按钮与抽盒上的缺口对齐。



d. 轻按驱动器顶部，向下旋转驱动器把手，直到驱动器卡入到位。

e. 安装前 12 个驱动器后，通过推动中间并轻轻合上两个拉杆，将抽盒滑回原位。

f. 对其他四个抽盒重复上述步骤。

6. 连接前挡板。

缆线设备**(SG5700**系列**)**

您必须将两个控制器彼此连接，连接每个控制器上的管理端口，并将 E5700SG 控制器上的 10/25/GbE 端口连接到网格网络和适用于 StorageGRID 的可选客户端网络。

您需要的内容

- 您已解压缩设备附带的以下物品：
  - 两根电源线。

- 两根光缆用于控制器上的 FC 互连端口。
- 八个 SFP+ 收发器，支持 10-GbE 或 16-Gbps FC 。如果您希望网络端口使用 10-GbE 链路速度，则可以将收发器与两个控制器上的两个互连端口以及 E5700SG 控制器上的四个 10/25GbE 网络端口结合使用。

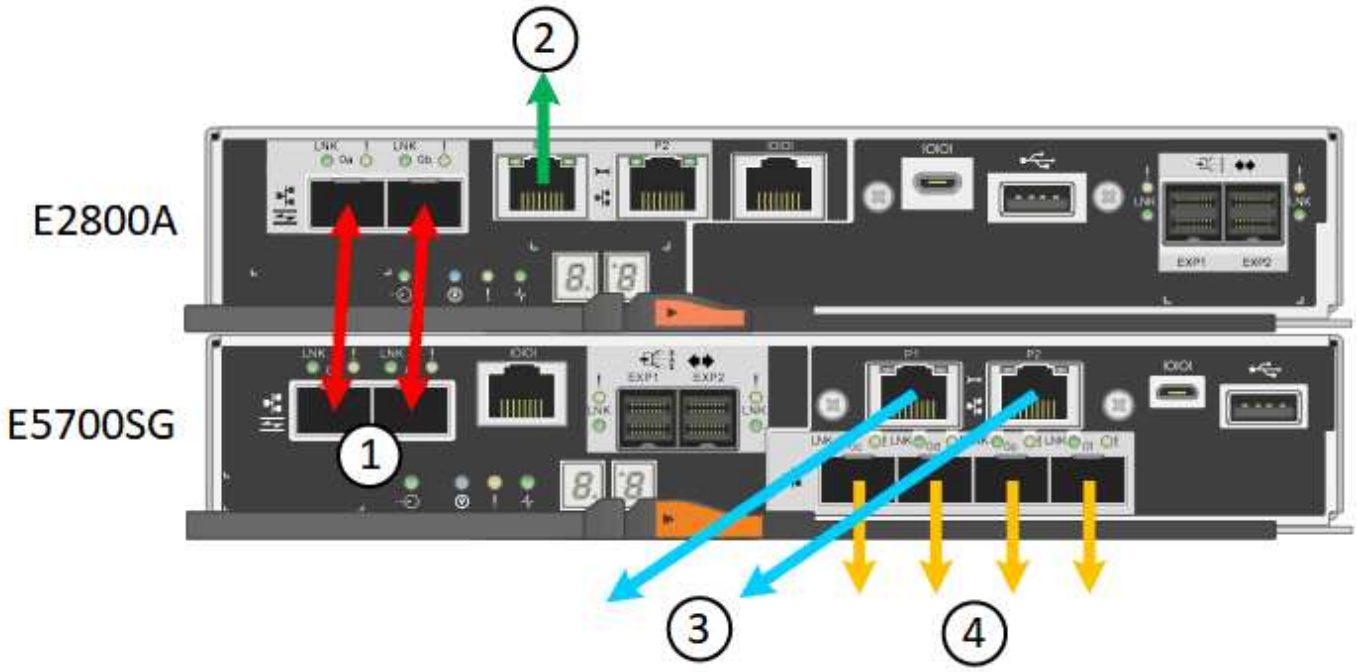
- 您已获取以下项目，但这些项目不包含在设备中：
  - 一到四根光缆，用于您计划使用的 10/225-GbE 端口。
  - 如果您计划使用 25 GbE 链路速度，则需要一到四个 SFP28 收发器。
  - 用于连接管理端口的以太网缆线。

* 受到激光辐射的风险 * —请勿拆卸或卸下 SFP 收发器的任何部件。您可能受到激光辐射的影响。

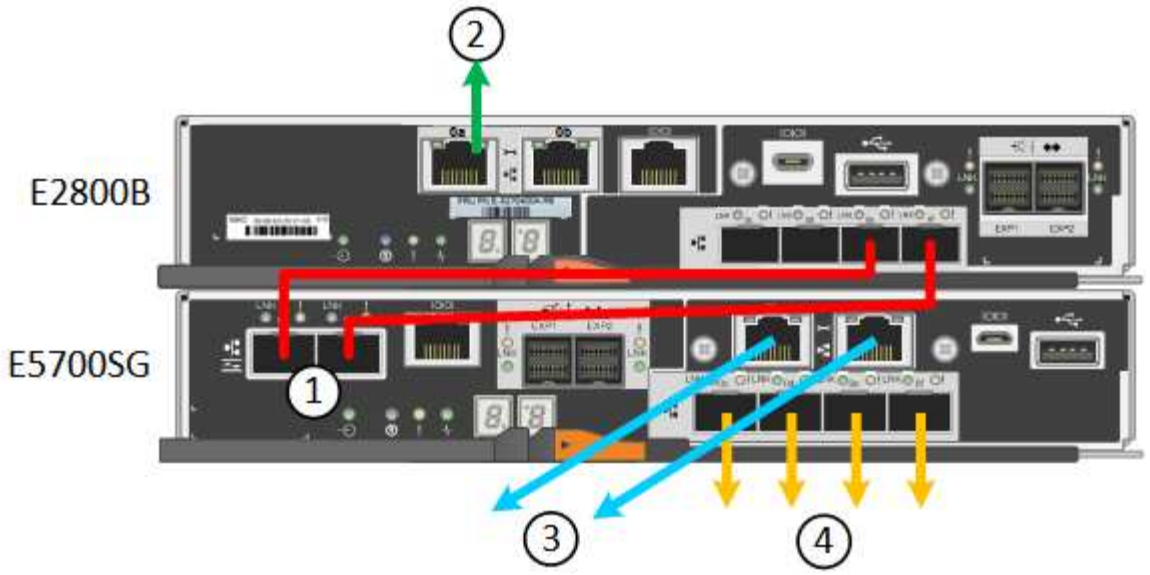
关于此任务

图中显示了SG5760和SG5760X中的两个控制器、其中顶部是E2800系列存储控制器、底部是E5700SG控制器。在SG5712和SG5712X中、从背面看、E2800系列存储控制器位于E5700SG控制器的左侧。

- SG5760连接*



- SG5760X连接*



	Port	端口类型	功能
1.	每个控制器上两个互连端口	16 GB/s FC 光纤 SFP+	将两个控制器彼此连接。
2.	E2800系列控制器上的管理端口1	1-GbE （RJ-45）	连接到访问 SANtricity System Manager 的网络。您可以使用适用于 StorageGRID 的管理网络或独立的管理网络。
2.	E2800系列控制器上的管理端口2	1-GbE （RJ-45）	为技术支持预留。
3.	E5700SG 控制器上的管理端口 1	1-GbE （RJ-45）	将 E5700SG 控制器连接到 StorageGRID 管理网络。
3.	E5700SG 控制器上的管理端口 2	1-GbE （RJ-45）	• 如果要与管理网络建立冗余连接，则可以与管理端口 1 绑定。 • 可以保持未连接状态，并可用于临时本地访问（IP 169.254.0.1）。 • 在安装期间，如果 DHCP 分配的 IP 地址不可用，则可以使用将 E5700SG 控制器连接到服务笔记本电脑。

	Port	端口类型	功能
4.	E5700SG 控制器上的 10/225-GbE 端口 1-4	10-GbE 或 25-GbE • 注： * 设备附带的 SFP+ 收发器支持 10-GbE 链路速度。如果要对四个网络端口使用 25 GbE 链路速度，则必须提供 SFP28 收发器。	连接到网格网络和 StorageGRID 客户端网络。请参见 " E5700SG 控制器的`10/225-GbE 端口连接 " 。`

步骤

1. 使用两根光缆和八个 SFP+ 收发器中的四根光缆将 E2800 控制器连接到 E5700SG 控制器。

连接此端口 ...	到此端口 ...
E2800 控制器上的互连端口 1	E5700SG 控制器上的互连端口 1
E2800 控制器上的互连端口 2	E5700SG 控制器上的互连端口 2

2. 如果您计划使用SANtricity System Manager、请使用以太网缆线将E2800控制器上的管理端口1 (E2800A上的P1和E2800B上的0A)(左侧的RJ-45端口)连接到SANtricity System Manager的管理网络。

   请勿使用E2800控制器上的管理端口2 (E2800A上的P2和E2800B上的0b)(右侧的RJ-45端口)。此端口是为技术支持预留的。

3. 如果您计划使用 StorageGRID 管理网络，请使用以太网缆线将 E5700SG 控制器上的管理端口 1 （左侧的 RJ-45 端口）连接到管理网络。

   如果您计划对管理网络使用主动备份网络绑定模式，请使用以太网缆线将 E5700SG 控制器上的管理端口 2 （右侧的 RJ-45 端口）连接到管理网络。

4. 使用光缆和 SFP+ 或 SFP28 收发器将 E5700SG 控制器上的 10/225-GbE 端口连接到相应的网络交换机。

   所有端口都必须使用相同的链路速度。如果您计划使用 10-GbE 链路速度，请安装 SFP+ 收发器。如果您计划使用 25 GbE 链路速度，请安装 SFP28 收发器。

   ◦ 如果您计划使用固定端口绑定模式（默认），请将端口连接到 StorageGRID 网格和客户端网络，如表所示。

Port	连接到 ...
端口 1	客户端网络（可选）
端口 2	网格网络
端口 3	客户端网络（可选）

Port	连接到 ...
端口 4	网格网络

- 如果您计划使用聚合端口绑定模式，请将一个或多个网络端口连接到一个或多个交换机。您应至少连接四个端口中的两个，以避免发生单点故障。如果在一个 LACP 绑定中使用多个交换机，则这些交换机必须支持 MLAG 或等效项。

相关信息

访问 StorageGRID 设备安装程序

E5700SG 控制器端口的端口绑定模式

连接电源线并接通电源（ **SG5700** ）

为设备通电后，两个控制器都会启动。

您需要的内容

在连接电源之前，两个设备电源开关都必须关闭。

* 电击风险 * —在连接电源线之前，请确保设备上的两个电源开关均已关闭。

步骤

1. 确认设备上的两个电源开关均已关闭。
2. 将两根电源线连接到设备。
3. 将两条电源线连接到机柜或机架中的不同配电单元（ PDU ）。
4. 打开设备上的两个电源开关。
   - 请勿在启动过程中关闭电源开关。
   - 首次启动时，风扇声音很大。启动期间发出较大的噪音是正常的。
5. 启动控制器后，检查其七段显示内容。

查看 **SG5700** 启动状态代码

设备启动时，每个控制器上的七段显示状态和错误代码。

关于此任务

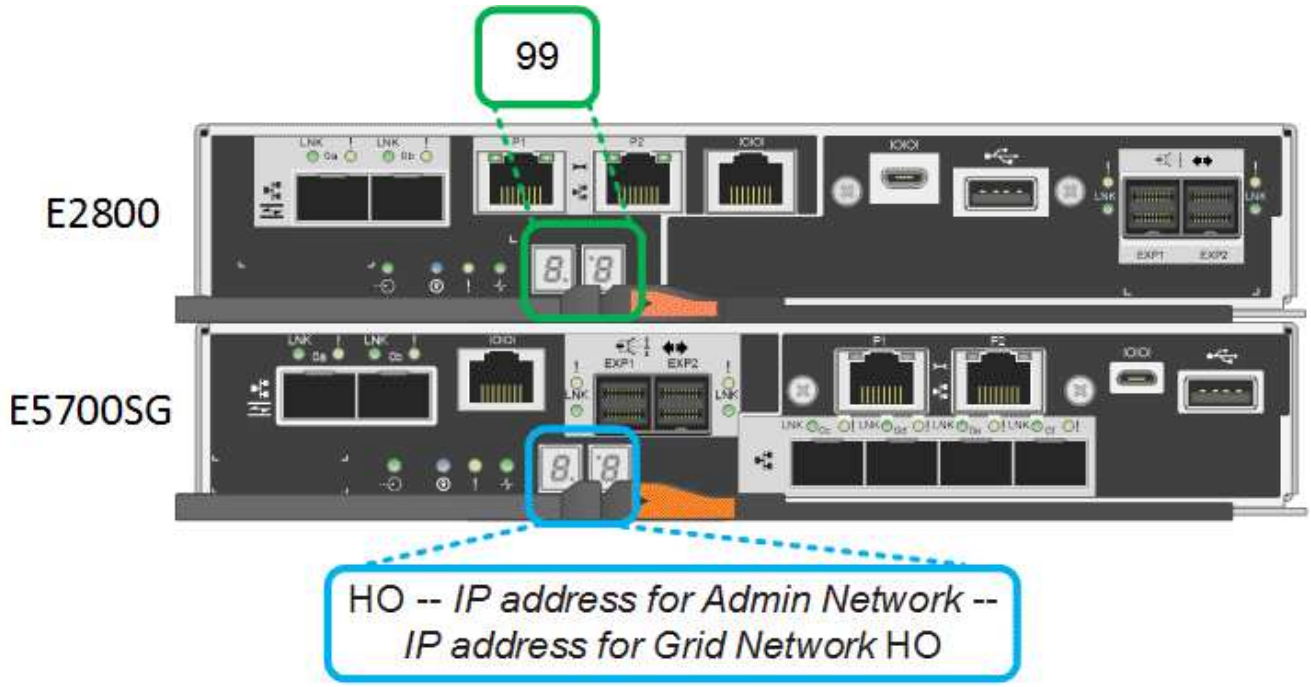
E2800 控制器和 E5700SG 控制器显示不同的状态和错误代码。

要了解这些代码的含义，请参见以下资源：

控制器	参考
E2800 控制器	_E5700 和 E2800 系统监控指南 _ • 注： * 为 E 系列 E5700 控制器列出的代码不适用于设备中的 E5700SG 控制器。
E5700SG 控制器	" s5700SG 控制器上的状态指示符 "

步骤

1. 在启动期间，通过查看七段显示器上显示的代码来监控进度。
   - E2800 控制器上的七段显示会显示重复序列 * 操作系统 * ， * 可持续发展 * ， ` * 空白 _*` ，以指示它正在执行每日开始处理。
   - E5700SG 控制器上的七段显示屏显示一系列代码，以 * AA* 和 * FF* 结尾。
2. 控制器启动后，确认七段显示内容如下：



控制器	七段式显示
E2800 控制器	显示 99 ，这是 E 系列控制器架的默认 ID 。

控制器	七段式显示
E5700SG 控制器	显示了 * 何 * ，后跟两个数字的重复序列。 `HO -- IP address for Admin Network -- IP address for Grid Network HO` 在此序列中，第一组数字是为控制器的管理端口 1 分配的 DHCP IP 地址。此地址用于将控制器连接到 StorageGRID 的管理网络。第二组数字是 DHCP 分配的 IP 地址，用于将设备连接到用于 StorageGRID 的网格网络。 • 注： * 如果无法使用 DHCP 分配 IP 地址，则会显示 0.0.0.0 。

3. 如果显示的七段显示其他值，请参见 硬件安装故障排除（ SG5700 ） 并确认您已正确完成安装步骤。如果无法解决此问题，请联系技术支持。

相关信息

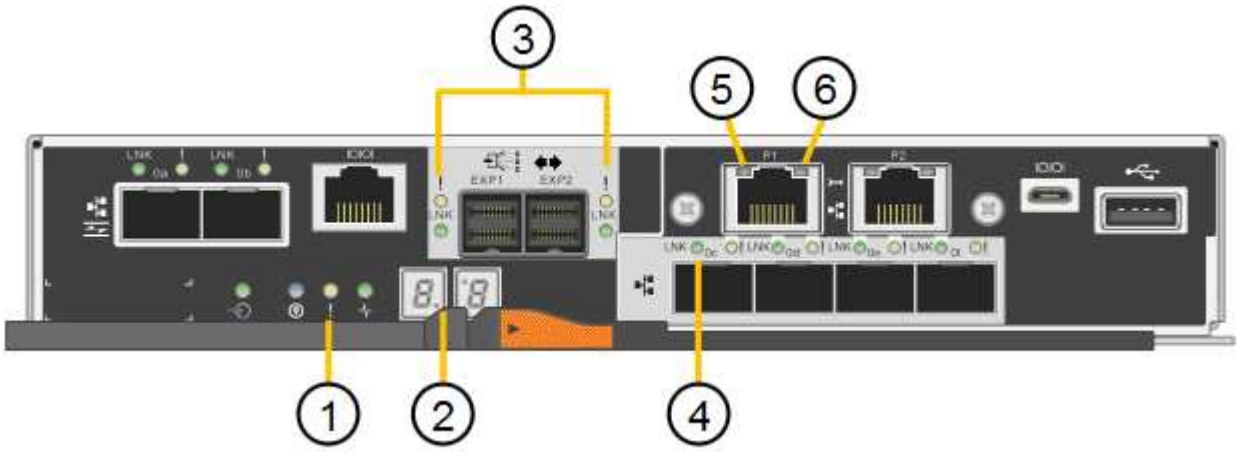
E5700SG 控制器上的状态指示灯

"《 E5700 和 E2800 系统监控指南》"

E5700SG 控制器上的状态指示灯

在设备启动和硬件初始化期间， E5700SG 控制器上的七段显示屏和 LED 会显示状态和错误代码。您可以使用这些显示来确定状态并对错误进行故障排除。

启动 StorageGRID 设备安装程序后，您应定期查看 E5700SG 控制器上的状态指示灯。



	显示	Description
1.	警示 LED	琥珀色：控制器出现故障，需要操作员注意，或者未找到安装脚本。 off ： 控制器运行正常。
2.	七段式显示	显示诊断代码 通过七段显示序列，您可以了解设备的错误和运行状态。
3.	扩展端口警示 LED	琥珀色：这些 LED 始终为琥珀色（未建立链路），因为设备不使用扩展端口。
4.	主机端口链路状态 LED	绿色：链路已启动。 off ： 链路已关闭。
5.	以太网链路状态 LED	绿色：已建立链路。 off ： 未建立任何链路。
6.	以太网活动 LED	绿色：管理端口与其连接的设备（例如以太网交换机）之间的链路已启动。 off ： 控制器与连接的设备之间没有链路。 呈绿色闪烁：存在以太网活动。

常规启动代码

在启动期间或设备硬重置后，将发生以下情况：

1. E5700SG 控制器上的七段显示显示了一个常规代码序列，这些代码不是特定于控制器的。常规序列以代码 AA 和 FF 结尾。
2. 此时将显示特定于 E5700SG 控制器的启动代码。

E5700SG 控制器启动代码

在设备正常启动期间， E5700SG 控制器上的七段显示屏将按所列顺序显示以下代码：

代码	表示
您好	主启动脚本已启动。

代码	表示
p	系统正在检查是否需要更新 FPGA 。
HP	系统正在检查 10/225-GbE 控制器固件是否需要更新。
RB	应用固件更新后，系统正在重新启动。
FP	硬件子系统固件更新检查已完成。控制器间通信服务正在启动。
他	系统正在等待与 E2800 控制器建立连接并与 SANtricity 操作系统同步。 • 注： * 如果此启动操作步骤 在此阶段未进行，请检查两个控制器之间的连接。
HC	系统正在检查现有 StorageGRID 安装数据。
好的	StorageGRID 设备安装程序正在运行。
HA	StorageGRID 正在运行。

E5700SG 控制器错误代码

这些代码表示设备启动时 E5700SG 控制器上可能显示的错误情况。如果发生特定的低级硬件错误，则会显示其他两位十六进制代码。如果其中任何一个代码持续一两秒以上，或者您无法通过执行规定的故障排除过程之一来解决此错误，请联系技术支持。

代码	表示
22.	在任何启动设备上均未找到主启动记录。
23	内部闪存磁盘未连接。
2A ， 2B	总线卡滞，无法读取 DIMM SPD 数据。
40	DIMM 无效。
41.	DIMM 无效。
42	内存测试失败。
51	SPD 读取失败。

代码	表示
92 到 96	PCI 总线初始化。
A0 到 A3	SATA 驱动器初始化。
AB	备用启动代码。
AE	正在启动操作系统。
EA	DDR4 训练失败。
E8.	未安装内存。
欧盟	未找到安装脚本。
EP	安装 E2800 控制器或与 E2800 控制器通信失败。

相关信息

硬件安装故障排除（ SG5700 ）

"NetApp 支持"

配置硬件（ **SG5700** ）

为设备接通电源后，您必须配置 SANtricity 系统管理器，该软件将用于监控硬件。您还必须配置 StorageGRID 要使用的网络连接。

配置 **StorageGRID** 连接（ **SG5700** ）

在将 StorageGRID 设备部署为 StorageGRID 网格中的存储节点之前，必须先配置设备与计划使用的网络之间的连接。您可以通过浏览到 StorageGRID 设备安装程序来配置网络连接，该安装程序包含在 E5700SG 控制器（设备中的计算控制器）上。

步骤

- 访问 StorageGRID 设备安装程序
- 验证并升级 StorageGRID 设备安装程序版本
- 配置网络链路（ SG5700 ）
- 设置 IP 配置
- 验证网络连接
- 验证端口级别的网络连接

您必须访问 StorageGRID 设备安装程序来配置设备与三个 StorageGRID 网络之间的连接：网格网络，管理网络（可选）和客户端网络（可选）。

您需要的内容

- 您正在使用 支持的 Web 浏览器。
- 此设备已连接到您计划使用的所有 StorageGRID 网络。
- 您知道这些网络上设备的 IP 地址，网关和子网。
- 您已配置计划使用的网络交换机。

关于此任务

首次访问 StorageGRID 设备安装程序时，您可以使用管理网络的 DHCP 分配的 IP 地址（假设设备已连接到管理网络）或网格网络的 DHCP 分配的 IP 地址。首选使用管理网络的 IP 地址。否则，如果使用网格网络的 DHCP 地址访问 StorageGRID 设备安装程序，则在更改链接设置和输入静态 IP 时，可能会与 StorageGRID 设备安装程序断开连接。

步骤

1. 在管理网络（如果已连接）或网格网络（如果未连接管理网络）上获取设备的 DHCP 地址。

   您可以执行以下任一操作：

   - 查看 E5700SG 控制器上的七段显示器。如果 E5700SG 控制器上的管理端口 1 和 10/25GbE 端口 2 和 4 连接到使用 DHCP 服务器的网络，则控制器会在打开机箱电源时尝试获取动态分配的 IP 地址。控制器完成启动过程后，其七段显示屏将显示 * HO* ，然后是两个数字的重复序列。

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     顺序：

     - 第一组数字是管理网络上设备存储节点的 DHCP 地址（如果已连接）。此 IP 地址将分配给 E5700SG 控制器上的管理端口 1 。
     - 第二组数字是网格网络上设备存储节点的 DHCP 地址。首次为设备接通电源时，此 IP 地址将分配给 10/225-GbE 端口 2 和 4 。

       如果无法使用 DHCP 分配 IP 地址，则会显示 0.0.0.0 。

   - 将管理端口 1 的 MAC 地址提供给网络管理员，以便他们可以在管理网络上查找此端口的 DHCP 地址。MAC 地址印在 E5700SG 控制器上端口旁边的标签上。

2. 如果您能够获取任一 DHCP 地址：

   a. 在服务笔记本电脑上打开 Web 浏览器。

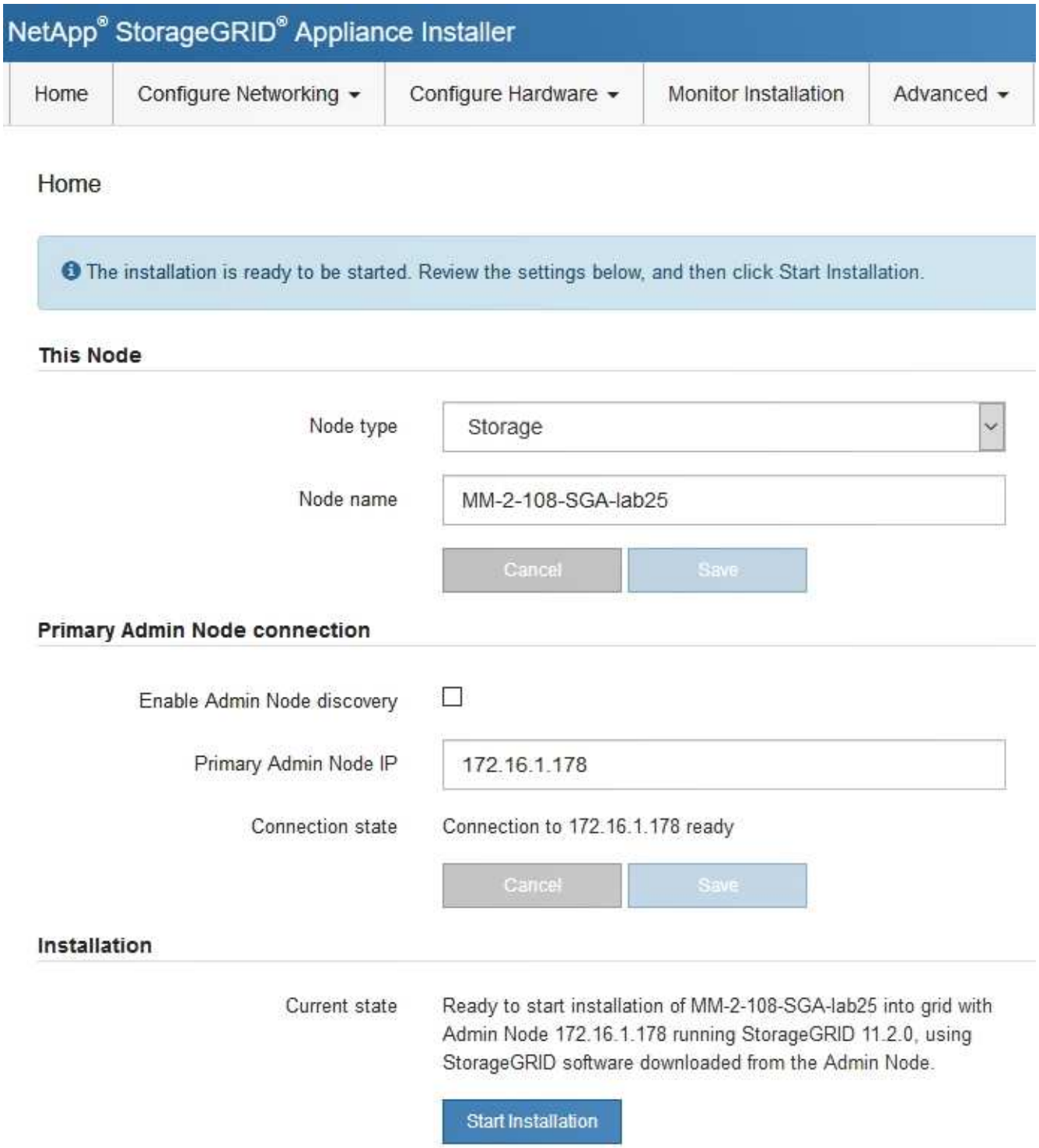
   b. 输入 StorageGRID 设备安装程序的 URL： + ` * https://*E5700SG_Controller_IP*:8443*`

      对于 ` *E5700SG_Controller_IP*` ，请使用控制器的 DHCP 地址（如果有，请使用管理网络的 IP 地址）。

c. 如果系统提示您显示安全警报，请使用浏览器的安装向导查看并安装证书。

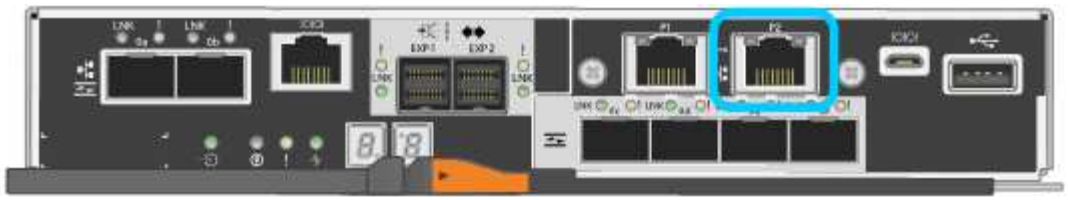
下次访问此 URL 时，不会显示此警报。

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。



3. 如果 E5700SG 控制器无法使用 DHCP 获取 IP 地址：

a. 使用以太网缆线将服务笔记本电脑连接到 E5700SG 控制器上的管理端口 2 。



b. 在服务笔记本电脑上打开 Web 浏览器。

c. 输入 StorageGRID 设备安装程序的 URL： + ` * https://169.254.0.1:8443*`

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前的连接方式。

如果无法通过链路本地连接访问主页，请将服务笔记本电脑 IP 地址配置为 `169.254.0.2` ，然后重试。

4. 查看主页页面上显示的所有消息，并根据需要配置链路配置和 IP 配置。

相关信息

Web 浏览器要求

验证并升级 **StorageGRID** 设备安装程序版本

设备上的 StorageGRID 设备安装程序版本必须与 StorageGRID 系统上安装的软件版本匹配，以确保所有 StorageGRID 功能均受支持。

您需要的内容

您已访问 StorageGRID 设备安装程序。

关于此任务

StorageGRID 设备出厂时预安装了 StorageGRID 设备安装程序。如果要将设备添加到最近升级的 StorageGRID 系统，则可能需要先手动升级 StorageGRID 设备安装程序，然后再将设备安装为新节点。

升级到新的 StorageGRID 版本时， StorageGRID 设备安装程序会自动升级。您无需升级已安装设备节点上的 StorageGRID 设备安装程序。只有在安装包含早期版本的 StorageGRID 设备安装程序的设备时，才需要此操作步骤 。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 升级固件 * 。
2. 将当前固件版本与 StorageGRID 系统上安装的软件版本进行比较。（从网格管理器的顶部，选择帮助图标并选择 * 关于 * 。）

   两个版本中的第二位数字应匹配。例如，如果您的 StorageGRID 系统运行的是 11.* 6* 。 *x.y* ，则 StorageGRID 设备安装程序版本应为 3.* 6* 。 *z* 。

3. 如果设备安装了StorageGRID 设备安装程序的低级版本、请转到 "NetApp下载：StorageGRID 设备"。

   使用您的 NetApp 帐户的用户名和密码登录。

4. 下载适当版本的 * StorageGRID Appliances * 支持文件以及相应的校验和文件。

StorageGRID 设备的支持文件是一个 ` .zip` 归档文件，其中包含所有 StorageGRID 设备型号的当前和先前固件版本，位于每种控制器类型的子目录中。

下载 StorageGRID 设备的支持文件后，解压缩 ` .zip` 归档并查看 README 文件，以了解有关安装 StorageGRID 设备安装程序的重要信息。

5. 按照 StorageGRID 设备安装程序的 " 升级固件 " 页面上的说明执行以下步骤：
   a. 上传适用于您的控制器类型的相应支持文件（固件映像）和校验和文件。
   b. 升级非活动分区。
   c. 重新启动和交换分区。
   d. 升级第二个（非活动）分区。

相关信息

访问 StorageGRID 设备安装程序

配置网络链路（ **SG5700** ）

您可以为用于将设备连接到网格网络，客户端网络和管理网络的端口配置网络链路。您可以设置链路速度以及端口和网络绑定模式。

您需要的内容

如果您计划对 10/25/GbE 端口使用 25-GbE 链路速度：

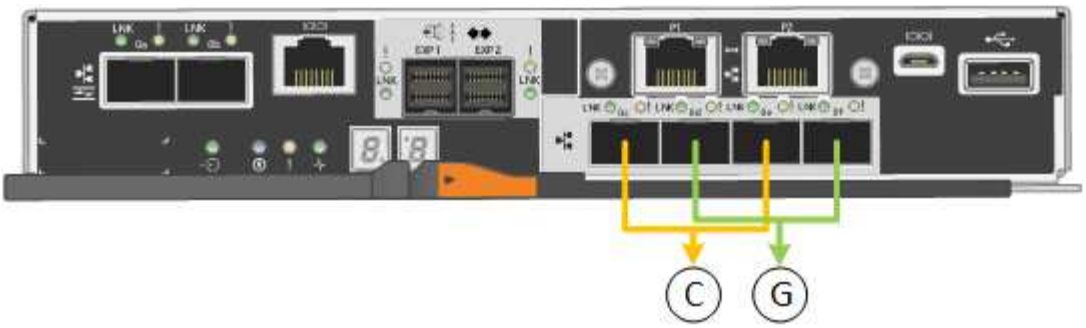
- 您已在计划使用的端口中安装 SFP28 收发器。
- 您已将端口连接到可支持这些功能的交换机。
- 您了解如何配置交换机以使用此较高的速度。

如果您计划对 10/225-GbE 端口使用聚合端口绑定模式， LACP 网络绑定模式或 VLAN 标记：

- 您已将设备上的端口连接到可支持 VLAN 和 LACP 的交换机。
- 如果多个交换机参与 LACP 绑定，则这些交换机支持多机箱链路聚合组（ MLAG ）或等效项。
- 您了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。
- 您知道要用于每个网络的唯一 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。
- 如果您计划对管理网络使用主动备份模式，则已将以太网缆线连接到控制器上的两个管理端口。

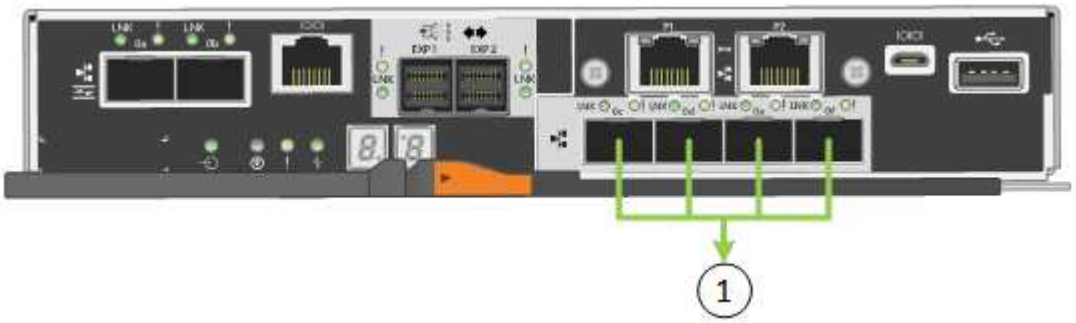
关于此任务

此图显示了在固定端口绑定模式（默认配置）下四个 10/225-GbE 端口的绑定方式。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

此图显示了四个 10/25GbE 端口在聚合端口绑定模式下的绑定方式。



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表总结了用于配置四个 10/225-GbE 端口的选项。默认设置以粗体显示。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

- * 固定（默认）端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 端口 1 和 3 对客户端网络使用主动备份绑定。 • 可以为两个网络指定VLAN标记。

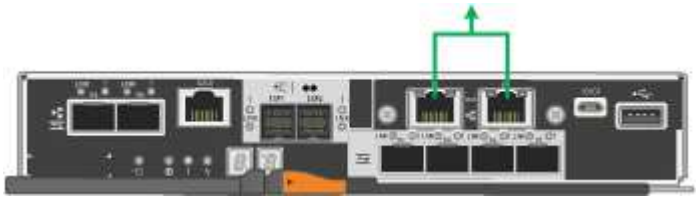
网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
LACP （ 802.3ad ）	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 端口 1 和 3 对客户端网络使用 LACP 绑定。 • 可以为两个网络指定VLAN标记。

- * 聚合端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （ 802.3ad ）	• 端口 1-4 对网格网络使用一个 LACP 绑定。 • 一个 VLAN 标记用于标识网格网络数据包。	• 端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。 • 通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

有关端口绑定和网络绑定模式的详细信息，请参见 E5700SG 控制器的 10/225-GbE 端口连接信息。

此图显示了 E5700SG 控制器上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。

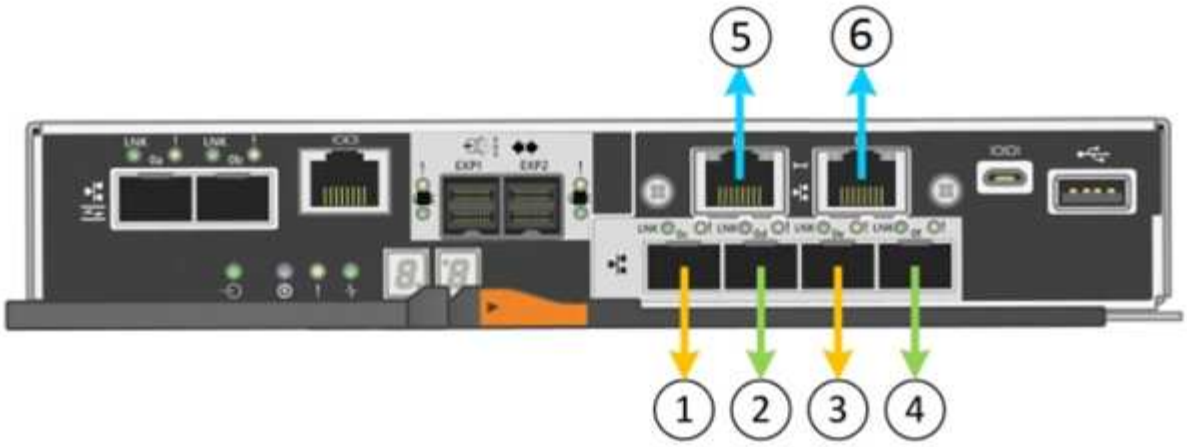


步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * 链接配置 * 。

   " 网络链路配置 " 页面显示设备示意图，其中包含编号为的网络和管理端口。

Network Link Configuration



⚠ You might lose your connection if you make changes to the network or link you are connected through. If you are not reconnected within 1 minute, re-enter the URL using one of the other IP addresses assigned to the appliance.

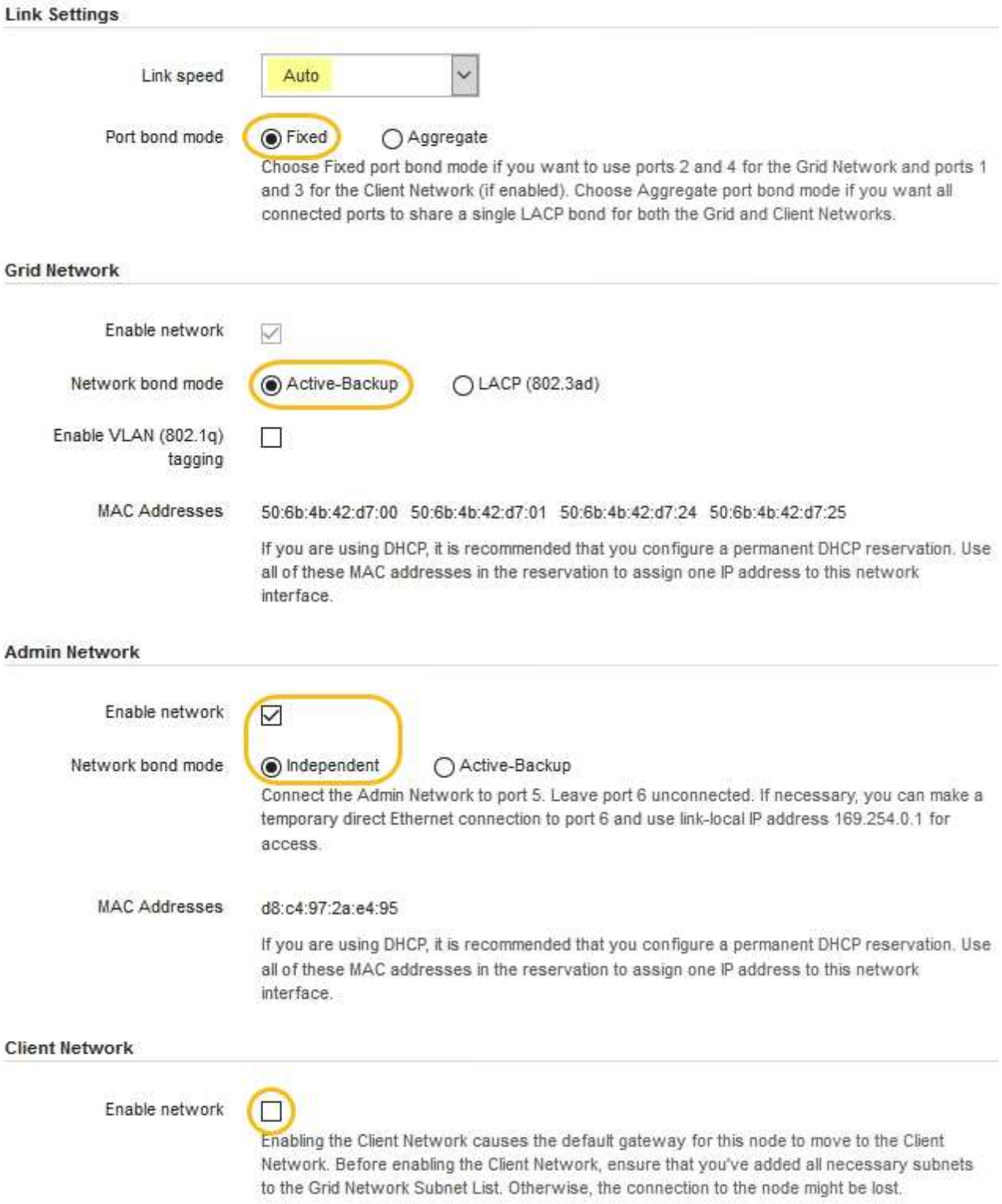
链路状态表列出了已编号端口的链路状态（启动 / 关闭）和速度（ 1/25/40/100 Gbps ）。

Link Status

Link	State	Speed (Gbps)
1	Up	25
2	Up	25
3	Up	25
4	Up	25
5	Up	1
6	Up	1

首次访问此页面时：

- * 链路速度 * 设置为 * 10GbE 。
- * 端口绑定模式 * 设置为 * 固定 * 。
- 网格网络的 * 网络绑定模式 * 设置为 * 主动备份 * 。
- 此时将启用 * 管理网络 * ，并将网络绑定模式设置为 * 独立 * 。
- 已禁用 * 客户端网络 * 。



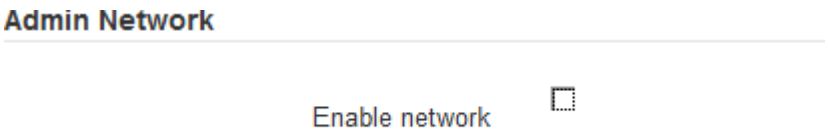
2. 如果您计划对 10/25 GbE 端口使用 25-GbE 链路速度，请从链路速度下拉列表中选择 * 25GbE* 。

   您用于网格网络和客户端网络的网络交换机也必须支持此速度并为此速度进行配置。SFP28 收发器必须安装在端口中。

3. 启用或禁用计划使用的 StorageGRID 网络。

   网格网络为必填项。您不能禁用此网络。

a. 如果设备未连接到管理网络，请取消选中管理网络的 * 启用网络 * 复选框。



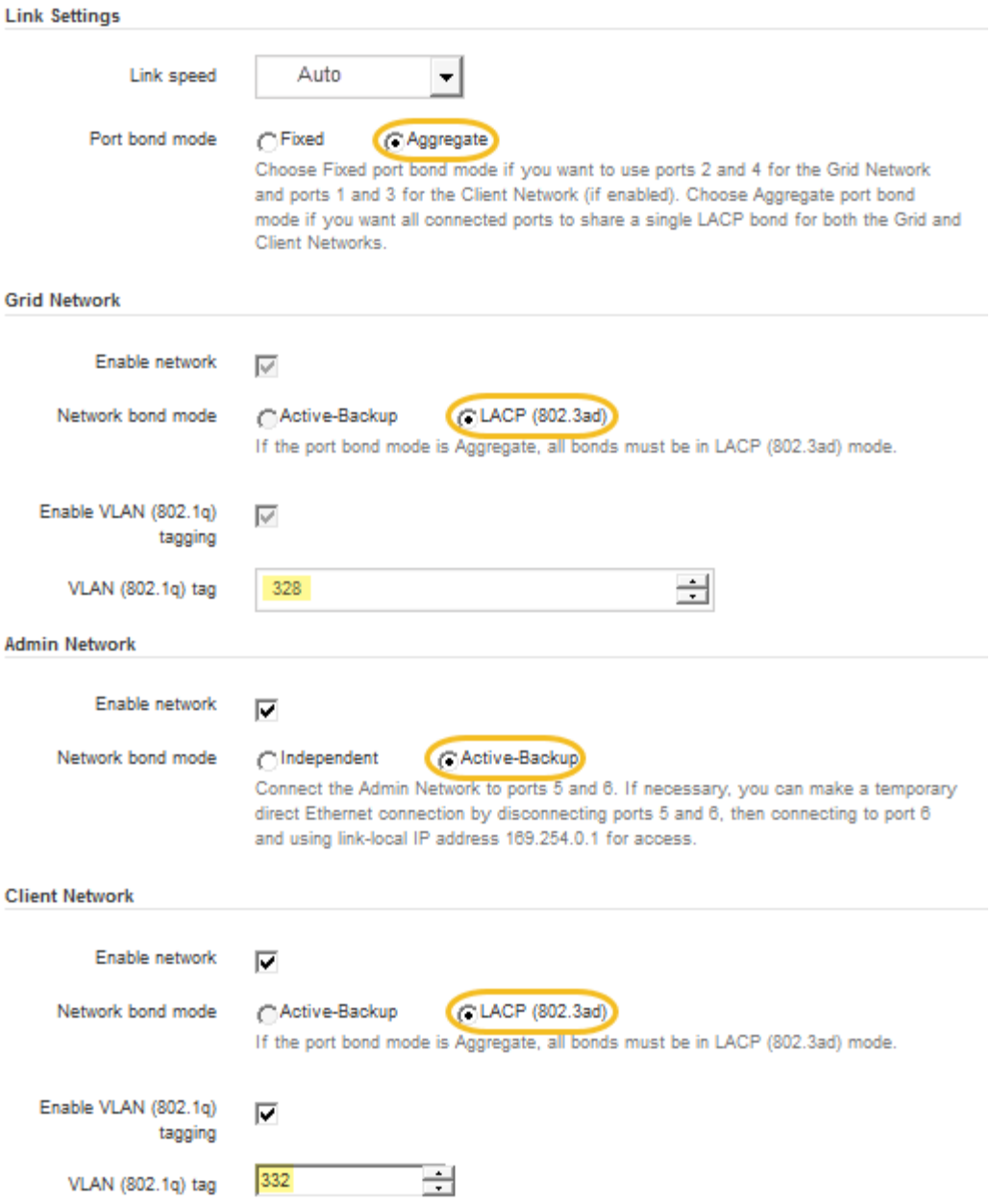
b. 如果设备已连接到客户端网络，请选中客户端网络的 * 启用网络 * 复选框。

现在，将显示 10/225-GbE 端口的客户端网络设置。

4. 请参见表，并配置端口绑定模式和网络绑定模式。

示例显示：

- 为网格和客户端网络选择了 * 聚合 * 和 * LACP * 。您必须为每个网络指定唯一的 VLAN 标记。您可以选择 0 到 4095 之间的值。
- 已为管理网络选择 * 主动备份 * 。



5. 对所做的选择感到满意后，单击 * 保存 * 。

> 如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*E5700SG_Controller_IP*:8443*`

相关信息

E5700SG 控制器端口的端口绑定模式

设置 **IP** 配置

您可以使用 StorageGRID 设备安装程序在 StorageGRID 网格，管理和客户端网络上配置设备存储节点所使用的 IP 地址和路由信息。

关于此任务

您必须为每个已连接网络上的设备分配一个静态 IP ，或者为 DHCP 服务器上的地址分配一个永久租约。

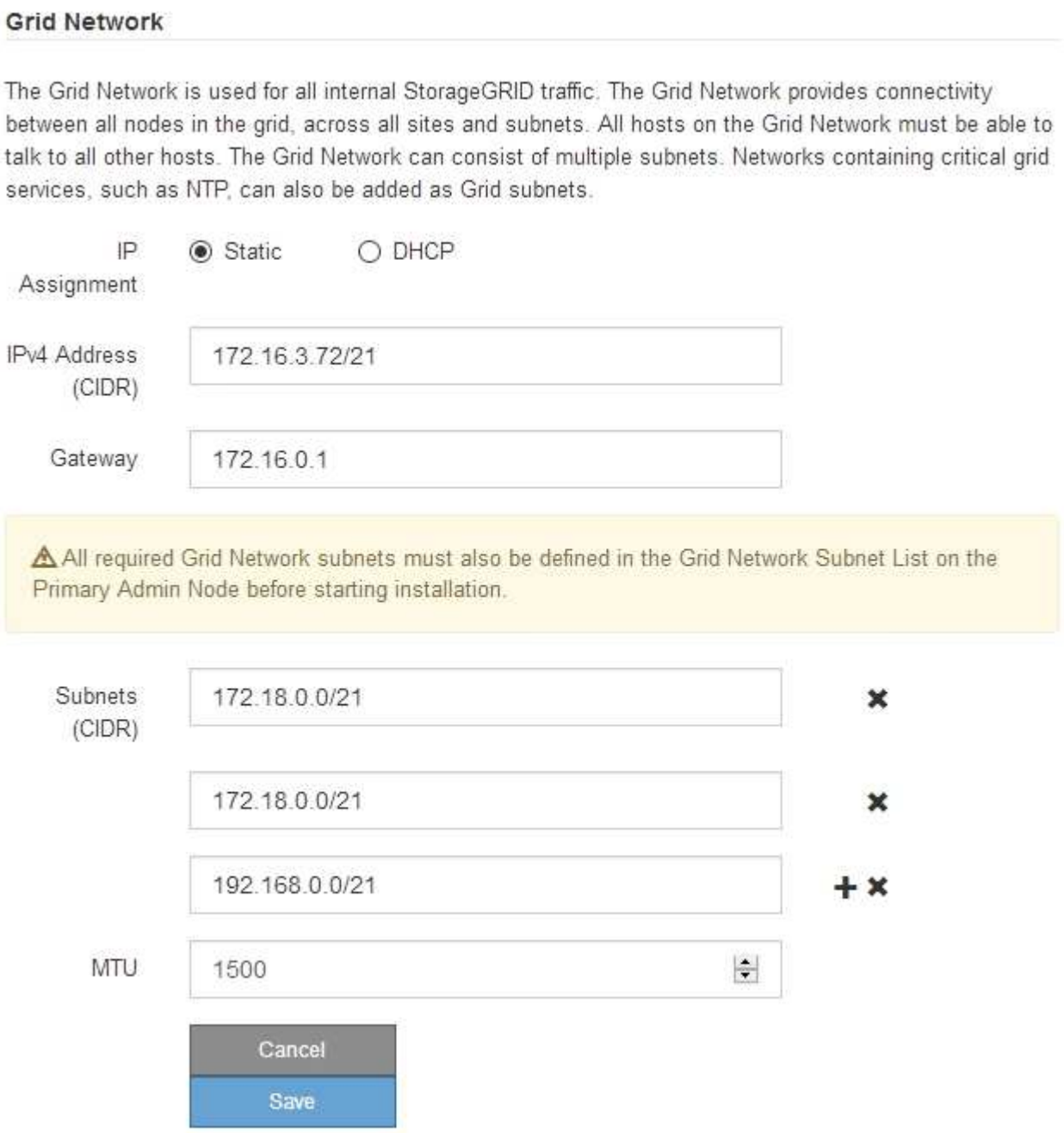
如果要更改链路配置，请参见有关更改 E5700SG 控制器的链路配置的说明。

步骤

1. 在 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。

   此时将显示 "IP Configuration" 页面。

2. 要配置网格网络，请在页面的 * 网格网络 * 部分中选择 * 静态 * 或 * DHCP * 。



3. 如果选择 * 静态 * ，请按照以下步骤配置网格网络：

a. 使用 CIDR 表示法输入静态 IPv4 地址。

b. 输入网关。

   如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

   网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

   为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

d. 单击 * 保存 * 。

   更改 IP 地址时，网关和子网列表可能也会发生更改。

   如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance_IP*:8443*`

e. 确认网格网络子网列表正确无误。

   如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

   未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

   - 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
   - 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

4. 如果选择了 * DHCP * ，请按照以下步骤配置网格网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

   系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

   您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认网格网络子网列表正确无误。

   如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

   未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

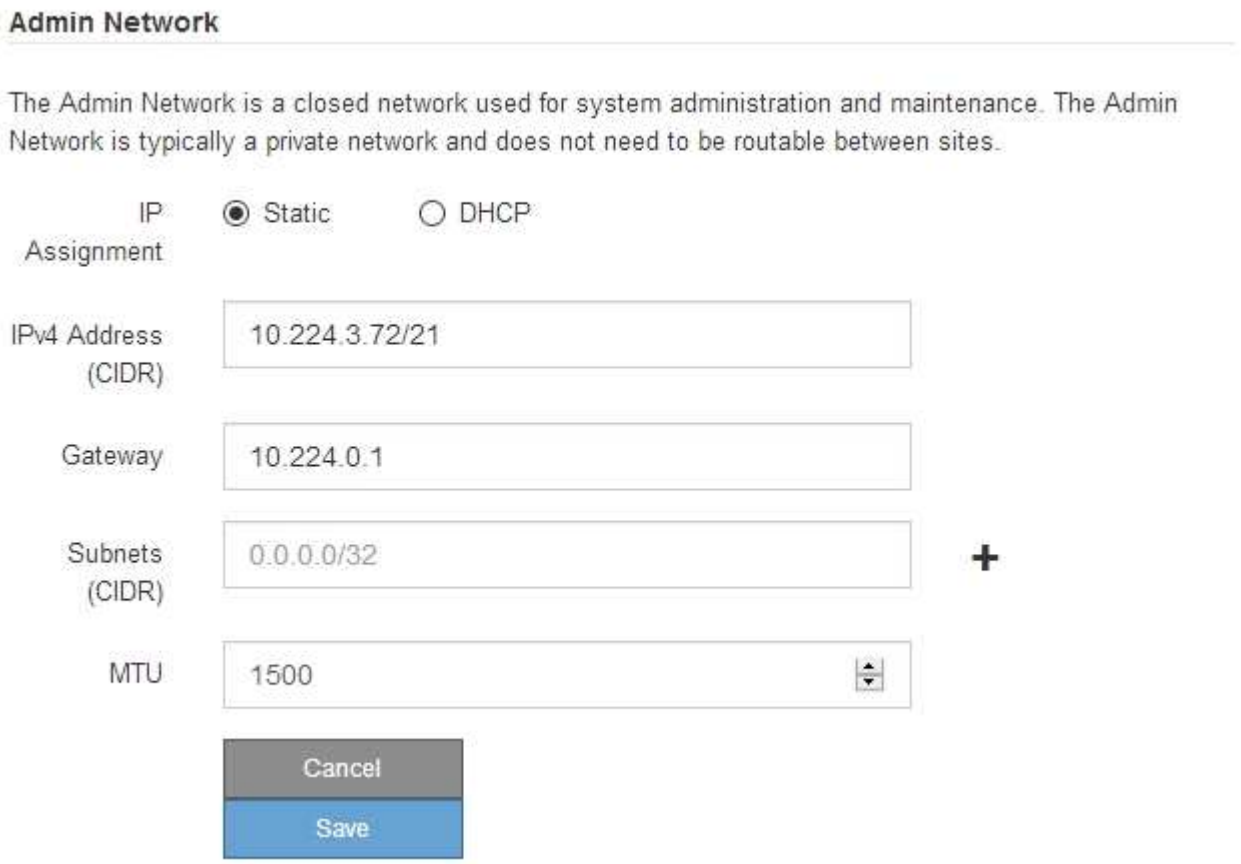
网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

a. 单击 * 保存 * 。

5. 要配置管理网络，请在页面的管理网络部分中选择 * 静态 * 或 * DHCP * 。

要配置管理网络，必须在链路配置页面上启用管理网络。



6. 如果选择 * 静态 * ，请按照以下步骤配置管理网络：

a. 使用 CIDR 表示法为设备上的管理端口 1 输入静态 IPv4 地址。

管理端口 1 位于设备右端的两个 1-GbE RJ45 端口的左侧。

b. 输入网关。

   如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

   网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

   更改 IP 地址时，网关和子网列表可能也会发生更改。

   如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance*:8443*`

e. 确认管理网络子网列表正确无误。

   您必须验证是否可以使用提供的网关访问所有子网。

   无法使用默认路由来使用管理网络网关。

   - 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
   - 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

7. 如果选择了 * DHCP * ，请按照以下步骤配置管理网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

   系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

   您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认管理网络子网列表正确无误。

   您必须验证是否可以使用提供的网关访问所有子网。

   无法使用默认路由来使用管理网络网关。

   - 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
   - 要删除未使用的子网，请单击删除图标 ✖。

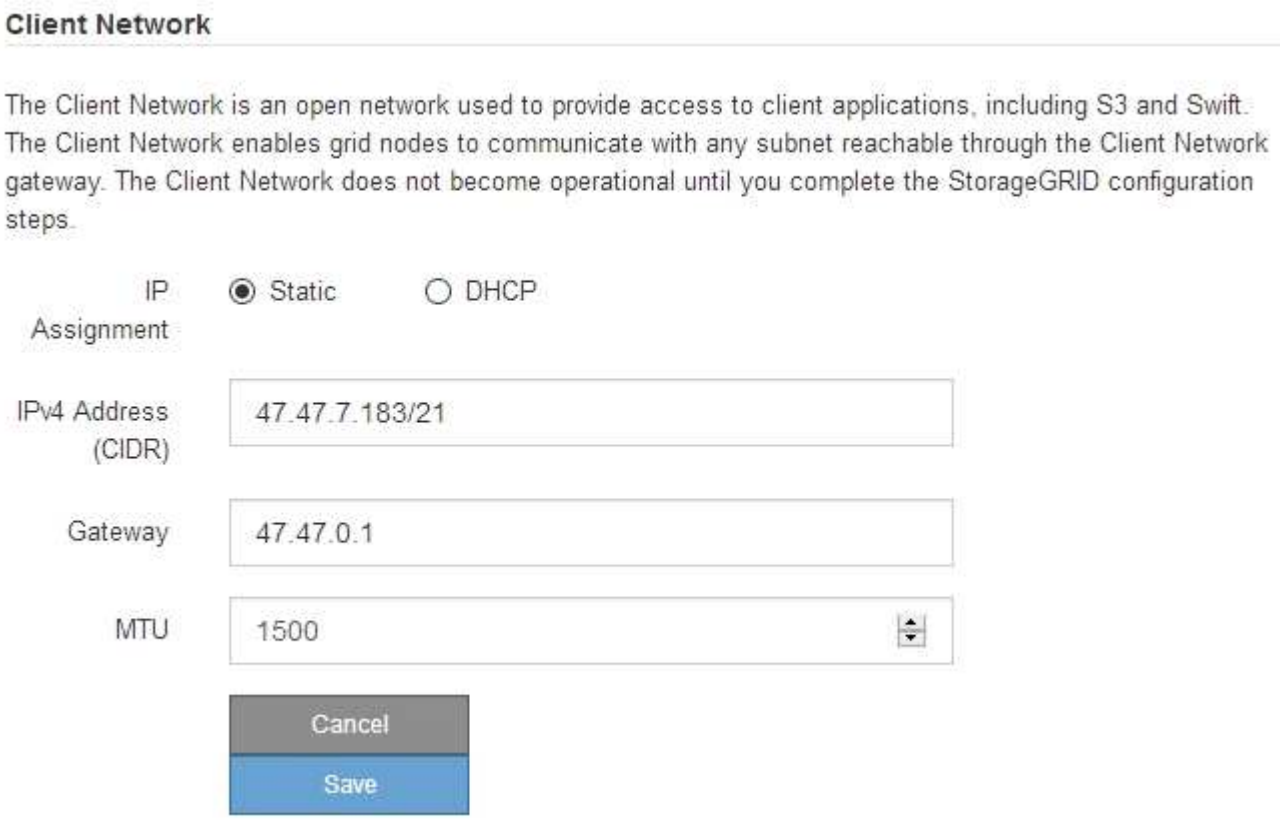
c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

   网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

8. 要配置客户端网络，请在页面的 * 客户端网络 * 部分中选择 * 静态 * 或 * DHCP * 。

要配置客户端网络，必须在链路配置页面上启用客户端网络。



9. 如果选择 * 静态 * ，请按照以下步骤配置客户端网络：

a. 使用 CIDR 表示法输入静态 IPv4 地址。

b. 单击 * 保存 * 。

c. 确认客户端网络网关的 IP 地址正确无误。

如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

d. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

e. 单击 * 保存 * 。

10. 如果选择了 * DHCP * ，请按照以下步骤配置客户端网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

系统会自动填充 * IPv4 地址 * 和 * 网关 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

a. 确认网关是否正确。

> 如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

b. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

相关信息

更改 E5700SG 控制器的链路配置

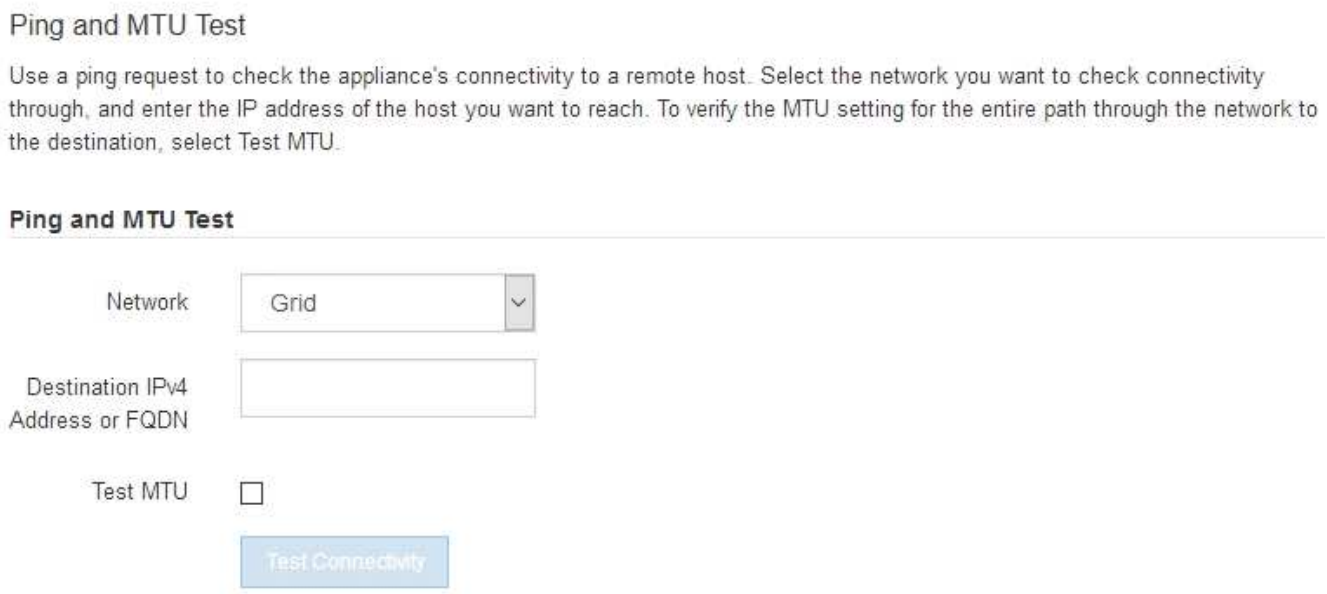
验证网络连接

您应确认可以从设备访问所使用的 StorageGRID 网络。要验证通过网络网关的路由，您应测试 StorageGRID 设备安装程序与不同子网上的 IP 地址之间的连接。您还可以验证 MTU 设置。

步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * Ping 和 MTU 测试 * 。

   此时将显示 Ping 和 MTU 测试页面。



2. 从 * 网络 * 下拉框中，选择要测试的网络：网格，管理员或客户端。

3. 输入该网络上某个主机的 IPv4 地址或完全限定域名（ FQDN ）。

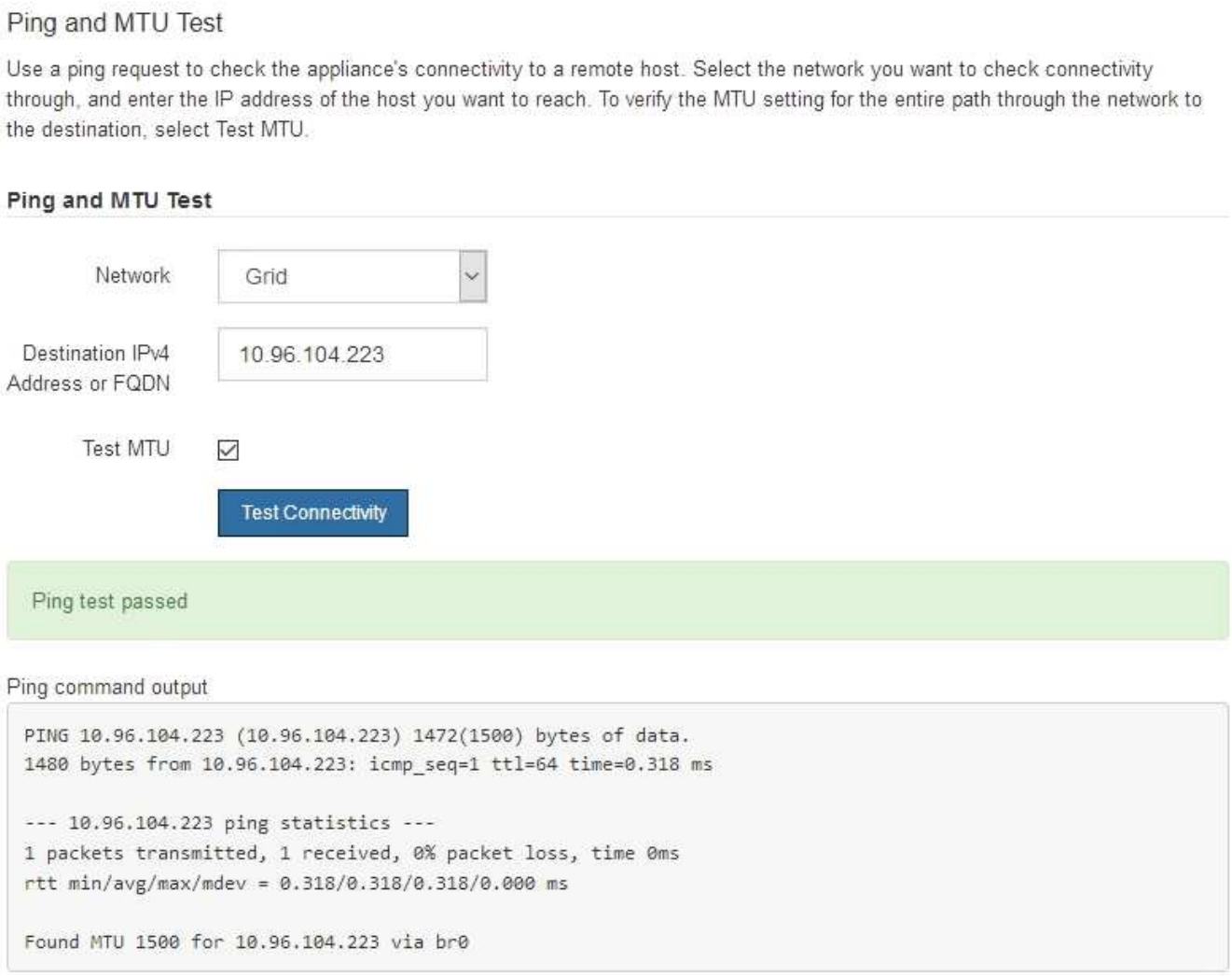
   例如，您可能需要对网络或主管理节点上的网关执行 ping 操作。

4. 或者，选中 * 测试 MTU* 复选框以验证通过网络到目标的整个路径的 MTU 设置。

   例如，您可以测试设备节点与其他站点的节点之间的路径。

5. 单击 * 测试连接 * 。

   如果网络连接有效，则会显示 "Ping test passed" 消息，并列出 ping 命令输出。



相关信息

配置网络链路（ SG5700 ）

更改 MTU 设置

验证端口级别的网络连接

要确保 StorageGRID 设备安装程序与其他节点之间的访问不会受到防火墙的阻碍，请确认

StorageGRID 设备安装程序可以连接到指定 IP 地址或地址范围内的特定 TCP 端口或端口集。

关于此任务

使用 StorageGRID 设备安装程序中提供的端口列表，您可以测试设备与网格网络中其他节点之间的连接。

此外，您还可以在管理和客户端网络以及 UDP 端口上测试连接，例如用于外部 NFS 或 DNS 服务器的端口。有关这些端口的列表，请参见 StorageGRID 网络连接准则中的端口参考。

端口连接表中列出的网格网络端口仅适用于 StorageGRID 11.6.0 版。要验证每种节点类型的端口是否正确，您应始终参考适用于您的 StorageGRID 版本的网络连接准则。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 端口连接测试（ nmap ） * 。

   此时将显示端口连接测试页面。

   端口连接表列出了网格网络上需要 TCP 连接的节点类型。对于每种节点类型，此表列出了设备应可访问的网格网络端口。

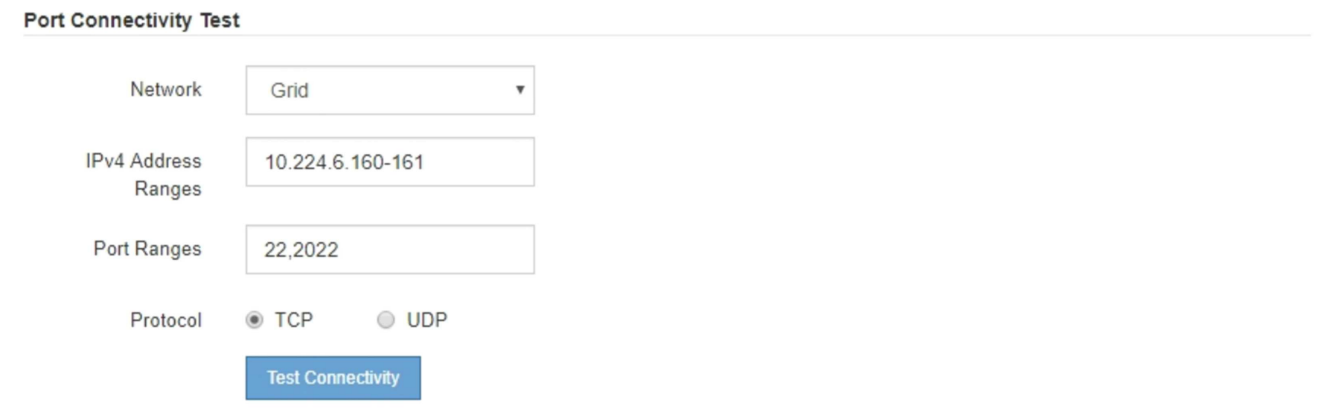
   您可以测试表中列出的设备端口与网格网络中的其他节点之间的连接。

2. 从 * 网络 * 下拉列表中，选择要测试的网络： * 网格 * ， * 管理 * 或 * 客户端 * 。
3. 为该网络上的主机指定一个 IPv4 地址范围。

   例如，您可能需要探测网络或主管理节点上的网关。

   使用连字符指定一个范围，如示例所示。

4. 输入 TCP 端口号，以逗号分隔的端口列表或端口范围。



5. 单击 * 测试连接 * 。

   ◦ 如果选定的端口级别网络连接有效，则绿色横幅中会显示 "`Port connectivity test passed` " 消息。nmap 命令输出列在横幅下方。

- 如果与远程主机建立了端口级网络连接，但主机未侦听一个或多个选定端口，则黄色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  主机未侦听的任何远程端口的状态为 "`closed" 。` 例如，当您尝试连接的节点处于预安装状态且 StorageGRID NMS 服务尚未在该节点上运行时，您可能会看到此黄色横幅。

- 如果无法为一个或多个选定端口建立端口级别网络连接，则红色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  红色横幅表示已尝试通过 TCP 连接到远程主机上的某个端口，但未向发送方返回任何内容。如果未返回任何响应，则此端口的状态为 " 已筛选 " ，并且可能会被防火墙阻止。

  此外，还会列出带有 "`closed` " 的端口。

相关信息

网络连接准则

访问和配置 **SANtricity System Manager** （ **SG5700** ）

您可以使用 SANtricity 系统管理器监控存储控制器，存储磁盘和存储控制器架中其他硬件组件的状态。此外，您还可以为 E 系列 AutoSupport 配置代理，使您能够在不使用管理端口的情况下从设备发送 AutoSupport 消息。

设置并访问 **SANtricity** 系统管理器

您可能需要访问存储控制器上的 SANtricity 系统管理器来监控存储控制器架中的硬件或配置 E 系列 AutoSupport 。

您需要的内容

- 您正在使用 支持的 Web 浏览器。
- 要通过网格管理器访问 SANtricity 系统管理器，您必须已安装 StorageGRID ，并且必须具有存储设备管理员权限或根访问权限。
- 要使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器，您必须具有 SANtricity 系统管理器管理员用户名和密码。
- 要使用 Web 浏览器直接访问 SANtricity System Manager ，您必须具有 SANtricity System Manager 管理员用户名和密码。

> 您必须具有SANtricity 固件8.70 (11.70)或更高版本、才能使用网格管理器或StorageGRID 设备安装程序访问SANtricity 系统管理器。您可以使用 StorageGRID 设备安装程序并选择 * 帮助 * > * 关于 * 来检查固件版本。

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

关于此任务

根据您所处的安装和配置过程的阶段，有三种方法可以访问 SANtricity System Manager ：

- 如果此设备尚未部署为 StorageGRID 系统中的节点，则应使用 StorageGRID 设备安装程序中的高级选项卡。

  部署节点后，您将无法再使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器。

- 如果此设备已部署为 StorageGRID 系统中的节点，请使用网格管理器中节点页面上的 SANtricity 系统管理器选项卡。
- 如果无法使用 StorageGRID 设备安装程序或网格管理器，则可以使用连接到管理端口的 Web 浏览器直接访问 SANtricity 系统管理器。

此操作步骤 包含首次访问 SANtricity System Manager 的步骤。如果您已设置 SANtricity 系统管理器，请转到 配置硬件警报 步骤。

使用网格管理器或 StorageGRID 设备安装程序，您可以访问 SANtricity 系统管理器，而无需配置或连接设备的管理端口。

您可以使用 SANtricity 系统管理器监控以下内容：

- 存储阵列级别性能， I/O 延迟， CPU 利用率和吞吐量等性能数据
- 硬件组件状态
- 支持的功能包括查看诊断数据

您可以使用 SANtricity 系统管理器配置以下设置：

- 存储控制器架中组件的电子邮件警报， SNMP 警报或系统日志警报
- 存储控制器架中组件的 E 系列 AutoSupport 设置。

  有关 E 系列 AutoSupport 的更多详细信息，请参见 E 系列文档中心。

  "NetApp E 系列系统文档站点"

- 驱动器安全密钥，用于解锁安全驱动器（如果启用了驱动器安全功能，则需要执行此步骤）
- 用于访问 SANtricity 系统管理器的管理员密码

步骤

1. 使用 StorageGRID 设备安装程序并选择 * 高级 * > * SANtricity 系统管理器 *

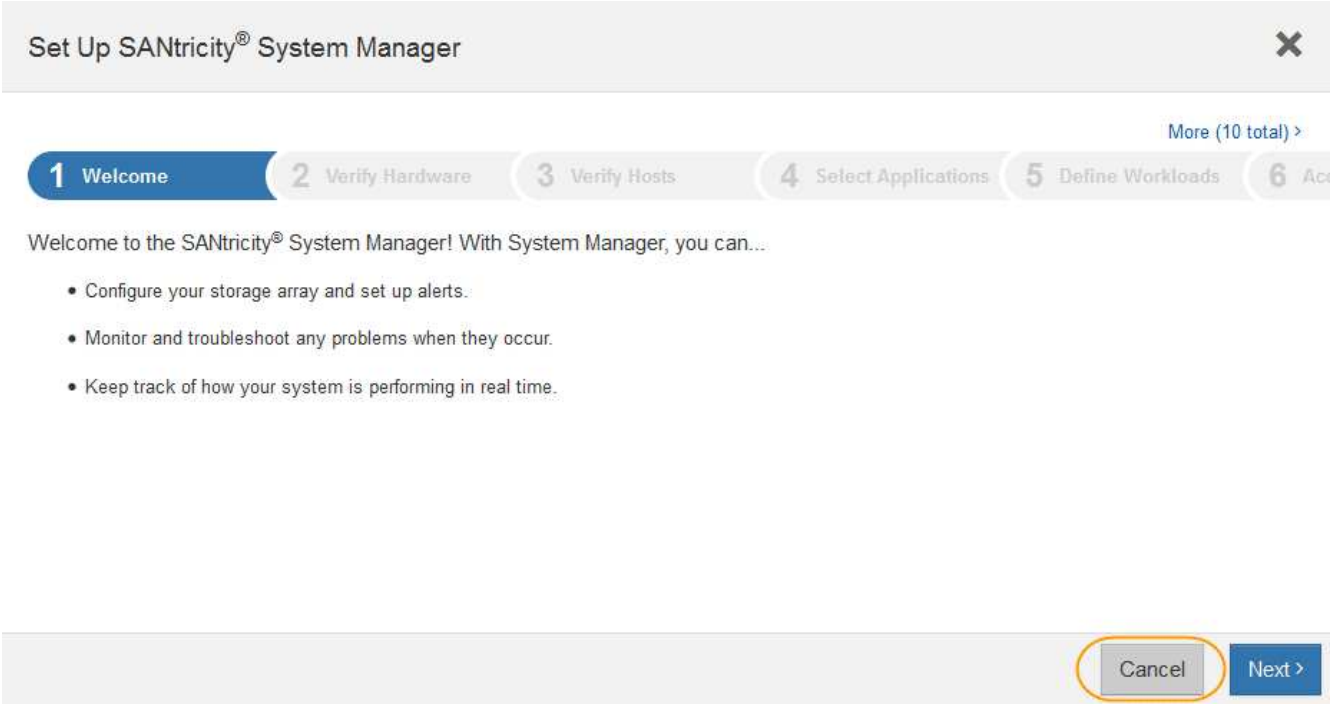
   如果StorageGRID 设备安装程序不可用或未显示登录页面、则必须使用存储控制器的IP地址。浏览到存储控制器 IP ： + ` * https://*Storage_Controller_IP*` 以访问 SANtricity System Manager

此时将显示 SANtricity 系统管理器的登录页面。

2. 设置或输入管理员密码。

   SANtricity 系统管理器使用一个管理员密码，该密码在所有用户之间共享。

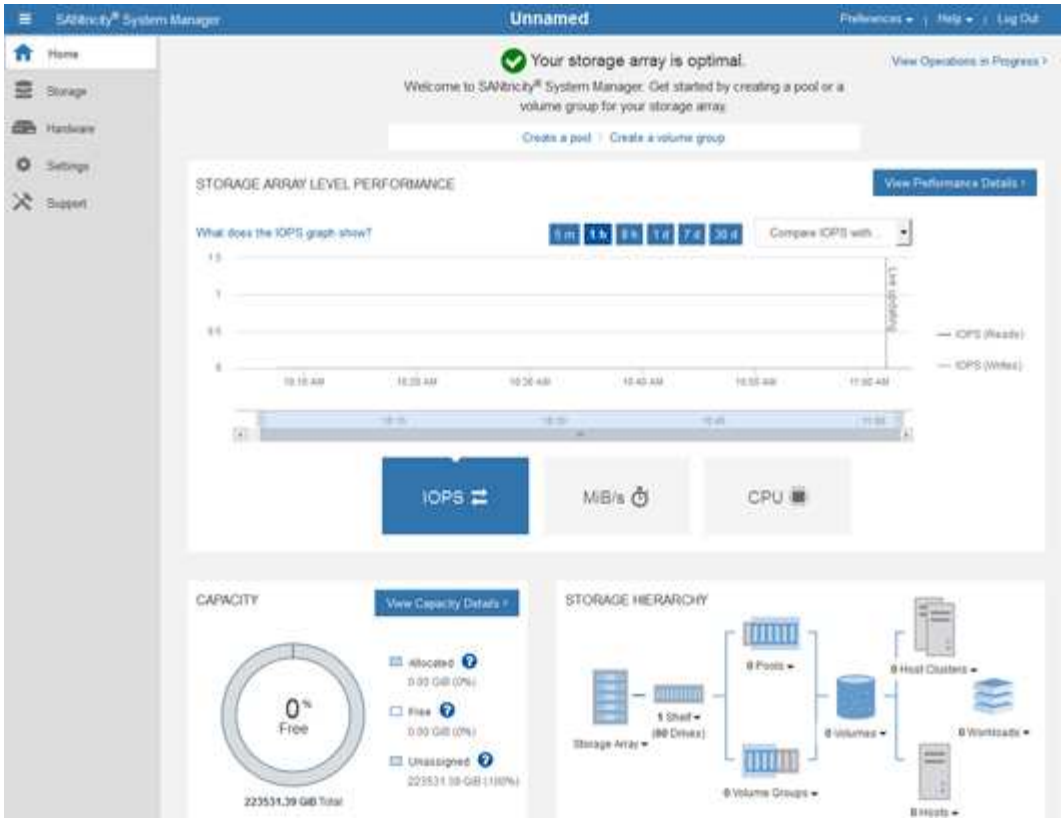
   此时将显示设置向导。



3. 选择 * 取消 * 以关闭向导。

   请勿完成 StorageGRID 设备的设置向导。

   此时将显示 SANtricity System Manager 主页。



4. 【 config_hardware_alerts_sg5700 ， start=4]] 配置硬件警报。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 设置 * > * 警报 * 部分了解警报。
   c. 按照 "`如何` " 说明设置电子邮件警报， SNMP 警报或系统日志警报。
5. 管理存储控制器架中组件的 AutoSupport 。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 支持 * > * 支持中心 * 部分了解 AutoSupport 功能。
   c. 按照 "`如何` " 说明管理 AutoSupport 。

      有关配置 StorageGRID 代理以在不使用管理端口的情况下发送 E 系列 AutoSupport 消息的具体说明，请转至 StorageGRID 管理说明并搜索 "E 系列 AutoSupport 的代理设置 " 。

   管理 StorageGRID

6. 如果为设备启用了驱动器安全功能，请创建并管理安全密钥。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 设置 * > * 系统 * > * 安全密钥管理 * 部分了解驱动器安全性。
   c. 按照 "`如何` " 说明创建和管理安全密钥。
7. 也可以更改管理员密码。
   a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
   b. 使用联机帮助的 * 主页 * > * 存储阵列管理 * 部分了解管理员密码。

c. 按照 " 操作 " 说明更改密码。

在 **SANtricity System Manager** 中查看硬件状态

您可以使用 SANtricity 系统管理器监控和管理存储控制器架中的各个硬件组件，并查看硬件诊断和环境信息，例如组件温度以及与驱动器相关的问题。

您需要的内容

- 您正在使用 支持的 Web 浏览器。
- 要通过网格管理器访问 SANtricity 系统管理器，您必须具有存储设备管理员权限或 root 访问权限。
- 要使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器，您必须具有 SANtricity 系统管理器管理员用户名和密码。
- 要使用 Web 浏览器直接访问 SANtricity System Manager ，您必须具有 SANtricity System Manager 管理员用户名和密码。

> 您必须具有SANtricity 固件8.70 (11.70)或更高版本、才能使用网格管理器或StorageGRID 设备安装程序访问SANtricity 系统管理器。

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

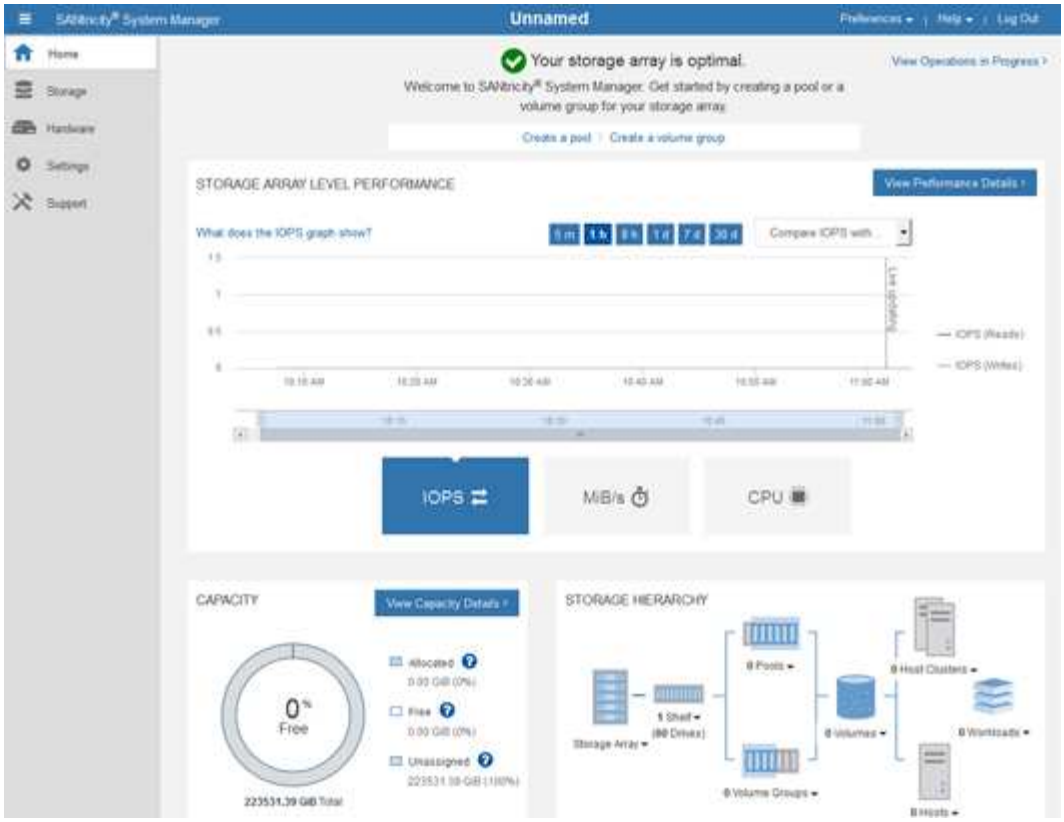
步骤

1. 访问 SANtricity 系统管理器。

   设置并访问 SANtricity 系统管理器

2. 如果需要，请输入管理员用户名和密码。
3. 单击 * 取消 * 以关闭设置向导并显示 SANtricity 系统管理器主页。

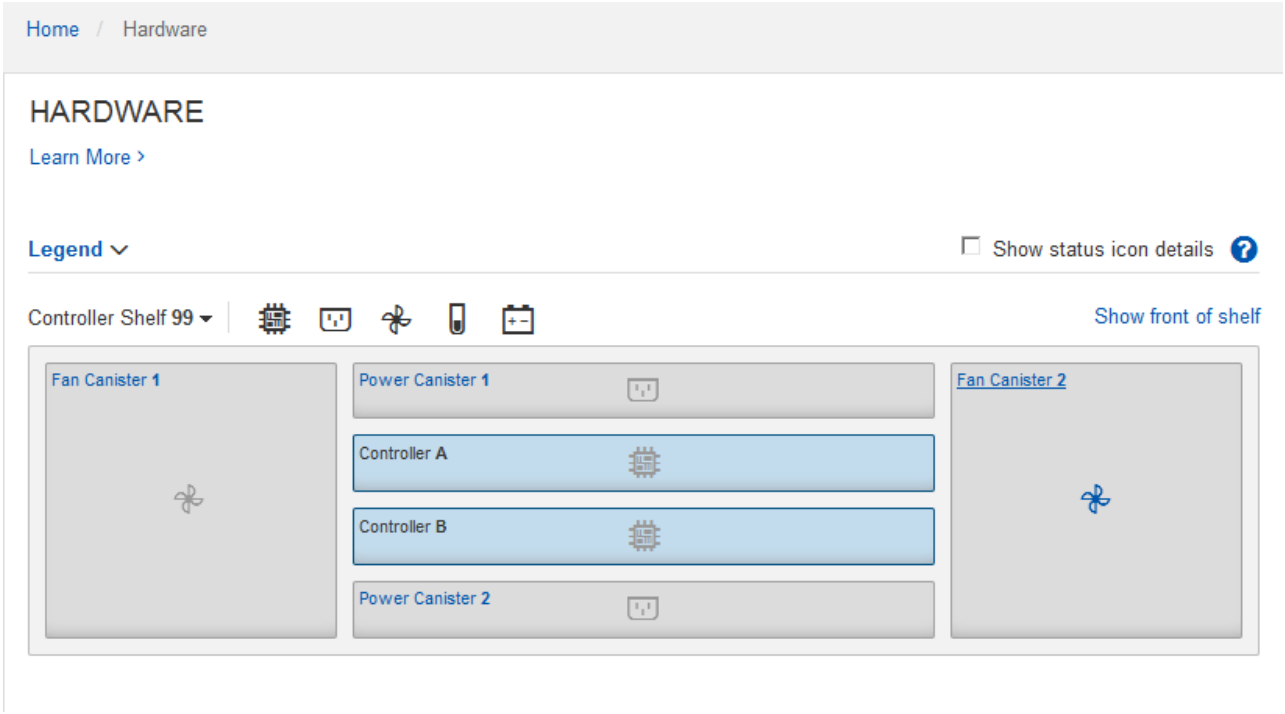
   此时将显示 SANtricity System Manager 主页。在 SANtricity 系统管理器中，控制器架称为存储阵列。



4. 查看显示的设备硬件信息，并确认所有硬件组件的状态均为最佳。

   a. 单击 * 硬件 * 选项卡。

   b. 单击 * 显示磁盘架的背面 * 。



从磁盘架背面，您可以查看两个存储控制器，每个存储控制器中的电池，两个电源箱，两个风扇箱和扩展架（如果有）。您还可以查看组件温度。

a. 要查看每个存储控制器的设置，请选择控制器，然后从上下文菜单中选择 * 查看设置 * 。
b. 要查看磁盘架背面其他组件的设置，请选择要查看的组件。
c. 单击 * 显示磁盘架正面 * ，然后选择要查看的组件。

   从磁盘架正面，您可以查看存储控制器磁盘架或扩展磁盘架（如果有）的驱动器和驱动器抽盒。

如果需要关注任何组件的状态，请按照 Recovery Guru 中的步骤解决问题描述 或联系技术支持。

使用 **StorageGRID** 设备安装程序设置存储控制器的 **IP** 地址

每个存储控制器上的管理端口 1 用于将设备连接到 SANtricity System Manager 的管理网络。如果无法从 StorageGRID 设备安装程序访问 SANtricity 系统管理器，则必须为每个存储控制器设置一个静态 IP 地址，以确保不会丢失与控制器架中的硬件和控制器固件的管理连接。

您需要的内容

- 您正在使用可以连接到 StorageGRID 管理网络的任何管理客户端，或者您使用的是服务笔记本电脑。
- 客户端或服务笔记本电脑具有受支持的 Web 浏览器。

关于此任务

DHCP 分配的地址可以随时更改。为控制器分配静态 IP 地址，以确保一致的可访问性。

> 只有当您无法从 StorageGRID 设备安装程序（ * 高级 * > * SANtricity 系统管理器 * ）或网格管理器（ * 节点 * > * SANtricity 系统管理器 * ）访问 SANtricity 系统管理器时，才应遵循此操作步骤。

步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*Appliance_Controller_IP*:8443*`

   对于 ` 设备控制器 IP` ，请在任何 StorageGRID 网络上使用设备的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 存储控制器网络配置 * 。

   此时将显示存储控制器网络配置页面。

3. 根据您的网络配置，对于 IPv4 ， IPv6 或这两者，请选择 * 已启用 * 。
4. 记下自动显示的 IPv4 地址。

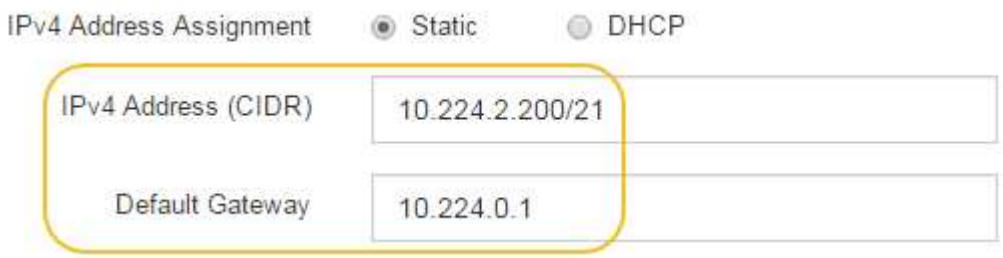
   DHCP 是为存储控制器管理端口分配 IP 地址的默认方法。

   > 显示 DHCP 值可能需要几分钟的时间。

5. （可选）设置存储控制器管理端口的静态 IP 地址。

   您应该为管理端口分配静态 IP ，或者为 DHCP 服务器上的地址分配永久租约。

   a. 选择 * 静态 * 。
   b. 使用 CIDR 表示法输入 IPv4 地址。
   c. 输入默认网关。



   d. 单击 * 保存 * 。

      应用所做的更改可能需要几分钟的时间。

连接到 SANtricity 系统管理器时，您将使用新的静态 IP 地址作为 URL： + ` * https://*Storage_Controller_IP*`

可选：启用节点加密

如果启用了节点加密，则可以通过安全密钥管理服务器（ KMS ）加密来保护设备中的磁盘，防止物理丢失或从站点中删除。您必须在设备安装期间选择并启用节点加密，并且在 KMS 加密过程开始后，不能取消选择节点加密。

您需要的内容

查看有关管理 StorageGRID 的说明中有关 KMS 的信息。

关于此任务

启用了节点加密的设备将连接到为 StorageGRID 站点配置的外部密钥管理服务器（ KMS ）。每个 KMS （或 KMS 集群）负责管理站点上所有设备节点的加密密钥。这些密钥对启用了节点加密的设备中每个磁盘上的数据进行加密和解密。

可以在 StorageGRID 中安装 KMS 之前或之后在网格管理器中设置此设备。有关更多详细信息，请参见管理 StorageGRID 的说明中有关 KMS 和设备配置的信息。

- 如果在安装设备之前设置了 KMS ，则在设备上启用节点加密并将其添加到配置了 KMS 的 StorageGRID 站点时， KMS 控制的加密将开始。
- 如果在安装此设备之前未设置 KMS ，则在为包含此设备节点的站点配置了 KMS 并可使用此 KMS 后，将对启用了节点加密的每个设备执行 KMS 控制的加密。

> 在连接到启用了节点加密的设备上的 KMS 之前存在的数据将使用不安全的临时密钥进行加密。除非将密钥设置为 KMS 提供的值，否则设备不会受到删除或被盗的保护。

如果没有对磁盘进行解密所需的 KMS 密钥，则无法检索设备上的数据，并且数据实际上会丢失。如果无法从 KMS 中检索到解密密钥，则会出现这种情况。如果清除KMS配置、KMS密钥过期、与KMS的连接断开或从安装了KMS密钥的StorageGRID 系统中删除设备、则无法访问此密钥。

步骤

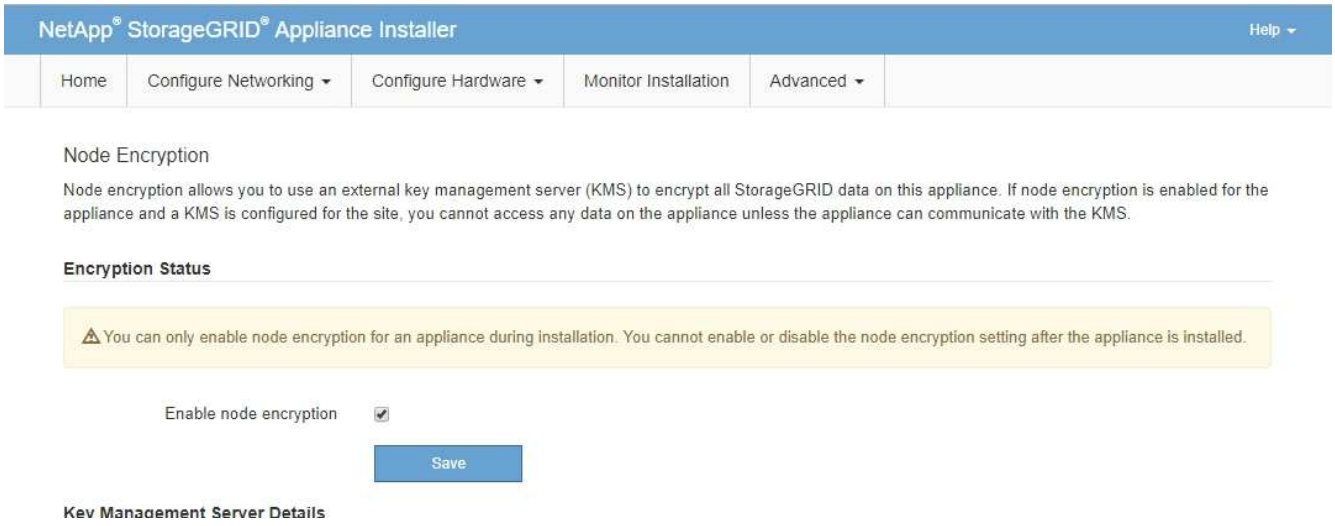
1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

   > 使用 KMS 密钥对设备加密后，如果不使用相同的 KMS 密钥，则无法对设备磁盘进行解密。

2. 选择 * 配置硬件 * > * 节点加密 * 。



3. 选择 * 启用节点加密 * 。

   在安装设备之前，您可以取消选择 * 启用节点加密 * ，而不会有数据丢失的风险。安装开始后，设备节点将访问 StorageGRID 系统中的 KMS 加密密钥并开始磁盘加密。安装设备后，您无法禁用节点加密。

   > 将启用了节点加密的设备添加到具有 KMS 的 StorageGRID 站点后，您无法停止对此节点使用 KMS 加密。

4. 选择 * 保存 * 。
5. 将设备部署为 StorageGRID 系统中的节点。

当设备访问为 StorageGRID 站点配置的 KMS 密钥时，便会开始使用由 KMS 控制的加密。安装程序会在 KMS 加密过程中显示进度消息，此过程可能需要几分钟时间，具体取决于设备中的磁盘卷数。

> 设备最初会配置一个随机的非 KMS 加密密钥，该密钥会分配给每个磁盘卷。磁盘会使用此临时加密密钥进行加密，这种加密密钥不安全，直到启用了节点加密的设备访问为 StorageGRID 站点配置的 KMS 密钥为止。

完成后

您可以查看节点加密状态， KMS 详细信息以及设备节点处于维护模式时正在使用的证书。

相关信息

管理 StorageGRID

在维护模式下监控节点加密（ SG5700 ）

可选：更改 **RAID** 模式（仅限 **SG5760** ）

如果您的 SG5760 包含 60 个驱动器，则可以更改为其他 RAID 模式以满足存储和恢复要求。您只能在部署 StorageGRID 设备存储节点之前更改此模式。

您需要的内容

- 您已安装 SG5760 。如果您使用的是 SG5712 ，则必须使用 DDP 模式。
- 您正在使用可以连接到 StorageGRID 的任何客户端。
- 客户端具有 支持的 Web 浏览器。

关于此任务

在将 SG5760 设备部署为存储节点之前，您可以选择以下卷配置选项之一：

- * DDP * ： 此模式每八个数据驱动器使用两个奇偶校验驱动器。这是所有设备的默认和建议模式。与 RAID6 相比， DDP 可提高系统性能，缩短驱动器发生故障后的重建时间，并简化管理。DDP 还可在 60 驱动器设备中提供抽盒丢失保护。
- * DDP16* ： 此模式每 16 个数据驱动器使用两个奇偶校验驱动器，因此与 DDP 相比，存储效率更高。与 RAID6 相比， DDP16 可提高系统性能，缩短驱动器故障后的重建时间，简化管理并提供同等的存储效率。要使用 DDP16 模式，您的配置必须至少包含 20 个驱动器。DDP16 不提供抽盒丢失保护。
- * RAID6* ： 此模式每 16 个或更多数据驱动器使用两个奇偶校验驱动器。要使用 RAID 6 模式，您的配置必须至少包含 20 个驱动器。虽然与 DDP 相比， RAID6 可以提高设备的存储效率，但不建议在大多数 StorageGRID 环境中使用。

> 如果已配置任何卷或先前已安装 StorageGRID ，则更改 RAID 模式会删除和更换这些卷。这些卷上的所有数据都将丢失。

步骤

1. 使用服务笔记本电脑打开 Web 浏览器并访问 StorageGRID 设备安装程序： + ` * https://*E5700SG_Controller_IP*:8443*`

   其中， ` *E5700SG_Controller_IP*` 是 E5700SG 控制器的任何 IP 地址。

2. 选择 * 高级 * > * RAID 模式 * 。
3. 在 * 配置 RAID 模式 * 页面上，从模式下拉列表中选择所需的 RAID 模式。
4. 单击 * 保存 * 。

相关信息

"NetApp E 系列系统文档站点"

可选：重新映射设备的网络端口

您可能需要将设备存储节点上的内部端口重新映射到不同的外部端口。例如，由于使用了防火墙问题描述 ，您可能需要重新映射端口。

您需要的内容

- 您先前已访问 StorageGRID 设备安装程序。
- 您尚未配置，也不打算配置负载平衡器端点。

> 如果重新映射任何端口，则不能使用相同的端口来配置负载平衡器端点。如果要配置负载平衡器端点且已重新映射端口，请按照中的步骤进行操作 删除端口重新映射。

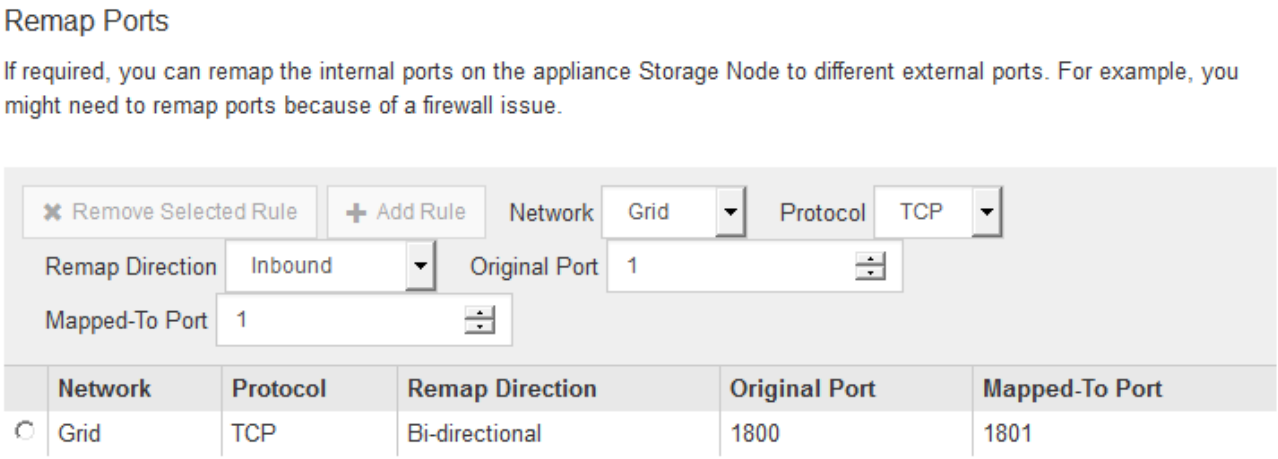
步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * 删除端口 * 。

   此时将显示 Remap Port 页面。

2. 从 * 网络 * 下拉框中，为要重新映射的端口选择网络：网格，管理员或客户端。
3. 从 * 协议 * 下拉框中，选择 IP 协议： TCP 或 UDP 。
4. 从 * 映射方向 * 下拉框中，选择要为此端口重新映射的流量方向：入站，出站或双向。
5. 对于 * 原始端口 * ，输入要重新映射的端口的编号。
6. 对于 * 映射到端口 * ，请输入要使用的端口编号。
7. 单击 * 添加规则 * 。

   此时，新端口映射将添加到表中，重新映射将立即生效。



8. 要删除端口映射，请选择要删除的规则对应的单选按钮，然后单击 * 删除选定规则 * 。

部署设备存储节点

安装和配置存储设备后，您可以将其部署为 StorageGRID 系统中的存储节点。将设备部署为存储节点时，您可以使用设备上随附的 StorageGRID 设备安装程序。

您需要的内容

- 如果要克隆设备节点，请继续执行恢复和维护过程。

  恢复和维护

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路， IP 地址和端口重新映射（如果需要）。
- 您知道分配给设备计算控制器的一个 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。
- 已部署 StorageGRID 系统的主管理节点。
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 您的服务笔记本电脑具有受支持的 Web 浏览器。

关于此任务

每个存储设备都用作一个存储节点。任何设备都可以连接到网格网络，管理网络和客户端网络

要在 StorageGRID 系统中部署设备存储节点，请访问 StorageGRID 设备安装程序并执行以下步骤：

- 您可以指定或确认主管理节点的 IP 地址以及存储节点的名称。
- 您可以开始部署，并等待卷配置完毕并安装软件。
- 当安装暂停完成设备安装任务后，您可以通过登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装和部署过程来恢复安装。

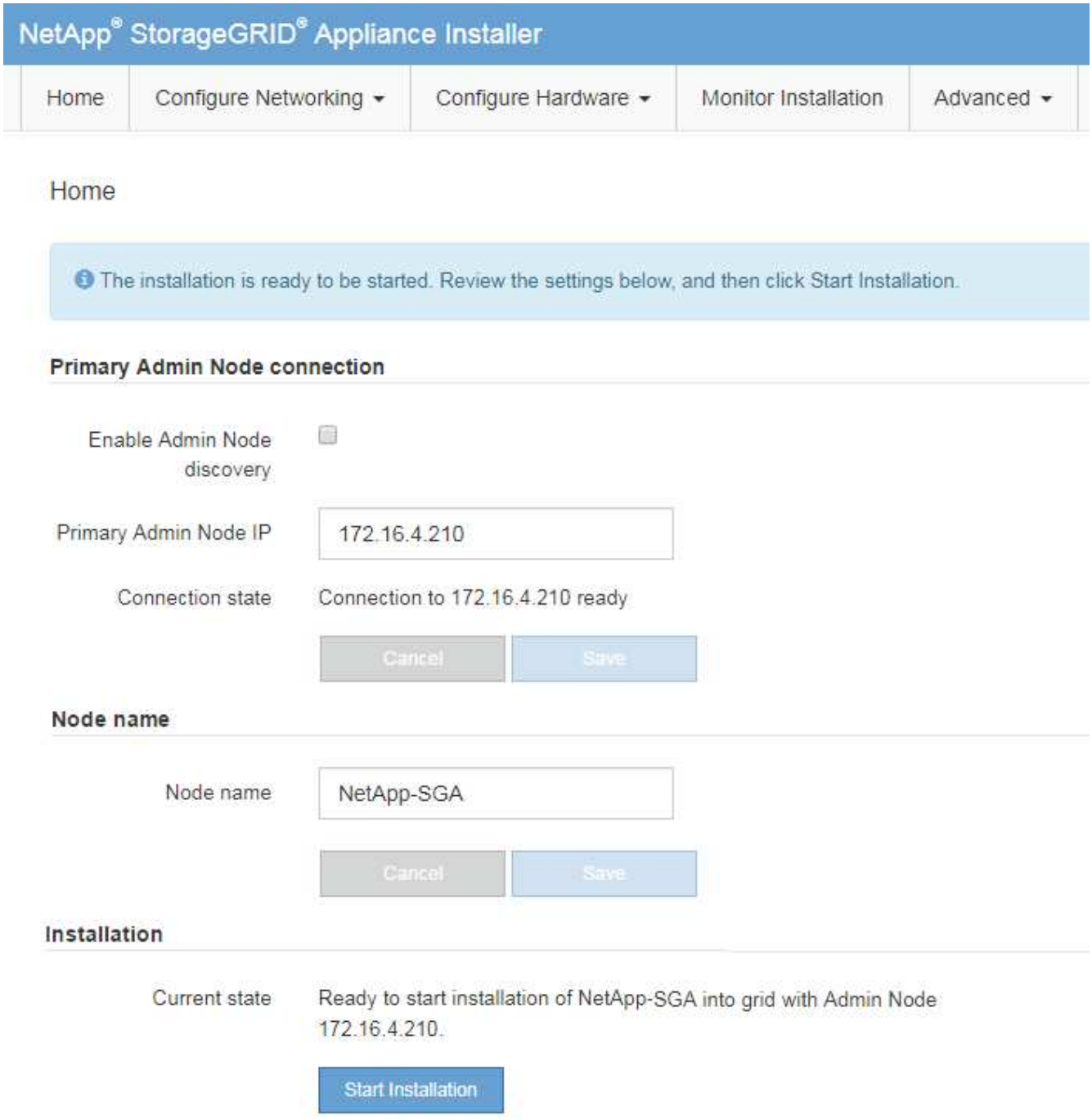
> 如果您需要一次部署多个设备节点，则可以使用 `configure-sGa.py` Appliance Installation 脚本自动执行安装过程。

- 如果要执行扩展或恢复操作，请按照相应说明进行操作：
  - 要将设备存储节点添加到现有 StorageGRID 系统，请参见有关扩展 StorageGRID 系统的说明。
  - 要在恢复操作中部署设备存储节点，请参见有关恢复和维护的说明。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   此时将显示 StorageGRID 设备安装程序主页页面。



2. 在 * 主管理节点连接 * 部分中，确定是否需要指定主管理节点的 IP 地址。

   如果先前已在此数据中心中安装了其他节点，则 StorageGRID 设备安装程序可以自动发现此 IP 地址，前提

是主管理节点或至少一个配置了 admin_IP 的其他网格节点位于同一子网上。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 等待连接状态，使新 IP 地址准备就绪。
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 等待显示发现的 IP 地址列表。 c. 为要部署此设备存储节点的网格选择主管理节点。 d. 单击 * 保存 * 。 e. 等待连接状态，使新 IP 地址准备就绪。

4. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后单击 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的节点页面（概述选项卡）上。如果需要，您可以在批准节点时更改名称。

5. 在 * 安装 * 部分中，确认当前状态为 "Ready to start installation of ` node_node name_` into grid with primary Admin Node ` *admin_IP*` " ，并且 * 开始安装 * 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

   > 如果要将存储节点设备部署为节点克隆目标，请在此停止部署过程，然后继续执行节点克隆操作步骤 的恢复和维护。

   恢复和维护

6. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。

   当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

   > 如果需要手动访问监控器安装页面，请单击 * 监控安装 * 。

7. 如果网格包含多个设备存储节点，请对每个设备重复这些步骤。

   > 如果您需要一次部署多个设备存储节点，则可以使用 `configure-sGa.py` Appliance Installation 脚本自动执行安装过程。

相关信息

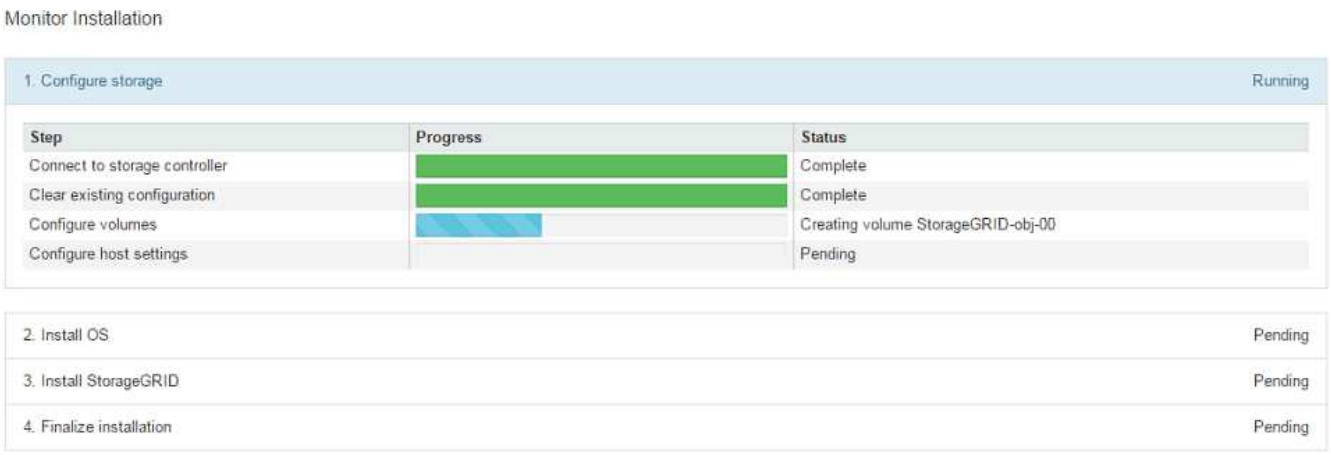
监控存储设备安装

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

步骤

1. 要监控安装进度，请单击 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

2. 查看前两个安装阶段的进度。

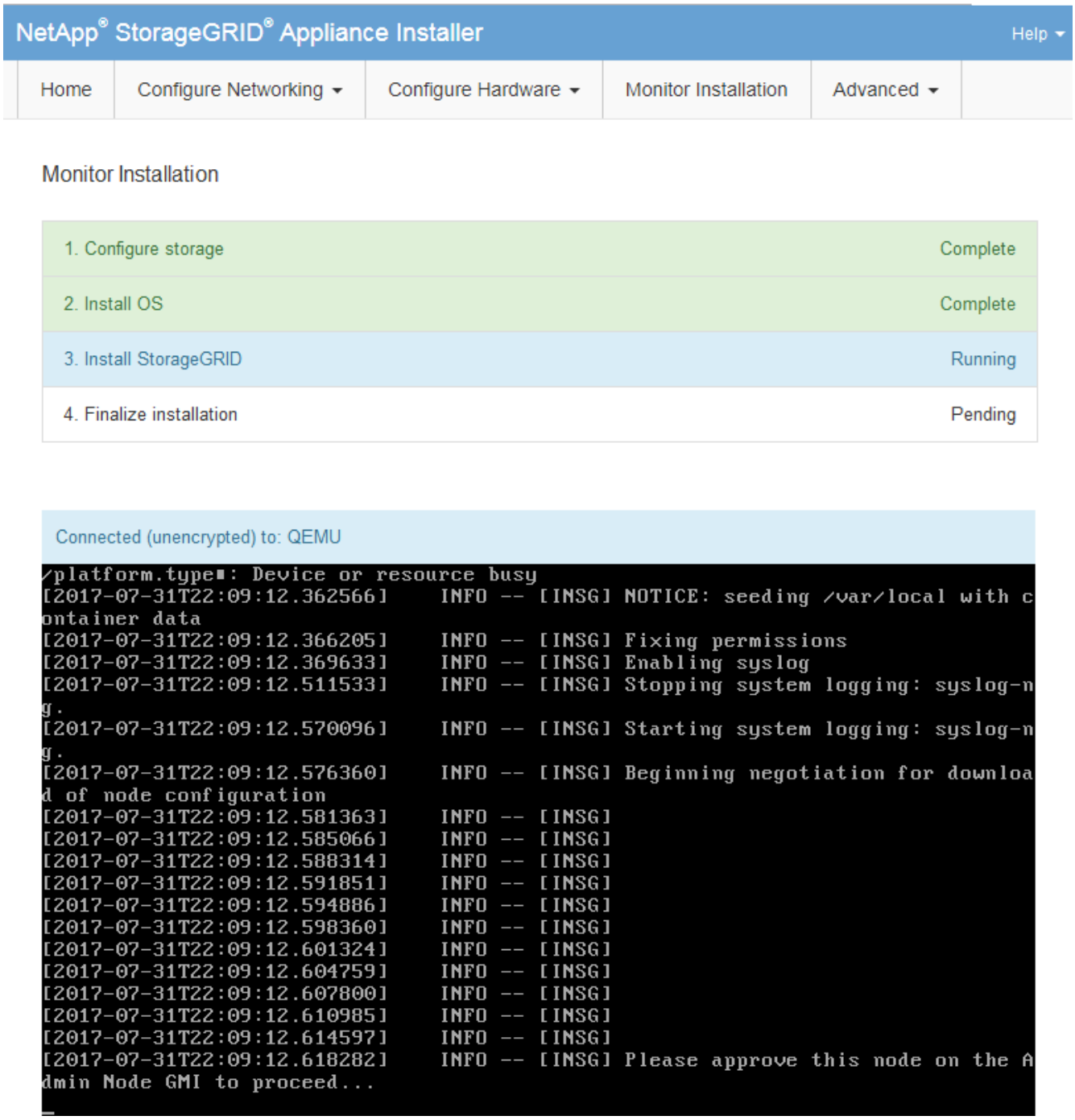
   - 。配置存储 *

     在此阶段，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。

   - 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

3. 继续监控安装进度，直到 * 安装 StorageGRID 网格管理器 * 阶段暂停，并且嵌入式控制台上显示一条消息，提示您使用网格管理器在管理节点上批准此节点。继续执行下一步。



4. 转至主管理节点的网格管理器，批准待定存储节点并完成 StorageGRID 安装过程。

   在网格管理器中单击 * 安装 * 后，第 3 阶段完成，第 4 阶段 * 完成安装 * 开始。阶段 4 完成后，控制器将重新启动。

自动化设备安装和配置（ **SG5700** ）

您可以自动安装和配置设备以及配置整个 StorageGRID 系统。

关于此任务

自动化安装和配置对于部署多个 StorageGRID 实例或一个大型复杂的 StorageGRID 实例非常有用。

要自动执行安装和配置，请使用以下一个或多个选项：

- 创建一个 JSON 文件，用于指定设备的配置设置。使用 StorageGRID 设备安装程序上传 JSON 文件。

  您可以使用同一文件配置多个设备。

- 使用 StorageGRID`configure-sGa.py` Python 脚本自动配置设备。
- 使用其他 Python 脚本配置整个 StorageGRID 系统的其他组件（ " 网格 " ）。

您可以直接使用 StorageGRID 自动化 Python 脚本，也可以使用它们作为示例，说明如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。请参见有关的信息 下载并提取 StorageGRID 安装文件 在恢复和维护说明中。

使用 **StorageGRID** 设备安装程序自动配置设备

您可以使用包含配置信息的 JSON 文件自动配置设备。您可以使用 StorageGRID 设备安装程序上传文件。

您需要的内容

- 您的设备必须使用与 StorageGRID 11.5 或更高版本兼容的最新固件。
- 您必须连接到要使用配置的设备上的 StorageGRID 设备安装程序 支持的 Web 浏览器。

关于此任务

您可以自动执行设备配置任务，例如配置以下内容：

- 网格网络，管理网络和客户端网络 IP 地址
- BMC 接口
- 网络链路
  - 端口绑定模式
  - 网络绑定模式
  - 链路速度

使用上传的 JSON 文件配置设备通常比在 StorageGRID 设备安装程序中使用多个页面手动执行配置效率更高，尤其是在需要配置多个节点时。您必须一次应用一个节点的配置文件。

有经验的用户如果希望自动安装和配置其设备，可以使用 `configure-sGA .py` 脚本。+使用 configure-sga.py 脚本自动安装和配置设备节点

步骤

1. 使用以下方法之一生成 JSON 文件：
   - ConfigBuilder 应用程序

     "ConfigBuilder.netapp.com"

   - `configure-sGa.py` 设备配置脚本。您可以从 StorageGRID 设备安装程序（ * 帮助 * > * 设备配置脚

本 * ）下载此脚本。请参见有关使用 configure-sga.py 脚本自动配置的说明。

使用 configure-sga.py 脚本自动安装和配置设备节点

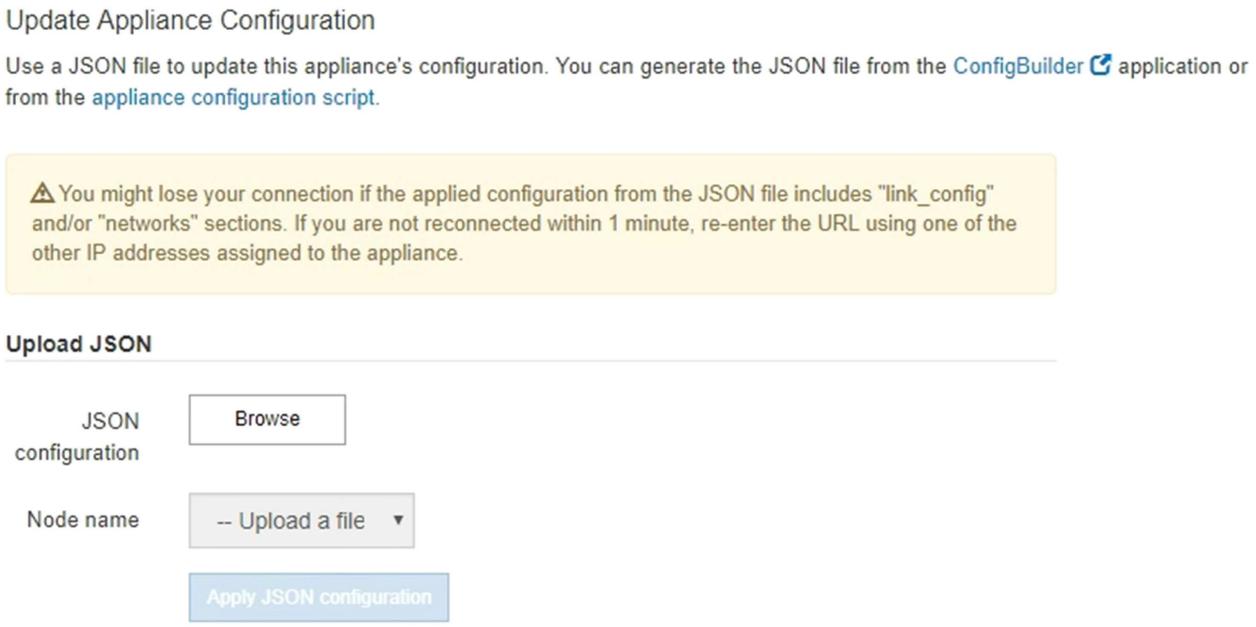
JSON 文件中的节点名称必须符合以下要求：

- 必须是一个有效的主机名，至少包含 1 个字符，并且不超过 32 个字符
- 可以使用字母，数字和连字符
- 不能以连字符开头或结尾
- 不能或仅包含数字

> 请确保 JSON 文件中的节点名称（顶级名称）是唯一的，否则您将无法使用 JSON 文件配置多个节点。

2. 选择 * 高级 * > * 更新设备配置 * 。

此时将显示更新设备配置页面。

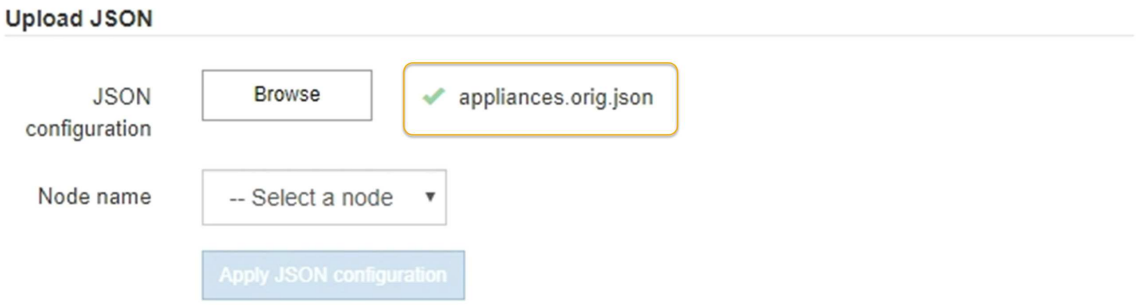


3. 选择包含要上传的配置的 JSON 文件。

a. 选择 * 浏览 * 。
b. 找到并选择文件。
c. 选择 * 打开 * 。

已上传并验证此文件。验证过程完成后，文件名会显示在绿色复选标记旁边。

如果 JSON 文件中的配置包含 "link_config" ， "networks" 或这两者的部分，则可能会断开与设备的连接。如果 1 分钟内未重新连接，请使用分配给设备的其他 IP 地址之一重新输入设备 URL 。

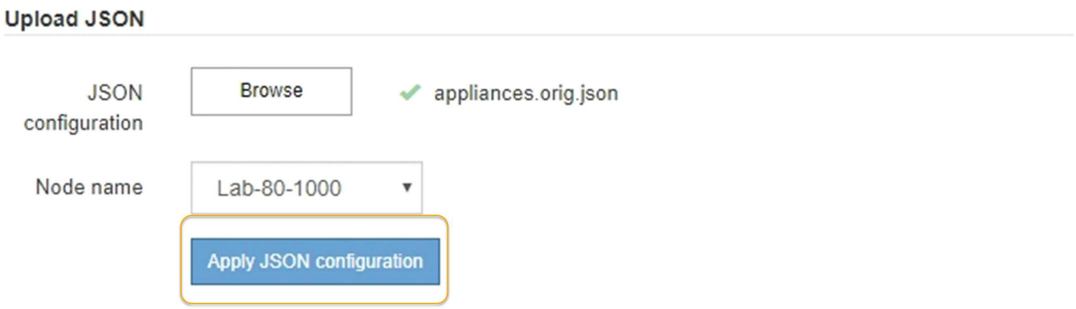


此时将使用 JSON 文件中定义的顶级节点名称填充 * 节点名称 * 下拉列表。

如果文件无效，则文件名将显示为红色，并在黄色横幅中显示一条错误消息。此无效文件不会应用于此设备。您可以使用 ConfigBuilder 来确保具有有效的 JSON 文件。

4. 从 * 节点名称 * 下拉列表中选择一个节点。

   此时将启用 * 应用 JSON 配置 * 按钮。



5. 选择 * 应用 JSON 配置 * 。

   此配置将应用于选定节点。

使用 **configure-sga.py** 脚本自动安装和配置设备节点

您可以使用 `configure-sGa.py` 脚本自动执行 StorageGRID 设备节点的许多安装和配置任务，包括安装和配置主管理节点。如果要配置大量设备，此脚本可能会很有用。您也可以使用此脚本生成包含设备配置信息的 JSON 文件。

关于此任务

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为主管理节点配置网络链路和 IP 地址。

- 如果要安装主管理节点，则您知道其 IP 地址。
- 如果要安装和配置其他节点，则已部署主管理节点，并且您知道其 IP 地址。
- 对于主管理节点以外的所有节点，已在主管理节点上的网格网络子网列表中定义 StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网。
- 您已下载 `configure-sGA .py` 文件。该文件包含在安装归档中，您也可以通过单击 StorageGRID 设备安装程序中的 * 帮助 * > * 设备安装脚本 * 来访问该文件。

> 此操作步骤 适用于在使用命令行界面方面具有一定经验的高级用户。或者，您也可以使用 StorageGRID 设备安装程序自动执行配置。+使用 StorageGRID 设备安装程序自动配置设备

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 要获得有关脚本语法的一般帮助以及查看可用参数列表，请输入以下内容：

```
configure-sga.py --help
```

`configure-sGa.py` 脚本使用五个子命令：

- **高级** 用于高级 StorageGRID 设备交互，包括 BMC 配置和创建包含设备当前配置的 JSON 文件
- `configure` 用于配置 RAID 模式，节点名称和网络参数
- `install` 用于开始 StorageGRID 安装
- `m` 监控 StorageGRID 安装
- `reboot` 用于重新启动设备

如果输入子命令（ advanced ， configure ， install ， monitor 或 reboot ）参数，然后输入 ` -help` 选项，则会收到其他帮助文本，其中提供了有关该子命令中可用选项的更多详细信息： + `configure-sga.py` *`subcommand`* `-help`

3. 要确认设备节点的当前配置，请输入以下内容，其中 ` *SGA-install-IP*` 是设备节点的任一 IP 地址： + `configure-sga.py configure` *`SGA-install-IP`*

结果将显示设备的当前 IP 信息，包括主管理节点的 IP 地址以及有关管理，网格和客户端网络的信息。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
```

```
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4

        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
```

```
                172.18.0.0/21
                192.168.0.0/21
    MTU:        1500

  Admin Network
    CIDR:       10.224.2.30/21 (Static)
    MAC:        00:80:E5:29:70:F4
    Gateway:    10.224.0.1
    Subnets:    10.0.0.0/8
                172.19.0.0/16
                172.21.0.0/16
    MTU:        1500

  Client Network
    CIDR:       47.47.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:89
    Gateway:    47.47.0.1
    MTU:        2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. 如果需要更改当前配置中的任何值，请使用 `configure` 子命令对其进行更新。例如，如果要将设备用于连接到主管理节点的 IP 地址更改为 `172.16.2.99` ，请输入以下内容： + `configure-sga.py configure -admin-IP 172.16.2.99 sGA-install-ip`
5. 如果要将设备配置备份到 JSON 文件，请使用 `advanced` 和 `backup-file` 子命令。例如，如果要将 IP 地址为 ` SGA-install-ip_` 的设备配置备份到名为 `appliance-SG1000.json` 的文件中，请输入以下命令： + `configure-sga.py advanced -backup-file appliance-SG1000.json SGA-install-IP`

   包含配置信息的 JSON 文件将写入执行脚本的同一目录。

   > 检查生成的 JSON 文件中的顶级节点名称是否与设备名称匹配。请勿对此文件进行任何更改，除非您是经验丰富的用户并全面了解 StorageGRID API 。

6. 如果对设备配置满意，请使用 `install` 和 `monitor` 子命令安装此设备： + `configure-sga.py install -monitor sGA-install-ip`
7. 如果要重新启动设备，请输入以下内容： + `configure-sga.py reboot sGA-install-ip`

自动配置 **StorageGRID**

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	Description
`configure-storaggrid.py`	用于自动配置的 Python 脚本
`configure-storaggrid.sample.json`	用于脚本的示例配置文件
`configure-storaggrid.blank.json`	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

关于此任务

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

> 您也可以使用网格管理器或安装 API 配置系统。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如： + `cd StorageGRID-Webscale -version/platform`

   其中，` *platform*` 是 `dEBS` ， `rpms` 或 `vSphere` 。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完成后

在配置过程中会生成一个恢复包 ` .zip` 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 `passwords.txt` 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

安装 **REST API** 概述

StorageGRID 提供了两个用于执行安装任务的 REST API： StorageGRID 安装 API 和 StorageGRID 设备安装程序 API 。

这两个 API 都使用 Swagger 开源 API 平台来提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 **API**

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。
- **recovery-package** —下载恢复软件包的操作。
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

StorageGRID 设备安装程序 API

StorageGRID 设备安装程序 API 可通过 HTTPS 从 ` Controller_IP_ ： 8443` 访问。

要访问 API 文档，请转到设备上的 StorageGRID 设备安装程序，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 设备安装程序 API 包括以下部分：

- * 克隆 * —用于配置和控制节点克隆的操作。
- * 加密 * —用于管理加密和查看加密状态的操作。
- * 硬件配置 * —用于在连接的硬件上配置系统设置的操作。
- * 安装 * —用于开始设备安装和监控安装状态的操作。
- * 网络连接 * - 与 StorageGRID 设备的网格，管理和客户端网络配置以及设备端口设置相关的操作。
- * 设置 * —用于帮助初始设备安装设置的操作，包括请求获取有关系统的信息并更新主管理节点 IP 。
- * 支持 * —用于重新启动控制器和获取日志的操作。
- * 升级 * —与升级设备固件相关的操作。
- **uploadsg** —用于上传 StorageGRID 安装文件的操作。

硬件安装故障排除（ SG5700 ）

如果您在安装期间遇到问题，查看与硬件设置和连接问题相关的故障排除信息可能会很有帮助。

硬件设置似乎挂起（ SG5700 ）

如果硬件故障或布线错误导致 E5700SG 控制器无法完成启动处理，则 StorageGRID 设备安装程序可能不可用。

步骤

1. 查看七段显示器上的代码。

   在启动期间初始化硬件时，两个七段显示一系列代码。硬件成功启动后，七段显示会为每个控制器显示不同的代码。

2. 查看 E5700SG 控制器的七段显示屏上的代码。

   > 安装和配置需要一些时间。某些安装阶段在几分钟内不会向 StorageGRID 设备安装程序报告更新。

   如果发生错误，七段显示屏将按顺序闪烁，例如， "he" 。

3. 要了解这些代码的含义，请参见以下资源：

控制器	参考
E5700SG 控制器	• " s5700SG 控制器上的状态指示符 " • "`错误：与 SANtricity OS 软件同步时出错` "
E2800 控制器	_E5700 和 E2800 系统监控指南 _ • 注： * 为 E 系列 E5700 控制器描述的代码不适用于设备中的 E5700SG 控制器。

4. 如果无法解决问题描述 问题，请联系技术支持。

相关信息

E5700SG 控制器上的状态指示灯

he error： Error synchronating with SANtricity OS Software

"NetApp E 系列系统文档站点"

he error： Error synchronating with SANtricity OS Software

如果 StorageGRID 设备安装程序无法与 SANtricity 操作系统软件同步，则计算控制器上的七段显示会显示一个错误代码。

关于此任务

如果显示错误代码，请执行此更正操作。

步骤

1. 检查两个控制器之间的两根互连缆线，并确认缆线和 SFP+ 收发器已牢固连接。
2. 根据需要，更换一根或两根缆线或 SFP+ 收发器，然后重试。
3. 如果无法解决问题描述 问题，请联系技术支持。

对连接问题进行故障排除（ **SG5700** ）

如果您在 StorageGRID 设备安装期间遇到连接问题，应执行列出的更正操作步骤。

无法连接到设备

如果无法连接到设备，则可能存在网络问题描述 ，或者硬件安装可能未成功完成。

步骤

1. 如果无法连接到 SANtricity 系统管理器：
   a. 尝试使用管理网络上 E2800 控制器的 IP 地址对设备执行 ping 操作，以查看 SANtricity System Manager： + ` * ping *E2800_Controller_IP**`
   b. 如果 ping 未收到任何响应，请确认您使用的 IP 地址正确无误。

      使用 E2800 控制器上管理端口 1 的 IP 地址。

c. 如果 IP 地址正确，请检查设备布线和网络设置。

   如果无法解决问题描述 问题，请联系技术支持。

d. 如果 ping 成功，请打开 Web 浏览器。

e. 输入 SANtricity 系统管理器的 URL： + ` * https://*E2800_Controller_IP*`

   此时将显示 SANtricity 系统管理器的登录页面。

2. 如果无法连接到 E5700SG 控制器：

   a. 尝试使用 E5700SG 控制器的 IP 地址对设备执行 ping 操作： + ` * ping *E5700SG_Controller_IP*`

   b. 如果 ping 未收到任何响应，请确认您使用的 IP 地址正确无误。

      您可以使用网格网络，管理网络或客户端网络上设备的 IP 地址。

   c. 如果 IP 地址正确，请检查设备布线， SFP 收发器和网络设置。

      如果无法解决问题描述 问题，请联系技术支持。

   d. 如果 ping 成功，请打开 Web 浏览器。

   e. 输入 StorageGRID 设备安装程序的 URL： + ` * https://*E5700SG_Controller_IP*:8443*`

      此时将显示主页页面。

在 **StorageGRID** 设备安装程序运行期间重新启动控制器

在 StorageGRID 设备安装程序运行期间，您可能需要重新启动计算控制器。例如，如果安装失败，您可能需要重新启动控制器。

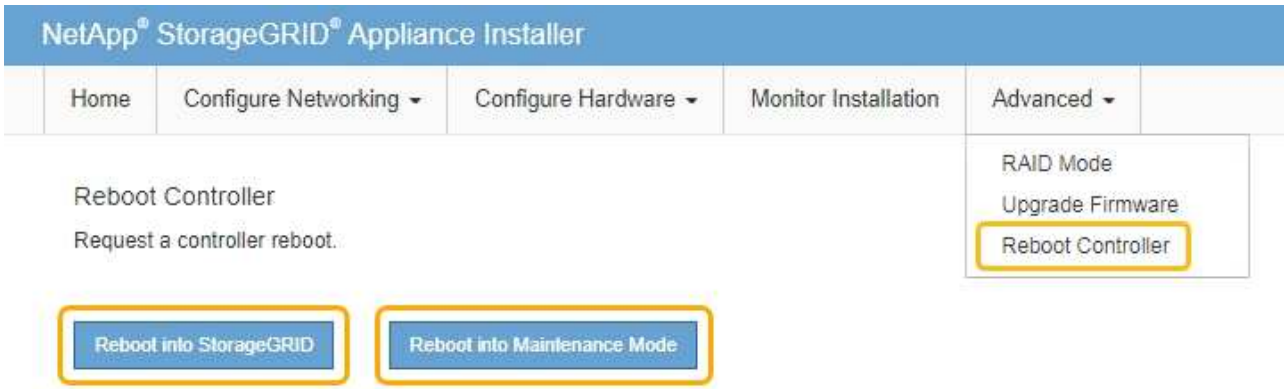
关于此任务

只有当计算控制器运行 StorageGRID 设备安装程序时，此操作步骤 才适用。安装完成后，此步骤将不再起作用，因为 StorageGRID 设备安装程序不再可用。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



控制器将重新启动。

维护 SG5700 设备

您可能需要升级 E2800 控制器上的 SANtricity 操作系统软件，更改 E5700SG 控制器的以太网链路配置，更换 E2800 控制器或 E5700SG 控制器或更换特定组件。本节中的过程假定设备已部署为 StorageGRID 系统中的存储节点。

将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

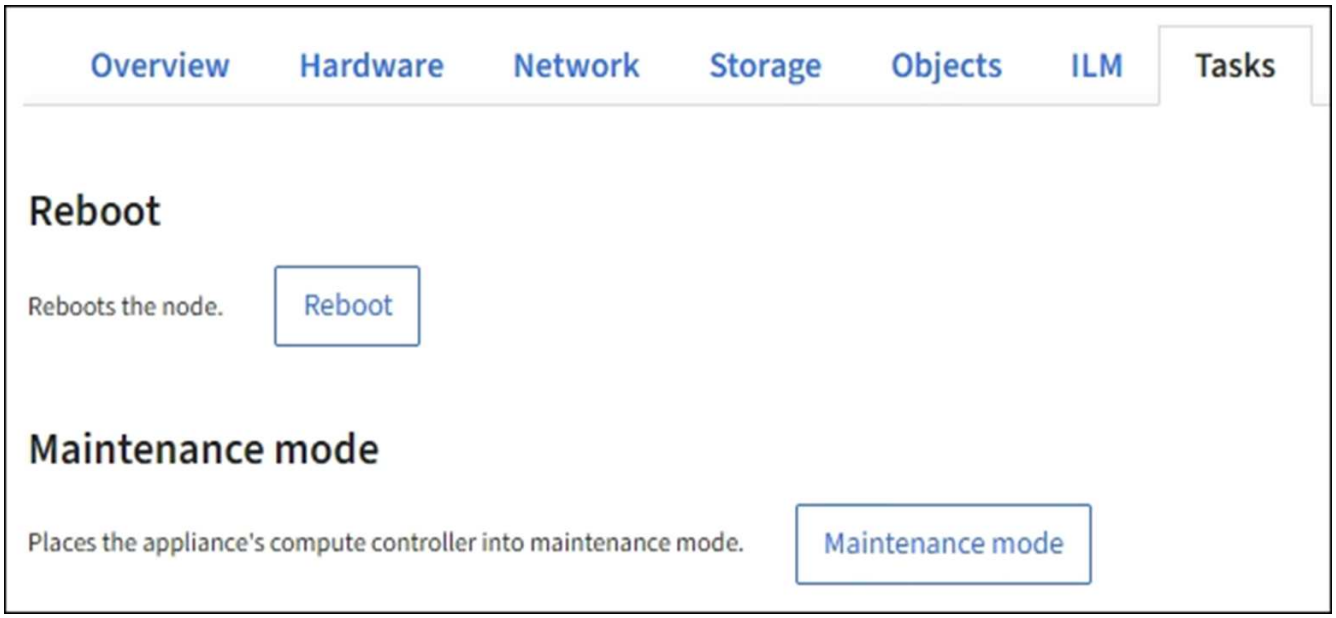
关于此任务

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

> 处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

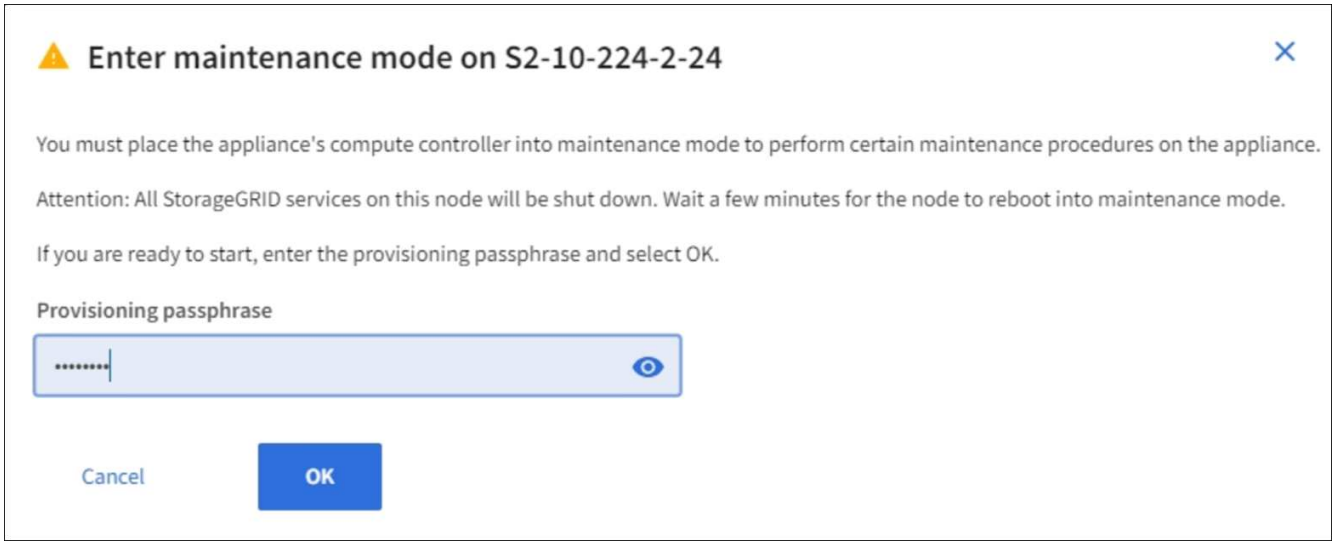
步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面的树视图中，选择设备存储节点。
3. 选择 * 任务 * 。



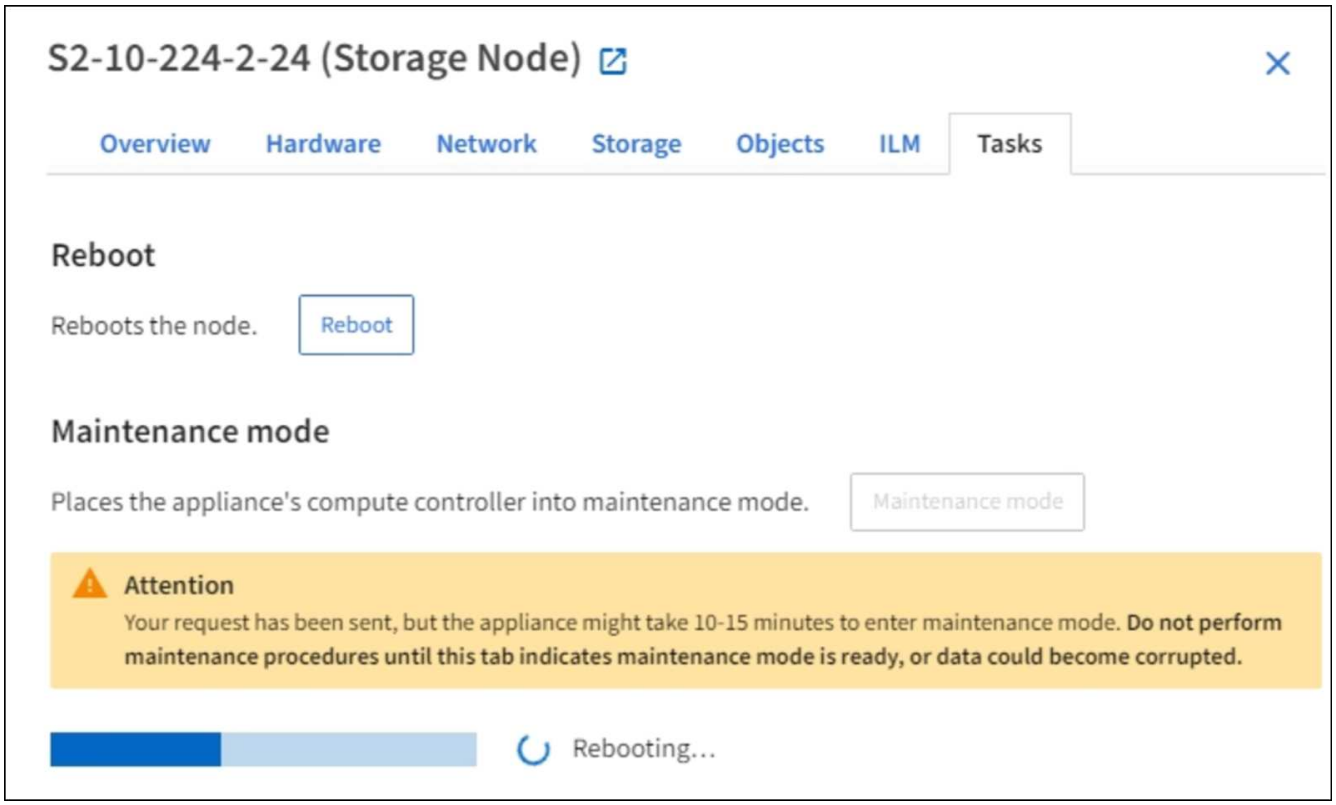
4. 选择 * 维护模式 * 。

   此时将显示确认对话框。

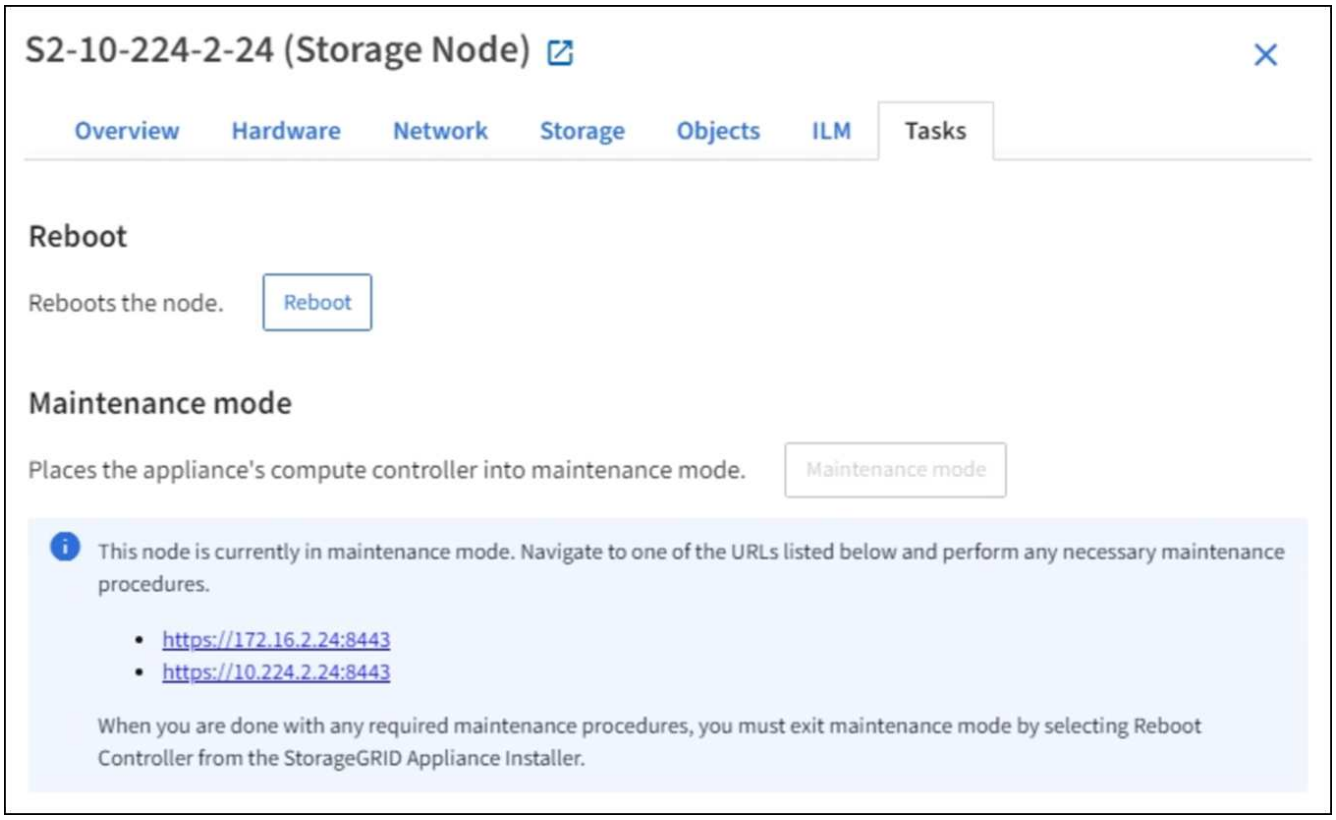


5. 输入配置密码短语，然后选择 * 确定 * 。

   进度条和一系列消息（包括 " 已发送请求 " ， " 正在停止 StorageGRID " 和 " 正在重新启动 " ）表示设备正在完成进入维护模式的步骤。



设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL 。



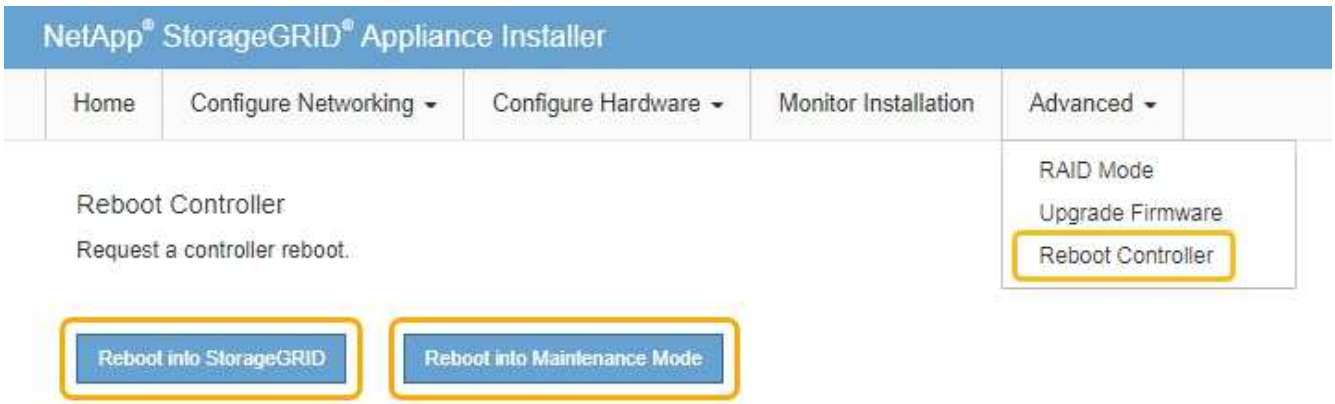
6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL 。

   如果可能，请使用包含设备管理网络端口 IP 地址的 URL 。

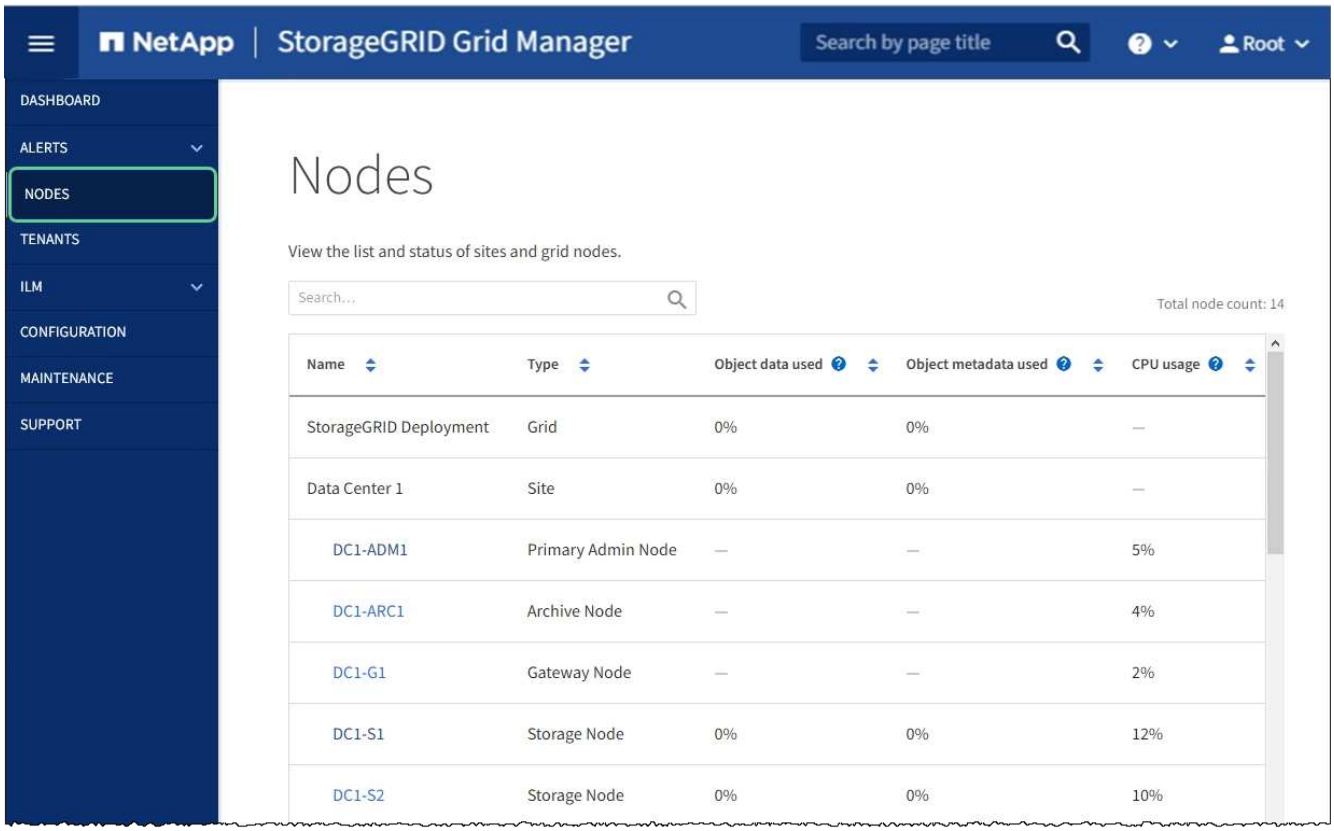
如果您直接连接到设备的管理端口，请使用 ` https://169.254.0.1:8443` 访问 StorageGRID 设备安装程序页面。

7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。

8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



升级存储控制器上的 **SANtricity** 操作系统

为了确保存储控制器能够以最佳方式运行，您必须升级到适用于您的 StorageGRID 设备的最新 SANtricity 操作系统维护版本。请参考 NetApp 互操作性表工具（ IMT ）来确定应使用的版本。如果需要帮助，请联系技术支持。

- 如果存储控制器使用的是 SANtricity OS 08.42.20.00 （ 11.42 ）或更高版本，请使用网格管理器执行升级。

  使用网格管理器升级存储控制器上的 SANtricity 操作系统

- 如果存储控制器使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ），请使用维护模式执行升级。

  使用维护模式升级 E2800 控制器上的 SANtricity 操作系统

相关信息

"NetApp 互操作性表工具"

"NetApp下载：StorageGRID 设备"

监控和故障排除

使用网格管理器升级存储控制器上的 **SANtricity** 操作系统

对于当前使用 SANtricity OS 08.42.20.00 （ 11.42 ）或更高版本的存储控制器，您必须使用网格管理器应用升级。

您需要的内容

- 您已查阅 NetApp 互操作性表工具（ IMT ）以确认用于升级的 SANtricity 操作系统版本与您的设备兼容。
- 您具有维护或 root 访问权限。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有配置密码短语。
- 您可以访问 SANtricity 操作系统的 NetApp 下载页面。

关于此任务

在完成 SANtricity 操作系统升级过程之前，您无法执行其他软件更新（ StorageGRID 软件升级或修补程序）。如果您尝试在 SANtricity 操作系统升级过程完成之前启动修补程序或 StorageGRID 软件升级，则系统会重定向到 SANtricity 操作系统升级页面。

只有在 SANtricity 操作系统升级成功应用于已选择进行升级的所有适用节点之后，操作步骤 才会完成。在每个节点上（按顺序）加载 SANtricity 操作系统可能需要 30 分钟以上的时间，并且最多需要 90 分钟来重新启动每个 StorageGRID 存储设备。

只有在使用网格管理器执行升级时，以下步骤才适用。如果设备中的存储控制器使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ），则无法使用网格管理器进行升级。

此操作步骤 会自动将 NVSRAM 升级到与 SANtricity 操作系统升级相关的最新版本。您无需应用单独的 NVSRAM 升级文件。

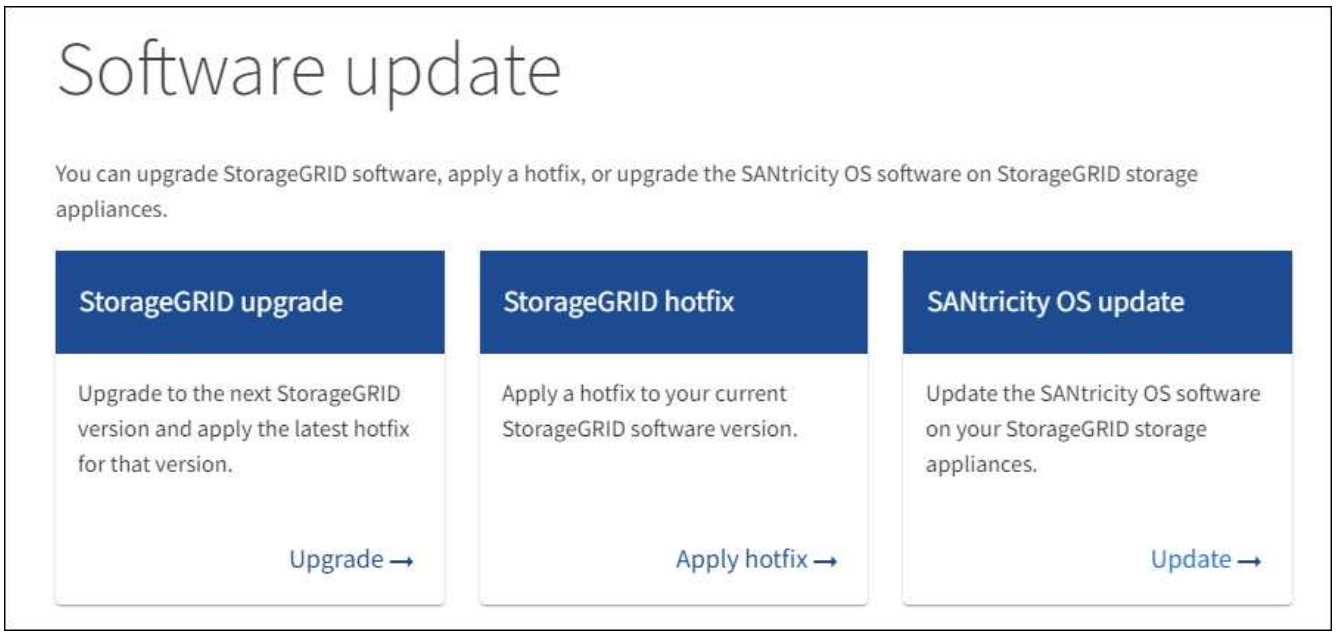
步骤

1. 【下载 _SANtricity 操作系统】从 NetApp 支持站点下载新的 SANtricity 操作系统软件文件。

   请务必为存储控制器选择 SANtricity 操作系统版本。

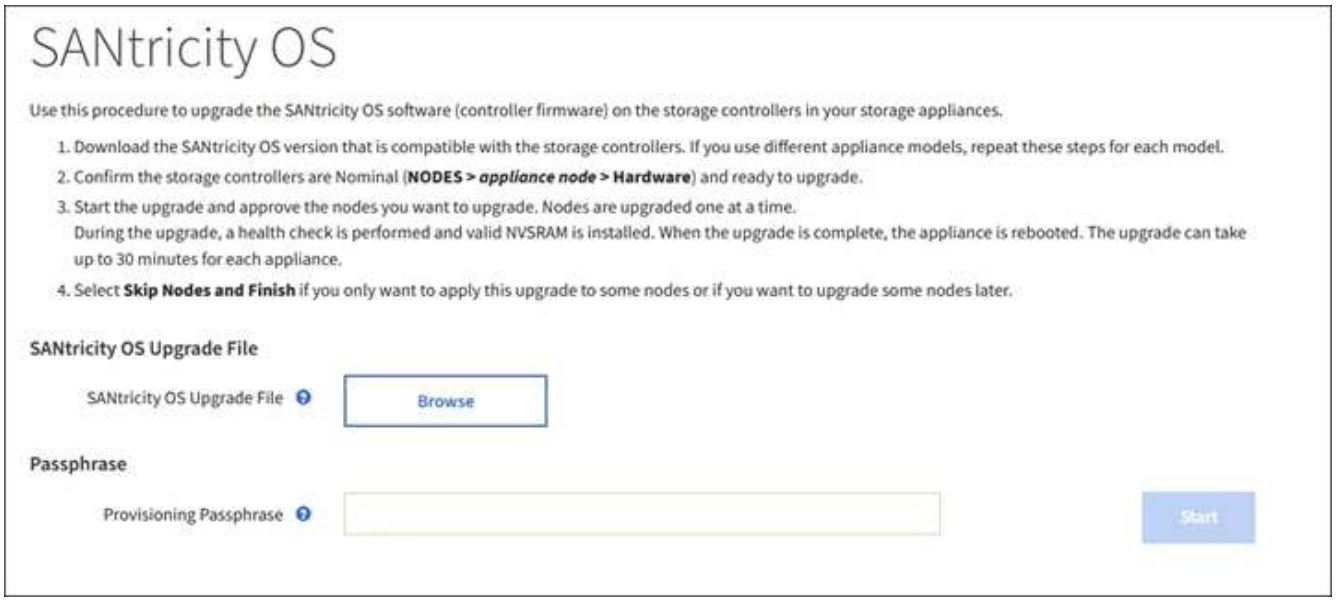
   "NetApp下载：StorageGRID 设备"

2. 选择 * 维护 * > * 系统 * > * 软件更新 * 。



3. 在 SANtricity OS update 部分中，选择 * 更新 * 。

   此时将显示 SANtricity OS 升级页面。



4. 选择从 NetApp 支持站点下载的 SANtricity OS 升级文件。

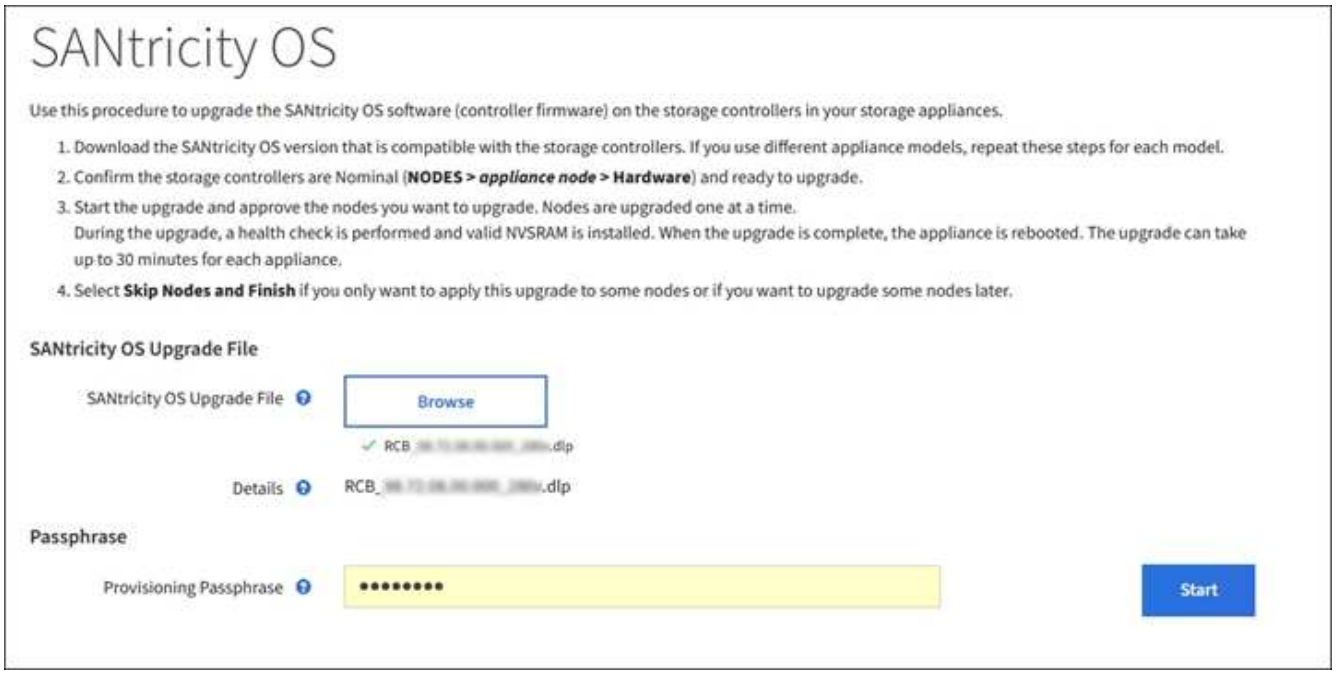
   a. 选择 * 浏览 * 。
   b. 找到并选择文件。
   c. 选择 * 打开 * 。

      已上传并验证此文件。验证过程完成后，文件名会显示在 * 浏览 * 按钮旁边。

      请勿更改文件名，因为它是验证过程的一部分。

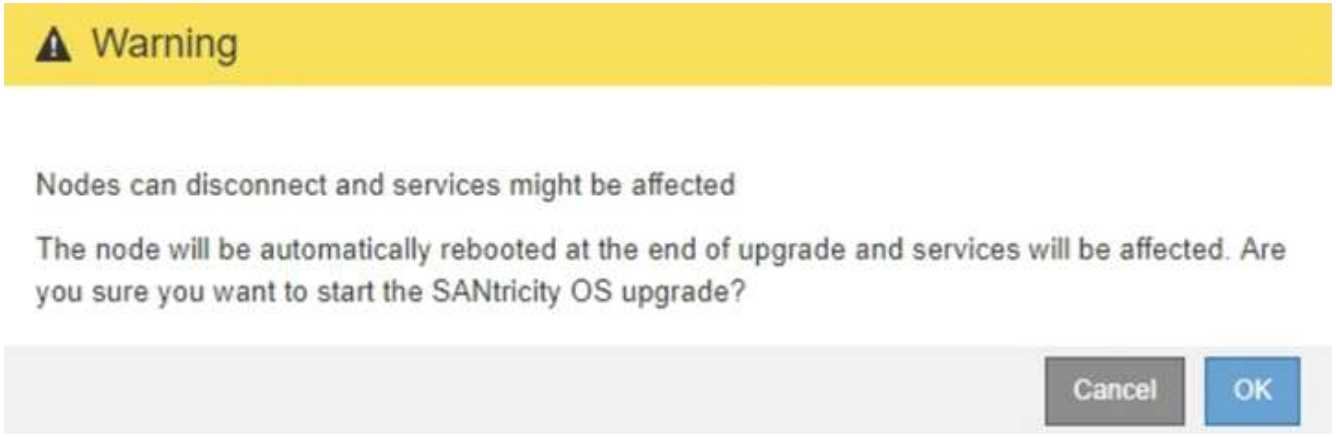
5. 输入配置密码短语。

   已启用 * 开始 * 按钮。



6. 选择 * 开始 * 。

此时将显示一个警告框，指出在重新启动已升级的节点上的服务时，浏览器的连接可能会暂时断开。



7. 选择 * 确定 * 将 SANtricity 操作系统升级文件暂存到主管理节点。

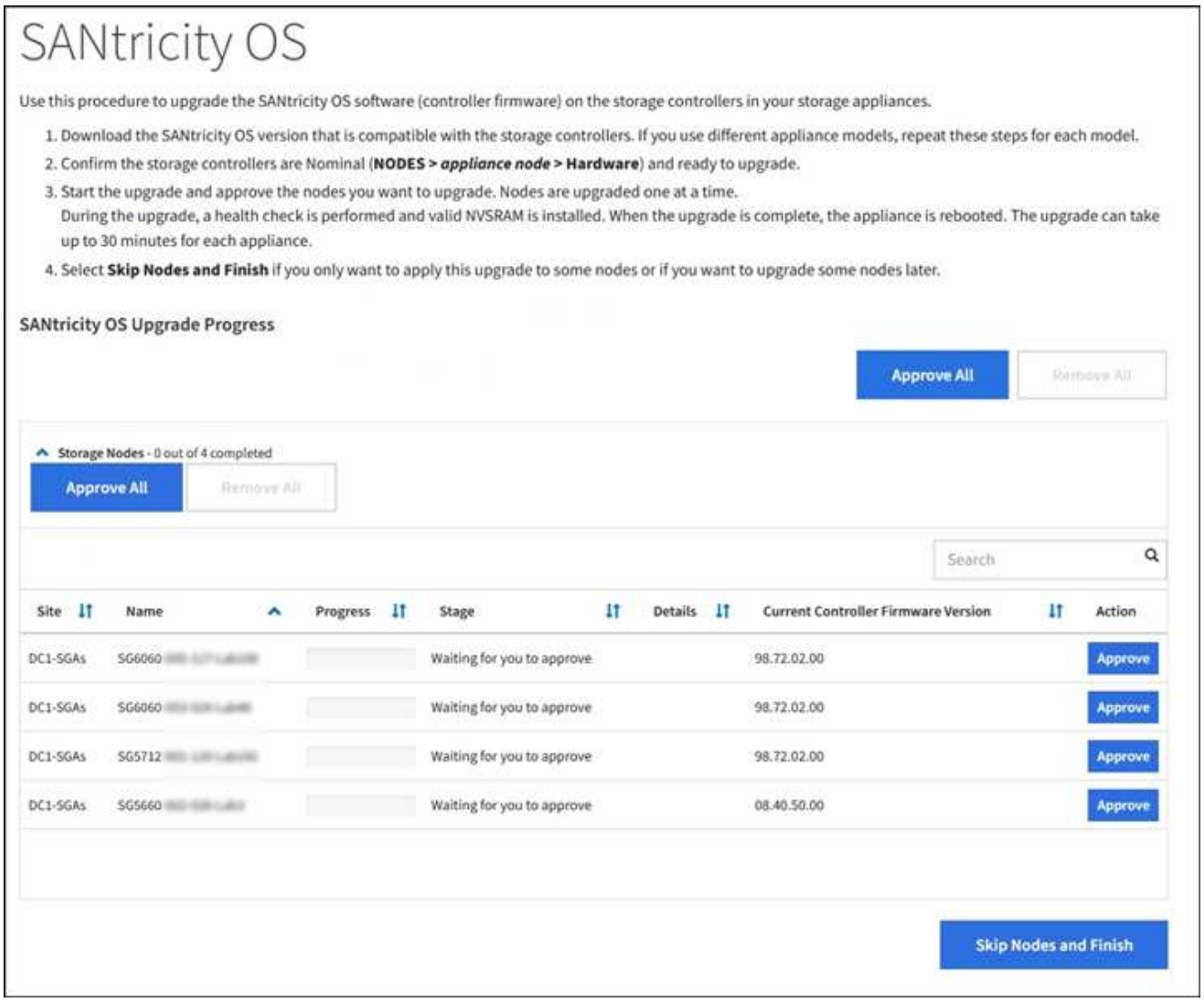
SANtricity 操作系统升级开始时：

a. 运行状况检查已运行。此过程会检查是否没有节点的状态为 "Needs Attention （需要注意） " 。

如果报告了任何错误，请解决这些错误并再次选择 * 启动 * 。

b. 此时将显示 SANtricity 操作系统升级进度表。此表显示了网格中的所有存储节点以及每个节点的当前升级阶段。

此表显示了所有设备存储节点。不会显示基于软件的存储节点。对于需要升级的所有节点，请选择 * 批准 * 。



8. 或者，也可以按 * 站点 * ， * 名称 * ， * 进度 * ， * 阶段 * ， * 详细信息 * 按升序或降序对节点列表进行排序。 或 * 当前控制器固件版本 * 。或者，在 * 搜索 * 框中输入一个术语以搜索特定节点。

   您可以使用此部分右下角的左箭头和右箭头滚动浏览节点列表。

9. 批准已准备好添加到升级队列的网格节点。相同类型的已批准节点将一次升级一个。

   请勿批准设备存储节点的 SANtricity 操作系统升级，除非您确定该节点已做好停止和重新启动的准备。在某个节点上批准 SANtricity 操作系统升级后，该节点上的服务将停止，升级过程将开始。稍后，当节点完成升级后，设备节点将重新启动。对于与节点通信的客户端，这些操作可能会导致发生原因 服务中断。

   - 选择 * 全部批准 * 按钮之一，将所有存储节点添加到 SANtricity 操作系统升级队列。

     如果节点升级顺序非常重要，请一次批准一个节点或一组节点，并等待每个节点完成升级，然后再批准下一个节点。

   - 选择一个或多个 * 批准 * 按钮将一个或多个节点添加到 SANtricity OS 升级队列。

     选择 * 批准 * 后，升级过程将确定是否可以升级此节点。如果某个节点可以升级，则会将其添加到升级

队列中。

对于某些节点，不会有意应用选定的升级文件，您可以在不升级这些特定节点的情况下完成升级过程。有意未升级的节点会显示完成阶段（已尝试升级），并在详细信息列中列出未升级此节点的原因。

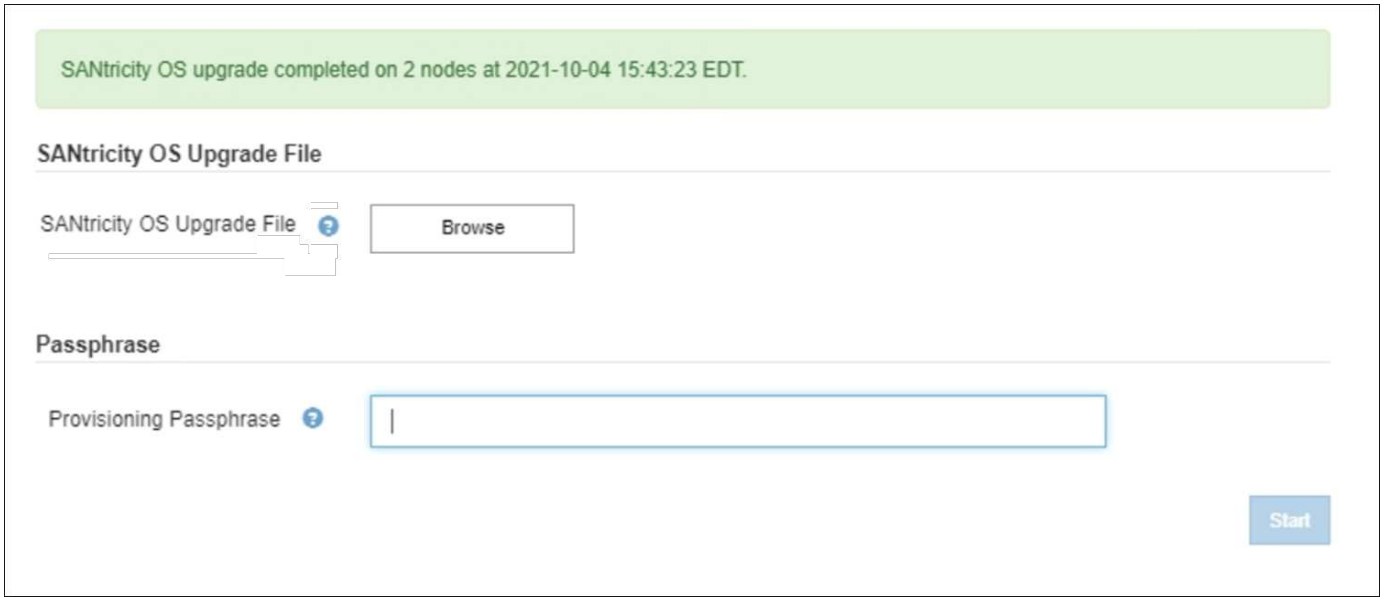
10. 如果需要从 SANtricity 操作系统升级队列中删除一个或所有节点，请选择 * 删除 * 或 * 全部删除 * 。

    当此阶段超过已排队时， * 删除 * 按钮将处于隐藏状态，您无法再从 SANtricity 操作系统升级过程中删除此节点。

11. 等待 SANtricity 操作系统升级应用于每个批准的网格节点。

    - 如果在应用 SANtricity 操作系统升级期间任何节点显示错误阶段，则此节点的升级将失败。在技术支持的协助下，您可能需要将设备置于维护模式才能进行恢复。
    - 如果节点上的固件版本太旧，无法使用网格管理器进行升级，则节点将显示错误阶段并提供详细信息："`您必须使用维护模式升级此节点上的 SANtricity OS 。请参见适用于您的设备的安装和维护说明。升级后，您可以使用此实用程序进行将来的升级。` 要解决此错误，请执行以下操作：
      i. 使用维护模式升级显示 " 错误 " 阶段的节点上的 SANtricity OS 。
      ii. 使用网格管理器重新启动并完成 SANtricity 操作系统升级。

    在所有已批准的节点上完成 SANtricity 操作系统升级后， SANtricity 操作系统升级进度表将关闭，绿色横幅将显示 SANtricity 操作系统升级完成的日期和时间。



1. 如果节点无法升级，请记下 "Details" 列中显示的原因并采取相应的措施：
   - " s存储节点已升级。 " 无需执行进一步操作。
   - "`SANtricity 操作系统升级不适用于此节点。` " 此节点没有可由 StorageGRID 系统管理的存储控制器。完成升级过程，而不升级显示此消息的节点。
   - "`SANtricity OS 文件与此节点不兼容。` " 节点所需的 SANtricity 操作系统文件与您选择的文件不同。完成当前升级后，下载适用于此节点的正确 SANtricity OS 文件，然后重复升级过程。

只有在所有列出的存储节点上批准 SANtricity 操作系统升级后， SANtricity 操作系统升级过程才会完成。

1. 如果要结束节点批准并返回到 SANtricity OS 页面以允许上传新的 SANtricity OS 文件，请执行以下操作：

   a. 选择 * 跳过节点并完成 * 。

      此时将显示一条警告，询问您是否确实要在不升级所有节点的情况下完成升级过程。

   b. 选择 * 确定 * 返回到 * SANtricity OS* 页面。

   c. 准备好继续批准节点后，请转至 下载 SANtricity 操作系统 重新启动升级过程。

   > 已批准并升级的节点仍保持升级状态，而不会出现错误。

2. 对处于完成阶段且需要其他 SANtricity 操作系统升级文件的所有节点重复此升级操作步骤 。

   > 对于状态为 "Needs Attenance" 的任何节点，请使用维护模式执行升级。

   > 重复升级操作步骤 时，您必须批准先前升级的节点。

相关信息

"NetApp 互操作性表工具"

使用维护模式升级 E2800 控制器上的 SANtricity 操作系统

使用维护模式升级 **E2800** 控制器上的 **SANtricity** 操作系统

对于当前使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ）的存储控制器，您必须使用维护模式操作步骤 来应用升级。

您需要的内容

- 您已查阅 NetApp 互操作性表工具（ IMT ）以确认用于升级的 SANtricity 操作系统版本与您的设备兼容。
- 您必须将E5700SG控制器置于中 维护模式、中断与E2800控制器的连接。

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

关于此任务

请勿一次在多个 StorageGRID 设备上升级 E 系列控制器中的 SANtricity 操作系统或 NVSRAM 。

> 一次升级多个 StorageGRID 设备可能会导致发生原因 数据不可用，具体取决于您的部署模式和 ILM 策略。

步骤

1. 确认设备已进入 维护模式。
2. 从服务笔记本电脑访问 SANtricity 系统管理器并登录。
3. 将新的 SANtricity OS 软件文件和 NVSRAM 文件下载到管理客户端。

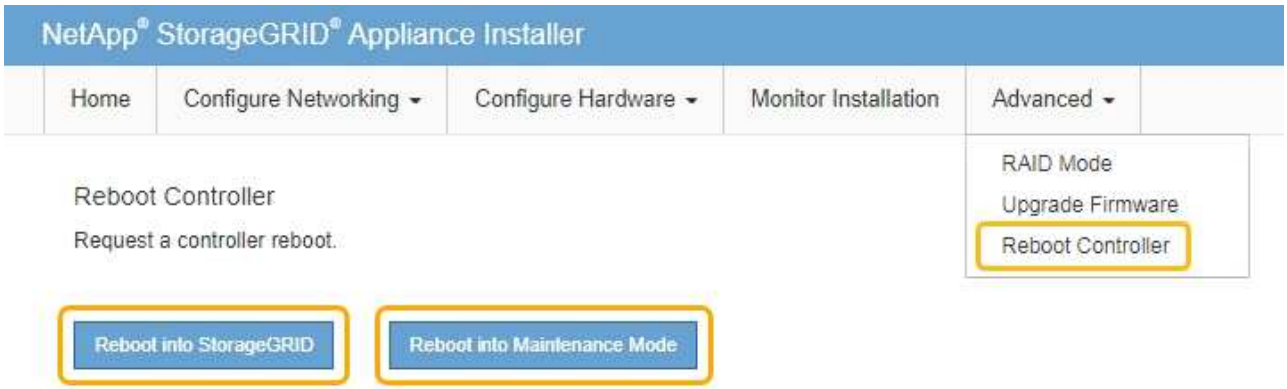
> NVSRAM 是特定于 StorageGRID 设备的。请勿使用标准 NVSRAM 下载。

4. 按照 _E2800 和 E5700 SANtricity 软件和固件升级指南 _ 或 SANtricity 系统管理器联机帮助中的说明升级 E2800 控制器的固件和 NVSRAM 。

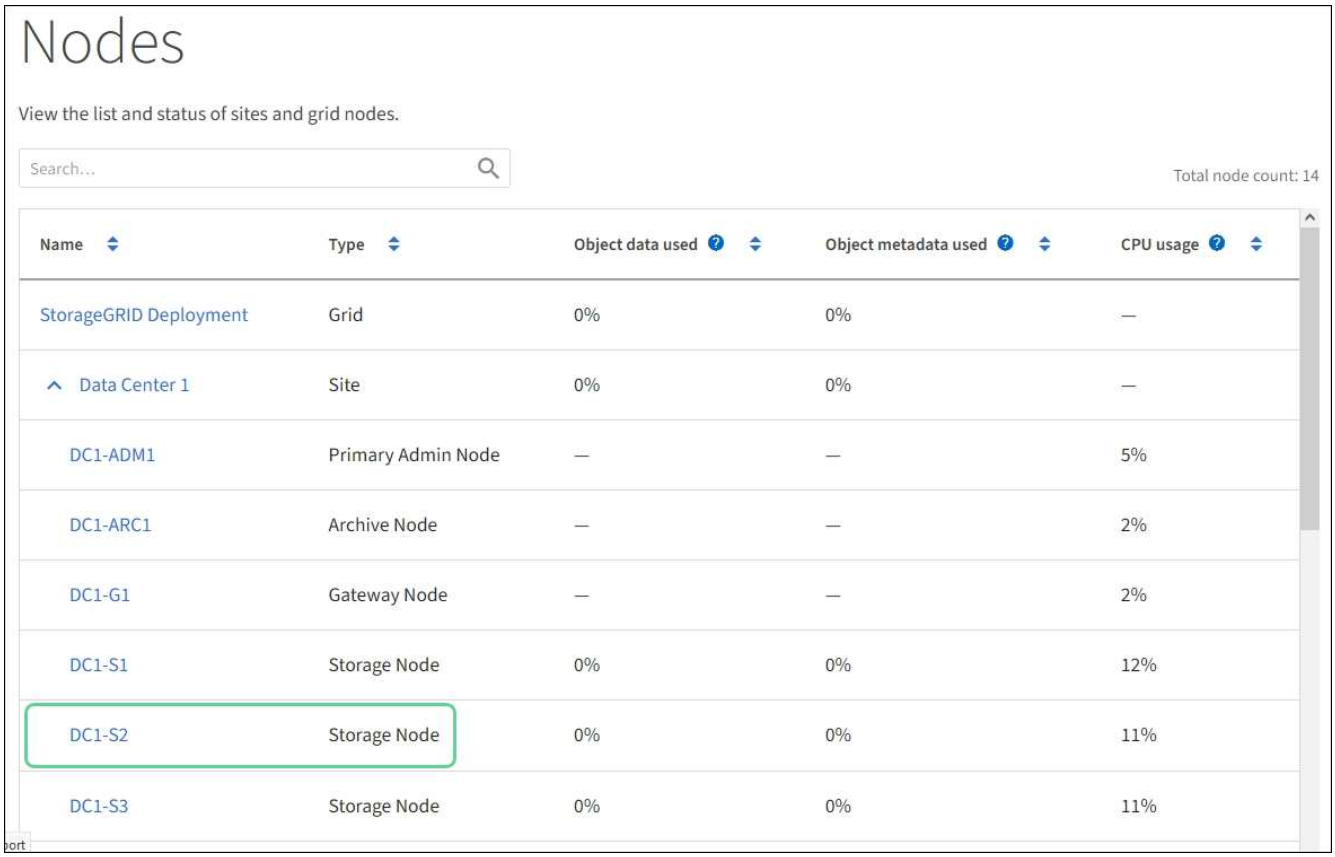
   立即激活升级文件。请勿延迟激活。

5. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



   设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。节点页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

使用网格管理器升级存储控制器上的 SANtricity 操作系统

使用 **SANtricity** 系统管理器升级驱动器固件

您可以升级驱动器固件，以确保具有所有最新功能和错误修复。

您需要的内容

- 存储设备处于最佳状态。
- 所有驱动器均处于最佳状态。
- 您已安装与您的 SANtricity 版本兼容的最新版本 StorageGRID System Manager 。
- 您已拥有 已将 StorageGRID 设备置于维护模式。

> 维护模式会中断与存储控制器的连接，停止所有 I/O 活动并使所有驱动器脱机。

> 请勿一次升级多个 StorageGRID 设备上的驱动器固件。这样做可能会导致发生原因 数据不可用，具体取决于您的部署模式和 ILM 策略。

步骤

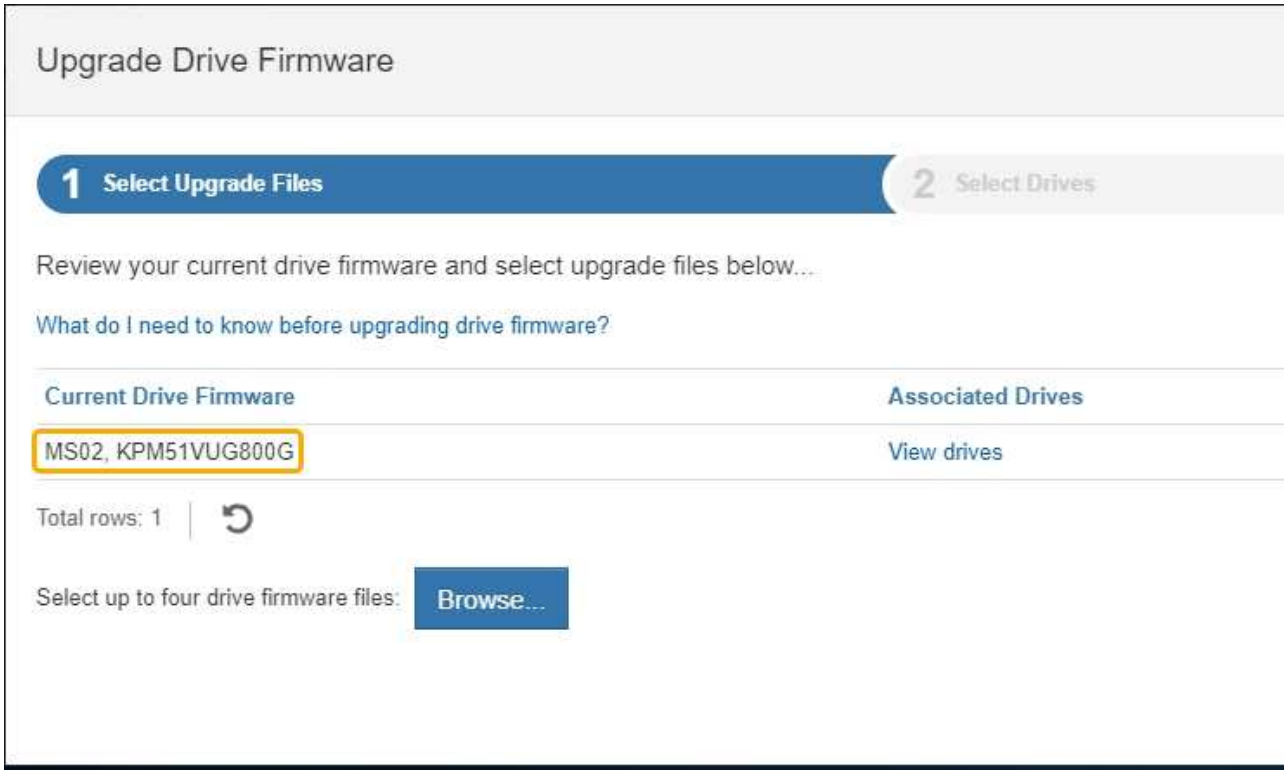
1. 确认此设备已位于中 维护模式。
2. 使用以下方法之一访问 SANtricity System Manager：
   - 使用 StorageGRID 设备安装程序并选择 * 高级 * > * SANtricity 系统管理器 *

◦ 通过浏览到存储控制器 IP： + ` * https://*Storage_Controller_IP*` 来使用 SANtricity 系统管理器

3. 如果需要，输入 SANtricity System Manager 管理员用户名和密码。
4. 验证存储设备中当前安装的驱动器固件版本：
   a. 在 SANtricity 系统管理器中，选择 * 支持 * > * 升级中心 * 。
   b. 在驱动器固件升级下，选择 * 开始升级 * 。

      升级驱动器固件将显示当前安装的驱动器固件文件。

   c. 请在当前驱动器固件列中记下当前驱动器固件版本和驱动器标识符。



      在此示例中：

      - 驱动器固件修订版为 * 。 MS02* 。
      - 驱动器标识符为 * 。 KPM51 VVG800G* 。

   在关联驱动器列中选择 * 查看驱动器 * ，以显示这些驱动器在存储设备中的安装位置。

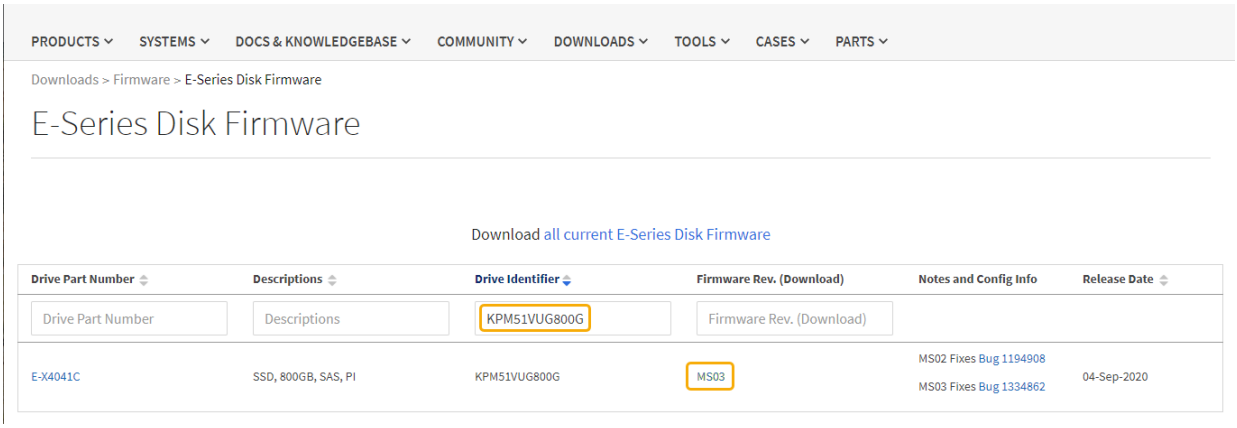
   a. 关闭升级驱动器固件窗口。

5. 下载并准备可用的驱动器固件升级：
   a. 在驱动器固件升级下，选择 * NetApp 支持 * 。
   b. 在 NetApp 支持网站上，选择 * 下载 * 选项卡，然后选择 * E 系列磁盘驱动器固件 * 。

      此时将显示 E 系列磁盘固件页面。

   c. 搜索存储设备中安装的每个 * 驱动器标识符 * ，并验证每个驱动器标识符是否具有最新的固件版本。

- 如果固件版本不是链接，则此驱动器标识符的固件版本为最新。
- 如果为驱动器标识符列出了一个或多个驱动器部件号，则可以对这些驱动器进行固件升级。您可以选择任何链接来下载固件文件。



d. 如果列出了更高版本的固件，请选择固件修订版中的链接（ download ）列以下载包含固件文件的 ` .zip` 归档。

e. 提取（解压缩）从支持站点下载的驱动器固件归档文件。

6. 安装驱动器固件升级：

a. 在 SANtricity 系统管理器的驱动器固件升级下，选择 * 开始升级 * 。

b. 选择 * 浏览 * ，然后选择从支持站点下载的新驱动器固件文件。

驱动器固件文件的文件名类似于 + `D HUC101212CS600_30602291_MS01_2800_0002.DLP`

您最多可以选择四个驱动器固件文件，一次一个。如果多个驱动器固件文件与同一驱动器兼容，则会收到文件冲突错误。确定要用于升级的驱动器固件文件，然后删除另一个驱动器固件文件。

c. 选择 * 下一步 * 。

- 选择驱动器 * 列出了可使用选定固件文件进行升级的驱动器。

  仅显示兼容的驱动器。

为驱动器选择的固件将显示在 * 建议的固件 * 中。如果必须更改此固件，请选择 * 返回 * 。

d. 选择 * 脱机（并行） * 升级。

您可以使用脱机升级方法，因为设备处于维护模式，此时所有驱动器和所有卷的 I/O 活动都将停止。

> 除非您确定设备处于维护模式，否则请勿继续。如果在启动脱机驱动器固件更新之前未将设备置于维护模式，则可能会丢失发生原因 数据。

e. 在表的第一列中，选择要升级的一个或多个驱动器。

最佳实践是，将所有相同型号的驱动器升级到相同的固件修订版。

f. 选择 * 开始 * ，然后确认要执行升级。

如果需要停止升级，请选择 * 停止 * 。当前正在进行的所有固件下载均已完成。已取消所有尚未启动的固件下载。

停止驱动器固件升级可能会导致数据丢失或驱动器不可用。

g. （可选）要查看已升级内容的列表，请选择 * 保存日志 * 。

此日志文件将保存在浏览器的下载文件夹中，名称为 `latest-upgrade-log-timestamp.txt` 。

如果在升级操作步骤期间出现以下任何错误，请采取适当的建议操作。

- * 已分配的驱动器出现故障 *

  出现此故障的一个原因可能是驱动器没有相应的签名。确保受影响的驱动器为授权驱动器。有关详细信息，请联系技术支持。

更换驱动器时，请确保更换驱动器的容量等于或大于要更换的故障驱动器。

您可以在存储阵列接收 I/O 时更换故障驱动器

- * 检查存储阵列 *
  - 确保已为每个控制器分配 IP 地址。
  - 确保连接到控制器的所有缆线均未损坏。
  - 确保所有缆线均已紧密连接。
- * 集成热备用驱动器 *

  必须先更正此错误情况，然后才能升级固件。

- * 卷组不完整 *

  如果一个或多个卷组或磁盘池不完整，则必须更正此错误情况，然后才能升级固件。

- * 当前正在任何卷组上运行的独占操作（后台介质 / 奇偶校验扫描除外） *

  如果正在执行一个或多个独占操作，则必须先完成这些操作，然后才能升级固件。使用 System Manager 监控操作进度。

- * 缺少卷 *

  您必须先更正缺少的卷情况，然后才能升级固件。

- * 任一控制器处于非最佳状态 *

  其中一个存储阵列控制器需要注意。必须先更正此情况，然后才能升级固件。

- 控制器对象图形之间的存储分区信息不匹配 *

  验证控制器上的数据时出错。请联系技术支持以解决此问题描述。

- * SPM 验证数据库控制器检查失败 *

控制器上发生存储分区映射数据库错误。请联系技术支持以解决此问题描述。

- * 配置数据库验证（如果存储阵列的控制器版本支持） *

  控制器上发生配置数据库错误。请联系技术支持以解决此问题描述。

- * 与 MEL 相关的检查 *

  请联系技术支持以解决此问题描述。

- * 在过去 7 天内报告了 10 个以上的 DDN 信息性或严重 MEL 事件 *

  请联系技术支持以解决此问题描述。

- * 过去 7 天报告了 2 页以上的 2C 严重 MEL 事件 *

  请联系技术支持以解决此问题描述。

- * 过去 7 天报告了 2 个以上的 " 降级驱动器通道 " 严重 MEL 事件 *

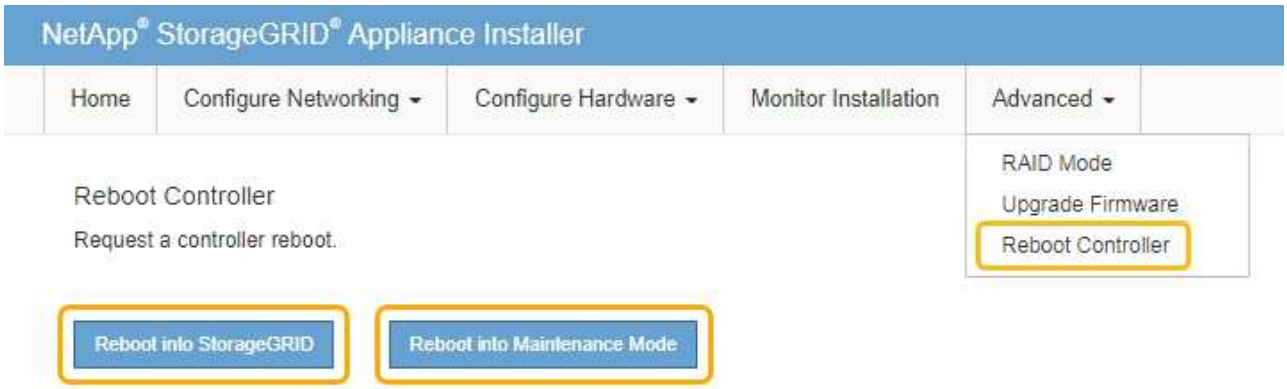
  请联系技术支持以解决此问题描述。

- * 过去 7 天内 4 个以上的关键 MEL 条目 *

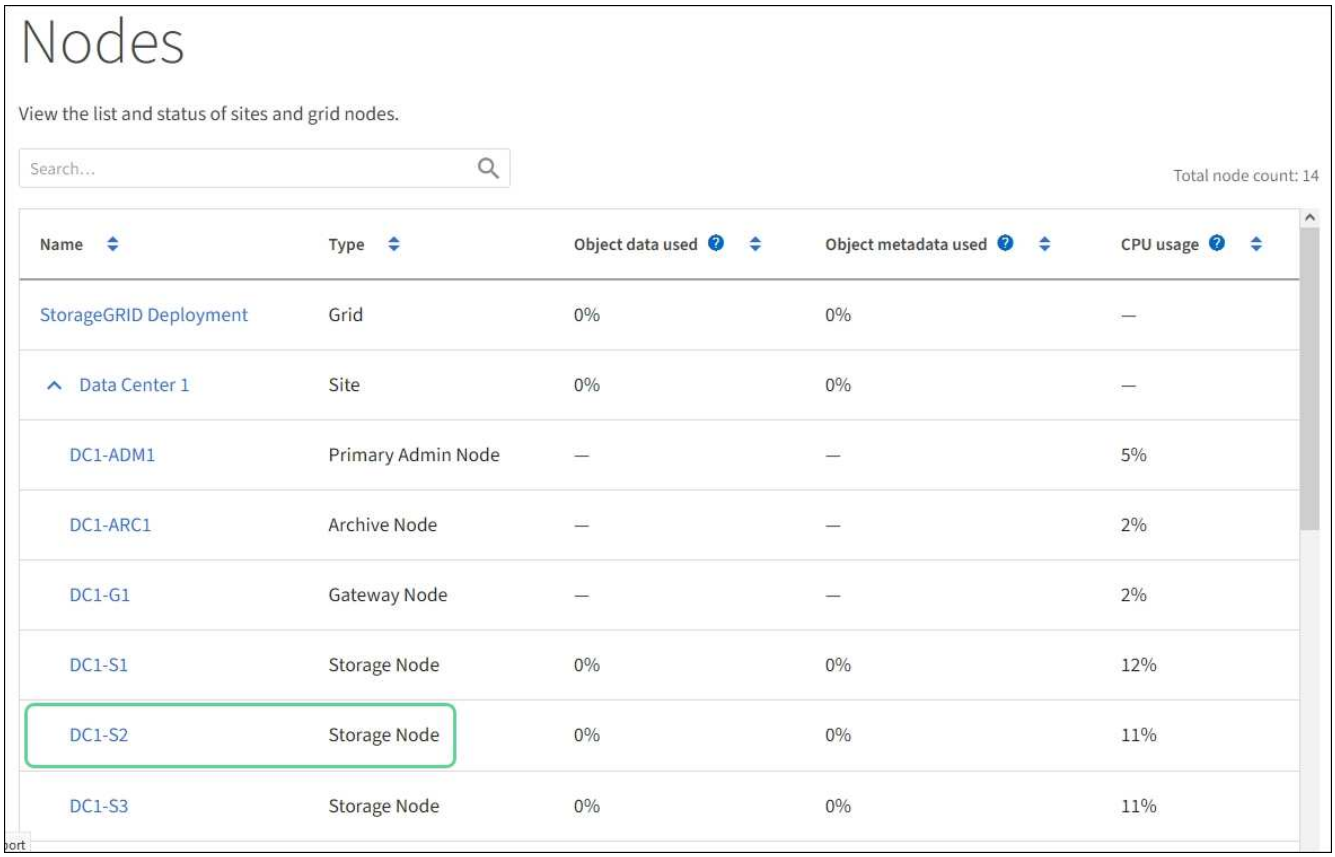
  请联系技术支持以解决此问题描述。

7. 。如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。节点页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

升级存储控制器上的 SANtricity 操作系统

更换**SG5700**中的**E2800**系列存储控制器

如果E2800系列控制器运行不正常或出现故障、您可能需要更换它。

关于此任务

- 您的更换控制器的部件号与要更换的控制器相同。

  请勿依赖 E 系列说明来更换 StorageGRID 设备中的控制器，因为这些过程是不同的。

- 您可以通过标签来识别连接到控制器的每个缆线。
- 如果所有驱动器均已安全保护、您已查看单工E2800系列控制器更换操作步骤 中的步骤。 其中包括从NetApp支持站点下载并安装E系列SANtricity 存储管理器、然后在更换控制器后使用企业管理窗口(EMW)解锁安全驱动器。

  只有在使用已保存的密钥解锁驱动器后，才能使用此设备。

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

关于此任务

您可以通过以下两种方式确定控制器箱是否发生故障：

- SANtricity System Manager 中的恢复 Guru 可指示您更换控制器。
- 控制器上的琥珀色警示 LED 亮起，表示控制器出现故障。

更换控制器后，无法访问设备存储节点。如果E2800系列控制器运行正常、您可以 将 E5700SG 控制器置于维护模式。

更换控制器时，您必须从原始控制器中取出电池，然后将其安装到替代控制器中。在某些情况下，您可能还需要从原始控制器中卸下主机接口卡，并将其安装在替代控制器中。

大多数设备型号中的存储控制器不包括主机接口卡（ HIC ）。

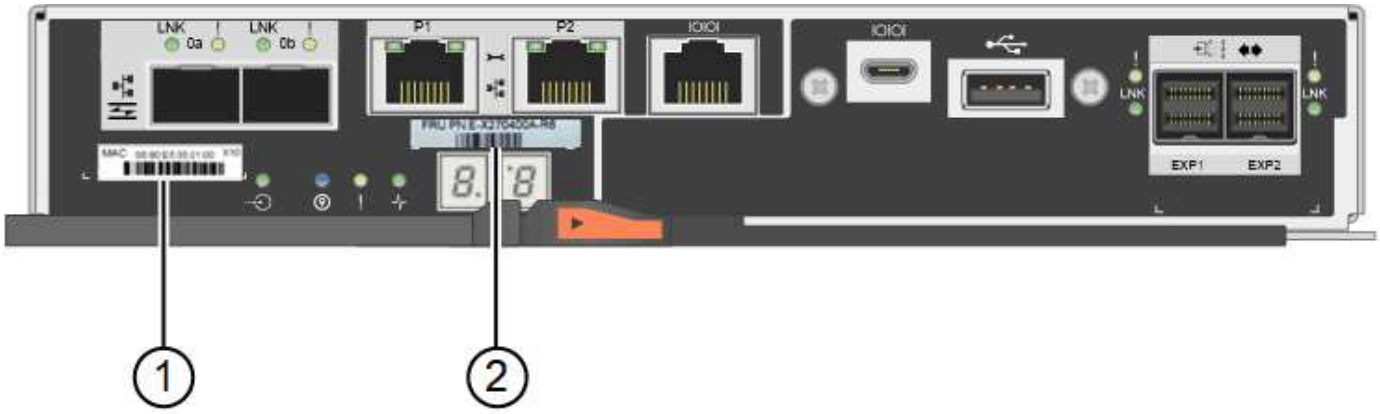
此任务包含以下部分：

1. 准备
2. 使控制器脱机
3. 删除控制器
4. 将电池移至新控制器
5. 如果需要、将HIC移至新控制器
6. 更换控制器

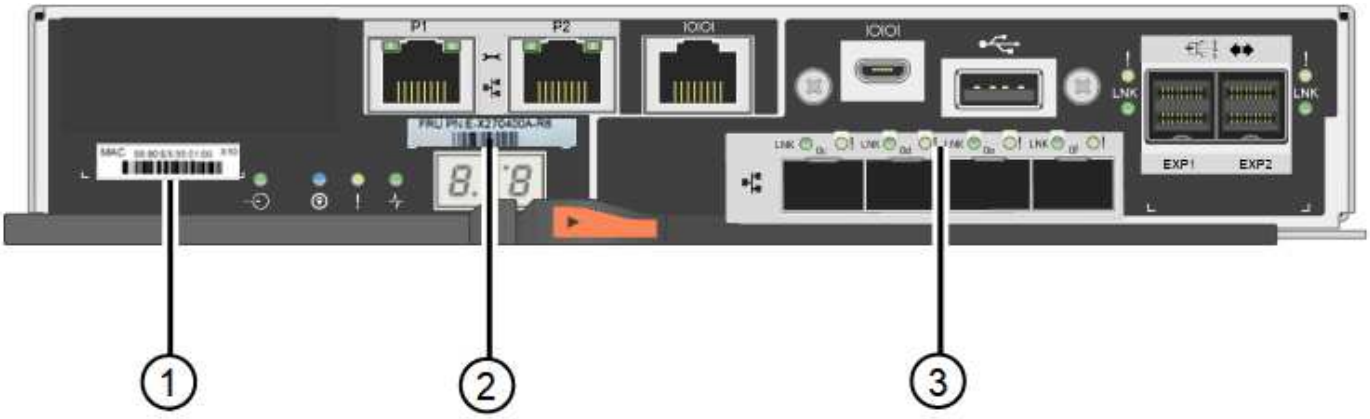
准备

这些图显示了E2800A控制器和E2800B控制器。用于更换E2800系列控制器和EF570控制器的操作步骤 是相同的。

- E2800A存储控制器*



- E2800B存储控制器*



Label	组件	Description
1.	MAC 地址	管理端口1的MAC地址(E2800A上的"`P1"和E2800B`上的0a)。如果您使用 DHCP 获取原始控制器的 IP 地址，则需要使用此地址连接到新控制器。
2.	FRU 部件号	FRU 部件号。此编号必须与当前安装的控制器的更换部件号匹配。
3.	4端口HIC	4端口主机接口卡(HIC)。在执行更换时、必须将此卡移至新控制器。 注：E2800A控制器没有HIC。

步骤

1. 按照 E2800 控制器更换操作步骤 中的说明准备卸下控制器。

   您可以使用 SANtricity 系统管理器执行这些步骤。

   a. 记下控制器上当前安装的 SANtricity OS 软件版本。

   b. 记下当前安装的 NVSRAM 版本。

   c. 如果启用了驱动器安全功能，请确保存在已保存的密钥，并且您知道安装该密钥所需的密码短语。

   *可能会丢失数据访问和#8212；*如果设备中的所有驱动器均已启用安全性、则新控制器将无法访问此设备、除非您使用SANtricity 存储管理器中的企业管理窗口解锁受保护的驱动器。

   d. 备份配置数据库。

   如果删除控制器时出现问题，您可以使用保存的文件还原配置。

   e. 收集设备的支持数据。

   在更换组件之前和之后收集支持数据可确保在更换组件无法解决问题时，您可以向技术支持发送一整套日志。

使控制器脱机

步骤

1. 如果 StorageGRID 设备正在 StorageGRID 系统中运行， 将 E5700SG 控制器置于维护模式。
2. 如果 E2800 控制器运行充分，可以进行可控的关闭，请确认所有操作均已完成。
   a. 从 SANtricity 系统管理器的主页中，选择 * 查看正在执行的操作 * 。
   b. 确认所有操作均已完成。

卸下控制器

步骤

1. 从设备中删除控制器：
   a. 戴上 ESD 腕带或采取其他防静电预防措施。
   b. 为缆线贴上标签，然后断开缆线和 SFP 的连接。

      To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

   c. 通过挤压凸轮把手上的闩锁，直到其释放，然后打开右侧的凸轮把手，将控制器从设备中释放。
   d. 用两只手和凸轮把手将控制器滑出设备。

      请始终用双手支撑控制器的重量。

   e. 将控制器放在无静电的平面上，可拆卸盖朝上。
   f. 向下按按钮并滑动外盖，以卸下外盖。

将电池移至新控制器

步骤

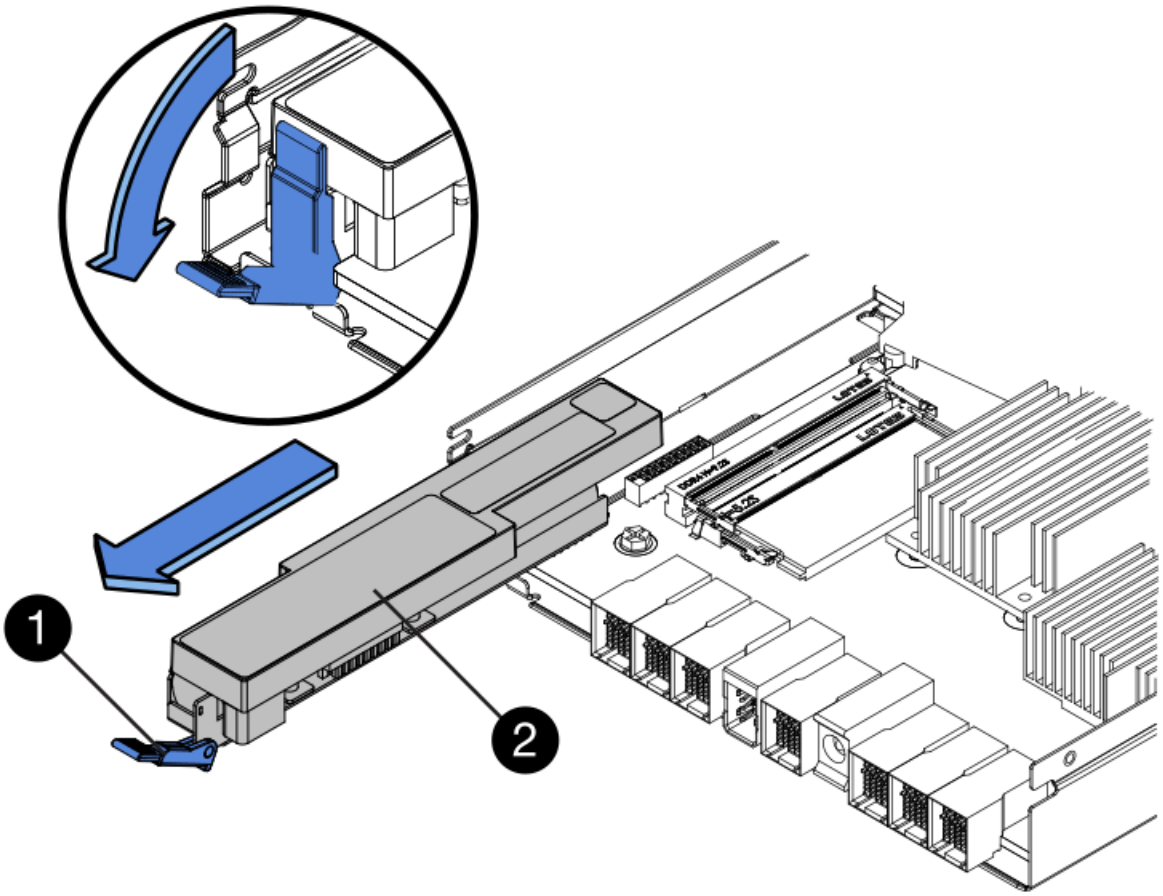
1. 从发生故障的控制器中取出电池，然后将其安装到替代控制器中：
   a. 确认控制器（电池和 DIMM 之间）中的绿色 LED 熄灭。

      如果此绿色 LED 亮起，则表示控制器仍在使用电池电源。您必须等待此 LED 熄灭，然后才能卸下任何组件。

项目	Description
1.	内部缓存活动 LED
2.	电池

b. 找到电池的蓝色释放闩锁。

c. 向下推动释放闩锁并将其从控制器中移出，以解锁电池。



项目	Description
1.	电池释放闩锁
2.	电池

d. 抬起电池，将其滑出控制器。

e. 从更换用的控制器上卸下盖板。

f. 调整更换控制器的方向，使电池插槽面向您。

g. 将电池略微向下插入控制器。

   您必须将电池前部的金属法兰插入控制器底部的插槽中，然后将电池顶部滑入控制器左侧的小对齐销下。

h. 向上移动电池闩锁以固定电池。

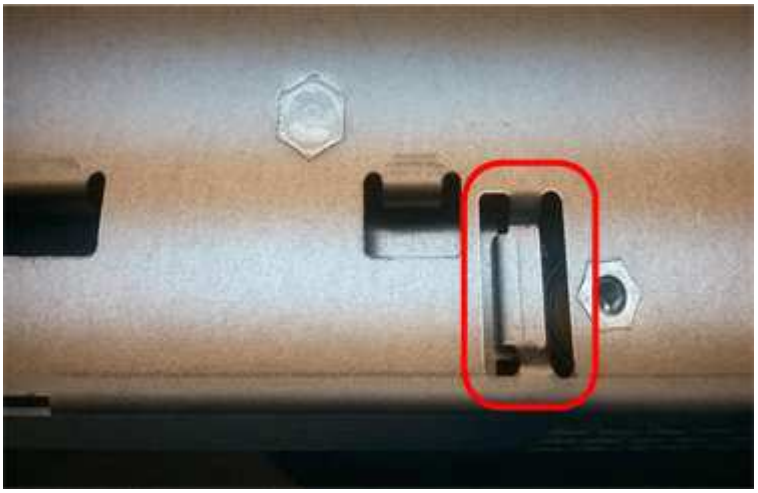
   当闩锁卡入到位时，闩锁的底部会挂到机箱上的金属插槽中。

i. 将控制器翻转，以确认电池安装正确。

* 可能的硬件损坏 * —电池正面的金属法兰必须完全插入控制器上的插槽（如第一图所示）。如果电池安装不正确（如图 2 所示），则金属法兰可能会接触控制器板，从而导致损坏。

- 正确—电池的金属法兰已完全插入控制器上的插槽：

- * 不正确 - 电池的金属法兰未插入控制器上的插槽： *



2. 更换控制器盖板。

如果需要、将**HIC**移至新控制器

步骤

1. 如果故障控制器包含主机接口卡(HIC)、请将HIC从故障控制器移至更换控制器。

   单独的HIC仅用于E2800B控制器。HIC安装在主控制器板上、并包含两个SPF连接器。

   此操作步骤 中的插图显示了一个双端口HIC。控制器中的HIC可能具有不同数量的端口。

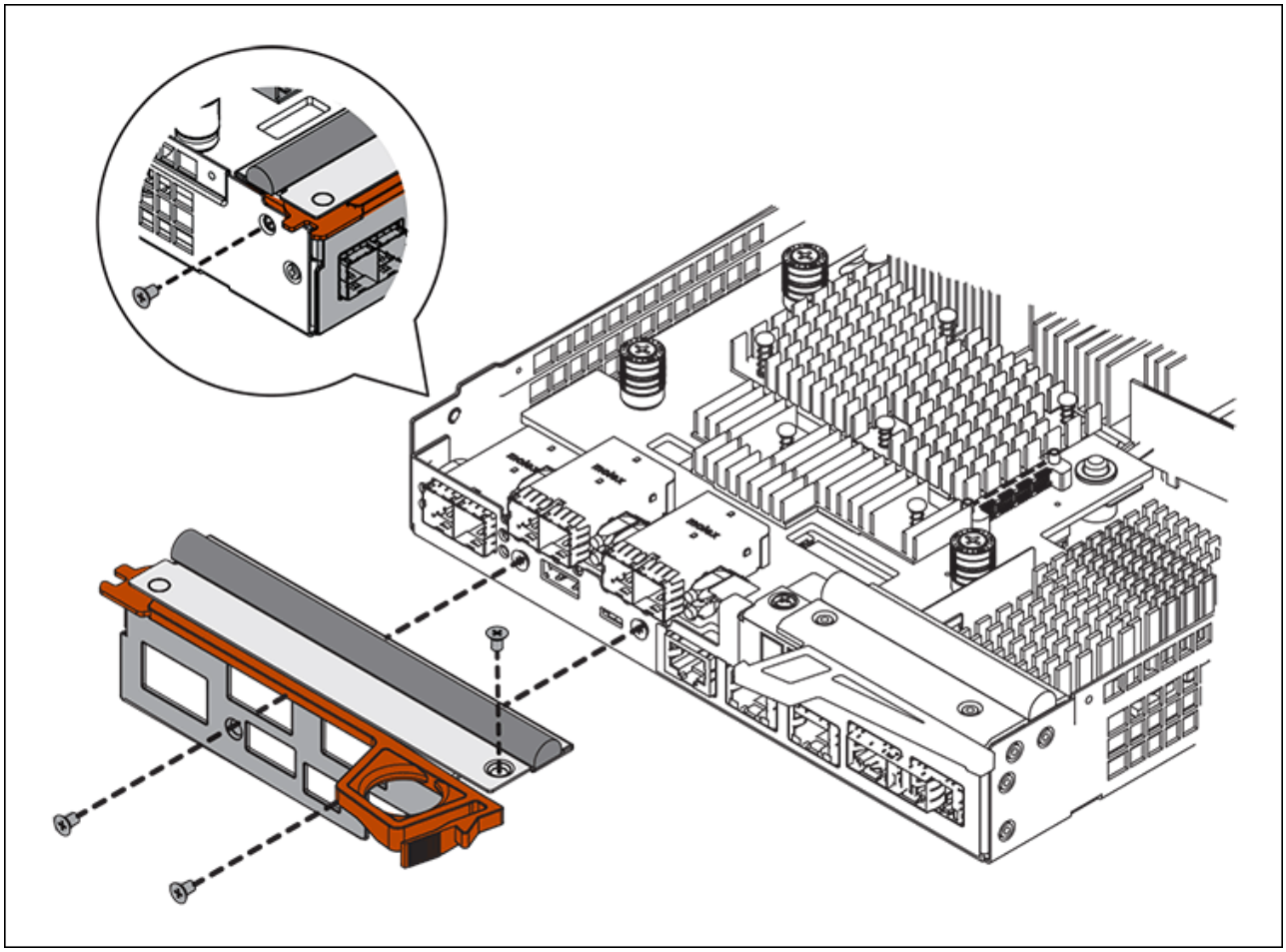
2. 如果控制器没有HIC (E2800A)、请更换控制器盖板。如果控制器确实具有HIC (E2800B)、请继续执行将HIC从故障控制器移至替代控制器。

a. 如果配有HIC、请将HIC从故障控制器移至更换控制器。

b. 从HIC中删除所有SFP。

c. 使用1号十字螺丝刀卸下将HIC面板连接到控制器的螺钉。

有四个螺钉：一个在顶部，一个在侧面，两个在正面。

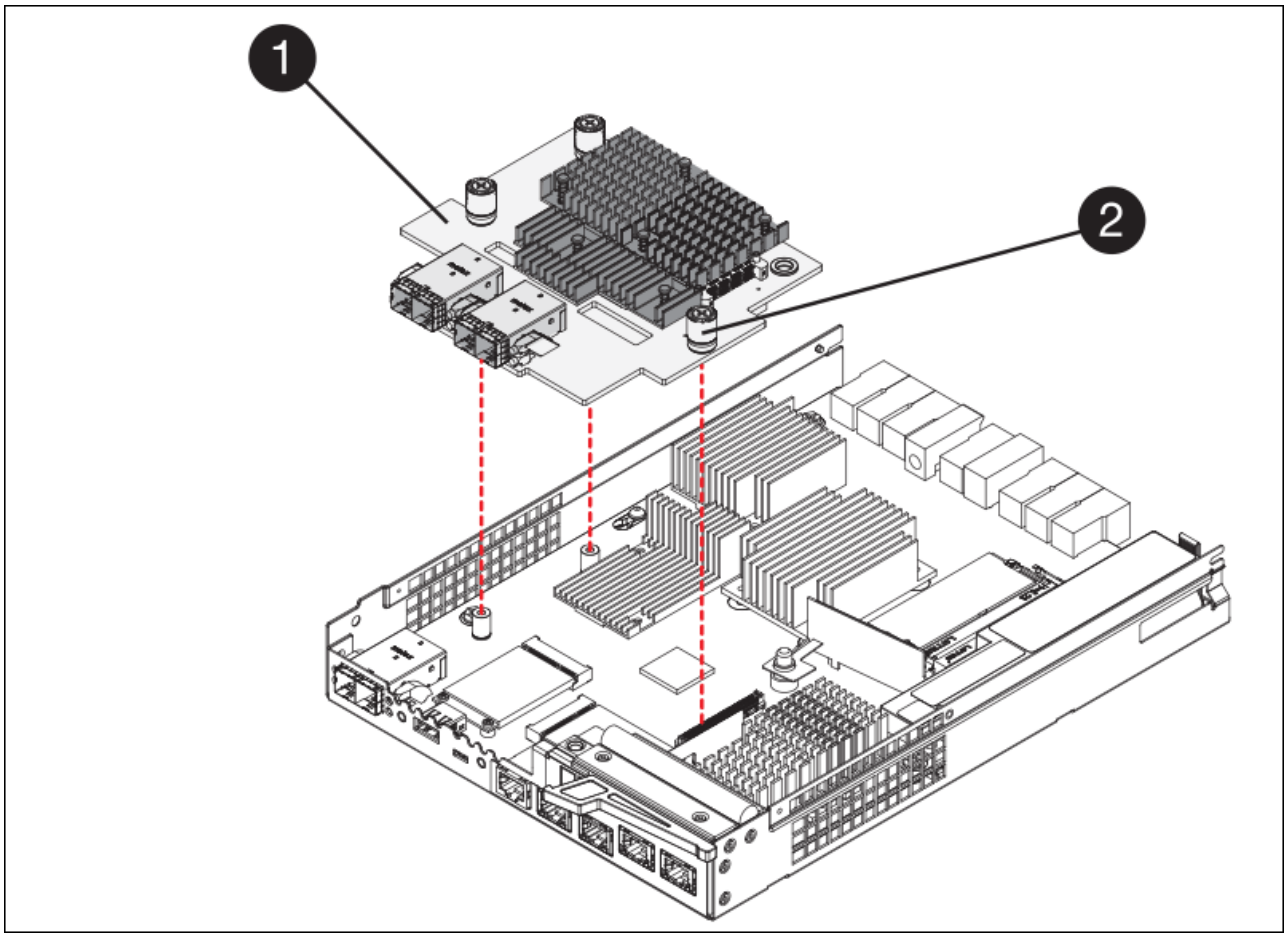


d. 卸下 HIC 面板。

e. 使用您的手指或十字螺丝刀松开将 HIC 固定到控制器卡的三个翼形螺钉。

f. 小心地将 HIC 从控制器卡上卸下，方法是将该卡抬起并滑回。

请注意，不要擦除或撞击 HIC 底部或控制器卡顶部的组件。



Label	Description
1.	主机接口卡
2.	翼形螺钉

g. 将 HIC 放置在无静电表面上。

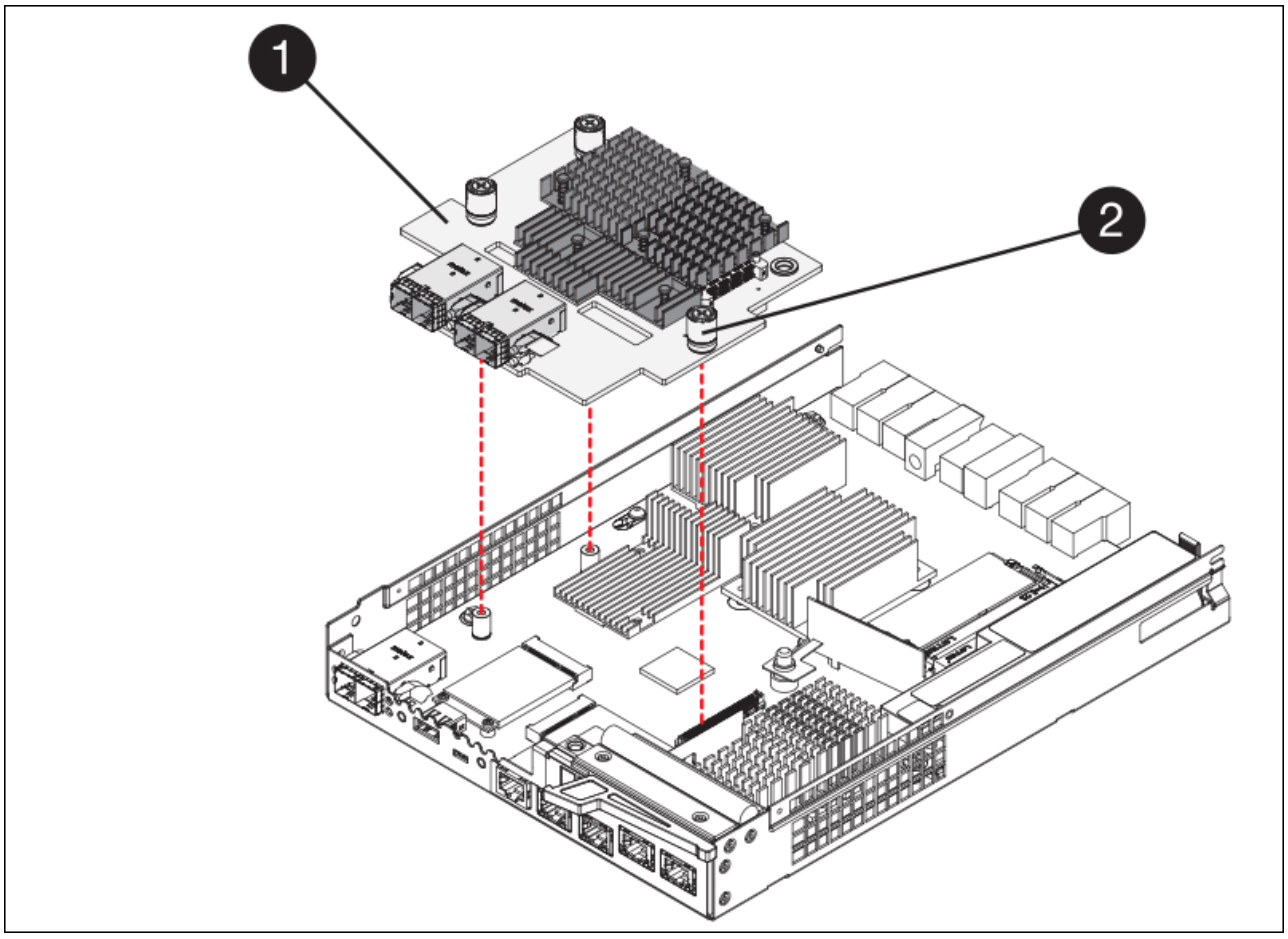
h. 使用1号十字螺丝刀卸下将空白面板连接到更换用控制器的四个螺钉、然后卸下面板。

i. 将HIC上的三个翼形螺钉与更换用的控制器上的相应孔对齐、并将HIC底部的连接器与控制器卡上的HIC接口连接器对齐。

   请注意，不要擦除或撞击 HIC 底部或控制器卡顶部的组件。

j. 小心地将 HIC 放低到位，然后轻按 HIC 以固定 HIC 连接器。

   * 可能的设备损坏 * —请务必小心，不要挤压 HIC 和翼形螺钉之间控制器 LED 的金带连接器。

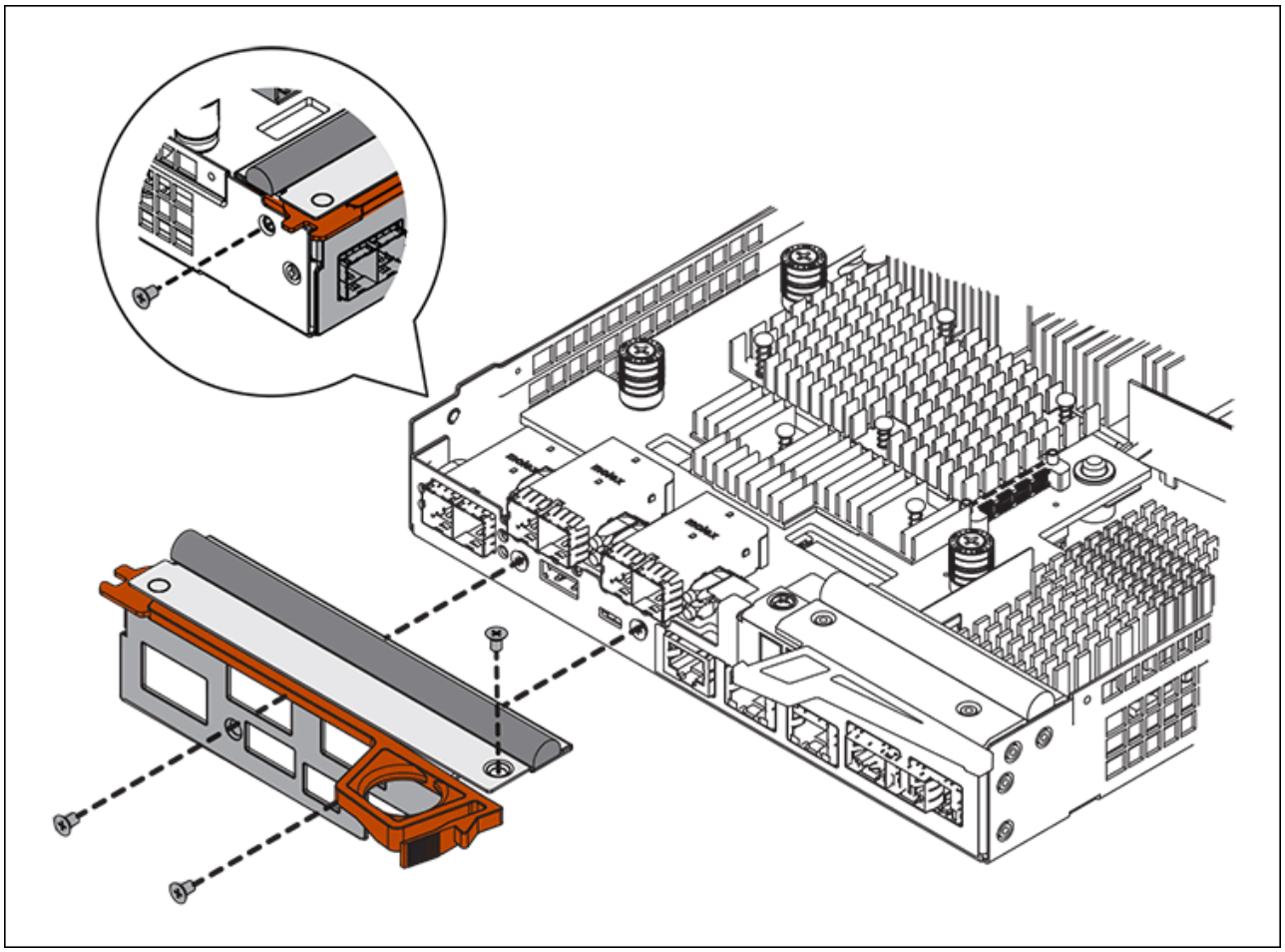


Label	Description
1.	主机接口卡
2.	翼形螺钉

a. 手动拧紧 HIC 翼形螺钉。

请勿使用螺丝刀，否则可能会过度拧紧螺钉。

b. 使用1号十字螺丝刀、使用四个螺钉将从原始控制器上卸下的HIC面板连接到新控制器。



c. 将所有已删除的SFP重新安装到HIC中。

更换控制器

步骤

1. 将替代控制器安装到设备中。

   a. 将控制器翻转，使可拆卸盖朝下。

   b. 在凸轮把手处于打开位置的情况下，将控制器完全滑入设备中。

   c. 将凸轮把手移至左侧，将控制器锁定到位。

   d. 更换缆线和 SFP 。

   e. 等待 E2800 控制器重新启动。验证七段显示屏是否显示状态 `99` 。

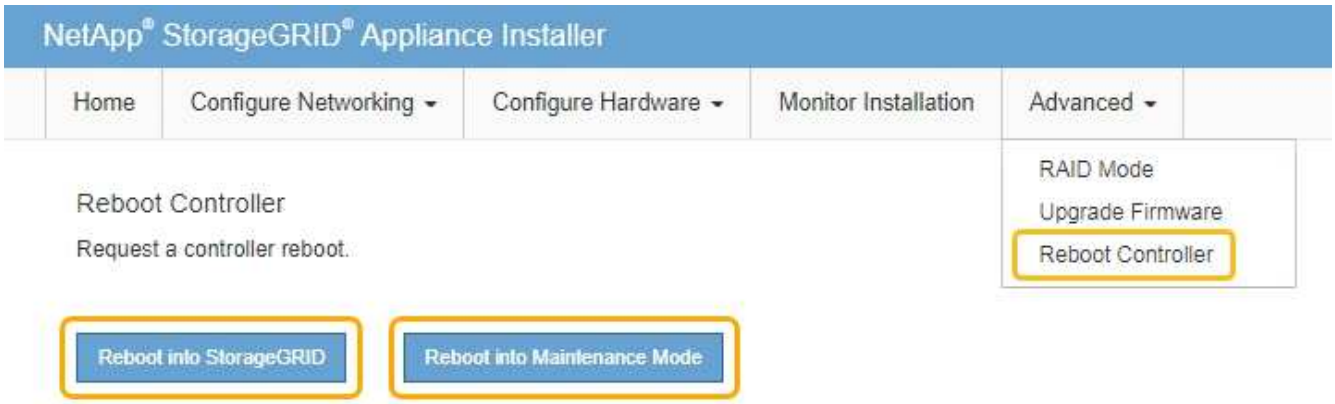
   f. 确定如何为替代控制器分配 IP 地址。

   > 为替代控制器分配 IP 地址的步骤取决于您是否已将管理端口 1 连接到使用 DHCP 服务器的网络，以及所有驱动器是否都安全。

   如果管理端口 1 连接到使用 DHCP 服务器的网络，则新控制器将从 DHCP 服务器获取其 IP 地址。此值可能与原始控制器的 IP 地址不同。

2. 如果设备使用安全驱动器，请按照 E2800 控制器更换操作步骤 中的说明导入驱动器安全密钥。

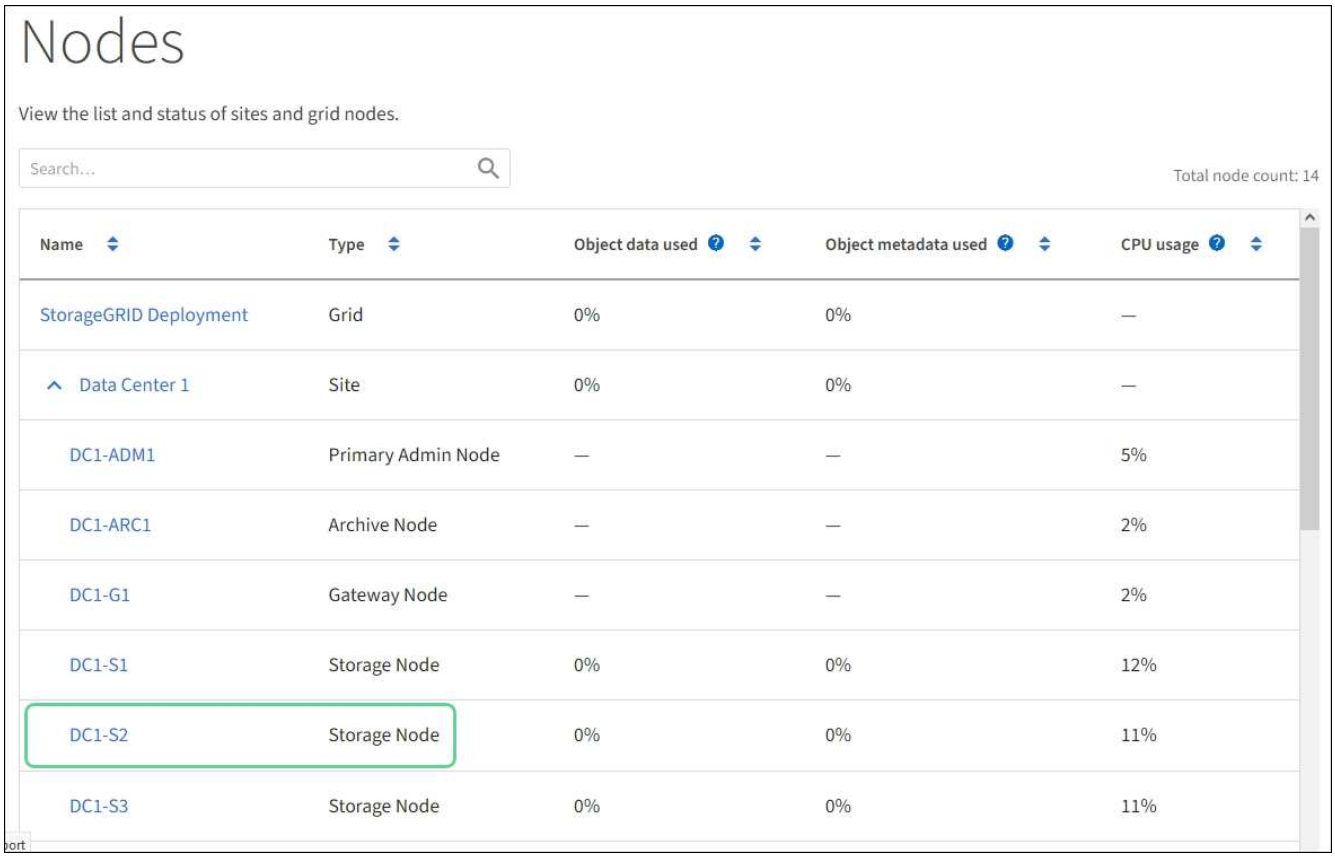
3. 将设备恢复到正常运行模式。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



4. 在重新启动期间、监控节点的状态、以确定节点何时重新加入网格。

   设备将重新启动并重新加入网格。此过程可能需要长达 20 分钟。

5. 确认重新启动已完成，并且节点已重新加入网格。在网格管理器中，验证节点页面是否显示设备节点的正常状态（节点名称左侧没有图标），表示没有活动警报且节点已连接到网格。



6. 从 SANtricity 系统管理器中，确认新控制器处于最佳状态，然后收集支持数据。

更换部件后，按照套件随附的 RMA 说明将故障部件退回 NetApp 。请参见 "部件退回和放大器；更换" 第页，了

解更多信息。

相关信息

"NetApp E 系列系统文档站点"

更换 **E5700SG** 控制器

如果 E5700SG 控制器运行不正常或出现故障，您可能需要更换它。

您需要的内容

- 您的更换控制器的部件号与要更换的控制器相同。
- 您已下载有关更换发生故障的 E5700 控制器的 E 系列说明。

> 仅当您需要执行特定步骤的更多详细信息时，才可参考 E 系列说明。请勿依赖 E 系列说明来更换 StorageGRID 设备中的控制器，因为这些过程是不同的。例如， E5700 控制器的 E 系列说明介绍了如何从发生故障的控制器中取出电池和主机接口卡（ HIC ）并将其安装到更换控制器中。这些步骤不适用于 E5700SG 控制器。

- 您可以通过标签来识别连接到控制器的每个缆线。
- 此设备已运行 已置于维护模式。

关于此任务

更换控制器后，无法访问设备存储节点。如果 E5700SG 控制器运行正常，则可以在此操作步骤 开始时执行受控关闭。

> 如果在安装 StorageGRID 软件之前更换控制器，则在完成此操作步骤 后，您可能无法立即访问 StorageGRID 设备安装程序。虽然您可以从与设备位于同一子网上的其他主机访问 StorageGRID 设备安装程序，但不能从其他子网上的主机访问它。此情况应在 15 分钟内自行解决（当原始控制器的任何 ARP 缓存条目超时），或者您也可以通过手动从本地路由器或网关清除任何旧的 ARP 缓存条目来立即清除此情况。

步骤

1. 将设备置于维护模式后，关闭 E5700SG 控制器。
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 关闭 E5700SG 控制器： + ` * shutdown -h now*`
   c. 等待缓存中的所有数据写入驱动器。

      当需要将缓存数据写入驱动器时， E2800 控制器背面的绿色缓存活动 LED 亮起。您必须等待此 LED 关闭。

2. 关闭电源。
   a. 从 SANtricity 系统管理器的主页中，选择 * 查看正在执行的操作 * 。
   b. 确认所有操作均已完成。
   c. 关闭设备上的两个电源开关。
   d. 等待所有 LED 熄灭。
3. 如果连接到控制器的 StorageGRID 网络使用 DHCP 服务器：
   a. 记下替代控制器上端口的 MAC 地址（位于控制器上的标签上）。
   b. 请网络管理员更新原始控制器的 IP 地址设置，以反映替代控制器的 MAC 地址。

   > 在为替代控制器接通电源之前，您必须确保已更新原始控制器的 IP 地址。否则，控制器将在启动时获取新的 DHCP IP 地址，并且可能无法重新连接到 StorageGRID 。此步骤将对连接到控制器的所有 StorageGRID 网络执行适用场景 。

4. 从设备中删除控制器：
   a. 戴上 ESD 腕带或采取其他防静电预防措施。
   b. 为缆线贴上标签，然后断开缆线和 SFP 的连接。

   > To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

   c. 通过挤压凸轮把手上的闩锁，直到其释放，然后打开右侧的凸轮把手，将控制器从设备中释放。
   d. 用两只手和凸轮把手将控制器滑出设备。

   > 请始终用双手支撑控制器的重量。

5. 将替代控制器安装到设备中。
   a. 将控制器翻转，使可拆卸盖朝下。
   b. 在凸轮把手处于打开位置的情况下，将控制器完全滑入设备中。
   c. 将凸轮把手移至左侧，将控制器锁定到位。
   d. 更换缆线和 SFP 。
6. 打开设备电源，并监控控制器 LED 和七段显示器。

   成功启动控制器后，七段显示屏应显示以下内容：

   - E2800 控制器：

     最终状态为 `99` 。

   - E5700SG 控制器：

     最终状态为 `HA` 。

7. 确认设备存储节点显示在网格管理器中且未显示任何警报。

相关信息

"NetApp E 系列系统文档站点"

更换其他硬件组件

您可能需要更换 StorageGRID 设备中的控制器电池，驱动器，风扇或电源。

您需要的内容

- 您已安装 E 系列硬件更换操作步骤 。
- 此设备已运行 已置于维护模式 如果组件更换操作步骤 要求您关闭设备。

关于此任务

要更换 E2800 控制器中的电池，请参见这些说明中有关更换 E2800 控制器的说明。这些说明介绍了如何从设备中卸下控制器，从控制器中取出电池，安装电池以及更换控制器。

要更换设备中的驱动器，电源风扇箱，风扇箱，电源箱或驱动器抽屉，请访问 E 系列维护 E2800 硬件的过程。

SG5712 组件更换说明

FRU	请参见 **E** 系列说明
驱动器	更换 E2800 12 驱动器或 24 驱动器磁盘架中的驱动器
电源风扇箱	更换 E2800 磁盘架中的电源风扇箱

SG5760 组件更换说明

FRU	请参见 **E** 系列说明
驱动器	更换 E2860 磁盘架中的驱动器
动力箱	更换 E2860 磁盘架中的电源箱
风扇箱	更换 E2860 磁盘架中的风扇箱
Drive drawer	更换 E2860 磁盘架中的驱动器抽盒

相关信息

更换 E2800 控制器

"NetApp E 系列系统文档站点"

更改 **E5700SG** 控制器的链路配置

您可以更改 E5700SG 控制器的以太网链路配置。您可以更改端口绑定模式，网络绑定模式和链路速度。

您需要的内容

将 E5700SG 控制器置于维护模式。

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

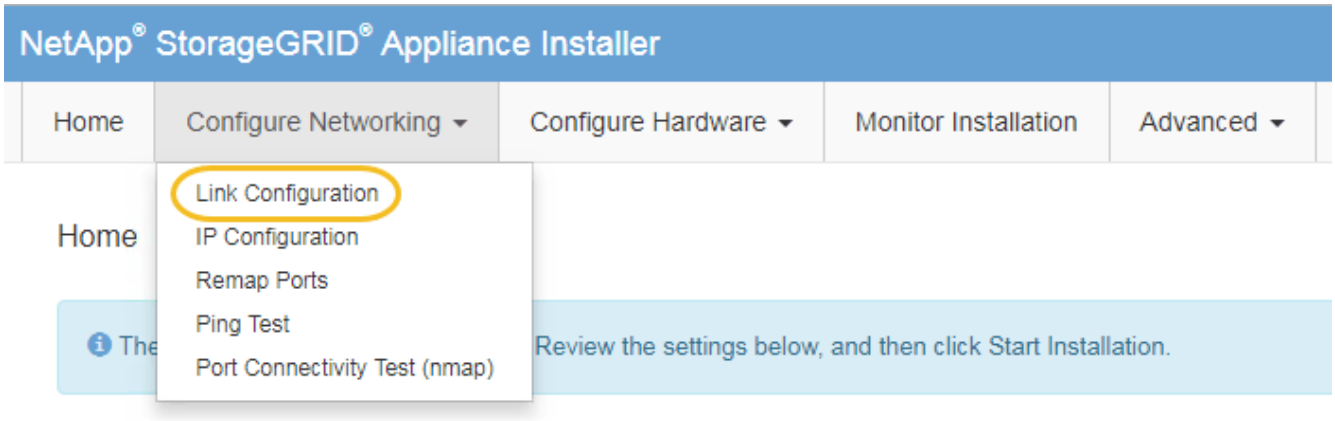
关于此任务

更改 E5700SG 控制器的以太网链路配置的选项包括：

- 将 * 端口绑定模式 * 从 " 固定 " 更改为 " 聚合 " 或从 " 聚合 " 更改为 " 固定 "
- 将 * 网络绑定模式 * 从主动备份更改为 LACP 或从 LACP 更改为主动备份
- 启用或禁用 VLAN 标记，或者更改 VLAN 标记的值
- 将链路速度从 10-GbE 更改为 25-GbE ，或从 25-GbE 更改为 10-GbE

步骤

1. 从菜单中选择 * 配置网络连接 * > * 链路配置 * 。



2. 【 change_link_configuration_sg5700 ， start=2]] 对链路配置进行所需的更改。

   有关这些选项的详细信息，请参见 "`配置网络链路 " 。`

3. 对所做的选择感到满意后，单击 * 保存 * 。

   如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*E5700SG_Controller_IP*:8443*`

   如果更改了 VLAN 设置，则设备的子网可能已更改。如果需要更改设备的 IP 地址，请按照执行操作 设置 IP 配置 说明。

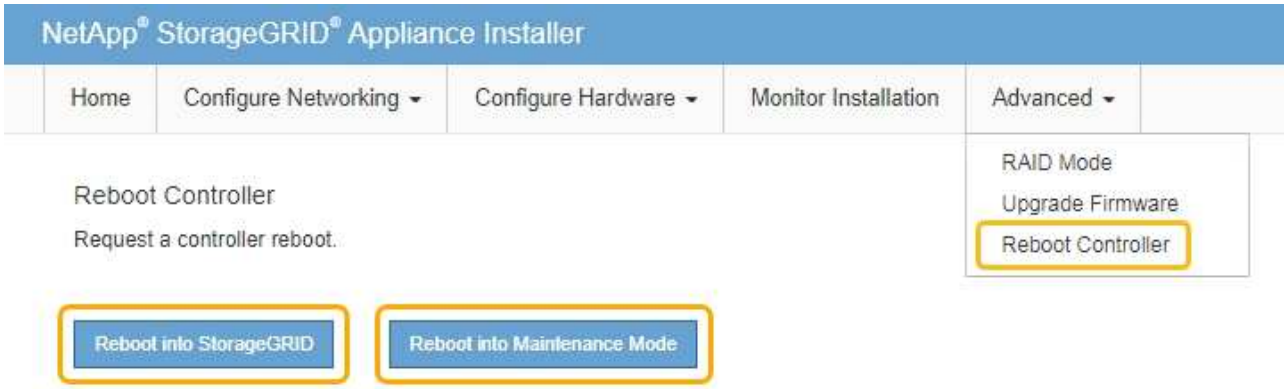
4. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * Ping 测试 * 。
5. 使用 Ping 测试工具检查可能受中所做链路配置更改影响的任何网络上的 IP 地址连接 更改链路配置 步骤。

   除了您选择执行的任何其他测试之外，请确认您可以对主管理节点的网格 IP 地址以及至少一个其他存储节点的网格 IP 地址执行 ping 操作。如有必要，请更正任何链路配置问题。

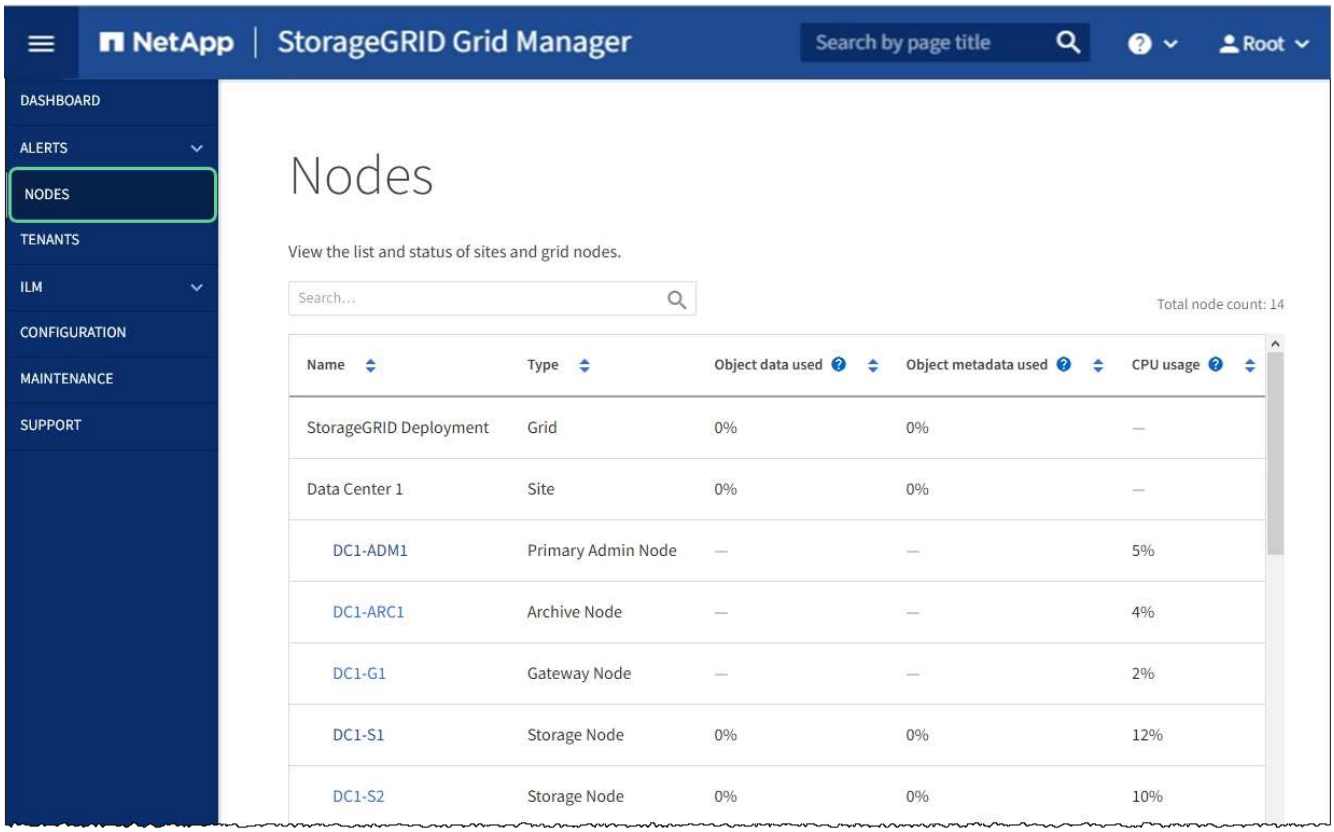
6. 在您确信链路配置更改正常运行后，请重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > *

重新启动控制器 * ，然后选择以下选项之一：

- 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
- 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

配置网络链路（ SG5700 ）

更改 MTU 设置

您可以更改在为设备节点配置 IP 地址时分配的 MTU 设置。

关于此任务

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

要在不重新启动设备节点的情况下更改 MTU 设置， 使用更改 IP 工具。

如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络， 使用维护模式更改 MTU 设置。

使用更改 IP 工具更改 MTU 设置

您需要的内容

您有 `passwords.txt` 文件可用于更改 IP 工具。

步骤

访问更改 IP 工具并按中所述更新 MTU 设置 更改节点网络配置。

使用维护模式更改 MTU 设置

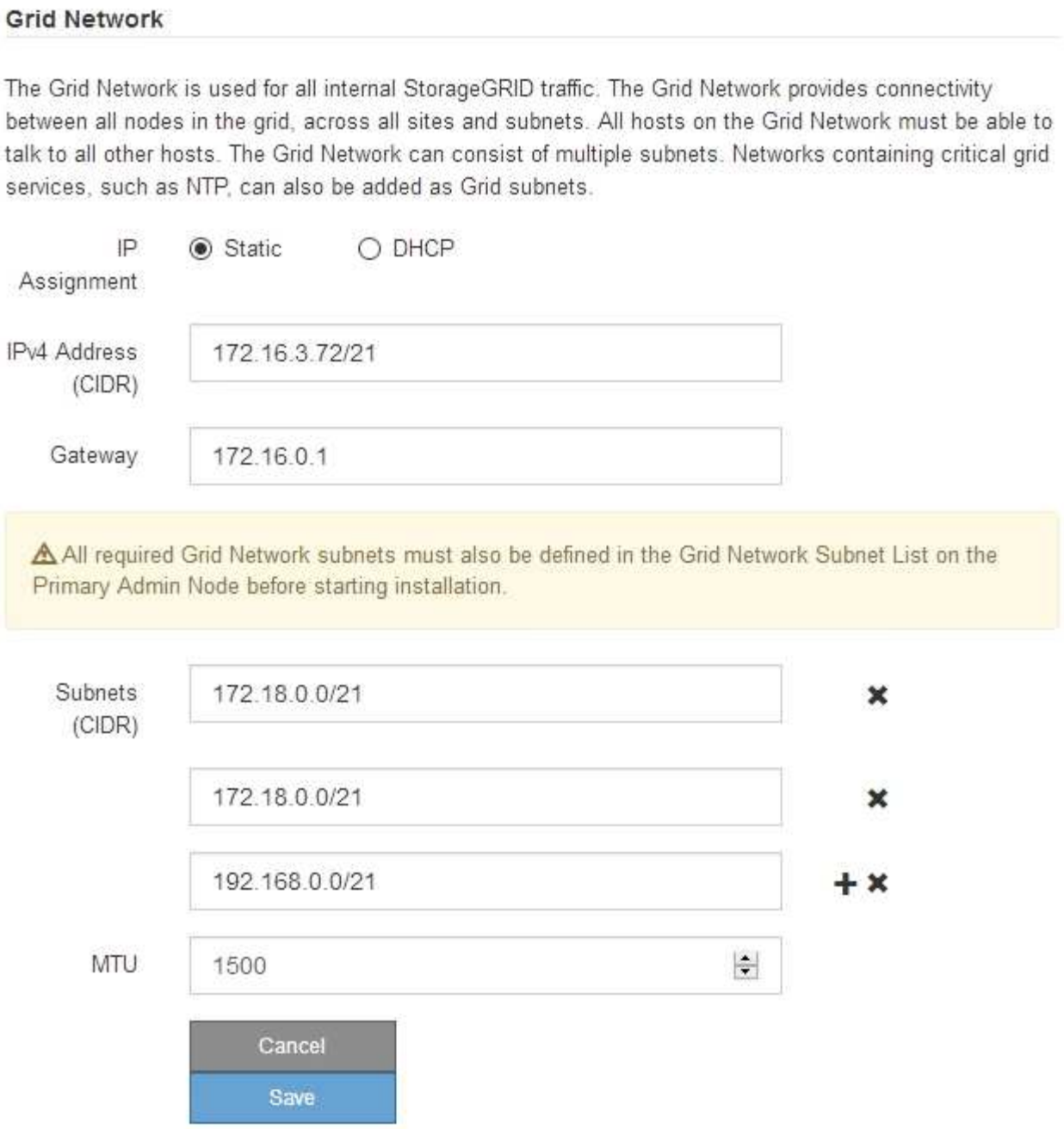
如果无法使用更改 IP 工具访问这些设置，请使用维护模式更改 MTU 设置。

您需要的内容

此设备已运行 已置于维护模式。

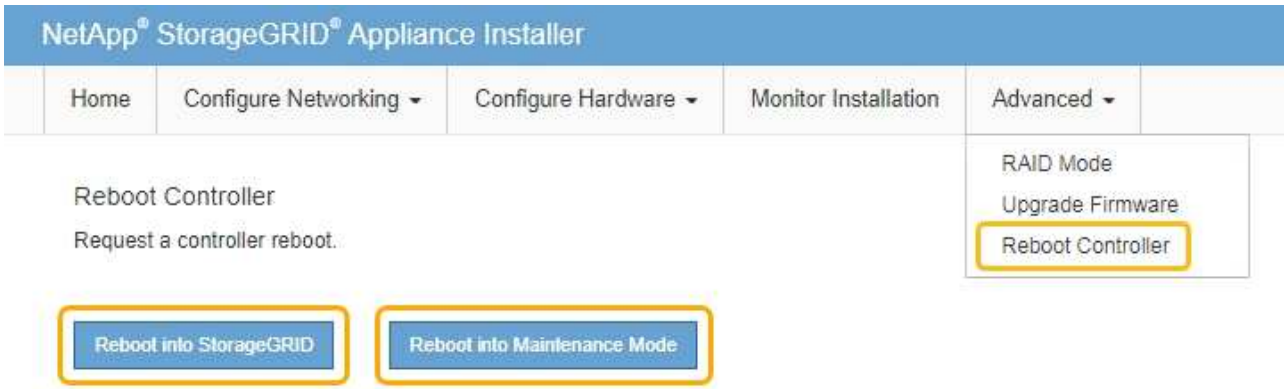
步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。
2. 对网格网络，管理网络和客户端网络的 MTU 设置进行所需的更改。

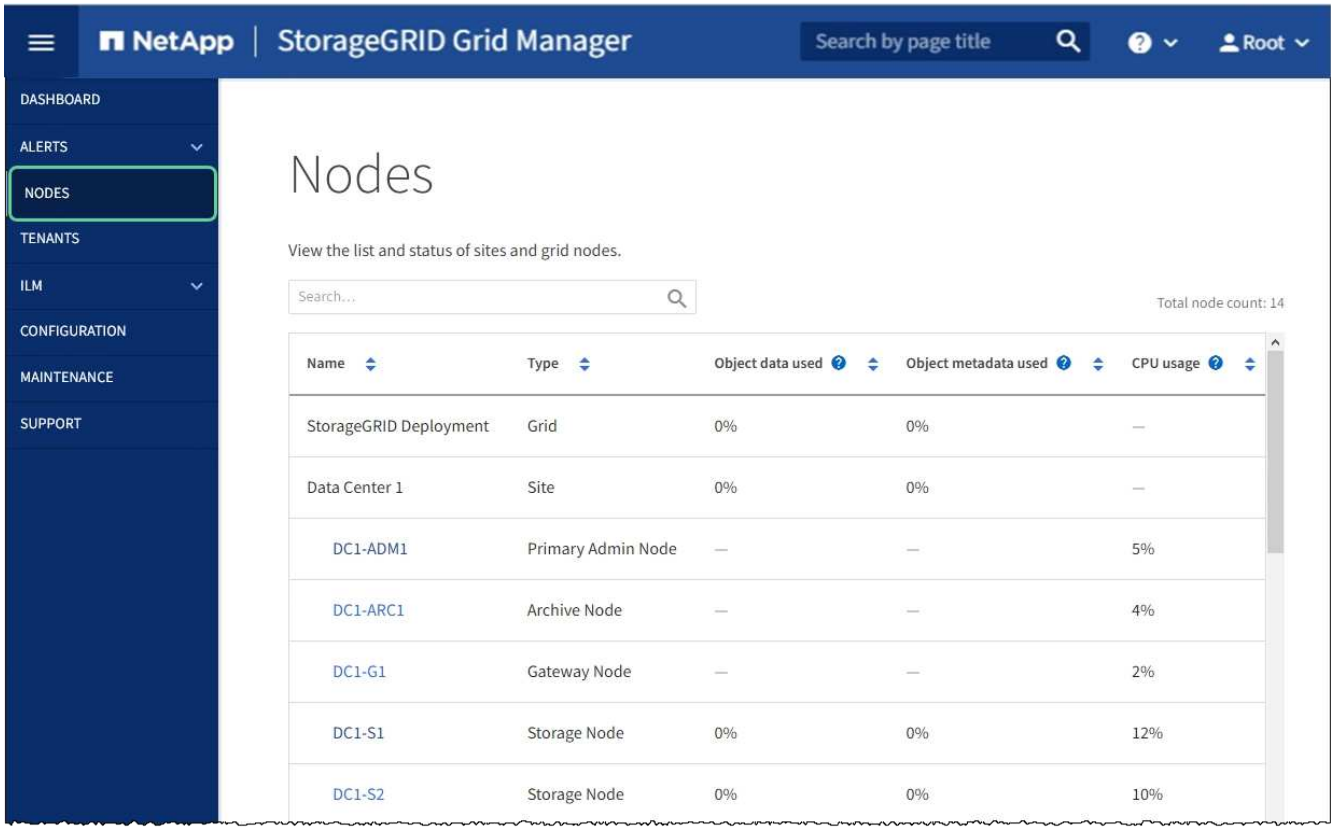


3. 如果对设置感到满意，请选择 * 保存 * 。
4. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

检查 **DNS** 服务器配置

您可以检查并临时更改此设备节点当前正在使用的域名系统（ DNS ）服务器。

您需要的内容

此设备已运行 已置于维护模式。

关于此任务

如果加密设备无法连接到密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群，则可能需要更改 DNS 服务器设置，因为 KMS 的主机名指定为域名，而不是 IP 地址。对设备的 DNS 设置所做的任何更改都是临时的，在退出维护模式时将丢失。要使这些更改永久生效，请在网格管理器中指定 DNS 服务器（ * 维护 * > * 网络 * > * DNS 服务器 * ）。

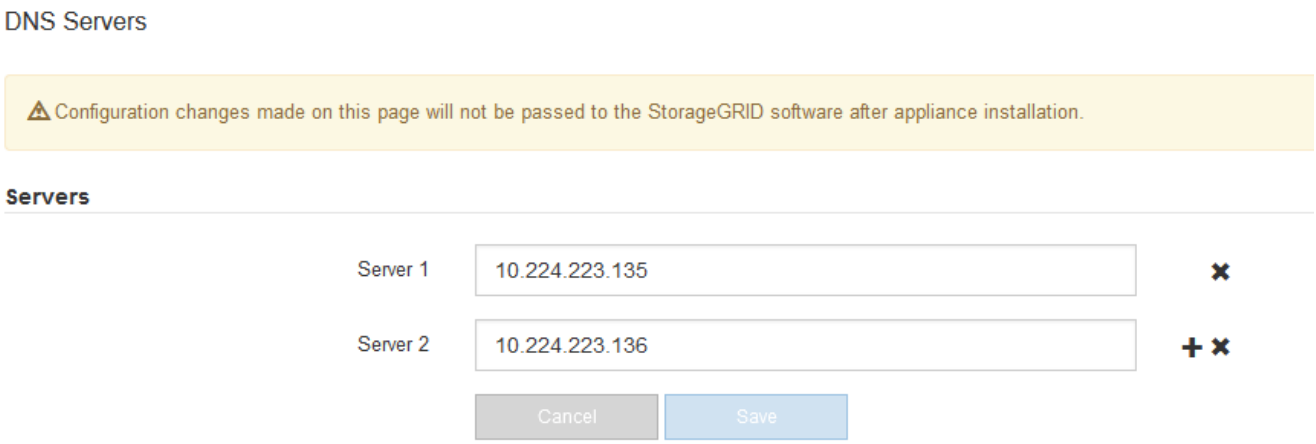
- 只有在节点加密的设备中，使用完全限定域名（而不是 IP 地址）为主机名定义 KMS 服务器时，才需要临时更改 DNS 配置。
- 当节点加密设备使用域名连接到 KMS 时，它必须连接到为网格定义的一个 DNS 服务器。然后，其中一个 DNS 服务器会将域名转换为 IP 地址。
- 如果节点无法访问网格的 DNS 服务器，或者您在节点加密设备节点脱机时更改了网格范围的 DNS 设置，则节点将无法连接到 KMS 。在解析 DNS 问题描述 之前，无法解密设备上的加密数据。

要解决 DNS 问题描述 阻止 KMS 连接的问题，请在 StorageGRID 设备安装程序中指定一个或多个 DNS 服务器的 IP 地址。通过这些临时 DNS 设置，设备可以连接到 KMS 并对节点上的数据进行解密。

例如，如果在加密节点脱机时网格的 DNS 服务器发生更改，则该节点将无法在重新联机时访问 KMS ，因为它仍在使用先前的 DNS 值。在 StorageGRID 设备安装程序中输入新的 DNS 服务器 IP 地址后，可以通过临时 KMS 连接对节点数据进行解密。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * DNS 配置 * 。
2. 验证指定的 DNS 服务器是否正确。



3. 如果需要，请更改 DNS 服务器。

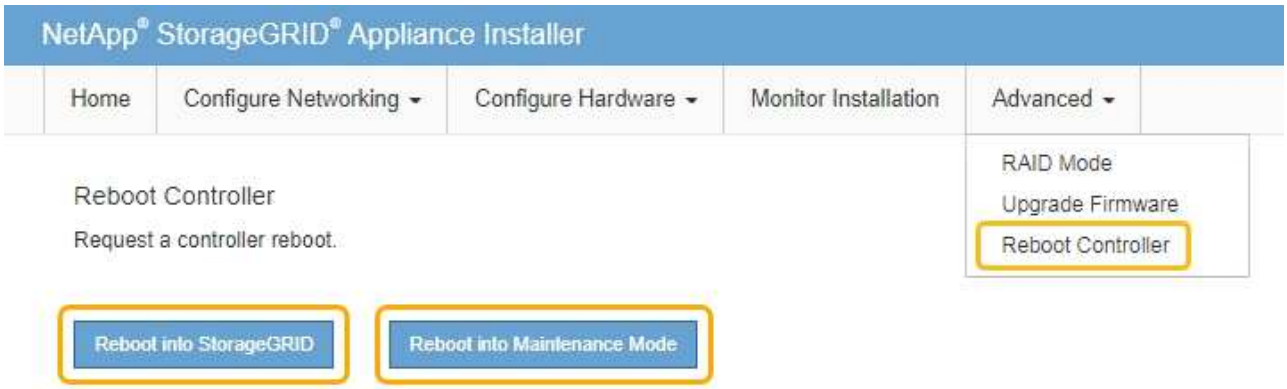
   对 DNS 设置所做的更改是临时的，当您退出维护模式时，这些更改将丢失。

4. 对临时 DNS 设置感到满意后，请选择 * 保存 * 。

   节点使用此页面上指定的 DNS 服务器设置重新连接到 KMS ，从而可以解密节点上的数据。

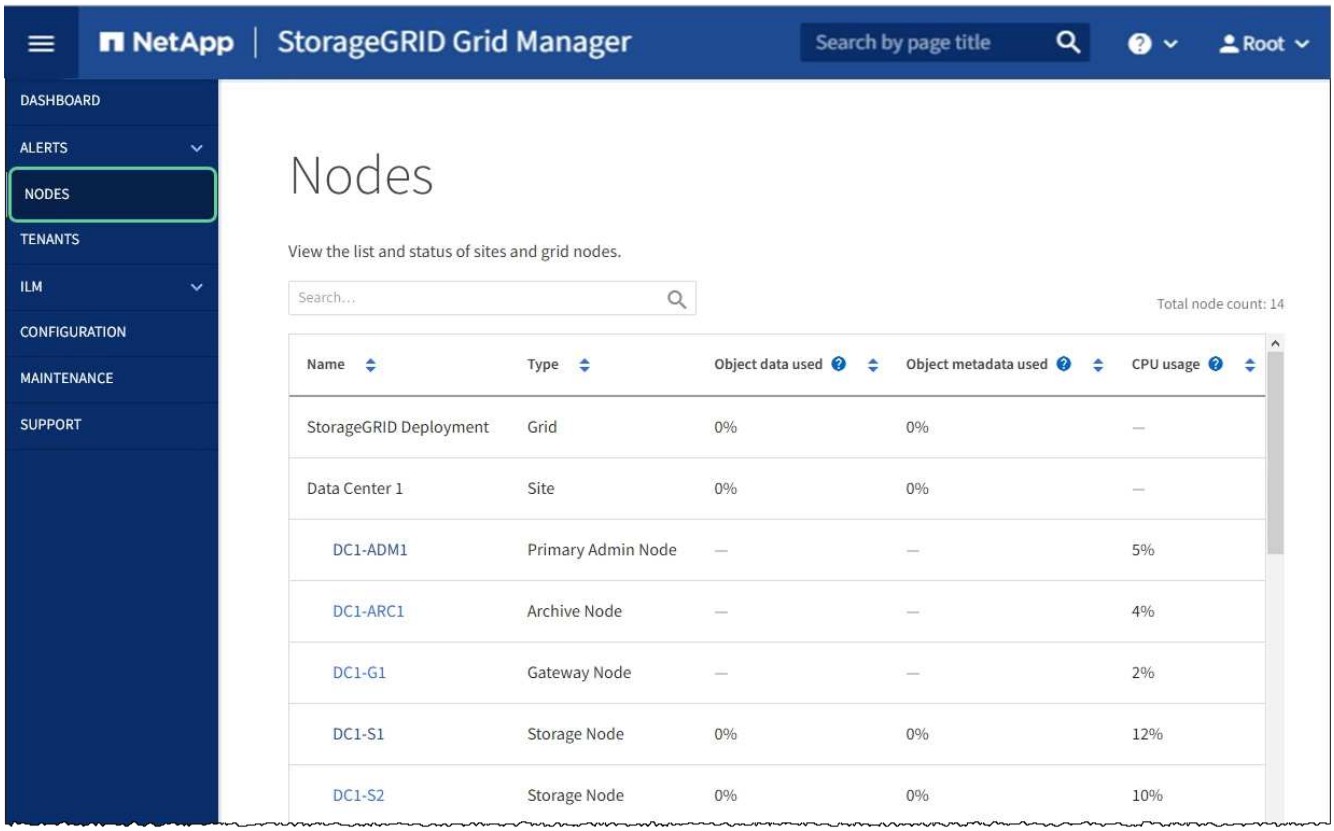
5. 解密节点数据后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

- 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
- 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



当节点重新启动并重新加入网格时，它将使用网格管理器中列出的系统范围的 DNS 服务器。重新加入网格后，在设备处于维护模式时，设备将不再使用 StorageGRID 设备安装程序中指定的临时 DNS 服务器。

设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



在维护模式下监控节点加密（ **SG5700** ）

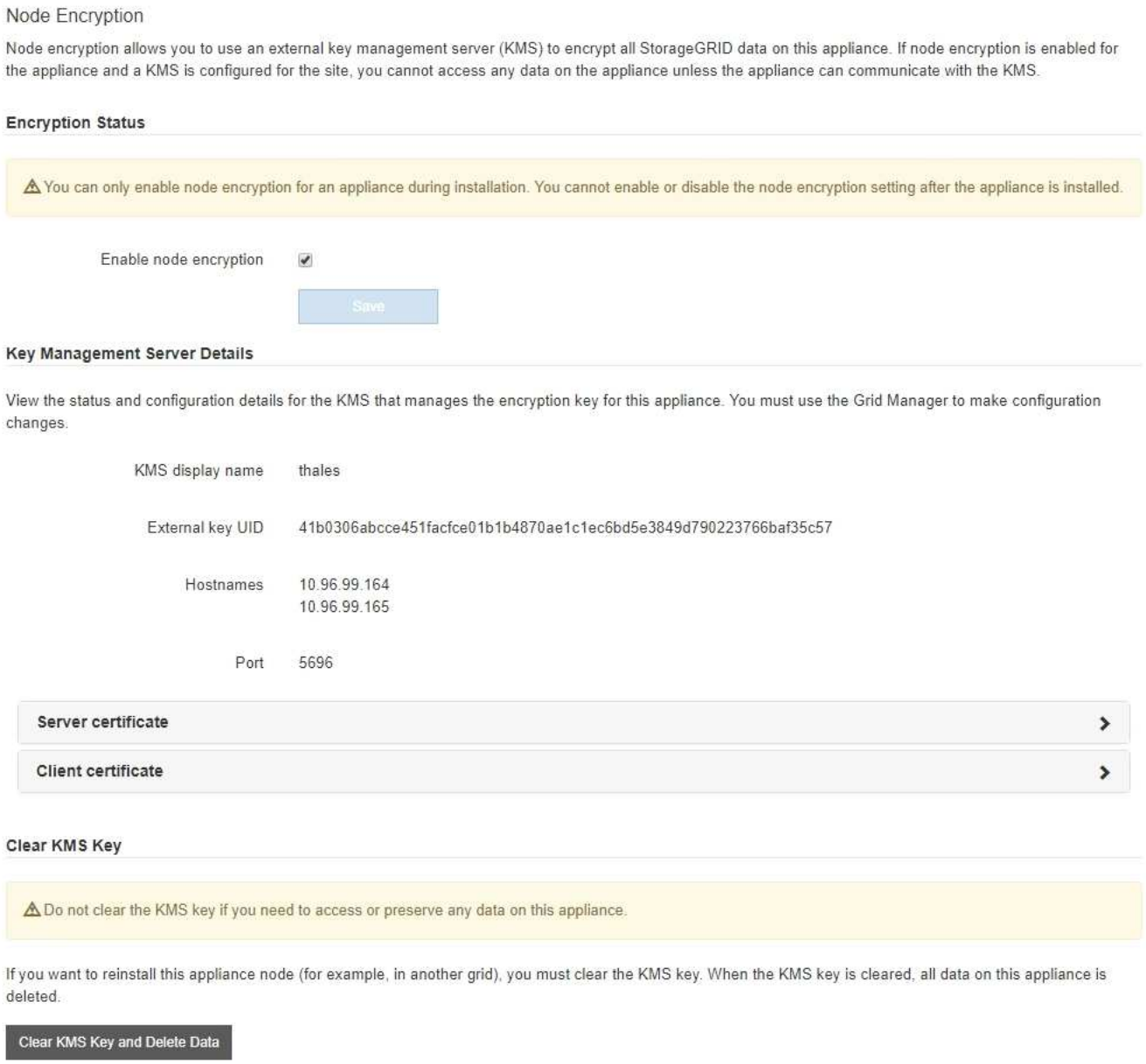
如果您在安装期间为设备启用了节点加密，则可以监控每个设备节点的节点加密状态，包括节点加密状态和密钥管理服务器（ KMS ）详细信息。

您需要的内容

- 必须在安装期间为设备启用节点加密。安装设备后，您无法启用节点加密。
- 此设备已运行 置于维护模式。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置硬件 * > * 节点加密 * 。



节点加密页面包括以下三个部分：

◦ " 加密状态 " 显示设备是启用还是禁用了节点加密。

- 密钥管理服务器详细信息显示了有关用于对设备进行加密的 KMS 的信息。您可以展开服务器和客户端证书部分以查看证书详细信息和状态。
  - 要解决证书本身的问题，例如续订已过期的证书，请参见管理 StorageGRID 的说明中有关 KMS 的信息。
  - 如果连接到 KMS 主机时出现意外问题，请验证域名系统（ DNS ）服务器是否正确以及设备网络连接是否配置正确。

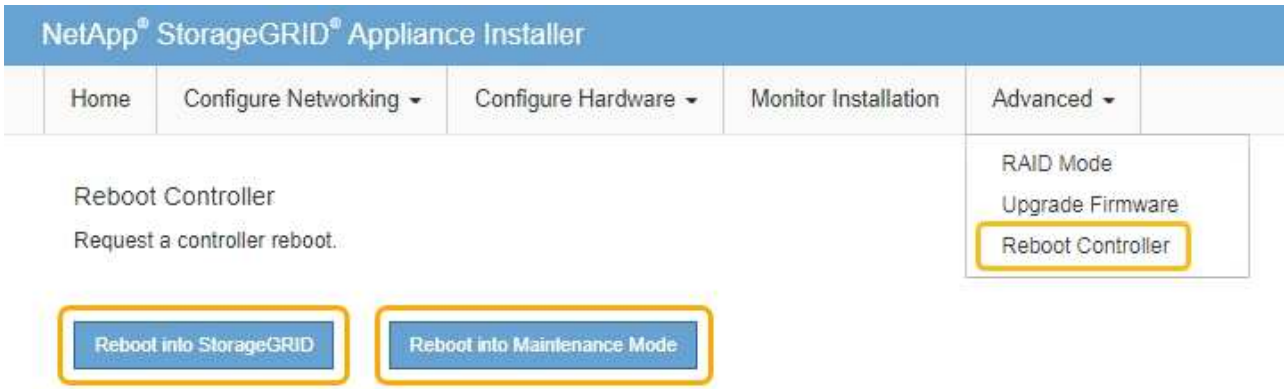
    检查 DNS 服务器配置

  - 如果无法解决证书问题，请联系技术支持。
- 清除 KMS 密钥会禁用设备的节点加密，删除设备与为 StorageGRID 站点配置的密钥管理服务器之间的关联，并删除设备中的所有数据。在将此设备安装到另一个 StorageGRID 系统之前，必须清除 KMS 密钥。

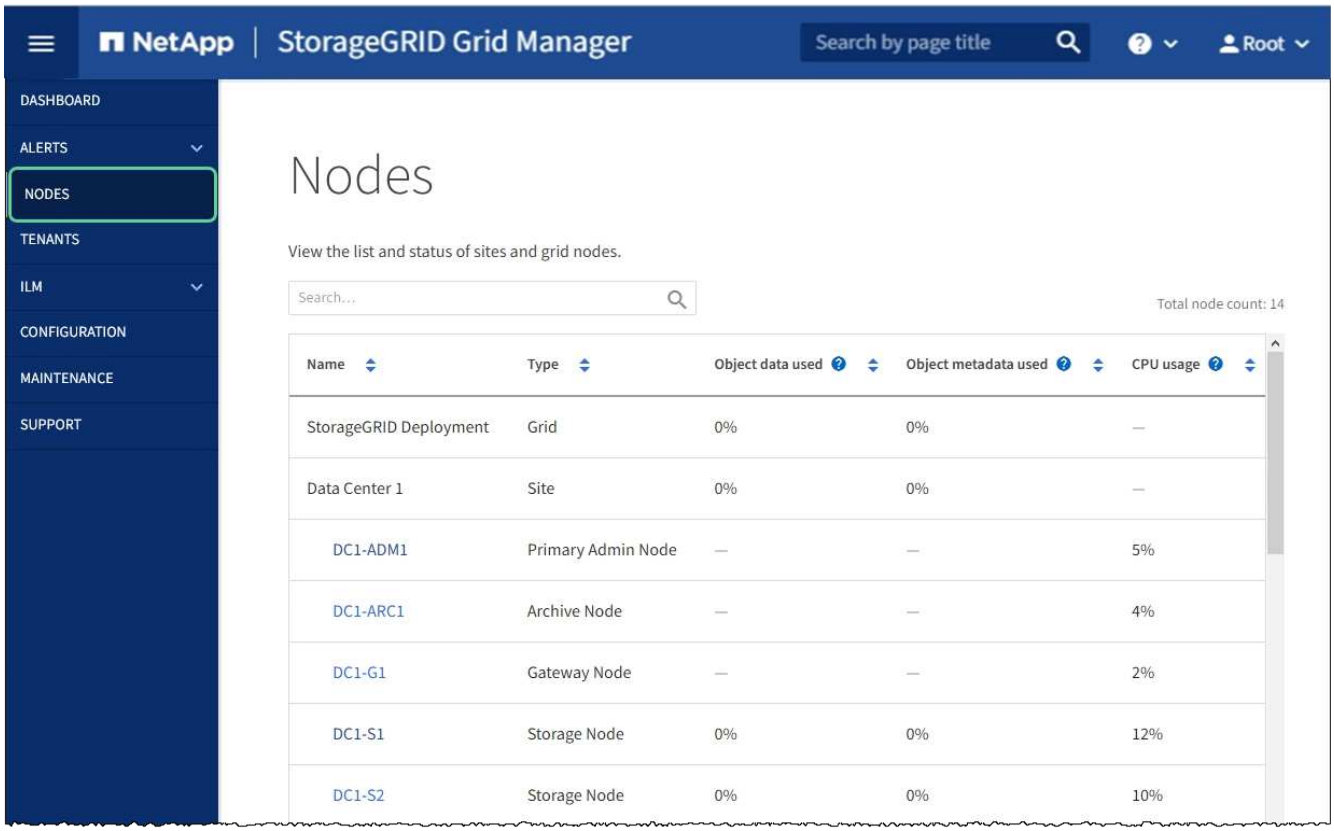
  清除密钥管理服务器配置

  清除 KMS 配置将从设备中删除数据，从而使其永远无法访问。此数据不可恢复。

2. 检查完节点加密状态后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：
   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

清除密钥管理服务器配置

清除密钥管理服务器（ KMS ）配置将禁用设备上的节点加密。清除 KMS 配置后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

您需要的内容

如果需要保留设备上的数据，则必须先执行节点停用操作步骤 或克隆节点，然后才能清除 KMS 配置。

清除 KMS 后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

停用节点 将其包含的任何数据移动到 StorageGRID 中的其他节点。

关于此任务

清除设备 KMS 配置将禁用节点加密，从而删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。然后，设备上的数据将被删除，并且设备将保持预安装状态。此过程不能逆转。

必须清除 KMS 配置：

- 在将设备安装到不使用 KMS 或使用其他 KMS 的其他 StorageGRID 系统之前，请先安装此设备。

如果您计划在使用相同 KMS 密钥的 StorageGRID 系统中重新安装设备节点，请勿清除 KMS 配置。

- 在恢复和重新安装 KMS 配置丢失且 KMS 密钥不可恢复的节点之前。
- 在退回您的站点上先前使用的任何设备之前。
- 停用已启用节点加密的设备后。

> 在清除 KMS 以将其数据移动到 StorageGRID 系统中的其他节点之前，请停用此设备。在停用设备之前清除 KMS 将导致数据丢失，并可能导致设备无法运行。

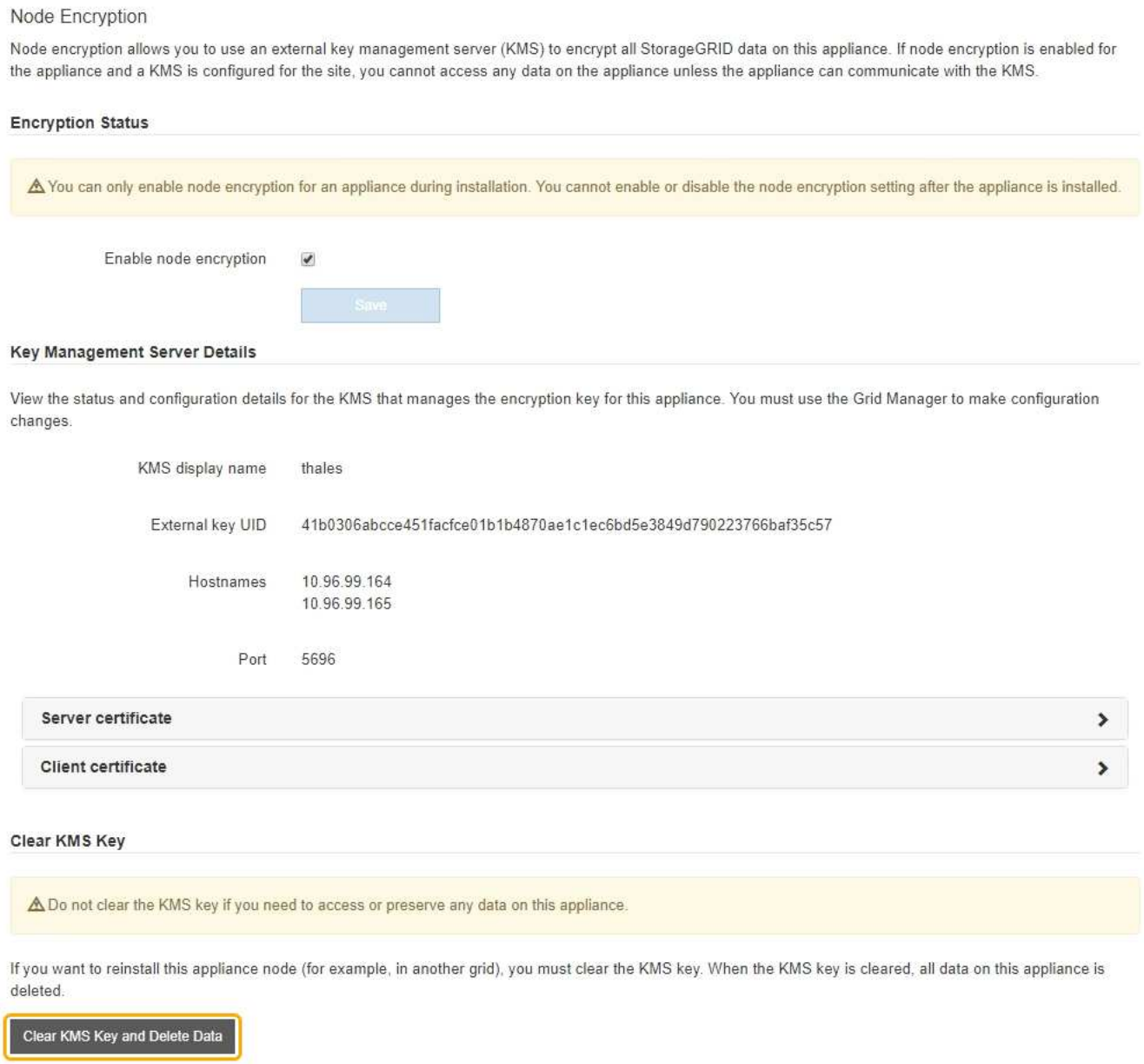
步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

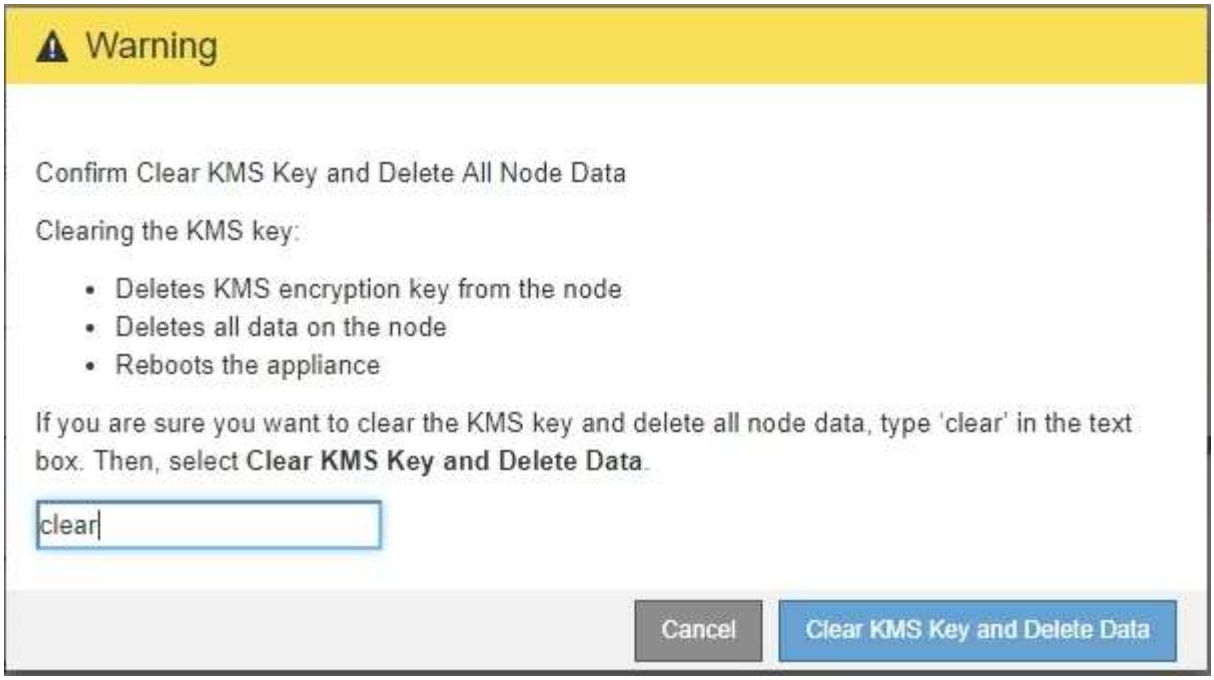
   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 节点加密 * 。



如果清除了 KMS 配置，则设备上的数据将被永久删除。此数据不可恢复。

3. 在窗口底部，选择 * 清除 KMS 密钥和删除数据 * 。
4. 如果确实要清除 KMS 配置，请键入 + ` * clear*` + 并选择 * 清除 KMS 密钥和删除数据 * 。



KMS 加密密钥和所有数据将从节点中删除，设备将重新启动。这可能需要长达 20 分钟。

5. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

6. 选择 * 配置硬件 * > * 节点加密 * 。
7. 验证是否已禁用节点加密，以及是否已从窗口中删除 * 密钥管理服务器详细信息 * 和 * 清除 KMS 密钥和删除数据 * 控件中的密钥和证书信息。

   在将设备重新安装到网格中之前，无法在设备上重新启用节点加密。

完成后

在设备重新启动并确认 KMS 已清除且设备处于预安装状态后，您可以从 StorageGRID 系统中物理删除此设备。有关的信息，请参见恢复和维护说明 准备要重新安装的设备。

相关信息

管理 StorageGRID

SG5600 存储设备

SG5600 设备：概述

StorageGRID SG5600 设备是一个集成的存储和计算平台，作为 StorageGRID 网格中的存储节点运行。

StorageGRID SG5600 设备包括以下组件：

组件	Description
E5600SG 控制器	计算服务器 E5600SG 控制器运行 Linux 操作系统和 StorageGRID 软件。 此控制器连接到以下项： • StorageGRID 系统的管理网络，网格网络和客户端网络 • E2700 控制器，使用双 SAS 路径（主动 / 主动），并将 E5600SG 控制器用作启动程序
E2700 控制器	存储控制器 E2700 控制器在单工模式下作为标准 E 系列存储阵列运行，并运行 SANtricity 操作系统（控制器固件）。 此控制器连接到以下项： • 安装 SANtricity 存储管理器的管理网络 • E5600SG 控制器，使用双 SAS 路径（主动 / 主动），以 E2700 控制器作为目标

SG5600 设备还包括以下组件，具体取决于型号：

组件	型号 **SG5612**	型号 **SG5660**
驱动器	12 个 NL-SAS 驱动器	60 个 NL-SAS 驱动器
机箱	DE1600 机箱，一种双机架单元（2U）机箱，用于容纳驱动器和控制器	DE6600 机箱，一种四机架单元（4U）机箱，用于容纳驱动器和控制器
电源和风扇	两个电源风扇箱	两个电源和两个风扇

E5600SG 控制器经过高度自定义，可在 StorageGRID 设备中使用。所有其他组件均按照 E 系列文档中所述的方式运行，除非这些说明中另有说明。

每个 StorageGRID 设备存储节点上可用的最大原始存储空间是固定的，具体取决于设备型号和配置。您不能通过添加具有额外驱动器的磁盘架来扩展可用存储。

StorageGRID 设备功能

StorageGRID SG5600 设备提供了一个集成的存储解决方案，用于创建新的 StorageGRID 系统或扩展现有系统的容量。

StorageGRID 设备可提供以下功能：

- 将 StorageGRID 存储节点计算和存储要素组合为一个高效的集成解决方案

- 简化存储节点的安装和配置，自动执行所需的大部分流程
- 提供具有两个机箱选项的高密度存储解决方案： 一个是 2U ，一个是 4U
- 直接使用连接到存储节点的 10-GbE IP 接口，而无需使用 FC 或 iSCSI 等中间存储接口
- 可以在使用 StorageGRID 设备和虚拟（基于软件）存储节点的混合网格环境中使用
- 包括预配置的存储，并预加载了 StorageGRID 设备安装程序（在 E5600SG 控制器上），用于现场部署和集成软件

硬件示意图

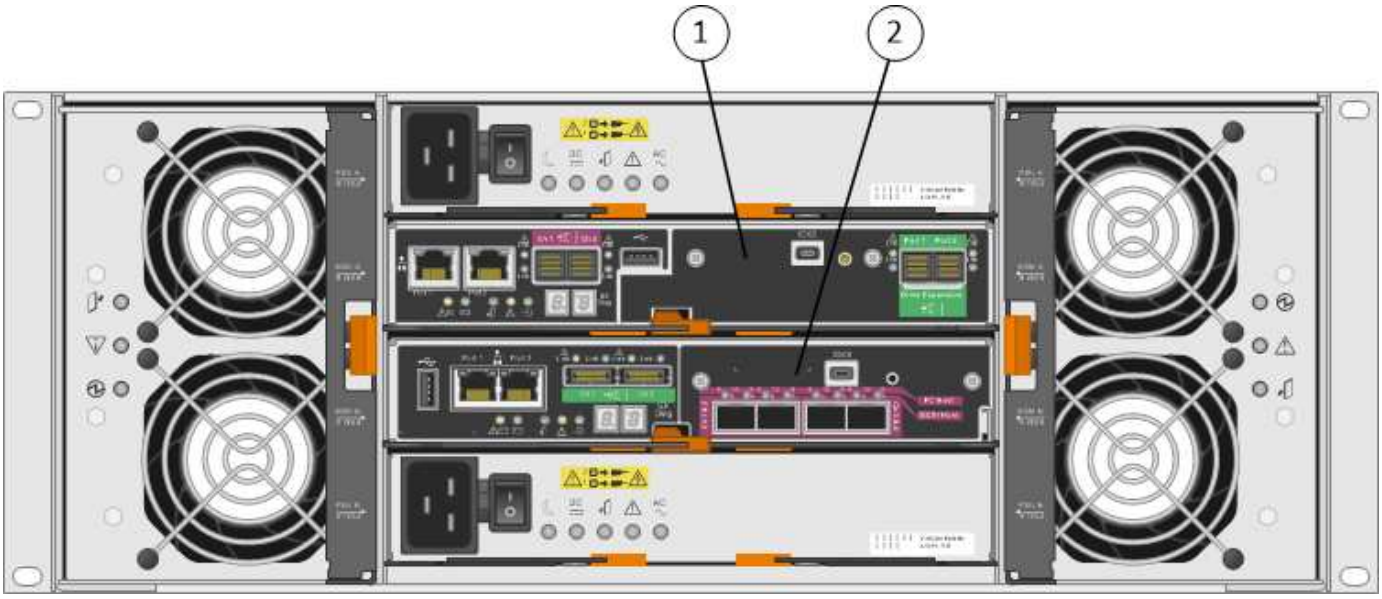
StorageGRID 设备的 SG5612 和 SG5660 型号都包括一个 E2700 控制器和一个 E5600SG 控制器。您应查看这些示意图，了解型号与控制器之间的差异。

SG5612 2U 型号： **E2700** 控制器和 **E5600SG** 控制器背面图

Callout	Description
1.	E2700 控制器
2.	E5600SG 控制器

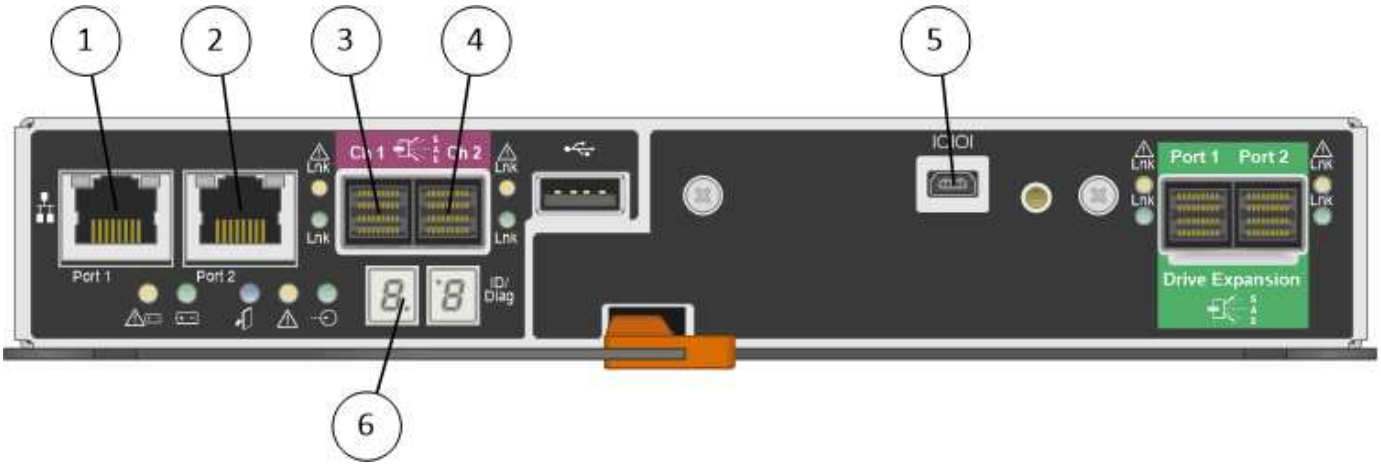
SG5660 4U 型号： **E2700** 控制器和 **E5600SG** 控制器背面图

E2700 控制器位于 E5600SG 控制器之上。



Callout	Description
1.	E2700 控制器
2.	E5600SG 控制器

E2700 控制器背面图

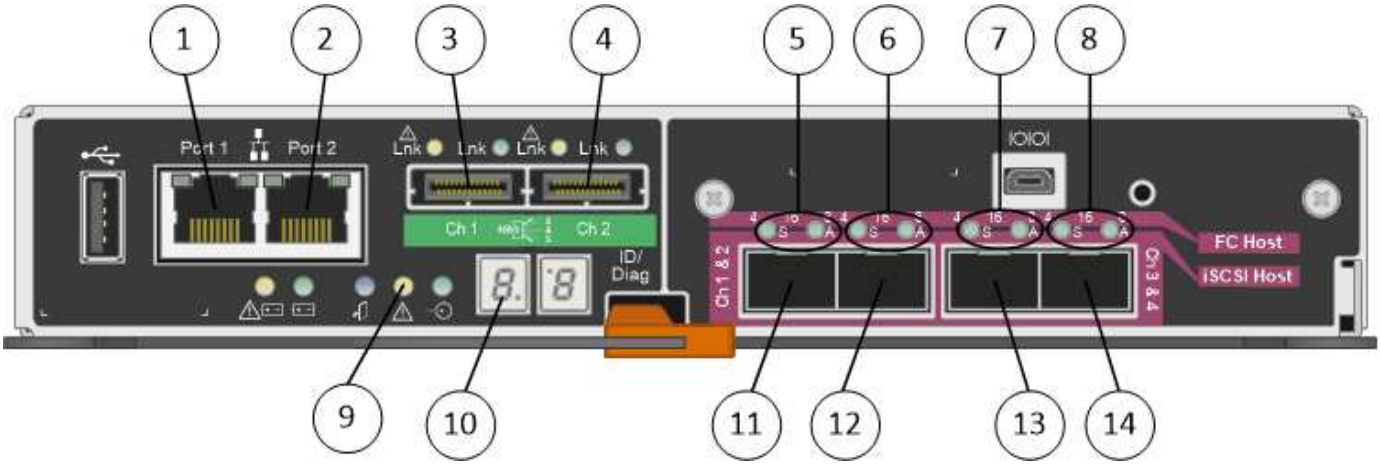


Callout	Description
1.	管理端口 1 （连接到安装 SANtricity 存储管理器的网络。）
2.	管理端口 2 （在安装期间用于连接到笔记本电脑。）
3.	SAS 互连端口 1
4.	SAS 互连端口 2

Callout	Description
5.	串行连接端口
6.	七段式显示

不使用 E2700 控制器背面标记为驱动器扩展（绿色）的两个 SAS 端口。StorageGRID 设备不支持扩展驱动器架。

E5600SG 控制器背面图



Callout	Description
1.	管理端口 1 连接到 StorageGRID 的管理网络。
2.	管理端口 2 选项： • 与管理端口 1 绑定，以便与 StorageGRID 的管理网络建立冗余连接。 • 保持未连接状态，并可用于临时本地访问（ IP 169.254.0.1 ）。 • 在安装期间，如果 DHCP 分配的 IP 地址不可用，请使用进行 IP 配置。
3.	SAS 互连端口 1
4.	SAS 互连端口 2
5.	10-GbE 网络端口 1 的故障和活动 LED
6.	10-GbE 网络端口 2 的故障和活动 LED

Callout	Description
7.	10-GbE 网络端口 3 的故障和活动 LED
8.	10-GbE 网络端口 4 的故障和活动 LED
9	需要引起注意的 LED
10	七段式显示
11.	10-GbE 网络端口 1
12	10-GbE 网络端口 2
13	10-GbE 网络端口 3
14	10-GbE 网络端口 4

StorageGRID 设备 E5600SG 控制器上的主机接口卡（ HIC ）仅支持 10-Gb 以太网连接。不能用于 iSCSI 连接。

安装和部署概述

您可以在首次部署 StorageGRID 时安装一个或多个 StorageGRID 设备，也可以稍后在扩展过程中添加设备存储节点。在恢复操作中，您可能还需要安装设备存储节点。

将 StorageGRID 存储设备添加到 StorageGRID 系统包括四个主要步骤：

1. 准备安装：
   - 正在准备安装站点
   - 打开包装箱的包装并检查包装箱中的物品
   - 获取其他设备和工具
   - 收集 IP 地址和网络信息
   - 可选：如果您计划对所有设备数据进行加密，请配置外部密钥管理服务器（ KMS ）。有关外部密钥管理的详细信息，请参见 StorageGRID 管理说明。
2. 安装硬件：
   - 注册硬件
   - 将设备安装到机柜或机架中
   - 安装驱动器（仅限 SG5660 ）
   - 为设备布线
   - 连接电源线并接通电源

- 查看启动状态代码

3. 配置硬件：
   - 访问 SANtricity 存储管理器，为 E2700 控制器上的管理端口 1 设置静态 IP 地址以及配置 SANtricity 存储管理器设置
   - 访问 StorageGRID 设备安装程序并配置连接到 StorageGRID 网络所需的链路和网络 IP 设置
   - 可选：如果您计划使用外部 KMS 对设备数据进行加密，请启用节点加密。
   - 可选：更改 RAID 模式。
4. 将设备部署为存储节点：

任务	请参见
在新的 StorageGRID 系统中部署设备存储节点	部署设备存储节点
将设备存储节点添加到现有 StorageGRID 系统	有关扩展 StorageGRID 系统的说明
在存储节点恢复操作中部署设备存储节点	恢复和维护说明

相关信息

准备安装（ SG5600 ）

安装硬件（ SG5600 ）

配置硬件（ SG5600 ）

扩展网格

恢复和维护

管理 StorageGRID

准备安装（ **SG5600** ）

准备安装 StorageGRID 设备需要准备站点并获取所有必需的硬件，缆线和工具。您还应收集 IP 地址和网络信息。

相关信息

Web 浏览器要求

准备站点（ **SG5600** ）

在安装设备之前，您必须确保要使用的站点和机柜或机架符合 StorageGRID 设备的规格。

步骤

1. 确认站点满足温度，湿度，海拔范围，气流，散热， 布线，电源和接地。有关详细信息，请参见 NetApp Hardware Universe 。

2. 获取一个 19 英寸（ 48.3 厘米）的机柜或机架，以适合此大小的磁盘架（不带缆线）：

设备型号	高度	宽度	深度	最大重量
SG5612 （ 12 个驱动器）	3.40 英寸 （ 8.64 厘米）	19.0 英寸 （ 48.26 厘米）	21.75 英寸 （ 55.25 厘米）	59.5 磅 （ 27 千克）
SG5660 （ 60 个驱动器）	7.00 英寸 （ 17.78 厘米）	17.75 英寸 （ 45.08 厘米）	32.50 英寸 （ 82.55 厘米）	236.2 磅 （ 107.1 千克）

3. 安装所需的任何网络交换机。有关兼容性信息，请参见 NetApp 互操作性表工具。

相关信息

"NetApp Hardware Universe"

"NetApp 互操作性"

打开包装箱（ **SG5600** ）

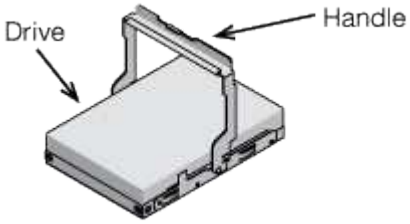
安装 StorageGRID 设备之前，请打开所有包装箱的包装，并将包装箱上的物品与包装清单上的物品进行比较。

- * SG5660 机箱，一个 4U 机箱，含 60 个驱动器 *

- * SG5612 机箱，一个 2U 机箱，含 12 个驱动器 *

- * 4U 挡板或 2U 端盖 *

- * NL-SAS 驱动器 *



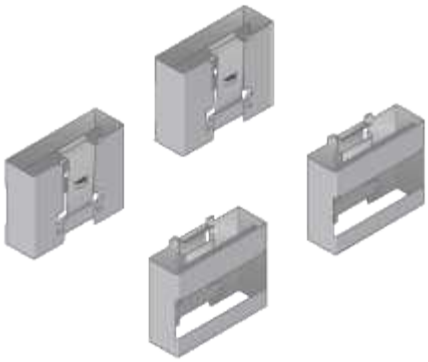
驱动器预装在 2U SG5612 中，但不安装在 4U SG5660 中，以确保运输安全。

- * E5600SG 控制器 *

- * E2700 控制器 *

- * 安装导轨和螺钉 *

- * 机箱手柄（仅限 4U 机箱） *



缆线和连接器

StorageGRID 设备的发货包括以下缆线和连接器：

- * 您所在国家或地区的电源线 *

设备随附两根交流电源线，用于连接到外部电源，例如墙上插座。您的机柜可能使用专用电源线，而不是设备随附的电源线。

- * SAS 互连缆线 *

两根 0.5 米 SAS 互连缆线，带迷你 SAS HD 和迷你 SAS 连接器。

方形连接器插入 E2700 控制器，而方形连接器插入 E5600SG 控制器。

获取其他设备和工具（ **SG5600** ）

在安装 SG5600 设备之前，请确认您拥有所需的所有附加设备和工具。

- * 螺丝刀 *

十字线编号2 把螺丝刀

中型平口螺丝刀

- * ESD 腕带 *

- * 以太网缆线 *

- * 以太网交换机 *

- * 服务笔记本电脑 *支持的 Web 浏览器

服务笔记本电脑要求

在安装 StorageGRID 设备硬件之前，您应检查服务笔记本电脑是否具有所需的最低资源。

硬件安装所需的服务笔记本电脑必须满足以下要求：

- Microsoft Windows 操作系统
- 网络端口
- 支持的 Web 浏览器
- NetApp SANtricity Storage Manager 11.40 或更高版本
- SSH 客户端（例如 PuTTY ）

相关信息

Web 浏览器要求

"NetApp 文档： SANtricity 存储管理器"

查看设备网络连接（ **SG5600** ）

在安装 StorageGRID 设备之前，您应了解可以将哪些网络连接到设备，以及如何使用每个控制器上的端口。

StorageGRID 设备网络

将 StorageGRID 设备部署为存储节点时，您可以将其连接到以下网络：

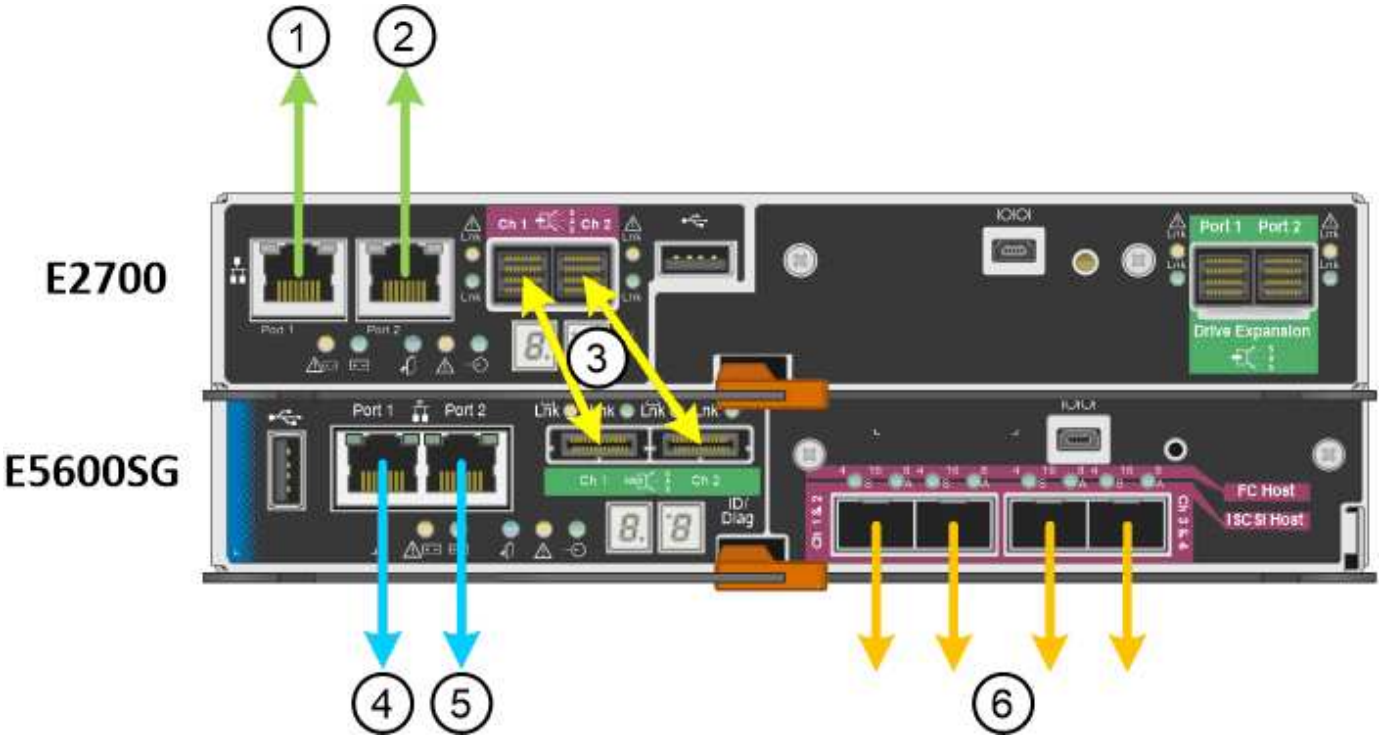
- * 适用于 StorageGRID 的网格网络 * ： 网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。网格网络为必填项。
- * 适用于 StorageGRID 的管理网络 * ： 管理网络是一个用于系统管理和维护的封闭网络。管理网络通常是一个专用网络，不需要在站点之间进行路由。管理网络是可选的。
- * 适用于 StorageGRID 的客户端网络 * ： 客户端网络是一种开放网络，用于访问客户端应用程序，包括 S3 和 Swift 。客户端网络可提供对网格的客户端协议访问，从而可以隔离和保护网格网络。客户端网络是可选的。
- * 适用于 SANtricity 存储管理器的管理网络 * （可选）： E2700 控制器连接到安装了 SANtricity 存储管理器的管理网络，可用于监控和管理设备中的硬件组件。此管理网络可以与 StorageGRID 的管理网络相同，也可以是一个独立的管理网络。

  如果未连接可选的 SANtricity 存储管理器网络，则可能无法使用某些 SANtricity 功能。

有关 StorageGRID 网络的详细信息，请参见 *Grid Primer* 。

StorageGRID 设备连接

安装 StorageGRID 设备时，必须将两个控制器彼此连接并连接到所需的网络。此图显示了 SG5660 中的两个控制器，其中 E2700 控制器位于顶部， E5600SG 控制器位于底部。在 SG5612 中， E2700 控制器位于 E5600SG 控制器的左侧。



项目	**Port**	端口类型	功能
1.	E2700 控制器上的管理端口 1	1 Gb （RJ-45）以太网	将 E2700 控制器连接到安装 SANtricity 存储管理器的网络。
2.	E2700 控制器上的管理端口 2	1 Gb （RJ-45）以太网	在安装期间将 E2700 控制器连接到服务笔记本电脑。
3.	每个控制器上有两个 SAS 互连端口，分别标记为通道 1 和通道 2	E2700 控制器： mini-SAS-HD E5600SG 控制器：迷你 SAS	将两个控制器彼此连接。
4.	E5600SG 控制器上的管理端口 1	1 Gb （RJ-45）以太网	将 E5600SG 控制器连接到 StorageGRID 管理网络。

项目	Port	端口类型	功能
5.	E5600SG 控制器上的管理端口 2	1 Gb （ RJ-45 ）以太网	• 如果要与管理网络建立冗余连接，则可以与管理端口 1 绑定。 • 可以保持未连接状态，并可用于临时本地访问（ IP 169.254.0.1 ）。 • 如果 DHCP 分配的 IP 地址不可用，则可以在安装期间使用此 IP 地址将 E5600SG 控制器连接到服务笔记本电脑。
6.	E5600SG 控制器上的四个网络端口	10-GbE （光纤）	连接到网格网络和 StorageGRID 客户端网络。请参见 "`E5600SG 控制器的 10-GbE 端口连接 "。`

相关信息

E5600SG 控制器端口的端口绑定模式

收集安装信息（ SG5600 ）

缆线设备（ SG5600 ）

网络连接准则

安装 VMware

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

E5600SG 控制器端口的端口绑定模式

在为 E5600SG 控制器端口配置网络链路时，您可以对连接到网格网络和可选客户端网络的 10-GbE 端口以及连接到可选管理网络的 1-GbE 管理端口使用端口绑定。端口绑定可在 StorageGRID 网络和设备之间提供冗余路径，从而有助于保护数据。

相关信息

配置网络链路（ SG5600 ）

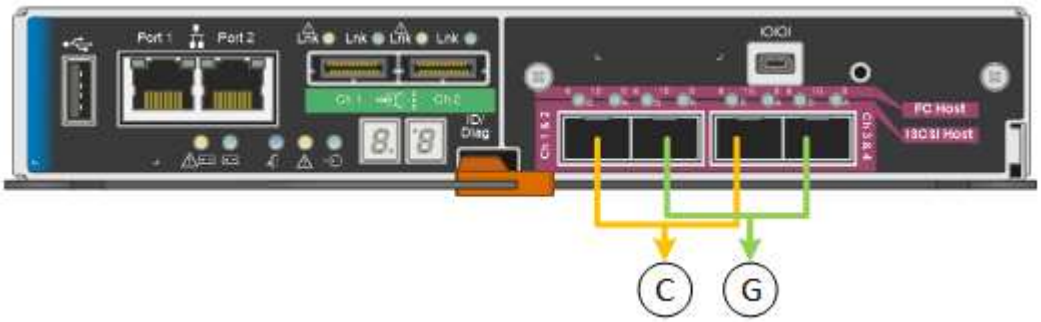
10-GbE 端口的网络绑定模式

E5600SG 控制器上的 10-GbE 网络端口支持网格网络和客户端网络连接的固定端口绑定模

式或聚合端口绑定模式。

固定端口绑定模式

固定模式是 10-GbE 网络端口的默认配置。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

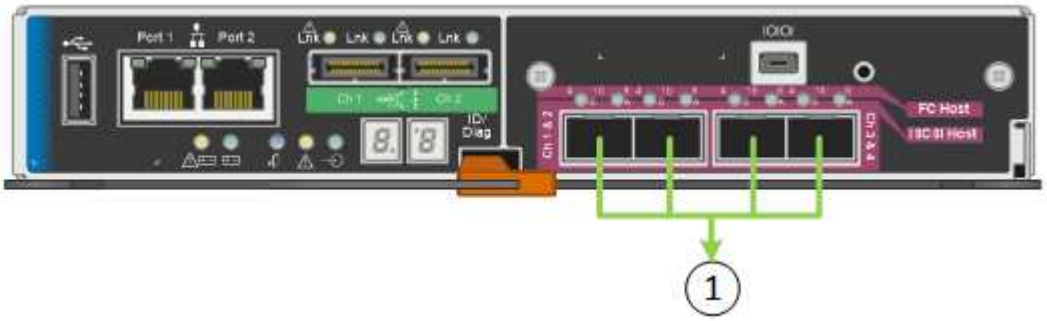
使用固定端口绑定模式时，可以使用主动备份模式或链路聚合控制协议模式（ LACP 802.3ad ）绑定端口。

- 在主动备份模式（默认）下，一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。端口 4 为端口 2 （网格网络）提供备份路径，端口 3 为端口 1 （客户端网络）提供备份路径。
- 在 LACP 模式下，每对端口在控制器和网络之间形成一个逻辑通道，从而提高吞吐量。如果一个端口发生故障，另一个端口将继续提供通道。吞吐量会降低，但连接不会受到影响。

如果不需要冗余连接，则每个网络只能使用一个端口。但是，请注意，安装 StorageGRID 后，网格管理器中将发出警报，指示已拔下缆线。您可以安全地确认此警报以将其清除。

聚合端口绑定模式

聚合端口绑定模式可显著提高每个 StorageGRID 网络的吞吐量，并提供额外的故障转移路径。



Callout	哪些端口已绑定
1.	所有连接的端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

如果您计划使用聚合端口绑定模式：

- 您必须使用 LACP 网络绑定模式。
- 您必须为每个网络指定唯一的 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。
- 这些端口必须连接到可支持 VLAN 和 LACP 的交换机。如果多个交换机参与 LACP 绑定，则这些交换机必须支持多机箱链路聚合组（ MLAG ）或等效项。
- 您必须了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。

如果您不想使用全部四个 10-GbE 端口，则可以使用一个，两个或三个端口。如果使用多个端口，则在其中一个 10-GbE 端口发生故障时，某些网络连接将保持可用的可能性最大。

如果您选择使用的端口少于四个、请注意、在安装设备节点后、可能会在网格管理器中触发*服务设备链路已关闭*警报、指示已拔下电缆。您可以安全地为触发的警报禁用此警报规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。

1-GbE 管理端口的网络绑定模式

对于 E5600SG 控制器上的两个 1-GbE 管理端口，您可以选择独立网络绑定模式或主动备份网络绑定模式来连接到可选的管理网络。

在独立模式下，只有管理端口 1 连接到管理网络。此模式不提供冗余路径。管理端口 2 未连接，可用于临时本地连接（使用 IP 地址 169.254.0.1 ）

在主动备份模式下，管理端口 1 和 2 均连接到管理网络。一次只有一个端口处于活动状态。如果活动端口发生故障，其备份端口会自动提供故障转移连接。将这两个物理端口绑定到一个逻辑管理端口可提供指向管理网络的冗余路径。

如果在将 1-GbE 管理端口配置为主动备份模式后需要临时本地连接到 E5600SG 控制器，请从两个管理端口拔下缆线，将临时缆线插入管理端口 2 ，然后使用 IP 地址 169.254.0.1 访问此设备。

收集安装信息（ **SG5600** ）

在安装和配置 StorageGRID 设备时，您必须做出决策并收集有关以太网交换机端口， IP 地址以及端口和网络绑定模式的信息。

关于此任务

您可以使用下表记录连接到设备的每个网络的信息。安装和配置硬件需要这些值。

将 **E2700** 控制器连接到 **SANtricity** 存储管理器所需的信息

您必须将 E2700 控制器连接到要用于 SANtricity 存储管理器的管理网络。

所需信息	您的价值
要连接到管理端口 1 的以太网交换机端口	
管理端口 1 的 MAC 地址（印在端口 P1 附近的标签上）	
DHCP 为管理端口 1 分配的 IP 地址（如果在启动后可用） • 注： * 如果要连接到 E2700 控制器的网络包含 DHCP 服务器，则网络管理员可以使用 MAC 地址确定 DHCP 服务器分配的 IP 地址。	
速度和双工模式 • 注： * 您必须确保 SANtricity 存储管理器管理网络的以太网交换机设置为自动协商。	必须为： • 自动协商（默认）
IP 地址格式	选择一项： • IPv4 • IPv6
您计划在管理网络上用于设备的静态 IP 地址	对于 IPv4 ： • IPv4 地址： • 子网掩码： • 网关 对于 IPv6 ： • IPv6 地址： • 可路由的 IP 地址： • E2700 控制器路由器 IP 地址：

将 **E5600SG** 控制器连接到管理网络所需的信息

StorageGRID 管理网络是一个可选网络，用于系统管理和维护。此设备使用 E5600SG 控制器上的 1-GbE 管理端口连接到管理网络。

所需信息	您的价值
已启用管理网络	选择一项： • 否 • 是（默认）
网络绑定模式	选择一项： • 独立 • 主动备份
管理端口 1 （ P1 ）的交换机端口	
管理端口 2 的交换机端口（ P2 ；仅限主动备份网络绑定模式）	
管理端口 1 的 MAC 地址（印在端口 P1 附近的标签上）	
DHCP 为管理端口 1 分配的 IP 地址（如果在启动后可用） • 注： * 如果管理网络包含 DHCP 服务器，则 E5600SG 控制器会在启动后在其七段显示器上显示 DHCP 分配的 IP 地址。您还可以使用 MAC 地址查找分配的 IP ，从而确定 DHCP 分配的 IP 地址。	• IPv4 地址（ CIDR ）： • 网关
您计划在管理网络上用于设备存储节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
管理网络子网（ CIDR ）	

在 **E5600SG** 控制器上连接和配置 **10-GbE** 端口所需的信息

E5600SG 控制器上的四个 10-GbE 端口连接到 StorageGRID 网格网络和客户端网络。

有关这些端口选项的详细信息，请参见 "E5600SG 控制器的 10-GbE 端口连接 " 。

所需信息	您的价值
端口绑定模式	选择一项： • FIXED （默认） • 聚合
端口 1 的交换机端口（固定模式的客户端网络）	
端口 2 的交换机端口（固定模式的网格网络）	
端口 3 的交换机端口（固定模式的客户端网络）	
端口 4 的交换机端口（固定模式的网格网络）	

将 **E5600SG** 控制器连接到网格网络所需的信息

适用于 StorageGRID 的网格网络是一个必需的网络，用于所有内部 StorageGRID 流量。此设备使用 E5600SG 控制器上的 10-GbE 端口连接到网格网络。

有关这些端口选项的详细信息，请参见 "E5600SG 控制器的 10-GbE 端口连接 " 。

所需信息	您的价值
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为网格网络分配的 IP 地址（如果在启动后可用） • 注： * 如果网格网络包含 DHCP 服务器，则 E5600SG 控制器会在启动后在其七段显示屏上显示为网格网络分配的 DHCP IP 地址。	• IPv4 地址（ CIDR ）： • 网关

所需信息	您的价值
您计划用于网格网络上设备存储节点的静态 IP 地址 • 注： * 如果您的网络没有网关，请为此网关指定相同的静态 IPv4 地址。	• IPv4 地址（ CIDR ）： • 网关
网格网络子网（ CIDR ） • 注： * 如果未启用客户端网络，则控制器上的默认路由将使用此处指定的网关。	

将 **E5600SG** 控制器连接到客户端网络所需的信息

适用于 StorageGRID 的客户端网络是一个可选网络，用于提供对网格的客户端协议访问。此设备使用 E5600SG 控制器上的 10-GbE 端口连接到客户端网络。

有关这些端口选项的详细信息，请参见 "E5600SG 控制器的 10-GbE 端口连接 " 。

所需信息	您的价值
已启用客户端网络	选择一项： • 否（默认） • 是的。
网络绑定模式	选择一项： • Active-Backup （默认） • LACP （ 802.3ad ）
已启用 VLAN 标记	选择一项： • 否（默认） • 是的。
VLAN 标记（如果启用了 VLAN 标记）	输入一个介于 0 到 4095 之间的值：
DHCP 为客户端网络分配的 IP 地址（如果在启动后可用）	• IPv4 地址（ CIDR ）： • 网关
您计划在客户端网络上用于设备存储节点的静态 IP 地址 • 注： * 如果启用了客户端网络，则控制器上的默认路由将使用此处指定的网关。	• IPv4 地址（ CIDR ）： • 网关

相关信息

查看设备网络连接（ SG5600 ）

配置硬件（ SG5600 ）

E5600SG 控制器端口的端口绑定模式

安装硬件（ SG5600 ）

硬件安装包括几项主要任务，包括安装硬件组件，为这些组件布线以及配置端口。

注册硬件

注册设备硬件具有支持优势。

步骤

1. 找到机箱序列号。

   您可以在装箱单上，确认电子邮件中或打开设备包装后在设备上找到此编号。

2. 访问 NetApp 支持站点，网址为 "mysupport.netapp.com"。
3. 确定是否需要注册硬件：

如果您是 ...	请按照以下步骤操作 ...
现有 NetApp 客户	a. 使用您的用户名和密码登录。 b. 选择 * 产品 * > * 我的产品 * 。 c. 确认新序列号已列出。 d. 如果不是，请按照适用于新 NetApp 客户的说明进行操作。
NetApp 新客户	a. 单击 * 立即注册 * ，然后创建帐户。 b. 选择 * 产品 * > * 注册产品 * 。 c. 输入产品序列号和请求的详细信息。 注册获得批准后，您可以下载所需的任何软件。审批过程可能需要长达 24 小时。

在机柜或机架中安装设备（ SG5600 ）

您必须在机柜或机架中安装导轨，然后将设备滑入导轨。如果您使用的是 SG5660 ，则还必须在安装设备后安装驱动器。

您需要的内容

- 您已查看包装盒中的安全通知文档，并了解移动和安装硬件的预防措施。
- 您已获得硬件的 E 系列安装说明。

从机架，机柜或机架的底部安装硬件，以防止设备发生倾翻。

在装满驱动器后， SG5612 重约 60 磅（ 27 千克）。要安全移动 SG5612 ，需要两个人或一台机械升降机。

SG5660 重约 132 磅（ 60 千克），未安装驱动器。要安全移动空的 SG5660 ，需要四个人或一台机械升降机。

为避免损坏硬件，如果安装了驱动器，请勿移动 SG5660 。在移动设备之前，您必须删除所有驱动器。

关于此任务

要在机柜或机架中安装 SG5660 设备，请完成以下任务。

- * 安装安装导轨 *

  将安装导轨安装在机柜或机架中。

  请参见 E2700 或 E5600 的 E 系列安装说明。

- * 将设备安装在机柜或机架中 *

  将设备滑入机柜或机架，然后将其固定。

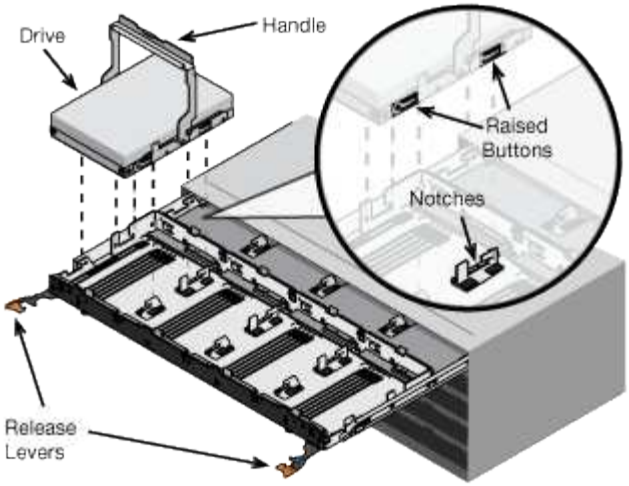
  如果您要用手提起 SG5660 ，请将四个手柄连接到机箱两侧。将设备滑入导轨时，请取下这些手柄。

- * 安装驱动器 *

  如果您使用的是 SG5660 ，请在 5 个驱动器抽盒中的每个抽盒中安装 12 个驱动器。

  您必须安装全部 60 个驱动器，以确保正常运行。

  a. 戴上 ESD 腕带，然后将驱动器从其包装中取出。
  b. 释放顶部驱动器抽盒上的拉杆，然后使用拉杆将抽盒滑出。
  c. 将驱动器把手提起至垂直位置，并将驱动器上的按钮与抽盒上的缺口对齐。



d. 轻按驱动器顶部，向下旋转驱动器把手，直到驱动器卡入到位。

e. 安装前 12 个驱动器后，通过推动中间并轻轻合上两个拉杆，将抽盒滑回原位。

f. 对其他四个抽盒重复上述步骤。

- * 连接前挡板 *
- SG5612*： 将左端和右端盖连接到正面。
- SG5660*： 将挡板连接到正面。

相关信息

"《 E2700 控制器驱动器托盘和相关驱动器托盘安装指南》"

"《 E5600 控制器驱动器托盘和相关驱动器托盘安装指南》"

缆线设备（ **SG5600** ）

您必须使用 SAS 互连缆线将两个控制器彼此连接，将管理端口连接到相应的管理网络，并将 E5600SG 控制器上的 10 GbE 端口连接到网格网络和适用于 StorageGRID 的可选客户端网络。

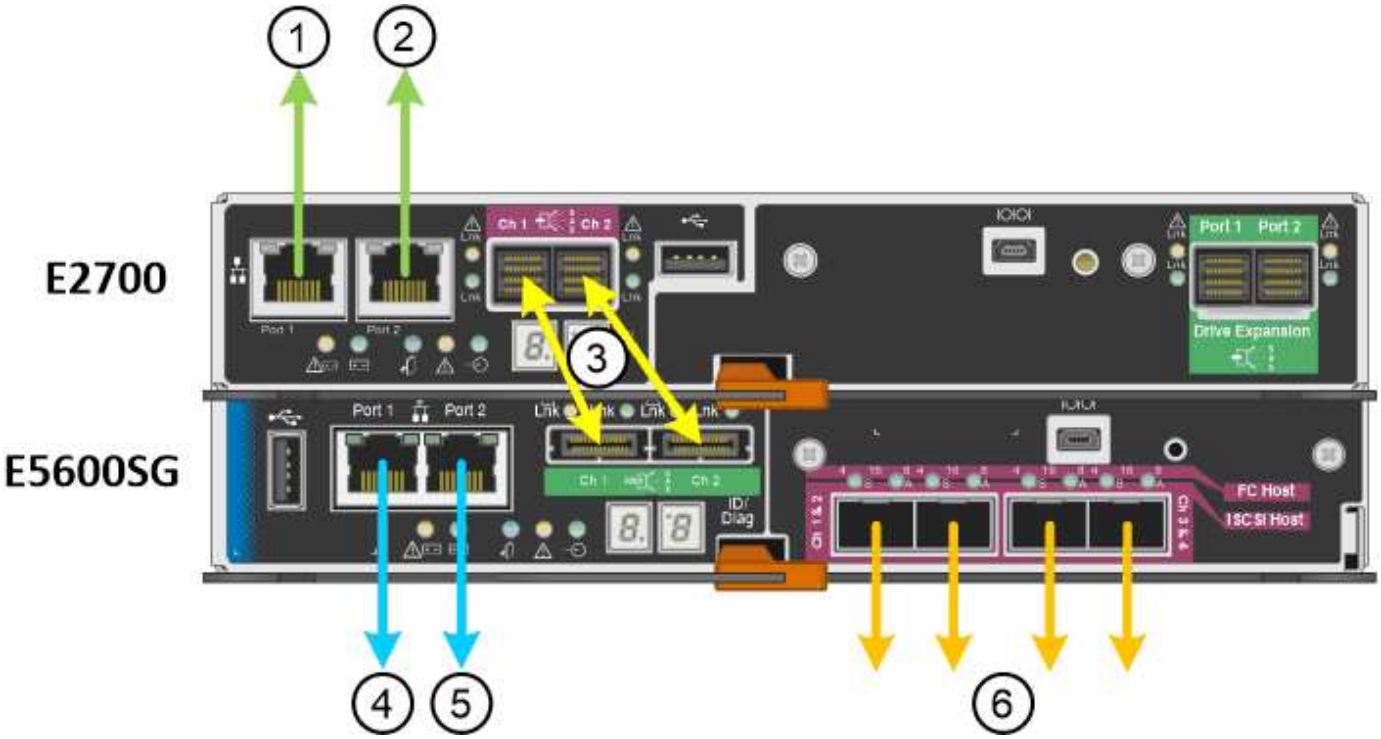
您需要的内容

- 您有用于连接管理端口的以太网缆线。
- 您可以使用光缆连接四个 10-GbE 端口（设备不提供这些端口）。

* 受到激光辐射的风险 * —请勿拆卸或卸下 SFP 收发器的任何部件。您可能受到激光辐射的影响。

关于此任务

连接缆线时，请参见下图，其中显示了顶部的 E2700 控制器和底部的 E5600SG 控制器。此图显示的是 SG5660 型号； SG5612 型号中的控制器是并排控制的，而不是堆栈控制。



项目	**Port**	端口类型	功能
1.	E2700 控制器上的管理端口 1	1 Gb （RJ-45）以太网	将 E2700 控制器连接到安装 SANtricity 存储管理器的网络。
2.	E2700 控制器上的管理端口 2	1 Gb （RJ-45）以太网	在安装期间将 E2700 控制器连接到服务笔记本电脑。
3.	每个控制器上有两个 SAS 互连端口，分别标记为通道 1 和通道 2	E2700 控制器： mini-SAS-HD E5600SG 控制器：迷你 SAS	将两个控制器彼此连接。
4.	E5600SG 控制器上的管理端口 1	1 Gb （RJ-45）以太网	将 E5600SG 控制器连接到 StorageGRID 管理网络。

项目	Port	端口类型	功能
5.	E5600SG 控制器上的管理端口 2	1 Gb （ RJ-45 ）以太网	• 如果要与管理网络建立冗余连接，则可以与管理端口 1 绑定。 • 可以保持未连接状态，并可用于临时本地访问（ IP 169.254.0.1 ）。 • 如果 DHCP 分配的 IP 地址不可用，则可以在安装期间使用此端口将 E5600SG 控制器连接到服务笔记本电脑。
6.	E5600SG 控制器上的四个网络端口	10-GbE （光纤）	将 E5600SG 控制器连接到网格网络和 StorageGRID 的客户端网络（如果使用）。这些端口可以绑定在一起，以便为控制器提供冗余路径。

步骤

1. 使用两根 SAS 互连缆线将 E2700 控制器连接到 E5600SG 控制器。

连接此端口 ...	到此端口 ...
E2700 控制器上的 SAS 互连端口 1 （标记为通道 1 ）	E5600SG 控制器上的 SAS 互连端口 1 （标记为通道 1 ）
E2700 控制器上的 SAS 互连端口 2 （标记为通道 2 ）	E5600SG 控制器上的 SAS 互连端口 2 （标记为通道 2 ）

对于 E2700 控制器，使用方形连接器（ mini-SAS HD ）；对于 E5600SG 控制器，使用方形连接器（ mini-SAS ）。

确保 SAS 连接器上的拉片位于底部，然后小心地插入每个连接器，直到其卡入到位。如果存在任何电阻，请勿推动连接器。继续操作前，请验证拉片的位置。

2. 使用以太网缆线将 E2700 控制器连接到安装了 SANtricity 存储管理器软件的管理网络。

连接此端口 ...	到此端口 ...
E2700 控制器上的端口 1 （左侧的 RJ-45 端口）	用于 SANtricity 存储管理器的管理网络上的交换机端口

连接此端口 ...	到此端口 ...
E2700 控制器上的端口 2	服务笔记本电脑（如果不使用 DHCP ）

3. 如果您计划使用 StorageGRID 管理网络，请使用以太网缆线连接 E5600SG 控制器。

连接此端口 ...	到此端口 ...
E5600SG 控制器上的端口 1 （左侧的 RJ-45 端口）	StorageGRID 管理网络上的交换机端口
E5600SG 控制器上的端口 2	服务笔记本电脑（如果不使用 DHCP ）

4. 使用光缆和 SFP+ 收发器将 E5600SG 控制器上的 10-GbE 端口连接到相应的网络交换机。
   - 如果您计划使用固定端口绑定模式（默认），请将端口连接到 StorageGRID 网格和客户端网络，如表所示。

Port	连接到 ...
端口 1	客户端网络（可选）
端口 2	网格网络
端口 3	客户端网络（可选）
端口 4	网格网络

   - 如果您计划使用聚合端口绑定模式，请将一个或多个网络端口连接到一个或多个交换机。您应至少连接四个端口中的两个，以避免发生单点故障。如果在一个 LACP 绑定中使用多个交换机，则这些交换机必须支持 MLAG 或等效项。

相关信息

E5600SG 控制器端口的端口绑定模式

访问 StorageGRID 设备安装程序

连接交流电源线（ **SG5600** ）

您必须将交流电源线连接到外部电源和每个控制器上的交流电源连接器。连接电源线后，您可以打开电源。

您需要的内容

在连接电源之前，两个设备电源开关都必须关闭。

* 电击风险 * —在连接电源线之前，请确保设备上的两个电源开关均已关闭。

关于此任务

- 每个电源都应使用单独的电源。

  连接到独立电源可保持电源冗余。

- 您可以使用控制器随附的电源线以及目标国家或地区使用的典型插座，例如无中断电源（ UPS ）的墙上插座。

  但是，这些电源线不适用于大多数符合环境影响评估的机柜。

步骤

1. 关闭机箱或机箱中的电源开关。
2. 关闭控制器上的电源开关。
3. 将机柜中的主电源线连接到外部电源。
4. 将电源线连接到每个控制器上的交流电源连接器。

打开电源（ **SG5600** ）

打开机箱电源可为两个控制器供电。

步骤

1. 打开机箱背面的两个电源开关。

   通电时，控制器上的 LED 会间歇性亮起和熄灭。

   启动过程可能需要长达十分钟才能完成。在初始启动序列期间，控制器会多次重新启动，从而导致风扇上升和下降，并且 LED 会闪烁。

2. 检查每个控制器上的电源 LED 和主机链路活动 LED ，确认电源已打开。
3. 等待所有驱动器显示持久绿色 LED ，指示它们已联机。
4. 检查机箱正面和背面是否有绿色 LED 。

   如果您看到任何琥珀色 LED ，请记下其位置。

5. 查看 E5600SG 控制器的七段显示屏。

   此显示内容将显示 * 。 HO* ，后跟两位数的重复序列。

   ```
   HO -- IP address for Admin Network -- IP address for Grid Network HO
   ```

   在此序列中，第一组数字是为控制器的管理端口 1 分配的 DHCP IP 地址。此地址用于将控制器连接到 StorageGRID 的管理网络。第二组数字是 DHCP 分配的 IP 地址，用于将设备连接到用于 StorageGRID 的网格网络。

   ⓘ 如果无法使用 DHCP 分配 IP 地址，则会显示 0.0.0.0 。

查看 **SG5600** 控制器的启动状态并查看错误代码

每个控制器上的七段显示会显示设备启动时，硬件初始化时以及硬件出现故障且必须退出初始化时的状态和错误代码。如果您要监控进度或进行故障排除，则应查看显示的代码顺序。

关于此任务

E5600SG 控制器的状态和错误代码与 E2700 控制器的状态和错误代码不同。

步骤

1. 在启动期间，查看七段显示器上显示的代码以监控进度。
2. 要查看 E5600SG 控制器的错误代码，请参见七段显示状态和错误代码信息。
3. 要查看 E2700 控制器的错误代码，请参见支持站点上的 E2700 控制器文档。

相关信息

E5600SG 控制器七段显示代码

"NetApp 文档： E2700 系列"

E5600SG 控制器七段显示代码

E5600SG 控制器上的七段显示在设备启动和硬件初始化期间显示状态和错误代码。您可以使用这些代码确定状态并对错误进行故障排除。

查看 E5600SG 控制器上的状态和错误代码时，您应查看以下类型的代码：

- * 常规启动代码 *

  表示标准启动事件。

- * 正常启动代码 *

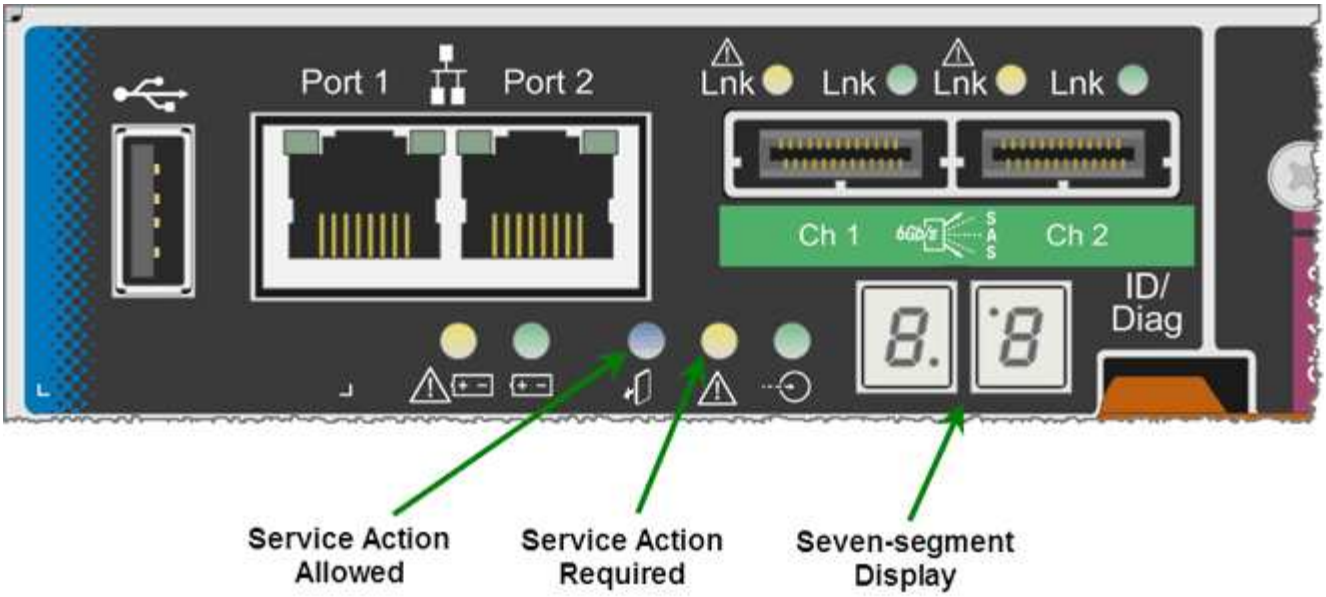
  表示设备中发生的正常启动事件。

- * 错误代码 *

  指示启动事件期间的问题。

StorageGRID 仅控制 E5600SG 控制器上的以下 LED ，并且仅在 StorageGRID 设备安装程序启动后才控制此 LED ：

- 允许服务操作 LED
- 需要执行服务操作 LED
- 七段式显示



StorageGRID 设备不会使用七段显示中的小数点：

- 与最小有效位数相邻的小数点上限为平台诊断 LED 。

  在重置和初始硬件配置期间会启用此功能。否则，它将关闭。

- 与最重要数字相邻的小数点下限将关闭。

要诊断其他问题，您可能需要查看以下资源：

- 要查看所有其他硬件和环境诊断信息，请参见 E 系列操作系统硬件诊断。

  其中包括查找电源，温度和磁盘驱动器等硬件问题。该设备依靠 E 系列操作系统监控所有平台环境状态。

- 要确定固件和驱动程序问题，请查看 SAS 和网络端口上的链路指示灯。

  有关详细信息，请参见 E 系列 E5600 文档。

常规启动代码

在启动期间或硬件硬重置后，硬件初始化期间，允许服务操作和需要服务操作 LED 亮起。七段显示屏显示一系列代码，这些代码对于 E 系列硬件是相同的，而不是特定于 E5600SG 控制器的。

在启动期间，现场可编程门阵列（ Field Programmable Gate Array ， FPGA ）可控制硬件的功能和初始化。

代码	指示
19	FPGA 初始化。
68	FPGA 初始化。
…	FPGA 初始化。这是一个快速连续的代码。

代码	指示
AA.	平台 BIOS 启动。
FF	BIOS 启动完成。这是 E5600SG 控制器初始化和管理 LED 以指示状态之前的中间状态。

出现 AA 和 FF 代码后，将显示正常启动代码或错误代码。此外，允许服务操作和需要服务操作 LED 也会关闭。

正常启动代码

这些代码按时间顺序表示设备中发生的正常启动事件。

代码	指示
您好	主启动脚本已启动。
p	平台 FPGA 固件正在检查更新。
HP	主机接口卡（ HIC ）正在检查更新。
RB	固件更新后，系统将根据需要重新启动。
FP	固件更新检查已完成。启动与 E2700 控制器进行通信和管理的进程（ utmagent ）。此过程有利于设备配置。
他	系统正在与 E 系列操作系统同步。
HC	正在检查 StorageGRID 安装。
好的	正在进行安装管理和主动连接。
HA	Linux 操作系统和 StorageGRID 正在运行。

E5600SG 控制器错误代码

这些代码表示设备启动时 E5600SG 控制器上可能显示的错误情况。如果发生特定的低级硬件错误，则会显示其他两位十六进制代码。如果其中任何一个代码持续一两秒以上，或者您无法通过执行规定的故障排除过程之一来解决此错误，请联系技术支持。

代码	指示
22.	在任何启动设备上均未找到主启动记录。

代码	指示
23	未安装 SATA 驱动器。
2A ， 2B	总线卡滞，无法读取 DIMM SPD 数据。
40	DIMM 无效。
41.	DIMM 无效。
42	内存测试失败。
51	SPD 读取失败。
92 到 96	PCI 总线初始化。
A0 到 A3	SATA 驱动器初始化。
AB	备用启动代码。
AE	正在启动操作系统。
EA	DDR3 培训失败。
E8.	未安装内存。
欧盟	未找到安装脚本。
EP	"ManagementSGa" 代码指示与 E2700 控制器的 pregrid 通信失败。

相关信息

硬件安装故障排除（ SG5600 ）

"NetApp 支持"

配置硬件（ **SG5600** ）

为设备接通电源后，您必须配置 SANtricity 存储管理器，该软件将用于监控硬件。您还必须配置 StorageGRID 要使用的网络连接。

配置 **StorageGRID** 连接（ **SG5600** ）

在将 StorageGRID 设备部署为 StorageGRID 网格中的存储节点之前，必须先配置设备与

计划使用的网络之间的连接。您可以通过浏览到 StorageGRID 设备安装程序来配置网络连接，该安装程序包含在 E5600SG 控制器（设备中的计算控制器）上。

访问 **StorageGRID** 设备安装程序

您必须访问 StorageGRID 设备安装程序来配置设备与三个 StorageGRID 网络之间的连接：网格网络，管理网络（可选）和客户端网络（可选）。

您需要的内容

- 您正在使用 支持的 Web 浏览器。
- 此设备已连接到您计划使用的所有 StorageGRID 网络。
- 您知道这些网络上设备的 IP 地址，网关和子网。
- 您已配置计划使用的网络交换机。

关于此任务

首次访问 StorageGRID 设备安装程序时，您可以使用管理网络的 DHCP 分配的 IP 地址（假设设备已连接到管理网络）或网格网络的 DHCP 分配的 IP 地址。首选使用管理网络的 IP 地址。否则，如果使用网格网络的 DHCP 地址访问 StorageGRID 设备安装程序，则在更改链接设置和输入静态 IP 时，可能会与 StorageGRID 设备安装程序断开连接。

步骤

1. 在管理网络（如果已连接）或网格网络（如果未连接管理网络）上获取设备的 DHCP 地址。

   您可以执行以下任一操作：

   - 将管理端口 1 的 MAC 地址提供给网络管理员，以便他们可以在管理网络上查找此端口的 DHCP 地址。MAC 地址印在 E5600SG 控制器上端口旁边的标签上。
   - 查看 E5600SG 控制器上的七段显示器。如果 E5600SG 控制器上的管理端口 1 和 10-GbE 端口 2 和 4 连接到使用 DHCP 服务器的网络，则控制器会在打开机箱电源时尝试获取动态分配的 IP 地址。控制器完成启动过程后，其七段显示屏将显示 * HO* ，然后是两个数字的重复序列。

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     顺序：

     - 第一组数字是管理网络上设备存储节点的 DHCP 地址（如果已连接）。此 IP 地址将分配给 E5600SG 控制器上的管理端口 1 。
     - 第二组数字是网格网络上设备存储节点的 DHCP 地址。首次为设备通电时，此 IP 地址将分配给 10-GbE 端口 2 和 4 。

       如果无法使用 DHCP 分配 IP 地址，则会显示 0.0.0.0 。

2. 如果您能够获取任一 DHCP 地址：

   a. 在服务笔记本电脑上打开 Web 浏览器。

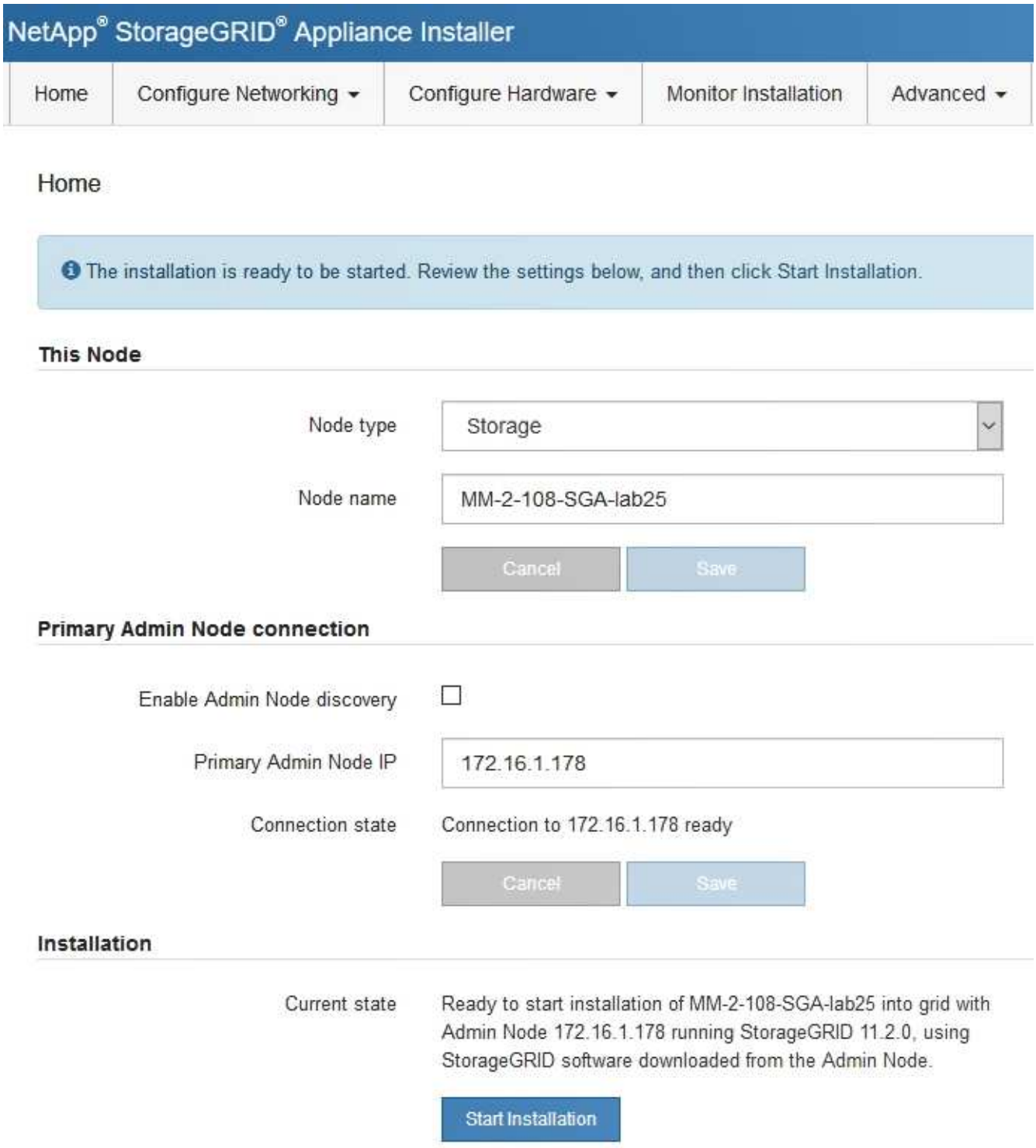
   b. 输入 StorageGRID 设备安装程序的 URL： + ` * https://*E5600SG_Controller_IP*:8443*`

对于 ` *E5600SG_Controller_IP*` ，请使用控制器的 DHCP 地址（如果有，请使用管理网络的 IP 地址）。

c. 如果系统提示您显示安全警报，请使用浏览器的安装向导查看并安装证书。

下次访问此 URL 时，不会显示此警报。

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。



3. 如果 E5600SG 控制器无法使用 DHCP 获取 IP 地址：

   a. 使用以太网缆线将服务笔记本电脑连接到 E5600SG 控制器上的管理端口 2 。

   b. 在服务笔记本电脑上打开 Web 浏览器。

   c. 输入 StorageGRID 设备安装程序的 URL： + ` * https://169.254.0.1:8443*`

   此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前的连接方式。

   如果无法通过链路本地连接访问主页，请将服务笔记本电脑 IP 地址配置为 `169.254.0.2` ，然后重试。

4. 查看主页页面上显示的所有消息，并根据需要配置链路配置和 IP 配置。

相关信息

Web 浏览器要求

验证并升级 **StorageGRID** 设备安装程序版本

设备上的 StorageGRID 设备安装程序版本必须与 StorageGRID 系统上安装的软件版本匹配，以确保所有 StorageGRID 功能均受支持。

您需要的内容

您已访问 StorageGRID 设备安装程序。

StorageGRID 设备出厂时预安装了 StorageGRID 设备安装程序。如果要将设备添加到最近升级的 StorageGRID 系统，则可能需要先手动升级 StorageGRID 设备安装程序，然后再将设备安装为新节点。

升级到新的 StorageGRID 版本时， StorageGRID 设备安装程序会自动升级。您无需升级已安装设备节点上的 StorageGRID 设备安装程序。只有在安装包含早期版本的 StorageGRID 设备安装程序的设备时，才需要此操作步骤 。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 升级固件 * 。
2. 将当前固件版本与 StorageGRID 系统上安装的软件版本进行比较。（从网格管理器的顶部，选择帮助图标并选择 * 关于 * 。）

   两个版本中的第二位数字应匹配。例如，如果您的 StorageGRID 系统运行的是 11.* 6* 。 *x.y* ，则 StorageGRID 设备安装程序版本应为 3.* 6* 。 *z* 。

3. 如果设备安装了StorageGRID 设备安装程序的低级版本、请转到https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["NetApp下载

：StorageGRID 设备"^]。

使用您的 NetApp 帐户的用户名和密码登录。

4. 下载适当版本的 * StorageGRID Appliances * 支持文件以及相应的校验和文件。

   StorageGRID 设备的支持文件是一个 ` .zip` 归档文件，其中包含所有 StorageGRID 设备型号的当前和先前固件版本，位于每种控制器类型的子目录中。

   下载 StorageGRID 设备的支持文件后，解压缩 ` .zip` 归档并查看 README 文件，以了解有关安装 StorageGRID 设备安装程序的重要信息。

5. 按照 StorageGRID 设备安装程序的 " 升级固件 " 页面上的说明执行以下步骤：

   a. 上传适用于您的控制器类型的相应支持文件（固件映像）和校验和文件。

   b. 升级非活动分区。

   c. 重新启动和交换分区。

   d. 升级第二个（非活动）分区。

相关信息

访问 StorageGRID 设备安装程序

配置网络链路（ **SG5600** ）

您可以为用于将设备连接到网格网络，客户端网络和管理网络的端口配置网络链路。您可以设置链路速度以及端口和网络绑定模式。

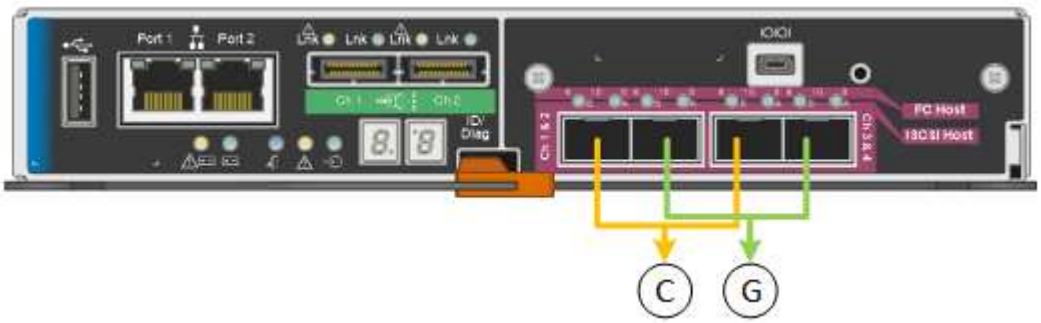
您需要的内容

如果您计划使用聚合端口绑定模式， LACP 网络绑定模式或 VLAN 标记：

- 您已将设备上的 10-GbE 端口连接到可支持 VLAN 和 LACP 的交换机。
- 如果多个交换机参与 LACP 绑定，则这些交换机支持多机箱链路聚合组（ MLAG ）或等效项。
- 您了解如何将交换机配置为使用 VLAN ， LACP 和 MLAG 或等效项。
- 您知道要用于每个网络的唯一 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。

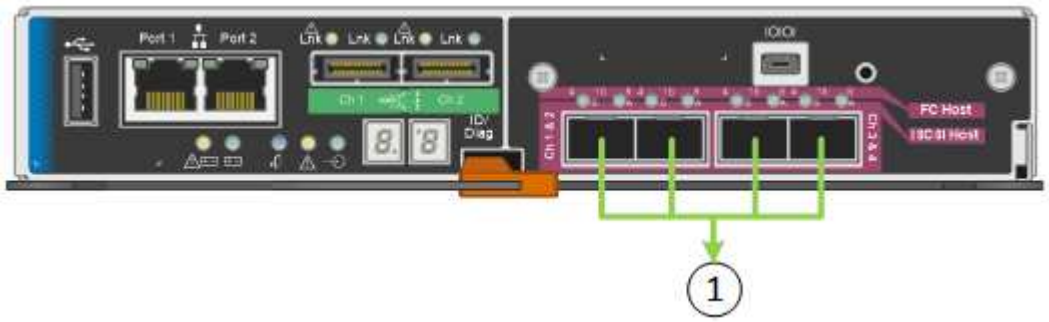
关于此任务

此图显示了四个 10-GbE 端口在固定端口绑定模式下的绑定方式（默认配置）。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

此图显示了四个 10-GbE 端口在聚合端口绑定模式下的绑定方式。



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表总结了用于配置四个 10-GbE 端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

- * 固定（默认）端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用主动备份绑定。 • 端口 1 和 3 对客户端网络使用主动备份绑定。 • 可以为两个网络指定VLAN标记。
LACP （ 802.3ad ）	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 不使用端口 1 和 3 。 • VLAN 标记是可选的。	• 端口 2 和 4 对网格网络使用 LACP 绑定。 • 端口 1 和 3 对客户端网络使用 LACP 绑定。 • 可以为两个网络指定VLAN标记。

- * 聚合端口绑定模式 *

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （ 802.3ad ）	• 端口 1-4 对网格网络使用一个 LACP 绑定。 • 一个 VLAN 标记用于标识网格网络数据包。	• 端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。 • 通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

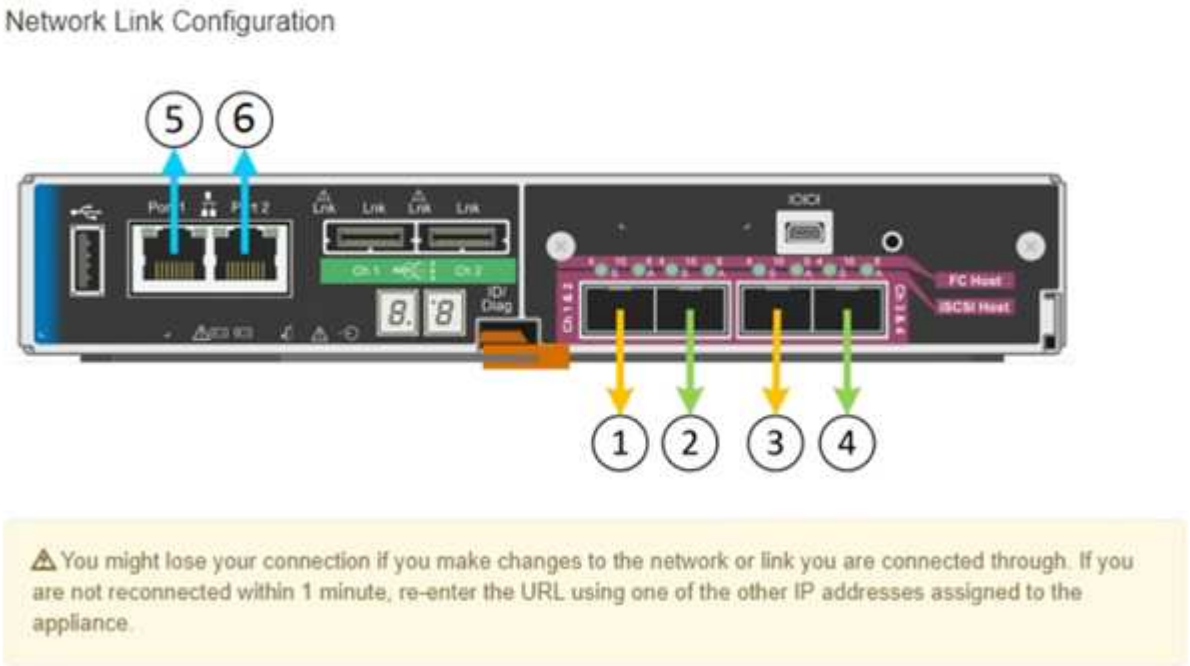
有关端口绑定和网络绑定模式的详细信息，请参见 "`10-GbE port connections for the E5600SG controller` " 。

此图显示了 E5600SG 控制器上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。

步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * 链接配置 * 。

   " 网络链路配置 " 页面显示设备示意图，其中包含编号为的网络和管理端口。



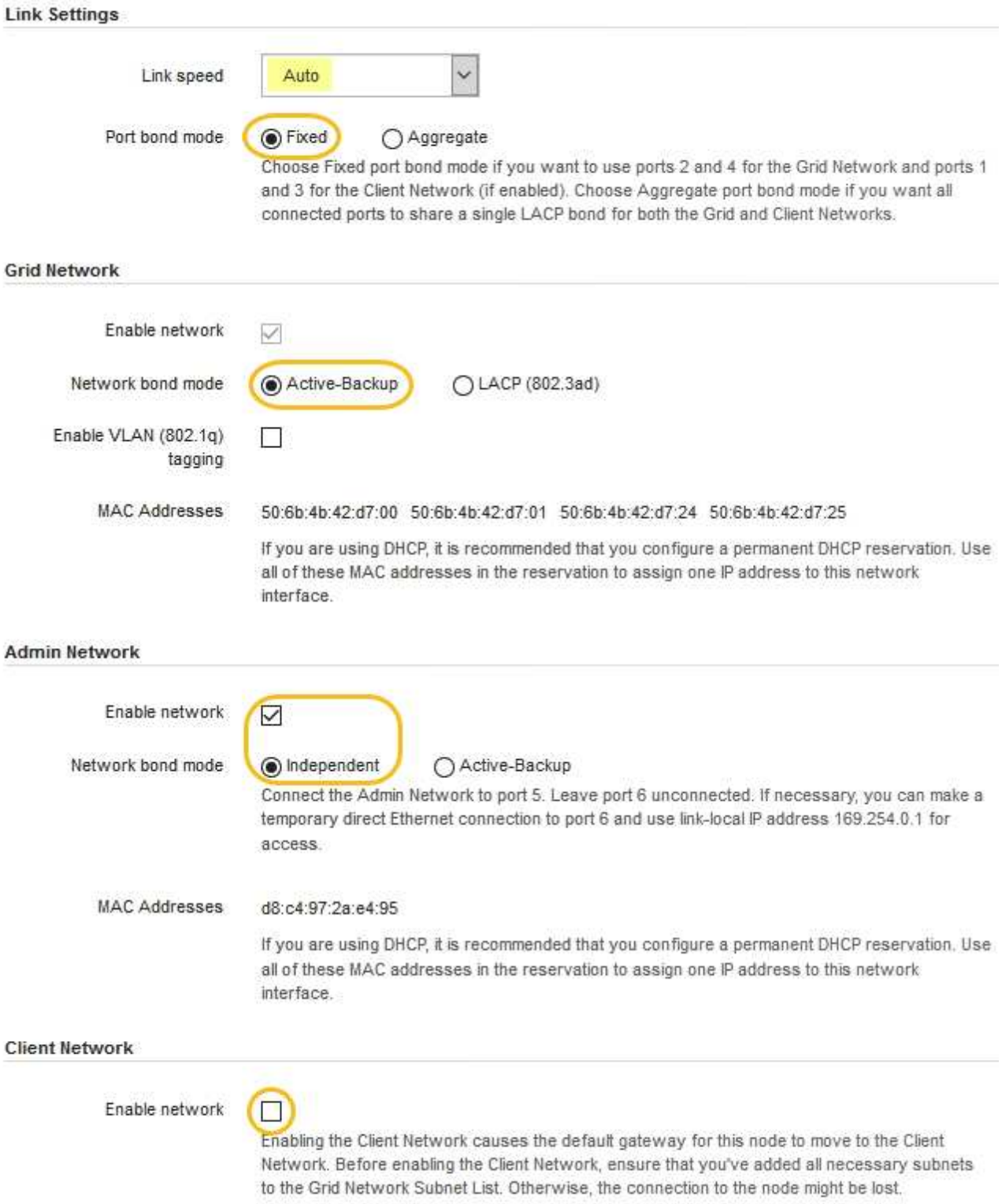
   链路状态表列出了已编号端口的链路状态（启动 / 关闭）和速度（ 1/25/40/100 Gbps ）。

Link Status

Link	State	Speed (Gbps)
1	Down	N/A
2	Up	10
3	Up	10
4	Down	N/A
5	Up	1
6	Up	1

首次访问此页面时：

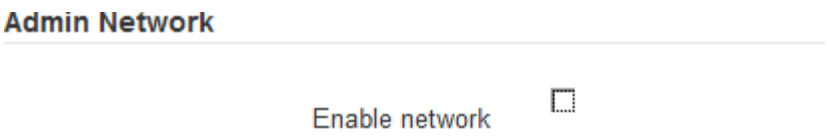
- * 链路速度 * 设置为 * 10GbE 。这是 E5600SG 控制器唯一可用的链路速度。
- * 端口绑定模式 * 设置为 * 固定 * 。
- 网格网络的 * 网络绑定模式 * 设置为 * 主动备份 * 。
- 此时将启用 * 管理网络 * ，并将网络绑定模式设置为 * 独立 * 。
- 已禁用 * 客户端网络 * 。



2. 启用或禁用计划使用的 StorageGRID 网络。

   网格网络为必填项。您不能禁用此网络。

   a. 如果设备未连接到管理网络，请取消选中管理网络的 * 启用网络 * 复选框。



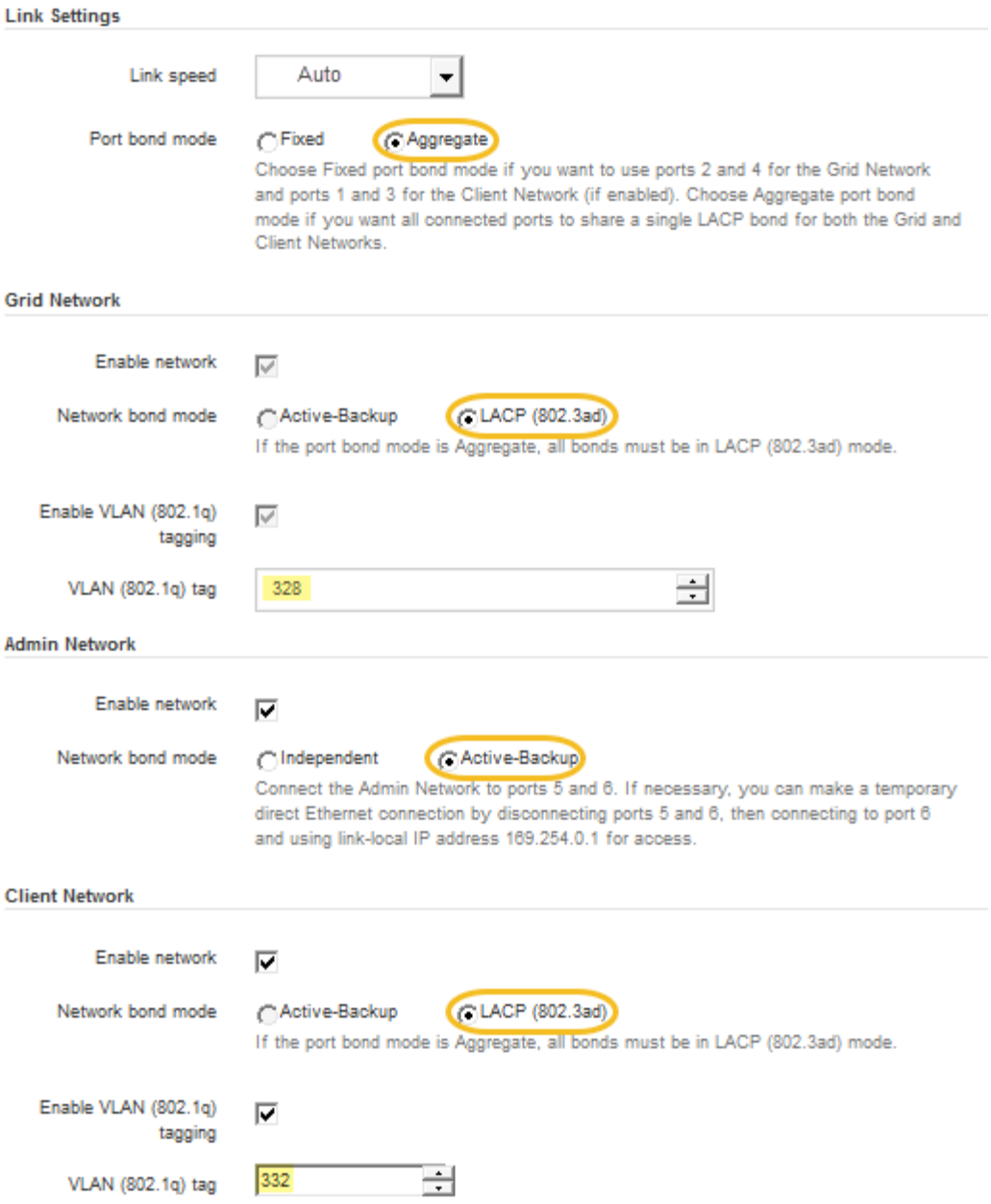
b. 如果设备已连接到客户端网络，请选中客户端网络的 * 启用网络 * 复选框。

   此时将显示 10-GbE 端口的客户端网络设置。

3. 请参见表，并配置端口绑定模式和网络绑定模式。

   示例显示：

   - 为网格和客户端网络选择了 * 聚合 * 和 * LACP * 。您必须为每个网络指定唯一的 VLAN 标记。您可以选择 0 到 4095 之间的值。
   - 已为管理网络选择 * 主动备份 * 。



4. 对所做的选择感到满意后，单击 * 保存 * 。

> 如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*E5600SG_Controller_IP*:8443*`

相关信息

E5600SG 控制器端口的端口绑定模式

设置 **IP** 配置

您可以使用 StorageGRID 设备安装程序在 StorageGRID 网格，管理和客户端网络上配置设备存储节点所使用的 IP 地址和路由信息。

关于此任务

您必须为每个已连接网络上的设备分配一个静态 IP ，或者为 DHCP 服务器上的地址分配一个永久租约。

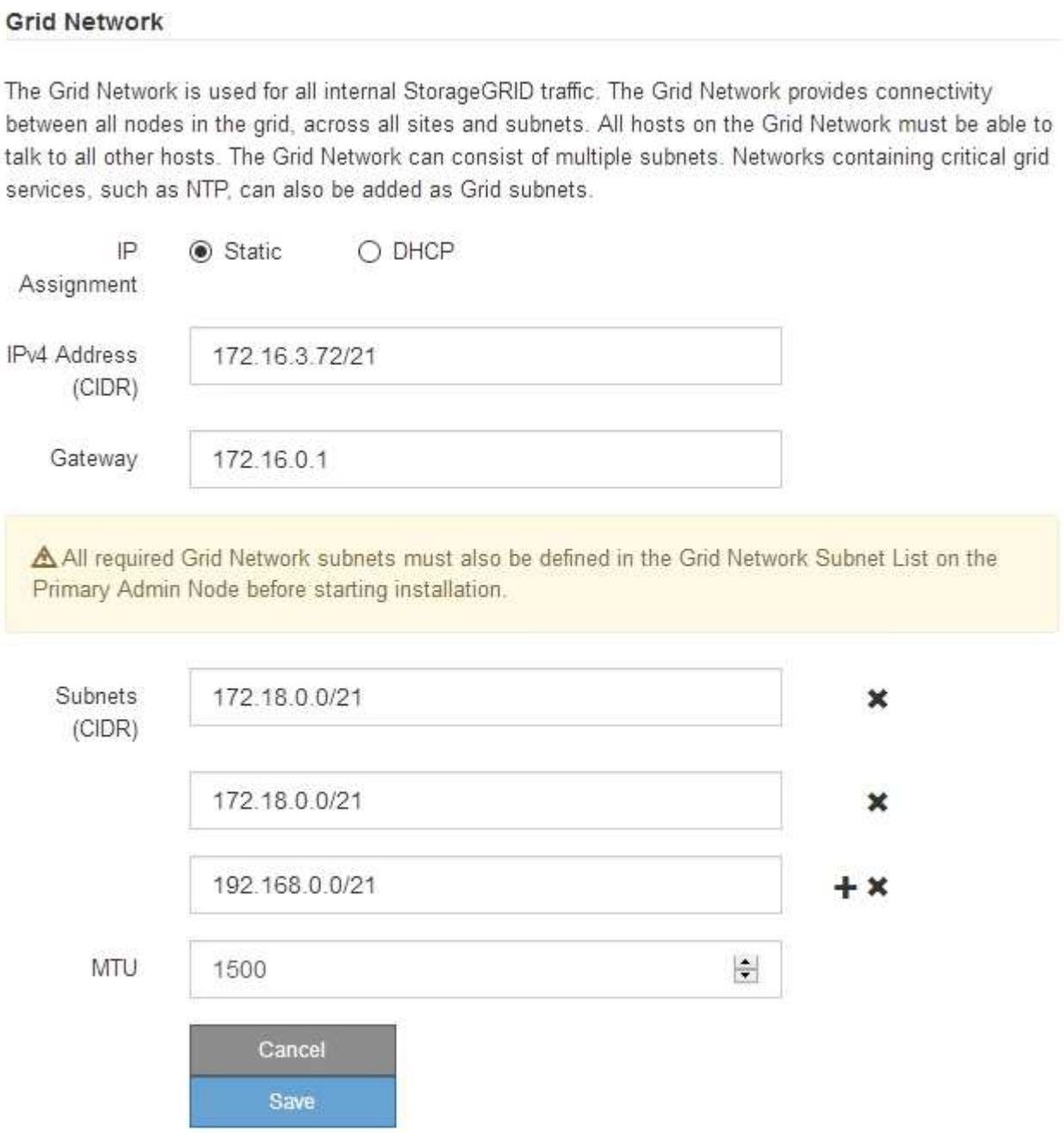
如果要更改链路配置，请参见有关更改 E5600SG 控制器的链路配置的说明。

步骤

1. 在 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。

   此时将显示 "IP Configuration" 页面。

2. 要配置网格网络，请在页面的 * 网格网络 * 部分中选择 * 静态 * 或 * DHCP * 。



3. 如果选择 * 静态 * ，请按照以下步骤配置网格网络：

a. 使用 CIDR 表示法输入静态 IPv4 地址。

b. 输入网关。

   如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

   网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

   为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

d. 单击 * 保存 * 。

   更改 IP 地址时，网关和子网列表可能也会发生更改。

   如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance_IP*:8443*`

e. 确认网格网络子网列表正确无误。

   如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

   未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

   - 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
   - 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

4. 如果选择了 * DHCP * ，请按照以下步骤配置网格网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

   系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

   您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认网格网络子网列表正确无误。

   如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。

   未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 ✚ 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 ✖。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

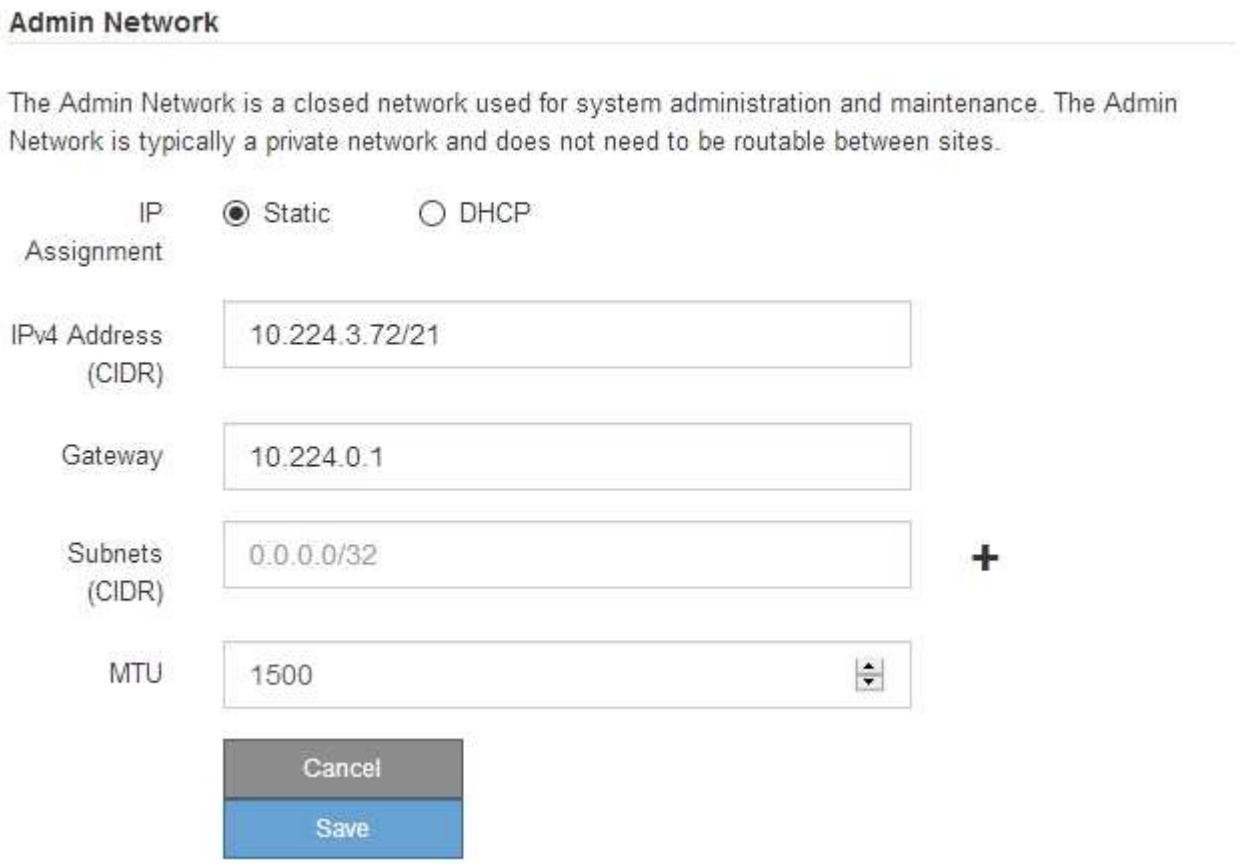
网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

a. 单击 * 保存 * 。

5. 要配置管理网络，请在页面的管理网络部分中选择 * 静态 * 或 * DHCP * 。

要配置管理网络，必须在链路配置页面上启用管理网络。



6. 如果选择 * 静态 * ，请按照以下步骤配置管理网络：

a. 使用 CIDR 表示法为设备上的管理端口 1 输入静态 IPv4 地址。

管理端口 1 位于设备右端的两个 1-GbE RJ45 端口的左侧。

b. 输入网关。

   如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

   网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

   更改 IP 地址时，网关和子网列表可能也会发生更改。

   如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如， + ` * https://*services_appliance*:8443*`

e. 确认管理网络子网列表正确无误。

   您必须验证是否可以使用提供的网关访问所有子网。

   无法使用默认路由来使用管理网络网关。

   - 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
   - 要删除未使用的子网，请单击删除图标 ✖。

f. 单击 * 保存 * 。

7. 如果选择了 * DHCP * ，请按照以下步骤配置管理网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

   系统会自动填充 * IPv4 地址 * ， * 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

   您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认管理网络子网列表正确无误。

   您必须验证是否可以使用提供的网关访问所有子网。

   无法使用默认路由来使用管理网络网关。

   - 要添加子网，请单击插入图标 ➕ 最后一个条目右侧。
   - 要删除未使用的子网，请单击删除图标 ✖。

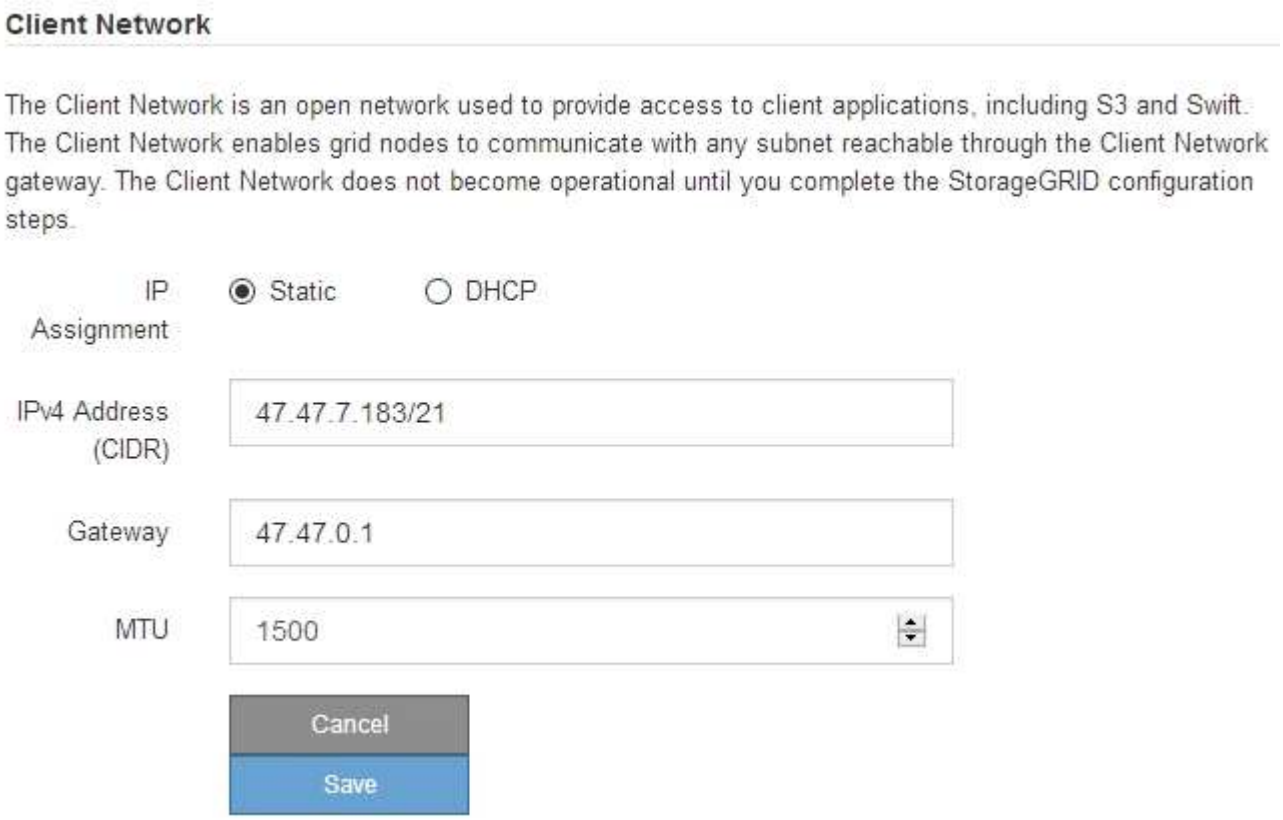
c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

   网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 * 。

8. 要配置客户端网络，请在页面的 * 客户端网络 * 部分中选择 * 静态 * 或 * DHCP * 。

要配置客户端网络，必须在链路配置页面上启用客户端网络。



9. 如果选择 * 静态 * ，请按照以下步骤配置客户端网络：

a. 使用 CIDR 表示法输入静态 IPv4 地址。

b. 单击 * 保存 * 。

c. 确认客户端网络网关的 IP 地址正确无误。

如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

d. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

e. 单击 * 保存 * 。

10. 如果选择了 * DHCP * ，请按照以下步骤配置客户端网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 * 。

系统会自动填充 * IPv4 地址 * 和 * 网关 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

a. 确认网关是否正确。

> 如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关，并且在启用客户端网络时无法移至其他接口。

b. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。

> 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

相关信息

更改 E5600SG 控制器的链路配置

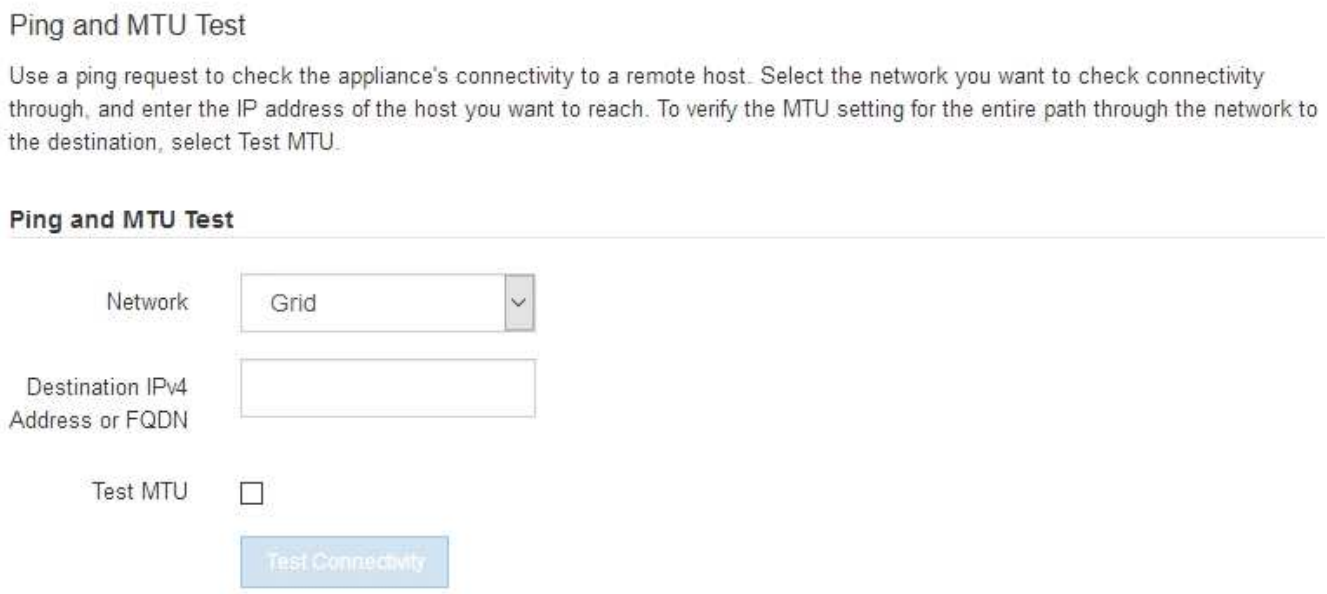
验证网络连接

您应确认可以从设备访问所使用的 StorageGRID 网络。要验证通过网络网关的路由，您应测试 StorageGRID 设备安装程序与不同子网上的 IP 地址之间的连接。您还可以验证 MTU 设置。

步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * Ping 和 MTU 测试 * 。

   此时将显示 Ping 和 MTU 测试页面。



2. 从 * 网络 * 下拉框中，选择要测试的网络：网格，管理员或客户端。

3. 输入该网络上某个主机的 IPv4 地址或完全限定域名（ FQDN ）。

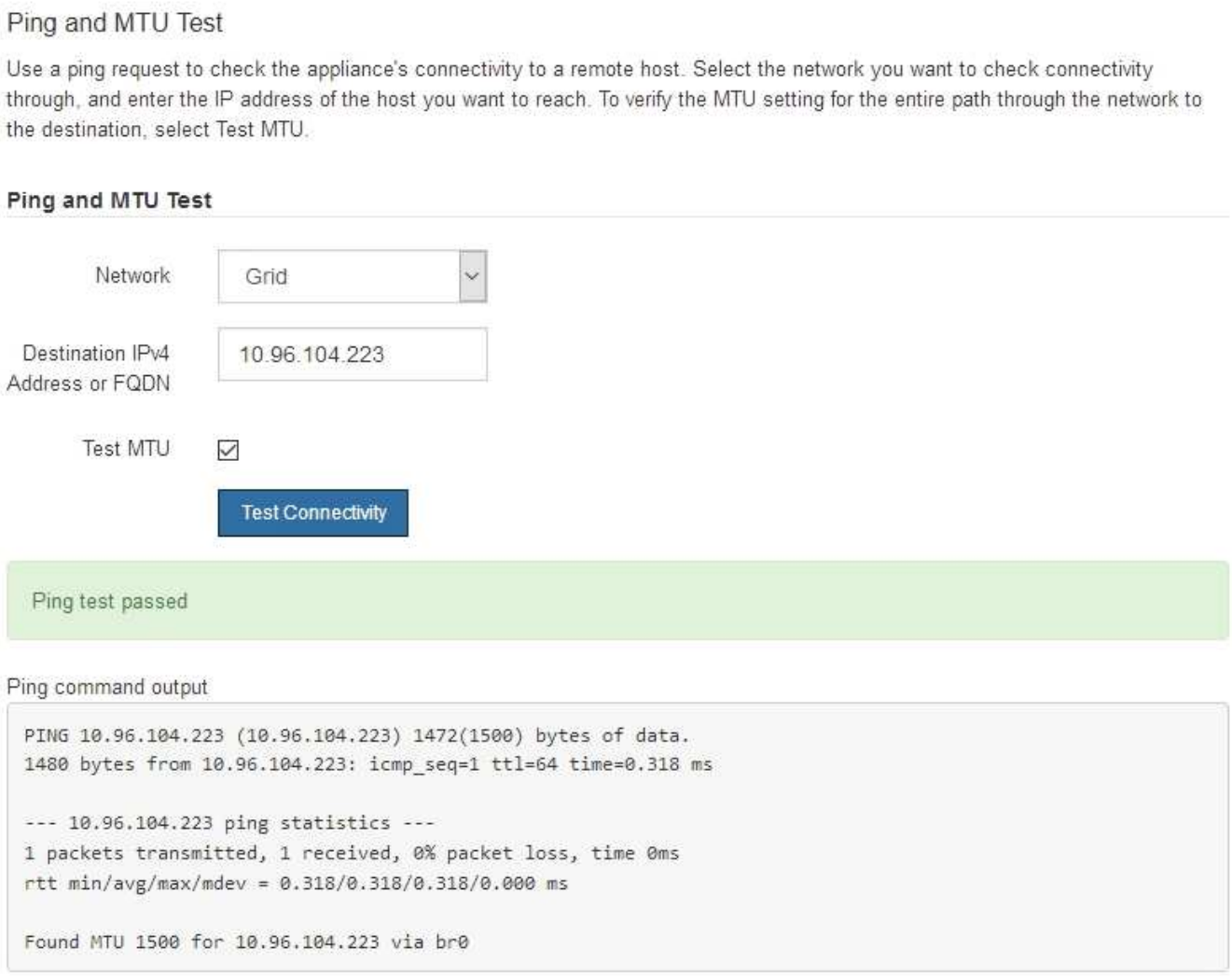
   例如，您可能需要对网络或主管理节点上的网关执行 ping 操作。

4. 或者，选中 * 测试 MTU* 复选框以验证通过网络到目标的整个路径的 MTU 设置。

   例如，您可以测试设备节点与其他站点的节点之间的路径。

5. 单击 * 测试连接 * 。

   如果网络连接有效，则会显示 "Ping test passed" 消息，并列出 ping 命令输出。



相关信息

配置网络链路（ SG5600 ）

更改 MTU 设置

验证端口级别的网络连接

要确保 StorageGRID 设备安装程序与其他节点之间的访问不会受到防火墙的阻碍，请确认

StorageGRID 设备安装程序可以连接到指定 IP 地址或地址范围内的特定 TCP 端口或端口集。

关于此任务

使用 StorageGRID 设备安装程序中提供的端口列表，您可以测试设备与网格网络中其他节点之间的连接。

此外，您还可以在管理和客户端网络以及 UDP 端口上测试连接，例如用于外部 NFS 或 DNS 服务器的端口。有关这些端口的列表，请参见 StorageGRID 网络连接准则中的端口参考。

端口连接表中列出的网格网络端口仅适用于 StorageGRID 11.6.0 版。要验证每种节点类型的端口是否正确，您应始终参考适用于您的 StorageGRID 版本的网络连接准则。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 端口连接测试（ nmap ） * 。

   此时将显示端口连接测试页面。

   端口连接表列出了网格网络上需要 TCP 连接的节点类型。对于每种节点类型，此表列出了设备应可访问的网格网络端口。

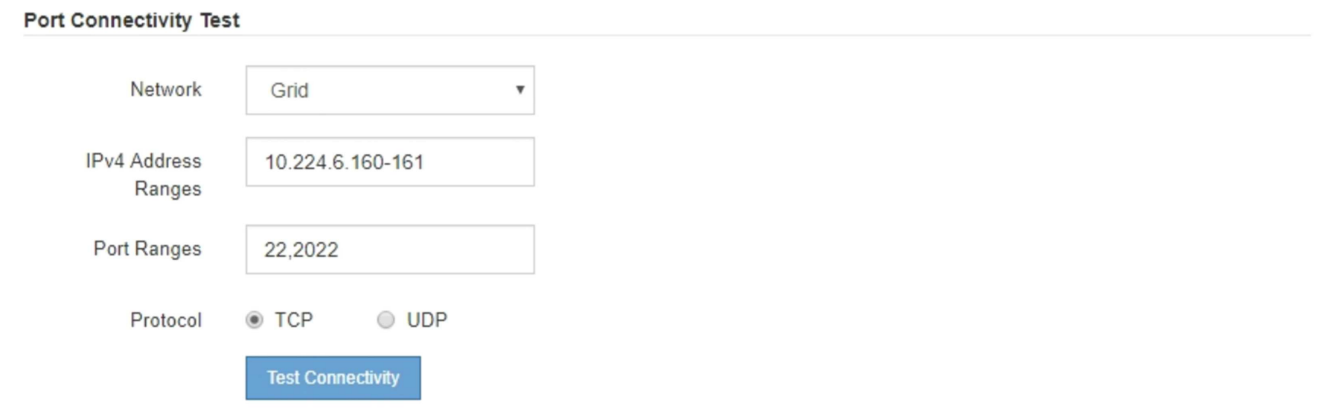
   您可以测试表中列出的设备端口与网格网络中的其他节点之间的连接。

2. 从 * 网络 * 下拉列表中，选择要测试的网络： * 网格 * ， * 管理 * 或 * 客户端 * 。
3. 为该网络上的主机指定一个 IPv4 地址范围。

   例如，您可能需要探测网络或主管理节点上的网关。

   使用连字符指定一个范围，如示例所示。

4. 输入 TCP 端口号，以逗号分隔的端口列表或端口范围。



5. 单击 * 测试连接 * 。

   ◦ 如果选定的端口级别网络连接有效，则绿色横幅中会显示 "`Port connectivity test passed` " 消息。nmap 命令输出列在横幅下方。

- 如果与远程主机建立了端口级网络连接，但主机未侦听一个或多个选定端口，则黄色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  主机未侦听的任何远程端口的状态为 "`closed" 。` 例如，当您尝试连接的节点处于预安装状态且 StorageGRID NMS 服务尚未在该节点上运行时，您可能会看到此黄色横幅。

- 如果无法为一个或多个选定端口建立端口级别网络连接，则红色横幅中会显示 "`Port connectivity test failed` " 消息。nmap 命令输出列在横幅下方。

  红色横幅表示已尝试通过 TCP 连接到远程主机上的某个端口，但未向发送方返回任何内容。如果未返回任何响应，则此端口的状态为 " 已筛选 " ，并且可能会被防火墙阻止。

  此外，还会列出带有 "`closed` " 的端口。

相关信息

网络连接准则

配置 **SANtricity** 存储管理器

您可以使用 SANtricity 存储管理器监控 StorageGRID 设备中存储磁盘和硬件组件的状态。要访问此软件，您必须知道 E2700 控制器（设备中的存储控制器）上管理端口 1 的 IP 地址。

设置 **E2700** 控制器的 **IP** 地址

E2700 控制器上的管理端口 1 用于将设备连接到 SANtricity 存储管理器的管理网络。您必须为 E2700 控制器设置静态 IP 地址，以确保不会丢失与 StorageGRID 设备中硬件和控制器固件的管理连接。

您需要的内容

您正在使用 支持的 Web 浏览器。

关于此任务

DHCP 分配的地址可能随时更改。为控制器分配一个静态 IP 地址，以确保可访问性一致。

步骤

1. 在客户端中，输入 StorageGRID 设备安装程序的 URL： + ` * https://*E5600SG_Controller_IP*:8443*`

   对于 ` *E5600SG_Controller_IP*` ，请在任何 StorageGRID 网络上使用设备的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 硬件配置 * > * 存储控制器网络配置 * 。

   此时将显示存储控制器网络配置页面。

3. 根据您的网络配置，对于 IPv4 ， IPv6 或这两者，请选择 * 已启用 * 。
4. 记下自动显示的 IPv4 地址。

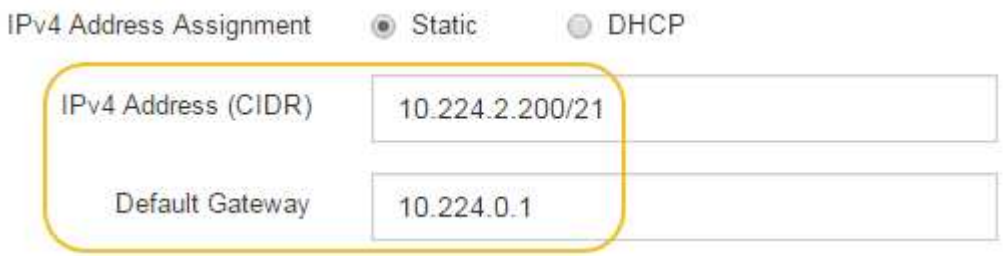
   DHCP 是为该端口分配 IP 地址的默认方法。

   显示 DHCP 值可能需要几分钟的时间。

5. （可选）为 E2700 控制器管理端口设置静态 IP 地址。

   您应该为管理端口分配静态 IP ，或者为 DHCP 服务器上的地址分配永久租约。

   a. 选择 * 静态 * 。
   b. 使用 CIDR 表示法输入 IPv4 地址。
   c. 输入默认网关。



   d. 单击 * 保存 * 。

      应用所做的更改可能需要几分钟的时间。

   连接到 SANtricity 存储管理器时，您将使用新的静态 IP 地址作为 URL： + ` * https://*E2700_Controller_IP*`*

相关信息

"NetApp 文档： SANtricity 存储管理器"

将设备添加到 **SANtricity** 存储管理器

将设备中的 E2700 控制器连接到 SANtricity 存储管理器，然后将设备添加为存储阵列。

您需要的内容

您正在使用 支持的 Web 浏览器。

关于此任务

有关详细说明，请参见 SANtricity 存储管理器文档。

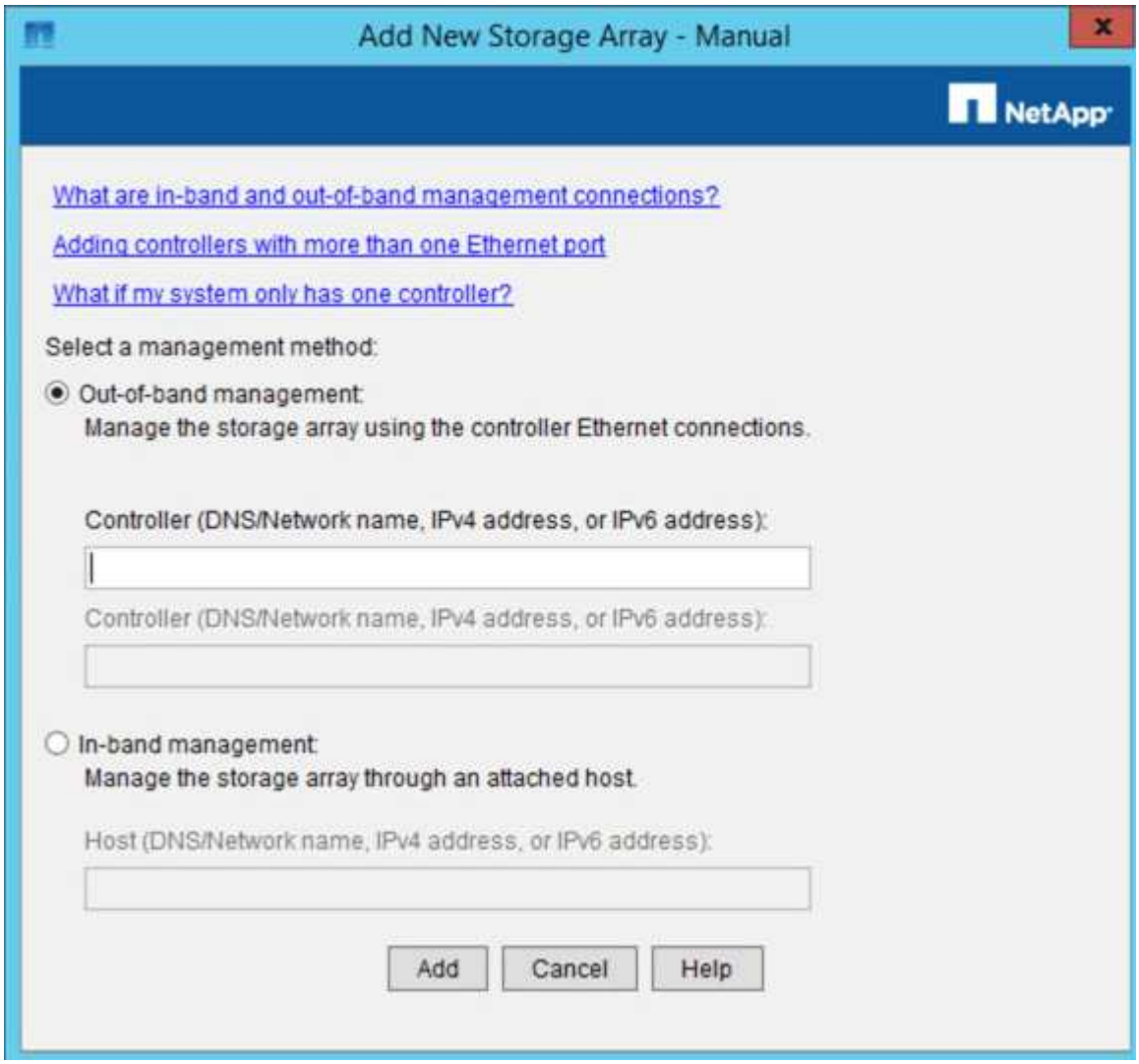
步骤

1. 打开 Web 浏览器，然后输入 IP 地址作为 SANtricity 存储管理器的 URL： + ` * https://*E2700_Controller_IP*`

   此时将显示 SANtricity 存储管理器的登录页面。

2. 在 * 选择添加方法 * 页面上，选择 * 手动 * ，然后单击 * 确定 * 。
3. 选择 * 编辑 * > * 添加存储阵列 * 。

   此时将显示 "Add New Storage Array - Manual" 页面。



4. 在 * 带外管理 * 框中，输入以下值之一：
   - * 使用 DHCP： * DHCP 服务器分配给 E2700 控制器上管理端口 1 的 IP 地址
   - * 未使用 DHCP： * `192.168.128.101`

   只有一个设备的控制器连接到 SANtricity 存储管理器，因此您只需要输入一个 IP 地址。

5. 单击 * 添加 * 。

相关信息

"NetApp 文档： SANtricity 存储管理器"

设置 **SANtricity** 存储管理器

访问 SANtricity 存储管理器后，您可以使用它配置硬件设置。通常，在将设备部署为 StorageGRID 系统中的存储节点之前，您需要配置这些设置。

配置 **AutoSupport**

AutoSupport 工具会从设备收集客户支持包中的数据，并自动将数据发送给技术支持。配置 AutoSupport 有助于技术支持进行远程故障排除和问题分析。

您需要的内容

- 必须在设备上启用并激活 AutoSupport 功能。

  AutoSupport 功能会在存储管理工作站上全局激活和停用。

- Storage Manager 事件监控器必须至少在一台能够访问设备的计算机上运行，并且最好在不超过一台计算机上运行。

关于此任务

所有数据都会在指定位置压缩为一个压缩归档文件格式（ .7z ）。

AutoSupport 提供以下类型的消息：

消息类型	**Description**
事件消息	• 受管设备上发生支持事件时发送 • 包括系统配置和诊断信息
每日消息	• 在设备的本地时间内，用户可配置的时间间隔内，每天发送一次 • 包括当前系统事件日志和性能数据
每周消息	• 在用户可配置的时间间隔内，在设备的本地时间内每周发送一次 • 包括配置和系统状态信息

步骤

1. 在 SANtricity 存储管理器的企业管理窗口中，选择 * 设备 * 选项卡，然后选择 * 已发现的存储阵列 * 。
2. 选择 * 工具 * > * AutoSupport * > * 配置 * 。
3. 如果需要，请使用 SANtricity 存储管理器联机帮助完成此任务。

相关信息

"NetApp 文档： SANtricity 存储管理器"

验证是否收到 **AutoSupport**

您应验证技术支持是否正在接收您的 AutoSupport 消息。您可以在 Active IQ 门户上找到系统的 AutoSupport 状态。验证是否收到这些消息可确保技术支持在您需要帮助时获取您的信息。

关于此任务

AutoSupport 可以显示以下状态之一：

- * 开 *

  "On" 状态表示技术支持当前正在从系统接收 AutoSupport 消息。

- * 关闭 *

  关闭状态表示您可能已禁用 AutoSupport ，因为技术支持在过去 15 个日历日内未收到系统的每周日志，或者您的环境或配置可能发生了更改（例如）。

- * 拒绝 *

  拒绝状态表示您已通知技术支持您不会启用 AutoSupport 。

技术支持从系统收到每周日志后， AutoSupport 状态将更改为 on 。

步骤

1. 访问 NetApp 支持站点，网址为 "mysupport.netapp.com"，然后登录到 Active IQ 门户。
2. 如果 AutoSupport 状态为 off ，并且您认为不正确，请完成以下操作：
   a. 检查系统配置，确保已打开 AutoSupport 。
   b. 请检查您的网络环境和配置，以确保系统可以向技术支持发送消息。

配置电子邮件和 **SNMP** 陷阱警报通知

SANtricity 存储管理器可以在设备或其某个组件的状态发生变化时向您发出通知。这称为警报通知。您可以通过两种不同的方法接收警报通知：电子邮件和 SNMP 陷阱。您必须配置要接收的警报通知。

步骤

1. 在 SANtricity 存储管理器的企业管理窗口中，选择 * 设备 * 选项卡，然后选择一个节点。
2. 选择 * 编辑 * > * 配置警报 * 。
3. 选择 * 电子邮件 * 选项卡以配置电子邮件警报通知。
4. 选择 * SNMP * 选项卡以配置 SNMP 陷阱警报通知。
5. 如果需要，请使用 SANtricity 存储管理器联机帮助完成此任务。

设置 **SANtricity** 存储管理器的密码

您可以在 SANtricity 存储管理器中设置设备使用的密码。设置密码可保持系统安全性。

步骤

1. 在 SANtricity 存储管理器的企业管理窗口中，双击控制器。
2. 从阵列管理窗口中，选择 * 存储阵列 * 菜单，然后选择 * 安全性 * > * 设置密码 * 。
3. 配置密码。
4. 如果需要，请使用 SANtricity 存储管理器联机帮助完成此任务。

可选：启用节点加密

如果启用了节点加密，则可以通过安全密钥管理服务器（ KMS ）加密来保护设备中的磁盘，防止物理丢失或从站点中删除。您必须在设备安装期间选择并启用节点加密，并且在 KMS 加密过程开始后，不能取消选择节点加密。

您需要的内容

查看有关管理 StorageGRID 的说明中有关 KMS 的信息。

关于此任务

启用了节点加密的设备将连接到为 StorageGRID 站点配置的外部密钥管理服务器（ KMS ）。每个 KMS （或 KMS 集群）负责管理站点上所有设备节点的加密密钥。这些密钥对启用了节点加密的设备中每个磁盘上的数据进行加密和解密。

可以在 StorageGRID 中安装 KMS 之前或之后在网格管理器中设置此设备。有关更多详细信息，请参见管理 StorageGRID 的说明中有关 KMS 和设备配置的信息。

- 如果在安装设备之前设置了 KMS ，则在设备上启用节点加密并将其添加到配置了 KMS 的 StorageGRID 站点时， KMS 控制的加密将开始。
- 如果在安装此设备之前未设置 KMS ，则在为包含此设备节点的站点配置了 KMS 并可使用此 KMS 后，将对启用了节点加密的每个设备执行 KMS 控制的加密。

> 在连接到启用了节点加密的设备上的 KMS 之前存在的数据将使用不安全的临时密钥进行加密。除非将密钥设置为 KMS 提供的值，否则设备不会受到删除或被盗的保护。

如果没有对磁盘进行解密所需的 KMS 密钥，则无法检索设备上的数据，并且数据实际上会丢失。如果无法从 KMS 中检索到解密密钥，则会出现这种情况。如果清除KMS配置、KMS密钥过期、与KMS的连接断开或从安装了KMS密钥的StorageGRID 系统中删除设备、则无法访问此密钥。

步骤

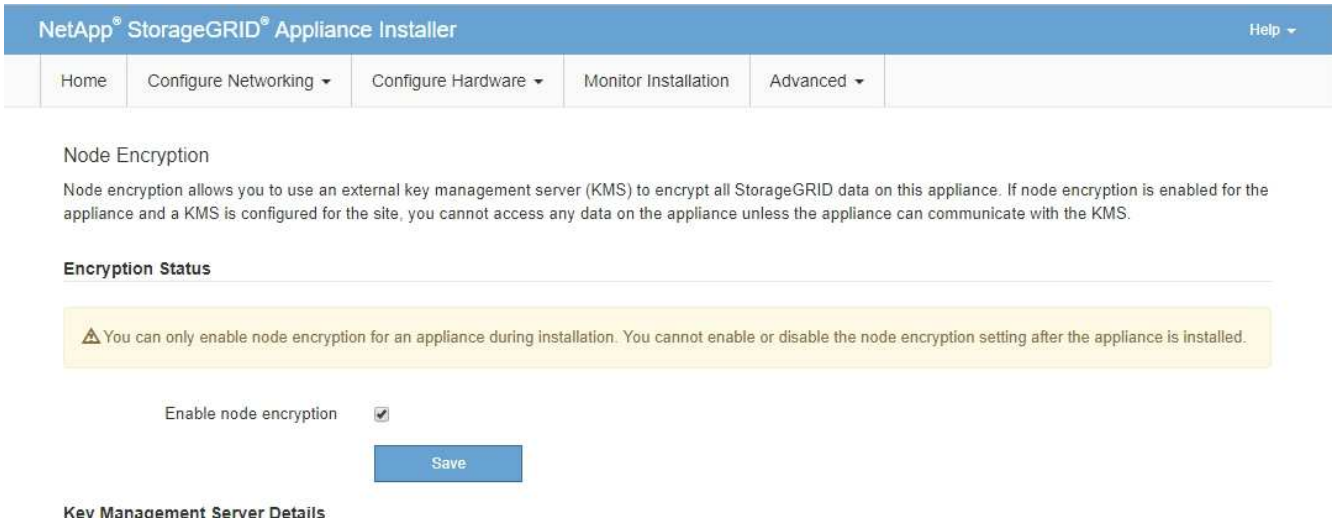
1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

   > 使用 KMS 密钥对设备加密后，如果不使用相同的 KMS 密钥，则无法对设备磁盘进行解密。

2. 选择 * 配置硬件 * > * 节点加密 * 。



3. 选择 * 启用节点加密 * 。

   在安装设备之前，您可以取消选择 * 启用节点加密 * ，而不会有数据丢失的风险。安装开始后，设备节点将访问 StorageGRID 系统中的 KMS 加密密钥并开始磁盘加密。安装设备后，您无法禁用节点加密。

   > 将启用了节点加密的设备添加到具有 KMS 的 StorageGRID 站点后，您无法停止对此节点使用 KMS 加密。

4. 选择 * 保存 * 。
5. 将设备部署为 StorageGRID 系统中的节点。

   当设备访问为 StorageGRID 站点配置的 KMS 密钥时，便会开始使用由 KMS 控制的加密。安装程序会在 KMS 加密过程中显示进度消息，此过程可能需要几分钟时间，具体取决于设备中的磁盘卷数。

   > 设备最初会配置一个随机的非 KMS 加密密钥，该密钥会分配给每个磁盘卷。磁盘会使用此临时加密密钥进行加密，这种加密密钥不安全，直到启用了节点加密的设备访问为 StorageGRID 站点配置的 KMS 密钥为止。

完成后

您可以查看节点加密状态， KMS 详细信息以及设备节点处于维护模式时正在使用的证书。

相关信息

管理 StorageGRID

在维护模式下监控节点加密（ SG5600 ）

可选：更改为 **RAID6** 模式（仅限 **SG5660** ）

如果您的 SG5660 包含 60 个驱动器，则可以将卷配置从其默认和建议设置动态磁盘池（ Dynamic Disk Pool ， DDP ）更改为 RAID6 。您只能在部署 StorageGRID 设备存储节点之前更改此模式。

您需要的内容

- 您已安装 SG5660 。SG5612 不支持 RAID6 。如果您使用的是 SG5612 ，则必须使用 DDP 模式。

> 如果已配置任何卷或先前已安装 StorageGRID ，则更改 RAID 模式会删除和更换这些卷。这些卷上的所有数据都将丢失。

关于此任务

在部署 StorageGRID 设备存储节点之前，您可以从两个卷配置选项中进行选择：

- * 动态磁盘池（ DDP ） * —这是默认设置和建议设置。DDP 是一种增强型硬件数据保护方案，可提高系统性能，缩短驱动器发生故障后的重建时间以及简化管理。
- **RAID6** —这是一种硬件保护方案，它在每个磁盘上使用奇偶校验条带，并允许在 RAID 集内发生两个磁盘故障，以免任何数据丢失。

> 建议不要在大多数 StorageGRID 环境中使用 RAID6 。虽然 RAID6 可以将存储效率提高到 88% （而 DDP 为 80% ），但 DDP 模式可以更高效地从驱动器故障中恢复。

步骤

1. 使用服务笔记本电脑打开 Web 浏览器并访问 StorageGRID 设备安装程序： + ` * https://*E5600SG_Controller_IP*:8443*`

   其中， ` *E5600SG_Controller_IP*` 是 E5600SG 控制器的任何 IP 地址。

2. 从菜单栏中，选择 * 高级 * > * RAID 模式 * 。
3. 在 * 配置 RAID 模式 * 页面上，从模式下拉列表中选择 * RAID6* 。
4. 单击 * 保存 * 。

可选：重新映射设备的网络端口

您可能需要将设备存储节点上的内部端口重新映射到不同的外部端口。例如，由于使用了防火墙问题描述 ，您可能需要重新映射端口。

您需要的内容

- 您先前已访问 StorageGRID 设备安装程序。
- 您尚未配置，也不打算配置负载平衡器端点。

> 如果重新映射任何端口，则不能使用相同的端口来配置负载平衡器端点。如果要配置负载平衡器端点且已重新映射端口，请按照中的步骤进行操作 删除端口重新映射。

步骤

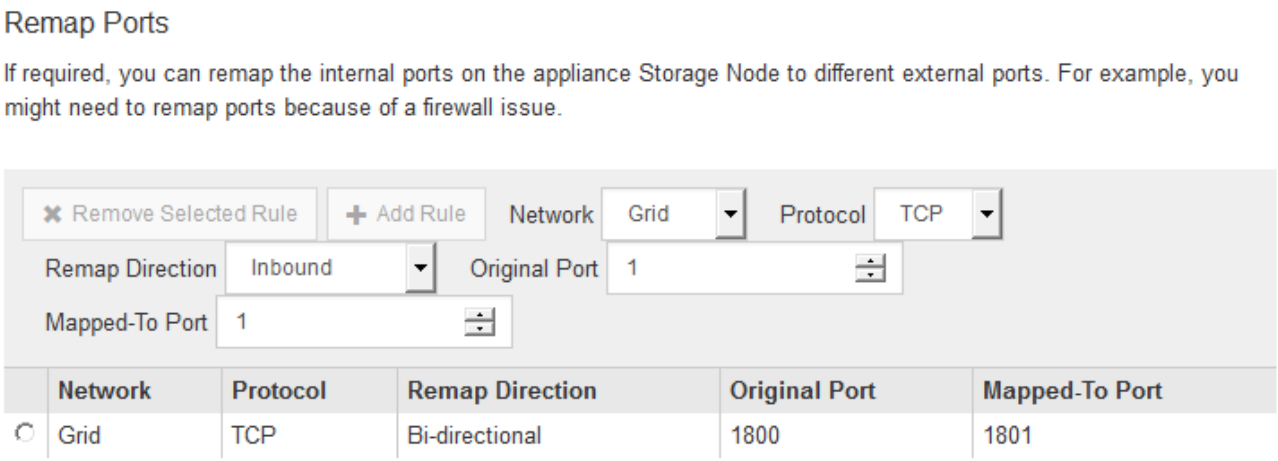
1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * 删除端口 * 。

   此时将显示 Remap Port 页面。

2. 从 * 网络 * 下拉框中，为要重新映射的端口选择网络：网格，管理员或客户端。

3. 从 * 协议 * 下拉框中，选择 IP 协议： TCP 或 UDP 。
4. 从 * 映射方向 * 下拉框中，选择要为此端口重新映射的流量方向：入站，出站或双向。
5. 对于 * 原始端口 * ，输入要重新映射的端口的编号。
6. 对于 * 映射到端口 * ，请输入要使用的端口编号。
7. 单击 * 添加规则 * 。

   此时，新端口映射将添加到表中，重新映射将立即生效。



8. 要删除端口映射，请选择要删除的规则对应的单选按钮，然后单击 * 删除选定规则 * 。

相关信息

恢复和维护

部署设备存储节点

安装和配置存储设备后，您可以将其部署为 StorageGRID 系统中的存储节点。将设备部署为存储节点时，您可以使用设备上随附的 StorageGRID 设备安装程序。

您需要的内容

- 如果要克隆设备节点，请继续执行恢复和维护过程。

  恢复和维护

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路， IP 地址和端口重新映射（如果需要）。
- 您知道分配给设备计算控制器的一个 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。
- 已部署 StorageGRID 系统的主管理节点。
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 您的服务笔记本电脑具有受支持的 Web 浏览器。

关于此任务

每个存储设备都用作一个存储节点。任何设备都可以连接到网格网络，管理网络和客户端网络

要在 StorageGRID 系统中部署设备存储节点，请访问 StorageGRID 设备安装程序并执行以下步骤：

- 您可以指定或确认主管理节点的 IP 地址以及存储节点的名称。
- 您可以开始部署，并等待卷配置完毕并安装软件。
- 当安装暂停完成设备安装任务后，您可以通过登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装和部署过程来恢复安装。

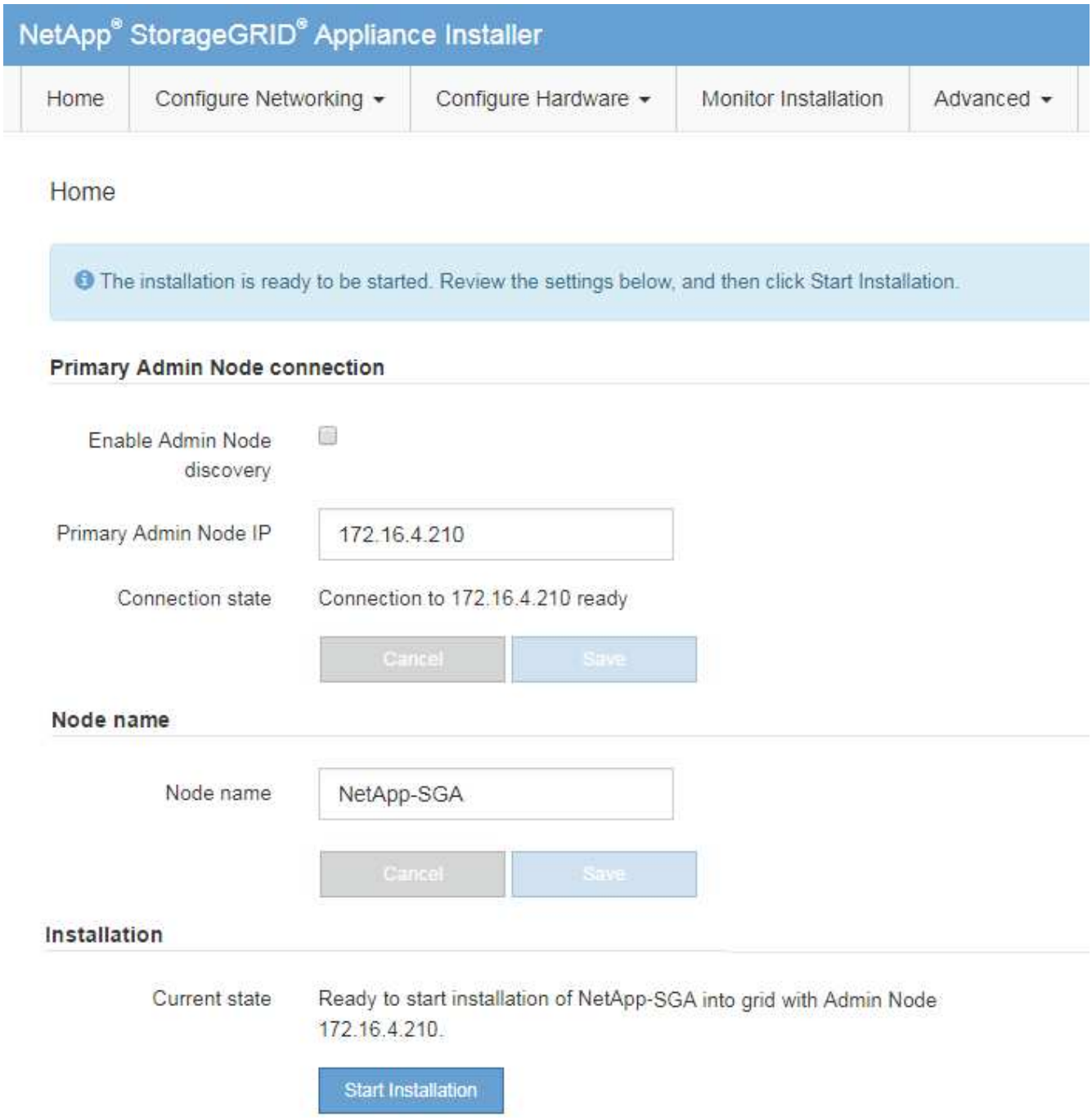
> 如果您需要一次部署多个设备节点，则可以使用 `configure-sGa.py` Appliance Installation 脚本自动执行安装过程。

- 如果要执行扩展或恢复操作，请按照相应说明进行操作：
  - 要将设备存储节点添加到现有 StorageGRID 系统，请参见有关扩展 StorageGRID 系统的说明。
  - 要在恢复操作中部署设备存储节点，请参见有关恢复和维护的说明。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   此时将显示 StorageGRID 设备安装程序主页页面。



2. 在 * 主管理节点 * 连接部分中，确定是否需要指定主管理节点的 IP 地址。

   如果先前已在此数据中心中安装了其他节点，则 StorageGRID 设备安装程序可以自动发现此 IP 地址，前提是主管理节点或至少一个配置了 admin_IP 的其他网格节点位于同一子网上。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 等待连接状态，使新 IP 地址准备就绪。
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 等待显示发现的 IP 地址列表。 c. 为要部署此设备存储节点的网格选择主管理节点。 d. 单击 * 保存 * 。 e. 等待连接状态，使新 IP 地址准备就绪。

4. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后单击 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的节点页面（概述选项卡）上。如果需要，您可以在批准节点时更改名称。

5. 在 Installation 部分中，确认当前状态为 "Ready to start installation of ` node_node name_` into grid with primary Admin Node ` *admin_IP*` " ，并且 * 开始安装 * 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

   > 如果要将存储节点设备部署为节点克隆目标，请在此停止部署过程，然后继续执行节点克隆操作步骤 的恢复和维护。

   恢复和维护

6. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。

   当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

   > 如果需要手动访问监控器安装页面，请单击 * 监控安装 * 。

7. 如果网格包含多个设备存储节点，请对每个设备重复这些步骤。

   > 如果您需要一次部署多个设备存储节点，则可以使用 `configure-sGa.py` appliance 安装脚本自动执行安装过程。

相关信息

扩展网格

恢复和维护

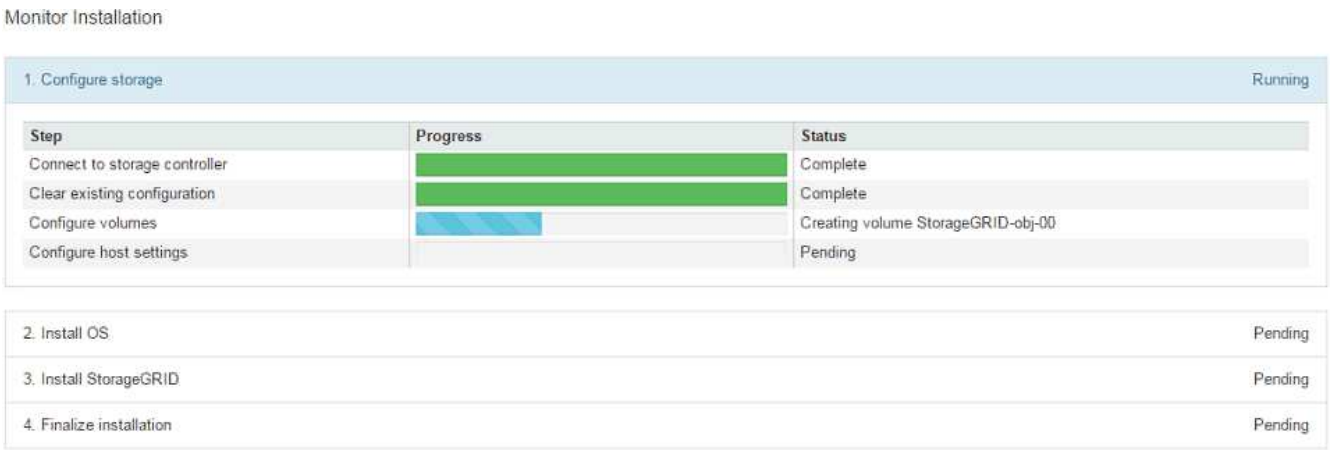
监控存储设备安装

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

步骤

1. 要监控安装进度，请单击 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

2. 查看前两个安装阶段的进度。

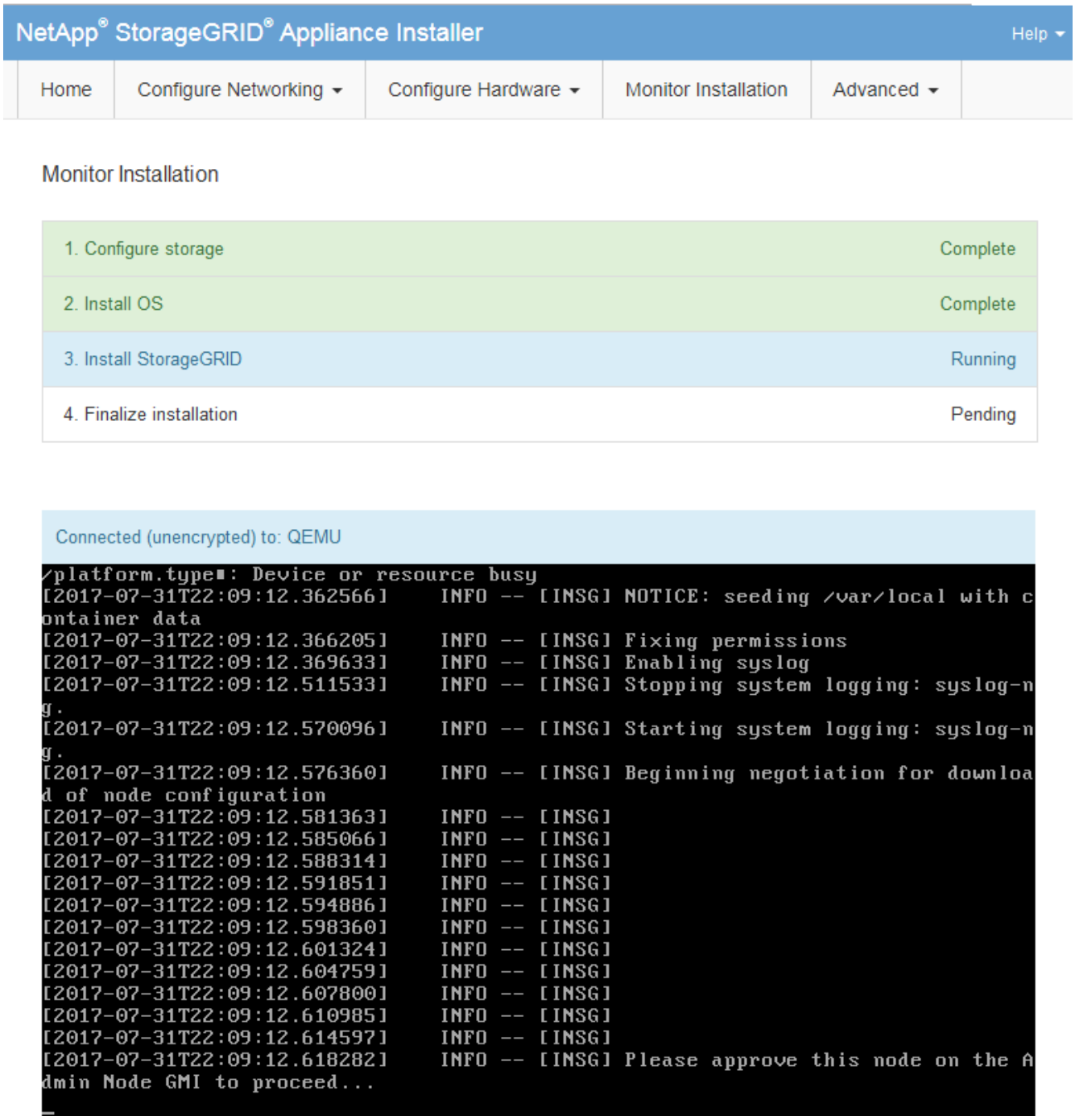
   ◦ 。配置存储 *

   在此阶段，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。

   ◦ 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

3. 继续监控安装进度，直到 * 安装 StorageGRID 网格管理器 * 阶段暂停，并且嵌入式控制台上显示一条消息，提示您使用网格管理器在管理节点上批准此节点。继续执行下一步。



4. 转至主管理节点的网格管理器，批准待定存储节点并完成 StorageGRID 安装过程。

   在网格管理器中单击 * 安装 * 后，第 3 阶段完成，第 4 阶段 * 完成安装 * 开始。阶段 4 完成后，控制器将重新启动。

自动化设备安装和配置（ **SG5600** ）

您可以自动安装和配置设备以及配置整个 StorageGRID 系统。

关于此任务

自动化安装和配置对于部署多个 StorageGRID 实例或一个大型复杂的 StorageGRID 实例非常有用。

要自动执行安装和配置，请使用以下一个或多个选项：

- 创建一个 JSON 文件，用于指定设备的配置设置。使用 StorageGRID 设备安装程序上传 JSON 文件。

  您可以使用同一文件配置多个设备。

- 使用 StorageGRID`configure-sGa.py` Python 脚本自动配置设备。
- 使用其他 Python 脚本配置整个 StorageGRID 系统的其他组件（ " 网格 " ）。

您可以直接使用 StorageGRID 自动化 Python 脚本，也可以使用它们作为示例，说明如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。请参见有关的信息 下载并提取 StorageGRID 安装文件。

使用 **StorageGRID** 设备安装程序自动配置设备

您可以使用包含配置信息的 JSON 文件自动配置设备。您可以使用 StorageGRID 设备安装程序上传文件。

您需要的内容

- 您的设备必须使用与 StorageGRID 11.5 或更高版本兼容的最新固件。
- 您必须连接到要使用配置的设备上的 StorageGRID 设备安装程序 支持的 Web 浏览器。

关于此任务

您可以自动执行设备配置任务，例如配置以下内容：

- 网格网络，管理网络和客户端网络 IP 地址
- BMC 接口
- 网络链路
  - 端口绑定模式
  - 网络绑定模式
  - 链路速度

使用上传的 JSON 文件配置设备通常比在 StorageGRID 设备安装程序中使用多个页面手动执行配置效率更高，尤其是在需要配置多个节点时。您必须一次应用一个节点的配置文件。

有经验的用户如果希望自动安装和配置其设备，可以使用 `configure-sGA .py` 脚本。+使用 configure-sga.py 脚本自动安装和配置设备节点

步骤

1. 使用以下方法之一生成 JSON 文件：
   - ConfigBuilder 应用程序

     "ConfigBuilder.netapp.com"

   - `configure-sGa.py` 设备配置脚本。您可以从 StorageGRID 设备安装程序（ * 帮助 * > * 设备配置脚

本 * ）下载此脚本。请参见有关使用 configure-sga.py 脚本自动配置的说明。

使用 configure-sga.py 脚本自动安装和配置设备节点

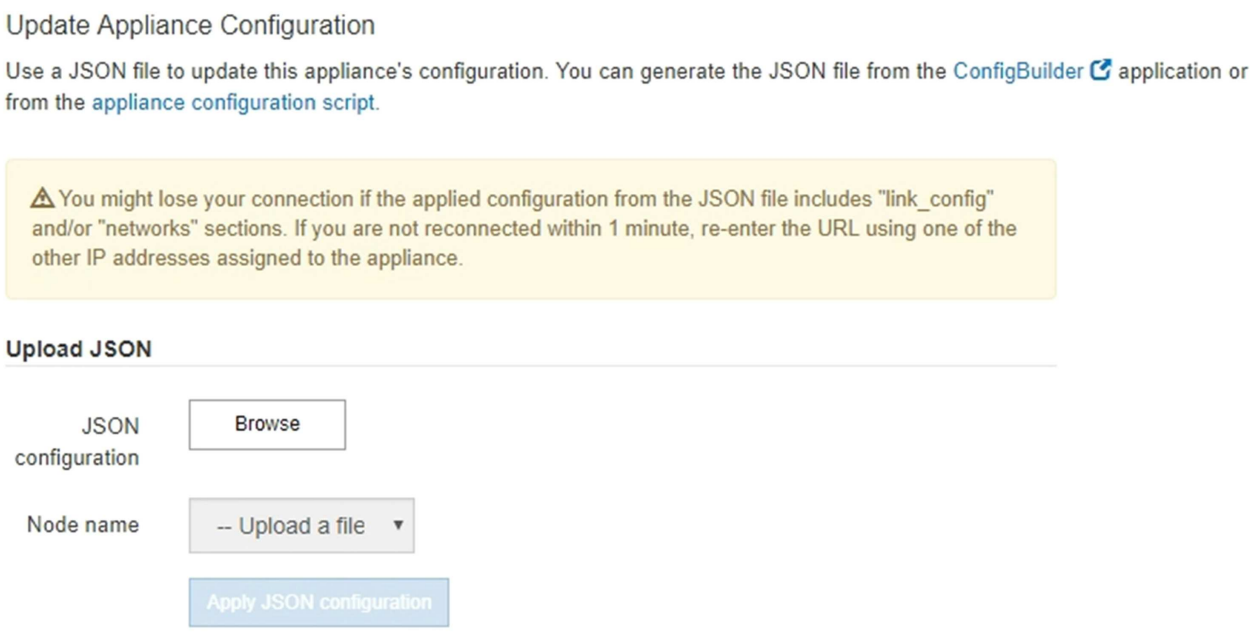
JSON 文件中的节点名称必须符合以下要求：

- 必须是一个有效的主机名，至少包含 1 个字符，并且不超过 32 个字符
- 可以使用字母，数字和连字符
- 不能以连字符开头或结尾
- 不能仅包含数字

> 请确保 JSON 文件中的节点名称（顶级名称）是唯一的，否则您将无法使用 JSON 文件配置多个节点。

2. 选择 * 高级 * > * 更新设备配置 * 。

此时将显示更新设备配置页面。

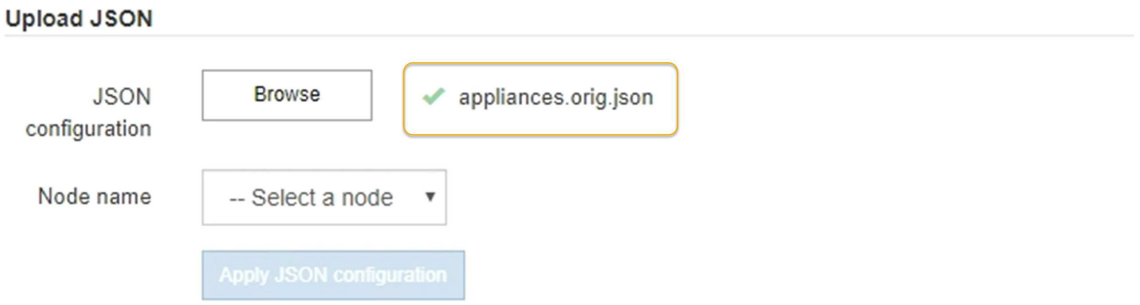


3. 选择包含要上传的配置的 JSON 文件。

a. 选择 * 浏览 * 。
b. 找到并选择文件。
c. 选择 * 打开 * 。

已上传并验证此文件。验证过程完成后，文件名会显示在绿色复选标记旁边。

如果 JSON 文件中的配置包含 "link_config" ， "networks" 或这两者的部分，则可能会断开与设备的连接。如果 1 分钟内未重新连接，请使用分配给设备的其他 IP 地址之一重新输入设备 URL 。

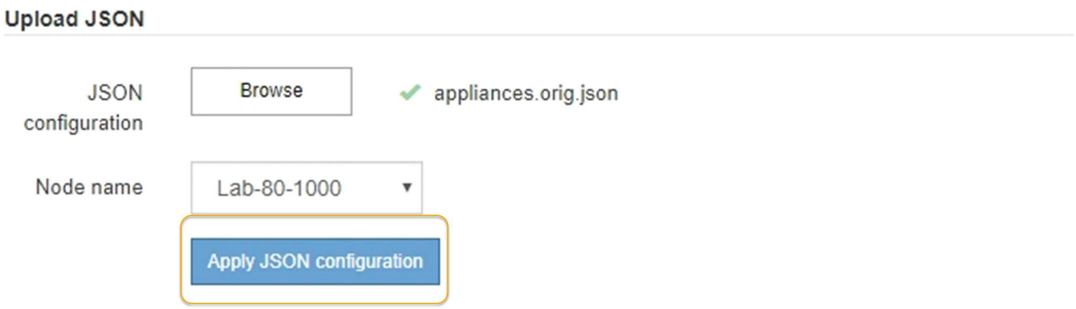


此时将使用 JSON 文件中定义的顶级节点名称填充 * 节点名称 * 下拉列表。

如果文件无效，则文件名将显示为红色，并在黄色横幅中显示一条错误消息。此无效文件不会应用于此设备。您可以使用 ConfigBuilder 来确保具有有效的 JSON 文件。

4. 从 * 节点名称 * 下拉列表中选择一个节点。

   此时将启用 * 应用 JSON 配置 * 按钮。



5. 选择 * 应用 JSON 配置 * 。

   此配置将应用于选定节点。

使用 **configure-sga.py** 脚本自动安装和配置设备节点

您可以使用 `configure-sGa.py` 脚本自动执行 StorageGRID 设备节点的许多安装和配置任务，包括安装和配置主管理节点。如果要配置大量设备，此脚本可能会很有用。您也可以使用此脚本生成包含设备配置信息的 JSON 文件。

您需要的内容

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为主管理节点配置网络链路和 IP 地址。

- 如果要安装主管理节点，则您知道其 IP 地址。
- 如果要安装和配置其他节点，则已部署主管理节点，并且您知道其 IP 地址。
- 对于主管理节点以外的所有节点，已在主管理节点上的网格网络子网列表中定义 StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网。
- 您已下载 `configure-sGA .py` 文件。该文件包含在安装归档中，您也可以通过单击 StorageGRID 设备安装程序中的 * 帮助 * > * 设备安装脚本 * 来访问该文件。

> 此操作步骤 适用于在使用命令行界面方面具有一定经验的高级用户。或者，您也可以使用 StorageGRID 设备安装程序自动执行配置。+使用 StorageGRID 设备安装程序自动配置设备

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 要获得有关脚本语法的一般帮助以及查看可用参数列表，请输入以下内容：

```
configure-sga.py --help
```

`configure-sGa.py` 脚本使用五个子命令：

- **高级** 用于高级 StorageGRID 设备交互，包括 BMC 配置和创建包含设备当前配置的 JSON 文件
- `configure` 用于配置 RAID 模式，节点名称和网络参数
- `install` 用于开始 StorageGRID 安装
- `m` 监控 StorageGRID 安装
- `reboot` 用于重新启动设备

如果输入子命令（ advanced ， configure ， install ， monitor 或 reboot ）参数，然后输入 ` -help` 选项，则会收到其他帮助文本，其中提供了有关该子命令中可用选项的更多详细信息： + `configure-sga.py` *`subcommand`* `-help`

3. 要确认设备节点的当前配置，请输入以下内容，其中 ` *SGA-install-IP*` 是设备节点的任一 IP 地址： + `configure-sga.py configure` *`SGA-install-IP`*

结果将显示设备的当前 IP 信息，包括主管理节点的 IP 地址以及有关管理，网格和客户端网络的信息。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
```

```
200

  StorageGRID Appliance
    Name:         LAB-SGA-2-30
    Node type:    storage

  StorageGRID primary Admin Node
    IP:         172.16.1.170
    State:      unknown
    Message:    Initializing...
    Version:    Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:       FIXED
        Link speed:           10GBE

        Grid Network:         ENABLED
            Bonding mode:     active-backup
            VLAN:             novlan
            MAC Addresses:    00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:        ENABLED
            Bonding mode:     no-bond
            MAC Addresses:    00:80:e5:29:70:f4

        Client Network:       ENABLED
            Bonding mode:     active-backup
            VLAN:             novlan
            MAC Addresses:    00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:       172.16.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:8A
    Gateway:    172.16.0.1
    Subnets:    172.17.0.0/21
```

```
                172.18.0.0/21
                192.168.0.0/21
    MTU:        1500

  Admin Network
    CIDR:       10.224.2.30/21 (Static)
    MAC:        00:80:E5:29:70:F4
    Gateway:    10.224.0.1
    Subnets:    10.0.0.0/8
                172.19.0.0/16
                172.21.0.0/16
    MTU:        1500

  Client Network
    CIDR:       47.47.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:89
    Gateway:    47.47.0.1
    MTU:        2000

######################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
######################################################################
```

4. 如果需要更改当前配置中的任何值，请使用 `configure` 子命令对其进行更新。例如，如果要将设备用于连接到主管理节点的 IP 地址更改为 `172.16.2.99` ，请输入以下内容： + `configure-sga.py configure -admin-IP 172.16.2.99 sGA-install-ip`
5. 如果要将设备配置备份到 JSON 文件，请使用 `advanced` 和 `backup-file` 子命令。例如，如果要将 IP 地址为 ` SGA-install-ip_` 的设备配置备份到名为 `appliance-SG1000.json` 的文件中，请输入以下命令： + `configure-sga.py advanced -backup-file appliance-SG1000.json SGA-install-IP`

   包含配置信息的 JSON 文件将写入执行脚本的同一目录。

   > 检查生成的 JSON 文件中的顶级节点名称是否与设备名称匹配。请勿对此文件进行任何更改，除非您是经验丰富的用户并全面了解 StorageGRID API 。

6. 如果对设备配置满意，请使用 `install` 和 `monitor` 子命令安装此设备： + `configure-sga.py install -monitor sGA-install-ip`
7. 如果要重新启动设备，请输入以下内容： + `configure-sga.py reboot sGA-install-ip`

自动配置 **StorageGRID**

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	Description
`configure-storaggrid.py`	用于自动配置的 Python 脚本
`configure-storaggrid.sample.json`	用于脚本的示例配置文件
`configure-storaggrid.blank.json`	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

关于此任务

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

> 您也可以使用网格管理器或安装 API 配置系统。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如： + `cd StorageGRID-Webscale -version/platform`

   其中，` *platform*` 是 `dEBS` ， `rpms` 或 `vSphere` 。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完成后

在配置过程中会生成一个恢复包 ` .zip` 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 `passwords.txt` 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

安装 **REST API** 概述

StorageGRID 提供了两个用于执行安装任务的 REST API： StorageGRID 安装 API 和 StorageGRID 设备安装程序 API 。

这两个 API 都使用 Swagger 开源 API 平台来提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 **API**

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。
- **recovery-package** —下载恢复软件包的操作。
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

StorageGRID 设备安装程序 API

StorageGRID 设备安装程序 API 可通过 HTTPS 从 ` Controller_IP_ ： 8443` 访问。

要访问 API 文档，请转到设备上的 StorageGRID 设备安装程序，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 设备安装程序 API 包括以下部分：

- * 克隆 * —用于配置和控制节点克隆的操作。
- * 加密 * —用于管理加密和查看加密状态的操作。
- * 硬件配置 * —用于在连接的硬件上配置系统设置的操作。
- * 安装 * —用于开始设备安装和监控安装状态的操作。
- * 网络连接 * - 与 StorageGRID 设备的网格，管理和客户端网络配置以及设备端口设置相关的操作。
- * 设置 * —用于帮助初始设备安装设置的操作，包括请求获取有关系统的信息并更新主管理节点 IP 。
- * 支持 * —用于重新启动控制器和获取日志的操作。
- * 升级 * —与升级设备固件相关的操作。
- **uploadsg** —用于上传 StorageGRID 安装文件的操作。

硬件安装故障排除（ **SG5600** ）

如果您在安装期间遇到问题，查看与硬件设置和连接问题相关的故障排除信息可能会很有帮助。

硬件设置似乎挂起（ **SG5600** ）

如果硬件故障或布线错误导致 E5600SG 控制器无法完成启动处理，则 StorageGRID 设备安装程序可能不可用。

步骤

1. 检查任一控制器上的 "Need Attention LED" ，并查找是否存在闪烁的错误代码。

   在启动期间，硬件初始化期间，允许服务操作和需要服务操作 LED 会亮起。较低位数的小数点上限（称为 *diagnostic LED* ）也会亮起。七段式显示会显示两个控制器共有的一系列代码。这是正常的，并不表示出现错误。硬件成功启动后，服务操作 LED 将关闭，而显示内容将由固件驱动。

2. 查看 E5600SG 控制器的七段显示屏上的代码。

   > 安装和配置需要一些时间。某些安装阶段在几分钟内不会向 StorageGRID 设备安装程序报告更新。

   如果发生错误，七段显示屏将按顺序闪烁，例如， "he" 。

3. 要了解这些代码的含义，请参见以下资源：

控制器	参考
E5600SG 控制器	• "`错误：与 SANtricity OS 软件同步时出错` " • "`E5600SG 控制器七段显示代码` "
E2700 控制器	E 系列文档 • 注： * 为 E 系列 E5600 控制器描述的代码不适用于设备中的 E5600SG 控制器。

4. 如果无法解决问题描述 问题，请联系技术支持。

相关信息

E5600SG 控制器七段显示代码

he error： Error synchronating with SANtricity OS Software

"《 E2700 控制器驱动器托盘和相关驱动器托盘安装指南》"

"NetApp 文档： E2700 系列"

he error： Error synchronating with SANtricity OS Software

如果 StorageGRID 设备安装程序无法与 SANtricity 操作系统软件同步，则计算控制器上的七段显示会显示一个错误代码。

关于此任务

如果显示错误代码，请执行此更正操作。

步骤

1. 检查两根 SAS 互连缆线的完整性，并确认它们已牢固连接。
2. 根据需要更换一根或两根缆线，然后重试。
3. 如果无法解决问题描述 问题，请联系技术支持。

对连接问题进行故障排除（ **SG5600** ）

如果您在 StorageGRID 设备安装期间遇到连接问题，应执行列出的更正操作步骤。

无法通过网络连接到 **StorageGRID** 设备

如果无法连接到设备，则可能存在网络问题描述 ，或者硬件安装可能未成功完成。

- * 问题描述 *

  您无法连接到设备。

- * 发生原因 *

如果存在网络问题描述 或硬件安装未成功完成，则可能会发生这种情况。

- * 更正操作 *
  a. 对设备执行 Ping 操作： + ` * ping *E5600_controller_IP*`
  b. 打开浏览器并输入以下命令来访问 StorageGRID 设备安装程序： + ` * https://*Management_Port_IP*:8443*`

     对于 Management_Port_IP ，输入 E5600SG 控制器上管理端口 1 的 IP 地址（在物理安装期间配置）。
  c. 单击 * 配置管理网络 * ，然后检查 IP 。
  d. 如果您收到 ping 响应，请检查防火墙中的端口 8443 是否已打开。
  e. 重新启动设备。
  f. 刷新安装网页。
  g. 如果此操作无法解决连接问题描述 ，请从 NetApp 支持站点联系技术支持，网址为 "mysupport.netapp.com"。

相关信息

E5600SG 控制器七段显示代码

在 **StorageGRID** 设备安装程序运行期间重新启动控制器

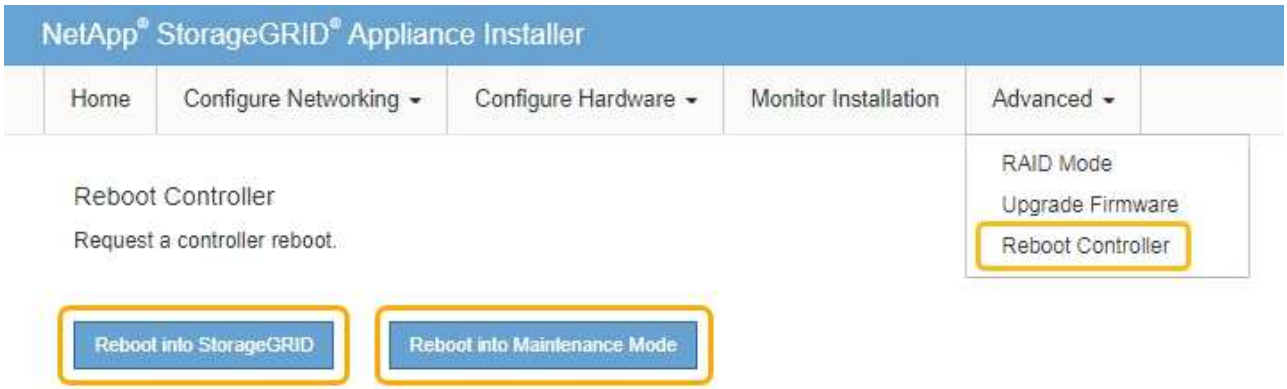
在 StorageGRID 设备安装程序运行期间，您可能需要重新启动计算控制器。例如，如果安装失败，您可能需要重新启动控制器。

关于此任务

只有当计算控制器运行 StorageGRID 设备安装程序时，此操作步骤 才适用。安装完成后，此步骤将不再起作用，因为 StorageGRID 设备安装程序不再可用。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：
   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



控制器将重新启动。

维护 SG5600 设备

您可能需要升级 E2700 控制器上的 SANtricity 操作系统软件，更换 E2700 控制器或 E5600SG 控制器或更换特定组件。本节中的过程假定设备已部署为 StorageGRID 系统中的存储节点。

将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

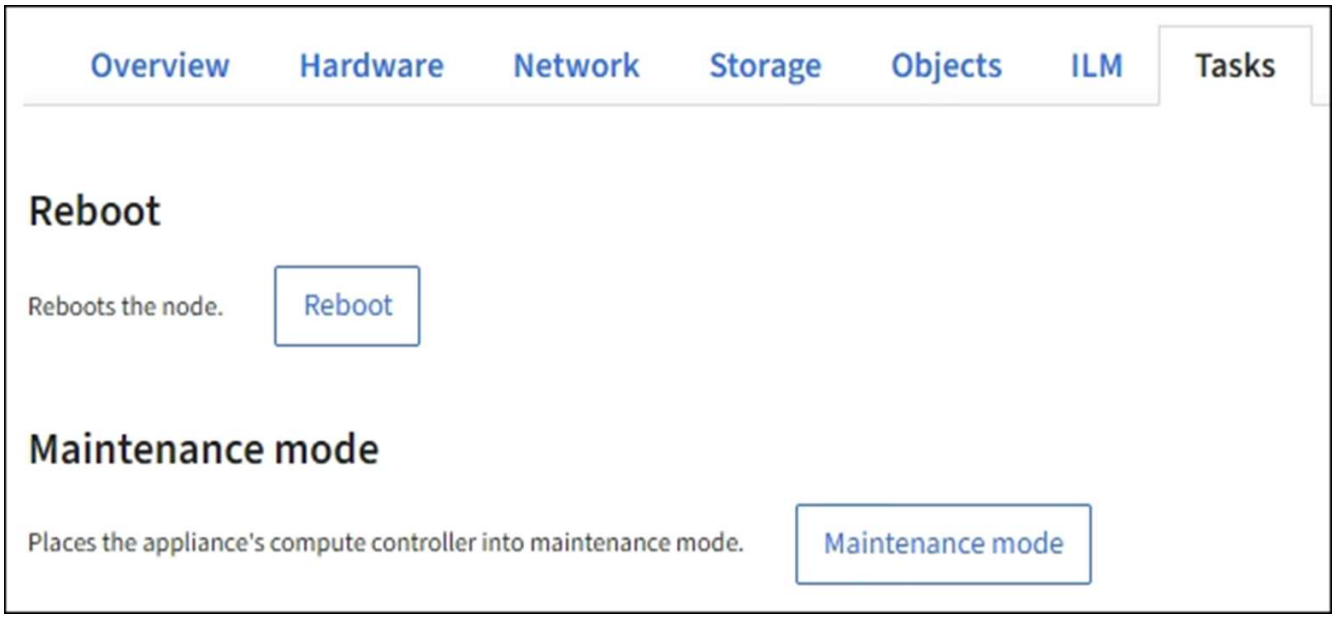
关于此任务

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

处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

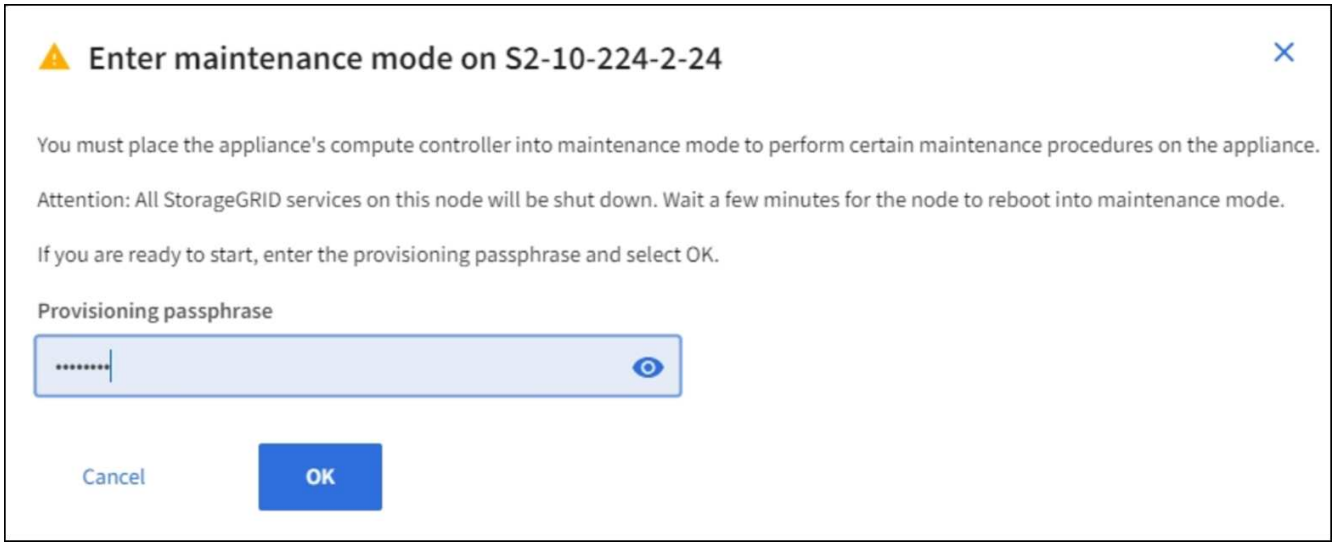
步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面的树视图中，选择设备存储节点。
3. 选择 * 任务 * 。



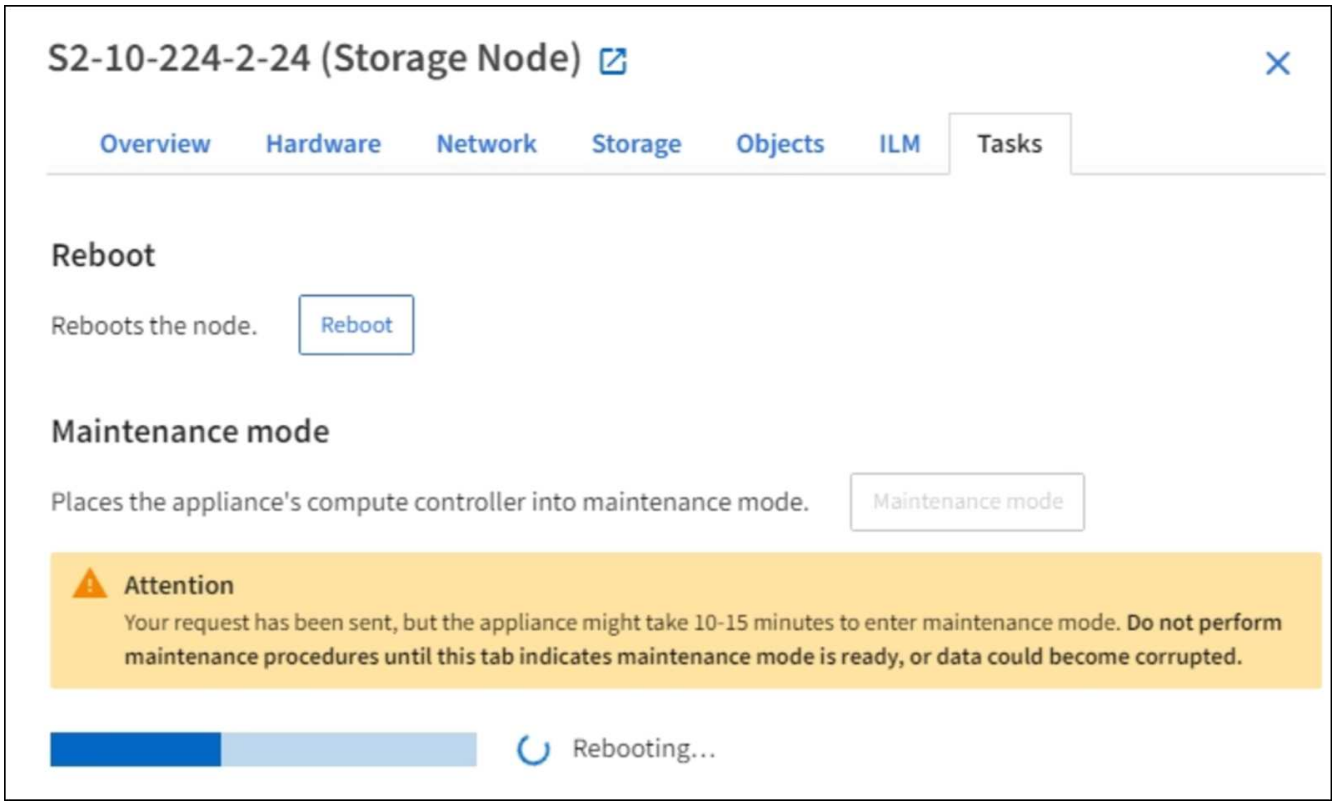
4. 选择 * 维护模式 * 。

   此时将显示确认对话框。

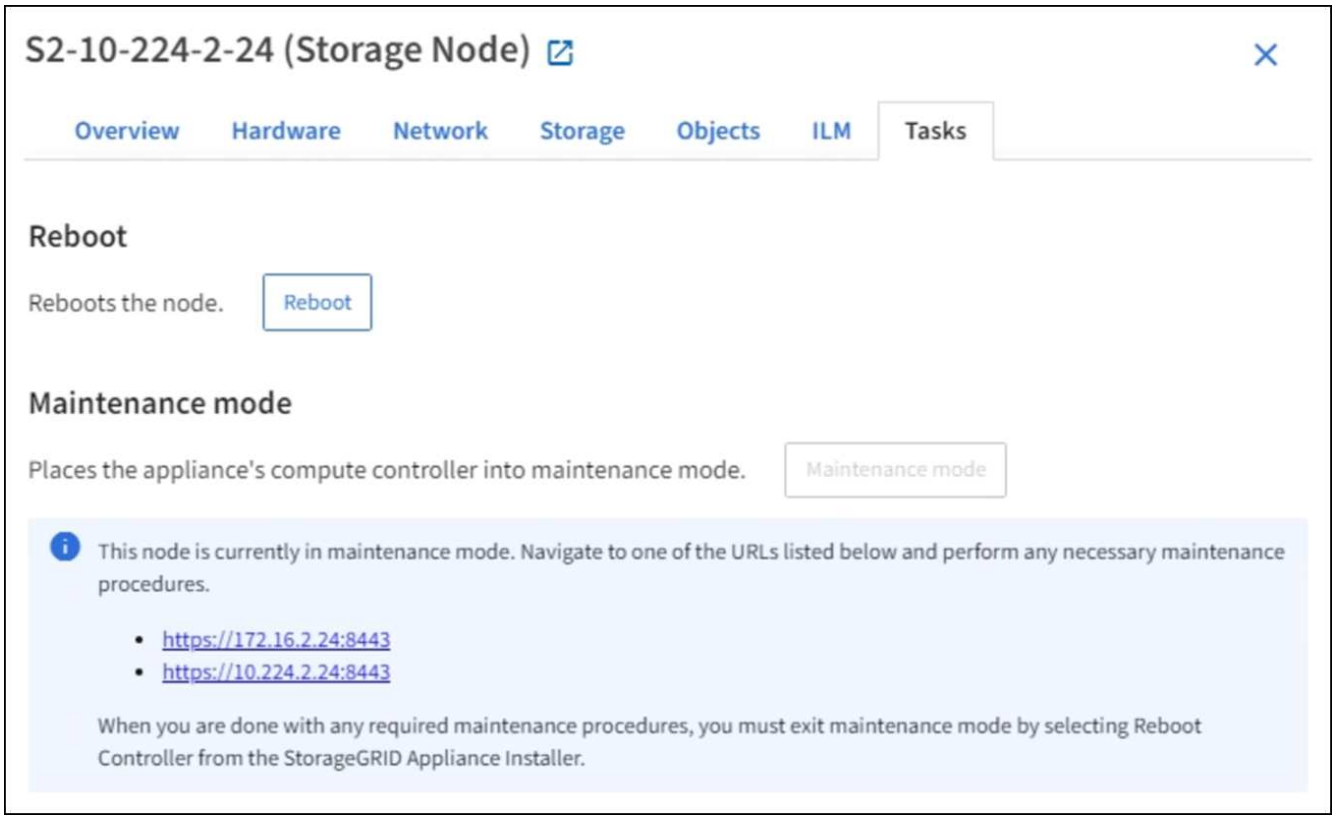


5. 输入配置密码短语，然后选择 * 确定 * 。

   进度条和一系列消息（包括 " 已发送请求 " ， " 正在停止 StorageGRID " 和 " 正在重新启动 " ）表示设备正在完成进入维护模式的步骤。



设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL 。



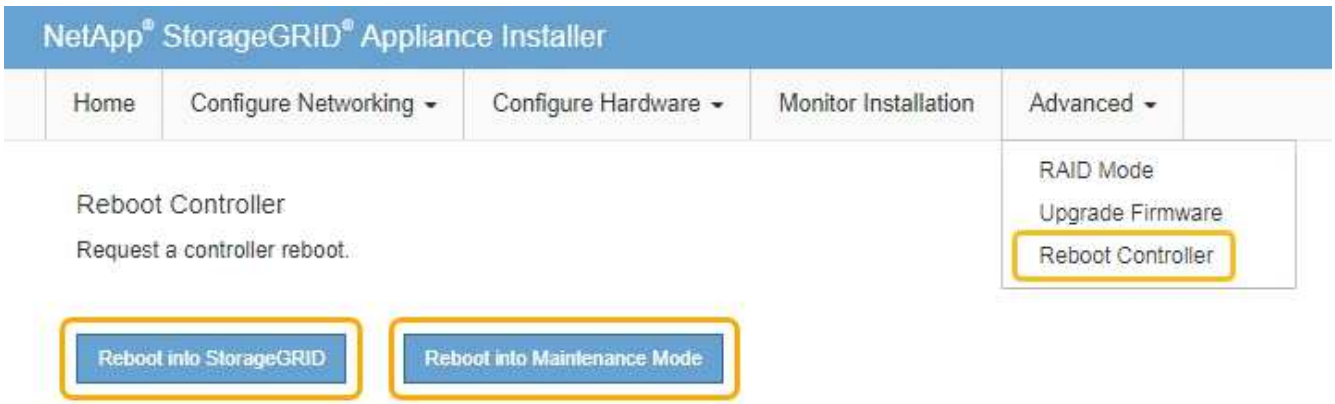
6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL 。

   如果可能，请使用包含设备管理网络端口 IP 地址的 URL 。

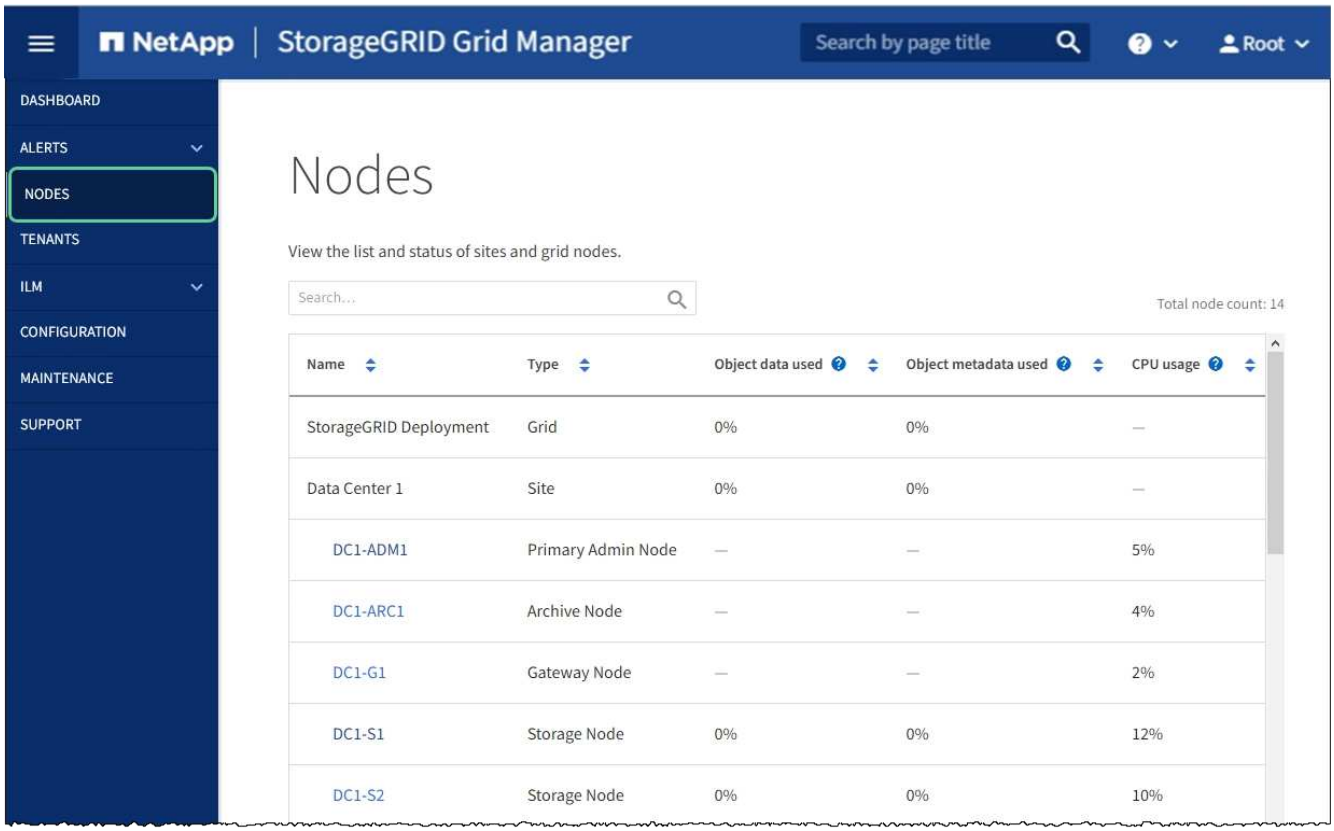
如果您直接连接到设备的管理端口，请使用 ` https://169.254.0.1:8443` 访问 StorageGRID 设备安装程序页面。

7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。

8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



使用网格管理器升级存储控制器上的 **SANtricity** 操作系统

对于当前使用 SANtricity OS 08.42.20.00 （ 11.42 ）或更高版本的存储控制器，您必须使用网格管理器应用升级。

您需要的内容

- 您已查阅 NetApp 互操作性表工具（ IMT ）以确认用于升级的 SANtricity 操作系统版本与您的设备兼容。
- 您具有维护或 root 访问权限。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有配置密码短语。
- 您可以访问 SANtricity 操作系统的 NetApp 下载页面。

关于此任务

在完成 SANtricity 操作系统升级过程之前，您无法执行其他软件更新（ StorageGRID 软件升级或修补程序）。如果您尝试在 SANtricity 操作系统升级过程完成之前启动修补程序或 StorageGRID 软件升级，则系统会重定向到 SANtricity 操作系统升级页面。

只有在 SANtricity 操作系统升级成功应用于已选择进行升级的所有适用节点之后，操作步骤 才会完成。在每个节点上（按顺序）加载 SANtricity 操作系统可能需要 30 分钟以上的时间，并且最多需要 90 分钟来重新启动每个 StorageGRID 存储设备。

只有在使用网格管理器执行升级时，以下步骤才适用。如果设备中的存储控制器使用的 SANtricity 操作系统版本早于 08.42.20.00 （ 11.42 ），则无法使用网格管理器进行升级。

此操作步骤 会自动将 NVSRAM 升级到与 SANtricity 操作系统升级相关的最新版本。您无需应用单独的 NVSRAM 升级文件。

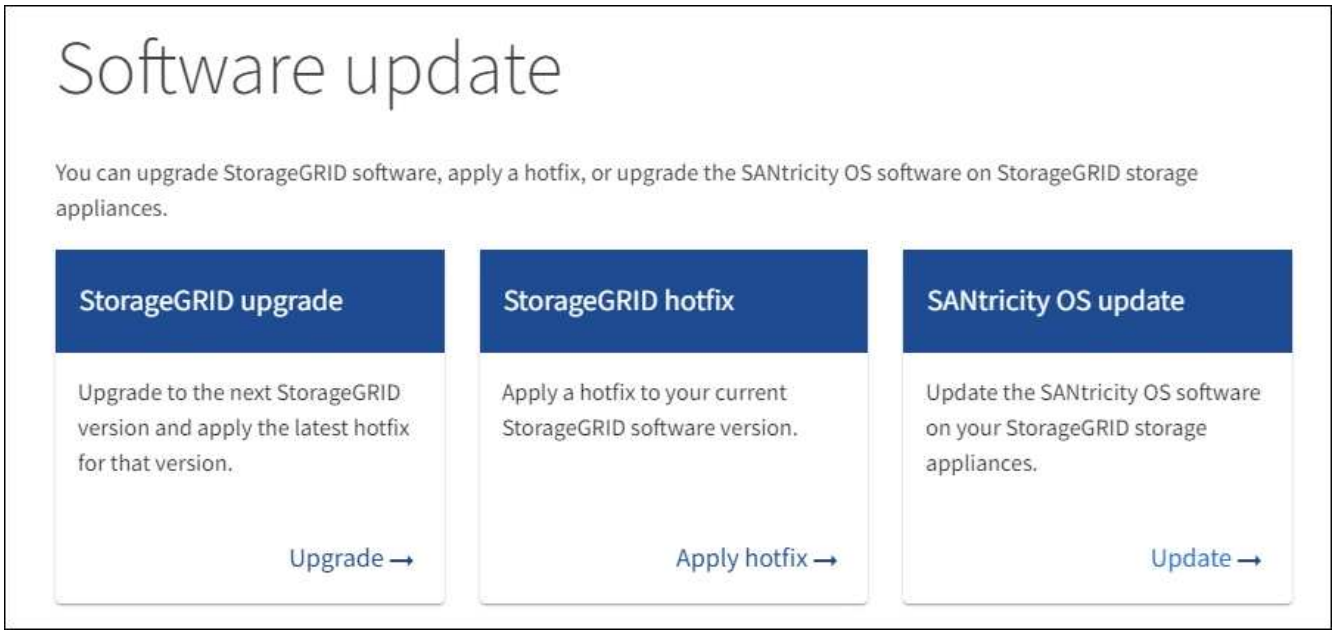
步骤

1. 【下载 _SANtricity 操作系统】从 NetApp 支持站点下载新的 SANtricity 操作系统软件文件。

   请务必为存储控制器选择 SANtricity 操作系统版本。

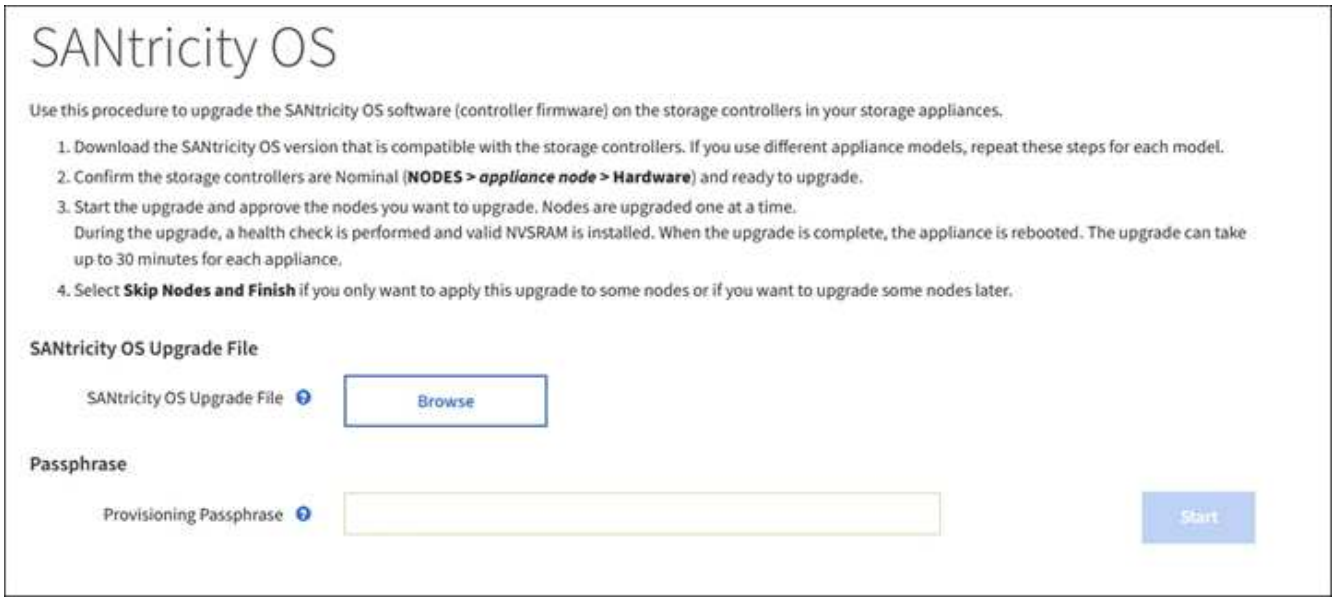
   "NetApp下载：StorageGRID 设备"

2. 选择 * 维护 * > * 系统 * > * 软件更新 * 。



3. 在 SANtricity OS update 部分中，选择 * 更新 * 。

   此时将显示 SANtricity OS 升级页面。



4. 选择从 NetApp 支持站点下载的 SANtricity OS 升级文件。

   a. 选择 * 浏览 * 。

   b. 找到并选择文件。

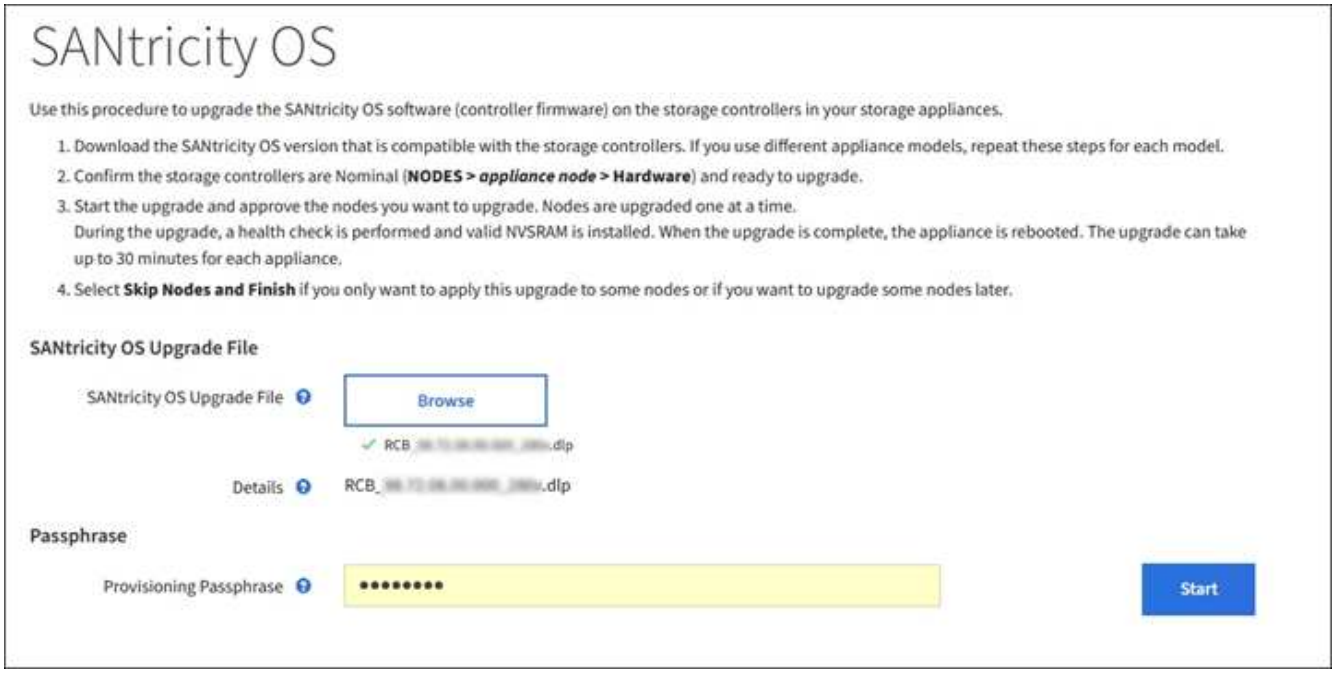
   c. 选择 * 打开 * 。

      已上传并验证此文件。验证过程完成后，文件名会显示在 * 浏览 * 按钮旁边。

      请勿更改文件名，因为它是验证过程的一部分。

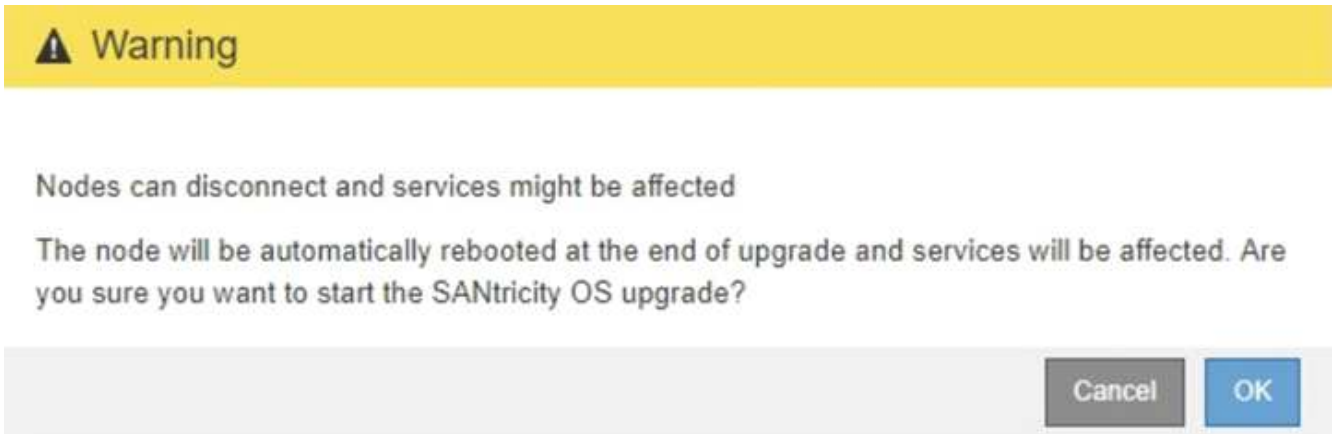
5. 输入配置密码短语。

   已启用 * 开始 * 按钮。



6. 选择 * 开始 * 。

   此时将显示一个警告框，指出在重新启动已升级的节点上的服务时，浏览器的连接可能会暂时断开。



7. 选择 * 确定 * 将 SANtricity 操作系统升级文件暂存到主管理节点。

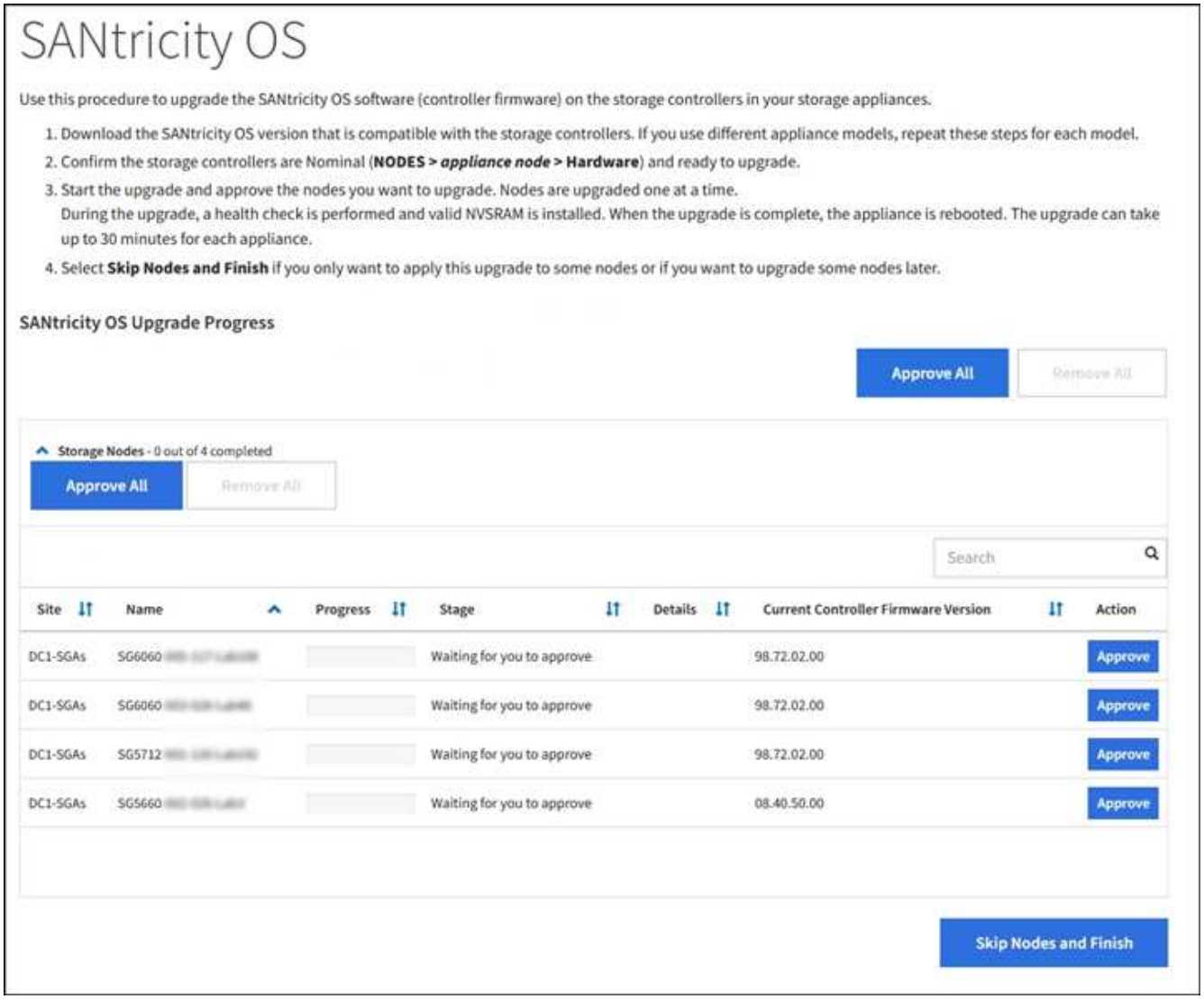
   SANtricity 操作系统升级开始时：

   a. 运行状况检查已运行。此过程会检查是否没有节点的状态为 "Needs Attention （需要注意） " 。

      如果报告了任何错误，请解决这些错误并再次选择 * 启动 * 。

   b. 此时将显示 SANtricity 操作系统升级进度表。此表显示了网格中的所有存储节点以及每个节点的当前升级阶段。

      此表显示了所有设备存储节点。不会显示基于软件的存储节点。对于需要升级的所有节点，请选择 * 批准 * 。



8. 或者，也可以按 * 站点 * ， * 名称 * ， * 进度 * ， * 阶段 * ， * 详细信息 * 按升序或降序对节点列表进行排序。 或 * 当前控制器固件版本 * 。或者，在 * 搜索 * 框中输入一个术语以搜索特定节点。

   您可以使用此部分右下角的左箭头和右箭头滚动浏览节点列表。

9. 批准已准备好添加到升级队列的网格节点。相同类型的已批准节点将一次升级一个。

请勿批准设备存储节点的 SANtricity 操作系统升级，除非您确定该节点已做好停止和重新启动的准备。在某个节点上批准 SANtricity 操作系统升级后，该节点上的服务将停止，升级过程将开始。稍后，当节点完成升级后，设备节点将重新启动。对于与节点通信的客户端，这些操作可能会导致发生原因 服务中断。

- 选择 * 全部批准 * 按钮之一，将所有存储节点添加到 SANtricity 操作系统升级队列。

  如果节点升级顺序非常重要，请一次批准一个节点或一组节点，并等待每个节点完成升级，然后再批准下一个节点。

- 选择一个或多个 * 批准 * 按钮将一个或多个节点添加到 SANtricity OS 升级队列。

  选择 * 批准 * 后，升级过程将确定是否可以升级此节点。如果某个节点可以升级，则会将其添加到升级队列中。

对于某些节点，不会有意应用选定的升级文件，您可以在不升级这些特定节点的情况下完成升级过程。有意未升级的节点会显示完成阶段（已尝试升级），并在详细信息列中列出未升级此节点的原因。

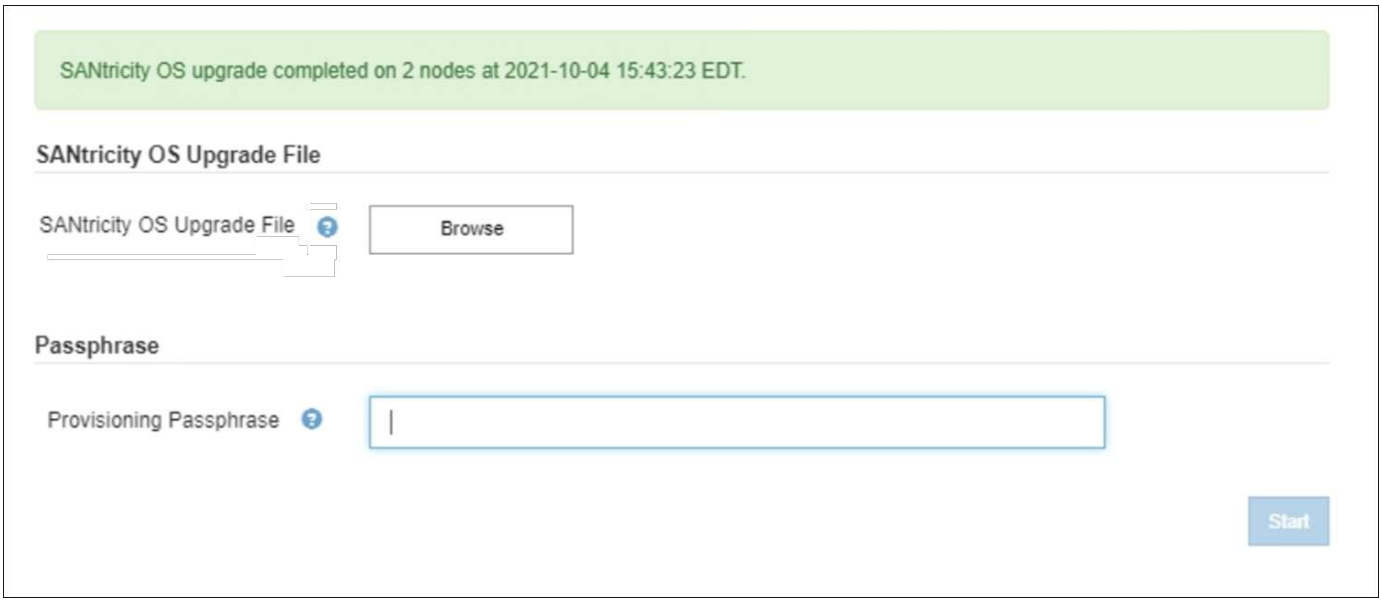
10. 如果需要从 SANtricity 操作系统升级队列中删除一个或所有节点，请选择 * 删除 * 或 * 全部删除 * 。

    当此阶段超过已排队时， * 删除 * 按钮将处于隐藏状态，您无法再从 SANtricity 操作系统升级过程中删除此节点。

11. 等待 SANtricity 操作系统升级应用于每个批准的网格节点。

    - 如果在应用 SANtricity 操作系统升级期间任何节点显示错误阶段，则此节点的升级将失败。在技术支持的协助下，您可能需要将设备置于维护模式才能进行恢复。
    - 如果节点上的固件版本太旧，无法使用网格管理器进行升级，则节点将显示错误阶段并提供详细信息："`您必须使用维护模式升级此节点上的 SANtricity OS 。请参见适用于您的设备的安装和维护说明。升级后，您可以使用此实用程序进行将来的升级。` 要解决此错误，请执行以下操作：
      i. 使用维护模式升级显示 " 错误 " 阶段的节点上的 SANtricity OS 。
      ii. 使用网格管理器重新启动并完成 SANtricity 操作系统升级。

在所有已批准的节点上完成 SANtricity 操作系统升级后， SANtricity 操作系统升级进度表将关闭，绿色横幅将显示 SANtricity 操作系统升级完成的日期和时间。



1. 如果节点无法升级，请记下 "Details" 列中显示的原因并采取相应的措施：
   - " s存储节点已升级。 " 无需执行进一步操作。
   - "`SANtricity 操作系统升级不适用于此节点。` " 此节点没有可由 StorageGRID 系统管理的存储控制器。完成升级过程，而不升级显示此消息的节点。
   - "`SANtricity OS 文件与此节点不兼容。` " 节点所需的 SANtricity 操作系统文件与您选择的文件不同。完成当前升级后，下载适用于此节点的正确 SANtricity OS 文件，然后重复升级过程。

> 只有在所有列出的存储节点上批准 SANtricity 操作系统升级后， SANtricity 操作系统升级过程才会完成。

1. 如果要结束节点批准并返回到 SANtricity OS 页面以允许上传新的 SANtricity OS 文件，请执行以下操作：
   a. 选择 * 跳过节点并完成 * 。

      此时将显示一条警告，询问您是否确实要在不升级所有节点的情况下完成升级过程。

   b. 选择 * 确定 * 返回到 * SANtricity OS* 页面。
   c. 准备好继续批准节点后，请转至 下载 SANtricity 操作系统 重新启动升级过程。

> 已批准并升级的节点仍保持升级状态，而不会出现错误。

2. 对处于完成阶段且需要其他 SANtricity 操作系统升级文件的所有节点重复此升级操作步骤 。

> 对于状态为 "Needs Attenance" 的任何节点，请使用维护模式执行升级。

> 重复升级操作步骤 时，您必须批准先前升级的节点。

相关信息

"NetApp 互操作性表工具"

使用维护模式升级 **E2700** 控制器上的 **SANtricity** 操作系统

如果无法使用网格管理器升级 SANtricity 操作系统软件，请使用维护模式操作步骤 应用升级。

您需要的内容

- 您已查阅 NetApp 互操作性表工具（ IMT ）以确认用于升级的 SANtricity 操作系统版本与您的设备兼容。
- 您必须将E5600控制器置于中 维护模式 如果您不使用网格管理器。将控制器置于维护模式会中断与 E2700 控制器的连接。

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

关于此任务

请勿一次在多个 StorageGRID 设备上升级 E 系列控制器中的 SANtricity 操作系统或 NVSRAM 。

> 一次升级多个 StorageGRID 设备可能会导致发生原因 数据不可用，具体取决于您的部署模式和 ILM 策略。

步骤

1. 确认设备已进入 维护模式。
2. 从服务笔记本电脑访问 SANtricity 存储管理器并登录。
3. 将新的 SANtricity OS 软件文件和 NVSRAM 文件下载到管理客户端。

   > NVSRAM 是特定于 StorageGRID 设备的。请勿使用标准 NVSRAM 下载。

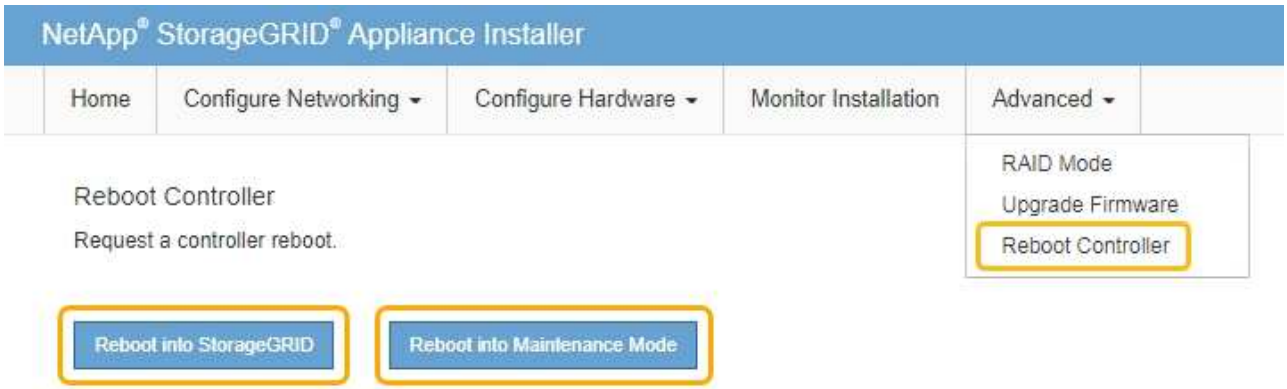
4. 按照 _E2700 和 E5600 SANtricity 软件和固件升级说明 _ 或 SANtricity 存储管理器联机帮助中的说明进行操作，升级 E2700 控制器的固件 NVSRAM 或两者。

   > 如果您需要升级 E2700 控制器中的 NVSRAM ，则必须确认您下载的 SANtricity 操作系统文件已指定与 StorageGRID 设备兼容。

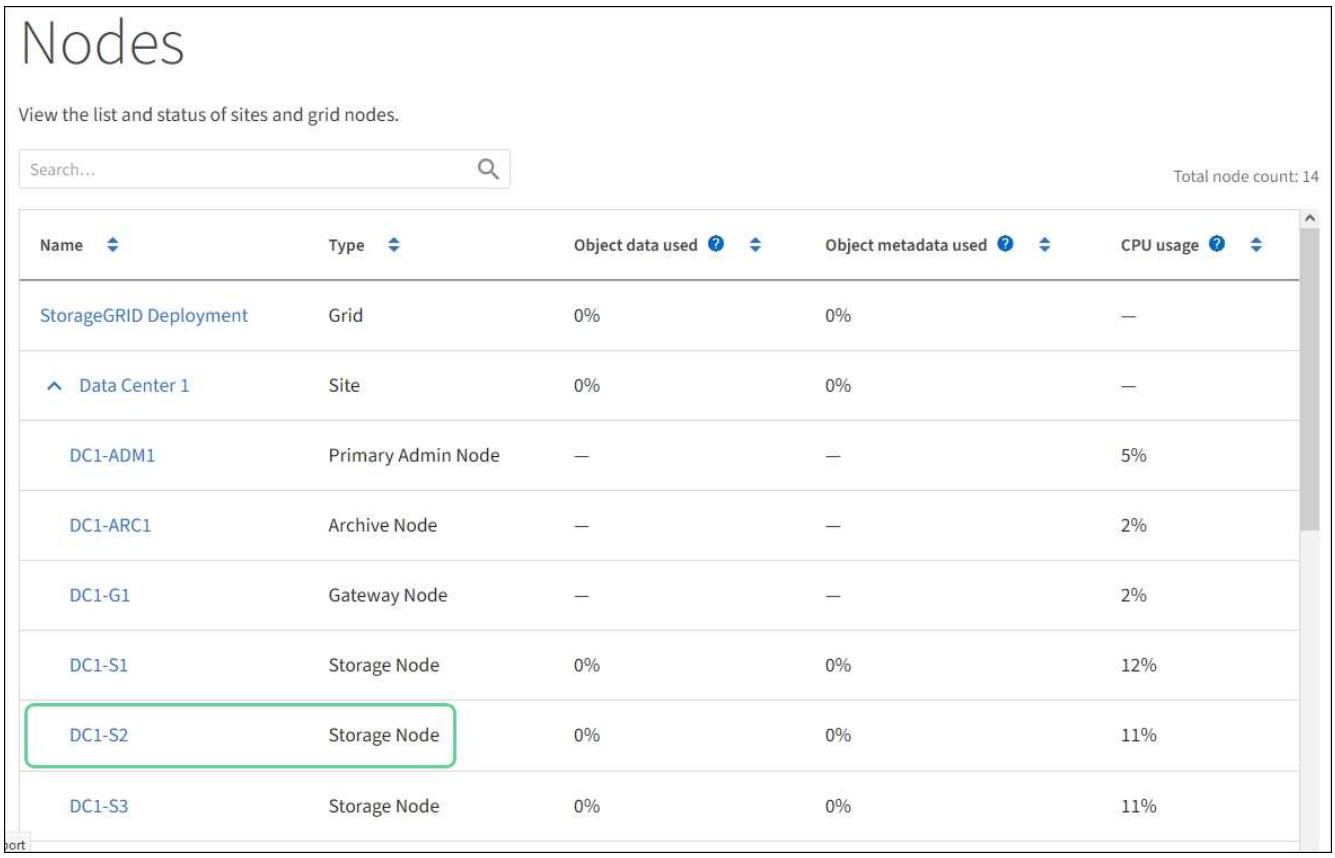
   > 立即激活升级文件。请勿延迟激活。

5. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID *
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。节点页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



使用 **SANtricity** 存储管理器升级驱动器固件

您可以升级驱动器固件，以确保具有所有最新功能和错误修复。

您需要的内容

- 存储设备处于最佳状态。
- 所有驱动器均处于最佳状态。

- 您已安装与您的 SANtricity 版本兼容的最新版本 StorageGRID 存储管理器。

  使用网格管理器升级存储控制器上的 SANtricity 操作系统

  使用维护模式升级 E2700 控制器上的 SANtricity 操作系统

- 您已拥有 已将 StorageGRID 设备置于维护模式。

  维护模式会中断与存储控制器的连接，停止所有 I/O 活动并使所有驱动器脱机。

请勿一次升级多个 StorageGRID 设备上的驱动器固件。这样做可能会导致发生原因 数据不可用，具体取决于您的部署模式和 ILM 策略。

步骤

1. 确认此设备已位于中 维护模式。
2. 打开 Web 浏览器，然后输入 IP 地址作为 SANtricity 存储管理器的 URL： + ` * https://*E2700_Controller_IP*`
3. 如果需要，输入 SANtricity Storage Manager 管理员用户名和密码。
4. 在 SANtricity 企业管理中，选择 * 设备 * 选项卡。

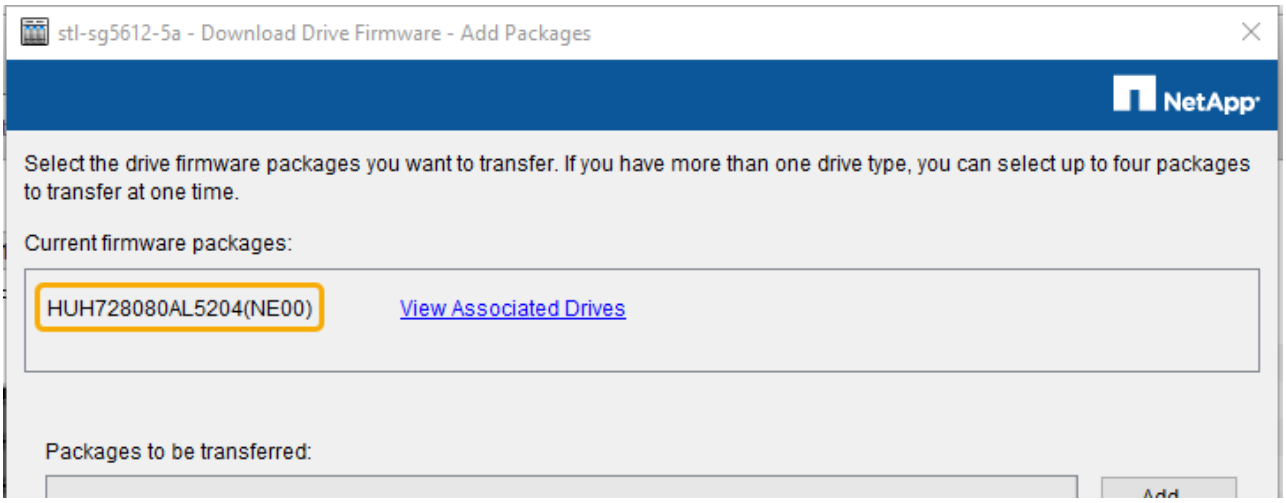
   此时将打开 SANtricity 阵列管理窗口。

5. 在 SANtricity 阵列管理中，双击包含要升级的驱动器的存储阵列。
6. 验证存储阵列和驱动器是否均处于最佳状态。
7. 验证存储设备中当前安装的驱动器固件版本：

   a. 在 SANtricity 企业管理中，选择 * 升级 * > * 驱动器固件 * 。

      Download Drive Firmware - Add Packages 窗口将显示当前正在使用的驱动器固件文件。

   b. 记下当前驱动器固件版本以及当前固件包下的驱动器标识符。



   在此示例中：

- 驱动器固件修订版为 * 。 NE00* 。
- 驱动器标识符为 * 。 HUH728080AL5204* 。

选择 * 查看关联驱动器 * 可显示这些驱动器在存储设备中的安装位置。

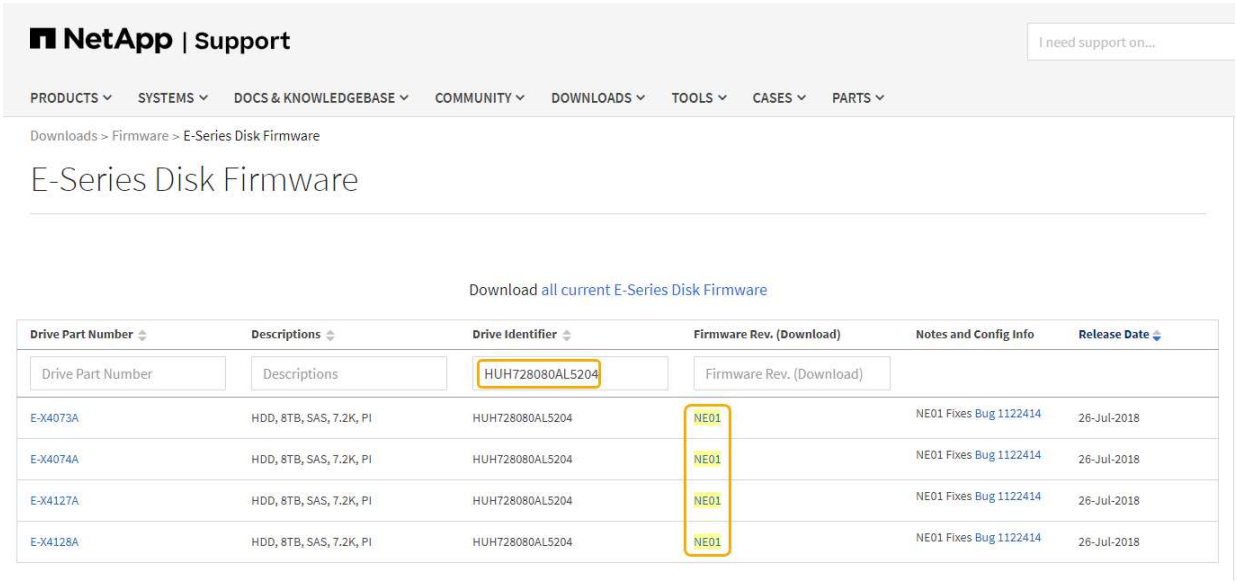
8. 下载并准备可用的驱动器固件升级：
   a. 打开 Web 浏览器，导航到 NetApp 支持网站，然后使用您的 ID 和密码登录。

      "NetApp 支持"

   b. 在 NetApp 支持网站上，选择 * 下载 * 选项卡，然后选择 * E 系列磁盘驱动器固件 * 。

      此时将显示 E 系列磁盘固件页面。

   c. 搜索存储设备中安装的每个 * 驱动器标识符 * ，并验证每个驱动器标识符是否具有最新的固件版本。
      - 如果固件版本不是链接，则此驱动器标识符的固件版本为最新。
      - 如果为驱动器标识符列出了一个或多个驱动器部件号，则可以对这些驱动器进行固件升级。您可以选择任何链接来下载固件文件。



   d. 如果列出了更高版本的固件，请选择固件修订版中的链接（ download ）列以下载包含固件文件的 ` .zip` 归档。
   e. 提取（解压缩）从支持站点下载的驱动器固件归档文件。

9. 安装驱动器固件升级：
   a. 从 SANtricity 存储管理器下载驱动器固件 - 添加软件包窗口中，选择 * 添加 * 。
   b. 导航到包含固件文件的目录，并最多选择四个固件文件。

      驱动器固件文件的文件名类似于 + `D HUC101212CS600_30602291_MS01_2800_0002.DLP`

      选择多个固件文件以升级同一驱动器的固件可能会导致文件冲突错误。如果发生文件冲突错误，则会显示一个错误对话框。要解决此错误，请选择 * 确定 * 并删除除要用于升级驱动器固件的固件之外的所有其他固件文件。要删除固件文件，请在要传输的软件包信息区域中选择固件文件，然后选择 * 删除 * 。

此外，一次最多只能选择四个驱动器固件包。

c. 选择 * 确定 * 。

系统将使用您选择的固件文件更新要传输的软件包信息区域。

d. 选择 * 下一步 * 。

此时将打开 Download Drive Firmware - Select Drives 窗口。

- 系统会扫描设备中的所有驱动器以获取配置信息和升级资格。
- 您可以根据存储阵列中的驱动器种类选择使用所选固件升级的兼容驱动器。默认情况下，系统会显示能够作为联机操作进行升级的驱动器。
- 为驱动器选择的固件将显示在建议的固件信息区域中。如果必须更改固件，请选择 * 返回 * 以返回上一个对话框。

e. 从驱动器升级功能中，选择 * 并行 * 下载操作或 * 全部 * 。

由于设备处于维护模式，所有驱动器和所有卷的 I/O 活动都将停止，因此您可以使用上述任一升级方法。

f. 在兼容驱动器中，选择要升级选定固件文件的驱动器。

- 对于一个或多个驱动器，选择要升级的每个驱动器。
- 对于所有兼容驱动器，请选择 * 全选 * 。

  最佳实践是，将所有相同型号的驱动器升级到相同的固件修订版。

g. 选择 * 完成 * ；然后键入 `yes` 并选择 * 确定 * 。

- 驱动器固件下载和升级将开始， Download Drive Firmware - progress 用于指示所有驱动器的固件传输状态。
- 参与升级的每个驱动器的状态将显示在 "Devices updateed" （已更新设备）的 "Transfer Progress" （传输进度）列中。

  如果在 24 驱动器系统上升级所有驱动器，则并行驱动器固件升级操作可能需要多达 90 秒才能完成。在较大的系统上，执行时间会稍长。

h. 在固件升级过程中，您可以： +

- 选择 * 停止 * 以停止正在进行的固件升级。当前正在进行的任何固件升级均已完成。任何已尝试固件升级的驱动器都会显示其各自的状态。列出的所有剩余驱动器的状态均为 "Not Attemped" 。

  停止驱动器固件升级过程可能会导致数据丢失或驱动器不可用。

- 选择 * 另存为 * 以保存固件升级进度摘要的文本报告。此报告将使用默认的 .log 文件扩展名进行保存。如果要更改文件扩展名或目录，请更改保存驱动器下载日志中的参数。

i. 使用 Download Drive Firmware - 进度监控驱动器固件升级的进度。驱动器更新区域包含计划进行固件升级的驱动器列表以及每个驱动器的下载和升级传输状态。

参与升级的每个驱动器的进度和状态将显示在传输进度列中。如果在升级期间发生任何错误，请采取适当的建议操作。

- * 待定 *

  对于已计划但尚未启动的联机固件下载操作，将显示此状态。

- 正在进行 *

  正在将固件传输到驱动器。

- * 正在进行重建 *

  如果在快速重建驱动器期间发生卷传输，则会显示此状态。这通常是由于控制器重置或故障以及控制器所有者传输卷造成的。

系统将启动驱动器的完整重建。

- * 失败 - 部分 *

  在出现问题之前，固件仅部分传输到驱动器，从而无法传输其余文件。

- * 失败 - 状态无效 *

  此固件无效。

- * 失败 - 其他 *

  无法下载固件，可能是因为驱动器出现物理问题。

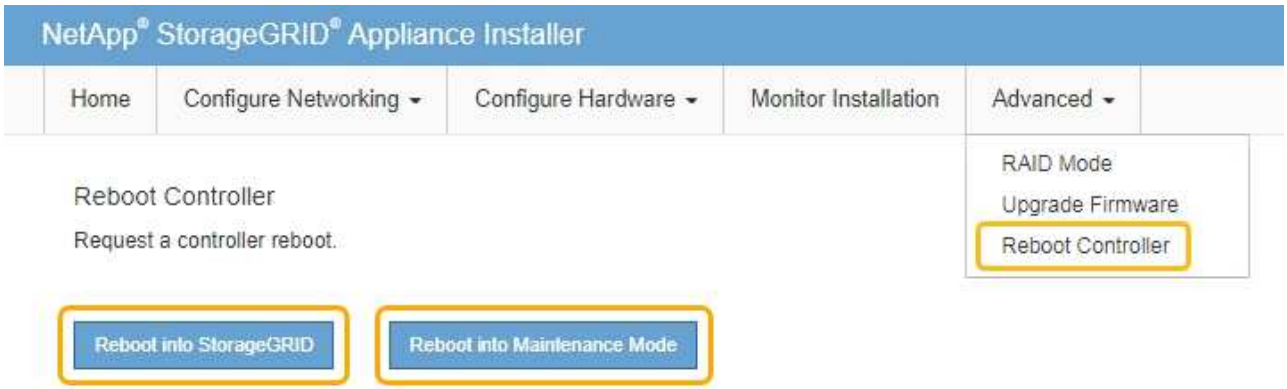
- * 未尝试 *

  未下载固件，原因可能有多种，例如下载在可能发生之前已停止，驱动器不符合升级条件或下载因错误而无法进行。

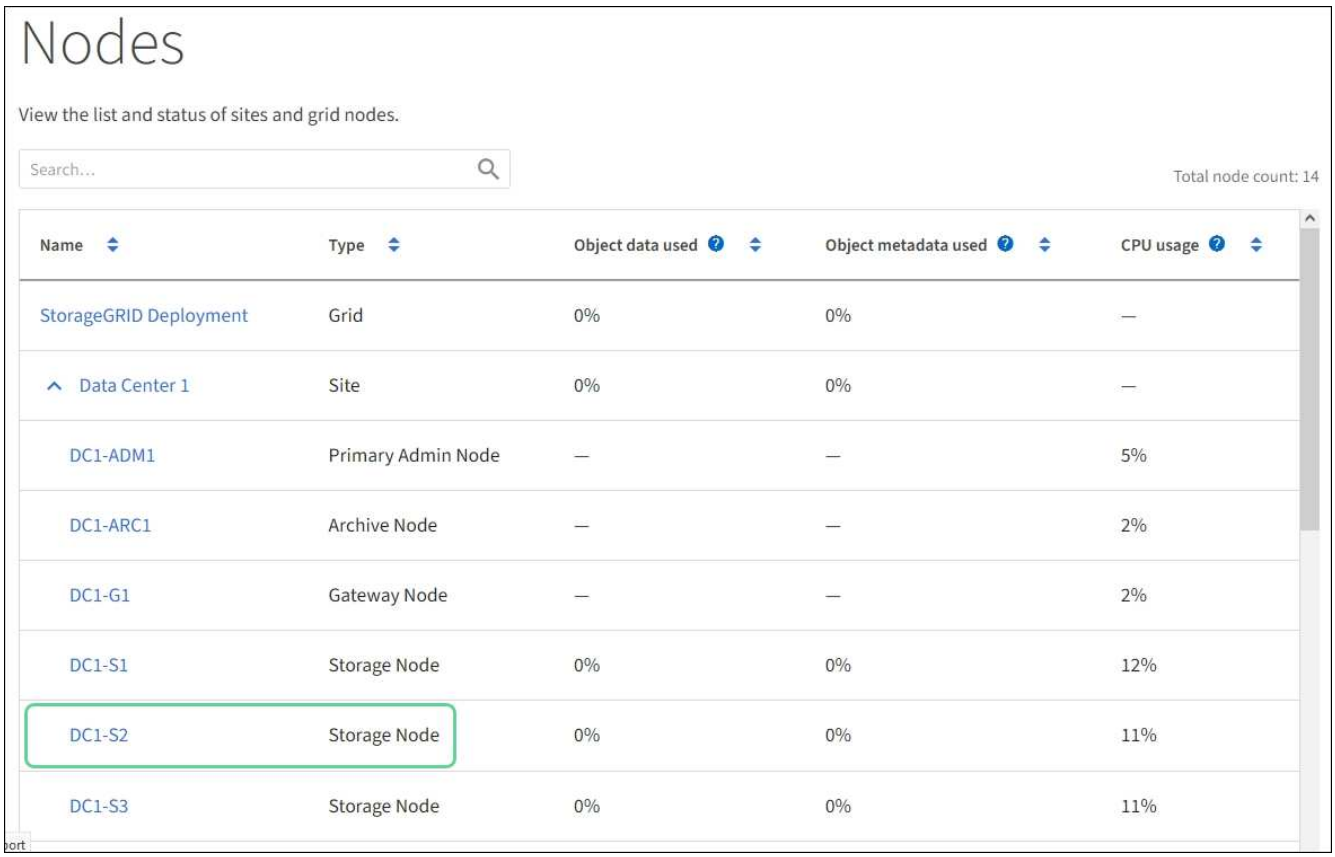
- * 成功 *

  已成功下载此固件。

10. 驱动器固件升级完成后：
    - 要关闭驱动器固件下载向导，请选择 * 关闭 * 。
    - 要重新启动向导，请选择 * 传输更多 * 。
11. 如果此操作步骤 已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：
    - 选择 * 重新启动到 StorageGRID *
    - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤 期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤 中的相应步骤重新启动。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"* 节点 * " 页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



更换 **E2700** 控制器

如果 E2700 控制器运行不正常或出现故障，您可能需要更换它。

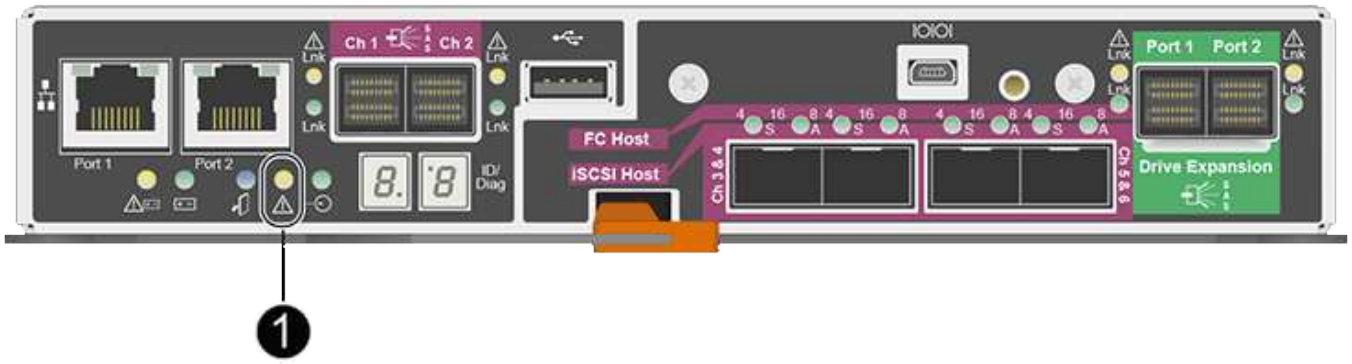
您需要的内容

- 您的更换控制器的部件号与要更换的控制器相同。
- 您可以通过标签来识别连接到控制器的每个缆线。

- 您已获得防静电保护。
- 您必须具有维护或根访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

关于此任务

您可以通过检查控制器上的琥珀色 "Service Action Required LED （需要执行维修操作） "（如图中的 1 所示）来确定控制器是否出现故障。如果此 LED 亮起，则应更换控制器。



更换控制器后，无法访问设备存储节点。如果 E2700 控制器运行正常，您可以将 E5600SG 控制器置于维护模式。

更换控制器时，您必须从原始控制器中取出电池，然后将其安装到替代控制器中。

步骤

1. 准备删除控制器。

   您可以使用 SANtricity 存储管理器执行这些步骤。

   a. 记下控制器上当前安装的 SANtricity OS 软件版本。

   b. 记下当前安装的 NVSRAM 版本。

   c. 如果启用了驱动器安全功能，请确保存在已保存的密钥，并且您知道安装该密钥所需的密码短语。

   > *可能会丢失数据访问和#8212；*如果设备中的所有驱动器均已启用安全性、则新控制器将无法访问此设备、除非您使用SANtricity 存储管理器中的企业管理窗口解锁受保护的驱动器。

   d. 备份配置数据库。

      如果删除控制器时出现问题，您可以使用保存的文件还原配置。

   e. 收集设备的支持数据。

   > 在更换组件之前和之后收集支持数据可确保在更换组件无法解决问题时，您可以向技术支持发送一整套日志。

2. 如果 StorageGRID 设备正在 StorageGRID 系统中运行， 将 E5600SG 控制器置于维护模式。
3. 如果 E2700 控制器运行充分，可以进行可控的关闭，请确认所有操作均已完成。

a. 从阵列管理窗口的标题栏中，选择 * 监控 * > * 报告 * > * 正在执行的操作 * 。

b. 确认所有操作均已完成。

4. 按照单工 E2700 控制器的替代操作步骤 中的说明完成以下步骤：

a. 为缆线贴上标签，然后断开缆线。

> To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

b. 从设备中删除故障控制器。

c. 卸下控制器盖板。

d. 拧下翼形螺钉并从故障控制器中取出电池。

e. 将电池安装到更换用的控制器中，然后更换控制器盖板。

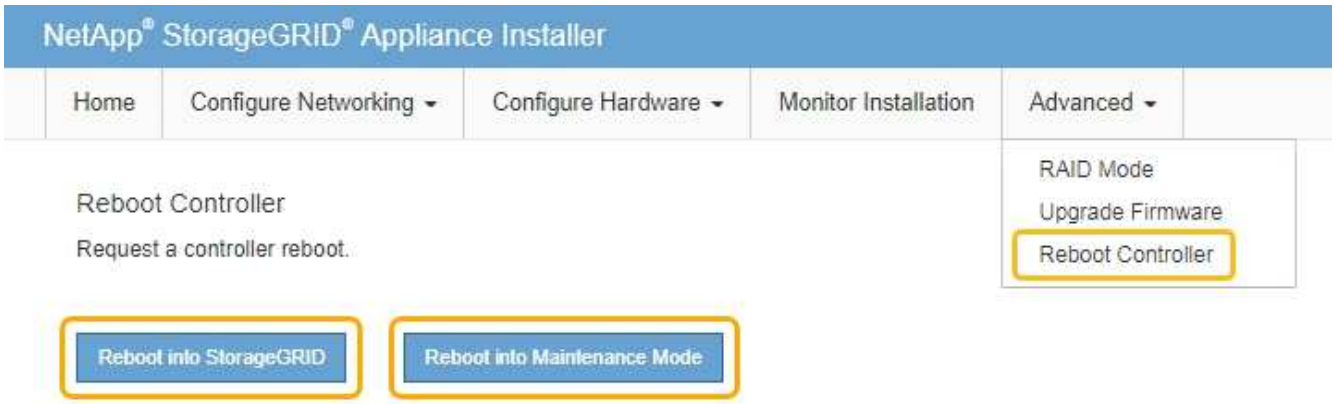
f. 将替代控制器安装到设备中。

g. 更换缆线。

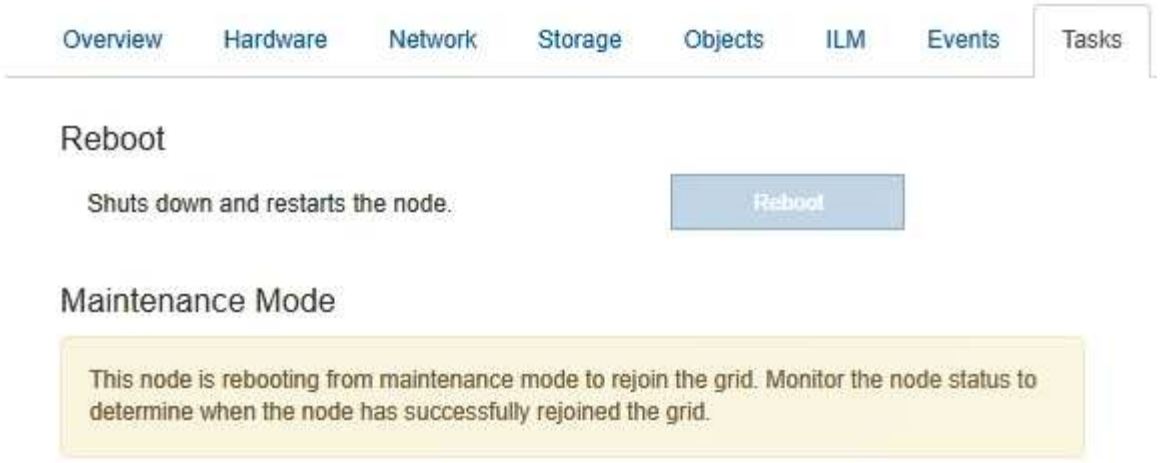
h. 等待 E2700 控制器重新启动。验证七段显示屏是否显示状态 `99` 。

5. 如果设备使用安全驱动器，请导入驱动器安全密钥。

6. 将设备恢复到正常运行模式。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。

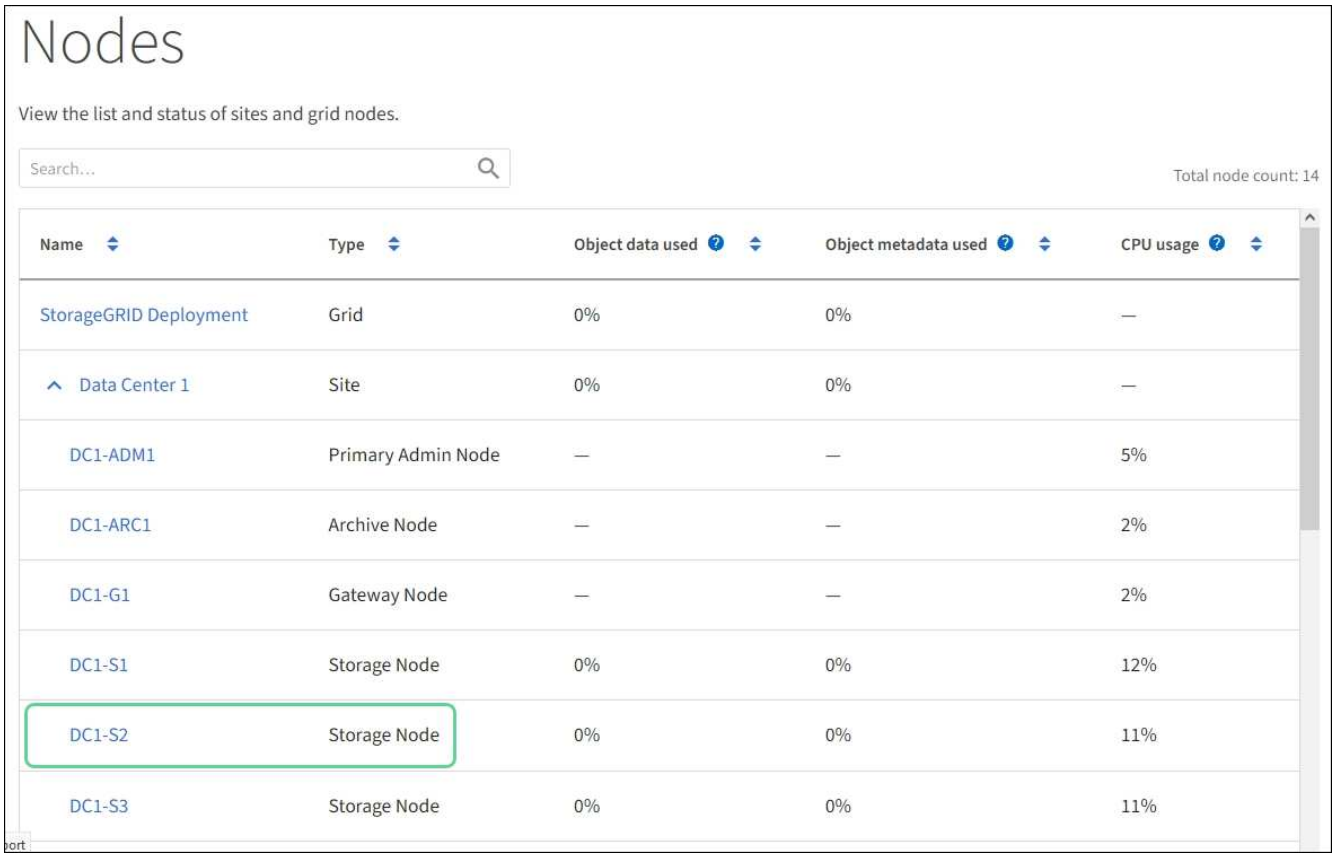


在重新启动期间，将显示以下屏幕：



设备将重新启动并重新加入网格。此过程可能需要长达 20 分钟。

7. 确认重新启动已完成，并且节点已重新加入网格。在网格管理器中，验证节点页面是否显示设备节点的正常状态（节点名称左侧没有图标），表示没有活动警报且节点已连接到网格。



8. 在 SANtricity 存储管理器中，确认新控制器处于最佳状态，然后收集支持数据。

相关信息

"NetApp E 系列和 EF 系列硬件更换过程"

"NetApp 文档： E2700 系列"

更换 **E5600SG** 控制器

您可能需要更换 E5600SG 控制器。

您需要的内容

您必须有权访问以下资源：

- NetApp 支持站点上的 E 系列硬件更换信息，网址为 +http://mysupport.netapp.com/["mysupport.netapp.com"^]
- 支持站点上的 E5600 文档
- 此设备已运行 已置于维护模式。

关于此任务

如果这两个控制器都运行充分，可以进行可控的关闭，则可以先关闭 E5600SG 控制器，以中断与 E2700 控制器的连接。

> 如果在安装 StorageGRID 软件之前更换控制器，则在完成此操作步骤 后，您可能无法立即访问 StorageGRID 设备安装程序。虽然您可以从与设备位于同一子网上的其他主机访问 StorageGRID 设备安装程序，但不能从其他子网上的主机访问它。此情况应在 15 分钟内自行解决（当原始控制器的任何 ARP 缓存条目超时），或者您也可以通过手动从本地路由器或网关清除任何旧的 ARP 缓存条目来立即清除此情况。

步骤

1. 请使用防静电保护。
2. 为连接到 E5600SG 控制器的每个缆线贴上标签，以便可以正确重新连接这些缆线。

> To prevent degraded performance, do not twist, fold, pinch, or step on the cables.请勿将缆线弯曲到半径小于 5 厘米（ 2 英寸）的位置。

3. 将设备置于维护模式后，关闭 E5600SG 控制器。
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 关闭 E5600SG 控制器： + ` * shutdown -h now*`
4. 关闭机箱电源，然后等待控制器背面的所有 LED 和七段显示活动停止。
5. 拔下缆线。
6. 按照 E5600SG 控制器文档中的说明删除控制器。
7. 按照 E5600SG 控制器文档中的说明插入新控制器。

8. 更换所有缆线。
9. 重新打开磁盘机箱的电源。
10. 监控七段代码。
    - E2700 控制器：

      最终 LED 状态为 `99` 。

    - E5600SG 控制器：

      最终 LED 状态为 `HA` 。

11. 在网格管理器中监控设备存储节点的状态。

    验证设备存储节点是否返回到预期状态。

相关信息

"NetApp E 系列和 EF 系列硬件更换过程"

"NetApp 文档： E5600 系列"

更换其他硬件组件

您可能需要更换 StorageGRID 设备中的驱动器，风扇，电源或电池。

您需要的内容

- 您已安装 E 系列硬件更换操作步骤 。
- 此设备已运行 置于维护模式 如果组件更换操作步骤 要求您关闭设备。

关于此任务

更换驱动器，电源风扇箱，风扇箱，电源箱，电池 或驱动器抽盒，请参见 E2700 和 E5600 存储阵列的标准过程。重点介绍有关拆卸和更换硬件本身的分步说明；许多 SANtricity 存储管理器过程不适用于设备。

SG5612 组件更换说明

FRU	请参见
驱动器	按照 E 系列说明中的步骤更换 E2600 ， E2700 ， E5400 ， E5500 ， E5600 或 12 驱动器或 24 驱动器托盘中的驱动器。
电源风扇箱	按照 E 系列说明中的步骤更换 E5612 或 E5624 控制器驱动器托盘中发生故障的电源风扇箱
E2700 控制器中的电池（需要卸下控制器）	按照中的步骤进行操作 更换 E2700 控制器，但请在现有控制器中安装新电池。

FRU	请参见
驱动器	按照 E 系列说明中的步骤更换 E2660 ， E2760 ， E5460 ， E5560 或 E5660 托盘中的驱动器。
动力箱	按照 E 系列说明中的步骤更换 E5660 控制器驱动器托盘中发生故障的电源箱
风扇箱	按照 E 系列说明中的步骤更换 E5660 控制器驱动器托盘中发生故障的风扇箱
E2700 控制器中的电池（需要卸下控制器）	按照中的步骤进行操作 更换 E2700 控制器，但请在现有控制器中安装新电池。

相关信息

"NetApp E 系列和 EF 系列硬件更换过程"

"NetApp 文档： E2700 系列"

"NetApp 文档： E5600 系列"

更改 E5600SG 控制器的链路配置

您可以更改 E5600SG 控制器的以太网链路配置。您可以更改端口绑定模式，网络绑定模式和链路速度。

您需要的内容

将 E5600SG 控制器置于维护模式。

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

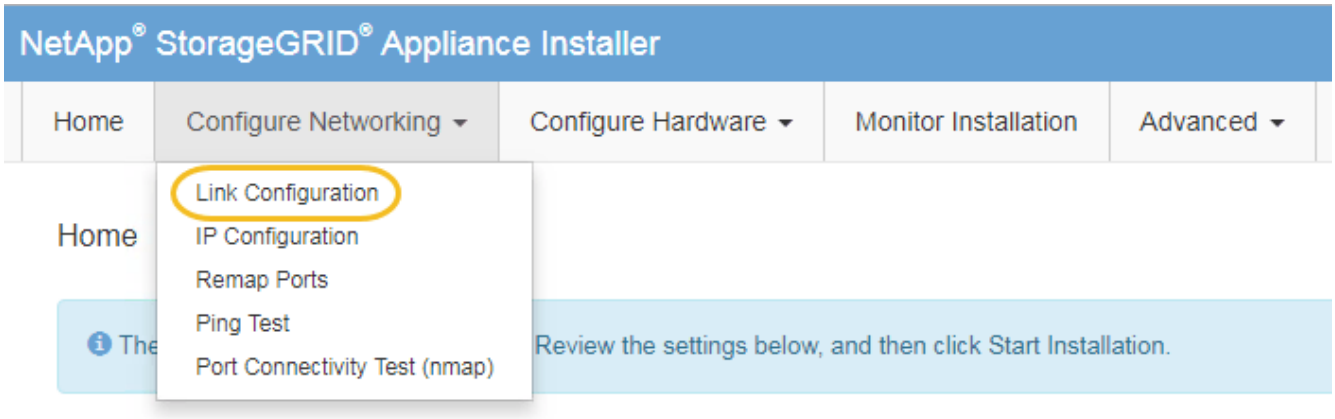
关于此任务

更改 E5600SG 控制器的以太网链路配置的选项包括：

- 将 * 端口绑定模式 * 从 " 固定 " 更改为 " 聚合 " 或从 " 聚合 " 更改为 " 固定 "
- 将 * 网络绑定模式 * 从主动备份更改为 LACP 或从 LACP 更改为主动备份
- 启用或禁用 VLAN 标记，或者更改 VLAN 标记的值
- 将链路速度从 10-GbE 更改为 25-GbE ，或从 25-GbE 更改为 10-GbE

步骤

1. 从菜单中选择 * 配置网络连接 * > * 链路配置 * 。



2. 【change_link_configuration_sg5600 ， start=2]] 对链路配置进行所需的更改。

   有关这些选项的详细信息，请参见 "`配置网络链路 " 。`

3. 对所做的选择感到满意后，单击 * 保存 * 。

   如果更改了所连接的网络或链路，则可能会断开连接。如果 1 分钟内未重新连接，请使用分配给 StorageGRID 设备的其他 IP 地址之一重新输入此设备安装程序的 URL： + ` * https://*E5600SG_Controller_IP*:8443*`

   如果更改了 VLAN 设置，则设备的子网可能已更改。如果需要更改设备的 IP 地址，请按照执行操作 设置 IP 配置 说明。

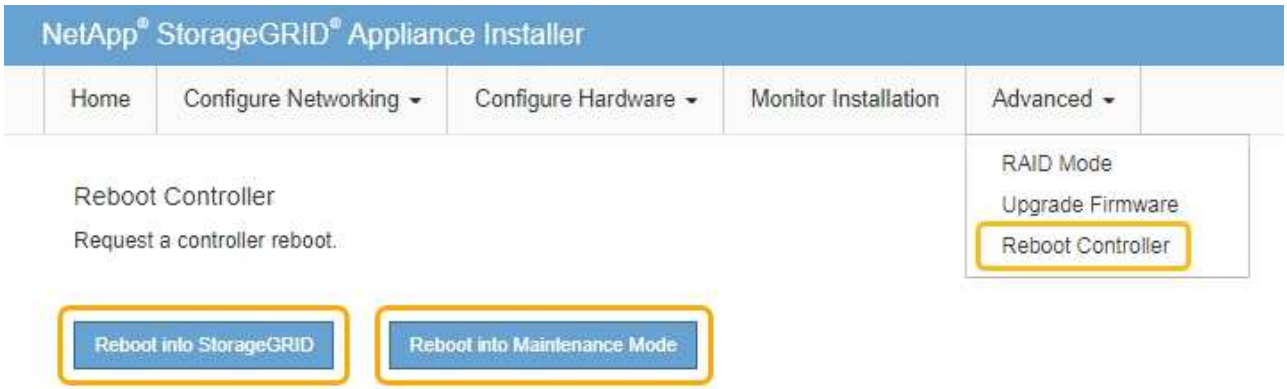
4. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * Ping 测试 * 。

5. 使用 Ping 测试工具检查可能受您在中所做的链路配置更改影响的任何网络上的 IP 地址连接 更改链路配置 步骤。

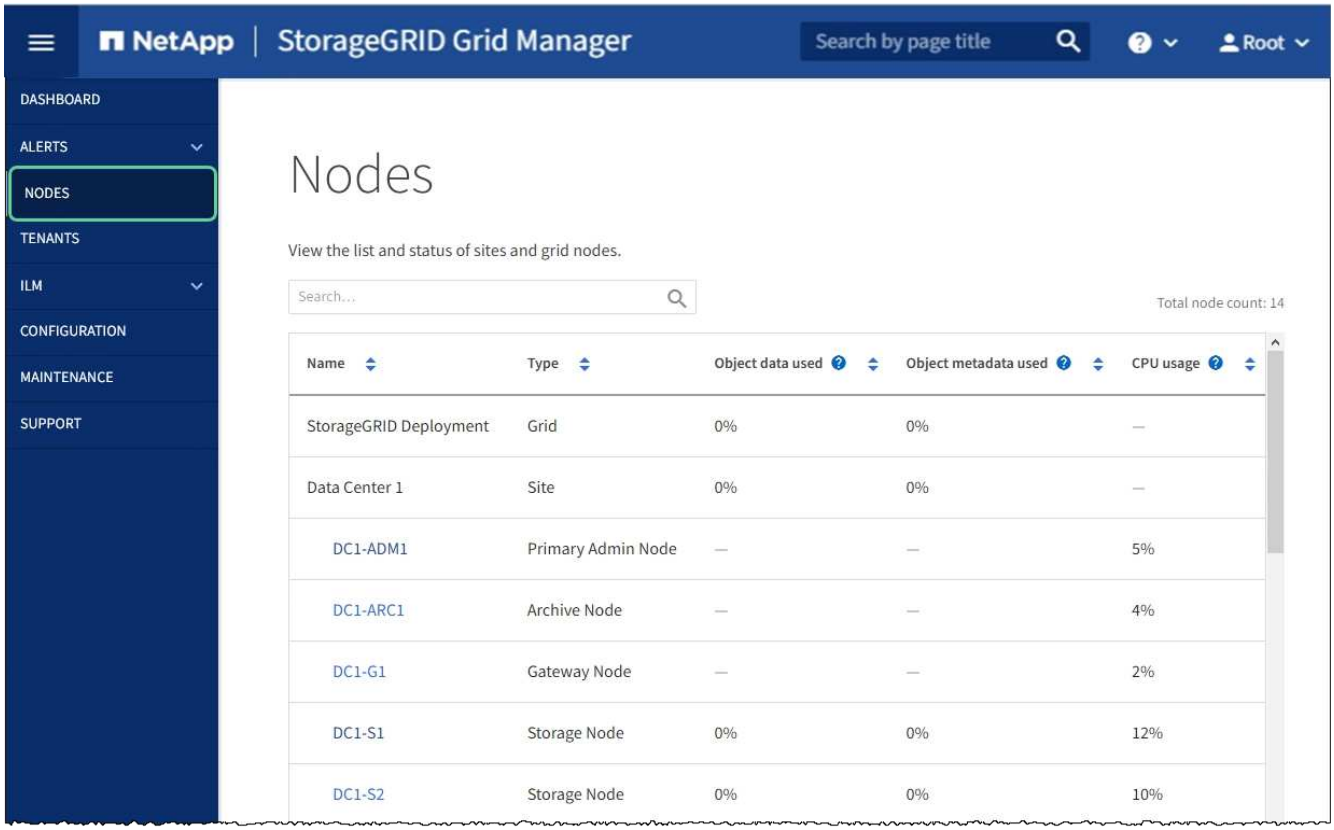
   除了您选择执行的任何其他测试之外，请确认您可以对主管理节点的网格 IP 地址以及至少一个其他存储节点的网格 IP 地址执行 ping 操作。如有必要，请更正任何链路配置问题。

6. 在您确信链路配置更改正常运行后，请重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

配置网络链路（ SG5600 ）

更改 **MTU** 设置

您可以更改在为设备节点配置 IP 地址时分配的 MTU 设置。

关于此任务

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

要在不重新启动设备节点的情况下更改 MTU 设置， 使用更改 IP 工具。

如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络， 使用维护模式更改 MTU 设置。

使用更改 **IP** 工具更改 **MTU** 设置

您需要的内容

您有 `passwords.txt` 文件可用于更改 IP 工具。

步骤

访问更改 IP 工具并按中所述更新 MTU 设置 更改节点网络配置。

使用维护模式更改 **MTU** 设置

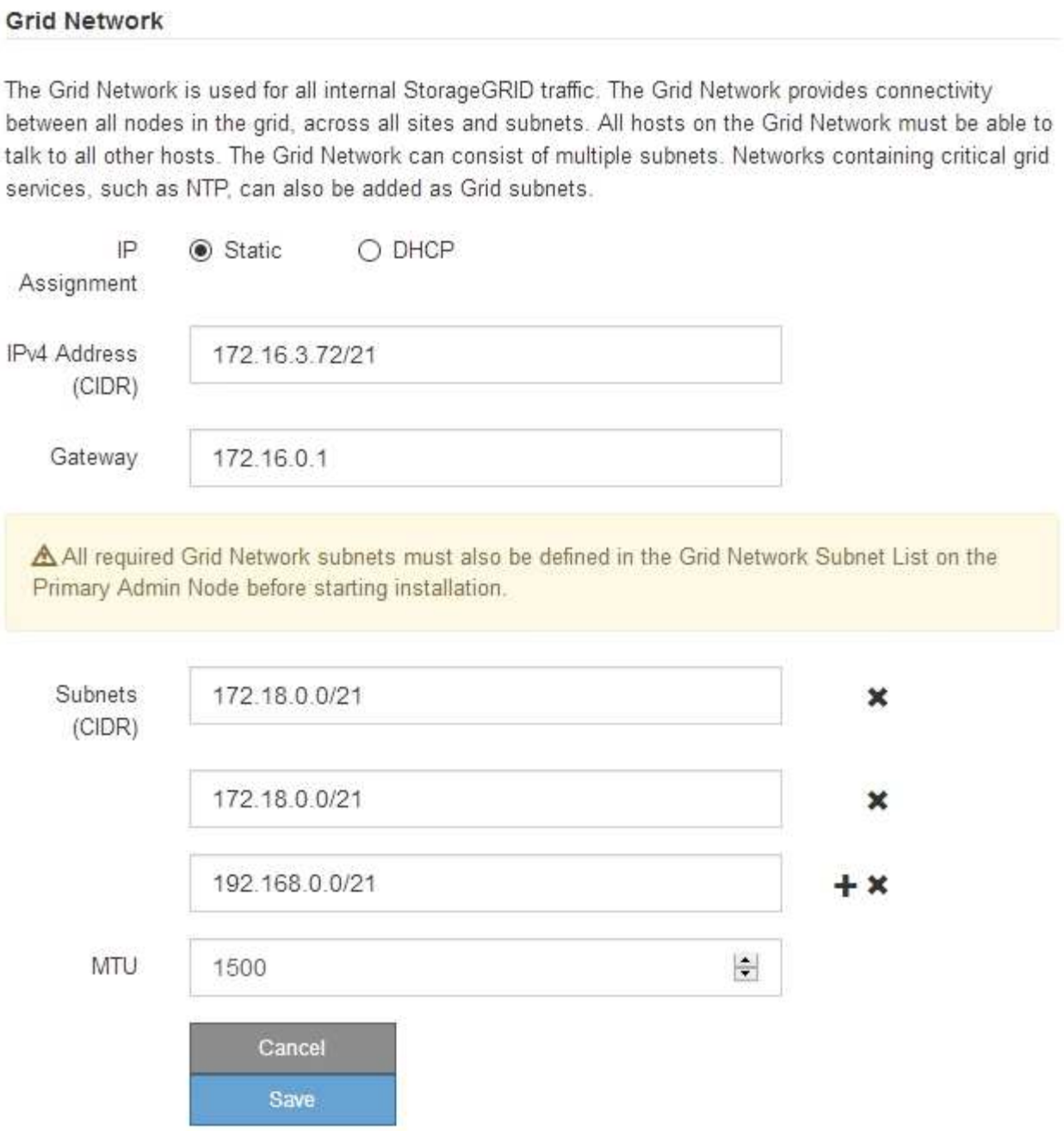
如果无法使用更改 IP 工具访问这些设置，请使用维护模式更改 MTU 设置。

您需要的内容

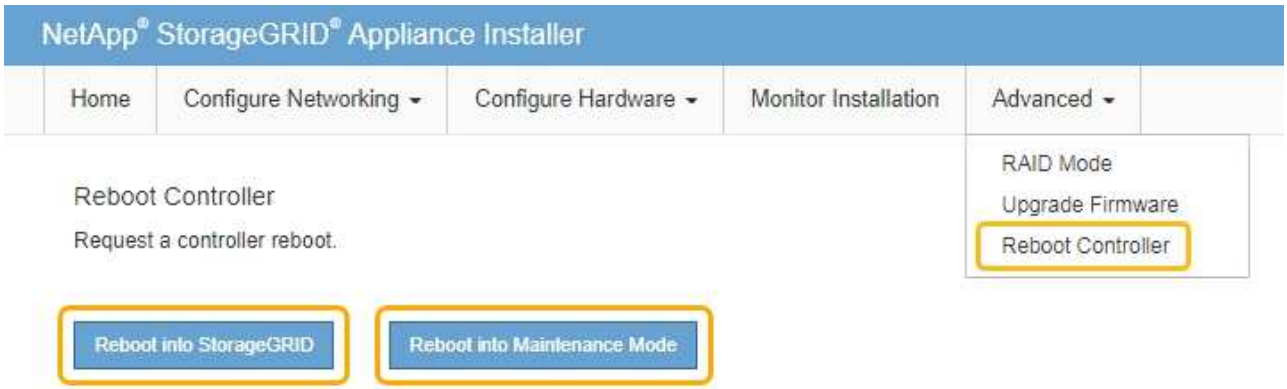
此设备已运行 已置于维护模式。

步骤

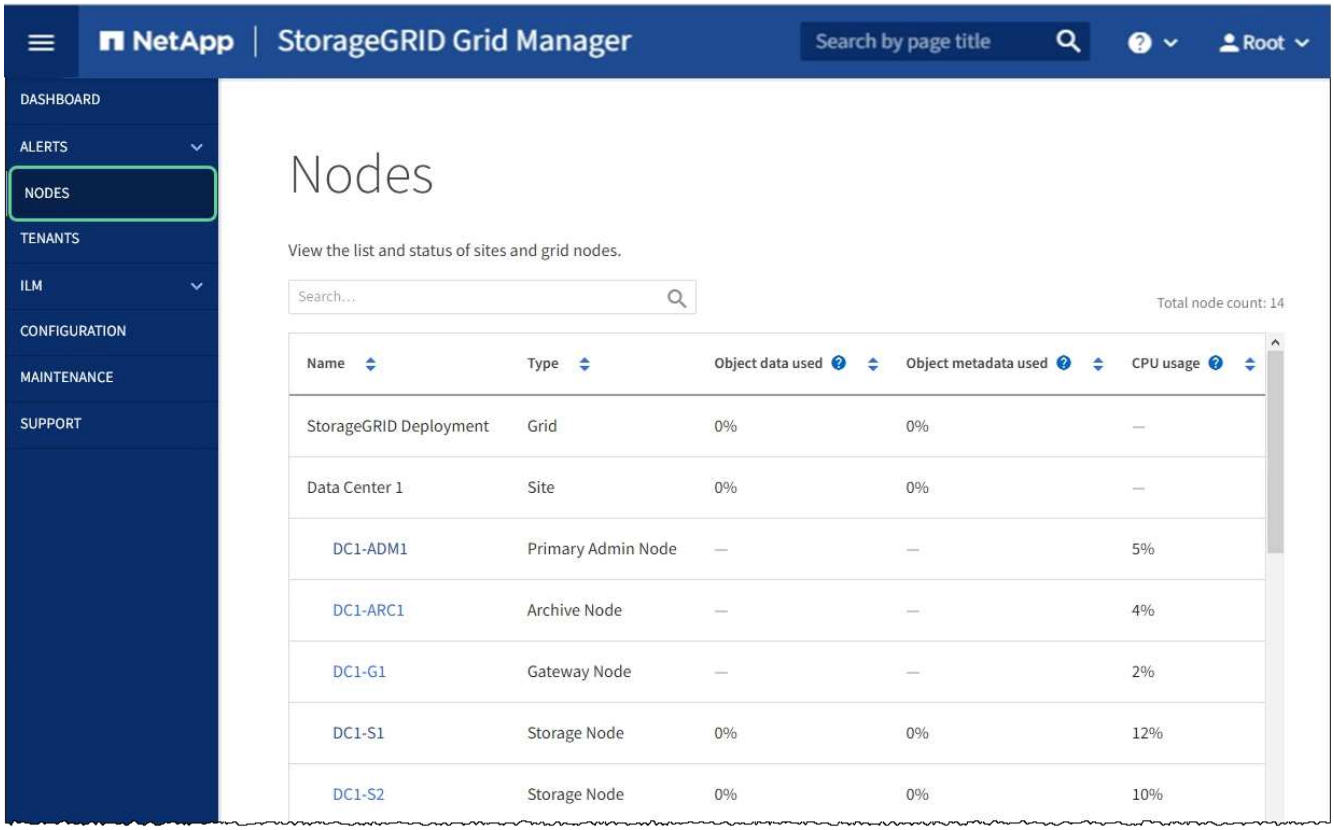
1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。
2. 对网格网络，管理网络和客户端网络的 MTU 设置进行所需的更改。



3. 如果对设置感到满意，请选择 * 保存 * 。
4. 重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：
   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

检查 **DNS** 服务器配置

您可以检查并临时更改此设备节点当前正在使用的域名系统（ DNS ）服务器。

您需要的内容

此设备已运行 已置于维护模式。

关于此任务

如果加密设备无法连接到密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群，则可能需要更改 DNS 服务器设置，因为 KMS 的主机名指定为域名，而不是 IP 地址。对设备的 DNS 设置所做的任何更改都是临时的，在退出维护模式时将丢失。要使这些更改永久生效，请在网格管理器中指定 DNS 服务器（ * 维护 * > * 网络 * > * DNS 服务器 * ）。

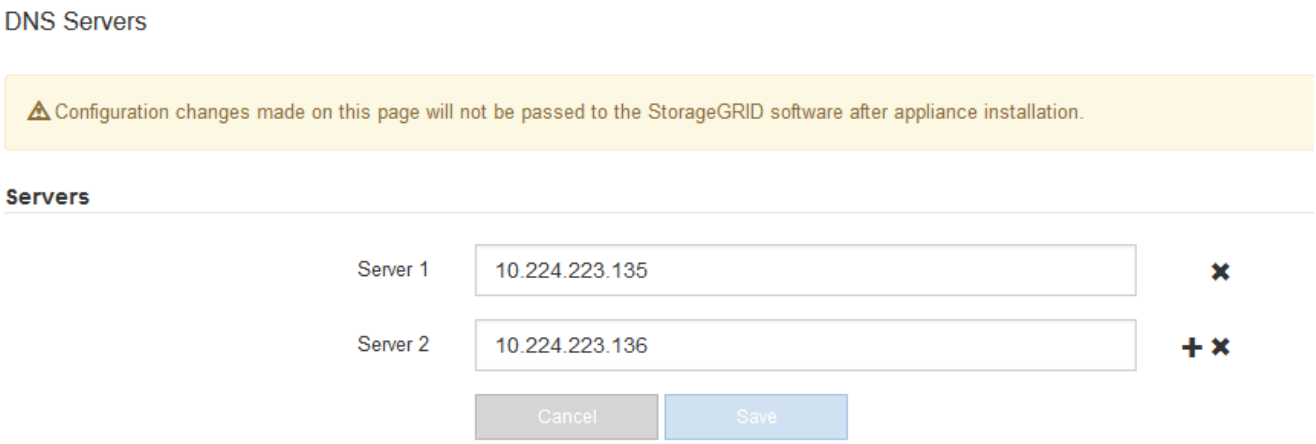
- 只有在节点加密的设备中，使用完全限定域名（而不是 IP 地址）为主机名定义 KMS 服务器时，才需要临时更改 DNS 配置。
- 当节点加密设备使用域名连接到 KMS 时，它必须连接到为网格定义的一个 DNS 服务器。然后，其中一个 DNS 服务器会将域名转换为 IP 地址。
- 如果节点无法访问网格的 DNS 服务器，或者您在节点加密设备节点脱机时更改了网格范围的 DNS 设置，则节点将无法连接到 KMS 。在解析 DNS 问题描述 之前，无法解密设备上的加密数据。

要解决 DNS 问题描述 阻止 KMS 连接的问题，请在 StorageGRID 设备安装程序中指定一个或多个 DNS 服务器的 IP 地址。通过这些临时 DNS 设置，设备可以连接到 KMS 并对节点上的数据进行解密。

例如，如果在加密节点脱机时网格的 DNS 服务器发生更改，则该节点将无法在重新联机时访问 KMS ，因为它仍在使用先前的 DNS 值。在 StorageGRID 设备安装程序中输入新的 DNS 服务器 IP 地址后，可以通过临时 KMS 连接对节点数据进行解密。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * DNS 配置 * 。
2. 验证指定的 DNS 服务器是否正确。



3. 如果需要，请更改 DNS 服务器。

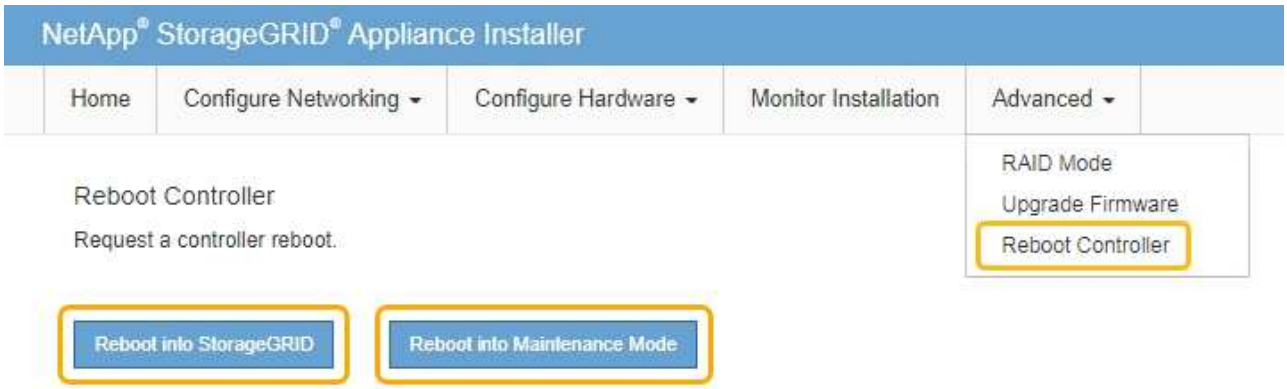
   对 DNS 设置所做的更改是临时的，当您退出维护模式时，这些更改将丢失。

4. 对临时 DNS 设置感到满意后，请选择 * 保存 * 。

   节点使用此页面上指定的 DNS 服务器设置重新连接到 KMS ，从而可以解密节点上的数据。

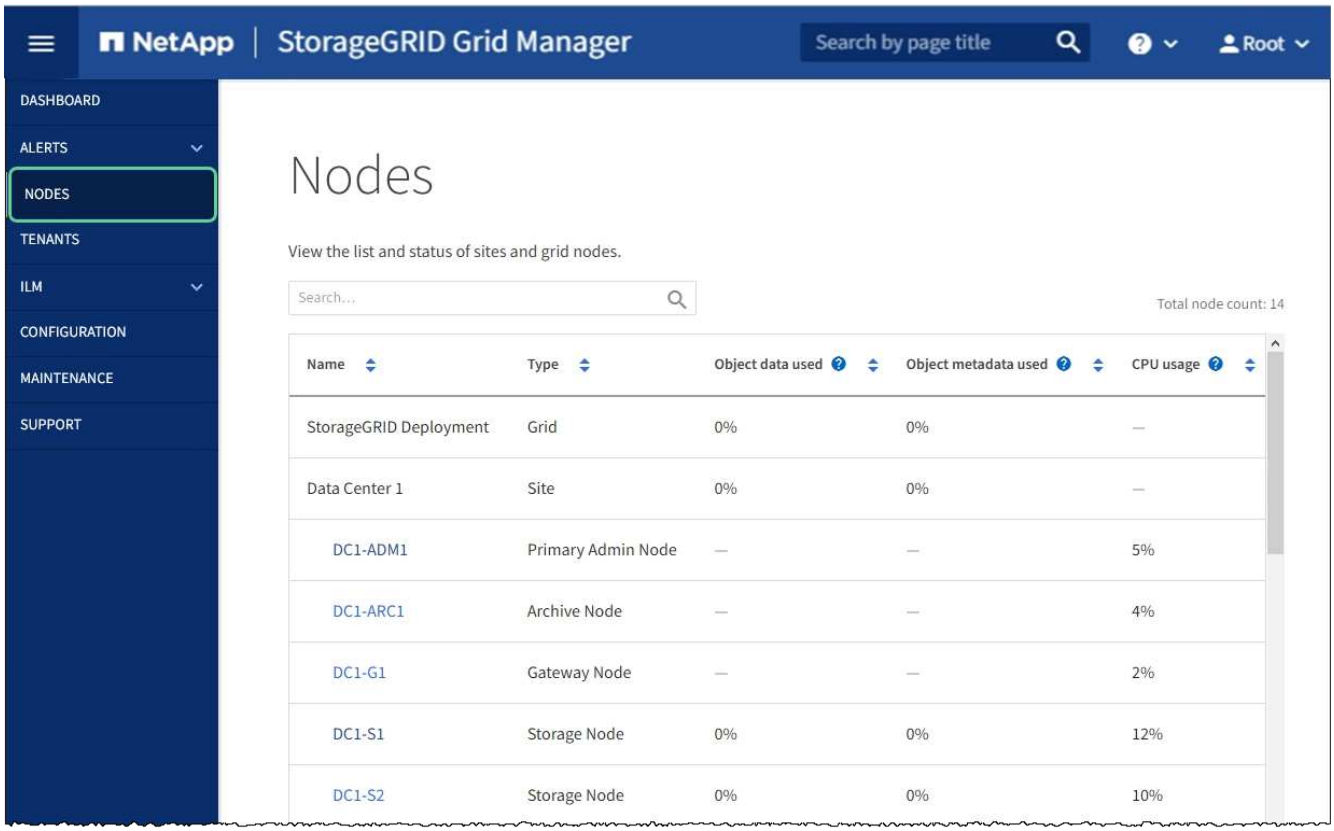
5. 解密节点数据后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：

- 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
- 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



当节点重新启动并重新加入网格时，它将使用网格管理器中列出的系统范围的 DNS 服务器。重新加入网格后，在设备处于维护模式时，设备将不再使用 StorageGRID 设备安装程序中指定的临时 DNS 服务器。

设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



在维护模式下监控节点加密（ **SG5600** ）

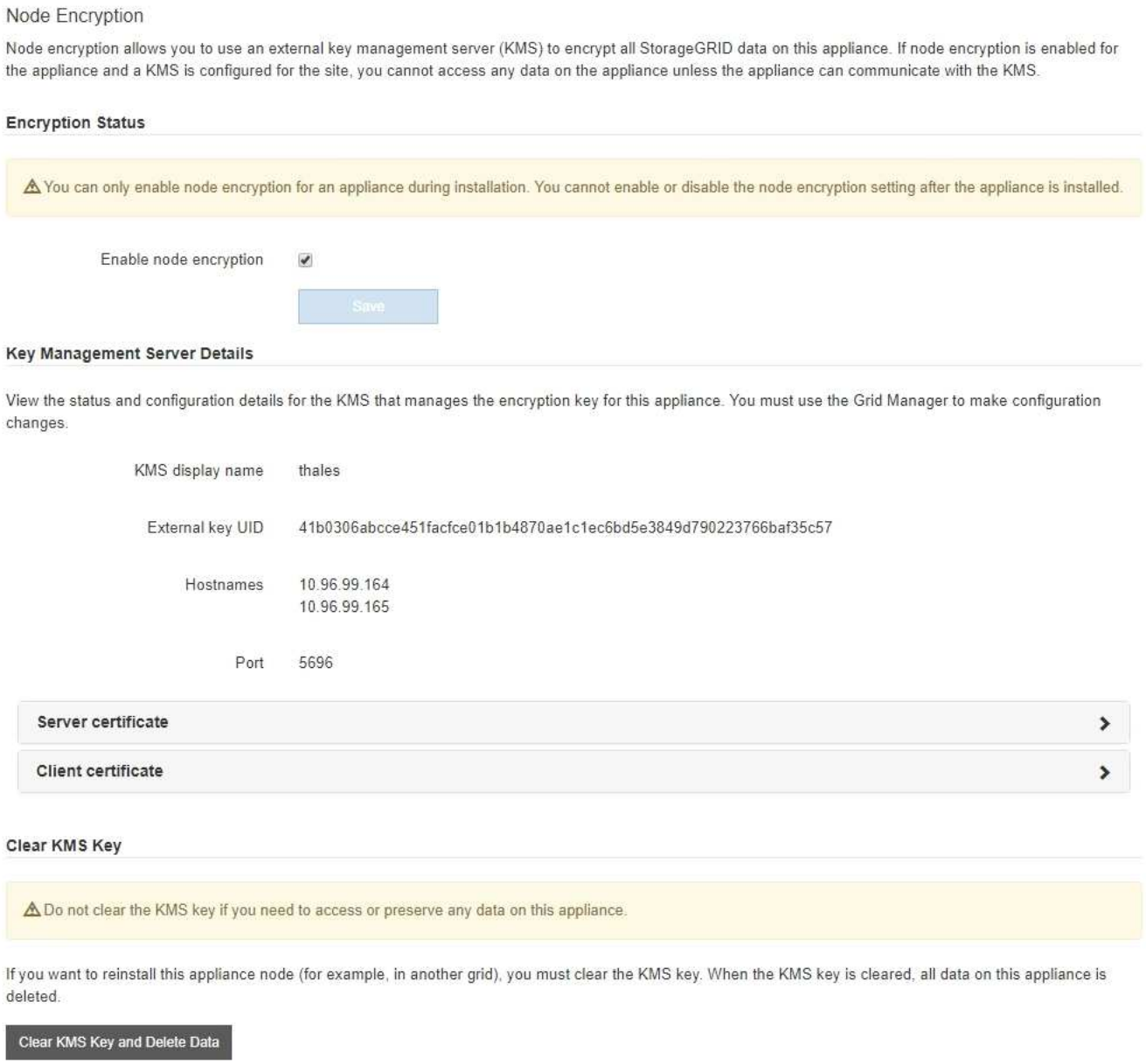
如果您在安装期间为设备启用了节点加密，则可以监控每个设备节点的节点加密状态，包括节点加密状态和密钥管理服务器（ KMS ）详细信息。

您需要的内容

- 必须在安装期间为设备启用节点加密。安装设备后，您无法启用节点加密。
- 此设备已运行 置于维护模式。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 配置硬件 * > * 节点加密 * 。



节点加密页面包括以下三个部分：

◦ " 加密状态 " 显示设备是启用还是禁用了节点加密。

- 密钥管理服务器详细信息显示了有关用于对设备进行加密的 KMS 的信息。您可以展开服务器和客户端证书部分以查看证书详细信息和状态。
  - 要解决证书本身的问题，例如续订已过期的证书，请参见管理 StorageGRID 的说明中有关 KMS 的信息。
  - 如果连接到 KMS 主机时出现意外问题，请验证域名系统（ DNS ）服务器是否正确以及设备网络连接是否配置正确。

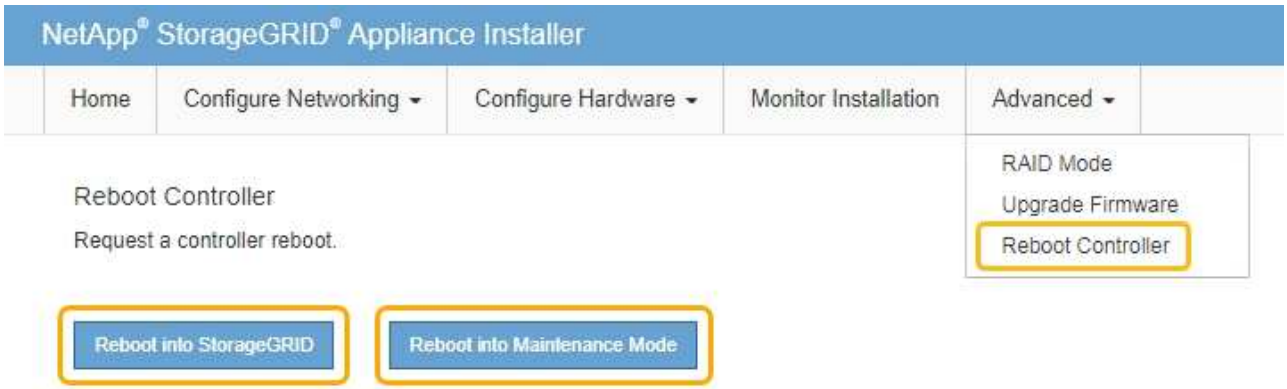
    检查 DNS 服务器配置

  - 如果无法解决证书问题，请联系技术支持。
- 清除 KMS 密钥会禁用设备的节点加密，删除设备与为 StorageGRID 站点配置的密钥管理服务器之间的关联，并删除设备中的所有数据。在将此设备安装到另一个 StorageGRID 系统之前，必须清除 KMS 密钥。

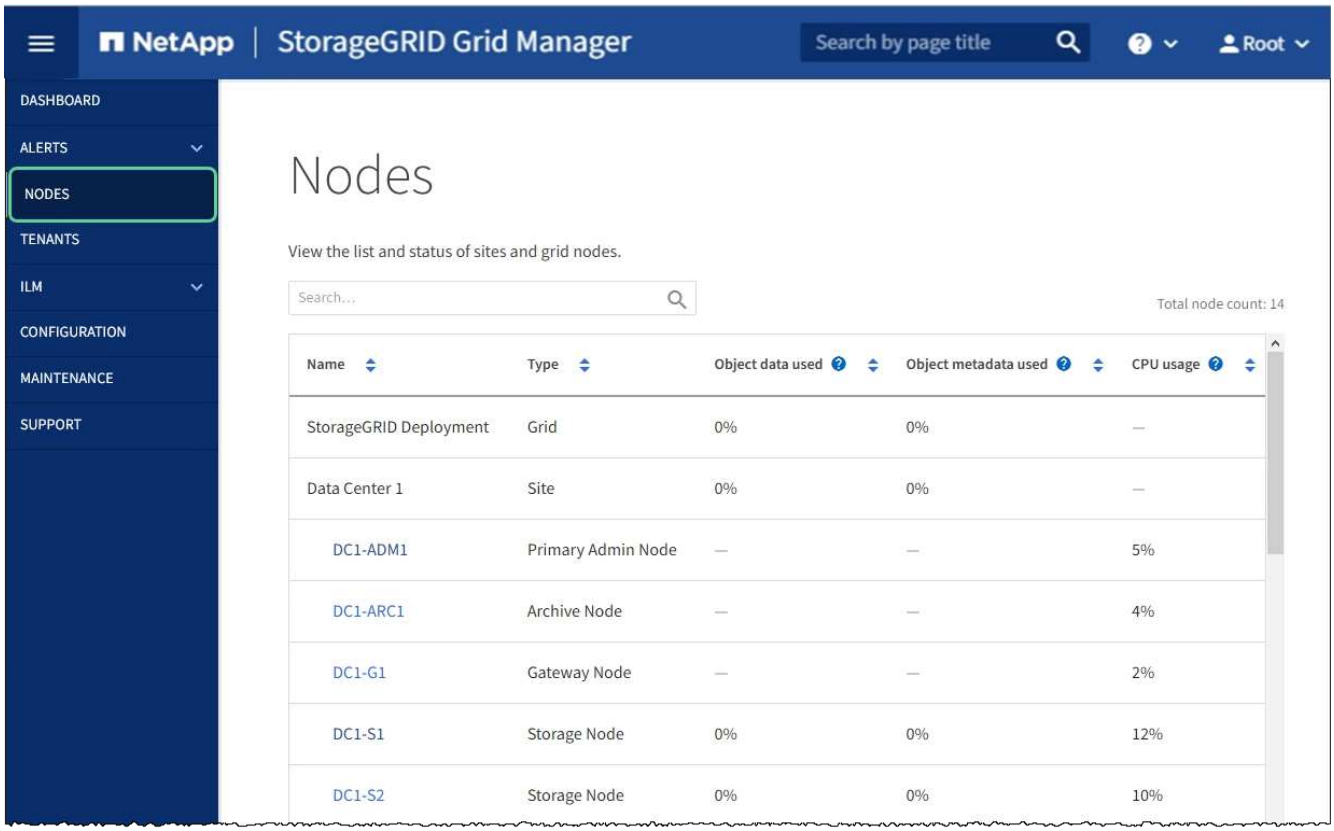
  清除密钥管理服务器配置

  清除 KMS 配置将从设备中删除数据，从而使其永远无法访问。此数据不可恢复。

2. 检查完节点加密状态后，重新启动节点。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择以下选项之一：
   - 选择 * 重新启动到 StorageGRID * 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
   - 选择 * 重新启动至维护模式 * 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。） 如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"**nodes** " 页面应显示设备节点的正常状态（无图标），表示没有处于活动状态的警报，并且节点已连接到网格。



相关信息

管理 StorageGRID

清除密钥管理服务器配置

清除密钥管理服务器（ KMS ）配置将禁用设备上的节点加密。清除 KMS 配置后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

您需要的内容

如果需要保留设备上的数据，则必须先执行节点停用操作步骤 或克隆节点，然后才能清除 KMS 配置。

清除 KMS 后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

停用节点 将其包含的任何数据移动到 StorageGRID 中的其他节点。

关于此任务

清除设备 KMS 配置将禁用节点加密，从而删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。然后，设备上的数据将被删除，并且设备将保持预安装状态。此过程不能逆转。

必须清除 KMS 配置：

- 在将设备安装到不使用 KMS 或使用其他 KMS 的其他 StorageGRID 系统之前，请先安装此设备。

如果您计划在使用相同 KMS 密钥的 StorageGRID 系统中重新安装设备节点，请勿清除 KMS 配置。

- 在恢复和重新安装 KMS 配置丢失且 KMS 密钥不可恢复的节点之前。
- 在退回您的站点上先前使用的任何设备之前。
- 停用已启用节点加密的设备后。

> 在清除 KMS 以将其数据移动到 StorageGRID 系统中的其他节点之前，请停用此设备。在停用设备之前清除 KMS 将导致数据丢失，并可能导致设备无法运行。

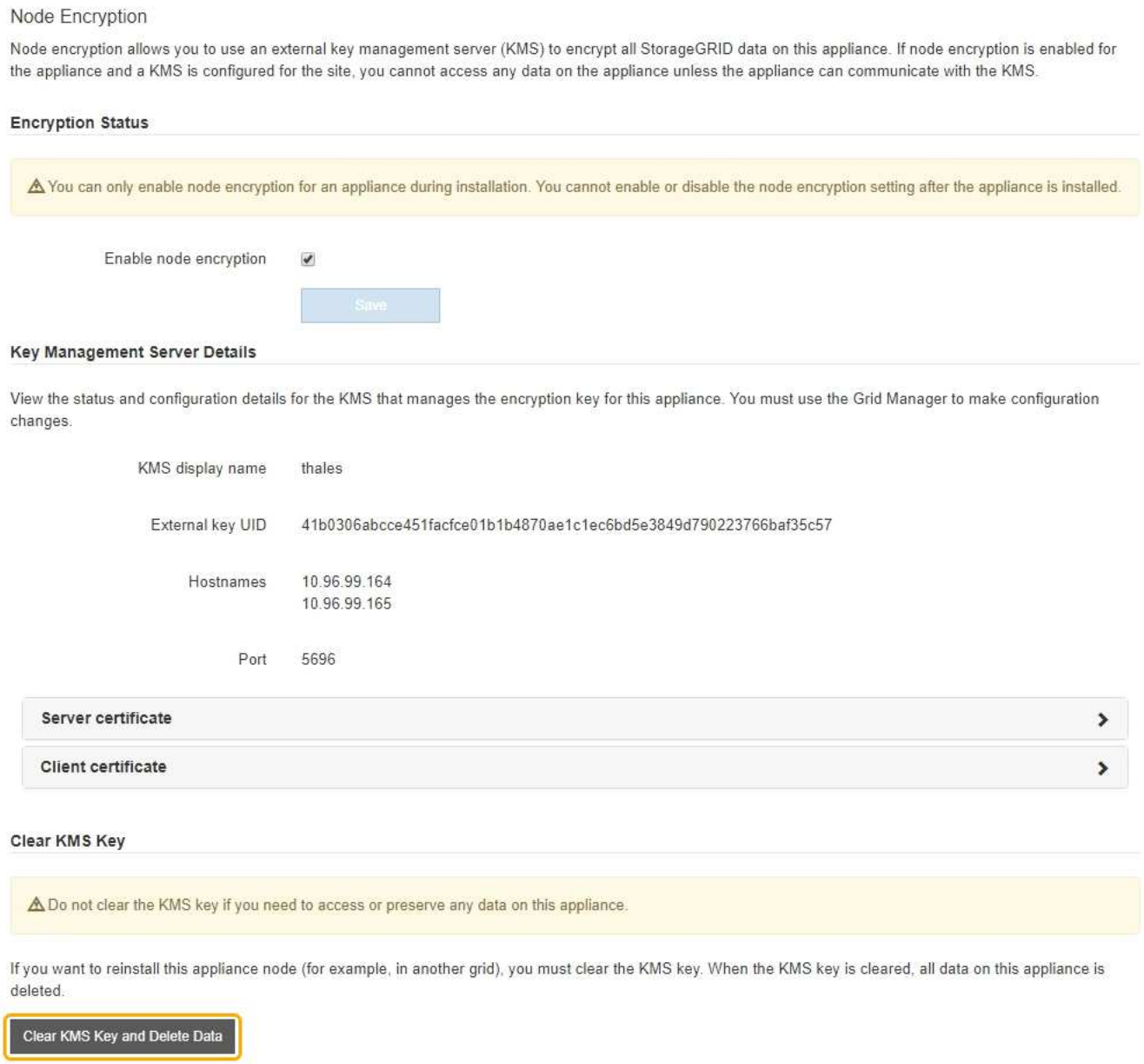
步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

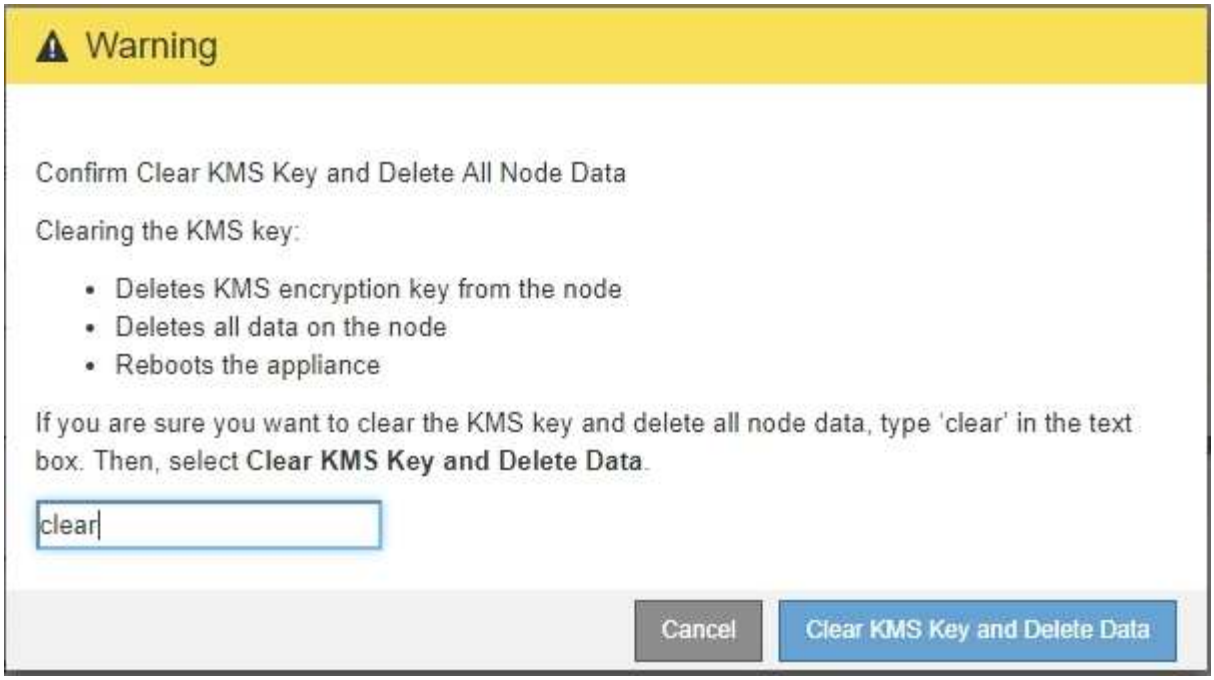
   此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 节点加密 * 。



如果清除了 KMS 配置，则设备上的数据将被永久删除。此数据不可恢复。

3. 在窗口底部，选择 * 清除 KMS 密钥和删除数据 * 。
4. 如果确实要清除 KMS 配置，请键入 + ` * clear*` + 并选择 * 清除 KMS 密钥和删除数据 * 。



KMS 加密密钥和所有数据将从节点中删除，设备将重新启动。这可能需要长达 20 分钟。

5. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。+ ` * https://*Controller_IP*:8443*`

   ` Controller_IP_` 是三个 StorageGRID 网络中任意一个网络上计算控制器（而不是存储控制器）的 IP 地址。

   此时将显示 StorageGRID 设备安装程序主页页面。

6. 选择 * 配置硬件 * > * 节点加密 * 。
7. 验证是否已禁用节点加密，以及是否已从窗口中删除 * 密钥管理服务器详细信息 * 和 * 清除 KMS 密钥和删除数据 * 控件中的密钥和证书信息。

   在将设备重新安装到网格中之前，无法在设备上重新启用节点加密。

完成后

在设备重新启动并确认 KMS 已清除且设备处于预安装状态后，您可以从 StorageGRID 系统中物理删除此设备。有关的信息，请参见恢复和维护说明 准备要重新安装的设备。

相关信息

管理 StorageGRID

安装和升级软件

升级 StorageGRID 软件

Upgrade StorageGRID software： 概述

按照以下说明将 StorageGRID 系统升级到新版本。

关于这些说明

这些说明介绍了 StorageGRID 11.6 中的新增功能，并提供了将 StorageGRID 系统中的所有节点升级到新版本的分步说明。

开始之前

查看这些主题，了解 StorageGRID 11.6 中的新增功能和增强功能，确定是否已弃用或删除任何功能，并了解对 StorageGRID API 所做的更改。

- StorageGRID 11.6.
- 已删除或已弃用的功能
- 对网格管理 API 进行的更改
- 对租户管理 API 进行的更改

StorageGRID 11.6.

此版本的 StorageGRID 引入了以下功能。

可用性增强功能

网格管理器用户界面经过大幅重新设计，可改善用户体验。

- 新的边栏取代了旧用户界面中的下拉菜单。
- 我们对多个菜单进行了重新组织，以便将相关选项放在一起。例如， * 配置 * 菜单包含一个新的 * 安全性 * 部分，用于 " 证书 " ， " 密钥管理服务器 " ， " 代理 " 设置和 " 不可信客户端网络 " 选项。
- 标题栏中的 * 搜索 * 字段可用于快速导航到网格管理器页面。
- "* 节点 * " 页面上的摘要表提供了所有站点和节点的详细信息，例如使用的对象数据和使用的对象元数据，并包含一个新的搜索字段。警报图标会显示在任何具有活动警报的节点旁边。
- 新向导将引导您完成更复杂的配置，例如管理组，管理员用户，租户，负载平衡器端点和高可用性（ HA ）组的工作流。
- 所有 UI 页面都会重新显示更新后的字体，按钮样式和表格式。

> 除非功能发生更改，否则 StorageGRID 11.6 文档站点中的屏幕截图不会进行更新，以反映新的网格管理器页面样式。

请参见以下内容：

- 管理 StorageGRID
- 监控和故障排除

多个 **VLAN** 接口

现在，您可以为管理节点和网关节点创建虚拟 LAN （ VLAN ）接口。您可以使用 HA 组和负载平衡器端点中的 VLAN 接口隔离客户端流量并对其进行分区，以提高安全性，灵活性和性能。

- 新的 * 创建 VLAN 接口 * 向导将指导您完成输入 VLAN ID 以及在一个或多个节点上选择父接口的过程。父接口可以是网格网络，客户端网络，也可以是 VM 或裸机主机的附加中继接口。请参见 配置 VLAN 接口。
- 现在，您可以向节点添加额外的中继或访问接口。如果添加中继接口，则必须配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。请参见以下内容：
  - * Linux （安装节点之前） * ： [安装增强功能]
  - * Linux （安装节点后） * ： Linux ： 向节点添加中继或访问接口
  - * VMware （安装节点后） * ： 收集有关部署环境的信息

可以使用 **Azure AD** 进行身份联合

现在，在为网格管理器或租户管理器配置身份联合时，您可以选择 Azure Active Directory （ Azure AD ）作为身份源。请参见 使用身份联合。

可以使用 **Azure AD** 和 **PingFederate** 进行 **SSO**

现在，在为网格配置单点登录（ SSO ）时，您可以选择 Azure AD 或 PingFederate 作为 SSO 类型。然后，您可以使用沙盒模式配置和测试 Azure AD 企业应用程序或 PingFederate 服务提供商（ SP ）与每个 StorageGRID 管理节点的连接。请参见 配置单点登录。

集中式证书管理

- 新的 " 证书 " 页面（ * 配置 * > * 安全性 * > * 证书 * ）将有关所有 StorageGRID 安全证书的信息整合到一个位置。您可以从新页面管理 StorageGRID 全局证书，网格 CA 证书和客户端证书，也可以查看有关其他证书的信息，例如用于负载平衡器端点，租户和身份联合的证书。请参见 关于安全证书。
- 在此更改中，以下全局证书已重命名：
  - 现在， * 管理接口服务器证书 * 是 * 管理接口证书 * 。
  - 对象存储 API 服务端点服务器证书 * （也称为存储 API 服务器证书）现在是 * S3 和 Swift API 证书 * 。
  - 现在， * 内部 CA 证书 * ， * 系统 CA 证书 * ， * CA 证书 * 和 * 默认 CA 证书 * 始终称为 * 网格 CA 证书 * 。

其他 **Grid Manager** 增强功能

- * 更新高可用性（ HA ）组 * 。现在，向导将指导您完成创建 HA 组的过程。请参见 配置高可用性组。
  - 除了选择网格网络（ eth0 ）或客户端网络（ eth2 ）上的接口之外，现在您还可以选择 VLAN 接口或已添加到节点的任何访问接口。
  - 现在，您可以为接口指定优先级顺序。您可以选择主接口并按顺序对每个备份接口进行排名。

- 如果任何 S3 ， Swift ，管理或租户客户端要从其他子网访问 HA 组的 VIP 地址，您现在可以为此网关提供 IP 地址。

- * 更新负载平衡器端点 * 。新向导将指导您完成创建负载平衡器端点的过程。请参见 配置负载平衡器端点。
  - 现在，您可以在首次创建端点时选择客户端类型（ S3 或 Swift ），而不是在创建端点后添加此详细信息。
  - 现在，您可以对负载平衡器端点使用全局 * StorageGRID S3 和 Swift 证书 * ，而不是上传或生成单独的证书。

> 此全局证书以前用于连接到已弃用的 CLB 服务和存储节点。如果要对负载平衡器端点使用全局证书，则必须在 S3 和 Swift API 证书页面上上传自定义证书。

新增租户管理器功能

- * 全新的试验性 S3 控制台 * 。新的试验性 S3 控制台可通过租户管理器中的 " 分段 " 页面提供的链接来使 S3 租户用户查看和管理其分段中的对象。请参见 使用试验性 S3 控制台。

> 试验性 S3 控制台尚未经过全面测试，不适用于对象批量管理或生产环境。只有在为少数对象执行功能时，或者在使用概念验证网格或非生产网格时，租户才应使用 S3 控制台。

- * 可以删除多个 S3 存储分段 * 。租户用户现在可以一次删除多个 S3 存储分段。要删除的每个存储分段必须为空。请参见 删除 S3 存储分段。
- * 更新租户帐户权限 * 。现在，属于具有租户帐户权限的组的管理员用户可以查看现有流量分类策略。以前，用户必须具有 root 访问权限才能查看这些指标。

新的升级和修复过程

- 重新设计了 * StorageGRID Upgrade* 页面（ * 维护 * > * 系统 * > * 软件更新 * > * StorageGRID upgrade* ）。
- 升级到 StorageGRID 11.6 后，您可以使用网格管理器升级到未来版本，并同时应用该版本的修补程序。StorageGRID 升级页面将显示建议的升级路径，并直接链接到正确的下载页面。
- 通过 AutoSupport 页面（ * 支持 * > * 工具 * > * AutoSupport * ）上的一个新 * 检查软件更新 * 复选框，您可以控制此功能。如果您的系统无法访问 WAN ，则可以禁用对可用软件更新的检查。请参见 配置 AutoSupport 并禁用软件更新检查。

> 要升级到 StorageGRID 11.6 ，您可以选择使用脚本同时升级和应用修补程序。请参见 "NetApp 知识库：如何为 StorageGRID 运行组合式主要升级和修补程序脚本"。

- 现在，如果需要稍后完成升级，您可以暂停 SANtricity 操作系统升级并跳过升级某些节点。请参见适用于您的存储设备的说明：
  - 使用网格管理器升级存储控制器上的 SANtricity 操作系统（ SG5600 ）
  - 使用网格管理器升级存储控制器上的 SANtricity 操作系统（ SG5700 ）
  - 使用网格管理器升级存储控制器上的 SANtricity 操作系统（ SG6000 ）

外部系统日志服务器支持

- 现在，如果要远程保存和管理审核消息以及部分 StorageGRID 日志（ * 配置 * > * 监控 * > * 审核和系统日

志服务器 * ），则可以配置外部系统日志服务器。配置外部系统日志服务器后，您可以在本地，远程或同时保存审核消息和某些日志文件。通过配置审核信息的目标，您可以减少管理节点上的网络流量。请参见 配置审核消息和日志目标。

- 与此功能相关的是，日志页面（ * 支持 * > * 工具 * > * 日志 * ）上的新复选框可用于指定要收集的日志类型，例如某些应用程序日志，审核日志，用于网络调试的日志以及 Prometheus 数据库日志。请参见 收集日志文件和系统数据。

S3 Select

现在，您可以选择允许 S3 租户对单个对象发出问题描述 SelectObjectContent 请求。S3 Select 可以高效地搜索大量数据，而无需部署数据库和相关资源即可启用搜索。它还可以降低检索数据的成本和延迟。请参见 管理租户帐户的 S3 Select 和 使用 S3 Select。

此外，还为 S3 Select 操作添加了 Grafana 图表。请参见 查看支持指标。

S3 对象锁定默认存储分段保留期限

现在，在使用 S3 对象锁定时，您可以为存储分段指定默认保留期限。默认保留期限适用场景 添加到存储分段中但没有自己保留设置的任何对象。请参见 使用 S3 对象锁定。

Google Cloud Platform 支持

现在，您可以使用 Google Cloud Platform （ GCP ）作为云存储池和 CloudMirror 平台服务的端点。请参见 指定平台服务端点的 URN 和 创建云存储池。

AWS C2S 支持

现在，您可以使用 AWS Commercial Cloud Services （ C2S ）端点进行 CloudMirror 复制。请参见 创建平台服务端点。

其他 **S3** 更改

- * 获取多部分对象的对象和头对象支持 * 。以前， StorageGRID 在 GET 对象或 HEAD 对象请求中不支持 `partnumber` request 参数。现在，您可以通过问题描述 GET 和 HEAD 请求检索多部件对象的特定部分。GET 和 HEAD 对象还支持 `x-AMZ-MP-parts-count` 响应元素，以指示对象包含的部件数。
- * 对 " 可用 " 一致性控制的更改 * 。现在， " 可用 " 一致性控制与 " 读后写 " 一致性级别相同，但可为 head 和 get 操作提供最终一致性。如果存储节点不可用，则 " 可用 " 一致性控制可以为 head 和 get 操作提供比 " 读后写入 " 更高的可用性。与 Amazon S3 对机头和 GET 操作的一致性保证不同。

  使用 S3

性能增强

- * 存储节点可支持 20 亿个对象 * 。存储节点上的底层目录结构经过优化，可提高可扩展性和性能。现在，存储节点可以使用额外的子目录来存储多达 20 亿个复制对象，并最大限度地提高性能。升级到 StorageGRID 11.6 时，节点子目录会进行修改，但现有对象不会重新分布到新目录中。
- * 对于高性能设备， ILM 驱动的删除性能提高 * 。现在，用于执行 ILM 删除操作的资源和吞吐量可根据每个 StorageGRID 设备节点的大小和功能进行调整。对于 SG5600 设备，吞吐量与 StorageGRID 11.5 相同。对于 SG5700 设备， ILM 删除性能略有提高。对于 RAM 较多且 CPU 较多的 SG6000 设备，现在处理 ILM 删除的速度更快。这些改进在全闪存 SGF6024 设备上尤为明显。

- * 存储卷水印已优化 * 。在先前版本中，三个存储卷水印的设置会应用于每个存储节点上的每个存储卷。现在， StorageGRID 可以根据存储节点的大小和卷的相对容量为每个存储卷优化这些水印。请参见 什么是存储卷水印。

  优化的水印会自动应用于所有新的和升级最广泛的 StorageGRID 11.6 系统。优化的水印将大于先前的默认设置。

  如果使用自定义水印，则升级后可能会触发 * 低只读水印覆盖 * 警报。通过此警报，您可以了解自定义水印设置是否太小。请参见 对低只读水印覆盖警报进行故障排除。

  在此更改中，添加了两个 Prometheus 指标：

  - `storagegRid_storage_volume_minimum_optimized_soft_readonly_slogm`
  - `storagegRid_storage_volume_max_optimized_soft_readonly_slogm`

- * 允许的最大元数据空间增加 * 。对于容量较高的节点，存储节点允许的最大元数据空间已增加到 3.96 TB （从 2.64 TB 增加到 3.96 TB ），这些节点是指实际为元数据预留的空间超过 4 TB 的节点。此新值允许在某些存储节点上存储更多对象元数据，并可将 StorageGRID 元数据容量最多增加 50% 。

  > 如果您尚未执行此操作，并且存储节点在卷 0 上具有足够的 RAM 和空间，则可以执行此操作 安装或升级后，手动将元数据预留空间设置提高到 8 TB。

  - 管理对象元数据存储和允许的元数据空间
  - 增加元数据预留空间设置

维护过程和支持工具的增强功能

- * 可以更改节点控制台密码 * 。现在，您可以使用网格管理器更改节点控制台密码（ * 配置 * > * 访问控制 * > * 网格密码 * ）。这些密码用于通过 SSH 以 "admin" 身份登录到节点，或者通过 VM/ 物理控制台连接登录到 root 用户。请参见 更改节点控制台密码。
- * 新建对象存在检查向导 * 。现在，您可以使用易于使用的对象存在检查向导（ * 维护 * > * 任务 * > * 对象存在检查 * ）来验证对象完整性，该向导将取代前台验证操作步骤 。新的操作步骤 所需时间不超过完成时间的三分之一，并且可以同时验证多个节点。请参见 验证对象完整性。
- "EC 重新平衡和 EC 修复作业的估计完成时间 " 图表 * 。现在，您可以查看当前 EC 重新平衡或 EC 修复作业的估计完成时间和完成百分比。
- * 复制数据修复的估计完成百分比 * 。现在，您可以将 `show -repliced-repair-status` 选项添加到 `repair-data` 命令中，以查看复制修复的估计完成百分比。

  > 在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请按照恢复过程中所述，继续使用 * 等待 - 全部 * ， * 尝试修复（ XRPA ）和 * 扫描期限 - 估计（ XSCM ） * 。

- 诊断页面（ * 支持 * > * 工具 * > * 诊断 * ）上的结果现在按严重性排序，然后按字母顺序排序。
- Prometheus 和 Grafana 已更新为更新版本，并修改了界面和图表。在此更改过程中，某些指标中的标签也发生了更改。
  - 如果您的自定义查询使用了 `node_network_up` 中的标签，则现在应改用 `node_network_info` 中的标签。

- 如果您还使用了 `node_network` 指标中的标签名称 `interface` ，则现在应改用 `device` 标签。

- 以前， Prometheus 指标存储在管理节点上 31 天。现在，指标会一直存储到为 Prometheus 数据预留的空间已满为止，这会显著延长历史指标的可用时间。

  当 ` /var/local/mysql_ibdata/` 卷达到容量时，首先删除最旧的指标。

安装增强功能

- 现在，您可以在安装 Red Hat Enterprise Linux 期间选择使用 Podman 作为容器。以前， StorageGRID 仅支持 Docker 容器。
- 现在， RedHat Enterprise Linux/CentOS ， Ubuntu 或 Debian 和 VMware 平台的安装归档中包含了适用于 StorageGRID 的 API 架构。提取归档后，您可以在 ` /ExtrS/API-schemas` 文件夹中找到这些模式。
- 对于裸机部署，节点配置文件中的 `block_device_RANGEDB` 密钥现在应包含三位数，而不是两位数。也就是说，您应指定 `block_device_RANGEDB_nn` ，而不是 `block_device_RANGEDB_nnn` 。

  为了与现有部署兼容，升级后的节点仍支持两位数的密钥。

- 您可以选择将新的 `interfaces_target_nnnn` 密钥的一个或多个实例添加到节点配置文件中，以进行裸机部署。每个密钥都提供裸机主机上物理接口的名称和问题描述 ，此名称和将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。
  - 为 Red Hat Enterprise Linux 或 CentOS 部署创建节点配置文件
  - 为 Ubuntu 或 Debian 部署创建节点配置文件

新警报

为 StorageGRID 11.6 添加了以下新警报：

- 正在将审核日志添加到内存队列中
- Cassandra 表损坏
- EC 重新平衡失败
- EC 修复失败
- EC 修复已停止
- S3 和 Swift API 的全局服务器证书到期
- 外部系统日志 CA 证书到期
- 外部系统日志客户端证书到期
- 外部系统日志服务器证书到期
- 外部系统日志服务器转发错误
- 租户的身份联合同步失败
- 检测到原有 CLB 负载平衡器活动
- 正在将日志添加到磁盘队列中
- 低只读水印覆盖
- tmp 目录可用空间不足

- 对象存在检查失败
- 对象存在检查已停止
- S3 PUT 对象大小太大

请参见 警报参考。

审核消息的更改

- 已向 ORLM ： 对象规则已满足审核消息添加一个新的 * BUID* 字段。"BUID* 字段显示用于内部操作的存储分段 ID 。只有当消息状态为 PRGD 时，才会显示新字段。
- 在以下审核消息中添加了一个新的 * SGRP* 字段。只有在删除对象的站点与插入对象的站点不同时， * SGRP* 字段才会显示。
  - idel ： ILM 已启动删除
  - OVWR ： 对象覆盖
  - SDEL ： S3 delete
  - WDEL ： Swift delete

请参见 查看审核日志。

StorageGRID 文档更改

StorageGRID 11.6 文档站点的外观已经过修改，现在使用 GitHub 作为底层平台。

NetApp 非常感谢对内容的反馈，并鼓励用户利用产品文档每页上提供的新的 " 请求文档更改 " 功能。文档平台还为 GitHub 用户提供嵌入式内容贡献功能。

请查看此文档并为其提供帮助。您可以编辑，请求更改或仅发送反馈。

已删除或已弃用的功能

此版本已删除或弃用某些功能。查看这些项目，了解在升级之前是需要更新客户端应用程序还是修改配置。

已弃用警报系统和基于警报的 **API**

自 StorageGRID 11.6 版起，原有警报系统已弃用。旧警报系统的用户界面和 API 将在未来版本中删除。

> 如果您仍在使用传统警报，请计划在升级到 StorageGRID 11.6 后完全过渡到警报系统。请参见 管理警报和警报：概述 了解有关警报的更多信息。

11.6 版本会弃用所有基于警报的 API 。以下 API 受此更改影响：

- `GET /grid/alarms` ： 完全弃用
- `GET /grid/health/topology` ： 完全弃用
- `get /grid/health` ： 响应的 `alarm-counts` 部分已弃用

未来版本不支持 **PUT** 对象的最大对象大小为 **5 TiB**

在未来的 StorageGRID 版本中，一个 PUT 对象操作的最大大小将为 5 GiB ，而不是 5 TiB 。您可以对大于 5 GiB 的对象使用多部分上传，最大上传量为 5 TiB （ 5 ， 497 ， 556 ， 138 ， 880 字节）。

为了帮助您将客户端过渡到在 PUT 对象中使用较小的对象大小，如果 S3 客户端尝试上传超过 5 GiB 的对象，则在 StorageGRID 11.6 中将触发 * S3 PUT 对象大小过大 * 警报。

NAS 网桥功能已弃用

NAS 网桥功能先前在 StorageGRID 11.4 版中进入了有限访问权限。NAS 网桥功能仍受限访问，自 StorageGRID 11.6 之日已弃用。

NAS 网桥 11.4 仍为最终版本，并将继续与 StorageGRID 11.6 兼容。查看 "NetApp 互操作性表工具" 确保 NAS 网桥 11.4 和 StorageGRID 版本之间的持续兼容性。

查看 NetApp 支持站点上的 "NAS 网桥的支持计划"。

对网格管理 **API** 进行的更改

StorageGRID 11.6 使用网格管理 API 版本 3 。版本 3 已弃用版本 2 ；但版本 1 和版本 2 仍受支持。

> 您可以继续在 StorageGRID 11.6 中使用管理 API 版本 1 和版本 2 ；但是，在未来版本的 StorageGRID 中，对这些版本的 API 的支持将被删除。升级到 StorageGRID 11.6 后，可以使用 `put /grid/config/management` API 停用已弃用的 v1 和 v2 API 。

要了解更多信息，请访问 使用网格管理 API。

可以访问 **Swagger** 文档以执行专用 **API** 操作

现在，您可以从网格管理器访问专用 API 的 Swagger 文档。要查看可用操作，请选择 Grid Manager 帮助图标并选择 * API Documentation" 。然后，从 StorageGRID 管理 API 页面中选择 * 转至专用 API 文档 * 。

StorageGRID 专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

已弃用基于警报的 **API**

11.6 版本会弃用所有基于警报的 API 。以下 API 受此更改影响：

- `GET /grid/alarms` ： 完全弃用
- `GET /grid/health/topology` ： 完全弃用
- `get /grid/health` ： 响应的 `alarm-counts` 部分已弃用

可以导入 **S3** 访问密钥

现在，您可以使用网格管理 API 为租户用户导入 S3 访问密钥。例如，您可以将访问密钥从另一个 S3 提供程序迁移到 StorageGRID ，或者使用此功能在网格之间保持用户凭据相同。

启用此功能后，任何具有更改租户 root 密码权限的 Grid Manager 用户都可以完全访问租户数据。使用此功能后，请立即禁用此功能以保护租户数据。

新帐户操作

添加了三个新的 网格 / 帐户 API 操作：

- post /m ü s/account-enable-s3-key-import grid：此请求将启用导入 S3 凭据功能。要启用此功能，您必须具有 root 访问权限。
- post / grid / accounts / { id } / users / { user_id } /s3-access-keys：此请求将为租户帐户中的给定用户导入 S3 凭据。您必须具有 root 访问权限或更改租户 root 密码权限，并且必须知道用户 ID 和租户帐户 ID 。
- post /m ü s/account-disable-s3-key-import grid：此请求会禁用导入 S3 凭据功能。要禁用此功能，您必须具有 root 访问权限。

已弃用修补方法

此修补程序方法现已弃用，并将在未来版本中删除。根据需要，执行 PUT 操作以替换资源，而不是使用修补程序操作来修改资源。

添加到 grid/logs/collect 端点

已向 grid/logs/Collect 端点添加四个布尔值：

- applicationLogs：技术支持最常用于故障排除的应用程序特定日志。收集的日志是可用应用程序日志的一部分。默认值为 true 。
- auditLogs：包含在正常系统操作期间生成的审核消息的日志。默认值为 true 。
- network跟踪：用于网络调试的日志。默认值为 false 。
- prometheusDatabase：所有节点上的服务的时间序列指标。默认值为 false 。

新增 node-details /grid/service-ids 端点

新的 或 grid /service-IDs 端点可将节点 UUID 映射到关联节点名称，服务 ID 和服务类型。

可以检索网格节点控制台密码

现在，您可以使用 POST /node-console 密码 grid 来检索网格节点及其关联控制台密码的列表。

对租户管理 API 进行的更改

StorageGRID 11.6 使用租户管理 API 版本 3 。版本 3 已弃用版本 2 ；但版本 1 和版本 2 仍受支持。

您可以继续在 StorageGRID 11.6 中使用管理 API 版本 1 和版本 2 ；但是，在未来版本的 StorageGRID 中，对这些版本的 API 的支持将被删除。升级到 StorageGRID 11.6 后，可以使用 put /grid/config/management API 停用已弃用的 v1 和 v2 API 。

要了解更多信息，请访问 了解租户管理 API。

已弃用修补方法

此修补程序方法现已弃用，并将在未来版本中删除。根据需要，执行 PUT 操作以替换资源，而不是使用修补程序操作来修改资源。

规划和准备升级

估计完成升级所需的时间

在计划升级到 StorageGRID 11.6 时，您必须根据升级可能需要的时间考虑何时进行升级。此外，您还必须了解在升级的每个阶段可以执行哪些操作，哪些操作不能执行。

关于此任务

完成 StorageGRID 升级所需的时间取决于多种因素，例如客户端负载和硬件性能。

下表汇总了主要升级任务，并列出了每个任务所需的大致时间。下表后面的步骤提供了一些说明，您可以使用这些说明来估计系统的升级时间。

升级任务	**Description**	所需大致时间	执行此任务期间
启动升级服务	运行升级预检，分发软件文件并启动升级服务。	每个网格节点 3 分钟，除非报告验证错误	根据需要，您可以在计划的升级维护窗口之前手动运行升级预检。
升级网格节点（主管理节点）	主管理节点将停止，升级并重新启动。	30 分钟到 1 小时，其中 SG100 和 SG1000 设备节点最需要时间。	您无法访问主管理节点。系统会报告连接错误，您可以忽略这些错误。
升级网格节点（所有其他节点）	所有其他网格节点上的软件将按照您批准节点的顺序进行升级。系统中的每个节点将逐个关闭，每个节点将停机几分钟。	每个节点 15 分钟到 1 小时，设备节点所需时间最多 • 注： * 对于设备节点，StorageGRID 设备安装程序会自动更新到最新版本。	• 请勿更改网格配置。 • 请勿更改审核级别配置。 • 请勿更新 ILM 配置。 • 系统会阻止您执行其他维护过程，例如修补程序，停用或扩展。 • 注： * 如果需要执行恢复，请联系技术支持。

升级任务	**Description**	所需大致时间	执行此任务期间
启用功能	新版本的新功能已启用。	不到 5 分钟	• 请勿更改网格配置。 • 请勿更改审核级别配置。 • 请勿更新 ILM 配置。 • 您不能执行其他维护操作步骤 。
升级数据库	升级过程会检查每个节点，以验证不需要更新 Cassandra 数据库。	每个节点 10 秒或整个网格几分钟	从 StorageGRID 11.5 升级到 11.5 不需要升级 Cassandra 数据库；但是， Cassandra 服务将在每个存储节点上停止并重新启动。 对于未来的 StorageGRID 功能版本， Cassandra 数据库更新步骤可能需要几天时间才能完成。
最终升级步骤	此时将删除临时文件，并完成到新版本的升级。	5 分钟	完成 * 最终升级步骤 * 任务后，您可以执行所有维护过程。

步骤

1. 估计升级所有网格节点所需的时间。
   a. 将 StorageGRID 系统中的节点数乘以每个节点 1 小时。

      一般来说，设备节点的升级时间比基于软件的节点要长。

   b. 此时再增加 1 小时，以说明下载 ` 。 upgrade` 文件，运行预检验证以及完成最终升级步骤所需的时间。
2. 如果您使用的是 Linux 节点，请为每个节点添加 15 分钟的时间，以考虑下载和安装 RPM 或 Deb 软件包所需的时间。
3. 通过添加步骤 1 和步骤 2 的结果来计算升级的总估计时间。

示例：升级到 **StorageGRID 11.6** 的估计时间

假设您的系统有 14 个网格节点，其中 8 个是 Linux 节点。

1. 将 14 乘以每个节点 1 小时。
2. 另外，还需要 1 小时的时间来说明下载，预检和最终步骤。

   升级所有节点的估计时间为 15 小时。

3. 将每个节点的 8 乘以 15 分钟，以说明在 Linux 节点上安装 RPM 或 Deb 软件包的时间。

此步骤的估计时间为 2 小时。

4. 将这些值相加。

   您应在长达 17 小时的时间内完成系统到 StorageGRID 11.0.0 的升级。

升级期间对系统的影响

您必须了解 StorageGRID 系统在升级期间会受到什么影响。

StorageGRID 升级不会造成系统中断

StorageGRID 系统可以在整个升级过程中从客户端应用程序载入和检索数据。在升级期间，网格节点会一次关闭一个，因此，目前并非所有网格节点都不可用。

要保证持续可用性，您必须确保使用适当的 ILM 策略以冗余方式存储对象。此外，您还必须确保将所有外部 S3 或 Swift 客户端配置为向以下客户端之一发送请求：

- 配置为高可用性（ HA ）组的 StorageGRID 端点
- 高可用性第三方负载平衡器
- 每个客户端具有多个网关节点
- 每个客户端具有多个存储节点

设备固件已升级

在 StorageGRID 11.6 升级期间：

- 所有 StorageGRID 设备节点都会自动升级到 StorageGRID 设备安装程序固件版本 3.6 。
- SG6060 和 SGF6024 设备会自动升级到 BIOS 固件版本 3B07.EX 和 BMC 固件版本 BMC 3.93.07 。
- SG100 和 SG1000 设备会自动升级到 BIOS 固件版本 3B12.EC 和 BMC 固件版本 4.67.07 。

可能会触发警报

服务启动和停止以及 StorageGRID 系统作为混合版本环境运行时（某些网格节点运行早期版本，而其他网格节点已升级到更高版本），可能会触发警报。升级完成后，可能会触发其他警报。

例如，服务停止时，您可能会看到 * 无法与节点 * 通信警报；或者，如果某些节点已升级到 StorageGRID 11.6 ，但其他节点仍在运行 StorageGRID 11.5 ，则可能会看到 * Cassandra communication error* 警报。通常，这些警报将在升级完成后清除。

在升级到 StorageGRID 11.6 期间停止存储节点时，可能会触发 "ILM placement unableableableable" 警报。升级完成后，此警报可能会持续 1 天。

如果对存储卷水印使用自定义值，则升级完成后可能会触发 * 低只读水印覆盖 * 警报。请参见 对低只读水印覆盖警报进行故障排除 了解详细信息。

升级完成后，您可以从网格管理器信息板中选择 * 最近解决的警报 * 或 * 当前警报 * 来查看任何与升级相关的警报。

系统会生成许多 **SNMP** 通知

请注意，在升级期间停止并重新启动网格节点时，可能会生成大量 SNMP 通知。要避免出现过多通知，请在开始升级之前取消选中 * 启用 SNMP 代理通知 * 复选框（ * 配置 * > * 监控 * > * SNMP 代理 * ）以禁用 SNMP 通知。然后，在升级完成后重新启用通知。

配置更改受限

> 受限配置更改的列表可能会随版本而异。升级到另一个 StorageGRID 版本时，请参阅相应升级说明中的列表。

直到 * 启用新功能 * 任务完成：

- 请勿更改任何网格配置。
- 请勿更改审核级别配置或配置外部系统日志服务器。
- 请勿启用或禁用任何新功能。
- 请勿更新 ILM 配置。否则，您可能会遇到不一致的意外 ILM 行为。
- 请勿应用修补程序或恢复网格节点。
- 升级到 StorageGRID 11.6 时，您无法管理 HA 组， VLAN 接口或负载平衡器端点。

完成 * 最终升级步骤 * 任务之前：

- 请勿执行扩展操作步骤 。
- 请勿执行停用操作步骤 。

您不能从租户管理器查看存储分段详细信息或管理存储分段

在升级到 StorageGRID 11.6 期间（即，当系统作为混合版本环境运行时），您无法使用租户管理器查看存储分段详细信息或管理存储分段。租户管理器中的 " 分段 " 页面显示以下错误之一：

- "`在升级到 11.6. 时不能使用此 API 。` "
- "`升级到 11.6.` 时，您无法在租户管理器中查看存储分段版本控制详细信息。 "

升级到 11.6 后，此错误将得以解决。

临时解决策

在执行 11.6 升级期间，请使用以下工具查看存储分段详细信息或管理存储分段，而不是使用租户管理器：

- 要对存储分段执行标准 S3 操作，请使用 S3 REST API 或租户管理 API 。
- 要对存储分段执行 StorageGRID 自定义操作（例如，查看和修改存储分段一致性级别，启用或禁用上次访问时间更新或配置搜索集成），请使用租户管理 API 。

请参见 了解租户管理 API 和 使用 S3 有关说明，请参见。

升级对组和用户帐户的影响

您必须了解 StorageGRID 升级的影响，以便可以在升级完成后相应地更新组和用户帐户。

对组权限和选项进行的更改

升级到 StorageGRID 11.6 后，可以选择以下更新或新的权限和选项（ * 配置 * > * 访问控制 * > * 管理组 * ）。

权限或选项	Description
租户帐户	除了允许用户创建，编辑和删除租户帐户之外，此权限现在还允许管理员用户查看现有流量分类策略（ * 配置 * > * 网络 * > * 流量分类 * ）。

请参见 管理管理组。

验证已安装的 **StorageGRID** 版本

在开始升级之前，您必须确认先前版本的 StorageGRID 当前已安装应用了最新可用的修补程序。

关于此任务

在升级到 StorageGRID 11.5 之前，网格必须安装 StorageGRID 11.5 。如果您当前使用的是早期版本的 StorageGRID ，则必须安装所有先前的升级文件及其最新的修补程序（强烈建议），直到网格的当前版本为 StorageGRID 11.5. *x.y* 为止。

中显示了一个可能的升级路径 示例。

> NetApp 强烈建议您在升级到下一个版本之前对每个 StorageGRID 版本应用最新的修补程序，同时对安装的每个新版本应用最新的修补程序。在某些情况下，您必须应用修补程序以避免数据丢失的风险。请参见 "NetApp 下载： StorageGRID" 以及每个修补程序的发行说明以了解更多信息。

请注意，您可以运行一个脚本，以便一步从 11.3.1.0.3+ 更新到 11.4.0.*y* ，一步从 11.4.0.7+ 更新到 11.5.0.*y* 。请参见 "NetApp 知识库：如何为 StorageGRID 运行组合式主要升级和修补程序脚本"。

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 从网格管理器的顶部，选择 * 帮助 * > * 关于 * 。
3. 验证 * 版本 * 是否为 11.5. *x.y* 。

   在 StorageGRID 11.5. *x.y* 版本号中：

   - 主要版本 * 的 *x* 值为 0 （ 11.5.0 ）。
   - 如果应用了一个 * 热修补程序 * ，则该热修补程序 * 具有 *y* 值（例如 11.5.0.1 ）。
4. 如果 * 版本 * 不是 11.5. *x.y* ，请转至 "NetApp 下载： StorageGRID" 下载每个先前版本的文件，包括每个版本的最新修补程序。
5. 获取下载的每个版本的升级说明。然后，对该版本执行软件升级操作步骤 ，并应用该版本的最新修补程序（强烈建议）。

   请参见 StorageGRID 热修补程序操作步骤。

示例：从 **11.3.0.8** 版升级到 **StorageGRID 11.5**

以下示例显示了从 StorageGRID 11.3.0.8 版升级到 11.5 版以准备 StorageGRID 11.5 版的步骤。

> 或者，您也可以运行一个脚本来合并步骤 2 和 3 （从 11.3.1.0.13 更新到 11.4.0.*y* ）以及合并步骤 4 和 5 （从 11.4.0.7+ 更新到 11.5.0.*y* ）。请参见 "NetApp 知识库：如何为 StorageGRID 运行组合式主要升级和修补程序脚本"。

按以下顺序下载并安装软件，以便为您的系统做好升级准备：

1. 应用最新的 StorageGRID 11.3.0.*y* 修补程序。
2. 升级到 StorageGRID 11.4.0 主要版本。
3. 应用最新的 StorageGRID 11.4.0.*y* 修补程序。
4. 升级到 StorageGRID 11.5.0 主要版本。
5. 应用最新的 StorageGRID 11.5.0.*y* 修补程序。

获取软件升级所需的材料

在开始软件升级之前，您必须获取所有必需的材料，才能成功完成升级。

项目	注释：
StorageGRID 升级文件	下载 StorageGRID 升级文件 连接到您的服务笔记本电脑。
服务笔记本电脑	服务笔记本电脑必须具有： • 网络端口 • SSH 客户端（例如 PuTTY ）
支持的 Web 浏览器	每个 StorageGRID 版本的浏览器支持通常会发生变化。确保您的浏览器与新的 StorageGRID 版本兼容。
恢复软件包（` .zip` ）文件	[下载恢复包] 升级之前，请将此文件保存在安全位置。通过恢复包文件，您可以在发生故障时还原系统。
`passwords.txt` file	该文件包含在上述软件包中，该软件包是恢复软件包 ` .zip` 文件的一部分。您必须获取最新版本的恢复软件包。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语未列在 `passwords.txt` 文件中。

项目	注释：
相关文档	• 发行说明 对于 StorageGRID 11.6.在开始升级之前，请务必仔细阅读这些内容。 • 说明 管理 StorageGRID。 • 如果要升级 Linux 部署，请参见适用于您的 Linux 平台的 StorageGRID 安装说明： ◦ 安装 Red Hat Enterprise Linux 或 CentOS ◦ 安装 Ubuntu 或 Debian • 根据需要提供其他 StorageGRID 文档。

下载 **StorageGRID** 升级文件

您必须下载一个或多个文件，具体取决于节点的安装位置。

- * 所有平台 * ： ` 。 upgrade` file

如果在 Linux 主机上部署了任何节点，则还必须下载 RPM 或 Deb 归档文件，此文件将在开始升级之前安装：

- * Red Hat Enterprise Linux 或 CentOS* ： 附加 RPM 文件（` .zip` 或 ` .tgz` ）
- * Ubuntu 或 Debian * ： 一个额外的 Deb 文件（` .zip` 或 ` .tgz` ）

步骤

1. 转至 "NetApp 下载： StorageGRID"。
2. 选择用于下载最新版本的按钮，或者从下拉菜单中选择其他版本并选择 * 执行 * 。

   StorageGRID 软件版本采用以下格式： 11.*x.y* 。StorageGRID 修补程序采用以下格式： 11.*x.y.z* 。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 如果显示 Caution/MustRead 语句，请阅读该语句并选中复选框。

   如果此版本需要修补程序，则会显示此语句。
5. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。

   此时将显示选定版本的下载页面。此页面包含三列：

   ◦ 安装 StorageGRID

   ◦ 升级 StorageGRID

   ◦ StorageGRID 设备的支持文件
6. 在 * 升级 StorageGRID * 列中，选择并下载 ` 。 upgrade` archive 。

   每个平台都需要 ` 。 upgrade` archive 。
7. 如果在 Linux 主机上部署了任何节点，请同时以 ` .tgz` 或 ` .zip` 格式下载 RPM 或 Deb 归档。如果您在服务笔记本电脑上运行 Windows ，请选择 ` .zip` 文件。

- Red Hat Enterprise Linux 或 CentOS + `StorageGRID-Webscale -version-RPM-uniqueID.zip` + `StorageGRID-Webscale -version-RPM-uniqueID.tgz`
- Ubuntu 或 Debian + `StorageGRID-Webscale -version-Deb-uniqueID.zip` + `StorageGRID-Webscale -version-Deb-uniqueID.tgz`

> SG100 或 SG1000 不需要其他文件。

下载恢复包

通过恢复包文件，您可以在发生故障时还原 StorageGRID 系统。在对 StorageGRID 系统进行网格拓扑更改之前或升级软件之前，请下载当前的恢复软件包文件。然后，在更改网格拓扑或升级软件后下载恢复包的新副本。

您需要的内容

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

步骤

1. 选择 * 维护 * > * 系统 * > * 恢复包 * 。
2. 输入配置密码短语，然后选择 * 开始下载 * 。

   下载将立即开始。

3. 下载完成后：
   a. 打开 ` .zip` 文件。
   b. 确认其中包含 `gpt-backup` 目录和内侧 ` .zip` 文件。
   c. 提取内部 ` .zip` 文件。
   d. 确认您可以打开 `passwords.txt` 文件。
4. 将下载的恢复软件包文件（` .zip` ）复制到两个安全的单独位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

检查系统的状况

在升级 StorageGRID 系统之前，您必须验证系统是否已准备好进行升级。您必须确保系统正常运行，并且所有网格节点均正常运行。

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 检查并解决所有活动警报。

   有关特定警报的信息，请参见 警报参考。

3. 确认没有处于活动状态或待定状态的存在冲突的网格任务。
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 主管理节点 _* > * CMN* > * 网格任务 * > * 配置 * 。

      信息生命周期管理评估（ ILME ）任务是唯一可与软件升级同时运行的网格任务。

   c. 如果任何其他网格任务处于活动状态或处于待定状态，请等待其完成或释放锁定。

      如果任务未完成或未解除锁定，请联系技术支持。

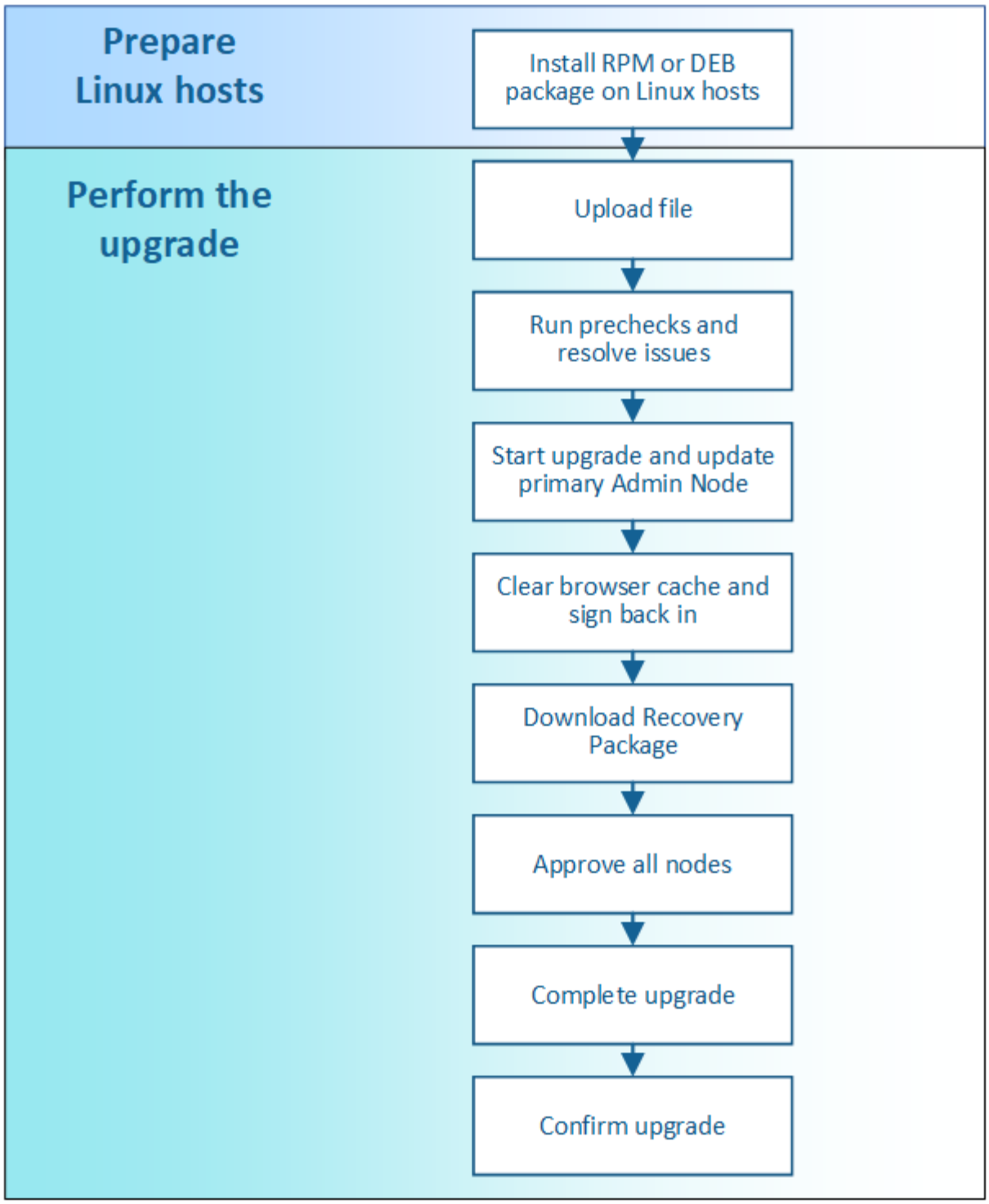
4. 请参见 内部网格节点通信 和 外部通信 确保在升级之前打开 StorageGRID 11.6 所需的所有端口。

   如果您已打开任何自定义防火墙端口，则在升级预检期间会收到通知。在继续升级之前，您必须联系技术支持。

升级 **StorageGRID** 软件

升级工作流

开始升级之前，请查看常规工作流。StorageGRID 升级页面将指导您完成每个升级步骤。



1. 如果在 Linux 主机上部署了任何 StorageGRID 节点， 在每个主机上安装 RPM 或 Deb 软件包 开始升级之前。
2. 在主管理节点上，访问 StorageGRID 升级页面并上传升级文件。
3. 您也可以在开始实际升级之前运行升级预检来检测和解决任何问题。
4. 启动升级，此过程将自动运行预检并升级主管理节点。在升级主管理节点时，您无法访问网格管理器。审核日志也将不可用。此升级可能需要长达 30 分钟的时间。
5. 升级主管理节点后，清除 Web 浏览器的缓存，重新登录并返回 StorageGRID 升级页面。
6. 下载新的恢复软件包。

7. 批准网格节点。您可以批准单个网格节点，一组网格节点或所有网格节点。

   除非您确定网格节点已准备好停止并重新启动，否则请勿批准网格节点的升级。

8. 恢复操作。升级完所有网格节点后，将启用新功能，您可以恢复操作。您必须等待执行停用或扩展操作步骤，直到后台 * 升级数据库 * 任务和 * 最终升级步骤 * 任务完成为止。
9. 升级完成后，确认软件版本并应用任何修补程序。

相关信息

估计完成升级所需的时间

Linux： 在所有主机上安装 **RPM** 或 **Deb** 软件包

如果在 Linux 主机上部署了任何 StorageGRID 节点，则在开始升级之前，必须在每个主机上安装一个额外的 RPM 或 Deb 软件包。

您需要的内容

您必须已从 StorageGRID 的 "NetApp 下载 " 页面下载以下 ` .tgz` 或 ` .zip` 文件之一。

如果您在服务笔记本电脑上运行 Windows ，请使用 ` .zip` 文件。

Linux 平台	其他文件（选择一个）
Red Hat Enterprise Linux 或 CentOS	• `storageGRID-Webscale -version-RPM-uniqueID.zip` • `storageGRID-Webscale -version-RPM-uniqueID.tgz`
Ubuntu 或 Debian	• `storageGRID-Webscale -version-Deb-uniqueID.zip` • `storageGRID-Webscale -version-Deb-uniqueID.tgz`

步骤

1. 从安装文件中提取 RPM 或 Deb 软件包。
2. 在所有 Linux 主机上安装 RPM 或 Deb 软件包。

   请参见适用于您的 Linux 平台的安装说明中有关安装 StorageGRID 主机服务的步骤。

   - 安装 Red Hat Enterprise Linux 或 CentOS
   - 安装 Ubuntu 或 Debian

   新软件包将作为附加软件包进行安装。请勿删除现有软件包。

执行升级

准备好执行升级后，请选择 ` .upgrade` archive 并输入配置密码短语。您可以选择在执行实际升级之前运行升级预检。

您需要的内容

您已查看所有注意事项并完成所有规划和准备步骤。

上传升级文件

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 维护 * > * 系统 * > * 软件更新 * 。

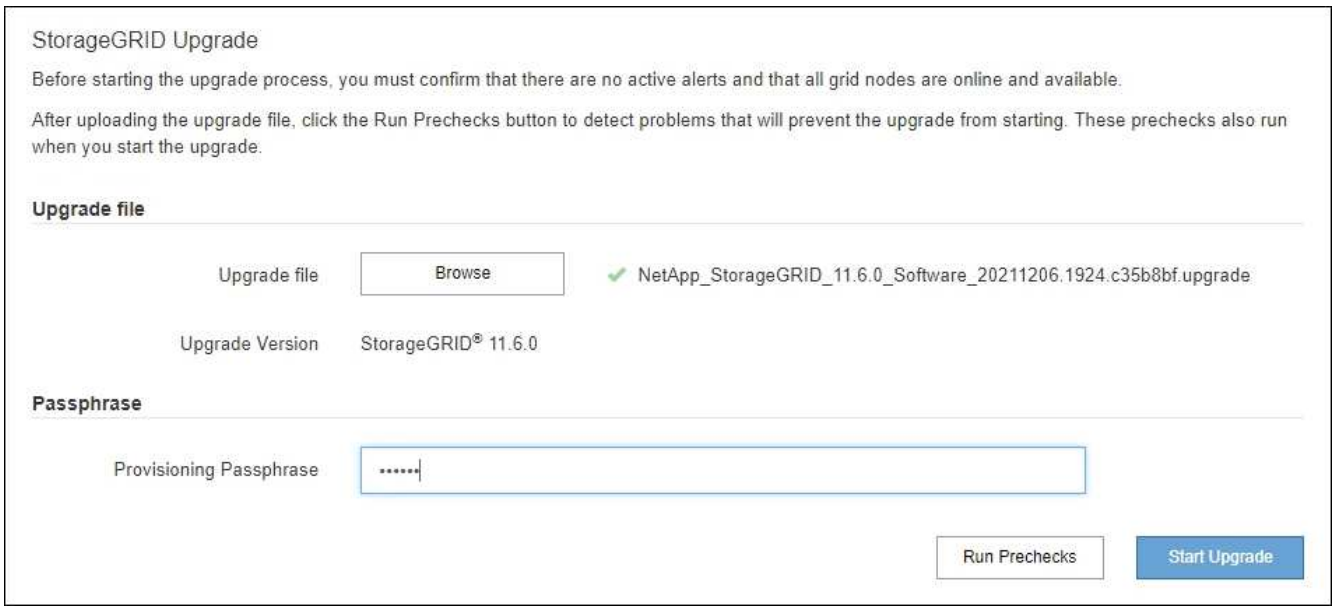
   此时将显示软件更新页面。

3. 选择 * StorageGRID Upgrade* 。
4. 在 StorageGRID 升级页面上，选择 ` .upgrade` archive 。
   a. 选择 * 浏览 * 。
   b. 找到并选择文件： `NetApp_StorageGRID_11.6.0_Software_uniqueID.upgrade`
   c. 选择 * 打开 * 。

      已上传并验证此文件。验证过程完成后，升级文件名称旁边会显示一个绿色复选标记。

5. 在文本框中输入配置密码短语。

   已启用 * 运行预检 * 和 * 开始升级 * 按钮。



运行预检

您也可以在开始实际升级之前验证系统的状况。选择 * 运行预检 * 可在开始升级之前检测并解决问题。开始升级时，系统会执行相同的预检。预检失败将停止升级过程，某些问题可能需要技术支持参与才能解决。

1. 选择 * 运行预检 * 。
2. 等待预检完成。
3. 按照说明解决报告的任何预检错误。

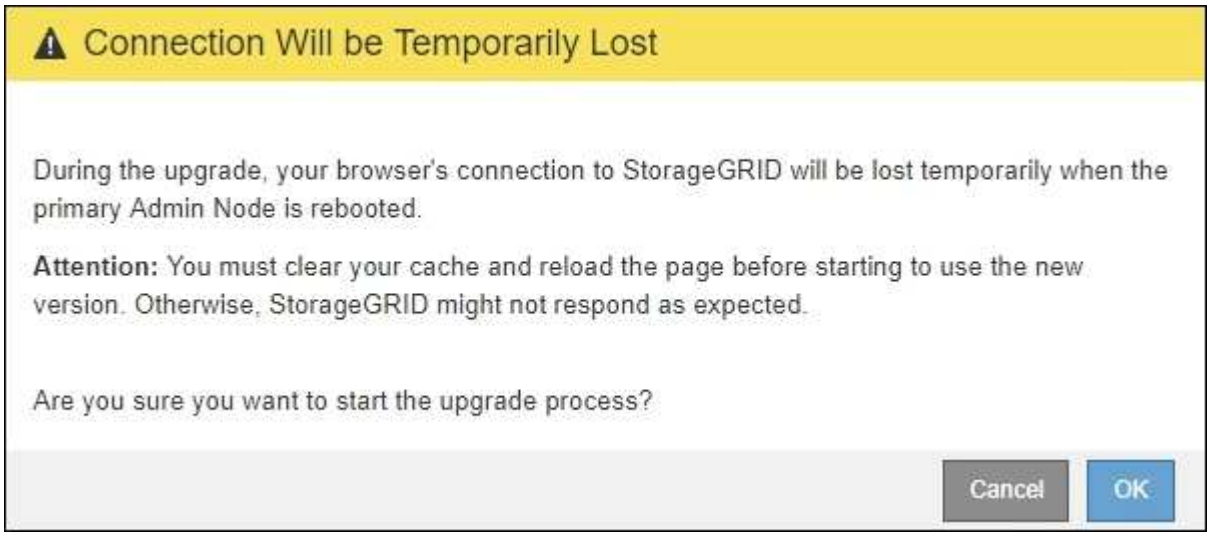
如果您已打开任何自定义防火墙端口，则会在预检验证期间收到通知。在继续升级之前，您必须联系技术支持。

开始升级并更新主管理节点

升级开始时，系统会执行升级预检，并升级主管理节点，其中包括停止服务，升级软件和重新启动服务。在升级主管理节点时，您无法访问网格管理器。审核日志也将不可用。此升级可能需要长达 30 分钟的时间。

1. 准备好执行升级后，请选择 * 开始升级 * 。

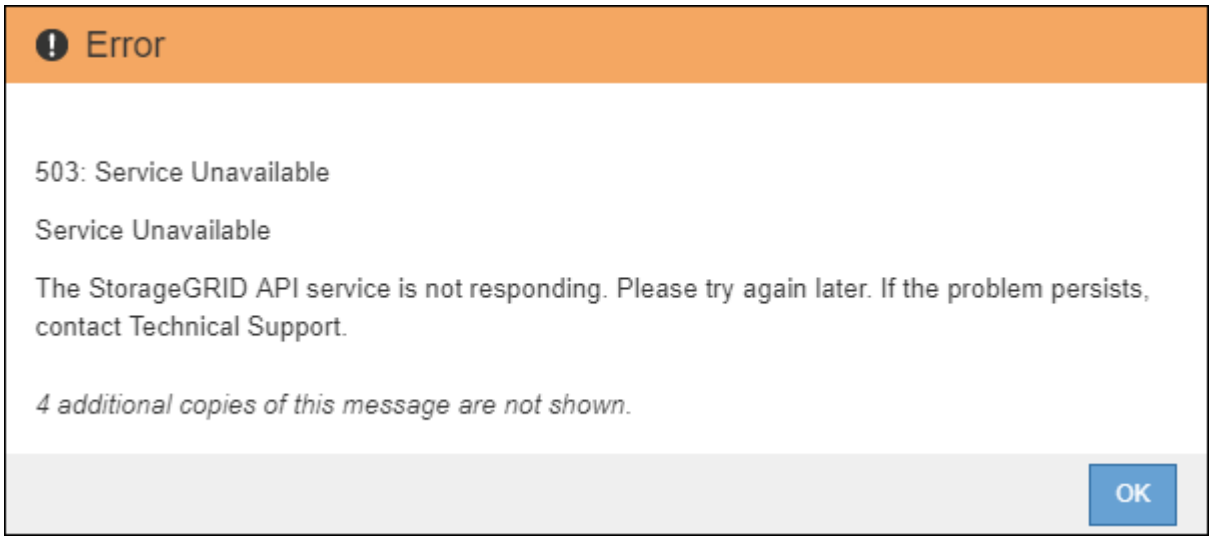
   此时将显示一条警告，提醒您在重新启动主管理节点后，浏览器的连接将断开。



2. 选择 * 确定 * 确认警告并启动升级过程。
3. 等待执行升级预检并升级主管理节点。

   如果报告了任何预检错误，请解决这些错误，然后再次选择 * 开始升级 * 。

   在升级主管理节点时，会显示多条 * 503： service unavail* 和 * 连接到服务器时出现问题 * 消息，您可以忽略这些消息。



4. 当您看到 * 400： bad request* 消息时，请转至下一步。管理节点升级已完成。

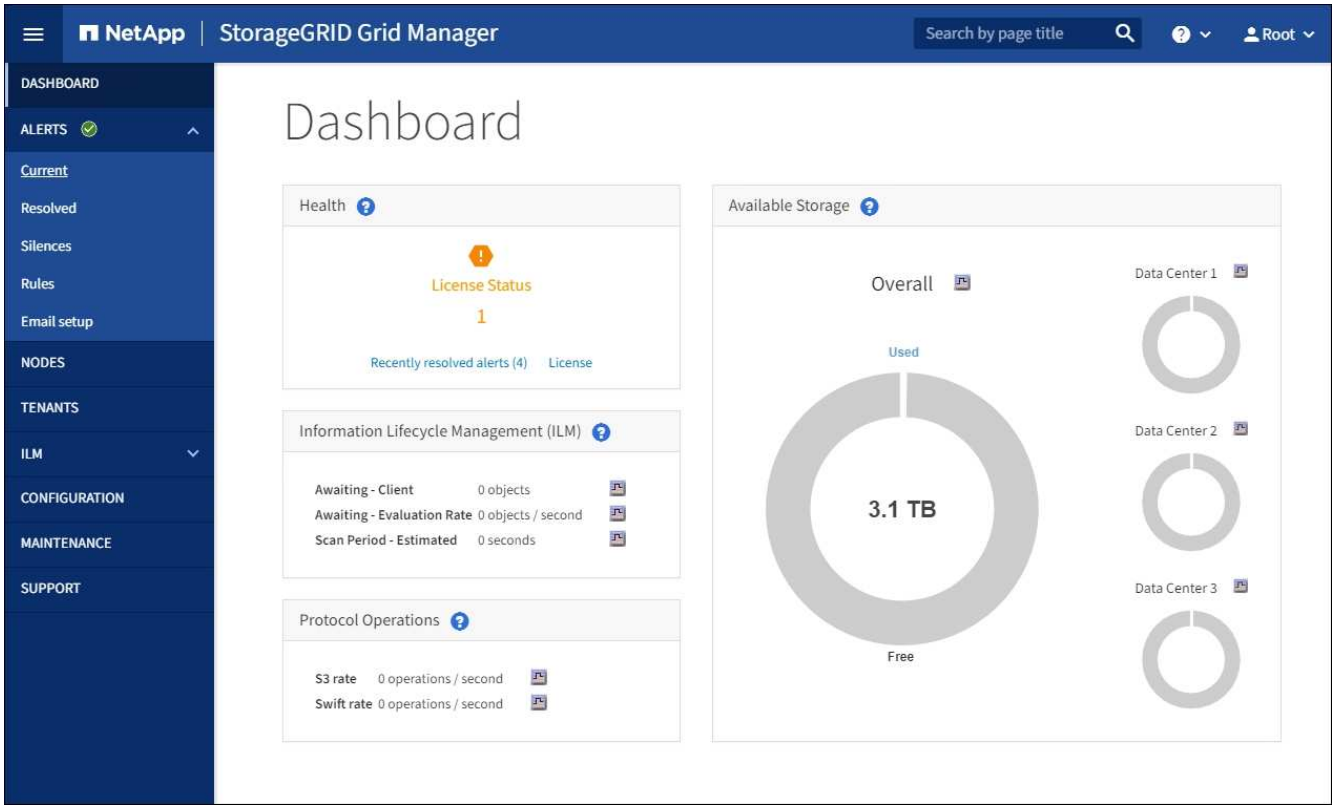
清除浏览器缓存并重新登录

1. 升级主管理节点后，清除 Web 浏览器的缓存并重新登录。

   有关说明，请参见 Web 浏览器的文档。

   您必须清除 Web 浏览器的缓存，才能删除先前版本的软件所使用的过时资源。

   此时将显示经过重新设计的 Grid Manager 界面，表示主管理节点已升级。



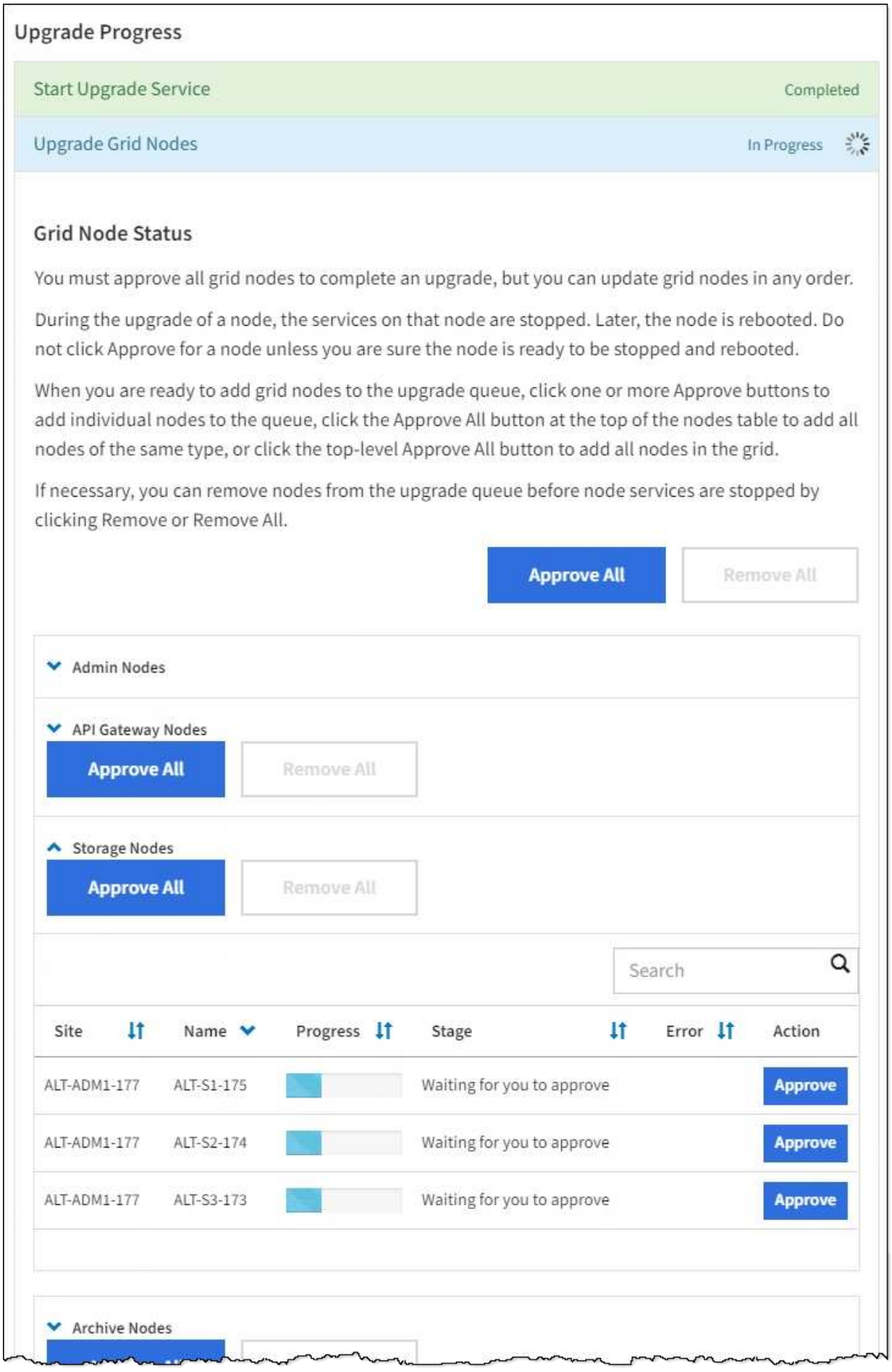
2. 从边栏中，选择 * 维护 * 以打开维护菜单。
3. 在 * 系统 * 部分中，选择 * 软件更新 * 。
4. 在 * StorageGRID Upgrade* 部分中，选择 * 升级 * 。
5. 查看 StorageGRID 升级页面上的升级进度部分，其中提供了有关每个主要升级任务的信息。
   a. * 启动升级服务 * 是第一个升级任务。在此任务期间，软件文件将分发到网格节点，并启动升级服务。
   b. 完成 * 启动升级服务 * 任务后， * 升级网格节点 * 任务将启动。
   c. 在执行 * 升级网格节点 * 任务期间，将显示网格节点状态表，其中显示了系统中每个网格节点的升级阶段。

下载恢复软件包并升级所有网格节点

1. 在网格节点状态表中显示网格节点之后，但在批准任何网格节点之前， 下载恢复软件包的新副本。

   升级主管理节点上的软件版本后，必须下载恢复软件包文件的新副本。通过恢复包文件，您可以在发生故障时还原系统。

2. 查看网格节点状态表中的信息。网格节点按管理节点， API 网关节点，存储节点和归档节点等类型按部分进行排列。


Upgrade Progress
Start Upgrade Service
Completed
Upgrade Grid Nodes
In Progress
Grid Node Status
You must approve all grid nodes to complete an upgrade, but you can update grid nodes in any order.
During the upgrade of a node, the services on that node are stopped. Later, the node is rebooted. Do not click Approve for a node unless you are sure the node is ready to be stopped and rebooted.
When you are ready to add grid nodes to the upgrade queue, click one or more Approve buttons to add individual nodes to the queue, click the Approve All button at the top of the nodes table to add all nodes of the same type, or click the top-level Approve All button to add all nodes in the grid.
If necessary, you can remove nodes from the upgrade queue before node services are stopped by clicking Remove or Remove All.
Approve All
Remove All
Admin Nodes
API Gateway Nodes
Approve All
Remove All
Storage Nodes
Approve All
Remove All
Search
Site
Name
Progress
Stage
Error
Action
ALT-ADM1-177
ALT-S1-175
Waiting for you to approve
Approve
ALT-ADM1-177
ALT-S2-174
Waiting for you to approve
Approve
ALT-ADM1-177
ALT-S3-173
Waiting for you to approve
Approve
Archive Nodes

首次显示此页面时，网格节点可能处于以下阶段之一：

- Done （完成）（仅限主管理节点）
- 正在准备升级
- 软件下载已排队
- 正在下载
- 正在等待您批准

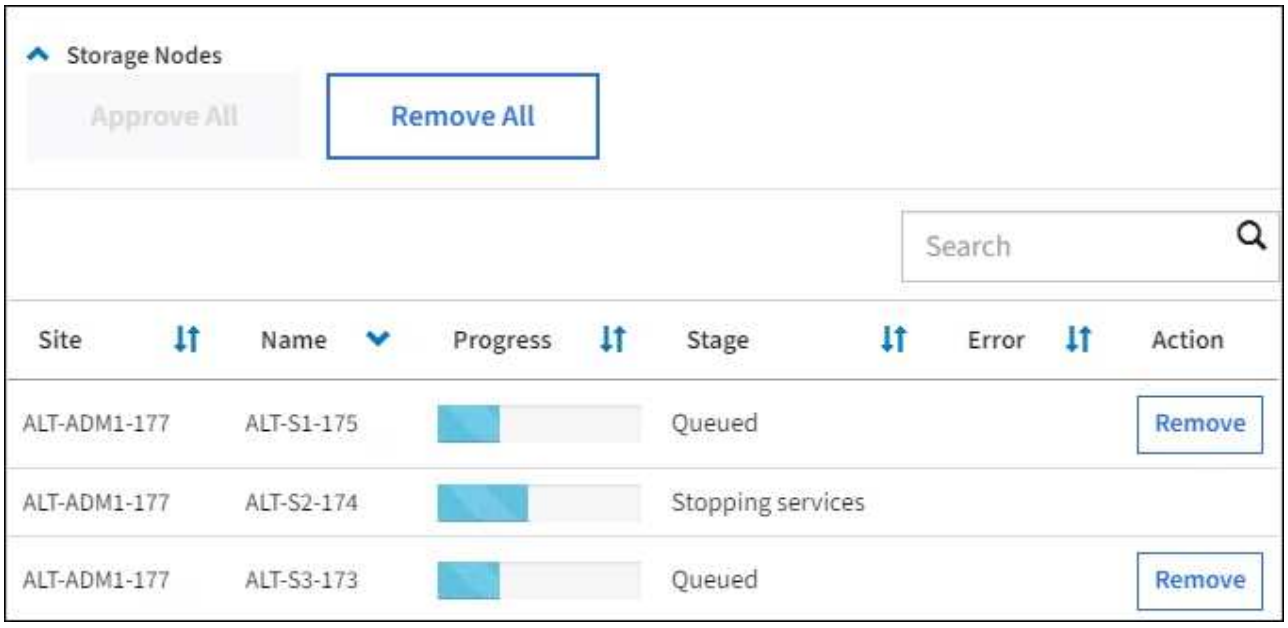
3. 批准已准备好添加到升级队列的网格节点。

> 在网格节点上开始升级时，该节点上的服务将停止。稍后，网格节点将重新启动。为避免与节点通信的客户端应用程序出现服务中断，请勿批准节点升级，除非您确定节点已做好停止和重新启动的准备。根据需要计划维护时段或通知客户。

您必须升级 StorageGRID 系统中的所有网格节点，但可以自定义升级顺序。您可以批准单个网格节点，一组网格节点或所有网格节点。

如果节点升级顺序非常重要，请逐个批准节点或节点组，并等待每个节点完成升级，然后再批准下一个节点或节点组。

- 选择一个或多个 * 批准 * 按钮将一个或多个单独的节点添加到升级队列。如果您批准多个相同类型的节点，则这些节点将一次升级一个。
- 在每个部分中选择 * 全部批准 * 按钮，将所有相同类型的节点添加到升级队列。
- 选择顶级 * 全部批准 * 按钮，将网格中的所有节点添加到升级队列。
- 选择 * 删除 * 或 * 全部删除 * 可从升级队列中删除一个或所有节点。当节点的阶段达到 * 正在停止服务 * 时，您无法删除该节点。此时将隐藏 * 删除 * 按钮。



4. 等待每个节点继续完成升级阶段，包括已排队，停止服务，停止容器，清理 Docker 映像，升级基础操作系统软件包，重新启动，重新启动后执行步骤，启动服务以及完成。

当设备节点达到升级基本操作系统软件包阶段时，设备上的 StorageGRID 设备安装程序软件将会更新。此自动化过程可确保 StorageGRID 设备安装程序版本与 StorageGRID 软件版本保持同步。

完成升级

当所有网格节点都完成升级阶段后， * 升级网格节点 * 任务将显示为已完成。其余升级任务将在后台自动执行。

1. 完成 * 启用功能 * 任务后（该任务会很快发生），您可以选择开始使用升级后的 StorageGRID 版本中的新功能。
2. 在执行 * 升级数据库 * 任务期间，升级过程会检查每个节点，以确认不需要更新 Cassandra 数据库。

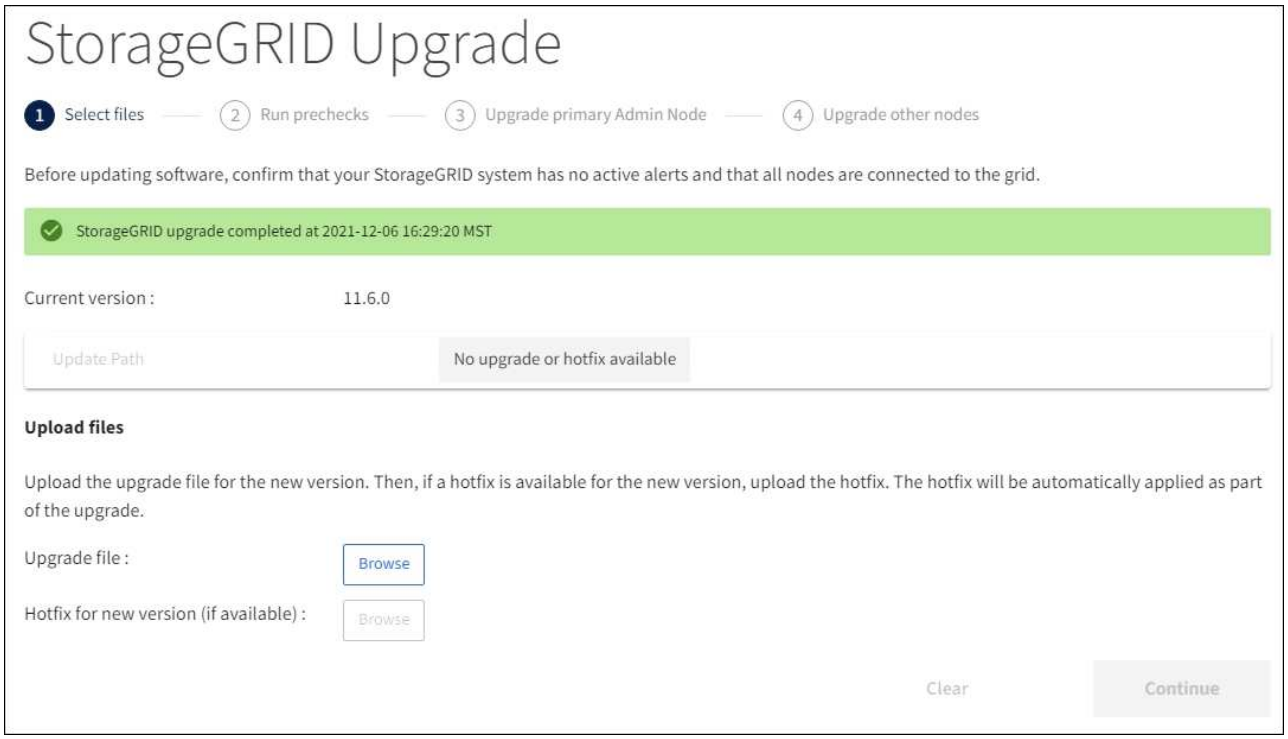
   从 StorageGRID 11.5 升级到 11.5 不需要升级 Cassandra 数据库；但是， Cassandra 服务将在每个存储节点上停止并重新启动。对于未来的 StorageGRID 功能版本， Cassandra 数据库更新步骤可能需要几天时间才能完成。

3. 完成 * 升级数据库 * 任务后，请等待几分钟，以完成 * 最终升级步骤 * 任务。

   完成最终升级步骤任务后，将完成升级。

确认升级

1. 确认升级已成功完成。
   a. 从网格管理器顶部，选择帮助图标并选择 * 关于 * 。
   b. 确认显示的版本符合您的预期。
   c. 选择 * 维护 * > * 系统 * > * 软件更新 * 。
   d. 在 * StorageGRID upgrade* 部分中，选择 * 升级 * 。
   e. 确认绿色横幅显示软件升级已在预期日期和时间完成。



2. 在 StorageGRID 升级页面中，确定当前 StorageGRID 版本是否有任何修补程序可用。

> 如果未显示更新路径，则您的浏览器可能无法访问 NetApp 支持站点。或者， AutoSupport 页面（ * 支持 * > * 工具 * > * AutoSupport * ）上的 * 检查软件更新 * 复选框可能已禁用。

3. 如果有可用的修补程序，请下载此文件。然后，使用 StorageGRID 热修补程序操作步骤 以应用此修补程序。
4. 验证网格操作是否已恢复正常：
   a. 检查这些服务是否正常运行，以及是否没有意外警报。
   b. 确认客户端与 StorageGRID 系统的连接是否按预期运行。

对升级问题进行故障排除

升级未完成

如果升级未成功完成，您可以自行解决问题描述 。如果无法解决问题描述 ，应先收集所需信息，然后再联系技术支持。

以下各节介绍如何从升级部分失败的情况中恢复。如果无法解决升级问题描述 ，请联系技术支持。

升级预检错误

要检测并解决问题，您可以在开始实际升级之前手动运行升级预检。大多数预检错误都提供了有关如何解决问题描述 的信息。如果需要帮助，请联系技术支持。

配置失败

如果自动配置过程失败，请联系技术支持。

网格节点崩溃或无法启动

如果网格节点在升级过程中崩溃或升级完成后无法成功启动，请联系技术支持以调查并更正任何潜在问题。

载入或数据检索中断

如果在不升级网格节点时数据载入或检索意外中断，请联系技术支持。

数据库升级错误

如果数据库升级失败并显示错误，请重试此升级。如果故障再次出现，请联系技术支持。

相关信息

升级软件前检查系统状况

对用户界面问题进行故障排除

升级到新版本的 StorageGRID 软件后，您可能会看到网格管理器或租户管理器出现问题。

Web 界面未按预期响应

升级 StorageGRID 软件后，网格管理器或租户管理器可能无法按预期做出响应。

如果您在使用 Web 界面时遇到问题：

- 确保您使用的是 支持的 Web 浏览器。

  每个 StorageGRID 版本的浏览器支持通常会发生变化。

- 清除 Web 浏览器缓存。

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

错误消息： **Docker** 映像可用性检查

尝试启动升级过程时，您可能会收到一条错误消息，指出 "`Docker 映像可用性检查验证套件发现以下问题。` 必须先解决所有问题，然后才能完成升级。

如果您不确定解决所发现问题所需的更改，请联系技术支持。

message	发生原因	解决方案
无法确定升级版本。升级版本信息文件 ` { file_path } ` 与预期格式不匹配。	升级软件包已损坏。	请重新上传升级包，然后重试。如果问题仍然存在，请联系技术支持。
未找到升级版本信息文件 ` { file_path } `。无法确定升级版本。	升级软件包已损坏。	请重新上传升级包，然后重试。如果问题仍然存在，请联系技术支持。

message	发生原因	解决方案
无法确定 ` { node_name } ` 上当前安装的版本。	节点上的关键文件已损坏。	请联系技术支持。
尝试列出 ` { node_name } ` 上的版本时出现连接错误	节点脱机或连接中断。	请检查以确保所有节点均联机并可从主管理节点访问，然后重试。
节点 ` { node_name } ` 的主机未加载 StorageGRID ` { upgrade_version } ` 映像。必须先在主机上安装映像和服务，然后才能继续升级。	用于升级的 RPM 或 Deb 软件包未安装在运行节点的主机上，或者映像仍在导入过程中。 • 注： * 此错误仅适用于在 Linux 上作为容器运行的适用场景 节点。	检查以确保 RPM 或 Deb 软件包已安装在运行节点的所有 Linux 主机上。确保服务和映像文件的版本正确。请稍等几分钟，然后重试。 请参见 Linux ： 在所有主机上安装 RPM 或 Deb 软件包。
检查节点 ` { node_name } ` 时出错	发生意外错误。	请稍等几分钟，然后重试。
运行预检时出现未捕捉的错误。 ` { error_string } `	发生意外错误。	请稍等几分钟，然后重试。

增加元数据预留空间设置

升级到 StorageGRID 11.6 后，如果存储节点满足 RAM 和可用空间的特定要求，则可以增加元数据预留空间系统设置。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有 " 根访问 " 权限或 " 网格拓扑页面配置 " 和 " 其他网格配置 " 权限。
- 您已完成 StorageGRID 11.6 升级。

关于此任务

升级到 StorageGRID 11.6 后，您可以手动将系统范围的元数据预留空间设置提高到 8 TB 。在升级到 11.6 后预留额外的元数据空间将简化未来的硬件和软件升级。

只有当以下两项陈述均为 true 时，才能增加系统范围的元数据预留空间设置的值：

- 系统中任何站点的存储节点均具有 128 GB 或更多 RAM 。
- 系统中任何站点的存储节点在存储卷 0 上都有足够的可用空间。

请注意，如果增加此设置，则会同时减少所有存储节点的存储卷 0 上可用于对象存储的空间。因此，您可能希望根据预期对象元数据要求将元数据预留空间设置为小于 8 TB 的值。

> 一般来说，最好使用较高的值，而不是较低的值。如果 " 元数据预留空间 " 设置过大，您可以稍后减小此设置。相比之下，如果稍后增加该值，系统可能需要移动对象数据以释放空间。

有关元数据预留空间设置如何影响特定存储节点上对象元数据存储允许的空间的详细说明，请转至 管理对象元数据存储。

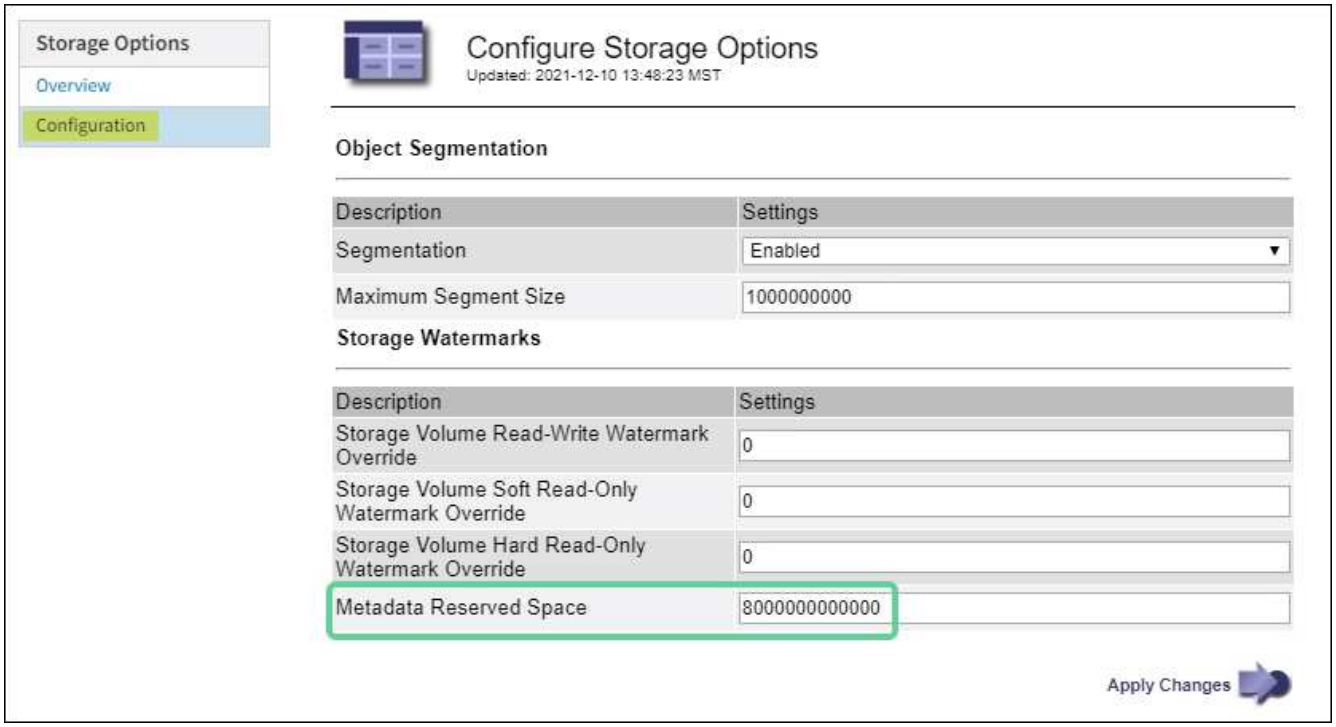
步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 确定当前的元数据预留空间设置。
   a. 选择 * 配置 * > * 系统 * > * 存储选项 * 。
   b. 在存储水印部分中，记下 * 元数据预留空间 * 的值。
3. 确保每个存储节点的存储卷 0 上有足够的可用空间来增加此值。
   a. 选择 * 节点 * 。
   b. 选择网格中的第一个存储节点。
   c. 选择存储选项卡。
   d. 在卷部分中，找到 * /var/local/rangedb/0* 条目。
   e. 确认可用值等于或大于要使用的新值与当前元数据预留空间值之间的差值。

      例如，如果元数据预留空间设置当前为 4 TB ，而您希望将其增加到 6 TB ，则可用值必须为 2 TB 或更大。

   f. 对所有存储节点重复上述步骤。
      - 如果一个或多个存储节点没有足够的可用空间，则无法增加元数据预留空间值。请勿继续使用此操作步骤。
      - 如果每个存储节点在卷 0 上都有足够的可用空间，请转至下一步。
4. 确保每个存储节点上至少有 128 GB 的 RAM 。
   a. 选择 * 节点 * 。
   b. 选择网格中的第一个存储节点。
   c. 选择 * 硬件 * 选项卡。
   d. 将光标悬停在 " 内存使用量 " 图表上。确保 * 总内存 * 至少为 128 GB 。
   e. 对所有存储节点重复上述步骤。
      - 如果一个或多个存储节点没有足够的可用总内存，则无法增加元数据预留空间值。请勿继续使用此操作步骤。
      - 如果每个存储节点的总内存至少为 128 GB ，请转至下一步。
5. 更新元数据预留空间设置。
   a. 选择 * 配置 * > * 系统 * > * 存储选项 * 。
   b. 选择配置选项卡。
   c. 在存储水印部分中，选择 * 元数据预留空间 * 。
   d. 输入新值。

      例如，要输入 8 TB 作为支持的最大值，请输入 * 80000000000000000* （ 8 ，后跟 12 个零）



a. 选择 * 应用更改 * 。

安装 Red Hat Enterprise Linux 或 CentOS

安装 Red Hat Enterprise Linux 或 CentOS： 概述

在 Red Hat Enterprise Linux （ RHEL ）或 CentOS Linux 环境中安装 StorageGRID 系统包括三个主要步骤。

1. * 准备 * ： 在规划和准备期间，您将执行以下任务：
   - 了解 StorageGRID 的硬件和存储要求。
   - 了解的具体信息 StorageGRID 网络连接 这样，您就可以正确配置网络了。
   - 确定并准备要用于托管 StorageGRID 网格节点的物理或虚拟服务器。
   - 在已准备好的服务器上：
     - 安装 Linux
     - 配置主机网络
     - 配置主机存储
     - 安装容器引擎
     - 安装 StorageGRID 主机服务
2. * 部署 * ： 使用适当的用户界面部署网格节点。部署网格节点时，它们会作为 StorageGRID 系统的一部分创建并连接到一个或多个网络。
   a. 使用 Linux 命令行和节点配置文件在步骤 1 准备的主机上部署基于软件的网格节点。
   b. 使用 StorageGRID 设备安装程序部署 StorageGRID 设备节点。

StorageGRID 安装操作步骤 中不包含特定于硬件的安装和集成说明。要了解如何安装 StorageGRID 设备，请参见适用于您的设备的安装和维护说明。

3. * 配置 * ： 部署完所有节点后，请使用网格管理器配置网格并完成安装。

以下说明为部署和配置 StorageGRID 系统建议了一种标准方法。另请参见有关以下替代方法的信息：

- 使用 Ansible ， Puppet 或 Chef 等标准业务流程框架安装 RHEL 或 CentOS ，配置网络和存储，安装容器引擎和 StorageGRID 主机服务以及部署虚拟网格节点。
- 使用 Python 配置脚本（在安装归档中提供）自动部署和配置 StorageGRID 系统。
- 使用 Python 配置脚本（可从安装归档或 StorageGRID 设备安装程序获取）自动部署和配置设备网格节点。
- 如果您是 StorageGRID 部署的高级开发人员，请使用安装 REST API 自动安装 StorageGRID 网格节点。

规划并准备安装 **Red Hat** 或 **CentOS**

安装前（ **Red Hat** 或 **CentOS** ）

在部署网格节点和配置 StorageGRID 网格之前，您必须熟悉完成操作步骤 的步骤和要求。

StorageGRID 部署和配置过程假定您熟悉 StorageGRID 系统的架构和操作。

您可以一次部署一个或多个站点；但是，所有站点必须满足至少有三个存储节点的最低要求。

在开始安装 StorageGRID 之前，您必须：

- 了解 StorageGRID 的计算要求，包括每个节点的最低 CPU 和 RAM 要求。
- 了解 StorageGRID 如何支持多个网络以实现流量隔离，安全性和管理便利性，并计划要连接到每个 StorageGRID 节点的网络。

  请参见 StorageGRID 网络连接准则。

- 了解每种类型的网格节点的存储和性能要求。
- 确定一组服务器（物理服务器，虚拟服务器或两者），这些服务器可在聚合中提供足够的资源来支持您计划部署的 StorageGRID 节点的数量和类型。
- 如果要在不中断任何服务的情况下对物理主机执行计划内维护，请了解节点迁移的要求。
- 提前收集所有网络信息。除非使用 DHCP ，否则请收集要分配给每个网格节点的 IP 地址以及要使用的域名系统（ DNS ）和网络时间协议（ NTP ）服务器的 IP 地址。
- 按照规格安装，连接和配置所有必需的硬件，包括任何 StorageGRID 设备。

  StorageGRID 安装操作步骤 中不包含特定于硬件的安装和集成说明。要了解如何安装 StorageGRID 设备，请参见适用于您的设备的安装和维护说明。

- 确定要使用的可用部署和配置工具。

相关信息

网络连接准则

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

所需材料

在安装 StorageGRID 之前，您必须收集并准备所需的材料。

项目	注释：
NetApp StorageGRID 许可证	您必须具有有效的数字签名 NetApp 许可证。 • 注意 * ： StorageGRID 安装归档中包含一个非生产许可证，可用于测试和概念验证网格。
StorageGRID 安装归档	您必须 下载 StorageGRID 安装归档并解压缩文件。
服务笔记本电脑	StorageGRID 系统通过服务笔记本电脑进行安装。 服务笔记本电脑必须具有： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器
StorageGRID 文档	• 发行说明 • 有关管理 StorageGRID 的说明

相关信息

"NetApp 互操作性表工具"

下载并提取 **StorageGRID** 安装文件

您必须下载 StorageGRID 安装归档并提取所需文件。

步骤

1. 转至 "StorageGRID 的 "NetApp 下载 " 页面"。
2. 选择用于下载最新版本的按钮，或者从下拉菜单中选择其他版本并选择 * 执行 * 。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 如果显示 Caution/MustRead 语句，请阅读该语句并选中复选框。

安装 StorageGRID 版本后，您必须应用任何所需的修补程序。有关详细信息，请参见 恢复和维护说明中的热修补程序操作步骤。

5. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。
6. 在 * 安装 StorageGRID * 列中，为 Red Hat Enterprise Linux 或 CentOS 选择 .tgz 或 .zip 文件。

   如果您在服务笔记本电脑上运行 Windows ，请选择 ` .zip` 文件。

7. 保存并提取归档文件。
8. 从以下列表中选择所需的文件。

   所需的文件取决于您规划的网格拓扑以及如何部署 StorageGRID 系统。

   表中列出的路径与提取的安装归档所安装的顶级目录相对

路径和文件名	**Description**
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 节点映像。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 主机服务。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	用于 `configure-storaggrid.py` 脚本的空配置文件。

路径和文件名	Description
	用于为 StorageGRID 容器部署配置 RHEL 或 CentOS 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

CPU 和 **RAM** 要求

在安装 StorageGRID 软件之前，请验证并配置硬件，使其可以支持 StorageGRID 系统。

有关受支持服务器的信息，请参见互操作性表。

每个 StorageGRID 节点需要以下最低资源：

- CPU 核心：每个节点 8 个
- RAM ：每个节点至少 24 GB ，比系统总 RAM 少 2 到 16 GB ，具体取决于可用 RAM 总量和系统上运行的非 StorageGRID 软件的数量

确保计划在每个物理或虚拟主机上运行的 StorageGRID 节点数不超过可用的 CPU 核心数或物理 RAM 数。如果主机不是专用于运行 StorageGRID 的（不建议使用），请务必考虑其他应用程序的资源要求。

> 定期监控 CPU 和内存使用情况，以确保这些资源能够持续满足您的工作负载需求。例如，将虚拟存储节点的 RAM 和 CPU 分配增加一倍将提供与为 StorageGRID 设备节点提供的资源类似的资源。此外，如果每个节点的元数据量超过 500 GB ，请考虑将每个节点的 RAM 增加到 48 GB 或更多。有关管理对象元数据存储，增加元数据预留空间设置以及监控 CPU 和内存使用量的信息，请参见有关管理，监控和升级 StorageGRID 的说明。

如果在底层物理主机上启用了超线程功能，则可以为每个节点提供 8 个虚拟核心（ 4 个物理核心）。如果底层物理主机上未启用超线程，则必须为每个节点提供 8 个物理核心。

如果要使用虚拟机作为主机并控制 VM 的大小和数量，则应为每个 StorageGRID 节点使用一个 VM 并相应地调整 VM 的大小。

对于生产部署，不应在同一物理存储硬件或虚拟主机上运行多个存储节点。一个 StorageGRID 部署中的每个存储节点都应位于其各自的隔离故障域中。如果您确保单个硬件故障只会影响单个存储节点，则可以最大限度地提高对象数据的持久性和可用性。

另请参见有关存储要求的信息。

相关信息

"NetApp 互操作性表工具"

存储和性能要求

管理 StorageGRID

监控和故障排除

升级软件

存储和性能要求

您必须了解 StorageGRID 节点的存储要求，以便提供足够的空间来支持初始配置和未来的存储扩展。

StorageGRID 节点需要三种逻辑存储类别：

- * 容器池 * - 节点容器的性能层（ 10K SAS 或 SSD ）存储，在支持 StorageGRID 节点的主机上安装和配置容器引擎时，此存储将分配给容器引擎存储驱动程序。
- * 系统数据 * —性能层（ 10K SAS 或 SSD ）存储，用于按节点永久存储系统数据和事务日志， StorageGRID 主机服务将使用这些存储并将其映射到各个节点。
- * 对象数据 * —性能层（ 10K SAS 或 SSD ）存储和容量层（ NL-SAS/SATA ）批量存储，用于永久存储对象数据和对象元数据。

您必须对所有存储类别使用 RAID 支持的块设备。不支持非冗余磁盘， SSD 或 JBOD 。您可以对任何存储类别使用共享或本地 RAID 存储；但是，如果要使用 StorageGRID 的节点迁移功能，则必须将系统数据和对象数据存储在共享存储上。

性能要求

用于容器池，系统数据和对象元数据的卷的性能会显著影响系统的整体性能。您应对这些卷使用性能层（ 10K SAS 或 SSD ）存储，以确保在延迟，每秒输入 / 输出操作数（ IOPS ）和吞吐量方面具有足够的磁盘性能。您可以使用容量层（ NL-SAS/SATA ）存储来永久存储对象数据。

用于容器池，系统数据和对象数据的卷必须启用回写缓存。缓存必须位于受保护或永久性介质上。

使用**NetApp ONTAP** 存储的主机的要求

如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

所需的主机数

每个 StorageGRID 站点至少需要三个存储节点。

> 在生产部署中，请勿在一个物理或虚拟主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

其他类型的节点（例如管理节点或网关节点）可以部署在同一主机上，也可以根据需要部署在自己的专用主机上。

每个主机的存储卷数量

下表显示了每个主机所需的存储卷（ LUN ）数量以及每个 LUN 所需的最小大小，具体取决于要在该主机上部署的节点。

测试的最大 LUN 大小为 39 TB 。

这些数字适用于每个主机，而不适用于整个网格。

LUN 用途	存储类别	**LUN** 数量	最小大小 **/LUN**
容器引擎存储池	容器池	1.	节点总数 × 100 GB
` /var/local` 卷	系统数据	此主机上的每个节点 1 个	90 GB
存储节点	对象数据	此主机上的每个存储节点 3 个 • 注： * 基于软件的存储节点可以包含 1 到 16 个存储卷；建议至少使用 3 个存储卷。	12 TB （ 4 TB/LUN ）请参见 存储节点的存储要求 有关详细信息 …
管理节点审核日志	系统数据	此主机上的每个管理节点 1 个	200 GB
管理节点表	系统数据	此主机上的每个管理节点 1 个	200 GB

根据配置的审核级别， S3 对象密钥名称等用户输入的大小以及需要保留的审核日志数据量，您可能需要增加每个管理节点上的审核日志 LUN 的大小。一般来说，网格在每个 S3 操作中生成大约 1 KB 的审核数据，这意味着 200 GB 的 LUN 每天支持 7 ， 000 万次操作，或者每秒 800 次操作，持续 2 到 3 天。

主机的最小存储空间

下表显示了每种类型的节点所需的最小存储空间。您可以使用此表根据要在每个存储类别中部署的节点确定必须为主机提供的最小存储量。

磁盘快照不能用于还原网格节点。请参阅每种类型节点的恢复和维护过程。

节点类型	容器池	系统数据	对象数据
存储节点	100 GB	90 GB	4 ， 000 GB
管理节点	100 GB	490 GB （ 3 个 LUN ）	_ 不适用 _

节点类型	容器池	系统数据	对象数据
网关节点	100 GB	90 GB	_ 不适用 _
归档节点	100 GB	90 GB	_ 不适用 _

示例：计算主机的存储要求

假设您计划在同一主机上部署三个节点：一个存储节点，一个管理节点和一个网关节点。您应至少为主机提供九个存储卷。节点容器至少需要 300 GB 的性能层存储，系统数据和事务日志至少需要 6.7 GB 的性能层存储，对象数据至少需要 12 TB 的容量层存储。

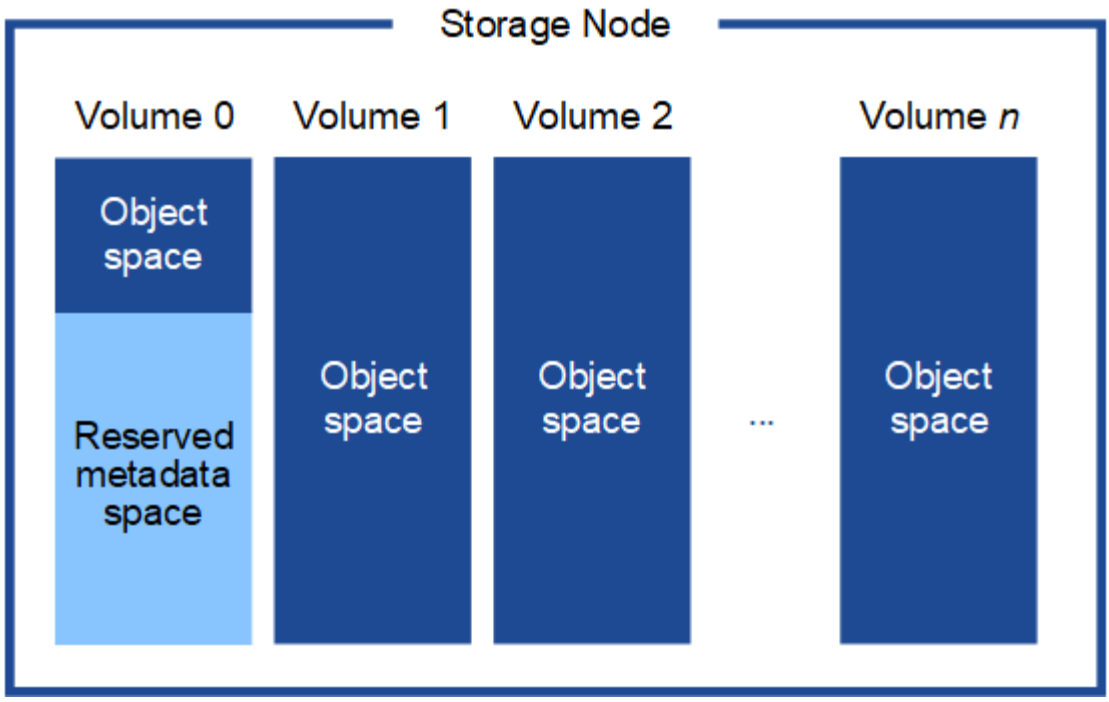
节点类型	**LUN** 用途	**LUN** 数量	**LUN** 大小
存储节点	容器引擎存储池	1.	300 GB （ 100 GB/ 节点 ）
存储节点	` /var/local` 卷	1.	90 GB
存储节点	对象数据	3.	12 TB （ 4 TB/LUN ）
管理节点	` /var/local` 卷	1.	90 GB
管理节点	管理节点审核日志	1.	200 GB
管理节点	管理节点表	1.	200 GB
网关节点	` /var/local` 卷	1.	90 GB
• 总计 *		**9**	• 容器池： * 300 GB • 系统数据： * 670GB • 对象数据： * 12 ，000 GB

存储节点的存储要求

一个基于软件的存储节点可以包含 1 到 16 个存储卷—建议使用 3 个或更多存储卷。每个存储卷应大于或等于 4 TB 。

一个设备存储节点最多可以包含 48 个存储卷。

如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。存储卷 0 和存储节点中的任何其他存储卷上的任何剩余空间专用于对象数据。



为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。对象元数据的三个副本均匀分布在每个站点的所有存储节点上。

在为新存储节点的卷 0 分配空间时，必须确保为该节点在所有对象元数据中的部分分配足够的空间。

- 您必须至少为卷 0 分配 4 TB 。

> 如果一个存储节点仅使用一个存储卷，而为该卷分配的存储空间不超过 4 TB ，则该存储节点可能会在启动时进入存储只读状态，并仅存储对象元数据。

- 如果要安装新的 StorageGRID 11.6 系统，并且每个存储节点的 RAM 为 128 GB 或更大，则应为卷 0 分配 8 TB 或更多。如果对卷 0 使用较大的值，则可以增加每个存储节点上允许的元数据空间。
- 在为站点配置不同的存储节点时，如果可能，请对卷 0 使用相同的设置。如果某个站点包含不同大小的存储节点，卷 0 最小的存储节点将确定该站点的元数据容量。

有关详细信息，请转至 管理对象元数据存储。

相关信息

节点容器迁移要求

恢复和维护

节点容器迁移要求

通过节点迁移功能，您可以手动将节点从一台主机移动到另一台主机。通常，两台主机位于同一物理数据中心。

通过节点迁移，您可以在不中断网格操作的情况下执行物理主机维护。您只需逐个将所有 StorageGRID 节点移动到另一台主机，然后再使物理主机脱机。迁移节点只需要每个节点短暂停机，不应影响网格服务的运行或可用性。

如果要使用 StorageGRID 节点迁移功能，则部署必须满足其他要求：

- 在一个物理数据中心的主机之间使用一致的网络接口名称
- StorageGRID 元数据和对象存储库卷的共享存储，可由单个物理数据中心中的所有主机访问。例如，您可以使用 NetApp E 系列存储阵列。

如果您使用的是虚拟主机，并且底层虚拟机管理程序层支持 VM 迁移，则可能需要使用此功能，而不是 StorageGRID 的节点迁移功能。在这种情况下，您可以忽略这些附加要求。

在执行迁移或虚拟机管理程序维护之前，请正常关闭节点。请参见的说明 关闭网格节点。

不支持 **VMware** 实时迁移

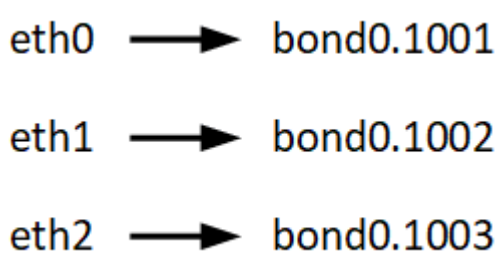
OpenStack 实时迁移和 VMware 实时 vMotion 发生原因 虚拟机时钟跳转时间，不支持任何类型的网格节点。尽管时钟时间不正确，但极少会导致数据丢失或配置更新。

支持冷迁移。在冷迁移中，您需要先关闭 StorageGRID 节点，然后再在主机之间迁移它们。请参见的说明 关闭网格节点。

网络接口名称一致

为了将节点从一台主机移动到另一台主机， StorageGRID 主机服务需要一定程度地确信该节点在其当前位置的外部网络连接可以在新位置进行复制。它可以通过在主机中使用一致的网络接口名称来获得这种信心。

例如，假设主机 1 上运行的 StorageGRID 节点 A 已配置以下接口映射：



箭头的左侧对应于从 StorageGRID 容器中查看的传统接口（即网格接口，管理接口和客户端网络接口）。箭头的右侧对应于提供这些网络的实际主机接口，它们是同一物理接口绑定下的三个 VLAN 接口。

现在，假设您要将节点 A 迁移到 Host2 。如果 Host2 还具有名为 bond0.1001 ， bond0.1002 和 bond0.1003 的接口，则系统将允许移动，前提是同名接口在 Host2 上提供的连接与在 Host1 上提供的连接相同。如果 Host2 的接口名称不相同，则不允许移动。

可以通过多种方法在多个主机之间实现一致的网络接口命名；请参见 配置主机网络 例如。

共享存储

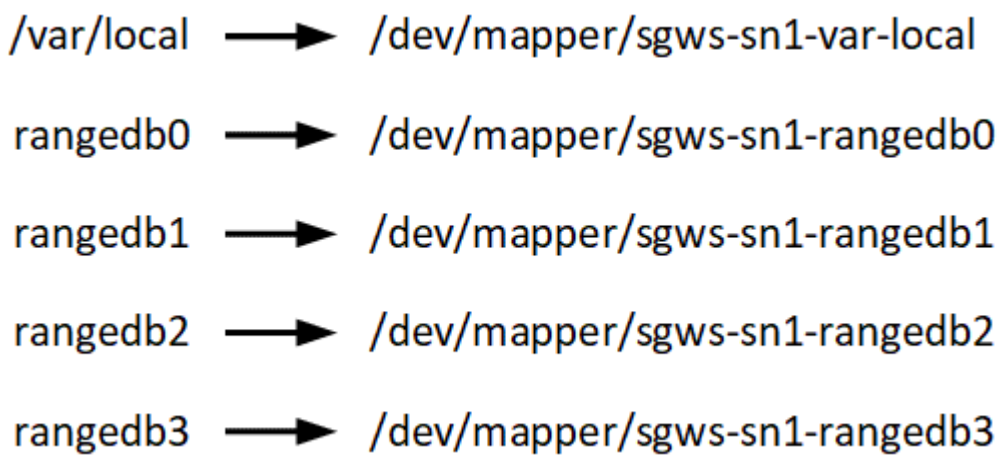
为了实现快速，低开销的节点迁移， StorageGRID 节点迁移功能不会物理移动节点数据。而是将节点迁移作为一对导出和导入操作来执行，如下所示：

1. 在 "`node export` " 操作期间，会从主机 A 上运行的节点容器中提取少量永久性状态数据，并将其缓存在该节点的系统数据卷上。然后，将对 HostA 上的节点容器进行实例化。
2. 在 "`node import` " 操作期间，系统将实例化 HostB 上使用与 HostA 相同的网络接口和块存储映射的节点容

器。然后，缓存的永久性状态数据将插入到新实例中。

在这种操作模式下，节点的所有系统数据和对象存储卷都必须可从主机 A 和主机 B 访问，才能允许迁移并正常运行。此外，它们必须已使用名称映射到节点，这些名称可以保证引用主机 A 和主机 B 上的相同 LUN 。

以下示例显示了一个解决方案 ，用于 StorageGRID 存储节点的块设备映射，其中主机正在使用 DM 多路径，并且在 ` /etc/multipath.conf` 中使用了 alias 字段，以提供所有主机上可用的一致且友好的块设备名称。



部署工具

自动执行全部或部分 StorageGRID 安装可能会让您受益匪浅。

在以下任一情况下，自动部署可能会很有用：

- 您已使用标准业务流程框架（例如 Ansible ， Puppet 或 Chef ）部署和配置物理或虚拟主机。
- 您打算部署多个 StorageGRID 实例。
- 您正在部署一个大型的复杂 StorageGRID 实例。

StorageGRID 主机服务由软件包安装，并由配置文件驱动，这些配置文件可以在手动安装期间以交互方式创建，也可以提前准备（或以编程方式），以便使用标准业务流程框架实现自动安装。StorageGRID 提供了可选的 Python 脚本，用于自动配置 StorageGRID 设备和整个 StorageGRID 系统（ "`grid` " ）。您可以直接使用这些脚本，也可以检查它们以了解如何使用 StorageGRID 安装 REST API 在网格部署和配置工具中，您可以自行开发。

如果您希望自动执行全部或部分 StorageGRID 部署，请查看 自动安装 开始安装过程之前。

准备主机（ **Red Hat** 或 **CentOS** ）

安装 **Linux**

您必须在所有网格主机上安装 Linux 。使用 "NetApp 互操作性表工具" 以获取支持的版本列表。

步骤

1. 按照分销商的说明或您的标准操作步骤 在所有物理或虚拟网格主机上安装 Linux 。

如果您使用的是标准 Linux 安装程序， NetApp 建议选择 "`compute node` " 软件配置（如果可用）或 " `minimal install` " 基础环境。请勿安装任何图形桌面环境。

2. 确保所有主机均可访问软件包存储库，包括其他通道。

   您可能需要在此安装操作步骤 中稍后再安装这些附加软件包。

3. 如果已启用交换：

   a. 运行以下命令： ` $sudo swapoff -all`

   b. 从 ` /etc/fstab` 中删除所有交换条目以保留这些设置。

   如果未完全禁用交换，则会严重降低性能。

配置主机网络（ **Red Hat Enterprise Linux** 或 **CentOS** ）

在主机上完成 Linux 安装后，您可能需要执行一些额外的配置，以便在每个主机上准备一组适合映射到稍后要部署的 StorageGRID 节点的网络接口。

您需要的内容

- 您已查看 StorageGRID 网络连接准则。
- 您已查看有关的信息 节点容器迁移要求。
- 如果您使用的是虚拟主机，则已阅读 MAC 地址克隆的注意事项和建议 配置主机网络之前。

如果要使用 VM 作为主机，则应选择 VMXNET 3 作为虚拟网络适配器。VMware E1000 网络适配器已导致在某些 Linux 版本上部署 StorageGRID 容器时出现连接问题。

关于此任务

网格节点必须能够访问网格网络，还可以访问管理网络和客户端网络。您可以通过创建映射来提供此访问权限，此映射会将主机的物理接口与每个网格节点的虚拟接口相关联。创建主机接口时，请使用友好名称以方便在所有主机之间进行部署，并启用迁移。

同一接口可以在主机与一个或多个节点之间共享。例如，您可以使用相同的接口进行主机访问和节点管理网络访问，以便于维护主机和节点。尽管主机和各个节点之间可以共享同一接口，但所有接口都必须具有不同的 IP 地址。不能在节点之间或主机与任何节点之间共享 IP 地址。

您可以使用相同的主机网络接口为主机上的所有 StorageGRID 节点提供网格网络接口；可以为每个节点使用不同的主机网络接口；也可以在这两者之间执行操作。但是，通常不会提供与单个节点的网格和管理网络接口相同的主机网络接口，也不会提供与一个节点的网格网络接口和另一个节点的客户端网络接口相同的主机网络接口。

您可以通过多种方式完成此任务。例如，如果您的主机是虚拟机，而您要为每个主机部署一个或两个 StorageGRID 节点，则只需在虚拟机管理程序中创建正确数量的网络接口并使用一对一映射即可。如果要在裸机主机上部署多个节点以供生产使用，则可以利用 Linux 网络堆栈对 VLAN 和 LACP 的支持来实现容错和带宽共享。以下各节详细介绍了这两个示例的方法。您无需使用上述任一示例；您可以使用任何满足您需求的方法。

请勿直接使用绑定或网桥设备作为容器网络接口。这样做可能会阻止内核问题描述 在容器命名空间中对绑定和网桥设备使用 MACVLAN 导致节点启动。请改用非绑定设备，例如 VLAN 或虚拟以太网（ Veth ）对。在节点配置文件中指定此设备作为网络接口。

相关信息

正在创建节点配置文件

MAC 地址克隆的注意事项和建议

【mac_address_cloning_rhel]]

MAC 地址克隆会使容器使用主机的 MAC 地址，而主机则使用您指定的地址或随机生成的地址的 MAC 地址。您应使用 MAC 地址克隆来避免使用混杂模式网络配置。

启用 MAC 克隆

在某些环境中，可以通过 MAC 地址克隆来增强安全性，因为它使您可以对管理网络，网格网络和客户端网络使用专用虚拟 NIC 。让容器使用主机上专用 NIC 的 MAC 地址可以避免使用混杂模式网络配置。

MAC 地址克隆用于安装虚拟服务器，可能无法在所有物理设备配置中正常运行。

如果某个节点由于 MAC 克隆目标接口繁忙而无法启动，则在启动节点之前，您可能需要将链路设置为 " 关闭 " 。此外，在链路启动时，虚拟环境可能会阻止网络接口上的 MAC 克隆。如果某个节点由于接口繁忙而无法设置 MAC 地址并启动，则在启动该节点之前将链路设置为 " 关闭 " 可能会修复问题描述 。

默认情况下， MAC 地址克隆处于禁用状态，必须通过节点配置密钥进行设置。您应在安装 StorageGRID 时启用它。

每个网络有一个密钥：

- `admin_network_target_type_interface_clone_MAC`
- `grid_network_target_type_interface_clone_MAC`
- `client_network_target_type_interface_clone_MAC`

如果将密钥设置为 "true" ，则容器将使用主机 NIC 的 MAC 地址。此外，主机将使用指定容器网络的 MAC 地址。默认情况下，容器地址是随机生成的地址，但如果您使用 ` _network_MAC` 节点配置密钥设置了一个地址，则会改用该地址。主机和容器始终具有不同的 MAC 地址。

在虚拟主机上启用 MAC 克隆而不同时在虚拟机管理程序上启用混杂模式可能会使用主机的接口发生原因 Linux 主机网络连接停止工作。

Mac 克隆使用情形

MAC 克隆需要考虑两种使用情形：

- 未启用 MAC 克隆：如果节点配置文件中的 ` clone_mac` 密钥未设置或设置为 "false" ，则主机将使用主机 NIC MAC ，并且容器将具有 StorageGRID 生成的 MAC ，除非在 ` _network_mac` 密钥中指定了 MAC 。如果在 ` _network_MAC` 项中设置了地址，则容器将具有在 ` _network_MAC` 项中指定的地址。此密钥配置要求使用混杂模式。
- 已启用 MAC 克隆：如果节点配置文件中的 ` clone_mac` 密钥设置为 "true" ，则容器将使用主机 NIC MAC ，而主机将使用 StorageGRID 生成的 MAC ，除非在 ` _network_mac` 密钥中指定了 MAC 。如果在 ` _network_MAC` 项中设置了地址，则主机将使用指定的地址，而不是生成的地址。在此密钥配置中，不应使用混杂模式。

如果您不希望使用 MAC 地址克隆，而希望允许所有接口接收和传输非虚拟机管理程序分配的 MAC 地址的数据， 对于配置模式， MAC 地址更改和伪造传输，请确保虚拟交换机和端口组级别的安全属性设置为 * 接受 * 。虚拟交换机上设置的值可以被端口组级别的值覆盖，因此请确保这两个位置的设置相同。

要启用 MAC 克隆，请参见 有关创建节点配置文件的说明。

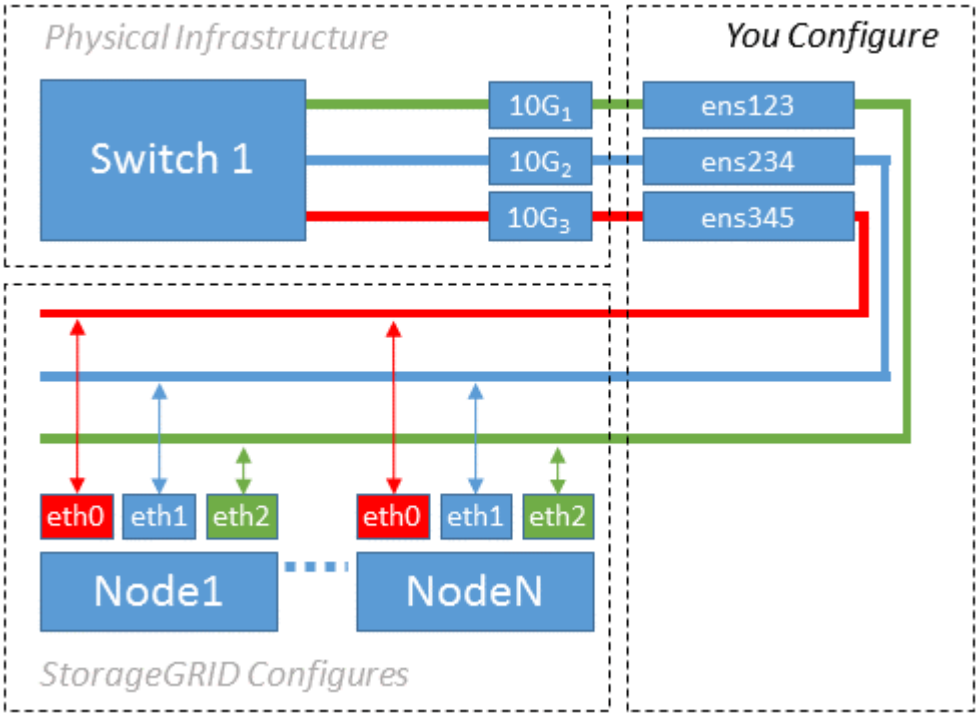
Mac 克隆示例

在 MAC 地址为 11： 22： 33： 44： 55： 66 的主机上为接口 ens256 启用 MAC 克隆的示例，以及节点配置文件中的以下密钥：

- `admin_network_target = ens256`
- `admin_network_MAC = B2 ： 9c ： 02 ： C2 ： 27 ： 10`
- `admin_network_target_type_interface_clone_MAC = true`
- 结果 * ： ens256 的主机 MAC 为 B2： 9c： 02： C2： 27： 10 ，管理网络 MAC 为 11： 22： 33： 44： 55： 66

示例 **1** ： 映射到物理或虚拟 **NIC** 的一对一映射

示例 1 介绍了一个简单的物理接口映射，该映射只需要很少的主机端配置或根本不需要主机端配置。



在安装或启动期间或热添加接口时， Linux 操作系统会自动创建 `ensXYZ` 接口。除了确保接口设置为在启动后自动启动之外，无需进行任何配置。您必须确定哪个 `ensXYZ` 对应于哪个 StorageGRID 网络（网格，管理员或客户端），以便稍后在配置过程中提供正确的映射。

请注意，此图显示了多个 StorageGRID 节点；但是，通常情况下，您会对单节点 VM 使用此配置。

如果交换机 1 是物理交换机，则应将连接到接口 10G1 到 10G3 的端口配置为访问模式，并将其放置在相应的

VLAN 上。

示例 2： LACP 绑定传输 VLAN

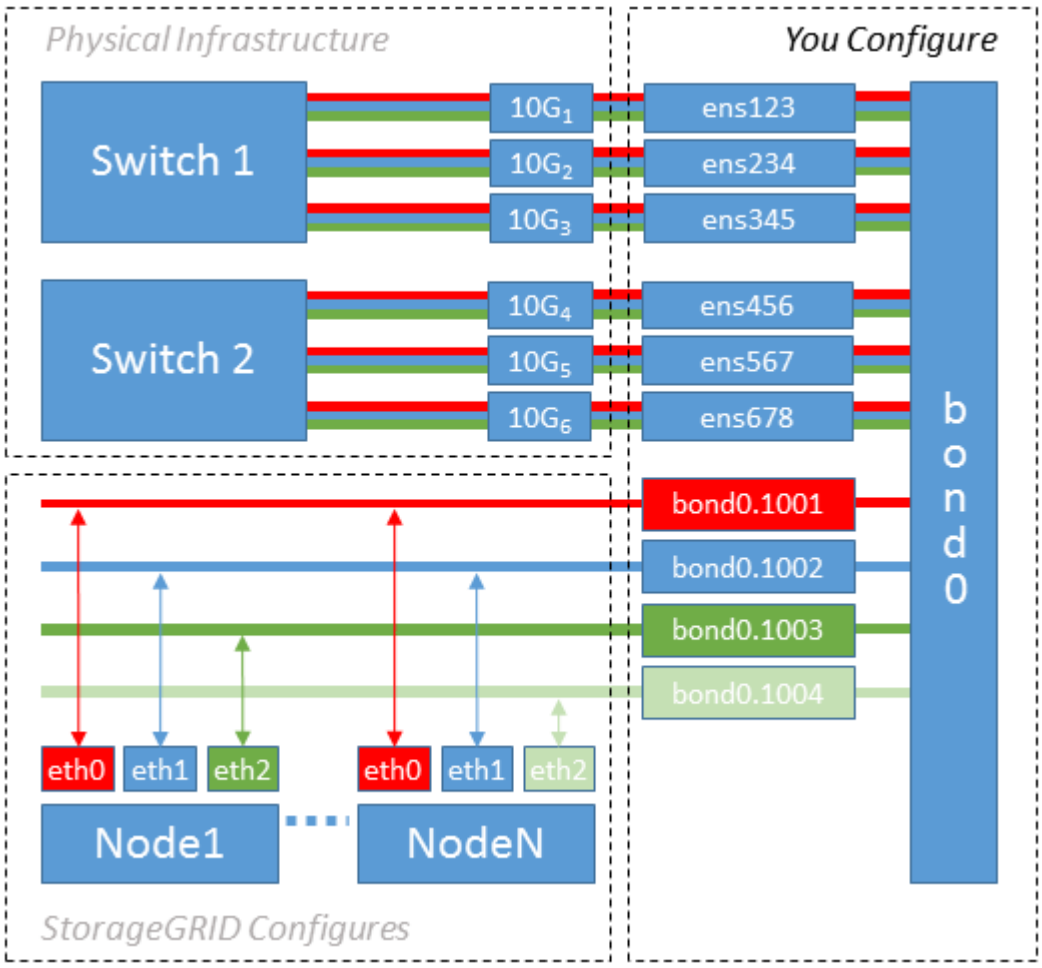
关于此任务

示例 2 假定您熟悉绑定网络接口以及在所使用的 Linux 分发版上创建 VLAN 接口。

示例 2 介绍了一种基于 VLAN 的通用灵活方案，该方案有助于在单个主机上的所有节点之间共享所有可用网络带宽。此示例尤其适用于裸机主机。

要了解此示例，假设每个数据中心有三个单独的网格网络，管理员网络和客户端网络子网。子网位于不同的 VLAN （ 1001 ， 1002 和 1003 ）上，并通过 LACP 绑定的中继端口（ bond0 ）提供给主机。您应在此绑定上配置三个 VLAN 接口： bond0.1001 ， bond0.1002 和 bond0.1003 。

如果同一主机上的节点网络需要单独的 VLAN 和子网，则可以在绑定上添加 VLAN 接口并将其映射到主机（如图中的 bond0.1004 所示）。



步骤

1. 将用于 StorageGRID 网络连接的所有物理网络接口聚合到一个 LACP 绑定中。

   对每个主机上的绑定使用相同的名称。例如， `bond0` 。

2. 使用标准 VLAN 接口命名约定 `physdev-name.vlan ID` 创建使用此绑定作为关联 "`物理设备，` " 的 VLAN 接口。

请注意，步骤 1 和 2 要求对终止网络链路另一端的边缘交换机进行适当配置。此外，边缘交换机端口还必须聚合到 LACP 端口通道中，并配置为中继，并允许通过所有必需的 VLAN 。

本文档提供了此每主机网络配置方案的示例接口配置文件。

相关信息

示例 /etc/sysconfig/network-scripts

配置主机存储

您必须为每个主机分配块存储卷。

您需要的内容

您已阅读以下主题，其中提供了完成此任务所需的信息：

存储和性能要求

节点容器迁移要求

关于此任务

在将块存储卷（ LUN ）分配给主机时，请使用 s存储要求 中的表确定以下内容：

- 每个主机所需的卷数（根据要在该主机上部署的节点的数量和类型）
- 每个卷的存储类别（即系统数据或对象数据）
- 每个卷的大小

在主机上部署 StorageGRID 节点时，您将使用此信息以及 Linux 为每个物理卷分配的永久性名称。

您无需对其中任何卷进行分区，格式化或挂载；您只需确保这些卷对主机可见即可。

在编写卷名称列表时，请避免使用 "`raw` " 特殊设备文件（例如，` /dev/sdb` ）。这些文件可能会在主机重新启动后发生更改，从而影响系统的正常运行。如果您使用的是 iSCSI LUN 和设备映射程序多路径，请考虑在 ` /dev/mapper` 目录中使用多路径别名，尤其是在 SAN 拓扑包含指向共享存储的冗余网络路径时。或者，您也可以在 ` /dev/disk/by-path/` 下使用系统创建的软链接作为永久性设备名称。

例如：

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

每个安装的结果会有所不同。

为每个块存储卷分配友好名称，以简化初始 StorageGRID 安装和未来维护过程。如果使用设备映射程序多路径驱动程序对共享存储卷进行冗余访问，则可以在 ` /etc/multipath.conf` 文件中使用 `alias` 字段。

例如：

```
multipaths {
      multipath {
            wwid 3600a09800059d6df00005df2573c2c30
            alias docker-storage-volume-hostA
      }
      multipath {
            wwid 3600a09800059d6df00005df3573c2c30
            alias sgws-adm1-var-local
      }
      multipath {
            wwid 3600a09800059d6df00005df4573c2c30
            alias sgws-adm1-audit-logs
      }
      multipath {
            wwid 3600a09800059d6df00005df5573c2c30
            alias sgws-adm1-tables
      }
      multipath {
            wwid 3600a09800059d6df00005df6573c2c30
            alias sgws-gw1-var-local
      }
      multipath {
            wwid 3600a09800059d6df00005df7573c2c30
            alias sgws-sn1-var-local
      }
      multipath {
            wwid 3600a09800059d6df00005df7573c2c30
            alias sgws-sn1-rangedb-0
      }
      …
```

这样就会对别名进行发生原因，使其显示为主机上的 ` /dev/mapper` 目录中的块设备，从而可以在配置或维护操作需要指定块存储卷时指定一个易于验证的友好名称。

> 如果要设置共享存储以支持 StorageGRID 节点迁移并使用设备映射程序多路径功能，则可以在所有主机上创建并安装通用的 ` /etc/multipath.conf` 。只需确保在每个主机上使用不同的容器引擎存储卷即可。使用别名并将目标主机名包含在每个容器引擎存储卷 LUN 的别名中，这样便于记住，建议这样做。

相关信息

配置容器引擎存储卷

在安装容器引擎（ Docker 或 Podman ）之前，您可能需要格式化存储卷并将其挂载。

关于此任务

如果您计划对 Docker 或 Podman 存储卷使用本地存储，并且在包含适用于 Docker 的 ` /var/lib/Docker` 和适用于 Podman 的 ` /var/lib/containers` 的主机分区上有足够的可用空间，则可以跳过这些步骤。

只有 Red Hat Enterprise Linux （ RHEL ）才支持 Podman 。

步骤

1. 在容器引擎存储卷上创建文件系统：

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. 挂载容器引擎存储卷：
   - 对于 Docker ：

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - 对于 Podman ：

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. 将 container-storage-volume-device 的条目添加到 /etc/fstab 中。

   此步骤可确保存储卷将在主机重新启动后自动重新挂载。

安装 **Docker**

StorageGRID 系统作为一组容器在 Red Hat Enterprise Linux 或 CentOS 上运行。如果您已选择使用 Docker 容器引擎，请按照以下步骤安装 Docker 。否则， 安装 Podman。

步骤

1. 按照适用于您的 Linux 版本的说明安装 Docker 。

   如果您的 Linux 分发版不包含 Docker ，您可以从 Docker 网站下载它。

2. 运行以下两个命令，确保已启用并启动 Docker ：

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 输入以下命令确认您已安装预期版本的 Docker：

```
sudo docker version
```

客户端和服务器版本必须为 1.11.0 或更高版本。

安装 **Podman**

StorageGRID 系统作为一组容器在 Red Hat Enterprise Linux 上运行。如果您已选择使用 Podman 容器引擎，请按照以下步骤安装 Podman 。否则， 安装 Docker。

只有 Red Hat Enterprise Linux （ RHEL ）才支持 Podman 。

步骤

1. 按照适用于您的 Linux 版本的说明安装 Podman 和 Podman-Docker 。

安装 Podman 时，您还必须安装 Podman-Docker 软件包。

2. 输入以下命令，确认您已安装所需的 Podman 和 Podman-Docker 版本：

```
sudo docker version
```

通过 Podman-Docker 软件包，您可以使用 Docker 命令。

客户端和服务器版本必须为 3.2.3 或更高版本。

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

安装 **StorageGRID** 主机服务

您可以使用 StorageGRID RPM 软件包安装 StorageGRID 主机服务。

关于此任务

以下说明介绍如何从 RPM 软件包安装主机服务。或者，您也可以使用安装归档中包含的 Yum 存储库元数据远程安装 RPM 软件包。请参见适用于 Linux 操作系统的 Yum 存储库说明。

步骤

1. 将 StorageGRID RPM 软件包复制到每个主机，或使其在共享存储上可用。

例如，将其放置在 ` /tmp` 目录中，以便您可以在下一步中使用示例命令。

2. 以 root 身份或使用具有 sudo 权限的帐户登录到每个主机，然后按指定顺序运行以下命令：

```
sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
```

您必须先安装映像软件包，然后再安装服务软件包。

如果您将软件包放置在非 ` /tmp` 目录中，请修改命令以反映您使用的路径。

部署虚拟网格节点（ **Red Hat** 或 **CentOS** ）

为 **Red Hat Enterprise Linux** 或 **CentOS** 部署创建节点配置文件

节点配置文件是一个小型文本文件，用于提供 StorageGRID 主机服务启动节点并将其连接到适当的网络和块存储资源所需的信息。节点配置文件用于虚拟节点，不用于设备节点。

应将节点配置文件放在何处?

您必须将每个 StorageGRID 节点的配置文件放置在要运行该节点的主机上的 ` /etc/storaggrid/nodes` 目录中。例如，如果您计划在主机 A 上运行一个管理节点，一个网关节点和一个存储节点，则必须将三个节点配置文件放置在主机 A 上的 ` /etc/storaggrid/nodes` 中。您可以使用文本编辑器（例如 vim 或 nanan ）在每个主机上直接创建配置文件，也可以在其他位置创建配置文件并将其移动到每个主机。

节点配置文件的名称是什么?

配置文件的名称非常重要。格式为 `node-name.conf` ，其中 `node-name` 是您分配给节点的名称。此名称显示在 StorageGRID 安装程序中，用于节点维护操作，例如节点迁移。

节点名称必须遵循以下规则：

- 必须是唯一的
- 必须以字母开头
- 可以包含字符 A 到 Z 和 a 到 z
- 可以包含数字 0 到 9
- 可以包含一个或多个连字符（ - ）
- 不得超过 32 个字符，不包括 ` 。 conf` 扩展名

主机服务不会解析 ` /etc/storaggrid/nodes` 中不符合这些命名约定的任何文件。

如果您为网格规划了多站点拓扑，则典型的节点命名方案可能是：

```
site-nodetype-nodenumber.conf
```

例如，您可以对 Data Center 1 中的第一个管理节点使用 `dc1-adm1.conf` ，而对 Data Center 2 中的第三个存储节点使用 `dc2-SN3.conf` 。但是，只要所有节点名称都遵循命名规则，您就可以使用所需的任何方案。

节点配置文件中的内容是什么？

配置文件包含密钥 / 值对，每行一个密钥和一个值。对于每个密钥 / 值对，您必须遵循以下规则：

- 密钥和值必须以等号（` =` ）和可选空格分隔。
- 密钥不能包含空格。
- 这些值可以包含嵌入的空格。
- 忽略任何前导或尾随空格。

每个节点都需要一些密钥，而其他密钥则是可选的，或者仅适用于某些节点类型。

下表定义了所有支持的密钥的可接受值。在中间列中：

- R* ： 必填项 + bp ： 最佳实践 + O ： 可选

密钥	**R** ， **Bp** 或 **O** ？	价值
admin_ip	bp	此节点所属网格的主管理节点的网格网络 IPv4 地址。使用为 node_type = VM_Admin_Node 且 admin_role = Primary 的网格节点的 grid_network_IP 指定的相同值。如果省略此参数，则节点将尝试使用 mDNS 发现主管理节点。 网格节点如何发现主管理节点 • 注 * ： 此值在主管理节点上被忽略，并且可能被禁止。
admin_network_config	O	DHCP ，静态或已禁用
admin_network_esl	O	此节点应通过管理网络网关与 CIDR 表示法中的子网列表，以逗号分隔。 示例： `172.16.0.0/21.172.17.0.0/21`

密钥	**R** ， **Bp** 或 **O** ？	价值

admin_network_gateway	O （ * R* ）	此节点的本地管理网络网关的 IPv4 地址。必须位于 admin_network_ip 和 admin_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。
		
		• 注释 * ： 如果指定 admin_network_esl ，则需要此参数。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

admin_network_ip	O	此节点在管理网络上的 IPv4 地址。只有当 admin_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

admin_network_MAC	O	容器中管理网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `B2 ： 9c ： 02 ： C2 ： 27 ： 10`

admin_network_mask	O	此节点的 IPv4 网络掩码，位于管理网络上。只有当 admin_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`255.255.255.0`
		
		`255.255.248.0`

密钥	**R** ， **Bp** 或 **O** ？	价值

admin_network_mtu	O	管理网络上此节点的最大传输单元（ MTU ）。请勿指定 admin_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
		
		如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
		
		• 重要信息 *： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
		
		示例
		
		`1500`
		
		`8192`

admin_network_target	bp	StorageGRID 节点用于管理网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 grid_network_target 或 client_network_target 指定的接口名称不同。
		
		• 注 *： 请勿使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
		• 最佳实践 *： 指定一个值，即使此节点最初不具有管理员网络 IP 地址也是如此。然后，您可以稍后添加管理员网络 IP 地址，而无需重新配置主机上的节点。
		
		示例
		
		`bond0.1002`
		
		`ens256`

admin_network_target_type	O	接口 （这是唯一受支持的值。）

密钥	R ， Bp 或 O ？	价值
admin_network_target_type_interface_clone_MAC	bp	判断对错 将密钥设置为 "true" 以发生原因 StorageGRID 容器使用管理网络上主机主机目标接口的 MAC 地址。 • 最佳实践： * 在需要混杂模式的网络中，请改用 admin_network_target_type_interface_clone_MAC 密钥。 有关 MAC 克隆的详细信息，请参见： MAC 地址克隆的注意事项和建议（ Red Hat Enterprise Linux 或 CentOS ） MAC 地址克隆（ Ubuntu 或 Debian ）的注意事项和建议
管理角色	• R*	主卷或非主卷 只有当 node_type = VM_Admin_Node 时才需要此密钥；不要为其他节点类型指定此密钥。

block_device_audit_logs	• R*	此节点将用于永久存储审核日志的块设备专用文件的路径和名称。只有 node_type = VM_Admin_Node 的节点才需要此密钥；不要为其他节点类型指定此密钥。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-ad1-audit-logs`

密钥	R ， Bp 或 O ？	价值

block_device_RANGEDB_000
 	
block_device_RANGEDB_001
 	
block_device_RANGEDB_002
 	
block_device_RANGEDB_003
 	
block_device_RANGEDB_004
 	
block_device_RANGEDB_005
 	
block_device_RANGEDB_006
 	
block_device_RANGEDB_007
 	
block_device_RANGEDB_008
 	
block_device_RANGEDB_009
 	
block_device_RANGEDB_010
 	
block_device_RANGEDB_011
 	
block_device_RANGEDB_012
 	
block_device_RANGEDB_013
 	
block_device_RANGEDB_014
 	
block_device_RANGEDB_015
	• R*	此节点将用于永久性对象存储的块设备专用文件的路径和名称。只有 node_type = VM_Storage_Node 的节点才需要此密钥；不要为其他节点类型指定此密钥。
		
		仅需要 block_device_RANGEDB_000 ；其余为可选。为 block_device_RANGEDB_000 指定的块设备必须至少为 4 TB ；其他块设备可以更小。
		
		请勿留下空隙。如果指定 block_device_RANGEDB_005 ，则还必须指定 block_device_RANGEDB_004 。
		
		• 注 * ： 为了与现有部署兼容，升级后的节点支持两位数的密钥。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-SN1-rangedb-000`

密钥	R ， Bp 或 O ？	价值

block_device_tables	• R*	此节点将用于永久存储数据库表的块设备专用文件的路径和名称。只有 node_type = VM_Admin_Node 的节点才需要此密钥；不要为其他节点类型指定此密钥。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-ad1-tables`

block_device_var_local	• R*	此节点将用于其 /var/local 永久性存储的块设备专用文件的路径和名称。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-SN1-var-local`

client_network_config	O	DHCP ，静态或已禁用

client_network_gateway	O	此节点的本地客户端网络网关的 IPv4 地址，该地址必须位于 client_network_ip 和 client_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

client_network_IP	O	此节点在客户端网络上的 IPv4 地址。只有当 client_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

密钥	**R** ， **Bp** 或 **O** ？	价值
客户端网络 MAC	O	容器中客户端网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `B2 ： 9c ： 02 ： C2 ： 27 ： 20`

client_network_mask	O	此节点在客户端网络上的 IPv4 网络掩码。只有当 client_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`255.255.255.0`
		
		`255.255.248.0`

client_network_mtu	O	客户端网络上此节点的最大传输单元（ MTU ）。请勿指定 client_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
		
		如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
		
		• 重要信息 *： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
		
		示例
		
		`1500`
		
		`8192`

密钥	**R** ， **Bp** 或 **O** ？	价值

client_network_target	bp	StorageGRID 节点用于客户端网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 grid_network_target 或 admin_network_target 指定的接口名称不同。
		
		• 注 * ：请勿使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
		• 最佳实践： * 指定一个值，即使此节点最初不会具有客户端网络 IP 地址也是如此。然后，您可以稍后添加客户端网络 IP 地址，而无需重新配置主机上的节点。
		
		示例
		
		`bond0.1003`
		
		`ens423`

client_network_target_type	O	接口 （此值仅受支持。）
client_network_target_type_interface_clone_MAC	bp	判断对错 将密钥设置为 "true" ，以便对 StorageGRID 容器进行发生原因 处理，以使用客户端网络上主机目标接口的 MAC 地址。 • 最佳实践： * 在需要混杂模式的网络中，请改用 client_network_target_type_interface_clone_MAC 密钥。 有关 MAC 克隆的详细信息，请参见： MAC 地址克隆的注意事项和建议（ Red Hat Enterprise Linux 或 CentOS ） MAC 地址克隆（ Ubuntu 或 Debian ）的注意事项和建议
grid_network_config	bp	静态或 DHCP （如果未指定，则默认为 static 。）

密钥	**R** ， **Bp** 或 **O** ？	价值
grid_network_gateway	• R*	此节点的本地网格网络网关的 IPv4 地址，该网关必须位于 grid_network_ip 和 grid_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。 如果网格网络是没有网关的单个子网，请使用该子网的标准网关地址（ X.y.Z.1 ）或此节点的 GRID_NETWORK_IP 值；任一值都将简化未来可能进行的网格网络扩展。

GRID_NETWORK_IP	• R*	此节点在网格网络上的 IPv4 地址。只有当 grid_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

GRID_NETWORK_MAC	O	容器中网格网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例：`B2 ： 9c ： 02 ： C2 ： 27 ： 30`

grid_network_mask	O	此节点在网格网络上的 IPv4 网络掩码。只有当 grid_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`255.255.255.0`
		
		`255.255.248.0`

密钥	**R** ， **Bp** 或 **O** ？	价值
grid_network_mtu	O	网格网络上此节点的最大传输单元（ MTU ）。请勿指定 grid_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。 如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。 • 重要信息 *： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。 • 重要信息 *： 为获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。 示例 1500 8192

grid_network_target	• R*	StorageGRID 节点要用于网格网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 admin_network_target 或 client_network_target 指定的接口名称不同。
		
		• 注 *： 请勿使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
		
		示例
		
		`bond0.1001`
		
		`ens192`

grid_network_target_type	O	接口 （这是唯一受支持的值。）

密钥	**R** ， **Bp** 或 **O** ？	价值
grid_network_target_type_interface_clone_MAC	• bp*	判断对错 将密钥值设置为 "true" ，以便对 StorageGRID 容器进行发生原因 处理，以使用网格网络上主机目标接口的 MAC 地址。 • 最佳实践： * 在需要混杂模式的网络中，请改用 grid_network_target_type_interface_clone_MAC 密钥。 有关 MAC 克隆的详细信息，请参见： MAC 地址克隆的注意事项和建议（ Red Hat Enterprise Linux 或 CentOS ） MAC 地址克隆（ Ubuntu 或 Debian ）的注意事项和建议
interfaces_target_nnnn	O	要添加到此节点的额外接口的名称和可选问题描述 。您可以向每个节点添加多个额外接口。 对于 *nnnn* ，请为要添加的每个 interfaces_target 条目指定一个唯一编号。 对于此值，请指定裸机主机上物理接口的名称。然后，也可以添加一个逗号并提供接口的问题描述 ，该接口将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。 例如： `interfaces_target_01=ens256 ， Trunk` 如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。

密钥	**R** ， **Bp** 或 **O** ？	价值

最大 RAM	O	此节点允许使用的最大 RAM 量。如果省略此密钥，则节点不存在内存限制。在为生产级节点设置此字段时，请指定一个值，该值应至少比系统 RAM 总量少 24 GB ，并且要少 16 到 32 GB 。
		
		• 注 *： RAM 值会影响节点的实际元数据预留空间。请参见有关管理 StorageGRID 的说明 用于问题描述 的元数据预留空间。
		
		此字段的格式为 ` < 数字 >< 单位 >` ，其中 ` < 单位 >` 可以是 `b` ， `k` ， `m` 或 `g` 。
		
		示例
		
		`24G`
		
		`38654705664b`
		
		• 注 *：如果要使用此选项，必须为内存 cgroups 启用内核支持。

node_type	• R*	节点类型： VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway
port_remap	O	重新映射节点用于内部网格节点通信或外部通信的任何端口。如果企业网络策略限制 StorageGRID 使用的一个或多个端口，则必须重新映射端口，如 "`内部网格节点通信` " 或 "`外部通信 " 中所述。` • 重要信息 *：请勿重新映射计划用于配置负载平衡器端点的端口。 • 注意 *：如果仅设置 port_remap ，则指定的映射将同时用于入站和出站通信。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。 使用的格式为： ` < 网络类型 >/< 协议 >/< 网格节点使用的默认端口 >/< 新端口 >` ，其中 ` < 网络类型 >` 是网格，管理员或客户端，协议是 TCP 或 UDP 。 例如： `port_remap = client/TCP/18082/443`

密钥	**R** ， **Bp** 或 **O** ？	价值
port_remap_inbound	O	将入站通信重新映射到指定端口。如果指定 port_remap_inbound ，但未指定 port_remap 的值，则端口的出站通信将保持不变。 • 重要信息 * ：请勿重新映射计划用于配置负载平衡器端点的端口。 使用的格式为： ` < 网络类型 >/< 协议： >/< 网格节点使用的默认端口 >/< 网格节点使用的默认端口 >` ，其中 ` < 网络类型 >` 是网格，管理员或客户端，协议是 TCP 或 UDP 。 例如： `port_remap_inbound = grid/tcp/3022/22`

相关信息

网络连接准则

网格节点如何发现主管理节点

网格节点与主管理节点进行通信以进行配置和管理。每个网格节点都必须知道网格网络上主管理节点的 IP 地址。

为了确保网格节点可以访问主管理节点，您可以在部署此节点时执行以下任一操作：

- 您可以使用 admin_ip 参数手动输入主管理节点的 IP 地址。
- 您可以省略 admin_ip 参数，以使网格节点自动发现该值。当网格网络使用 DHCP 为主管理节点分配 IP 地址时，自动发现尤其有用。

可以使用多播域名系统（ mDNS ）自动发现主管理节点。主管理节点首次启动时，它会使用 mDNS 发布其 IP 地址。然后，同一子网上的其他节点可以查询 IP 地址并自动获取该地址。但是，由于多播 IP 流量通常不能跨子网路由，因此其他子网上的节点无法直接获取主管理节点的 IP 地址。

如果使用自动发现：

- 必须在主管理节点未直接连接到的任何子网上至少包含一个网格节点的 admin_IP 设置。然后，此网格节点将发布子网中其他节点的主管理节点 IP 地址，以便使用 mDNS 进行发现。
- 确保您的网络基础架构支持在子网内传递多播 IP 流量。

示例节点配置文件

您可以使用示例节点配置文件帮助设置 StorageGRID 系统的节点配置文件。这些示例显示了所有类型网格节点的节点配置文件。

对于大多数节点，在使用网格管理器或安装 API 配置网格时，您可以添加管理员和客户端网络地址信息（ IP ，掩码，网关等）。主管理节点除外。如果要浏览到主管理节点的管理网络 IP 以完成网格配置（例如，由于网格

网络未路由），则必须在主管理节点的节点配置文件中配置主管理节点的管理网络连接。示例显示了这一点。

> 在这些示例中，已将客户端网络目标配置为最佳实践，即使客户端网络默认处于禁用状态也是如此。

主管理节点的示例

- 示例文件名 * ： ` /etc/storagegRid/nodes/DC1-ad1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

存储节点示例

- 示例文件名： * ` /etc/storagegRid/nodes/DC1-SN1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

归档节点示例

- 示例文件名： * ` /etc/storagegriid/nodes/DC1-arc1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

网关节点示例

- 示例文件名： * ` /etc/storagegRid/nodes/DC1-GW1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

非主管理节点的示例

- 示例文件名： * ` /etc/storagegRid/nodes/DC1-adm2.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

验证 **StorageGRID** 配置

在 ` /etc/storaggrid/nodes` 中为每个 StorageGRID 节点创建配置文件后，您必须验证这些文件的内容。

要验证配置文件的内容，请在每个主机上运行以下命令：

```
sudo storagegrid node validate all
```

如果这些文件正确无误，则输出将为每个配置文件显示 * 已通过 * ，如示例所示。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

对于自动安装，您可以通过在 `StorageGRID` 命令中使用 ` -q` 或 ` -quiet` 选项（例如，`StorageGRID --quiet …`）来禁止此输出。如果禁止输出，则在检测到任何配置警告或错误时，命令的退出值将为非零。

如果配置文件不正确，则这些问题将显示为 * 警告 * 和 * 错误 * ，如示例所示。如果发现任何配置错误，则必须先更正这些错误，然后再继续安装。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

启动 **StorageGRID** 主机服务

要启动 StorageGRID 节点并确保它们在主机重新启动后重新启动，您必须启用并启动 StorageGRID 主机服务。

步骤

1. 在每个主机上运行以下命令：

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 运行以下命令以确保部署正在进行：

```
sudo storagegrid node status node-name
```

对于返回状态为 "`not-running` " 或 " S顶部 " 的任何节点，请运行以下命令：

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

3. 如果您先前已启用并启动 StorageGRID 主机服务（或者不确定此服务是否已启用和启动），请同时运行以下命令：

```
sudo systemctl reload-or-restart storagegrid
```

配置网格并完成安装（ **Red Hat** 或 **CentOS** ）

导航到网格管理器

您可以使用网格管理器定义配置 StorageGRID 系统所需的所有信息。

您需要的内容

必须部署主管理节点，并且已完成初始启动序列。

步骤

1. 打开 Web 浏览器并导航到以下地址之一：

```
https://primary_admin_node_ip

client_network_ip
```

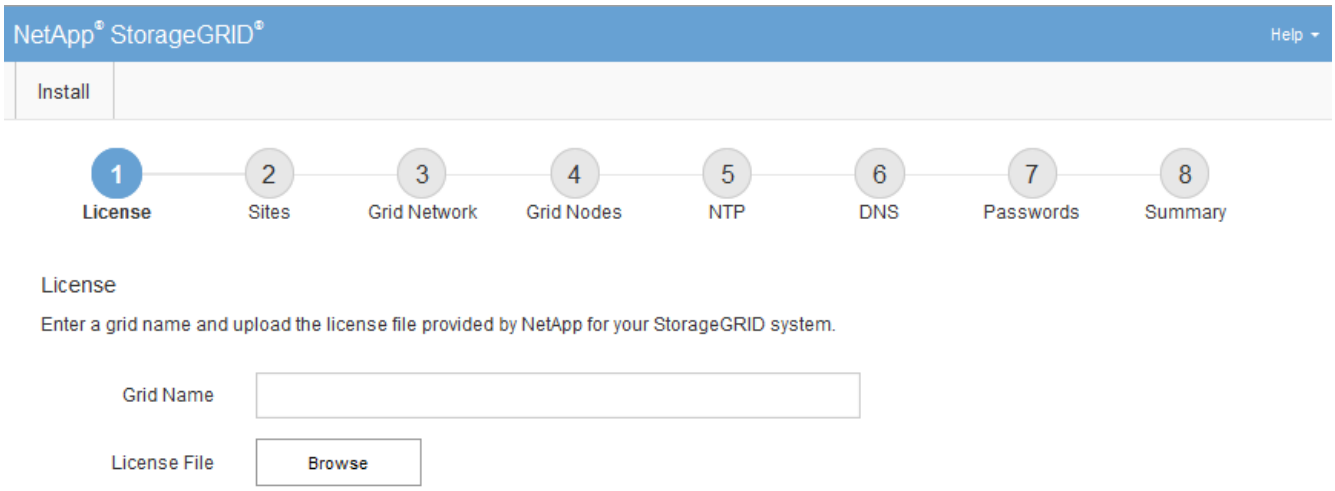
或者，您也可以通过端口 8443 访问网格管理器：

```
https://primary_admin_node_ip:8443
```

根据您的网络配置，您可以使用网格网络或管理网络上的主管理节点 IP 的 IP 地址。

1. 单击 * 安装 StorageGRID 系统 * 。

此时将显示用于配置 StorageGRID 系统的页面。



指定 **StorageGRID** 许可证信息

您必须指定 StorageGRID 系统的名称并上传 NetApp 提供的许可证文件。

步骤

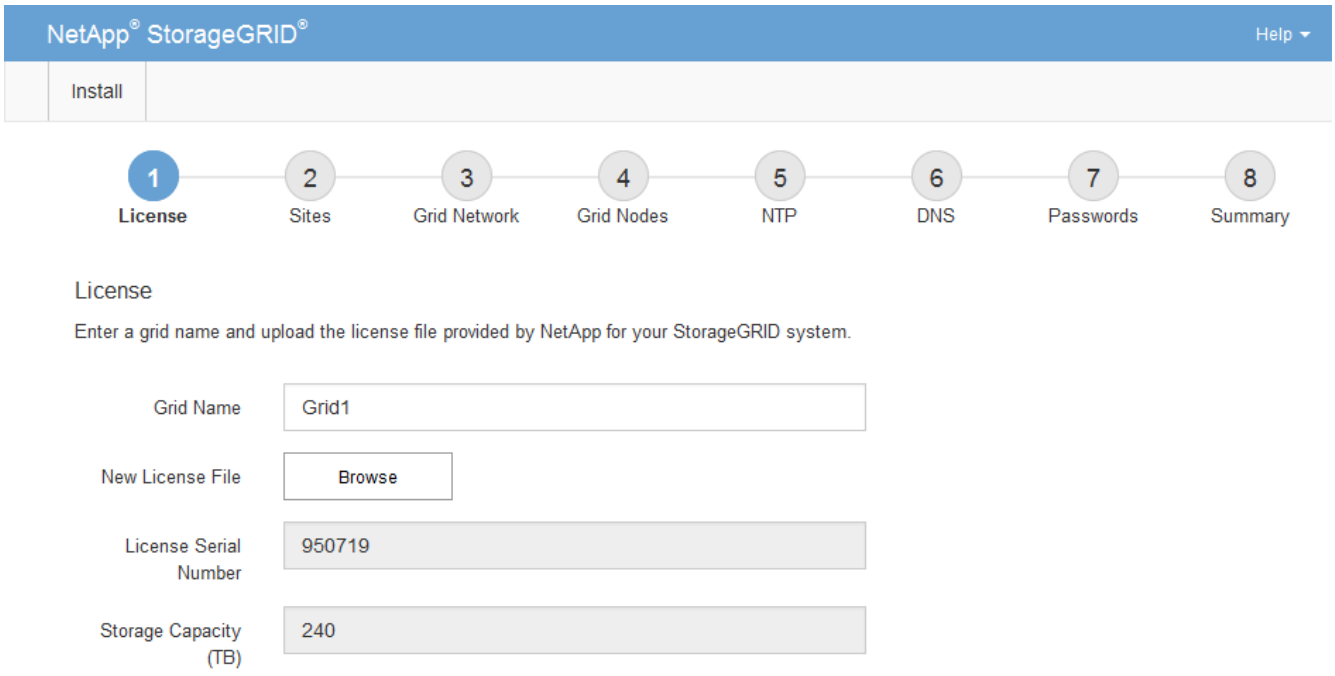
1. 在许可证页面上，在 * 网格名称 * 中为您的 StorageGRID 系统输入一个有意义的名称。

   安装后，此名称将显示在节点菜单的顶部。

2. 单击 * 浏览 * ，找到 NetApp 许可证文件（`NLFunique_id.txt`），然后单击 * 打开 * 。

   此时将验证许可证文件，并显示序列号和许可的存储容量。

   StorageGRID 安装归档包含一个免费许可证，不提供产品的任何支持授权。您可以在安装后更新为提供支持的许可证。



3. 单击 * 下一步 * 。

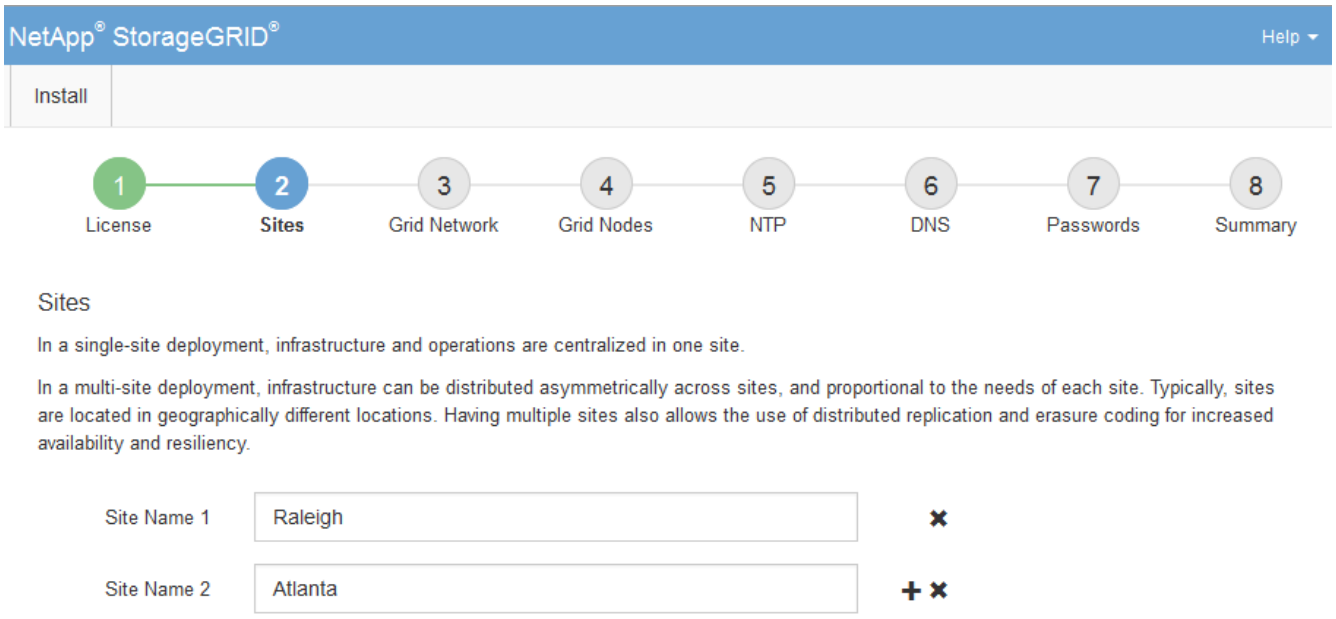
添加站点

安装 StorageGRID 时，必须至少创建一个站点。您可以创建其他站点来提高 StorageGRID 系统的可靠性和存储容量。

步骤

1. 在 Sites 页面上，输入 * 站点名称 * 。
2. 要添加其他站点，请单击最后一个站点条目旁边的加号，然后在新的 * 站点名称 * 文本框中输入名称。

   根据需要为网格拓扑添加尽可能多的其他站点。您最多可以添加 16 个站点。



3. 单击 * 下一步 * 。

指定网格网络子网

您必须指定网格网络上使用的子网。

关于此任务

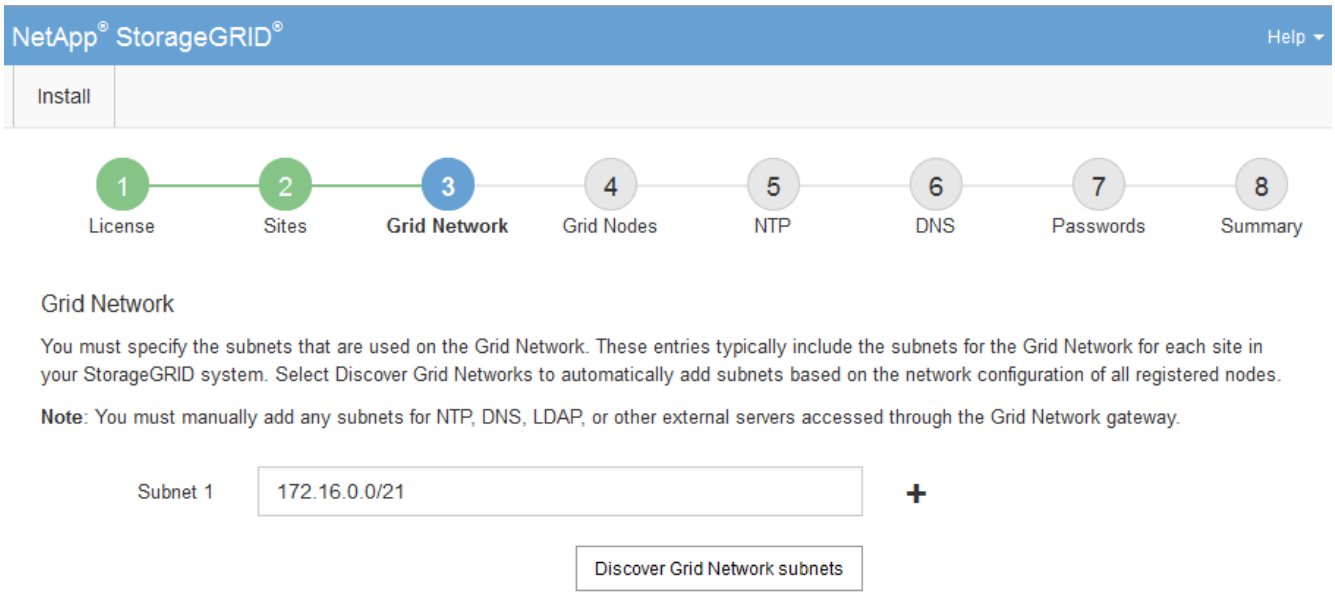
子网条目包括 StorageGRID 系统中每个站点的网格网络子网，以及需要通过网格网络访问的任何子网。

如果您有多个网格子网，则需要使用网格网络网关。指定的所有网格子网都必须可通过此网关访问。

步骤

1. 在 * 子网 1* 文本框中至少为一个网格网络指定 CIDR 网络地址。
2. 单击最后一个条目旁边的加号以添加其他网络条目。

   如果已至少部署一个节点，请单击 * 发现网格网络子网 * 以自动使用已向网格管理器注册的网格节点报告的子网填充网格网络子网列表。



3. 单击 * 下一步 * 。

批准待定网格节点

您必须先批准每个网格节点，然后才能将其加入 StorageGRID 系统。

您需要的内容

您已部署所有虚拟设备和 StorageGRID 设备网格节点。

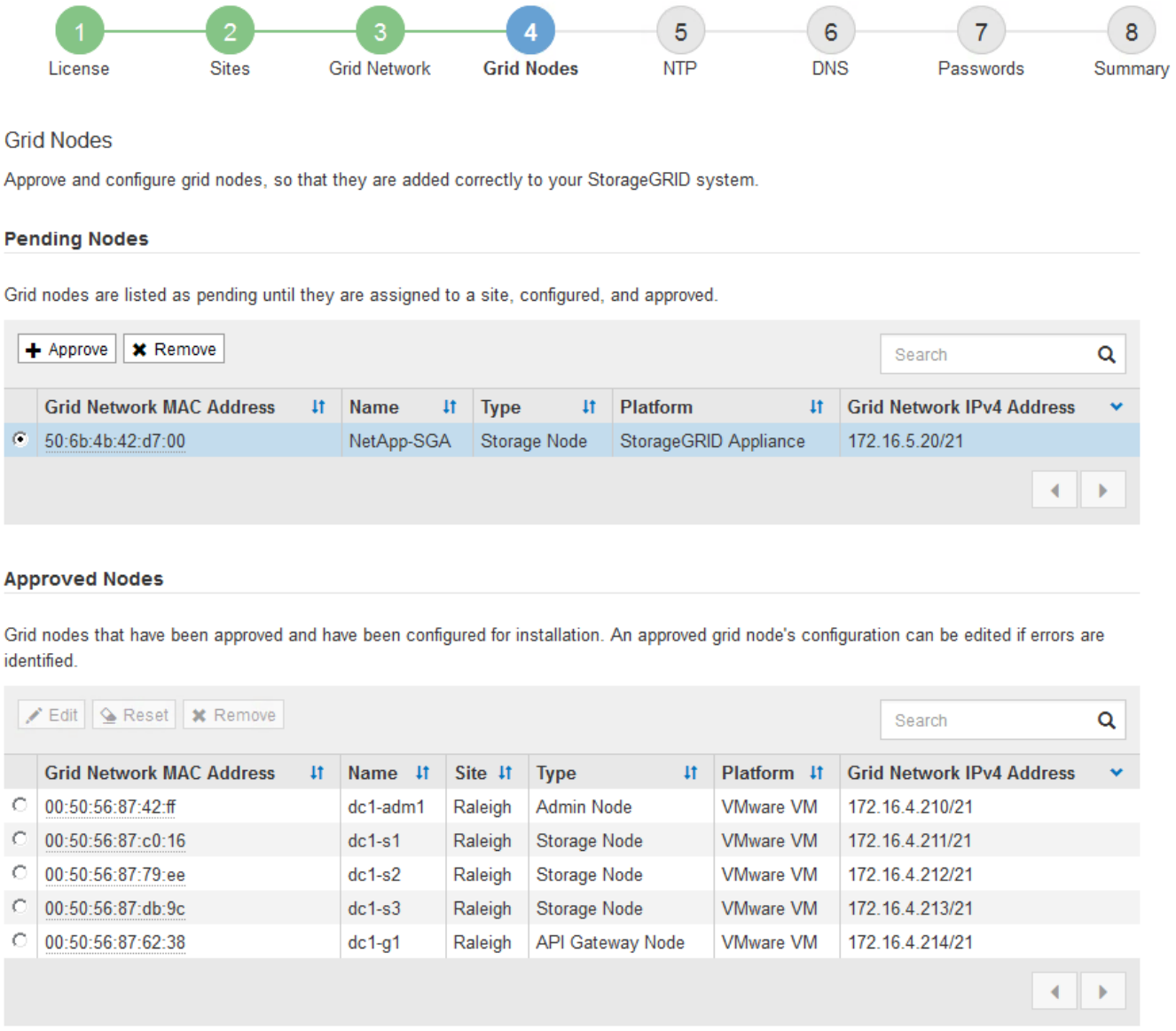
对所有节点执行一次安装比现在安装某些节点以及稍后安装某些节点更高效。

步骤

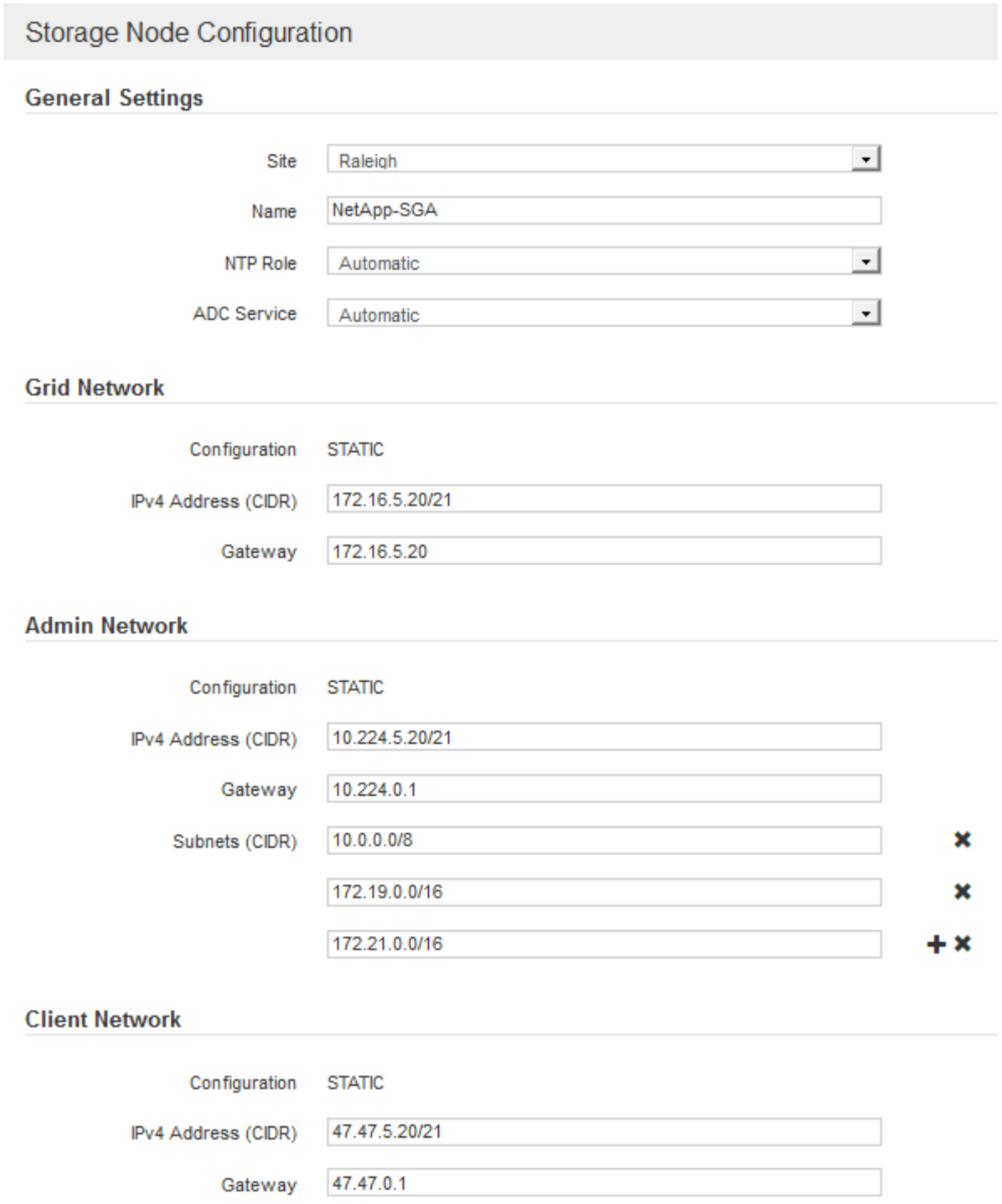
1. 查看 Pending Nodes 列表，并确认它显示了您部署的所有网格节点。

   如果缺少网格节点，请确认已成功部署该节点。

2. 选择要批准的待定节点旁边的单选按钮。



3. 单击 * 批准 * 。
4. 在常规设置中，根据需要修改以下属性的设置：



◦ * 站点 * ： 要与此网格节点关联的站点的名称。

◦ * 名称 * ： 分配给节点的名称以及将在网格管理器中显示的名称。此名称默认为您在配置节点时指定的名称。在安装过程的此步骤中，您可以根据需要更改名称。

完成安装后，您将无法更改节点的名称。

对于 VMware 节点，您可以在此处更改名称，但此操作不会更改 vSphere 中虚拟机的名称。

◦ * NTP 角色 * ： 网格节点的网络时间协议（ NTP ）角色。选项包括 * 自动 * ， * 主 * 和 * 客户端 * 。选

择 * 自动 * 会将主角色分配给管理节点，具有模板转换服务的存储节点，网关节点以及具有非静态 IP 地址的任何网格节点。所有其他网格节点都分配有客户端角色。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

- * ADC* 服务 * （仅限存储节点）：选择 * 自动 * ，让系统确定节点是否需要管理域控制器（ ADC* ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。每个站点至少有三个存储节点必须包含此 ADC-Service 。在部署此节点后，您不能将此 ADC 服务添加到该节点中。

5. 在网格网络中，根据需要修改以下属性的设置：

   - * IPv4 地址（ CIDR ） *：网格网络接口（容器中的 eth0 ）的 CIDR 网络地址。例如： 192.168.1.234/21
   - * 网关 *： 网格网络网关。例如： 192.168.0.1

     如果存在多个网格子网，则需要使用网关。

     > 如果您为网格网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

6. 如果要为网格节点配置管理网络，请根据需要在管理网络部分中添加或更新设置。

   在 * 子网（ CIDR ） * 文本框中输入从此接口路由的目标子网。如果存在多个管理子网，则需要使用管理网关。

   > 如果您为管理网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

   - 设备： * 对于 StorageGRID 设备，如果在初始安装期间未使用 StorageGRID 设备安装程序配置管理网络，则无法在此网格管理器对话框中进行配置。而是必须执行以下步骤：

     a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

        重新启动可能需要几分钟时间。

     b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。
     c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。
     d. 返回主页页面，然后单击 * 开始安装 * 。
     e. 在网格管理器中：如果节点列在 "Approved Nodes" 表中，请重置节点。
     f. 从 Pending Nodes 表中删除此节点。
     g. 等待节点重新出现在 "Pending Nodes" 列表中。
     h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。

        对于追加信息 ，请参见适用于您的设备型号的安装和维护说明。

7. 如果要为网格节点配置客户端网络，请根据需要在客户端网络部分中添加或更新设置。如果配置了客户端网络，则需要使用网关，安装后，它将成为节点的默认网关。

如果您为客户端网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

- 设备： * 对于 StorageGRID 设备，如果在初始安装期间未使用 StorageGRID 设备安装程序配置客户端网络，则无法在此网格管理器对话框中进行配置。而是必须执行以下步骤：

  a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

     重新启动可能需要几分钟时间。

  b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。

  c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。

  d. 返回主页页面，然后单击 * 开始安装 * 。

  e. 在网格管理器中：如果节点列在 "Approved Nodes" 表中，请重置节点。

  f. 从 Pending Nodes 表中删除此节点。

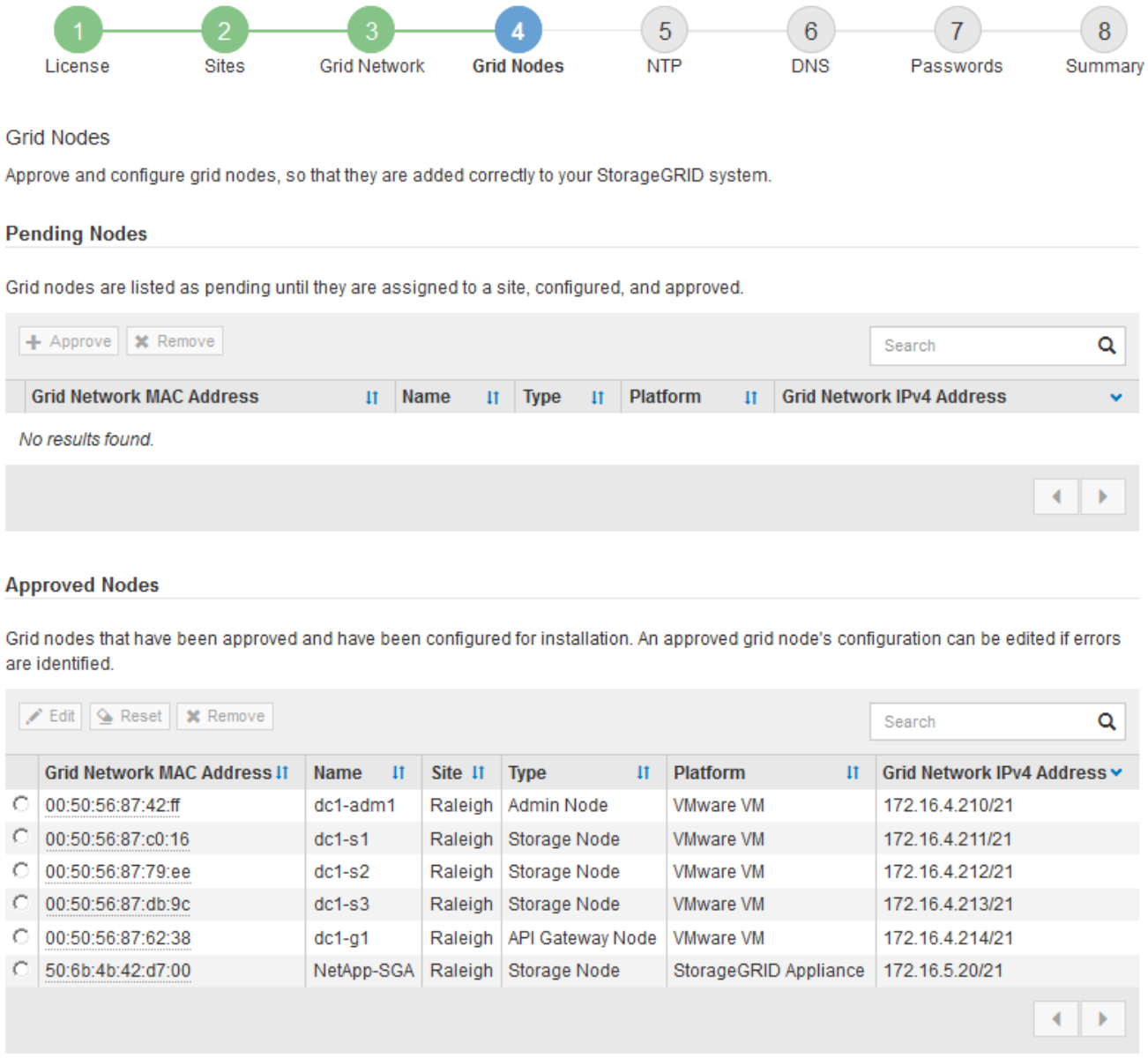
  g. 等待节点重新出现在 "Pending Nodes" 列表中。

  h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。

     对于追加信息 ，请参见适用于您的设备的安装和维护说明。

8. 单击 * 保存 * 。

网格节点条目将移至 "Approved Nodes" 列表。



9. 对要批准的每个待定网格节点重复上述步骤。

   您必须批准网格中所需的所有节点。但是，在单击 " 摘要 " 页面上的 * 安装 * 之前，您可以随时返回此页面。您可以通过选择已批准的网格节点的单选按钮并单击 * 编辑 * 来修改其属性。

10. 批准完网格节点后，单击 * 下一步 * 。

指定网络时间协议服务器信息

您必须为 StorageGRID 系统指定网络时间协议（ NTP ）配置信息，以便在不同服务器上执行的操作保持同步。

关于此任务

您必须为 NTP 服务器指定 IPv4 地址。

您必须指定外部 NTP 服务器。指定的 NTP 服务器必须使用 NTP 协议。

您必须指定四个引用 Stratum 3 或更高配置的 NTP 服务器，以防止出现时间偏差问题。

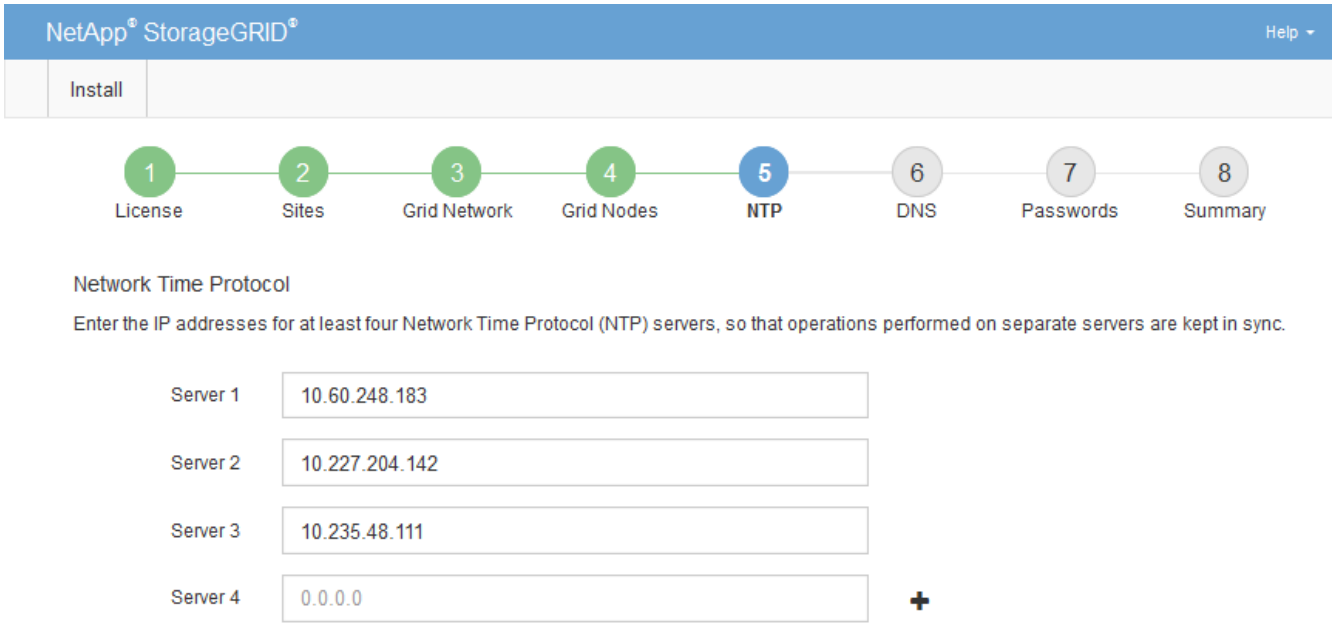
> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。
>
> "支持边界，用于为高精度环境配置 Windows 时间服务"

外部 NTP 服务器由先前分配了主 NTP 角色的节点使用。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

步骤

1. 在 * 服务器 1* 到 * 服务器 4* 文本框中指定至少四个 NTP 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



3. 选择 * 下一步 * 。

指定域名系统服务器信息

您必须为 StorageGRID 系统指定域名系统（ DNS ）信息，以便可以使用主机名而非 IP 地址访问外部服务器。

关于此任务

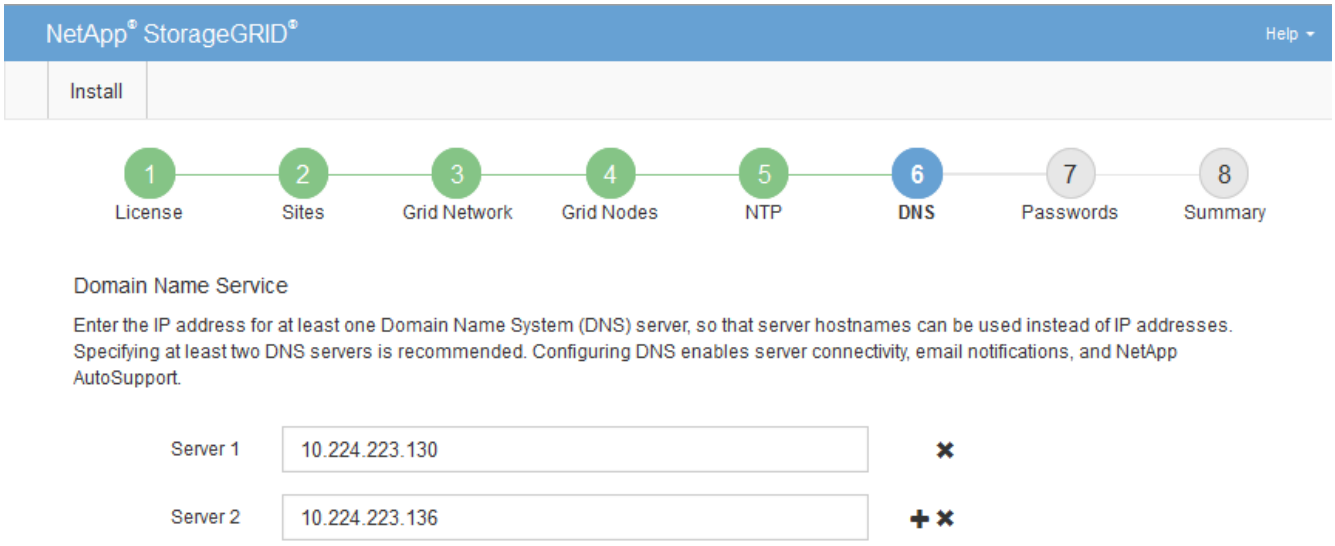
通过指定 DNS 服务器信息，您可以对电子邮件通知和 AutoSupport 使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。建议至少指定两个 DNS 服务器。

为 DNS 服务器提供两到六个 IPv4 地址。您应选择 DNS 服务器，以便在网络隔离时每个站点都可以在本地访问这些服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以进一步自定义每个节点的 DNS 服务器列表。有关详细信息，请参见恢复和维护说明中有关修改 DNS 配置的信息。

如果省略 DNS 服务器信息或 DNS 服务器信息配置不正确，则会在每个网格节点的 SSM 服务上触发 DNST 警报。如果 DNS 配置正确且新服务器信息已到达所有网格节点，则警报将清除。

步骤

1. 在 * 服务器 1* 文本框中至少指定一个 DNS 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



最佳实践是至少指定两个 DNS 服务器。最多可以指定六个 DNS 服务器。

3. 选择 * 下一步 * 。

指定 **StorageGRID** 系统密码

在安装 StorageGRID 系统时，您需要输入密码以保护系统安全并执行维护任务。

关于此任务

使用安装密码页面指定配置密码短语和网格管理 root 用户密码。

- 配置密码短语用作加密密钥，不会由 StorageGRID 系统存储。
- 您必须具有用于安装，扩展和维护过程的配置密码短语，包括下载恢复软件包。因此，请务必将配置密码短语存储在安全位置。
- 如果您使用的是最新的网格管理器，则可以从网格管理器更改配置密码短语。
- 可以使用网格管理器更改网格管理 root 用户密码。
- 随机生成的命令行控制台和 SSH 密码存储在恢复软件包的 Passwords.txt 文件中。

步骤

1. 在 * 配置密码短语 * 中，输入更改 StorageGRID 系统网格拓扑所需的配置密码短语。

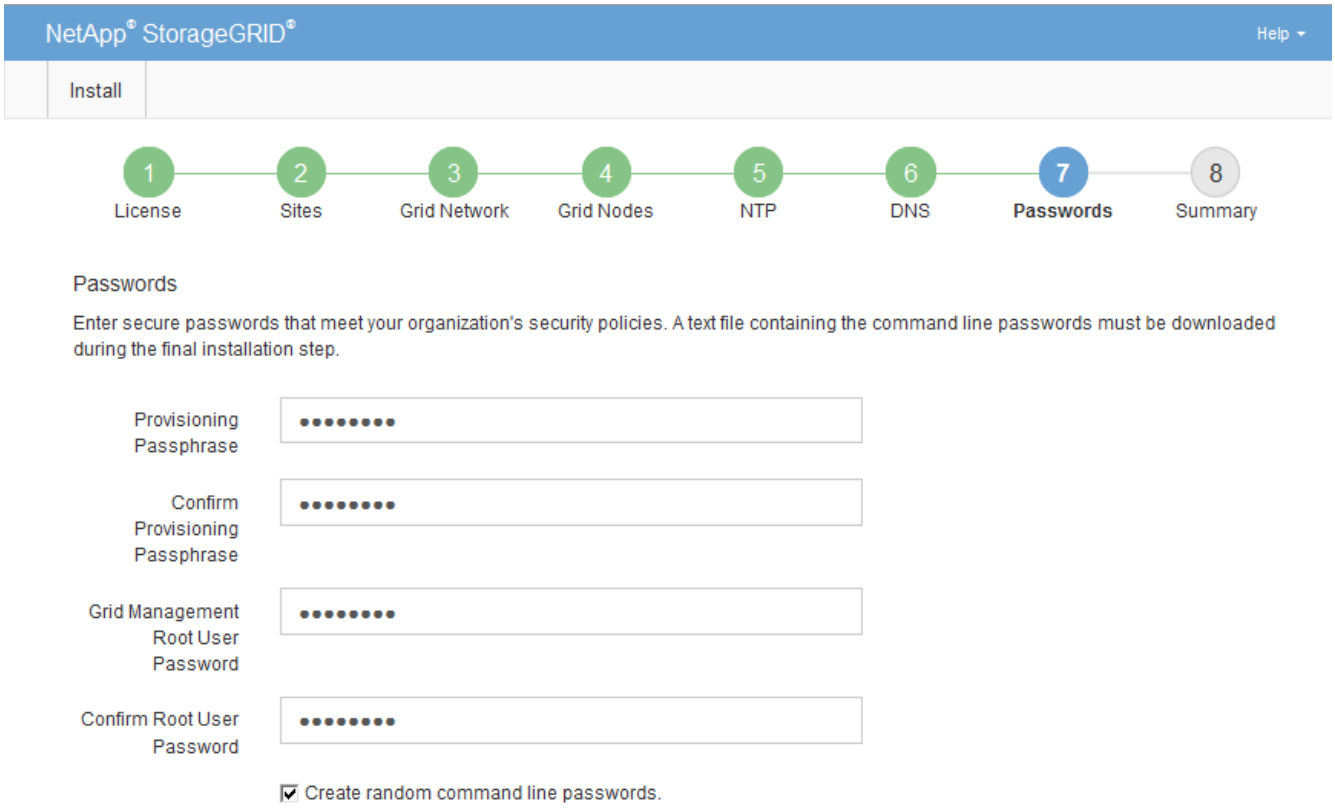
将配置密码短语存储在安全位置。

> 如果在安装完成后您希望稍后更改配置密码短语，则可以使用网格管理器。选择 * 配置 * > * 访问控制 * > * 网格密码 * 。

2. 在 * 确认配置密码短语 * 中，重新输入配置密码短语进行确认。
3. 在 * 网格管理 root 用户密码 * 中，以 "`root` " 用户身份输入用于访问网格管理器的密码。

   将密码存储在安全的位置。

4. 在 * 确认 root 用户密码 * 中，重新输入网格管理器密码进行确认。



5. 如果要安装网格以进行概念验证或演示，也可以取消选中 * 创建随机命令行密码 * 复选框。

   对于生产部署，出于安全原因，应始终使用随机密码。如果要使用默认密码通过命令行使用 "`root` " 或 "`admin` " 帐户访问网格节点，请取消选择 * 仅为演示网格创建随机命令行密码 * 。

> 单击摘要页面上的 * 安装 * 后，系统将提示您下载恢复软件包文件（ `sGWS-recovery-package-id-revision.zip` ）。您必须 下载此文件 以完成安装。访问系统所需的密码存储在恢复软件包文件中的 `passwords.txt` 文件中。

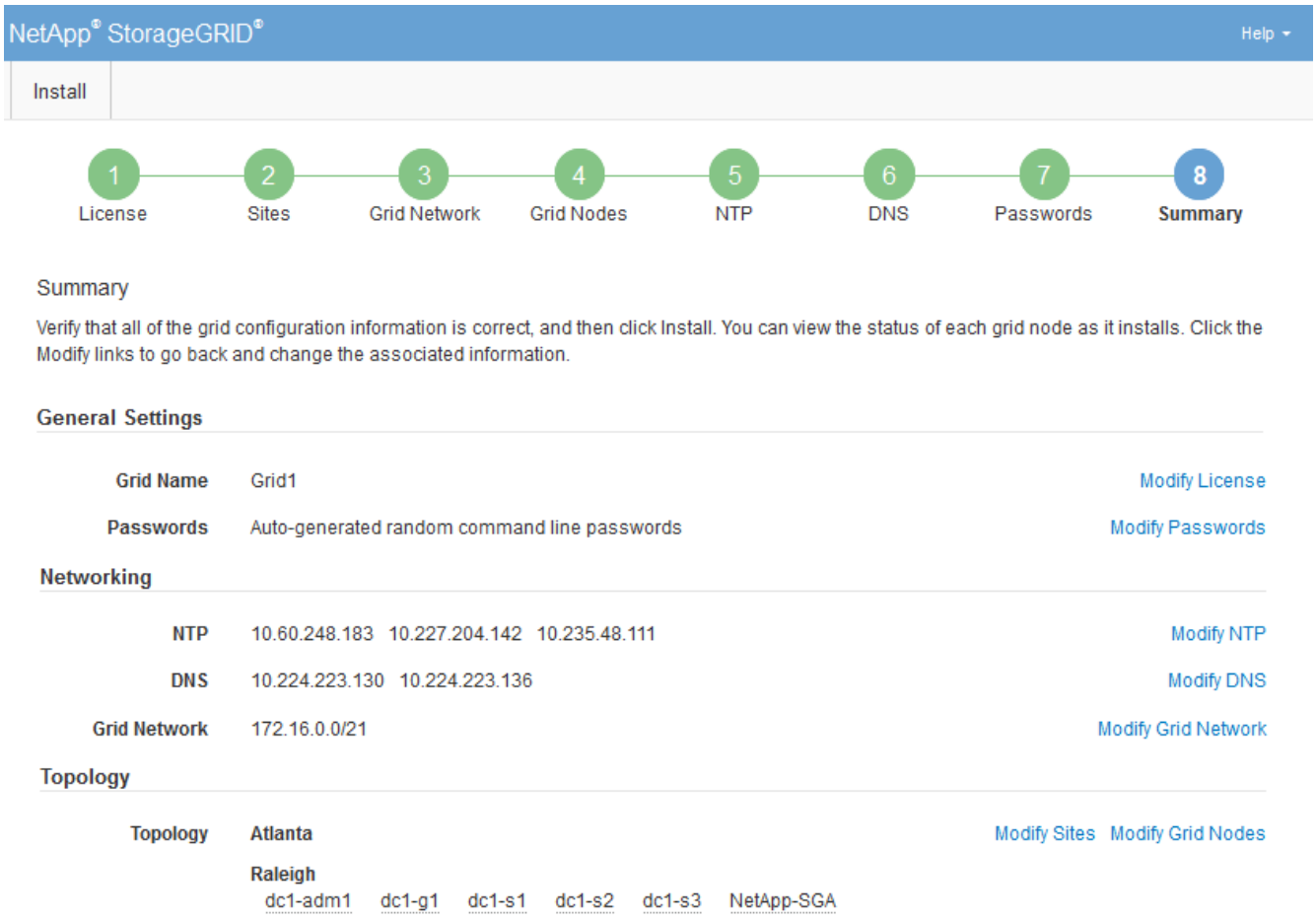
6. 单击 * 下一步 * 。

查看您的配置并完成安装

您必须仔细查看输入的配置信息，以确保安装成功完成。

步骤

1. 查看 * 摘要 * 页面。



2. 验证所有网格配置信息是否正确。使用摘要页面上的修改链接返回并更正任何错误。
3. 单击 * 安装 * 。

> 如果将某个节点配置为使用客户端网络，则在单击 * 安装 * 时，该节点的默认网关会从网格网络切换到客户端网络。如果连接断开，则必须确保通过可访问的子网访问主管理节点。请参见 网络连接准则 了解详细信息。

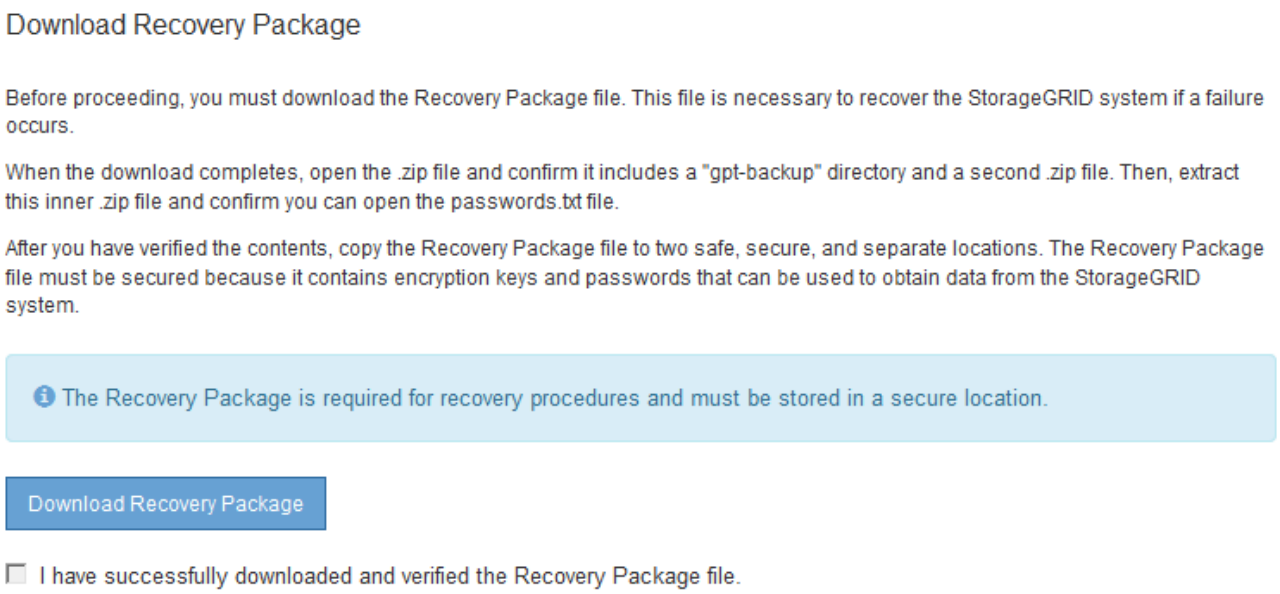
4. 单击 * 下载恢复包 * 。

   当安装过程进展到定义网格拓扑时，系统会提示您下载恢复包文件（` .zip` ），并确认您可以成功访问此文件的内容。您必须下载恢复软件包文件，以便在一个或多个网格节点出现故障时恢复 StorageGRID 系统。安装将在后台继续进行，但您无法完成安装并访问 StorageGRID 系统，直到下载并验证此文件为止。

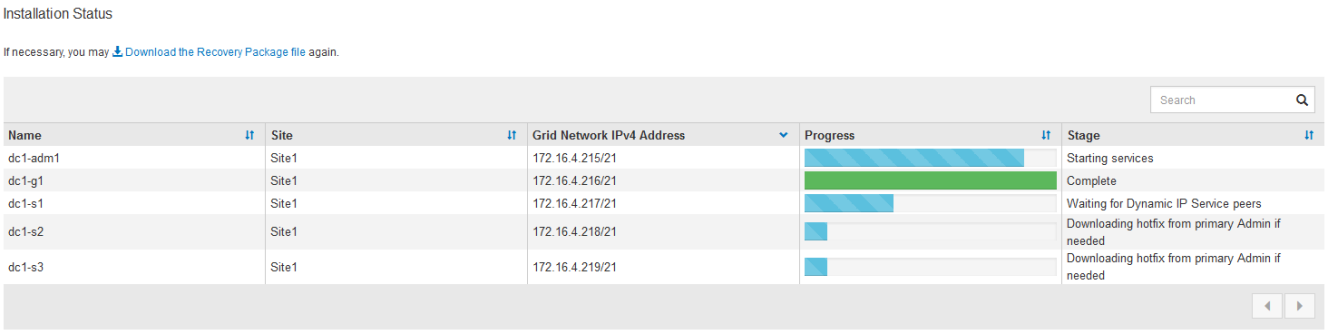
5. 验证您是否可以提取 ` .zip` 文件的内容，然后将其保存在两个安全，安全和独立的位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

6. 选中 * 我已成功下载并验证恢复软件包文件 * 复选框，然后单击 * 下一步 * 。



如果安装仍在进行中，则会显示状态页面。此页面指示每个网格节点的安装进度。



当所有网格节点达到完成阶段后，将显示网格管理器的登录页面。

7. 使用 "root" 用户和您在安装期间指定的密码登录到网格管理器。

安装后准则

完成网格节点部署和配置后，请按照以下准则更改 DHCP 地址和网络配置。

- 如果使用 DHCP 分配 IP 地址，请为所使用网络上的每个 IP 地址配置 DHCP 预留。

  您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。

  > 当节点的 IP 地址发生更改时，节点会重新启动，如果 DHCP 地址更改同时影响多个节点，则发生原因 可能会中断。

- 如果要更改网格节点的 IP 地址，子网掩码和默认网关，必须使用更改 IP 过程。请参见 配置 IP 地址。
- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改，您可能需要重新建立这些连接。

自动安装（Red Hat Enterprise Linux 或 CentOS ）

您可以自动安装 StorageGRID 主机服务和配置网格节点。

在以下任一情况下，自动部署可能会很有用：

- 您已使用标准业务流程框架（例如 Ansible ， Puppet 或 Chef ）部署和配置物理或虚拟主机。
- 您打算部署多个 StorageGRID 实例。
- 您正在部署一个大型的复杂 StorageGRID 实例。

StorageGRID 主机服务由软件包安装，并由配置文件驱动。您可以使用以下方法之一创建配置文件：

- 创建配置文件 手动安装期间以交互方式进行。
- 如本文所述，提前（或以编程方式）准备配置文件，以便使用标准业务流程框架实现自动安装。

  StorageGRID 提供了可选的 Python 脚本，用于自动配置 StorageGRID 设备和整个 StorageGRID 系统（"`grid` "）。您可以直接使用这些脚本，也可以对其进行检查，了解如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。

自动安装和配置 StorageGRID 主机服务

您可以使用 Ansible ， Puppet ， Chef ， Fabric 或 SaltStack 等标准业务流程框架自动安装 StorageGRID 主机服务。

StorageGRID 主机服务打包在 RPM 中，并由配置文件驱动，您可以提前（或以编程方式）准备这些配置文件，以启用自动安装。如果您已经使用标准业务流程框架来安装和配置 RHEL 或 CentOS ，则在攻略手册或秘诀中添加 StorageGRID 应该非常简单。

请参见随安装归档提供的 ` 或 Extras` 文件夹中的示例 Ansible 角色和攻略手册。Ansible 攻略手册介绍了 `StorageGRID` 角色如何准备主机并将 StorageGRID 安装到目标服务器上。您可以根据需要自定义角色或攻略手册。

> 此示例攻略手册不包括在启动 StorageGRID 主机服务之前创建网络设备所需的步骤。在完成并使用攻略手册之前，请添加以下步骤。

您可以自动执行准备主机和部署虚拟网格节点的所有步骤。

自动配置 StorageGRID

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	Description
configure-storagegrid.py	用于自动配置的 Python 脚本

文件名	Description
configure-storaggrid.sample.json	用于脚本的示例配置文件
configure-storaggrid.blank.json	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

关于此任务

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

> 您也可以使用网格管理器或安装 API 配置系统。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中 `platform` is `dEBS` ， `rpms` 或 `vSphere` 。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

结果

在配置过程中会生成一个恢复包 ` .zip` 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 `passwords.txt` 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

相关信息

安装 REST API 概述

安装 **REST API** 概述

StorageGRID 提供了用于执行安装任务的 StorageGRID 安装 API 。

API 使用 Swagger 开源 API 平台提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 **API**

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。
- **recovery-package** —下载恢复软件包的操作。

- * 模式 * —用于高级部署的 API 模式
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

下一步行动

完成安装后，您必须执行一系列集成和配置步骤。某些步骤是必需的；其他步骤是可选的。

所需任务

- 为要用于在 StorageGRID 系统上存储对象的每个客户端协议（ Swift 或 S3 ）创建一个租户帐户。
- 通过配置组和用户帐户来控制系统访问。您也可以配置联合身份源（例如 Active Directory 或 OpenLDAP ），以便导入管理组和用户。或者，您也可以创建本地组和用户。
- 集成并测试用于将对象上传到 StorageGRID 系统的 S3 或 Swift API 客户端应用程序。
- 准备好后，配置要用于保护对象数据的信息生命周期管理（ ILM ）规则和 ILM 策略。

> 安装 StorageGRID 时，默认 ILM 策略 " 基线 2 副本策略 " 处于活动状态。此策略包括常用 ILM 规则（创建 2 个副本），如果未激活任何其他策略，则此策略适用。

- 如果您的安装包括设备存储节点，请使用 SANtricity 软件完成以下任务：
  - 连接到每个 StorageGRID 设备。
  - 验证是否收到 AutoSupport 数据。
- 如果 StorageGRID 系统包含任何归档节点，请配置归档节点与目标外部归档存储系统的连接。

> 如果任何归档节点将使用 Tivoli Storage Manager 作为外部归档存储系统，则还必须配置 Tivoli Storage Manager 。

- 查看并遵循 StorageGRID 系统强化准则，以消除安全风险。
- 为系统警报配置电子邮件通知。

可选任务

- 如果要从（原有）警报系统接收通知，请配置警报的邮件列表和电子邮件通知。
- 如果自规划部署并生成恢复包以来网格节点 IP 地址发生了更改，请更新这些地址。请参见恢复和维护说明中有关更改 IP 地址的信息。
- 根据需要配置存储加密。
- 如果需要，配置存储压缩以减小存储对象的大小。
- 配置审核客户端访问。您可以通过 NFS 或 CIFS 文件共享配置对系统的访问，以供审核使用。请参见有关管理 StorageGRID 的说明。

> 已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

相关信息

管理 StorageGRID

使用 S3

使用 Swift

使用 ILM 管理对象

监控和故障排除

恢复和维护

SG100 和 SG1000 服务设备

SG5600 存储设备

SG5700 存储设备

SG6000 存储设备

发行说明

系统强化

查看审核日志

升级软件

对安装问题进行故障排除

如果在安装 StorageGRID 系统时出现任何问题，您可以访问安装日志文件。技术支持可能还需要使用安装日志文件来解决问题。

运行每个节点的容器提供了以下安装日志文件：

- ` /var/local/log/install.log` （可在所有网格节点上找到）
- ` /var/local/log/gdu-server.log` （位于主管理节点上）

主机上提供了以下安装日志文件：

- ` /var/log/storaggrid/daema.log`
- ` /var/log/storagegRid/nodes/node-name.log`

要了解如何访问日志文件，请参见有关 StorageGRID 监控和故障排除的说明。有关排除设备安装问题的帮助，请参见适用于您的设备的安装和维护说明。如果您需要其他帮助，请联系技术支持。

相关信息

监控和故障排除

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

"NetApp 支持"

示例 /etc/sysconfig/network-scripts

您可以使用示例文件将四个 Linux 物理接口聚合到一个 LACP 绑定中，然后建立三个 VLAN 接口，将此绑定分包为 StorageGRID 网格，管理和客户端网络接口。

物理接口

请注意，链路另一端的交换机还必须将这四个端口视为一个 LACP 中继或端口通道，并且必须至少通过三个带标记的参考 VLAN 。

` * /etc/sysconfig/network-scripts/ifcfg-ens160*`

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

` * /etc/sysconfig/network-scripts/ifcfg-ens192*`

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

` * /etc/sysconfig/network-scripts/ifcfg-ens224*`

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

` * /etc/sysconfig/network-scripts/ifcfg-ens256*`

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

绑定接口

` * /etc/sysconfig/network-scripts/ifcfg-bond0*`

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLAN 接口

` * /etc/sysconfig/network-scripts/ifcfg-bond0.1001*`

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

` * /etc/sysconfig/network-scripts/ifcfg-bond0.1002*`

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

` * /etc/sysconfig/network-scripts/ifcfg-bond0.1003*`

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

安装 Ubuntu 或 Debian

安装 Ubuntu 或 Debian： 概述

在 Ubuntu 或 Debian 环境中安装 StorageGRID 系统包括三个主要步骤。

1. * 准备 *： 在规划和准备期间，您将执行以下任务：
   - 了解 StorageGRID 的硬件和存储要求。
   - 了解的具体信息 StorageGRID 网络连接 这样，您就可以正确配置网络了。
   - 确定并准备要用于托管 StorageGRID 网格节点的物理或虚拟服务器。
   - 在已准备好的服务器上：
     - 安装 Linux
     - 配置主机网络
     - 配置主机存储
     - 安装 Docker
     - 安装 StorageGRID 主机服务

2. * 部署 * ： 使用适当的用户界面部署网格节点。部署网格节点时，它们会作为 StorageGRID 系统的一部分创建并连接到一个或多个网络。

   a. 使用 Linux 命令行和节点配置文件在步骤 1 准备的主机上部署虚拟网格节点。

   b. 使用 StorageGRID 设备安装程序部署 StorageGRID 设备节点。

   > StorageGRID 安装操作步骤 中不包含特定于硬件的安装和集成说明。要了解如何安装 StorageGRID 设备，请参见适用于您的设备的安装和维护说明。

3. * 配置 * ： 部署完所有节点后，请使用网格管理器配置网格并完成安装。

以下说明为在 Ubuntu 或 Debian 环境中部署和配置 StorageGRID 系统提供了标准方法。另请参见有关以下替代方法的信息：

- 使用 Ansible ， Puppet 或 Chef 等标准业务流程框架安装 Ubuntu 或 Debian ，配置网络和存储，安装 Docker 和 StorageGRID 主机服务以及部署虚拟网格节点。
- 使用 Python 配置脚本（在安装归档中提供）自动部署和配置 StorageGRID 系统。
- 使用 Python 配置脚本（可从安装归档或 StorageGRID 设备安装程序获取）自动部署和配置设备网格节点。
- 如果您是 StorageGRID 部署的高级开发人员，请使用安装 REST API 自动安装 StorageGRID 网格节点。

规划并准备安装 **Ubuntu** 或 **Debian**

安装之前（ **Ubuntu** 或 **Debian** ）

在部署网格节点和配置 StorageGRID 网格之前，您必须熟悉完成操作步骤 的步骤和要求。

StorageGRID 部署和配置过程假定您熟悉 StorageGRID 系统的架构和操作。

您可以一次部署一个或多个站点；但是，所有站点必须满足至少有三个存储节点的最低要求。

在开始安装 StorageGRID 之前，您必须：

- 了解 StorageGRID 的计算要求，包括每个节点的最低 CPU 和 RAM 要求。
- 了解 StorageGRID 如何支持多个网络以实现流量隔离，安全性和管理便利性，并计划要连接到每个 StorageGRID 节点的网络。

  请参见 StorageGRID 网络连接准则。

- 了解每种类型的网格节点的存储和性能要求。
- 确定一组服务器（物理服务器，虚拟服务器或两者），这些服务器可在聚合中提供足够的资源来支持您计划部署的 StorageGRID 节点的数量和类型。
- 如果要在不中断任何服务的情况下对物理主机执行计划内维护，请了解节点迁移的要求。
- 提前收集所有网络信息。除非使用 DHCP ，否则请收集要分配给每个网格节点的 IP 地址以及要使用的域名系统（ DNS ）和网络时间协议（ NTP ）服务器的 IP 地址。
- 按照规格安装，连接和配置所有必需的硬件，包括任何 StorageGRID 设备。

StorageGRID 安装操作步骤 中不包含特定于硬件的安装和集成说明。要了解如何安装 StorageGRID 设备，请参见适用于您的设备的安装和维护说明。

- 确定要使用的可用部署和配置工具。

相关信息

网络连接准则

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

节点容器迁移要求

所需材料

在安装 StorageGRID 之前，您必须收集并准备所需的材料。

项目	注释：
NetApp StorageGRID 许可证	您必须具有有效的数字签名 NetApp 许可证。 • 注意 * ： StorageGRID 安装归档中包含一个非生产许可证，可用于测试和概念验证网格。
StorageGRID 安装归档	您必须 下载 StorageGRID 安装归档并解压缩文件。
服务笔记本电脑	StorageGRID 系统通过服务笔记本电脑进行安装。 服务笔记本电脑必须具有： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器
StorageGRID 文档	• 发行说明 • 有关管理 StorageGRID 的说明

相关信息

"NetApp 互操作性表工具"

下载并提取 **StorageGRID** 安装文件

您必须下载 StorageGRID 安装归档并提取所需文件。

步骤

1. 转至 "StorageGRID 的 "NetApp 下载 " 页面"。
2. 选择用于下载最新版本的按钮，或者从下拉菜单中选择其他版本并选择 * 执行 * 。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 如果显示 Caution/MustRead 语句，请阅读该语句并选中复选框。

   安装 StorageGRID 版本后，您必须应用任何所需的修补程序。有关详细信息，请参见 恢复和维护说明中的热修补程序操作步骤

5. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。

   此时将显示选定版本的下载页面。此页面包含三列：

6. 在 * 安装 StorageGRID * 列中，为 Ubuntu 或 Debian 选择 .tgz 或 .zip 文件。

   如果您在服务笔记本电脑上运行 Windows ，请选择 ` .zip` 文件。

7. 保存并提取归档文件。
8. 从以下列表中选择所需的文件。

   所需的文件集取决于您规划的网格拓扑以及如何部署 StorageGRID 网格。

   表中列出的路径与提取的安装归档所安装的顶级目录相对。

路径和文件名	**Description**
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。
	文件 ` /debs/storagegrid-webscale-images-version-SHA.deb` 的 MD5 校验和。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。

路径和文件名	Description
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 * ： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

相关信息

恢复和维护

CPU 和 RAM 要求

在安装 StorageGRID 软件之前，请验证并配置硬件，使其可以支持 StorageGRID 系统。

有关受支持服务器的信息，请参见互操作性表。

每个 StorageGRID 节点需要以下最低资源：

- CPU 核心：每个节点 8 个
- RAM ： 每个节点至少 24 GB ，比系统总 RAM 少 2 到 16 GB ，具体取决于可用 RAM 总量和系统上运行的非 StorageGRID 软件的数量

确保计划在每个物理或虚拟主机上运行的 StorageGRID 节点数不超过可用的 CPU 核心数或物理 RAM 数。如果主机不是专用于运行 StorageGRID 的（不建议使用），请务必考虑其他应用程序的资源要求。

定期监控 CPU 和内存使用情况，以确保这些资源能够持续满足您的工作负载需求。例如，将虚拟存储节点的 RAM 和 CPU 分配增加一倍将提供与为 StorageGRID 设备节点提供的资源类似的资源。此外，如果每个节点的元数据量超过 500 GB ，请考虑将每个节点的 RAM 增加到 48 GB 或更多。有关管理对象元数据存储，增加元数据预留空间设置以及监控 CPU 和内存使用量的信息，请参见有关管理，监控和升级 StorageGRID 的说明。

如果在底层物理主机上启用了超线程功能，则可以为每个节点提供 8 个虚拟核心（ 4 个物理核心）。如果底层物理主机上未启用超线程，则必须为每个节点提供 8 个物理核心。

如果要使用虚拟机作为主机并控制 VM 的大小和数量，则应为每个 StorageGRID 节点使用一个 VM 并相应地调整 VM 的大小。

对于生产部署，不应在同一物理存储硬件或虚拟主机上运行多个存储节点。一个 StorageGRID 部署中的每个存储节点都应位于其各自的隔离故障域中。如果您确保单个硬件故障只会影响单个存储节点，则可以最大限度地提高对象数据的持久性和可用性。

另请参见有关存储要求的信息。

相关信息

"NetApp 互操作性表工具"

存储和性能要求

管理 StorageGRID

监控和故障排除

升级软件

存储和性能要求

您必须了解 StorageGRID 节点的存储要求，以便提供足够的空间来支持初始配置和未来的存储扩展。

StorageGRID 节点需要三种逻辑存储类别：

- * 容器池 * - 节点容器的性能层（ 10K SAS 或 SSD ）存储，在支持 StorageGRID 节点的主机上安装和配置 Docker 时，此存储将分配给 Docker 存储驱动程序。
- * 系统数据 * —性能层（ 10K SAS 或 SSD ）存储，用于按节点永久存储系统数据和事务日志， StorageGRID 主机服务将使用这些存储并将其映射到各个节点。
- * 对象数据 * —性能层（ 10K SAS 或 SSD ）存储和容量层（ NL-SAS/SATA ）批量存储，用于永久存储对象数据和对象元数据。

您必须对所有存储类别使用 RAID 支持的块设备。不支持非冗余磁盘， SSD 或 JBOD 。您可以对任何存储类别使用共享或本地 RAID 存储；但是，如果要使用 StorageGRID 的节点迁移功能，则必须将系统数据和对象数据存储在共享存储上。

性能要求

用于容器池，系统数据和对象元数据的卷的性能会显著影响系统的整体性能。您应对这些卷使用性能层（ 10K SAS 或 SSD ）存储，以确保在延迟，每秒输入 / 输出操作数（ IOPS ）和吞吐量方面具有足够的磁盘性能。您

可以使用容量层（ NL-SAS/SATA ）存储来永久存储对象数据。

用于容器池，系统数据和对象数据的卷必须启用回写缓存。缓存必须位于受保护或永久性介质上。

使用**NetApp ONTAP** 存储的主机的要求

如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

所需的主机数

每个 StorageGRID 站点至少需要三个存储节点。

> 在生产部署中，请勿在一个物理或虚拟主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

其他类型的节点（例如管理节点或网关节点）可以部署在同一主机上，也可以根据需要部署在自己的专用主机上。

每个主机的存储卷数量

下表显示了每个主机所需的存储卷（ LUN ）数量以及每个 LUN 所需的最小大小，具体取决于要在该主机上部署的节点。

测试的最大 LUN 大小为 39 TB 。

> 这些数字适用于每个主机，而不适用于整个网格。

LUN 用途	存储类别	**LUN** 数量	最小大小 **/LUN**
容器引擎存储池	容器池	1.	节点总数 × 100 GB
` /var/local` 卷	系统数据	此主机上的每个节点 1 个	90 GB
存储节点	对象数据	此主机上的每个存储节点 3 个 • 注： * 基于软件的存储节点可以包含 1 到 16 个存储卷；建议至少使用 3 个存储卷。	12 TB （ 4 TB/LUN ）有关详细信息，请参见存储节点的存储要求。
管理节点审核日志	系统数据	此主机上的每个管理节点 1 个	200 GB

LUN 用途	存储类别	LUN 数量	最小大小 /LUN
管理节点表	系统数据	此主机上的每个管理节点 1 个	200 GB

根据配置的审核级别， S3 对象密钥名称等用户输入的大小以及需要保留的审核日志数据量，您可能需要增加每个管理节点上的审核日志 LUN 的大小。一般来说，网格在每个 S3 操作中生成大约 1 KB 的审核数据，这意味着 200 GB 的 LUN 每天支持 7 ， 000 万次操作，或者每秒 800 次操作，持续 2 到 3 天。

主机的最小存储空间

下表显示了每种类型的节点所需的最小存储空间。您可以使用此表根据要在每个存储类别中部署的节点确定必须为主机提供的最小存储量。

磁盘快照不能用于还原网格节点。请参阅每种类型节点的恢复和维护过程。

节点类型	容器池	系统数据	对象数据
存储节点	100 GB	90 GB	4 ， 000 GB
管理节点	100 GB	490 GB （ 3 个 LUN ）	_ 不适用 _
网关节点	100 GB	90 GB	_ 不适用 _
归档节点	100 GB	90 GB	_ 不适用 _

示例：计算主机的存储要求

假设您计划在同一主机上部署三个节点：一个存储节点，一个管理节点和一个网关节点。您应至少为主机提供九个存储卷。节点容器至少需要 300 GB 的性能层存储，系统数据和事务日志至少需要 6.7 GB 的性能层存储，对象数据至少需要 12 TB 的容量层存储。

节点类型	LUN 用途	LUN 数量	LUN 大小
存储节点	Docker 存储池	1.	300 GB （ 100 GB/ 节点 ）
存储节点	` /var/local` 卷	1.	90 GB
存储节点	对象数据	3.	12 TB （ 4 TB/LUN ）
管理节点	` /var/local` 卷	1.	90 GB
管理节点	管理节点审核日志	1.	200 GB

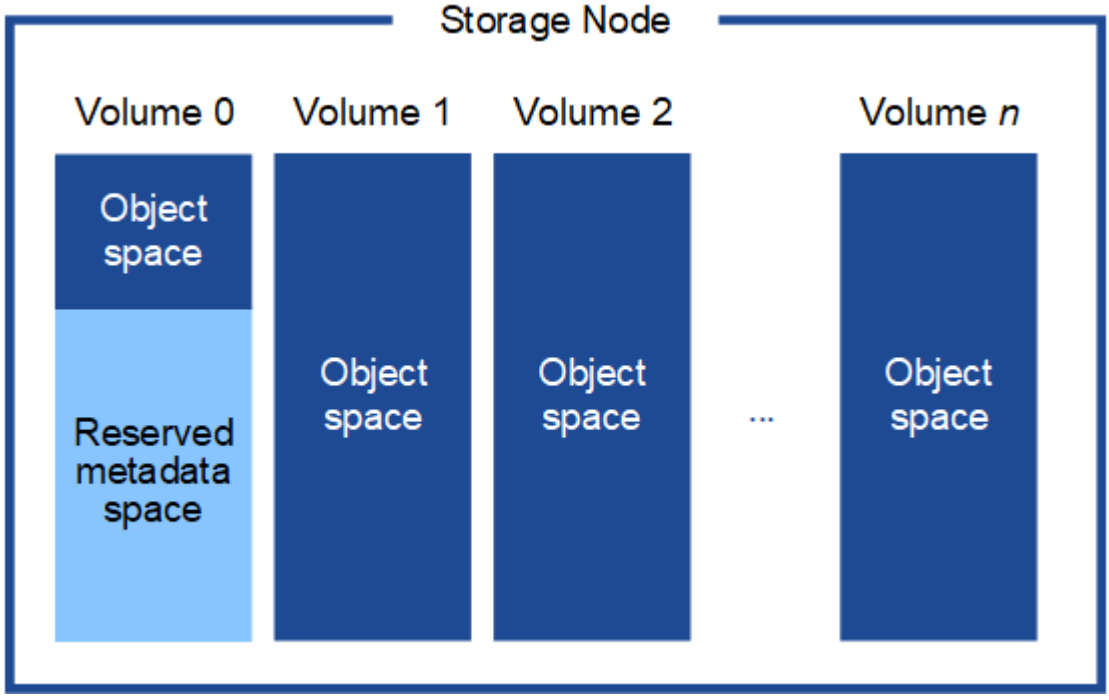
节点类型	**LUN** 用途	**LUN** 数量	**LUN** 大小
管理节点	管理节点表	1.	200 GB
网关节点	` /var/local` 卷	1.	90 GB
• 总计 *		**9**	• 容器池： * 300 GB • 系统数据： * 670GB • 对象数据： * 12 ，000 GB

存储节点的存储要求

一个基于软件的存储节点可以包含 1 到 16 个存储卷—建议使用 3 个或更多存储卷。每个存储卷应大于或等于 4 TB 。

一个设备存储节点最多可以包含 48 个存储卷。

如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。存储卷 0 和存储节点中的任何其他存储卷上的任何剩余空间专用于对象数据。



为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。对象元数据的三个副本均匀分布在每个站点的所有存储节点上。

在为新存储节点的卷 0 分配空间时，必须确保为该节点在所有对象元数据中的部分分配足够的空间。

- 您必须至少为卷 0 分配 4 TB 。

如果一个存储节点仅使用一个存储卷，而为该卷分配的存储空间不超过 4 TB ，则该存储节点可能会在启动时进入存储只读状态，并仅存储对象元数据。

- 如果要安装新的 StorageGRID 11.6 系统，并且每个存储节点的 RAM 为 128 GB 或更大，则应为卷 0 分配 8 TB 或更多。如果对卷 0 使用较大的值，则可以增加每个存储节点上允许的元数据空间。
- 在为站点配置不同的存储节点时，如果可能，请对卷 0 使用相同的设置。如果某个站点包含不同大小的存储节点，卷 0 最小的存储节点将确定该站点的元数据容量。

有关详细信息，请转至 管理对象元数据存储。

相关信息

节点容器迁移要求

恢复和维护

节点容器迁移要求

通过节点迁移功能，您可以手动将节点从一台主机移动到另一台主机。通常，两台主机位于同一物理数据中心。

通过节点迁移，您可以在不中断网格操作的情况下执行物理主机维护。您只需逐个将所有 StorageGRID 节点移动到另一台主机，然后再使物理主机脱机。迁移节点只需要每个节点短暂停机，不应影响网格服务的运行或可用性。

如果要使用 StorageGRID 节点迁移功能，则部署必须满足其他要求：

- 在一个物理数据中心的主机之间使用一致的网络接口名称
- StorageGRID 元数据和对象存储库卷的共享存储，可由单个物理数据中心中的所有主机访问。例如，您可以使用 NetApp E 系列存储阵列。

如果您使用的是虚拟主机，并且底层虚拟机管理程序层支持 VM 迁移，则可能需要使用此功能，而不是 StorageGRID 的节点迁移功能。在这种情况下，您可以忽略这些附加要求。

在执行迁移或虚拟机管理程序维护之前，请正常关闭节点。请参见的说明 关闭网格节点。

不支持 **VMware** 实时迁移

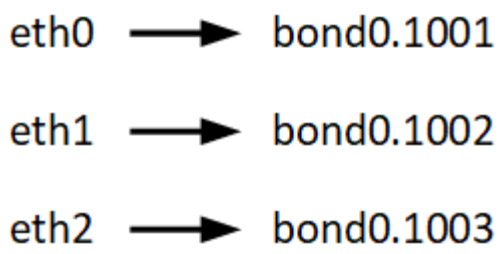
OpenStack 实时迁移和 VMware 实时 vMotion 发生原因 虚拟机时钟跳转时间，不支持任何类型的网格节点。尽管时钟时间不正确，但极少会导致数据丢失或配置更新。

支持冷迁移。在冷迁移中，您需要先关闭 StorageGRID 节点，然后再在主机之间迁移它们。请参见的说明 关闭网格节点。

网络接口名称一致

为了将节点从一台主机移动到另一台主机， StorageGRID 主机服务需要一定程度地确信该节点在其当前位置的外部网络连接可以在新位置进行复制。它可以通过在主机中使用一致的网络接口名称来获得这种信心。

例如，假设主机 1 上运行的 StorageGRID 节点 A 已配置以下接口映射：



箭头的左侧对应于从 StorageGRID 容器中查看的传统接口（即网格接口，管理接口和客户端网络接口）。箭头的右侧对应于提供这些网络的实际主机接口，它们是同一物理接口绑定下的三个 VLAN 接口。

现在，假设您要将节点 A 迁移到 Host2 。如果 Host2 还具有名为 bond0.1001 ， bond0.1002 和 bond0.1003 的接口，则系统将允许移动，前提是同名接口在 Host2 上提供的连接与在 Host1 上提供的连接相同。如果 Host2 的接口名称不相同，则不允许移动。

可以通过多种方法在多个主机之间实现一致的网络接口命名；请参见 配置主机网络 例如。

共享存储

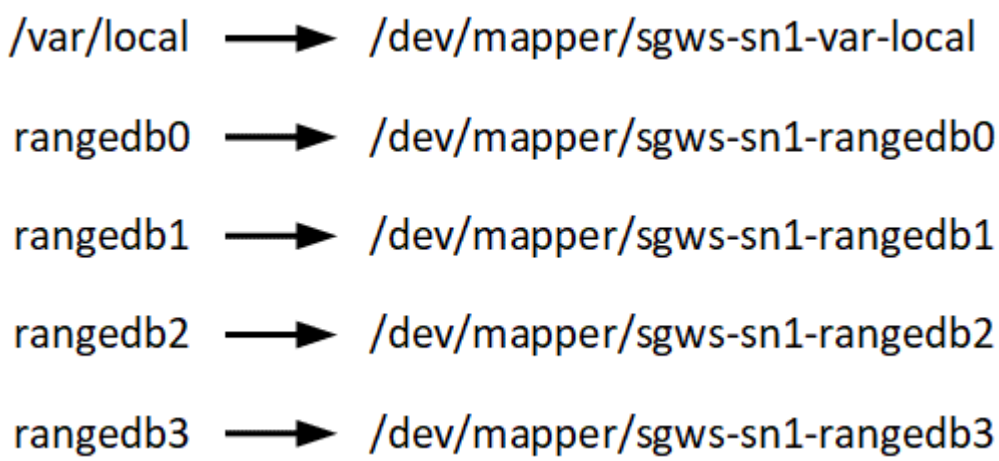
为了实现快速，低开销的节点迁移， StorageGRID 节点迁移功能不会物理移动节点数据。而是将节点迁移作为一对导出和导入操作来执行，如下所示：

步骤

1. 在 "`node export` " 操作期间，会从主机 A 上运行的节点容器中提取少量永久性状态数据，并将其缓存在该节点的系统数据卷上。然后，将对 HostA 上的节点容器进行实例化。
2. 在 "`node import` " 操作期间，系统将实例化 HostB 上使用与 HostA 相同的网络接口和块存储映射的节点容器。然后，缓存的永久性状态数据将插入到新实例中。

在这种操作模式下，节点的所有系统数据和对象存储卷都必须可从主机 A 和主机 B 访问，才能允许迁移并正常运行。此外，它们必须已使用名称映射到节点，这些名称可以保证引用主机 A 和主机 B 上的相同 LUN 。

以下示例显示了一个解决方案 ，用于 StorageGRID 存储节点的块设备映射，其中主机正在使用 DM 多路径，并且在 ` /etc/multipath.conf` 中使用了 alias 字段，以提供所有主机上可用的一致且友好的块设备名称。



部署工具

自动执行全部或部分 StorageGRID 安装可能会让您受益匪浅。

在以下任一情况下，自动部署可能会很有用：

- 您已使用标准业务流程框架（例如 Ansible ， Puppet 或 Chef ）部署和配置物理或虚拟主机。
- 您打算部署多个 StorageGRID 实例。
- 您正在部署一个大型的复杂 StorageGRID 实例。

StorageGRID 主机服务由软件包安装，并由配置文件驱动，这些配置文件可以在手动安装期间以交互方式创建，也可以提前准备（或以编程方式），以便使用标准业务流程框架实现自动安装。StorageGRID 提供了可选的 Python 脚本，用于自动配置 StorageGRID 设备和整个 StorageGRID 系统（ "`grid` " ）。您可以直接使用这些脚本，也可以对其进行检查，了解如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。

如果您希望自动执行全部或部分 StorageGRID 部署，请查看 自动安装 开始安装过程之前。

准备主机（ **Ubuntu** 或 **Debian** ）

安装 **Linux**

您必须在所有网格主机上安装 Linux 。使用 "NetApp 互操作性表工具" 以获取支持的版本列表。

步骤

1. 按照分销商的说明或您的标准操作步骤 在所有物理或虚拟网格主机上安装 Linux 。

   请勿安装任何图形桌面环境。安装 Ubuntu 时，必须选择 * 标准系统实用程序 * 。建议选择 * OpenSSH 服务器 * 以启用对 Ubuntu 主机的 ssh 访问。所有其他选项均可保持未选中状态。

2. 确保所有主机均可访问 Ubuntu 或 Debian 软件包存储库。
3. 如果已启用交换：

   a. 运行以下命令： ` $sudo swapoff -all`

   b. 从 ` /etc/fstab` 中删除所有交换条目以保留这些设置。

   如果未完全禁用交换，则会严重降低性能。

了解安装的 **AppArmor.** 配置文件

如果您在自行部署的 Ubuntu 环境中运行并使用了必需的 AppArmor-Access Control 系统，则与在基础系统上安装的软件包关联的 StorageGRID 配置文件可能会被随一起安装的相应软件包阻止。

默认情况下，系统会为您在基础操作系统上安装的软件包安装 AppArmort 配置文件。从 StorageGRID 系统容器运行这些软件包时，将阻止这些配置文件。DHCP ， MySQL ， NTP 和 TCdump 基本软件包与 AppArp 冲突，而其他基本软件包也可能发生冲突。

您可以选择两种方法来处理 AppArmor 配置文件：

- 为基础系统上安装的与 StorageGRID 系统容器中的软件包重叠的软件包禁用各个配置文件。禁用各个配置文件时， StorageGRID 日志文件中会显示一个条目，指示已启用。

  使用以下命令：

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

- 示例： *

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- 完全禁用 AppArmor 。对于 Ubuntu 9.10 或更高版本，请按照 Ubuntu 联机社区中的说明进行操作： "禁用 AppArmor"。

  禁用了 StorageGRID 后，日志文件中将不会显示任何指示已启用该功能的条目。

配置主机网络（ **Ubuntu** 或 **Debian** ）

在主机上完成 Linux 安装后，您可能需要执行一些额外的配置，以便在每个主机上准备一组适合映射到稍后要部署的 StorageGRID 节点的网络接口。

您需要的内容

- 您已查看 StorageGRID 网络连接准则。
- 您已查看有关的信息 节点容器迁移要求。
- 如果您使用的是虚拟主机，则已阅读 MAC 地址克隆的注意事项和建议 配置主机网络之前。

> 如果要使用 VM 作为主机，则应选择 VMXNET 3 作为虚拟网络适配器。VMware E1000 网络适配器已导致在某些 Linux 版本上部署 StorageGRID 容器时出现连接问题。

关于此任务

网格节点必须能够访问网格网络，还可以访问管理网络和客户端网络。您可以通过创建映射来提供此访问权限，此映射会将主机的物理接口与每个网格节点的虚拟接口相关联。创建主机接口时，请使用友好名称以方便在所有主机之间进行部署，并启用迁移。

同一接口可以在主机与一个或多个节点之间共享。例如，您可以使用相同的接口进行主机访问和节点管理网络访问，以便于维护主机和节点。尽管主机和各个节点之间可以共享同一接口，但所有接口都必须具有不同的 IP 地址。不能在节点之间或主机与任何节点之间共享 IP 地址。

您可以使用相同的主机网络接口为主机上的所有 StorageGRID 节点提供网格网络接口；可以为每个节点使用不同的主机网络接口；也可以在这两者之间执行操作。但是，通常不会提供与单个节点的网格和管理网络接口相同的主机网络接口，也不会提供与一个节点的网格网络接口和另一个节点的客户端网络接口相同的主机网络接口。

您可以通过多种方式完成此任务。例如，如果您的主机是虚拟机，而您要为每个主机部署一个或两个 StorageGRID 节点，则只需在虚拟机管理程序中创建正确数量的网络接口并使用一对一映射即可。如果要在裸机主机上部署多个节点以供生产使用，则可以利用 Linux 网络堆栈对 VLAN 和 LACP 的支持来实现容错和带宽共享。以下各节详细介绍了这两个示例的方法。您无需使用上述任一示例；您可以使用任何满足您需求的方法。

> 请勿直接使用绑定或网桥设备作为容器网络接口。这样做可能会阻止内核问题描述 在容器命名空间中对绑定和网桥设备使用 MACVLAN 导致节点启动。请改用非绑定设备，例如 VLAN 或虚拟以太网（ Veth ）对。在节点配置文件中指定此设备作为网络接口。

MAC 地址克隆的注意事项和建议

【Mac_address_cloning_Ubuntu】

MAC 地址克隆会使容器使用主机的 MAC 地址，而主机则使用您指定的地址或随机生成的地址的 MAC 地址。您应使用 MAC 地址克隆来避免使用混杂模式网络配置。

启用 **MAC** 克隆

在某些环境中，可以通过 MAC 地址克隆来增强安全性，因为它使您可以对管理网络，网格网络和客户端网络使用专用虚拟 NIC 。让容器使用主机上专用 NIC 的 MAC 地址可以避免使用混杂模式网络配置。

> MAC 地址克隆用于安装虚拟服务器，可能无法在所有物理设备配置中正常运行。

> 如果某个节点由于 MAC 克隆目标接口繁忙而无法启动，则在启动节点之前，您可能需要将链路设置为 " 关闭 " 。此外，在链路启动时，虚拟环境可能会阻止网络接口上的 MAC 克隆。如果某个节点由于接口繁忙而无法设置 MAC 地址并启动，则在启动该节点之前将链路设置为 " 关闭 " 可能会修复问题描述 。

默认情况下， MAC 地址克隆处于禁用状态，必须通过节点配置密钥进行设置。您应在安装 StorageGRID 时启用它。

每个网络有一个密钥：

- `admin_network_target_type_interface_clone_MAC`
- `grid_network_target_type_interface_clone_MAC`
- `client_network_target_type_interface_clone_MAC`

如果将密钥设置为 "true" ，则容器将使用主机 NIC 的 MAC 地址。此外，主机将使用指定容器网络的 MAC 地址。默认情况下，容器地址是随机生成的地址，但如果您使用 ` _network_MAC` 节点配置密钥设置了一个地址，则会改用该地址。主机和容器始终具有不同的 MAC 地址。

> 在虚拟主机上启用 MAC 克隆而不同时在虚拟机管理程序上启用混杂模式可能会使用主机的接口发生原因 Linux 主机网络连接停止工作。

Mac 克隆使用情形

MAC 克隆需要考虑两种使用情形：

- 未启用 MAC 克隆：如果节点配置文件中的 ` clone_mac` 密钥未设置或设置为 "false" ，则主机将使用主机 NIC MAC ，并且容器将具有 StorageGRID 生成的 MAC ，除非在 ` _network_mac` 密钥中指定了 MAC 。

如果在 ` _network_MAC` 项中设置了地址，则容器将具有在 ` _network_MAC` 项中指定的地址。此密钥配置要求使用混杂模式。

- 已启用 MAC 克隆：如果节点配置文件中的 ` clone_mac` 密钥设置为 "true" ，则容器将使用主机 NIC MAC ，而主机将使用 StorageGRID 生成的 MAC ，除非在 ` _network_mac` 密钥中指定了 MAC 。如果在 ` _network_MAC` 项中设置了地址，则主机将使用指定的地址，而不是生成的地址。在此密钥配置中，不应使用混杂模式。

> 如果您不希望使用 MAC 地址克隆，而希望允许所有接口接收和传输非虚拟机管理程序分配的 MAC 地址的数据， 对于配置模式， MAC 地址更改和伪造传输，请确保虚拟交换机和端口组级别的安全属性设置为 * 接受 * 。虚拟交换机上设置的值可以被端口组级别的值覆盖，因此请确保这两个位置的设置相同。

要启用 MAC 克隆，请参见 有关创建节点配置文件的说明。

Mac 克隆示例

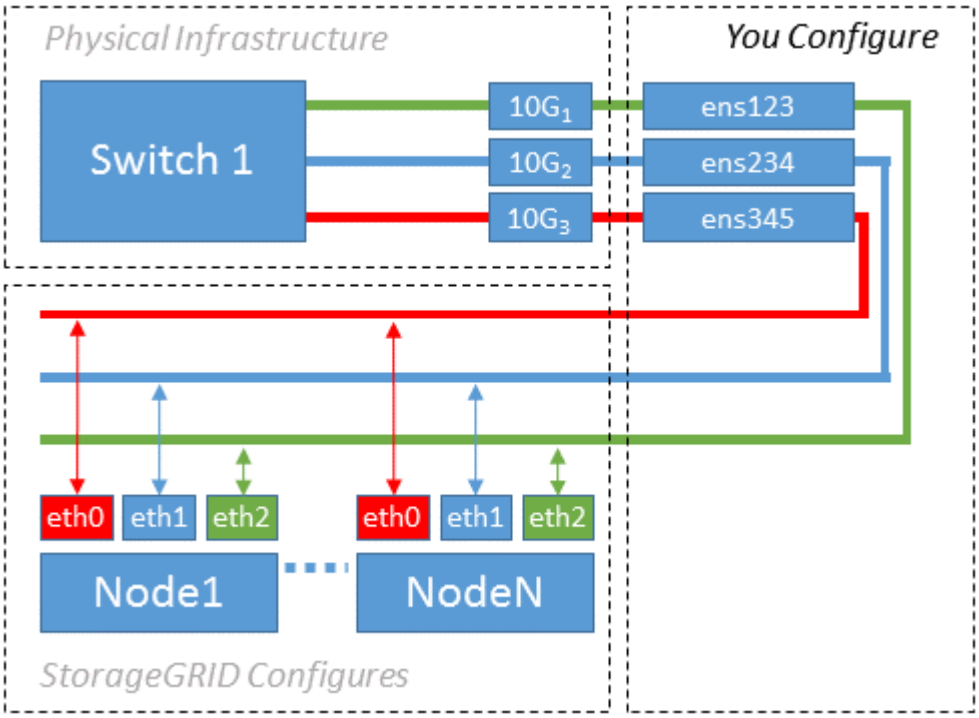
在 MAC 地址为 11： 22： 33： 44： 55： 66 的主机上为接口 ens256 启用 MAC 克隆的示例，以及节点配置文件中的以下密钥：

- `admin_network_target = ens256`
- `admin_network_MAC = B2 : 9c : 02 : C2 : 27 : 10`
- `admin_network_target_type_interface_clone_MAC = true`

结果： ens256 的主机 MAC 为 B2： 9c： 02： C2： 27： 10 ，管理网络 MAC 为 11： 22： 33： 44： 55： 66

示例 **1** ： 映射到物理或虚拟 **NIC** 的一对一映射

示例 1 介绍了一个简单的物理接口映射，该映射只需要很少的主机端配置或根本不需要主机端配置。



Linux 操作系统会在安装或启动期间或热添加接口时自动创建 ensXYZ 接口。除了确保接口设置为在启动后自动启动之外，无需进行任何配置。您必须确定哪个 ensXYZ 与哪个 StorageGRID 网络（网格，管理员或客户端）相对应，以便稍后在配置过程中提供正确的映射。

请注意，此图显示了多个 StorageGRID 节点；但是，通常情况下，您会对单节点 VM 使用此配置。

如果交换机 1 是物理交换机，则应将连接到接口 $10G_1$ 到 $10G_3$ 的端口配置为访问模式，并将其放置在相应的 VLAN 上。

示例 2： LACP 绑定传输 VLAN

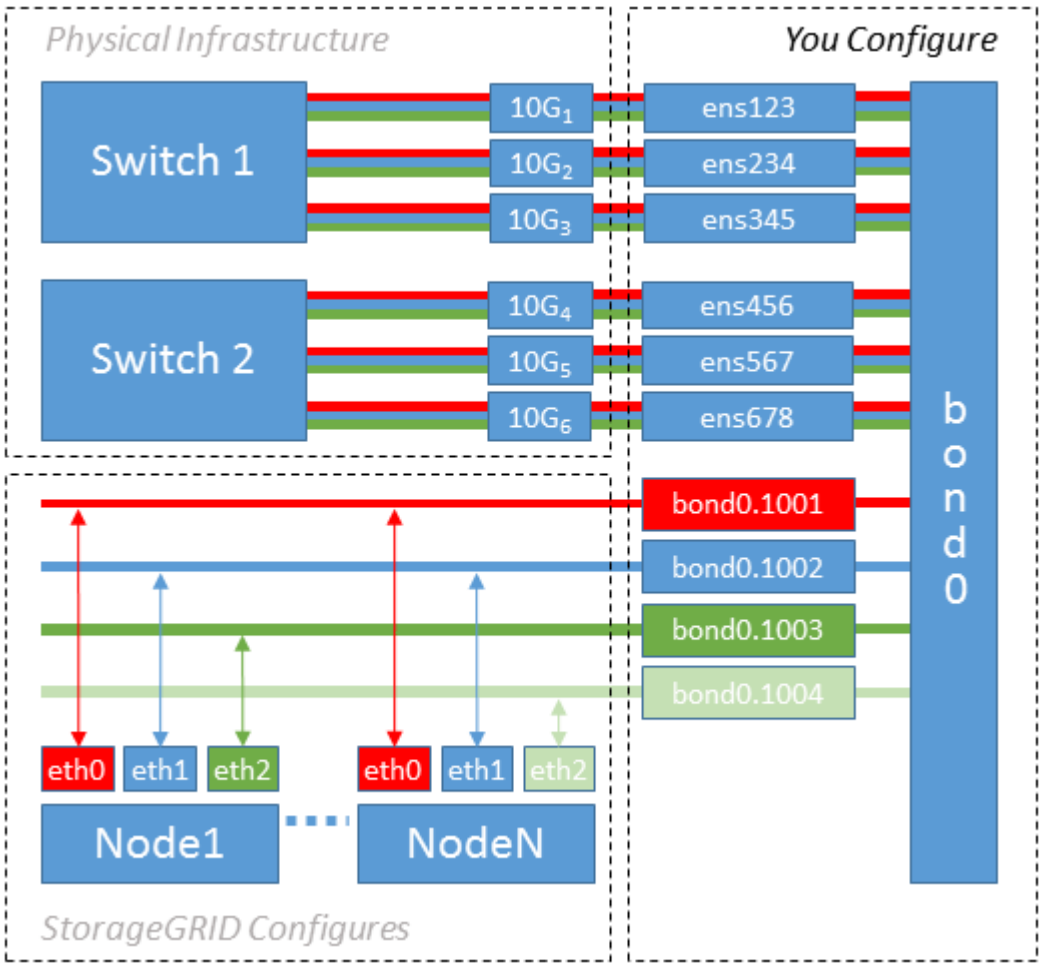
示例 2 假定您熟悉绑定网络接口以及在所使用的 Linux 分发版上创建 VLAN 接口。

关于此任务

示例 2 介绍了一种基于 VLAN 的通用灵活方案，该方案有助于在单个主机上的所有节点之间共享所有可用网络带宽。此示例尤其适用于裸机主机。

要了解此示例，假设每个数据中心有三个单独的网格网络，管理员网络和客户端网络子网。子网位于不同的 VLAN （ 1001 ， 1002 和 1003 ）上，并通过 LACP 绑定的中继端口（ bond0 ）提供给主机。您应在此绑定上配置三个 VLAN 接口： bond0.1001 ， bond0.1002 和 bond0.1003 。

如果同一主机上的节点网络需要单独的 VLAN 和子网，则可以在绑定上添加 VLAN 接口并将其映射到主机（如图中的 bond0.1004 所示）。



步骤

1. 将用于 StorageGRID 网络连接的所有物理网络接口聚合到一个 LACP 绑定中。

   对每个主机上的绑定使用相同的名称，例如 bond0 。

2. 使用标准 VLAN 接口命名约定 `physdev-name.vlan ID` 创建使用此绑定作为关联 "`物理设备，`" 的 VLAN 接口。

   请注意，步骤 1 和 2 要求对终止网络链路另一端的边缘交换机进行适当配置。此外，边缘交换机端口还必须聚合到 LACP 端口通道中，并配置为中继，并允许通过所有必需的 VLAN 。

   本文档提供了此每主机网络配置方案的示例接口配置文件。

相关信息

/etc/network/interfaces 示例

配置主机存储

您必须为每个主机分配块存储卷。

您需要的内容

您已阅读以下主题，其中提供了完成此任务所需的信息：

存储和性能要求

节点容器迁移要求

关于此任务

在将块存储卷（ LUN ）分配给主机时，请使用 S存储要求 中的表确定以下内容：

- 每个主机所需的卷数（根据要在该主机上部署的节点的数量和类型）
- 每个卷的存储类别（即系统数据或对象数据）
- 每个卷的大小

在主机上部署 StorageGRID 节点时，您将使用此信息以及 Linux 为每个物理卷分配的永久性名称。

> 您无需对其中任何卷进行分区，格式化或挂载；您只需确保这些卷对主机可见即可。

在编写卷名称列表时，请避免使用 "`raw`" 特殊设备文件（例如，`/dev/sdb`）。这些文件可能会在主机重新启动后发生更改，从而影响系统的正常运行。如果您使用的是 iSCSI LUN 和设备映射程序多路径，请考虑在 `/dev/mapper` 目录中使用多路径别名，尤其是在 SAN 拓扑包含指向共享存储的冗余网络路径时。或者，您也可以在 `/dev/disk/by-path/` 下使用系统创建的软链接作为永久性设备名称。

例如：

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

每个安装的结果会有所不同。

为每个块存储卷分配友好名称，以简化初始 StorageGRID 安装和未来维护过程。如果使用设备映射程序多路径驱动程序对共享存储卷进行冗余访问，则可以在 ` /etc/multipath.conf` 文件中使用 `alias` 字段。

例如：

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

这样就会对别名进行发生原因，使其显示为主机上的 ` /dev/mapper` 目录中的块设备，从而可以在配置或维护操作需要指定块存储卷时指定一个易于验证的友好名称。

> 如果要设置共享存储以支持 StorageGRID 节点迁移并使用设备映射程序多路径功能，则可以在所有主机上创建并安装通用的 ` /etc/multipath.conf` 。只需确保在每个主机上使用不同的 Docker 存储卷即可。使用别名并将目标主机名包含在每个 Docker 存储卷 LUN 的别名中，这一点便于记住，建议这样做。

相关信息

存储和性能要求

节点容器迁移要求

配置 **Docker** 存储卷

在安装 Docker 之前，您可能需要格式化 Docker 存储卷并将其挂载到 ` /var/lib/Docker` 上。

关于此任务

如果您计划对 Docker 存储卷使用本地存储，并且包含 ` /var/lib` 的主机分区上有足够的可用空间，则可以跳过这些步骤。

步骤

1. 在 Docker 存储卷上创建文件系统：

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. 挂载 Docker 存储卷：

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. 将 Docker 存储卷设备条目添加到 /etc/fstab 中。

   此步骤可确保存储卷将在主机重新启动后自动重新挂载。

安装 **Docker**

StorageGRID 系统作为一组 Docker 容器在 Linux 上运行。在安装 StorageGRID 之前，您必须先安装 Docker 。

步骤

1. 按照适用于您的 Linux 版本的说明安装 Docker 。

   如果您的 Linux 分发版不包含 Docker ，您可以从 Docker 网站下载它。

2. 运行以下两个命令，确保已启用并启动 Docker：

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 输入以下命令确认您已安装预期版本的 Docker：

```
sudo docker version
```

客户端和服务器版本必须为 1.11.0 或更高版本。

相关信息

配置主机存储

安装 **StorageGRID** 主机服务

您可以使用 StorageGRID Deb 软件包安装 StorageGRID 主机服务。

关于此任务

以下说明介绍如何从 Deb 软件包安装主机服务。或者，您也可以使用安装归档中包含的 APT 存储库元数据远程安装 Deb 软件包。请参见适用于 Linux 操作系统的 APT 存储库说明。

步骤

1. 将 StorageGRID Deb 软件包复制到每个主机，或使其在共享存储上可用。

   例如，将其放置在 ` /tmp` 目录中，以便您可以在下一步中使用示例命令。

2. 以 root 身份或使用具有 sudo 权限的帐户登录到每个主机，然后运行以下命令。

   您必须先安装 `images` 软件包，再安装 `sservice` 软件包。如果您将软件包放置在非 ` /tmp` 目录中，请修改命令以反映您使用的路径。

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
   ```

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
   ```

   必须先安装 Python 2.7 ，然后才能安装 StorageGRID 软件包。`sudo dpkg -install /tmp/storagegrid-webscale-images-version-SHA.deb` 命令将失败，直到您执行此操作为止。

部署虚拟网格节点（ **Ubuntu** 或 **Debian** ）

为 **Ubuntu** 或 **Debian** 部署创建节点配置文件

节点配置文件是一个小型文本文件，用于提供 StorageGRID 主机服务启动节点并将其连接到适当的网络和块存储资源所需的信息。节点配置文件用于虚拟节点，不用于设备节点。

应将节点配置文件放在何处?

您必须将每个 StorageGRID 节点的配置文件放置在要运行该节点的主机上的 ` /etc/storaggrid/nodes` 目录中。例如，如果您计划在主机 A 上运行一个管理节点，一个网关节点和一个存储节点，则必须将三个节点配置文件放置在主机 A 上的 ` /etc/storaggrid/nodes` 中。您可以使用文本编辑器（例如 vim 或 nanan ）在每个主机上直接创建配置文件，也可以在其他位置创建配置文件并将其移动到每个主机。

节点配置文件的名称是什么?

配置文件的名称非常重要。格式为 `node-name.conf` ，其中 `node-name` 是您分配给节点的名称。此名称显示在 StorageGRID 安装程序中，用于节点维护操作，例如节点迁移。

节点名称必须遵循以下规则：

- 必须是唯一的
- 必须以字母开头
- 可以包含字符 A 到 Z 和 a 到 z
- 可以包含数字 0 到 9
- 可以包含一个或多个连字符（ - ）
- 不得超过 32 个字符，不包括 ` 。 conf` 扩展名

主机服务不会解析 ` /etc/storaggrid/nodes` 中不符合这些命名约定的任何文件。

如果您为网格规划了多站点拓扑，则典型的节点命名方案可能是：

```
site-nodetype-nodenumber.conf
```

例如，您可以对 Data Center 1 中的第一个管理节点使用 `dc1-adm1.conf` ，而对 Data Center 2 中的第三个存储节点使用 `dc2-SN3.conf` 。但是，只要所有节点名称都遵循命名规则，您就可以使用所需的任何方案。

节点配置文件中的内容是什么?

配置文件包含密钥 / 值对，每行一个密钥和一个值。对于每个密钥 / 值对，您必须遵循以下规则：

- 密钥和值必须以等号（` =` ）和可选空格分隔。
- 密钥不能包含空格。
- 这些值可以包含嵌入的空格。
- 忽略任何前导或尾随空格。

每个节点都需要一些密钥，而其他密钥则是可选的，或者仅适用于某些节点类型。

下表定义了所有支持的密钥的可接受值。在中间列中：

- R* ： 必填项 + bp ： 最佳实践 + O ： 可选

密钥	**R** ， **Bp** 或 **O** ？	价值
admin_ip	bp	此节点所属网格的主管理节点的网格网络 IPv4 地址。使用为 node_type = VM_Admin_Node 且 admin_role = Primary 的网格节点的 grid_network_IP 指定的相同值。如果省略此参数，则节点将尝试使用 mDNS 发现主管理节点。 网格节点如何发现主管理节点 • 注 * ： 此值在主管理节点上被忽略，并且可能被禁止。
admin_network_config	O	DHCP ，静态或已禁用
admin_network_esl	O	此节点应通过管理网络网关与 CIDR 表示法中的子网列表，以逗号分隔。 示例： `172.16.0.0/21.172.17.0.0/21`

admin_network_gateway	O （ * R* ）	此节点的本地管理网络网关的 IPv4 地址。必须位于 admin_network_ip 和 admin_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。
		
		• 注释 * ： 如果指定 admin_network_esl ，则需要此参数。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

admin_network_ip	O	此节点在管理网络上的 IPv4 地址。只有当 admin_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

admin_network_MAC	O	容器中管理网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `B2 ： 9c ： 02 ： C2 ： 27 ： 10`

密钥	**R** ， **Bp** 或 **O** ？	价值

admin_network_mask	O	此节点的 IPv4 网络掩码，位于管理网络上。只有当 admin_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`255.255.255.0`
		
		`255.255.248.0`

admin_network_mtu	O	管理网络上此节点的最大传输单元（ MTU ）。请勿指定 admin_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
		
		如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
		
		• 重要信息 * ： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
		
		示例
		
		`1500`
		
		`8192`

admin_network_target	bp	StorageGRID 节点用于管理网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 grid_network_target 或 client_network_target 指定的接口名称不同。
		
		• 注 * ： 请勿使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
		• 最佳实践 * ： 指定一个值，即使此节点最初不具有管理员网络 IP 地址也是如此。然后，您可以稍后添加管理员网络 IP 地址，而无需重新配置主机上的节点。
		
		示例
		
		`bond0.1002`
		
		`ens256`

密钥	R ， Bp 或 O ？	价值
admin_network_target_type	O	接口 （这是唯一受支持的值。）
admin_network_target_type_interface_clone_MAC	bp	判断对错 将密钥设置为 "true" 以发生原因 StorageGRID 容器使用管理网络上主机主机目标接口的 MAC 地址。 • 最佳实践： * 在需要混杂模式的网络中，请改用 admin_network_target_type_interface_clone_MAC 密钥。 有关 MAC 克隆的详细信息，请参见： MAC 地址克隆的注意事项和建议（ Red Hat Enterprise Linux 或 CentOS ） MAC 地址克隆（ Ubuntu 或 Debian ）的注意事项和建议
管理角色	• R*	主卷或非主卷 只有当 node_type = VM_Admin_Node 时才需要此密钥；不要为其他节点类型指定此密钥。

block_device_audit_logs	• R*	此节点将用于永久存储审核日志的块设备专用文件的路径和名称。只有 node_type = VM_Admin_Node 的节点才需要此密钥；不要为其他节点类型指定此密钥。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-ad1-audit-logs`

密钥	R ， Bp 或 O ？	价值

block_device_RANGEDB_000
 	
block_device_RANGEDB_001
 	
block_device_RANGEDB_002
 	
block_device_RANGEDB_003
 	
block_device_RANGEDB_004
 	
block_device_RANGEDB_005
 	
block_device_RANGEDB_006
 	
block_device_RANGEDB_007
 	
block_device_RANGEDB_008
 	
block_device_RANGEDB_009
 	
block_device_RANGEDB_010
 	
block_device_RANGEDB_011
 	
block_device_RANGEDB_012
 	
block_device_RANGEDB_013
 	
block_device_RANGEDB_014
 	
block_device_RANGEDB_015
	• R*	此节点将用于永久性对象存储的块设备专用文件的路径和名称。只有 node_type = VM_Storage_Node 的节点才需要此密钥；不要为其他节点类型指定此密钥。
		
		仅需要 block_device_RANGEDB_000 ；其余为可选。为 block_device_RANGEDB_000 指定的块设备必须至少为 4 TB ；其他块设备可以更小。
		
		请勿留下空隙。如果指定 block_device_RANGEDB_005 ，则还必须指定 block_device_RANGEDB_004 。
		
		• 注 * ： 为了与现有部署兼容，升级后的节点支持两位数的密钥。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-SN1-rangedb-000`

密钥	**R** ， **Bp** 或 **O** ？	价值

block_device_tables	• R*	此节点将用于永久存储数据库表的块设备专用文件的路径和名称。只有 node_type = VM_Admin_Node 的节点才需要此密钥；不要为其他节点类型指定此密钥。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-ad1-tables`

block_device_var_local	• R*	此节点将用于其 /var/local 永久性存储的块设备专用文件的路径和名称。
		
		示例
		
		` /dev/disk/by-path/PCI-0000： 03： 00.0-SCSI-0： 0： 0： 0： 0`
		
		` /dev/disk/by-id/WWS-0x600a09800059d6df000060d757b475fd`
		
		` /dev/mapper/sgws-SN1-var-local`

client_network_config	O	DHCP ，静态或已禁用

client_network_gateway	O	此节点的本地客户端网络网关的 IPv4 地址，该地址必须位于 client_network_ip 和 client_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

client_network_IP	O	此节点在客户端网络上的 IPv4 地址。只有当 client_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

密钥	**R** ， **Bp** 或 **O** ？	价值
客户端网络 MAC	O	容器中客户端网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `B2 ： 9c ： 02 ： C2 ： 27 ： 20`

client_network_mask	O	此节点在客户端网络上的 IPv4 网络掩码。只有当 client_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`255.255.255.0`
		
		`255.255.248.0`

client_network_mtu	O	客户端网络上此节点的最大传输单元（ MTU ）。请勿指定 client_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
		
		如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
		
		• 重要信息 *： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
		
		示例
		
		`1500`
		
		`8192`

密钥	**R** ， **Bp** 或 **O** ？	价值

client_network_target	bp	StorageGRID 节点用于客户端网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 grid_network_target 或 admin_network_target 指定的接口名称不同。
		
		• 注 * ：请勿使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
		• 最佳实践： * 指定一个值，即使此节点最初不会具有客户端网络 IP 地址也是如此。然后，您可以稍后添加客户端网络 IP 地址，而无需重新配置主机上的节点。
		
		示例
		
		`bond0.1003`
		
		`ens423`

client_network_target_type	O	接口 （此值仅受支持。）
client_network_target_type_interface_clone_MAC	bp	判断对错 将密钥设置为 "true" ，以便对 StorageGRID 容器进行发生原因 处理，以使用客户端网络上主机目标接口的 MAC 地址。 • 最佳实践： * 在需要混杂模式的网络中，请改用 client_network_target_type_interface_clone_MAC 密钥。 有关 MAC 克隆的详细信息，请参见： MAC 地址克隆的注意事项和建议（ Red Hat Enterprise Linux 或 CentOS ） MAC 地址克隆（ Ubuntu 或 Debian ）的注意事项和建议
grid_network_config	bp	静态或 DHCP （如果未指定，则默认为 static 。）

密钥	**R** ， **Bp** 或 **O** ？	价值
grid_network_gateway	• R*	此节点的本地网格网络网关的 IPv4 地址，该网关必须位于 grid_network_ip 和 grid_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。 如果网格网络是没有网关的单个子网，请使用该子网的标准网关地址（ X.y.Z.1 ）或此节点的 GRID_NETWORK_IP 值；任一值都将简化未来可能进行的网格网络扩展。

GRID_NETWORK_IP	• R*	此节点在网格网络上的 IPv4 地址。只有当 grid_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`1.1.1.1`
		
		`10.2244.81`

GRID_NETWORK_MAC	O	容器中网格网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例：`B2 ： 9c ： 02 ： C2 ： 27 ： 30`

grid_network_mask	O	此节点在网格网络上的 IPv4 网络掩码。只有当 grid_network_config = static 时才需要此密钥；不要为其他值指定此密钥。
		
		示例
		
		`255.255.255.0`
		
		`255.255.248.0`

密钥	**R** ， **Bp** 或 **O** ？	价值
grid_network_mtu	O	网格网络上此节点的最大传输单元（ MTU ）。请勿指定 grid_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。 如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。 • 重要信息 *： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。 • 重要信息 *： 为获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。 示例 1500 8192

grid_network_target	• R*	StorageGRID 节点要用于网格网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 admin_network_target 或 client_network_target 指定的接口名称不同。
		
		• 注 *： 请勿使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
		
		示例
		
		`bond0.1001`
		
		`ens192`

grid_network_target_type	O	接口 （这是唯一受支持的值。）

密钥	**R** ， **Bp** 或 **O** ？	价值
grid_network_target_type_interface_clone_MAC	• bp*	判断对错 将密钥值设置为 "true" ，以便对 StorageGRID 容器进行发生原因 处理，以使用网格网络上主机目标接口的 MAC 地址。 • 最佳实践： * 在需要混杂模式的网络中，请改用 grid_network_target_type_interface_clone_MAC 密钥。 有关 MAC 克隆的详细信息，请参见： MAC 地址克隆的注意事项和建议（ Red Hat Enterprise Linux 或 CentOS ） MAC 地址克隆（ Ubuntu 或 Debian ）的注意事项和建议
interfaces_target_nnnn	O	要添加到此节点的额外接口的名称和可选问题描述 。您可以向每个节点添加多个额外接口。 对于 *nnnn* ，请为要添加的每个 interfaces_target 条目指定一个唯一编号。 对于此值，请指定裸机主机上物理接口的名称。然后，也可以添加一个逗号并提供接口的问题描述 ，该接口将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。 例如： `interfaces_target_01=ens256 ， Trunk` 如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。

密钥	**R** ， **Bp** 或 **O** ？	价值

最大 RAM	O	此节点允许使用的最大 RAM 量。如果省略此密钥，则节点不存在内存限制。在为生产级节点设置此字段时，请指定一个值，该值应至少比系统 RAM 总量少 24 GB ，并且要少 16 到 32 GB 。
		
		• 注 *： RAM 值会影响节点的实际元数据预留空间。请参见有关管理 StorageGRID 的说明 用于问题描述 的元数据预留空间。
		
		此字段的格式为 ` < 数字 >< 单位 >` ，其中 ` < 单位 >` 可以是 `b` ， `k` ， `m` 或 `g` 。
		
		示例
		
		`24G`
		
		`38654705664b`
		
		• 注 *：如果要使用此选项，必须为内存 cgroups 启用内核支持。

node_type	• R*	节点类型： VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway
port_remap	O	重新映射节点用于内部网格节点通信或外部通信的任何端口。如果企业网络策略限制 StorageGRID 使用的一个或多个端口，则必须重新映射端口，如 "`内部网格节点通信` " 或 "`外部通信 " 中所述。` • 重要信息 *：请勿重新映射计划用于配置负载平衡器端点的端口。 • 注意 *：如果仅设置 port_remap ，则指定的映射将同时用于入站和出站通信。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。 使用的格式为： ` < 网络类型 >/< 协议 >/< 网格节点使用的默认端口 >/< 新端口 >` ，其中 ` < 网络类型 >` 是网格，管理员或客户端，协议是 TCP 或 UDP 。 例如： `port_remap = client/TCP/18082/443`

密钥	**R** ， **Bp** 或 **O** ？	价值
port_remap_inbound	O	将入站通信重新映射到指定端口。如果指定 port_remap_inbound ，但未指定 port_remap 的值，则端口的出站通信将保持不变。 • 重要信息 * ：请勿重新映射计划用于配置负载平衡器端点的端口。 使用的格式为： ` < 网络类型 >/< 协议： >/< 网格节点使用的默认端口 >/< 网格节点使用的默认端口 >` ，其中 ` < 网络类型 >` 是网格，管理员或客户端，协议是 TCP 或 UDP 。 例如： `port_remap_inbound = grid/tcp/3022/22`

相关信息

网络连接准则

网格节点如何发现主管理节点

网格节点与主管理节点进行通信以进行配置和管理。每个网格节点都必须知道网格网络上主管理节点的 IP 地址。

为了确保网格节点可以访问主管理节点，您可以在部署此节点时执行以下任一操作：

- 您可以使用 admin_ip 参数手动输入主管理节点的 IP 地址。
- 您可以省略 admin_ip 参数，以使网格节点自动发现该值。当网格网络使用 DHCP 为主管理节点分配 IP 地址时，自动发现尤其有用。

可以使用多播域名系统（ mDNS ）自动发现主管理节点。主管理节点首次启动时，它会使用 mDNS 发布其 IP 地址。然后，同一子网上的其他节点可以查询 IP 地址并自动获取该地址。但是，由于多播 IP 流量通常不能跨子网路由，因此其他子网上的节点无法直接获取主管理节点的 IP 地址。

如果使用自动发现：

- 必须在主管理节点未直接连接到的任何子网上至少包含一个网格节点的 admin_IP 设置。然后，此网格节点将发布子网中其他节点的主管理节点 IP 地址，以便使用 mDNS 进行发现。
- 确保您的网络基础架构支持在子网内传递多播 IP 流量。

示例节点配置文件

您可以使用示例节点配置文件帮助设置 StorageGRID 系统的节点配置文件。这些示例显示了所有类型网格节点的节点配置文件。

对于大多数节点，在使用网格管理器或安装 API 配置网格时，您可以添加管理员和客户端网络地址信息（ IP ，掩码，网关等）。主管理节点除外。如果要浏览到主管理节点的管理网络 IP 以完成网格配置（例如，由于网格

网络未路由），则必须在主管理节点的节点配置文件中配置主管理节点的管理网络连接。示例显示了这一点。

> 在这些示例中，已将客户端网络目标配置为最佳实践，即使客户端网络默认处于禁用状态也是如此。

主管理节点的示例

- 示例文件名 * ： ` /etc/storagegRid/nodes/DC1-ad1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

存储节点示例

- 示例文件名： * ` /etc/storagegRid/nodes/DC1-SN1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

归档节点示例

- 示例文件名： * ` /etc/storagegriid/nodes/DC1-arc1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

网关节点示例

- 示例文件名： * ` /etc/storagegRid/nodes/DC1-GW1.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

非主管理节点的示例

- 示例文件名： * ` /etc/storagegRid/nodes/DC1-adm2.conf`
- 示例文件内容： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

验证 **StorageGRID** 配置

在 ` /etc/storaggrid/nodes` 中为每个 StorageGRID 节点创建配置文件后，您必须验证这些文件的内容。

要验证配置文件的内容，请在每个主机上运行以下命令：

```
sudo storagegrid node validate all
```

如果这些文件正确无误，则输出将为每个配置文件显示 * 已通过 * ，如示例所示。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

对于自动安装，您可以通过在 `StorageGRID` 命令中使用 ` -q` 或 ` -quiet` 选项（例如，`StorageGRID --quiet …`）来禁止此输出。如果禁止输出，则在检测到任何配置警告或错误时，命令的退出值将为非零。

如果配置文件不正确，则这些问题将显示为 * 警告 * 和 * 错误 * ，如示例所示。如果发现任何配置错误，则必须先更正这些错误，然后再继续安装。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

启动 **StorageGRID** 主机服务

要启动 StorageGRID 节点并确保它们在主机重新启动后重新启动，您必须启用并启动 StorageGRID 主机服务。

步骤

1. 在每个主机上运行以下命令：

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 运行以下命令以确保部署正在进行：

```
sudo storagegrid node status node-name
```

对于返回状态为 "`not running` " 或 " S顶部 " 的任何节点，请运行以下命令：

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

3. 如果您先前已启用并启动 StorageGRID 主机服务（或者不确定此服务是否已启用和启动），请同时运行以下命令：

```
sudo systemctl reload-or-restart storagegrid
```

配置网格并完成安装（ **Ubuntu** 或 **Debian** ）

导航到网格管理器

您可以使用网格管理器定义配置 StorageGRID 系统所需的所有信息。

您需要的内容

必须部署主管理节点，并且已完成初始启动序列。

步骤

1. 打开 Web 浏览器并导航到以下地址之一：

```
https://primary_admin_node_ip

client_network_ip
```

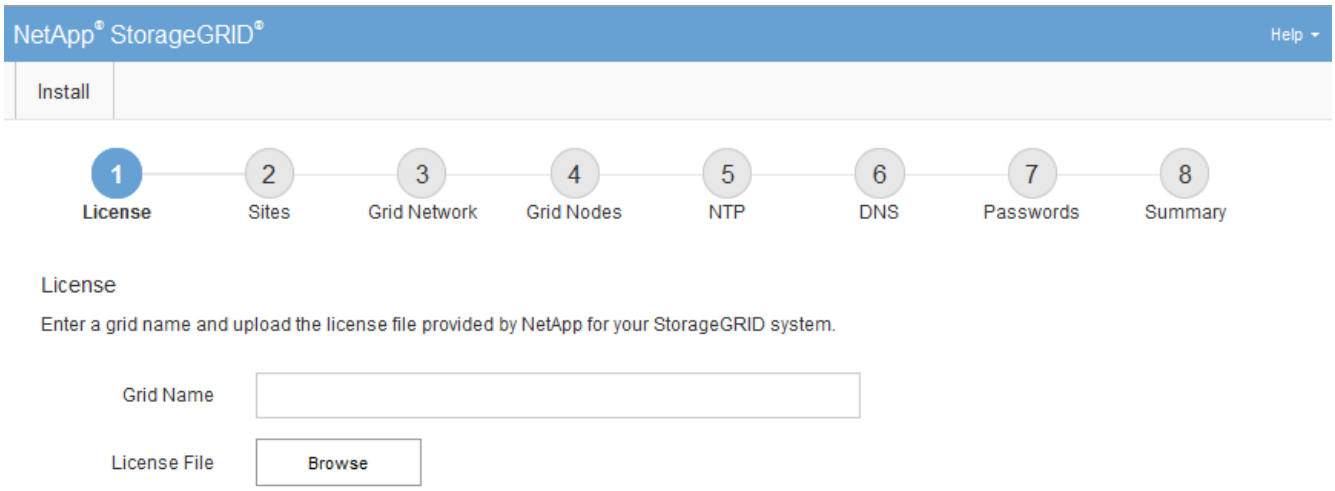
或者，您也可以通过端口 8443 访问网格管理器：

```
https://primary_admin_node_ip:8443
```

根据您的网络配置，您可以使用网格网络或管理网络上的主管理节点 IP 的 IP 地址。

1. 单击 * 安装 StorageGRID 系统 * 。

此时将显示用于配置 StorageGRID 网格的页面。



指定 **StorageGRID** 许可证信息

您必须指定 StorageGRID 系统的名称并上传 NetApp 提供的许可证文件。

步骤

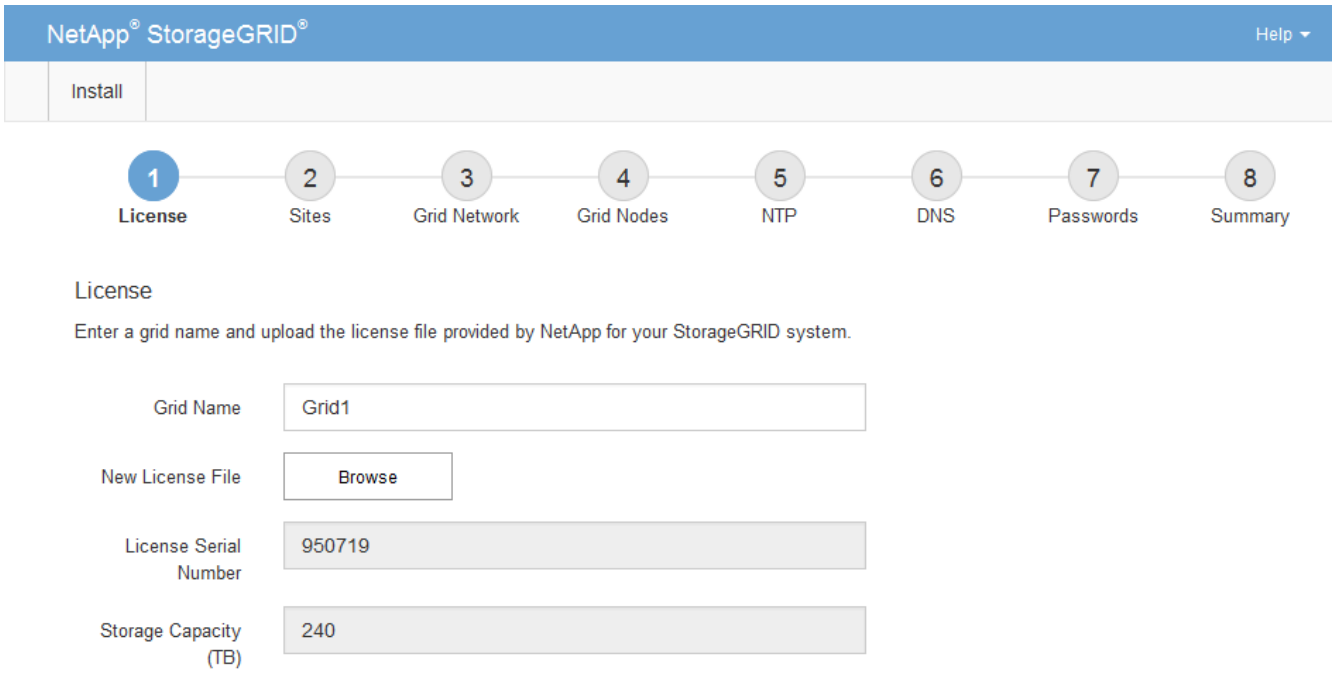
1. 在许可证页面上，在 * 网格名称 * 中为您的 StorageGRID 系统输入一个有意义的名称。

   安装后，此名称将显示在节点菜单的顶部。

2. 单击 * 浏览 * ，找到 NetApp 许可证文件（`NLFunique_id.txt`），然后单击 * 打开 * 。

   此时将验证许可证文件，并显示序列号和许可的存储容量。

   StorageGRID 安装归档包含一个免费许可证，不提供产品的任何支持授权。您可以在安装后更新为提供支持的许可证。



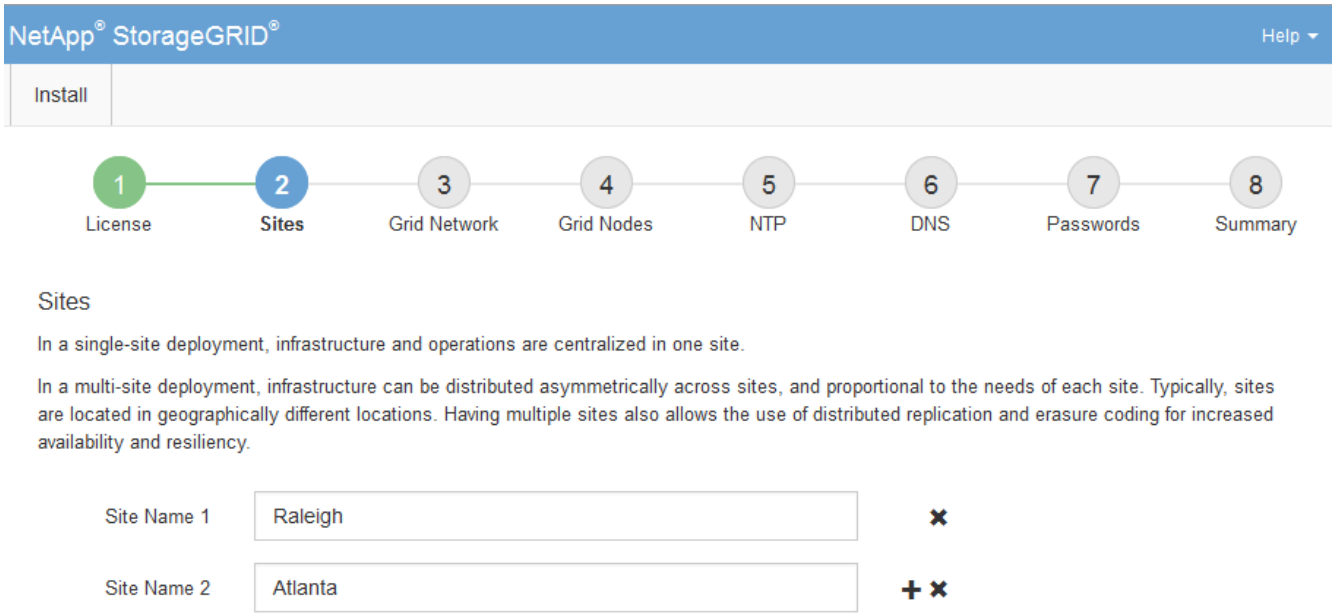
3. 单击 * 下一步 * 。

添加站点

安装 StorageGRID 时，必须至少创建一个站点。您可以创建其他站点来提高 StorageGRID 系统的可靠性和存储容量。

1. 在 Sites 页面上，输入 * 站点名称 * 。
2. 要添加其他站点，请单击最后一个站点条目旁边的加号，然后在新的 * 站点名称 * 文本框中输入名称。

   根据需要为网格拓扑添加尽可能多的其他站点。您最多可以添加 16 个站点。



3. 单击 * 下一步 * 。

指定网格网络子网

您必须指定网格网络上使用的子网。

关于此任务

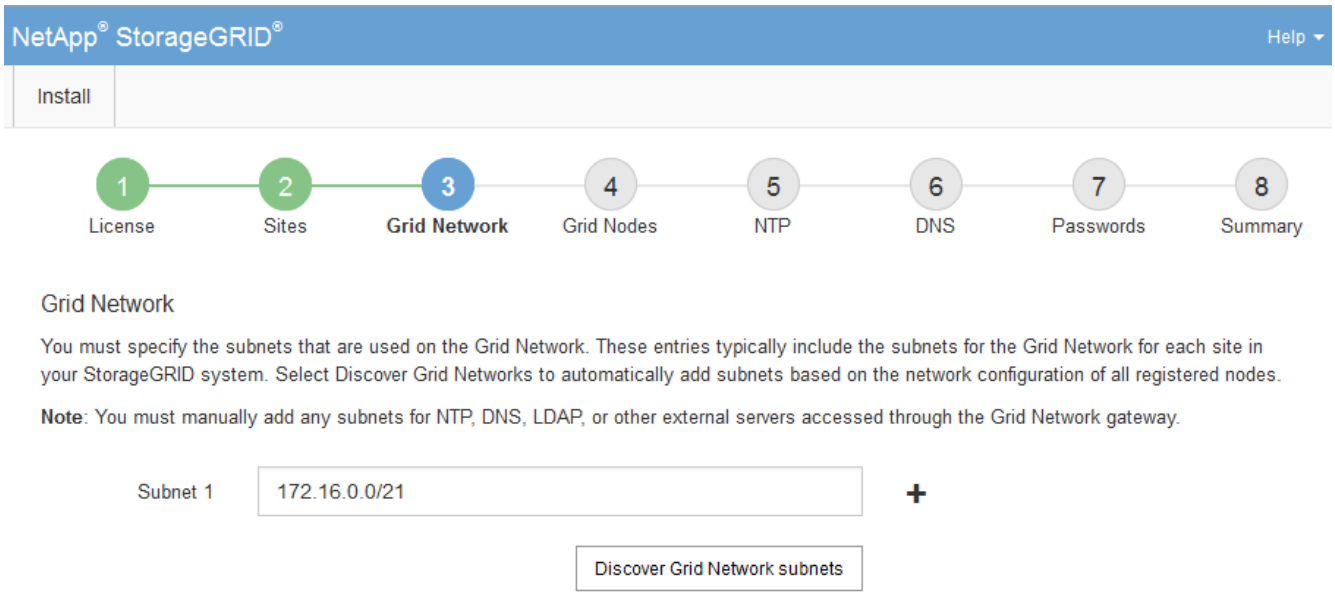
子网条目包括 StorageGRID 系统中每个站点的网格网络子网，以及需要通过网格网络访问的任何子网。

如果您有多个网格子网，则需要使用网格网络网关。指定的所有网格子网都必须可通过此网关访问。

步骤

1. 在 * 子网 1* 文本框中至少为一个网格网络指定 CIDR 网络地址。
2. 单击最后一个条目旁边的加号以添加其他网络条目。

   如果已至少部署一个节点，请单击 * 发现网格网络子网 * 以自动使用已向网格管理器注册的网格节点报告的子网填充网格网络子网列表。



3. 单击 * 下一步 * 。

批准待定网格节点

您必须先批准每个网格节点，然后才能将其加入 StorageGRID 系统。

您需要的内容

您已部署所有虚拟设备和 StorageGRID 设备网格节点。

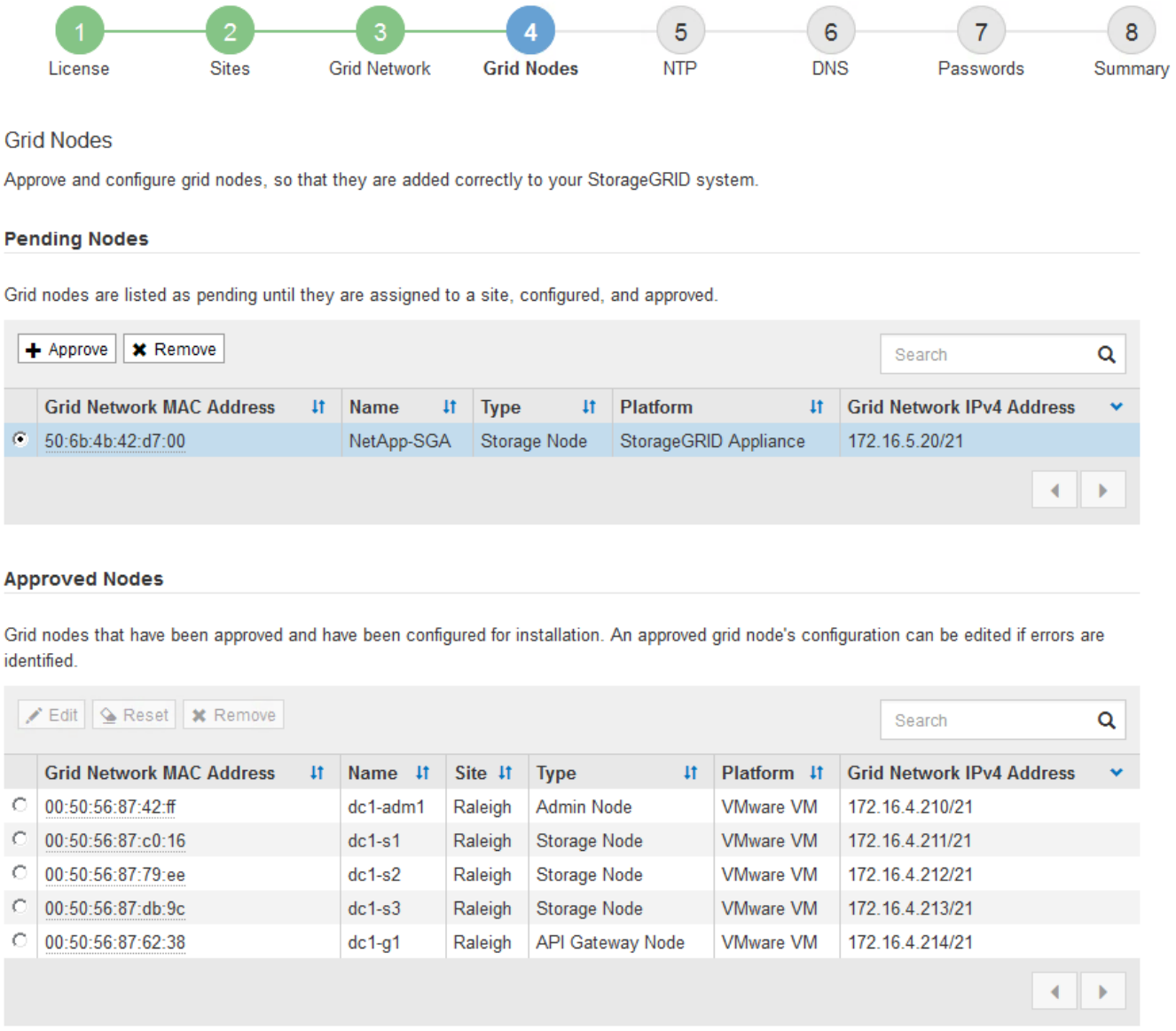
对所有节点执行一次安装比现在安装某些节点以及稍后安装某些节点更高效。

步骤

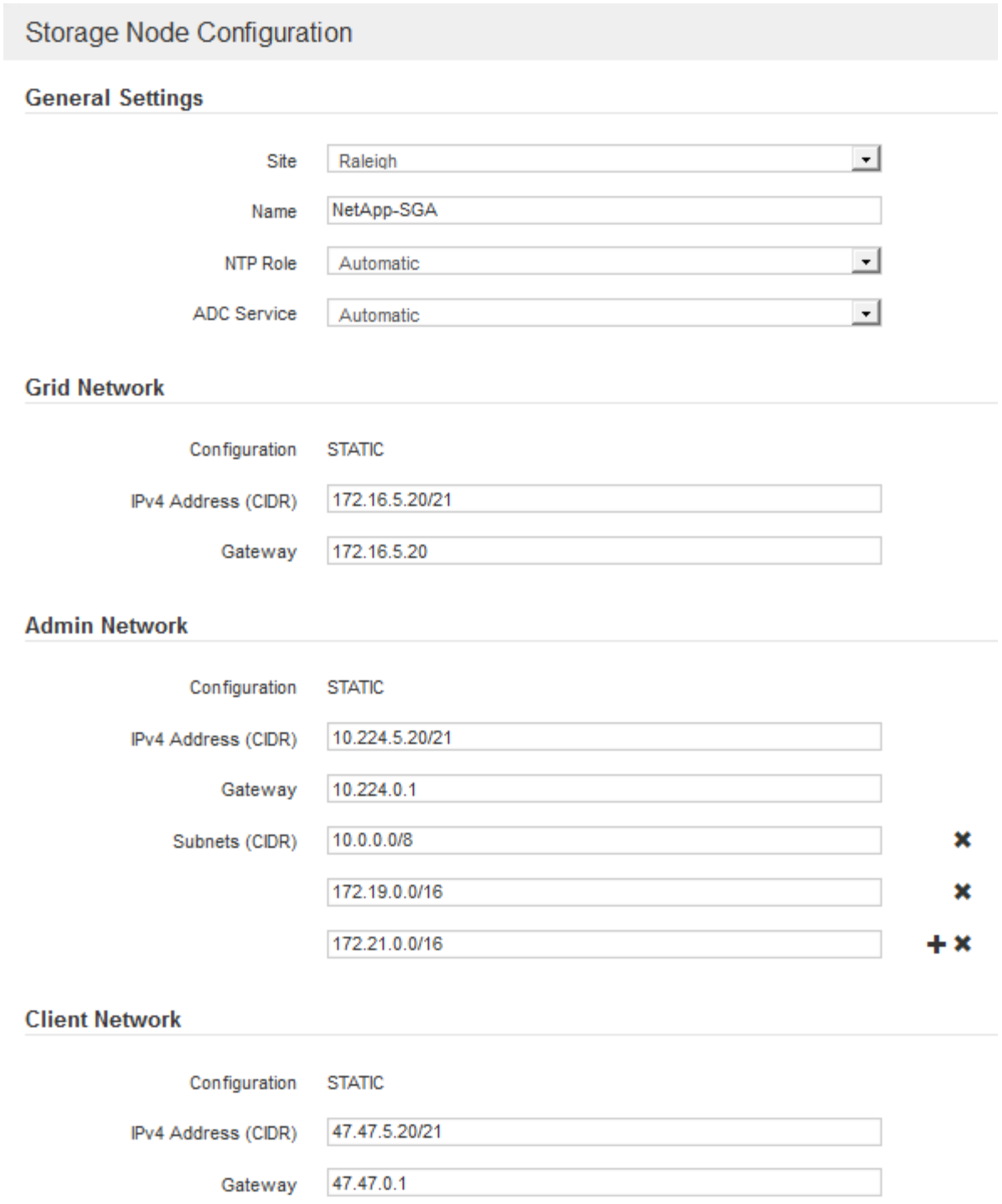
1. 查看 Pending Nodes 列表，并确认它显示了您部署的所有网格节点。

   如果缺少网格节点，请确认已成功部署该节点。

2. 选择要批准的待定节点旁边的单选按钮。



3. 单击 * 批准 * 。
4. 在常规设置中，根据需要修改以下属性的设置：



◦ * 站点 * ： 要与此网格节点关联的站点的名称。

◦ * 名称 * ： 分配给节点的名称以及将在网格管理器中显示的名称。此名称默认为您在配置节点时指定的名称。在安装过程的此步骤中，您可以根据需要更改名称。

完成安装后，您将无法更改节点的名称。

对于 VMware 节点，您可以在此处更改名称，但此操作不会更改 vSphere 中虚拟机的名称。

◦ * NTP 角色 * ： 网格节点的网络时间协议（ NTP ）角色。选项包括 * 自动 * ， * 主 * 和 * 客户端 * 。选

择 * 自动 * 会将主角色分配给管理节点，具有模板转换服务的存储节点，网关节点以及具有非静态 IP 地址的任何网格节点。所有其他网格节点都分配有客户端角色。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

- * ADC* 服务 * （仅限存储节点）：选择 * 自动 * ，让系统确定节点是否需要管理域控制器（ ADC* ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。每个站点至少有三个存储节点必须包含此 ADC-Service 。在部署此节点后，您不能将此 ADC 服务添加到该节点中。

5. 在网格网络中，根据需要修改以下属性的设置：

   - * IPv4 地址（ CIDR ） *：网格网络接口（容器中的 eth0 ）的 CIDR 网络地址。例如： 192.168.1.234/21
   - * 网关 *： 网格网络网关。例如： 192.168.0.1

     如果存在多个网格子网，则需要使用网关。

     > 如果您为网格网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

6. 如果要为网格节点配置管理网络，请根据需要在管理网络部分中添加或更新设置。

   在 * 子网（ CIDR ） * 文本框中输入从此接口路由的目标子网。如果存在多个管理子网，则需要使用管理网关。

   > 如果您为管理网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

   - 设备： * 对于 StorageGRID 设备，如果在初始安装期间未使用 StorageGRID 设备安装程序配置管理网络，则无法在此网格管理器对话框中进行配置。而是必须执行以下步骤：

     a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

        重新启动可能需要几分钟时间。

     b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。
     c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。
     d. 返回主页页面，然后单击 * 开始安装 * 。
     e. 在网格管理器中：如果节点列在 "Approved Nodes" 表中，请重置节点。
     f. 从 Pending Nodes 表中删除此节点。
     g. 等待节点重新出现在 "Pending Nodes" 列表中。
     h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。

        对于追加信息 ，请参见适用于您的设备型号的安装和维护说明。

7. 如果要为网格节点配置客户端网络，请根据需要在客户端网络部分中添加或更新设置。如果配置了客户端网络，则需要使用网关，安装后，它将成为节点的默认网关。

如果您为客户端网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

- 设备： * 对于 StorageGRID 设备，如果在初始安装期间未使用 StorageGRID 设备安装程序配置客户端网络，则无法在此网格管理器对话框中进行配置。而是必须执行以下步骤：

  a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

     重新启动可能需要几分钟时间。

  b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。

  c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。

  d. 返回主页页面，然后单击 * 开始安装 * 。

  e. 在网格管理器中：如果节点列在 "Approved Nodes" 表中，请重置节点。

  f. 从 Pending Nodes 表中删除此节点。

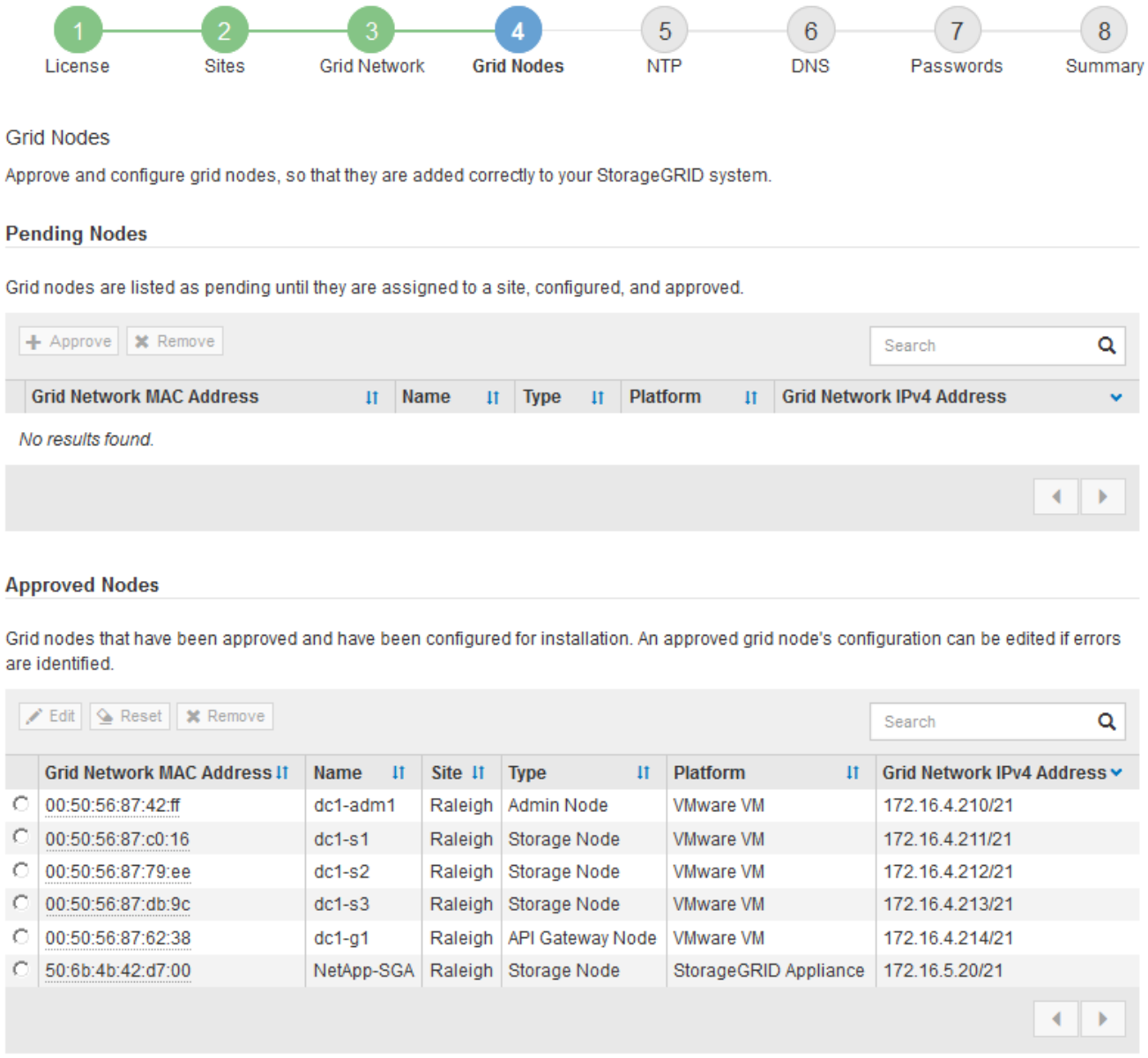
  g. 等待节点重新出现在 "Pending Nodes" 列表中。

  h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。

     对于追加信息 ，请参见适用于您的设备的安装和维护说明。

8. 单击 * 保存 * 。

网格节点条目将移至 "Approved Nodes" 列表。



9. 对要批准的每个待定网格节点重复上述步骤。

   您必须批准网格中所需的所有节点。但是，在单击 " 摘要 " 页面上的 * 安装 * 之前，您可以随时返回此页面。您可以通过选择已批准的网格节点的单选按钮并单击 * 编辑 * 来修改其属性。

10. 批准完网格节点后，单击 * 下一步 * 。

指定网络时间协议服务器信息

您必须为 StorageGRID 系统指定网络时间协议（ NTP ）配置信息，以便在不同服务器上执行的操作保持同步。

关于此任务

您必须为 NTP 服务器指定 IPv4 地址。

您必须指定外部 NTP 服务器。指定的 NTP 服务器必须使用 NTP 协议。

您必须指定四个引用 Stratum 3 或更高配置的 NTP 服务器，以防止出现时间偏差问题。

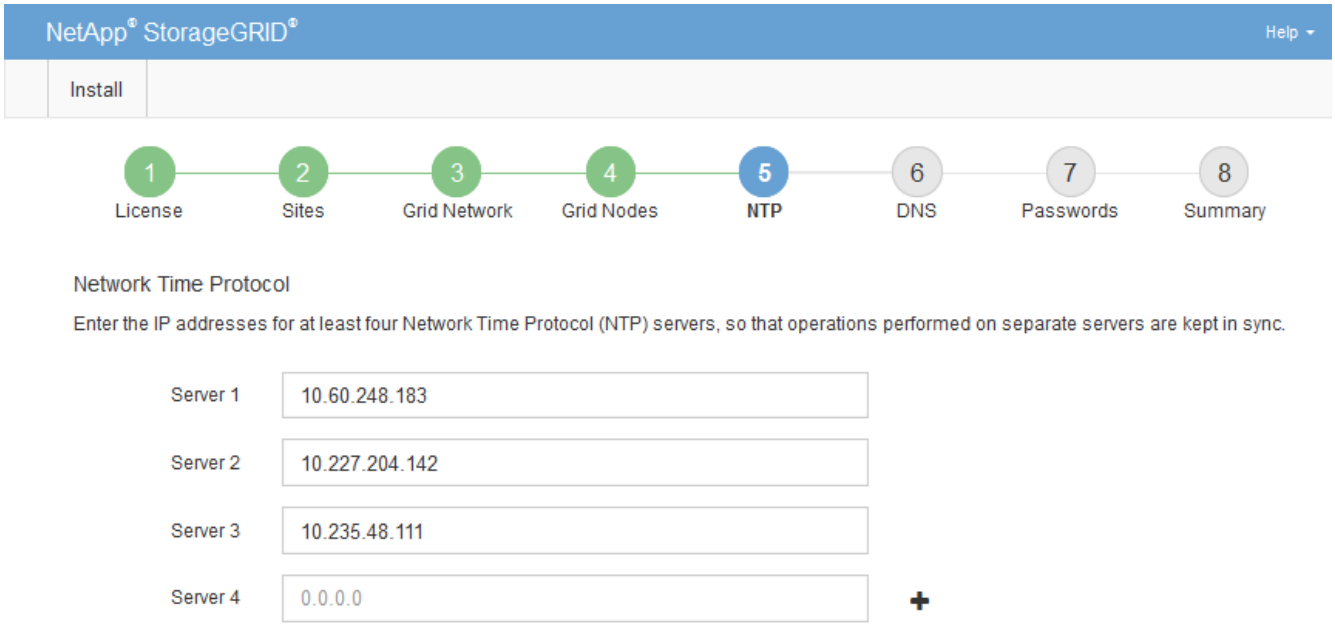
> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。
>
> "支持边界，用于为高精度环境配置 Windows 时间服务"

外部 NTP 服务器由先前分配了主 NTP 角色的节点使用。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

步骤

1. 在 * 服务器 1* 到 * 服务器 4* 文本框中指定至少四个 NTP 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



3. 选择 * 下一步 * 。

相关信息

网络连接准则

指定域名系统服务器信息

您必须为 StorageGRID 系统指定域名系统（ DNS ）信息，以便可以使用主机名而非 IP 地址访问外部服务器。

关于此任务

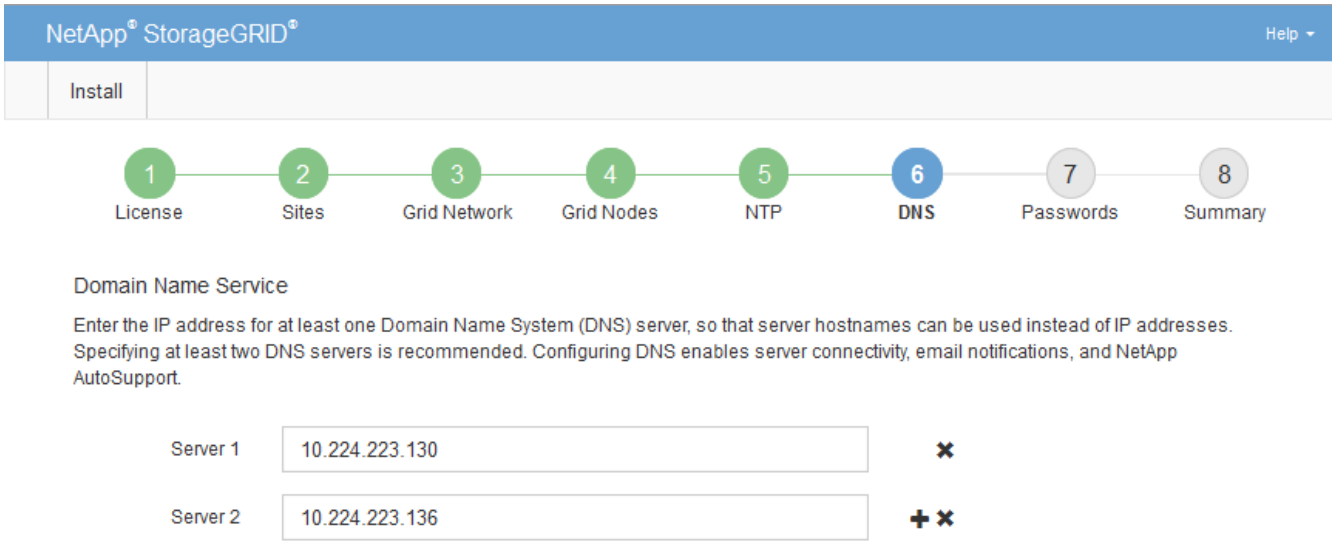
通过指定 DNS 服务器信息，您可以对电子邮件通知和 AutoSupport 使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。建议至少指定两个 DNS 服务器。

为 DNS 服务器提供两到六个 IPv4 地址。您应选择 DNS 服务器，以便在网络隔离时每个站点都可以在本地访问这些服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以进一步自定义每个节点的 DNS 服务器列表。有关详细信息，请参见恢复和维护说明中有关修改 DNS 配置的信息。

如果省略 DNS 服务器信息或 DNS 服务器信息配置不正确，则会在每个网格节点的 SSM 服务上触发 DNST 警报。如果 DNS 配置正确且新服务器信息已到达所有网格节点，则警报将清除。

步骤

1. 在 * 服务器 1* 文本框中至少指定一个 DNS 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



最佳实践是至少指定两个 DNS 服务器。最多可以指定六个 DNS 服务器。

3. 选择 * 下一步 * 。

指定 **StorageGRID** 系统密码

在安装 StorageGRID 系统时，您需要输入密码以保护系统安全并执行维护任务。

关于此任务

使用安装密码页面指定配置密码短语和网格管理 root 用户密码。

- 配置密码短语用作加密密钥，不会由 StorageGRID 系统存储。
- 您必须具有用于安装，扩展和维护过程的配置密码短语，包括下载恢复软件包。因此，请务必将配置密码短语存储在安全位置。
- 如果您使用的是最新的网格管理器，则可以从网格管理器更改配置密码短语。
- 可以使用网格管理器更改网格管理 root 用户密码。
- 随机生成的命令行控制台和 SSH 密码存储在恢复软件包的 Passwords.txt 文件中。

步骤

1. 在 * 配置密码短语 * 中，输入更改 StorageGRID 系统网格拓扑所需的配置密码短语。

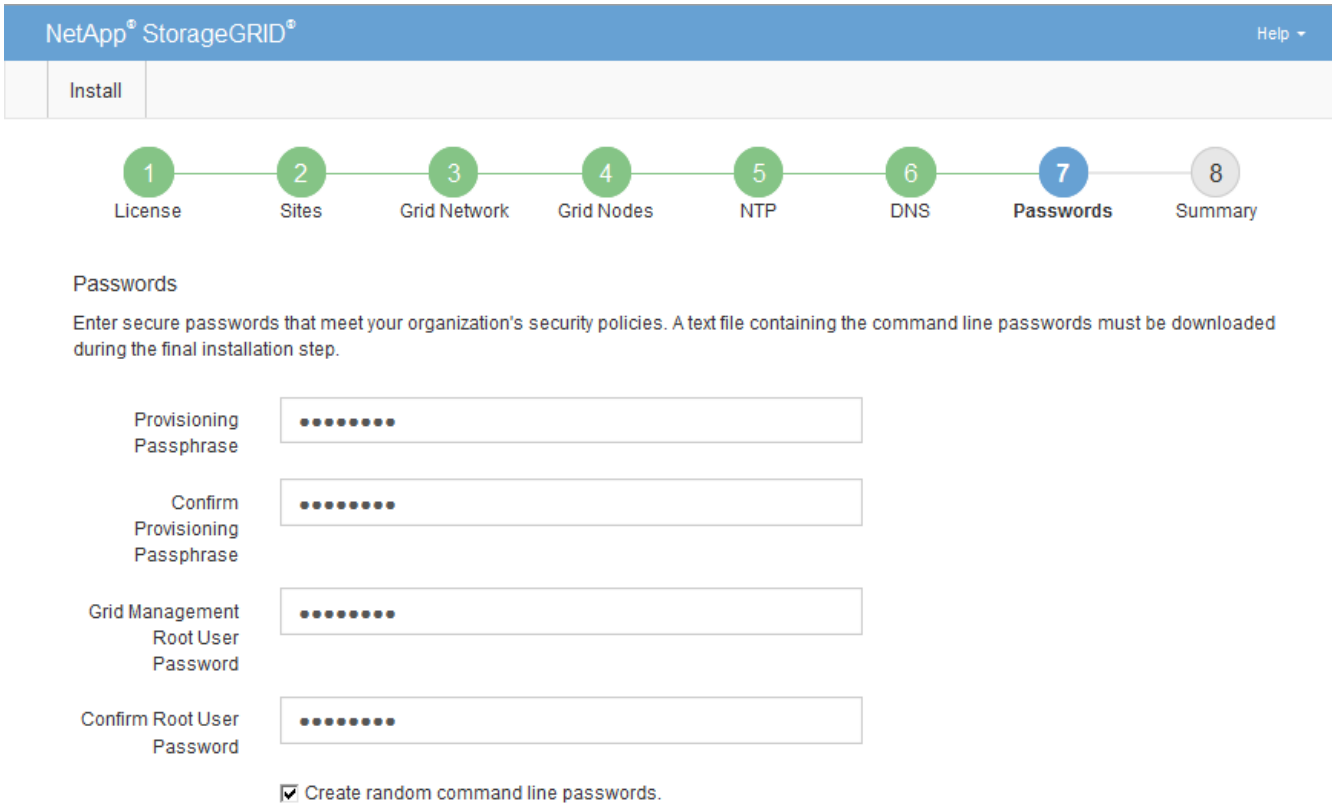
将配置密码短语存储在安全位置。

> 如果在安装完成后您希望稍后更改配置密码短语，则可以使用网格管理器。选择 * 配置 * > * 访问控制 * > * 网格密码 * 。

2. 在 * 确认配置密码短语 * 中，重新输入配置密码短语进行确认。
3. 在 * 网格管理 root 用户密码 * 中，以 "`root` " 用户身份输入用于访问网格管理器的密码。

   将密码存储在安全的位置。

4. 在 * 确认 root 用户密码 * 中，重新输入网格管理器密码进行确认。



5. 如果要安装网格以进行概念验证或演示，也可以取消选中 * 创建随机命令行密码 * 复选框。

   对于生产部署，出于安全原因，应始终使用随机密码。如果要使用默认密码通过命令行使用 "`root` " 或 "`admin` " 帐户访问网格节点，请取消选择 * 仅为演示网格创建随机命令行密码 * 。

> 单击摘要页面上的 * 安装 * 后，系统将提示您下载恢复软件包文件（ `sGWS-recovery-package-id-revision.zip` ）。您必须 下载此文件 以完成安装。访问系统所需的密码存储在恢复软件包文件中的 Passwords.txt 文件中。

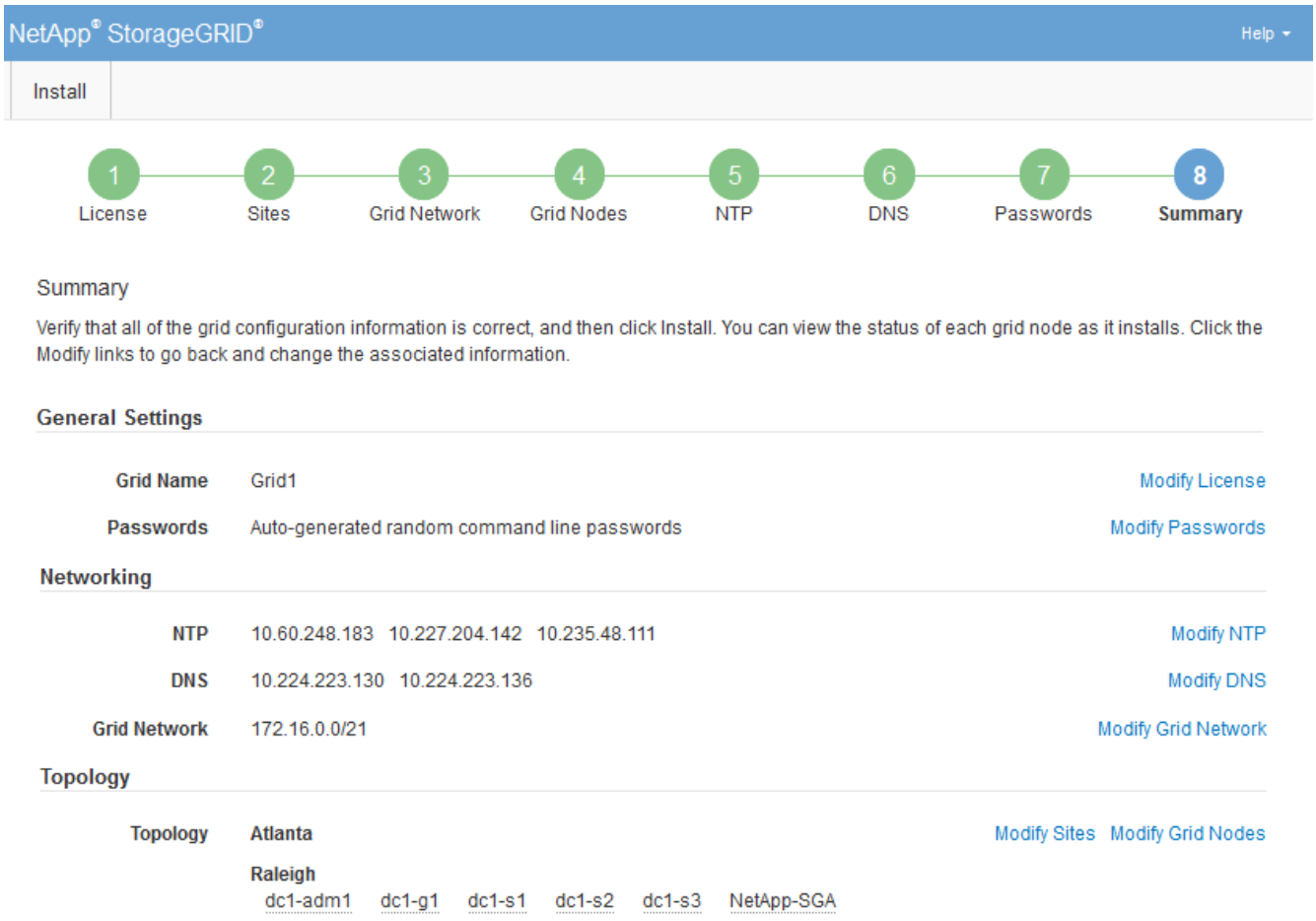
6. 单击 * 下一步 * 。

查看您的配置并完成安装

您必须仔细查看输入的配置信息，以确保安装成功完成。

步骤

1. 查看 * 摘要 * 页面。



2. 验证所有网格配置信息是否正确。使用摘要页面上的修改链接返回并更正任何错误。
3. 单击 * 安装 * 。

> 如果将某个节点配置为使用客户端网络，则在单击 * 安装 * 时，该节点的默认网关会从网格网络切换到客户端网络。如果连接断开，则必须确保通过可访问的子网访问主管理节点。请参见 网络连接准则 了解详细信息。

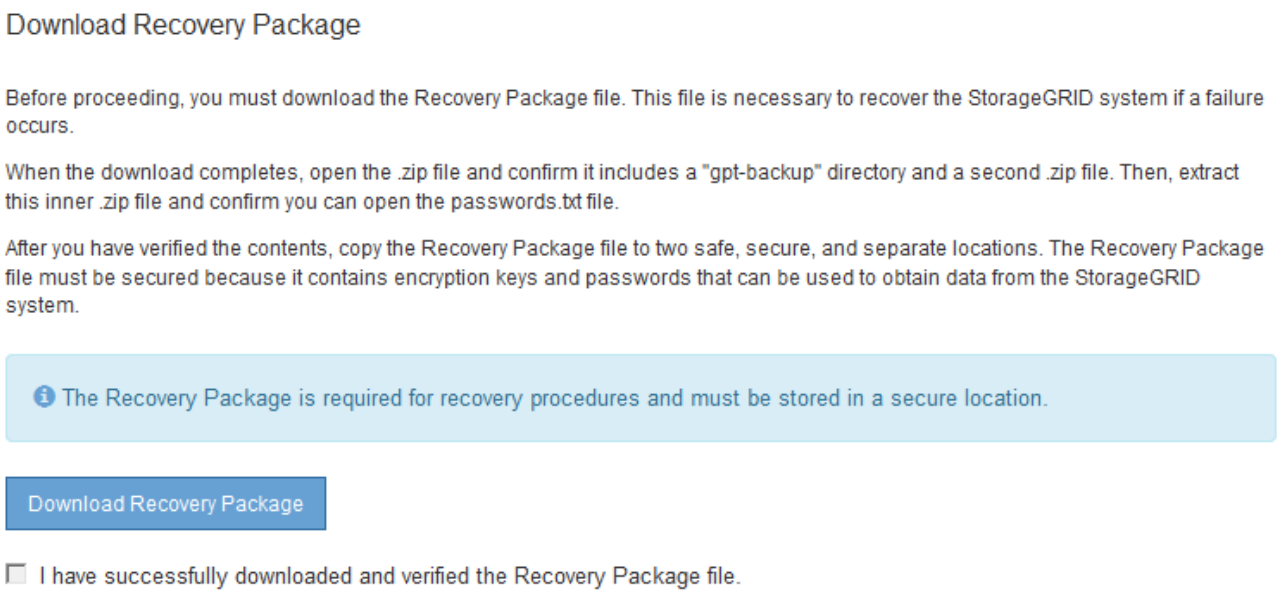
4. 单击 * 下载恢复包 * 。

   当安装过程进展到定义网格拓扑时，系统会提示您下载恢复包文件（` .zip` ），并确认您可以成功访问此文件的内容。您必须下载恢复软件包文件，以便在一个或多个网格节点出现故障时恢复 StorageGRID 系统。安装将在后台继续进行，但您无法完成安装并访问 StorageGRID 系统，直到下载并验证此文件为止。

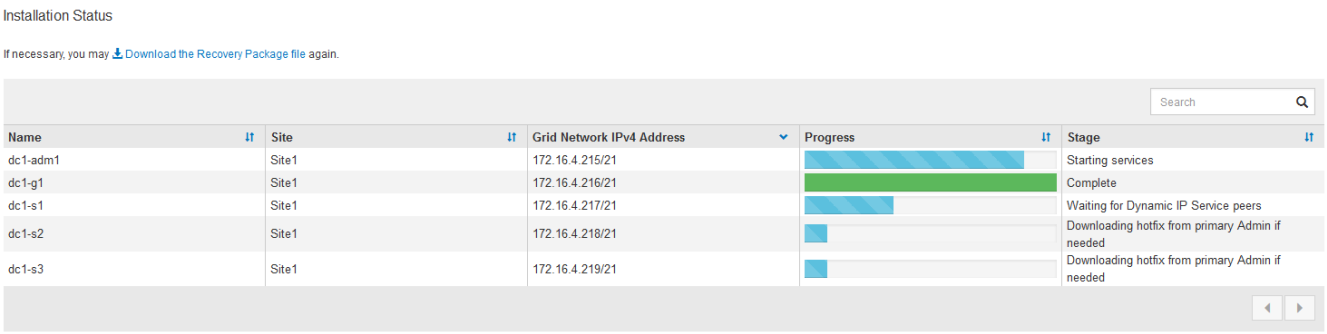
5. 验证您是否可以提取 ` .zip` 文件的内容，然后将其保存在两个安全，安全和独立的位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

6. 选中 * 我已成功下载并验证恢复软件包文件 * 复选框，然后单击 * 下一步 * 。



如果安装仍在进行中，则会显示状态页面。此页面指示每个网格节点的安装进度。



当所有网格节点达到完成阶段后，将显示网格管理器的登录页面。

7. 使用 "root" 用户和您在安装期间指定的密码登录到网格管理器。

安装后准则

完成网格节点部署和配置后，请按照以下准则更改 DHCP 地址和网络配置。

- 如果使用 DHCP 分配 IP 地址，请为所使用网络上的每个 IP 地址配置 DHCP 预留。

  您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。

  > 当节点的 IP 地址发生更改时，节点会重新启动，如果 DHCP 地址更改同时影响多个节点，则发生原因 可能会中断。

- 如果要更改网格节点的 IP 地址，子网掩码和默认网关，必须使用更改 IP 过程。请参见 配置 IP 地址。
- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改，您可能需要重新建立这些连接。

自动安装（ **Ubuntu** 或 **Debian** ）

您可以自动安装 StorageGRID 主机服务和配置网格节点。

关于此任务

在以下任一情况下，自动部署可能会很有用：

- 您已使用标准业务流程框架（例如 Ansible ， Puppet 或 Chef ）部署和配置物理或虚拟主机。
- 您打算部署多个 StorageGRID 实例。
- 您正在部署一个大型的复杂 StorageGRID 实例。

StorageGRID 主机服务由软件包安装，并由配置文件驱动，这些配置文件可以在手动安装期间以交互方式创建，也可以提前准备（或以编程方式），以便使用标准业务流程框架实现自动安装。StorageGRID 提供了可选的 Python 脚本，用于自动配置 StorageGRID 设备和整个 StorageGRID 系统（ "`grid` " ）。您可以直接使用这些脚本，也可以对其进行检查，了解如何在您自己开发的网格部署和配置工具中使用 StorageGRID 安装 REST API 。

自动安装和配置 **StorageGRID** 主机服务

您可以使用 Ansible ， Puppet ， Chef ， Fabric 或 SaltStack 等标准业务流程框架自动安装 StorageGRID 主机服务。

StorageGRID 主机服务打包在 DEB 中，并由配置文件驱动，这些配置文件可以提前准备（或以编程方式）以启用自动安装。如果您已经使用标准业务流程框架来安装和配置 Ubuntu 或 Debian ，则在攻略手册或秘诀中添加 StorageGRID 应该非常简单。

您可以自动执行以下任务：

1. 安装 Linux
2. 配置 Linux
3. 配置主机网络接口以满足 StorageGRID 要求
4. 配置主机存储以满足 StorageGRID 要求
5. 安装 Docker
6. 安装 StorageGRID 主机服务
7. 在 ` /etc/storaggrid/nodes` 中创建 StorageGRID 节点配置文件
8. 正在验证 StorageGRID 节点配置文件
9. 启动 StorageGRID 主机服务

Ansible 角色和攻略手册示例

安装归档在 /Extras 文件夹中提供了示例 Ansible 角色和攻略手册。Ansible 攻略手册介绍了 `StorageGRID` 角色如何准备主机并将 StorageGRID 安装到目标服务器上。您可以根据需要自定义角色或攻略手册。

自动配置 **StorageGRID**

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	Description
configure-storagegrid.py	用于自动配置的 Python 脚本
configure-storaggrid.sample.json	用于脚本的示例配置文件
configure-storaggrid.blank.json	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

关于此任务

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

您也可以使用网格管理器或安装 API 配置系统。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中 `platform` is `dEBS` ， `rpms` 或 `vSphere` 。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

结果

在配置过程中会生成一个恢复包 ` .zip` 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 `passwords.txt` 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

相关信息

安装 REST API 概述

安装 REST API 概述

StorageGRID 提供了用于执行安装任务的 StorageGRID 安装 API 。

API 使用 Swagger 开源 API 平台提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 API

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。

- **recovery-package** —下载恢复软件包的操作。
- * 模式 * —用于高级部署的 API 模式
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

相关信息

自动化安装

下一步行动

完成安装后，您必须执行一系列集成和配置步骤。某些步骤是必需的；其他步骤是可选的。

所需任务

- 为要用于在 StorageGRID 系统上存储对象的每个客户端协议（ Swift 或 S3 ）创建一个租户帐户。
- 通过配置组和用户帐户来控制系统访问。您也可以配置联合身份源（例如 Active Directory 或 OpenLDAP ），以便导入管理组和用户。或者，您也可以创建本地组和用户。
- 集成并测试用于将对象上传到 StorageGRID 系统的 S3 或 Swift API 客户端应用程序。
- 准备好后，配置要用于保护对象数据的信息生命周期管理（ ILM ）规则和 ILM 策略。

> 安装 StorageGRID 时，默认 ILM 策略 " 基线 2 副本策略 " 处于活动状态。此策略包括常用 ILM 规则（创建 2 个副本），如果未激活任何其他策略，则此策略适用。

- 如果您的安装包括设备存储节点，请使用 SANtricity 软件完成以下任务：
  - 连接到每个 StorageGRID 设备。
  - 验证是否收到 AutoSupport 数据。
- 如果 StorageGRID 系统包含任何归档节点，请配置归档节点与目标外部归档存储系统的连接。

> 如果任何归档节点将使用 Tivoli Storage Manager 作为外部归档存储系统，则还必须配置 Tivoli Storage Manager 。

- 查看并遵循 StorageGRID 系统强化准则，以消除安全风险。
- 为系统警报配置电子邮件通知。

可选任务

- 如果要从（原有）警报系统接收通知，请配置警报的邮件列表和电子邮件通知。
- 如果自规划部署并生成恢复包以来网格节点 IP 地址发生了更改，请更新这些地址。请参见恢复和维护说明中有关更改 IP 地址的信息。
- 根据需要配置存储加密。
- 如果需要，配置存储压缩以减小存储对象的大小。
- 配置审核客户端访问。您可以通过 NFS 或 CIFS 文件共享配置对系统的访问，以供审核使用。请参见有关管理 StorageGRID 的说明。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

相关信息

管理 StorageGRID

使用 S3

使用 Swift

使用 ILM 管理对象

监控和故障排除

恢复和维护

SG100 和 SG1000 服务设备

SG5600 存储设备

SG5700 存储设备

SG6000 存储设备

发行说明

系统强化

查看审核日志

升级软件

对安装问题进行故障排除

如果在安装 StorageGRID 系统时出现任何问题，您可以访问安装日志文件。技术支持可能还需要使用安装日志文件来解决问题。

运行每个节点的容器提供了以下安装日志文件：

- ` /var/local/log/install.log` （可在所有网格节点上找到）
- ` /var/local/log/gdu-server.log` （位于主管理节点上）

主机上提供了以下安装日志文件：

- ` /var/log/storaggrid/daema.log`
- ` /var/log/storaggrid/nodes/<node-name>.log`

要了解如何访问日志文件，请参见有关 StorageGRID 监控和故障排除的说明。有关排除设备安装问题的帮助，请参见适用于您的设备的安装和维护说明。如果您需要其他帮助，请联系技术支持。

相关信息

监控和故障排除

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

"NetApp 支持"

/etc/network/interfaces 示例

` /etc/network/interfaces` 文件包括三个部分，分别定义了物理接口，绑定接口和 VLAN 接口。您可以将这三个示例部分合并为一个文件，该文件将四个 Linux 物理接口聚合为一个 LACP 绑定，然后建立三个 VLAN 接口，将此绑定分包为 StorageGRID 网格，管理和客户端网络接口。

物理接口

请注意，链路另一端的交换机还必须将这四个端口视为一个 LACP 中继或端口通道，并且必须至少通过三个带标记的参考 VLAN 。

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

绑定接口

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLAN 接口

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

安装 VMware

安装 VMware： 概述

在 VMware 环境中安装 StorageGRID 系统包括三个主要步骤。

1. * 准备 *： 在规划和准备期间，您将执行以下任务：
   - 了解 StorageGRID 的硬件，软件，虚拟机，存储和性能要求。
   - 了解的具体信息 StorageGRID 网络连接 这样，您就可以正确配置网络了。
   - 确定并准备要用于托管 StorageGRID 网格节点的物理服务器。
   - 在已准备好的服务器上：
     - 安装 VMware vSphere 虚拟机管理程序
     - 配置 ESX 主机
     - 安装和配置 VMware vSphere 和 vCenter
2. * 部署 *： 使用 VMware vSphere Web Client 部署网格节点。部署网格节点时，它们会作为 StorageGRID 系统的一部分创建并连接到一个或多个网络。
   a. 使用 VMware vSphere Web Client ， .vmdk 文件和一组 .OVF 文件模板将基于软件的节点部署为您在步骤 1 中准备的服务器上的虚拟机（ VM ）。
   b. 使用 StorageGRID 设备安装程序部署 StorageGRID 设备节点。

   > StorageGRID 安装操作步骤 中不包含特定于硬件的安装和集成说明。要了解如何安装 StorageGRID 设备，请参见适用于您的设备的安装和维护说明。

3. * 配置 *： 部署完所有节点后，请使用网格管理器配置网格并完成安装。

以下说明为在 VMware 环境中部署和配置 StorageGRID 系统建议了一种标准方法。另请参见有关以下替代方法的信息：

- 使用 deploy-vsphere-ovftool.sh Bash 脚本（可从安装归档中获取）在 VMware vSphere 中部署网格节点。
- 使用 Python 配置脚本（在安装归档中提供）自动部署和配置 StorageGRID 系统。
- 使用 Python 配置脚本（可从安装归档或 StorageGRID 设备安装程序获取）自动部署和配置设备网格节点。
- 如果您是 StorageGRID 部署的高级开发人员，请使用安装 REST API 自动安装 StorageGRID 网格节点。

规划并准备 **VMware** 安装

安装前（ **VMware** ）

在部署网格节点和配置 StorageGRID 网格之前，您必须熟悉完成操作步骤 的步骤和要求。

StorageGRID 部署和配置过程假定您熟悉 StorageGRID 系统的架构和操作功能。

您可以一次部署一个或多个站点；但是，所有站点必须满足至少有三个存储节点的最低要求。

StorageGRID 不支持使用虚拟存储区域网络（ VSAN ），因为底层磁盘保护不是硬件 RAID 。

在开始节点部署和网格配置操作步骤 之前，您必须：

- 规划 StorageGRID 部署。
- 按照规格安装，连接和配置所有必需的硬件，包括任何 StorageGRID 设备。

StorageGRID 安装操作步骤 中不包含特定于硬件的安装和集成说明。要了解如何安装 StorageGRID 设备，请参见适用于您的设备的安装和维护说明。

- 了解 可用网络选项以及如何在网格节点上实施每个网络选项。
- 提前收集所有网络信息。除非使用 DHCP ，否则请收集要分配给每个网格节点的 IP 地址以及要使用的域名系统（ DNS ）和网络时间协议（ NTP ）服务器的 IP 地址。
- 确定要使用的可用部署和配置工具。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

所需材料

在安装 StorageGRID 之前，您必须收集并准备所需的材料。

项目	注释：
NetApp StorageGRID 许可证	您必须具有有效的数字签名 NetApp 许可证。 • 注意 * ： StorageGRID 安装归档包含一个免费许可证，不提供产品的任何支持授权。
StorageGRID 安装归档	您必须 下载 StorageGRID 安装归档并解压缩文件。
VMware 软件和文档	在安装期间，您可以使用 VMware vSphere Web Client 在虚拟机上部署虚拟网格节点。有关支持的版本，请参见互操作性表。
服务笔记本电脑	StorageGRID 系统通过服务组件进行安装服务笔记本电脑必须具有： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器
StorageGRID 文档	• 发行说明 • 有关管理 StorageGRID 的说明

相关信息

"NetApp 互操作性表工具"

下载并提取 **StorageGRID** 安装文件

您必须下载 StorageGRID 安装归档并提取文件。

步骤

1. 转至 "StorageGRID 的 "NetApp 下载 " 页面"。
2. 选择用于下载最新版本的按钮，或者从下拉菜单中选择其他版本并选择 * 执行 * 。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 如果显示 Caution/MustRead 语句，请阅读该语句并选中复选框。

   安装 StorageGRID 版本后，您必须应用任何所需的修补程序。有关详细信息，请参见 恢复和维护说明中的热修补程序操作步骤

5. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。
6. 在 * 安装 vmware* 列中，选择 StorageGRID 的 .tgz 或 .zip 文件。

   如果您在服务笔记本电脑上运行 Windows ，请使用 ` .zip` 文件。

7. 保存并提取归档文件。

8. 从以下列表中选择所需的文件。

   所需的文件取决于您规划的网格拓扑以及如何部署 StorageGRID 系统。

   表中列出的路径与提取的安装归档所安装的顶级目录相对。

路径和文件名	**Description**
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。
	用于部署主管理节点的开放式虚拟化格式模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署非主管理节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署归档节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署网关节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署基于虚拟机的存储节点的模板文件（`.OVF`）和清单文件（`.MF`）。
部署脚本工具	Description
	Bash shell 脚本，用于自动部署虚拟网格节点。
	与 `deept-vsphere-ovftool.sh` 脚本结合使用的示例配置文件。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。

路径和文件名	Description
	与 `configure-storagrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storagrid.py` 脚本的空配置文件。
	StorageGRID 的 API 架构。 • 注意 *：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

相关信息

恢复和维护

软件要求

您可以使用虚拟机托管任何类型的 StorageGRID 网格节点。VMware 服务器上安装的每个网格节点都需要一个虚拟机。

VMware vSphere 虚拟机管理程序

您必须在已准备好的物理服务器上安装 VMware vSphere 虚拟机管理程序。在安装 VMware 软件之前，必须正确配置硬件（包括固件版本和 BIOS 设置）。

- 根据需要在虚拟机管理程序中配置网络，以支持要安装的 StorageGRID 系统的网络连接。

  网络连接准则

- 确保数据存储库足够大，足以容纳托管网格节点所需的虚拟机和虚拟磁盘。
- 如果创建多个数据存储库，请为每个数据存储库命名，以便在创建虚拟机时轻松确定要用于每个网格节点的数据存储库。

ESX 主机配置要求

> 您必须在每个 ESX 主机上正确配置网络时间协议（ NTP ）。如果主机时间不正确，可能会产生负面影响，包括数据丢失。

VMware 配置要求

在部署 StorageGRID 网格节点之前，您必须安装和配置 VMware vSphere 和 vCenter 。

有关受支持的 VMware vSphere 虚拟机管理程序和 VMware vCenter Server 软件版本，请参见互操作性表。

有关安装这些 VMware 产品所需的步骤，请参见 VMware 文档。

相关信息

"NetApp 互操作性表工具"

CPU 和 RAM 要求

在安装 StorageGRID 软件之前，请验证并配置硬件，使其可以支持 StorageGRID 系统。

有关受支持服务器的信息，请参见互操作性表。

每个 StorageGRID 节点需要以下最低资源：

- CPU 核心：每个节点 8 个
- RAM ： 每个节点至少 24 GB ，比系统总 RAM 少 2 到 16 GB ，具体取决于可用 RAM 总量和系统上运行的非 StorageGRID 软件的数量

确保计划在每个物理或虚拟主机上运行的 StorageGRID 节点数不超过可用的 CPU 核心数或物理 RAM 数。如果主机不是专用于运行 StorageGRID 的（不建议使用），请务必考虑其他应用程序的资源要求。

> 定期监控 CPU 和内存使用情况，以确保这些资源能够持续满足您的工作负载需求。例如，将虚拟存储节点的 RAM 和 CPU 分配增加一倍将提供与为 StorageGRID 设备节点提供的资源类似的资源。此外，如果每个节点的元数据量超过 500 GB ，请考虑将每个节点的 RAM 增加到 48 GB 或更多。有关管理对象元数据存储，增加元数据预留空间设置以及监控 CPU 和内存使用量的信息，请参见有关管理，监控和升级 StorageGRID 的说明。

如果在底层物理主机上启用了超线程功能，则可以为每个节点提供 8 个虚拟核心（ 4 个物理核心）。如果底层物理主机上未启用超线程，则必须为每个节点提供 8 个物理核心。

如果要使用虚拟机作为主机并控制 VM 的大小和数量，则应为每个 StorageGRID 节点使用一个 VM 并相应地调整 VM 的大小。

对于生产部署，不应在同一物理存储硬件或虚拟主机上运行多个存储节点。一个 StorageGRID 部署中的每个存储节点都应位于其各自的隔离故障域中。如果您确保单个硬件故障只会影响单个存储节点，则可以最大限度地提高对象数据的持久性和可用性。

另请参见有关存储要求的信息。

相关信息

"NetApp 互操作性表工具"

存储和性能要求

管理 StorageGRID

监控和故障排除

升级软件

存储和性能要求

您必须了解虚拟机托管的 StorageGRID 节点的存储和性能要求，以便提供足够的空间来支

持初始配置和未来的存储扩展。

性能要求

操作系统卷和第一个存储卷的性能会显著影响系统的整体性能。请确保在延迟，每秒输入 / 输出操作数（ IOPS ）和吞吐量方面提供足够的磁盘性能。

所有 StorageGRID 节点都要求操作系统驱动器和所有存储卷启用回写缓存。缓存必须位于受保护或永久性介质上。

使用**NetApp ONTAP** 存储的虚拟机的要求

如果您要将StorageGRID 节点部署为虚拟机、并从NetApp ONTAP 系统分配存储、则表示您已确认卷未启用FabricPool 分层策略。例如，如果 StorageGRID 节点在 VMware 主机上作为虚拟机运行，请确保为该节点的数据存储库提供支持的卷未启用 FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

所需的虚拟机数量

每个 StorageGRID 站点至少需要三个存储节点。

> 在生产部署中，请勿在一个虚拟机服务器上运行多个存储节点。对每个存储节点使用专用虚拟机主机可提供一个隔离的故障域。

其他类型的节点（例如管理节点或网关节点）可以部署在同一虚拟机主机上，也可以根据需要部署在自己的专用虚拟机主机上。但是，如果您有多个相同类型的节点（例如两个网关节点），请勿将所有实例安装在同一虚拟机主机上。

按节点类型划分的存储要求

在生产环境中， StorageGRID 网格节点的虚拟机必须满足不同的要求，具体取决于节点类型。

> 磁盘快照不能用于还原网格节点。请参阅每种类型节点的恢复和维护过程。

节点类型	存储
管理节点	100 GB LUN ，用于操作系统 200 GB LUN ，用于管理节点表 200 GB LUN ，用于管理节点审核日志

节点类型	存储
存储节点	100 GB LUN ，用于操作系统 此主机上每个存储节点 3 个 LUN • 注 * ： 一个存储节点可以包含 1 到 16 个存储 LUN ； 建议至少使用 3 个存储 LUN 。 每个 LUN 的最小大小： 4 TB 测试的最大 LUN 大小： 39 TB 。
网关节点	100 GB LUN ，用于操作系统
归档节点	100 GB LUN ，用于操作系统

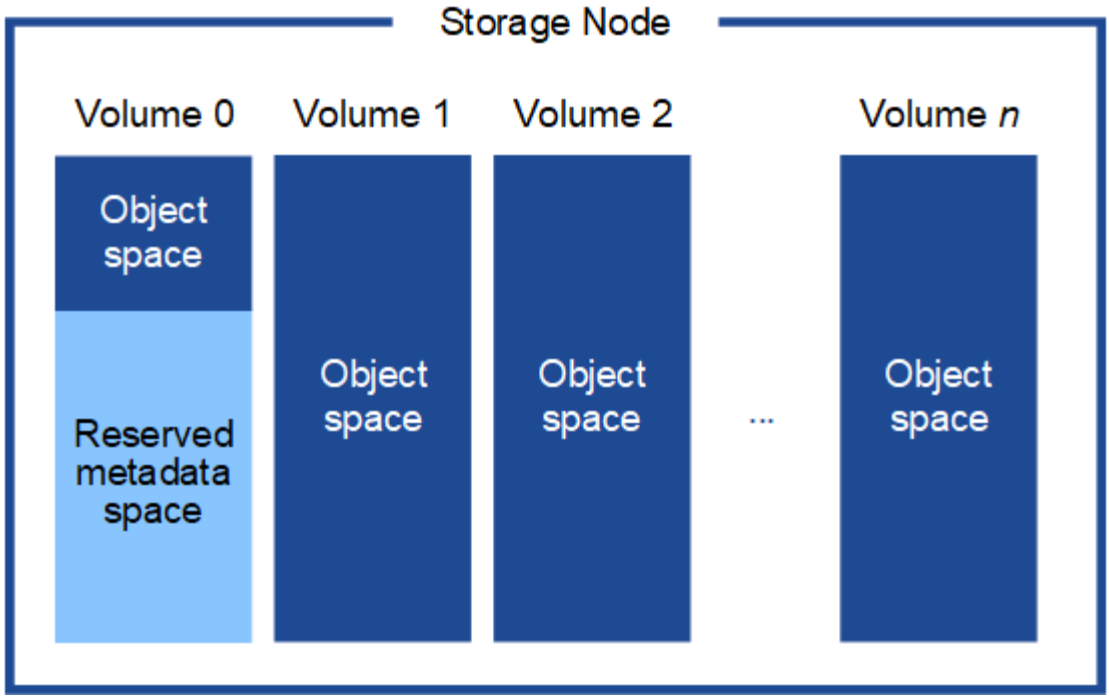
根据配置的审核级别， S3 对象密钥名称等用户输入的大小以及需要保留的审核日志数据量，您可能需要增加每个管理节点上的审核日志 LUN 的大小。一般来说，网格在每个 S3 操作中生成大约 1 KB 的审核数据，这意味着 200 GB 的 LUN 每天支持 7 ， 000 万次操作，或者每秒 800 次操作，持续 2 到 3 天。

存储节点的存储要求

一个基于软件的存储节点可以包含 1 到 16 个存储卷—建议使用 3 个或更多存储卷。每个存储卷应大于或等于 4 TB 。

一个设备存储节点最多可以包含 48 个存储卷。

如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。存储卷 0 和存储节点中的任何其他存储卷上的任何剩余空间专用于对象数据。



为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。对象元数据的三个副本均匀分布在每个站点的所有存储节点上。

在为新存储节点的卷 0 分配空间时，必须确保为该节点在所有对象元数据中的部分分配足够的空间。

- 您必须至少为卷 0 分配 4 TB 。

  如果一个存储节点仅使用一个存储卷，而为该卷分配的存储空间不超过 4 TB ，则该存储节点可能会在启动时进入存储只读状态，并仅存储对象元数据。

- 如果要安装新的 StorageGRID 11.6 系统，并且每个存储节点的 RAM 为 128 GB 或更大，则应为卷 0 分配 8 TB 或更多。如果对卷 0 使用较大的值，则可以增加每个存储节点上允许的元数据空间。
- 在为站点配置不同的存储节点时，如果可能，请对卷 0 使用相同的设置。如果某个站点包含不同大小的存储节点，卷 0 最小的存储节点将确定该站点的元数据容量。

有关详细信息，请转至 管理对象元数据存储。

相关信息

恢复和维护

部署虚拟机网格节点（ **VMware** ）

收集有关部署环境的信息

在部署网格节点之前，您必须收集有关网络配置和 VMware 环境的信息。

对所有节点执行一次安装比现在安装某些节点以及稍后安装某些节点更高效。

VMware 信息

您必须访问部署环境并收集以下信息： VMware 环境；为网格网络，管理网络和客户端网络创建的网络；以及计划用于存储节点的存储卷类型。

您必须收集有关 VMware 环境的信息，包括以下信息：

- 具有完成部署所需的适当权限的 VMware vSphere 帐户的用户名和密码。
- 每个 StorageGRID 网格节点虚拟机的主机，数据存储库和网络配置信息。

> VMware Live vMotion 会导致虚拟机时钟时间跳转，任何类型的网格节点均不支持此功能。尽管时钟时间不正确，但极少会导致数据丢失或配置更新。

网格网络信息

您必须收集有关为 StorageGRID 网格网络（必需）创建的 VMware 网络的信息，包括：

- 网络名称。
- 如果不使用 DHCP ，则为每个网格节点提供所需的网络详细信息（ IP 地址，网关和网络掩码）。
- 如果不使用 DHCP ，则为网格网络上主管理节点的 IP 地址。有关详细信息，请参见 "`网格节点如何发现主管理节点` " 。

管理网络信息

对于要连接到可选 StorageGRID 管理网络的节点，您必须收集有关为此网络创建的 VMware 网络的信息，包括：

- 网络名称。
- 用于分配静态或 DHCP IP 地址的方法。
- 如果使用的是静态 IP 地址，则为每个网格节点提供所需的网络详细信息（ IP 地址，网关，网络掩码）。
- 管理网络的外部子网列表（ ESL ）。

客户端网络信息

对于要连接到可选 StorageGRID 客户端网络的节点，您必须收集有关为此网络创建的 VMware 网络的信息，包括：

- 网络名称。
- 用于分配静态或 DHCP IP 地址的方法。
- 如果使用的是静态 IP 地址，则为每个网格节点提供所需的网络详细信息（ IP 地址，网关，网络掩码）。

有关其他接口的信息

安装节点后，您可以选择在 vCenter 中为虚拟机添加中继或访问接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

您添加的接口将显示在 "VLAN interfaces" 页面和网格管理器的 "HA Groups" 页面上。

- 如果要添加中继接口，请为每个新的父接口配置一个或多个 VLAN 接口。请参见 配置 VLAN 接口。
- 如果添加访问接口，则必须将其直接添加到 HA 组。请参见 配置高可用性组。

虚拟存储节点的存储卷

您必须收集基于虚拟机的存储节点的以下信息：

- 计划添加的存储卷（存储 LUN ）的数量和大小。请 `s" 存储和性能要求 " 。`

网格配置信息

您必须收集信息才能配置网格：

- 网格许可证
- 网络时间协议（ NTP ）服务器 IP 地址
- 域名系统（ DNS ）服务器 IP 地址

相关信息

网格节点如何发现主管理节点

存储和性能要求

网格节点如何发现主管理节点

网格节点与主管理节点进行通信以进行配置和管理。每个网格节点都必须知道网格网络上主管理节点的 IP 地址。

为了确保网格节点可以访问主管理节点，您可以在部署此节点时执行以下任一操作：

- 您可以使用 admin_ip 参数手动输入主管理节点的 IP 地址。
- 您可以省略 admin_ip 参数，以使网格节点自动发现该值。当网格网络使用 DHCP 为主管理节点分配 IP 地址时，自动发现尤其有用。

可以使用多播域名系统（ mDNS ）自动发现主管理节点。主管理节点首次启动时，它会使用 mDNS 发布其 IP 地址。然后，同一子网上的其他节点可以查询 IP 地址并自动获取该地址。但是，由于多播 IP 流量通常不能跨子网路由，因此其他子网上的节点无法直接获取主管理节点的 IP 地址。

如果使用自动发现：

- 必须在主管理节点未直接连接到的任何子网上至少包含一个网格节点的 admin_IP 设置。然后，此网格节点将发布子网中其他节点的主管理节点 IP 地址，以便使用 mDNS 进行发现。
- 确保您的网络基础架构支持在子网内传递多播 IP 流量。

将 **StorageGRID** 节点部署为虚拟机

您可以使用 VMware vSphere Web Client 将每个网格节点部署为虚拟机。在部署期间，系统会创建每个网格节点并将其连接到一个或多个 StorageGRID 网络。

如果需要部署任何 StorageGRID 设备存储节点，请参见该设备的安装和维护说明。

您也可以在打开节点电源之前重新映射节点端口或增加节点的 CPU 或内存设置。

您需要的内容

- 您已查看如何操作 规划并准备安装，您了解软件， CPU 和 RAM 以及存储和性能的要求。
- 您熟悉 VMware vSphere 虚拟机管理程序，并具有在此环境中部署虚拟机的经验。

> StorageGRID 虚拟机附带了 `open-vm-tools` 软件包，该软件包是一种类似于 VMware Tools 的开源实施方案。您无需手动安装 VMware Tools 。

- 您已下载并提取适用于 VMware 的正确版本的 StorageGRID 安装归档。

> 如果要在扩展或恢复操作中部署新节点，则必须使用网格上当前运行的 StorageGRID 版本。

- 您已有 StorageGRID 虚拟机磁盘（` .vmdk` ）文件：

```
NetApp-SG-version-SHA.vmdk
```

- 您已为要部署的每种网格节点配置了 ` .OVF` 和 ` .MF` 文件：

文件名	Description
vsphere-primary-admin.OVF vsphere-primary-admin.mf	主管理节点的模板文件和清单文件。
vsphere-non-primary-admin.OVF vsphere-non-primary-admin.mf	非主管理节点的模板文件和清单文件。
vsphere-archive.OVF vsphere-archive.mf	归档节点的模板文件和清单文件。
vsphere-gateway.OVF vsphere-gateway.mf	网关节点的模板文件和清单文件。
vsphere-storage.OVF vsphere-storage.mf	存储节点的模板文件和清单文件。

- ` .vdmk` ， ` .OVF` 和 ` .MF` 文件均位于同一目录中。
- 您计划最大限度地减少故障域。例如，不应将所有网关节点部署在一个虚拟机服务器上。

> 在生产部署中，请勿在一个虚拟机服务器上运行多个存储节点。对每个存储节点使用专用虚拟机主机可提供一个隔离的故障域。

- 如果要在扩展或恢复操作中部署节点，则可以使用 有关扩展 StorageGRID 系统的说明 或 恢复和维护说明。
- 如果您要将StorageGRID 节点部署为虚拟机、并从NetApp ONTAP 系统分配存储、则表示您已确认卷未启用FabricPool 分层策略。例如，如果 StorageGRID 节点在 VMware 主机上作为虚拟机运行，请确保为该节

点的数据存储库提供支持的卷未启用 FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

关于此任务

按照以下说明开始部署 VMware 节点，在扩展中添加新的 VMware 节点或在恢复操作中更换 VMware 节点。除步骤中所述外，所有节点类型的节点部署操作步骤 均相同，包括管理节点，存储节点，网关节点和归档节点。

如果要安装新的 StorageGRID 系统：

- 在部署任何其他网格节点之前，必须先部署主管理节点。
- 您必须确保每个虚拟机均可通过网格网络连接到主管理节点。
- 在配置网格之前，必须部署所有网格节点。

如果要执行扩展或恢复操作：

- 您必须确保新虚拟机可以通过网格网络连接到主管理节点。

如果您需要重新映射节点的任何端口，请勿打开新节点的电源，直到端口重新映射配置完成为止。

步骤

1. 使用 vCenter 部署 OVF 模板。

   如果指定 URL ，请指向包含以下文件的文件夹。否则，请从本地目录中选择其中每个文件。

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

   例如，如果这是要部署的第一个节点，请使用以下文件为 StorageGRID 系统部署主管理节点：

   ```
   NetApp-SG-version-SHA.vmdk
   sphere-primary-admin.ovf
   sphere-primary-admin.mf
   ```

2. 提供虚拟机的名称。

   标准做法是，对虚拟机和网格节点使用相同的名称。

3. 将虚拟机放置在相应的 vApp 或资源池中。
4. 如果要部署主管理节点，请阅读并接受最终用户许可协议。

   根据您的 vCenter 版本，在接受最终用户许可协议，指定虚拟机名称以及选择数据存储库方面，步骤顺序会有所不同。

5. 为虚拟机选择存储。

   如果要在恢复操作中部署节点，请执行中的说明 存储恢复步骤 要添加新的虚拟磁盘，请从故障网格节点重新连接虚拟硬盘，或者同时从这两个节点重新连接虚拟硬盘。

   部署存储节点时，请使用 3 个或更多存储卷，每个存储卷的容量为 4 TB 或更大。您必须至少为卷 0 分配 4 TB 。

   > 存储节点 .OVF 文件为存储定义了多个 VMDK 。除非这些 VMDK 满足您的存储要求，否则应先将其删除，并为存储分配适当的 VMDK 或 RDM ，然后再启动节点。VMDK 在 VMware 环境中更常用，并且更易于管理，而 RDM 则可以为使用较大对象大小（例如大于 100 MB ）的工作负载提供更好的性能。

   > 某些 StorageGRID 安装可能会使用比典型虚拟化工作负载更大，更活跃的存储卷。要获得最佳性能，您可能需要调整某些虚拟机管理程序参数，例如 `MaxAddressableSpaceTB` 。如果遇到性能不佳的问题，请联系虚拟化支持资源，以确定您的环境是否可以从特定于工作负载的配置调整中受益。

6. 选择网络。

   通过为每个源网络选择一个目标网络来确定节点要使用的 StorageGRID 网络。

   - 网格网络为必填项。您必须在 vSphere 环境中选择目标网络。
   - 如果使用管理网络，请在 vSphere 环境中选择其他目标网络。如果不使用管理网络，请选择为网格网络选择的同一目标。
   - 如果您使用客户端网络，请在 vSphere 环境中选择其他目标网络。如果不使用客户端网络，请选择为网格网络选择的同一目标。

7. 在 * 自定义模板 * 下，配置所需的 StorageGRID 节点属性。

   a. 输入 * 节点名称 * 。

      > 如果要恢复网格节点，则必须输入要恢复的节点的名称。

   b. 在 * 网格网络（ eth0 ） * 部分中，为 * 网格网络 IP 配置 * 选择静态或 DHCP 。

      - 如果选择静态，请输入 * 网格网络 IP* ， * 网格网络掩码 * ， * 网格网络网关 * 和 * 网格网络 MTU* 。
      - 如果选择 DHCP ，则会自动分配 * 网格网络 IP* ， * 网格网络掩码 * 和 * 网格网络网关 * 。

   c. 在 * 主管理 IP* 字段中，输入网格网络的主管理节点的 IP 地址。

      > 如果要部署的节点是主管理节点，则此步骤不适用。

   如果省略主管理节点 IP 地址，则如果主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上，则会自动发现此 IP 地址。但是，建议在此处设置主管理节点 IP 地址。

   a. 在 * 管理网络（ eth1 ） * 部分中，为 * 管理网络 IP 配置 * 选择静态， DHCP 或禁用。

      - 如果不想使用管理网络，请选择 disabled 并为管理网络 IP 输入 * 。 0.0.0.0* 。您可以将其他字段留空。

- 如果选择 static ，请输入 * 管理网络 IP* ， * 管理网络掩码 * ， * 管理网络网关 * 和 * 管理网络 MTU* 。
- 如果选择 static ，请输入 * 管理网络外部子网列表 * 。您还必须配置网关。
- 如果选择 DHCP ，则会自动分配 * 管理网络 IP* ， * 管理网络掩码 * 和 * 管理网络网关 * 。

b. 在 * 客户端网络（ eth2 ） * 部分中，为 * 客户端网络 IP 配置 * 选择静态， DHCP 或禁用。

- 如果不想使用客户端网络，请选择 disabled 并为客户端网络 IP 输入 * 。 0.0.0.0* 。您可以将其他字段留空。
- 如果选择 static ，请输入 * 客户端网络 IP* ， * 客户端网络掩码 * ， * 客户端网络网关 * 和 * 客户端网络 MTU* 。
- 如果选择 DHCP ，则会自动分配 * 客户端网络 IP* ， * 客户端网络掩码 * 和 * 客户端网络网关 * 。

8. 查看虚拟机配置并进行必要的更改。
9. 准备好完成后，选择 * 完成 * 以开始上传虚拟机。
10. 如果您在恢复操作中部署了此节点，而此节点不是全节点恢复，请在部署完成后执行以下步骤：

a. 右键单击虚拟机，然后选择 * 编辑设置 * 。

b. 选择已指定用于存储的每个默认虚拟硬盘，然后选择 * 删除 * 。

c. 根据您的数据恢复情况，根据您的存储要求添加新的虚拟磁盘，重新连接从先前删除的故障网格节点中保留的任何虚拟硬盘，或者同时重新连接这两者。

请注意以下重要准则：

- 如果要添加新磁盘，则应使用节点恢复之前使用的相同类型的存储设备。
- 存储节点 .OVF 文件为存储定义了多个 VMDK 。除非这些 VMDK 满足您的存储要求，否则应先将其删除，并为存储分配适当的 VMDK 或 RDM ，然后再启动节点。VMDK 在 VMware 环境中更常用，并且更易于管理，而 RDM 则可以为使用较大对象大小（例如大于 100 MB ）的工作负载提供更好的性能。

11. 如果需要重新映射此节点使用的端口，请按照以下步骤进行操作。

如果企业网络策略限制对 StorageGRID 使用的一个或多个端口的访问，则可能需要重新映射端口。请参见网络连接准则 用于 StorageGRID 使用的端口。

> 请勿重新映射负载平衡器端点中使用的端口。

a. 选择新虚拟机。

b. 从配置选项卡中，选择 * 设置 * > * vApp 选项 * 。* vApp Options* 的位置取决于 vCenter 的版本。

c. 在 * 属性 * 表中，找到 port_remap_inbound 和 port_remap 。

d. 要对称映射端口的入站和出站通信，请选择 * 端口重新映射 * 。

> 如果仅设置 port_remap ，则表示您指定的适用场景 入站和出站通信映射。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。

i. 滚动回表顶部，然后选择 * 编辑 * 。

ii. 在类型选项卡上，选择 * 用户可配置 * ，然后选择 * 保存 * 。

iii. 选择 * 设置值 * 。

iv. 输入端口映射：

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

` < 网络类型 >` 是网格，管理员或客户端， ` < 协议 >` 是 TCP 或 UDP 。

例如，要将 ssh 流量从端口 22 重新映射到端口 3022 ，请输入：

```
client/tcp/22/3022
```

i. 选择 * 确定 * 。

e. 要指定用于与节点的入站通信的端口，请选择 * 端口重新映射 _inbound* 。

如果指定 port_remap_inbound 且不指定 port_remap 的值，则端口的出站通信将保持不变。

i. 滚动回表顶部，然后选择 * 编辑 * 。

ii. 在类型选项卡上，选择 * 用户可配置 * ，然后选择 * 保存 * 。

iii. 选择 * 设置值 * 。

iv. 输入端口映射：

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

` < 网络类型 >` 是网格，管理员或客户端， ` < 协议 >` 是 TCP 或 UDP 。

例如，要重新映射发送到端口 3022 的入站 SSH 流量，以便网格节点在端口 22 接收此流量，请输入以下内容：

```
client/tcp/3022/22
```

i. 选择 * 确定 *

12. 如果要从默认设置中增加节点的 CPU 或内存：

a. 右键单击虚拟机，然后选择 * 编辑设置 * 。

b. 根据需要更改 CPU 数量或内存量。

将 * 内存预留 * 设置为与分配给虚拟机的 * 内存 * 大小相同的大小。

c. 选择 * 确定 * 。

13. 启动虚拟机。

完成后

如果将此节点部署为扩展或恢复操作步骤 的一部分，请返回到这些说明以完成此操作步骤 。

配置网格并完成安装（ **VMware** ）

导航到网格管理器

您可以使用网格管理器定义配置 StorageGRID 系统所需的所有信息。

您需要的内容

必须部署主管理节点，并且已完成初始启动序列。

步骤

1. 打开 Web 浏览器并导航到以下地址之一：

   `https://primary_admin_node_ip`

   ` 客户端网络 IP`

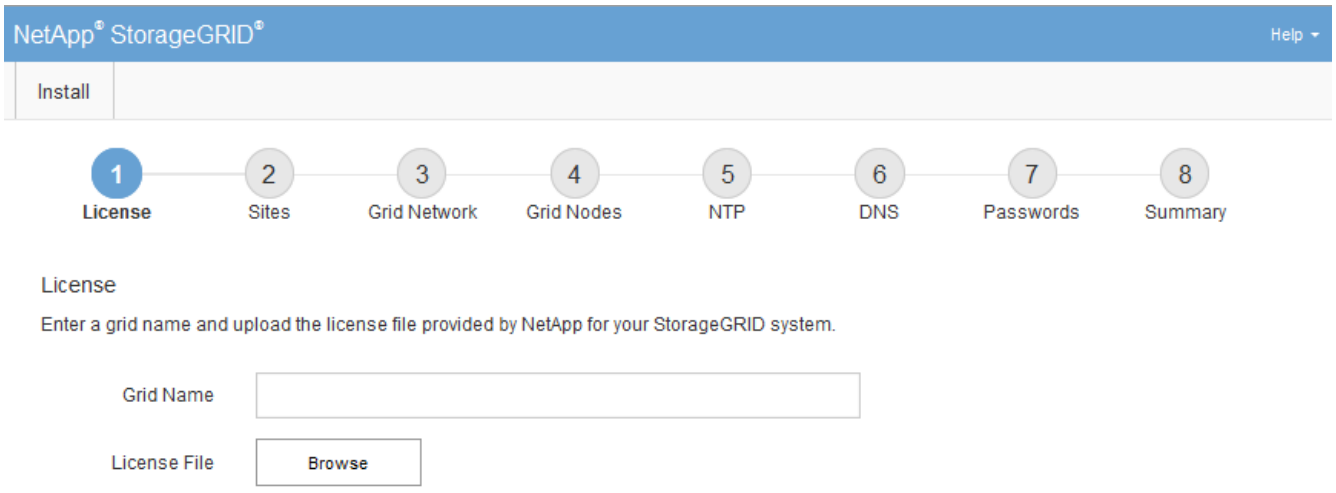
   或者，您也可以通过端口 8443 访问网格管理器：

   `https://primary_admin_node_ip:8443`

   根据您的网络配置，您可以使用网格网络或管理网络上的主管理节点 IP 的 IP 地址。

2. 单击 * 安装 StorageGRID 系统 * 。

   此时将显示用于配置 StorageGRID 网格的页面。



指定 **StorageGRID** 许可证信息

您必须指定 StorageGRID 系统的名称并上传 NetApp 提供的许可证文件。

步骤

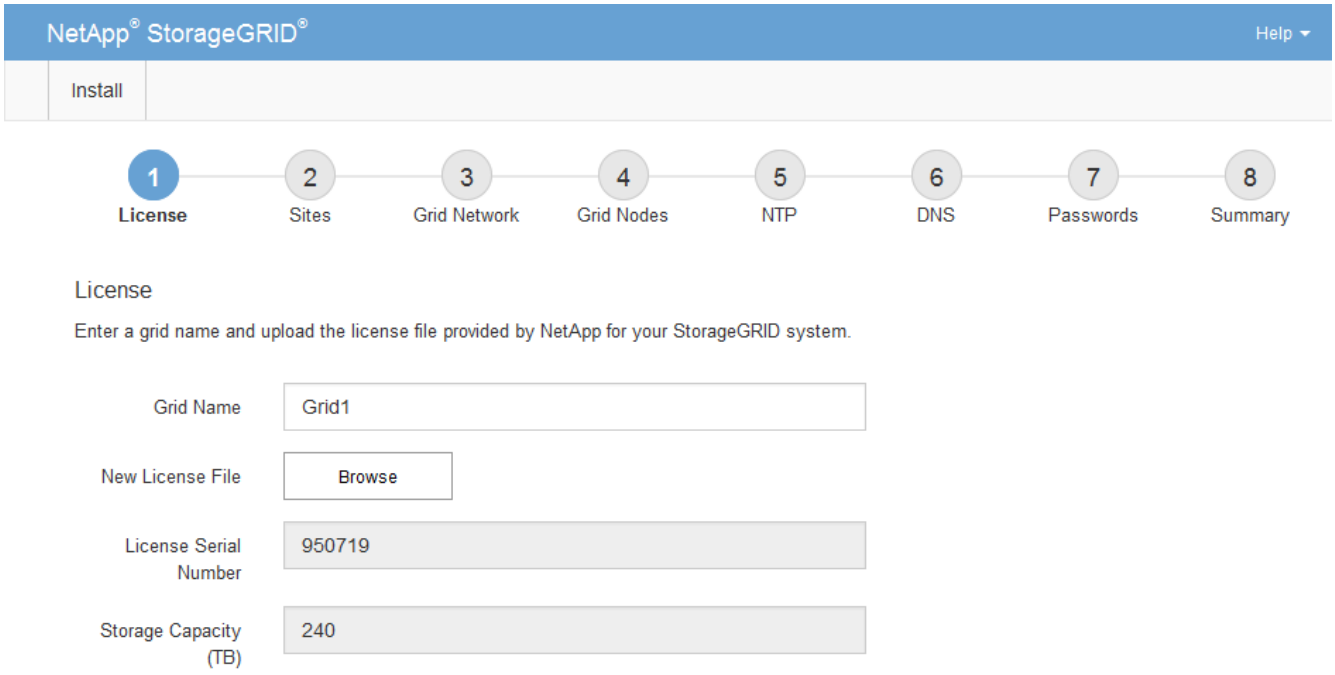
1. 在许可证页面上，在 * 网格名称 * 中为您的 StorageGRID 系统输入一个有意义的名称。

   安装后，此名称将显示在节点菜单的顶部。

2. 单击 * 浏览 * ，找到 NetApp 许可证文件（`NLFunique_id.txt`），然后单击 * 打开 * 。

   此时将验证许可证文件，并显示序列号和许可的存储容量。

   StorageGRID 安装归档包含一个免费许可证，不提供产品的任何支持授权。您可以在安装后更新为提供支持的许可证。



3. 单击 * 下一步 * 。

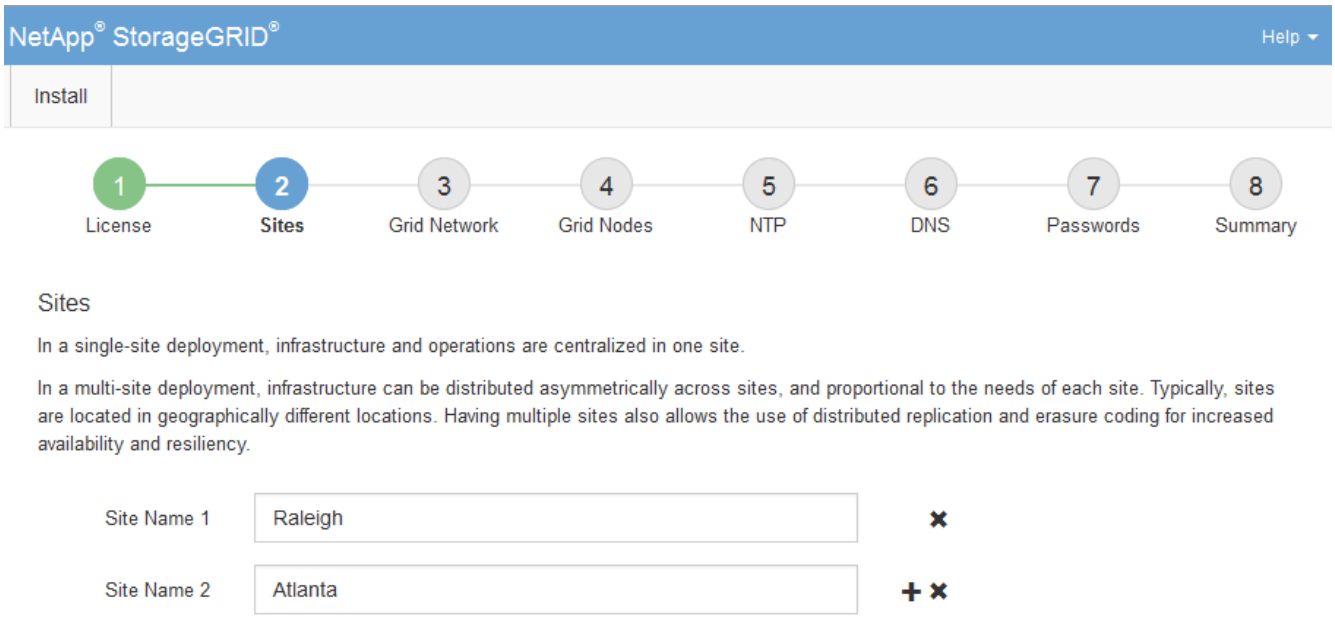
添加站点

安装 StorageGRID 时，必须至少创建一个站点。您可以创建其他站点来提高 StorageGRID 系统的可靠性和存储容量。

步骤

1. 在 Sites 页面上，输入 * 站点名称 * 。
2. 要添加其他站点，请单击最后一个站点条目旁边的加号，然后在新的 * 站点名称 * 文本框中输入名称。

   根据需要为网格拓扑添加尽可能多的其他站点。您最多可以添加 16 个站点。



3. 单击 * 下一步 * 。

指定网格网络子网

您必须指定网格网络上使用的子网。

关于此任务

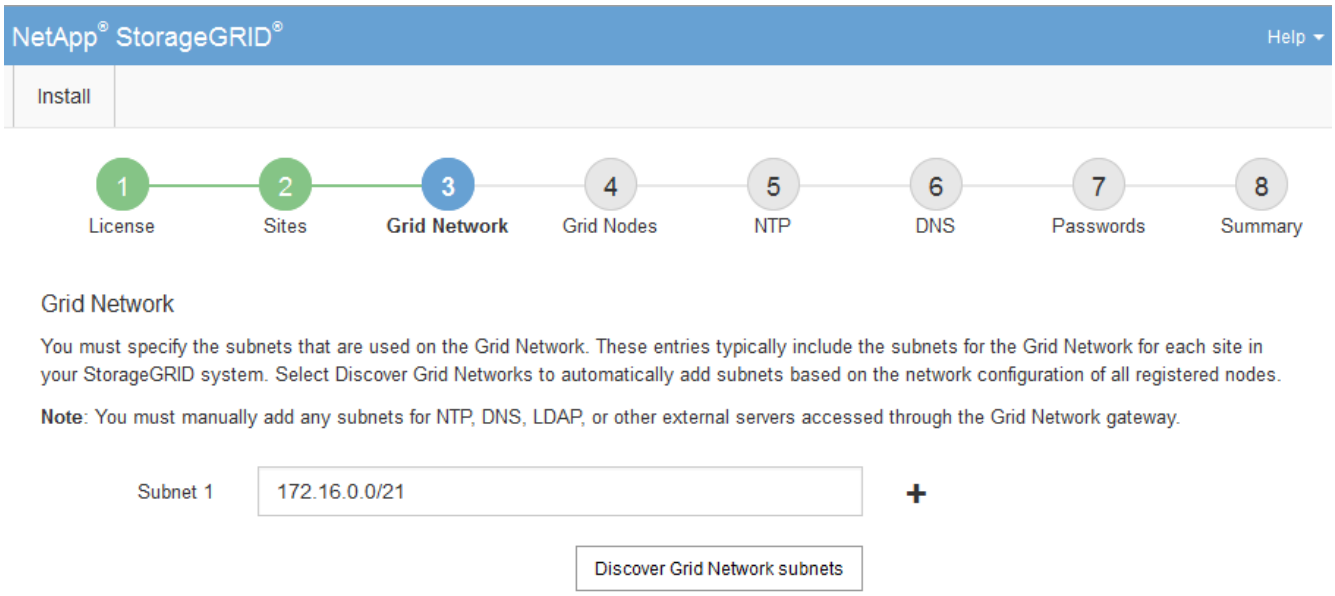
子网条目包括 StorageGRID 系统中每个站点的网格网络子网，以及需要通过网格网络访问的任何子网。

如果您有多个网格子网，则需要使用网格网络网关。指定的所有网格子网都必须可通过此网关访问。

步骤

1. 在 * 子网 1* 文本框中至少为一个网格网络指定 CIDR 网络地址。
2. 单击最后一个条目旁边的加号以添加其他网络条目。

   如果已至少部署一个节点，请单击 * 发现网格网络子网 * 以自动使用已向网格管理器注册的网格节点报告的子网填充网格网络子网列表。



3. 单击 * 下一步 * 。

批准待定网格节点

您必须先批准每个网格节点，然后才能将其加入 StorageGRID 系统。

您需要的内容

您已部署所有虚拟设备和 StorageGRID 设备网格节点。

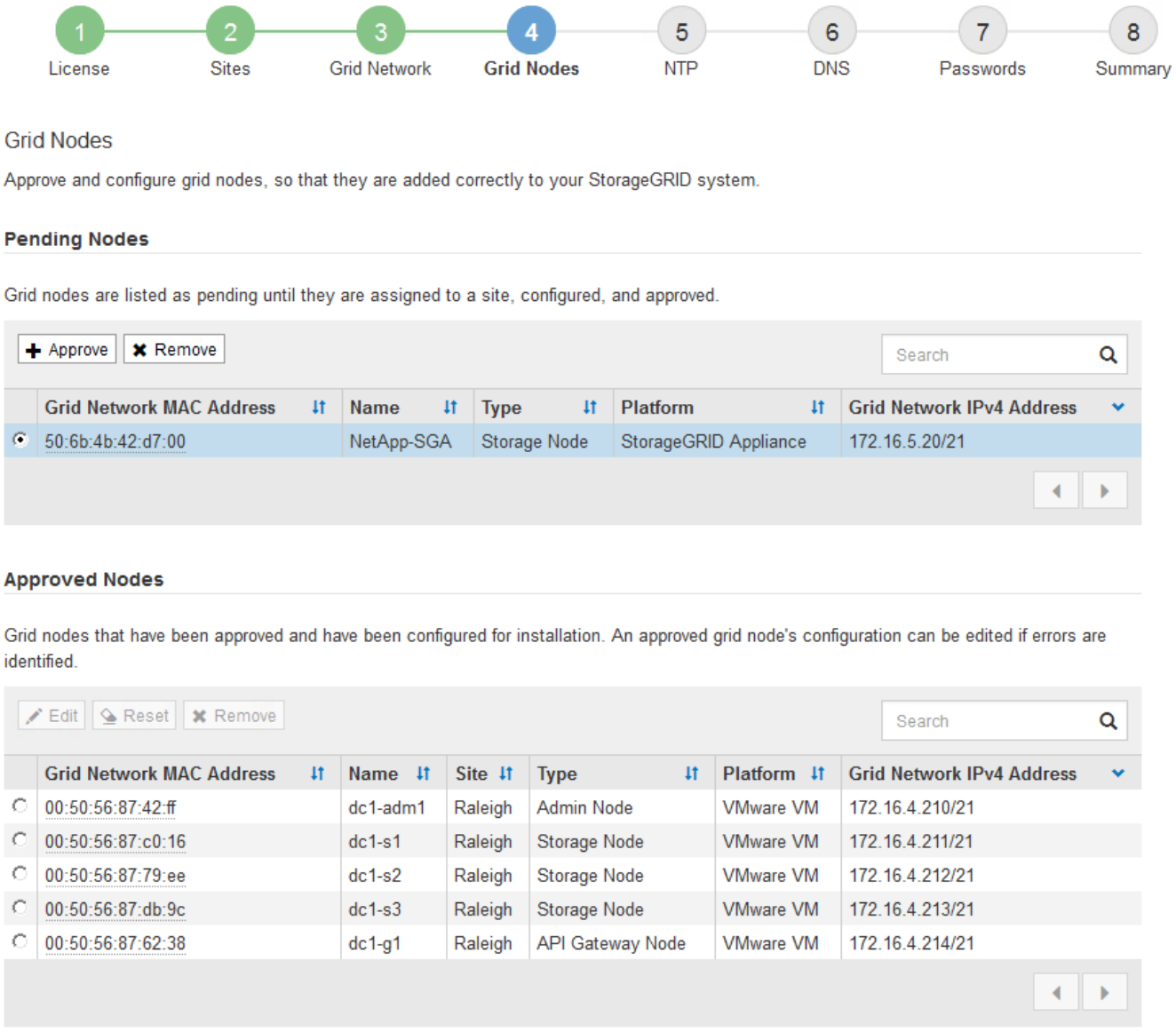
对所有节点执行一次安装比现在安装某些节点以及稍后安装某些节点更高效。

步骤

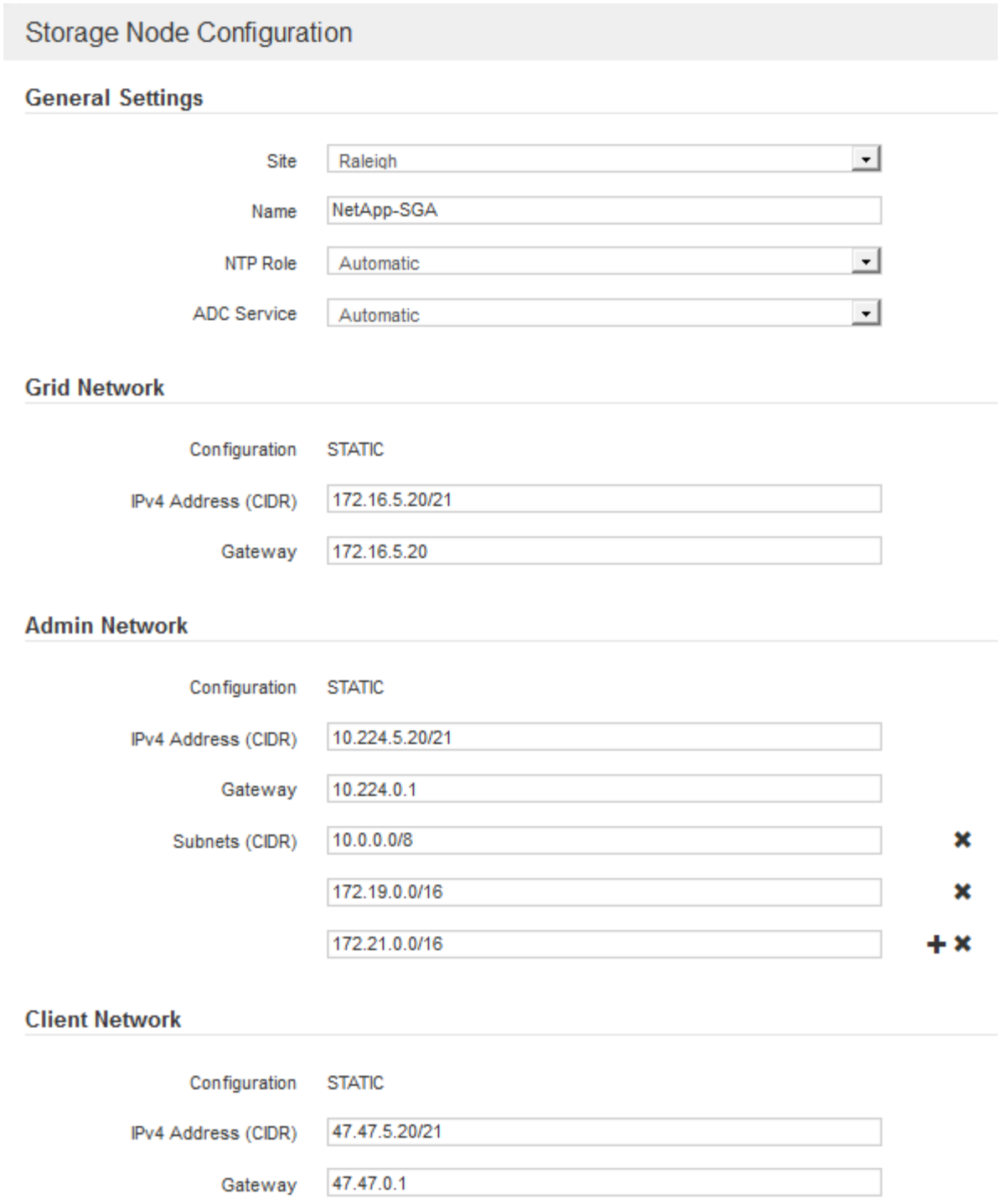
1. 查看 Pending Nodes 列表，并确认它显示了您部署的所有网格节点。

   如果缺少网格节点，请确认已成功部署该节点。

2. 选择要批准的待定节点旁边的单选按钮。



3. 单击 * 批准 * 。
4. 在常规设置中，根据需要修改以下属性的设置：



◦ * 站点 * ： 要与此网格节点关联的站点的名称。

◦ * 名称 * ： 分配给节点的名称以及将在网格管理器中显示的名称。此名称默认为您在配置节点时指定的名称。在安装过程的此步骤中，您可以根据需要更改名称。

完成安装后，您将无法更改节点的名称。

对于 VMware 节点，您可以在此处更改名称，但此操作不会更改 vSphere 中虚拟机的名称。

◦ * NTP 角色 * ： 网格节点的网络时间协议（ NTP ）角色。选项包括 * 自动 * ， * 主 * 和 * 客户端 * 。选

择 * 自动 * 会将主角色分配给管理节点，具有模板转换服务的存储节点，网关节点以及具有非静态 IP 地址的任何网格节点。所有其他网格节点都分配有客户端角色。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

- * ADC* 服务 * （仅限存储节点）：选择 * 自动 * ，让系统确定节点是否需要管理域控制器（ ADC* ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。每个站点至少有三个存储节点必须包含此 ADC-Service 。在部署此节点后，您不能将此 ADC 服务添加到该节点中。

5. 在网格网络中，根据需要修改以下属性的设置：

   - * IPv4 地址（ CIDR ） *：网格网络接口（容器中的 eth0 ）的 CIDR 网络地址。例如： 192.168.1.234/21
   - * 网关 *： 网格网络网关。例如： 192.168.0.1

     > 如果存在多个网格子网，则需要使用网关。

   > 如果您为网格网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

6. 如果要为网格节点配置管理网络，请根据需要在管理网络部分中添加或更新设置。

   在 * 子网（ CIDR ） * 文本框中输入从此接口路由的目标子网。如果存在多个管理子网，则需要使用管理网关。

   > 如果您为管理网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

   - 设备： * 对于 StorageGRID 设备，如果在初始安装期间未使用 StorageGRID 设备安装程序配置管理网络，则无法在此网格管理器对话框中进行配置。而是必须执行以下步骤：

     a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

        重新启动可能需要几分钟时间。

     b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。
     c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。
     d. 返回主页页面，然后单击 * 开始安装 * 。
     e. 在网格管理器中：如果节点列在 "Approved Nodes" 表中，请重置节点。
     f. 从 Pending Nodes 表中删除此节点。
     g. 等待节点重新出现在 "Pending Nodes" 列表中。
     h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。

        对于追加信息 ，请参见适用于您的设备型号的安装和维护说明。

7. 如果要为网格节点配置客户端网络，请根据需要在客户端网络部分中添加或更新设置。如果配置了客户端网

络，则需要使用网关，安装后，它将成为节点的默认网关。

> 如果您为客户端网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保生成的 IP 地址不在 DHCP 地址池中。

- 设备： * 对于 StorageGRID 设备，如果在初始安装期间未使用 StorageGRID 设备安装程序配置客户端网络，则无法在此网格管理器对话框中进行配置。而是必须执行以下步骤：

  a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

     重新启动可能需要几分钟时间。

  b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。

  c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。

  d. 返回主页页面，然后单击 * 开始安装 * 。

  e. 在网格管理器中：如果节点列在 "Approved Nodes" 表中，请重置节点。

  f. 从 Pending Nodes 表中删除此节点。

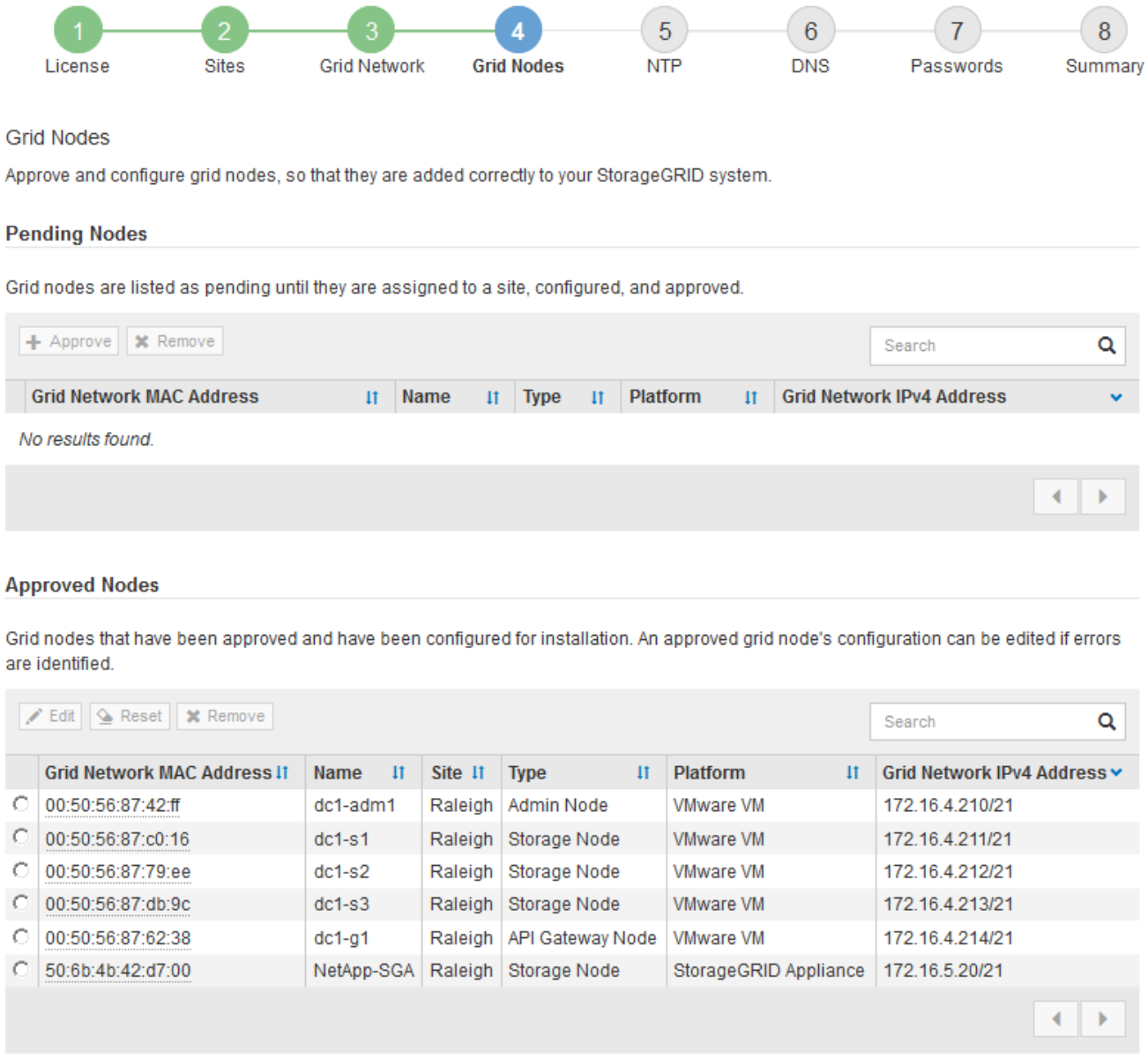
  g. 等待节点重新出现在 "Pending Nodes" 列表中。

  h. 确认您可以配置适当的网络。它们应已填充您在 IP 配置页面上提供的信息。

     对于追加信息 ，请参见适用于您的设备的安装和维护说明。

8. 单击 * 保存 * 。

网格节点条目将移至 "Approved Nodes" 列表。



9. 对要批准的每个待定网格节点重复上述步骤。

   您必须批准网格中所需的所有节点。但是，在单击 " 摘要 " 页面上的 * 安装 * 之前，您可以随时返回此页面。您可以通过选择已批准的网格节点的单选按钮并单击 * 编辑 * 来修改其属性。

10. 批准完网格节点后，单击 * 下一步 * 。

指定网络时间协议服务器信息

您必须为 StorageGRID 系统指定网络时间协议（ NTP ）配置信息，以便在不同服务器上执行的操作保持同步。

关于此任务

您必须为 NTP 服务器指定 IPv4 地址。

您必须指定外部 NTP 服务器。指定的 NTP 服务器必须使用 NTP 协议。

您必须指定四个引用 Stratum 3 或更高配置的 NTP 服务器，以防止出现时间偏差问题。

> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。

"支持边界，用于为高精度环境配置 Windows 时间服务"

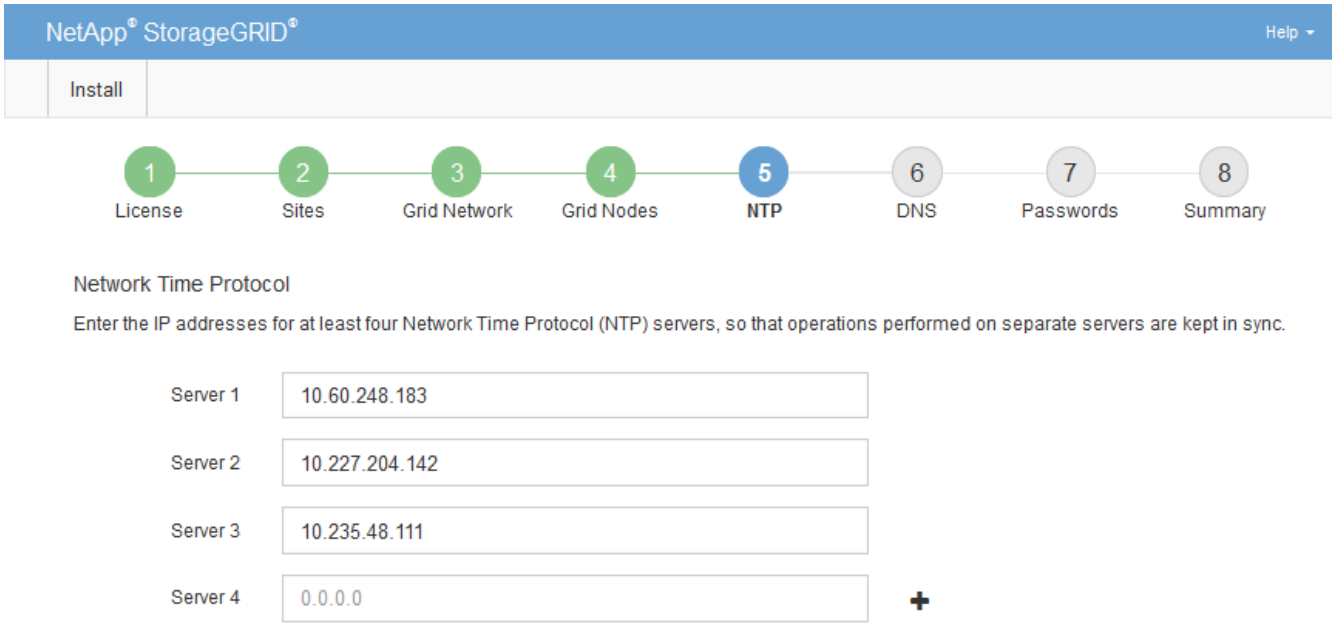
外部 NTP 服务器由先前分配了主 NTP 角色的节点使用。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

对 VMware 执行其他检查，例如确保虚拟机管理程序与虚拟机使用相同的 NTP 源，以及使用 VMTools 禁用虚拟机管理程序与 StorageGRID 虚拟机之间的时间同步。

步骤

1. 在 * 服务器 1* 到 * 服务器 4* 文本框中指定至少四个 NTP 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



3. 选择 * 下一步 * 。

指定域名系统服务器信息

您必须为 StorageGRID 系统指定域名系统（ DNS ）信息，以便可以使用主机名而非 IP 地址访问外部服务器。

关于此任务

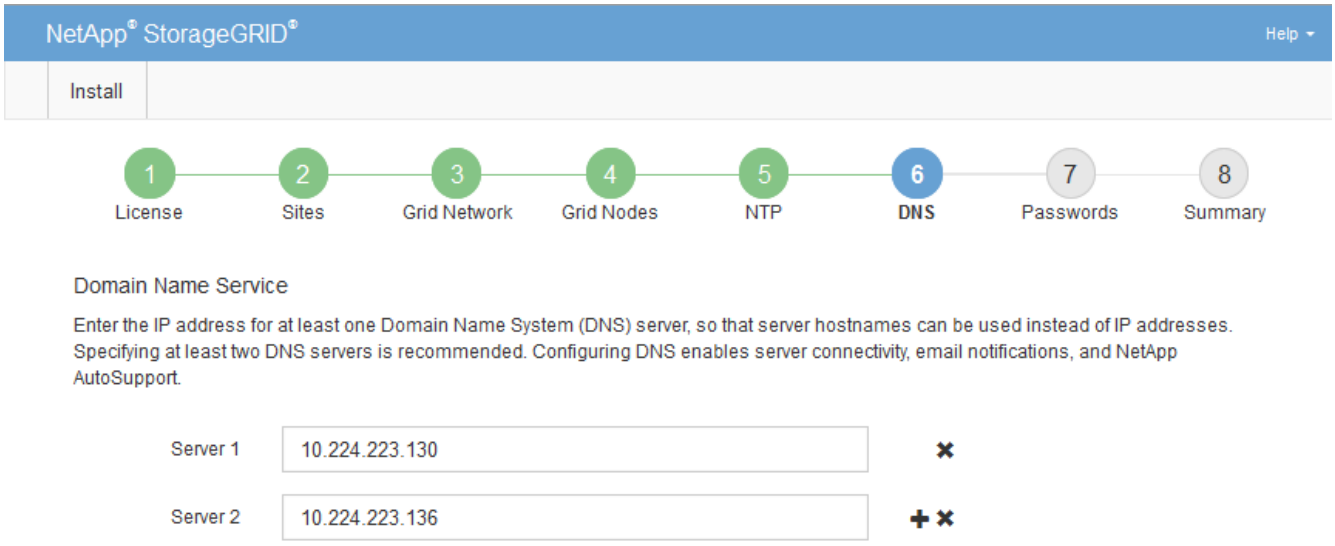
通过指定 DNS 服务器信息，您可以对电子邮件通知和 AutoSupport 使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。建议至少指定两个 DNS 服务器。

为 DNS 服务器提供两到六个 IPv4 地址。您应选择 DNS 服务器，以便在网络隔离时每个站点都可以在本地访问这些服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以进一步自定义每个节点的 DNS 服务器列表。有关详细信息，请参见恢复和维护说明中有关修改 DNS 配置的信息。

如果省略 DNS 服务器信息或 DNS 服务器信息配置不正确，则会在每个网格节点的 SSM 服务上触发 DNST 警报。如果 DNS 配置正确且新服务器信息已到达所有网格节点，则警报将清除。

步骤

1. 在 * 服务器 1* 文本框中至少指定一个 DNS 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



最佳实践是至少指定两个 DNS 服务器。最多可以指定六个 DNS 服务器。

3. 选择 * 下一步 * 。

相关信息

恢复和维护

指定 **StorageGRID** 系统密码

在安装 StorageGRID 系统时，您需要输入密码以保护系统安全并执行维护任务。

关于此任务

使用安装密码页面指定配置密码短语和网格管理 root 用户密码。

- 配置密码短语用作加密密钥，不会由 StorageGRID 系统存储。
- 您必须具有用于安装，扩展和维护过程的配置密码短语，包括下载恢复软件包。因此，请务必将配置密码短语存储在安全位置。
- 如果您使用的是最新的网格管理器，则可以从网格管理器更改配置密码短语。
- 可以使用网格管理器更改网格管理 root 用户密码。
- 随机生成的命令行控制台和 SSH 密码存储在恢复软件包中的 `passwords.txt` 文件中。

步骤

1. 在 * 配置密码短语 * 中，输入更改 StorageGRID 系统网格拓扑所需的配置密码短语。

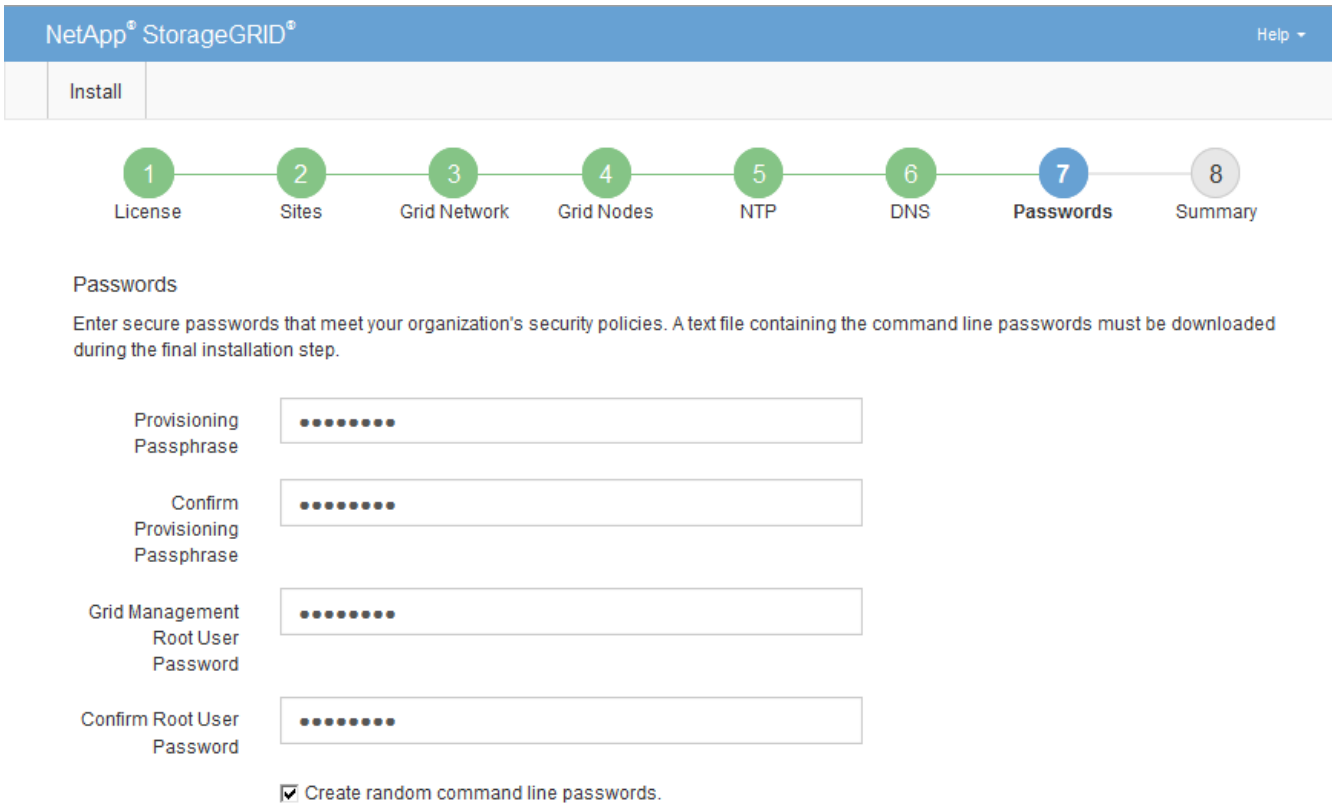
   将配置密码短语存储在安全位置。

   > 如果在安装完成后您希望稍后更改配置密码短语，则可以使用网格管理器。选择 * 配置 * > * 访问控制 * > * 网格密码 * 。

2. 在 * 确认配置密码短语 * 中，重新输入配置密码短语进行确认。
3. 在 * 网格管理 root 用户密码 * 中，以 "`root` " 用户身份输入用于访问网格管理器的密码。

   将密码存储在安全的位置。

4. 在 * 确认 root 用户密码 * 中，重新输入网格管理器密码进行确认。



5. 如果要安装网格以进行概念验证或演示，也可以取消选中 * 创建随机命令行密码 * 复选框。

   对于生产部署，出于安全原因，应始终使用随机密码。如果要使用默认密码通过命令行使用 "`root` " 或 "`admin` " 帐户访问网格节点，请取消选择 * 仅为演示网格创建随机命令行密码 * 。

   > 单击摘要页面上的 * 安装 * 后，系统将提示您下载恢复软件包文件（ `sGWS-recovery-package-id-revision.zip` ）。您必须 下载此文件 以完成安装。访问系统所需的密码存储在恢复软件包文件中的 `passwords.txt` 文件中。

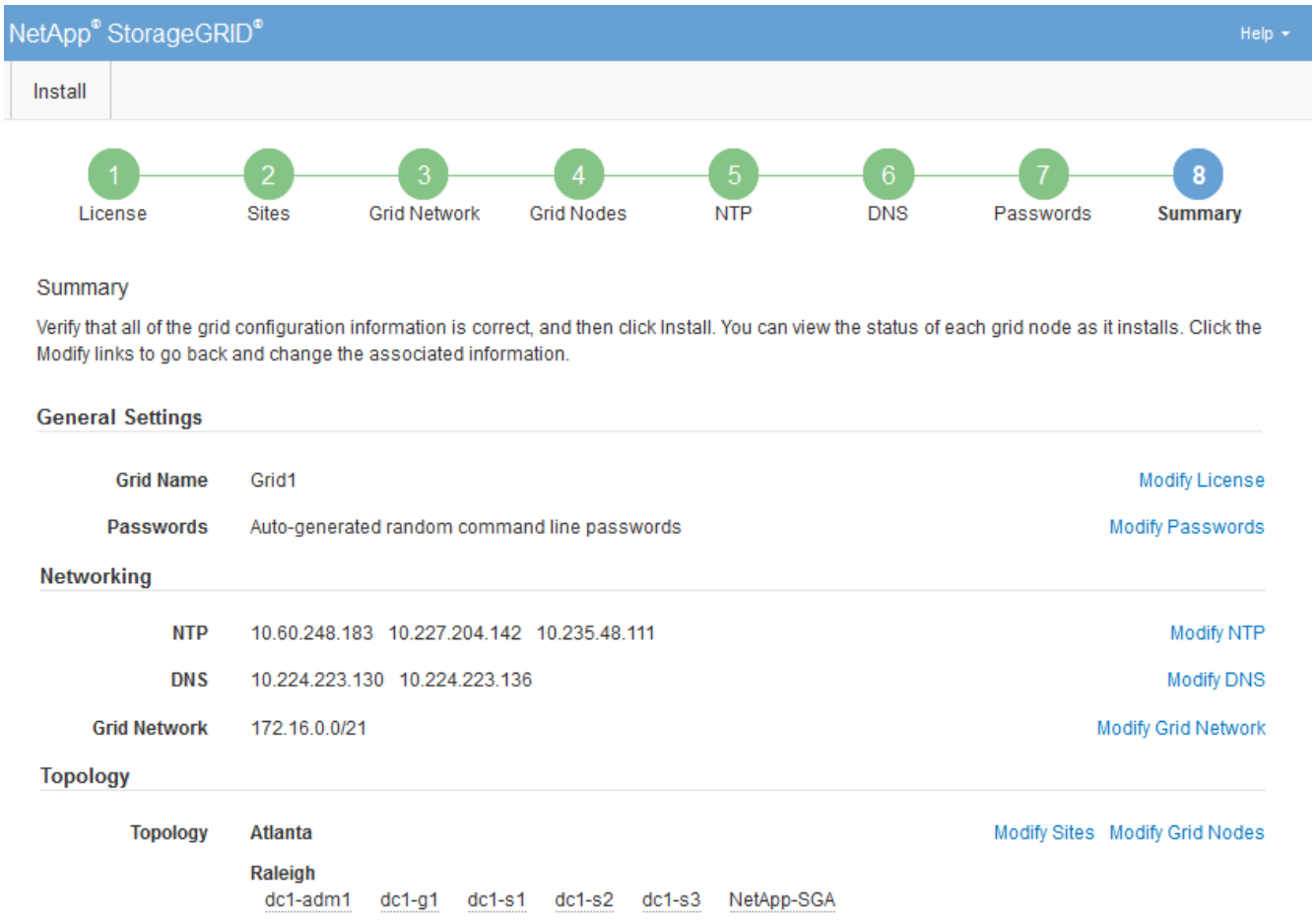
6. 单击 * 下一步 * 。

查看您的配置并完成安装

您必须仔细查看输入的配置信息，以确保安装成功完成。

步骤

1. 查看 * 摘要 * 页面。



2. 验证所有网格配置信息是否正确。使用摘要页面上的修改链接返回并更正任何错误。
3. 单击 * 安装 * 。

> 如果将某个节点配置为使用客户端网络，则在单击 * 安装 * 时，该节点的默认网关会从网格网络切换到客户端网络。如果连接断开，则必须确保通过可访问的子网访问主管理节点。请参见 网络连接准则 了解详细信息。

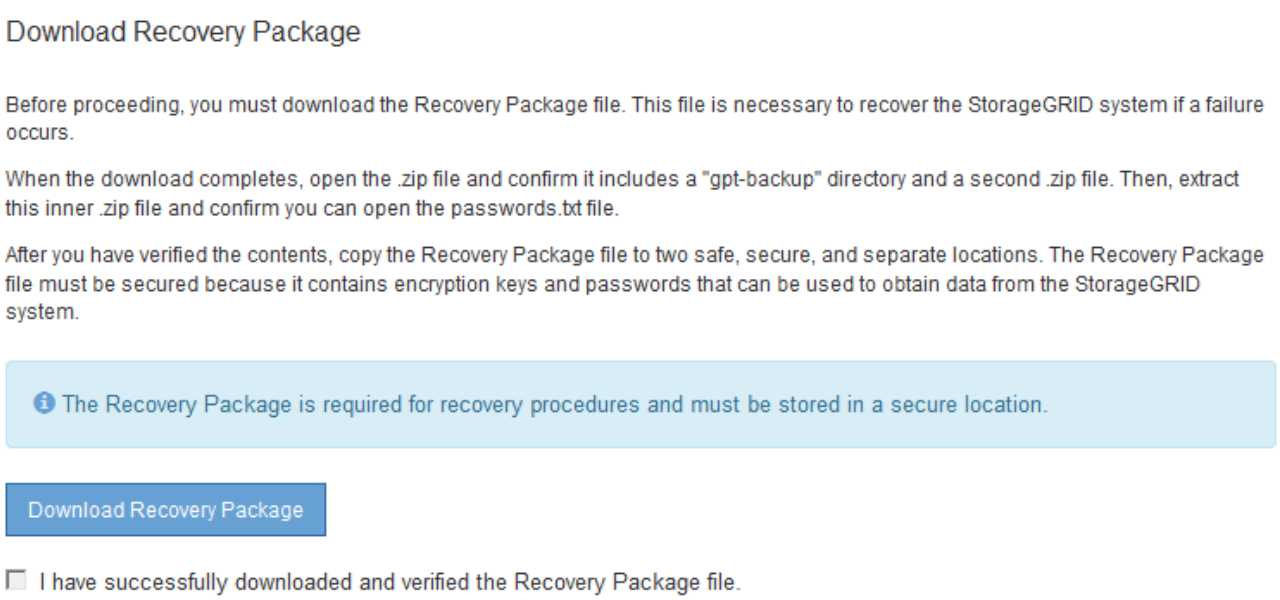
4. 单击 * 下载恢复包 * 。

   当安装过程进展到定义网格拓扑时，系统会提示您下载恢复包文件（` .zip` ），并确认您可以成功访问此文件的内容。您必须下载恢复软件包文件，以便在一个或多个网格节点出现故障时恢复 StorageGRID 系统。安装将在后台继续进行，但您无法完成安装并访问 StorageGRID 系统，直到下载并验证此文件为止。

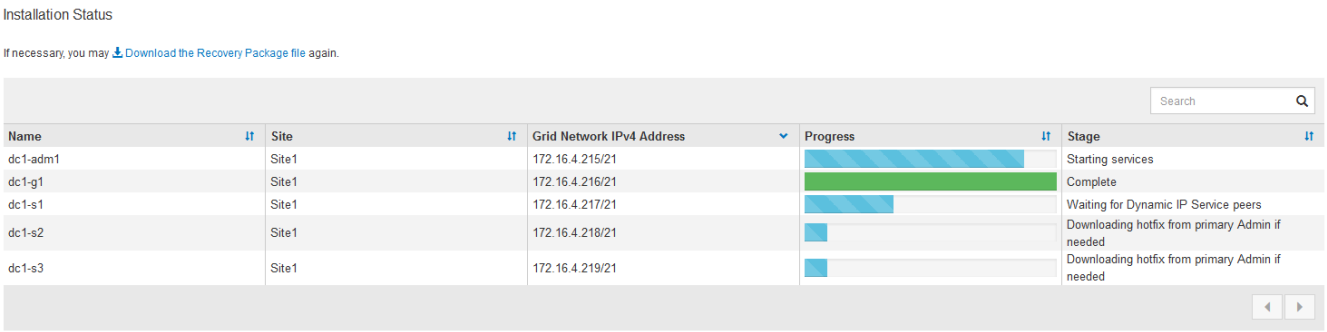
5. 验证您是否可以提取 ` .zip` 文件的内容，然后将其保存在两个安全，安全和独立的位置。

恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

6. 选中 * 我已成功下载并验证恢复软件包文件 * 复选框，然后单击 * 下一步 * 。



如果安装仍在进行中，则会显示状态页面。此页面指示每个网格节点的安装进度。



当所有网格节点达到完成阶段后，将显示网格管理器的登录页面。

7. 使用 "`root` " 用户和您在安装期间指定的密码登录到网格管理器。

安装后准则

完成网格节点部署和配置后，请按照以下准则更改 DHCP 地址和网络配置。

- 如果使用 DHCP 分配 IP 地址，请为所使用网络上的每个 IP 地址配置 DHCP 预留。

  您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。

  当节点的 IP 地址发生更改时，节点会重新启动，如果 DHCP 地址更改同时影响多个节点，则发生原因 可能会中断。

- 如果要更改网格节点的 IP 地址，子网掩码和默认网关，必须使用更改 IP 过程。请参见 配置 IP 地址。
- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改，您可能需要重新建立这些连接。

自动化安装（ **VMware** ）

您可以使用 VMware vSphere 自动部署网格节点。您还可以自动配置 StorageGRID 。

自动部署网格节点

使用 VMware vSphere 自动部署网格节点。

您需要的内容

- 您可以访问使用 Bash 3.2 或更高版本的 Linux/Unix 系统。
- 您已安装并正确配置 VMware OVF Tool 4.1 。
- 您知道使用 OVF 工具访问 VMware vSphere 所需的用户名和密码。
- 您知道 vSphere 中要部署 StorageGRID 虚拟机的位置的虚拟基础架构（ VI ） URL 。此 URL 通常为 vApp 或资源池。例如： `vi ： //vcenter.example.com/vi/sgws`

> 您可以使用 VMware `ovftool` 实用程序来确定此值（有关详细信息，请参见 `ovftool` 文档）。

> 如果要部署到 vApp ，虚拟机不会首次自动启动，您必须手动启动它们。

- 您已收集此配置文件所需的所有信息。请参见 收集有关部署环境的信息 以了解相关信息。
- 您可以从适用于 StorageGRID 的 VMware 安装归档文件访问以下文件：

文件名	Description
netapp-sg-version-sha.vmdk	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。 • 注： * 此文件必须与 ` .OVF` 和 ` .MF` 文件位于同一文件夹中。
vsphere-primary-admin.OVF vsphere-primary-admin.mf	用于部署主管理节点的开放式虚拟化格式模板文件（` .OVF` ）和清单文件（` .MF` ）。
vsphere-non-primary-admin.OVF vsphere-non-primary-admin.mf	用于部署非主管理节点的模板文件（` .OVF` ）和清单文件（` .MF` ）。
vsphere-archive.OVF vsphere-archive.mf	用于部署归档节点的模板文件（` .OVF` ）和清单文件（` .MF` ）。
vsphere-gateway.OVF vsphere-gateway.mf	用于部署网关节点的模板文件（` .OVF` ）和清单文件（` .MF` ）。

文件名	Description
vsphere-storage.OVF vsphere-storage.mf	用于部署基于虚拟机的存储节点的模板文件（` .OVF` ）和清单文件（` .MF` ）。
deploy-vsphere-ovftool.sh	Bash shell 脚本，用于自动部署虚拟网格节点。
deploy-vsphere-ovftool-sample.ini	与 `deept-vsphere-ovftool.sh` 脚本结合使用的示例配置文件。

定义部署的配置文件

您可以在配置文件中指定为 StorageGRID 部署虚拟网格节点所需的信息，此配置文件由 `dedeploy-vsphere-ovftool.sh` Bash 脚本使用。您可以修改配置文件示例，这样就不必从头创建文件了。

步骤

1. 为示例配置文件（ `deploy-vsphere-ovftool.sample.ini` ）创建一份副本。将此新文件另存为 `deploy-vsphere-ovftool.ini` ，并保存在与 `deept-vsphere-ovftool.sh` 相同的目录中。
2. 打开 `deploy-vsphere-ovftool.ini` 。
3. 输入部署 VMware 虚拟网格节点所需的所有信息。

   请参见 配置文件设置 以了解相关信息。

4. 输入并验证所有必要信息后，请保存并关闭此文件。

配置文件设置

`deploy-vsphere-ovftool.ini` 配置文件包含部署虚拟网格节点所需的设置。

配置文件首先列出全局参数，然后在节点名称定义的部分中列出节点专用参数。使用文件时：

- 全局参数 _ 应用于所有网格节点。
- _Node-specific parameters_override 全局参数。

全局参数

全局参数将应用于所有网格节点，除非它们被各个部分中的设置所覆盖。将应用于多个节点的参数置于全局参数部分中，然后根据需要在各个节点的部分中覆盖这些设置。

- * OVFTOOL_FUFFESESESESES* ： 您可以将 OVFTOOL_FUFFICESPORITES* 指定为全局设置，也可以将参数单独应用于特定节点。例如：

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  您可以使用 ` -powerOffTarget` 和 ` -overwrite` 选项关闭并更换现有虚拟机。

您应将节点部署到不同的数据存储库，并为每个节点指定 OVFTOOL_FUFFICESYUESYUESL ，而不是全局参数。

- * 源 * ： 单个网格节点的 StorageGRID 虚拟机模板（` .vmdk` ）文件以及 ` .OVF` 和 ` .MF` 文件的路径。默认为当前目录。

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- * 目标 * ： 要部署 StorageGRID 的位置的 VMware vSphere 虚拟基础架构（ VI ） URL 。例如：

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- * 网格网络配置 * ： 用于获取静态或 DHCP IP 地址的方法。默认值为 static 。如果所有或大多数节点使用相同的方法获取 IP 地址，则可以在此处指定该方法。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_CONFIG = DHCP
```

- * 网格网络目标 * ： 要用于网格网络的现有 VMware 网络的名称。如果所有或大多数节点使用相同的网络名称，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- * 网格网络掩码 * ： 网格网络的网络掩码。如果所有或大多数节点使用相同的网络掩码，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_MASK = 255.255.255.0
```

- * 网格网络网关 * ： 网格网络的网络网关。如果所有或大多数节点使用同一个网络网关，则可以在此处指定此网关。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- * 网格网络 MTU * ： 可选。网格网络上的最大传输单元（ MTU ）。如果指定，则此值必须介于 1280 和 9216 之间。例如：

```
GRID_NETWORK_MTU = 8192
```

如果省略，则使用 1400 。

如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。

网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

- * 管理网络配置 * ： 用于获取 IP 地址的方法，可以是禁用，静态或 DHCP 。默认值为 disabled 。如果所有或大多数节点使用相同的方法获取 IP 地址，则可以在此处指定该方法。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_CONFIG = STATIC
```

- * 管理网络目标 * ： 用于管理网络的现有 VMware 网络的名称。除非禁用管理网络，否则此设置为必填项。如果所有或大多数节点使用相同的网络名称，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- * 管理网络掩码 * ： 管理网络的网络掩码。如果使用的是静态 IP 寻址，则需要此设置。如果所有或大多数节点使用相同的网络掩码，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- * 管理网络网关 * ： 管理网络的网络网关。如果您使用的是静态 IP 寻址，并且在 admin_network_esl 设置中指定了外部子网，则需要此设置。（也就是说，如果 admin_network_esl 为空，则不需要执行此操作。）如果所有或大多数节点使用同一个网络网关，则可以在此处指定此网关。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- * 管理网络 _NETWORK_ESL* ： 管理网络的外部子网列表（路由），指定为 CIDR 路由目标的逗号分隔列表。如果所有或大多数节点使用相同的外部子网列表，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- * 管理网络 MTU * ： 可选。管理网络上的最大传输单元（ MTU ）。请勿指定 admin_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1400 。如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。如果所有或大多数节点对管理网络使用相同的 MTU ，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设

置。例如：

```
ADMIN_NETWORK_MTU = 8192
```

- * 客户端网络配置 * ：用于获取 IP 地址的方法，可以是禁用，静态或 DHCP 。默认值为 disabled 。如果所有或大多数节点使用相同的方法获取 IP 地址，则可以在此处指定该方法。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_CONFIG = STATIC
```

- * 客户端网络目标 * ：用于客户端网络的现有 VMware 网络的名称。除非禁用客户端网络，否则此设置为必填项。如果所有或大多数节点使用相同的网络名称，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- * 客户端网络掩码 * ：客户端网络的网络掩码。如果使用的是静态 IP 寻址，则需要此设置。如果所有或大多数节点使用相同的网络掩码，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- * 客户端网络网关 * ：客户端网络的网络网关。如果使用的是静态 IP 寻址，则需要此设置。如果所有或大多数节点使用同一个网络网关，则可以在此处指定此网关。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- * 客户端网络 MTU * ：可选。客户端网络上的最大传输单元（ MTU ）。请勿指定 client_network_config 是否为 DHCP 。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1400 。如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。如果所有或大多数节点对客户端网络使用相同的 MTU ，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_MTU = 8192
```

- * 端口重新映射 * ：重新映射节点用于内部网格节点通信或外部通信的任何端口。如果企业网络策略限制 StorageGRID 使用的一个或多个端口，则必须重新映射端口。有关 StorageGRID 使用的端口列表，请参见中的内部网格节点通信和外部通信 网络连接准则。

> 不要重新映射计划用于配置负载平衡器端点的端口。

如果仅设置 port_remap ，则您指定的映射将同时用于入站和出站通信。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。

使用的格式为：网格节点 / 新端口 _` 使用的 ` 网络类型 / 协议 / 默认端口，其中网络类型为网格，管理员或客户端，协议为 TCP 或 UDP 。

例如：

```
PORT_REMAP = client/tcp/18082/443
```

如果单独使用，则此示例设置会将网格节点的入站和出站通信从端口 18082 对称映射到端口 443 。如果与 port_remap_inbound 结合使用，则此示例设置会将出站通信从端口 18082 映射到端口 443 。

- * 端口重新映射入站 * ： 重新映射指定端口的入站通信。如果指定 port_remap_inbound ，但未指定 port_remap 的值，则端口的出站通信将保持不变。

不要重新映射计划用于配置负载平衡器端点的端口。

使用的格式为： ` node_/*protocol*/_*default port used by grid node*/*new port*` ，其中 network type 为 grid ，admin 或 client ， protocol 为 tcp 或 udp 。

例如：

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

此示例将接收发送到端口 443 以通过内部防火墙的流量，并将其定向到端口 18082 ，网格节点正在侦听 S3 请求。

节点专用参数

每个节点都位于配置文件中各自的部分中。每个节点都需要以下设置：

- 此部分标题定义了将在网格管理器中显示的节点名称。您可以通过为节点指定可选的 node_name 参数来覆盖该值。
- * 节点类型 * ： VM_Admin_Node ， VM_Storage_Node ， VM_Archive_Node 或 VM_API_Gateway_Node
- * 网格网络 IP ： 网格网络上节点的 IP 地址。
- * 管理网络 IP ： 管理网络上节点的 IP 地址。只有当节点已连接到管理网络且 admin_network_config 设置为 static 时才需要。
- * 客户端网络 IP* ： 客户端网络上节点的 IP 地址。只有当节点已连接到客户端网络且此节点的 client_network_config 设置为 static 时才需要此选项。
- * 管理 _IP* ： 网格网络上主管理节点的 IP 地址。使用指定的值作为主管理节点的 grid_network_IP 。如果省略此参数，则节点将尝试使用 mDNS 发现主管理节点 IP 。有关详细信息，请参见 网格节点如何发现主管理节点。

对于主管理节点， admin_ip 参数将被忽略。

- 未全局设置的任何参数。例如，如果某个节点已连接到管理网络，而您未全局指定 admin_network 参数，则必须为此节点指定这些参数。

主管理节点

主管理节点需要以下附加设置：

- * 节点类型 * ： VM_Admin_Node
- * 管理角色 * ：主

此示例条目适用于所有三个网络上的主管理节点：

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

以下附加设置对于主管理节点是可选的：

- * 磁盘 * ：默认情况下，会为管理节点另外分配两个 200 GB 的硬盘，以供审核和数据库使用。您可以使用 disk 参数增加这些设置。例如：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

对于管理节点，实例必须始终等于 2 。

存储节点

存储节点需要以下附加设置：

- * 节点类型 * ： VM_Storage_Node

  此示例条目适用于网格和管理网络上的存储节点，但不适用于客户端网络。此节点使用 admin_ip 设置指定网格网络上主管理节点的 IP 地址。

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

第二个示例条目适用于客户端网络上的存储节点，其中，客户的企业网络策略指出， S3 客户端应用程序仅允许使用端口 80 或 443 访问存储节点。示例配置文件使用 port_remap 使存储节点能够通过端口 443 发送和接收 S3 消息。

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

最后一个示例为从端口 22 到端口 3022 的 ssh 流量创建了对称重新映射，但明确设置了入站和出站流量的值。

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

以下附加设置对于存储节点是可选的：

- * 磁盘 * ：默认情况下，为存储节点分配三个 4 TB 磁盘，以供 RangeDB 使用。您可以使用 disk 参数增加这些设置。例如：

```
DISK = INSTANCES=16, CAPACITY=4096
```

归档节点

归档节点需要以下附加设置：

- * 节点类型 * ： VM_Archive_Node

此示例条目适用于网格和管理网络上的归档节点，但不适用于客户端网络。

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

网关节点

网关节点需要以下附加设置：

- * 节点类型 * ： VM_API_Gateway

此示例条目适用于所有三个网络上的示例网关节点。在此示例中，未在配置文件的全局部分中指定客户端网络参数，因此必须为节点指定这些参数：

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

非主管理节点

非主管理节点需要以下附加设置：

- * 节点类型 * ： VM_Admin_Node
- * 管理角色 * ： 非主要

此示例条目适用于不在客户端网络上的非主管理节点：

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

以下附加设置对于非主管理节点是可选的：

- * 磁盘 * ：默认情况下，会为管理节点另外分配两个 200 GB 的硬盘，以供审核和数据库使用。您可以使用 disk 参数增加这些设置。例如：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  对于管理节点，实例必须始终等于 2 。

运行 **Bash** 脚本

您可以使用 `dedeploy-vsphere-ovftool.sh` Bash 脚本和您修改的 deploy-vsphere-ovftool.ini 配置文件在 VMware vSphere 中自动部署 StorageGRID 网格节点。

您需要的内容

- 您已为您的环境创建 deploy-vsphere-ovftool.ini 配置文件。

您可以通过输入 help 命令（` -h/-help` ）来使用 Bash 脚本提供的帮助。例如：

```
./deploy-vsphere-ovftool.sh -h
```

或

```
./deploy-vsphere-ovftool.sh --help
```

步骤

1. 登录到用于运行 Bash 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如：

```
cd StorageGRID-Webscale-version/vsphere
```

3. 要部署所有网格节点，请使用适用于您环境的选项运行 Bash 脚本。

   例如：

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
vsphere-ovftool.ini
```

4. 如果某个网格节点由于出现错误而无法部署，请解决此错误并仅为该节点重新运行 Bash 脚本。

   例如：

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

当每个节点的状态为 "`passed" 时，部署完成。`

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

自动配置 StorageGRID

部署网格节点后，您可以自动配置 StorageGRID 系统。

您需要的内容

- 您可以从安装归档中了解以下文件的位置。

文件名	Description
configure-storagegrid.py	用于自动配置的 Python 脚本
configure-storaggrid.sample.json	用于脚本的示例配置文件

文件名	Description
configure-storaggrid.blank.json	用于脚本的空配置文件

- 您已创建 `configure-storaggrid.json` 配置文件。要创建此文件，您可以修改示例配置文件（`configure-storaggrid.sample.json`）或空白配置文件（`config-storaggrid.blank.json`）。

您可以使用 `configure-storaggrid.py` Python 脚本和 `configure-storaggrid.json` 配置文件来自动配置 StorageGRID 系统。

> 您也可以使用网格管理器或安装 API 配置系统。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为提取安装归档的目录。

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中， `platform` 是 debs ， rpms 或 vsphere 。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

结果

在配置过程中会生成一个恢复包 .zip 文件，该文件将下载到运行安装和配置过程的目录中。您必须备份恢复软件包文件，以便在一个或多个网格节点发生故障时恢复 StorageGRID 系统。例如，将其复制到安全的备份网络位置和安全的云存储位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

如果您指定应生成随机密码，则需要提取 Passwords.txt 文件并查找访问 StorageGRID 系统所需的密码。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

系统会在显示确认消息时安装并配置 StorageGRID 系统。

```
StorageGRID has been configured and installed.
```

相关信息

导航到网格管理器

安装 REST API 概述

安装 **REST API** 概述

StorageGRID 提供了用于执行安装任务的 StorageGRID 安装 API 。

API 使用 Swagger 开源 API 平台提供 API 文档。Swagger 允许开发人员和非开发人员在用户界面中与 API 进行交互，以说明 API 如何响应参数和选项。本文档假定您熟悉标准 Web 技术和 JSON （ JavaScript 对象表示法）数据格式。

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

每个 REST API 命令都包括 API 的 URL ， HTTP 操作，任何必需或可选的 URL 参数以及预期的 API 响应。

StorageGRID 安装 **API**

只有在首次配置 StorageGRID 系统时，以及在需要执行主管理节点恢复时， StorageGRID 安装 API 才可用。可以从网格管理器通过 HTTPS 访问安装 API 。

要访问 API 文档，请转到主管理节点上的安装网页，然后从菜单栏中选择 * 帮助 * > * API 文档 * 。

StorageGRID 安装 API 包括以下部分：

- **config** —与 API 的产品版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 网格 * - 网格级配置操作。您可以获取和更新网格设置，包括网格详细信息，网格网络子网，网格密码以及 NTP 和 DNS 服务器 IP 地址。
- "**Nodes** - 节点级别的配置操作 " 。您可以检索网格节点列表，删除网格节点，配置网格节点，查看网格节点以及重置网格节点的配置。
- * 配置 * —配置操作。您可以启动配置操作并查看配置操作的状态。
- * 恢复 * —主管理节点恢复操作。您可以重置信息，上传恢复软件包，启动恢复以及查看恢复操作的状态。

- **recovery-package** —下载恢复软件包的操作。
- * 模式 * —用于高级部署的 API 模式
- * 站点 * —站点级配置操作。您可以创建，查看，删除和修改站点。

下一步行动

完成安装后，您必须执行一系列集成和配置步骤。某些步骤是必需的；其他步骤是可选的。

所需任务

- 配置 VMware vSphere 虚拟机管理程序以自动重新启动。

  您必须将虚拟机管理程序配置为在服务器重新启动时重新启动虚拟机。如果不自动重新启动，虚拟机和网格节点将在服务器重新启动后保持关闭状态。有关详细信息，请参见 VMware vSphere 虚拟机管理程序文档。

- 为要用于在 StorageGRID 系统上存储对象的每个客户端协议（ Swift 或 S3 ）创建一个租户帐户。
- 通过配置组和用户帐户来控制系统访问。您也可以配置联合身份源（例如 Active Directory 或 OpenLDAP ），以便导入管理组和用户。或者，您也可以创建本地组和用户。
- 集成并测试用于将对象上传到 StorageGRID 系统的 S3 或 Swift API 客户端应用程序。
- 准备好后，配置要用于保护对象数据的信息生命周期管理（ ILM ）规则和 ILM 策略。

  安装 StorageGRID 时，默认 ILM 策略 " 基线 2 副本策略 " 处于活动状态。此策略包括常用 ILM 规则（创建 2 个副本），如果未激活任何其他策略，则此策略适用。

- 如果您的安装包括设备存储节点，请使用 SANtricity 软件完成以下任务：
  - 连接到每个 StorageGRID 设备。
  - 验证是否收到 AutoSupport 数据。
- 如果 StorageGRID 系统包含任何归档节点，请配置归档节点与目标外部归档存储系统的连接。

  如果任何归档节点将使用 Tivoli Storage Manager 作为外部归档存储系统，则还必须配置 Tivoli Storage Manager 。

- 查看并遵循 StorageGRID 系统强化准则，以消除安全风险。
- 为系统警报配置电子邮件通知。

可选任务

- 如果要从（原有）警报系统接收通知，请配置警报的邮件列表和电子邮件通知。
- 如果自规划部署并生成恢复包以来网格节点 IP 地址发生了更改，请更新这些地址。请参见恢复和维护说明中有关更改 IP 地址的信息。
- 根据需要配置存储加密。
- 如果需要，配置存储压缩以减小存储对象的大小。
- 配置审核客户端访问。您可以通过 NFS 或 CIFS 文件共享配置对系统的访问，以供审核使用。请参见有关管

理 StorageGRID 的说明。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

相关信息

管理 StorageGRID

使用 S3

使用 Swift

使用 ILM 管理对象

监控和故障排除

恢复和维护

SG100 和 SG1000 服务设备

SG5600 存储设备

SG5700 存储设备

SG6000 存储设备

发行说明

系统强化

查看审核日志

升级软件

对安装问题进行故障排除

如果在安装 StorageGRID 系统时出现任何问题，您可以访问安装日志文件。

以下是主要安装日志文件，技术支持可能需要这些文件来解决问题。

- ` /var/local/log/install.log` （可在所有网格节点上找到）
- ` /var/local/log/gdu-server.log` （位于主管理节点上）

要了解如何访问日志文件，请参见 StorageGRID 监控和故障排除说明。有关排除设备安装问题的帮助，请参见适用于您的设备的安装和维护说明。如果您需要其他帮助，请联系技术支持。

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

"NetApp 支持"

虚拟机资源预留需要调整

OVF 文件包含一个资源预留，用于确保每个网格节点都有足够的 RAM 和 CPU 来高效运行。如果通过在 VMware 上部署这些 OVF 文件来创建虚拟机，但预定义的资源数量不可用，则虚拟机将无法启动。

关于此任务

如果您确定 VM 主机具有足够的资源来支持每个网格节点，请手动调整为每个虚拟机分配的资源，然后尝试启动虚拟机。

步骤

1. 在 VMware vSphere 虚拟机管理程序客户端树中，选择未启动的虚拟机。
2. 右键 - 单击虚拟机，然后选择 * 编辑设置 * 。
3. 从虚拟机属性窗口中，选择 * 资源 * 选项卡。
4. 调整分配给虚拟机的资源：
   a. 选择 * CPU * ，然后使用预留滑块调整为此虚拟机预留的 MHz 。
   b. 选择 * 内存 * ，然后使用预留滑块调整为此虚拟机预留的 MB 。
5. 单击 * 确定 * 。
6. 根据需要对同一 VM 主机上托管的其他虚拟机重复上述步骤。

执行系统管理

管理 StorageGRID

管理 StorageGRID： 概述

按照以下说明配置和管理 StorageGRID 系统。

关于这些说明

以下说明介绍如何使用网格管理器设置组和用户，创建租户帐户以允许 S3 和 Swift 客户端应用程序存储和检索对象，配置和管理 StorageGRID 网络，配置 AutoSupport ，管理节点设置等。

本说明适用于在安装 StorageGRID 系统后配置，管理和支持该系统的技术人员。

开始之前

- 您已大致了解 StorageGRID 系统。
- 您对 Linux 命令 Shell ，网络连接以及服务器硬件设置和配置有相当详细的了解。

开始使用 StorageGRID

Web 浏览器要求

您必须使用受支持的 Web 浏览器。

Web 浏览器	支持的最低版本
Google Chrome	96
Microsoft Edge	96
Mozilla Firefox	94.

您应将浏览器窗口设置为建议的宽度。

浏览器宽度	像素
最小值	1024
最佳	1280

登录到网格管理器

您可以通过在支持的 Web 浏览器的地址栏中输入管理节点的完全限定域名（ FQDN ）或

IP 地址来访问网格管理器登录页面。

您需要的内容

- 您已拥有登录凭据。
- 您已获得网格管理器的 URL 。
- 您正在使用 支持的 Web 浏览器。
- 已在 Web 浏览器中启用 Cookie 。
- 您具有特定的访问权限。

关于此任务

每个 StorageGRID 系统都包括一个主管理节点和任意数量的非主管理节点。您可以登录到任何管理节点上的网格管理器来管理 StorageGRID 系统。但是，管理节点不完全相同：

- 在一个管理节点上进行的警报确认（原有系统）不会复制到其他管理节点。因此，为警报显示的信息在每个管理节点上可能不相同。
- 某些维护过程只能从主管理节点执行。

如果管理节点包含在高可用性（ HA ）组中，则可以使用 HA 组的虚拟 IP 地址或映射到虚拟 IP 地址的完全限定域名进行连接。应选择主管理节点作为组的主接口，以便在访问网格管理器时，您可以在主管理节点上访问它，除非主管理节点不可用。

步骤

1. 启动受支持的 Web 浏览器。
2. 在浏览器的地址栏中，输入网格管理器的 URL ：

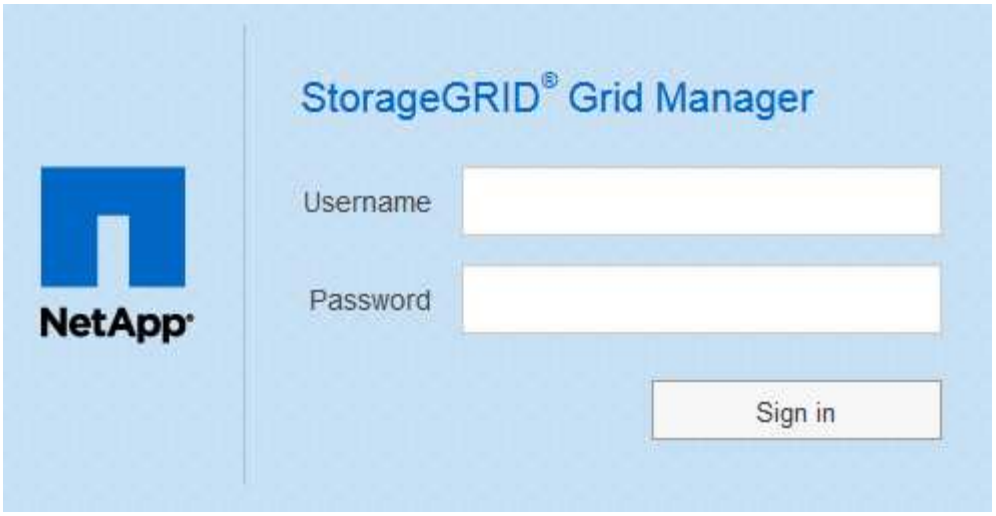
   `https://FQDN_or_Admin_Node_IP/`

   其中， ` fqdn_or_Admin_Node_IP_` 是完全限定域名或管理节点的 IP 地址，或者是管理节点 HA 组的虚拟 IP 地址。

   如果您必须在 HTTPS 标准端口（ 443 ）以外的端口上访问网格管理器，请输入以下内容，其中 ` fqdn_or_Admin_Node_IP_` 是完全限定域名或 IP 地址， port 是端口号：

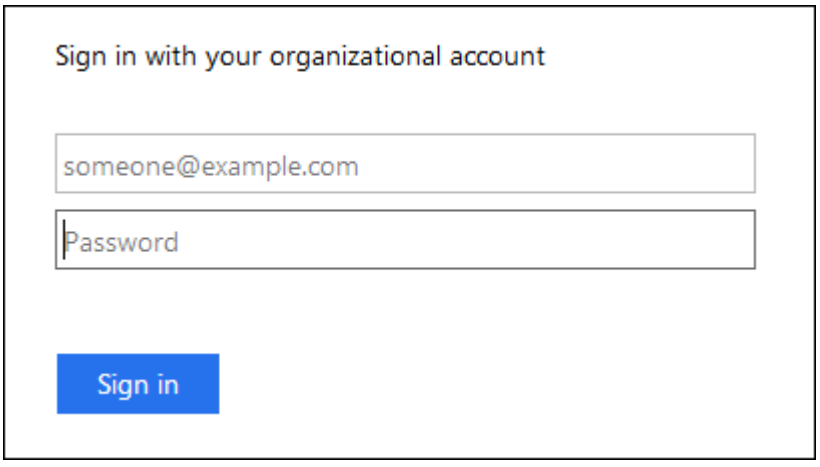
   `https://FQDN_or_Admin_Node_IP:port/`

3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书（请参见 关于安全证书）。
4. 登录到网格管理器：
   - 如果 StorageGRID 系统未使用单点登录（ SSO ）：
     i. 输入网格管理器的用户名和密码。
     ii. 选择 * 登录 * 。



- 如果为 StorageGRID 系统启用了 SSO ，并且这是您首次在此浏览器上访问此 URL ：
  i. 选择 * 登录 * 。您可以将 "Account ID" 字段留空。

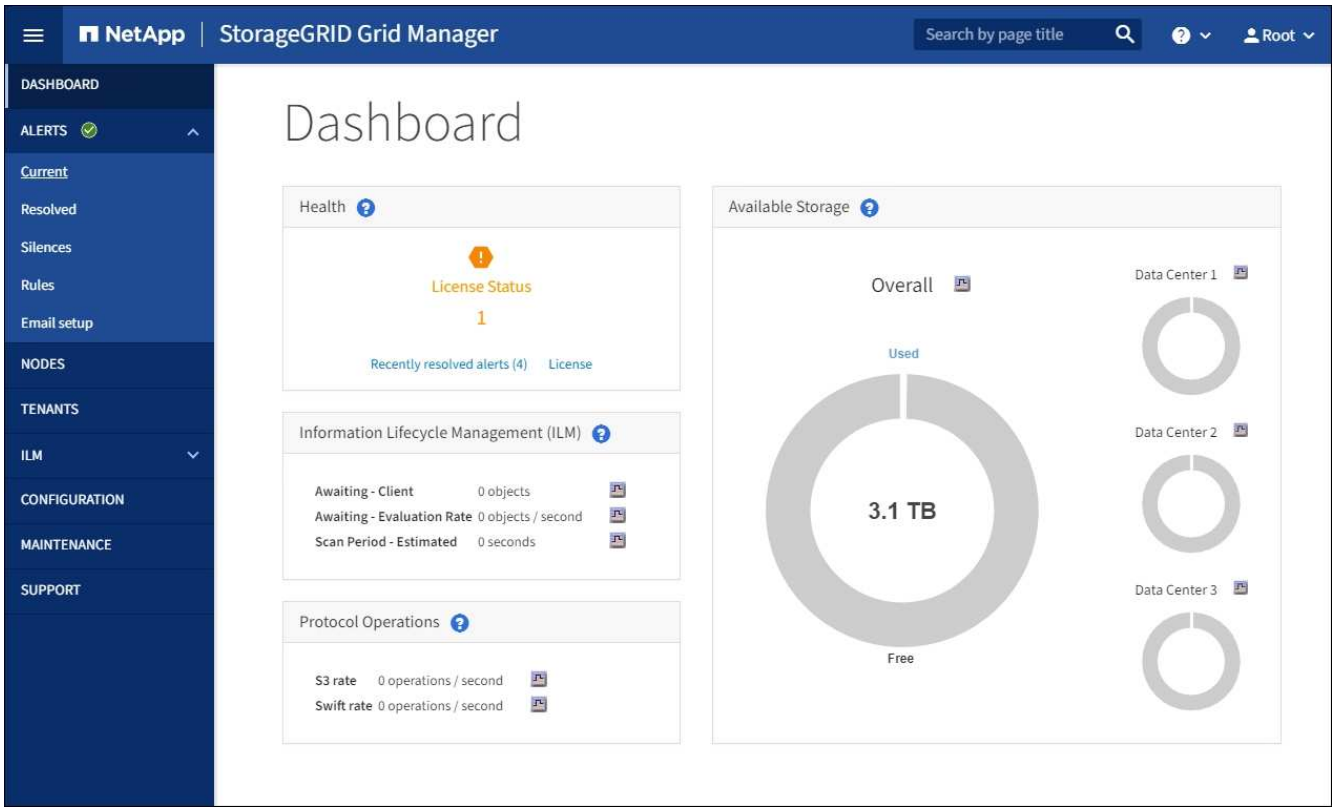
  ii. 在组织的 SSO 登录页面上输入标准 SSO 凭据。例如：



- 如果为 StorageGRID 系统启用了 SSO ，并且您先前已访问网格管理器或租户帐户：
  i. 执行以下任一操作：

- 输入 * 。 0* （网格管理器的帐户 ID ），然后选择 * 登录 * 。
- 如果近期帐户列表中显示了 * 网格管理器 * ，请选择 * 登录 * 。

ii. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。登录后，将显示网格管理器的主页，其中包括信息板。要了解所提供的信息，请参见 查看信息板。



5. 如果要登录到另一个管理节点：

选项	步骤
未启用 SSO	a. 在浏览器的地址栏中，输入另一个管理节点的完全限定域名或 IP 地址。根据需要包括端口号。 b. 输入网格管理器的用户名和密码。 c. 选择 * 登录 * 。
已启用 SSO	在浏览器的地址栏中，输入另一个管理节点的完全限定域名或 IP 地址。 如果您已登录到一个管理节点，则无需重新登录即可访问其他管理节点。但是，如果您的 SSO 会话到期，系统会再次提示您输入凭据。 • 注： * 受限网格管理器端口上不提供 SSO 。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

相关信息

- 通过防火墙控制访问
- 配置单点登录
- 管理管理组
- 管理高可用性组
- 使用租户帐户
- 监控和故障排除

注销 **Grid Manager**

使用完网格管理器后，您必须注销以确保未经授权的用户无法访问 StorageGRID 系统。根据浏览器 Cookie 设置，关闭浏览器可能无法将您从系统中注销。

步骤

1. 在右上角选择您的用户名。

2. 选择 * 注销 * 。

选项	Description
SSO 未使用	您已从管理节点注销。 此时将显示网格管理器登录页面。 • 注意： * 如果您已登录到多个管理节点，则必须从每个节点注销。
已启用 SSO	您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。* 网格管理器 * 在 * 近期帐户 * 下拉列表中列为默认值， * 帐户 ID* 字段显示 0 。 • 注意： * 如果启用了 SSO ，并且您还登录到租户管理器，则还必须注销租户帐户才能注销 SSO 。

相关信息

- 配置单点登录
- 使用租户帐户

更改密码

如果您是网格管理器的本地用户，则可以更改自己的密码。

您需要的内容

您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

如果您以联合用户身份登录到 StorageGRID 或启用了单点登录（ Single Sign-On ， SSO ），则无法在网格管理器中更改密码。而是必须更改外部身份源中的密码，例如 Active Directory 或 OpenLDAP 。

步骤

1. 从网格管理器标题中，选择 * 。您的姓名 _* > * 更改密码 * 。
2. 输入当前密码。
3. 键入新密码。

   您的密码必须至少包含 8 个字符，并且不能超过 32 个字符。密码区分大小写。

4. 重新输入新密码。
5. 选择 * 保存 * 。

更改浏览器会话超时

如果 Grid Manager 和租户管理器用户处于非活动状态的时间超过一段时间，您可以控制他们是否已注销。

您需要的内容

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

关于此任务

GUI 非活动超时默认为 900 秒（ 15 分钟）。如果用户的浏览器会话在此时间内未处于活动状态，则此会话将超时。

您可以根据需要通过设置 GUI 非活动超时显示选项来增加或减少超时时间。

如果启用了单点登录（ SSO ），并且用户的浏览器会话超时，系统的行为就像用户手动选择了 * 注销 * 一样。用户必须重新输入其 SSO 凭据才能再次访问 StorageGRID 。请参见 配置单点登录。

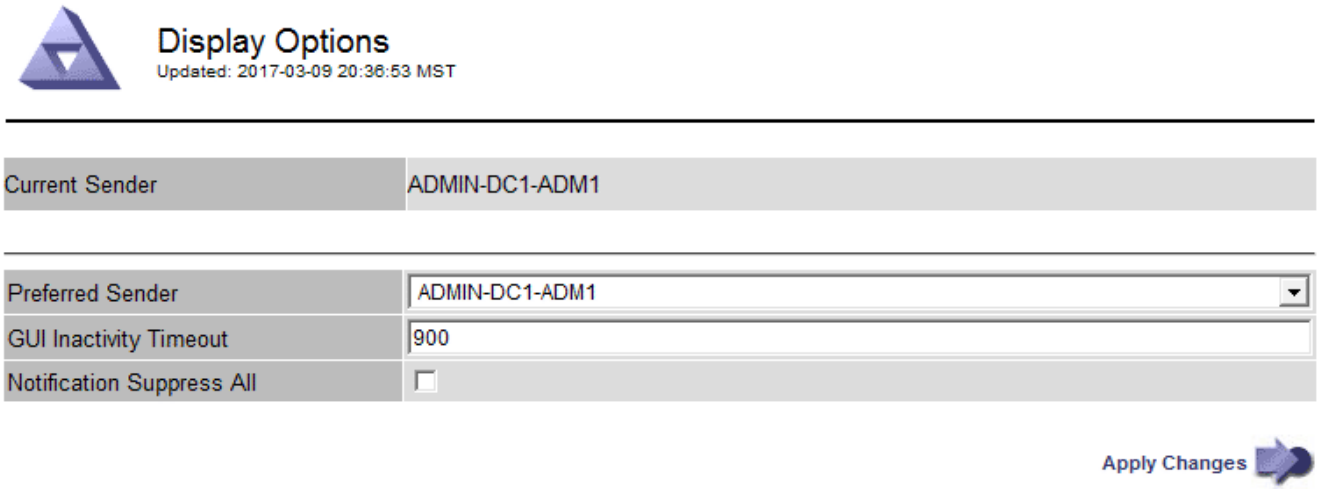
用户会话超时也可通过以下方式控制：

- 一个单独的不可配置 StorageGRID 计时器，其中包括用于系统安全保护的计时器。默认情况下，每个用户的身份验证令牌在用户登录后 16 小时到期。用户的身份验证过期后，即使尚未达到 GUI 非活动超时值，该用户也会自动注销。要续订令牌，用户必须重新登录。
- 身份提供程序的超时设置（假设已为 StorageGRID 启用 SSO ）。

步骤

1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。
2. 对于 * 图形用户界面非活动超时 * ，请输入 60 秒或更长时间的超时期限。

   如果不想使用此功能，请将此字段设置为 0 。用户在登录后 16 小时，身份验证令牌过期时将注销。



3. 选择 * 应用更改 * 。

   新设置不会影响当前已登录的用户。用户必须重新登录或刷新浏览器，新的超时设置才能生效。

查看 **StorageGRID** 许可证信息

您可以根据需要查看 StorageGRID 系统的许可证信息，例如网格的最大存储容量。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

如果问题描述 具有此 StorageGRID 系统的软件许可证，则信息板上的 " 运行状况 " 面板将包含一个 " 许可证状态 " 图标和一个 * 许可证 * 链接。此数字表示存在多少个与许可证相关的问题。

步骤

要查看许可证，请执行以下操作之一：

- 从信息板上的 " 运行状况 " 面板中，选择许可证状态图标或 * 许可证 * 链接。只有当具有许可证的问题描述时，才会显示此链接。
- 选择 * 维护 * > * 系统 * > * 许可证 * 。

此时将显示 License 页面，其中提供了有关当前许可证的以下只读信息：

- StorageGRID 系统 ID ，此 ID 是此 StorageGRID 安装的唯一标识号
- 许可证序列号
- 网格的许可存储容量
- 软件许可证结束日期
- 支持服务合同结束日期
- 许可证文本文件的内容

对于在 StorageGRID 10.3 之前发布的许可证，许可的存储容量不会包含在许可证文件中，并且会显示 " 请参见许可协议 " 消息而不是值。

更新 **StorageGRID** 许可证信息

您必须在许可证条款发生更改时随时更新 StorageGRID 系统的许可证信息。例如，如果为网格购买了额外的存储容量，则必须更新许可证信息。

您需要的内容

- 您有一个新的许可证文件可应用于 StorageGRID 系统。
- 您具有特定的访问权限。

- 您具有配置密码短语。

步骤

1. 选择 * 维护 * > * 系统 * > * 许可证 * 。
2. 在 * 配置密码短语 * 文本框中输入 StorageGRID 系统的配置密码短语。
3. 选择 * 浏览 * 。
4. 在打开对话框中，找到并选择新的许可证文件（` .txt` ），然后选择 * 打开 * 。

   此时将验证并显示新许可证文件。

5. 选择 * 保存 * 。

使用 **API**

使用网格管理 **API**

您可以使用网格管理 REST API 执行系统管理任务，而不是使用网格管理器用户界面。例如，您可能希望使用 API 来自动执行操作或更快地创建多个实体，例如用户。

顶级资源

网格管理 API 可提供以下顶级资源：

- ` / 网格` ： 仅限网格管理器用户访问，且访问权限取决于配置的组权限。
- ` /Org` ： 仅限属于租户帐户的本地或联合 LDAP 组的用户访问。有关详细信息，请参见 使用租户帐户。
- ` / 私有` ： 仅限 Grid Manager 用户访问，并且访问权限取决于配置的组权限。专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

问题描述 **API** 请求

网格管理 API 使用 Swagger 开源 API 平台。Swagger 提供了一个直观的用户界面，使开发人员和非开发人员能够使用 API 在 StorageGRID 中执行实时操作。

Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。

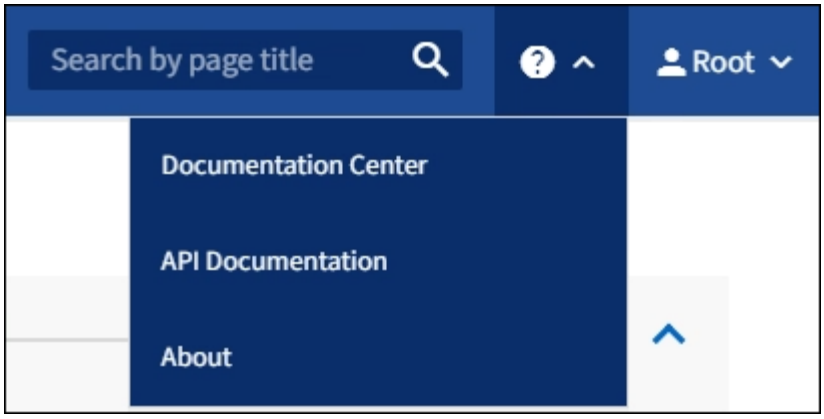
您需要的内容

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

> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

步骤

1. 从网格管理器标题中，选择帮助图标并选择 * API Documentation" 。



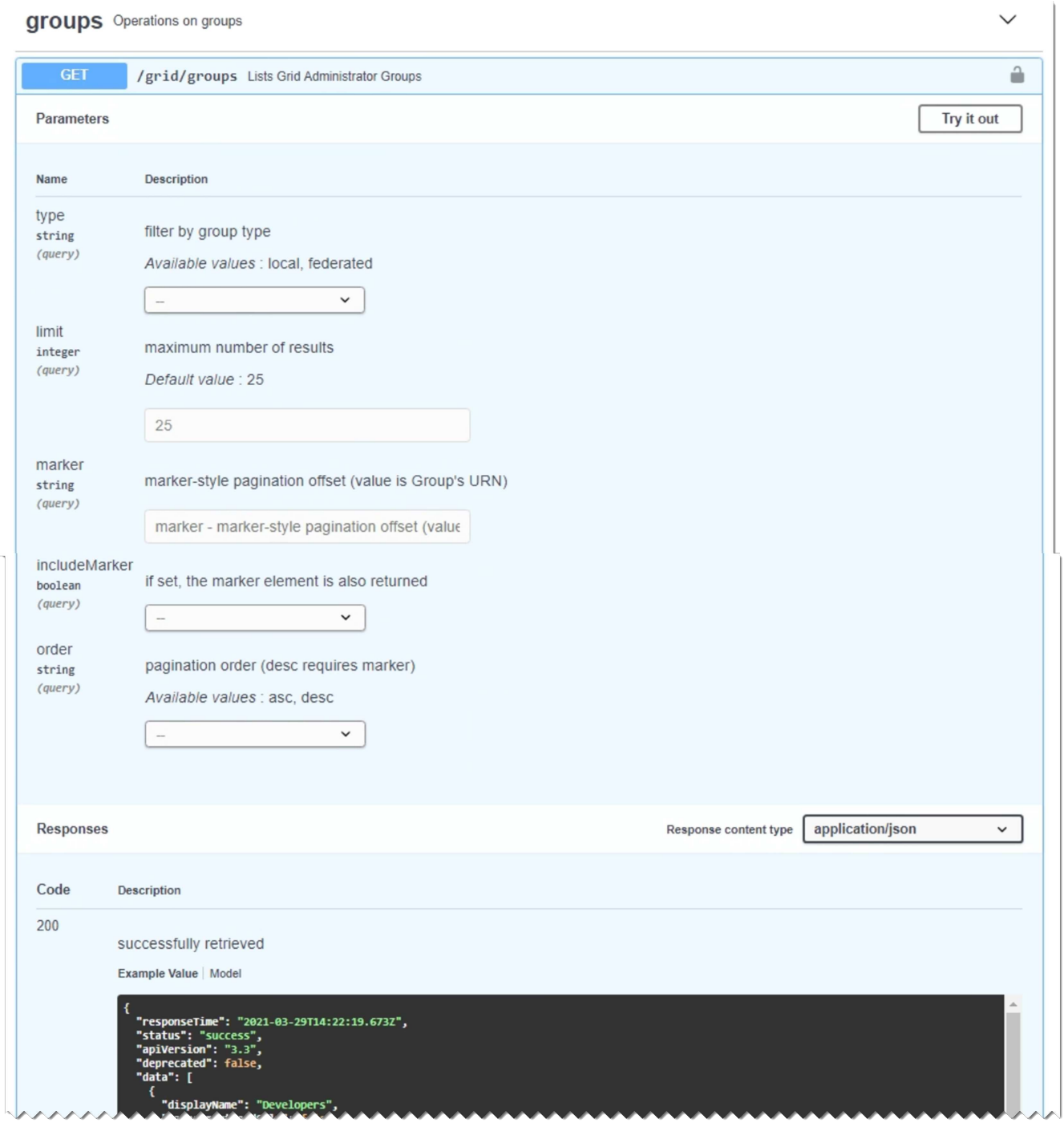
2. 要使用专用 API 执行操作，请在 StorageGRID 管理 API 页面上选择 * 转至专用 API 文档 * 。

   专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

3. 选择所需的操作。

   展开 API 操作时，您可以看到可用的 HTTP 操作，例如 GET ， PUT ， UPDATE 和 DELETE 。

4. 选择 HTTP 操作可查看请求详细信息，包括端点 URL ，任何必需或可选参数的列表，请求正文示例（如果需要）以及可能的响应。



5. 确定此请求是否需要其他参数，例如组或用户 ID 。然后，获取这些值。您可能需要先对其他 API 请求进行问题描述 处理，以获取所需的信息。
6. 确定是否需要修改示例请求正文。如果是，您可以选择 * 型号 * 来了解每个字段的要求。
7. 选择 * 试用 * 。
8. 提供所需的任何参数，或根据需要修改请求正文。
9. 选择 * 执行 * 。
10. 查看响应代码以确定请求是否成功。

网格管理 API 将可用操作组织到以下部分中。

此列表仅包含公有 API 中可用的操作。

- * 帐户 * —用于管理存储租户帐户的操作，包括创建新帐户和检索给定帐户的存储使用情况。
- * 警报 * —用于列出当前警报（旧系统）并返回有关网格运行状况的信息的操作，包括当前警报和节点连接状态摘要。
- **alert-histori** —对已解决警报执行的操作。
- * 警报接收器 * —对警报通知接收器（电子邮件）的操作。
- **alert-rules** —对警报规则执行的操作。
- **alert-silences** —对警报静音执行的操作。
- * 警报 * - 对警报执行的操作。
- * 审核 * —用于列出和更新审核配置的操作。
- * 身份验证 * —执行用户会话身份验证的操作。

  网格管理 API 支持不可承载令牌身份验证方案。要登录，请在身份验证请求的 JSON 正文中提供用户名和密码（即 `post /apI/v3/authorize`）。如果用户已成功通过身份验证，则会返回一个安全令牌。此令牌必须在后续 API 请求的标题中提供（ "Authorization： bearer *token*" ）。

  如果为 StorageGRID 系统启用了单点登录，则必须执行不同的步骤进行身份验证。请参见 "` 在启用单点登录后对 API 进行身份验证。` "

  有关提高身份验证安全性的信息，请参见 "`防止跨站点请求伪造` " 。

- * 客户端证书 * —用于配置客户端证书以便使用外部监控工具安全访问 StorageGRID 的操作。
- **config** —与网格管理 API 的产品版本和版本相关的操作。您可以列出该版本支持的网格管理 API 的产品版本和主要版本，并且可以禁用已弃用的 API 版本。
- "*deactived-features * - 用于查看可能已停用的功能的操作 " 。
- **DNS-servers** —用于列出和更改已配置外部 DNS 服务器的操作。
- * 端点域名 * —用于列出和更改端点域名的操作。
- * 擦除编码 * —擦除编码配置文件的操作。
- * 扩展 * —扩展操作（过程级）。
- * 扩展节点 * —扩展操作（节点级别）。
- * 扩展站点 * —扩展操作（站点级）。
- * 网格网络 * —用于列出和更改网格网络列表的操作。
- * 网格密码 * —网格密码管理操作。
- * 组 * —用于管理本地网格管理员组以及从外部 LDAP 服务器检索联合网格管理员组的操作。
- **identity-source** —用于配置外部身份源以及手动同步联合组和用户信息的操作。

- * ILM * —信息生命周期管理（ ILM ）操作。
- * 许可证 * —用于检索和更新 StorageGRID 许可证的操作。
- * 日志 * —用于收集和下载日志文件的操作。
- * 指标 * —对 StorageGRID 指标的操作，包括单个时间点的即时指标查询和一段时间内的范围指标查询。网格管理 API 使用 Prometheus 系统监控工具作为后端数据源。有关构建 Prometheus 查询的信息，请参见 Prometheus 网站。

> 名称中包含 *private* 的指标仅供内部使用。这些指标可能会在 StorageGRID 版本之间发生更改，恕不另行通知。

- "node-details* "- 对节点详细信息的操作。
- "node-health* " —对节点运行状况执行的操作。
- * ntp-servers* —用于列出或更新外部网络时间协议（ NTP ）服务器的操作。
- * 对象 * - 对对象和对象元数据执行的操作。
- * 恢复 * —恢复操作步骤 的操作。
- **recovery-package** —下载恢复软件包的操作。
- * 区域 * - 用于查看和创建区域的操作。
- * s3-object-lock* —对全局 S3 对象锁定设置执行的操作。
- * 服务器证书 * —用于查看和更新 Grid Manager 服务器证书的操作。
- "* SNMP* - 对当前 SNMP 配置执行的操作 " 。
- *traffic 类 * —流量分类策略的操作。
- * 不可信客户端网络 * —对不可信客户端网络配置执行的操作。
- * 用户 * —用于查看和管理 Grid Manager 用户的操作。

网格管理 **API** 版本控制

网格管理 API 使用版本控制来支持无中断升级。

例如，此请求 URL 指定 API 版本 3 。

```
https://hostname_or_ip_address/api/v3/authorize
```

如果对旧版本进行了 * 不兼容 _* 的更改，则租户管理 API 的主要版本将发生递增。如果对 * 与旧版本兼容 _* 进行了更改，则租户管理 API 的次要版本将发生递增。兼容的更改包括添加新端点或新属性。以下示例说明了如何根据所做更改的类型对 API 版本进行递增。

API 的更改类型	旧版本	新版本
与旧版本兼容	2.1	2.2
与旧版本不兼容	2.1	3.0

首次安装 StorageGRID 软件时，仅会启用最新版本的网格管理 API 。但是，在升级到 StorageGRID 的新功能

版本时，您仍可以访问至少一个 StorageGRID 功能版本的旧版 API 。

> 您可以使用网格管理 API 配置受支持的版本。有关详细信息，请参见 Swagger API 文档中的 "`config` " 一节。在更新所有网格管理 API 客户端以使用较新版本后，您应停用对较旧版本的支持。

已过时的请求将通过以下方式标记为已弃用：

- 响应标头为 "depression: true"
- JSON 响应正文包含 "depressioned" ： true
- NMS.log 中会添加一个已弃用的警告。例如：

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

确定当前版本支持哪些 **API** 版本

请使用以下 API 请求返回受支持的 API 主要版本列表：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

指定请求的 **API** 版本

您可以使用路径参数（` API/v3` ）或标头（`API-Version ： 3`）指定 API 版本。如果同时提供这两个值，则标头值将覆盖路径值。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

防止跨站点请求伪造（ **CSRF** ）

您可以通过使用 CSRF 令牌增强使用 Cookie 的身份验证，帮助防止 StorageGRID 受到跨站点请求伪造（ CSRF ）攻击。网格管理器和租户管理器会自动启用此安全功能；其他 API 客户端可以选择在登录时是否启用此功能。

如果攻击者可能触发对其他站点的请求（例如使用 HTTP 表单发布），则可以对使用已登录用户的 cookie 发出的某些请求进行发生原因 处理。

StorageGRID 可通过使用 CSRF 令牌帮助防止 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标题或特定后处理正文参数的内容匹配。

要启用此功能，请在身份验证期间将 `csrfToken` 参数设置为 `true` 。默认值为 `false` 。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果为 true ，则使用随机值为 `GridCsrfToken` cookie 设置网格管理器登录，并使用随机值为 `AccountCsrfToken` cookie 设置为登录租户管理器。

如果存在 Cookie ，则可以修改系统状态的所有请求（ POST ， PUT ， patch ， delete ）都必须包括以下项之一：

- `X-CSRF-Token` 标头，标头的值设置为 CSRF 令牌 cookie 的值。
- 对于接受表单编码正文的端点： a `csrfToken` form-enc编码 请求正文参数。

有关其他示例和详细信息，请参见联机 API 文档。

> 设置了 CSRF 令牌 cookie 的请求还会对任何希望 JSON 请求正文作为额外保护来抵御 CSRF 攻击的请求强制使用 ` "Content-Type： application/json"` 标头。

如果启用了单点登录，请使用 **API**

如果启用了单点登录，请使用 **API** （ **Active Directory** ）

如果您有 已配置并启用单点登录（ SSO ） 如果您使用 Active Directory 作为 SSO 提供程序，则必须对一系列 API 请求进行问题描述 处理，以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了单点登录，请登录到 **API**

如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用。

您需要的内容

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- `storagegrid-ssoauth.py` Python 脚本，该脚本位于 StorageGRID 安装文件目录中（对于 Red Hat Enterprise Linux 或 CentOS ，为` ./rpms` ；对于 Ubuntu 或 Debian ，为 ` ./de-s` ；对于 VMware ，为 ` ./vSphere` ）。
- cURL 请求的示例工作流。

  如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误： `A valid SubjectConfirmation was not found on this response` 。

  示例 cURL 工作流不会保护密码不会被其他用户看到。

如果您使用的是 URL 编码问题描述 ，则可能会看到错误： 不支持 `SAML` 版本 。

步骤

1. 选择以下方法之一以获取身份验证令牌：
   - 使用 `storagegrid-ssoauth.py` Python 脚本。转至步骤 2 。
   - 使用 curl 请求。转至步骤 3 。
2. 如果要使用 `storagegrid-ssoauth.py` 脚本，请将此脚本传递给 Python 解释器并运行此脚本。

   出现提示时，输入以下参数的值：
   - SSO 方法。输入 ADFS 或 ADFS 。
   - SSO 用户名
   - 安装 StorageGRID 的域
   - StorageGRID 的地址
   - 要访问租户管理 API 的租户帐户 ID 。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。
3. 如果要使用 curl 请求，请使用以下操作步骤 。
   a. 声明登录所需的变量。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

要访问网格管理 API ，请使用 0 作为 `TENANTACCOBTID` 。

b. 要接收签名的身份验证 URL ，问题描述 请将 POST 请求发送到 ` /apl/v3/authorize -SAML` ，然后从响应中删除额外的 JSON 编码。

此示例显示了 `TENANTACCOBTID` 的已签名身份验证 URL 的 POST 请求。结果将传递到 `python -m json.tool` 以删除 JSON 编码。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 从响应中保存 `SAMLRequest` ，以便在后续命令中使用。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. 从 AD FS 获取包含客户端请求 ID 的完整 URL 。

一种方法是使用上一响应中的 URL 请求登录表单。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

此响应包括客户端请求 ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 保存响应中的客户端请求 ID 。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 将您的凭据发送到上一响应中的表单操作。

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS 返回 302 重定向，并在标题中显示追加信息 。

> 如果为 SSO 系统启用了多因素身份验证（ MFA ），则此表单发布还将包含第二个密码或其他凭据。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 从响应中保存 `MSISAuth` cookie 。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 使用身份验证 POST 中的 Cookie 将 GET 请求发送到指定位置。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

响应标头将包含 AD FS 会话信息，以便日后注销时使用，而响应正文将 SAMLResponse 隐藏在一个格式的字段中。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 从隐藏字段中保存 `SAMLResponse`：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用已保存的 `SAMLResponse` 发出 StorageGRID `/API/SAML` 响应 请求以生成 StorageGRID 身份验

证令牌。

对于 `RelayState` ，请使用租户帐户 ID ，或者如果要登录到网格管理 API ，请使用 0 。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

响应包括身份验证令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 将此身份验证令牌保存在响应中为 `MYTOKEN` 。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

现在，您可以对其他请求使用 `MYTOKEN` ，类似于未使用 SSO 时使用 API 的方式。

如果启用了单点登录，请注销 API

如果已启用单点登录（ Single Sign-On ， SSO ），则必须对一系列 API 请求进行问题描述 ，才能注销网格管理 API 或租户管理 API 。如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要，只需从组织的单个注销页面注销即可注销 StorageGRID API 。或者，您也可以从 StorageGRID 触发单点注销（ SLO ），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求，请将 `cookie "sso=true"` 传递到 SLO API ：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回注销 URL：

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 保存注销 URL 。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。如果未提供 `cookie "sso=true"` ，则用户将从 StorageGRID 中注销，而不会影响 SSO 状态。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

`204 No Content` 响应表示用户现在已注销。

```
HTTP/1.1 204 No Content
```

如果启用了单点登录，请使用 **API** （ **Azure** ）

如果您有 已配置并启用单点登录（ SSO ） 使用 Azure 作为 SSO 提供程序时，您可以使用两个示例脚本来获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了 **Azure** 单点登录，请登录到 **API**

如果您使用 Azure 作为 SSO 身份提供程序，则以下说明适用

您需要的内容

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 电子邮件地址和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例脚本：

- `storagegrid-ssoauth-azure.py` Python 脚本
- `storagegrid-ssoauth-azure.js` Node.js 脚本

这两个脚本都位于 StorageGRID 安装文件目录中（对于 Red Hat Enterprise Linux 或 CentOS ，为` ./rpms` ；对于 Ubuntu 或 Debian ，为 ` ./debs` ；对于 VMware ，为 ` ./vSphere` ）。

要编写您自己与 Azure 的 API 集成，请参见 `storagegrid-ssoauth-azure.py` 脚本。Python 脚本会直接向 StorageGRID 发出两个请求（首先获取 SAMLRequest ，然后再获取授权令牌），同时还会调用 Node.js 脚本与 Azure 交互以执行 SSO 操作。

可以使用一系列 API 请求执行 SSO 操作，但这样做并不简单。puppeteer Node.js 模块用于擦除 Azure SSO 接口。

如果您使用的是 URL 编码问题描述 ，则可能会看到错误： 不支持 `SAML` 版本 。

步骤

1. 安装所需的依赖关系，如下所示：
   a. 安装 Node.js （请参见 "https://nodejs.org/en/download/"）。
   b. 安装所需的 Node.js 模块（ puppeteer 和 jsdom ）：

      ```
      npm install -g <module>
      ```

2. 将 Python 脚本传递给 Python 解释器以运行此脚本。

   然后， Python 脚本将调用相应的 Node.js 脚本以执行 Azure SSO 交互。

3. 出现提示时，输入以下参数的值（或使用参数传递这些值）：
   ◦ 用于登录到 Azure 的 SSO 电子邮件地址

- StorageGRID 的地址
- 要访问租户管理 API 的租户帐户 ID

4. 出现提示时，输入密码，并在收到请求时准备向 Azure 提供 MFA 授权。

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> 此脚本假定 MFA 是使用 Microsoft Authenticator 完成的。您可能需要修改此脚本以支持其他形式的 MFA （例如输入通过文本消息接收的代码）。

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

如果启用了单点登录，请使用 **API** （ **PingFederate** ）

如果您有 已配置并启用单点登录（ SSO ） 如果使用 PingFederate 作为 SSO 提供程序，则必须对一系列 API 请求进行问题描述 处理，以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了单点登录，请登录到 **API**

如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

您需要的内容

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- `storagegrid-ssoauth.py` Python 脚本，该脚本位于 StorageGRID 安装文件目录中（对于 Red Hat Enterprise Linux 或 CentOS ，为` ./rpms` ；对于 Ubuntu 或 Debian ，为 ` ./de-s` ；对于 VMware ，为 ` ./vSphere` ）。
- cURL 请求的示例工作流。

  如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误： `A valid SubjectConfirmation was not found on this response`。

  > 示例 cURL 工作流不会保护密码不会被其他用户看到。

  如果您使用的是 URL 编码问题描述 ，则可能会看到错误： 不支持 `SAML` 版本 。

步骤

1. 选择以下方法之一以获取身份验证令牌：
   - 使用 `storagegrid-ssoauth.py` Python 脚本。转至步骤 2 。
   - 使用 curl 请求。转至步骤 3 。
2. 如果要使用 `storagegrid-ssoauth.py` 脚本，请将此脚本传递给 Python 解释器并运行此脚本。

   出现提示时，输入以下参数的值：
   - SSO 方法。您可以输入 "`pingFederate` " 的任何变体（ PNGFEDERATE ， PingFederate 等）。
   - SSO 用户名
   - 安装 StorageGRID 的域。此字段不用于 PingFederate 。您可以将其留空或输入任何值。
   - StorageGRID 的地址
   - 要访问租户管理 API 的租户帐户 ID 。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。
3. 如果要使用 curl 请求，请使用以下操作步骤 。
   a. 声明登录所需的变量。

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   ```

   > 要访问网格管理 API ，请使用 0 作为 `TENANTACCOBTID` 。

   b. 要接收签名的身份验证 URL ，问题描述 请将 POST 请求发送到 ` /apl/v3/authorize -SAML` ，然后从响应中删除额外的 JSON 编码。

   此示例显示了一个 POST 请求，用于为 TENANTACCOBTID 提供签名身份验证 URL 。结果将传递到 python -m json.tool 以删除 JSON 编码。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 从响应中保存 `SAMLRequest` ，以便在后续命令中使用。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 导出响应和 cookie ，并对响应执行回显：

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 导出 "pf.adapterId" 值，并对响应执行回显：

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 导出 "href" 值（删除后斜杠 / ），并对响应执行回显：

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 导出 "act" 值：

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 发送 Cookie 以及凭据：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 从隐藏字段中保存 `SAMLResponse`：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用已保存的 `SAMLResponse` 发出 StorageGRID `/API/SAML` 响应 请求以生成 StorageGRID 身份验证令牌。

对于 `RelayState` ，请使用租户帐户 ID ，或者如果要登录到网格管理 API ，请使用 0 。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

响应包括身份验证令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 将此身份验证令牌保存在响应中为 `MYTOKEN` 。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

现在，您可以对其他请求使用 `MYTOKEN` ，类似于未使用 SSO 时使用 API 的方式。

如果启用了单点登录，请注销 API

如果已启用单点登录（ Single Sign-On ， SSO ），则必须对一系列 API 请求进行问题描述 ，才能注销网格管理 API 或租户管理 API 。如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要，只需从组织的单个注销页面注销即可注销 StorageGRID API 。或者，您也可以从 StorageGRID 触发单点注销（ SLO ），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求，请将 `cookie "sso=true"` 传递到 SLO API ：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回注销 URL ：

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 保存注销 URL 。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。如果未提供 `cookie "sso=true"` ，则用户将从 StorageGRID 中注销，而不会影响 SSO 状态。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

`204 No Content` 响应表示用户现在已注销。

```
HTTP/1.1 204 No Content
```

控制对 **StorageGRID** 的访问

更改配置密码短语

使用此操作步骤 更改 StorageGRID 配置密码短语。恢复，扩展和维护过程需要密码短语。下载恢复软件包备份时也需要使用密码短语，其中包括网格拓扑信息，网格节点控制台密码以及 StorageGRID 系统的加密密钥。

您需要的内容

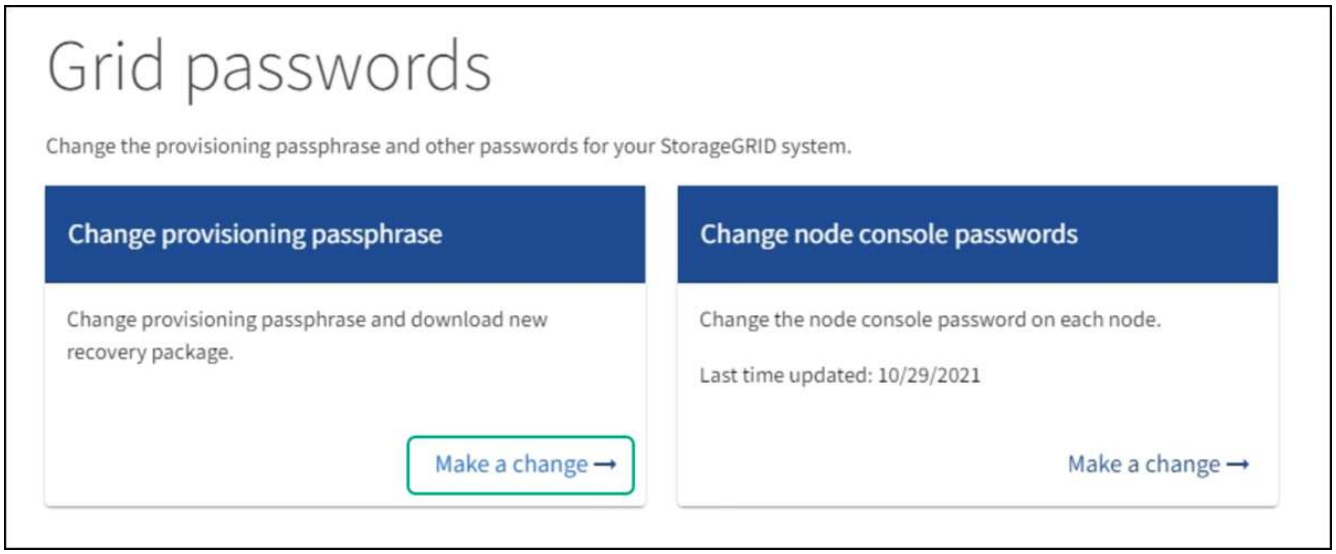
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有当前配置密码短语。

关于此任务

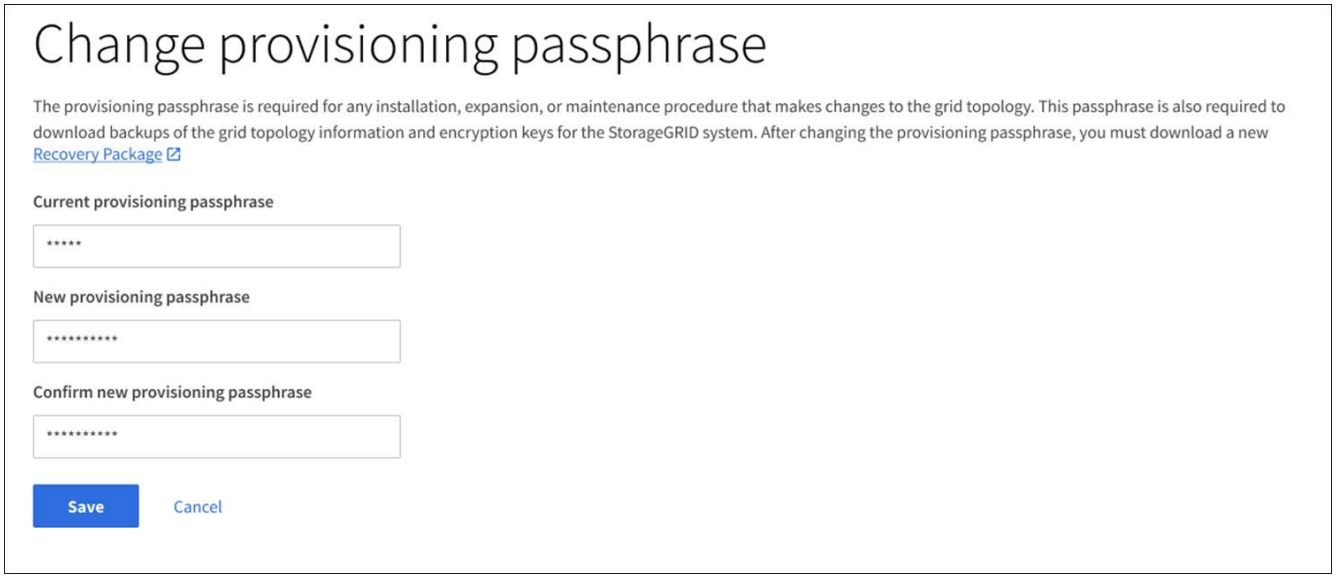
许多安装和维护过程以及都需要配置密码短语 正在下载恢复包。配置密码短语未列在 `passwords.txt` 文件中。请务必记录配置密码短语并将其保存在安全的位置。

步骤

1. 选择 * 配置 * > * 访问控制 * > * 网格密码 * 。

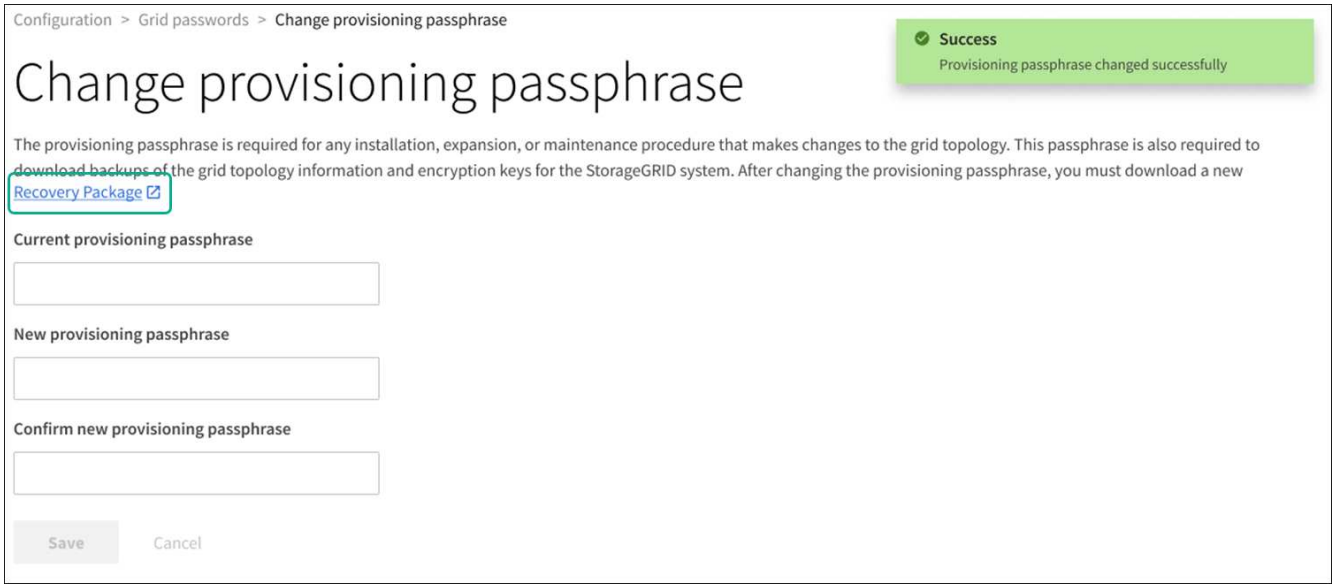


2. 在 * 更改配置密码短语 * 下选择 * 进行更改 * 。



3. 输入当前配置密码短语。
4. 输入新密码短语。密码短语必须至少包含 8 个字符，并且不能超过 32 个字符。密码短语区分大小写。
5. 将新配置密码短语存储在安全位置。安装，扩展和维护过程需要使用它。
6. 重新输入新密码短语，然后选择 * 保存 * 。

   配置密码短语更改完成后，系统将显示一个绿色的成功横幅。



7. 选择 * 恢复包 * 。
8. 输入新的配置密码短语以下载新的恢复软件包。

> 更改配置密码短语后，您必须立即下载新的恢复软件包。通过恢复包文件，您可以在发生故障时还原系统。

更改节点控制台密码

网格中的每个节点都有一个唯一的节点控制台密码，您需要使用该密码登录到该节点。按照以下步骤更改网格中每个节点的每个唯一节点控制台密码。

您需要的内容

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有维护或 root 访问权限。
- 您具有当前配置密码短语。

关于此任务

使用节点控制台密码以 "admin" 身份使用 SSH 登录到节点，或者以 VM/ 物理控制台连接上的 root 用户身份登录到节点。更改节点控制台密码过程会为网格中的每个节点创建新密码、并将这些密码存储在更新的中 `Passwords.txt` 文件。密码将在中的密码列中列出 `Passwords.txt` 文件

> 用于节点间通信的 SSH 密钥具有单独的 SSH 访问密码。此操作步骤 不会更改 SSH 访问密码。

访问向导

步骤

1. 选择 * 配置 * > * 访问控制 * > * 网格密码 * 。
2. 在*更改节点控制台密码*下、选择*进行更改*。

输入配置密码短语

步骤

1. 输入网格的配置密码短语。
2. 选择 * 继续 * 。

【下载当前版本】下载当前的恢复包

在更改节点控制台密码之前、请下载当前的恢复软件包。如果任何节点的密码更改过程失败、您可以使用此文件中的密码。

步骤

1. 选择 * 下载恢复包 * 。
2. 复制恢复包文件 (`.zip`)连接到两个安全、安全和独立的位置。

   恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

3. 选择 * 继续 * 。
4. 出现确认对话框时、如果您已准备好开始更改节点控制台密码、请选择*是*。

   此过程启动后、您无法取消。

更改节点控制台密码

当节点控制台密码过程开始时、将生成一个包含新密码的新恢复包。然后、在每个节点上更新密码。

步骤

1. 等待生成新的恢复软件包、这可能需要几分钟的时间。
2. 选择 * 下载新恢复包 * 。
3. 下载完成后：

   a. 打开 ` .zip` 文件。
   b. 确认您可以访问内容、包括 `Passwords.txt` 文件、其中包含新的节点控制台密码。
   c. 复制新的恢复软件包文件 (`.zip`)连接到两个安全、安全和独立的位置。

      请勿覆盖旧的恢复软件包。

   恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

4. 选中此复选框以指示您已下载新的恢复软件包并验证其内容。
5. 选择*更改节点控制台密码*、然后等待所有节点使用新密码进行更新。这可能需要几分钟时间。

   如果所有节点的密码均已更改，则会显示一个绿色的成功横幅。继续执行下一步。

   如果更新过程中出现错误，则会显示一条横幅消息，列出无法更改密码的节点数。系统将在任何无法更改密

码的节点上自动重试此过程。如果此过程结束时某些节点仍没有更改密码，则会显示 * 重试 * 按钮。

如果一个或多个节点的密码更新失败：

a. 查看表中列出的错误消息。

b. 解决问题。

c. 选择 * 重试 * 。

> 重试仅会更改先前尝试更改密码期间失败的节点上的节点控制台密码。

6. 更改所有节点的节点控制台密码后、请删除 下载的第一个恢复软件包。
7. 或者，也可以使用 * 恢复软件包 * 链接下载新恢复软件包的其他副本。

通过防火墙控制访问

如果要通过防火墙控制访问，请打开或关闭外部防火墙上的特定端口。

控制外部防火墙的访问

您可以通过在外部防火墙中打开或关闭特定端口来控制对 StorageGRID 管理节点上用户界面和 API 的访问。例如，除了使用其他方法控制系统访问之外，您可能还希望防止租户能够在防火墙处连接到网格管理器。

Port	Description	端口是否已打开 ...
443.	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问网格管理器，网格管理 API ，租户管理器和租户管理 API 。 • 注： * 端口 443 也用于某些内部流量。
8443	管理节点上的网格管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问网格管理器和网格管理 API 。 • Web 浏览器和管理 API 客户端无法访问租户管理器或租户管理 API 。 • 请求内部内容将被拒绝。
9443	管理节点上的租户管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问租户管理器和租户管理 API 。 • Web 浏览器和管理 API 客户端无法访问网格管理器或网格管理 API 。 • 请求内部内容将被拒绝。

> 受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

相关信息

- 登录到网格管理器
- 创建租户帐户
- 外部通信

使用身份联合

使用身份联合可以加快设置组和用户的速度，并允许用户使用熟悉的凭据登录到 StorageGRID 。

为 **Grid Manager** 配置身份联合

如果您希望在 Active Directory ， Azure Active Directory （ Azure AD ）， OpenLDAP 或 Oracle Directory Server 等其他系统中管理管理管理组和用户，则可以在网格管理器中配置身份联合。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您正在使用 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  如果要使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参见 配置 OpenLDAP 服务器的准则。
- 如果您计划启用单点登录（ SSO ），则已查看 使用单点登录的要求。
- 如果您计划使用传输层安全（ Transport Layer Security ， TLS ）与 LDAP 服务器进行通信，则身份提供程序正在使用 TLS 1.2 或 1.3 。请参见 支持传出 TLS 连接的密码。

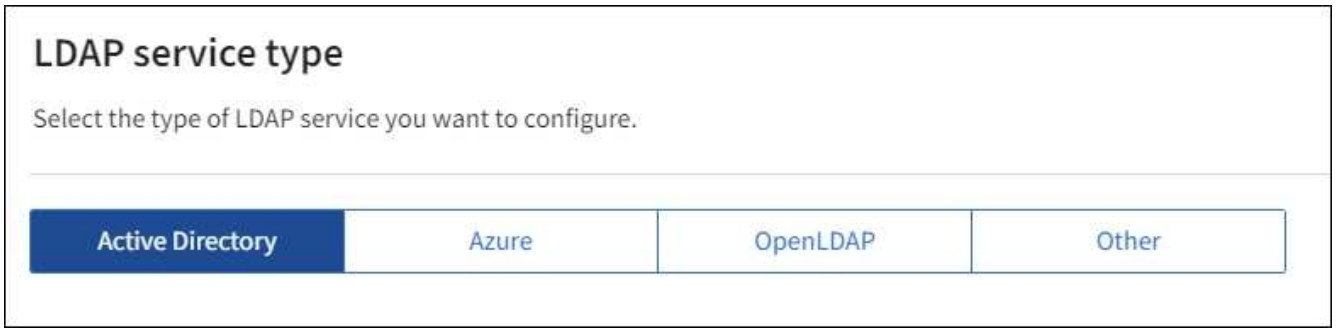
关于此任务

如果要从 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 等其他系统导入组，则可以为网格管理器配置身份源。您可以导入以下类型的组：

- 管理组。管理组中的用户可以登录到网格管理器并根据分配给该组的管理权限执行任务。
- 不使用自己身份源的租户的租户用户组。租户组中的用户可以登录到租户管理器，并根据在租户管理器中为该组分配的权限执行任务。请参见 创建租户帐户 和 使用租户帐户 了解详细信息。

输入配置

1. 选择 * 配置 * > * 访问控制 * > * 身份联合 * 。
2. 选择 * 启用身份联合 * 。
3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - * 用户唯一名称 * ： 包含 LDAP 用户唯一标识符的属性的名称。此属性相当于 `sAMAccountName` 用于 Active Directory ， `uid` 用于 OpenLDAP 。如果要配置 Oracle Directory Server ，请输入 `uid` 。
   - * 用户 UID* ： 包含 LDAP 用户的永久唯一标识符的属性的名称。此属性等效于 Active Directory 的 `objectGUID` 和 OpenLDAP 的 `entryUUID` 。如果要配置 Oracle Directory Server ，请输入 `nssuniqueid` 。每个用户在指定属性中的值都必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
   - * 组唯一名称 * ： 包含 LDAP 组唯一标识符的属性的名称。对于 Active Directory ，此属性相当于 `sAMAccountName` ；对于 OpenLDAP ，此属性相当于 `CN` 。如果要配置 Oracle Directory Server ，请输入 `CN` 。
   - * 组 UID* ： 包含 LDAP 组的永久唯一标识符的属性的名称。此属性等效于 Active Directory 的 `objectGUID` 和 OpenLDAP 的 `entryUUID` 。如果要配置 Oracle Directory Server ，请输入 `nssuniqueid` 。每个组在指定属性中的值必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
5. 对于所有 LDAP 服务类型，请在配置 LDAP 服务器部分中输入所需的 LDAP 服务器和网络连接信息。
   - * 主机名 * ： LDAP 服务器的完全限定域名（ FQDN ）或 IP 地址。
   - * 端口 * ： 用于连接到 LDAP 服务器的端口。

     STARTTLS 的默认端口为 389 ， LDAPS 的默认端口为 636 。但是，只要防火墙配置正确，您就可以使用任何端口。

   - * 用户名 * ： 要连接到 LDAP 服务器的用户的可分辨名称（ DN ）的完整路径。

     对于 Active Directory ，您还可以指定低级别的登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

     - `sAMAccountName` 或 `uid`
     - `objectGUID` ， `entryUUID` 或 `nssuniqueid`
     - `CN`
     - `memberOf` 或 `isMemberOf`
     - * Active Directory* ： `objectSid` ， `primaryGroupID` ， `userAccountControl` 和 `userPrincipalName`

- * Azure * ： `accountEnabled` 和 `userPrincipalName`

- * 密码 * ： 与用户名关联的密码。
- * 组基本 DN* ： 要搜索组的 LDAP 子树的可分辨名称（ DN ）的完整路径。在 Active Directory 示例（如下）中，可分辨名称相对于基础 DN （ DC=storagegrid ， DC=example ， DC=com ）的所有组均可用作联合组。

  * 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

- * 用户基础 DN* ： 要搜索用户的 LDAP 子树的可分辨名称（ DN ）的完整路径。

  用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

- * 绑定用户名格式 * （可选）： 如果无法自动确定模式， StorageGRID 应使用默认用户名模式。

  建议提供 * 绑定用户名格式 * ，因为如果 StorageGRID 无法绑定到服务帐户，它可以允许用户登录。

  输入以下模式之一：

  - * 用户 PrincipalName 模式（ Active Directory 和 Azure ） * ： `` 用户名@*example*.com
  - * 低级登录名称模式（ Active Directory 和 Azure ） * ： ` 示例 _\[ 用户名 ]`
  - * 可分辨名称模式 * ： `CN=[ 用户名 ] ， CN=Users ， DC=*example* ， DC=com`

    与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   - * 使用 STARTTLS * ： 使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是建议的 Active Directory ， OpenLDAP 或其他选项，但 Azure 不支持此选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。您必须为 Azure 选择此选项。
   - * 请勿使用 TLS* ： StorageGRID 系统与 LDAP 服务器之间的网络流量将不会受到保护。Azure 不支持此选项。

     如果 Active Directory 服务器强制实施 LDAP 签名，则不支持使用 * 不使用 TLS* 选项。您必须使用 STARTTLS 或 LDAPS 。

7. 如果选择 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认网格 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义安全证书。

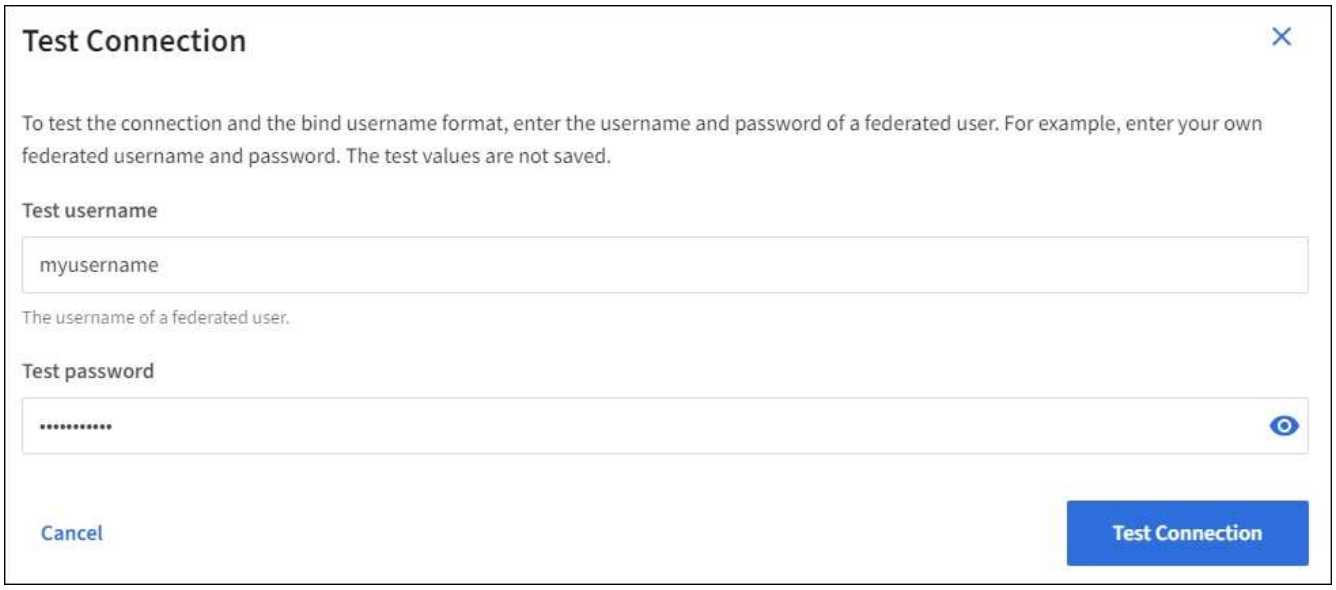
     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

1. 选择 * 测试连接 * 。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效，则会显示 "`test connection could not be established` " 消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

   例如，输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符，例如 @ 或 / 。



   - 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到身份联合页面。
2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以临时或永久禁用组和用户的身份联合。禁用身份联合后， StorageGRID 与身份源之间不会进行通信。但是，您配置的任何设置都将保留下来，以便将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，并且不会为尚未同步的帐户发出警报或警报。
- 如果单点登录（ SSO ）设置为 * 已启用 * 或 * 沙盒模式 * ，则 * 启用身份联合 * 复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 * 已禁用 * 。请参见 禁用单点登录。

步骤

1. 转到身份联合页面。
2. 取消选中 * 启用身份联合 * 复选框。

配置 **OpenLDAP** 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于非 ActiveDirectory 或 Azure 身份源， StorageGRID 不会自动阻止外部禁用的用户进行 S3 访问。要阻止 S3 访问，请删除该用户的任何 S3 密钥，并从所有组中删除该用户。

memberOf 和 **fint** 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex ： objectclass 均衡器`
- `olcDbIndex ： UID eq ， pres ， sub`
- `olcDbIndex ： CN eq ， pres ， sub`
- `olcDbIndex ： entryUUID 均衡器`

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

管理管理组

您可以创建管理组来管理一个或多个管理员用户的安全权限。用户必须属于要授予对 StorageGRID 系统访问权限的组。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

创建管理组

通过管理组，您可以确定哪些用户可以访问网格管理器和网格管理 API 中的哪些功能和操作。

访问向导

1. 选择 * 配置 * > * 访问控制 * > * 管理组 * 。
2. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

- 如果要为本地用户分配权限，请创建本地组。
- 创建联合组以从身份源导入用户。

本地组

1. 选择 * 本地组 * 。
2. 输入组的显示名称，您可以稍后根据需要更新该名称。例如， " M维护用户 " 或 "`ILM 管理员。`
3. 输入组的唯一名称，您不能稍后更新。
4. 选择 * 继续 * 。

联合组

1. 选择 * 联合组 * 。
2. 输入要导入的组的名称，与此名称在配置的身份源中显示的名称完全相同。
   - 对于 Active Directory 和 Azure ，请使用 sAMAccountName 。
   - 对于 OpenLDAP ，请使用 CN （公用名）。
   - 对于另一个 LDAP ，请为 LDAP 服务器使用适当的唯一名称。
3. 选择 * 继续 * 。

管理组权限

1. 对于 * 访问模式 * ，选择组中的用户是否可以在网格管理器和网格管理 API 中更改设置并执行操作，或者选择他们是否只能查看设置和功能。
   - * 读写 * （默认）： 用户可以更改其管理权限允许的设置并执行这些操作。
   - * 只读 * ： 用户只能查看设置和功能。他们不能在网格管理器或网格管理 API 中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

如果用户属于多个组，并且任何组设置为 * 只读 * ，则用户将对所有选定设置和功能具有只读访问权限。

2. 选择一个或多个 [组权限]。

   您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到 StorageGRID 。

3. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

1. 或者，为此组选择一个或多个本地用户。

   如果尚未创建本地用户，则可以保存此组，而无需添加用户。您可以在用户页面上将此组添加到用户。请参见管理用户 了解详细信息。

2. 选择 * 创建组 * 和 * 完成 * 。

查看和编辑管理组

您可以查看现有组的详细信息，修改组或复制组。

- 要查看所有组的基本信息，请查看组页面上的表。
- 要查看特定组的所有详细信息或编辑组，请使用 * 操作 * 菜单或详细信息页面。

任务	操作菜单	详细信息页面
查看组详细信息	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。	在表中选择组名称。
编辑显示名称（仅限本地组）	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 编辑组名称 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存更改 * 。
编辑访问模式或权限	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。 c. 也可以更改组的访问模式。 d. 或者，也可以选择或取消选择 [组权限]。 e. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 也可以更改组的访问模式。 c. 或者，也可以选择或取消选择 [组权限]。 d. 选择 * 保存更改 * 。

复制组

1. 选中组对应的复选框。

2. 选择 * 操作 * > * 复制组 * 。
3. 完成复制组向导。

删除组

如果要从系统中删除某个管理组，则可以删除该组，并删除与该组关联的所有权限。删除管理员组会从组中删除任何用户，但不会删除这些用户。

1. 在组页面中，选中要删除的每个组对应的复选框。
2. 选择 * 操作 * > * 删除组 * 。
3. 选择 * 删除组 * 。

组权限

创建管理员用户组时，您可以选择一个或多个权限来控制对网格管理器特定功能的访问。然后，您可以将每个用户分配给一个或多个管理组，以确定用户可以执行的任务。

您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到网格管理器或网格管理 API 。

默认情况下，属于至少具有一个权限的组的任何用户均可执行以下任务：

- 登录到网格管理器
- 查看信息板
- 查看节点页面
- 监控网格拓扑
- 查看当前警报和已解决警报
- 查看当前和历史警报（旧系统）
- 更改自己的密码（仅限本地用户）
- 在配置和维护页面上查看特定信息

权限与访问模式之间的交互

对于所有权限，组的 * 访问模式 * 设置将确定用户是否可以更改设置并执行操作，或者是否只能查看相关设置和功能。如果用户属于多个组，并且任何组设置为 * 只读 * ，则用户将对所有选定设置和功能具有只读访问权限。

以下各节介绍了在创建或编辑管理组时可以分配的权限。未明确提及的任何功能都需要具有 * 根访问权限 * 。

root 访问权限

通过此权限，可以访问所有网格管理功能。

确认警报（传统）

此权限可用于确认和响应警报（旧系统）。所有已登录用户均可查看当前和历史警报。

如果您希望用户仅监控网格拓扑并确认警报，则应分配此权限。

更改租户 **root** 密码

通过此权限，您可以访问租户页面上的 * 更改 root 密码 * 选项，从而可以控制谁可以更改租户的本地 root 用户的密码。启用 S3 密钥导入功能后，此权限也用于迁移 S3 密钥。不具有此权限的用户无法看到 * 更改 root 密码 * 选项。

要授予对包含 * 更改 root 密码 * 选项的租户页面的访问权限，还需要分配 * 租户帐户 * 权限。

网格拓扑页面配置

通过此权限，您可以访问 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的配置选项卡。

ILM

通过此权限，您可以访问以下 * ILM * 菜单选项：

- rules
- 策略
- 纠删编码
- regions
- 存储池

用户必须具有 * 其他网格配置 * 和 * 网格拓扑页面配置 * 权限才能管理存储级别。

维护

用户必须具有维护权限才能使用以下选项：

- * 配置 * > * 访问控制 * ：
  - 网格密码
- * 维护 * > * 任务 * ：
  - 停用
  - 扩展
  - 对象存在检查
  - 恢复
- * 维护 * > * 系统 * ：
  - 恢复包
  - 软件更新
- * 支持 * > * 工具 * ：
  - 日志

没有维护权限的用户可以查看但不能编辑以下页面：

- * 维护 * > * 网络 * ：
  - DNS 服务器
  - 网格网络
  - NTP 服务器
- * 维护 * > * 系统 * ：
  - 许可证
- * 配置 * > * 安全性 * ：
  - 证书
  - 域名
- * 配置 * > * 监控 * ：
  - 审核和系统日志服务器

管理警报

通过此权限，您可以访问用于管理警报的选项。用户必须具有此权限才能管理静音，警报通知和警报规则。

指标查询

通过此权限，您可以访问 * 支持 * > * 工具 * > * 指标 * 页面。通过此权限，还可以使用网格管理 API 的 * 指标 * 部分访问自定义的 Prometheus 指标查询。

对象元数据查找

通过此权限，您可以访问 * ILM * > * 对象元数据查找 * 页面。

其他网格配置

通过此权限可以访问其他网格配置选项。

要查看这些附加选项，用户还必须具有 * 网格拓扑页面配置 * 权限。

- * ILM ：
  - 存储等级
- * 配置 * > * 网络 * ：
  - 链路成本
- * 配置 * > * 系统 * ：
  - 显示选项
  - 网格选项
  - 存储选项
- * 支持 * > * 警报（传统） * ：
  - 自定义事件

- 全局警报
- 传统电子邮件设置

存储设备管理员

通过此权限，您可以通过网格管理器访问存储设备上的 E 系列 SANtricity 系统管理器。

租户帐户

通过此权限，您可以访问租户页面，在此可以创建，编辑和删除租户帐户。此权限还允许用户查看现有流量分类策略。

使用 **API** 停用功能

您可以使用网格管理 API 完全停用 StorageGRID 系统中的某些功能。停用某个功能后，不能为任何人分配执行与该功能相关的任务的权限。

关于此任务

停用的功能系统允许您阻止访问 StorageGRID 系统中的某些功能。停用某个功能是防止 root 用户或具有 * root 访问权限 * 的管理组中的用户能够使用该功能的唯一方法。

要了解此功能的有用程度，请考虑以下情形：

_Company A 是一家服务提供商，通过创建租户帐户租用其 StorageGRID 系统的存储容量。为了保护租户对象的安全， A 公司希望确保自己的员工在部署帐户后永远不能访问任何租户帐户。 _

_Company A 可以通过使用网格管理 API 中的停用功能系统来实现此目标。通过完全停用网格管理器中的 * 更改租户根密码 * 功能（ UI 和 API ），公司 A 可以确保任何管理员用户（包括 root 用户和属于具有 * root 访问权限 * 组的用户）都不能更改任何租户帐户的 root 用户的密码

步骤

1. 访问网格管理 API 的 Swagger 文档。请参见 使用网格管理 API。
2. 找到停用功能端点。
3. 要停用更改租户 root 密码等功能，请按如下所示向 API 发送正文：

   ` { "grid"： { "change租 户 RootPassword"： true } } `

   请求完成后，更改租户根密码功能将被禁用。用户界面中不再显示 * 更改租户根密码 * 管理权限，尝试更改租户根密码的任何 API 请求将失败，并显示 "`403 For禁用 。`

重新激活已停用的功能

默认情况下，您可以使用网格管理 API 重新激活已停用的功能。但是，如果要防止重新激活已停用的功能，则可以停用 * 激活功能 * 功能本身。

> 无法重新激活 * 活动功能 * 功能。如果您决定停用此功能，请注意，您将永远无法重新激活任何其他已停用的功能。要还原任何丢失的功能，您必须联系技术支持。

步骤

1. 访问网格管理 API 的 Swagger 文档。
2. 找到停用功能端点。
3. 要重新激活所有功能，请按如下所示将正文发送到 API：

   ` { "grid" : null } `

   此请求完成后，包括更改租户 root 密码功能在内的所有功能都将重新激活。现在， " 更改租户根密码 " 管理权限将显示在用户界面中，如果用户具有 * 根访问权限 * 或 * 更改租户根密码 * 管理权限，则尝试更改租户根密码的任何 API 请求都将成功。

> 上一示例将重新激活 *all* 已停用的功能。如果其他功能已停用，而这些功能应保持停用状态，则必须在 PUT 请求中明确指定它们。例如，要重新激活更改租户 root 密码功能并继续停用警报确认功能，请发送此 PUT 请求：
>
> ` { "grid" : { "alarmAction" : true } } `

管理用户

您可以查看本地用户和联合用户。您还可以创建本地用户并将其分配给本地管理组，以确定这些用户可以访问哪些网格管理器功能。

您需要的内容

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

创建本地用户

您可以创建一个或多个本地用户，并将每个用户分配给一个或多个本地组。组的权限控制用户可以访问的网格管理器和网格管理 API 功能。

您只能创建本地用户。使用外部身份源管理联合用户和组。

网格管理器包括一个名为 "`root" 的预定义本地用户。` 您不能删除 root 用户。

> 如果启用了单点登录（ SSO ），则本地用户将无法登录到 StorageGRID 。

访问向导

1. 选择 * 配置 * > * 访问控制 * > * 管理用户 * 。
2. 选择 * 创建用户 * 。

输入用户凭据

1. 输入用户的全名，唯一用户名和密码。
2. 或者，如果此用户不应访问网格管理器或网格管理 API ，请选择 * 是 * 。
3. 选择 * 继续 * 。

分配给组

1. （可选）将用户分配给一个或多个组以确定用户的权限。

   如果尚未创建组，则可以保存用户而不选择组。您可以在组页面上将此用户添加到组中。

   如果用户属于多个组，则权限是累积的。请参见管理管理组 了解详细信息。

2. 选择 * 创建用户 * 并选择 * 完成 * 。

查看和编辑本地用户

您可以查看现有本地用户和联合用户的详细信息。您可以修改本地用户以更改用户的全名，密码或组成员资格。您还可以暂时阻止用户访问网格管理器和网格管理 API 。

您只能编辑本地用户。使用外部身份源管理联合用户。

- 要查看所有本地和联合用户的基本信息，请查看用户页面上的表。
- 要查看特定用户的所有详细信息，编辑本地用户或更改本地用户的密码，请使用 * 操作 * 菜单或详细信息页面。

  用户下次注销后重新登录到网格管理器时，系统将应用任何编辑。

  本地用户可以使用网格管理器横幅中的 * 更改密码 * 选项更改自己的密码。

任务	操作菜单	详细信息页面
查看用户详细信息	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。	在表中选择用户名。
编辑全名（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 编辑全名 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存更改 * 。
拒绝或允许 StorageGRID 访问	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择访问选项卡。 d. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 e. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择访问选项卡。 c. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 d. 选择 * 保存更改 * 。

任务	操作菜单	详细信息页面
更改密码（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择密码选项卡。 d. 输入新密码。 e. 选择 * 更改密码 * 。	a. 选择用户的名称以显示详细信息。 b. 选择密码选项卡。 c. 输入新密码。 d. 选择 * 更改密码 * 。
更改组（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择组选项卡。 d. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 e. 选择 * 编辑组 * 以选择不同的组。 f. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择组选项卡。 c. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 d. 选择 * 编辑组 * 以选择不同的组。 e. 选择 * 保存更改 * 。

复制用户

您可以复制现有用户以创建具有相同权限的新用户。

1. 选中用户对应的复选框。
2. 选择 * 操作 * > * 复制用户 * 。
3. 完成复制用户向导。

删除用户

您可以删除本地用户，以便从系统中永久删除该用户。

您不能删除 root 用户。

1. 在用户页面中，选中要删除的每个用户对应的复选框。
2. 选择 * 操作 * > * 删除用户 * 。
3. 选择 * 删除用户 * 。

使用单点登录（ **SSO** ）

配置单点登录

启用单点登录（ SSO ）后，只有在用户凭据通过贵组织实施的 SSO 登录过程获得授权的情况下，用户才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用

户无法登录到 StorageGRID 。

单点登录的工作原理

StorageGRID 系统支持使用安全断言标记语言 2.0 （ SAML 2.0 ）标准的单点登录（ SSO ）。

在启用单点登录（ SSO ）之前，请查看启用 SSO 后 StorageGRID 登录和注销过程会受到什么影响。

启用 **SSO** 后登录

启用 SSO 并登录到 StorageGRID 后，系统会将您重定向到组织的 SSO 页面以验证您的凭据。

步骤

1. 在 Web 浏览器中输入任何 StorageGRID 管理节点的完全限定域名或 IP 地址。

   此时将显示 StorageGRID 登录页面。

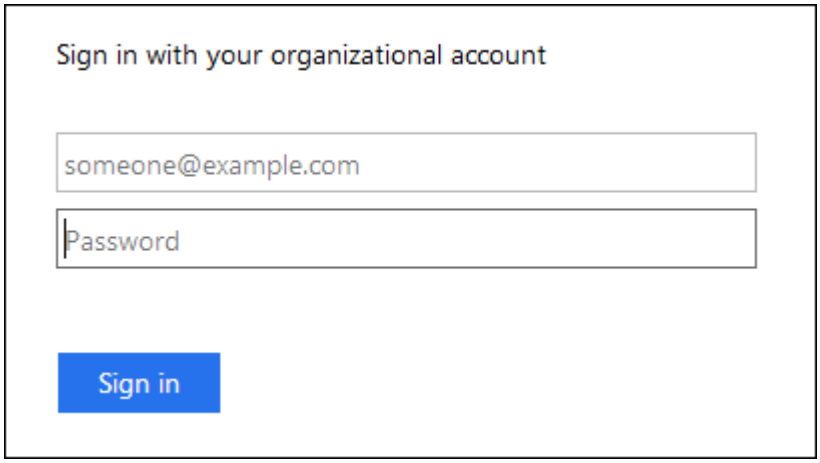
   - 如果这是您首次在此浏览器上访问此 URL ，系统将提示您输入帐户 ID ：

   - 如果您之前访问过网格管理器或租户管理器，系统将提示您选择最近的帐户或输入帐户 ID ：

输入租户帐户的完整 URL （即，完全限定域名或 IP 地址后跟 ` / ？ AccountID=*20-Digit-account-id*` ）时，不会显示 StorageGRID 登录页面。而是会立即重定向到您所在组织的 SSO 登录页面，您可以在该页面上进行登录 使用您的 SSO 凭据登录。

2. 指示您是要访问网格管理器还是租户管理器：
   - 要访问网格管理器，请将 * 帐户 ID* 字段留空，输入 * 0 * 作为帐户 ID ，或者选择 * 网格管理器 * （如果它显示在近期帐户列表中）。
   - 要访问租户管理器，请输入 20 位租户帐户 ID ，或者如果某个租户显示在近期帐户列表中，则按名称选择此租户。
3. 选择 * 登录 *

   StorageGRID 会将您重定向到贵组织的 SSO 登录页面。例如：



4. 【签名 _sso]] 使用您的 SSO 凭据登录。

   如果您的 SSO 凭据正确：

   a. 身份提供程序（ IdP ）为 StorageGRID 提供身份验证响应。
   b. StorageGRID 将验证身份验证响应。
   c. 如果响应有效，并且您属于具有 StorageGRID 访问权限的联合组，则您将登录到网格管理器或租户管理器，具体取决于您选择的帐户。

   如果此服务帐户不可访问，则只要您是具有 StorageGRID 访问权限的联合组的现有用户，您仍可登录。

5. 或者，如果您拥有足够的权限，也可以访问其他管理节点，或者访问网格管理器或租户管理器。

   您无需重新输入 SSO 凭据。

启用 **SSO** 后注销

为 StorageGRID 启用 SSO 后，注销时会发生什么情况取决于您登录到的内容以及注销的位置。

步骤

1. 找到用户界面右上角的 * 注销 * 链接。
2. 选择 * 注销 * 。

   此时将显示 StorageGRID 登录页面。更新了 * 近期帐户 * 下拉列表，其中包含 * 网格管理器 * 或租户名称，以便您将来可以更快地访问这些用户界面。

如果您已登录到 ...	您可以从以下位置注销 ...	您已注销 ...
一个或多个管理节点上的网格管理器	任何管理节点上的网格管理器	所有管理节点上的网格管理器 • 注意： * 如果您使用 Azure 进行 SSO ，则从所有管理节点中注销可能需要几分钟的时间。
一个或多个管理节点上的租户管理器	任何管理节点上的租户管理器	所有管理节点上的租户管理器
网格管理器和租户管理器	网格管理器	仅限网格管理器。您还必须注销租户管理器才能注销 SSO 。

下表总结了在使用单个浏览器会话时注销时会发生的情况。如果您通过多个浏览器会话登录到 StorageGRID ，则必须单独注销所有浏览器会话。

使用单点登录的要求

在为 StorageGRID 系统启用单点登录（ SSO ）之前，请查看本节中的要求。

身份提供程序要求

StorageGRID 支持以下 SSO 身份提供程序（ IdP ）：

- Active Directory 联合身份验证服务（ AD FS ）
- Azure Active Directory （ Azure AD ）
- PingFederate

您必须先为 StorageGRID 系统配置身份联合，然后才能配置 SSO 身份提供程序。用于身份联合的 LDAP 服务类型控制您可以实施的 SSO 类型。

已配置 **LDAP** 服务类型	**SSO** 身份提供程序的选项
Active Directory	• Active Directory • Azure 酒店 • PingFederate
Azure 酒店	Azure 酒店

AD FS 要求

您可以使用以下任意版本的 AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 应使用 "KB3201845 更新"或更高版本。

- AD FS 3.0 ，随 Windows Server 2012 R2 更新或更高版本提供。

其他要求

- 传输层安全（ Transport Layer Security ， TLS ） 1.2 或 1.3
- Microsoft .NET Framework 3.5.1 或更高版本

服务器证书要求

默认情况下， StorageGRID 会在每个管理节点上使用管理接口证书来保护对网格管理器，租户管理器，网格管理 API 和租户管理 API 的访问。在为 StorageGRID 配置依赖方信任（ AD FS ），企业应用程序（ Azure ）或服务提供商连接（ PingFederate ）时，您可以使用服务器证书作为 StorageGRID 请求的签名证书。

如果您尚未执行此操作 已为管理接口配置自定义证书，您现在应执行此操作。安装自定义服务器证书时，该证书将用于所有管理节点，您可以在所有 StorageGRID 依赖方信任关系，企业应用程序或 SP 连接中使用该证书。

> 建议不要在依赖方信任，企业应用程序或 SP 连接中使用管理节点的默认服务器证书。如果节点发生故障而您恢复了该节点，则会生成一个新的默认服务器证书。在登录到已恢复的节点之前，您必须使用新证书更新依赖方信任，企业应用程序或 SP 连接。

您可以通过登录到管理节点的命令 Shell 并转到 ` /var/local/mgmt-api` 目录来访问管理节点的服务器证书。自定义服务器证书名为 `custom-server.crt` 。节点的默认服务器证书名为 `sserver.crt` 。

端口要求

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。请参见 通过防火墙控制访问。

确认联合用户可以登录

在启用单点登录（ SSO ）之前，您必须确认至少有一个联合用户可以登录到网格管理器以及任何现有租户帐户的租户管理器。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已配置身份联合。

步骤

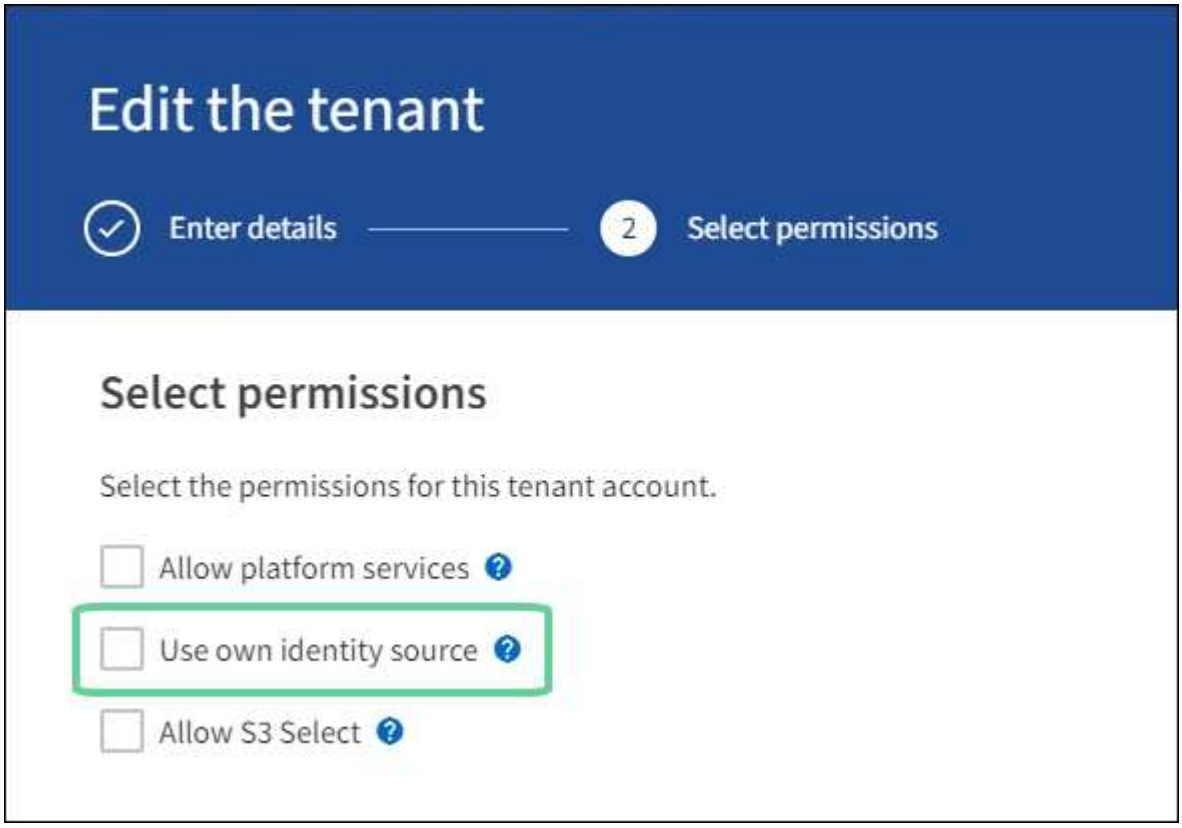
1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

> 启用 SSO 后，在租户管理器中配置的身份源将被网格管理器中配置的身份源覆盖。属于租户身份源的用户将无法再登录，除非他们拥有网格管理器身份源帐户。

   a. 登录到每个租户帐户的租户管理器。
   b. 选择 * 访问管理 * > * 身份联合 * 。
   c. 确认未选中 * 启用身份联合 * 复选框。
   d. 如果是，请确认不再需要可能用于此租户帐户的任何联合组，取消选中此复选框，然后选择 * 保存 * 。

2. 确认联合用户可以访问网格管理器：
   a. 在网格管理器中，选择 * 配置 * > * 访问控制 * > * 管理组 * 。
   b. 确保已从 Active Directory 身份源导入至少一个联合组，并已为其分配 root 访问权限。
   c. 注销。
   d. 确认您可以以联合组中的用户身份重新登录到网格管理器。

3. 如果存在现有租户帐户，请确认具有 root 访问权限的联合用户可以登录：
   a. 在网格管理器中，选择 * 租户 * 。
   b. 选择租户帐户，然后选择 * 操作 * > * 编辑 * 。
   c. 在输入详细信息选项卡上，选择 * 继续 * 。
   d. 如果选中了 * 使用自己的身份源 * 复选框，请取消选中该复选框并选择 * 保存 * 。



此时将显示租户页面。

a. 选择租户帐户，选择 * 登录 * ，然后以本地 root 用户身份登录到租户帐户。
b. 在租户管理器中，选择 * 访问管理 * > * 组 * 。
c. 确保至少已为此租户为网格管理器中的一个联合组分配 root 访问权限。
d. 注销。
e. 确认您可以以联盟组中的用户身份重新登录到租户。

相关信息

- 使用单点登录的要求
- 管理管理组
- 使用租户帐户

使用沙盒模式

在为所有 StorageGRID 用户启用单点登录（ SSO ）之前，您可以使用沙盒模式配置和测试单点登录（ SSO ）。启用 SSO 后，您可以在需要更改或重新测试配置时返回到沙盒模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 您已为 StorageGRID 系统配置身份联合。
- 对于身份联合 * LDAP 服务类型 * ，您根据计划使用的 SSO 身份提供程序选择了 Active Directory 或 Azure 。

已配置 **LDAP** 服务类型	**SSO** 身份提供程序的选项
Active Directory	• Active Directory • Azure 酒店 • PingFederate
Azure 酒店	Azure 酒店

关于此任务

启用 SSO 后，如果用户尝试登录到管理节点，则 StorageGRID 会向 SSO 身份提供程序发送身份验证请求。然后， SSO 身份提供程序会向 StorageGRID 发回身份验证响应，指示身份验证请求是否成功。对于成功的请求：

- Active Directory 或 PingFederate 的响应包括用户的通用唯一标识符（ UUID ）。
- Azure 的响应包括用户主体名称（ UPN ）。

要允许 StorageGRID （服务提供商）和 SSO 身份提供程序就用户身份验证请求进行安全通信，您必须在 StorageGRID 中配置某些设置。接下来，您必须使用 SSO 身份提供程序的软件为每个管理节点创建依赖方信任

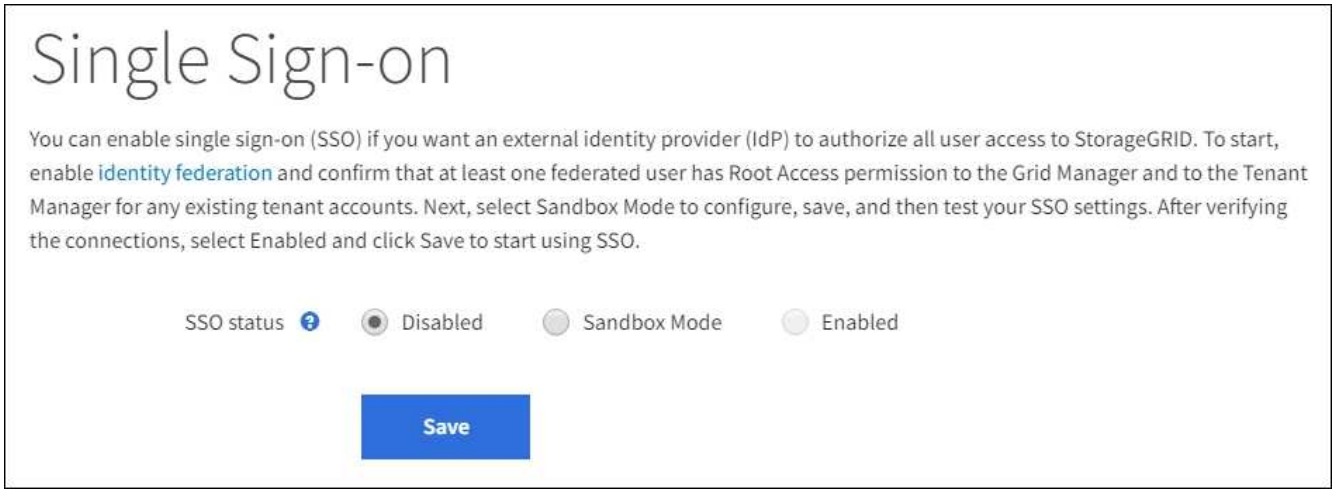
（AD FS），企业应用程序（Azure）或服务提供商（PingFederate）。最后，您必须返回到 StorageGRID 以启用 SSO 。

使用沙盒模式，可以轻松执行此背面配置，并在启用 SSO 之前测试所有设置。使用沙盒模式时，用户无法使用 SSO 登录。

访问沙盒模式

1. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。

   此时将显示 Single Sign-On 页面，并选择 * 已禁用 * 选项。



   如果未显示 SSO 状态选项，请确认您已将身份提供程序配置为联合身份源。请参见 使用单点登录的要求。

2. 选择 * 沙盒模式 * 。

   此时将显示 "Identity Provider" 部分。

输入身份提供程序详细信息

1. 从下拉列表中选择 * SSO 类型 * 。
2. 根据您选择的 SSO 类型填写身份提供程序部分中的字段。

Active Directory

1. 输入身份提供程序的 * 联合服务名称 * ，与 Active Directory 联合身份验证服务（ AD FS ）中显示的名称完全相同。

   要查找联合服务名称，请转到 Windows Server Manager 。选择 * 工具 * > * AD FS 管理 * 。从操作菜单中，选择 * 编辑联合身份验证服务属性 * 。联合服务名称显示在第二个字段中。

2. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。
3. 在依赖方部分中，指定 StorageGRID 的 * 依赖方标识符 * 。此值控制 AD FS 中每个依赖方信任所使用的名称。
   - 例如，如果您的网格只有一个管理节点，并且您预计将来不会添加更多管理节点，请输入 `SG` 或 `StorageGRID` 。
   - 如果网格包含多个管理节点，请在标识符中包含字符串 ` HOSTNAME]` 。例如， `SG-[HOSTNAME]` 。此时将生成一个表，其中根据节点的主机名显示系统中每个管理节点的依赖方标识符。

   您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

4. 选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

Azure 酒店

1. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。
2. 在企业应用程序部分中，为 StorageGRID 指定 * 企业应用程序名称 * 。此值控制 Azure AD 中每个企业应用程序使用的名称。

- 例如，如果您的网格只有一个管理节点，并且您预计将来不会添加更多管理节点，请输入 `SG` 或 `StorageGRID` 。
- 如果网格包含多个管理节点，请在标识符中包含字符串 ` HOSTNAME]` 。例如， `SG-[HOSTNAME]` 。此时将生成一个表，其中根据节点的主机名显示系统中每个管理节点的企业应用程序名称。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

3. 按照中的步骤进行操作 在 Azure AD 中创建企业级应用程序 为表中列出的每个管理节点创建企业级应用程序。
4. 从 Azure AD 中，复制每个企业应用程序的联合元数据 URL 。然后，将此 URL 粘贴到 StorageGRID 中相应的 * 联合元数据 URL* 字段中。
5. 复制并粘贴所有管理节点的联合元数据 URL 后，选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

PingFederate

1. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。
   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。
2. 在服务提供商（ SP ）部分中，为 StorageGRID 指定 * SP 连接 ID* 。此值控制 PingFederate 中每个 SP 连接使用的名称。
   - 例如，如果您的网格只有一个管理节点，并且您预计将来不会添加更多管理节点，请输入 `SG` 或 `StorageGRID` 。
   - 如果网格包含多个管理节点，请在标识符中包含字符串 ` HOSTNAME]` 。例如， `SG-[HOSTNAME]` 。此时将生成一个表，其中根据节点的主机名显示系统中每个管理节点的 SP 连接 ID 。

   > 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接。为每个管理节点建立 SP 连接可确保用户可以安全地登录和注销任何管理节点。

3. 在 * 联合元数据 URL* 字段中指定每个管理节点的联合元数据 URL 。

   请使用以下格式：

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
ID>
```

4. 选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

配置依赖方信任，企业应用程序或 **SP** 连接

保存配置后，将显示沙盒模式确认通知。此通知用于确认沙盒模式现已启用，并提供了概述说明。

只要需要， StorageGRID 就可以保持沙盒模式。但是，如果在 Single Sign-On 页面上选择了 * 沙盒模式 * ，则所有 StorageGRID 用户都将禁用 SSO 。只有本地用户才能登录。

按照以下步骤配置依赖方信任（ Active Directory ），完整的企业应用程序（ Azure ）或配置 SP 连接（ PingFederate ）。

Active Directory

1. 转至 Active Directory 联合身份验证服务（ AD FS ）。
2. 使用 StorageGRID 单点登录页面上的表中所示的每个依赖方标识符为 StorageGRID 创建一个或多个依赖方信任。

   您必须为表中所示的每个管理节点创建一个信任。

   有关说明，请转至 在 AD FS 中创建依赖方信任。

Azure 酒店

1. 从当前登录到的管理节点的单点登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到节点。
   b. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 Azure 门户。
4. 按照中的步骤进行操作 在 Azure AD 中创建企业级应用程序 将每个管理节点的 SAML 元数据文件上传到其对应的 Azure 企业应用程序中。

PingFederate

1. 从当前登录到的管理节点的单点登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到节点。
   b. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 PingFederate 。
4. 为 StorageGRID 创建一个或多个服务提供商（ SP ）连接。使用每个管理节点的 SP 连接 ID （如 StorageGRID 单点登录页面上的表所示）以及为该管理节点下载的 SAML 元数据。

   您必须为表中所示的每个管理节点创建一个 SP 连接。

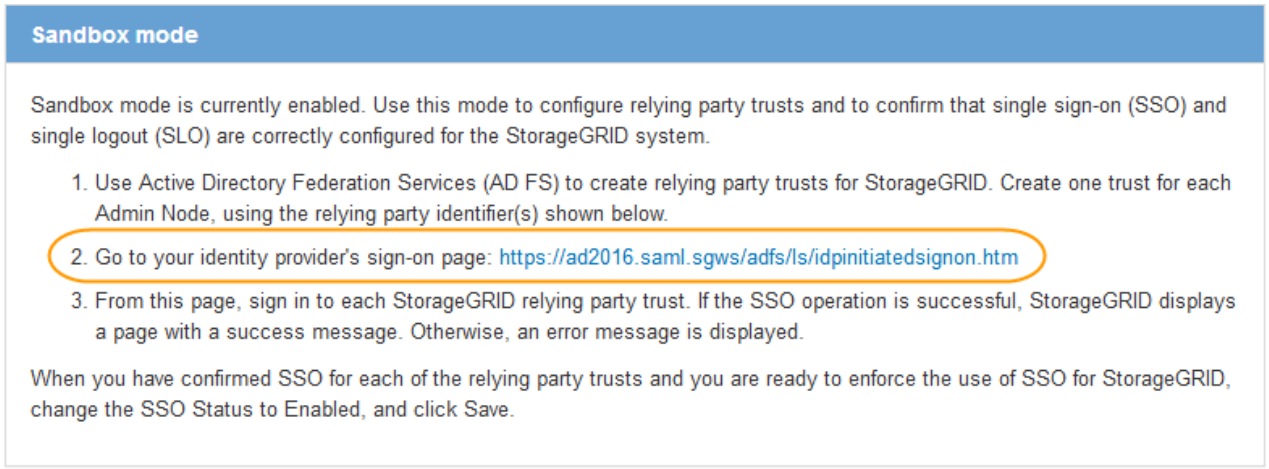
测试 **SSO** 连接

在对整个 StorageGRID 系统强制使用单点登录之前，您应确认已为每个管理节点正确配置单点登录和单点注销。

Active Directory

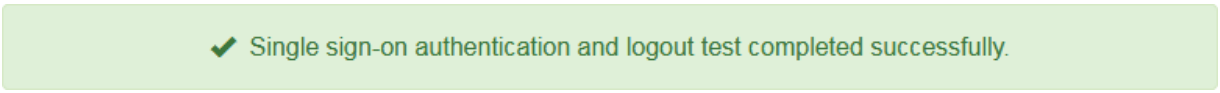
1. 在 StorageGRID 单点登录页面中，找到沙盒模式消息中的链接。

   此 URL 是从您在 * 联合服务名称 * 字段中输入的值派生的。

2. 选择此链接，或者将此 URL 复制并粘贴到浏览器中，以访问身份提供程序的登录页面。
3. 要确认您可以使用 SSO 登录到 StorageGRID ，请选择 * 登录到以下站点之一 * ，选择主管理节点的依赖方标识符，然后选择 * 登录 * 。

4. 输入您的联合用户名和密码。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
5. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

Azure 酒店

1. 转到 Azure 门户中的单点登录页面。
2. 选择 * 测试此应用程序 * 。

3. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

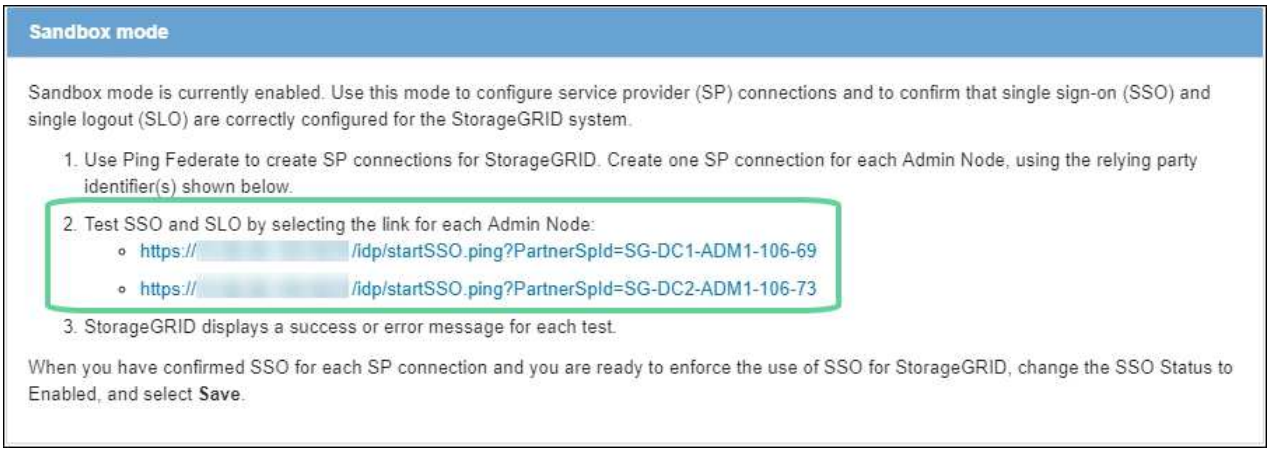
     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
4. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

PingFederate

1. 从 StorageGRID 单点登录页面中，选择沙盒模式消息中的第一个链接。

   一次选择并测试一个链路。



2. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
3. 选择下一个链接以验证网格中每个管理节点的 SSO 连接。

   如果您看到页面已过期消息，请在浏览器中选择 * 返回 * 按钮，然后重新提交您的凭据。

启用单点登录

确认可以使用 SSO 登录到每个管理节点后，您可以为整个 StorageGRID 系统启用 SSO 。

> ⓘ 启用 SSO 后，所有用户都必须使用 SSO 访问网格管理器，租户管理器，网格管理 API 和租户管理 API 。本地用户无法再访问 StorageGRID 。

1. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
2. 将 SSO 状态更改为 * 已启用 * 。

3. 选择 * 保存 * 。
4. 查看警告消息，然后选择 * 确定 * 。

   现在，已启用单点登录。

> 如果您使用的是 Azure 门户，并且从用于访问 Azure 的同一计算机访问 StorageGRID ，请确保 Azure 门户用户也是授权的 StorageGRID 用户（已导入到 StorageGRID 的联合组中的用户） 或者，在尝试登录到 StorageGRID 之前，请先从 Azure 门户中注销。

在 **AD FS** 中创建依赖方信任

您必须使用 Active Directory 联合身份验证服务（ AD FS ）为系统中的每个管理节点创建依赖方信任。您可以使用 PowerShell 命令，从 StorageGRID 导入 SAML 元数据或手动输入数据来创建依赖方信任。

您需要的内容

- 您已为 StorageGRID 配置单点登录，并选择了 * AD FS* 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 使用沙盒模式。
- 您知道系统中每个管理节点的完全限定域名（或 IP 地址）和依赖方标识符。您可以在 StorageGRID 单点登录页面上的管理节点详细信息表中找到这些值。

> 您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

- 您有在 AD FS 中创建依赖方信任的经验，也可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。
- 如果您要手动创建依赖方信任，则可以获得为 StorageGRID 管理界面上传的自定义证书，或者知道如何从命令 Shell 登录到管理节点。

关于此任务

以下说明适用于 Windows Server 2016 AD FS 。如果您使用的是其他版本的 AD FS ，则会注意到操作步骤 略有不同。如果您有任何疑问，请参见 Microsoft AD FS 文档。

使用 **Windows PowerShell** 创建依赖方信任

您可以使用 Windows PowerShell 快速创建一个或多个依赖方信任。

步骤

1. 从 Windows 开始菜单中，右键选择 PowerShell 图标，然后选择 * 以管理员身份运行 * 。
2. 在 PowerShell 命令提示符处，输入以下命令：

   <code>Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL "<a href="https://Admin_Node_FQDN/api/saml-metadata"</code>" class="bare">https://Admin_Node_FQDN/api/saml-metadata"</code>

   ◦ 对于 ` *Admin_Node_Identifier* ` ，请输入管理节点的依赖方标识符，就像它显示在 Single Sign-On 页面

上一样。例如， `SG-DC1-ADM1` 。

- 对于 `Admin_Node_FQDN_` ，输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

3. 在 Windows Server Manager 中，选择 * 工具 * > * AD FS 管理 * 。

   此时将显示 AD FS 管理工具。

4. 选择 * AD FS* > * 依赖方信任 * 。

   此时将显示依赖方信任列表。

5. 向新创建的依赖方信任添加访问控制策略：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击信任，然后选择 * 编辑访问控制策略 * 。
   c. 选择访问控制策略。
   d. 选择 * 应用 * ，然后选择 * 确定 *
6. 将款项申请发放策略添加到新创建的相关方信任：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   c. 选择 * 添加规则 * 。
   d. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。
   e. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。

   f. 对于属性存储，选择 * Active Directory* 。
   g. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。
   h. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。
   i. 选择 * 完成 * ，然后选择 * 确定 * 。
7. 确认元数据已成功导入。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

      如果缺少元数据，请确认联合元数据地址是否正确，或者只需手动输入值即可。

8. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。
9. 完成后，返回到 StorageGRID 并测试所有相关方信任，以确认其配置正确。请参见 使用沙盒模式 有关说明，请参见。

通过导入联合元数据创建依赖方信任

您可以通过访问每个管理节点的 SAML 元数据来导入每个依赖方信任的值。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。
2. 在操作下，选择 * 添加依赖方信任 * 。
3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。
4. 选择 * 导入有关依赖方的在线或本地网络上发布的数据 * 。
5. 在 * 联合元数据地址（主机名或 URL ） * 中，键入此管理节点的 SAML 元数据的位置：

   `https://Admin_Node_FQDN/api/saml-metadata`

   对于 `Admin_Node_FQDN_` ，输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

6. 完成依赖方信任向导，保存依赖方信任并关闭该向导。

   输入显示名称时，请使用管理节点的相关方标识符，与网格管理器的 Single Sign-On 页面上显示的完全相同。例如， `SG-DC1-ADM1` 。

7. 添加声明规则：
   a. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   b. 选择 * 添加规则 * ：
   c. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。
   d. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。

   e. 对于属性存储，选择 * Active Directory* 。
   f. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。
   g. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。
   h. 选择 * 完成 * ，然后选择 * 确定 * 。
8. 确认元数据已成功导入。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

      如果缺少元数据，请确认联合元数据地址是否正确，或者只需手动输入值即可。

9. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。
10. 完成后，返回到 StorageGRID 并测试所有相关方信任，以确认其配置正确。请参见 使用沙盒模式 有关说明，请参见。

手动创建依赖方信任

如果您选择不导入依赖部件信任的数据，则可以手动输入值。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。
2. 在操作下，选择 * 添加依赖方信任 * 。
3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。
4. 选择 * 手动输入有关依赖方的数据 * ，然后选择 * 下一步 * 。
5. 完成依赖方信任向导：

   a. 输入此管理节点的显示名称。

      为了确保一致性，请使用管理节点的依赖方标识符，与网格管理器的单点登录页面上显示的一致。例如， `SG-DC1-ADM1` 。

   b. 跳过此步骤可配置可选令牌加密证书。

   c. 在配置 URL 页面上，选中 * 启用对 SAML 2.0 WebSSO 协议的支持 * 复选框。

   d. 键入管理节点的 SAML 服务端点 URL ：

      `https://Admin_Node_FQDN/api/saml-response`

      对于 ` Admin_Node_FQDN_` ，输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

   e. 在配置标识符页面上，指定同一管理节点的依赖方标识符：

      ` 管理节点标识符 _`

      对于 ` *Admin_Node_Identifier*` ，请输入管理节点的依赖方标识符，就像它显示在 Single Sign-On 页面上一样。例如， `SG-DC1-ADM1` 。

   f. 查看设置，保存依赖方信任并关闭向导。

      此时将显示编辑款项申请发放策略对话框。

      如果未显示此对话框，请右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。

6. 要启动 Claim Rule 向导，请选择 * 添加规则 * ：

   a. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。

   b. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。

   c. 对于属性存储，选择 * Active Directory* 。

   d. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。

e. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。

f. 选择 * 完成 * ，然后选择 * 确定 * 。

7. 右键单击依赖方信任以打开其属性。

8. 在 * 端点 * 选项卡上，为单点注销（ SLO ）配置端点：

a. 选择 * 添加 SAML * 。

b. 选择 * 端点类型 * > * SAML 注销 * 。

c. 选择 * 绑定 * > * 重定向 * 。

d. 在 * 可信 URL* 字段中，输入用于从此管理节点单点注销（ SLO ）的 URL ：

```
https://Admin_Node_FQDN/api/saml-logout
```

对于 ` Admin_Node_FQDN_` ，输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

a. 选择 * 确定 * 。

9. 在 * 签名 * 选项卡上，指定此依赖方信任的签名证书：

a. 添加自定义证书：

- 如果您已将自定义管理证书上传到 StorageGRID ，请选择此证书。
- 如果您没有自定义证书，请登录到管理节点，转到管理节点的 ` /var/local/mgmt-api` 目录，然后添加 `custom-server.crt` 证书文件。
  - 注： * 不建议使用管理节点的默认证书（ `server.crt` ）。如果管理节点出现故障，则在恢复节点时将重新生成默认证书，您需要更新依赖方信任。

b. 选择 * 应用 * ，然后选择 * 确定 * 。

依赖方属性将被保存并关闭。

10. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

11. 完成后，返回到 StorageGRID 并测试所有相关方信任，以确认其配置正确。请参见 使用沙盒模式 有关说明，请参见。

在 **Azure AD** 中创建企业级应用程序

您可以使用 Azure AD 为系统中的每个管理节点创建企业级应用程序。

您需要的内容

- 您已开始为 StorageGRID 配置单点登录，并选择了 * Azure * 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 使用沙盒模式。
- 系统中每个管理节点都有 * 企业级应用程序名称 * 。您可以从 StorageGRID 单点登录页面上的管理节点详细信息表复制这些值。

您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

- 您有在 Azure Active Directory 中创建企业级应用程序的经验。
- 您有一个 Azure 帐户且订阅有效。
- 您在 Azure 帐户中具有以下角色之一：全局管理员，云应用程序管理员，应用程序管理员或服务主体的所有者。

访问 **Azure AD**

1. 登录到 "Azure 门户"。
2. 导航到 "Azure Active Directory"。
3. 选择 … "企业级应用程序"。

创建企业级应用程序并保存 **StorageGRID SSO** 配置

要在 StorageGRID 中保存 Azure 的 SSO 配置，您必须使用 Azure 为每个管理节点创建一个企业级应用程序。您将从 Azure 复制联合元数据 URL ，并将其粘贴到 StorageGRID Single Sign-On 页面上对应的 * 联合元数据 URL* 字段中。

1. 对每个管理节点重复以下步骤。
   a. 在 Azure Enterprise 应用程序窗格中，选择 * 新建应用程序 * 。
   b. 选择 * 创建您自己的应用程序 * 。
   c. 对于此名称，请输入您从 StorageGRID Single Sign-On 页面上的管理节点详细信息表中复制的 * 企业应用程序名称 * 。
   d. 保持选中 * 集成在库（非库）中找不到的任何其他应用程序 * 单选按钮。
   e. 选择 * 创建 * 。
   f. 选择 * 。 2.设置单点登录 * 框，或者选择左侧边距中的 * 单点登录 * 链接。
   g. 选择 * SAML * 框。
   h. 复制 * 应用程序联合元数据 URL* ，该 URL 可在 * 步骤 3 SAML 签名证书 * 下找到。
   i. 转到 StorageGRID 单点登录页面，然后将 URL 粘贴到与您使用的 * 企业应用程序名称 * 对应的 * 联合元数据 URL* 字段中。
2. 为每个管理节点粘贴联合元数据 URL 并对 SSO 配置进行所有其他所需更改后，请在 StorageGRID Single Sign-On 页面上选择 * 保存 * 。

下载每个管理节点的 **SAML** 元数据

保存 SSO 配置后，您可以为 StorageGRID 系统中的每个管理节点下载 SAML 元数据文件。

对每个管理节点重复以下步骤：

1. 从管理节点登录到 StorageGRID 。
2. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。

3. 选择按钮以下载此管理节点的 SAML 元数据。
4. 保存要上传到 Azure AD 的文件。

将 **SAML** 元数据上传到每个企业级应用程序

为每个 StorageGRID 管理节点下载 SAML 元数据文件后，在 Azure AD 中执行以下步骤：

1. 返回到 Azure 门户。
2. 对每个企业级应用程序重复以下步骤：

   > 您可能需要刷新 " 企业应用程序 " 页面才能查看先前在列表中添加的应用程序。

   a. 转到企业应用程序的属性页面。
   b. 将 * 需要分配 * 设置为 * 否 * （除非您要单独配置分配）。
   c. 转到单点登录页面。
   d. 完成 SAML 配置。
   e. 选择 * 上传元数据文件 * 按钮，然后选择为相应管理节点下载的 SAML 元数据文件。
   f. 加载文件后，选择 * 保存 * ，然后选择 * X * 以关闭窗格。此时将返回到使用 SAML 设置单点登录页面。
3. 按照中的步骤进行操作 使用沙盒模式 测试每个应用程序。

在 **PingFederate** 中创建服务提供商（ **SP** ）连接

您可以使用 PingFederate 为系统中的每个管理节点创建服务提供商（ SP ）连接。要加快此过程，您需要从 StorageGRID 导入 SAML 元数据。

您需要的内容

- 您已为 StorageGRID 配置单点登录，并选择了 * Ping 联邦 * 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 使用沙盒模式。
- 您拥有系统中每个管理节点的 * SP 连接 ID* 。您可以在 StorageGRID 单点登录页面上的管理节点详细信息表中找到这些值。
- 您已为系统中的每个管理节点下载 * SAML 元数据 * 。
- 您在 PingFederate 服务器中创建 SP 连接的经验。
- 您拥有https://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["《管理员参考指南》"^] PingFederate 服务器。PingFederate 文档提供了详细的分步说明和说明。
- 您具有 PingFederate 服务器的管理员权限。

关于此任务

以下说明总结了如何将 PingFederate 服务器 10.3 版配置为 StorageGRID 的 SSO 提供程序。如果您使用的是其他版本的 PingFederate ，则可能需要调整这些说明。有关您的版本的详细说明，请参见 PingFederate 服务器文档。

完成 **PingFederate** 中的前提条件

在创建要用于 StorageGRID 的 SP 连接之前，必须先在 PingFederate 中完成前提条件任务。配置 SP 连接时，您将使用这些前提条件中的信息。

创建数据存储库**[Data -store]]**

如果尚未创建数据存储库，请将 PingFederate 连接到 AD FS LDAP 服务器。使用您在使用时使用的值 配置身份联合 在 StorageGRID 中。

- * 类型 * ： 目录（ LDAP ）
- * LDAP 类型 * ： Active Directory
- * 二进制属性名称 * ： 在 "LDAP 二进制属性 " 选项卡上输入 * 对象 GUID* ，具体如图所示。

创建密码凭据验证器**[password-validator]]**

如果尚未创建密码凭据验证程序，请创建一个。

- * 类型 * ： LDAP 用户名密码凭据验证器
- * 数据存储 * ： 选择您创建的数据存储。
- * 搜索基础 * ： 输入 LDAP 中的信息（例如， DC=SAML ， DC=sgws ）。
- * 搜索筛选器 * ： sAMAccountName=$ ｛username｝
- * 范围 * ： 子树

创建**IdP**适配器实例**[adapter-instance]]**

如果尚未创建 IdP 适配器实例，请创建此实例。

1. 转至 * 身份验证 * > * 集成 * > * IdP 适配器 * 。
2. 选择 * 创建新实例 * 。
3. 在类型选项卡上，选择 * HTML 表单 IdP 适配器 * 。
4. 在 IdP 适配器选项卡上，选择 * 向 " 凭据验证器 "* 添加新行。
5. 选择 密码凭据验证程序 您已创建。
6. 在适配器属性选项卡上，为 * 伪名称 * 选择 * 用户名 * 属性。
7. 选择 * 保存 * 。

创建或导入签名证书

如果尚未创建，请创建或导入签名证书。

1. 转至 * 安全性 * > * 签名和解密密钥和证书 * 。
2. 创建或导入签名证书。

在 PingFederate 中创建 SP 连接

在 PingFederate 中创建 SP 连接时，您可以导入从 StorageGRID 为管理节点下载的 SAML 元数据。元数据文件包含您需要的许多特定值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接，以便用户可以安全地登录和注销任何节点。按照以下说明创建第一个 SP 连接。然后，转到 创建其他 SP 连接 创建所需的任何其他连接。

选择 SP 连接类型

1. 转至 * 应用程序 * > * 集成 * > * SP 连接 * 。
2. 选择 * 创建连接 * 。
3. 选择 * 不对此连接使用模板 * 。
4. 选择 * 浏览器 SSO 配置文件 * 和 * SAML 2.0* 作为协议。

导入 SP 元数据

1. 在导入元数据选项卡上，选择 * 文件 * 。
2. 选择从管理节点的 StorageGRID 单点登录页面下载的 SAML 元数据文件。
3. 查看元数据摘要以及常规信息选项卡上的信息。

   合作伙伴的实体 ID 和连接名称设置为 StorageGRID SP 连接 ID 。（例如 10.96.105.200-DC1-ADM1-105-200 ）。基本 URL 是 StorageGRID 管理节点的 IP 。
4. 选择 * 下一步 * 。

配置 IdP 浏览器 SSO

1. 从浏览器 SSO 选项卡中，选择 * 配置浏览器 SSO* 。
2. 在 SAML 配置文件选项卡上，选择 * SP 启动的 SSO* ， * SP 初始 SLO* ， * IdP-Initiated SSO* 和 * IdP-Initiated SLO* 选项。
3. 选择 * 下一步 * 。
4. 在 Assertion Lifetime 选项卡上，不进行任何更改。
5. 在断言创建选项卡上，选择 * 配置断言创建 * 。
   a. 在身份映射选项卡上，选择 * 标准 * 。
   b. 在属性合同选项卡上，使用 * SAML 主题 * 作为属性合同以及导入的未指定名称格式。
6. 对于扩展合同，请选择 * 删除 * 以删除未使用的 `urn ： OID` 。

映射适配器实例

1. 在身份验证源映射选项卡上，选择 * 映射新适配器实例 * 。
2. 在适配器实例选项卡上，选择 适配器实例 您已创建。
3. 在映射方法选项卡上，选择 * 从数据存储中检索其他属性 * 。

4. 在属性源和用户查找选项卡上，选择 * 添加属性源 * 。
5. 在数据存储选项卡上，提供问题描述 并选择 数据存储 您已添加。
6. 在 LDAP 目录搜索选项卡上：
   - 输入 * 基本 DN* ，该 DN 应与您在 StorageGRID 中为 LDAP 服务器输入的值完全匹配。
   - 对于搜索范围，请选择 * 子树 * 。
   - 对于根对象类，搜索 * 对象 GUID* 属性并添加它。
7. 在 LDAP 二进制属性编码类型选项卡上，为 * 对象 GUID* 属性选择 * Base64* 。
8. 在 LDAP 筛选器选项卡上，输入 * 。 sAMAccountName=$ ｛username｝ * 。
9. 在属性合同履行选项卡上，从源下拉列表中选择 * LDAP （ attribute ） * ，然后从值下拉列表中选择 * 对象 GUID* 。
10. 查看并保存属性源。
11. 在故障保存属性源选项卡上，选择 * 中止 SSO 事务 * 。
12. 查看摘要并选择 * 完成 * 。
13. 选择 * 完成 * 。

配置协议设置

1. 在 * SP Connection* > * 浏览器 SSO* > * 协议设置 * 选项卡上，选择 * 配置协议设置 * 。
2. 在 Assertion Conset Service URL 选项卡上，接受从 StorageGRID SAML 元数据导入的默认值（对于绑定，为 * 后 * ；对于端点 URL ，为 ` /API/SAML 响应` ）。
3. 在 SLO 服务 URL 选项卡上，接受从 StorageGRID SAML 元数据导入的默认值（ * 重定向 * 表示绑定， ` /API/SAML 注销` 表示端点 URL 。
4. 在允许的 SAML 绑定选项卡上，取消选择 * 项目 * 和 * SOAP * 。仅需要 * 发布 * 和 * 重定向 * 。
5. 在签名策略选项卡上，保持选中 * 需要对 Authn 请求签名 * 和 * 始终对断言签名 * 复选框。
6. 在加密策略选项卡上，选择 * 无 * 。
7. 查看摘要并选择 * 完成 * 以保存协议设置。
8. 查看摘要并选择 * 完成 * 以保存浏览器 SSO 设置。

配置凭据

1. 从 SP 连接选项卡中，选择 * 凭据 * 。
2. 从凭据选项卡中，选择 * 配置凭据 * 。
3. 选择 正在签名证书 您已创建或导入。
4. 选择 * 下一步 * 转到 * 管理签名验证设置 * 。
   a. 在信任模式选项卡上，选择 * 已取消锁定 * 。
   b. 在签名验证证书选项卡上，查看从 StorageGRID SAML 元数据导入的签名证书信息。
5. 查看摘要屏幕并选择 * 保存 * 以保存 SP 连接。

创建其他 SP 连接

您可以复制第一个 SP 连接，以便为网格中的每个管理节点创建所需的 SP 连接。您可以为每个副本上传新元数据。

不同管理节点的 SP 连接使用相同的设置，但合作伙伴的实体 ID ，基本 URL ，连接 ID ，连接名称，签名验证除外。 和 SLO 响应 URL 。

1. 选择 * 操作 * > * 复制 * 为每个附加管理节点创建初始 SP 连接的副本。
2. 输入副本的连接 ID 和连接名称，然后选择 * 保存 * 。
3. 选择与管理节点对应的元数据文件：
   a. 选择 * 操作 * > * 使用元数据更新 * 。
   b. 选择 * 选择文件 * 并上传元数据。
   c. 选择 * 下一步 * 。
   d. 选择 * 保存 * 。
4. 解决由于属性未使用而导致的错误：
   a. 选择新连接。
   b. 选择 * 配置浏览器 SSO > 配置断言创建 > 属性合同 * 。
   c. 删除 * urn ： oid* 的条目。
   d. 选择 * 保存 * 。

禁用单点登录

如果您不再希望使用单点登录（ SSO ）功能，则可以禁用此功能。必须先禁用单点登录，然后才能禁用身份联合。

您需要的内容

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

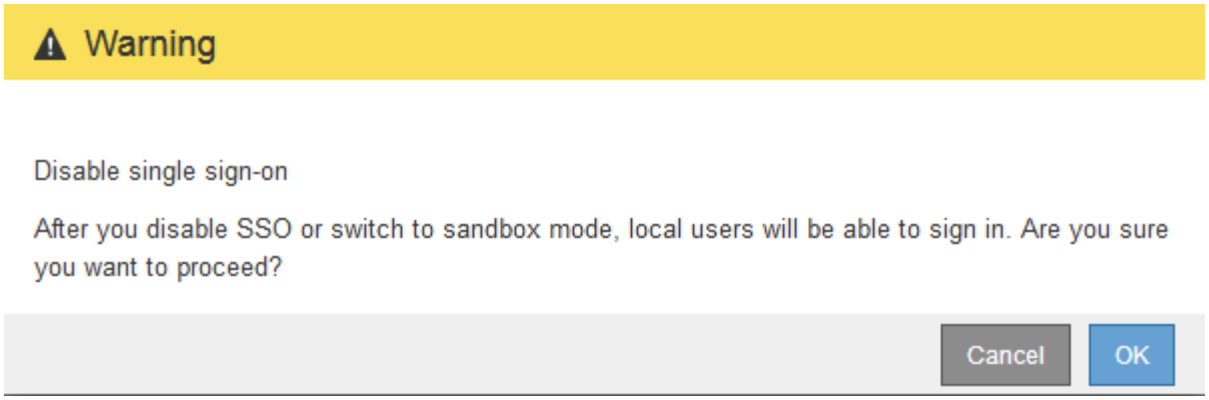
步骤

1. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。

   此时将显示 Single Sign-On 页面。

2. 选择 * 已禁用 * 选项。
3. 选择 * 保存 * 。

   此时将显示一条警告消息，指示本地用户现在可以登录。



4. 选择 * 确定 * 。

   下次登录到 StorageGRID 时，将显示 StorageGRID 登录页面，您必须输入本地或联合 StorageGRID 用户的用户名和密码。

临时禁用并重新启用一个管理节点的单点登录

如果单点登录（ Single Sign-On ， SSO ）系统发生故障，您可能无法登录到网格管理器。在这种情况下，您可以为一个管理节点临时禁用并重新启用 SSO 。要禁用并重新启用 SSO ，必须访问节点的命令 Shell 。

您需要的内容

- 您具有特定的访问权限。
- 您已有 `passwords.txt` 文件。
- 您知道本地 root 用户的密码。

关于此任务

为一个管理节点禁用 SSO 后，您可以以本地 root 用户身份登录到网格管理器。要保护 StorageGRID 系统的安全，您必须在注销后立即使用节点的命令 Shell 在管理节点上重新启用 SSO 。

> 为一个管理节点禁用 SSO 不会影响网格中任何其他管理节点的 SSO 设置。网格管理器的单点登录页面上的 * 启用 SSO* 复选框将保持选中状态，并且所有现有的 SSO 设置都将保持不变，除非您对其进行更新。

步骤

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

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 运行以下命令：`disable-SAML`

此时将显示一条消息，指出命令适用场景 this Admin Node only 。

3. 确认要禁用 SSO 。

   显示一条消息，指示节点上已禁用单点登录。

4. 从 Web 浏览器访问同一管理节点上的网格管理器。

   现在，由于已禁用 SSO ，将显示网格管理器登录页面。

5. 使用用户名 root 和本地 root 用户的密码登录。
6. 如果您因需要更正 SSO 配置而临时禁用 SSO ：
   a. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   b. 更改不正确或过时的 SSO 设置。
   c. 选择 * 保存 * 。

      从 Single Sign-On 页面选择 * 保存 * 会自动为整个网格重新启用 SSO 。

7. 如果您因某些其他原因需要访问网格管理器而临时禁用 SSO ：
   a. 执行需要执行的任何任务。
   b. 选择 * 注销 * ，然后关闭网格管理器。
   c. 在管理节点上重新启用 SSO 。您可以执行以下任一步骤：

      - 运行以下命令： `enable-SAML`

        此时将显示一条消息，指出命令适用场景 this Admin Node only 。

      确认要启用 SSO 。

   显示一条消息，指示节点上已启用单点登录。

   ◦ 重新启动网格节点： `reboot`
8. 从 Web 浏览器中，从同一管理节点访问网格管理器。
9. 确认此时将显示 StorageGRID 登录页面，并且您必须输入 SSO 凭据才能访问网格管理器。

管理安全设置

管理证书

关于安全证书

安全证书是一个小型数据文件，用于在 StorageGRID 组件之间以及 StorageGRID 组件与外部系统之间创建安全可信的连接。

StorageGRID 使用两种类型的安全证书：

- 使用 HTTPS 连接时需要 * 服务器证书 * 。服务器证书用于在客户端和服务器之间建立安全连接，向客户端验证服务器的身份并为数据提供安全通信路径。服务器和客户端都有一个证书副本。
- * 客户端证书 * 可对服务器的客户端或用户身份进行身份验证，从而提供比单独使用密码更安全的身份验证。客户端证书不会对数据进行加密。

当客户端使用 HTTPS 连接到服务器时，服务器会使用包含公有 密钥的服务器证书进行响应。客户端通过将服务器签名与其证书副本上的签名进行比较来验证此证书。如果签名匹配，则客户端将使用相同的公有 密钥启动与服务器的会话。

StorageGRID 用作某些连接的服务器（例如负载平衡器端点）或其他连接的客户端（例如 CloudMirror 复制服务）。

- 默认网格 CA 证书 *

StorageGRID 包含一个内置证书颁发机构（ Certificate Authority ， CA ），可在系统安装期间生成内部网格 CA 证书。默认情况下，使用网格 CA 证书保护内部 StorageGRID 流量。外部证书颁发机构（ CA ）可以对完全符合组织信息安全策略的自定义证书进行问题描述 。虽然您可以在非生产环境中使用网格 CA 证书，但在生产环境中，最佳做法是使用由外部证书颁发机构签名的自定义证书。此外，还支持无证书的不安全连接，但不建议这样做。

- 自定义 CA 证书不会删除内部证书；但是，自定义证书应是为验证服务器连接而指定的证书。
- 所有自定义证书都必须满足 系统强化准则 服务器证书。
- StorageGRID 支持将 CA 中的证书捆绑到一个文件中（称为 CA 证书包）。

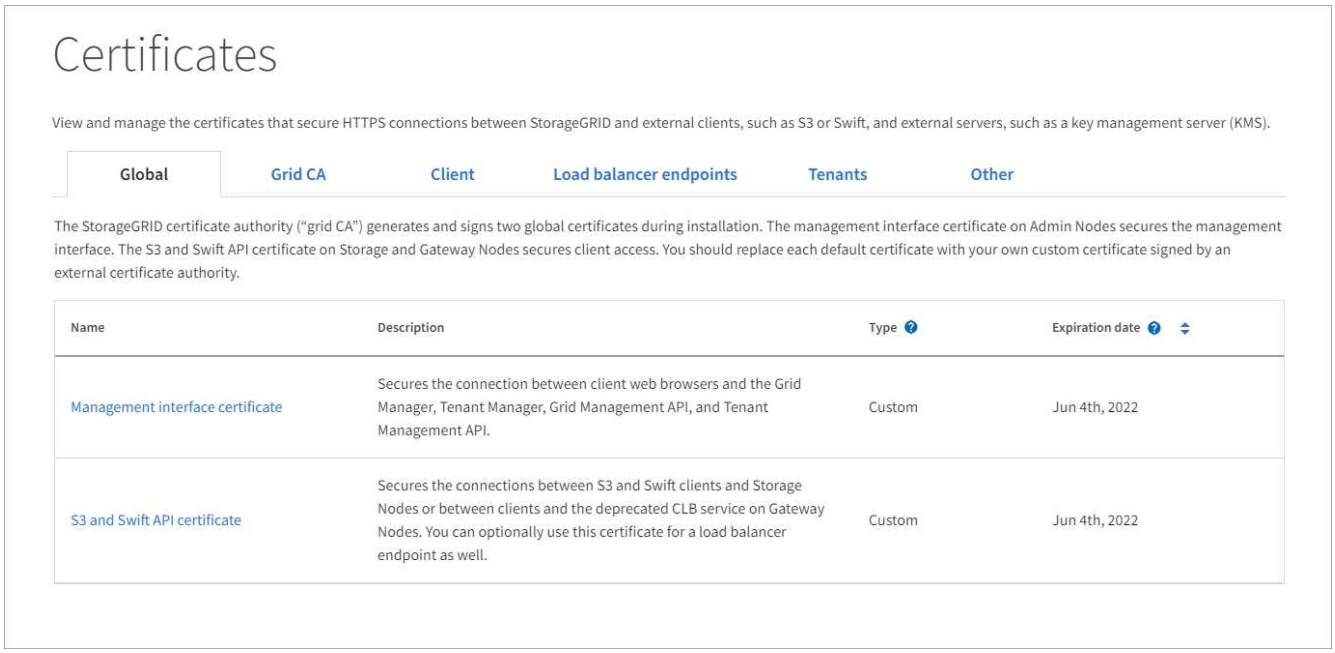
> StorageGRID 还包括在所有网格上相同的操作系统 CA 证书。在生产环境中，请确保指定一个由外部证书颁发机构签名的自定义证书，以替代操作系统 CA 证书。

服务器和客户端证书类型的变体通过多种方式实现。在配置系统之前，您应准备好特定 StorageGRID 配置所需的所有证书。

访问安全证书

您可以在一个位置访问有关所有 StorageGRID 证书的信息，以及指向每个证书的配置工作流的链接。

1. 在 Grid Manager 中，选择 * 配置 * > * 安全性 * > * 证书 * 。



2. 在证书页面上选择一个选项卡，以获取有关每个证书类别的信息并访问证书设置。只有在拥有相应权限的情况下，才能访问选项卡。

   - * 全局 * ： 确保从 Web 浏览器和外部 API 客户端访问 StorageGRID 的安全。
   - * 网格 CA* ： 保护内部 StorageGRID 流量的安全。
   - * 客户端 * ： 保护外部客户端与 StorageGRID Prometheus 数据库之间的连接。
   - * 负载平衡器端点 * ： 确保 S3 和 Swift 客户端与 StorageGRID 负载平衡器之间的连接安全。
   - * 租户 * ： 保护与身份联合服务器或从平台服务端点到 S3 存储资源的连接。
   - * 其他 * ： 保护需要特定证书的 StorageGRID 连接。

   下面介绍了每个选项卡，并提供了指向其他证书详细信息的链接。

全局

这些全局证书可确保从 Web 浏览器以及外部 S3 和 Swift API 客户端访问 StorageGRID 的安全。在安装期间， StorageGRID 证书颁发机构最初会生成两个全局证书。生产环境的最佳实践是使用由外部证书颁发机构签名的自定义证书。

- [管理接口证书]：确保客户端 Web 浏览器与 StorageGRID 管理界面的连接安全。
- S3 和 Swift API 证书：保护与存储节点，管理节点和网关节点的客户端 API 连接的安全， S3 和 Swift 客户端应用程序使用这些连接上传和下载对象数据。

有关已安装的全局证书的信息包括：

- * 名称 *：证书名称，其中包含用于管理证书的链接。
- * 问题描述 *
- * 类型 *：自定义或默认。+ 为了提高网格安全性，您应始终使用自定义证书。
- * 到期日期 *：如果使用默认证书，则不会显示到期日期。

您可以

- 将默认证书替换为由外部证书颁发机构签名的自定义证书，以提高网格安全性：
  - 替换由 StorageGRID 生成的默认管理接口证书 用于网格管理器和租户管理器连接。
  - 替换 S3 和 Swift API 证书 用于存储节点， CLB 服务（已弃用）和负载平衡器端点（可选）连接。
- 还原默认管理接口证书。
- 还原默认 S3 和 Swift API 证书。
- 使用脚本生成新的自签名管理接口证书。
- 复制或下载 管理接口证书 或 S3 和 Swift API 证书。

网格 **CA**

。 网格 CA 证书由 StorageGRID 证书颁发机构在 StorageGRID 安装期间生成，可保护所有内部 StorageGRID 流量。

证书信息包括证书到期日期和证书内容。

您可以 复制或下载网格 CA 证书，但您无法更改它。

客户端

客户端证书由外部证书颁发机构生成，用于保护外部监控工具与 StorageGRID Prometheus 数据库之间的连接。

证书表中的每个已配置客户端证书都有一行，用于指示此证书是否可用于 Prometheus 数据库访问以及证书到期日期。

您可以

- 上传或生成新的客户端证书。
- 选择一个证书名称以显示证书详细信息，您可以在其中执行以下操作：

- 更改客户端证书名称。
- 设置 Prometheus 访问权限。
- 上传并替换客户端证书。
- 复制或下载客户端证书。
- 删除客户端证书。

- 选择 * 操作 * 以快速执行 编辑， 附加或 删除 客户端证书。您最多可以选择 10 个客户端证书，并使用 * 操作 * > * 删除 * 一次删除这些证书。

负载平衡器端点

负载平衡器端点证书上载或生成的，用于保护 S3 和 Swift 客户端之间的连接以及网关节点和管理节点上的 StorageGRID 负载平衡器服务。

负载平衡器端点表对每个已配置的负载平衡器端点都有一行，用于指示此端点是否使用全局 S3 和 Swift API 证书或自定义负载平衡器端点证书。此外，还会显示每个证书的到期日期。

对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

您可以

- 选择一个端点名称以打开一个浏览器选项卡，其中包含有关负载平衡器端点的信息，包括其证书详细信息。
- 为 FabricPool 指定负载平衡器端点证书。
- 使用全局 S3 和 Swift API 证书 而不是生成新的负载平衡器端点证书。

Tenants

租户可以使用 身份联合服务器证书 或 平台服务端点证书 以确保其与 StorageGRID 的连接安全。

租户表中的每个租户都有一行，用于指示每个租户是否有权使用自己的身份源或平台服务。

您可以

- 选择一个租户名称以登录到租户管理器
- 选择租户名称以查看租户身份联合详细信息
- 选择租户名称以查看租户平台服务详细信息
- 在创建端点期间指定平台服务端点证书

其他

StorageGRID 会将其他安全证书用于特定目的。这些证书按其功能名称列出。其他安全证书包括：

- 身份联合证书
- 云存储池证书
- 密钥管理服务器（ KMS ）证书
- 单点登录证书
- 通过电子邮件发送警报通知证书

- 外部系统日志服务器证书

信息指示函数使用的证书类型及其服务器和客户端证书的到期日期（如果适用）。选择功能名称将打开一个浏览器选项卡，您可以在此查看和编辑证书详细信息。

只有在拥有相应权限的情况下，才能查看和访问其他证书的信息。

您可以

- 查看和编辑身份联合证书
- 上传密钥管理服务器（ KMS ）服务器和客户端证书
- 为 S3 ， C2S S3 或 Azure 指定云存储池证书
- 手动为依赖方信任指定 SSO 证书
- 指定警报电子邮件通知的证书
- 指定外部系统日志服务器证书

安全证书详细信息

下面介绍了每种类型的安全证书，并提供了指向包含实施说明的文章的链接。

管理接口证书

证书类型	**Description**	导航位置	详细信息
服务器	对客户端 Web 浏览器和 StorageGRID 管理界面之间的连接进行身份验证，使用户能够访问网格管理器和租户管理器，而不会出现安全警告。 此证书还会对网格管理 API 和租户管理 API 连接进行身份验证。 您可以使用安装期间创建的默认证书，也可以上传自定义证书。	• 配置 * > * 安全性 * > * 证书 * ，选择 * 全局 * 选项卡，然后选择 * 管理接口证书 *	配置管理接口证书

S3 和 **Swift API** 证书

证书类型	Description	导航位置	详细信息
服务器	对与存储节点，网关节点上已弃用的连接负载平衡器（ CLB ）服务以及负载平衡器端点（可选）的安全 S3 或 Swift 客户端连接进行身份验证。	• 配置 * > * 安全性 * > * 证书 * ，选择 * 全局 * 选项卡，然后选择 * S3 和 Swift API 证书 *	配置 S3 和 Swift API 证书

网格 **CA** 证书

请参见 默认网格 CA 证书问题描述。

管理员客户端证书

证书类型	Description	导航位置	详细信息
客户端	安装在每个客户端上，使 StorageGRID 能够对外部客户端访问进行身份验证。 • 允许授权的外部客户端访问 StorageGRID Prometheus 数据库。 • 允许使用外部工具安全监控 StorageGRID 。	• 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡	配置客户端证书

负载平衡器端点证书

证书类型	Description	导航位置	详细信息
服务器	对 S3 或 Swift 客户端与网关节点和管理节点上的 StorageGRID 负载平衡器服务之间的连接进行身份验证。您可以在配置负载平衡器端点时上传或生成负载平衡器证书。客户端应用程序在连接到 StorageGRID 时使用负载平衡器证书来保存和检索对象数据。 您也可以使用自定义版本的全局 S3 和 Swift API 证书 用于对与负载平衡器服务的连接进行身份验证的证书。如果使用全局证书对负载平衡器连接进行身份验证，则无需为每个负载平衡器端点上传或生成单独的证书。 • 注意： * 用于负载平衡器身份验证的证书是正常 StorageGRID 操作期间使用量最多的证书。	• 配置 * > * 网络 * > * 负载平衡器端点 *	• 配置负载平衡器端点 • 为 FabricPool 创建负载平衡器端点

身份联合证书

证书类型	Description	导航位置	详细信息
服务器	对 StorageGRID 与外部身份提供程序（例如 Active Directory ， OpenLDAP 或 Oracle 目录服务器）之间的连接进行身份验证。用于身份联合，允许管理组和用户由外部系统管理。	• 配置 * > * 访问控制 * > * 身份联合 *	使用身份联合

平台服务端点证书

证书类型	Description	导航位置	详细信息
服务器	对从 StorageGRID 平台服务到 S3 存储资源的连接进行身份验证。	• 租户管理器 * > * 存储（ S3 ） * > * 平台服务端点 *	创建平台服务端点 编辑平台服务端点

云存储池端点证书

证书类型	Description	导航位置	详细信息
服务器	对从 StorageGRID 云存储池到外部存储位置（例如 S3 Glacier 或 Microsoft Azure Blob 存储）的连接进行身份验证。每种云提供商类型都需要一个不同的证书。	• ILM * > * 存储池 *	创建云存储池

密钥管理服务器（ **KMS** ）证书

证书类型	Description	导航位置	详细信息
服务器和客户端	对 StorageGRID 与外部密钥管理服务器（ KMS ）之间的连接进行身份验证，该服务器可为 StorageGRID 设备节点提供加密密钥。	• 配置 * > * 安全性 * > * 密钥管理服务器 *	添加密钥管理服务器（ KMS ）

单点登录（ **SSO** ）证书

证书类型	Description	导航位置	详细信息
服务器	对身份联合服务（例如 Active Directory 联合身份验证服务（ AD FS ））与用于单点登录（ SSO ）请求的 StorageGRID 之间的连接进行身份验证。	• 配置 * > * 访问控制 * > * 单点登录 *	配置单点登录

通过电子邮件发送警报通知证书

证书类型	Description	导航位置	详细信息
服务器和客户端	对 SMTP 电子邮件服务器与用于警报通知的 StorageGRID 之间的连接进行身份验证。 • 如果与 SMTP 服务器的通信需要传输层安全（ Transport Layer Security ， TLS ），则必须指定电子邮件服务器 CA 证书。 • 仅当 SMTP 电子邮件服务器需要客户端证书进行身份验证时，才指定客户端证书。	• 警报 * > * 电子邮件设置 *	为警报设置电子邮件通知

外部系统日志服务器证书

证书类型	Description	导航位置	详细信息
服务器	对在 StorageGRID 中记录事件的外部系统日志服务器之间的 TLS 或 RELP/TLS 连接进行身份验证。 • 注： * 与外部系统日志服务器的 TCP ， RELP/TCP 和 UDP 连接不需要外部系统日志服务器证书。	• 配置 * > * 监控 * > * 审核和系统日志服务器 * ，然后选择 * 配置外部系统日志服务器 *	配置外部系统日志服务器

证书示例

示例 **1** ： 负载平衡器服务

在此示例中， StorageGRID 充当服务器。

1. 您可以在 StorageGRID 中配置负载平衡器端点并上传或生成服务器证书。
2. 您可以配置与负载平衡器端点的 S3 或 Swift 客户端连接，并将同一证书上传到客户端。
3. 当客户端要保存或检索数据时，它会使用 HTTPS 连接到负载平衡器端点。
4. StorageGRID 会使用包含公有 密钥的服务器证书进行响应，并使用基于私钥的签名进行响应。
5. 客户端通过将服务器签名与其证书副本上的签名进行比较来验证此证书。如果签名匹配，客户端将使用相同的公有 密钥启动会话。
6. 客户端将对象数据发送到 StorageGRID 。

示例 **2** ： 外部密钥管理服务器（ **KMS** ）

在此示例中， StorageGRID 充当客户端。

1. 您可以使用外部密钥管理服务器软件将 StorageGRID 配置为 KMS 客户端，并获取 CA 签名的服务器证书，公有 客户端证书以及客户端证书的专用密钥。
2. 使用网格管理器，您可以配置 KMS 服务器并上传服务器和客户端证书以及客户端专用密钥。
3. 当 StorageGRID 节点需要加密密钥时，它会向 KMS 服务器发出请求，请求包含证书中的数据以及基于私钥的签名。
4. KMS 服务器会验证证书签名，并决定它可以信任 StorageGRID 。
5. KMS 服务器使用经过验证的连接进行响应。

配置服务器证书

支持的服务器证书类型

StorageGRID 系统支持使用 RSA 或 ECDSA （椭圆曲线数字签名算法）加密的自定义证书。

有关 StorageGRID 如何为 REST API 保护客户端连接的详细信息，请参见 使用 S3 或 使用 Swift。

配置管理接口证书

您可以将默认管理接口证书替换为一个自定义证书，使用户可以访问 Grid Manager 和租户管理器，而不会遇到安全警告。您还可以还原到默认管理接口证书或生成新的管理接口证书。

关于此任务

默认情况下，每个管理节点都会获得一个由网格 CA 签名的证书。这些 CA 签名的证书可以替换为一个通用的自定义管理接口证书和相应的专用密钥。

由于所有管理节点都使用一个自定义管理接口证书，因此，如果客户端在连接到网格管理器和租户管理器时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有管理节点匹配。

您需要在服务器上完成配置，根据所使用的根证书颁发机构（ CA ），用户可能还需要在用于访问网格管理器和租户管理器的 Web 浏览器中安装网格 CA 证书。

为了确保操作不会因服务器证书失败而中断，当此服务器证书即将到期时，将触发 * 管理接口的服务器证书到期 * 警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在全局选项卡上查看管理接口证书的到期日期来查看当前证书的到期时间。

如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：

- 您的自定义管理接口证书将过期。
- 您 从自定义管理接口证书还原到默认服务器证书。

添加自定义管理接口证书

要添加自定义管理接口证书，您可以提供自己的证书或使用网格管理器生成一个证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - * 证书专用密钥 * ： 自定义服务器证书专用密钥文件（` 。 key` ）。

     EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

     例如： `storagegRid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

生成证书

生成服务器证书文件。

生产环境的最佳实践是使用由外部证书颁发机构签名的自定义管理接口证书。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

   - * 域名 * ： 要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
   - * IP * ： 要包含在证书中的一个或多个 IP 地址。
   - * 主题 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
   - * 有效天数 * ： 创建证书后的天数到期。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

例如： `storagegRid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

5. 刷新页面以确保 Web 浏览器已更新。

上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 添加自定义管理接口证书后， " 管理接口证书 " 页面将显示正在使用的证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认管理接口证书

您可以使用网格管理器和租户管理器连接的默认管理接口证书还原到。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用默认证书 * 。

   还原默认管理接口证书时，您配置的自定义服务器证书文件将被删除，无法从系统中恢复。默认管理接口证书将用于所有后续的新客户端连接。

4. 刷新页面以确保 Web 浏览器已更新。

使用脚本生成新的自签名管理接口证书

如果需要严格验证主机名，可以使用脚本生成管理接口证书。

您需要的内容

- 您具有特定的访问权限。
- 您已有 `passwords.txt` 文件。

关于此任务

生产环境的最佳实践是使用由外部证书颁发机构签名的证书。

步骤

1. 获取每个管理节点的完全限定域名（ FQDN ）。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

3. 使用新的自签名证书配置 StorageGRID 。

` $sudo make-certificate -domains *wilder-admin-node-fqdn* -type management`

- 对于 ` 域` ，请使用通配符表示所有管理节点的完全限定域名。例如， ` * .ui.storagegrid.example.com` 使用 * 通配符表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com` 。
- 将 ` 键入` 设置为 `management` 以配置管理接口证书，网格管理器和租户管理器将使用该证书。
- 默认情况下，生成的证书有效期为一年（ 365 天），必须在证书过期之前重新创建。您可以使用 ` -days` 参数覆盖默认有效期。

> 运行 `make-certificate` 时，证书的有效期开始。您必须确保管理客户端与 StorageGRID 同步到同一个时间源；否则，客户端可能会拒绝此证书。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

生成的输出包含管理 API 客户端所需的公有 证书。

4. 选择并复制证书。

在您的选择中包括开始和结束标记。

5. 从命令 Shell 中注销。` $ 退出`
6. 确认已配置证书：
   a. 访问网格管理器。
   b. 选择 * 配置 * > * 安全性 * > * 证书 *
   c. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
7. 将管理客户端配置为使用您复制的公有 证书。包括开始和结束标记。

下载或复制管理接口证书

您可以保存或复制管理接口证书内容，以便在其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或 CA 捆绑包 ` .pem` 文件。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

   例如： `storagegRid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存扩展名为 ` .pem` 的文本文件。

   例如： `storagegRid_certificate.pem`

配置 **S3** 和 **Swift API** 证书

您可以替换或还原用于通过 S3 或 Swift 客户端连接到存储节点，网关节点上已弃用的连接负载平衡器（ CLB ）服务或负载平衡器端点的服务器证书。替换的自定义服务器证书特定于您的组织。

关于此任务

默认情况下，每个存储节点都会获得一个由网格 CA 签名的 X.509 服务器证书。这些 CA 签名的证书可以替换为一个通用的自定义服务器证书和相应的专用密钥。

所有存储节点都使用一个自定义服务器证书，因此，如果客户端在连接到存储端点时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有存储节点匹配。

在服务器上完成配置后，您可能还需要在用于访问系统的 S3 或 Swift API 客户端中安装网格 CA 证书，具体取决于您正在使用的根证书颁发机构（ CA ）。

> 为了确保操作不会因服务器证书失败而中断，根服务器证书即将过期时会触发 * S3 和 Swift APi* 全局服务器证书到期警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在全局选项卡上查看 S3 和 Swift API 证书的到期日期来查看当前证书的到期时间。

您可以上传或生成自定义 S3 和 Swift API 证书。

添加自定义 **S3** 和 **Swift API** 证书

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - * 证书专用密钥 * ： 自定义服务器证书专用密钥文件（` 。 key` ）。

     EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 选择证书详细信息以显示上传的每个自定义 S3 和 Swift API 证书的元数据和 PEM 。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

     例如： `storagegRid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 保存 * 。

   自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

生成证书

生成服务器证书文件。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

   - * 域名 * ： 要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
   - * IP * ： 要包含在证书中的一个或多个 IP 地址。
   - * 主题 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
   - * 有效天数 * ： 创建证书后的天数到期。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可显示生成的自定义 S3 和 Swift API 证书的元数据和 PEM 。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

     例如： `storagegRid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。

自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

5. 选择一个选项卡以显示默认 StorageGRID 服务器证书，已上传的 CA 签名证书或已生成的自定义证书的元数据。

上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 刷新页面以确保 Web 浏览器已更新。
7. 添加自定义 S3 和 Swift API 证书后， S3 和 Swift API 证书页面将显示正在使用的自定义 S3 和 Swift API 证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认 **S3** 和 **Swift API** 证书

对于 S3 和 Swift 客户端与存储节点的连接以及网关节点上已弃用的 CLB 服务，您可以还原为使用默认 S3 和 Swift API 证书。但是，您不能对负载平衡器端点使用默认 S3 和 Swift API 证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 使用默认证书 * 。

还原全局 S3 和 Swift API 证书的默认版本时，您配置的自定义服务器证书文件将被删除，无法从系统中恢复。默认的 S3 和 Swift API 证书将用于以后与存储节点以及网关节点上已弃用的 CLB 服务建立的新 S3 和 Swift 客户端连接。

4. 选择 * 确定 * 确认警告并还原默认 S3 和 Swift API 证书。

如果您拥有根访问权限，并且自定义 S3 和 Swift API 证书用于负载平衡器端点连接，则会显示一个负载平衡器端点列表，这些端点将无法再使用默认 S3 和 Swift API 证书进行访问。转至 配置负载平衡器端点 编辑或删除受影响的端点。

5. 刷新页面以确保 Web 浏览器已更新。

下载或复制 **S3** 和 **Swift API** 证书

您可以保存或复制 S3 和 Swift API 证书内容，以便在其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或 CA 捆绑包 ` .pem` 文件。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

   例如： `storagegRid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存扩展名为 ` .pem` 的文本文件。

   例如： `storagegRid_certificate.pem`

相关信息

- 使用 S3
- 使用 Swift
- 配置 S3 API 端点域名

复制网格 **CA** 证书

StorageGRID 使用内部证书颁发机构（ CA ）来保护内部流量。如果您上传自己的证书，则此证书不会更改。

您需要的内容

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

关于此任务

如果配置了自定义服务器证书，则客户端应用程序应使用自定义服务器证书验证服务器。他们不应从 StorageGRID 系统复制 CA 证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 网格 CA* 选项卡。

2. 在 * 证书 PEM* 部分中，下载或复制证书。

下载证书文件

下载证书 ` .pem` 文件。

a. 选择 * 下载证书 * 。

b. 指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

例如： `storagegRid_certificate.pem`

复制证书 **PEM**

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存扩展名为 ` .pem` 的文本文件。

例如： `storagegRid_certificate.pem`

为 **FabricPool** 配置 **StorageGRID** 证书

对于执行严格主机名验证且不支持禁用严格主机名验证的 S3 客户端，例如使用 FabricPool 的 ONTAP 客户端，您可以在配置负载平衡器端点时生成或上传服务器证书。

您需要的内容

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

关于此任务

创建负载平衡器端点时，您可以生成自签名服务器证书或上传由已知证书颁发机构（ CA ）签名的证书。在生产环境中，您应使用由已知 CA 签名的证书。由 CA 签名的证书可以无中断地轮换。它们也更安全，因为它们可以更好地防止中间人攻击。

以下步骤为使用 FabricPool 的 S3 客户端提供了一般准则。有关更多详细信息和过程，请参见 为 FabricPool 配置 StorageGRID。

网关节点上的单独连接负载平衡器（ CLB ）服务已弃用，不建议用于 FabricPool 。

步骤

1. （可选）配置一个高可用性（ High Availability ， HA ）组以供 FabricPool 使用。
2. 创建 S3 负载平衡器端点以供 FabricPool 使用。

创建 HTTPS 负载平衡器端点时，系统会提示您上传服务器证书，证书专用密钥和可选的 CA 捆绑包。

3. 在 ONTAP 中将 StorageGRID 附加为云层。

   指定负载平衡器端点端口以及上载的 CA 证书中使用的完全限定域名。然后，提供 CA 证书。

   如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。

配置客户端证书

客户端证书允许授权的外部客户端访问 StorageGRID Prometheus 数据库，从而为外部工具监控 StorageGRID 提供了一种安全的方式。

如果您需要使用外部监控工具访问StorageGRID 、则必须使用网格管理器上传或生成客户端证书、并将证书信息复制到外部工具。

请参见有关的信息 常规安全证书用途 和 配置自定义服务器证书。

为了确保操作不会因服务器证书失败而中断，当此服务器证书即将到期时，系统将触发 " 证书 " 页面上配置的 * 客户端证书到期 " 警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在客户端选项卡上查看客户端证书的到期日期来查看当前证书的到期时间。

如果您使用密钥管理服务器（ KMS ）保护专门配置的设备节点上的数据，请参见有关的特定信息 上传 KMS 客户端证书。

您需要的内容

- 您具有 root 访问权限。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 配置客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 如果已配置StorageGRID 管理接口证书、则可以使用CA、客户端证书和专用密钥来配置管理接口证书。
  - 要上传您自己的证书、您的本地计算机上提供了证书的专用密钥。
  - 私钥必须在创建时已保存或记录。如果您没有原始私钥、则必须创建一个新的私钥。
- 编辑客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 要上传您自己的证书或新证书、您的本地计算机上提供了私钥、客户端证书和CA (如果使用)。

添加客户端证书

按照适用于您的场景的操作步骤 添加客户端证书：

- [已配置管理接口证书]
- CA颁发的客户端证书
- [从网格管理器生成的证书]

已配置管理接口证书

如果已使用客户提供的CA、客户端证书和专用密钥配置管理接口证书、请使用此操作步骤 添加客户端证书。

步骤

1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择 * 添加 * 。
3. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
5. 在*证书类型*部分中、上传管理接口证书`.pem`文件。
   a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
   b. 上传管理接口证书文件(`.pem`)。
      - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
      - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   c. 选择 * 创建 * 以在网格管理器中保存证书。

      新证书将显示在客户端选项卡上。
6. 在外部监控工具上配置以下设置，例如 Grafana 。
   a. * 名称 * ： 输入连接的名称。

      StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。
   b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

      例如： `+ https://admin-node.example.com:9091+`
   c. 启用 * TLS 客户端身份验证 * 和 * 使用 CA 证书 * 。
   d. 在TLS/SSL身份验证详细信息下、复制并粘贴：+
      - 管理接口CA证书到"** CA证书"
      - 到"Client Cert"的客户端证书
      - "**客户端密钥"的专用密钥
   e. * 服务器名称 * ： 输入管理节点的域名。

      servername 必须与管理接口证书中显示的域名匹配。
   f. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

      现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

有关指标的信息，请参见 有关监控 StorageGRID 的说明。

CA颁发的客户端证书

如果未配置管理接口证书、并且您计划为使用CA颁发的客户端证书和专用密钥的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 执行步骤至 配置管理接口证书。
2. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
3. 选择 * 添加 * 。
4. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
6. 在*证书类型*部分中、上传客户端证书、私钥和CA捆绑包`.pem` files：
   a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
   b. 上传客户端证书、私钥和CA捆绑包文件(`.pem`)。
      - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
      - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   c. 选择 * 创建 * 以在网格管理器中保存证书。

      新证书将显示在客户端选项卡上。
7. 在外部监控工具上配置以下设置，例如 Grafana 。
   a. * 名称 * ： 输入连接的名称。

      StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。
   b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

      例如： ` + https://admin-node.example.com:9091+`
   c. 启用 * TLS 客户端身份验证 * 和 * 使用 CA 证书 * 。
   d. 在TLS/SSL身份验证详细信息下、复制并粘贴：+
      - 管理接口CA证书到"** CA证书"
      - 到"Client Cert"的客户端证书
      - "**客户端密钥"的专用密钥
   e. * 服务器名称 * ： 输入管理节点的域名。

      servername 必须与管理接口证书中显示的域名匹配。
   f. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

      现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

有关指标的信息，请参见 有关监控 StorageGRID 的说明。

从网格管理器生成的证书

如果未配置管理接口证书、并且您计划为使用网格管理器中的生成证书功能的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择 * 添加 * 。
3. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
5. 在*证书类型*部分中、选择*生成证书*。
6. 指定证书信息：
   - 域名：要包含在证书中的管理节点的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
   - * IP：要包含在证书中的一个或多个管理节点IP地址。
   - * 主题 * ：证书所有者的 X.509 主题或可分辨名称（ DN ）。
7. 选择 * 生成 * 。
8. 【客户端证书详细信息】选择*客户端证书详细信息*可显示证书元数据和证书PEM。

   关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

   例如： `storagegRid_certificate.pem`

   - 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
   - 选择 * 下载私钥 * 将私钥另存为文件。

     指定私钥文件名和下载位置。

9. 选择 * 创建 * 以在网格管理器中保存证书。

   新证书将显示在客户端选项卡上。

10. 在网格管理器中、选择*配置*>*安全性*>*证书*、然后选择*全局*选项卡。
11. 选择*管理接口证书*。
12. 选择 * 使用自定义证书 * 。
13. 从上传certificate.pem和private_key.pem文件 客户端证书详细信息 步骤。无需上传CA捆绑包。
    a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
    b. 上传每个证书文件(`.pem`)。

c. 选择 * 创建 * 以在网格管理器中保存证书。

新证书将显示在客户端选项卡上。

14. 在外部监控工具上配置以下设置，例如 Grafana 。

a. * 名称 * ： 输入连接的名称。

StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。

b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

例如： ` + https://admin-node.example.com:9091+`

c. 启用 * TLS 客户端身份验证 * 和 * 使用 CA 证书 * 。

d. 在TLS/SSL身份验证详细信息下、复制并粘贴：+

- 管理接口客户端证书同时提供给"**CA**证书"和"客户端证书"
- "**客户端密钥"的专用密钥

e. * 服务器名称 * ： 输入管理节点的域名。

servername 必须与管理接口证书中显示的域名匹配。

f. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

有关指标的信息，请参见 有关监控 StorageGRID 的说明。

编辑客户端证书

您可以编辑管理员客户端证书以更改其名称，启用或禁用 Prometheus 访问，或者在当前证书已过期时上传新证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择 * 编辑名称和权限 *
4. 输入一个证书名称、该名称至少包含1个字符、但不超过32个字符。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 * 允许 Prometheus* 。
6. 选择 * 继续 * 以在网格管理器中保存证书。

更新后的证书将显示在客户端选项卡上。

附加新的客户端证书

您可以在当前证书过期后上传新证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

   表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择编辑选项。

上传证书

复制证书文本以粘贴到其他位置。

a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
b. 上传客户端证书名称（` .pem` ）。

   选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

     例如： `storagegRid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
c. 选择 * 创建 * 以在网格管理器中保存证书。

   更新后的证书将显示在客户端选项卡上。

生成证书

生成要粘贴到其他位置的证书文本。

a. 选择 * 生成证书 * 。
b. 指定证书信息：
   - * 域名 * ： 要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
   - * IP * ： 要包含在证书中的一个或多个 IP 地址。
   - * 主题 * ： 证书所有者的 X.509 主题或可分辨名称（ DN ）。
   - * 有效天数 * ： 创建证书后的天数到期。
c. 选择 * 生成 * 。
d. 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

   关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

     例如： `storagegRid_certificate.pem`

   - 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
   - 选择 * 下载私钥 * 将私钥另存为文件。

     指定私钥文件名和下载位置。

e. 选择 * 创建 * 以在网格管理器中保存证书。

新证书将显示在客户端选项卡上。

下载或复制客户端证书

您可以下载或复制客户端证书以供其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择要复制或下载的证书。
3. 下载或复制证书。

下载证书文件

下载证书 ` .pem` 文件。

a. 选择 * 下载证书 * 。
b. 指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

例如： `storagegRid_certificate.pem`

复制证书

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 保存扩展名为 ` .pem` 的文本文件。

例如： `storagegRid_certificate.pem`

删除客户端证书

如果您不再需要管理员客户端证书，可以将其删除。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择要删除的证书。
3. 选择 * 删除 * ，然后确认。

要删除最多 10 个证书，请在客户端选项卡上选择要删除的每个证书，然后选择 * 操作 * > * 删除 * 。

删除证书后，使用该证书的客户端必须指定一个新的客户端证书，才能访问 StorageGRID Prometheus 数据库。

配置密钥管理服务器

配置密钥管理服务器：概述

您可以配置一个或多个外部密钥管理服务器（ KMS ）来保护专门配置的设备节点上的数据。

什么是密钥管理服务器（ **KMS** ）？

密钥管理服务器（ Key Management Server ， KMS ）是一种外部第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为关联 StorageGRID 站点上的 StorageGRID 设备节点提供加密密钥。

您可以使用一个或多个密钥管理服务器来管理安装期间启用了 * 节点加密 * 设置的任何 StorageGRID 设备节点的节点加密密钥。通过将密钥管理服务器与这些设备节点结合使用，您可以保护数据，即使设备已从数据中心中删除也是如此。对设备卷进行加密后，除非节点可以与 KMS 通信，否则无法访问设备上的任何数据。

> StorageGRID 不会创建或管理用于对设备节点进行加密和解密的外部密钥。如果您计划使用外部密钥管理服务器来保护 StorageGRID 数据，则必须了解如何设置该服务器，并且必须了解如何管理加密密钥。执行密钥管理任务不在本说明的范围之内。如果需要帮助，请参见密钥管理服务器的文档或联系技术支持。

查看 **StorageGRID** 加密方法

StorageGRID 提供了多种数据加密选项。您应查看可用的方法，以确定哪些方法符合数据保护要求。

下表简要总结了 StorageGRID 中可用的加密方法。

加密选项	工作原理	适用场景
网格管理器中的密钥管理服务器（ KMS ）	您可以为 StorageGRID 站点配置密钥管理服务器（ * 配置 * > * 安全性 * > * 密钥管理服务器 * ），并为设备启用节点加密。然后，设备节点将连接到 KMS 以请求密钥加密密钥（ Key Encryption Key ， KEK ）。此密钥用于对每个卷上的数据加密密钥（ DEK ）进行加密和解密。	安装期间启用了 * 节点加密 * 的设备节点。设备上的所有数据均可防止物理丢失或从数据中心删除。 只有存储节点和服务设备才支持使用KMS管理加密密钥。

加密选项	工作原理	适用场景
SANtricity System Manager 中的驱动器安全性	如果为存储设备启用了驱动器安全功能，则可以使用 SANtricity 系统管理器创建和管理安全密钥。要访问受保护驱动器上的数据，需要使用此密钥。	具有全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS ）驱动器的存储设备。安全驱动器上的所有数据均可防止物理丢失或从数据中心中删除。不能用于某些存储设备或任何服务设备。 • SG6000 存储设备 • SG5700 存储设备 • SG5600 存储设备
存储对象加密网格选项	可以在网格管理器中启用 * 存储对象加密 * 选项（ * 配置 * > * 系统 * > * 网格选项 * ）。启用后，任何未在存储分段级别或对象级别加密的新对象都会在载入期间进行加密。	新载入的 S3 和 Swift 对象数据。 现有存储对象未加密。对象元数据和其他敏感数据未加密。 • 配置存储的对象加密
S3 存储分段加密	问题描述 PUT 分段加密请求以对分段启用加密。任何未在对象级别加密的新对象都会在载入期间进行加密。	仅新载入的 S3 对象数据。 必须为存储分段指定加密。现有存储分段对象未加密。对象元数据和其他敏感数据未加密。 • 使用 S3
S3 对象服务器端加密（ SS3 ）	您可以问题描述 S3 请求以存储对象，并包含 `x-AMZ-server-side encryption` request 标头。	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据未加密。 StorageGRID 负责管理密钥。 • 使用 S3

加密选项	工作原理	适用场景
使用客户提供的密钥（ SSI-C ）进行 S3 对象服务器端加密	您可以问题描述 S3 请求以存储一个对象并包含三个请求标头。 • `x-AMZ-server-side encrypt-customer-encryption` • `x-AMZ-server-side encrypt-customer-key` • `x-AMZ-server-side encrypt-customer-key-md5`	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据未加密。 密钥在 StorageGRID 之外进行管理。 • 使用 S3
外部卷或数据存储库加密	如果您的部署平台支持，则可以在 StorageGRID 外部使用加密方法对整个卷或数据存储库进行加密。	所有对象数据，元数据和系统配置数据，假设每个卷或数据存储库都已加密。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。
StorageGRID 外部的对象加密	在将对象数据和元数据载入 StorageGRID 之前，您可以在 StorageGRID 外部使用加密方法对这些数据和元数据进行加密。	仅限对象数据和元数据（系统配置数据不加密）。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。 • "Amazon Simple Storage Service —开发人员指南：使用客户端加密保护数据"

使用多种加密方法

根据您的要求，您一次可以使用多种加密方法。例如：

- 您可以使用 KMS 来保护设备节点，也可以使用 SANtricity 系统管理器中的驱动器安全功能在同一设备中的自加密驱动器上 " d 进行灵活加密 " 数据。
- 您可以使用 KMS 来保护设备节点上的数据安全，也可以使用存储对象加密网格选项在载入所有对象时对其进行加密。

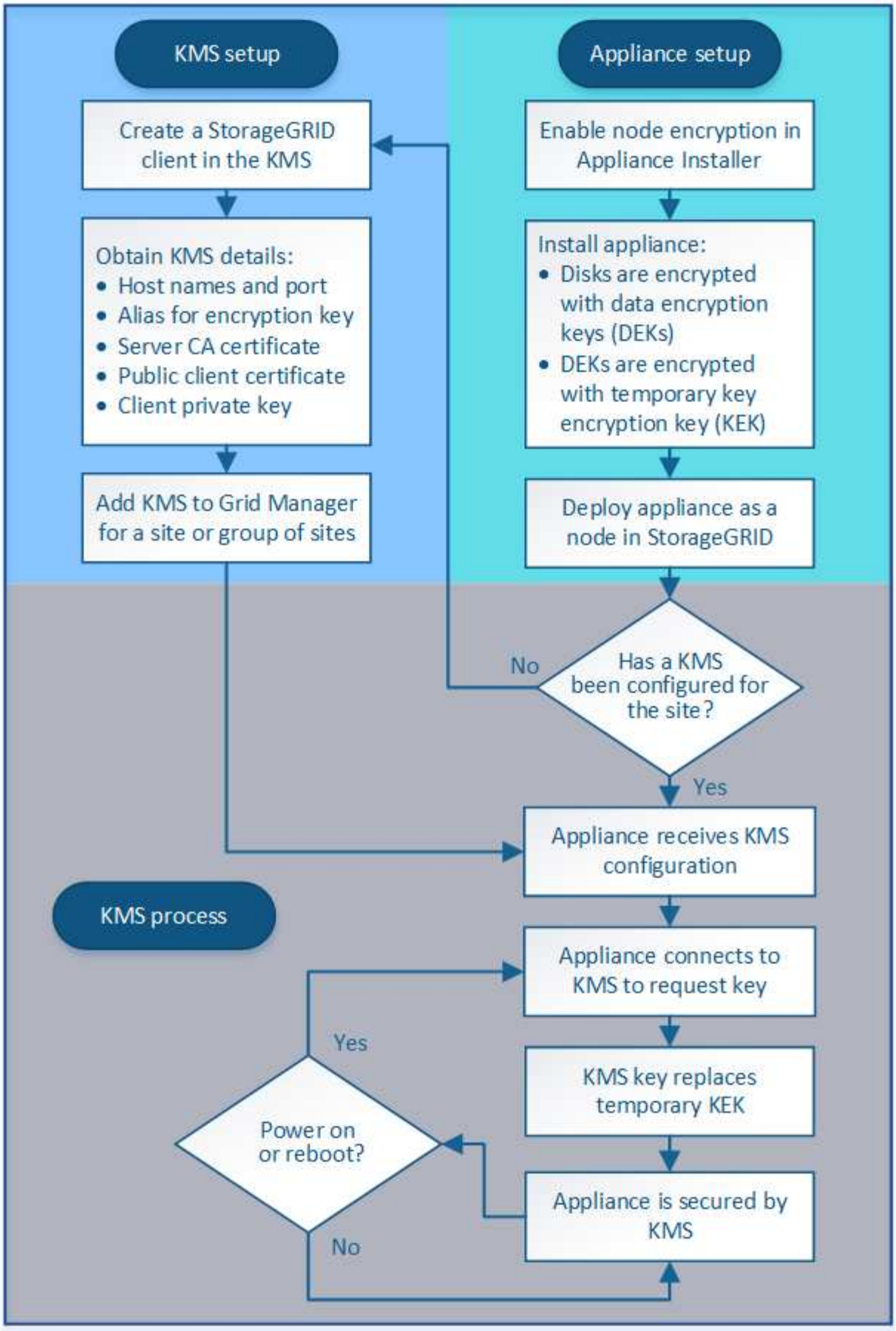
如果只有一小部分对象需要加密，请考虑在存储分段或单个对象级别控制加密。启用多个级别的加密会产生额外的性能成本。

KMS 和设备配置概述

在使用密钥管理服务器（ KMS ）保护设备节点上的 StorageGRID 数据之前，必须完成两项配置任务：设置一个或多个 KMS 服务器以及为设备节点启用节点加密。完成这两项配

置任务后，密钥管理过程将自动进行。

此流程图显示了使用 KMS 在设备节点上保护 StorageGRID 数据的高级步骤。



流程图显示了 KMS 设置和设备设置并行进行；但是，您可以根据需要在为新设备节点启用节点加密之前或之后

设置密钥管理服务器。

设置密钥管理服务器（ **KMS** ）

设置密钥管理服务器包括以下高级步骤。

步骤	请参见
访问 KMS 软件，并向每个 KMS 或 KMS 集群添加一个 StorageGRID 客户端。	在 KMS 中将 StorageGRID 配置为客户端
在 KMS 上获取 StorageGRID 客户端所需的信息。	在 KMS 中将 StorageGRID 配置为客户端
将 KMS 添加到网格管理器中，将其分配到一个站点或一组默认站点，上传所需的证书并保存 KMS 配置。	添加密钥管理服务器（ KMS ）

设置设备

设置要使用 KMS 的设备节点包括以下高级步骤。

1. 在设备安装的硬件配置阶段，使用 StorageGRID 设备安装程序为设备启用 * 节点加密 * 设置。

   在将设备添加到网格后，您无法启用 * 节点加密 * 设置，也无法对未启用节点加密的设备使用外部密钥管理。

2. 运行 StorageGRID 设备安装程序。在安装期间，系统会为每个设备卷分配一个随机数据加密密钥（ DEK ），如下所示：
   - 这些 DEks 用于对每个卷上的数据进行加密。这些密钥是通过设备操作系统中的 Linux 统一密钥设置（ LUKS ）磁盘加密生成的，不能更改。
   - 每个 DEK 都通过主密钥加密密钥（ KEK ）进行加密。初始 KEK 是一个临时密钥，用于对密钥进行加密，直到设备可以连接到 KMS 为止。
3. 将设备节点添加到 StorageGRID 。

有关详细信息，请参阅以下内容：

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

密钥管理加密过程（自动发生）

密钥管理加密包括以下高级步骤，这些步骤会自动执行。

1. 在网格中安装启用了节点加密的设备时， StorageGRID 会确定包含新节点的站点是否存在 KMS 配置。
   - 如果已为站点配置 KMS ，则设备将接收 KMS 配置。

- 如果尚未为站点配置 KMS ，则设备上的数据将继续由临时 KEK 加密，直到您为站点配置 KMS 且设备收到 KMS 配置为止。

2. 设备使用 KMS 配置连接到 KMS 并请求加密密钥。
3. KMS 会向设备发送加密密钥。KMS 中的新密钥将取代临时的 KEK ，现在用于对设备卷的 DEK 进行加密和解密。

> 加密设备节点连接到配置的 KMS 之前存在的任何数据都将使用临时密钥进行加密。但是，在将临时密钥替换为 KMS 加密密钥之前，不应将设备卷视为不受从数据中心删除的保护。

4. 如果设备已启动或重新启动，它将重新连接到 KMS 以请求密钥。保存在易失性内存中的密钥在断电或重新启动后无法生存。

使用密钥管理服务器的注意事项和要求

在配置外部密钥管理服务器（ KMS ）之前，您必须了解注意事项和要求。

KMIP 要求是什么?

StorageGRID 支持 KMIP 1.4 版。

"密钥管理互操作性协议规范 1.4 版"

设备节点与配置的 KMS 之间的通信使用安全 TLS 连接。StorageGRID 支持 KMIP 使用以下 TLS v1.2 密码：

- tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_ECDSA_WIT_AES_256_GCM_SHA384

您必须确保使用节点加密的每个设备节点都可以通过网络访问为站点配置的 KMS 或 KMS 集群。

网络防火墙设置必须允许每个设备节点通过用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口进行通信。默认 KMIP 端口为 5696 。

支持哪些设备?

您可以使用密钥管理服务器（ Key Management Server ， KMS ）管理网格中启用了 * 节点加密 * 设置的任何 StorageGRID 设备的加密密钥。只有在使用 StorageGRID 设备安装程序安装设备的硬件配置阶段，才能启用此设置。

> 在将设备添加到网格后，您无法启用节点加密，并且不能对未启用节点加密的设备使用外部密钥管理。

您可以对以下 StorageGRID 设备和设备节点使用已配置的 KMS ：

设备	节点类型
SG1000 服务设备	管理节点或网关节点
SG100 服务设备	管理节点或网关节点

设备	节点类型
SG6000 存储设备	存储节点
SG5700 存储设备	存储节点
SG5600 存储设备	存储节点

您不能对基于软件（非设备）的节点使用已配置的 KMS ，包括以下节点：

- 部署为虚拟机（ VM ）的节点
- 在 Linux 主机上的容器引擎中部署的节点

在这些其他平台上部署的节点可以在数据存储库或磁盘级别使用 StorageGRID 外部的加密。

应在何时配置密钥管理服务器？

对于新安装，通常应在创建租户之前在网格管理器中设置一个或多个密钥管理服务器。此顺序可确保节点在存储任何对象数据之前受到保护。

您可以在安装设备节点之前或之后在网格管理器中配置密钥管理服务器。

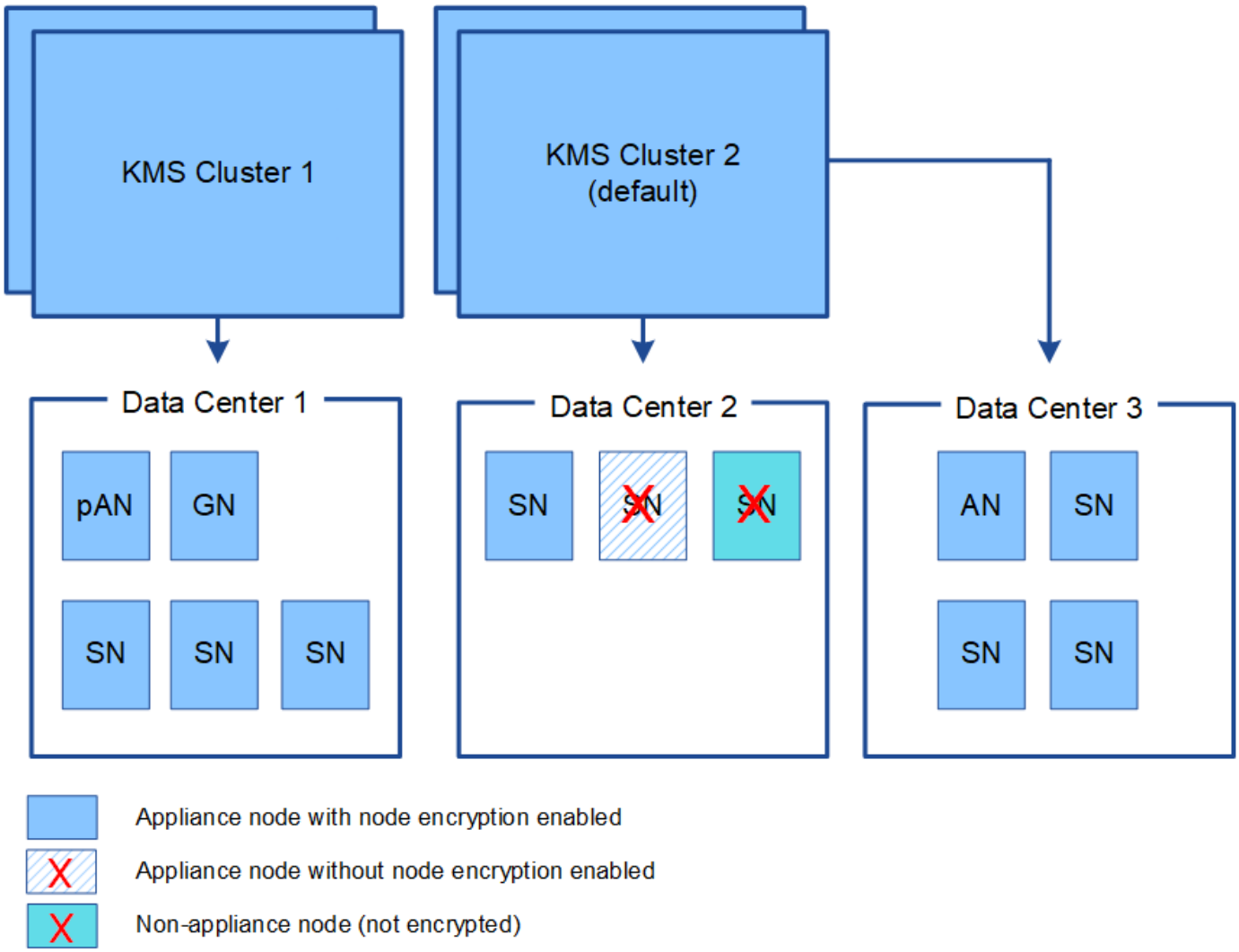
我需要多少个密钥管理服务器？

您可以配置一个或多个外部密钥管理服务器，以便为 StorageGRID 系统中的设备节点提供加密密钥。每个 KMS 都为单个站点或一组站点上的 StorageGRID 设备节点提供一个加密密钥。

StorageGRID 支持使用 KMS 集群。每个 KMS 集群都包含多个复制的密钥管理服务器，这些服务器共享配置设置和加密密钥。建议使用 KMS 集群进行密钥管理，因为它可以提高高可用性配置的故障转移功能。

例如，假设您的 StorageGRID 系统有三个数据中心站点。您可以将一个 KMS 集群配置为为为 Data Center 1 上的所有设备节点提供密钥，而将另一个 KMS 集群配置为为为所有其他站点上的所有设备节点提供密钥。添加第二个 KMS 集群时，您可以为 Data Center 2 和 Data Center 3 配置默认 KMS 。

请注意，不能对非设备节点或在安装期间未启用 * 节点加密 * 设置的任何设备节点使用 KMS 。



轮换密钥时会发生什么情况?

作为安全最佳实践，您应定期轮换每个已配置的 KMS 使用的加密密钥。

在旋转加密密钥时，请使用 KMS 软件将该密钥从上次使用的版本轮换到同一密钥的新版本。请勿旋转到完全不同的密钥。

> 切勿尝试通过在网格管理器中更改 KMS 的密钥名称（别名）来轮换密钥。而是通过更新 KMS 软件中的密钥版本来轮换密钥。对新密钥使用与先前密钥相同的密钥别名。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。

新密钥版本可用时：

- 它会自动分发到与 KMS 关联的站点上的加密设备节点。分发应在轮换密钥后的一小时内完成。
- 如果在分发新密钥版本时加密设备节点脱机，则该节点将在重新启动后立即收到新密钥。
- 如果由于任何原因无法使用新密钥版本对设备卷进行加密，则会为此设备节点触发 * KMS 加密密钥轮换失败 * 警报。您可能需要联系技术支持以帮助解决此警报。

是否可以在设备节点加密后重复使用它?

如果需要将加密设备安装到另一个 StorageGRID 系统中，则必须先停用网格节点，才能将对象数据移动到另一个节点。然后，您可以使用 StorageGRID 设备安装程序清除 KMS 配置。清除 KMS 配置将禁用 * 节点加密 * 设置，并删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。

如果无法访问 KMS 加密密钥，则设备上保留的任何数据将无法再访问并永久锁定。

相关信息

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

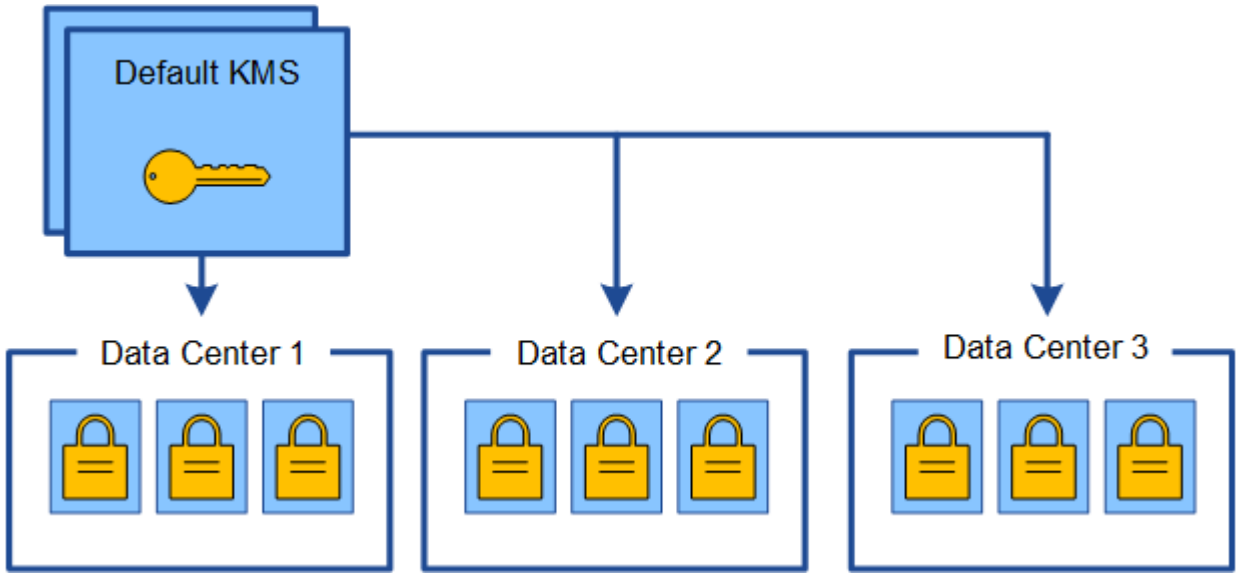
更改站点的 **KMS** 的注意事项

每个密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群都会为单个站点或一组站点上的所有设备节点提供一个加密密钥。如果需要更改站点使用的 KMS ，则可能需要将加密密钥从一个 KMS 复制到另一个 KMS 。

如果更改站点使用的 KMS ，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS 。您必须确保 KMS 具有正确的密钥，以便对站点上的加密设备节点进行解密。

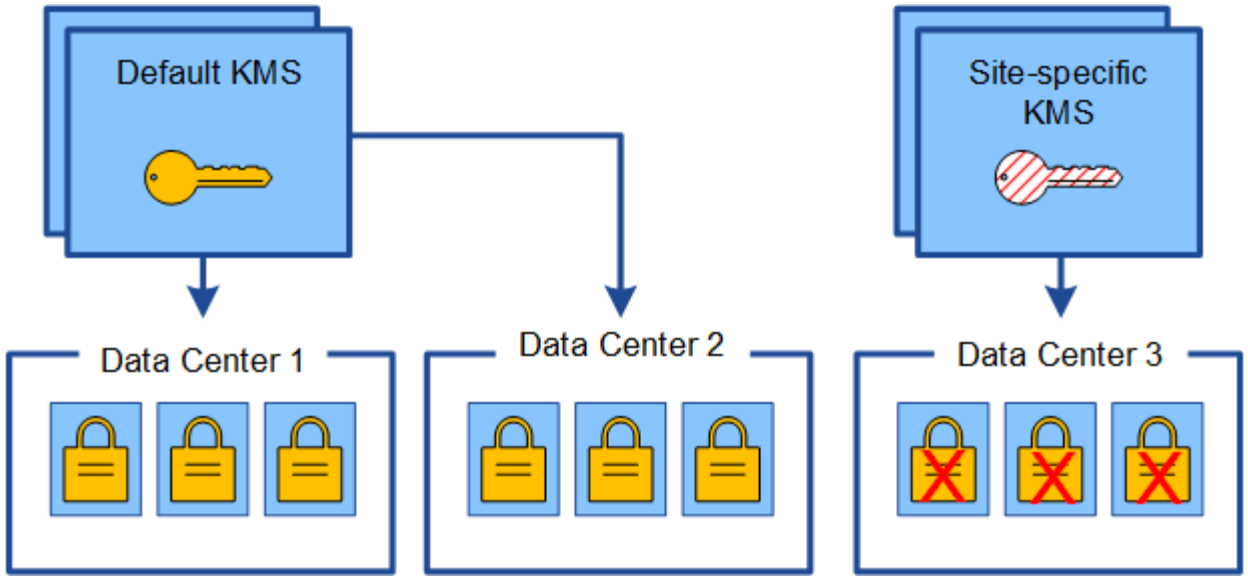
例如：

1. 您最初会配置一个默认 KMS ，以便对没有专用 KMS 的所有站点进行适用场景 。
2. 保存 KMS 后，所有启用了 * 节点加密 * 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于对所有站点上的设备节点进行加密。此外，还必须使用此相同密钥对这些设备进行解密。

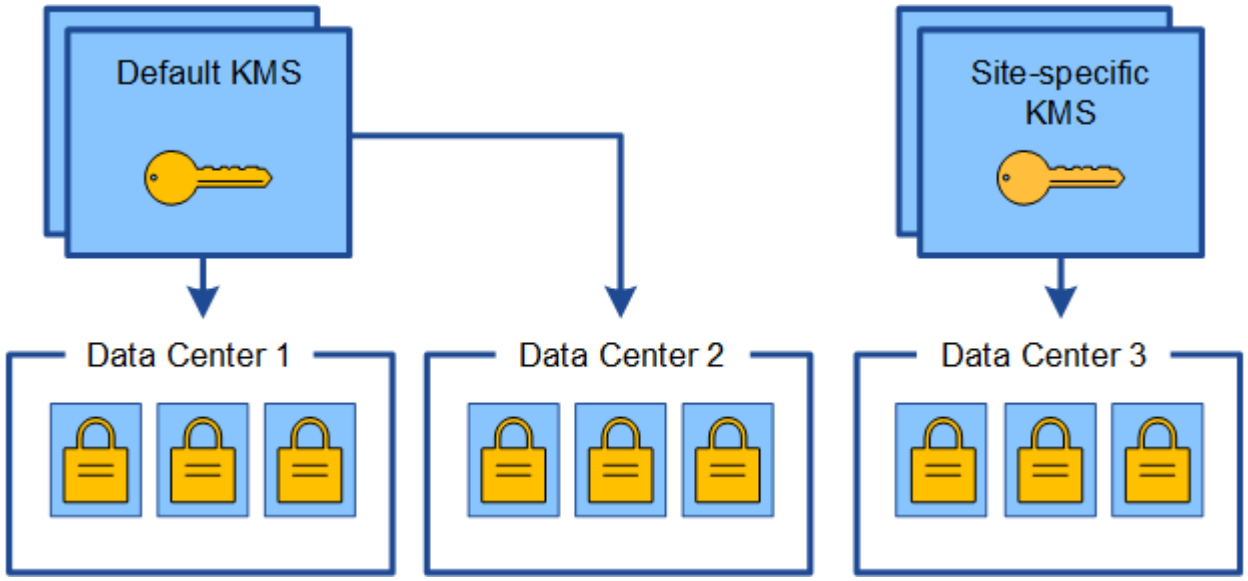


3. 您决定为一个站点（图中的数据中心 3 ）添加站点专用的 KMS 。但是，由于设备节点已加密，因此在尝试保存站点专用 KMS 的配置时会发生验证错误。之所以出现此错误，是因为站点特定的 KMS 没有正确的密

钥来对该站点上的节点进行解密。



4. 要解决问题描述 问题，请将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。（从技术上讲，您可以将原始密钥复制到具有相同别名的新密钥。原始密钥将成为新密钥的先前版本。） 现在，站点特定的 KMS 具有用于对数据中心 3 上的设备节点进行解密的正确密钥，因此可以将其保存在 StorageGRID 中。



更改站点使用的 **KMS** 的用例

下表总结了更改站点 KMS 的最常见情况下所需的步骤。

更改站点 **KMS** 的用例	所需步骤
您有一个或多个站点特定的 KMS 条目，并且希望使用其中一个条目作为默认 KMS 。	编辑站点特定的 KMS 。在 * 管理密钥 * 字段中，选择 * 不受其他 KMS （默认 KMS ）管理的站点 * 。现在，站点专用的 KMS 将用作默认 KMS 。它将适用于没有专用 KMS 的任何站点。 编辑密钥管理服务器（ KMS ）
您有一个默认 KMS ，并且在扩展中添加了一个新站点。您不希望对新站点使用默认 KMS 。	1. 如果新站点上的设备节点已被默认 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从默认 KMS 复制到新 KMS 。 2. 使用网格管理器添加新的 KMS 并选择站点。 添加密钥管理服务器（ KMS ）
您希望站点的 KMS 使用其他服务器。	1. 如果站点上的设备节点已由现有 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从现有 KMS 复制到新 KMS 。 2. 使用网格管理器编辑现有 KMS 配置并输入新的主机名或 IP 地址。 添加密钥管理服务器（ KMS ）

在 **KMS** 中将 **StorageGRID** 配置为客户端

您必须将 StorageGRID 配置为每个外部密钥管理服务器或 KMS 集群的客户端，然后才能将 KMS 添加到 StorageGRID 。

关于此任务

这些说明适用于 Thales CipherTrust Manager k170v 2.0 ， 2.1 和 2.2 版。如果您对在 StorageGRID 中使用其他密钥管理服务器有任何疑问，请联系技术支持。

"Thales CipherTrust Manager"

步骤

1. 在 KMS 软件中，为计划使用的每个 KMS 或 KMS 集群创建一个 StorageGRID 客户端。

   每个 KMS 都会为单个站点或一组站点上的 StorageGRID 设备节点管理一个加密密钥。

2. 在 KMS 软件中，为每个 KMS 或 KMS 集群创建 AES 加密密钥。

   加密密钥需要可导出。

3. 记录每个 KMS 或 KMS 集群的以下信息。

   将 KMS 添加到 StorageGRID 时需要此信息。

   - 每个服务器的主机名或 IP 地址。

- KMS 使用的 KMIP 端口。
- KMS 中加密密钥的密钥别名。

> 此加密密钥必须已存在于 KMS 中。StorageGRID 不会创建或管理 KMS 密钥。

4. 对于每个 KMS 或 KMS 集群，获取一个由证书颁发机构（ CA ）签名的服务器证书，或者一个包含 PEM 编码的每个 CA 证书文件的证书捆绑包，这些证书按证书链顺序串联。

   通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

   - 证书必须使用 Privacy Enhanced Mail （ PEM ） Base — 64 编码的 X.509 格式。
   - 每个服务器证书中的 " 使用者备用名称（ SAN ） " 字段必须包含 StorageGRID 要连接到的完全限定域名（ FQDN ）或 IP 地址。

     > 在 StorageGRID 中配置 KMS 时，必须在 * 主机名 * 字段中输入相同的 FQDN 或 IP 地址。

   - 服务器证书必须与 KMS 的 KMIP 接口使用的证书匹配，该接口通常使用端口 5696 。
5. 获取外部 KMS 颁发给 StorageGRID 的公有 客户端证书以及客户端证书的专用密钥。

   客户端证书允许 StorageGRID 向 KMS 进行身份验证。

添加密钥管理服务器（ **KMS** ）

您可以使用 StorageGRID 密钥管理服务器向导添加每个 KMS 或 KMS 集群。

您需要的内容

- 您已查看 使用密钥管理服务器的注意事项和要求。
- 您已拥有 已在 KMS 中将 StorageGRID 配置为客户端和您具有每个 KMS 或 KMS 集群所需的信息。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。

关于此任务

如果可能，请先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对所有不受另一个 KMS 管理的站点进行适用场景 。如果首先创建默认 KMS ，则网格中所有节点加密的设备都将使用默认 KMS 进行加密。如果要稍后创建站点专用的 KMS ，则必须先将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。请参见 更改站点的 KMS 的注意事项 了解详细信息。

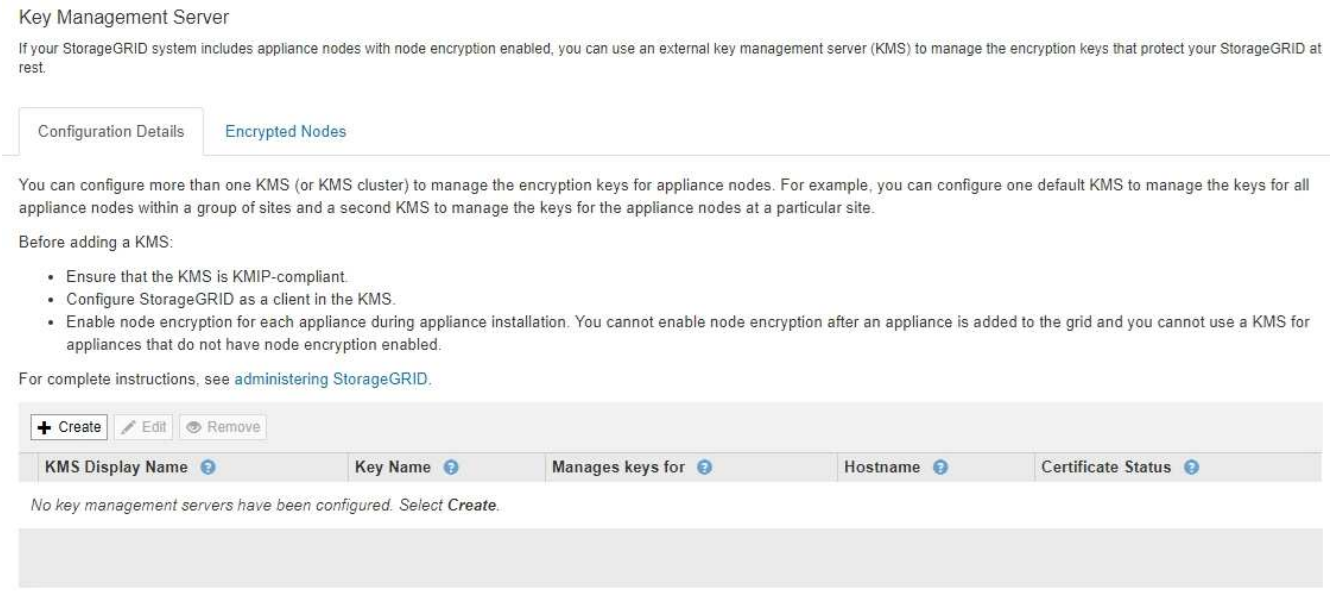
第 **1** 步：输入 **KMS** 详细信息

在添加密钥管理服务器向导的步骤 1 （输入 KMS 详细信息）中，您可以提供有关 KMS 或 KMS 集群的详细信息。

步骤

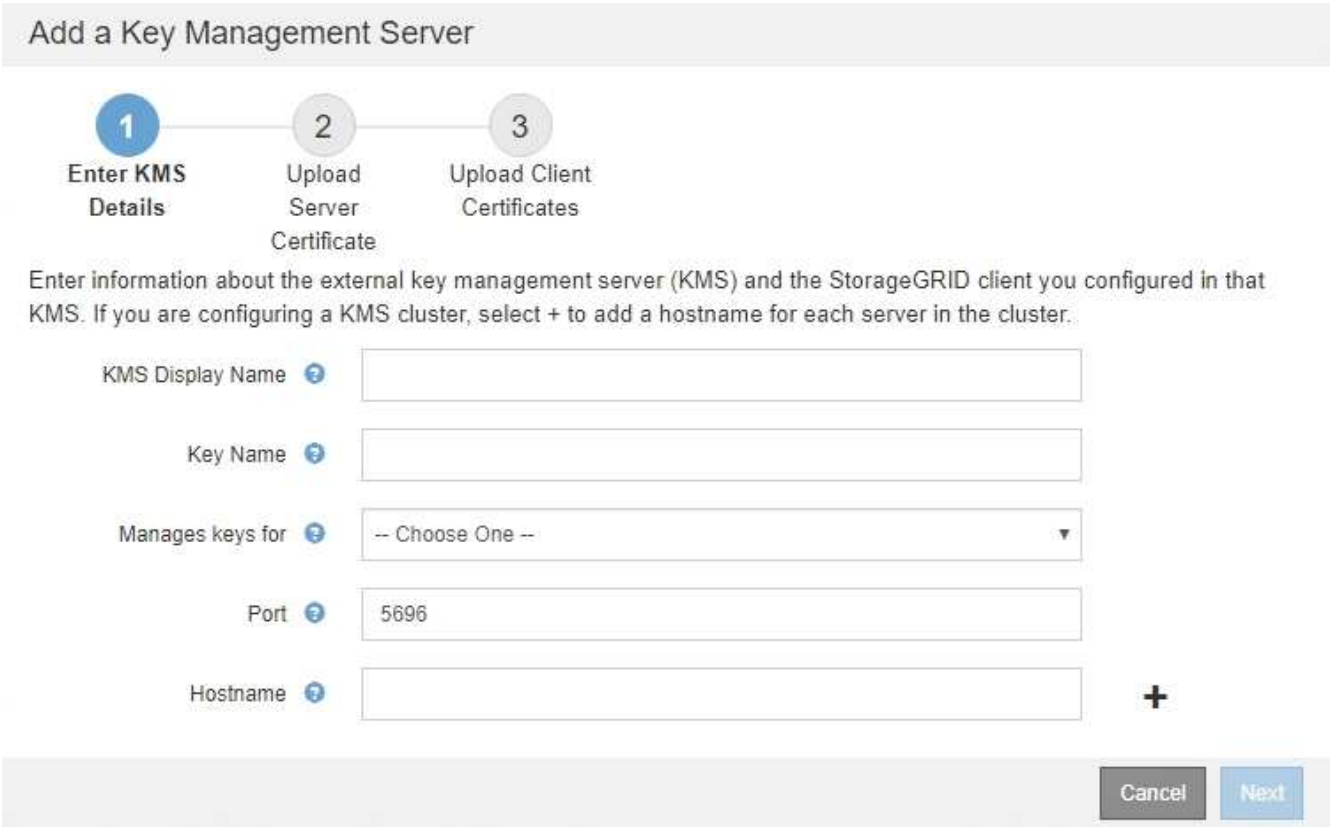
1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面，并选中配置详细信息选项卡。



2. 选择 * 创建 * 。

此时将显示添加密钥管理服务器向导的第 1 步（输入 KMS 详细信息）。



3. 为 KMS 和您在该 KMS 中配置的 StorageGRID 客户端输入以下信息。

字段	Description
Kms 显示名称	一个描述性名称，可帮助您标识此 KMS 。必须介于 1 到 64 个字符之间。

字段	Description
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。
管理的密钥	将与此 KMS 关联的 StorageGRID 站点。如果可能，您应先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对不受另一个 KMS 管理的所有站点进行适用场景 。 • 如果此 KMS 将管理特定站点上设备节点的加密密钥，请选择一个站点。 • 选择 * 不受其他 KMS 管理的站点（默认 KMS ）* 可配置一个默认 KMS ，该 KMS 将应用于没有专用 KMS 的任何站点以及您在后续扩展中添加的任何站点。 ◦ 注意： * 如果您选择的站点先前已被默认 KMS 加密，但未向新 KMS 提供当前版本的原始加密密钥，则保存 KMS 配置时将发生验证错误。
Port	KMS 服务器用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口。默认为 5696 ，即 KMIP 标准端口。
主机名	KMS 的完全限定域名或 IP 地址。 • 注： * 服务器证书的 SAN 字段必须包含您在此处输入的 FQDN 或 IP 地址。否则，StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

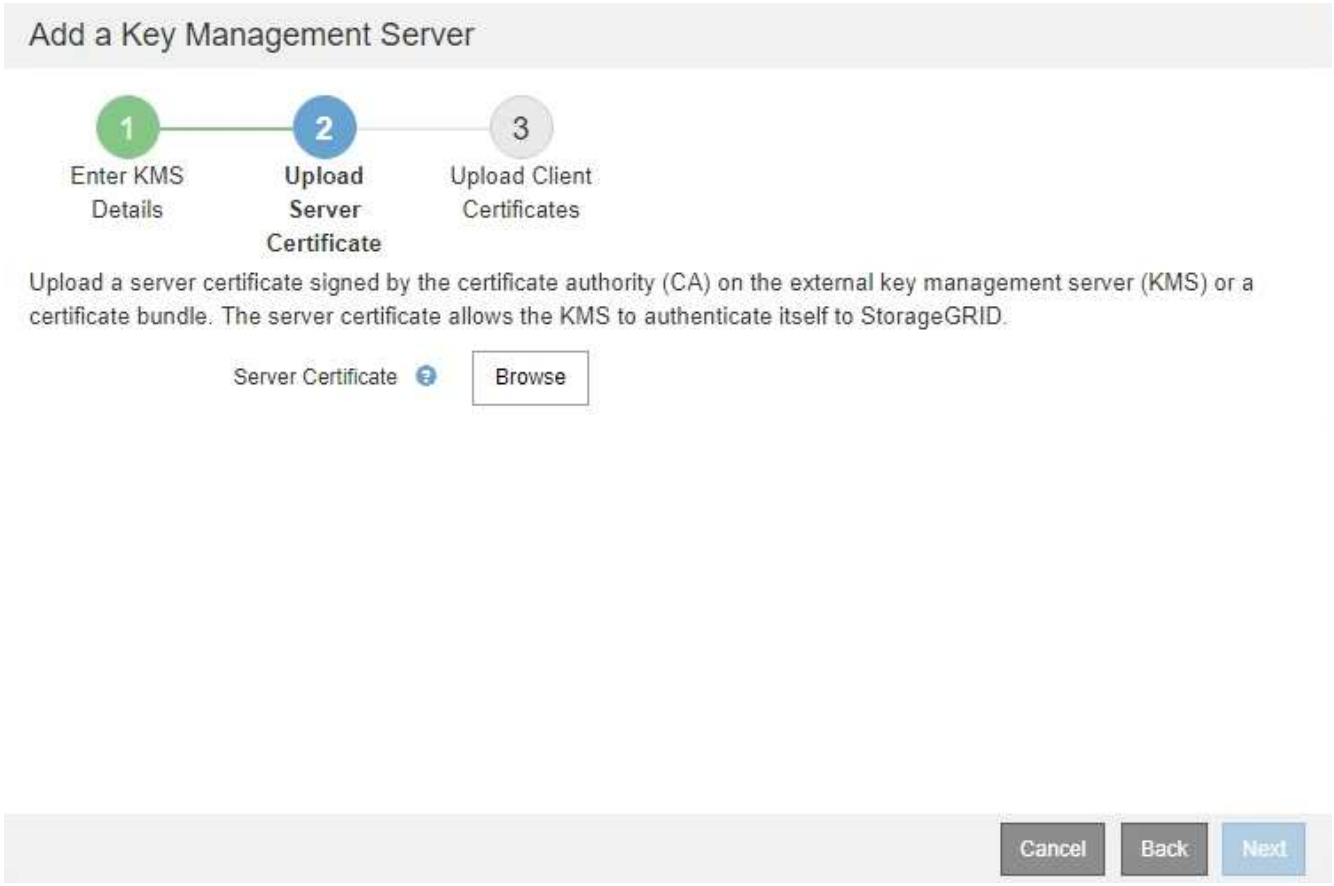
4. 如果您使用的是 KMS 集群，请选择加号 ➕ 为集群中的每个服务器添加主机名。
5. 选择 * 下一步 * 。

第 **2** 步：上传服务器证书

在添加密钥管理服务器向导的第 2 步（上传服务器证书）中，您可以上传 KMS 的服务器证书（或证书包）。通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

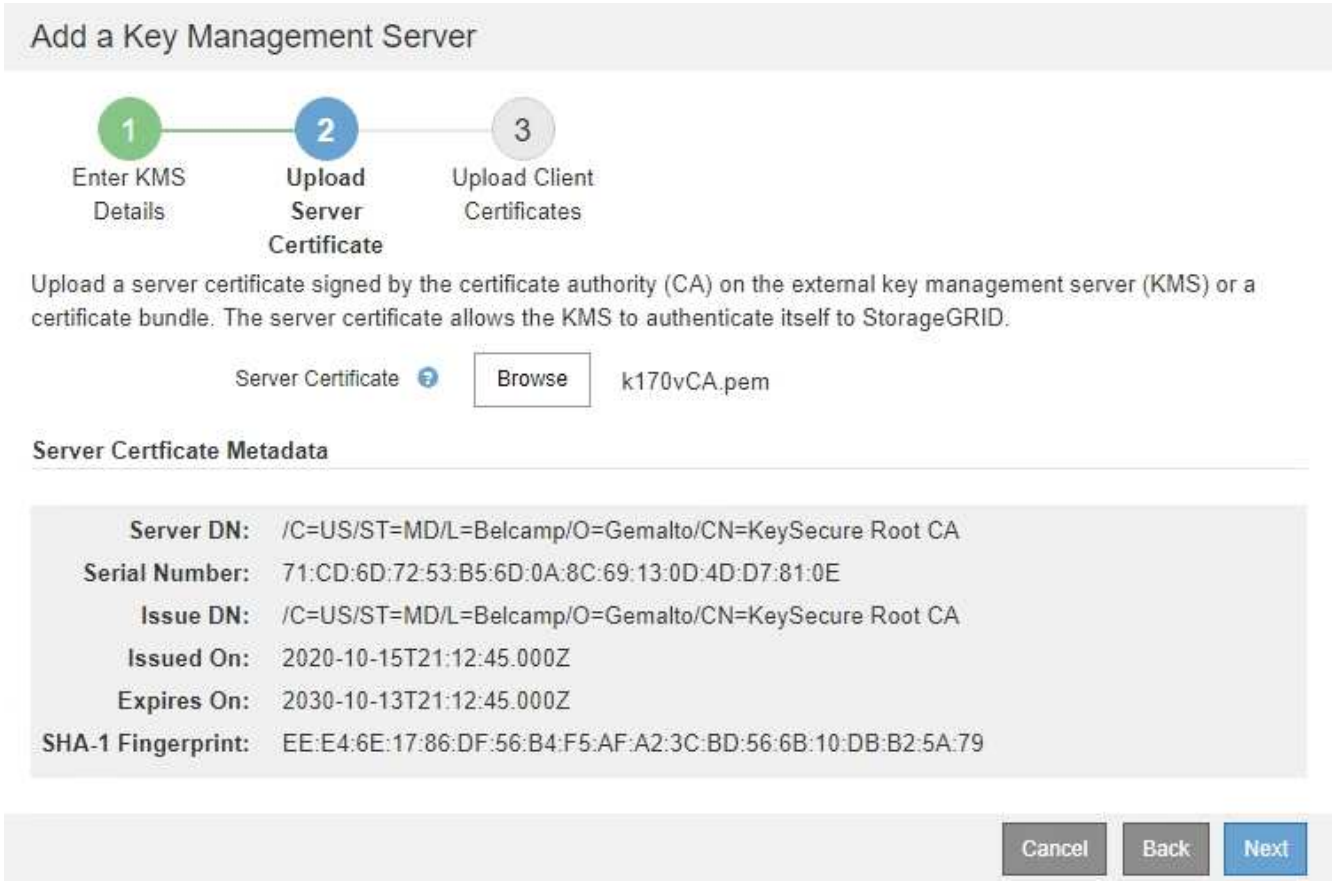
步骤

1. 从 * 步骤 2 （上传服务器证书） * 中，浏览到保存的服务器证书或证书包的位置。



2. 上传证书文件。

   此时将显示服务器证书元数据。



如果您上传的是证书捆绑包，则每个证书的元数据将显示在其自己的选项卡上。

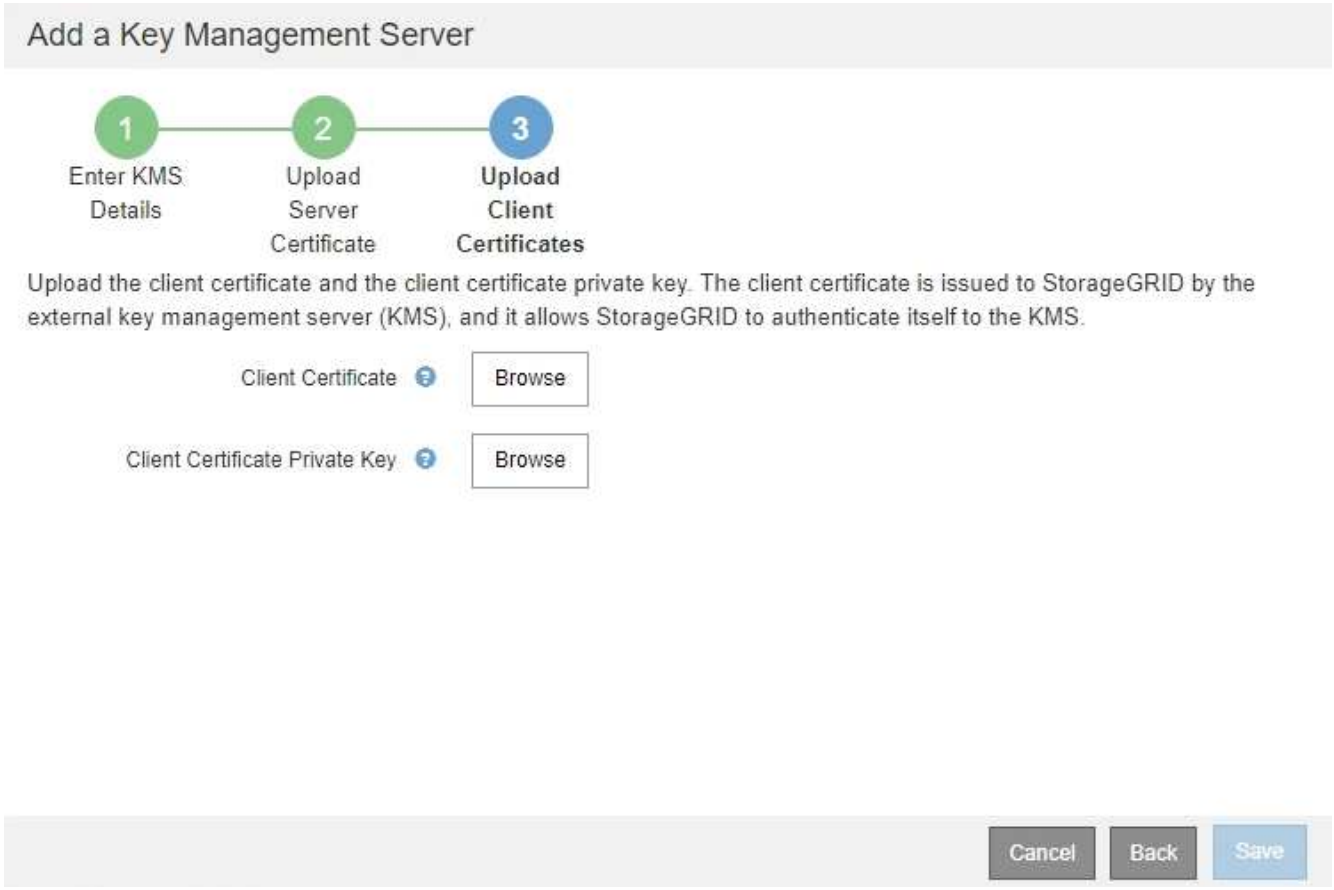
3. 选择 * 下一步 * 。

第 **3** 步：上传客户端证书

在添加密钥管理服务器向导的第 3 步（上传客户端证书）中，您可以上传客户端证书和客户端证书专用密钥。客户端证书允许 StorageGRID 向 KMS 进行身份验证。

步骤

1. 从 * 步骤 3 （上传客户端证书） * 中，浏览到客户端证书的位置。

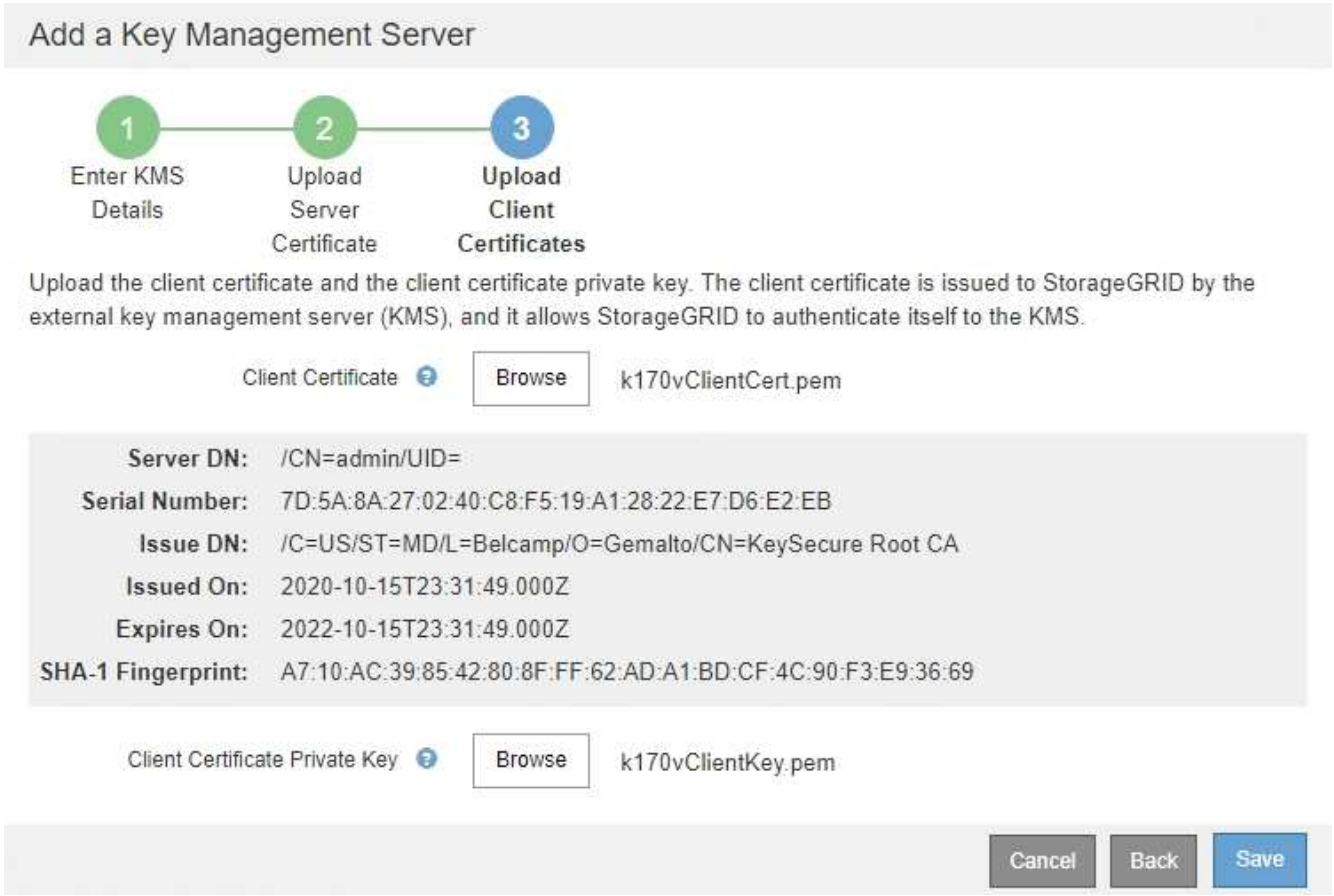


2. 上传客户端证书文件。

   此时将显示客户端证书元数据。

3. 浏览到客户端证书的专用密钥位置。
4. 上传私钥文件。

   此时将显示客户端证书和客户端证书专用密钥的元数据。



5. 选择 * 保存 * 。

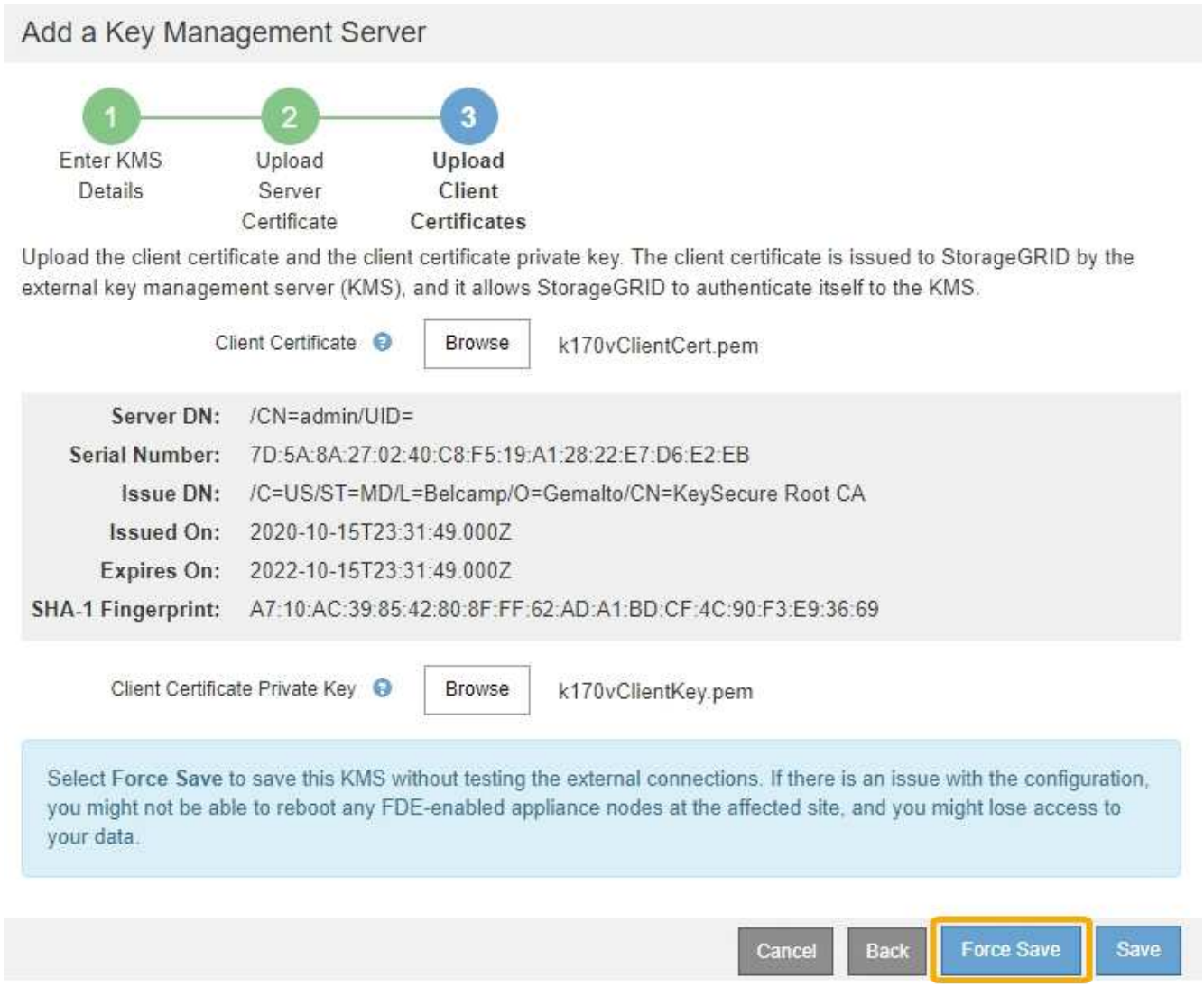
   测试密钥管理服务器与设备节点之间的连接。如果所有连接均有效，并且在 KMS 上找到正确的密钥，则新的密钥管理服务器将添加到密钥管理服务器页面上的表中。

   > 添加 KMS 后，密钥管理服务器页面上的证书状态将立即显示为未知。StorageGRID 可能需要长达 30 分钟才能获取每个证书的实际状态。您必须刷新 Web 浏览器才能查看当前状态。

6. 如果选择 * 保存 * 时显示错误消息，请查看消息详细信息，然后选择 * 确定 * 。

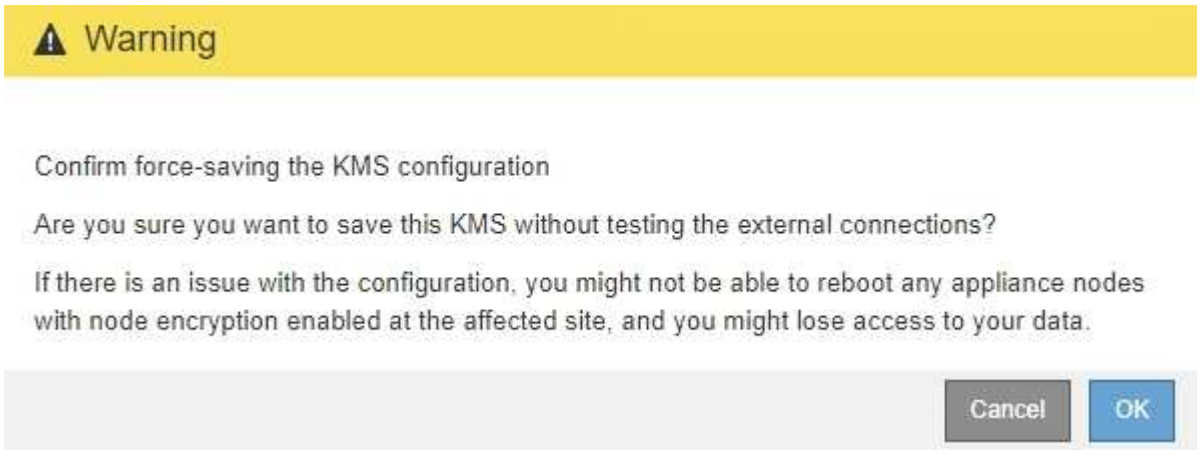
   例如，如果连接测试失败，您可能会收到 422： Unprocessable Entity 错误。

7. 如果需要保存当前配置而不测试外部连接，请选择 * 强制保存 * 。



选择 * 强制保存 * 可保存 KMS 配置，但不会测试每个设备与该 KMS 的外部连接。如果具有此配置的问题描述 ，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

8. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 * 。



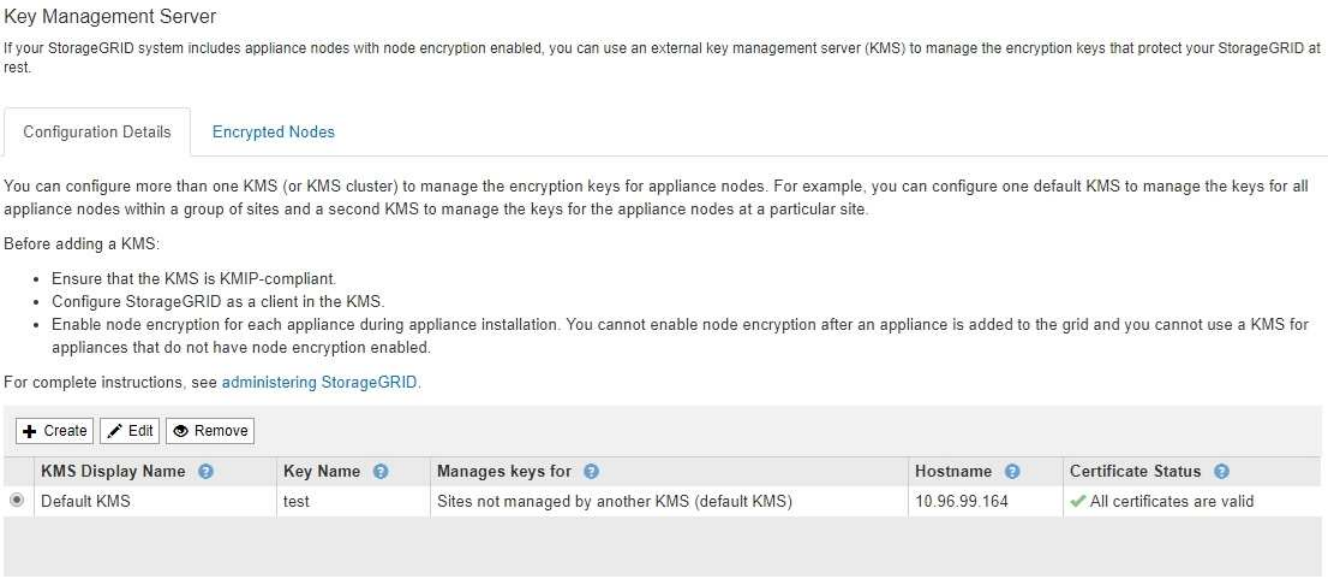
已保存 KMS 配置，但未测试与 KMS 的连接。

您可以查看有关 StorageGRID 系统中每个密钥管理服务器（ KMS ）的信息，包括服务器和客户端证书的当前状态。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面。配置详细信息选项卡显示了已配置的任何密钥管理服务器。



2. 查看每个 KMS 的表中的信息。

字段	**Description**
Kms 显示名称	KMS 的描述性名称。
密钥名称	KMS 中 StorageGRID 客户端的密钥别名。
管理的密钥	与 KMS 关联的 StorageGRID 站点。 此字段显示特定 StorageGRID 站点的名称或 * 不由其他 KMS （默认 KMS ）管理的站点。 *

字段	Description
主机名	KMS 的完全限定域名或 IP 地址。 如果集群包含两个密钥管理服务器，则会列出这两个服务器的完全限定域名或 IP 地址。如果集群中有两个以上的密钥管理服务器，则会列出第一个 KMS 的完全限定域名或 IP 地址以及集群中其他密钥管理服务器的数量。 例如： `10.10.10.10` 和 `10.10.10.11` 或 `10.10.10.10` 和其他 `2` 。 要查看集群中的所有主机名，请选择一个 KMS ，然后选择 * 编辑 * 。
证书状态	服务器证书，可选 CA 证书和客户端证书的当前状态：有效，已过期，即将到期或未知。 • 注意： * StorageGRID 可能需要长达 30 分钟才能更新证书状态。您必须刷新 Web 浏览器才能查看当前值。

3. 如果证书状态为未知，请等待长达 30 分钟，然后刷新 Web 浏览器。

> 添加 KMS 后，密钥管理服务器页面上的证书状态将立即显示为未知。StorageGRID 可能需要长达 30 分钟才能获取每个证书的实际状态。您必须刷新 Web 浏览器才能查看实际状态。

4. 如果证书状态列指示证书已过期或即将到期，请尽快解决问题描述 。

请参见的说明中针对 * KMS CA 证书到期 * ， * KMS 客户端证书到期 * 和 * KMS 服务器证书到期 * 警报的建议操作 监控 StorageGRID 并对其进行故障排除。

> 要保持数据访问，您必须尽快解决任何证书问题。

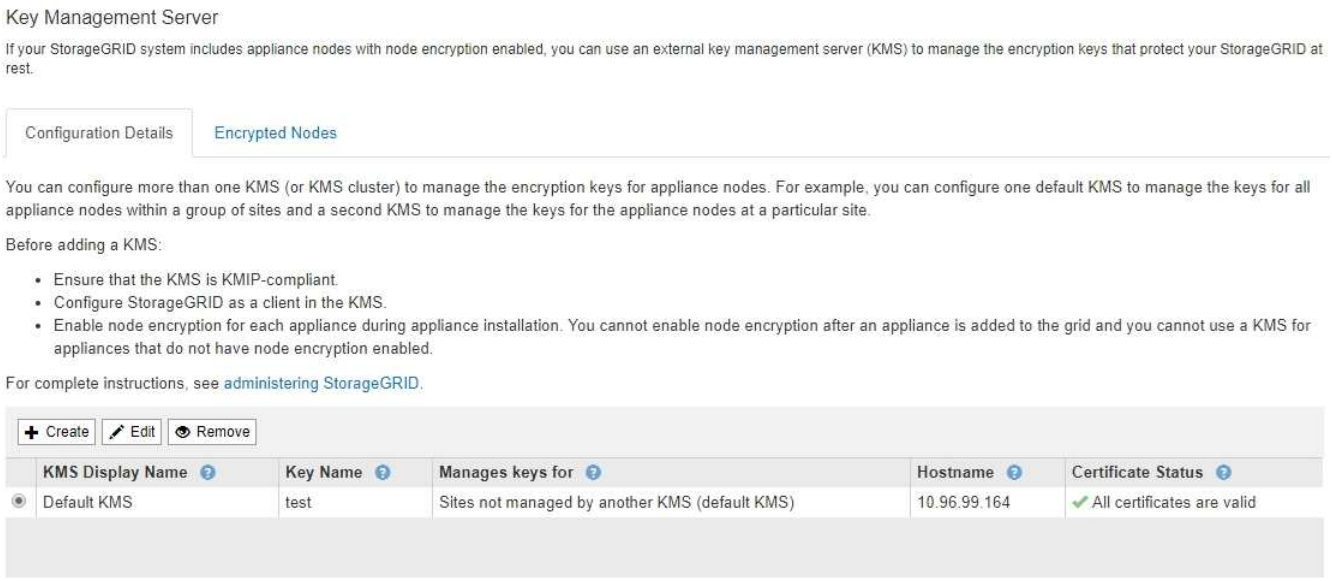
查看加密节点

您可以查看有关 StorageGRID 系统中已启用 * 节点加密 * 设置的设备节点的信息。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

此时将显示密钥管理服务器页面。配置详细信息选项卡显示已配置的任何密钥管理服务器。



2. 从页面顶部，选择 * 加密节点 * 选项卡。

加密节点选项卡列出了 StorageGRID 系统中已启用 * 节点加密 * 设置的设备节点。

3. 查看表中每个设备节点的信息。

列	Description
节点名称	设备节点的名称。
节点类型	节点的类型：存储，管理或网关。
站点	安装节点的 StorageGRID 站点的名称。

列	Description
Kms 显示名称	用于节点的 KMS 的描述性名称。 如果未列出任何 KMS ，请选择配置详细信息选项卡以添加 KMS 。 添加密钥管理服务器（ KMS ）
密钥 UID	用于对设备节点上的数据进行加密和解密的加密密钥的唯一 ID 。要查看整个密钥 UID ，请将光标悬停在单元格上方。 短划线（ - ）表示密钥 UID 未知，可能是因为设备节点和 KMS 之间存在连接问题描述 。
Status	KMS 与设备节点之间的连接状态。如果节点已连接，则时间戳每 30 分钟更新一次。更改 KMS 配置后，可能需要几分钟才能更新连接状态。 • 注意： * 您必须刷新 Web 浏览器才能查看新值。

4. 如果状态列指示 KMS 问题描述 ，请立即解决此问题描述 。

   在正常的 KMS 操作期间，状态将为 * 已连接到 KMS* 。如果节点与网格断开连接，则会显示节点连接状态（ administratively down 或 Unknown ）。

   其他状态消息对应于同名的 StorageGRID 警报：

   ◦ 无法加载 Kms 配置
   ◦ Kms 连接错误
   ◦ 未找到 Kms 加密密钥名称
   ◦ Kms 加密密钥轮换失败
   ◦ Kms 密钥无法对设备卷进行解密
   ◦ 未配置公里

   请参见的说明中针对这些警报建议的操作 监控 StorageGRID 并对其进行故障排除。

   您必须立即解决任何问题，以确保您的数据得到完全保护。

编辑密钥管理服务器（ **KMS** ）

例如，如果证书即将到期，您可能需要编辑密钥管理服务器的配置。

您需要的内容

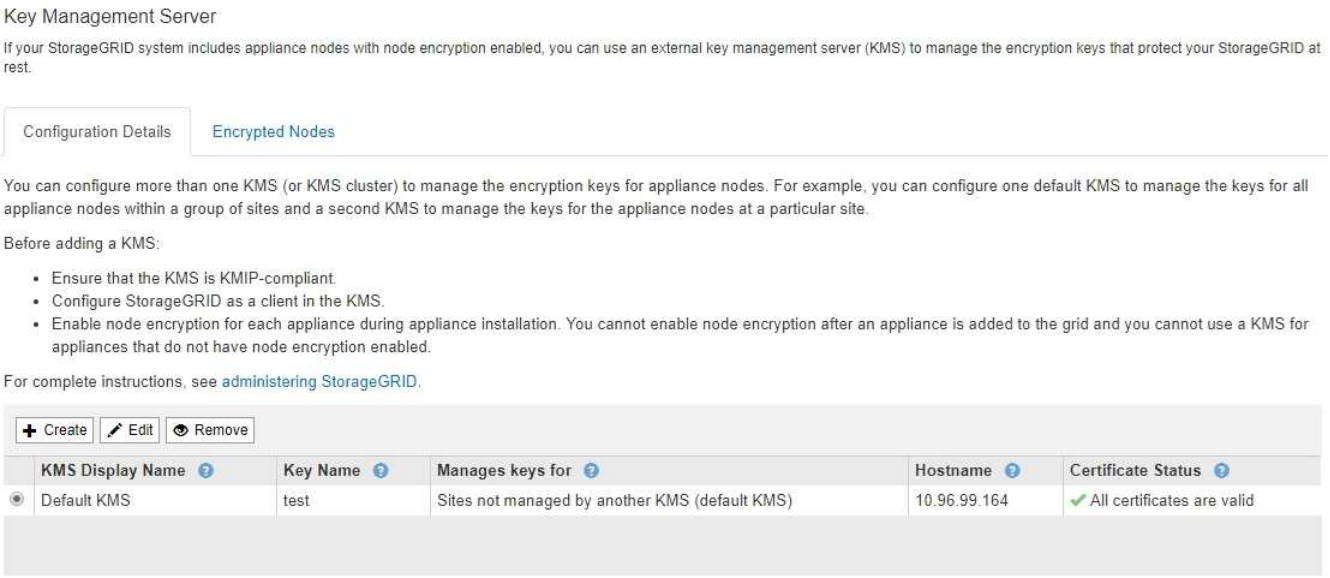
- 您已查看 使用密钥管理服务器的注意事项和要求。
- 如果您计划更新为 KMS 选择的站点，则已查看 更改站点的 KMS 的注意事项。
- 您将使用登录到网格管理器 支持的 Web 浏览器。

- 您具有 root 访问权限。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面，其中显示了已配置的所有密钥管理服务器。



2. 选择要编辑的 KMS ，然后选择 * 编辑 * 。
3. 或者，更新编辑密钥管理服务器向导的 * 步骤 1 （输入 KMS 详细信息） * 中的详细信息。

字段	Description
Kms 显示名称	一个描述性名称，可帮助您标识此 KMS 。必须介于 1 到 64 个字符之间。
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。 在极少数情况下，您只需要编辑密钥名称。例如，如果在 KMS 中重命名了别名，或者先前密钥的所有版本都已复制到新别名的版本历史记录中，则必须编辑密钥名称。 切勿尝试通过更改 KMS 的密钥名称（别名）来旋转密钥。而是通过更新 KMS 软件中的密钥版本来轮换密钥。StorageGRID 要求使用相同密钥别名从 KMS 访问以前使用的所有密钥版本（以及将来的任何密钥版本）。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。 使用密钥管理服务器的注意事项和要求

字段	Description
管理的密钥	如果您正在编辑站点特定的 KMS ，并且尚未设置默认 KMS ，则也可以选择 * 不由其他 KMS 管理的站点（默认 KMS ） * 。此选项会将站点特定的 KMS 转换为默认 KMS ，该 KMS 将应用于没有专用 KMS 的所有站点以及在扩展中添加的任何站点。 • 注意： * 如果要编辑站点特定的 KMS ，则无法选择其他站点。如果要编辑默认 KMS ，则无法选择特定站点。
Port	KMS 服务器用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口。默认为 5696 ，即 KMIP 标准端口。
主机名	KMS 的完全限定域名或 IP 地址。 • 注： * 服务器证书的 SAN 字段必须包含您在此处输入的 FQDN 或 IP 地址。否则， StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

4. 如果要配置 KMS 集群，请选择加号 ➕ 为集群中的每个服务器添加主机名。
5. 选择 * 下一步 * 。

   此时将显示编辑密钥管理服务器向导的第 2 步（上传服务器证书）。

6. 如果需要替换服务器证书，请选择 * 浏览 * 并上传新文件。
7. 选择 * 下一步 * 。

   此时将显示编辑密钥管理服务器向导的第 3 步（上传客户端证书）。

8. 如果需要替换客户端证书和客户端证书专用密钥，请选择 * 浏览 * 并上传新文件。
9. 选择 * 保存 * 。

   测试密钥管理服务器与受影响站点上的所有节点加密设备节点之间的连接。如果所有节点连接均有效，并且在 KMS 上找到正确的密钥，则密钥管理服务器将添加到密钥管理服务器页面上的表中。

10. 如果显示错误消息，请查看消息详细信息，然后选择 * 确定 * 。

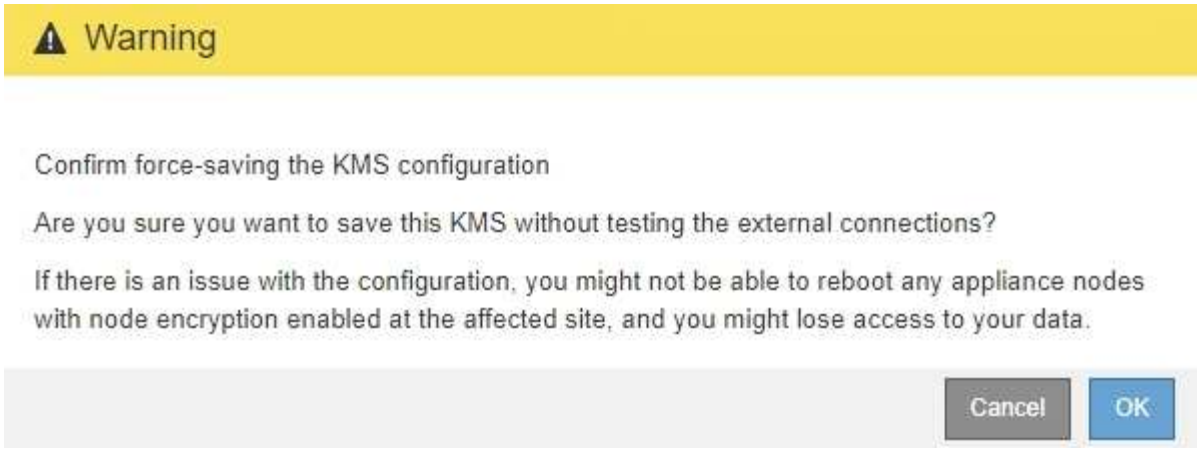
    例如，如果为此 KMS 选择的站点已由另一个 KMS 管理，或者连接测试失败，则可能会收到 422 ： Unprocessable Entity 错误。

11. 如果在解决连接错误之前需要保存当前配置，请选择 * 强制保存 * 。

    > ⓘ 选择 * 强制保存 * 可保存 KMS 配置，但不会测试每个设备与该 KMS 的外部连接。如果具有此配置的问题描述 ，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

    此时将保存 KMS 配置。

12. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 * 。



已保存 KMS 配置，但未测试与 KMS 的连接。

删除密钥管理服务器（ **KMS** ）

在某些情况下，您可能需要删除密钥管理服务器。例如，如果您已停用站点，则可能需要删除站点专用的 KMS 。

您需要的内容

- 您已查看 使用密钥管理服务器的注意事项和要求。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。

关于此任务

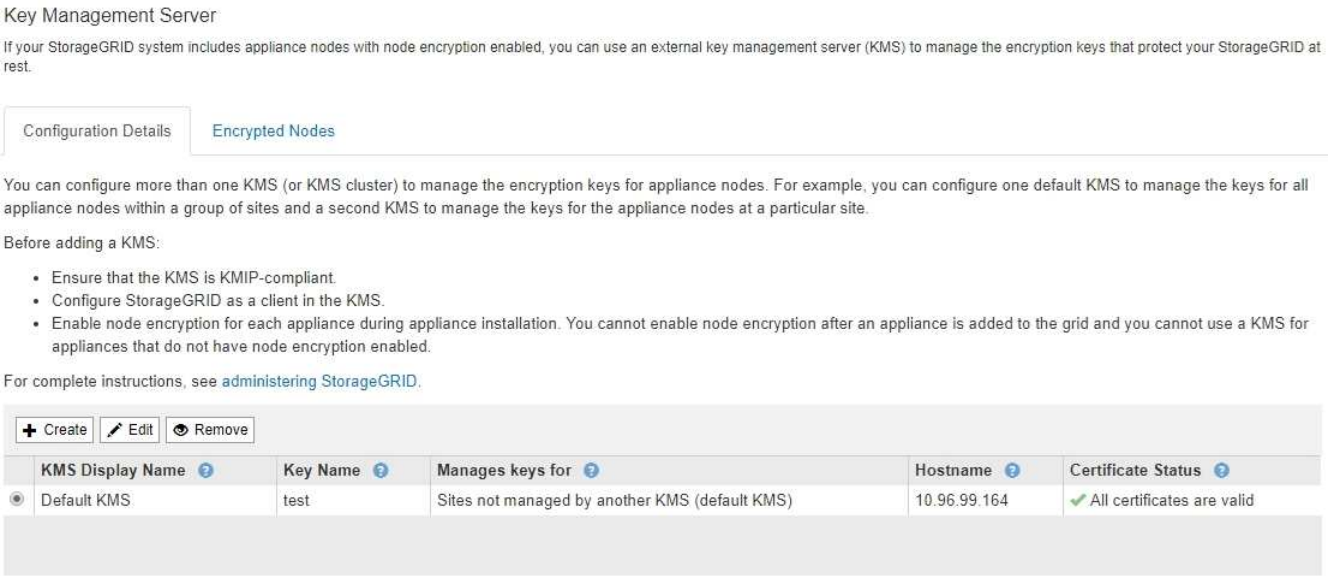
在以下情况下，您可以删除 KMS ：

- 如果站点已停用，或者站点中没有启用节点加密的设备节点，则可以删除站点专用的 KMS 。
- 如果每个站点已存在站点专用的 KMS ，并且已启用设备节点加密，则可以删除默认 KMS 。

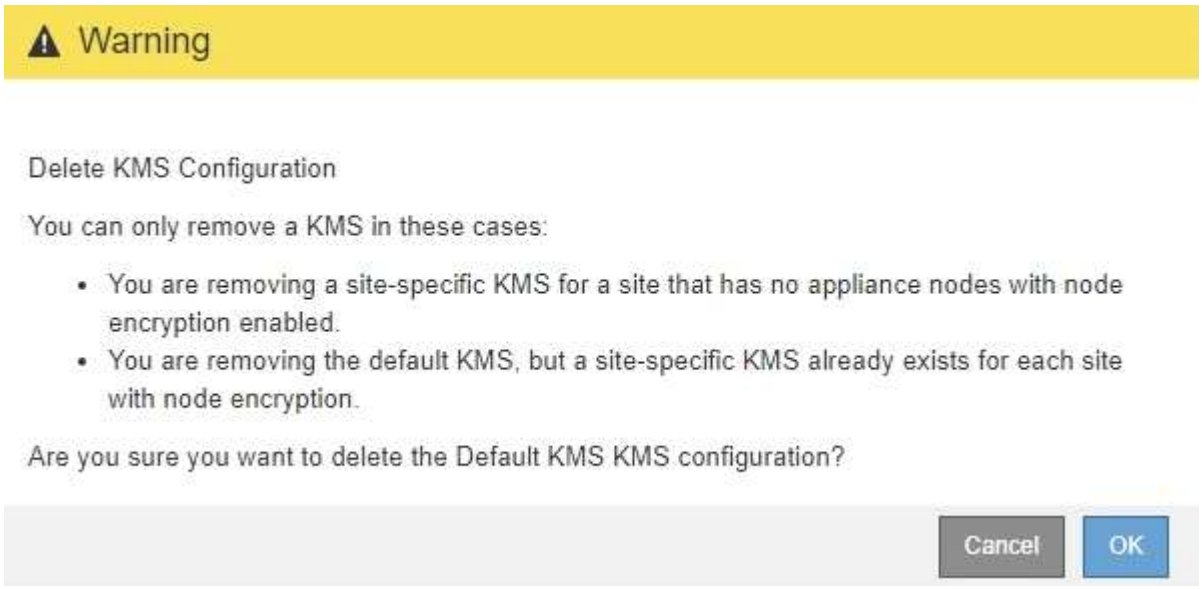
步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面，其中显示了已配置的所有密钥管理服务器。



2. 选择要删除的 KMS 的单选按钮，然后选择 * 删除 * 。
3. 查看警告对话框中的注意事项。



4. 选择 * 确定 * 。

   此时将删除 KMS 配置。

管理代理设置

配置存储代理设置

如果您使用的是平台服务或云存储池，则可以在存储节点和外部 S3 端点之间配置非透明代理。例如，您可能需要一个非透明代理来允许将平台服务消息发送到外部端点，例如 Internet 上的端点。

您需要的内容

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

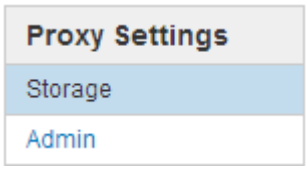
关于此任务

您可以为单个存储代理配置设置。

步骤

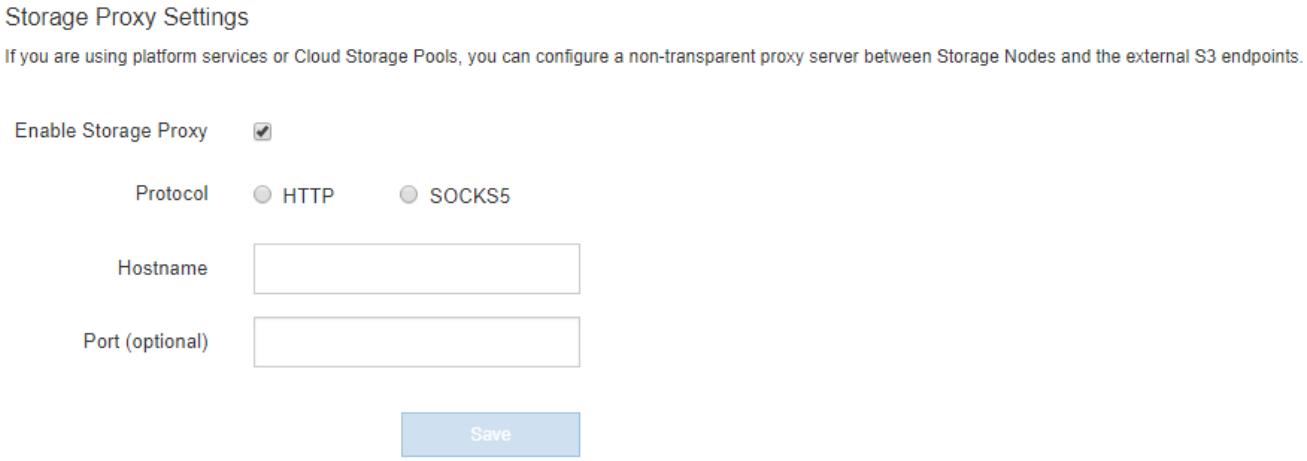
1. 选择 * 配置 * > * 安全性 * > * 代理设置 * 。

   此时将显示存储代理设置页面。默认情况下，在边栏菜单中选择了 * 存储 * 。



2. 选中 * 启用存储代理 * 复选框。

   此时将显示用于配置存储代理的字段。



3. 为非透明存储代理选择协议。
4. 输入代理服务器的主机名或 IP 地址。
5. （可选）输入用于连接到代理服务器的端口。

   如果对协议使用默认端口，则可以将此字段留空： 80 表示 HTTP ， 1080 表示 SOCKS5 。

6. 选择 * 保存 * 。

   保存存储代理后，可以配置和测试平台服务或云存储池的新端点。

   代理更改可能需要长达 10 分钟才能生效。

7. 检查代理服务器的设置，以确保不会阻止来自 StorageGRID 的平台服务相关消息。

完成后

如果需要禁用存储代理，请取消选中 * 启用存储代理 * 复选框，然后选择 * 保存 * 。

相关信息

- 用于平台服务的网络和端口
- 使用 ILM 管理对象

配置管理员代理设置

如果使用 HTTP 或 HTTPS 发送 AutoSupport 消息（请参见 配置 AutoSupport），您可以在管理节点和技术支持（ AutoSupport ）之间配置非透明代理服务器。

您需要的内容

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

关于此任务

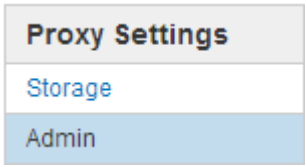
您可以为单个管理员代理配置设置。

步骤

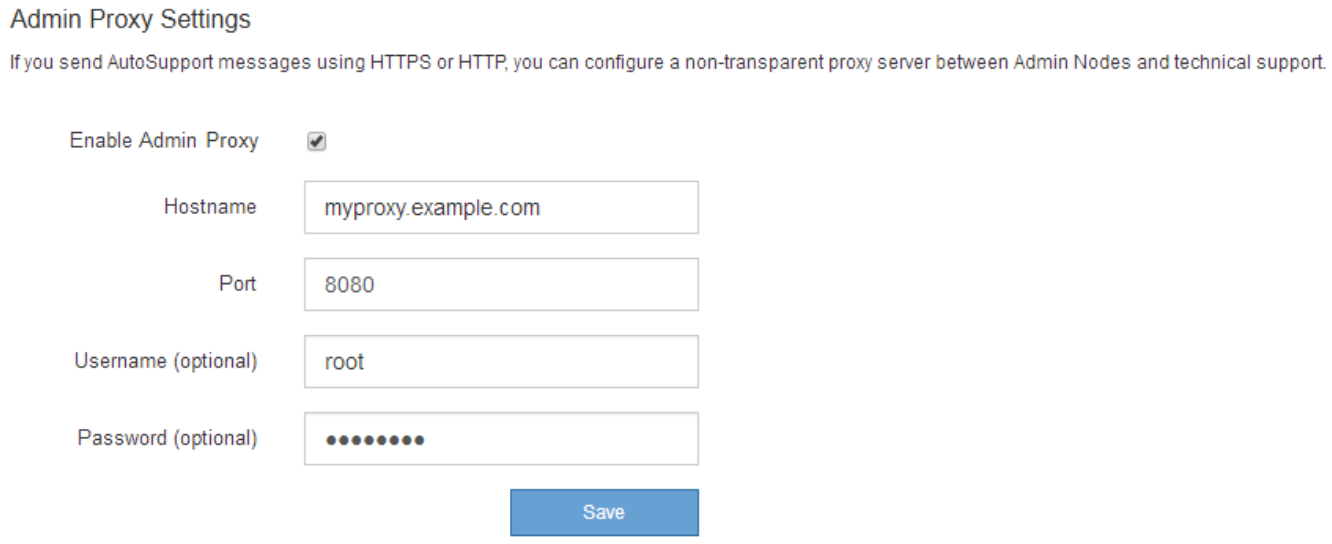
1. 选择 * 配置 * > * 安全性 * > * 代理设置 * 。

   此时将显示 Admin Proxy Settings 页面。默认情况下，在边栏菜单中选择了 * 存储 * 。

2. 从边栏菜单中选择 * 管理 * 。



3. 选中 * 启用管理代理 * 复选框。



4. 输入代理服务器的主机名或 IP 地址。
5. 输入用于连接到代理服务器的端口。
6. （可选）输入代理用户名。

   如果您的代理服务器不需要用户名，请将此字段留空。

7. （可选）输入代理密码。

   如果您的代理服务器不需要密码，请将此字段留空。

8. 选择 * 保存 * 。

   保存管理代理后，将在管理节点和技术支持之间配置代理服务器。

   代理更改可能需要长达 10 分钟才能生效。

9. 如果需要禁用代理，请取消选中 * 启用管理代理 * 复选框，然后选择 * 保存 * 。

管理不可信的客户端网络

Manage Untrusted Client Networks ： 概述

如果您使用的是客户端网络，则可以通过仅在显式配置的端点上接受入站客户端流量来帮助保护 StorageGRID 免受恶意攻击。

默认情况下，每个网格节点上的客户端网络均为 *trusted* 。也就是说，默认情况下， StorageGRID 会信任所有可用外部端口上与每个网格节点的入站连接（请参见中有关外部通信的信息 网络连接准则）。

您可以通过指定每个节点上的客户端网络为 *untrused_* 来减少对 StorageGRID 系统的恶意攻击威胁。如果节点的客户端网络不可信，则节点仅接受显式配置为负载平衡器端点的端口上的入站连接。请参见 配置负载平衡器端点。

示例 **1** ： 网关节点仅接受 **HTTPS S3** 请求

假设您希望网关节点拒绝客户端网络上除 HTTPS S3 请求以外的所有入站流量。您应执行以下常规步骤：

1. 在负载平衡器端点页面中，通过 HTTPS 在端口 443 上为 S3 配置负载平衡器端点。
2. 在不可信客户端网络页面中，指定网关节点上的客户端网络不可信。

保存配置后，网关节点客户端网络上的所有入站流量都会被丢弃，但端口 443 上的 HTTPS S3 请求和 ICMP 回显（ ping ）请求除外。

示例 **2** ： 存储节点发送 **S3** 平台服务请求

假设您要从存储节点启用出站 S3 平台服务流量，但要阻止与客户端网络上的该存储节点建立任何入站连接。您应执行此常规步骤：

- 在不可信客户端网络页面中，指示存储节点上的客户端网络不可信。

保存配置后，存储节点将不再接受客户端网络上的任何传入流量，但它仍允许向 Amazon Web Services 发出出

站请求。

指定节点的客户端网络不可信

如果您使用的是客户端网络，则可以指定每个节点的客户端网络是可信还是不可信。您还可以为扩展中添加的新节点指定默认设置。

您需要的内容

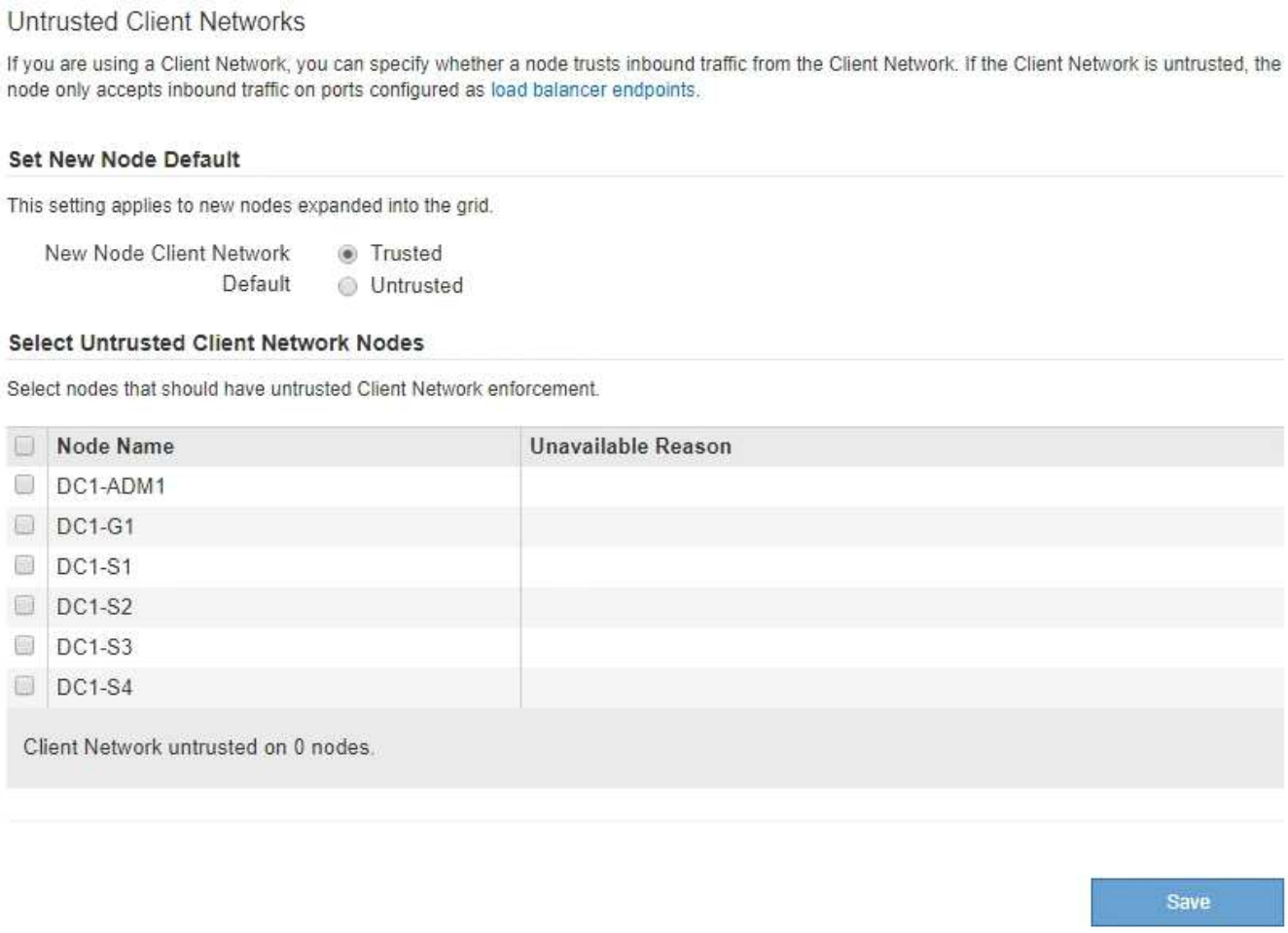
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 如果您希望管理节点或网关节点仅在显式配置的端点上接受入站流量，则已定义负载平衡器端点。

> 如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

步骤

1. 选择 * 配置 * > * 安全性 * > * 不可信客户端网络 * 。

   不可信客户端网络页面列出了 StorageGRID 系统中的所有节点。如果节点上的客户端网络必须可信，则不可用原因列将包含一个条目。



2. 在 * 设置新节点默认值 * 部分中，指定在扩展操作步骤 的网格中添加新节点时应采用的默认设置。

- * 可信 *：在扩展中添加节点时，其客户端网络是可信的。
- * 不可信 *：在扩展中添加节点时，其客户端网络不可信。根据需要，您可以返回此页面以更改特定新节点的设置。

> 此设置不会影响 StorageGRID 系统中的现有节点。

3. 在 * 选择不可信客户端网络节点 * 部分中，选择应仅允许在显式配置的负载平衡器端点上进行客户端连接的节点。

   您可以选中或取消选中标题中的复选框以选择或取消选择所有节点。

4. 选择 * 保存 * 。

   此时将立即添加并强制实施新的防火墙规则。如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

管理租户

管理租户

作为网格管理员，您可以创建和管理 S3 和 Swift 客户端用来存储和检索对象，监控存储使用情况以及管理客户端使用 StorageGRID 系统能够执行的操作的租户帐户。

什么是租户帐户？

租户帐户允许使用简单存储服务（ S3 ） REST API 或 Swift REST API 的客户端应用程序在 StorageGRID 上存储和检索对象。

每个租户帐户都支持使用一个协议，您可以在创建帐户时指定该协议。要将对象存储和检索到使用这两种协议的 StorageGRID 系统，您必须创建两个租户帐户：一个用于 S3 分段和对象，一个用于 Swift 容器和对象。每个租户帐户都有自己的帐户 ID ，授权组和用户，分段或容器以及对象。

或者，如果要将系统上存储的对象隔离为不同的实体，则可以创建其他租户帐户。例如，您可以在以下任一使用情形中设置多个租户帐户：

- * 企业用例： * 如果您在企业应用程序中管理 StorageGRID 系统，则可能需要按组织中的不同部门隔离网格的对象存储。在这种情况下，您可以为营销部门，客户支持部门，人力资源部门等创建租户帐户。

  > 如果使用 S3 客户端协议，则只需使用 S3 分段和分段策略来隔离企业中各个部门之间的对象即可。您不需要使用租户帐户。有关详细信息，请参见实施 S3 客户端应用程序的说明。

- * 服务提供商用例： * 如果您将 StorageGRID 系统作为服务提供商进行管理，则可以按要在网格上租用存储的不同实体来隔离网格的对象存储。在这种情况下，您将为公司 A ，公司 B ，公司 C 等创建租户帐户。

创建和配置租户帐户

创建租户帐户时，您可以指定以下信息：

- 租户帐户的显示名称。
- 租户帐户（ S3 或 Swift ）将使用哪种客户端协议。

- 对于 S3 租户帐户：租户帐户是否有权对 S3 分段使用平台服务。如果您允许租户帐户使用平台服务，则必须确保已将网格配置为支持其使用。请 `M" 管理平台服务 "` 。
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。如果超过配额，租户将无法创建新对象。

> 租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。

- 如果为 StorageGRID 系统启用了身份联合，则哪个联合组具有 root 访问权限来配置租户帐户。
- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。

创建租户帐户后，您可以执行以下任务：

- * 管理网格的平台服务 * ：如果您为租户帐户启用平台服务，请确保您了解如何传送平台服务消息以及使用平台服务对 StorageGRID 部署的网络要求。
- * 监控租户帐户的存储使用情况 * ：租户开始使用其帐户后，您可以使用 Grid Manager 监控每个租户占用的存储容量。

> 如果节点与网格中的其他节点隔离，则租户的存储使用量值可能会过时。恢复网络连接后，总数将更新。

  如果已为租户设置配额，则可以启用 * 租户配额使用量高 * 警报以确定租户是否正在使用其配额。如果启用，则在租户已使用其配额的 90% 时触发此警报。有关详细信息，请参见 StorageGRID 监控和故障排除说明中的警报参考。

- * 配置客户端操作 * ：您可以配置是否禁止某些类型的客户端操作。

配置 **S3** 租户

创建 S3 租户帐户后，租户用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享）并创建本地组和用户
- 管理 S3 访问密钥
- 创建和管理 S3 存储分段
- 监控存储使用情况
- 使用平台服务（如果已启用）

> S3 租户用户可以使用租户管理器创建和管理 S3 访问密钥和存储分段，但必须使用 S3 客户端应用程序载入和管理对象。

配置 **Swift** 租户

创建 Swift 租户帐户后，租户的 root 用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享），并创建本地组和用户
- 监控存储使用情况

Swift 用户必须具有 root 访问权限才能访问租户管理器。但是，" 根 " 访问权限不允许用户通过 Swift REST API 的身份验证来创建容器和载入对象。用户必须具有 Swift 管理员权限才能向 Swift REST API 进行身份验证。

相关信息

使用租户帐户

创建租户帐户

您必须至少创建一个租户帐户，才能控制对 StorageGRID 系统中存储的访问。

创建租户帐户时，您可以指定名称，客户端协议以及存储配额（可选）。如果为 StorageGRID 启用了单点登录（ SSO ），则还可以指定具有 root 访问权限的联合组来配置租户帐户。如果 StorageGRID 不使用单点登录，则还必须指定租户帐户是否使用其自己的身份源，并为租户的本地 root 用户配置初始密码。

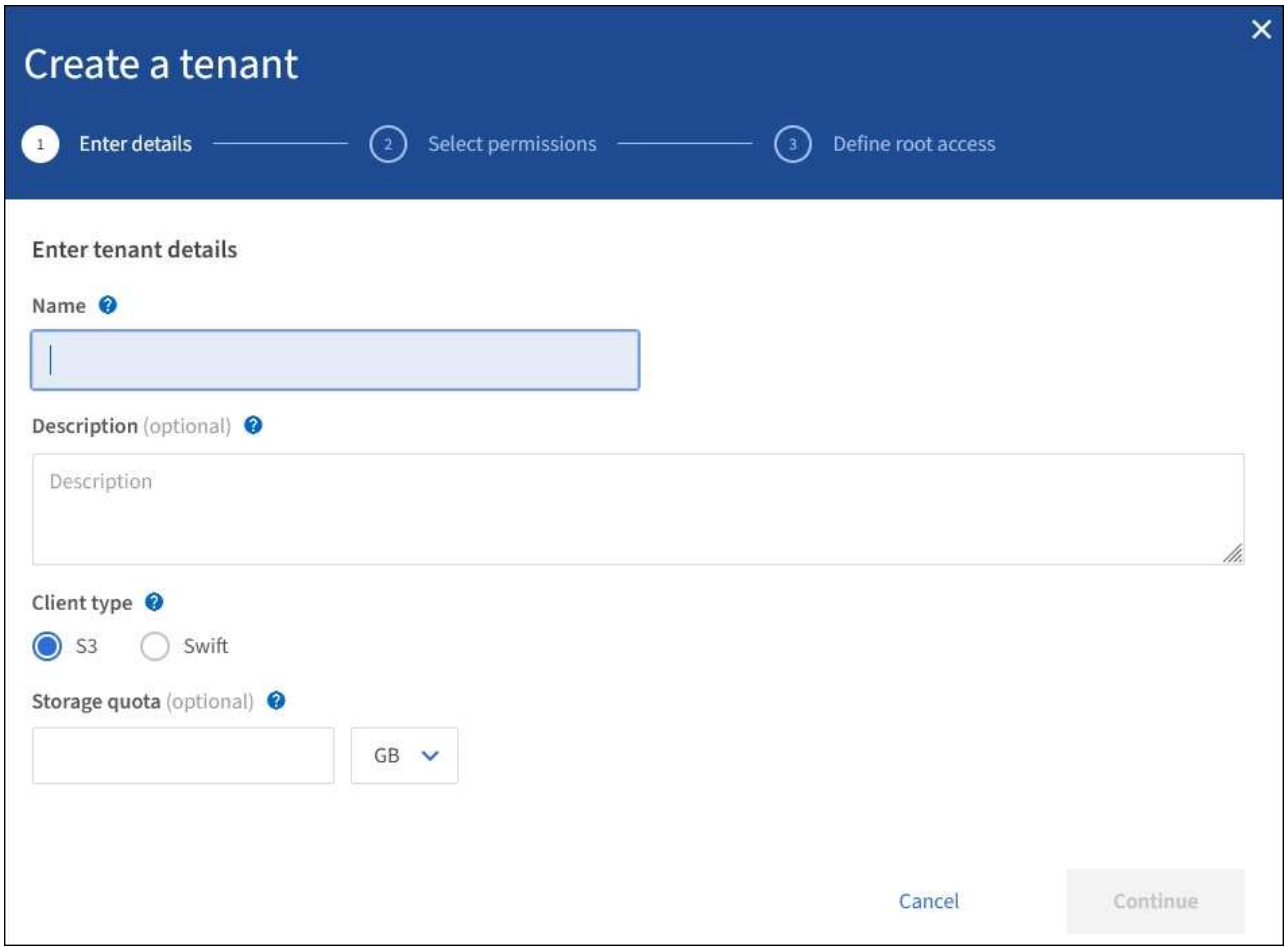
网格管理器提供了一个向导，用于指导您完成创建租户帐户的步骤。这些步骤因是否而异 身份联合 和 单点登录 已配置，并且您用于创建租户帐户的网格管理器帐户是否属于具有 root 访问权限的管理组。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 如果租户帐户将使用为网格管理器配置的身份源，并且您要将租户帐户的 root 访问权限授予某个联合组，则您已将该联合组导入到网格管理器中。您无需为此管理员组分配任何 Grid Manager 权限。请参见 管理组的管理说明。

步骤

1. 选择 * 租户 * 。
2. 选择 * 创建 * ，然后为租户输入以下信息：
   a. * 名称 * ： 输入租户帐户的名称。租户名称不必唯一。创建租户帐户时，它会收到一个唯一的数字帐户 ID 。
   b. * 问题描述 * （可选）： 输入有助于识别租户的问题描述 。
   c. * 客户端类型 * ： 选择客户端类型为 * S3 * 或 * Swift* 。
   d. * 存储配额 * （可选）： 如果希望此租户具有存储配额，请为配额输入一个数值，然后选择正确的单位（ GB ， TB 或 PB ）。



3. 选择 * 继续 * 并配置 S3 或 Swift 租户。

S3 租户

为租户选择适当的权限。其中某些权限还有其他要求。有关详细信息，请参见每个权限的联机帮助。

- 允许平台服务
- 使用自己的身份源（仅当未使用 SSO 时才可选择）
- 允许 S3 选择（请参见 管理租户帐户的 S3 Select）

Swift 租户

如果租户要使用自己的身份源，请选择 * 使用自己的身份源 * （只有在未使用 SSO 时才可选择）。

1. 选择 * 继续 * 并为租户帐户定义 root 访问权限。

未配置身份联合

1. 输入本地 root 用户的密码。
2. 选择 * 创建租户 * 。

已启用 **SSO**

为 StorageGRID 启用 SSO 后，租户必须使用为网格管理器配置的身份源。没有本地用户可以登录。您可以指定具有 root 访问权限的联合组来配置租户帐户。

1. 从网格管理器中选择一个现有联合组，以获得租户的初始 root 访问权限。

   如果您拥有足够的权限，则在选择此字段时，将列出网格管理器中的现有联合组。否则，请输入组的唯一名称。

2. 选择 * 创建租户 * 。

未启用 **SSO**

1. 根据租户是管理自己的组和用户，还是使用为网格管理器配置的身份源，完成表中所述的步骤。

租户是否要 ...	执行此操作 ...
管理自己的组和用户	a. 选择 * 使用自己的身份源 * 。 ◦ 注 * ： 如果选中此复选框，并且您要对租户组和用户使用身份联合，则租户必须配置自己的身份源。请参见 有关使用租户帐户的说明。 b. 为租户的本地 root 用户指定密码，然后选择 * 创建租户 * 。 c. 选择 * 以 root 用户身份登录 * 以配置租户，或者选择 * 完成 * 以稍后配置租户。
使用为网格管理器配置的组和用户	a. 执行以下操作之一或同时执行这两项操作： ◦ 从网格管理器中选择一个应具有租户初始根访问权限的现有联合组。 ▪ 注 * ： 如果您拥有足够的权限，则在选择此字段时，将列出网格管理器中的现有联合组。否则，请输入组的唯一名称。 ◦ 为租户的本地 root 用户指定密码。 b. 选择 * 创建租户 * 。

1. 要立即登录到租户，请执行以下操作：

   ◦ 如果您要通过受限端口访问网格管理器，请在租户表中选择 * 受限 * ，了解有关访问此租户帐户的更多信息。

   租户管理器的 URL 格式如下：

   `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`

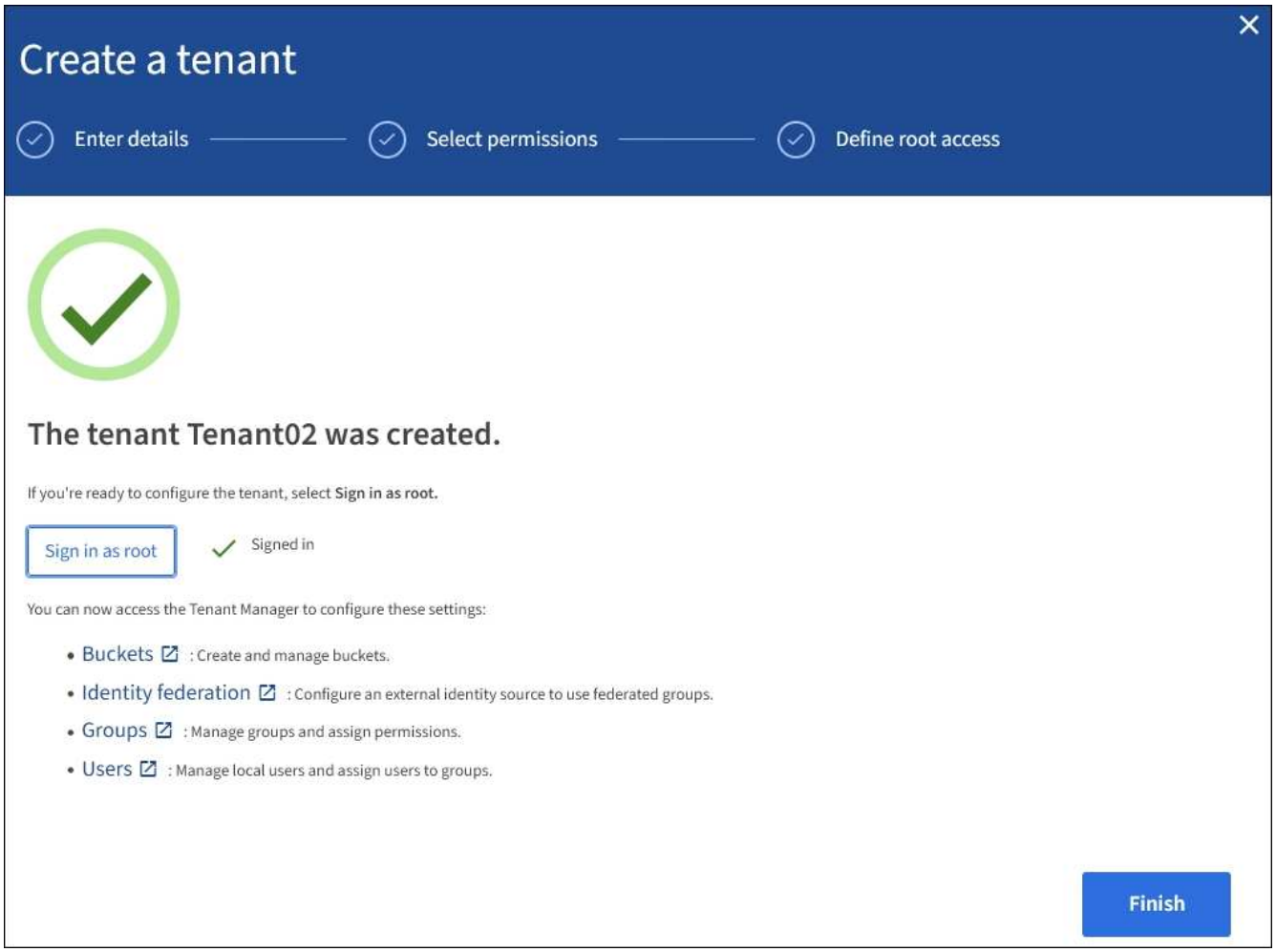
- ` fqdn_or_Admin_Node_IP_` 是完全限定域名或管理节点的 IP 地址
- ` 端口 _` 是仅租户端口
- ` *20-Digid-account-id*` 是租户的唯一帐户 ID

◦ 如果您正在通过端口 443 访问网格管理器，但未为本地 root 用户设置密码，请在网格管理器的租户表中选择 * 登录 * ，然后在 root 访问联合组中输入用户的凭据。

◦ 如果要通过端口 443 访问网格管理器并为本地 root 用户设置密码：

i. 选择 * 以 root 用户身份登录 * 以立即配置租户。

登录时，将显示用于配置分段或容器，身份联合，组和用户的链接。



i. 选择用于配置租户帐户的链接。

每个链接都会在租户管理器中打开相应的页面。要完成此页面，请参见 有关使用租户帐户的说明。

ii. 否则，请选择 * 完成 * 以稍后访问租户。

2. 要稍后访问租户，请执行以下操作：

如果您使用的是 ...	执行以下操作之一 ...
端口 443	• 在网格管理器中，选择 * 租户 * ，然后选择租户名称右侧的 * 登录 * 。 • 在 Web 浏览器中输入租户的 URL ： `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ ` fqdn_or_Admin_Node_IP_` 是完全限定域名或管理节点的 IP 地址 ◦ ` *20-Digid-account-id*` 是租户的唯一帐户 ID
受限端口	• 在网格管理器中，选择 * 租户 * ，然后选择 * 受限 * 。 • 在 Web 浏览器中输入租户的 URL ： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ ` fqdn_or_Admin_Node_IP_` 是完全限定域名或管理节点的 IP 地址 ◦ ` 端口 _` 是仅租户的受限端口 ◦ ` *20-Digid-account-id*` 是租户的唯一帐户 ID

相关信息

- 通过防火墙控制访问
- 管理 S3 租户帐户的平台服务

更改租户的本地 **root** 用户的密码

如果 root 用户被锁定在帐户之外，您可能需要更改租户的本地 root 用户的密码。

您需要的内容

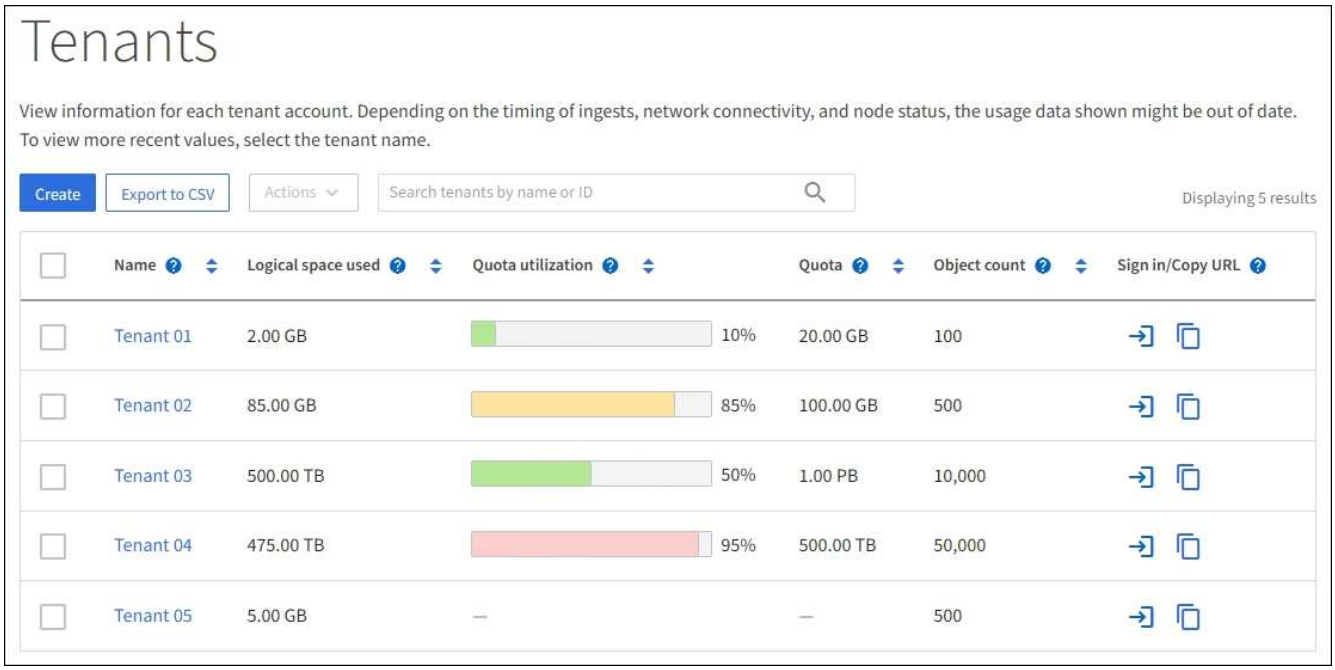
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。

关于此任务

如果为 StorageGRID 系统启用了单点登录（ SSO ），则本地 root 用户将无法登录到租户帐户。要执行 root 用户任务，用户必须属于对租户具有 root 访问权限的联合组。

步骤

1. 选择 * 租户 * 。



2. 选择要编辑的租户帐户。

   此时， "Actions" 按钮将变为启用状态。

3. 从 * 操作 * 下拉列表中，选择 * 更改 root 密码 * 。
4. 输入租户帐户的新密码。
5. 选择 * 保存 * 。

编辑租户帐户

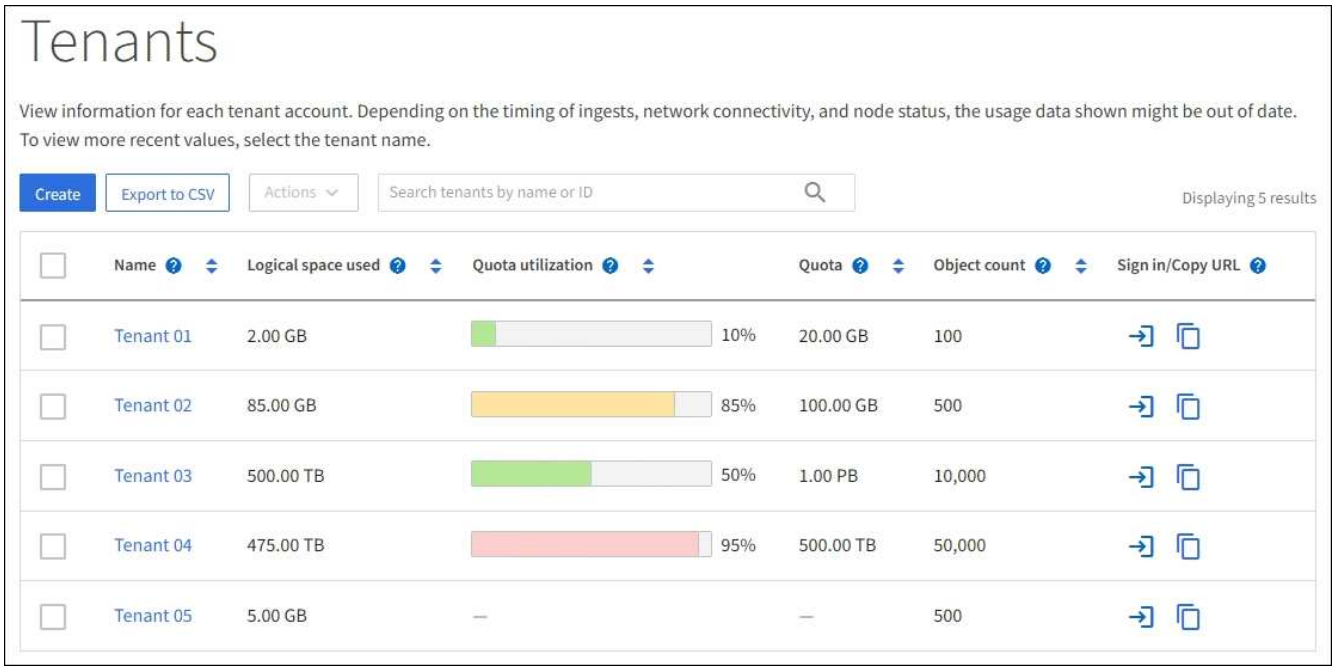
您可以编辑租户帐户以更改显示名称，更改身份源设置，允许或禁止平台服务或输入存储配额。

您需要的内容

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

步骤

1. 选择 * 租户 * 。

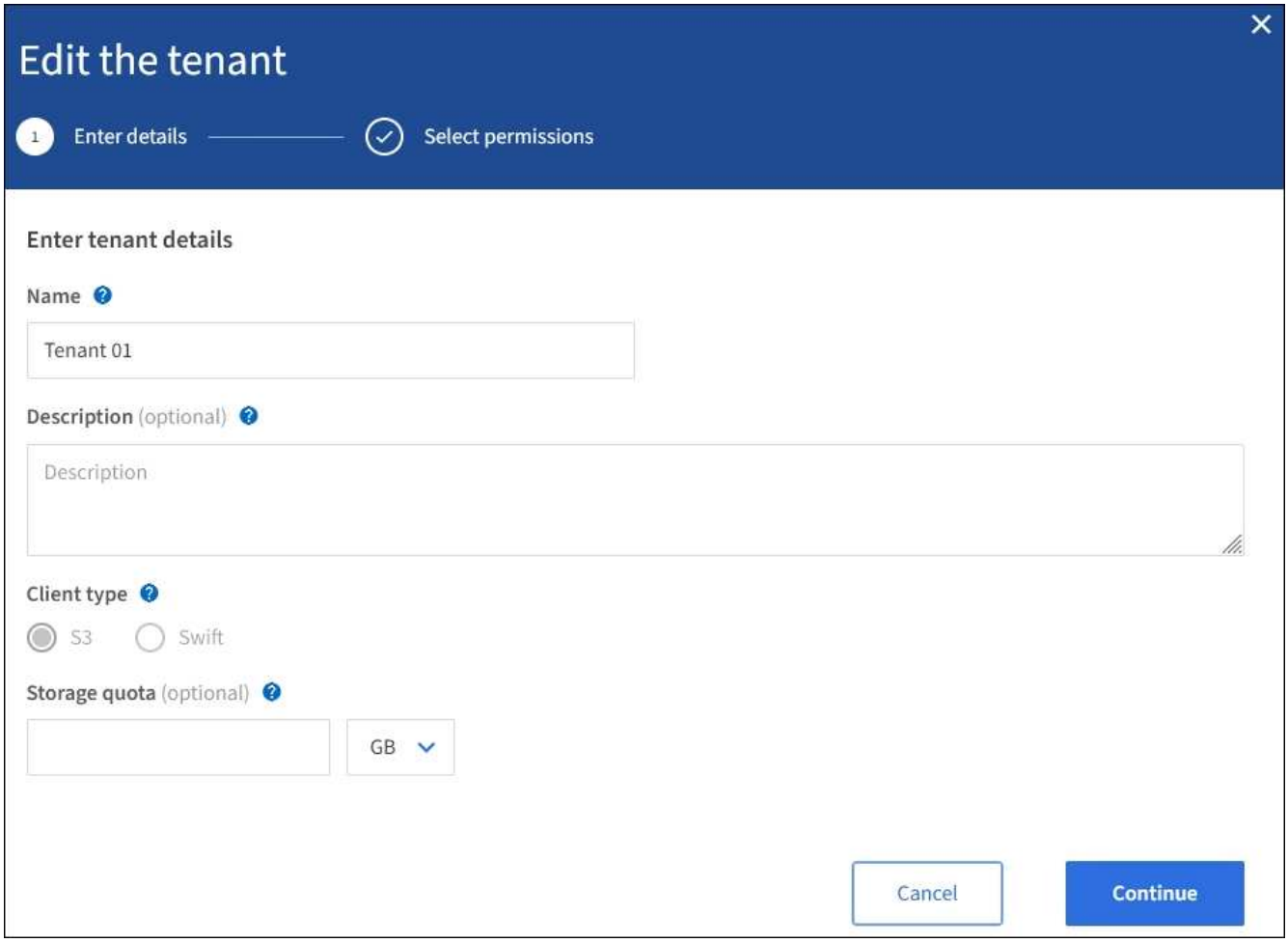


2. 选择要编辑的租户帐户。

   使用搜索框按名称或租户 ID 搜索租户帐户。

3. 从操作下拉列表中，选择 * 编辑 * 。

   此示例适用于不使用单点登录（ SSO ）的网格。此租户帐户未配置其自己的身份源。



4. 根据需要更改这些字段的值：
   - * 名称 *
   - * 问题描述 *
   - * 客户端类型 *
   - * 存储配额 *
5. 选择 * 继续 * 。
6. 选择或取消选择租户帐户的权限。
   - 如果对已在使用 * 平台服务 * 的租户禁用此服务，则其为 S3 分段配置的服务将停止工作。不会向租户发送任何错误消息。例如，如果租户已为 S3 存储分段配置了 CloudMirror 复制，则他们仍可将对象存储在存储分段中，但这些对象的副本将不再创建在已配置为端点的外部 S3 存储分段中。
   - 更改 * 使用自己的身份源 * 复选框的设置，以确定租户帐户是使用自己的身份源还是使用为网格管理器配置的身份源。

     如果 * 使用自己的身份源 * 复选框为：

     - 已禁用并选中租户已启用其自己的身份源。租户必须先禁用其身份源，然后才能使用为网格管理器配置的身份源。
     - 已禁用并取消选中，已为 StorageGRID 系统启用 SSO 。租户必须使用为网格管理器配置的身份源。

◦ 根据需要启用或禁用 * S3 Select* 。请参见 管理租户帐户的 S3 Select。

7. 选择 * 保存 * 。

相关信息

- 管理 S3 租户帐户的平台服务
- 使用租户帐户

删除租户帐户

如果要永久删除租户对系统的访问权限，可以删除租户帐户。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须已删除与租户帐户关联的所有分段（ S3 ），容器（ Swift ）和对象。

步骤

1. 选择 * 租户 * 。
2. 选择要删除的租户帐户。

   使用搜索框按名称或租户 ID 搜索租户帐户。

3. 从 * 操作 * 下拉列表中，选择 * 删除 * 。
4. 选择 * 确定 * 。

管理平台服务

管理 **S3** 租户帐户的平台服务

如果为 S3 租户帐户启用平台服务，则必须配置网格，以便租户可以访问使用这些服务所需的外部资源。

什么是平台服务?

平台服务包括 CloudMirror 复制，事件通知和搜索集成服务。

这些服务允许租户对其 S3 分段使用以下功能：

- * CloudMirror 复制 * ： StorageGRID CloudMirror 复制服务用于将特定对象从 StorageGRID 存储分段镜像到指定的外部目标。

  例如，您可以使用 CloudMirror 复制将特定客户记录镜像到 Amazon S3 ，然后利用 AWS 服务对数据执行分析。

  > 如果源存储分段启用了 S3 对象锁定，则不支持 CloudMirror 复制。

- * 通知 * ：每个存储分段的事件通知用于向指定的外部 Amazon Simple Notification Service （ SNS ）发送

有关对对象执行的特定操作的通知。

例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

> 虽然可以在启用了 S3 对象锁定的存储分段上配置事件通知，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留至日期和合法保留状态）。

- * 搜索集成服务 * ：搜索集成服务用于将 S3 对象元数据发送到指定的 Elasticsearch 索引，在此索引中可以使用外部服务搜索或分析元数据。

  例如，您可以将存储分段配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 跨存储分段执行搜索，并对对象元数据中存在的模式执行复杂的分析。

  > 虽然可以在启用了 S3 对象锁定的情况下在存储分段上配置 Elasticsearch 集成，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留截止日期和合法保留状态）。

通过平台服务，租户可以对其数据使用外部存储资源，通知服务以及搜索或分析服务。由于平台服务的目标位置通常位于 StorageGRID 部署外部，因此您必须确定是否要允许租户使用这些服务。如果是，则必须在创建或编辑租户帐户时启用平台服务。您还必须配置网络，使租户生成的平台服务消息能够访问其目标。

使用平台服务的建议

在使用平台服务之前，请注意以下建议：

- 如果 StorageGRID 系统中的 S3 存储分段同时启用了版本控制和 CloudMirror 复制，则还应为目标端点启用 S3 存储分段版本控制。这样， CloudMirror 复制就可以在端点上生成类似的对象版本。
- 如果 S3 请求需要进行 CloudMirror 复制，通知和搜索集成，则使用的活动租户不应超过 100 个。如果活动租户超过 100 个，则可能会导致 S3 客户端性能下降。
- 对无法完成的端点的请求将排队，最多 500 ， 000 个请求。此限制在活动租户之间平均共享。新租户可以暂时超过这 500 ， 000 个上限，这样新创建的租户就不会受到不公正的处罚。

相关信息

- 使用租户帐户
- 配置存储代理设置
- 监控和故障排除

用于平台服务的网络和端口

如果允许 S3 租户使用平台服务，则必须为网格配置网络连接，以确保平台服务消息可以传送到其目标。

在创建或更新 S3 租户帐户时，您可以为该租户帐户启用平台服务。如果启用了平台服务，则租户可以创建端点，用作 CloudMirror 复制，事件通知或从其 S3 存储分段搜索集成消息的目标。这些平台服务消息会从运行此 ADA 服务的存储节点发送到目标端点。

例如，租户可以配置以下类型的目标端点：

- 本地托管的 Elasticsearch 集群
- 一种支持接收简单通知服务（ SNS ）消息的本地应用程序
- 同一个或另一个 StorageGRID 实例上本地托管的 S3 存储分段
- 外部端点，例如 Amazon Web Services 上的端点。

要确保可以传送平台服务消息，您必须配置一个或多个包含此 ADA 存储节点的网络。您必须确保可使用以下端口向目标端点发送平台服务消息。

默认情况下，平台服务消息在以下端口上发送：

- * 80* ： 对于以 http 开头的端点 URI
- * 443 ： 对于以 https 开头的端点 URI

租户可以在创建或编辑端点时指定其他端口。

> 如果使用 StorageGRID 部署作为 CloudMirror 复制的目标，则可能会在 80 或 443 以外的端口上收到复制消息。确保已在端点中指定目标 StorageGRID 部署用于 S3 的端口。

如果使用非透明代理服务器，则还必须使用 配置存储代理设置 允许将消息发送到外部端点，例如 Internet 上的端点。

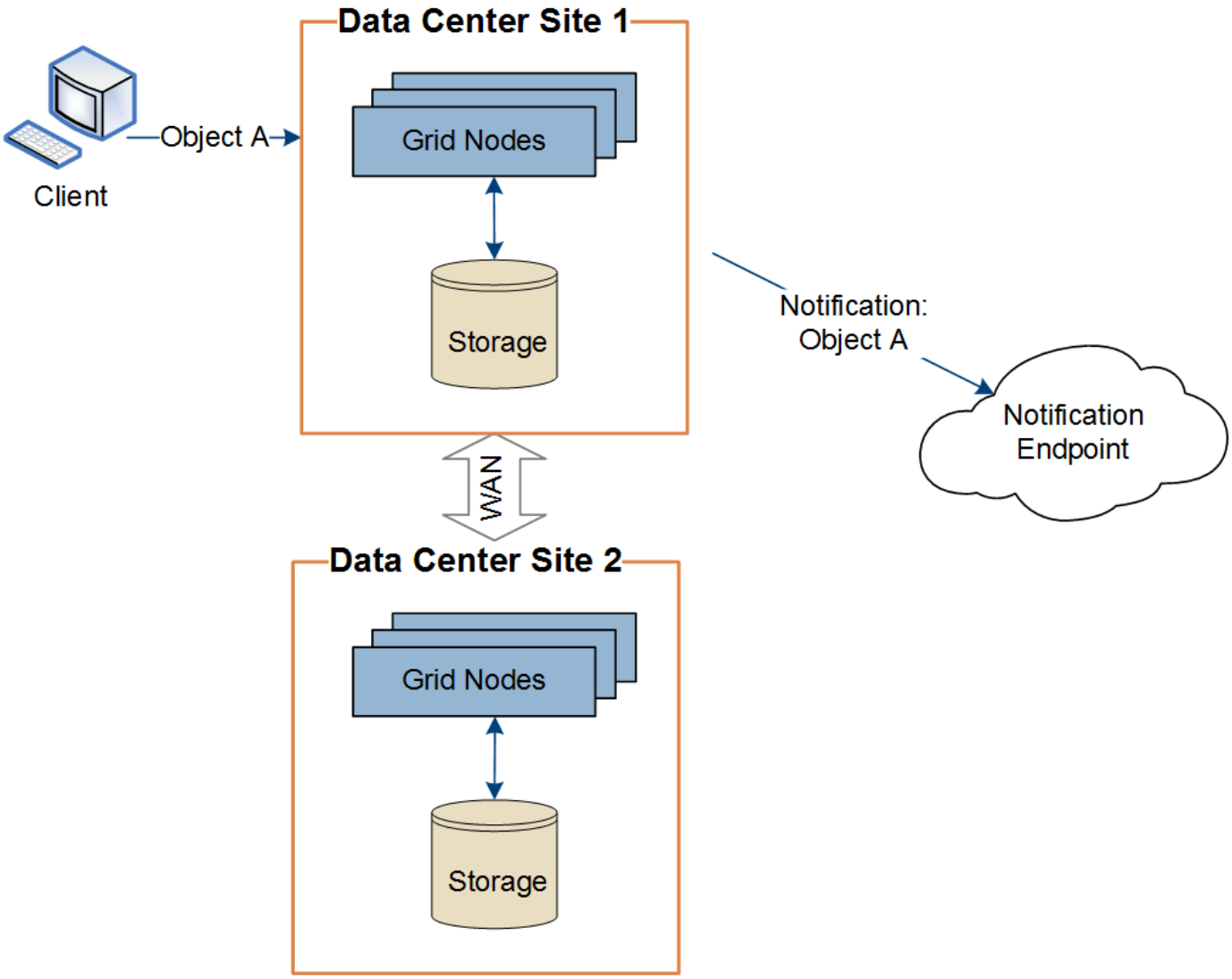
相关信息

- 使用租户帐户

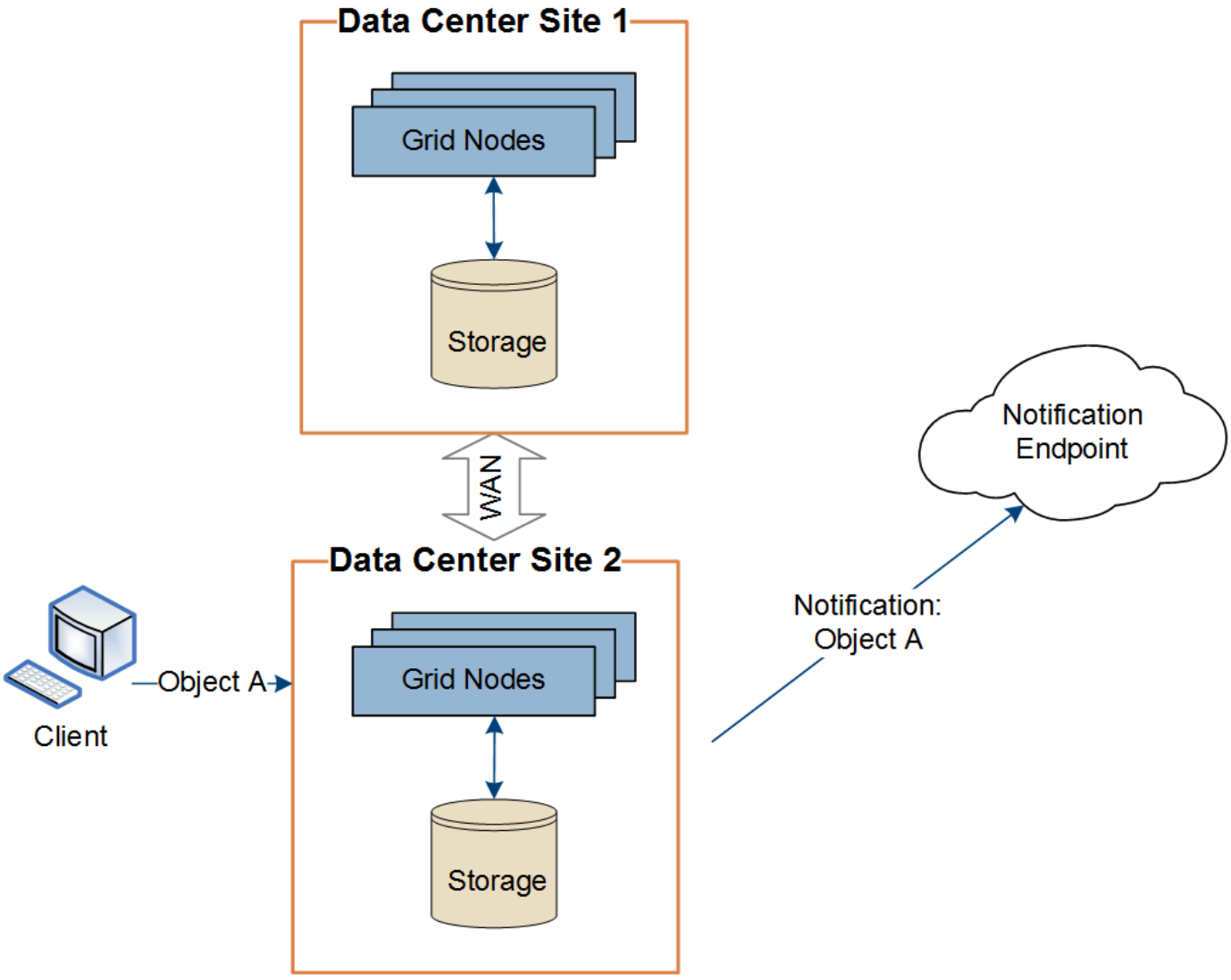
按站点交付平台服务消息

所有平台服务操作均按站点执行。

也就是说，如果租户使用客户端通过连接到数据中心站点 1 的网关节点对对象执行 S3 API 创建操作，则会从数据中心站点 1 触发并发送有关该操作的通知。



如果客户端随后从数据中心站点 2 对同一对象执行 S3 API 删除操作，则会从数据中心站点 2 触发并发送有关删除操作的通知。



请确保在每个站点上配置网络，以便平台服务消息可以传送到其目标。

对平台服务进行故障排除

平台服务中使用的端点由租户管理器中的租户用户创建和维护；但是，如果租户在配置或使用平台服务时遇到问题，您可能可以使用网格管理器帮助解决问题描述 。

新端点出现问题

租户必须先使用租户管理器创建一个或多个端点，才能使用平台服务。每个端点表示一个平台服务的外部目标，例如 StorageGRID S3 存储分段， Amazon Web 服务分段，简单通知服务主题或本地或 AWS 上托管的 Elasticsearch 集群。每个端点都包括外部资源的位置以及访问该资源所需的凭据。

租户创建端点时， StorageGRID 系统会验证此端点是否存在，以及是否可以使用指定的凭据访问此端点。系统会从每个站点的一个节点验证与端点的连接。

如果端点验证失败，则会显示一条错误消息，说明端点验证失败的原因。租户用户应解析问题描述 ，然后重新尝试创建端点。

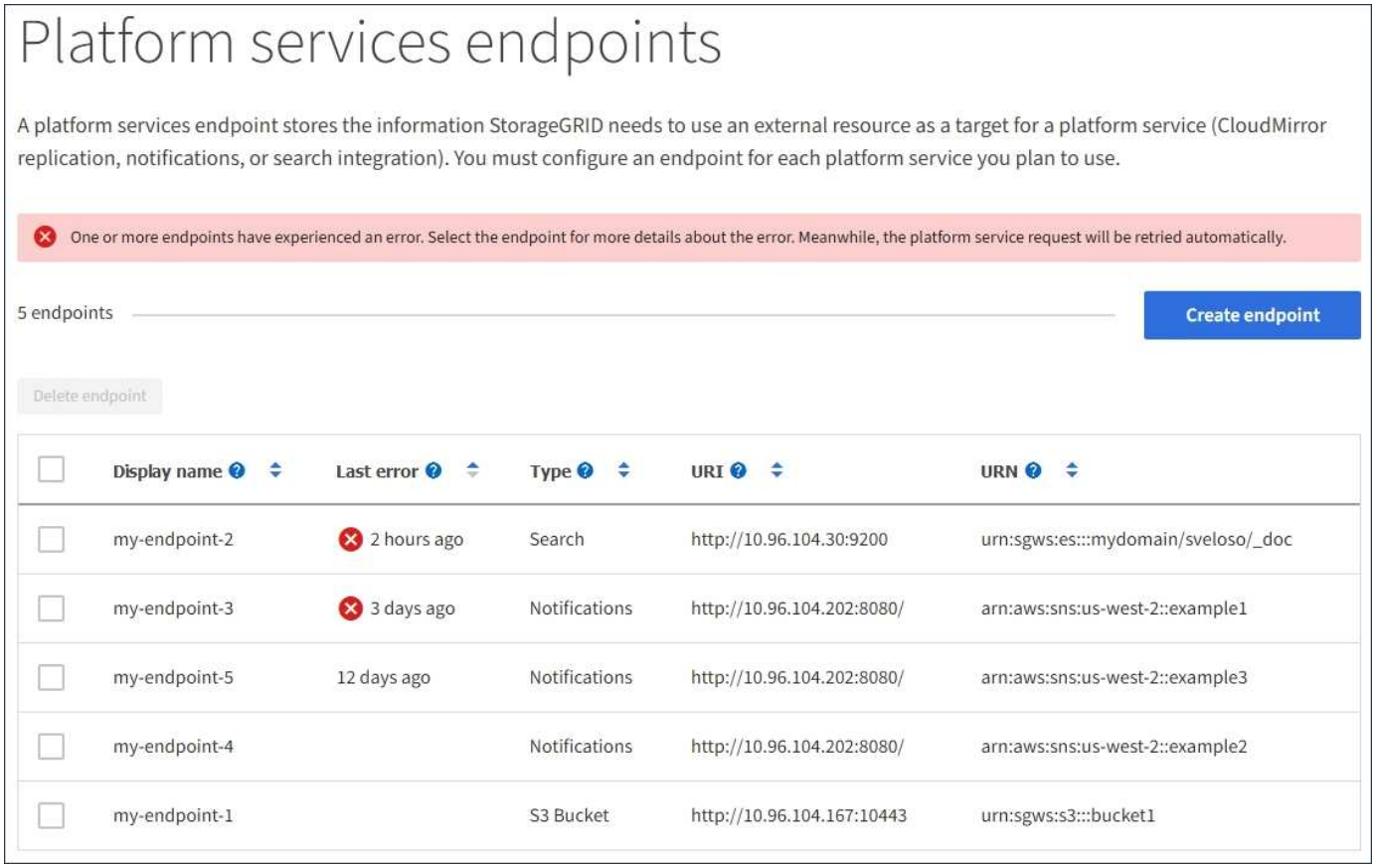
如果未为租户帐户启用平台服务，则端点创建将失败。

现有端点存在问题

如果在 StorageGRID 尝试访问现有端点时发生错误，则租户管理器的信息板上将显示一条消息。

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

租户用户可以转到 " 端点 " 页面查看每个端点的最新错误消息，并确定错误发生多长时间。"* 最后一个错误 * " 列显示每个端点的最新错误消息，并指示错误发生的时间。包含的错误 图标在过去 7 天内出现。



* 最后一个错误 * 列中的某些错误消息可能会在圆括号中包含日志 ID 。网格管理员或技术支持可以使用此 ID 在 bycast.log 中查找有关此错误的更多详细信息。

与代理服务器相关的问题

如果您在存储节点和平台服务端点之间配置了存储代理，则如果您的代理服务不允许来自 StorageGRID 的消息，则可能会发生错误。要解决这些问题，请检查代理服务器的设置，以确保不会阻止与平台服务相关的消息。

确定是否发生错误

如果在过去 7 天内发生任何端点错误，则租户管理器中的信息板将显示一条警报消息。您可以转到 " 端点 " 页面以查看有关此错误的更多详细信息。

客户端操作失败

某些平台服务问题可能会导致 S3 存储分段上的发生原因 客户端操作失败。例如，如果内部复制状态计算机（ RSM ）服务停止，或者排队等待传送的平台服务消息太多， S3 客户端操作将失败。

要检查服务状态，请执行以下操作：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* > * SSM* > * 服务 * 。

可恢复和不可恢复的端点错误

创建端点后，平台服务请求错误可能会因各种原因而发生。某些错误可通过用户干预进行恢复。例如，可能会发生可恢复的错误，原因如下：

- 用户凭据已删除或已过期。
- 目标存储分段不存在。
- 无法传送通知。

如果 StorageGRID 遇到可恢复的错误，将重试平台服务请求，直到成功。

其他错误不可恢复。例如，如果删除端点，则会发生不可恢复的错误。

如果 StorageGRID 遇到不可恢复的端点错误，则会在网格管理器中触发总事件（ SMTT） 原有警报。要查看总事件旧警报，请执行以下操作：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。
3. 在表顶部查看上次事件。

   事件消息也会在 ` /var/local/log/byncast-err.log` 中列出。
4. 按照 SMT 警报内容中提供的指导更正问题描述 。
5. 选择 * 配置 * 选项卡以重置事件计数。
6. 将尚未传送平台服务消息的对象通知租户。
7. 指示租户通过更新对象的元数据或标记来重新触发失败的复制或通知。

   租户可以重新提交现有值，以避免进行不必要的更改。

无法传送平台服务消息

如果目标遇到的问题描述 阻止其接受平台服务消息，则在存储分段上执行的客户端操作将成功，但不会传送平台服务消息。例如，如果更新了目标上的凭据，使 StorageGRID 无法再向目标服务进行身份验证，则可能会发生此错误。

如果由于不可恢复的错误而无法传送平台服务消息，则会在网格管理器中触发总事件（ SMTT） 原有警报。

降低平台服务请求的性能

如果发送请求的速率超过目标端点接收请求的速率， StorageGRID 软件可能会限制传入的存储分段 S3 请求。只有在等待发送到目标端点的请求积压时，才会发生限制。

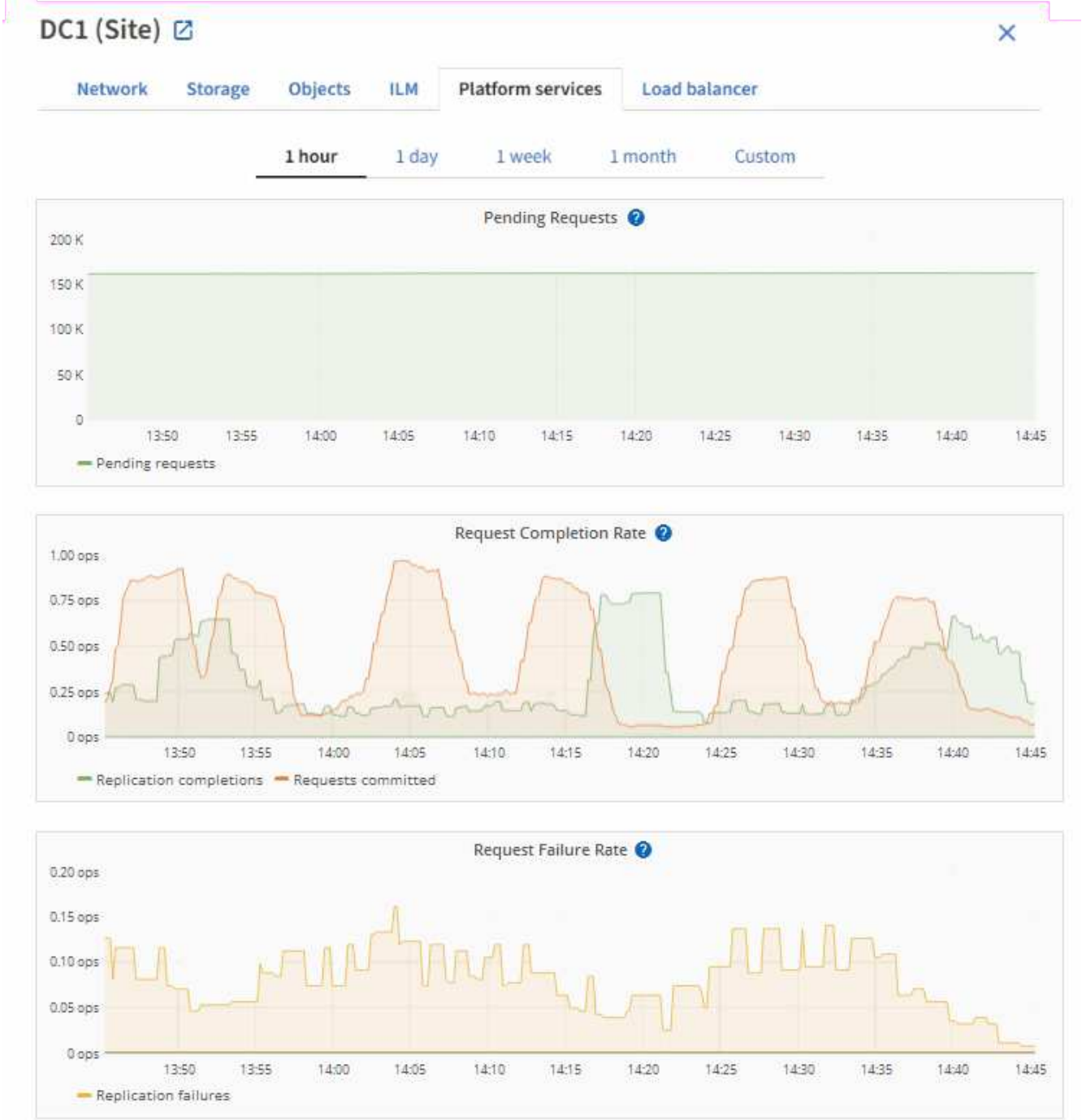
唯一明显的影响是，传入的 S3 请求执行时间较长。如果您开始检测到性能明显较慢，则应降低载入速率或使用容量较高的端点。如果积压的请求持续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。

CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求所涉及的数据传输通常多于搜索集成或事件通知请求。

平台服务请求失败

要查看平台服务的请求失败率，请执行以下操作：

1. 选择 * 节点 * 。
2. 选择 ***site*** > * 平台服务 * 。
3. 查看请求错误率图表。



平台服务不可用警报

" 平台服务不可用 * " 警报表示无法在站点上执行平台服务操作，因为运行或可用的 RSM 服务存储节点太少。

RSM 服务可确保将平台服务请求发送到其各自的端点。

要解决此警报，请确定站点上的哪些存储节点包含 RSM 服务。（ RSM 服务位于也包含此 ADC 服务的存储节点上。） 然后，确保这些存储节点中的大多数都在运行且可用。

如果某个站点上有多个包含 RSM 服务的存储节点出现故障，则该站点的任何待定平台服务请求都将丢失。

有关平台服务端点的其他故障排除指南

有关追加信息 对平台服务端点进行故障排除的信息，请参见的说明 使用租户帐户。

相关信息

- 监控和故障排除
- 配置存储代理设置

管理租户帐户的 **S3 Select**

您可以允许某些 S3 租户对单个对象使用 S3 Select 到问题描述 SelectObjectContent 请求。

S3 Select 可以高效地搜索大量数据，而无需部署数据库和相关资源即可启用搜索。它还可以降低检索数据的成本和延迟。

什么是 **S3 Select** ？

S3 Select 允许 S3 客户端使用 SelectObjectContent 请求仅筛选和检索对象所需的数据。S3 Select 的 StorageGRID 实施包括部分 S3 Select 命令和功能。

使用 **S3 Select** 的注意事项和要求

对于 S3 Select 查询， StorageGRID 需要满足以下要求：

- 要查询的对象为 CSV 格式，或者为包含 CSV 格式文件的 GZIP 或 bzip 2 压缩文件。
- 网格管理员必须授予租户 S3 Select 功能。选择 * 允许 S3 选择 * 时间 创建租户 或 编辑租户。
- SelectObjectContent 请求必须发送到 StorageGRID 负载平衡器端点。端点使用的管理节点和网关节点必须是 SG100 或 SG1000 设备节点或基于 VMware 的软件节点。

请注意以下限制：

- 不支持裸机负载平衡器节点。
- 查询不能直接发送到存储节点。
- 不支持通过已弃用的 CLB 服务发送的查询。

> SelectObjectContent 请求会降低所有 S3 客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。

请参见 有关使用 S3 Select 的说明。

以查看 Grafana 图表 对于随时间变化的 S3 Select 操作，请在网格管理器中选择 * 支持 * > * 工具 * > * 指标 * 。

配置 **S3** 和 **Swift** 客户端连接

关于 **S3** 和 **Swift** 客户端连接

作为网格管理员，您可以管理控制 S3 和 Swift 租户如何将客户端应用程序连接到

StorageGRID 系统以存储和检索数据的配置选项。有多种不同的选项可满足不同的客户端和租户要求。

客户端应用程序可以通过连接到以下任一项来存储或检索对象：

- 管理节点或网关节点上的负载平衡器服务，或者也可以是管理节点或网关节点高可用性（ HA ）组的虚拟 IP 地址
- 网关节点上的 CLB 服务，或者也可以是网关节点高可用性组的虚拟 IP 地址

> CLB 服务已弃用。在 StorageGRID 11.3 版本之前配置的客户端可以继续在网关节点上使用 CLB 服务。所有其他依靠 StorageGRID 提供负载平衡的客户端应用程序都应使用负载平衡器服务进行连接。

- 存储节点，具有或不具有外部负载平衡器

您可以选择在 StorageGRID 系统上配置以下功能：

- * VLAN 接口 * ：您可以在管理节点和网关节点上创建虚拟 LAN （ VLAN ）接口，以隔离和分区客户端和租户流量，从而提高安全性，灵活性和性能。创建 VLAN 接口后，您可以将其添加到高可用性（ HA ）组中。
- * 高可用性组 * ：您可以为网关节点或管理节点的接口创建一个 HA 组来创建主动备份配置，也可以使用轮循 DNS 或第三方负载平衡器以及多个 HA 组来实现主动 - 主动配置。客户端连接使用 HA 组的虚拟 IP 地址进行。
- * 负载平衡器服务 * ：您可以通过为客户端连接创建负载平衡器端点来使客户端能够使用负载平衡器服务。创建负载平衡器端点时，您可以指定端口号，端点是否接受 HTTP 或 HTTPS 连接，将使用此端点的客户端类型（ S3 或 Swift ）以及用于 HTTPS 连接的证书（如果适用）。
- * 不可信客户端网络 * ：您可以通过将客户端网络配置为不可信来提高其安全性。如果客户端网络不可信，则客户端只能使用负载平衡器端点进行连接。

此外，您还可以为直接连接到存储节点或使用 CLB 服务（已弃用）连接到 StorageGRID 的客户端启用 HTTP ，并且可以为 S3 客户端配置 S3 API 端点域名。

摘要：客户端连接的 **IP** 地址和端口

客户端应用程序可以使用网格节点的 IP 地址以及该节点上服务的端口号连接到 StorageGRID 。如果配置了高可用性（ HA ）组，则客户端应用程序可以使用 HA 组的虚拟 IP 地址进行连接。

关于此任务

此表总结了客户端连接到 StorageGRID 的不同方式以及每种连接类型所使用的 IP 地址和端口。这些说明介绍了在已配置负载平衡器端点和高可用性（ HA ）组的情况下如何在网格管理器中查找此信息。

建立连接的位置	客户端连接到的服务	**IP** 地址	**Port**
HA 组	负载平衡器	HA 组的虚拟 IP 地址	• 负载平衡器端点端口

建立连接的位置	客户端连接到的服务	IP 地址	Port
HA 组	CLB • 注： * CLB 服务已弃用。	HA 组的虚拟 IP 地址	默认 S3 端口： • HTTPS： 8082 • HTTP： 8084 默认 Swift 端口： • HTTPS： 8083 • HTTP： 8085
管理节点	负载平衡器	管理节点的 IP 地址	• 负载平衡器端点端口
网关节点	负载平衡器	网关节点的 IP 地址	• 负载平衡器端点端口
网关节点	CLB • 注： * CLB 服务已弃用。	网关节点的 IP 地址 • 注意： * 默认情况下，CLB 和 LDR 的 HTTP 端口未启用。	默认 S3 端口： • HTTPS： 8082 • HTTP： 8084 默认 Swift 端口： • HTTPS： 8083 • HTTP： 8085
存储节点	LDR	存储节点的 IP 地址	默认 S3 端口： • HTTPS： 18082 • HTTP： 18084 默认 Swift 端口： • HTTPS： 18083 • HTTP： 18085

示例

要将 S3 客户端连接到网关节点 HA 组的负载平衡器端点，请使用以下结构化 URL：

- `https://VIP-of-HA-group:LB-endpoint-port`

例如，如果 HA 组的虚拟 IP 地址为 192.0.2.5 ，而 S3 负载平衡器端点的端口号为 10443 ，则 S3 客户端可以使用以下 URL 连接到 StorageGRID：

- ` https://192.0.2.5:10443`

要将 Swift 客户端连接到网关节点 HA 组的负载平衡器端点，请使用以下结构化 URL：

- `https://VIP-of-HA-group:LB-endpoint-port`

例如，如果 HA 组的虚拟 IP 地址为 192.0.2.6 ， Swift 负载平衡器端点的端口号为 10444 ，则 Swift 客户端可以使用以下 URL 连接到 StorageGRID ：

- ` https://192.0.2.6:10444`

可以为客户端用于连接到 StorageGRID 的 IP 地址配置 DNS 名称。请与本地网络管理员联系。

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 要查找网格节点的 IP 地址，请执行以下操作：
   a. 选择 * 节点 * 。
   b. 选择要连接到的管理节点，网关节点或存储节点。
   c. 选择 * 概述 * 选项卡。
   d. 在节点信息部分中，记下节点的 IP 地址。
   e. 选择 * 显示更多 * 可查看 IPv6 地址和接口映射。

      您可以建立从客户端应用程序到列表中任何 IP 地址的连接：

      - * eth0 ： * 网格网络
      - * eth1 ： * 管理网络（可选）
      - * eth2 ： * 客户端网络（可选）

      > 如果您正在查看管理节点或网关节点，并且该节点是高可用性组中的活动节点，则 eth2 上会显示 HA 组的虚拟 IP 地址。

3. 要查找高可用性组的虚拟 IP 地址，请执行以下操作：
   a. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。
   b. 在表中，记下 HA 组的虚拟 IP 地址。
4. 查找负载平衡器端点的端口号：
   a. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。

      此时将显示负载平衡器端点页面，其中显示了已配置的端点列表。

   b. 选择一个端点，然后选择 * 编辑端点 * 。

      此时将打开编辑端点窗口，并显示有关此端点的其他详细信息。

   c. 确认已将选定端点配置为使用正确的协议（ S3 或 Swift ），然后选择 * 取消 * 。
   d. 记下要用于客户端连接的端点的端点端口号。

      > 如果端口号为 80 或 443 ，则仅在网关节点上配置端点，因为这些端口是在管理节点上保留的。所有其他端口都在网关节点和管理节点上进行配置。

配置 VLAN 接口

您可以在管理节点和网关节点上创建虚拟 LAN （ VLAN ）接口，并在 HA 组和负载平衡器端点中使用这些接口隔离和分区流量，以提高安全性，灵活性和性能。

VLAN 接口注意事项

- 您可以通过输入 VLAN ID 并在一个或多个节点上选择父接口来创建 VLAN 接口。
- 必须在交换机上将父接口配置为中继接口。
- 父接口可以是网格网络（ eth0 ），客户端网络（ eth2 ），也可以是虚拟机或裸机主机的附加中继接口（例如 ens256 ）。
- 对于每个 VLAN 接口，您只能为给定节点选择一个父接口。例如，不能将同一网关节点上的网格网络接口和客户端网络接口同时用作同一 VLAN 的父接口。
- 如果 VLAN 接口用于管理节点流量，其中包括与网格管理器和租户管理器相关的流量，请仅选择管理节点上的接口。
- 如果 VLAN 接口用于 S3 或 Swift 客户端流量，请选择管理节点或网关节点上的接口。
- 如果需要添加中继接口，请参见以下内容了解详细信息：
  - * VMware （安装节点后） *： VMware ： 向节点添加中继或访问接口
  - * RHEL 或 CentOS （安装节点之前） *： 创建节点配置文件
  - * Ubuntu 或 Debian （安装节点之前） *： 创建节点配置文件
  - * RHEL ， CentOS ， Ubuntu 或 Debian （安装节点后） *： Linux ： 向节点添加中继或访问接口

创建 VLAN 接口

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 已在网络中配置中继接口并将其连接到 VM 或 Linux 节点。您知道中继接口的名称。
- 您知道要配置的 VLAN 的 ID 。

关于此任务

网络管理员可能已配置一个或多个中继接口以及一个或多个 VLAN ，以隔离属于不同应用程序或租户的客户端或管理流量。每个 VLAN 都通过一个数字 ID 或标记来标识。例如，您的网络可能使用 VLAN 100 传输 FabricPool 流量，而使用 VLAN 200 传输归档应用程序。

您可以使用网格管理器创建 VLAN 接口，以允许客户端访问特定 VLAN 上的 StorageGRID 。创建 VLAN 接口时，您可以指定 VLAN ID 并选择一个或多个节点上的父（中继）接口。

访问向导

1. 选择 * 配置 * > * 网络 * > * VLAN 接口 * 。
2. 选择 * 创建 * 。

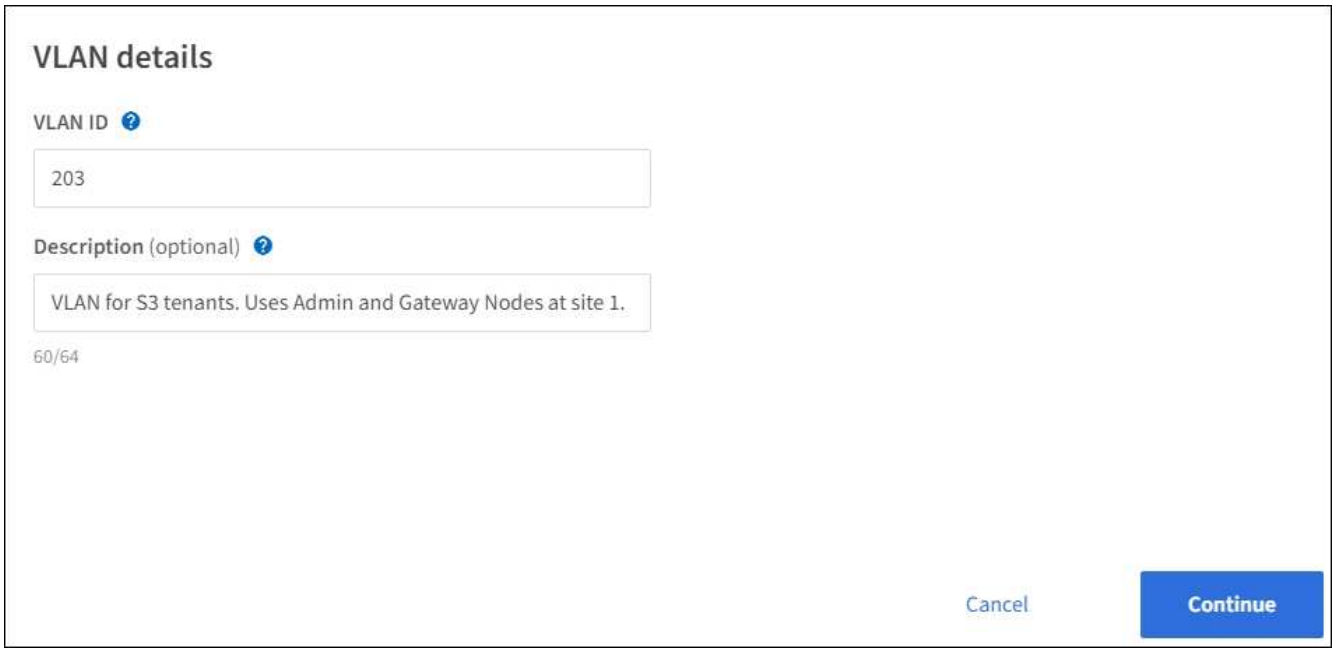
输入 **VLAN** 接口的详细信息

1. 指定网络中 VLAN 的 ID 。您可以输入 1 到 4094 之间的任何值。

   VLAN ID 不需要唯一。例如，您可以对一个站点的管理流量使用 VLAN ID 200 ，而对另一个站点的客户端流量使用相同的 VLAN ID 。您可以在每个站点使用不同的父接口集创建单独的 VLAN 接口。但是， ID 相同的两个 VLAN 接口不能在一个节点上共享同一个接口。

   如果指定的 ID 已被使用，则会显示一条消息。您可以继续为同一 VLAN ID 创建另一个 VLAN 接口，也可以选择 * 取消 * ，然后编辑现有 ID 。

2. 或者，输入 VLAN 接口的短问题描述 。



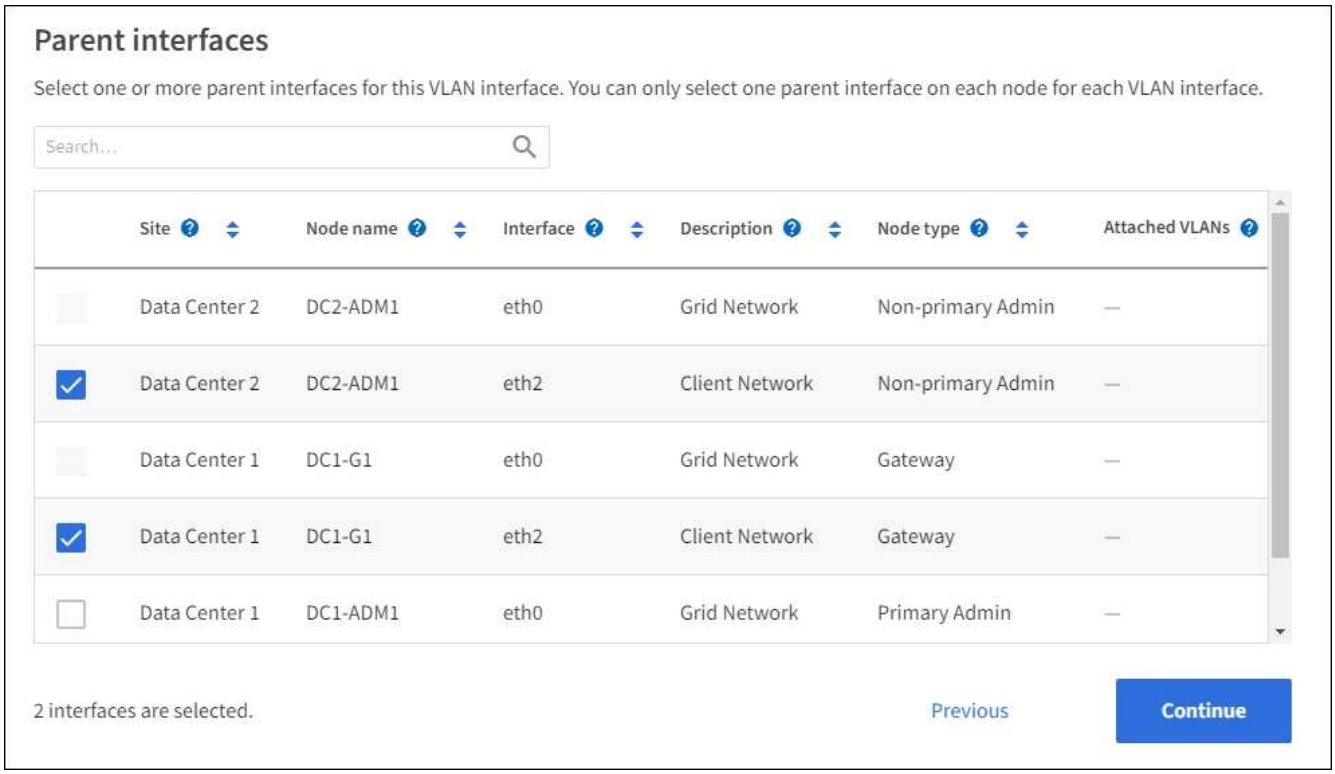
3. 选择 * 继续 * 。

选择父接口

下表列出了网格中每个站点上所有管理节点和网关节点的可用接口。管理网络（ eth1 ）接口不能用作父接口，也不会显示。

1. 选择一个或多个要将此 VLAN 连接到的父接口。

   例如，您可能希望将 VLAN 连接到网关节点和管理节点的客户端网络（ eth2 ）接口。



2. 选择 * 继续 * 。

确认设置

1. 查看配置并进行任何更改。
   - 如果需要更改 VLAN ID 或问题描述 ，请选择页面顶部的 * 输入 VLAN 详细信息 * 。
   - 如果需要更改父接口，请选择页面顶部的 * 选择父接口 * 或选择 * 上一个 * 。
   - 如果需要删除父接口，请选择垃圾桶 。
2. 选择 * 保存 * 。
3. 等待 5 分钟，使新接口显示为 " 高可用性组 " 页面上的一个选项，并在节点的 * 网络接口 * 表中列出（ * 节点 * > * 父接口节点 _* > * 网络 * ）。

编辑 VLAN 接口

编辑 VLAN 接口时，可以进行以下类型的更改：

- 更改 VLAN ID 或问题描述 。
- 添加或删除父接口。

例如，如果您计划停用关联节点，则可能需要从 VLAN 接口中删除父接口。

请注意以下事项：

- 如果在 HA 组中使用 VLAN 接口，则无法更改 VLAN ID 。
- 如果父接口在 HA 组中使用，则不能删除该父接口。

例如，假设 VLAN 200 连接到节点 A 和 B 上的父接口如果 HA 组对节点 A 使用 VLAN 200 接口，而对节点 B 使用 eth2 接口，则可以删除节点 B 未使用的父接口，但不能删除节点 A 使用的父接口

步骤

1. 选择 * 配置 * > * 网络 * > * VLAN 接口 * 。
2. 选中要编辑的 VLAN 接口对应的复选框。然后，选择 * 操作 * > * 编辑 * 。
3. 也可以更新 VLAN ID 或问题描述 。然后，选择 * 继续 * 。

   如果在 HA 组中使用 VLAN ，则无法更新 VLAN ID 。
4. 或者，选中或取消选中复选框以添加父接口或删除未使用的接口。然后，选择 * 继续 * 。
5. 查看配置并进行任何更改。
6. 选择 * 保存 * 。

删除 **VLAN** 接口

您可以删除一个或多个 VLAN 接口。

如果 VLAN 接口当前正在 HA 组中使用，则无法将其删除。必须先从 HA 组中删除 VLAN 接口，然后才能将其删除。

要避免客户端流量发生任何中断，请考虑执行以下操作之一：

- 在删除此 VLAN 接口之前，请向 HA 组添加一个新的 VLAN 接口。
- 创建不使用此 VLAN 接口的新 HA 组。
- 如果要删除的 VLAN 接口当前为活动接口，请编辑 HA 组。将要删除的 VLAN 接口移至优先级列表的底部。等待新主接口建立通信，然后从 HA 组中删除旧接口。最后，删除该节点上的 VLAN 接口。

步骤

1. 选择 * 配置 * > * 网络 * > * VLAN 接口 * 。
2. 选中要删除的每个 VLAN 接口对应的复选框。然后，选择 * 操作 * > * 删除 * 。
3. 选择 * 是 * 确认您的选择。

   选定的所有 VLAN 接口都将被删除。VLAN 接口页面上会显示一个绿色的成功横幅。

管理高可用性组

管理高可用性（ **HA** ）组：概述

您可以将多个管理节点和网关节点的网络接口分组到一个高可用性（ HA ）组中。如果 HA 组中的活动接口发生故障，则备份接口可以管理工作负载。

什么是 **HA** 组?

您可以使用高可用性（ High Availability ， HA ）组为 S3 和 Swift 客户端提供高可用性数据连接，或者为 Grid Manager 和租户管理器提供高可用性连接。

每个 HA 组均可访问选定节点上的共享服务。

- 包括网关节点，管理节点或两者在内的 HA 组可为 S3 和 Swift 客户端提供高可用性数据连接。
- 仅包含管理节点的 HA 组可提供与网格管理器和租户管理器的高可用性连接。
- 如果 HA 组仅包含 SG100 或 SG1000 设备以及基于 VMware 的软件节点，则可以为提供高可用性连接 使用 S3 Select 的 S3 租户。建议在使用 S3 Select 时使用 HA 组，但不要求使用 HA 组。

如何创建 **HA** 组?

1. 您可以为一个或多个管理节点或网关节点选择一个网络接口。您可以使用网格网络（ eth0 ）接口，客户端网络（ eth2 ）接口， VLAN 接口或已添加到节点的访问接口。

   如果 HA 组具有 DHCP 分配的 IP 地址，则不能将接口添加到该组中。

2. 您可以指定一个接口作为主接口。主接口是活动接口，除非发生故障。
3. 您可以确定任何备份接口的优先级顺序。
4. 您可以为组分配 1 到 10 个虚拟 IP （ VIP ）地址。客户端应用程序可以使用其中任何 VIP 地址连接到 StorageGRID 。

有关说明，请参见 配置高可用性组。

什么是活动接口?

在正常操作期间， HA 组的所有 VIP 地址都会添加到主接口，这是优先级顺序中的第一个接口。只要主接口保持可用，客户端就会连接到组的任何 VIP 地址。也就是说，在正常操作期间，主接口是组的 "`active` " 接口。

同样，在正常操作期间， HA 组的任何低优先级接口都充当 "`backup` " 接口。除非主（当前活动）接口不可用，否则不会使用这些备份接口。

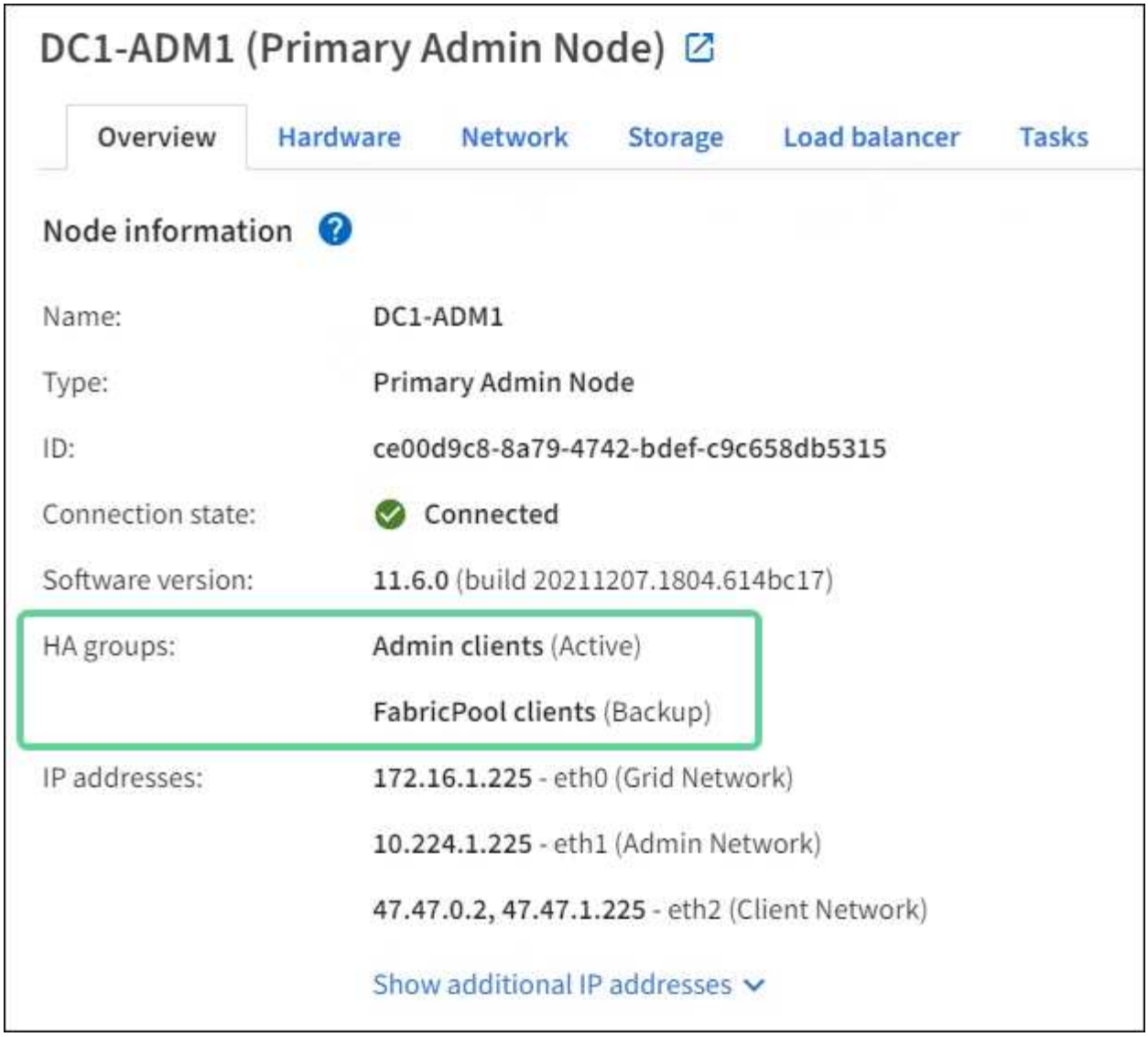
查看节点的当前 **HA** 组状态

要查看节点是否已分配给 HA 组并确定其当前状态，请选择 * 节点 * > * 节点 _节点 _* 。

如果 * 概述 * 选项卡包含 * HA 组 * 的条目，则节点将分配给列出的 HA 组。组名称后面的值是 HA 组中节点的当前状态：

- * 活动 * ： HA 组当前正在此节点上托管。
- * 备份 * ： HA 组当前未使用此节点；这是一个备份接口。
- * 已停止 * ：无法在此节点上托管 HA 组，因为已手动停止高可用性（ keepalived ）服务。
- * 故障 * ：由于以下一项或多项原因，无法在此节点上托管 HA 组：
  - 此节点上未运行负载平衡器（ nginx -gw ）服务。
  - 节点的 eth0 或 VIP 接口已关闭。
  - 节点已关闭。

在此示例中，主管理节点已添加到两个 HA 组中。此节点当前是管理客户端组的活动接口，也是 FabricPool 客户端组的备份接口。



活动接口发生故障时会发生什么情况?

当前托管 VIP 地址的接口是活动接口。如果 HA 组包含多个接口且活动接口发生故障，则 VIP 地址将按优先级顺序移至第一个可用的备份接口。如果该接口发生故障， VIP 地址将移至下一个可用备份接口，依此类推。

触发故障转移的原因如下：

- 配置接口的节点将关闭。
- 配置了该接口的节点与所有其他节点的连接至少断开 2 分钟。
- 活动接口关闭。
- 负载平衡器服务将停止。
- 高可用性服务将停止。

托管活动接口的节点外部的网络故障可能不会触发故障转移。同样， CLB 服务（已弃用）或网格管理器或租户管理器服务失败也不会触发故障转移。

故障转移过程通常只需几秒钟，并且速度足以使客户端应用程序不会受到任何影响，并且可以依靠正常的重试行

为来继续运行。

解决故障后，如果更高优先级的接口再次可用，则 VIP 地址会自动移至可用的最高优先级接口。

如何使用 **HA** 组?

您可以使用高可用性（ High Availability ， HA ）组提供与 StorageGRID 的高可用性连接，以用于对象数据和管理目的。

- HA 组可以为网格管理器或租户管理器提供高度可用的管理连接。
- HA 组可以为 S3 和 Swift 客户端提供高可用性数据连接。
- 如果 HA 组仅包含一个接口，则可以提供多个 VIP 地址并明确设置 IPv6 地址。

只有当 HA 组中包含的所有节点都提供相同的服务时， HA 组才能提供高可用性。创建 HA 组时，请从提供所需服务的节点类型中添加接口。

- * 管理节点 * ： 包括负载平衡器服务，并允许访问网格管理器或租户管理器。
- * 网关节点 * ： 包括负载平衡器服务和 CLB 服务（已弃用）。

HA 组的用途	将此类型的节点添加到 **HA** 组
访问 Grid Manager	• 主管理节点（ * 主 * ） • 非主管理节点 • 注： * 主管理节点必须为主接口。某些维护过程只能从主管理节点执行。
仅访问租户管理器	• 主管理节点或非主管理节点
S3 或 Swift 客户端访问—负载平衡器服务	• 管理节点 • 网关节点
的 S3 客户端访问 S3 Select	• SG100 或 SG1000 设备 • 基于 VMware 的软件节点 • 注 * ： 使用 S3 Select 时建议使用 HA 组，但不要求使用 HA 组。
S3 或 Swift 客户端访问— CLB 服务 • 注： * CLB 服务已弃用。	• 网关节点

将 **HA** 组与 **Grid Manager** 或租户管理器结合使用的限制

如果 Grid Manager 或租户管理器服务失败，则不会触发 HA 组故障转移。

如果在发生故障转移时登录到网格管理器或租户管理器，则您将注销并必须重新登录才能恢复任务。

当主管理节点不可用时，无法执行某些维护过程。在故障转移期间，您可以使用网格管理器监控 StorageGRID

系统。

将 **HA** 组与 **CLB** 服务结合使用的限制

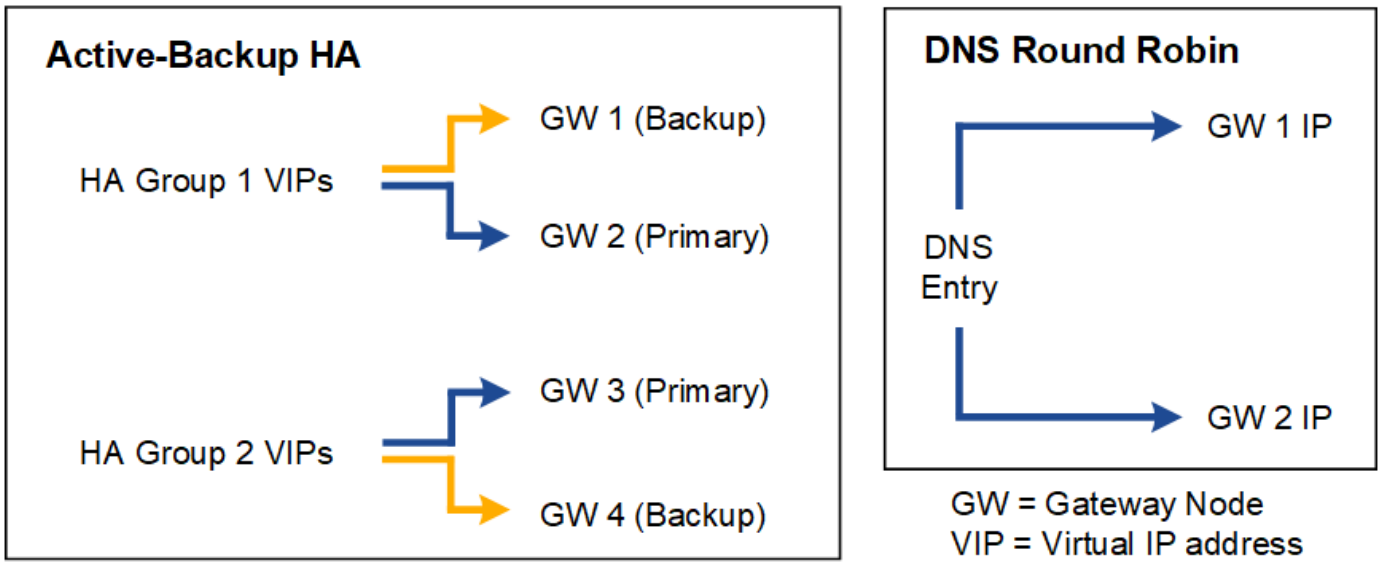
CLB 服务发生故障不会在 HA 组中触发故障转移。

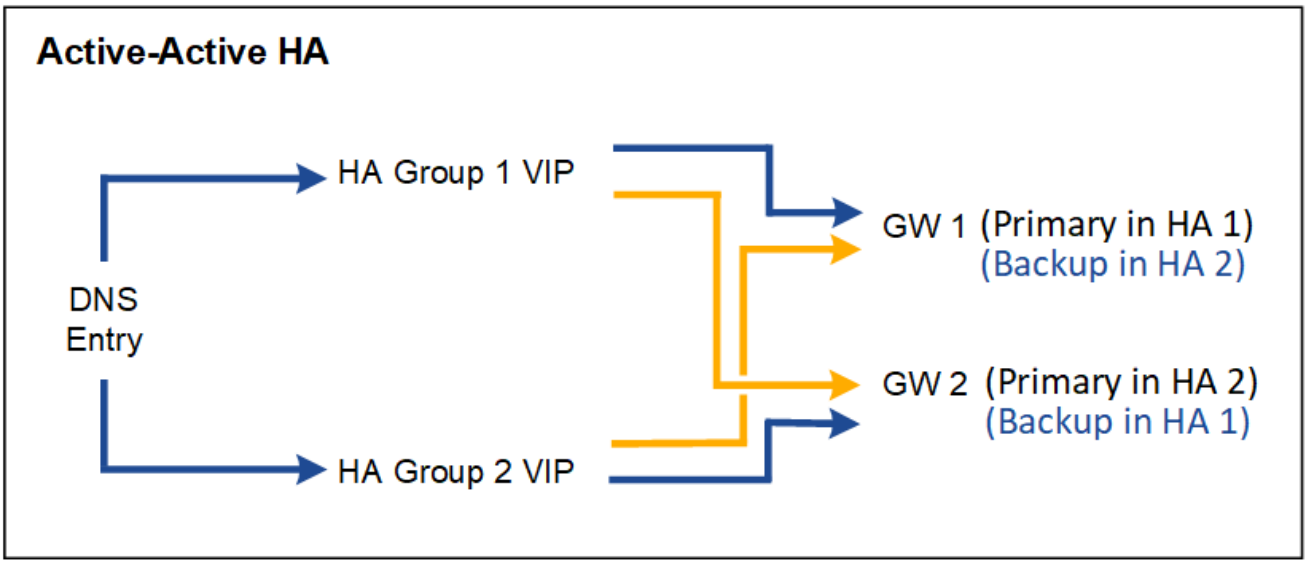
CLB 服务已弃用。

HA 组的配置选项

下图举例说明了配置 HA 组的不同方式。每个选项都有优缺点。

在图中，蓝色表示 HA 组中的主接口，黄色表示 HA 组中的备份接口。





下表总结了图中所示每个 HA 配置的优势。

Configuration	优势	缺点
主动备份 HA	• 由 StorageGRID 管理，无外部依赖关系。 • 快速故障转移。	• 一个 HA 组中只有一个节点处于活动状态。每个 HA 组至少有一个节点处于空闲状态。
DNS 轮循	• 提高聚合吞吐量。 • 无闲置主机。	• 故障转移速度较慢，这可能取决于客户端行为。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。
主动 - 主动 HA	• 流量分布在多个 HA 组中。 • 可随 HA 组数量扩展的高聚合吞吐量。 • 快速故障转移。	• 配置更复杂。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。

配置高可用性组

您可以配置高可用性（ High Availability ， HA ）组，以提供对管理节点或网关节点上服务的高可用性访问。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 如果您计划在 HA 组中使用 VLAN 接口，则已创建 VLAN 接口。请参见 配置 VLAN 接口。
- 如果您计划对 HA 组中的节点使用访问接口，则已创建此接口：
  - * Red Hat Enterprise Linux 或 CentOS （安装节点之前） * ： 创建节点配置文件
  - * Ubuntu 或 Debian （安装节点之前） * ： 创建节点配置文件
  - * Linux （安装节点后） * ： Linux ： 向节点添加中继或访问接口
  - * VMware （安装节点后） * ： VMware ： 向节点添加中继或访问接口

创建高可用性组

创建高可用性组时，您可以选择一个或多个接口并按优先级顺序对其进行组织。然后，您将一个或多个 VIP 地址分配给该组。

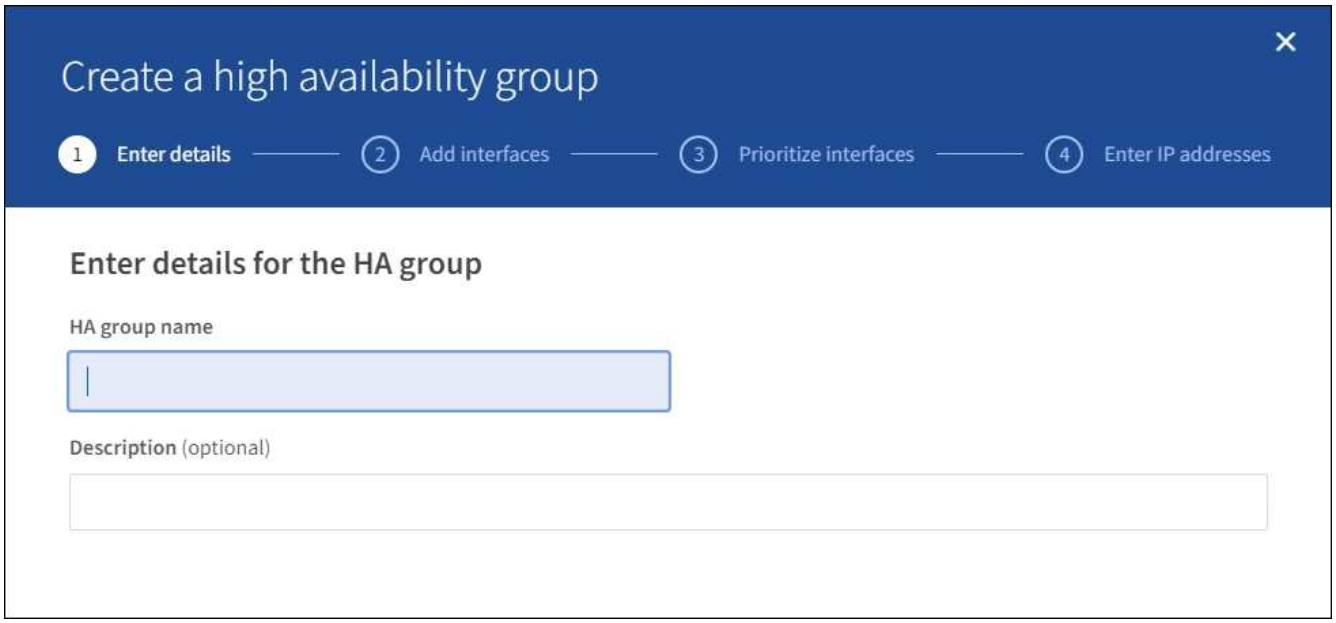
接口必须是要将网关节点或管理节点包含在 HA 组中的接口。一个 HA 组只能对任何给定节点使用一个接口；但是，同一节点的其他接口也可以在其他 HA 组中使用。

访问向导

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。
2. 选择 * 创建 * 。

输入 **HA** 组的详细信息

1. 为 HA 组提供一个唯一名称。

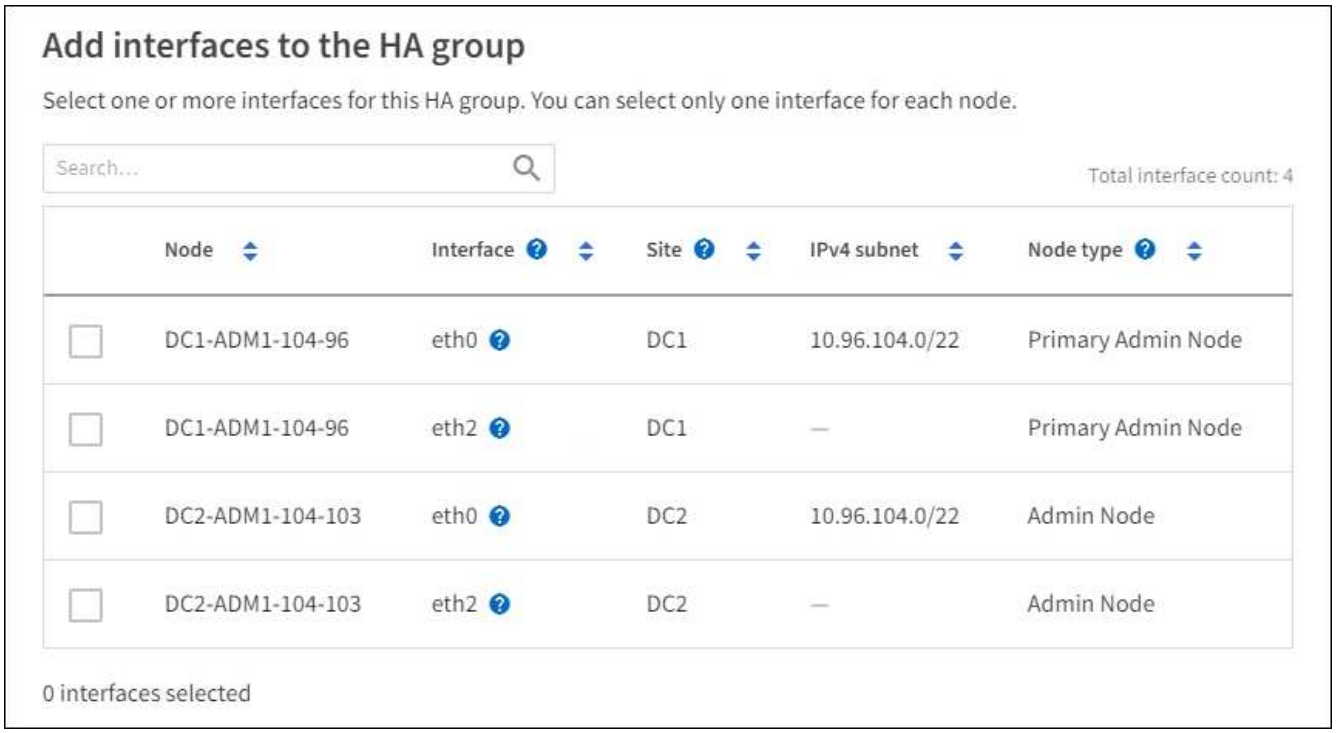


2. 或者，输入 HA 组的问题描述 。
3. 选择 * 继续 * 。

向 **HA** 组添加接口

1. 选择一个或多个接口以添加到此 HA 组。

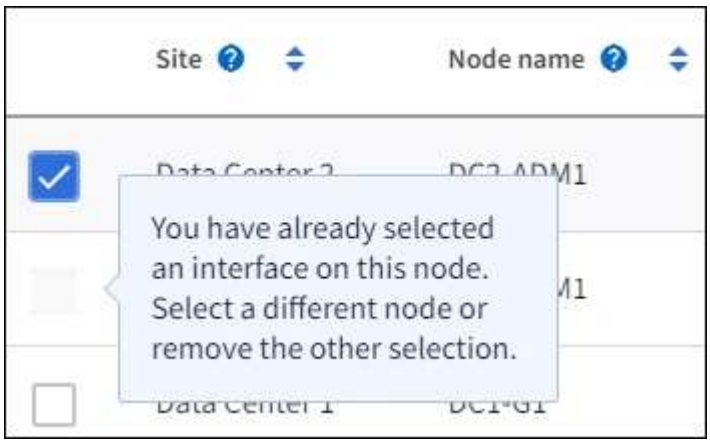
   使用列标题对行进行排序，或者输入搜索词以更快地找到接口。



创建 VLAN 接口后，请等待最多 5 分钟，使新接口显示在表中。

选择接口的准则

- 必须至少选择一个接口。
- 您只能为一个节点选择一个接口。
- 如果 HA 组用于管理节点服务（包括网格管理器和租户管理器）的 HA 保护，请仅选择管理节点上的接口。
- 如果 HA 组用于对 S3 或 Swift 客户端流量进行 HA 保护，请选择管理节点，网关节点或两者上的接口。
- 如果 HA 组用于对已弃用的 CLB 服务进行 HA 保护，请仅选择网关节点上的接口。
- 如果选择不同类型节点上的接口，则会显示一条信息性注释。系统会提醒您，如果发生故障转移，则新活动节点上可能无法使用先前活动节点提供的服务。例如，备份网关节点无法为管理节点服务提供 HA 保护。同样，备份管理节点也无法执行主管理节点可以提供的所有维护过程。
- 如果无法选择接口，则其复选框将被禁用。工具提示提供了更多信息。



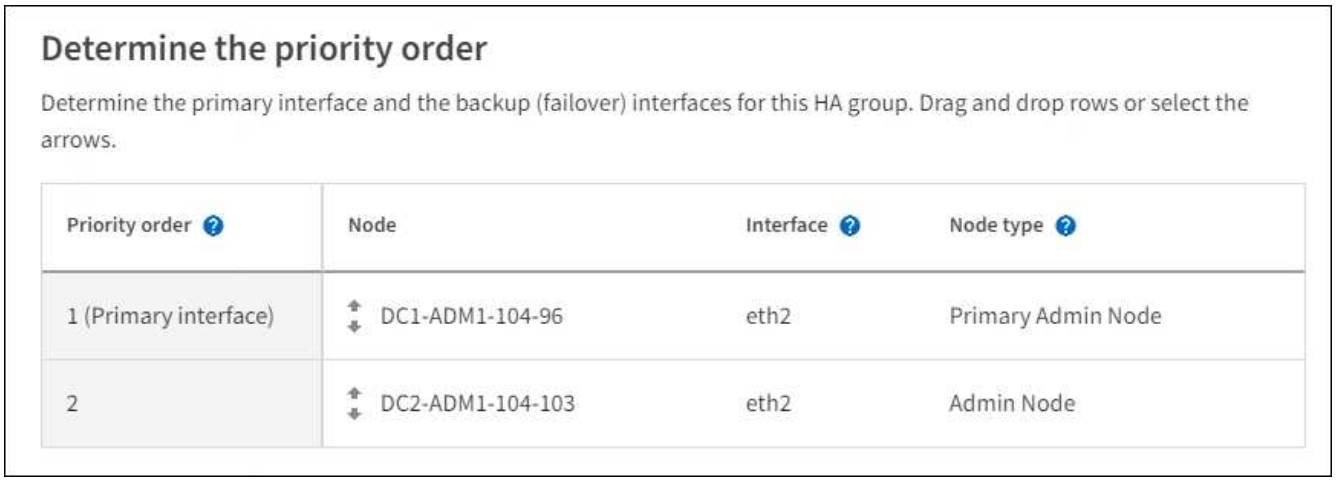
- 如果某个接口的子网值或网关与另一个选定接口冲突，则无法选择该接口。
- 如果已配置的接口没有静态 IP 地址，则无法选择该接口。

2. 选择 * 继续 * 。

确定优先级顺序

1. 确定此 HA 组的主接口和任何备份（故障转移）接口。

   拖放行以更改 * 优先级顺序 * 列中的值。



如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行。

列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。

如果 HA 组包含多个接口，而主接口出现故障，则 VIP 地址将移至可用的最高优先级接口。如果该接口发生故障， VIP 地址将移至可用的下一个最高优先级接口，依此类推。

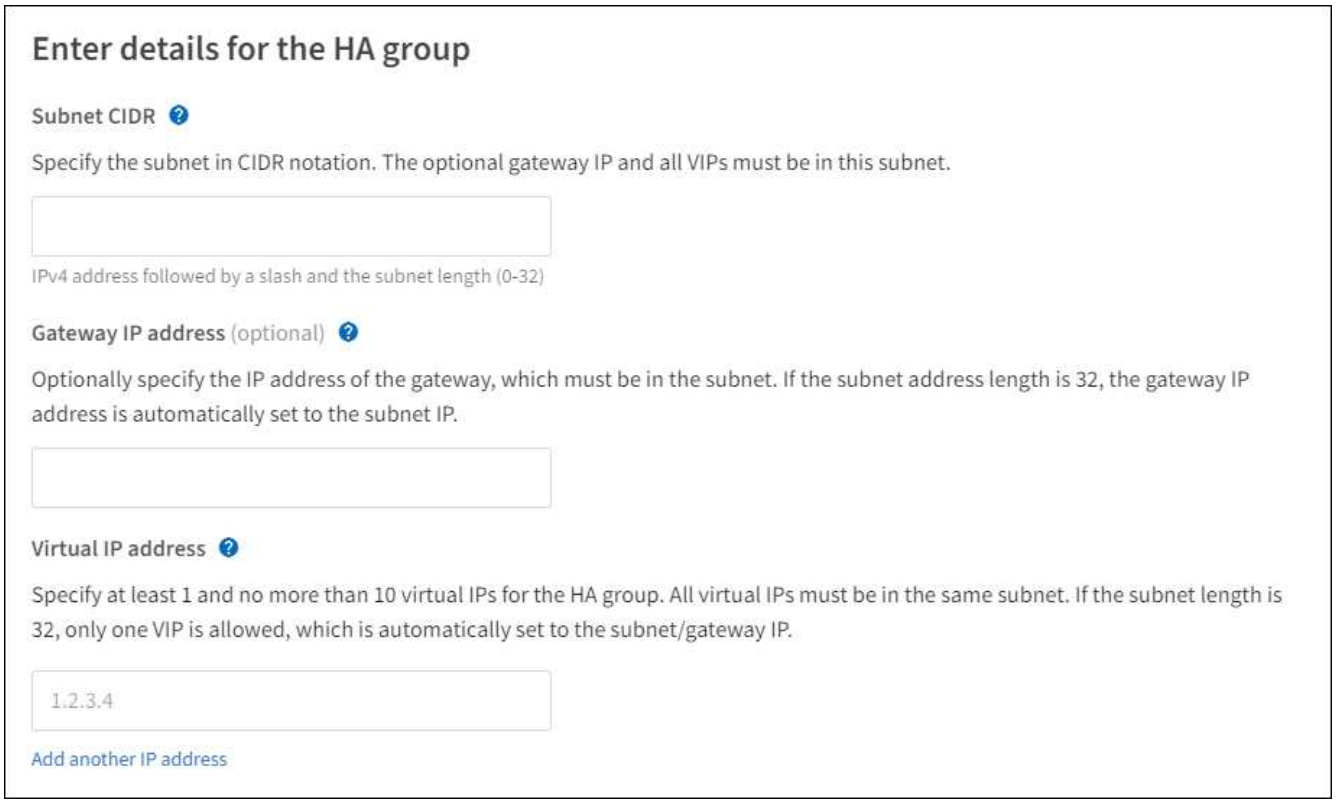
2. 选择 * 继续 * 。

输入 **IP** 地址

1. 在 * 子网 CIDR * 字段中，以 CIDR 表示法指定 VIP 子网— IPv4 地址后跟斜杠和子网长度（ 0-32 ）。

   网络地址不能设置任何主机位。例如， `192.16.0.0/22` 。

   如果使用 32 位前缀，则 VIP 网络地址也会用作网关地址和 VIP 地址。



2. 或者，如果任何 S3 ， Swift ，管理或租户客户端要从其他子网访问这些 VIP 地址，请输入 * 网关 IP 地址 * 。网关地址必须在 VIP 子网中。

   客户端和管理员用户将使用此网关访问虚拟 IP 地址。

3. 为 HA 组输入一个或多个 * 虚拟 IP 地址 * 。最多可以添加 10 个 IP 地址。所有 VIP 都必须位于 VIP 子网中。

   您必须至少提供一个 IPv4 地址。您也可以指定其他 IPv4 和 IPv6 地址。

4. 选择 * 创建 HA 组 * 并选择 * 完成 * 。

   此时将创建 HA 组，您现在可以使用已配置的虚拟 IP 地址。

> 等待长达 15 分钟，以便对 HA 组所做的更改应用于所有节点。

后续步骤

如果要使用此 HA 组进行负载平衡，请创建一个负载平衡器端点以确定端口和网络协议并附加任何所需的证书。请参见 配置负载平衡器端点。

编辑高可用性组

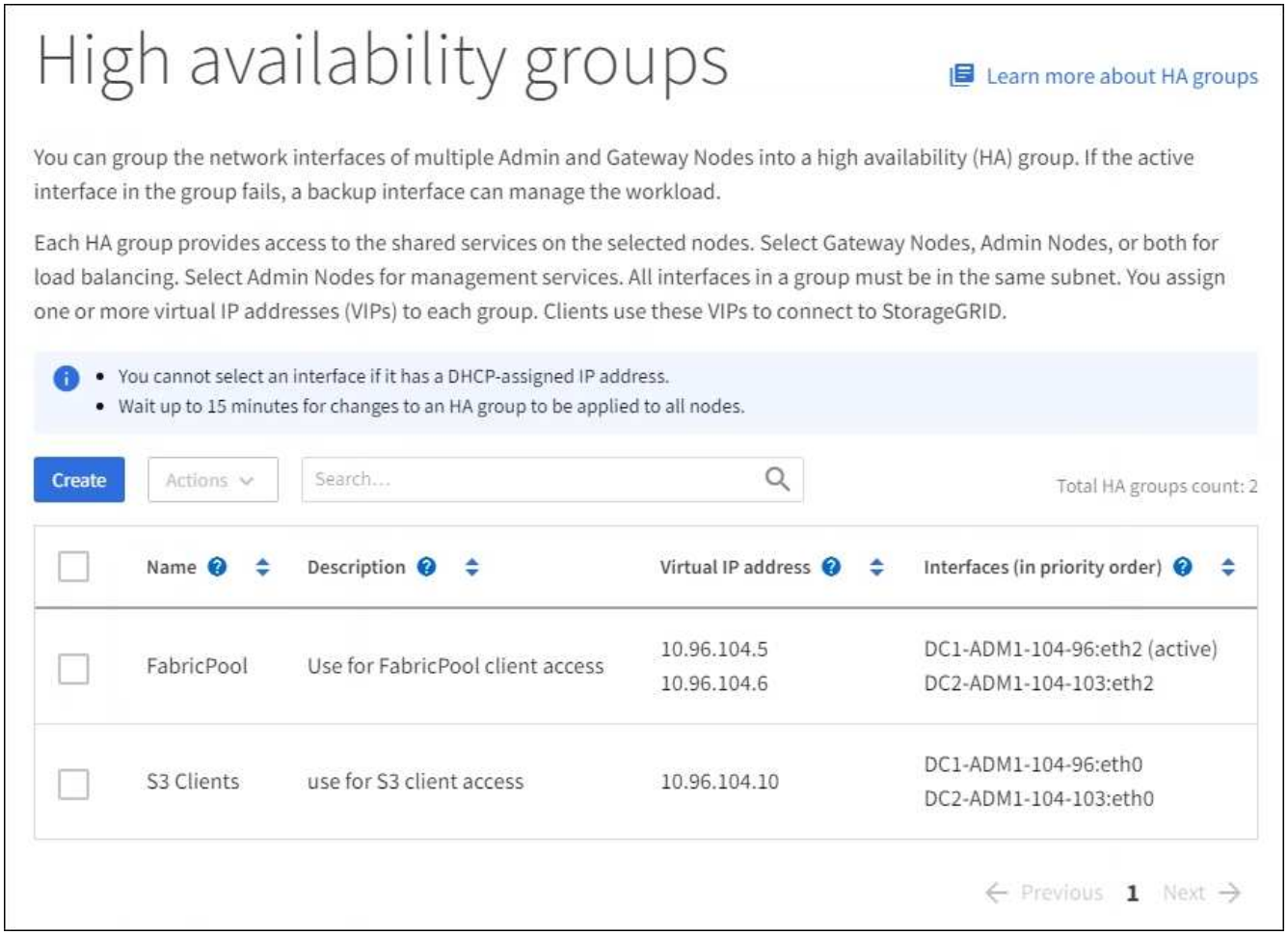
您可以编辑高可用性（ High Availability ， HA ）组以更改其名称和问题描述 ，添加或删除接口，更改优先级顺序或添加或更新虚拟 IP 地址。

例如，如果要删除与站点或节点停用操作步骤 中选定接口关联的节点，则可能需要编辑 HA 组。

步骤

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。

   " 高可用性组 " 页面显示所有现有的 HA 组。



2. 选中要编辑的 HA 组对应的复选框。
3. 根据要更新的内容执行以下操作之一：
   - 选择 * 操作 * > * 编辑虚拟 IP 地址 * 以添加或删除 VIP 地址。
   - 选择 * 操作 * > * 编辑 HA 组 * 可更新组的名称或问题描述 ，添加或删除接口，更改优先级顺序或添加或删除 VIP 地址。
4. 如果选择了 * 编辑虚拟 IP 地址 * ：
   a. 更新 HA 组的虚拟 IP 地址。
   b. 选择 * 保存 * 。
   c. 选择 * 完成 * 。
5. 如果选择了 * 编辑 HA 组 * ：
   a. （可选）更新组的名称或问题描述 。
   b. 或者，选中或取消选中这些复选框以添加或删除接口。

如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行

c. 或者，也可以拖放行来更改此 HA 组的主接口和任何备份接口的优先级顺序。

d. 也可以更新虚拟 IP 地址。

e. 选择 * 保存 * ，然后选择 * 完成 * 。

等待长达 15 分钟，以便对 HA 组所做的更改应用于所有节点。

删除高可用性组

您可以一次删除一个或多个高可用性（ HA ）组。但是，如果 HA 组绑定到一个或多个负载平衡器端点，则无法删除该组。

为防止客户端中断，请在删除 HA 组之前更新任何受影响的 S3 或 Swift 客户端应用程序。更新每个客户端以使用其他 IP 地址进行连接，例如，安装期间为接口配置的不同 HA 组的虚拟 IP 地址或 IP 地址。

步骤

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。
2. 选中要删除的每个 HA 组对应的复选框。然后，选择 * 操作 * > * 删除 HA 组 * 。
3. 查看此消息并选择 * 删除 HA 组 * 以确认您的选择。

   选定的所有 HA 组都将被删除。高可用性组页面上会显示一个绿色的成功横幅。

管理负载平衡

Manage load balancing：概述

您可以使用 StorageGRID 负载平衡功能处理从 S3 和 Swift 客户端载入和检索工作负载。负载平衡通过在多个存储节点之间分布工作负载和连接来最大限度地提高速度和连接容量。

您可以通过以下方式对客户端工作负载进行负载平衡：

- 使用负载平衡器服务，该服务安装在管理节点和网关节点上。负载平衡器服务提供第 7 层负载平衡，并对客户端请求执行 TLS 终止，检查请求并建立与存储节点的新安全连接。这是建议的负载平衡机制。

  请参见 负载平衡的工作原理—负载平衡器服务。

- 使用已弃用的连接负载平衡器（ CLB ）服务，该服务仅安装在网关节点上。CLB 服务提供第 4 层负载平衡并支持链路成本。

  请参见 负载平衡的工作原理— CLB 服务（已弃用）。

- 集成第三方负载平衡器。有关详细信息，请联系您的 NetApp 客户代表。

负载平衡器服务将传入的网络连接从客户端应用程序分发到存储节点。要启用负载平衡，必须使用网格管理器配置负载平衡器端点。

您只能为管理节点或网关节点配置负载平衡器端点，因为这些节点类型包含负载平衡器服务。您不能为存储节点或归档节点配置端点。

每个负载平衡器端点都指定一个端口，一个网络协议（ HTTP 或 HTTPS ），一个客户端类型（ S3 或 Swift ）和一个绑定模式。HTTPS 端点需要服务器证书。通过绑定模式，您可以将端点端口的可访问性限制为：

- 特定高可用性（ HA ）组的虚拟 IP 地址（ VIP ）
- 特定管理节点和网关节点的特定网络接口

端口注意事项

客户端可以访问您在运行负载平衡器服务的任何节点上配置的任何端点，但有两个例外：端口 80 和 443 在管理节点上保留，因此在这些端口上配置的端点仅支持网关节点上的负载平衡操作。

如果已重新映射任何端口，则不能使用相同的端口配置负载平衡器端点。您可以使用重新映射的端口创建端点，但这些端点将重新映射到原始 CLB 端口和服务，而不是负载平衡器服务。按照中的步骤进行操作 删除端口重新映射。

CLB 服务已弃用。

CPU 可用性

在向存储节点转发 S3 或 Swift 流量时，每个管理节点和网关节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。节点 CPU 负载信息每隔几分钟更新一次，但权重可能会更频繁地更新。即使节点报告利用率为 100% 或未能报告利用率，也会为所有存储节点分配最小基本权重值。

在某些情况下，有关 CPU 可用性的信息仅限于负载平衡器服务所在的站点。

负载平衡器端点决定了 S3 和 Swift 客户端在连接到网关和管理节点上的 StorageGRID 负载平衡器时可以使用的端口和网络协议。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 如果您先前已重新映射要用于负载平衡器端点的端口，则表示您已重新映射 已删除端口重新映射。
- 您已创建计划使用的任何高可用性（ HA ）组。建议使用 HA 组，但不要求使用 HA 组。请参见 管理高可用性组。
- 负载平衡器端点是否将由使用 S3 Select 的 S3 租户，不能使用任何裸机节点的 IP 地址或 FQDN 。用于 S3 Select 的负载平衡器端点仅允许使用 SG100 或 SG1000 设备以及基于 VMware 的软件节点。
- 您已配置计划使用的任何 VLAN 接口。请参见 配置 VLAN 接口。

- 如果要创建 HTTPS 端点（建议），则您具有服务器证书的信息。

  对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

  - 要上传证书，您需要服务器证书，证书专用密钥以及 CA 捆绑包（可选）。
  - 要生成证书，您需要 S3 或 Swift 客户端用于访问此端点的所有域名和 IP 地址。您还必须知道主题（可分辨名称）。
  - 如果要使用 StorageGRID S3 和 Swift API 证书（也可用于直接连接到存储节点），则已将默认证书替换为由外部证书颁发机构签名的自定义证书。请参见配置 S3 和 Swift API 证书。

    此证书可以使用通配符表示运行负载平衡器服务的所有管理节点和网关节点的完全限定域名。例如，`*.storagegrid.*example*.com` 使用 * 通配符表示 `adm1.storagegrid.example.com` 和 `gn1.storagegrid.example.com` 。请参见 配置 S3 API 端点域名。

创建负载平衡器端点

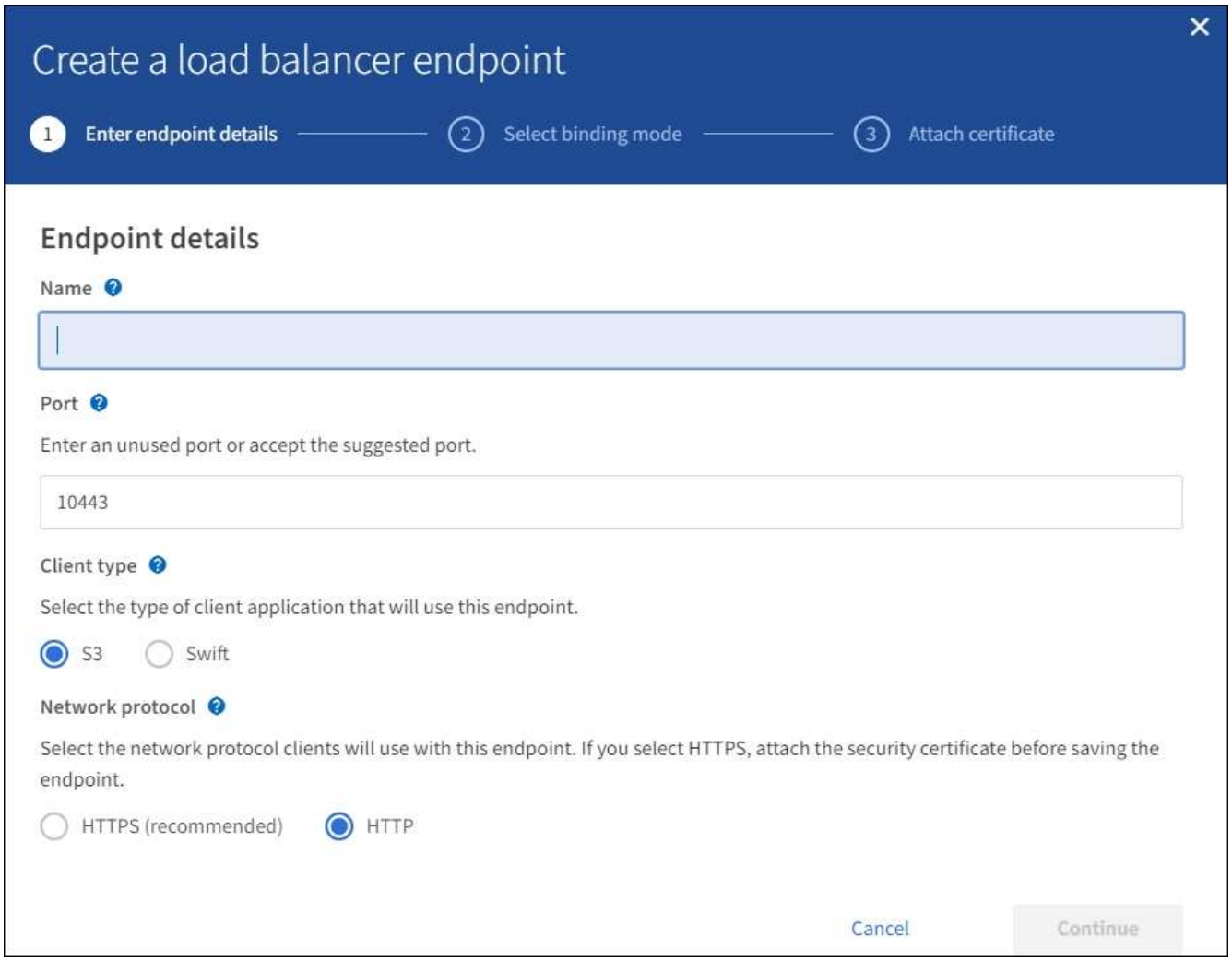
每个负载平衡器端点都指定一个端口，一个客户端类型（ S3 或 Swift ）和一个网络协议（ HTTP 或 HTTPS ）。

访问向导

1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。
2. 选择 * 创建 * 。

输入端点详细信息

1. 输入端点的详细信息。



字段	Description
Name	端点的描述性名称，将显示在负载平衡器端点页面的表中。
Port	端口客户端将使用连接到管理节点和网关节点上的负载平衡器服务。 接受建议的端口号或输入其他网格服务未使用的任何外部端口。输入一个介于 1 到 65535 之间的值。 如果输入 * 。 80* 或 * 。 443* ，则仅在网关节点上配置端点。这些端口在管理节点上预留。 请参见 网络连接准则 有关外部端口的信息。
客户端类型	要使用此端点的客户端应用程序类型，可以是 * S3 或 * Swift* 。

字段	Description
网络协议	客户端在连接到此端点时将使用的网络协议。 • 选择 * HTTPS * 可进行安全的 TLS 加密通信（建议）。您必须附加安全证书，然后才能保存此端点。 • 选择 * HTTP * 可实现不太安全的未加密通信。对于非生产网格，请仅使用 HTTP 。

2. 选择 * 继续 * 。

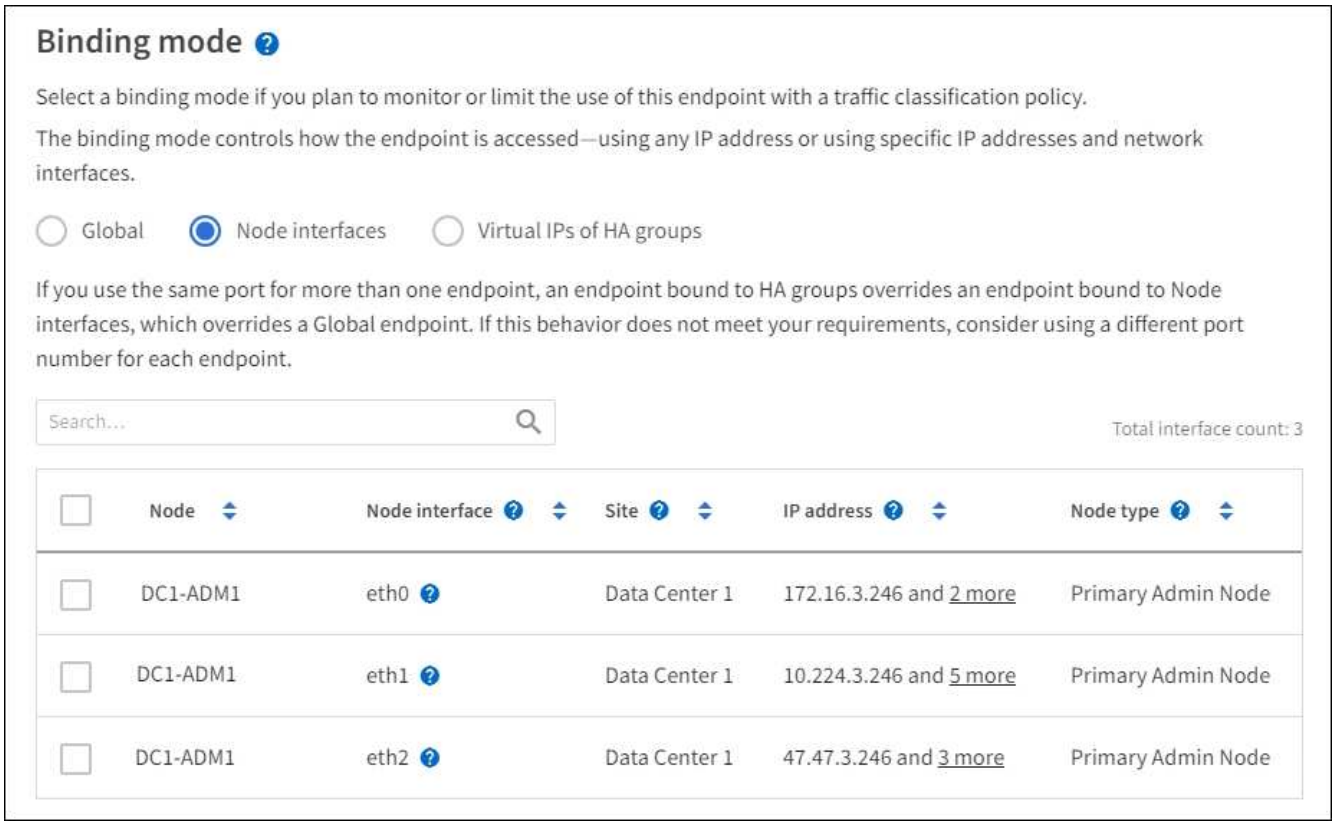
选择绑定模式

1. 为端点选择绑定模式以控制端点的访问方式。

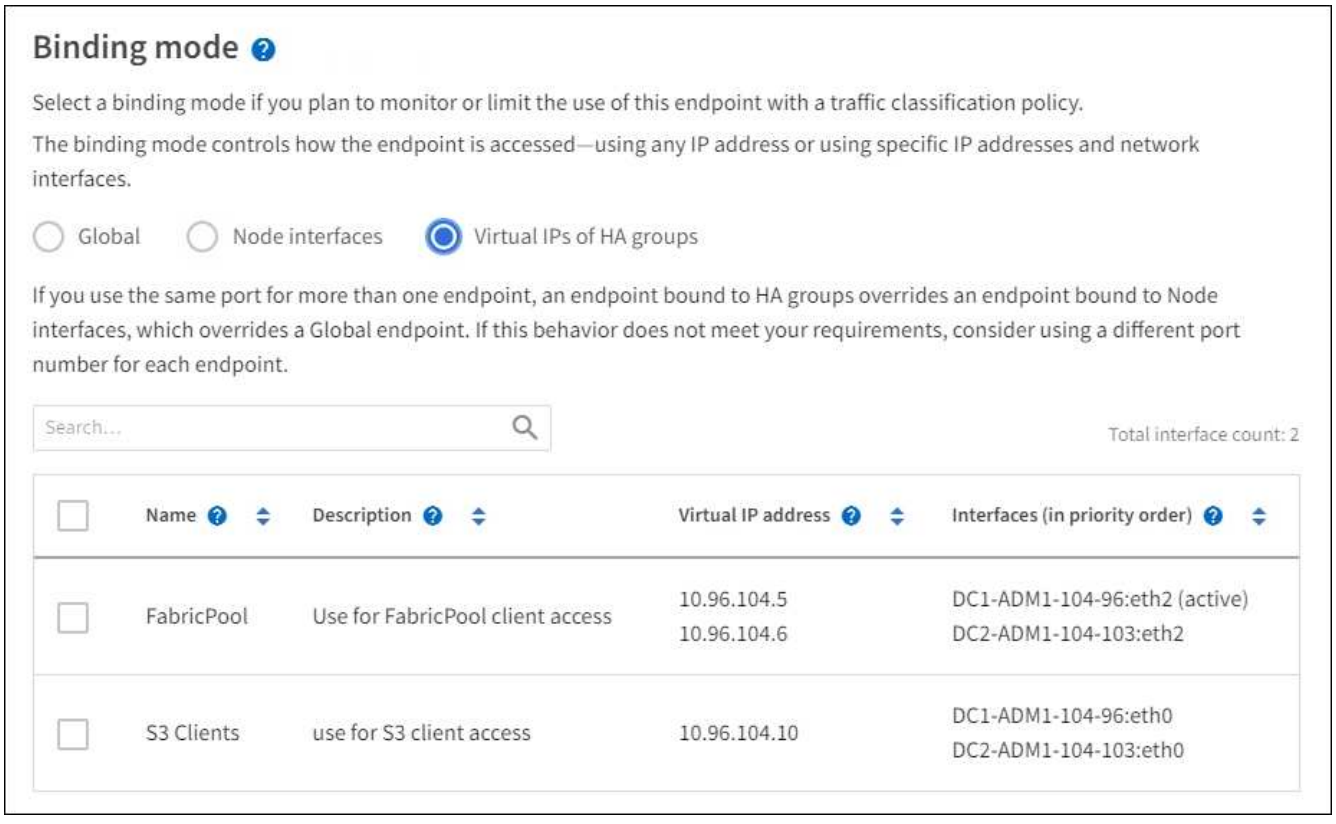
选项	Description
全局（默认）	客户端可以使用完全限定域名（ FQDN ），任何网关节点或管理节点的 IP 地址或任何网络上任何 HA 组的虚拟 IP 地址来访问此端点。 除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。
节点接口	客户端必须使用选定节点的 IP 地址和网络接口来访问此端点。
HA 组的虚拟 IP	客户端必须使用 HA 组的虚拟 IP 地址来访问此端点。 只要为端点选择的 HA 组不重叠，具有此绑定模式的端点都可以使用相同的端口号。 只要您为端点选择的接口不重叠，采用此模式的端点都可以使用相同的端口号。

如果对多个端点使用同一端口，则使用 * HA 组的虚拟 IP * 模式的端点将覆盖使用 * 节点接口 * 模式的端点，而此模式将覆盖使用 * 全局 * 模式的端点。

2. 如果选择了 * 节点接口 * ，请为要与此端点关联的每个管理节点或网关节点选择一个或多个节点接口。



3. 如果选择了 * HA 组的虚拟 IP * ，请选择一个或多个 HA 组。



4. 如果要创建 * HTTP * 端点，则不需要附加证书。选择 * 创建 * 以添加新的负载平衡器端点。然后，转到 完成后。否则，请选择 * 继续 * 以附加证书。

附加证书

1. 如果要创建 * HTTPS * 端点，请选择要附加到该端点的安全证书类型。

   此证书可保护 S3 和 Swift 客户端之间的连接以及管理节点或网关节点上的负载平衡器服务。

   - * 上传证书 * 。如果您要上传自定义证书，请选择此选项。
   - * 生成证书 * 。如果您具有生成自定义证书所需的值，请选择此选项。
   - * 使用 StorageGRID S3 和 Swift 证书 * 。如果要使用全局 S3 和 Swift API 证书，则选择此选项，此证书也可用于直接连接到存储节点。

     除非已将由网格 CA 签名的默认 S3 和 Swift API 证书替换为由外部证书颁发机构签名的自定义证书，否则无法选择此选项。请参见配置 S3 和 Swift API 证书。

2. 如果您未使用 StorageGRID S3 和 Swift 证书，请上传或生成此证书。

上传证书

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

- * 服务器证书 * ： PEM 编码的自定义服务器证书文件。
- * 证书专用密钥 * ：自定义服务器证书专用密钥文件（` 。 key` ）。

> EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

- * CA bundle* ：一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

- 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

  指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

例如： `storagegRid_certificate.pem`

- 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 创建 * 。+ 已创建负载平衡器端点。自定义证书用于 S3 和 Swift 客户端与端点之间的所有后续新连接。

生成证书

a. 选择 * 生成证书 * 。

b. 指定证书信息：

- * 域名 * ：要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
- * IP * ：要包含在证书中的一个或多个 IP 地址。
- * 主题 * ：证书所有者的 X.509 主题或可分辨名称（ DN ）。
- * 有效天数 * ：创建证书后的天数到期。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名 ` .pem` 保存文件。

例如： `storagegRid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 创建 * 。

此时将创建负载平衡器端点。自定义证书用于 S3 和 Swift 客户端与此端点之间的所有后续新连接。

完成后的操作

1. 如果您使用域名系统（ DNS ），请确保 DNS 包含一条记录，以便将 StorageGRID 完全限定域名与客户端用于建立连接的每个 IP 地址相关联。

   在 DNS 记录中输入的 IP 地址取决于您是否使用的是由负载平衡节点组成的 HA 组：

   - 如果已配置HA组、则客户端将连接到该HA组的虚拟IP地址。
   - 如果您不使用HA组、则客户端将使用任何网关节点或管理节点的IP地址连接到StorageGRID 负载平衡器服务。

     此外，还必须确保 DNS 记录引用所有必需的端点域名，包括任何通配符名称。

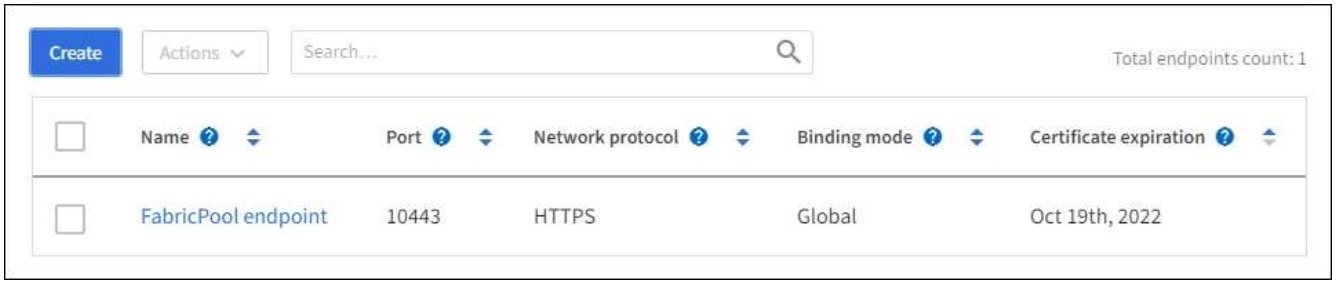
2. 为 S3 和 Swift 客户端提供连接到端点所需的信息：
   - 端口号
   - 完全限定域名或 IP 地址
   - 任何必需的证书详细信息

查看和编辑负载平衡器端点

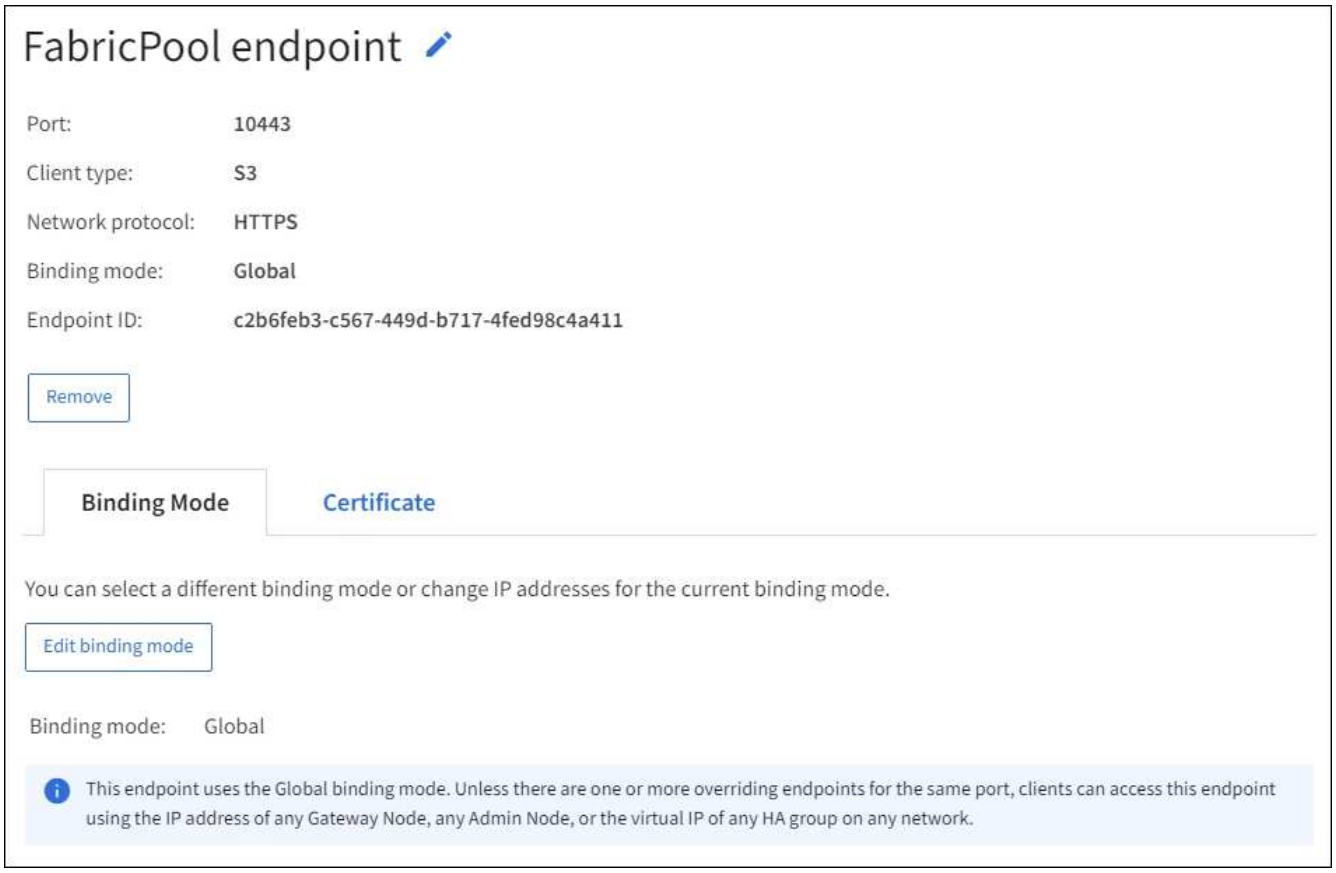
您可以查看现有负载平衡器端点的详细信息，包括安全端点的证书元数据。您还可以更改端点的名称或绑定模式，并更新任何关联的证书。

您不能更改服务类型（ S3 或 Swift ），端口或协议（ HTTP 或 HTTPS ）。

- 要查看所有负载平衡器端点的基本信息，请查看负载平衡器端点页面上的表。



- 要查看有关特定端点的所有详细信息，包括证书元数据，请在表中选择端点的名称。



- 要编辑端点，请使用负载平衡器端点页面上的 * 操作 * 菜单或特定端点的详细信息页面。

  编辑端点后，您可能需要等待长达 15 分钟，才能将所做的更改应用于所有节点。

任务	操作菜单	详细信息页面
编辑端点名称	a. 选中端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点名称 * 。 c. 输入新名称。 d. 选择 * 保存 * 。	a. 选择端点名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存 * 。
编辑端点绑定模式	a. 选中端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 编辑绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。

任务	操作菜单	详细信息页面
编辑端点证书	a. 选中端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点证书 * 。 c. 根据需要上传或生成新的自定义证书或开始使用全局 S3 和 Swift 证书。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 证书 * 选项卡。 c. 选择 * 编辑证书 * 。 d. 根据需要上传或生成新的自定义证书或开始使用全局 S3 和 Swift 证书。 e. 选择 * 保存更改 * 。

删除负载平衡器端点

您可以使用 * 操作 * 菜单删除一个或多个端点，也可以从详细信息页面中删除单个端点。

> 为防止客户端中断，请在删除负载平衡器端点之前更新任何受影响的 S3 或 Swift 客户端应用程序。更新每个客户端以使用分配给另一个负载平衡器端点的端口进行连接。请务必同时更新所需的任何证书信息。

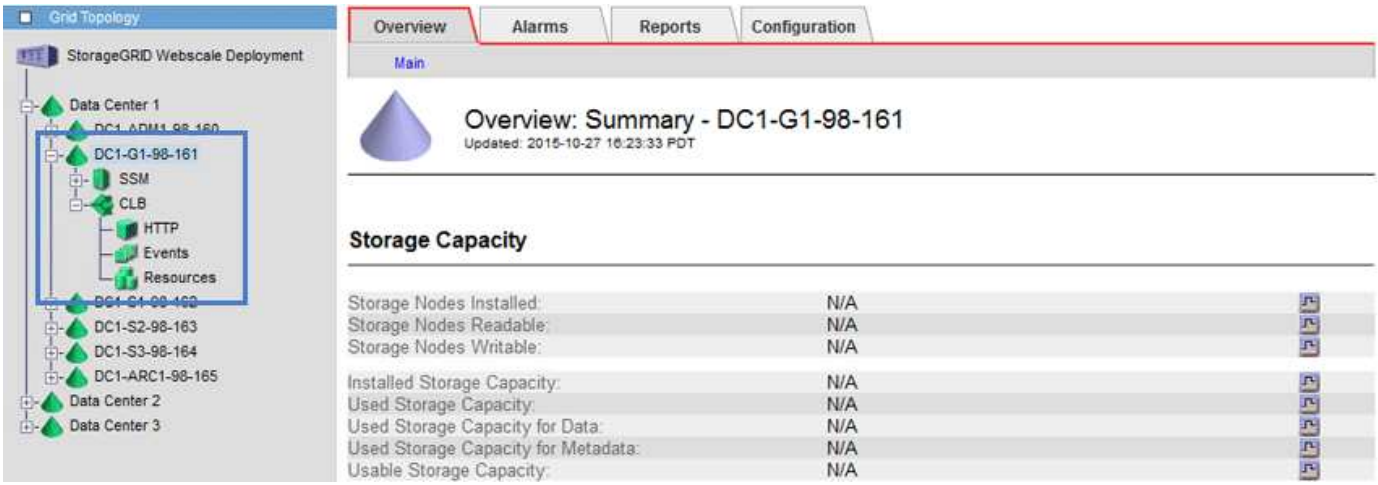
- 删除一个或多个端点：
  a. 在负载平衡器页面中，选中要删除的每个端点对应的复选框。
  b. 选择 * 操作 * > * 删除 * 。
  c. 选择 * 确定 * 。
- 从详细信息页面中删除一个端点：
  a. 从负载平衡器页面。选择端点名称。
  b. 在详细信息页面上选择 * 删除 * 。
  c. 选择 * 确定 * 。

负载平衡的工作原理— **CLB** 服务（已弃用）

网关节点上的连接负载平衡器（ CLB ）服务已弃用。现在，建议使用负载平衡器服务。

CLB 服务使用第 4 层负载平衡功能，根据可用性，系统负载和管理员配置的链路成本，将传入的 TCP 网络连接从客户端应用程序分发到最佳存储节点。选择最佳存储节点后， CLB 服务将建立双向网络连接，并将流量转发到选定节点和从选定节点转发流量。在定向传入网络连接时， CLB 不考虑网格网络配置。

要查看有关 CLB 服务的信息，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后展开网关节点，直到可以选择 * CLB* 及其下方的选项为止。



如果您选择使用 CLB 服务，则应考虑为 StorageGRID 系统配置链路成本。

- 链路成本是多少
- 更新链路成本

配置 **S3 API** 端点域名

要支持 S3 虚拟托管模式请求，您必须使用网格管理器配置 S3 客户端连接到的端点域名列表。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已确认网格升级未在进行中。

> 在进行网格升级时，请勿对域名配置进行任何更改。

关于此任务

要使客户端能够使用 S3 端点域名，您必须执行以下所有操作：

- 使用网格管理器将 S3 端点域名添加到 StorageGRID 系统。
- 确保客户端用于与 StorageGRID 的 HTTPS 连接的证书已针对客户端所需的所有域名进行签名。

  例如，如果端点为 `s3.company.com` ，则必须确保用于 HTTPS 连接的证书包含 `s3.company.com` 端点和端点的通配符使用者备用名称（ SAN ）： `* .s3.company.com` 。

- 配置客户端使用的 DNS 服务器。为客户端用于建立连接的 IP 地址提供 DNS 记录，并确保这些记录引用所有必需的端点域名，包括任何通配符名称。

> 客户端可以使用网关节点，管理节点或存储节点的 IP 地址或连接到高可用性组的虚拟 IP 地址连接到 StorageGRID 。您应了解客户端应用程序如何连接到网格，以便在 DNS 记录中包含正确的 IP 地址。

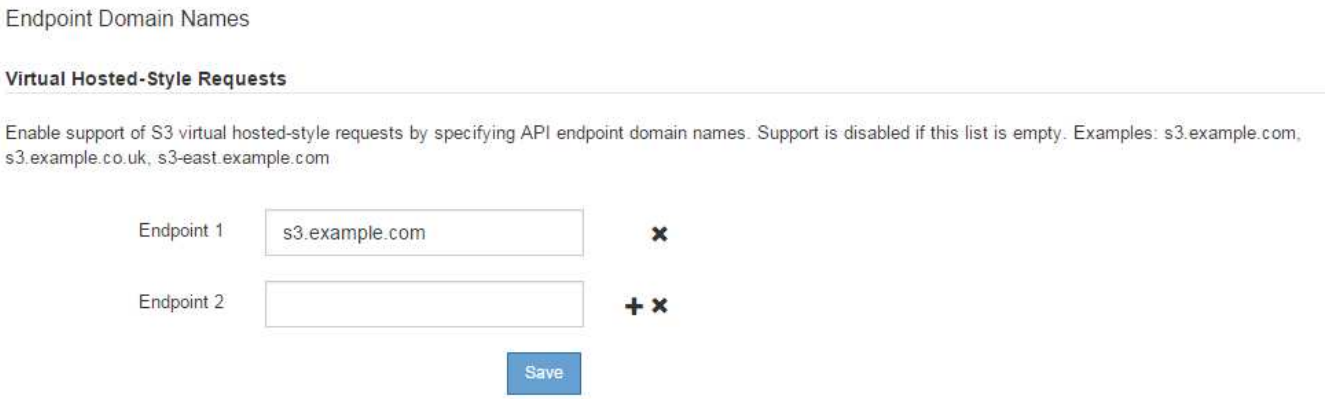
使用 HTTPS 连接（建议）连接到网格的客户端可以使用以下任一证书：

- 连接到负载平衡器端点的客户端可以对该端点使用自定义证书。可以对每个负载平衡器端点进行配置，以识别不同的端点域名。
- 如果客户端连接到负载平衡器端点，直接连接到存储节点或直接连接到网关节点上已弃用的 CLB 服务，则可以自定义全局 S3 和 Swift API 证书，以包含所有必需的端点域名。

步骤

1. 选择 * 配置 * > * 网络 * > * 域名 * 。

   此时将显示 Endpoint Domain Names 页面。



2. 在 * 端点 * 字段中输入 S3 API 端点域名列表。使用 ✚ 图标以添加其他字段。

   如果此列表为空，则会禁用对 S3 虚拟托管模式请求的支持。

3. 选择 * 保存 * 。
4. 确保客户端使用的服务器证书与所需的端点域名匹配。
   - 如果客户端连接到使用自己证书的负载平衡器端点，请更新与此端点关联的证书。
   - 如果客户端连接到使用全局 S3 和 Swift API 证书的负载平衡器端点，直接连接到存储节点或网关节点上的 CLB 服务，请更新全局 S3 和 Swift API 证书。
5. 添加所需的 DNS 记录，以确保可以解决端点域名请求。

结果

现在，当客户端使用端点 `bucket.s3.company.com` 时， DNS 服务器会解析到正确的端点，并且证书会按预期对端点进行身份验证。

相关信息

- 使用 S3
- 查看 IP 地址
- 配置高可用性组
- 配置 S3 和 Swift API 证书
- 配置负载平衡器端点

为客户端通信启用 **HTTP**

默认情况下，客户端应用程序会使用 HTTPS 网络协议连接到存储节点或网关节点上已弃用的 CLB 服务。您可以选择为这些连接启用 HTTP ，例如在测试非生产网格时。

您需要的内容

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

关于此任务

只有当 S3 和 Swift 客户端需要直接与存储节点或网关节点上已弃用的 CLB 服务建立 HTTP 连接时，才能完成此任务。

对于仅使用 HTTPS 连接的客户端或连接到负载平衡器服务的客户端，您无需完成此任务（因为您可以将每个负载平衡器端点配置为使用 HTTP 或 HTTPS ）。有关详细信息，请参见有关配置负载平衡器端点的信息。

请参见 摘要：客户端连接的 IP 地址和端口 了解使用 HTTP 或 HTTPS 连接到存储节点或已弃用的 CLB 服务时 S3 和 Swift 客户端使用的端口

为生产网格启用 HTTP 时请务必小心，因为请求会以未加密方式发送。

步骤

1. 选择 * 配置 * > * 系统 * > * 网格选项 * 。
2. 在网络选项部分中，选中 * 启用 HTTP 连接 * 复选框。

3. 选择 * 保存 * 。

相关信息

- 配置负载平衡器端点
- 使用 S3
- 使用 Swift

控制允许哪些客户端操作

您可以选择阻止客户端修改网格选项来拒绝特定的 HTTP 客户端操作。

您需要的内容

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

关于此任务

" 阻止客户端修改 " 是系统范围的设置。选择阻止客户端修改选项后，以下请求将被拒绝：

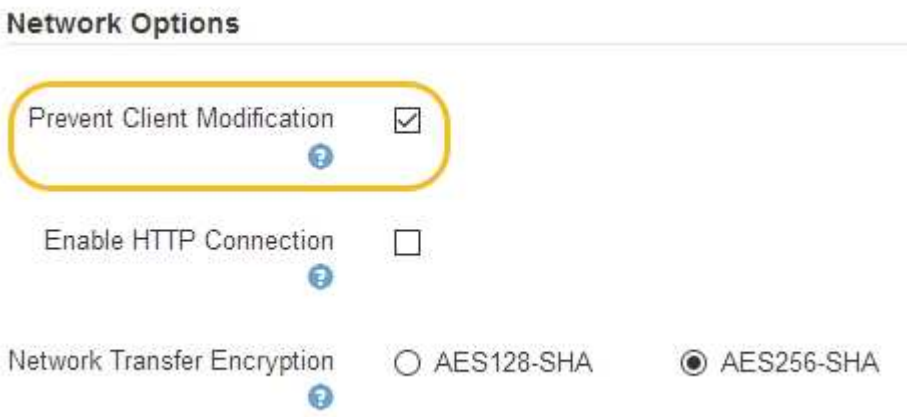
- * S3 REST APi*
  - 删除存储分段请求
  - 修改现有对象数据，用户定义的元数据或 S3 对象标记的任何请求

> 此设置不适用于启用了版本控制的存储分段。版本控制已阻止对对象数据，用户定义的元数据和对象标记进行修改。

- * Swift REST APi*
  - 删除容器请求
  - 修改任何现有对象的请求。例如，以下操作被拒绝： PUT 覆盖，删除，元数据更新等。

步骤

1. 选择 * 配置 * > * 系统 * > * 网格选项 * 。
2. 在网络选项部分中，选中 * 阻止客户端修改 * 复选框。



3. 选择 * 保存 * 。

管理网络和连接

StorageGRID 网络准则

您可以使用网格管理器配置和管理 StorageGRID 网络和连接。

请参见 配置 S3 和 Swift 客户端连接 了解如何连接 S3 或 Swift 客户端。

默认 StorageGRID 网络

默认情况下， StorageGRID 支持每个网格节点使用三个网络接口，从而可以根据您的安全和访问要求为每个网格节点配置网络。

有关网络拓扑的详细信息，请参见 网络连接准则。

网格网络

Required网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。

管理网络

可选。管理网络通常用于系统管理和维护。它也可用于客户端协议访问。管理网络通常是一个专用网络，不需要在站点之间进行路由。

客户端网络

可选。客户端网络是一种开放网络，通常用于提供对 S3 和 Swift 客户端应用程序的访问，因此网格网络可以进行隔离和保护。客户端网络可以与可通过本地网关访问的任何子网进行通信。

准则

- 每个 StorageGRID 网格节点都需要为其分配到的每个网络配置一个专用网络接口， IP 地址，子网掩码和网关。
- 一个网格节点在一个网络上不能有多个接口。
- 支持每个网格节点在每个网络上使用一个网关，并且该网关必须与节点位于同一子网中。如果需要，您可以在网关中实施更复杂的路由。
- 在每个节点上，每个网络都映射到一个特定的网络接口。

网络	接口名称
网格	eth0
admin （可选）	Eth1
客户端（可选）	Eth2

- 如果节点连接到 StorageGRID 设备，则每个网络都使用特定端口。有关详细信息，请参见适用于您的设备的安装说明。
- 每个节点都会自动生成默认路由。如果启用了 eth2 ，则 0.0.0.0/0 将在 eth2 上使用客户端网络。如果未启用 eth2 ，则 0.0.0.0/0 将在 eth0 上使用网格网络。
- 只有在网格节点加入网格后，客户端网络才会正常运行
- 可以在网格节点部署期间配置管理网络，以便在网格完全安装之前能够访问安装用户界面。

可选接口

您也可以向节点添加额外的接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口 隔离属于不同应用程序或租户的流量。或者，您可能希望添加要在中使用的访问接口 高可用性（ HA ）组。

要添加中继或访问接口，请参见以下内容：

- * VMware （安装节点后） *： VMware： 向节点添加中继或访问接口
- * RHEL 或 CentOS （安装节点之前） *： 创建节点配置文件
- * Ubuntu 或 Debian （安装节点之前） *： 创建节点配置文件
- * RHEL ， CentOS ， Ubuntu 或 Debian （安装节点后） *： Linux： 向节点添加中继或访问接口

查看 **IP** 地址

您可以查看 StorageGRID 系统中每个网格节点的 IP 地址。然后，您可以使用此 IP 地址通过命令行登录到网格节点并执行各种维护过程。

您需要的内容

您将使用登录到网格管理器 支持的 Web 浏览器。

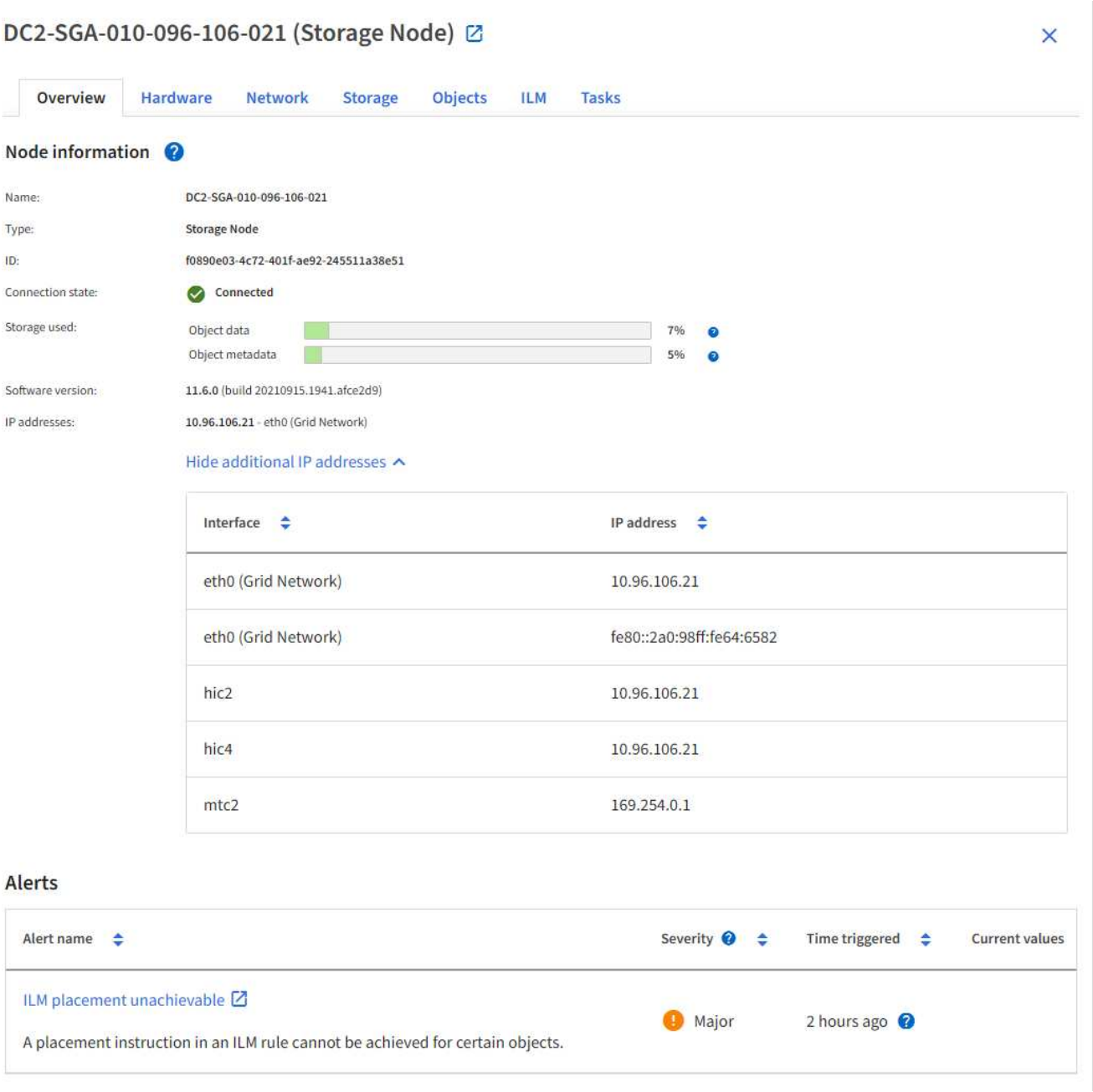
关于此任务

有关更改 IP 地址的信息，请参见 恢复和维护。

步骤

1. 选择 * 节点 * > * 网格节点 _* > * 概述 * 。
2. 选择 IP 地址标题右侧的 * 显示更多 * 。

   此网格节点的 IP 地址会在表中列出。



支持传出 **TLS** 连接的密码

StorageGRID 系统支持一组有限的密码套件，用于将传输层安全（ Transport Layer Security ， TLS ）连接到用于身份联合和云存储池的外部系统。

支持的 **TLS** 版本

StorageGRID 支持使用 TLS 1.2 和 TLS 1.3 连接到用于身份联合和云存储池的外部系统。

为了确保与一系列外部系统兼容，我们选择了可与外部系统结合使用的 TLS 密码。此列表大于支持在 S3 或 Swift 客户端应用程序中使用的密码列表。

协议版本，密码，密钥交换算法和 MAC 算法等 TLS 配置选项在 StorageGRID 中不可配置。如果您对这些设置有特定要求，请联系您的 NetApp 客户代表。

支持的 **TLS 1.2** 密码套件

支持以下 TLS 1.2 密码套件：

- tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256
- tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_ECDSA_WIT_AES_128_GCM_SHA256
- tls_ECDHE_ECDSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_RSA_WIT_CHACHA20_POLY1305
- tls_ECDHE_ECDSA_ING_CHACHA20_POLY1305
- tls_rsa_and_aes_128_gcm_SHA256
- tls_rsa_and_aes_256_gcm_SHA384

支持的 **TLS 1.3** 密码套件

支持以下 TLS 1.3 密码套件：

- tls_aes_256_gcm_SHA384
- tls_chacHA20_POLY1305_SHA256
- tls_aes_128_gcm_SHA256

更改网络传输加密

StorageGRID 系统使用传输层安全（ Transport Layer Security ， TLS ）保护网格节点之间的内部控制流量。网络传输加密选项用于设置 TLS 用于加密网格节点之间的控制流量的算法。此设置不会影响数据加密。

您需要的内容

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

关于此任务

默认情况下，网络传输加密使用 AES256-SHA 算法。此外，还可以使用 AES128-SHA 算法对控制流量进行加密。

步骤

1. 选择 * 配置 * > * 系统 * > * 网格选项 * 。
2. 在网络选项部分中，将网络传输加密更改为 * AES128-SHA* 或 * AES256-SHA* （默认）。

3. 选择 * 保存 * 。

管理流量分类策略

管理流量分类策略

为了增强服务质量（ QoS ）服务，您可以创建流量分类策略来识别和监控不同类型的网络流量。这些策略有助于限制和监控流量。

流量分类策略应用于网关节点和管理节点的 StorageGRID 负载平衡器服务上的端点。要创建流量分类策略，必须已创建负载平衡器端点。

匹配规则

每个流量分类策略都包含一个或多个匹配规则，用于标识与以下一个或多个实体相关的网络流量：

- 存储分段
- Tenants
- 子网（包含客户端的 IPv4 子网）
- 端点（负载平衡器端点）

StorageGRID 会根据规则的目标监控与策略中任何规则匹配的流量。与某个策略的任何规则匹配的任何流量均由该策略处理。相反，您可以设置规则来匹配除指定实体之外的所有流量。

流量限制

您也可以根据以下参数为策略设置限制：

- 中的聚合带宽
- 聚合带宽不足
- 并发读取请求
- 并发写入请求
- 每个请求的带宽
- 每个请求的带宽不足
- 读取请求速率
- 写入请求速率

限制值按负载平衡器强制实施。如果流量同时分布在多个负载平衡器上，则总最大速率是您指定的速率限制的倍数。

> 您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是， StorageGRID 不能同时限制这两种类型的带宽。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。

对于聚合或每个请求的带宽限制，请求将以您设置的速率传入或移出。StorageGRID 只能强制执行一个速度，因此，按匹配器类型强制执行最具体的策略匹配。对于所有其他限制类型，客户端请求会延迟 250 毫秒，对于超过任何匹配策略限制的请求，客户端请求会收到 503 个响应速度较慢的响应。

在网格管理器中，您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

使用具有 **SLA** 的流量分类策略

您可以将流量分类策略与容量限制和数据保护结合使用来实施服务级别协议（ SLA ），这些协议提供了有关容量，数据保护和性能的具体信息。

每个负载平衡器都会实施流量分类限制。如果流量同时分布在多个负载平衡器上，则总最大速率是您指定的速率限制的倍数。

以下示例显示了一个 SLA 的三个层。您可以创建流量分类策略以实现每个 SLA 层的性能目标。

服务级别层	**Capacity**	数据保护	性能	成本
金牌	允许 1 PB 存储	3 复制 ILM 规则	25 K 请求 / 秒 5 GB/ 秒（ 40 Gbps ）带宽	每月 $$
银牌	允许使用 250 TB 存储	2 复制 ILM 规则	每秒 10 K 个请求 1.25 GB/ 秒（ 10 Gbps ）带宽	每月 $$
铜牌	允许 100 TB 存储	2 复制 ILM 规则	5 K 请求 / 秒 1 GB/ 秒（ 8 Gbps ）带宽	每月 $

创建流量分类策略

如果要按分段，租户， IP 子网或负载平衡器端点监控网络流量，并可选择限制此流量，则可以创建流量分类策略。您也可以根据带宽，并发请求数或请求率为策略设置限制。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 您已创建要匹配的任何负载平衡器端点。

- 您已创建要匹配的任何租户。

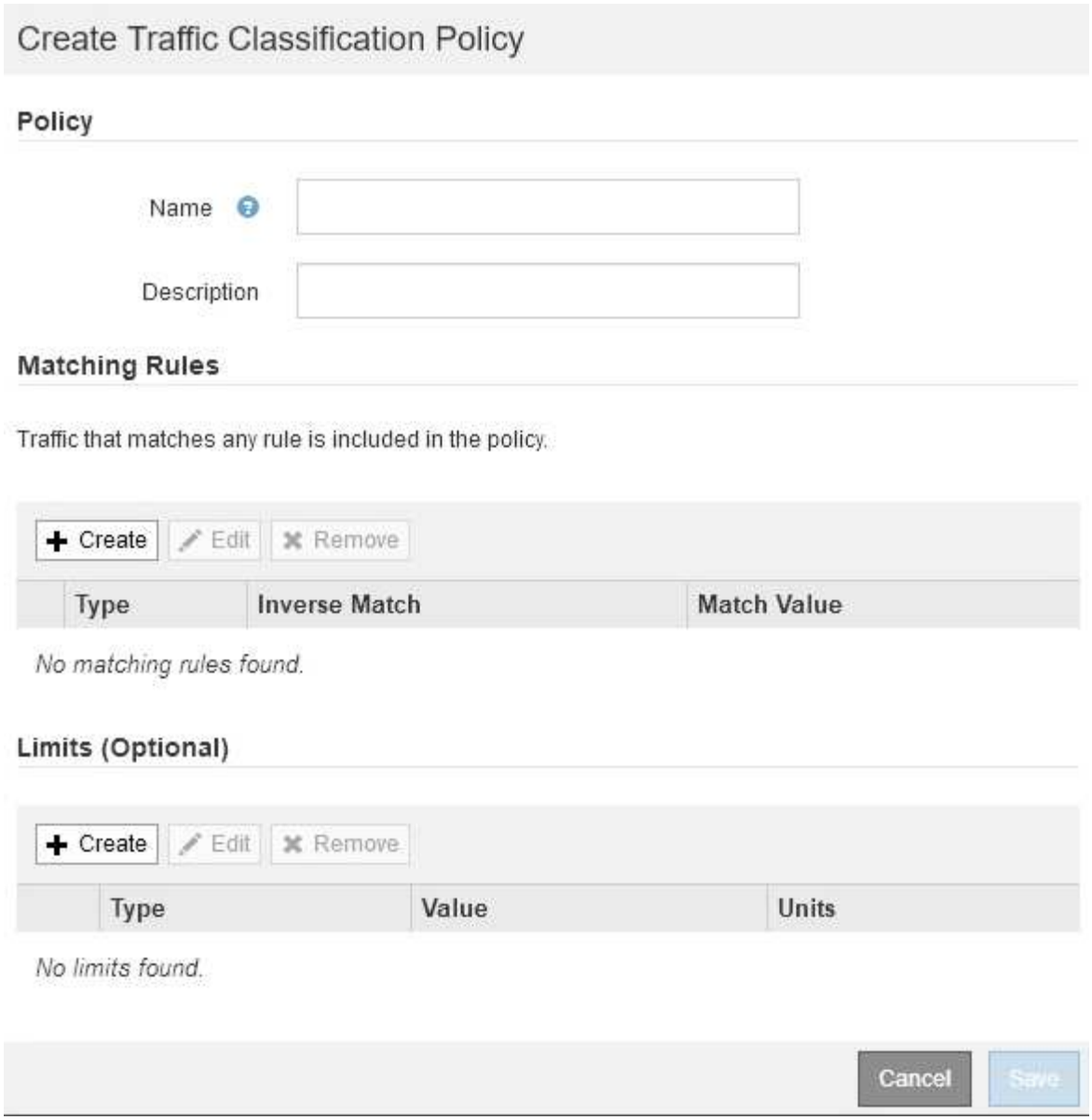
步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示 " 流量分类策略 " 页面。

2. 选择 * 创建 * 。

   此时将显示创建流量分类策略对话框。



3. 在 * 名称 * 字段中，输入策略的名称。

   输入描述性名称，以便识别策略。

4. 也可以在 * 问题描述 * 字段中为策略添加问题描述 。

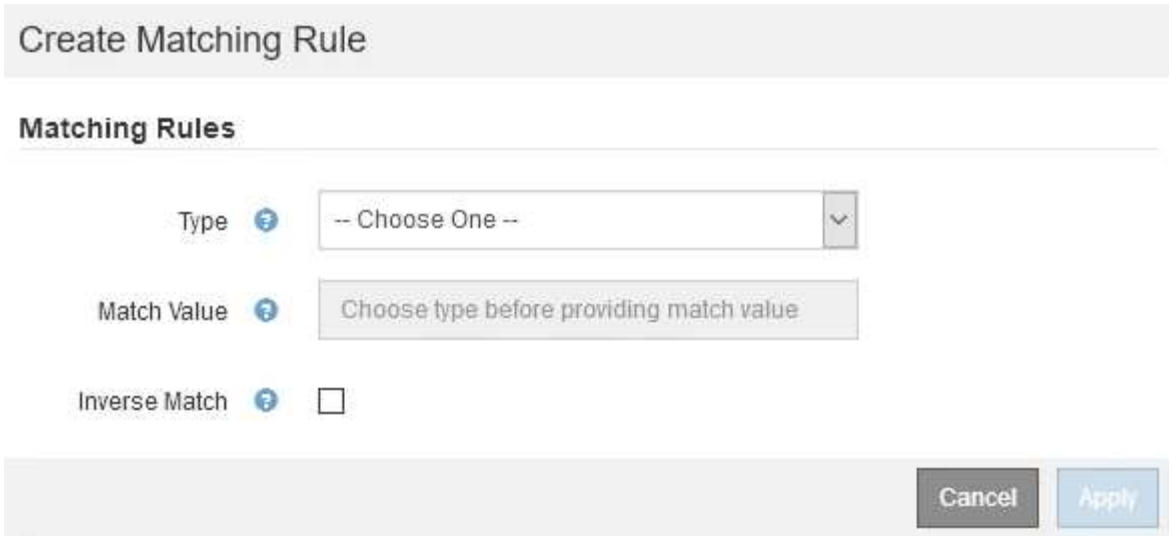
   例如，描述此流量分类策略适用场景 及其限制。

5. 为策略创建一个或多个匹配规则。

   匹配规则控制哪些实体将受此流量分类策略的影响。例如，如果要将此策略应用于特定租户的网络流量，请选择租户。或者，如果要将此策略应用于特定负载平衡器端点上的网络流量，请选择 Endpoint 。

   a. 在 * 匹配规则 * 部分中选择 * 创建 * 。

      此时将显示创建匹配规则对话框。



b. 从 * 类型 * 下拉列表中，选择要包含在匹配规则中的实体类型。

c. 在 * 匹配值 * 字段中，根据您选择的实体类型输入匹配值。

- 存储分段：输入存储分段名称。
- Bucket Rex ： 输入用于匹配一组存储分段名称的正则表达式。

  正则表达式已取消锁定。使用 ｛caret｝ 定位点在存储分段名称开头匹配，并使用 $ 定位点在存储分段名称末尾匹配。

- CIDR ： 以 CIDR 表示法输入与所需子网匹配的 IPv4 子网。
- Endpoint ： 从现有端点列表中选择一个端点。这些是您在负载平衡器端点页面上定义的负载平衡器端点。请参见 配置负载平衡器端点。
- 租户：从现有租户列表中选择一个租户。租户匹配取决于所访问的存储分段的所有权。对存储分段的匿名访问与拥有存储分段的租户匹配。

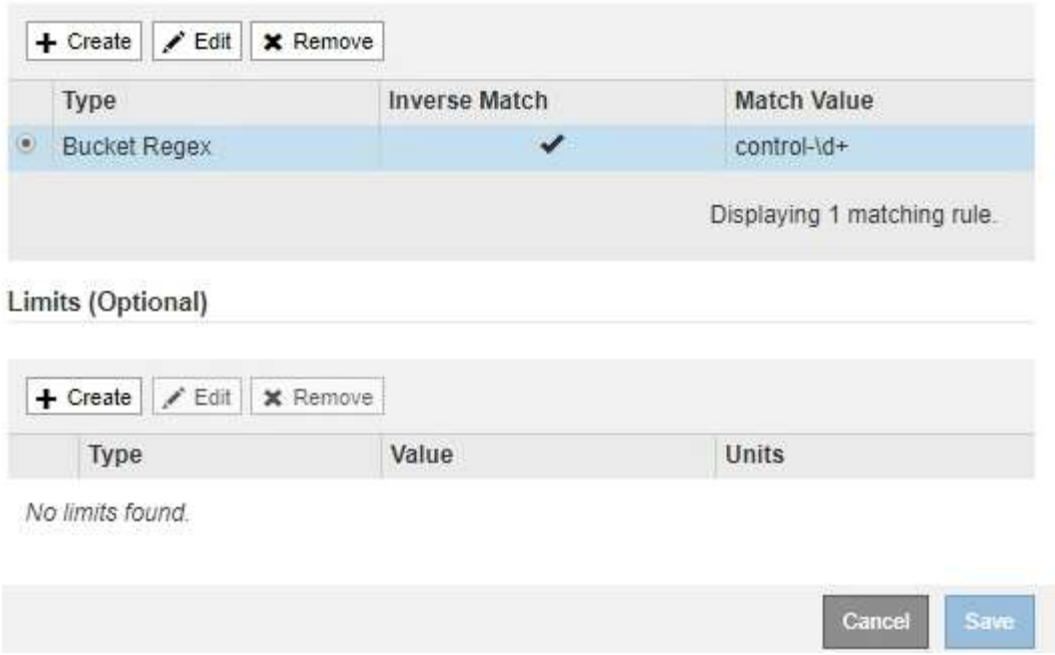
d. 如果要匹配与刚刚定义的类型和匹配值一致的所有网络流量 _except _ 流量，请选中 * 反向 * 复选框。否则，请取消选中此复选框。

例如，如果要将此策略应用于除一个负载平衡器端点之外的所有其他端点，请指定要排除的负载平衡器端点，然后选择 * 反向 * 。

> 对于包含多个匹配器且至少有一个是反向匹配器的策略，请注意不要创建与所有请求匹配的策略。

e. 选择 * 应用 * 。

此时将创建此规则，并将其列在匹配规则表中。



a. 对要为策略创建的每个规则重复上述步骤。

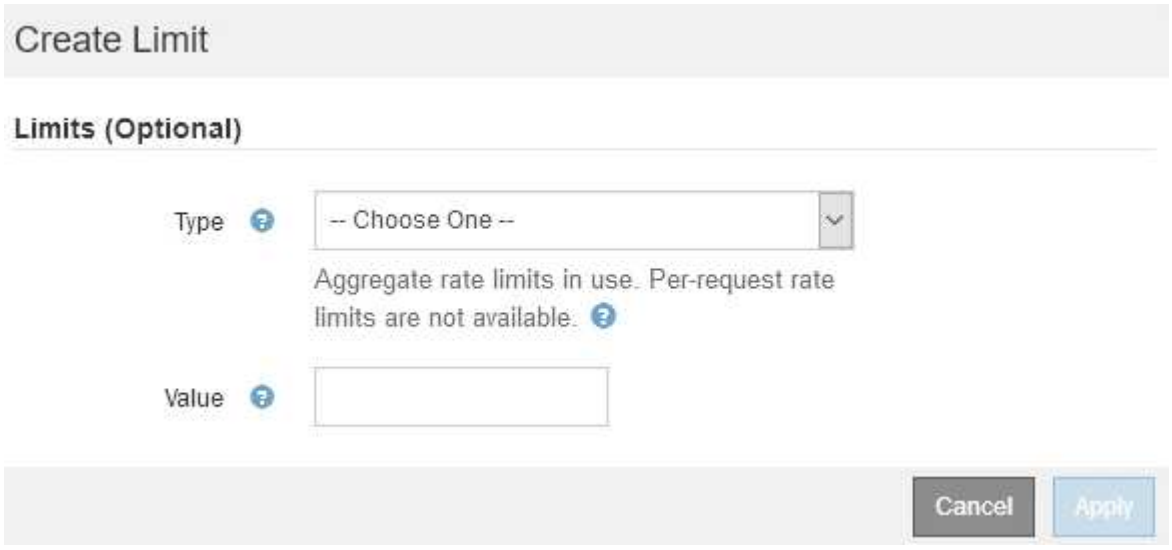
> 与任何规则匹配的流量由策略处理。

6. 也可以为策略创建限制。

> 即使不创建限制， StorageGRID 也会收集指标，以便监控与策略匹配的网络流量。

a. 在 * 限制 * 部分中选择 * 创建 * 。

此时将显示创建限制对话框。



b. 从 * 类型 * 下拉列表中，选择要应用于策略的限制类型。

在以下列表中， * 输入 * 是指从 S3 或 Swift 客户端到 StorageGRID 负载平衡器的流量， * 输出 * 是指从负载平衡器到 S3 或 Swift 客户端的流量。

- 中的聚合带宽
- 聚合带宽不足
- 并发读取请求
- 并发写入请求
- 每个请求的带宽
- 每个请求的带宽不足
- 读取请求速率
- 写入请求速率

> 您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是， StorageGRID 不能同时限制这两种类型的带宽。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。

对于带宽限制， StorageGRID 会应用与设置的限制类型最匹配的策略。例如，如果您的策略仅限制一个方向的流量，则相反方向的流量将是无限制的，即使存在与具有带宽限制的其他策略匹配的流量也是如此。StorageGRID 按以下顺序实施 "`最佳` " 匹配的带宽限制：

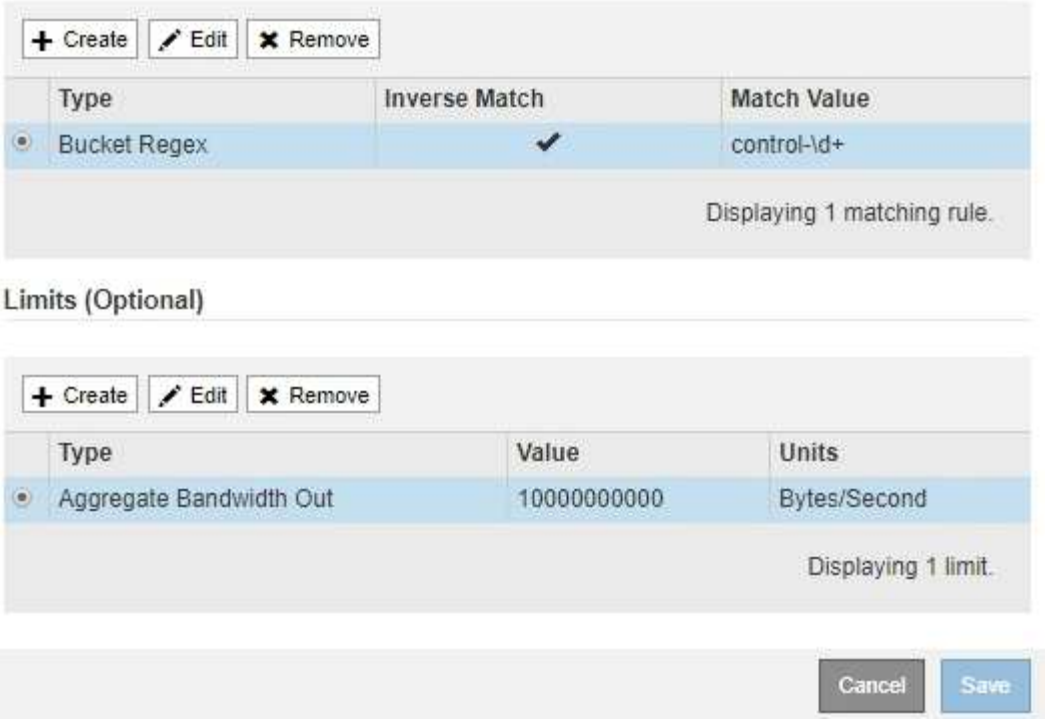
- 确切的 IP 地址（ /32 掩码）
- 确切的存储分段名称
- 分段正则表达式
- 租户
- 端点
- 非精确的 CIDR 匹配项（非 /32 ）
- 反向匹配

c. 在 * 值 * 字段中，输入所选限制类型的数值。

选择限制时，系统将显示预期单位。

d. 选择 * 应用 * 。

此时将创建此限制，并将其列在限制表中。



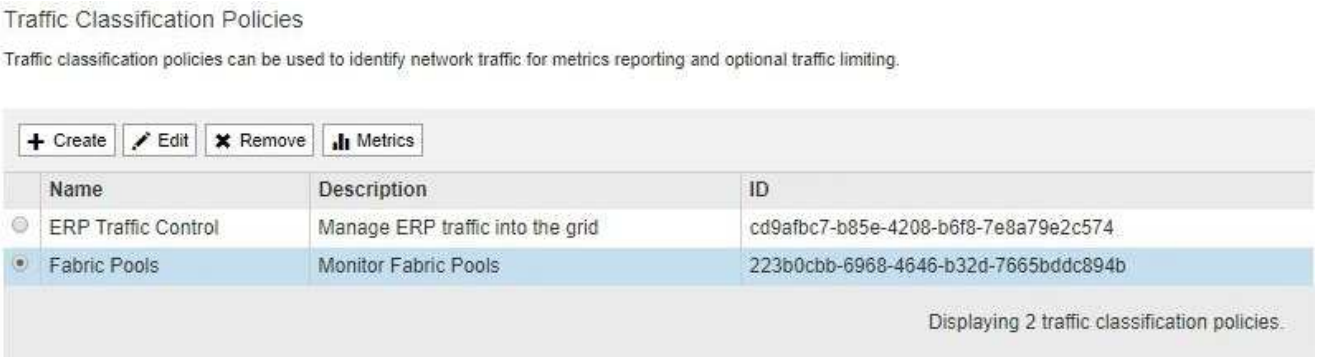
e. 对要添加到策略中的每个限制重复上述步骤。

例如，如果要为 SLA 层创建 40 Gbps 带宽限制，请创建 " 聚合带宽限制 " 和 " 聚合带宽超限 " ，并将每个限制设置为 40 Gbps 。

要将每秒兆字节数转换为每秒千兆位数，请乘以 8 。例如， 125 MB/ 秒相当于 1 ， 000 Mbps 或 1 Gbps 。

7. 创建完规则和限制后，请选择 * 保存 * 。

此策略将保存并列出在 " 流量分类策略 " 表中。



现在， S3 和 Swift 客户端流量将根据流量分类策略进行处理。您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。请参见 查看网络流量指标。

编辑流量分类策略

您可以编辑流量分类策略以更改其名称或问题描述 ，或者创建，编辑或删除此策略的任何规则或限制。

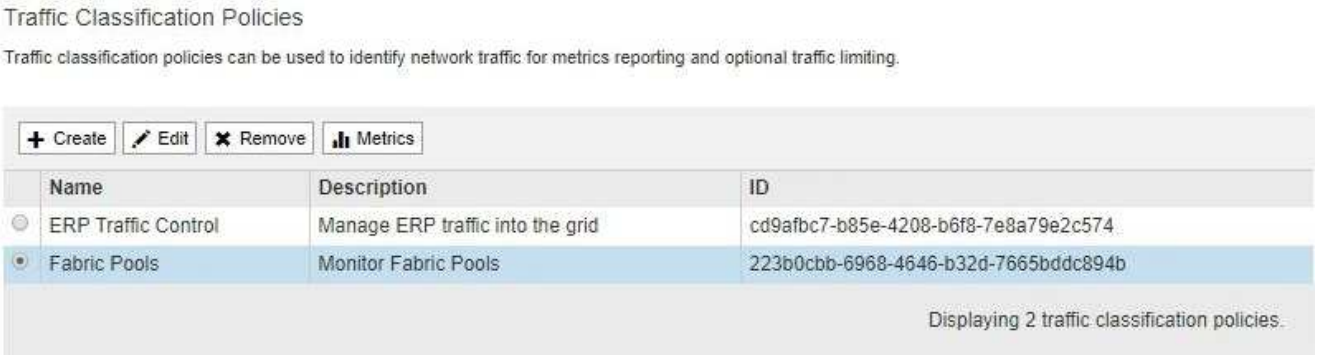
您需要的内容

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

步骤

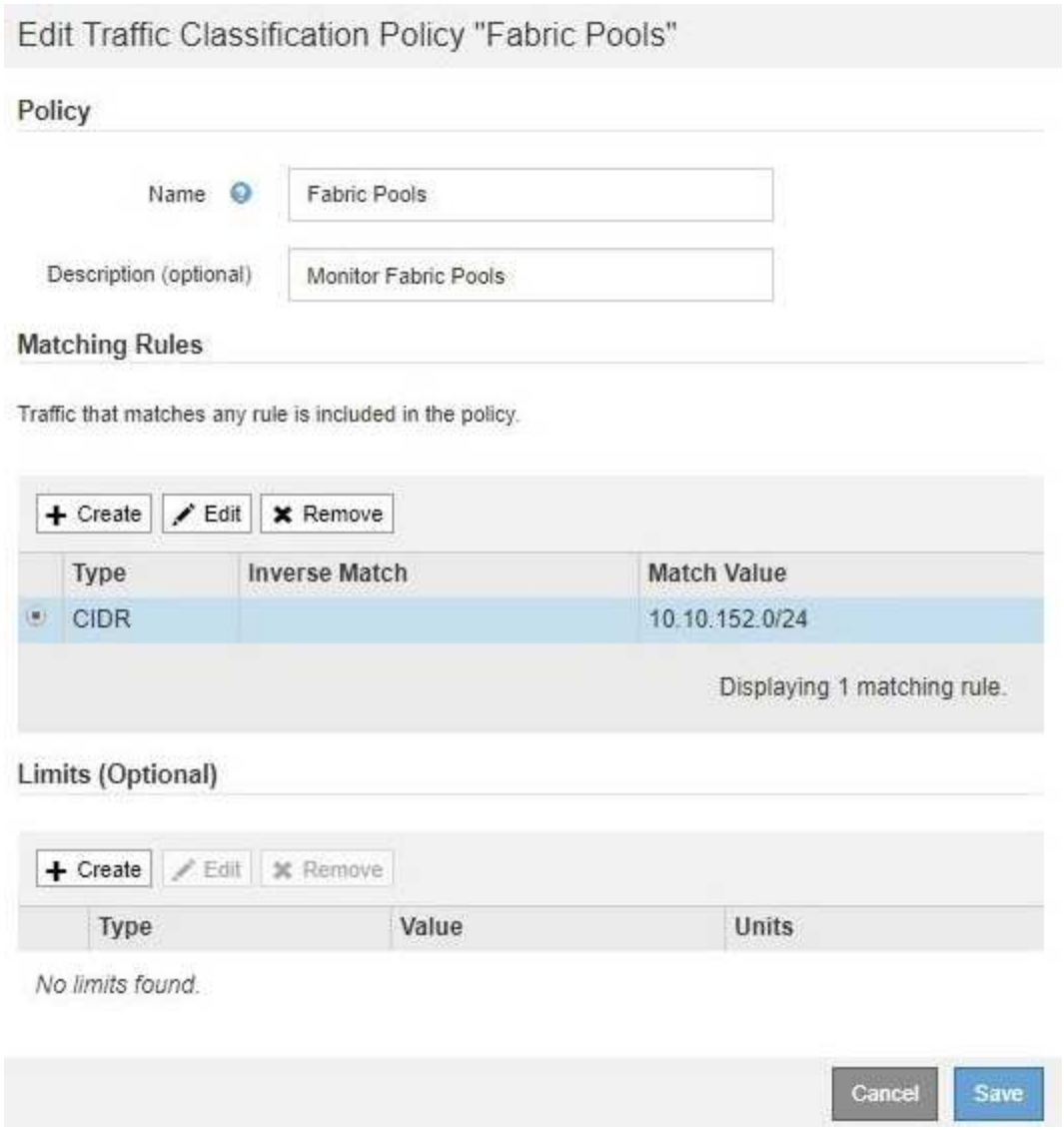
1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



2. 选择要编辑的策略左侧的单选按钮。
3. 选择 * 编辑 * 。

   此时将显示编辑流量分类策略对话框。



4. 根据需要创建，编辑或删除匹配的规则和限制。
   a. 要创建匹配的规则或限制，请选择 * 创建 * ，然后按照说明创建规则或创建限制。
   b. 要编辑匹配的规则或限制，请选择规则或限制的单选按钮，在 * 匹配规则 * 部分或 * 限制 * 部分中选择 * 编辑 * ，然后按照说明创建规则或创建限制。
   c. 要删除匹配的规则或限制，请选择规则或限制的单选按钮，然后选择 * 删除 * 。然后，选择 * 确定 * 以确认要删除规则或限制。
5. 创建或编辑规则或限制后，请选择 * 应用 * 。
6. 编辑完策略后，选择 * 保存 * 。

   您对策略所做的更改将被保存，网络流量现在将根据流量分类策略进行处理。您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

删除流量分类策略

如果您不再需要流量分类策略，可以将其删除。

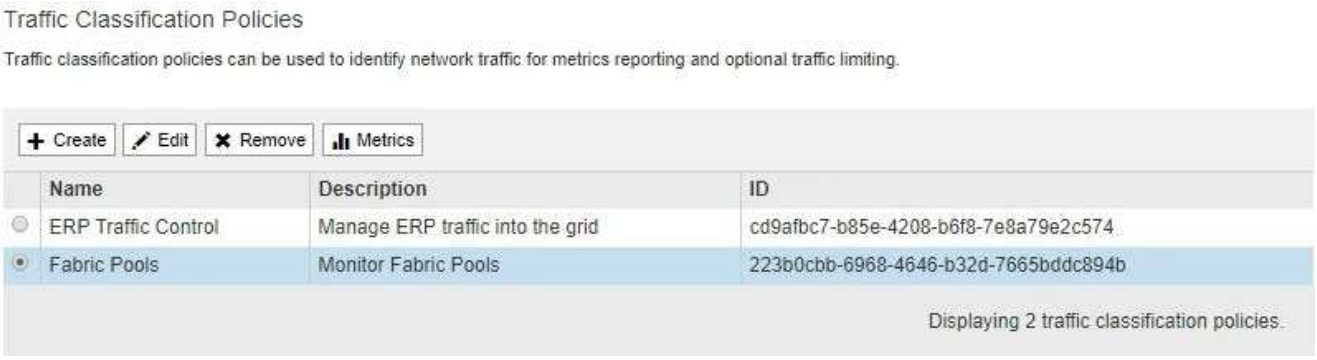
您需要的内容

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

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



2. 选择要删除的策略左侧的单选按钮。
3. 选择 * 删除 * 。

   此时将显示警告对话框。

4. 选择 * 确定 * 确认要删除此策略。

   此策略将被删除。

查看网络流量指标

您可以通过查看 " 流量分类策略 " 页面上的图形来监控网络流量。

您需要的内容

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

关于此任务

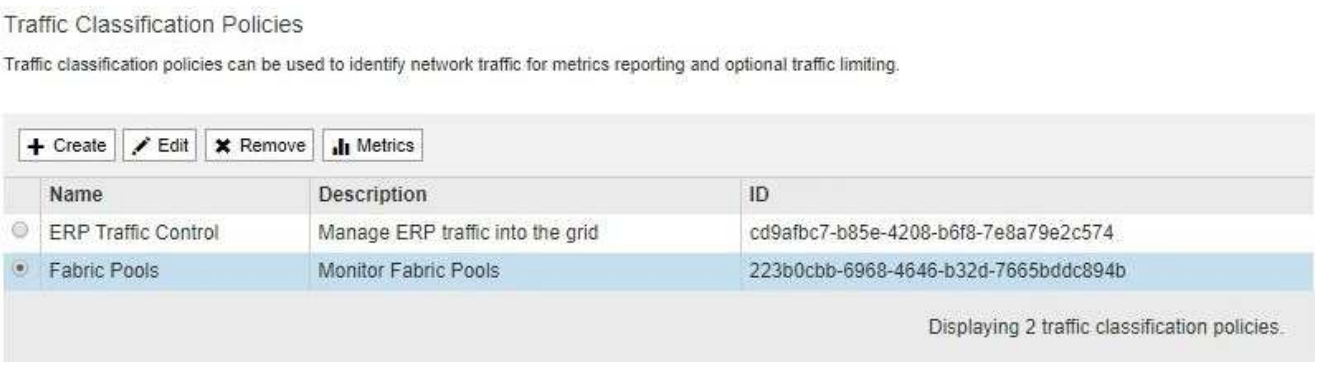
对于任何现有流量分类策略，您可以查看负载平衡器服务的指标，以确定该策略是否成功限制网络中的流量。图形中的数据可以帮助您确定是否需要调整策略。

即使没有为流量分类策略设置限制，也会收集指标，并且图形可提供有用的信息来了解流量趋势。

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



   如果您具有租户帐户权限，但没有 root 访问权限，则 * 创建 * ， * 编辑 * 和 * 删除 * 按钮将被禁用。

2. 选择要查看指标的策略左侧的单选按钮。
3. 选择 * 指标 * 。

   此时将打开一个新浏览器窗口，并显示流量分类策略图形。这些图形仅显示与选定策略匹配的流量的指标。

   您可以使用 * 策略 * 下拉列表选择其他要查看的策略。

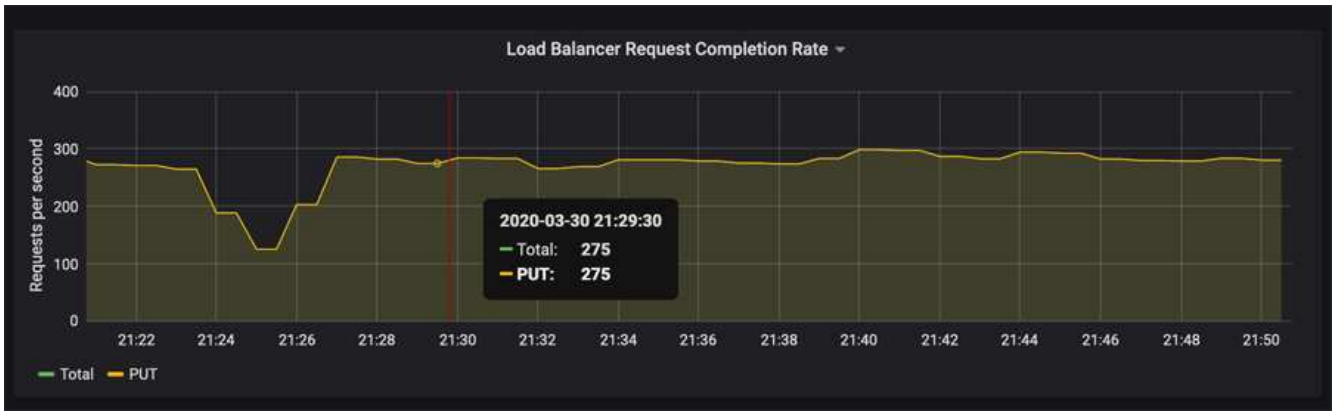
   网页上包含以下图形。

   - 负载平衡器请求流量：此图提供负载平衡器端点与发出请求的客户端之间传输的数据吞吐量的 3 分钟移

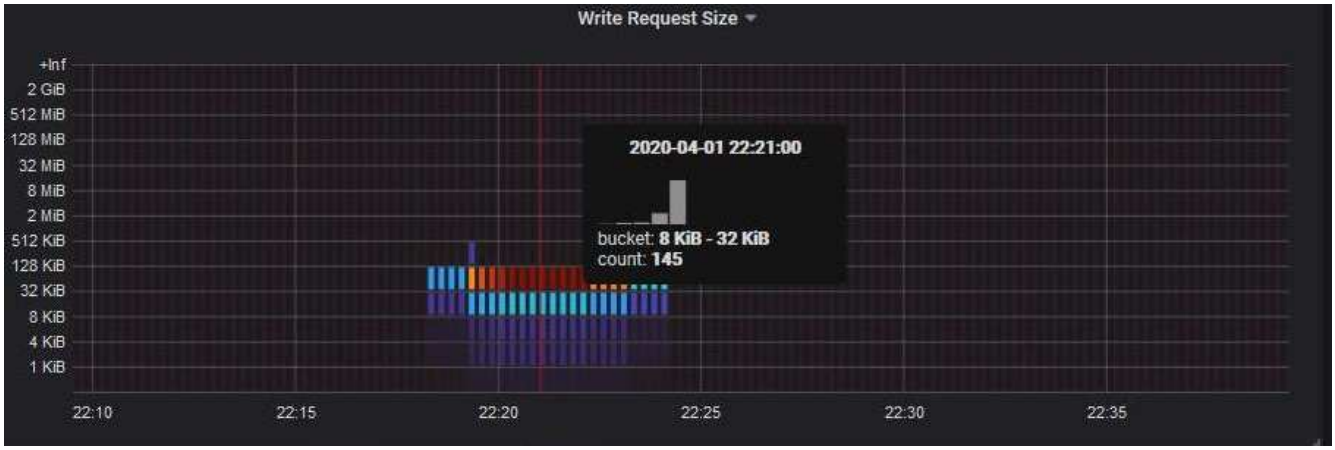
动平均值，以每秒位数为单位。

- 负载平衡器请求完成率：此图按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分，提供每秒已完成请求数的 3 分钟移动平均值。验证新请求的标头后，此值将更新。
- 错误响应率：此图提供了每秒返回给客户端的错误响应数的 3 分钟移动平均值，并按错误响应代码进行细分。
- 平均请求持续时间（非错误）：此图提供了按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分的 3 分钟移动平均请求持续时间。每个请求持续时间从负载平衡器服务解析请求标头时开始，到将完整的响应正文返回给客户端时结束。
- 按对象大小划分的写入请求速率：此热图根据对象大小提供 3 分钟的写入请求完成速率移动平均值。在这种情况下，写入请求仅指 PUT 请求。
- 按对象大小划分的读取请求速率：此热图提供了根据对象大小完成读取请求的 3 分钟移动平均值。在这种情况下，读取请求仅指获取请求。热图中的颜色表示各个图形中对象大小的相对频率。较冷的颜色（例如紫色和蓝色）表示相对速率较低，较热的颜色（例如橙色和红色）表示相对速率较高。

4. 将光标悬停在折线图上可查看该图特定部分的值弹出窗口。



5. 将光标悬停在热图上可看到一个弹出窗口，其中显示样本的日期和时间，聚合到计数中的对象大小以及该时间段内的每秒请求数。



6. 使用左上角的 * 策略 * 下拉列表选择其他策略。

   此时将显示选定策略的图形。

7. 或者，也可以从 * 支持 * 菜单访问这些图形。

   a. 选择 * 支持 * > * 工具 * > * 指标 * 。

b. 在页面的 * Grafan* 部分中，选择 * 流量分类策略 * 。

c. 从页面左上角的下拉列表中选择策略。

流量分类策略通过其 ID 进行标识。策略 ID 会列在 " 流量分类策略 " 页面上。

8. 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。

相关信息

监控和故障排除

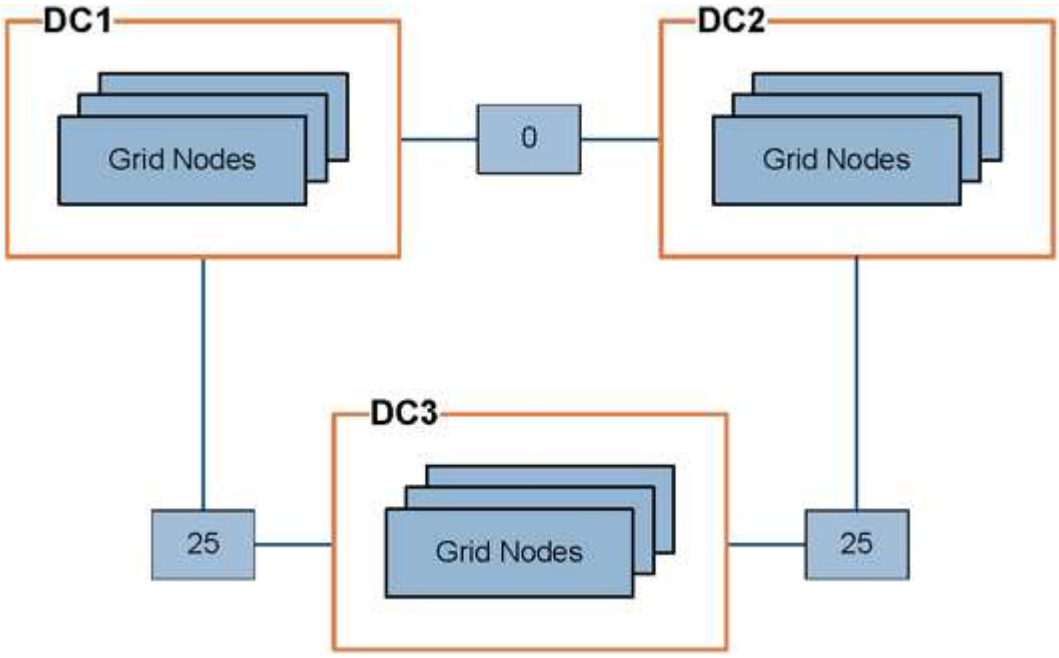
管理链路成本

链路成本是多少

链路成本可用于确定存在两个或更多数据中心站点时哪个数据中心站点提供请求的服务的优先级。您可以调整链路成本以反映站点之间的延迟。

- 链接成本用于确定用于实现对象检索的对象副本的优先级。
- 网格管理 API 和租户管理 API 使用链路成本来确定要使用的内部 StorageGRID 服务。
- 链路成本由网关节点上已弃用的连接负载平衡器（ CLB ）服务用于指导客户端连接。请参见 负载平衡的工作原理— CLB 服务。

此图显示了一个三站点网格，其中在站点之间配置了链路成本：



- 网关节点上的 CLB 服务会将客户端连接平均分布到同一数据中心站点上的所有存储节点以及任何数据中心站点，链路成本为 0 。

  在此示例中，数据中心站点 1 （ DC1 ）的网关节点会将客户端连接平均分布到 DC1 的存储节点和 DC2 的存储节点。DC3 上的网关节点仅向 DC3 上的存储节点发送客户端连接。

- 在检索作为多个复制副本存在的对象时， StorageGRID 会在链路成本最低的数据中心检索此副本。

在此示例中，如果 DC2 上的客户端应用程序检索存储在 DC1 和 DC3 上的对象，则会从 DC1 检索该对象，因为从 DC1 到 D2 的链路成本为 0 ，低于从 DC3 到 DC2 的链路成本（ 25 ）。

链路成本是任意的相对数字，没有特定的度量单位。例如，使用链路成本 50 比使用链路成本 25 更低。下表显示了常用链路成本。

链接。	链路成本	注释：
物理数据中心站点之间	25 （默认）	通过 WAN 链路连接的数据中心。
位于同一物理位置的逻辑数据中心站点之间	0	逻辑数据中心位于通过 LAN 连接的同一物理建筑或园区中。

更新链路成本

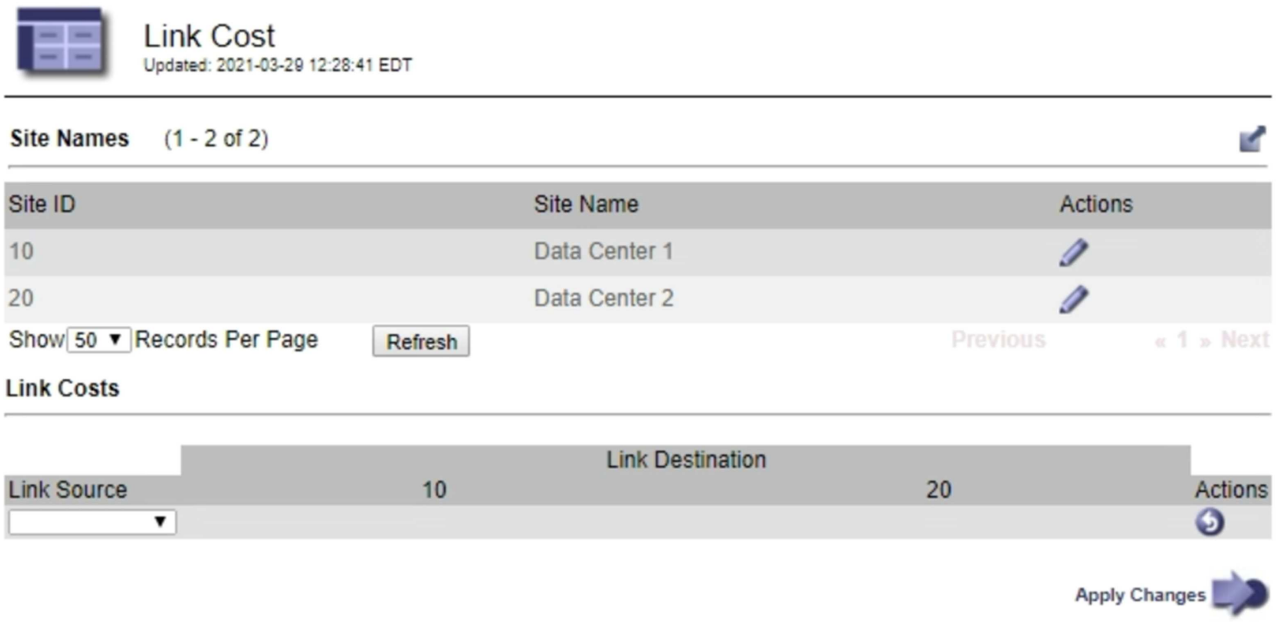
您可以更新数据中心站点之间的链路成本，以反映站点之间的延迟。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有网格拓扑页面配置权限。

步骤

1. 选择 * 配置 * > * 网络 * > * 链路成本 * 。



2. 在 * 链路源 * 下选择一个站点，然后在 * 链路目标 * 下输入一个介于 0 和 100 之间的成本值。

   如果源与目标相同，则无法更改链路成本。

   要取消更改，请选择 * 还原 * 。

3. 选择 * 应用更改 * 。

使用 AutoSupport

什么是 AutoSupport ？

通过 AutoSupport 功能， StorageGRID 系统可以向技术支持发送运行状况和状态消息。

使用 AutoSupport 可以显著加快问题的确定和解决速度。技术支持还可以监控系统的存储需求，并帮助您确定是否需要添加新节点或站点。您也可以将 AutoSupport 消息配置为发送到另一个目标。

AutoSupport 消息中包含的信息

AutoSupport 消息包含如下信息：

- StorageGRID 软件版本
- 操作系统版本
- 系统级别和位置级别属性信息
- 近期警报和警报（旧系统）
- 所有网格任务的当前状态，包括历史数据
- 管理节点数据库使用情况
- 丢失或缺失对象的数量
- 网格配置设置
- NMS 实体
- 活动 ILM 策略
- 已配置网格规范文件
- 诊断指标

您可以在首次安装 StorageGRID 时启用 AutoSupport 功能和各个 AutoSupport 选项，也可以稍后启用它们。如果未启用 AutoSupport ，网格管理器信息板上将显示一条消息。此消息包含指向 AutoSupport 配置页面的链接。

如果关闭此消息，则此消息将不会再次显示，直到清除浏览器缓存为止，即使 AutoSupport 仍处于禁用状态。

什么是 Active IQ ？

Active IQ 是一名基于云的数字顾问，利用 NetApp 客户群的预测性分析和社区智慧。其持续风险评估，预测性警报，规范化指导和自动化操作可帮助您在问题发生之前防患于未然，从而改善系统运行状况并提高系统可用性。

如果要使用 NetApp 支持站点上的 Active IQ 信息板和功能，则必须启用 AutoSupport 。

"Active IQ 数字顾问文档"

用于发送 **AutoSupport** 消息的协议

您可以选择以下三种协议之一来发送 AutoSupport 消息：

- HTTPS
- HTTP
- SMTP

如果使用 HTTPS 或 HTTP 发送 AutoSupport 消息，则可以在管理节点和技术支持之间配置非透明代理服务器。

如果使用 SMTP 作为 AutoSupport 消息的协议，则必须配置 SMTP 邮件服务器。

AutoSupport 选项

您可以使用以下选项的任意组合向技术支持发送 AutoSupport 消息：

- * 每周 * ： 每周自动发送一次 AutoSupport 消息。默认设置： enabled 。
- * 事件触发 * ： 每小时或发生重大系统事件时自动发送 AutoSupport 消息。默认设置： enabled 。
- * 按需 * ： 允许技术支持请求您的 StorageGRID 系统自动发送 AutoSupport 消息，这在他们正在使用问题描述 （需要 HTTPS AutoSupport 传输协议）时非常有用。默认设置： disabled 。
- * 用户触发 * ： 随时手动发送 AutoSupport 消息。

相关信息

"NetApp 支持"

配置 **AutoSupport**

您可以在首次安装 StorageGRID 时启用 AutoSupport 功能和各个 AutoSupport 选项，也可以稍后启用它们。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限或其他网格配置权限。
- 如果您要使用 HTTPS 或 HTTP 协议发送 AutoSupport 消息，则可以直接或使用代理服务器（不需要入站连接）提供对主管理节点的出站 Internet 访问。
- 如果要使用 HTTPS 或 HTTP 协议，并且要使用代理服务器，则可以使用 已配置管理员代理服务器。
- 如果要使用 SMTP 作为 AutoSupport 消息的协议，则表示已配置 SMTP 邮件服务器。警报电子邮件通知使用相同的邮件服务器配置（旧系统）。

指定 **AutoSupport** 消息的协议

您可以使用以下任一协议发送 AutoSupport 消息：

- * HTTPS ： 这是新安装的默认和建议设置。HTTPS 协议使用端口 443 。如果要启用 AutoSupport On Demand 功能，则必须使用 HTTPS 协议。
- * HTTP * ： 此协议不安全，除非在可信环境中使用，在该环境中，代理服务器在通过 Internet 发送数据时会转换为 HTTPS 。HTTP 协议使用端口 80 。
- * SMTP ： 如果要通过电子邮件发送 AutoSupport 消息，请使用此选项。如果使用 SMTP 作为 AutoSupport 消息的协议，则必须在 " 旧电子邮件设置 " 页面上配置 SMTP 邮件服务器（ * 支持 * > * 警报（旧） * > * 旧电子邮件设置 * ）。

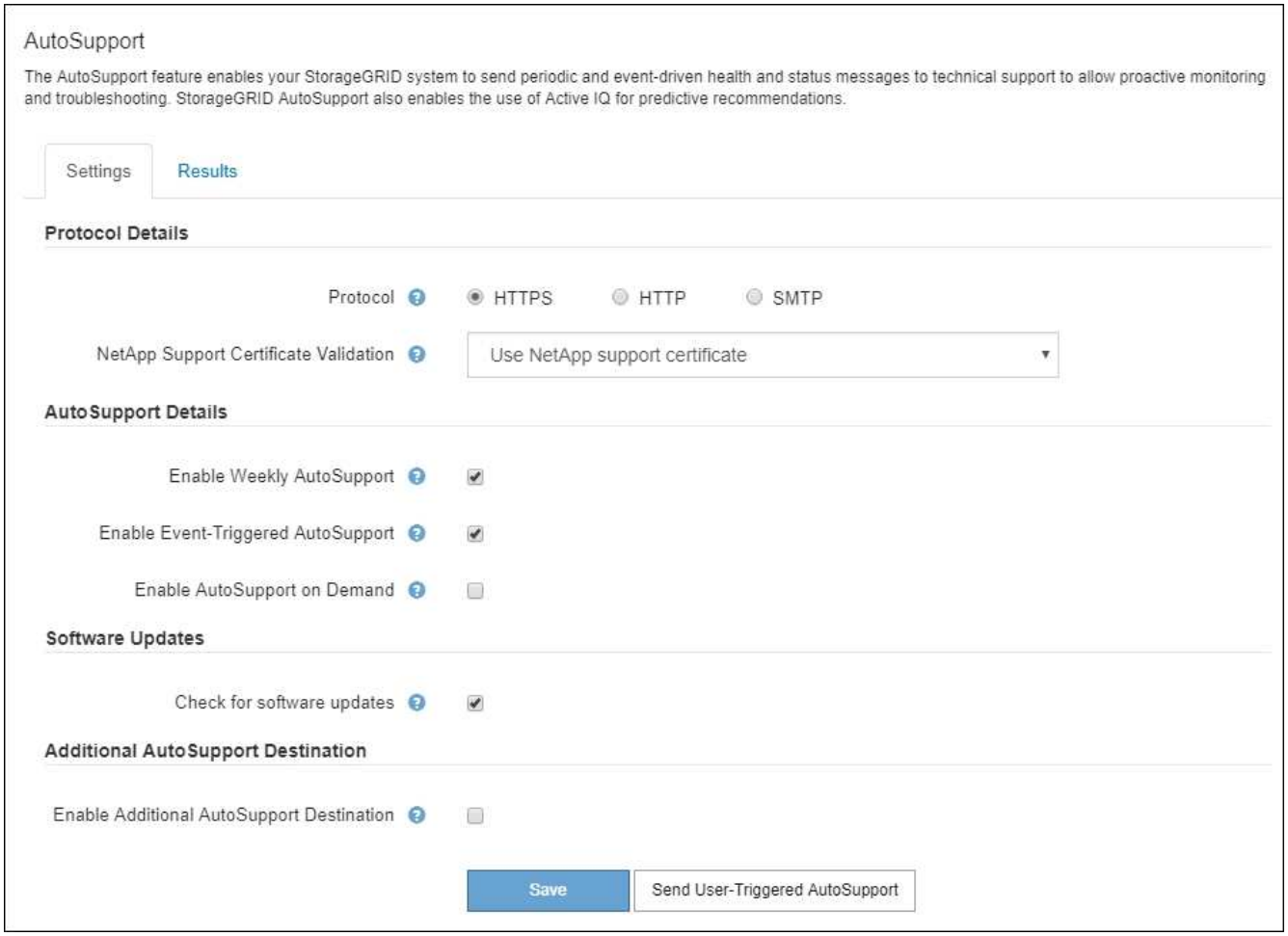
> 在 StorageGRID 11.2 版本之前， SMTP 是唯一可用于 AutoSupport 消息的协议。如果您最初安装的是早期版本的 StorageGRID ，则可能选择了 SMTP 协议。

您设置的协议用于发送所有类型的 AutoSupport 消息。

步骤

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

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



2. 选择要用于发送 AutoSupport 消息的协议。
3. 如果选择了 * HTTPS * ，请选择是否使用 TLS 证书来保护与 NetApp 支持服务器的连接。
   - * 使用 NetApp 支持证书 * （默认）： 证书验证可确保 AutoSupport 消息的传输安全。NetApp 支持证书

已随 StorageGRID 软件一起安装。

- * 不验证证书 * ： 只有当您有充分理由不使用证书验证时，例如证书出现临时问题时，才选择此选项。

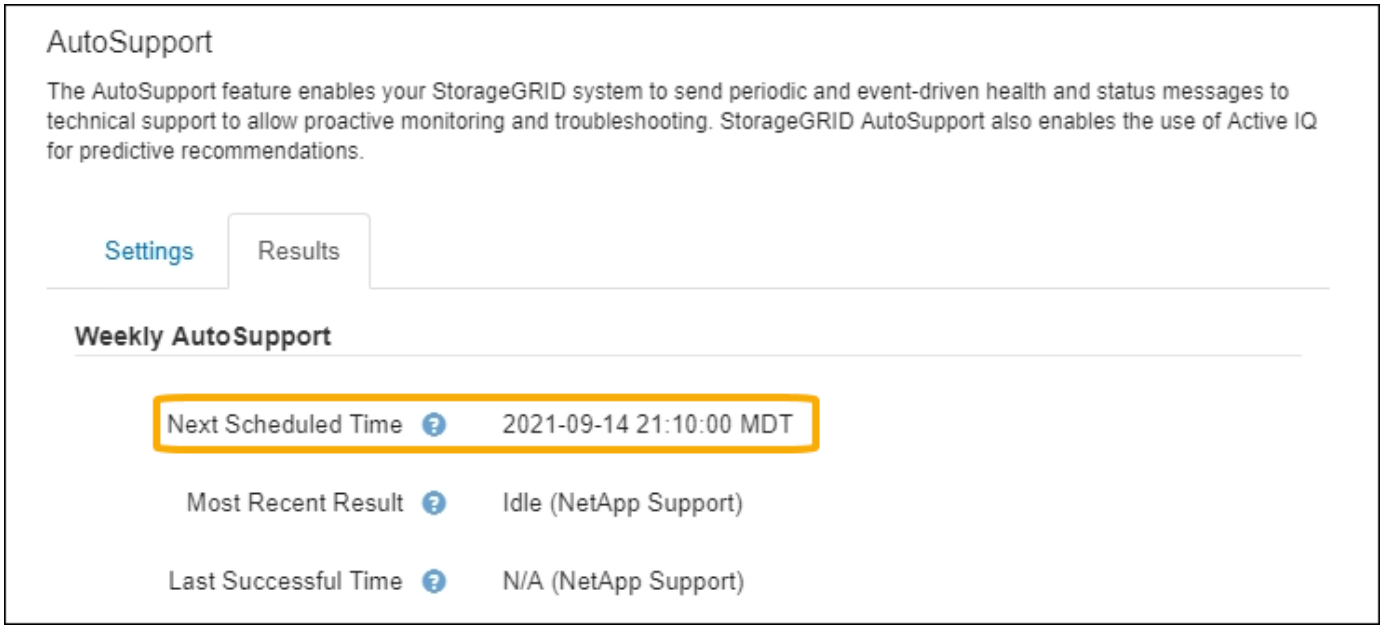
4. 选择 * 保存 * 。

所有每周消息，用户触发的消息和事件触发的消息均使用选定协议发送。

禁用每周 **AutoSupport** 消息

默认情况下， StorageGRID 系统配置为每周向 NetApp 支持发送一次 AutoSupport 消息。

要确定每周 AutoSupport 消息的发送时间，请转到 * AutoSupport * > * 结果 * 选项卡。在 * 每周 AutoSupport * 部分中，查看 * 下一计划时间 * 的值。



您可以随时禁止自动发送每周 AutoSupport 消息。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 取消选中 * 启用每周 AutoSupport * 复选框。
3. 选择 * 保存 * 。

禁用事件触发的 **AutoSupport** 消息

默认情况下， StorageGRID 系统配置为在发生重要警报或其他重要系统事件时向 NetApp 支持发送 AutoSupport 消息。

您可以随时禁用事件触发的 AutoSupport 消息。

> 在系统范围内禁止电子邮件通知时，也会禁止显示事件触发的 AutoSupport 消息。（选择 * 配置 * > * 系统 * > * 显示选项 * 。然后，选择 * 通知禁止全部 * 。）

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 取消选中 * 启用事件触发的 AutoSupport * 复选框。
3. 选择 * 保存 * 。

启用 **AutoSupport On Demand**

AutoSupport On Demand 可帮助解决技术支持正在积极处理的问题。

默认情况下， AutoSupport On Demand 处于禁用状态。启用此功能后，技术支持可以请求 StorageGRID 系统自动发送 AutoSupport 消息。技术支持还可以为 AutoSupport On Demand 查询设置轮询时间间隔。

技术支持无法启用或禁用 AutoSupport On Demand 。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 为协议选择 * HTTPS * 。
3. 选中 * 启用每周 AutoSupport * 复选框。
4. 选中 * 启用按需 AutoSupport * 复选框。
5. 选择 * 保存 * 。

   已启用 AutoSupport On Demand ，技术支持可以将 AutoSupport On Demand 请求发送到 StorageGRID 。

禁用软件更新检查

默认情况下， StorageGRID 会联系 NetApp 以确定您的系统是否有可用的软件更新。如果提供了 StorageGRID 修补程序或新版本，则新版本将显示在 StorageGRID 升级页面上。

根据需要，您可以选择禁用软件更新检查。例如，如果您的系统无法访问 WAN ，则应禁用此检查以避免下载错误。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 取消选中 * 检查软件更新 * 复选框。
3. 选择 * 保存 * 。

添加其他 **AutoSupport** 目标

启用 AutoSupport 后，系统会向 NetApp 支持部门发送运行状况和状态消息。您可以为所有 AutoSupport 消息指定一个其他目标。

要验证或更改用于发送 AutoSupport 消息的协议，请参见中的说明 指定 AutoSupport 消息的协议。

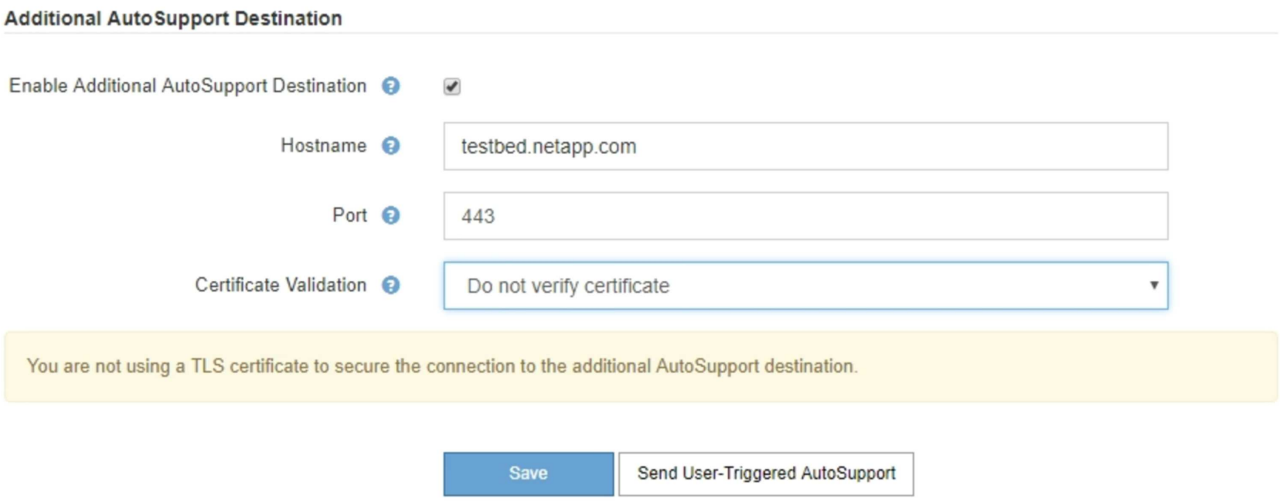
> 您不能使用 SMTP 协议将 AutoSupport 消息发送到其他目标。

步骤

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

2. 选择 * 启用其他 AutoSupport 目标 * 。

   此时将显示其他 AutoSupport 目标字段。



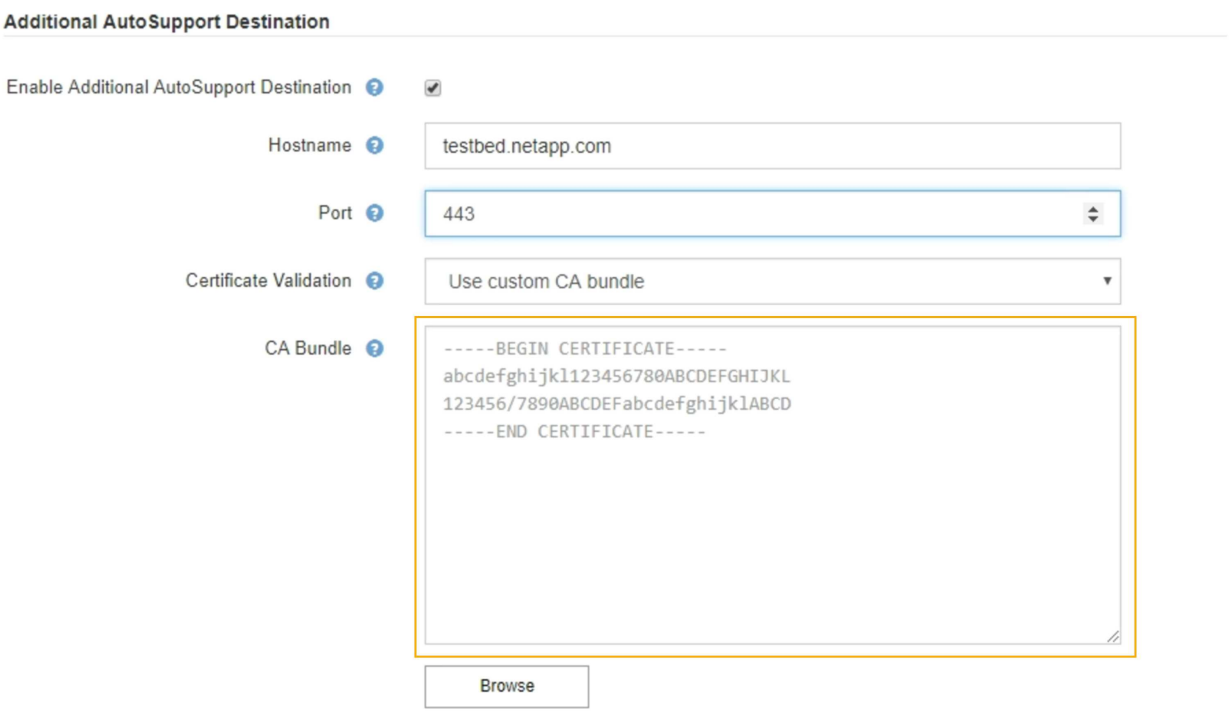
3. 输入其他 AutoSupport 目标服务器的服务器主机名或 IP 地址。

   您只能输入一个附加目标。

4. 输入用于连接到其他 AutoSupport 目标服务器的端口（对于 HTTP ，默认为端口 80 ，对于 HTTPS ，默认为端口 443 ）。

5. 要发送包含证书验证的 AutoSupport 消息，请在 * 证书验证 * 下拉列表中选择 * 使用自定义 CA 捆绑包 * 。然后，执行以下操作之一：

   - 使用编辑工具将 PEM 编码的每个 CA 证书文件的所有内容复制并粘贴到 * CA bundle* 字段中，该字段按证书链顺序串联。您必须在所选内容中包含 ` ---begin certificate--` 和 ` --end certificate--` 。



◦ 选择 * 浏览 * ，导航到包含证书的文件，然后选择 * 打开 * 上传文件。证书验证可确保 AutoSupport 消息的传输安全。

6. 要在不验证证书的情况下发送 AutoSupport 消息，请在 * 证书验证 * 下拉列表中选择 * 不验证证书 * 。

   只有当您有充分的理由不使用证书验证时，例如证书出现临时问题时，才选择此选项。

   警告此时将显示一条消息： " 您未使用 TLS 证书来保护与其他 AutoSupport 目标的连接。 "

7. 选择 * 保存 * 。

   未来所有每周，事件触发和用户触发的 AutoSupport 消息都将发送到其他目标。

手动触发 **AutoSupport** 消息

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

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限或其他网格配置权限。

步骤

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

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

2. 选择 * 发送用户触发的 AutoSupport * 。

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

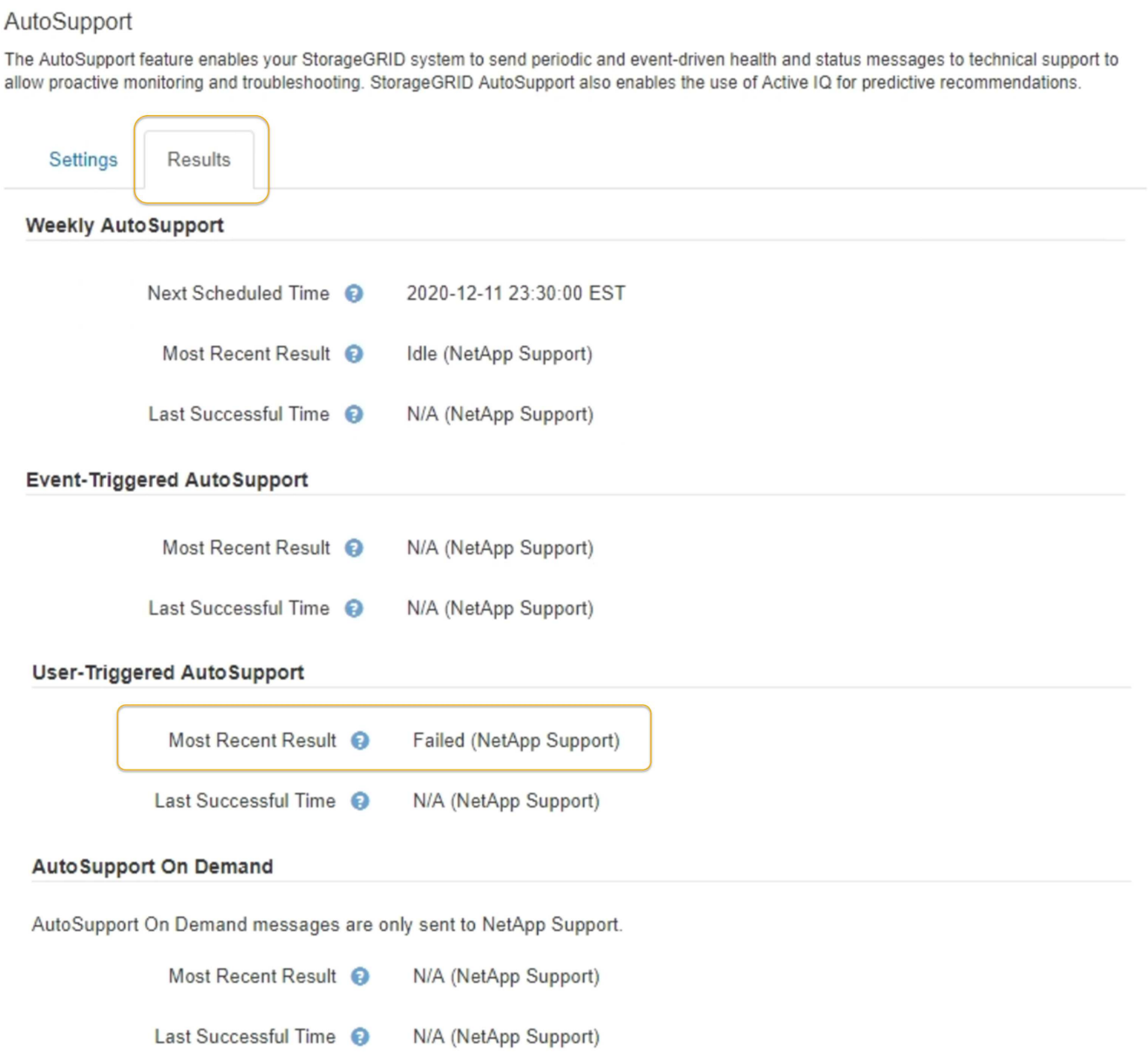
   发送用户触发的 AutoSupport 消息后，请在 1 分钟后刷新浏览器中的 AutoSupport 页面以访问最新结果。

对 **AutoSupport** 消息进行故障排除

如果尝试发送 AutoSupport 消息失败， StorageGRID 系统将根据 AutoSupport 消息的类型采取不同的操作。您可以通过选择 * 支持 * > * 工具 * > * AutoSupport * > * 结果 * 来检查 AutoSupport 消息的状态。

如果在系统范围内禁止发送电子邮件通知，则会禁止显示事件触发的 AutoSupport 消息。（选择 * 配置 * > * 系统 * > * 显示选项 * 。然后，选择 * 通知禁止全部 * 。）

如果 AutoSupport 消息无法发送，则 "`failed` " 将显示在 * AutoSupport * 页面的 * 结果 * 选项卡上。



每周 **AutoSupport** 消息失败

如果每周 AutoSupport 消息无法发送， StorageGRID 系统将执行以下操作：

1. 更新最新的 result 属性以重试。
2. 尝试每四分钟重新发送 15 次 AutoSupport 消息，持续一小时。
3. 发送失败一小时后，将最新结果属性更新为 Failed 。
4. 尝试在下次计划的时间重新发送 AutoSupport 消息。
5. 如果消息因 NMS 服务不可用而失败，并且消息在七天之前发送，则会保留常规 AutoSupport 计划。
6. 当 NMS 服务再次可用时，如果消息在七天或更长时间内未发送，则会立即发送 AutoSupport 消息。

用户触发或事件触发的 **AutoSupport** 消息失败

如果用户触发或事件触发的 AutoSupport 消息无法发送， StorageGRID 系统将执行以下操作：

1. 如果已知错误，则显示错误消息。例如，如果用户选择 SMTP 协议而未提供正确的电子邮件配置设置，则会显示以下错误： **由于电子邮件服务器页面上的设置不正确，无法使用 `SMTP` 协议发送 `AutoSupport` 消息。**
2. 不会再次尝试发送消息。
3. 在 `NMS.log` 中记录此错误。

如果发生故障且所选协议为 SMTP ，请验证 StorageGRID 系统的电子邮件服务器是否已正确配置且电子邮件服务器是否正在运行（ * 支持 * > * 警报（原有） * > * > 旧电子邮件设置 * ）。AutoSupport 页面可能会显示以下错误消息： **由于电子邮件服务器页面上的设置不正确，无法使用 `SMTP` 协议发送 `AutoSupport` 消息。**

了解如何在中配置电子邮件服务器设置 监控和故障排除说明。

更正 **AutoSupport** 消息故障

如果发生故障且所选协议为 SMTP ，请验证 StorageGRID 系统的电子邮件服务器是否已正确配置且您的电子邮件服务器是否正在运行。AutoSupport 页面可能会显示以下错误消息： **由于电子邮件服务器页面上的设置不正确，无法使用 `SMTP` 协议发送 `AutoSupport` 消息。**

通过 **StorageGRID** 发送 **E** 系列 **AutoSupport** 消息

您可以通过 StorageGRID 管理节点而不是存储设备管理端口向技术支持发送 E 系列 SANtricity System Manager AutoSupport 消息。

您需要的内容

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

> 要使用网格管理器访问SANtricity 系统管理器、您必须具有SANtricity 固件8.70 (11.7)或更高版本。

关于此任务

E 系列 AutoSupport 消息包含存储硬件的详细信息，比 StorageGRID 系统发送的其他 AutoSupport 消息更具体。

在 SANtricity 系统管理发生原因 器中配置一个特殊的代理服务器地址，以便在不使用设备管理端口的情况下通过 StorageGRID 管理节点传输 AutoSupport 消息。以这种方式传输的 AutoSupport 消息与可能已在网格管理器中配置的首选发件人和管理员代理设置相关。

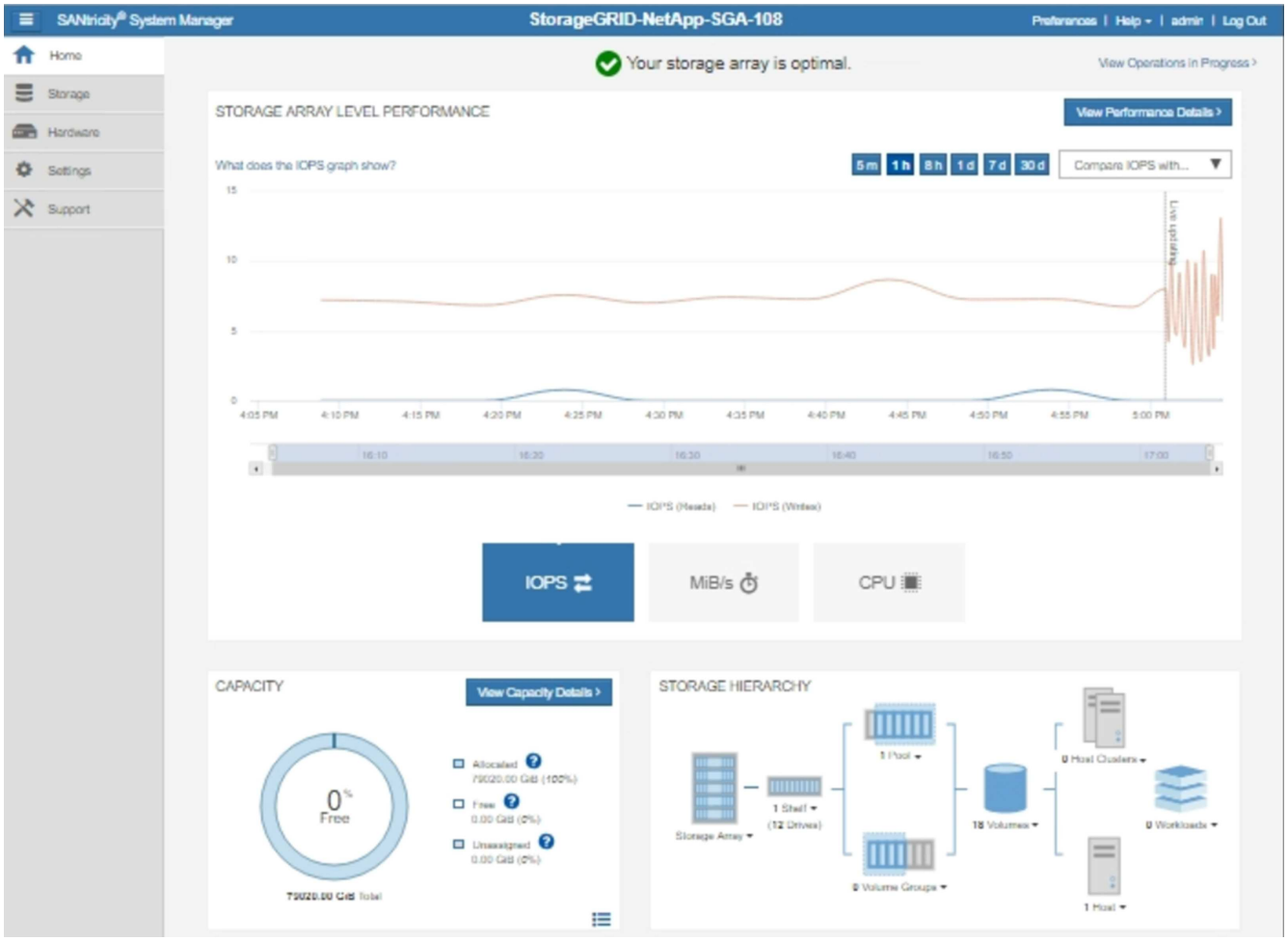
如果要在网格管理器中配置管理代理服务器，请参见 配置管理员代理设置。

> 此操作步骤 仅用于为 E 系列 AutoSupport 消息配置 StorageGRID 代理服务器。有关 E 系列 AutoSupport 配置的更多详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

步骤

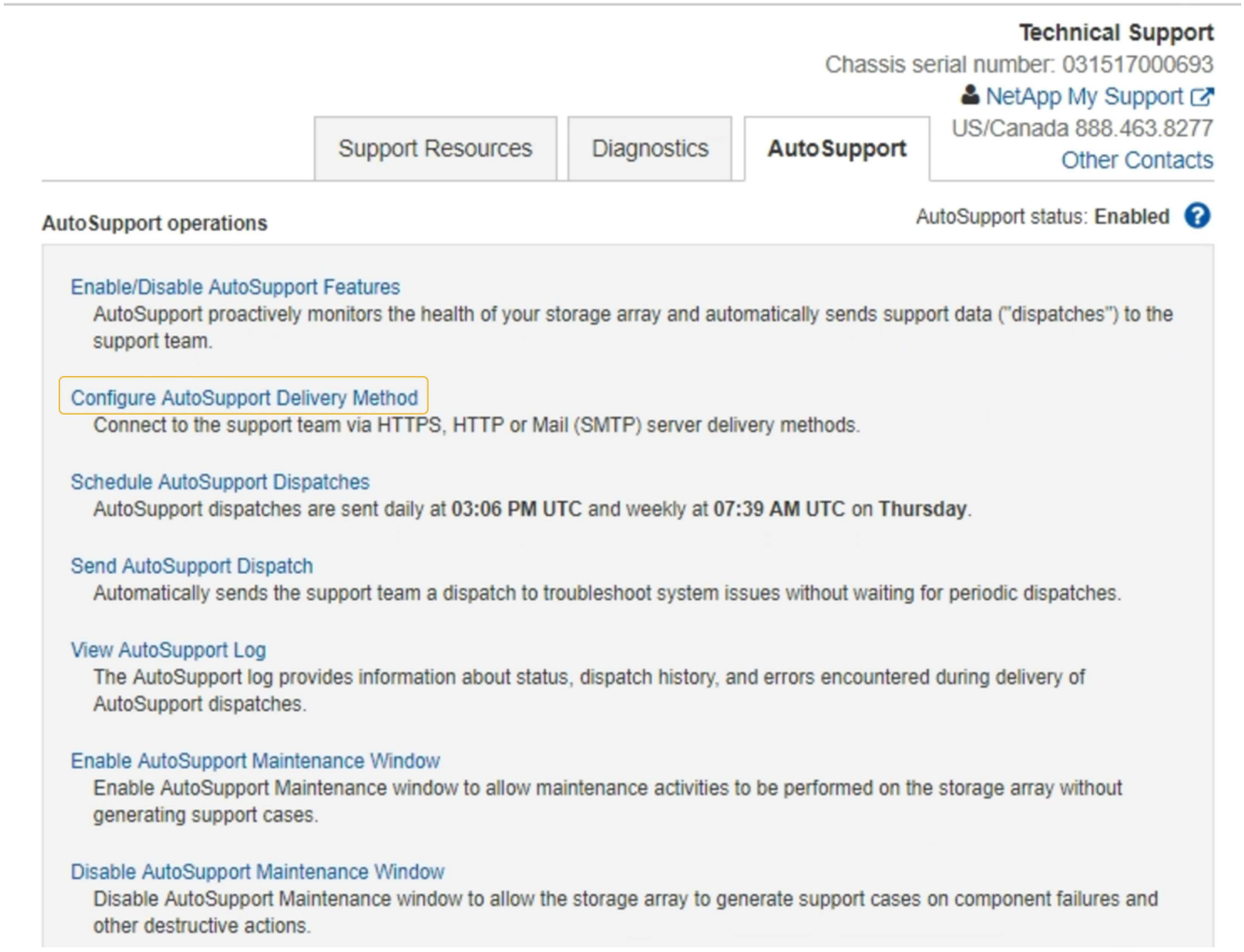
1. 在网格管理器中，选择 * 节点 * 。
2. 从左侧的节点列表中，选择要配置的存储设备节点。
3. 选择 * SANtricity 系统管理器 * 。

此时将显示 SANtricity System Manager 主页。



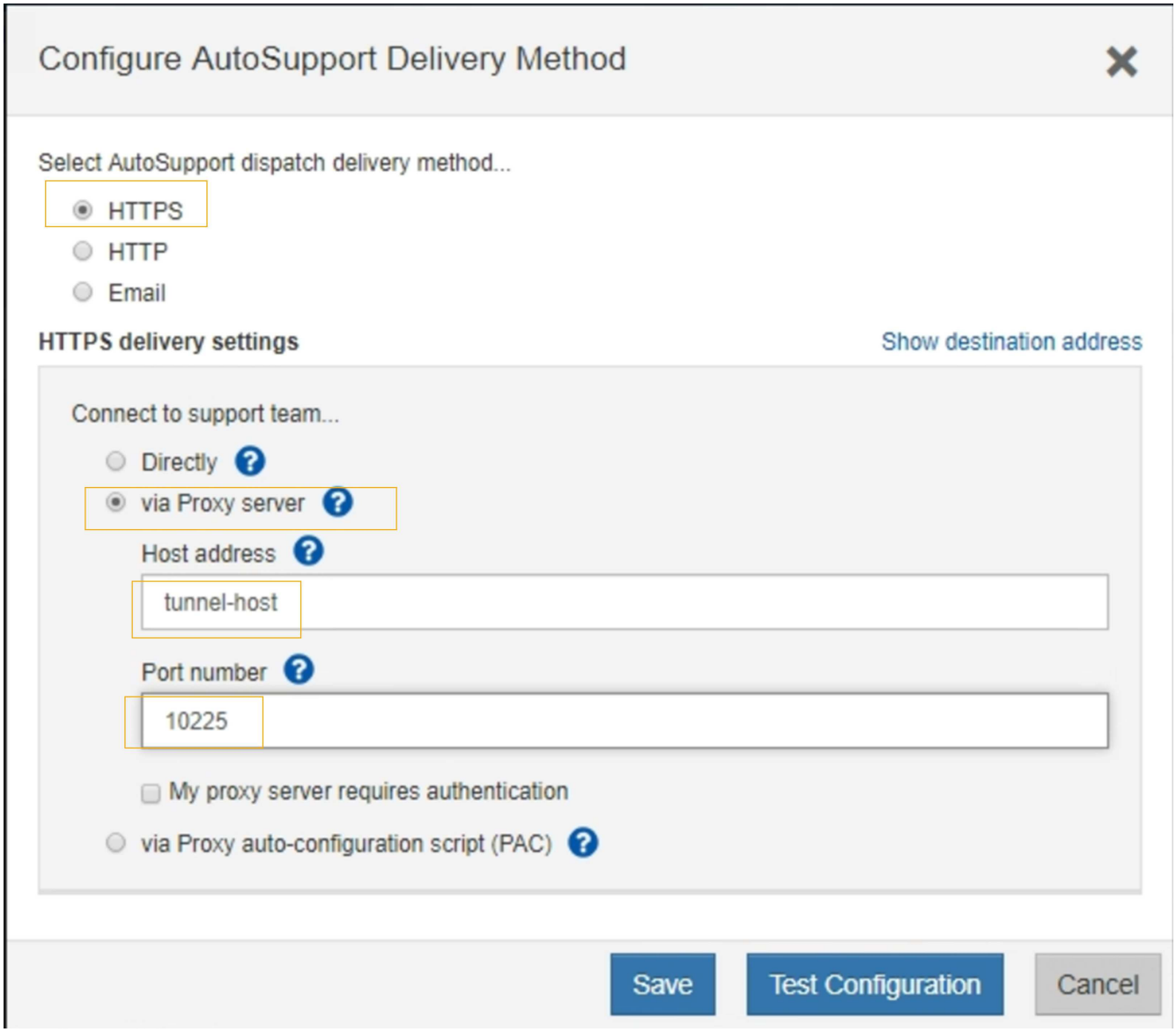
4. 选择 * 支持 * > * 支持中心 * > * AutoSupport * 。

   此时将显示 AutoSupport 操作页面。



5. 选择 * 配置 AutoSupport 交付方法 * 。

   此时将显示配置 AutoSupport 交付方法页面。



6. 选择 * HTTPS * 作为传送方法。

   启用 HTTPS 协议的证书已预先安装。

7. 选择 * 通过代理服务器 * 。
8. 输入 `tunnate-host` 作为 * 主机地址 * 。

   `tunnate-host` 是使用管理节点发送 E 系列 AutoSupport 消息的特殊地址。

9. 为 * 端口号 * 输入 `10225` 。

   `10225` 是 StorageGRID 代理服务器上从设备中的 E 系列控制器接收 AutoSupport 消息的端口号。

10. 选择 * 测试配置 * 以测试 AutoSupport 代理服务器的路由和配置。

    如果正确，则绿色横幅中会显示一条消息： "`您的 AutoSupport 配置已验证。` "

    如果测试失败，则会在红色横幅中显示一条错误消息。检查 StorageGRID DNS 设置和网络连接，确保首选

发件人管理节点可以连接到 NetApp 支持站点，然后重试此测试。

11. 选择 * 保存 * 。

此时将保存此配置，并显示一条确认消息： "`AutoSupport delivery method has been configured 。` "

管理存储节点

关于管理存储节点

存储节点可提供磁盘存储容量和服务。管理存储节点需要执行以下操作：

- 管理存储选项
- 了解什么是存储卷水印，以及如何使用水印覆盖来控制存储节点何时变为只读
- 监控和管理用于对象元数据的空间
- 为已存储对象配置全局设置
- 正在应用存储节点配置设置
- 管理完整存储节点

什么是存储节点？

存储节点可管理和存储对象数据和元数据。每个 StorageGRID 系统必须至少具有三个存储节点。如果您有多个站点，则 StorageGRID 系统中的每个站点也必须有三个存储节点。

存储节点包括在磁盘上存储，移动，验证和检索对象数据和元数据所需的服务和进程。您可以在 * 节点 * 页面上查看有关存储节点的详细信息。

什么是模数转换器服务？

管理域控制器（ ADC-A ）服务对网格节点及其彼此连接进行身份验证。一个站点的前三个存储节点中的每个存储节点都托管了此类模块转换服务。

此 ADA 服务可维护拓扑信息，包括服务的位置和可用性。当网格节点需要来自另一个网格节点的信息或由另一个网格节点执行操作时，它会联系一个模数转换器服务来查找处理其请求的最佳网格节点。此外，该 StorageGRID 服务还会保留一份部署配置包的副本，以便任何网格节点都可以检索当前配置信息。您可以在网格拓扑页面（ * 支持 * > * 网格拓扑 * ）上查看存储节点的数据转换信息。

为了便于分布式和孤岛式操作，每个 StorageGRID 服务会将证书，配置包以及有关服务和拓扑的信息与系统中的其他 ADE 服务进行同步。

通常，所有网格节点都会至少与一个 ADC 服务保持连接。这样可以确保网格节点始终访问最新信息。当网格节点连接时，它们会缓存其他网格节点的` 证书，从而使系统能够继续使用已知网格节点运行，即使某个模数转换器服务不可用也是如此。新的网格节点只能通过使用模数转换器服务建立连接。

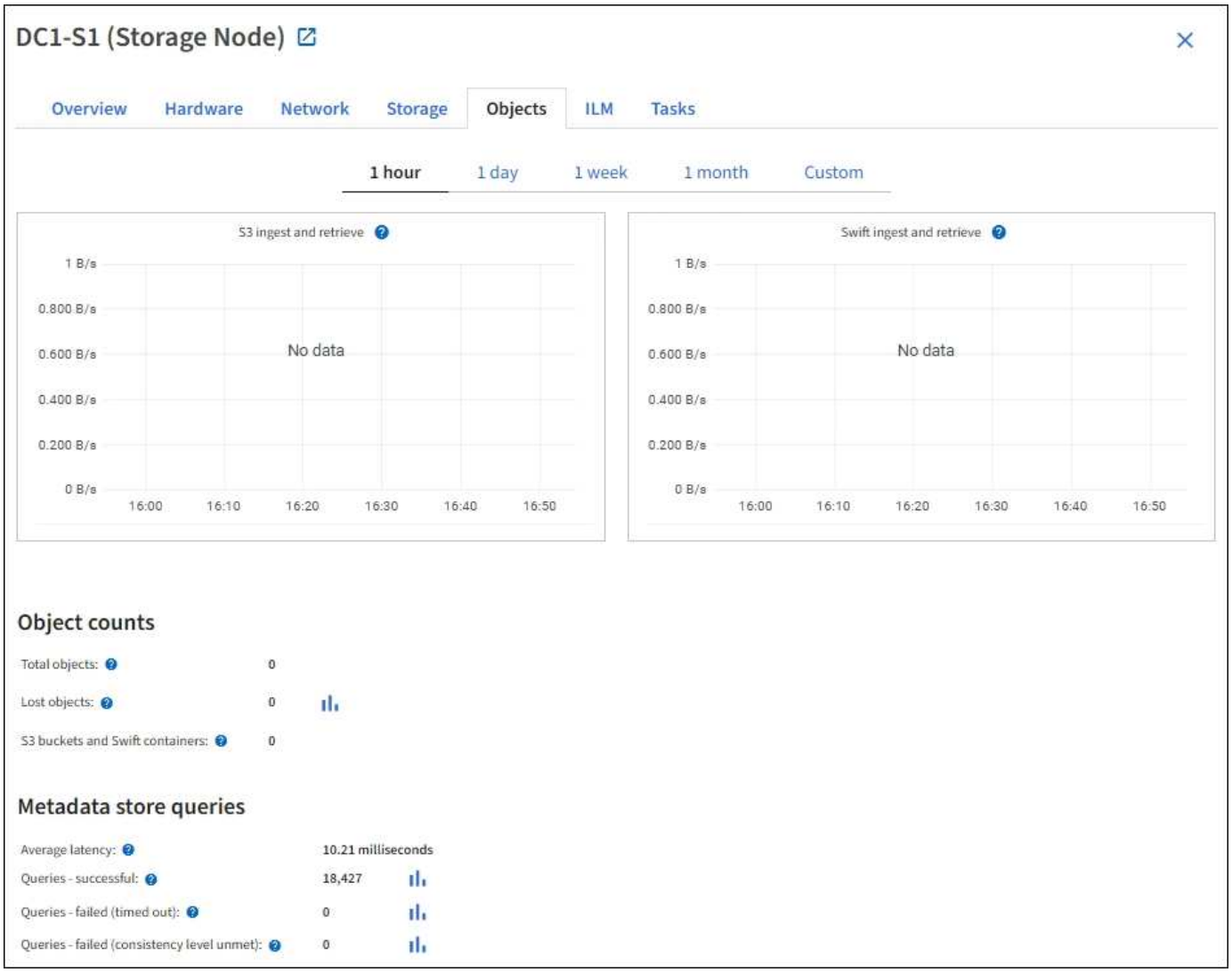
通过每个网格节点的连接，可以使此 ADA 服务收集拓扑信息。此网格节点信息包括 CPU 负载，可用磁盘空间（如果有存储），支持的服务以及网格节点的站点 ID 。其他服务则通过拓扑查询向此类服务请求拓扑信息。对于从 StorageGRID 系统收到的最新信息，此 ADA 服务会对每个查询做出响应。

分布式数据存储（ DDS ）服务由存储节点托管，它与 Cassandra 数据库建立接口，以便对存储在 StorageGRID 系统中的对象元数据执行后台任务。

对象计数

DDS 服务可跟踪载入到 StorageGRID 系统中的对象总数，以及通过每个系统支持的接口（ S3 或 Swift ）载入的对象总数。

您可以在任何存储节点的 "Nodes" 页面 >"Object" 选项卡上查看对象总数。



查询

您可以确定通过特定 DDS 服务对元数据存储运行查询所需的平均时间，成功查询的总数以及因问题描述 超时而失败的查询总数。

您可能希望查看查询信息以监控元数据存储 Cassandra 的运行状况，这会影响系统的载入和检索性能。例如，如果平均查询的延迟较慢，并且因超时而导致查询失败的次数较多，则元数据存储可能会遇到较高的负载或执行其他操作。

您还可以查看因一致性失败而失败的查询总数。通过特定 DDS 服务执行查询时，可用元数据存储数量不足，导致一致性级别失败。

您可以使用 " 诊断 " 页面获取网格当前状态的追加信息 。请参见 Run diagnostics。

一致性保证和控制

StorageGRID 保证新创建的对象的写入后读一致性。成功完成 PUT 操作后的任何 GET 操作都将能够读取新写入的数据。现有对象的覆盖，元数据更新和删除操作最终保持一致。

什么是 **LDR** 服务?

本地分发路由器（ LDR ）服务由每个存储节点托管，负责处理 StorageGRID 系统的内容传输。内容传输包含许多任务，包括数据存储，路由和请求处理。LDR 服务通过处理数据传输负载和数据流量功能来完成 StorageGRID 系统的大部分繁重工作。

LDR 服务可处理以下任务：

- 查询
- 信息生命周期管理（ ILM ）活动
- 对象删除
- 对象数据存储
- 从其他 LDR 服务（存储节点）传输对象数据
- 数据存储管理
- 协议接口（ S3 和 Swift ）

此外， LDR 服务还可管理 S3 和 Swift 对象到 StorageGRID 系统为每个载入对象分配的唯一 "`content handles` " （ UUID ）的映射。

查询

LDR 查询包括在检索和归档操作期间查询对象位置。您可以确定运行查询所需的平均时间，成功查询的总数以及因超时问题描述 而失败的查询总数。

您可以查看查询信息以监控元数据存储的运行状况，这会影响系统的载入和检索性能。例如，如果平均查询的延迟较慢，并且因超时而导致查询失败的次数较多，则元数据存储可能会遇到较高的负载或执行其他操作。

您还可以查看因一致性失败而失败的查询总数。通过特定 LDR 服务执行查询时，可用元数据存储数量不足会导致一致性级别失败。

您可以使用 " 诊断 " 页面获取网格当前状态的追加信息 。请参见 Run diagnostics。

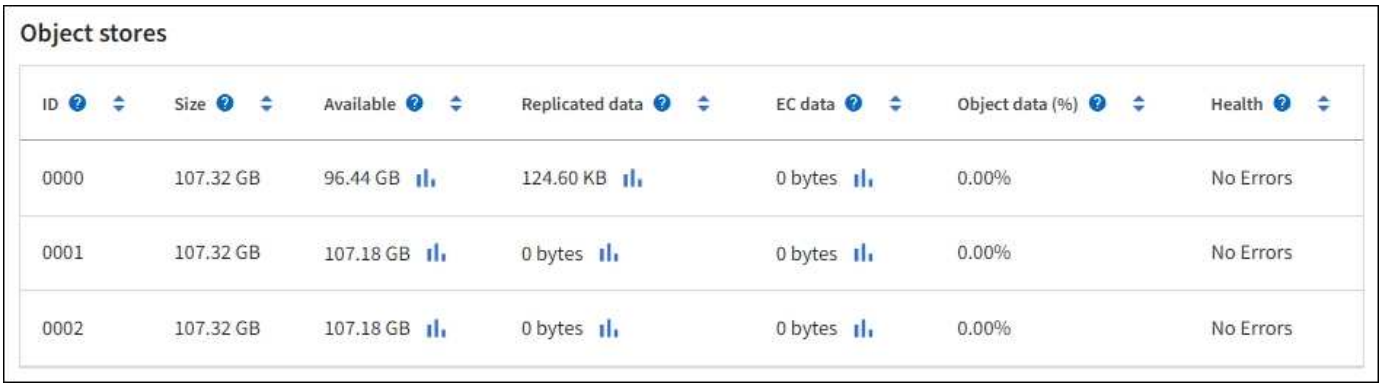
ILM 活动

通过信息生命周期管理（ ILM ）指标，您可以监控对象在实施 ILM 时的评估速率。您可以在信息板或 * 节点 * > * 存储节点 _* > * ILM * 上查看这些指标。

对象存储

LDR 服务的底层数据存储分为固定数量的对象存储（也称为存储卷）。每个对象存储都是一个单独的挂载点。

您可以在节点页面 > 存储选项卡上查看存储节点的对象存储。



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

存储在存储节点中的对象使用从 0000 到 002F 的十六进制数字进行标识，该数字称为卷 ID 。在第一个对象存储（卷 0 ）中预留空间用于 Cassandra 数据库中的对象元数据；该卷上的任何剩余空间用于对象数据。所有其他对象存储仅用于对象数据，其中包括复制的副本和经过纠删编码的片段。

为了确保复制的副本的空间使用量均匀，给定对象的对象数据会根据可用存储空间存储到一个对象存储中。当一个或多个对象存储填满容量时，其余对象存储将继续存储对象，直到存储节点上没有更多空间为止。

元数据保护

对象元数据是指与对象或对象的问题描述 相关的信息，例如对象修改时间或存储位置。StorageGRID 将对象元数据存储在与 LDR 服务连接的 Cassandra 数据库中。

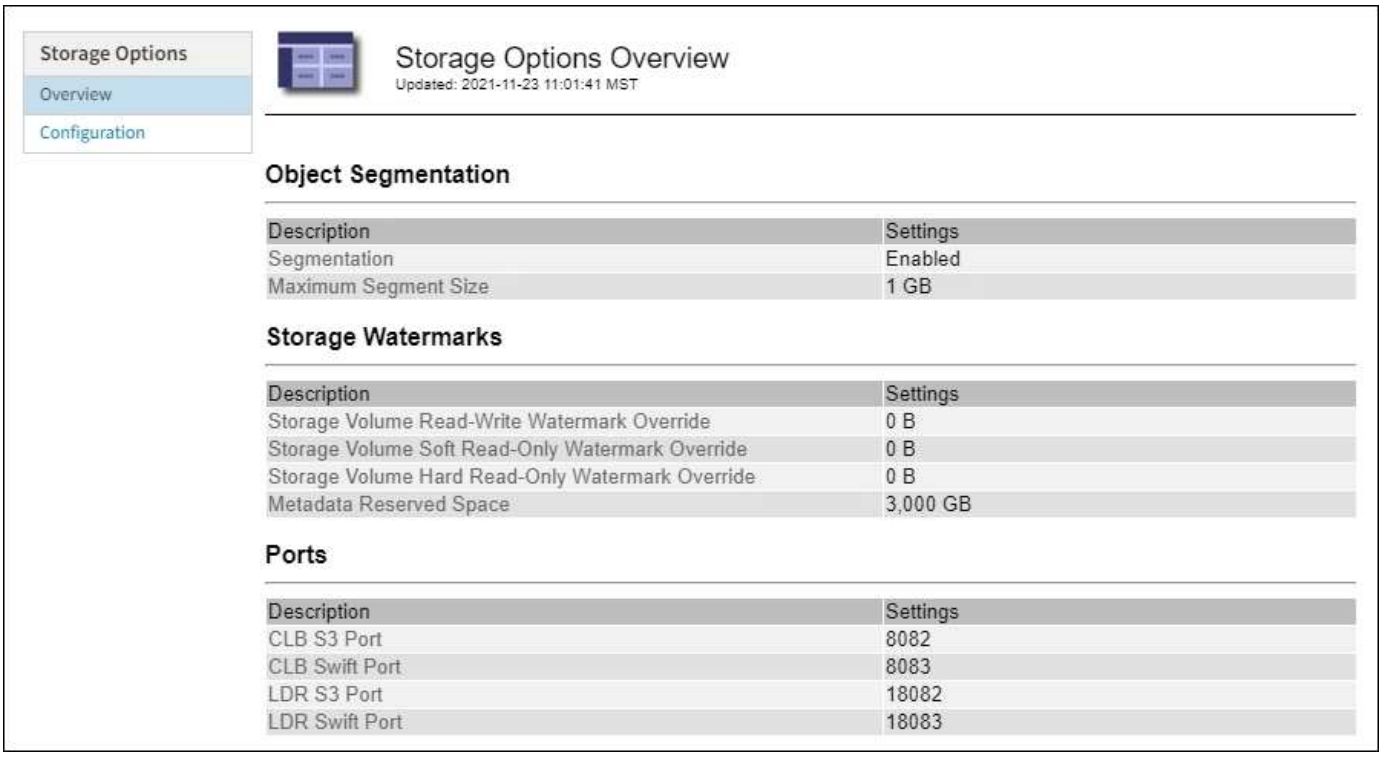
为了确保冗余并防止丢失，每个站点维护三个对象元数据副本。这些副本会均匀分布在每个站点的所有存储节点上。此复制不可配置，并且会自动执行。

管理对象元数据存储

管理存储选项

存储选项包括对象分段设置，存储卷水印的当前值以及元数据预留空间设置。您还可以查看网关节点上已弃用的 CLB 服务以及存储节点上的 LDR 服务使用的 S3 和 Swift 端口。

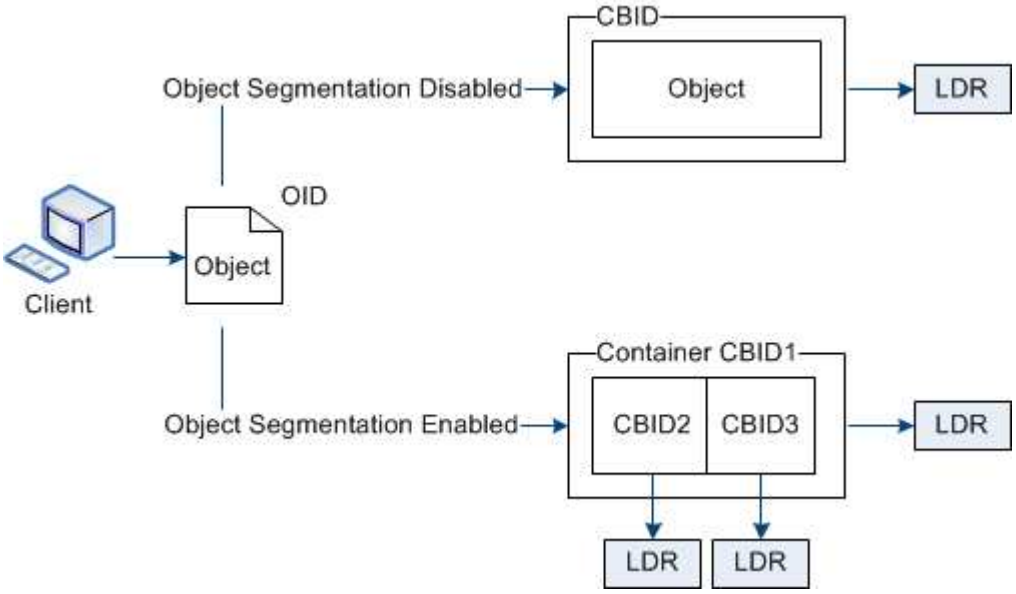
有关端口分配的信息，请参见 摘要：客户端连接的 IP 地址和端口。



什么是对象分段?

对象分段是指将对象拆分成一组固定大小的较小对象，以优化大型对象的存储和资源使用量的过程。S3 多部分上传还会创建分段对象，其中每个部分都有一个对象。

将对象载入 StorageGRID 系统后， LDR 服务会将该对象拆分为多个区块，并创建一个区块容器，其中会将所有区块的标题信息列为内容。



检索分段容器时， LDR 服务会从其分段中汇集原始对象并将该对象返回给客户端。

容器和分段不一定存储在同一个存储节点上。容器和分段可以存储在 ILM 规则中指定的存储池中的任何存储节点上。

StorageGRID 系统会单独处理每个区块，并计入受管对象和存储对象等属性的数量。例如，如果存储在 StorageGRID 系统中的对象拆分为两个区块，则在载入完成后，受管对象的值将增加三个，如下所示：

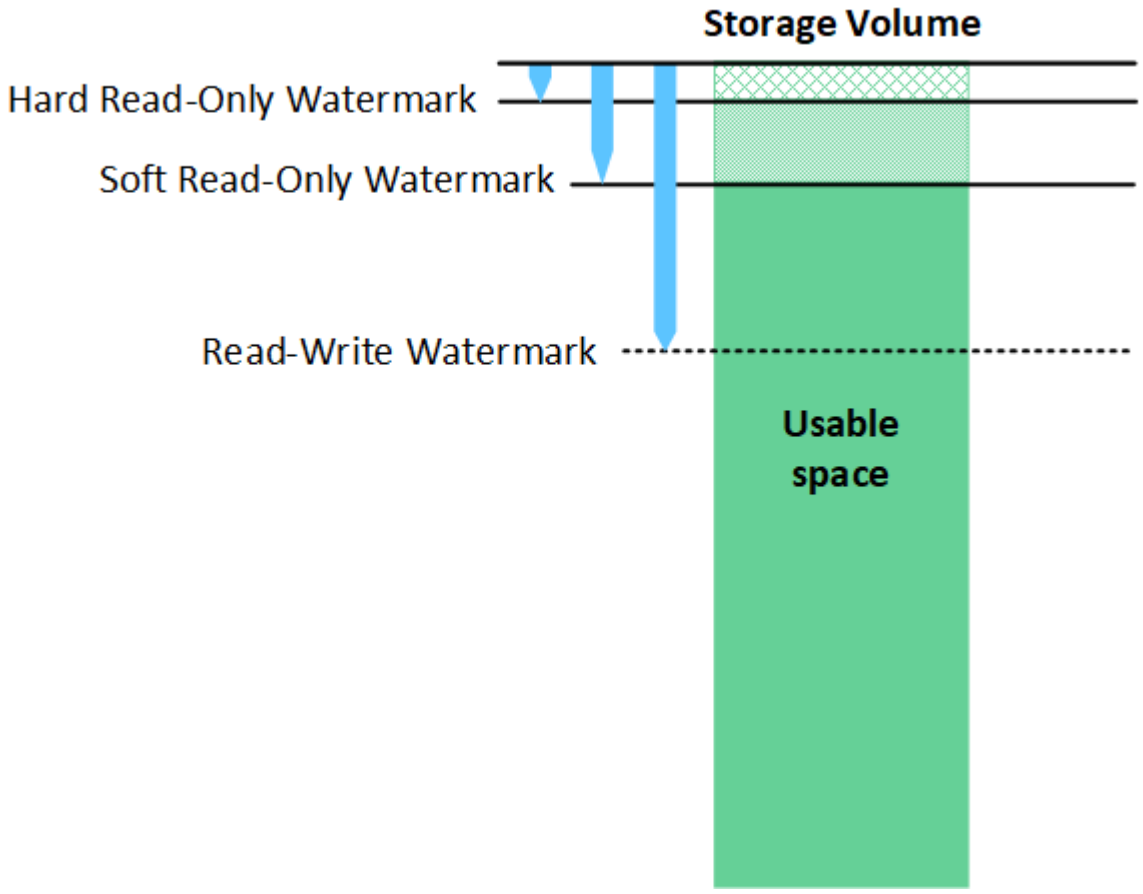
分段容器 + 分段 1 + 分段 2 = 三个已存储对象

您可以通过确保以下各项来提高处理大型对象时的性能：

- 每个网关和存储节点都有足够的网络带宽来满足所需的吞吐量。例如，在 10 Gbps 以太网接口上配置单独的网格网络和客户端网络。
- 已部署足够多的网关和存储节点以满足所需的吞吐量。
- 每个存储节点都具有足够的磁盘 IO 性能来满足所需的吞吐量。

什么是存储卷水印？

StorageGRID 使用三个存储卷水印来确保存储节点在空间严重不足之前安全地过渡到只读状态，并允许已过渡到只读状态的存储节点再次变为读写状态。



存储卷水印仅适用于用于复制和擦除编码对象数据的空间。要了解为卷 0 上的对象元数据预留的空间，请转至管理对象元数据存储。

什么是软只读水印？

第一个水印是 * 存储卷软只读水印 * ，用于指示存储节点用于对象数据的可用空间正在变满。

如果存储节点中的每个卷的可用空间小于该卷的软只读水印，则存储节点将过渡到 _read-only mode" 。只读模式表示存储节点向 StorageGRID 系统的其余部分公布只读服务，但满足所有待处理的写入请求。

例如，假设存储节点中的每个卷都有一个 10 GB 的软只读水印。一旦每个卷的可用空间小于 10 GB ，存储节点就会过渡到软只读模式。

什么是硬只读水印?

下一个水印是 * 存储卷硬只读水印 * ，用于指示节点的对象数据可用空间正在变满。

如果卷上的可用空间小于该卷的硬只读水印，则写入该卷将失败。但是，可以继续向其他卷写入数据，直到这些卷上的可用空间小于其硬只读水印为止。

例如，假设存储节点中的每个卷都有一个 5 GB 的硬只读水印。一旦每个卷的可用空间小于 5 GB ，存储节点就不再接受任何写入请求。

硬只读水印始终小于软只读水印。

什么是读写水印?

- 存储卷读写水印 * 仅适用于已过渡到只读模式的适用场景 存储节点。它可确定节点何时可以重新变为读写状态。如果存储节点中任一存储卷上的可用空间大于该卷的读写水印，则该节点会自动过渡回读写状态。

例如，假设存储节点已过渡到只读模式。另外，假设每个卷都有一个读写水印 30 GB 。任何卷的可用空间增加到 30 GB 后，节点将再次变为读写状态。

读写水印始终大于软只读水印和硬只读水印。

查看存储卷水印

您可以查看当前水印设置和系统优化的值。如果未使用优化的水印，您可以确定是否可以或应该调整设置。

您需要的内容

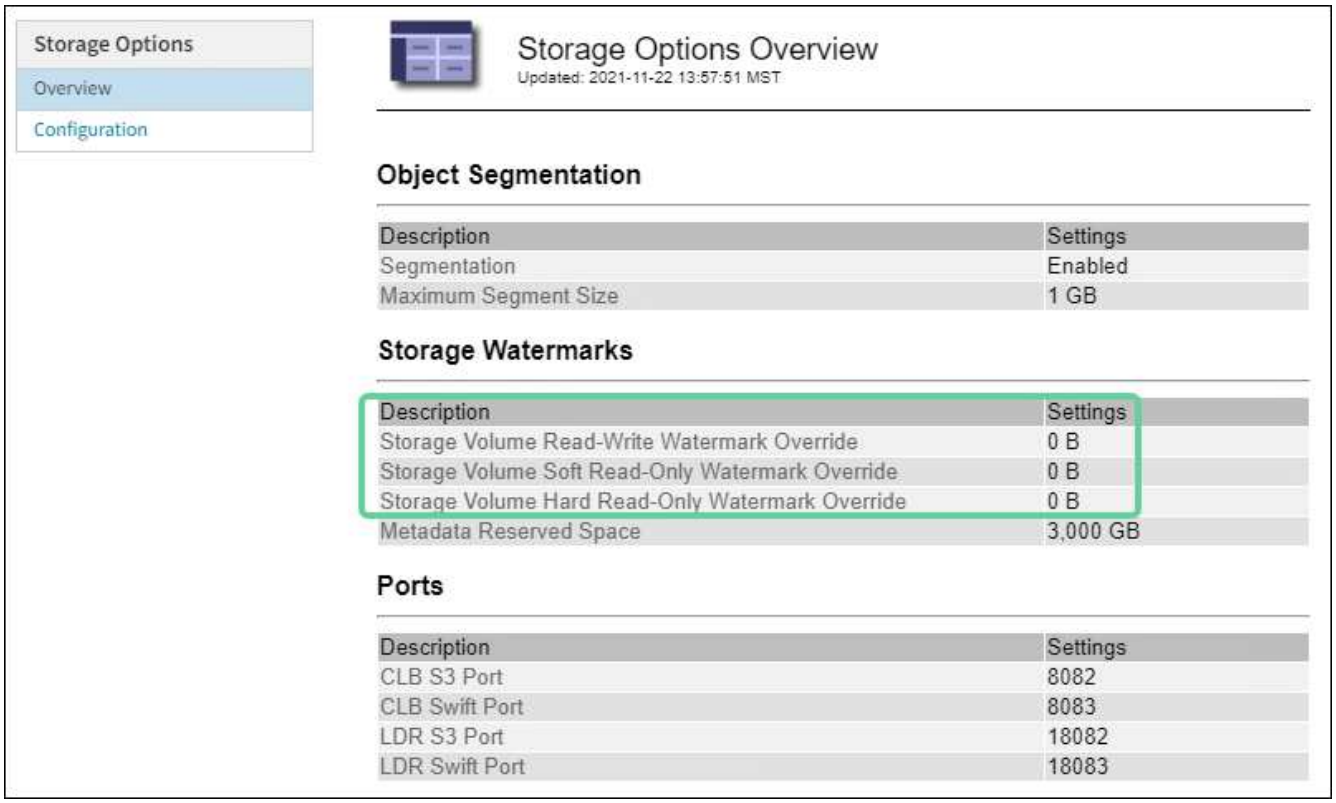
- 您已完成 StorageGRID 11.6 的升级。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。

查看当前水印设置

您可以在网格管理器中查看当前存储水印设置。

步骤

1. 选择 * 配置 * > * 系统 * > * 存储选项 * 。
2. 在存储水印部分中，查看三个存储卷水印覆盖的设置。



- 如果水印覆盖为 * 0 * ，则所有三个水印都会根据存储节点的大小和卷的相对容量针对每个存储节点上的每个存储卷进行优化。

  这是默认的建议设置。您不应更新这些值。根据需要，您可以选择 [查看优化的存储水印]。

- 如果水印覆盖值不是 0 ，则会使用自定义（非优化）水印。不建议使用自定义水印设置。按照说明进行操作 对低只读水印覆盖警报进行故障排除 以确定是否可以或应该调整设置。

查看优化的存储水印

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

1. 选择 * 支持 * > * 工具 * > * 指标 * 。
2. 在 Prometheus 部分中，选择用于访问 Prometheus 用户界面的链接。
3. 要查看建议的最小软只读水印，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegRid_storage_volume_minimum_optimized_soft_readonly_slogm
   ```

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

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

   ```
   storagegRid_storage_volume_max_optimized_soft_readonly_slogm
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

StorageGRID 系统的对象元数据容量用于控制可存储在该系统上的最大对象数。为了确保 StorageGRID 系统有足够的空间来存储新对象，您必须了解 StorageGRID 在何处以及如何存储对象元数据。

什么是对象元数据?

对象元数据是指描述对象的任何信息。StorageGRID 使用对象元数据跟踪网格中所有对象的位置，并管理每个对象的生命周期。

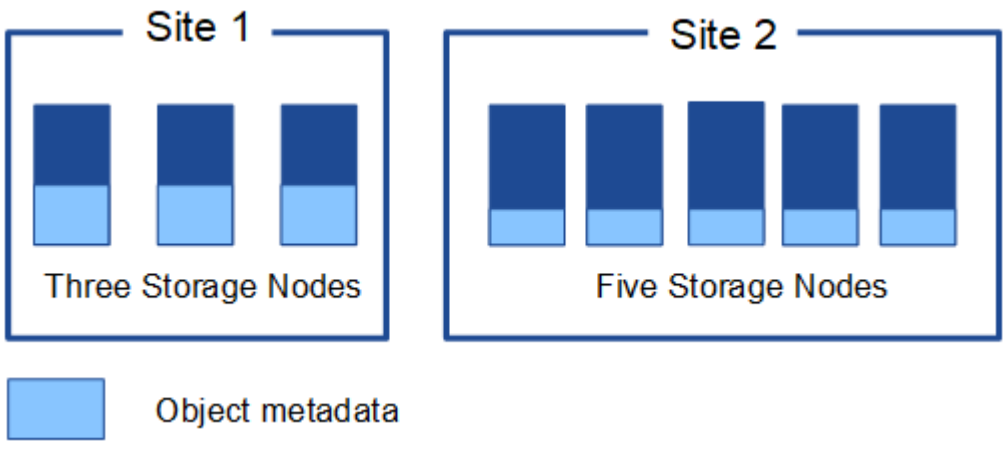
对于 StorageGRID 中的对象，对象元数据包括以下类型的信息：

- 系统元数据，包括每个对象的唯一 ID （ UUID ），对象名称， S3 存储分段或 Swift 容器的名称，租户帐户名称或 ID ，对象的逻辑大小，首次创建对象的日期和时间， 以及上次修改对象的日期和时间。
- 与对象关联的任何自定义用户元数据键值对。
- 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
- 对于复制的对象副本，为每个副本提供当前存储位置。
- 对于经过擦除编码的对象副本，为每个片段的当前存储位置。
- 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。
- 对于分段对象和多部分对象，分段标识符和数据大小。

如何存储对象元数据?

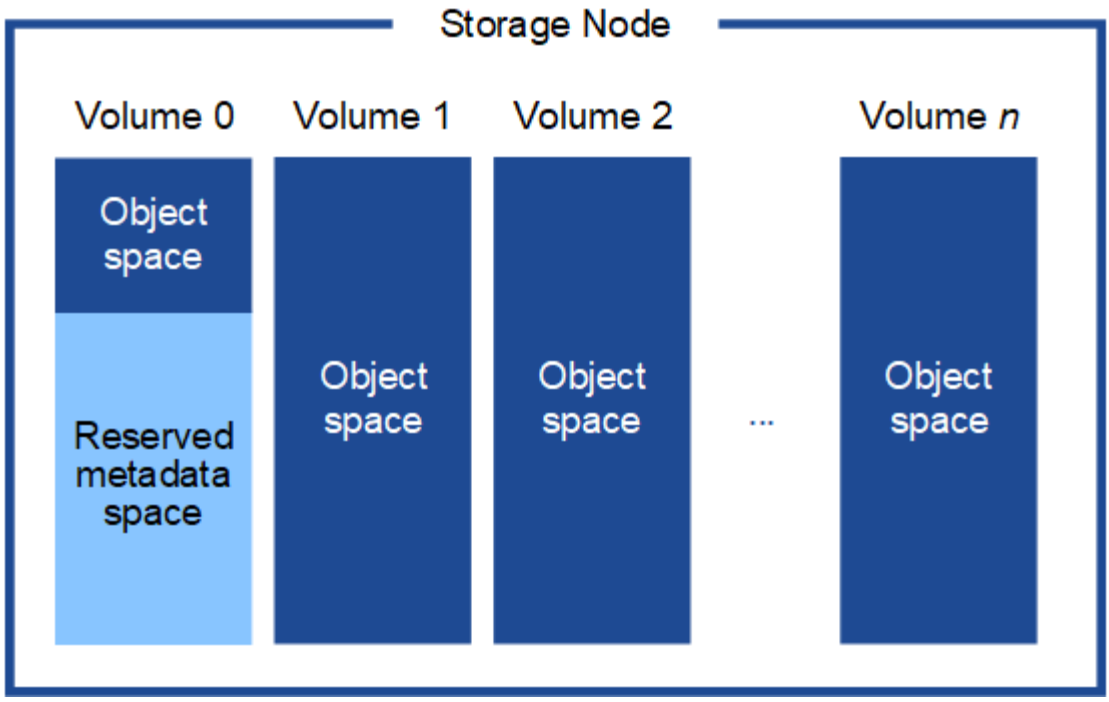
StorageGRID 在 Cassandra 数据库中维护对象元数据，该数据库独立于对象数据进行存储。为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。对象元数据的三个副本均匀分布在每个站点的所有存储节点上。

此图表示两个站点上的存储节点。每个站点都具有相同数量的对象元数据，这些元数据会在该站点的存储节点之间平均分布。



对象元数据存储在何处?

此图表示单个存储节点的存储卷。



如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。它会使用预留空间存储对象元数据并执行基本数据库操作。存储卷 0 和存储节点中所有其他存储卷上的任何剩余空间仅用于对象数据（复制的副本和经过纠删编码的片段）。

为特定存储节点上的对象元数据预留的空间量取决于多种因素，如下所述。

元数据预留空间设置

元数据预留空间 _ 是一个系统范围设置，表示将为每个存储节点的卷 0 上的元数据预留的空间量。如表所示， StorageGRID 11.6 的此设置的默认值如下所示：

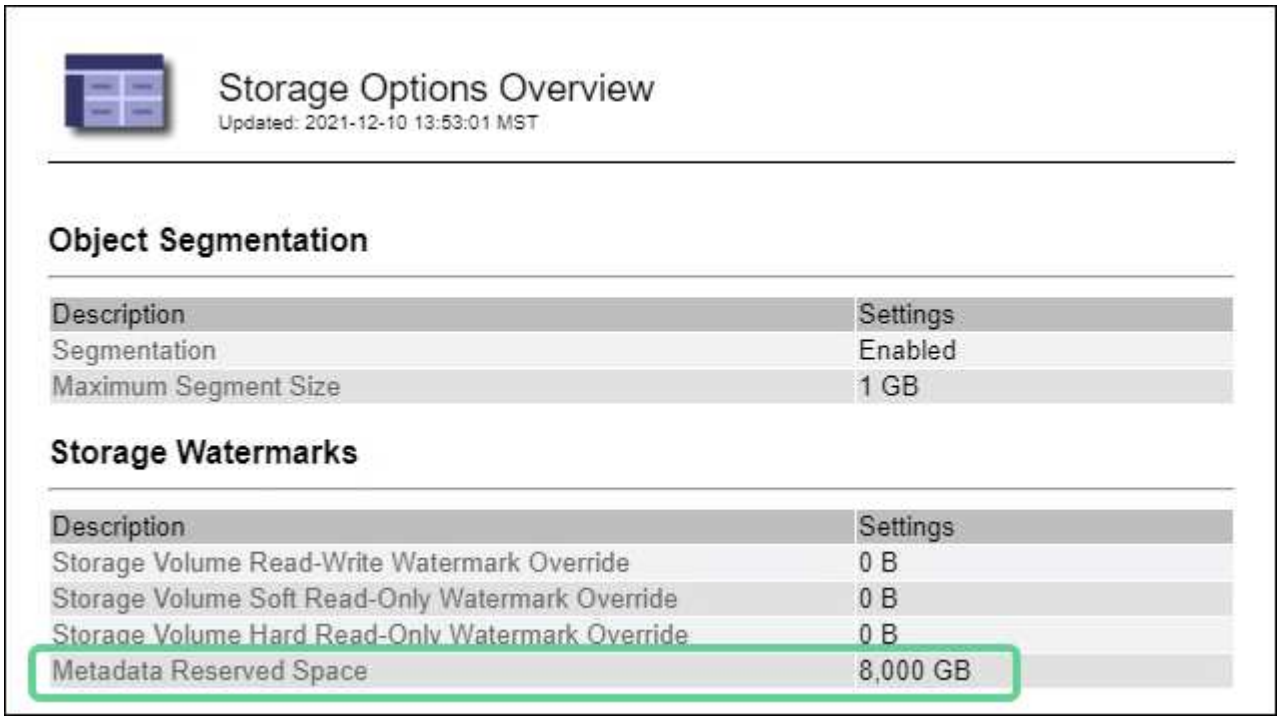
- 最初安装 StorageGRID 时使用的软件版本。
- 每个存储节点上的 RAM 量。

用于初始 **StorageGRID** 安装的版本	存储节点上的 **RAM** 量	**StorageGRID 11.6.** 的默认元数据预留空间设置
11.5/11.6.	网格中的每个存储节点上的容量为 128 GB 或更大	8 TB （ 8 ， 000 GB ）
	网格中任何存储节点上的容量小于 128 GB	3 TB （ 3 ， 000 GB ）
11.1 到 11.4	任何一个站点的每个存储节点上的容量为 128 GB 或更大	4 TB （ 4 ， 000 GB ）
	每个站点的任何存储节点上的容量小于 128 GB	3 TB （ 3 ， 000 GB ）

用于初始 **StorageGRID** 安装的版本	存储节点上的 **RAM** 量	**StorageGRID 11.6.** 的默认元数据预留空间设置
11.0 或更早版本	任意数量	2 TB （ 2 ， 000 GB ）

要查看 StorageGRID 系统的元数据预留空间设置，请执行以下操作：

1. 选择 * 配置 * > * 系统 * > * 存储选项 * 。
2. 在存储水印表中，找到 * 元数据预留空间 * 。



在屏幕截图中， * 元数据预留空间 * 值为 8 ， 000 GB （ 8 TB ）。这是新 StorageGRID 11.6 安装的默认设置，其中每个存储节点的 RAM 均为 128 GB 或以上。

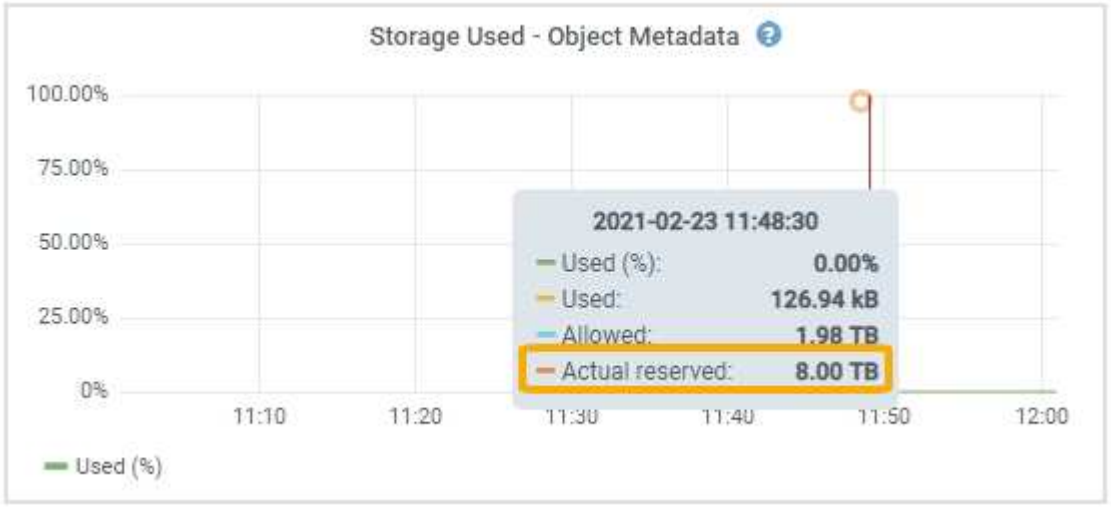
元数据的实际预留空间

与系统范围的元数据预留空间设置不同，系统会为每个存储节点确定对象元数据的 *actual reserved space* 。对于任何给定的存储节点，元数据的实际预留空间取决于节点的卷 0 大小以及系统范围的 * 元数据预留空间 * 设置。

节点的卷 **0** 大小	元数据的实际预留空间
小于 500 GB （非生产用）	卷 0 的 10%
500 GB 或更大	这些值中较小的值： • 卷 0 • 元数据预留空间设置

要查看特定存储节点上元数据的实际预留空间，请执行以下操作：

1. 在网格管理器中，选择 * 节点 * > * 存储节点 _* 。
2. 选择 * 存储 * 选项卡。
3. 将光标悬停在 "Storage Used - Object Metadata " 图表上，找到 "* 实际预留 * " 值。



在屏幕截图中， * 实际预留 * 值为 8 TB 。此屏幕截图适用于新 StorageGRID 11.6 安装中的大型存储节点。由于此存储节点的系统范围元数据预留空间设置小于卷 0 ，因此此节点的实际预留空间等于元数据预留空间设置。

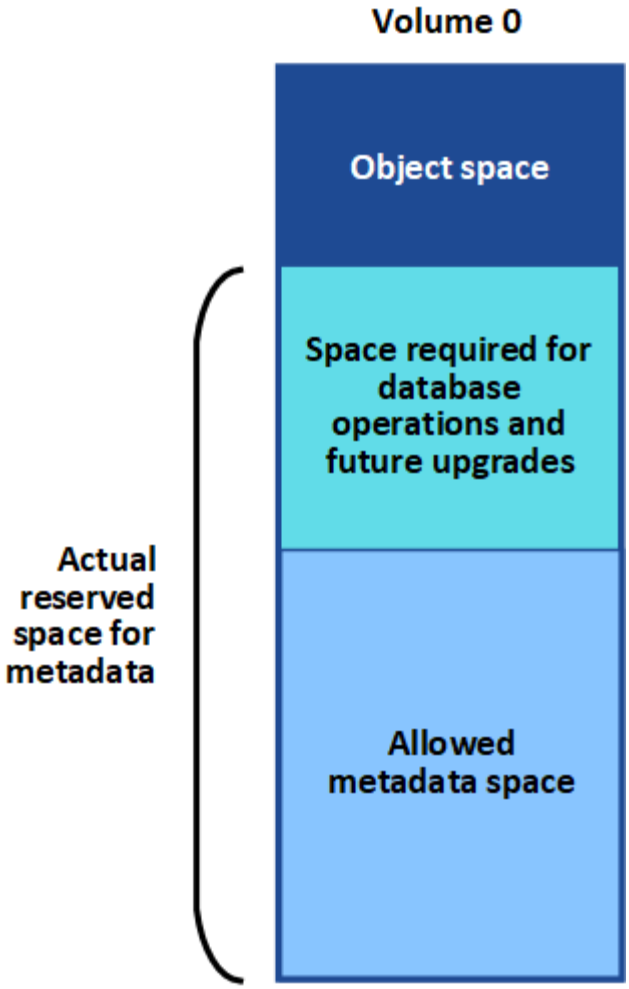
实际预留的元数据空间示例

假设您安装的是使用版本 11.6 的新 StorageGRID 系统。在此示例中，假设每个存储节点的 RAM 超过 128 GB ，并且存储节点 1 （ SN1 ）的卷 0 为 6 TB 。基于以下值：

- 系统范围的 * 元数据预留空间 * 设置为 8 TB 。（如果每个存储节点的 RAM 超过 128 GB ，则这是新 StorageGRID 11.6 安装的默认值。）
- SN1 元数据的实际预留空间为 6 TB 。（由于卷 0 小于 * 元数据预留空间 * 设置，因此会保留整个卷。）

允许的元数据空间

每个存储节点为元数据实际预留的空间细分为可用于对象元数据的空间（允许的元数据空间 _ ）以及基本数据库操作（如数据缩减和修复）以及未来硬件和软件升级所需的空间。允许的元数据空间用于控制整体对象容量。

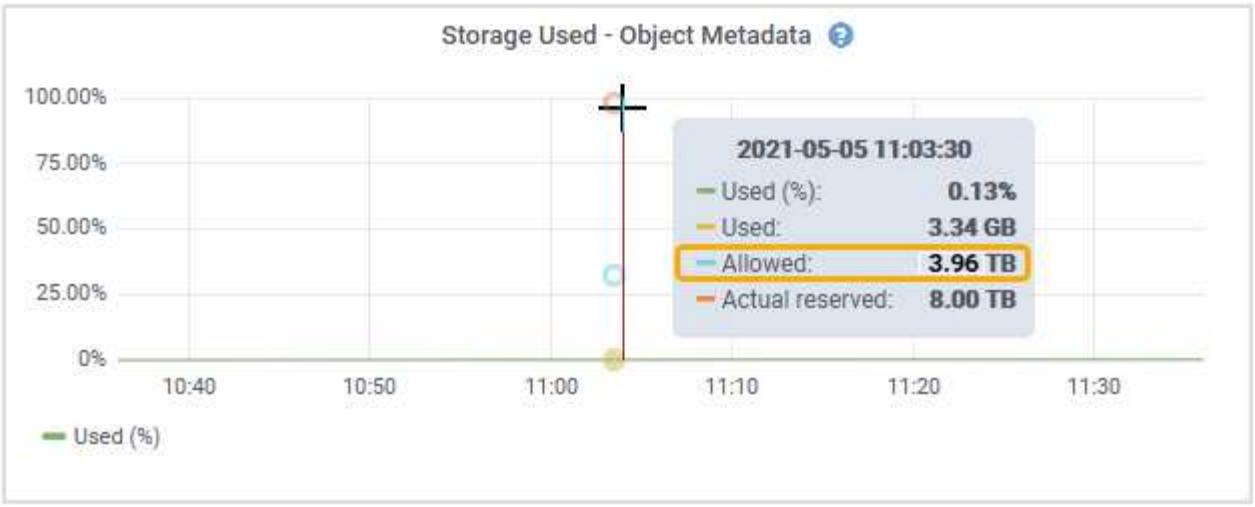


下表显示了StorageGRID 如何根据不同存储节点的内存量和元数据的实际预留空间计算不同存储节点的*允许元数据空间*。

		存储节点上的内存量	
	&lt； 128 GB	&gt； = 128 GB	元数据的实际预留空间
&lt； = 4 TB	元数据的实际预留空间的 60% ，最多 1.32 TB	元数据实际预留空间的 60% ，最大 1.98 TB	管理； 4 TB

要查看存储节点允许的元数据空间，请执行以下操作：

1. 在网格管理器中，选择 * 节点 * 。
2. 选择存储节点。
3. 选择 * 存储 * 选项卡。
4. 将光标悬停在已用存储 - 对象元数据图表上，找到 * 允许 * 值。



在屏幕截图中、*允许*值为3.96 TB、这是存储节点的最大值、该存储节点的元数据实际预留空间超过4 TB。

- 允许 * 值对应于此 Prometheus 指标：

```
storagegRid_storage_utilization metadata_allowed_bytes
```

允许的元数据空间示例

假设您安装的是使用版本 11.6 的 StorageGRID 系统。在此示例中，假设每个存储节点的 RAM 超过 128 GB ，并且存储节点 1 （ SN1 ）的卷 0 为 6 TB 。基于以下值：

- 系统范围的 * 元数据预留空间 * 设置为 8 TB 。（当每个存储节点的 RAM 超过 128 GB 时，这是 StorageGRID 11.6 的默认值。）
- SN1 元数据的实际预留空间为 6 TB 。（由于卷 0 小于 * 元数据预留空间 * 设置，因此会保留整个卷。）
- 根据中所示的计算、SN1上的元数据允许的空间为3 TB 元数据允许的空间表：(元数据的实际预留空间−1 TB)×60%、最多3.96 TB。

不同大小的存储节点如何影响对象容量

如上所述， StorageGRID 会在每个站点的存储节点之间均匀分布对象元数据。因此，如果某个站点包含不同大小的存储节点，则该站点上最小的节点将决定该站点的元数据容量。

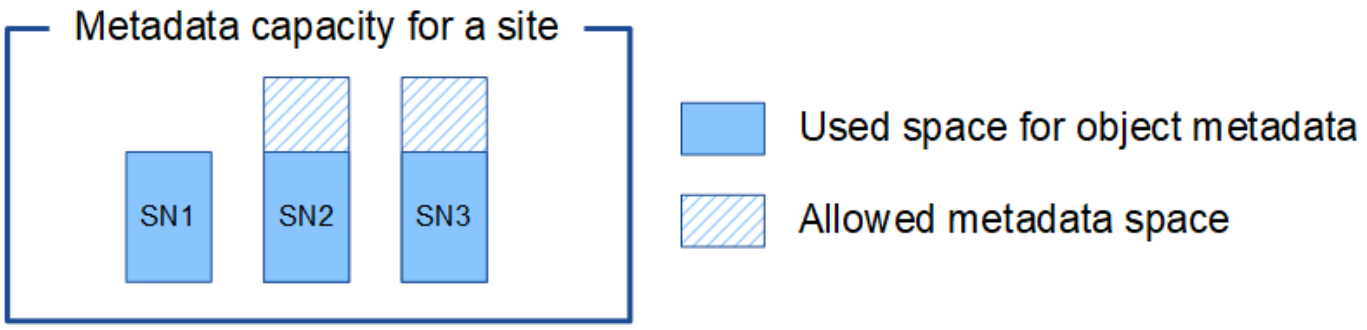
请考虑以下示例：

- 您有一个单站点网格，其中包含三个大小不同的存储节点。
- * 元数据预留空间 * 设置为 4 TB 。
- 对于实际预留的元数据空间和允许的元数据空间，存储节点具有以下值。

存储节点	卷 **0** 的大小	实际预留的元数据空间	允许的元数据空间
SN1	2.2 TB	2.2 TB	1.32 TB

存储节点	卷 **0** 的大小	实际预留的元数据空间	允许的元数据空间
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

由于对象元数据在站点的存储节点之间平均分布，因此本示例中的每个节点只能持有 1.32 TB 的元数据。不能使用 SN2 和 SN3 允许的额外 0.66 TB 元数据空间。



同样，由于 StorageGRID 会维护每个站点上 StorageGRID 系统的所有对象元数据，因此 StorageGRID 系统的整体元数据容量取决于最小站点的对象元数据容量。

由于对象元数据容量控制最大对象数，因此当一个节点用尽元数据容量时，网格实际上已满。

相关信息

- 要了解如何监控每个存储节点的对象元数据容量，请转至 监控和故障排除。
- 要增加系统的对象元数据容量，请添加新的存储节点。转至 扩展网格。

配置已存储对象的全局设置

配置存储的对象压缩

您可以使用 " 压缩存储的对象 " 网格选项减小 StorageGRID 中存储的对象的大小，从而减少对象占用的存储。

您需要的内容

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

关于此任务

默认情况下， " 压缩存储的对象 " 网格选项处于禁用状态。如果启用此选项，则 StorageGRID 会在保存每个对象时尝试使用无损压缩对其进行压缩。

> 如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

启用此选项之前，请注意以下事项：

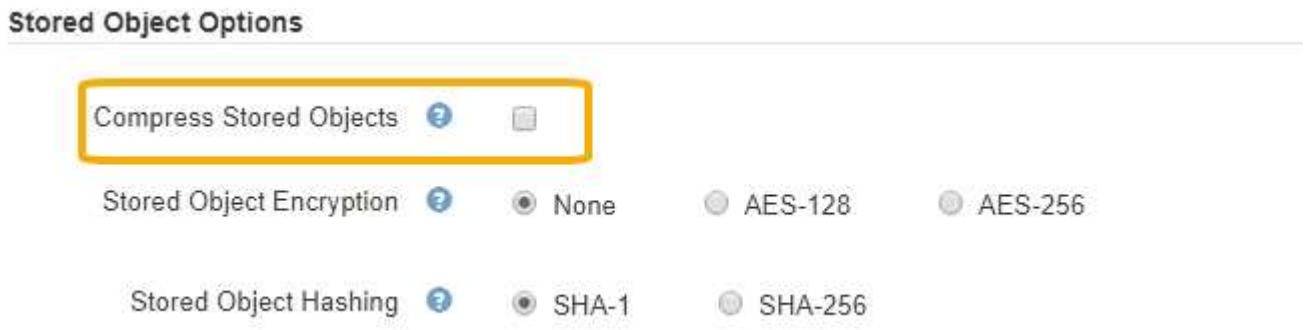
- 除非您知道要存储的数据是可压缩的，否则不应启用数据压缩。
- 将对象保存到 StorageGRID 的应用程序可能会在保存对象之前对其进行压缩。如果客户端应用程序在将对象保存到 StorageGRID 之前已对其进行了压缩，则启用压缩存储的对象不会进一步减小对象的大小。
- 如果将 NetApp FabricPool 与 StorageGRID 结合使用，请勿启用数据压缩。
- 如果启用了 " 压缩存储的对象 " 网格选项，则 S3 和 Swift 客户端应用程序应避免执行指定要返回的字节数范围的 GET 对象操作。这些 "`range read` " 操作效率低下，因为 StorageGRID 必须有效解压缩对象以访问请求的字节。从非常大的对象请求少量字节的获取对象操作效率尤其低下；例如，从 50 GB 压缩对象读取 10 MB 范围的操作效率低下。

  如果从压缩对象读取范围，则客户端请求可能会超时。

> 如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

步骤

1. 选择 * 配置 * > * 系统 * > * 网格选项 * 。
2. 在存储的对象选项部分中，选中 * 压缩存储的对象 * 复选框。



3. 选择 * 保存 * 。

配置存储的对象加密

如果要确保在对象存储受到影响时无法以可读形式检索数据，则可以对存储的对象进行加密。默认情况下，对象不会加密。

您需要的内容

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

关于此任务

存储的对象加密可对通过 S3 或 Swift 载入的所有对象数据进行加密。启用此设置后，所有新载入的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密，则当前加密的对象将保持加密状态，但新载入的对象不会加密。

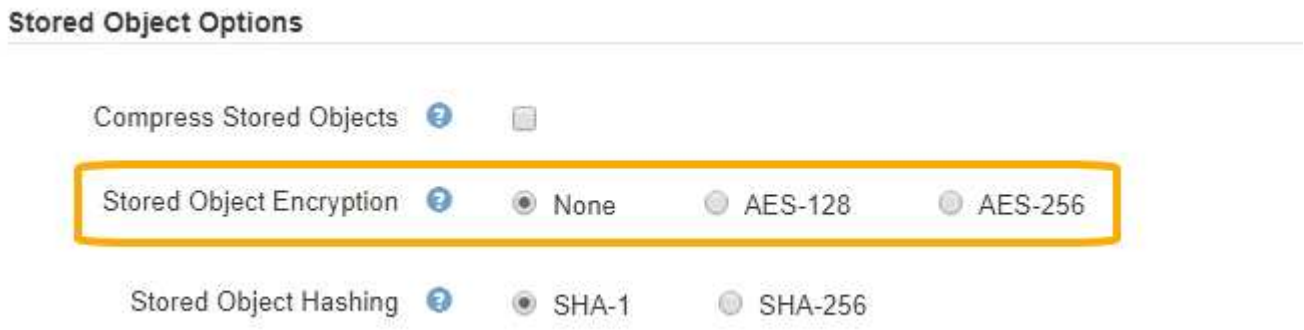
> 如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

存储的对象可以使用 AES - 128 或 AES - 256 加密算法进行加密。

存储对象加密设置仅适用于尚未通过存储分段级别或对象级别加密进行加密的 S3 对象。

步骤

1. 选择 * 配置 * > * 系统 * > * 网格选项 * 。
2. 在存储的对象选项部分中，将存储的对象加密更改为 * 无 * （默认）， * AES-128* 或 * AES-256* 。



3. 选择 * 保存 * 。

配置存储的对象哈希

存储对象哈希选项指定用于验证对象完整性的哈希算法。

您需要的内容

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

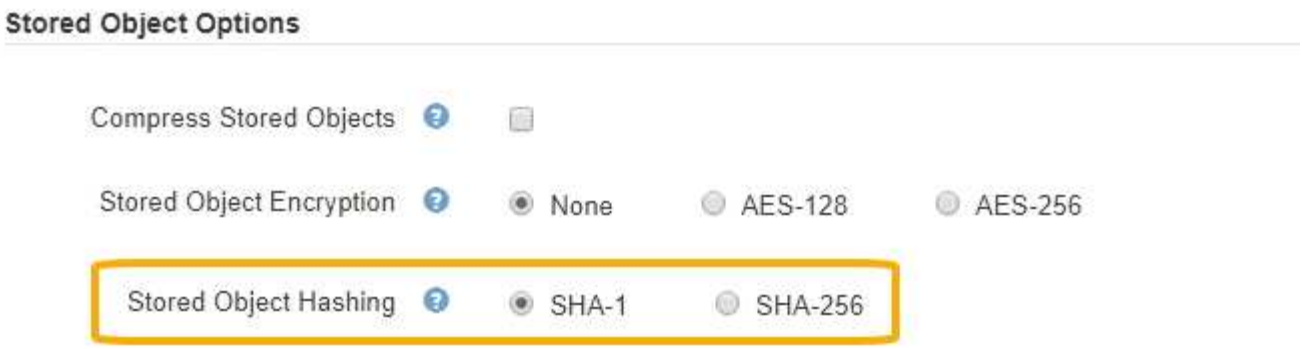
关于此任务

默认情况下，对象数据使用 SHA-1 算法进行哈希。SHA-256 算法需要额外的 CPU 资源，通常不建议用于完整性验证。

如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

步骤

1. 选择 * 配置 * > * 系统 * > * 网格选项 * 。
2. 在存储的对象选项部分中，将存储的对象哈希更改为 * SHA-1* （默认）或 * SHA-256* 。



3. 选择 * 保存 * 。

存储节点配置设置

每个存储节点都使用许多配置设置和计数器。您可能需要查看当前设置或重置计数器才能清除警报（旧系统）。

除非文档中有明确说明，否则在修改任何存储节点配置设置之前，应咨询技术支持。您可以根据需要重置事件计数器以清除原有警报。

要访问存储节点的配置设置和计数器，请执行以下操作：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* 。
3. 展开存储节点并选择服务或组件。
4. 选择 * 配置 * 选项卡。

下表汇总了存储节点配置设置。

LDR

属性名称	代码	Description
HTTP 状态	HSTE	S3 ， Swift 和其他内部 StorageGRID 流量的 HTTP 协议的当前状态： • 脱机：不允许执行任何操作，任何尝试打开与 LDR 服务的 HTTP 会话的客户端应用程序都会收到错误消息。活动会话正常关闭。 • 联机：操作继续正常

属性名称	代码	Description
自动启动 HTTP	HTA	• 如果选择此选项，则重新启动时系统的状态取决于 * LDR* > * 存储 * 组件的状态。如果重新启动时 * LDR* > * 存储 * 组件为只读，则 HTTP 接口也为只读。如果 * LDR* > * 存储 * 组件为联机，则 HTTP 也为联机。否则， HTTP 接口将保持脱机状态。 • 如果未选中，则 HTTP 接口将保持脱机状态，直到显式启用为止。

LDR > 数据存储

属性名称	代码	Description
重置丢失的对象计数	RCOR	重置此服务中丢失的对象数量的计数器。

LDR > 存储

属性名称	代码	Description
存储状态—所需	SSD	用户可配置的存储组件所需状态设置。LDR 服务将读取此值并尝试与此属性指示的状态匹配。此值在重新启动后保持不变。 例如，您可以使用此设置强制存储成为只读存储，即使有足够的可用存储空间也是如此。这对于故障排除非常有用。 属性可以采用以下值之一： • 脱机：当所需状态为脱机时， LDR 服务会使 * LDR* > * 存储 * 组件脱机。 • 只读：当所需状态为只读时， LDR 服务会将存储状态移至只读状态并停止接受新内容。请注意，内容可能会继续短时间保存到存储节点中，直到打开的会话关闭为止。 • 联机：在正常系统操作期间，将此值保留为联机。存储状态—存储组件的当前状态将由服务根据 LDR 服务的状况（例如可用对象存储空间量）动态设置。如果空间不足，则组件将变为只读。
运行状况检查超时	SHCT	运行状况检查测试必须完成才能将存储卷视为运行状况良好的时间限制（以秒为单位）。只有在支持部门要求更改此值时，才更改此值。

LDR > 验证

属性名称	代码	Description
重置缺少的对象计数	VNMI	重置检测到的缺失对象数（ Oomis ）。请仅在对象存在检查完成后使用。StorageGRID 系统会自动还原缺少的复制对象数据。
验证率	VPRI.	设置进行后台验证的速率。请参见有关配置后台验证速率的信息。
重置损坏对象计数	VCCR	重置在后台验证期间发现的已复制对象数据损坏的计数器。此选项可用于清除检测到损坏的对象（ OCOR ）警报条件。有关详细信息，请参见 StorageGRID 监控和故障排除说明。
删除隔离的对象	OQRT	从隔离目录中删除损坏的对象，将隔离对象的计数重置为零，然后清除检测到的隔离对象（ OQRT ）警报。在 StorageGRID 系统自动还原损坏的对象后，将使用此选项。 如果触发对象丢失警报，技术支持可能希望访问隔离的对象。在某些情况下，隔离的对象对于数据恢复或调试导致对象副本损坏的底层问题可能很有用。

LDR > 擦除编码

属性名称	代码	Description
重置写入失败计数	RSWF	将擦除编码对象数据写入失败时的计数器重置到存储节点。
重置读取失败计数	RSRF	重置从存储节点读取经过纠删编码的对象数据失败的计数器。
重置删除失败计数	RSDF	重置从存储节点删除经过纠删编码的对象数据失败的计数器。
重置检测到的损坏副本计数	RSCC	重置存储节点上经过纠删编码的对象数据的损坏副本数计数器。
重置检测到的损坏片段计数	RSCD	重置存储节点上擦除编码对象数据损坏片段的计数器。
重置检测到的缺失片段计数	R贴 片式	重置存储节点上缺少纠删编码对象数据片段的计数器。请仅在对象存在检查完成后使用。

LDR > 复制

属性名称	代码	Description
重置入站复制失败计数	RICR	重置入站复制失败的计数器。此操作可用于清除 RIRF （入站复制 - 失败）警报。
重置出站复制失败计数	ROCR	重置出站复制失败的计数器。此操作可用于清除 RORF （出站复制 - 失败）警报。
禁用入站复制	DSIR	选择此项可在维护或测试操作步骤 过程中禁用入站复制。在正常操作期间保持未选中状态。 禁用入站复制后，可以从存储节点检索对象以复制到 StorageGRID 系统中的其他位置，但不能从其他位置将对象复制到此存储节点： LDR 服务为只读服务。
禁用出站复制	DSOR	选择此选项可在维护或测试操作步骤 过程中禁用出站复制（包括 HTTP 检索的内容请求）。在正常操作期间保持未选中状态。 禁用出站复制后，可以将对象复制到此存储节点，但无法从存储节点检索对象以复制到 StorageGRID 系统中的其他位置。LDR 服务为只写服务。

相关信息

监控和故障排除

管理完整存储节点

当存储节点达到容量时，您必须通过添加新存储来扩展 StorageGRID 系统。有三种选项可供选择：添加存储卷，添加存储扩展架和添加存储节点。

添加存储卷

每个存储节点均支持最大数量的存储卷。定义的最大值因平台而异。如果存储节点包含的存储卷数少于最大数量，则可以添加卷以增加其容量。请参见的说明 扩展 StorageGRID 系统。

添加存储扩展架

某些 StorageGRID 设备存储节点（例如 SG6060 ）可以支持更多存储架。如果您的 StorageGRID 设备具有扩展功能，但尚未扩展到最大容量，则可以添加存储架以增加容量。请参见的说明 扩展 StorageGRID 系统。

添加存储节点

您可以通过添加存储节点来增加存储容量。添加存储时，必须仔细考虑当前活动的 ILM 规则和容量要求。请参见的说明 扩展 StorageGRID 系统。

管理管理节点

什么是管理节点

管理节点可提供系统配置，监控和日志记录等管理服务。每个网格都必须有一个主管理节点，并且可能有任意数量的非主管理节点，以实现冗余。

登录到网格管理器或租户管理器时，您正在连接到管理节点。您可以连接到任何管理节点，每个管理节点都会显示一个类似的 StorageGRID 系统视图。但是，必须使用主管理节点执行维护过程。

管理节点还可用于对 S3 和 Swift 客户端流量进行负载平衡。

管理节点托管以下服务：

- AMS 服务
- CMN 服务
- NMS 服务
- Prometheus 服务
- 负载平衡器和高可用性服务（用于支持 S3 和 Swift 客户端流量）

管理节点还支持管理应用程序程序接口（ Management Application Program Interface ， mgmt-API ）处理来自网格管理 API 和租户管理 API 的请求。请参见 使用网格管理 API。

什么是 **AMS** 服务

审核管理系统（ Audit Management System ， AMS ）服务可跟踪系统活动和事件。

什么是 **CMN** 服务

配置管理节点（ CMN ）服务负责管理所有服务所需的连接和协议功能的系统范围配置。此外， CMN 服务还用于运行和监控网格任务。每个 StorageGRID 部署只有一个 CMN 服务。托管 CMN 服务的管理节点称为主管理节点。

什么是 **NMS** 服务

网络管理系统（ Network Management System ， NMS ）服务为通过网格管理器（ StorageGRID 系统基于浏览器的界面）显示的监控，报告和配置选项提供支持。

什么是 **Prometheus** 服务

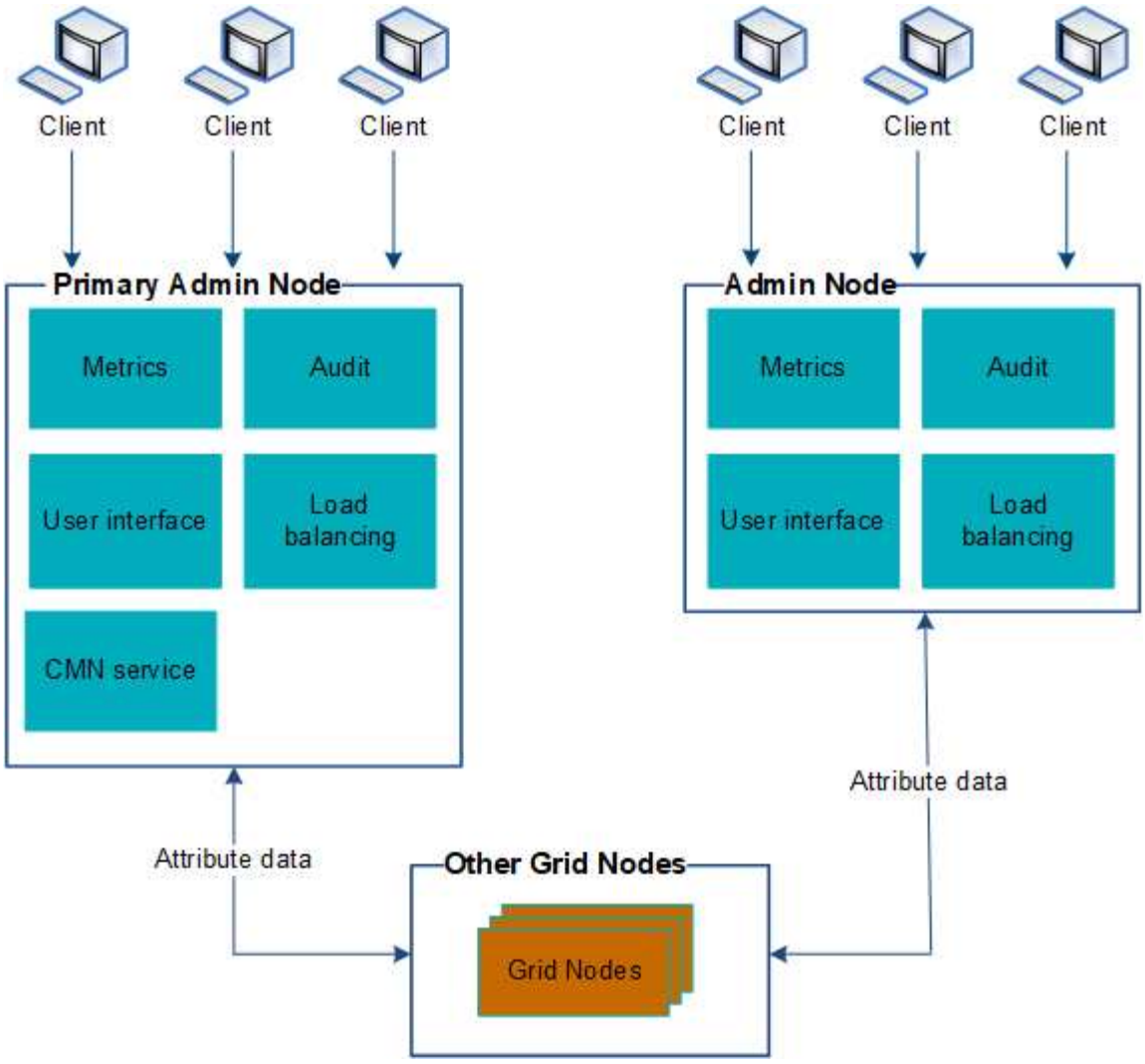
Prometheus 服务从所有节点上的服务收集时间序列指标。

使用多个管理节点

一个 StorageGRID 系统可以包含多个管理节点，这样，即使一个管理节点出现故障，您也可以持续监控和配置 StorageGRID 系统。

如果管理节点不可用，则属性处理将继续，警报和警报（旧系统）仍会触发，同时仍会发送电子邮件通知和 AutoSupport 消息。但是，拥有多个管理节点不会提供故障转移保护，但通知和 AutoSupport 消息除外。特别是

，从一个管理节点发出的警报确认不会复制到其他管理节点。



如果管理节点出现故障，可以通过两种方法继续查看和配置 StorageGRID 系统：

- Web 客户端可以重新连接到任何其他可用的管理节点。
- 如果系统管理员配置了高可用性管理节点组，则 Web 客户端可以继续使用 HA 组的虚拟 IP 地址访问网格管理器或租户管理器。请参见 管理高可用性组。

> 使用 HA 组时，如果主管理节点出现故障，访问将中断。用户必须在 HA 组的虚拟 IP 地址故障转移到组中的另一个管理节点后重新登录。

某些维护任务只能使用主管理节点执行。如果主管理节点出现故障，则必须先对其进行恢复，然后 StorageGRID 系统才能重新完全正常运行。

确定主管理节点

主管理节点托管 CMN 服务。某些维护过程只能使用主管理节点执行。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

- 您具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ； site_* > * 管理节点 * ，然后选择 ➕ 展开拓扑树并显示此管理节点上托管的服务。

   主管理节点托管 CMN 服务。

3. 如果此管理节点不托管 CMN 服务，请检查其他管理节点。

选择首选发件人

如果您的 StorageGRID 部署包含多个管理节点，则可以选择哪个管理节点应是通知的首选发送方。默认情况下，系统会选择主管理节点，但任何管理节点都可以是首选发送方。

您需要的内容

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

关于此任务

"* 配置 * > * 系统 * > * 显示选项 * " 页面显示了当前选择用作首选发送方的管理节点。默认情况下会选择主管理节点。

在正常系统操作下，只有首选发件人才会发送以下通知：

- AutoSupport 消息
- SNMP 通知
- 警报电子邮件
- 警报电子邮件（旧系统）

但是，所有其他管理节点（备用发送器）都会监控首选发送器。如果检测到问题，备用发件人也可以发送这些通知。

在以下情况下，首选发件人和备用发件人都可能发送通知：

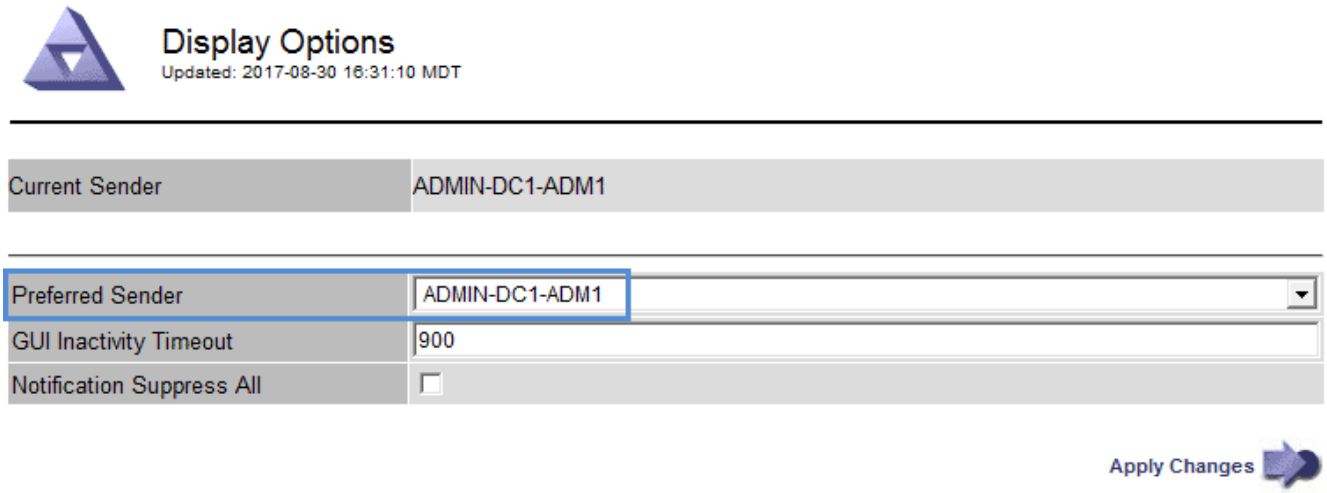
- 如果管理节点彼此变为 "`islanded` " ，则首选发件人和备用发件人都将尝试发送通知，并且可能会收到多个通知副本。
- 备用发件人检测到首选发件人存在问题并开始发送通知后，首选发件人可能会重新获得其发送通知的能力。如果发生这种情况，可能会发送重复的通知。当备用发件人不再检测到首选发件人的错误时，它将停止发送通知。

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

步骤

1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。
2. 从显示选项菜单中，选择 * 选项 * 。

3. 从下拉列表中选择要设置为首选发送方的管理节点。



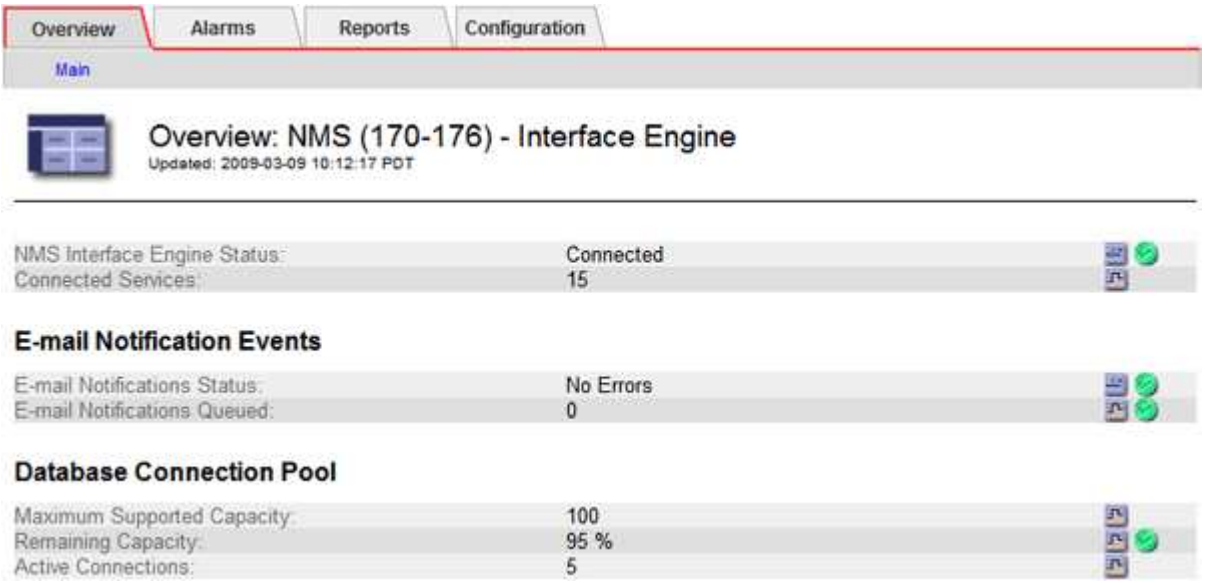
4. 选择 * 应用更改 * 。

   管理节点设置为通知的首选发件人。

查看通知状态和队列

管理节点上的网络管理系统（ Network Management System ， NMS ）服务会向邮件服务器发送通知。您可以在接口引擎页面上查看 NMS 服务的当前状态及其通知队列大小。

要访问接口引擎页面，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。最后，选择 * 站点 _* > * 管理节点 _* > * NMS* > * 接口引擎 * 。

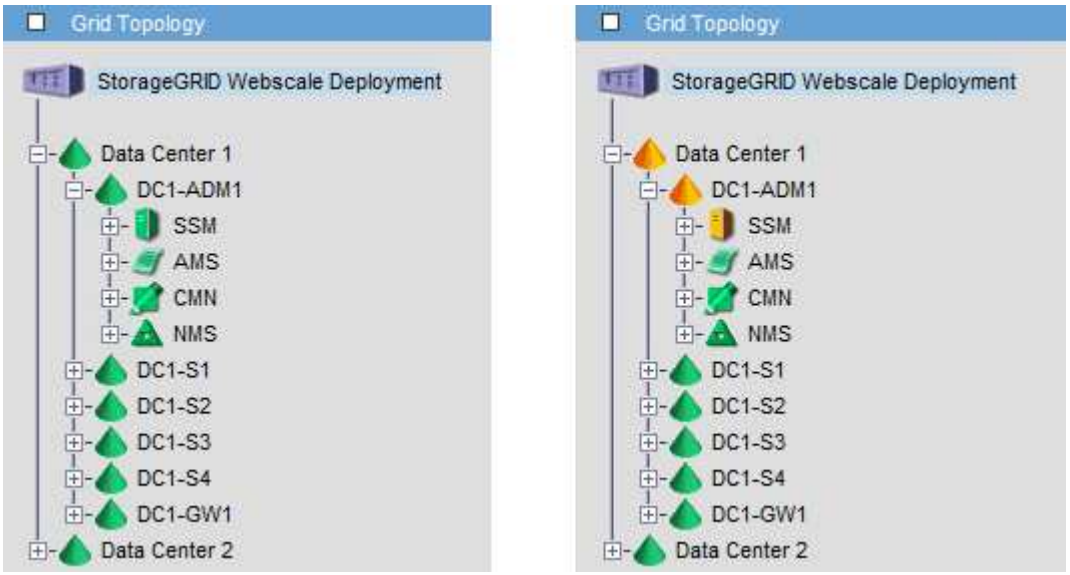


通知通过电子邮件通知队列进行处理，并按触发顺序逐个发送到邮件服务器。如果出现问题（例如网络连接错误），并且在尝试发送通知时邮件服务器不可用，则尽力将通知重新发送到邮件服务器的操作将持续 60 秒。如果通知在 60 秒后未发送到邮件服务器，则通知将从通知队列中删除，并尝试在队列中发送下一个通知。由于通知可以从通知队列中删除而不发送，因此，在不发送通知的情况下，可能会触发警报。如果通知从队列中删除而未发送，则会触发分钟（电子邮件通知状态）次要警报。

管理节点如何显示已确认的警报（旧系统）

在一个管理节点上确认警报时，已确认的警报不会复制到任何其他管理节点。由于确认不会复制到其他管理节点，因此对于每个管理节点，网格拓扑树可能看起来不同。

在连接 Web 客户端时，这种差异非常有用。根据管理员的需求， Web 客户端可以具有不同的 StorageGRID 系统视图。



请注意，通知是从发生确认的管理节点发送的。

配置审核客户端访问

管理节点通过审核管理系统（ Audit Management System ， AMS ）服务将所有审核的系统事件记录到可通过审核共享访问的日志文件中，该文件会在安装时添加到每个管理节点中。为了便于访问审核日志，您可以配置客户端对 CIFS 和 NFS 的审核共享的访问权限。

StorageGRID 系统会使用肯定确认来防止在将审核消息写入日志文件之前丢失这些消息。消息会一直在服务中排队，直到 AMS 服务或中间审核中继服务确认对其进行控制为止。

有关详细信息，请参见 查看审核日志。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。如果您可以选择使用 CIFS 或 NFS ，请选择 NFS 。

为 **CIFS** 配置审核客户端

用于配置审核客户端的操作步骤 取决于身份验证方法： Windows 工作组或 Windows Active Directory （ AD ）。添加后，审核共享将自动启用为只读共享。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

为工作组配置审核客户端

对 StorageGRID 部署中要从中检索审核消息的每个管理节点执行此操作步骤 。

您需要的内容

- 您已拥有 `passwords.txt` 文件以及 root/admin 帐户密码（可从上述软件包中获取）。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。

关于此任务

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

步骤

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

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 确认所有服务的状态均为 running 或 Verified： `storagegRid-status`

   如果所有服务均未运行或未验证，请先解决问题，然后再继续。
3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 启动 CIFS 配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. 为 Windows 工作组设置身份验证：

   如果已设置身份验证，则会显示一条建议消息。如果已设置身份验证，请转至下一步。

   a. 输入： `set-authentication`

b. 当系统提示您安装 Windows 工作组或 Active Directory 时，输入： `workgroup`

c. 出现提示时，输入工作组名称： ` *workgroup_name*`

d. 出现提示时，创建有意义的 NetBIOS 名称： ` netbios_name_`

或

按 * 输入 * 以使用管理节点的主机名作为 NetBIOS 名称。

此脚本将重新启动 Samba 服务器并应用更改。此操作需要不到一分钟的时间。设置身份验证后，添加审核客户端。

a. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

6. 添加审核客户端：

a. 输入： `add-audit-share`

共享将自动添加为只读。

b. 出现提示时，添加用户或组： ` *user*`

c. 出现提示时，输入审核用户名： ` *audit_user_name*`

d. 出现提示时，输入审核用户的密码： ` *password*`

e. 出现提示时，重新输入相同的密码以进行确认： ` *password*`

f. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

无需输入目录。已预定义审核目录名称。

7. 如果允许多个用户或组访问审核共享，请添加其他用户：

a. 输入： `add-user-on-share`

此时将显示已启用共享的编号列表。

b. 出现提示时，输入审核导出共享的编号： ` *share_number*`

c. 出现提示时，添加用户或组： `user`

或 `group`

d. 出现提示时，输入审核用户或组的名称： ` *audit_user* 或 *audit_group*`

e. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

f. 对有权访问审核共享的每个其他用户或组重复这些子步骤。

8. （可选）验证您的配置： `validate-config`

此时将检查并显示这些服务。您可以安全地忽略以下消息：

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. 出现提示时，按 * 输入 * 。

此时将显示审核客户端配置。

b. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

9. 关闭 CIFS 配置实用程序： `exit`
10. 启动 Samba 服务： `sservice smbd start`
11. 如果 StorageGRID 部署是单个站点，请转至下一步。

或

或者，如果 StorageGRID 部署包括其他站点的管理节点，则根据需要启用这些审核共享：

a. 远程登录到站点的管理节点：
   i. 输入以下命令： `ssh admin@ grid_node_ip_`
   ii. 输入 `passwords.txt` 文件中列出的密码。
   iii. 输入以下命令切换到 root： `su -`
   iv. 输入 `passwords.txt` 文件中列出的密码。
b. 重复上述步骤为每个附加管理节点配置审核共享。
c. 关闭远程安全 Shell 登录到远程管理节点： `exit`

12. 注销命令 Shell： `exit`

为 **Active Directory** 配置审核客户端

对 StorageGRID 部署中要从中检索审核消息的每个管理节点执行此操作步骤 。

您需要的内容

- 您已拥有 `passwords.txt` 文件以及 root/admin 帐户密码（可从上述软件包中获取）。

- 您具有 CIFS Active Directory 用户名和密码。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

步骤

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

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 确认所有服务的状态均为 running 或 Verified： `storagegRid-status`

   如果所有服务均未运行或未验证，请先解决问题，然后再继续。
3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 启动 CIFS 配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. 为 Active Directory 设置身份验证： `sET-authentication`

   在大多数部署中，您必须在添加审核客户端之前设置身份验证。如果已设置身份验证，则会显示一条建议消息。如果已设置身份验证，请转至下一步。

   a. 当系统提示您安装工作组或 Active Directory 时： `ad`
   b. 出现提示时，输入 AD 域的名称（短域名）。
   c. 出现提示时，输入域控制器的 IP 地址或 DNS 主机名。
   d. 出现提示时，输入完整的域域名。

使用大写字母。

e. 当系统提示您启用 winbind 支持时，键入 * 。

winbind 用于解析 AD 服务器中的用户和组信息。

f. 出现提示时，输入 NetBIOS 名称。

g. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

6. 加入域：

a. 如果尚未启动，请启动 CIFS 配置实用程序： `config_cifs.rb`

b. 加入域： `join-domain`

c. 系统会提示您测试管理节点当前是否为有效的域成员。如果此管理节点先前未加入此域，请输入： `no`

d. 出现提示时，请提供管理员的用户名： ` 管理员用户名 _`

其中， ` 管理员用户名 _` 是 CIFS Active Directory 用户名，而不是 StorageGRID 用户名。

e. 出现提示时，请提供管理员密码： ` 管理员密码 _ 密码 _`

`` *administrator_password* 是 CIFS Active Directory 用户名，而不是 StorageGRID 密码。

f. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

7. 验证您是否已正确加入域：

a. 加入域： `join-domain`

b. 当系统提示测试服务器当前是否为域的有效成员时，输入： `y`

如果您收到消息 "`join is OK ，` " you have successfully joined the domain.如果未收到此响应，请尝试设置身份验证并重新加入域。

c. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

8. 添加审核客户端： `add-audit-share`

a. 当系统提示您添加用户或组时，输入： `user`

b. 当系统提示您输入审核用户名时，请输入审核用户名。

c. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

9. 如果允许多个用户或组访问审核共享，请添加其他用户： `add-user-to share`

此时将显示已启用共享的编号列表。

a. 输入审核导出共享的编号。
b. 当系统提示您添加用户或组时，输入： `group`

   系统将提示您输入审核组名称。

c. 当系统提示您输入审核组名称时，输入审核用户组的名称。
d. 出现提示时，按 * 输入 * 。

   此时将显示 CIFS 配置实用程序。

e. 对有权访问审核共享的每个其他用户或组重复此步骤。

10. （可选）验证您的配置： `validate-config`

此时将检查并显示这些服务。您可以安全地忽略以下消息：

- 找不到 include 文件 ` /etc/samba/includes/cifs-interfaces.inc`
- 找不到 include 文件 ` /etc/samba/includes/cifs-filesystem.inc`
- 找不到 include 文件 ` /etc/samba/includes/cifs-interfaces.inc`
- 找不到 include 文件 ` /etc/samba/includes/cifs-custom-config.inc`
- 找不到 include 文件 ` /etc/samba/includes/cifs-shares.inc`
- rlimit_max ： 将 rlimit_max （ 1024 ）增加到最小 Windows 限制（ 16384 ）

> 请勿将设置 "security=ads" 与 "password server" 参数结合使用。（默认情况下， Samba 会自动发现要联系的正确 DC ）。

i. 出现提示时，按 * 输入 * 以显示审核客户端配置。
ii. 出现提示时，按 * 输入 * 。

   此时将显示 CIFS 配置实用程序。

11. 关闭 CIFS 配置实用程序： `exit`
12. 如果 StorageGRID 部署是单个站点，请转至下一步。

或

或者，如果 StorageGRID 部署包括其他站点的管理节点，则根据需要启用这些审核共享：

a. 远程登录到站点的管理节点：
   i. 输入以下命令： `ssh admin@ grid_node_ip_`
   ii. 输入 `passwords.txt` 文件中列出的密码。
   iii. 输入以下命令切换到 root ： `su -`
   iv. 输入 `passwords.txt` 文件中列出的密码。

b. 重复上述步骤为每个管理节点配置审核共享。

c. 关闭远程安全 Shell 登录到管理节点： `exit`

13. 注销命令 Shell： `exit`

将用户或组添加到 **CIFS** 审核共享

您可以将用户或组添加到与 AD 身份验证集成的 CIFS 审核共享。

您需要的内容

- 您已拥有 `passwords.txt` 文件以及 root/admin 帐户密码（可从上述软件包中获取）。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。

关于此任务

以下操作步骤 适用于与 AD 身份验证集成的审核共享。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

步骤

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

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 确认所有服务的状态均为正在运行或已验证。输入： `storagegRid-status`

   如果所有服务均未运行或未验证，请先解决问题，然后再继续。

3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 启动 CIFS 配置实用程序： `config_cifs.rb`

```
-------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------------
```

5. 开始添加用户或组： `add-user-on-share`

   此时将显示已配置的审核共享的编号列表。

6. 出现提示时，输入审核共享（审核 - 导出）的编号： ` *audit_share_number*`

   系统会询问您是否要授予用户或组对此审核共享的访问权限。

7. 出现提示时，添加用户或组： `user` 或 `group`
8. 当系统提示您输入此 AD 审核共享的用户或组名称时，请输入此名称。

   此用户或组将作为审核共享的只读添加到服务器的操作系统和 CIFS 服务中。系统将重新加载 Samba 配置，以使用户或组能够访问审核客户端共享。

9. 出现提示时，按 * 输入 * 。

   此时将显示 CIFS 配置实用程序。

10. 对有权访问审核共享的每个用户或组重复上述步骤。
11. （可选）验证您的配置： `validate-config`

    此时将检查并显示这些服务。您可以安全地忽略以下消息：

    - 找不到 include 文件 /etc/samba/includes/cifs-interfaces.inc
    - 找不到 include 文件 /etc/samba/includes/cifs-filesystem.inc
    - 找不到 include 文件 /etc/samba/includes/cifs-custom-config.inc
    - 找不到 include 文件 /etc/samba/includes/cifs-shares.inc
      i. 出现提示时，按 * 输入 * 以显示审核客户端配置。
      ii. 出现提示时，按 * 输入 * 。
12. 关闭 CIFS 配置实用程序： `exit`
13. 确定是否需要启用其他审核共享，如下所示：
    - 如果 StorageGRID 部署是单个站点，请转至下一步。

- 如果 StorageGRID 部署包括其他站点的管理节点，请根据需要启用这些审核共享：
  i. 远程登录到站点的管理节点：
     A. 输入以下命令： `ssh admin@ grid_node_ip_`
     B. 输入 `passwords.txt` 文件中列出的密码。
     C. 输入以下命令切换到 root： `su -`
     D. 输入 `passwords.txt` 文件中列出的密码。
  ii. 重复上述步骤为每个管理节点配置审核共享。
  iii. 关闭远程安全 Shell 登录到远程管理节点： `exit`

14. 注销命令 Shell： `exit`

从 **CIFS** 审核共享中删除用户或组

您不能删除允许访问审核共享的最后一个用户或组。

您需要的内容

- 您已有 `passwords.txt` 文件以及根帐户密码（可在上述软件包中找到）。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。

关于此任务

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

步骤

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

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 启动 CIFS 配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

3. 开始删除用户或组： `remove-user-from-share`

   此时将显示一个编号列表，其中列出了管理节点的可用审核共享。审核共享标记为 audit-export 。

4. 输入审核共享的编号：` *audit_share_number*`
5. 当系统提示删除用户或组时： `user` 或 `group`

   此时将显示审核共享的用户或组的编号列表。

6. 输入与要删除的用户或组对应的数字：` *number*`

   此时将更新审核共享，并且不再允许用户或组访问此审核共享。例如：

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. 关闭 CIFS 配置实用程序： `exit`
8. 如果 StorageGRID 部署包括其他站点的管理节点，请根据需要在每个站点禁用审核共享。
9. 配置完成后，从每个命令 Shell 中注销： `exit`

更改 CIFS 审核共享用户或组名称

您可以通过添加新用户或组并删除旧用户或组来更改 CIFS 审核共享的用户或组名称。

关于此任务

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

步骤

1. 将名称已更新的新用户或组添加到审核共享中。
2. 删除旧用户或组名称。

相关信息

- 将用户或组添加到 CIFS 审核共享
- 从 CIFS 审核共享中删除用户或组

验证 CIFS 审核集成

审核共享为只读。日志文件可由计算机应用程序读取，验证不包括打开文件。我们认为，审核日志文件是否显示在 Windows 资源管理器窗口中已足够验证。验证连接后，关闭所有窗口。

为 NFS 配置审核客户端

审核共享会自动启用为只读共享。

您需要的内容

- 您已拥有 `passwords.txt` 文件以及 root/admin 密码（可在上述软件包中找到）。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。
- 审核客户端正在使用 NFS 版本 3 （ NFSv3 ）。

关于此任务

对 StorageGRID 部署中要从中检索审核消息的每个管理节点执行此操作步骤 。

步骤

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

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 确认所有服务的状态均为正在运行或已验证。输入： `storagegRid-status`

   如果任何服务未列为 "Running or Verifified （正在运行或已验证） " ，请先解决问题，然后再继续。

3. 返回到命令行。按 * 。 Ctrl+* 。
4. 启动 NFS 配置实用程序。输入： `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. 添加审核客户端： `add-audit-share`
   a. 出现提示时，输入审核共享的审核客户端 IP 地址或 IP 地址范围： `client_ip_address`
   b. 出现提示时，按 * 输入 * 。
6. 如果允许多个审核客户端访问审核共享，请添加其他用户的 IP 地址： `add-ip-o-share`
   a. 输入审核共享的编号： ` *audit_share_number*`
   b. 出现提示时，输入审核共享的审核客户端 IP 地址或 IP 地址范围： ` client_ip_address_`
   c. 出现提示时，按 * 输入 * 。

      此时将显示 NFS 配置实用程序。

   d. 对有权访问审核共享的其他每个审核客户端重复这些子步骤。
7. （可选）验证您的配置。
   a. 输入以下内容： `validate-config`

      此时将检查并显示这些服务。

   b. 出现提示时，按 * 输入 * 。

      此时将显示 NFS 配置实用程序。

   c. 关闭 NFS 配置实用程序： `exit`
8. 确定是否必须在其他站点启用审核共享。
   - 如果 StorageGRID 部署是单个站点，请转至下一步。
   - 如果 StorageGRID 部署包括其他站点的管理节点，请根据需要启用这些审核共享：
     i. 远程登录到站点的管理节点：
        A. 输入以下命令： `ssh admin@ grid_node_ip_`
        B. 输入 `passwords.txt` 文件中列出的密码。
        C. 输入以下命令切换到 root： `su -`

D. 输入 `passwords.txt` 文件中列出的密码。

ii. 重复上述步骤为每个附加管理节点配置审核共享。

iii. 关闭远程安全 Shell 登录到远程管理节点。输入： `exit`

9. 注销命令 Shell： `exit`

NFS 审核客户端将根据其 IP 地址获得对审核共享的访问权限。通过将新 NFS 审核客户端的 IP 地址添加到共享中来向该客户端授予对审核共享的访问权限，或者通过删除现有审核客户端的 IP 地址来删除该客户端。

将 **NFS** 审核客户端添加到审核共享

NFS 审核客户端将根据其 IP 地址获得对审核共享的访问权限。通过将新 NFS 审核客户端的 IP 地址添加到审核共享，将审核共享的访问权限授予给该客户端。

您需要的内容

- 您已拥有 `passwords.txt` 文件以及 root/admin 帐户密码（可从上述软件包中获取）。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。
- 审核客户端正在使用 NFS 版本 3 （ NFSv3 ）。

步骤

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

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 启动 NFS 配置实用程序： `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients               | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config  |
| enable-disable-share  | remove-ip-from-share  | refresh-config   |
|                       |                       | help             |
|                       |                       | exit             |
----------------------------------------------------------------------
```

3. 输入： `add-ip-on-share`

此时将显示在管理节点上启用的 NFS 审核共享列表。此审核共享列出为： ` /var/local/audit/export`

4. 输入审核共享的编号：`audit_share_number`
5. 出现提示时，输入审核共享的审核客户端 IP 地址或 IP 地址范围：`client_ip_address_`

   此时，审核客户端将添加到审核共享中。

6. 出现提示时，按 * 输入 * 。

   此时将显示 NFS 配置实用程序。

7. 对应添加到审核共享中的每个审核客户端重复上述步骤。
8. （可选）验证您的配置： `validate-config`

   此时将检查并显示这些服务。

   a. 出现提示时，按 * 输入 * 。

      此时将显示 NFS 配置实用程序。

9. 关闭 NFS 配置实用程序： `exit`
10. 如果 StorageGRID 部署是单个站点，请转至下一步。

    否则，如果 StorageGRID 部署包括其他站点的管理节点，则可以根据需要选择启用这些审核共享：

    a. 远程登录到站点的管理节点：
       i. 输入以下命令： `ssh admin@ grid_node_ip_`
       ii. 输入 `passwords.txt` 文件中列出的密码。
       iii. 输入以下命令切换到 root： `su -`
       iv. 输入 `passwords.txt` 文件中列出的密码。
    b. 重复上述步骤为每个管理节点配置审核共享。
    c. 关闭远程安全 Shell 登录到远程管理节点： `exit`
11. 注销命令 Shell： `exit`

验证 **NFS** 审核集成

配置审核共享并添加 NFS 审核客户端后，您可以挂载审核客户端共享并验证这些文件是否可从审核共享访问。

步骤

1. 使用托管 AMS 服务的管理节点的客户端 IP 地址验证连接（或客户端系统的变体）。输入： `ping ip_address`

   验证服务器是否响应，指示连接。

2. 使用适用于客户端操作系统的命令挂载审核只读共享。Linux 命令示例为（在一行中输入）：

   `mount -t nfs -o hard , intr Admin_Node_ip_address : /var/local/audit/export`

_myAudit _

使用托管 AMS 服务的管理节点的 IP 地址以及审核系统的预定义共享名称。挂载点可以是客户端选择的任何名称（例如，在上一个命令中为 ` myAudit _` ）。

3. 验证这些文件是否可从审核共享访问。输入： `ls _myAudit _/*`

   其中，` myAudit _` 是审核共享的挂载点。应至少列出一个日志文件。

从审核共享中删除 **NFS** 审核客户端

NFS 审核客户端将根据其 IP 地址获得对审核共享的访问权限。您可以通过删除现有审核客户端的 IP 地址来删除此客户端。

您需要的内容

- 您已拥有 `passwords.txt` 文件以及 root/admin 帐户密码（可从上述软件包中获取）。
- 您已有 `Configuration.txt` 文件（可在上述软件包中找到）。

关于此任务

您不能删除允许访问审核共享的最后一个 IP 地址。

步骤

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

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 启动 NFS 配置实用程序： `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config         |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                       |                       | help           |
|                       |                       | exit           |
------------------------------------------------------------------
```

3. 从审核共享中删除 IP 地址： `remove-ip-from-share`

   此时将显示服务器上配置的审核共享的编号列表。此审核共享列出为： ` /var/local/audit/export`

4. 输入与审核共享对应的数字：`*audit_share_number*`

   此时将显示允许访问审核共享的 IP 地址的编号列表。

5. 输入与要删除的 IP 地址对应的数字。

   此时将更新审核共享，并且不再允许使用此 IP 地址的任何审核客户端进行访问。

6. 出现提示时，按 * 输入 * 。

   此时将显示 NFS 配置实用程序。

7. 关闭 NFS 配置实用程序： `exit`
8. 如果您的 StorageGRID 部署为多数据中心站点部署，而其他站点上有更多管理节点，请根据需要禁用这些审核共享：
   a. 远程登录到每个站点的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 重复上述步骤为每个附加管理节点配置审核共享。
   c. 关闭远程安全 Shell 登录到远程管理节点： `exit`
9. 注销命令 Shell： `exit`

更改 **NFS** 审核客户端的 **IP** 地址

如果需要更改 NFS 审核客户端的 IP 地址，请完成以下步骤。

步骤

1. 向现有 NFS 审核共享添加新 IP 地址。
2. 删除原始 IP 地址。

相关信息

- 将 NFS 审核客户端添加到审核共享
- 从审核共享中删除 NFS 审核客户端

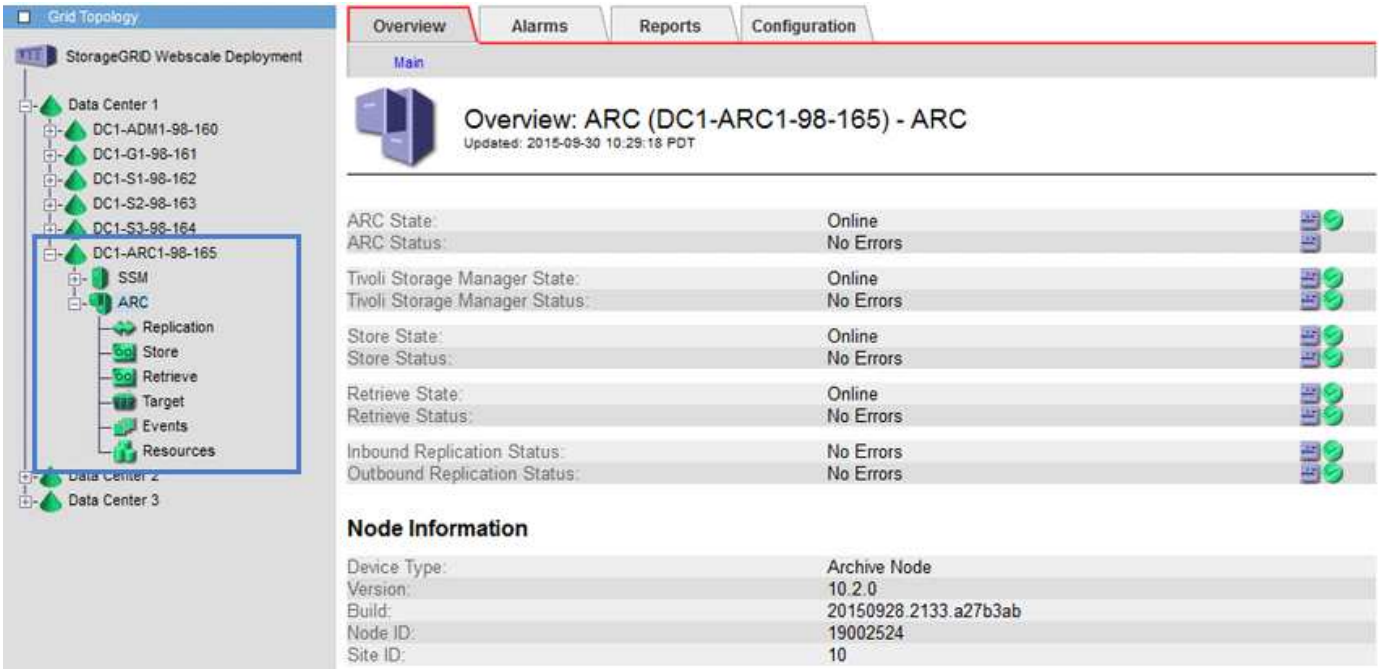
管理归档节点

什么是归档节点

您也可以选择使用归档节点部署每个 StorageGRID 数据中心站点，以便连接到目标外部归档存储系统，例如 Tivoli Storage Manager （ TSM ）。

归档节点提供了一个接口，您可以通过该接口将外部归档存储系统作为长期存储对象数据的目标。归档节点还会

监控此连接以及 StorageGRID 系统与目标外部归档存储系统之间的对象数据传输。



配置与外部目标的连接后，您可以配置归档节点以优化 TSM 性能，在 TSM 服务器容量接近或不可用时使归档节点脱机，以及配置复制和检索设置。您还可以为归档节点设置自定义警报。

无法删除但未定期访问的对象数据可以随时从存储节点的旋转磁盘移出，并移至云或磁带等外部归档存储。对象数据的这种归档是通过配置数据中心站点的归档节点以及配置 ILM 规则来实现的，在这些规则中，此归档节点被选为内容放置说明的 " 目标 " 。归档节点不会管理归档对象数据本身；这可通过外部归档设备实现。

对象元数据不会归档，但会保留在存储节点上。

什么是 **ARC-Service**

归档节点上的归档（ Archive ， ARC-） 服务提供了一个管理界面，您可以使用此界面来配置通过 TSM 中间件连接到外部归档存储（例如磁带）的连接。

它是一种可与外部归档存储系统交互的应用程序服务，用于为近线存储发送对象数据，并在客户端应用程序请求归档对象时执行检索。当客户端应用程序请求归档对象时，存储节点会从 ARC-Service 请求对象数据。ARC-Service 会向外部归档存储系统发出请求，该系统会检索请求的对象数据并将其发送到 ARC-Service 。此应用程序服务会验证对象数据并将其转发到存储节点，然后存储节点会将此对象返回到请求的客户端应用程序。

通过 TSM 中间件将对象数据归档到磁带的请求可以进行管理，以提高检索效率。可以对请求进行排序，以便按同一顺序请求按顺序存储在磁带上的对象。然后，请求将排队等待提交到存储设备。根据归档设备的不同，可以同时处理对不同卷上的对象的多个请求。

通过 **S3 API** 归档到云

您可以将归档节点配置为直接连接到 Amazon Web Services （ AWS ）或可通过 S3 API 连接到 StorageGRID 系统的任何其他系统。

通过 S3 API 将对象从归档节点移动到外部归档存储系统已被 ILM 云存储池所取代，它可提供更多功能。仍然支持 * 云分层 - 简单存储服务（ S3 ） * 选项，但您可能更喜欢实施云存储池。

如果您当前正在使用具有 * 云分层 - 简单存储服务（ S3 ） * 选项的归档节点，请考虑将对象迁移到云存储池。请参见的说明 使用 ILM 管理对象。

配置 **S3 API** 的连接设置

如果要使用 S3 接口连接到归档节点，则必须配置 S3 API 的连接设置。在配置这些设置之前，由于无法与外部归档存储系统进行通信，因此， ARC-Service 将保持主要警报状态。

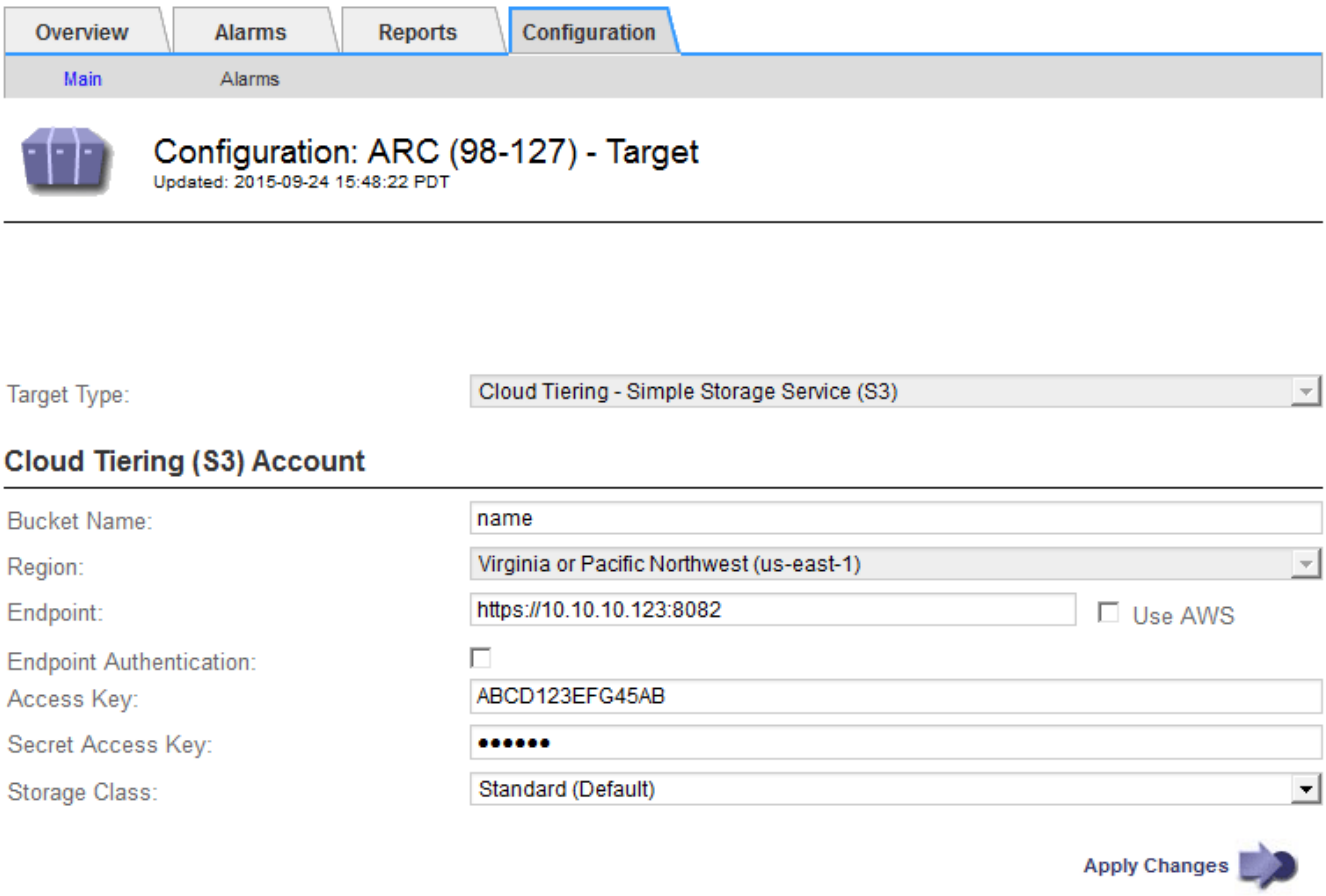
> 通过 S3 API 将对象从归档节点移动到外部归档存储系统已被 ILM 云存储池所取代，它可提供更多功能。仍然支持 * 云分层 - 简单存储服务（ S3 ） * 选项，但您可能更喜欢实施云存储池。
>
> 如果您当前正在使用具有 * 云分层 - 简单存储服务（ S3 ） * 选项的归档节点，请考虑将对象迁移到云存储池。请参见 使用 ILM 管理对象。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已在目标归档存储系统上创建存储分段：
  - 此存储分段专用于一个归档节点。它不能由其他归档节点或其他应用程序使用。
  - 存储分段已为您的位置选择相应的区域。
  - 应在存储分段配置中暂停版本控制。
- 已启用对象分段，并且最大分段大小小于或等于 4.5 GiB （ 4 ， 831 ， 838 ， 208 字节）。如果使用 S3 作为外部归档存储系统，超过此值的 S3 API 请求将失败。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARE* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。



4. 从目标类型下拉列表中选择 * 云分层 - 简单存储服务（ S3 ） * 。

   只有在选择目标类型后，配置设置才可用。

5. 配置云分层（ S3 ）帐户，归档节点将通过该帐户连接到支持 S3 的目标外部归档存储系统。

   此页面上的大多数字段都是不言自明的。下面介绍了可能需要指导的字段。

   - * 地区 * ： 仅在选择 * 使用 AWS* 时可用。您选择的区域必须与存储分段的区域匹配。
   - * 端点 * 和 * 使用 AWS* ： 对于 Amazon Web Services （ AWS ），请选择 * 使用 AWS* 。然后，系统会根据 " 分段名称 " 和 " 区域 " 属性自动为 * 端点 * 填充端点 URL 。例如：

     ` https://bucket.region.amazonaws.com`

     对于非 AWS 目标，输入托管存储分段的系统的 URL ，包括端口号。例如：

` https://system.com:1080`

   - * 端点身份验证 * ： 默认情况下处于启用状态。如果外部归档存储系统的网络是可信的，则可以取消选中此复选框，以便为目标外部归档存储系统禁用端点 SSL 证书和主机名验证。如果 StorageGRID 系统的另一个实例是目标归档存储设备，并且系统配置了公共签名证书，则可以保持选中复选框。
   - * 存储类 * ： 选择 * 标准（默认） * 作为常规存储。仅为易于重新创建的对象选择 * 精简冗余 * 。* 冗余减少 * 可降低存储成本，降低可靠性。如果目标归档存储系统是 StorageGRID 系统的另一个实例，则如果在目标系统上载入对象时使用了双提交，则 * 存储类 * 将控制在目标系统上载入时为该对象创建的中间副本数。

6. 选择 * 应用更改 * 。

   系统将验证指定的配置设置并将其应用于 StorageGRID 系统。配置后，无法更改目标。

修改 **S3 API** 的连接设置

将归档节点配置为通过 S3 API 连接到外部归档存储系统后，如果连接发生变化，您可以修改某些设置。

您需要的内容

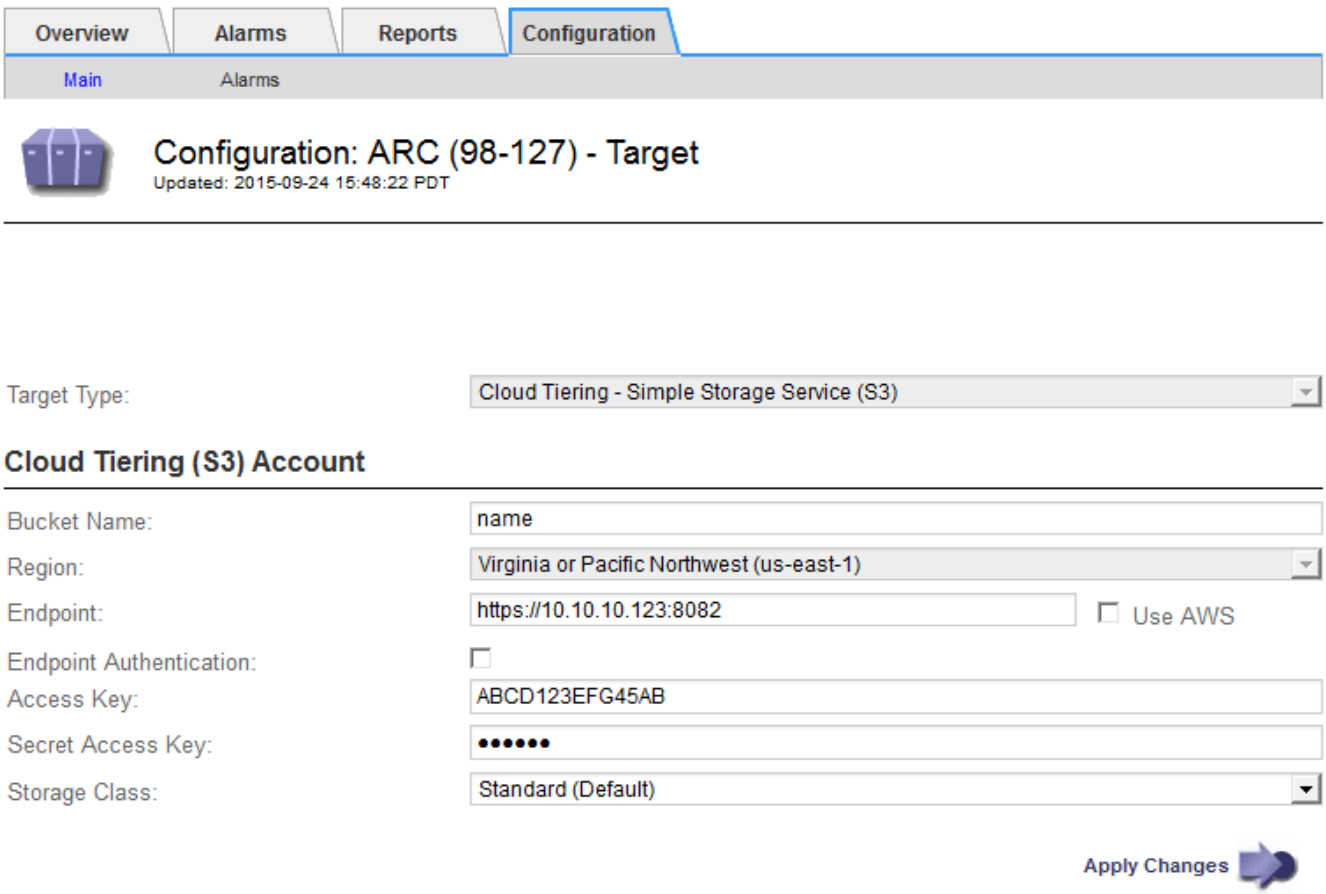
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。

关于此任务

如果更改 Cloud Tiering （ S3 ）帐户，则必须确保用户访问凭据对存储分段具有读 / 写访问权限，包括先前归档节点向存储分段载入的所有对象。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。



4. 根据需要修改帐户信息。

如果更改存储类，则新对象数据将与新存储类一起存储。载入时，现有对象仍存储在存储类集下。

分段名称，区域和端点，使用 AWS 值，不能更改。

5. 选择 * 应用更改 * 。

修改 **Cloud Tiering Service** 状态

您可以通过更改 Cloud Tiering 服务的状态来控制归档节点对通过 S3 API 连接的目标外部归档存储系统的读写能力。

您需要的内容

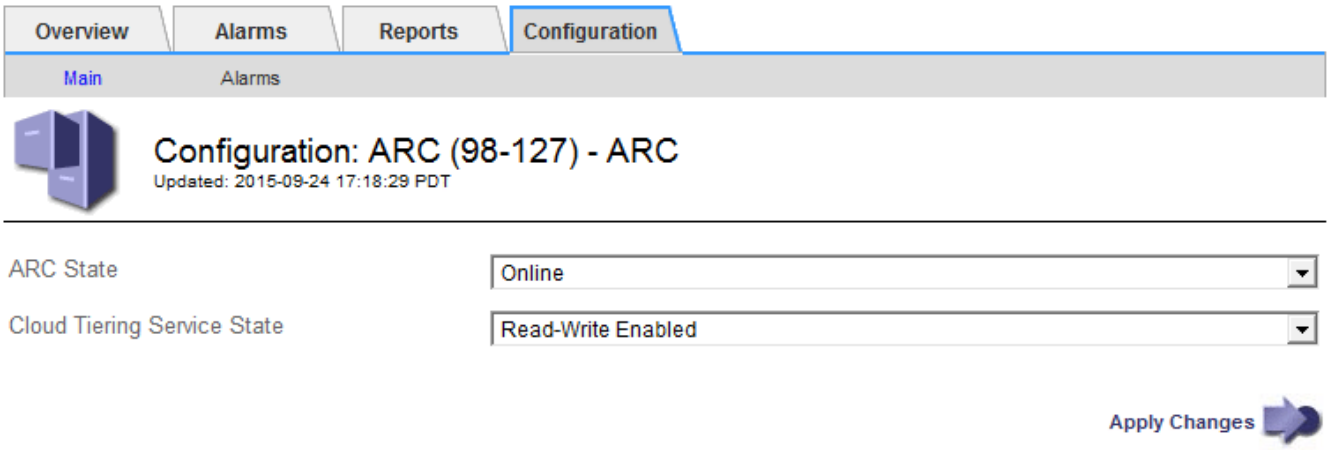
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 必须配置归档节点。

关于此任务

通过将 Cloud Tiering 服务状态更改为 * 已禁用读写 * ，可以有效地使归档节点脱机。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 。归档节点 _* > * 。 ARR* 。
3. 选择 * 配置 * > * 主 * 。



4. 选择 * 云分层服务状态 * 。
5. 选择 * 应用更改 * 。

重置 **S3 API** 连接的存储故障计数

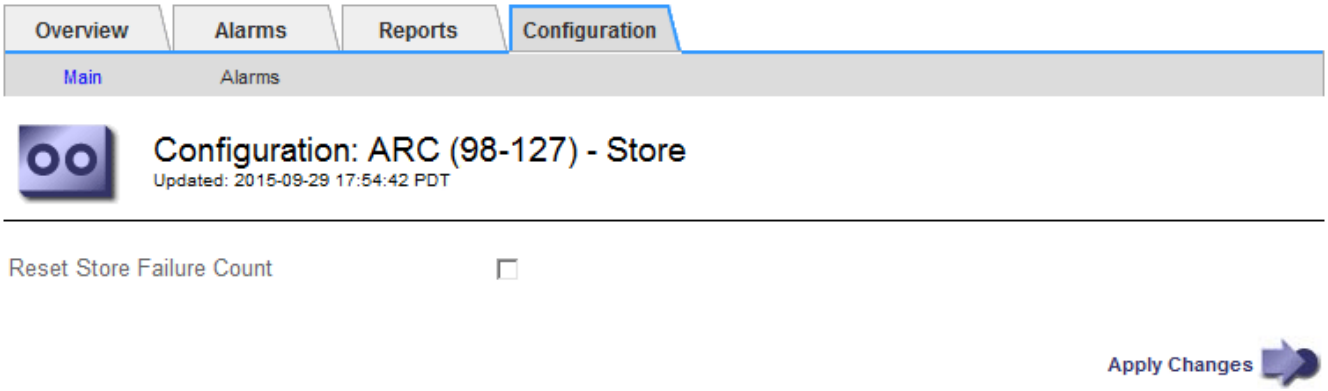
如果归档节点通过 S3 API 连接到归档存储系统，则可以重置存储故障计数，此计数可用于清除 ARVF （存储故障）警报。

您需要的内容

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

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 存储 * 。
3. 选择 * 配置 * > * 主 * 。



4. 选择 * 重置存储故障计数 * 。
5. 选择 * 应用更改 * 。

   存储故障属性重置为零。

将对象从 **Cloud Tiering - S3** 迁移到云存储池

如果您当前正在使用 * 云分层 - 简单存储服务（ S3 ） * 功能将对象数据分层到 S3 存储分段，请考虑将对象迁移到云存储池。云存储池提供了一种可扩展的方法，可利用 StorageGRID 系统中的所有存储节点。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已将对象存储在为 Cloud Tiering 配置的 S3 存储分段中。

迁移对象数据之前，请联系您的 NetApp 客户代表，了解并管理任何相关成本。

关于此任务

从 ILM 角度来看，云存储池与存储池类似。但是，虽然存储池包含 StorageGRID 系统中的存储节点或归档节点，但云存储池包含一个外部 S3 存储分段。

在将对象从 Cloud Tiering - S3 迁移到云存储池之前，必须先创建 S3 存储分段，然后在 StorageGRID 中创建云存储池。然后，您可以创建一个新的 ILM 策略，并将用于存储 Cloud Tiering 分段中对象的 ILM 规则替换为在 Cloud Storage Pool 中存储相同对象的克隆 ILM 规则。

如果对象存储在云存储池中，则这些对象的副本也无法存储在 StorageGRID 中。如果您当前用于云分层的 ILM 规则配置为同时将对象存储在多个位置，请考虑是否仍要执行此可选迁移，因为您将丢失此功能。如果继续执行此迁移，则必须创建新规则，而不是克隆现有规则。

步骤

1. 创建云存储池。

   为云存储池使用新的 S3 存储分段，以确保其仅包含由云存储池管理的数据。

2. 在活动 ILM 策略中找到要存储在云分层分段中的发生原因 对象的任何 ILM 规则。
3. 克隆上述每个规则。
4. 在克隆的规则中，将放置位置更改为新的云存储池。
5. 保存克隆的规则。
6. 创建使用新规则的新策略。
7. 模拟并激活新策略。

   激活新策略并进行 ILM 评估后，对象将从为 Cloud Tiering 配置的 S3 存储分段移动到为 Cloud Storage Pool 配置的 S3 存储分段。网格上的可用空间不受影响。将对象移至云存储池后，这些对象将从 Cloud Tiering 分段中删除。

相关信息

使用 ILM 管理对象

通过 **TSM** 中间件归档到磁带

您可以将归档节点配置为以 Tivoli Storage Manager （ TSM ）服务器为目标，该服务器可提供逻辑接口，用于将对象数据存储和检索到随机或顺序访问存储设备，包括磁带库。

归档节点的 ARC 服务充当 TSM 服务器的客户端，使用 Tivoli Storage Manager 作为与归档存储系统通信的中间件。

TSM 管理类

TSM 中间件定义的管理类概括了 TSM's 备份和归档操作的工作原理，可用于为 TSM 服务器应用的内容指定规则。此类规则独立于 StorageGRID 系统的 ILM 策略运行，并且必须符合 StorageGRID 系统的要求，即对象永久存储，并且始终可供归档节点检索。在归档节点将对象数据发送到 TSM 服务器后，将应用 TSM 生命周期和保留规则，同时将对象数据存储到 TSM 服务器管理的磁带。

在归档节点将对象发送到 TSM 服务器后， TSM 服务器将使用 TSM 管理类应用数据位置或保留规则。例如，标识为数据库备份的对象（可使用较新数据覆盖的临时内容）可以与应用程序数据（必须无限期保留的固定内容）不同。

配置与 **TSM** 中间件的连接

在归档节点能够与 Tivoli Storage Manager （ TSM ）中间件进行通信之前，您必须配置多项设置。

您需要的内容

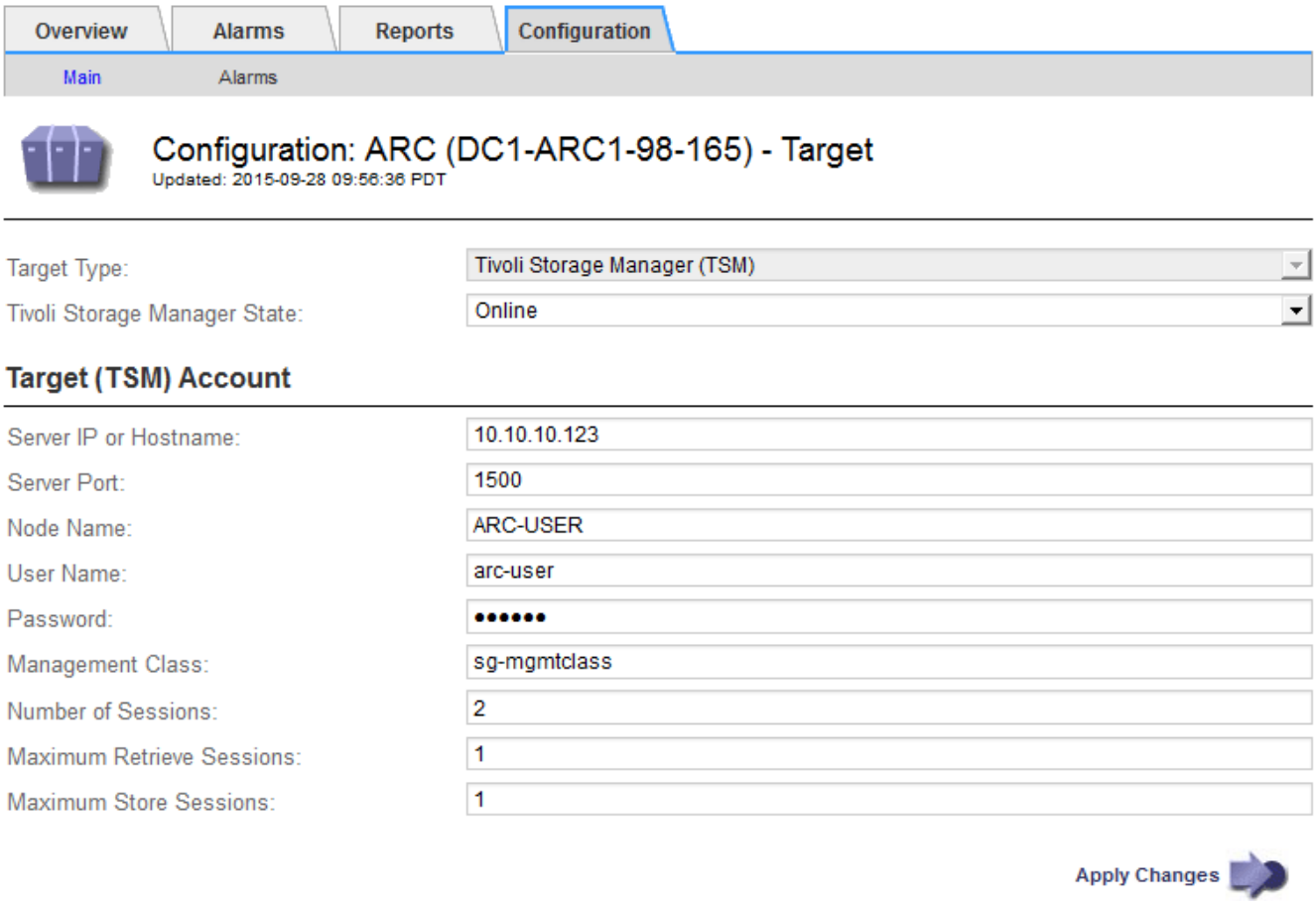
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。

关于此任务

在配置这些设置之前，由于无法与 Tivoli Storage Manager 进行通信，因此，此 ARC-Service 仍会处于主要警报状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。



4. 从 * 目标类型 * 下拉列表中，选择 * Tivoli Storage Manager （ TSM ） * 。
5. 对于 * Tivoli Storage Manager State* ，请选择 * 脱机 * 以防止从 TSM 中间件服务器进行检索。

   默认情况下， Tivoli Storage Manager 状态设置为联机，这意味着归档节点能够从 TSM 中间件服务器检索对象数据。

6. 填写以下信息：

   - * 服务器 IP 或主机名 * ： 指定用于此 ART 服务的 TSM 中间件服务器的 IP 地址或完全限定域名。默认 IP 地址为 127.0.0.1 。
   - * 服务器端口 * ： 指定此 ARE 服务将连接到的 TSM 中间件服务器上的端口号。默认值为 1500 。

- * 节点名称 *：指定归档节点的名称。您必须输入在 TSM 中间件服务器上注册的名称（ arc - user ）。
- * 用户名 *：指定应用程序中心服务用于登录到 TSM 服务器的用户名。输入为归档节点指定的默认用户名（ arc - user ）或管理用户。
- * 密码 *：指定用于登录到 TSM 服务器的应用程序服务的密码。
- * 管理类 *：指定在将对象保存到 StorageGRID 系统时未指定管理类或在 TSM 中间件服务器上未定义指定管理类时要使用的默认管理类。
- * 会话数 *：指定 TSM 中间件服务器上专用于归档节点的磁带驱动器数量。归档节点会同时为每个挂载点最多创建一个会话，并另外创建少量会话（少于五个）。

  您必须将此值更改为与注册或更新归档节点时为 MAXNUMMP （最大挂载点数）设置的值相同。（在 register 命令中，如果未设置任何值，则使用的 MAXNUMMP 默认值为 1 。）

此外，您还必须将 TSM 服务器的 MaxSessions 值更改为至少与为该应用程序服务设置的会话数相同的数字。TSM 服务器上的 MaxSessions 默认值为 25 。

- * 最大检索会话数 *：指定可由应用程序控制的服务为 TSM 中间件服务器打开以执行检索操作的最大会话数。在大多数情况下，适当的值为会话数减去最大存储会话数。如果需要共享一个磁带驱动器以进行存储和检索，请指定一个等于会话数的值。
- * 最大存储会话数 *：指定可通过应用程序中心服务打开到 TSM 中间件服务器进行归档操作的最大并发会话数。

  此值应设置为 1 ，但目标归档存储系统已满且只能执行检索时除外。将此值设置为零可使用所有会话进行检索。

7. 选择 * 应用更改 * 。

针对 **TSM** 中间件会话优化归档节点

您可以通过配置归档节点的会话来优化连接到 Tivoli Server Manager （ TSM ）的归档节点的性能。

您需要的内容

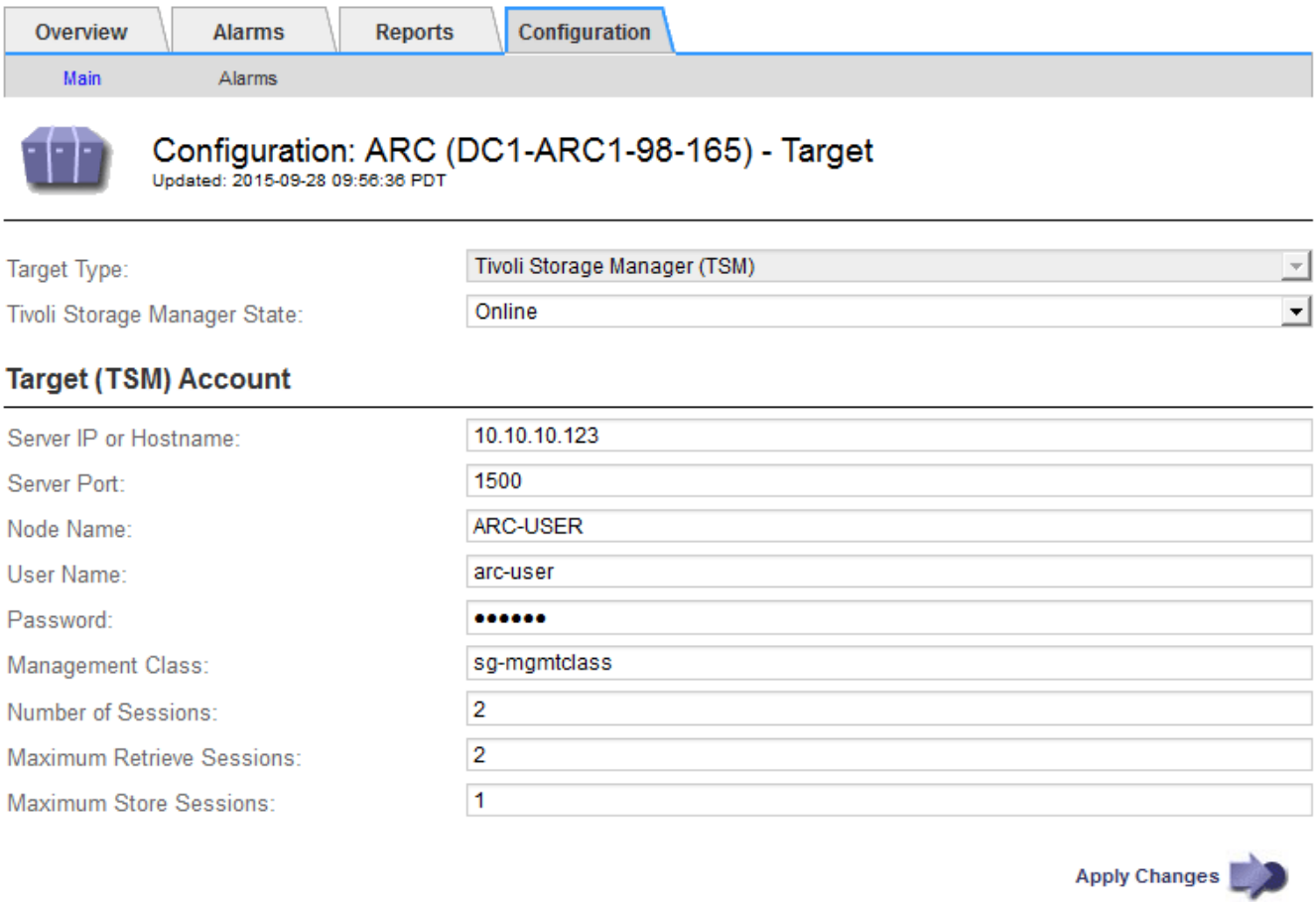
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。

关于此任务

通常，归档节点向 TSM 中间件服务器打开的并发会话数会设置为 TSM 服务器专用于归档节点的磁带驱动器数。一个磁带驱动器分配给存储，而其余磁带驱动器分配给检索。但是，如果要从归档节点副本重建存储节点或归档节点以只读模式运行，则可以通过将最大检索会话数设置为与并发会话数相同来优化 TSM 服务器性能。这样，所有驱动器都可以同时用于检索，如果适用，这些驱动器中最多有一个也可以用于存储。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 *： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。
4. 将 * 最大检索会话数 * 更改为与 * 会话数 * 相同。



5. 选择 * 应用更改 * 。

配置 **TSM** 的归档状态和计数器

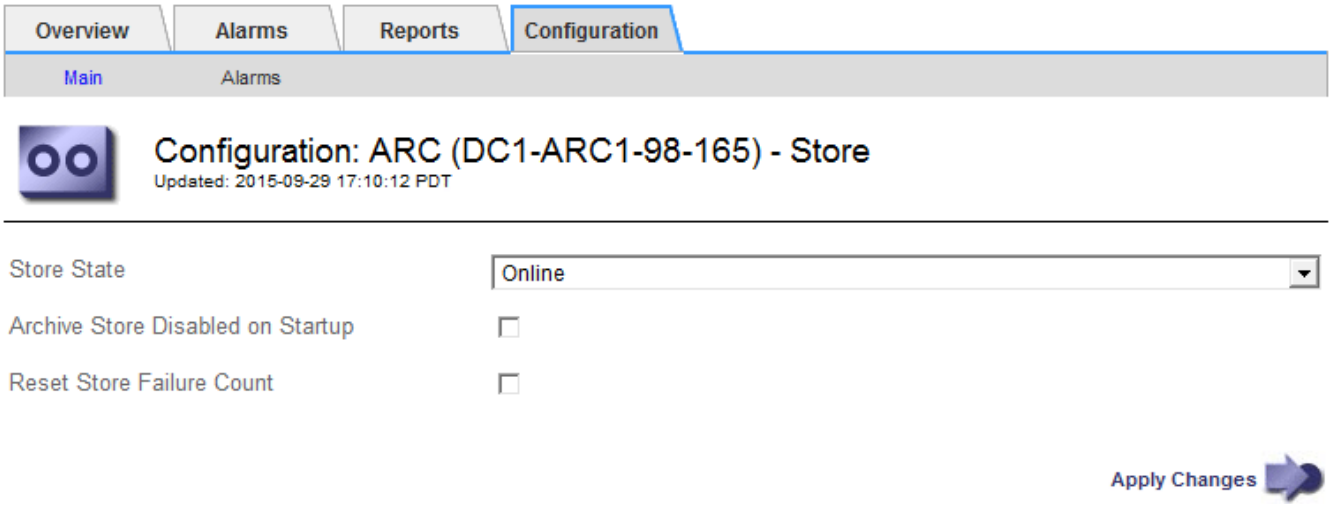
如果归档节点连接到 TSM 中间件服务器，则可以将归档节点的归档存储状态配置为联机或脱机。您还可以在归档节点首次启动时禁用归档存储，或者重置为关联警报跟踪的故障计数。

您需要的内容

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

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 存储 * 。
3. 选择 * 配置 * > * 主 * 。



4. 根据需要修改以下设置：
   - 存储状态：将组件状态设置为：
     - 联机：归档节点可用于处理要存储到归档存储系统的对象数据。
     - 脱机：归档节点不可用于将要存储的对象数据处理到归档存储系统。
   - 启动时禁用归档存储：选中后，重新启动时归档存储组件将保持只读状态。用于持久禁用目标归档存储系统的存储。当目标归档存储系统无法接受内容时，此功能非常有用。
   - Reset Store Failure Count ： 重置存储故障计数器。此选项可用于清除 ARVF （存储故障）警报。
5. 选择 * 应用更改 * 。

相关信息

在 TSM 服务器达到容量时管理归档节点

在 **TSM** 服务器达到容量时管理归档节点

当 TSM 数据库或 TSM 服务器管理的归档介质存储即将达到容量时， TSM 服务器无法通知归档节点。可以通过主动监控 TSM 服务器来避免这种情况。

您需要的内容

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

关于此任务

在 TSM 服务器停止接受新内容后，归档节点将继续接受要传输到 TSM 服务器的对象数据。此内容无法写入 TSM 服务器管理的介质。如果发生这种情况，将触发警报。

阻止应用程序保护服务向 **TSM** 服务器发送内容

为了防止此 ARC-Service 向 TSM 服务器发送更多内容，您可以使归档节点的 * ARC/ * 组件脱机，从而使其 * 存储 * 组件脱机。此操作步骤 还有助于防止在 TSM 服务器不可维护时发出警报。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

2. 选择 * ： 归档节点 _* > * 。 ARR* > * 存储 * 。
3. 选择 * 配置 * > * 主 * 。

4. 将 * 存储状态 * 更改为 脱机 。
5. 选择 * 启动时已禁用归档存储 * 。
6. 选择 * 应用更改 * 。

如果 **TSM** 中间件达到容量，请将归档节点设置为只读

如果目标 TSM 中间件服务器达到容量，则可以对归档节点进行优化，使其仅执行检索。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。
4. 将最大检索会话数更改为与会话数中列出的并发会话数相同。
5. 将最大存储会话数更改为 0 。

> 如果归档节点为只读，则无需将最大存储会话数更改为 0 。不会创建存储会话。

6. 选择 * 应用更改 * 。

配置归档节点检索设置

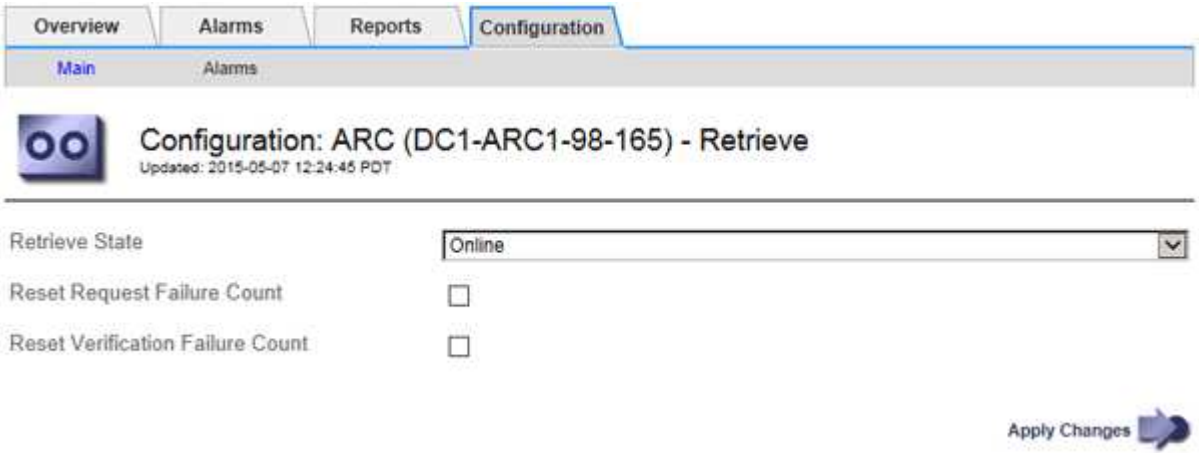
您可以配置归档节点的检索设置，将状态设置为联机或脱机，或者重置为关联警报跟踪的故障计数。

您需要的内容

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

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARC/ * 检索 * 。
3. 选择 * 配置 * > * 主 * 。



4. 根据需要修改以下设置：
   - * 检索状态 * ： 将组件状态设置为：
     - 联机：网格节点可用于从归档介质设备检索对象数据。
     - 脱机：网格节点不可用于检索对象数据。
   - 重置请求失败计数：选中此复选框可重置请求失败的计数器。此选项可用于清除 ARRF （请求失败）警报。
   - 重置验证失败计数：选中此复选框可重置已检索对象数据的验证失败计数器。此操作可用于清除 ARRV （验证失败）警报。
5. 选择 * 应用更改 * 。

配置归档节点复制

您可以为归档节点配置复制设置并禁用入站和出站复制，或者重置为关联警报跟踪的故障计数。

您需要的内容

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

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 复制 * 。
3. 选择 * 配置 * > * 主 * 。

4. 根据需要修改以下设置：
   - * 重置入站复制失败计数 * ： 选择此项可重置入站复制失败的计数器。此操作可用于清除 RIRF （入站复制 - 失败）警报。

- * 重置出站复制失败计数 * ： 选择此项可重置出站复制失败的计数器。此操作可用于清除 RORF （出站复制 - 失败）警报。
- * 禁用入站复制 * ： 选择此项可在维护或测试操作步骤 过程中禁用入站复制。在正常操作期间保持清除状态。

  禁用入站复制后，可以从应用程序中心服务检索对象数据，以便复制到 StorageGRID 系统中的其他位置，但不能将对象从其他系统位置复制到此应用程序中心服务。此 - 服务为只读。

- * 禁用出站复制 * ： 选中此复选框可在维护或测试操作步骤 过程中禁用出站复制（包括 HTTP 检索的内容请求）。在正常操作期间保持未选中状态。

  禁用出站复制后，可以将对象数据复制到此应用程序中心服务以满足 ILM 规则的要求，但无法从应用程序中心服务检索对象数据以复制到 StorageGRID 系统中的其他位置。此 ARC 服务为 write - only 。

5. 选择 * 应用更改 * 。

为归档节点设置自定义警报

您应为 ARQL 和 ARLRL 属性建立自定义警报，用于监控归档节点从归档存储系统检索对象数据的速度和效率。

- ARQL ： 平均队列长度。从归档存储系统中检索对象数据的平均排队时间（以微秒为单位）。
- ARRL ： 平均请求延迟。归档节点从归档存储系统检索对象数据所需的平均时间（以微秒为单位）。

这些属性的可接受值取决于归档存储系统的配置和使用方式。（转至 * ARC/ * * 检索 * > * 概述 * > * 主要 * 。）为请求超时设置的值以及可用于检索请求的会话数尤其具有影响。

集成完成后，监控归档节点的对象数据检索，以确定正常检索时间和队列长度的值。然后，为 ARQL 和 ARLRL 创建自定义警报，以便在出现异常运行状况时触发警报。请参见 监控和故障排除。

集成 **Tivoli Storage Manager**

归档节点配置和操作

您的 StorageGRID 系统会将归档节点作为一个位置来管理，在该位置，对象会无限期地存储，并且始终可以访问。

在载入对象时，系统会根据为 StorageGRID 系统定义的信息生命周期管理（ ILM ）规则将副本复制到所有必需的位置，包括归档节点。归档节点充当 TSM 服务器的客户端， TSM 客户端库通过 StorageGRID 软件安装过程安装在归档节点上。定向到归档节点进行存储的对象数据会在收到时直接保存到 TSM 服务器。归档节点不会在将对象数据保存到 TSM 服务器之前暂存对象数据，也不会执行对象聚合。但是，如果数据速率需要，归档节点可以在一个事务中向 TSM 服务器提交多个副本。

在归档节点将对象数据保存到 TSM 服务器后， TSM 服务器将使用其生命周期 / 保留策略来管理对象数据。必须定义这些保留策略，使其与归档节点的操作兼容。也就是说，归档节点保存的对象数据必须无限期存储，并且必须始终可由归档节点访问，除非归档节点将其删除。

StorageGRID 系统的 ILM 规则与 TSM 服务器的生命周期 / 保留策略之间没有连接。每个对象彼此独立运行；但是，在将每个对象载入 StorageGRID 系统时，您可以为其分配一个 TSM 管理类。此管理类将与对象数据一起传递到 TSM 服务器。通过将不同的管理类分配给不同的对象类型，您可以将 TSM 服务器配置为将对象数据放置在不同的存储池中，或者根据需要应用不同的迁移或保留策略。例如，标识为数据库备份的对象（临时内容，

不能使用较新的数据覆盖）的处理方式可能与应用程序数据（必须无限期保留的固定内容）不同。

归档节点可以与新的或现有的 TSM 服务器集成；它不需要专用的 TSM 服务器。TSM 服务器可以与其他客户端共享，但前提是 TSM 服务器的大小应适合最大预期负载。TSM 必须安装在与归档节点不同的服务器或虚拟机上。

可以将多个归档节点配置为写入同一个 TSM 服务器；但是，只有当归档节点向 TSM 服务器写入不同的数据集时，才建议使用此配置。当每个归档节点向归档写入相同对象数据的副本时，建议不要将多个归档节点配置为写入同一 TSM 服务器。在后一种情况下，对于对象数据的独立冗余副本，这两个副本都会发生单点故障（ TSM 服务器）。

归档节点不会使用 TSM 的分层存储管理（ HSM ）组件。

配置最佳实践

在调整 TSM 服务器的大小并对其进行配置时，应应用一些最佳实践来优化它，以便与归档节点配合使用。

在估算 TSM 服务器的规模并对其进行配置时，应考虑以下因素：

- 由于归档节点在将对象保存到 TSM 服务器之前不会聚合对象，因此必须对 TSM 数据库进行大小调整，以保留对要写入归档节点的所有对象的引用。
- 归档节点软件不能容忍将对象直接写入磁带或其他可移动介质所涉及的延迟。因此，无论何时使用可移动介质， TSM 服务器都必须配置一个磁盘存储池，用于初始存储归档节点保存的数据。
- 您必须配置 TSM 保留策略，以使用基于事件 - 的保留。归档节点不支持基于创建的 TSM 保留策略。在保留策略中使用以下建议设置 remin=0 和 rever=0 （这表示保留从归档节点触发保留事件时开始，并在此之后保留 0 天）。但是， remin 和 rever 的这些值是可选的。

必须对磁盘池进行配置，以便将数据迁移到磁带池（即，磁带池必须是磁盘池的 NXTSTGPOOL ）。不能将磁带池配置为磁盘池的副本池，并同时向两个池写入数据（即，磁带池不能是磁盘池的 COPYSTGPOOL ）。要为包含归档节点数据的磁带创建脱机副本，请为 TSM 服务器配置第二个磁带池，该磁带池是用于归档节点数据的磁带池的副本池。

完成归档节点设置

完成安装过程后，归档节点无法正常运行。在 StorageGRID 系统将对象保存到 TSM 归档节点之前，您必须完成 TSM 服务器的安装和配置，并配置归档节点以与 TSM 服务器进行通信。

在准备 TSM 服务器以便与 StorageGRID 系统中的归档节点集成时，请根据需要参考以下 IBM 文档：

- "《 IBM 磁带设备驱动程序安装和用户指南》"
- "《 IBM 磁带设备驱动程序编程参考》"

安装新的 **TSM** 服务器

您可以将归档节点与新的或现有的 TSM 服务器集成在一起。如果要安装新的 TSM 服务器，请按照 TSM 文档中的说明完成安装。

归档节点不能与 TSM 服务器托管。

配置 **TSM** 服务器

本节介绍了按照 TSM 最佳实践准备 TSM 服务器的示例说明。

以下说明将指导您完成以下过程：

- 在 TSM 服务器上定义磁盘存储池和磁带存储池（如果需要）
- 为从归档节点保存的数据定义使用 TSM 管理类的域策略，并注册节点以使用此域策略

这些说明仅供您参考；它们并不是为了取代 TSM 文档，也不是为了提供适用于所有配置的完整而全面的说明。应由熟悉您的详细要求和一整套 TSM Server 文档的 TSM 管理员提供部署特定的说明。

定义 **TSM** 磁带和磁盘存储池

归档节点将写入磁盘存储池。要将内容归档到磁带，必须配置磁盘存储池以将内容移动到磁带存储池。

关于此任务

对于 TSM 服务器，您必须在 Tivoli Storage Manager 中定义磁带存储池和磁盘存储池。定义磁盘池后，创建一个磁盘卷并将其分配给磁盘池。如果您的 TSM 服务器仅使用磁盘 - 存储，则不需要磁带池。

您必须先在 TSM 服务器上完成多个步骤，然后才能创建磁带存储池。（在磁带库中创建一个磁带库和至少一个驱动器。定义从服务器到库以及从服务器到驱动器的路径，然后为驱动器定义设备类。） 根据站点的硬件配置和存储要求，这些步骤的详细信息可能会有所不同。有关详细信息，请参见 TSM 文档。

以下一组说明说明了此过程。请注意，根据部署要求，您的站点可能会有所不同。有关配置详细信息和说明，请参见 TSM 文档。

您必须使用管理权限登录到服务器，并使用 dsmadc 工具执行以下命令。

步骤

1. 创建磁带库。

   ```
   define library tapelibre libtype=SCSI
   ```

   其中，` *tapeliborle*` 是为磁带库选择的任意名称， `libtype` 的值可能因磁带库类型而异。

2. 定义从服务器到磁带库的路径。

   ```
   define path servername tapelibre srctype=server desttype=library device=lib-
   devicename
   ```

   - ` servername_` 是 TSM 服务器的名称
   - ` *tapeliborle*` 是您定义的磁带库名称
   - ` *lib-devicename*` 是磁带库的设备名称

3. 为库定义驱动器。

```
define drive tapelibre drivename
```

- ` *drivename*` 是要为驱动器指定的名称
- ` *tapeliborle*` 是您定义的磁带库名称

  根据您的硬件配置，您可能需要配置一个或多个驱动器。（例如，如果 TSM 服务器连接到一个光纤通道交换机，而该交换机具有来自磁带库的两个输入，则您可能需要为每个输入定义一个驱动器。）

4. 定义从服务器到您定义的驱动器的路径。

```
define path servername drivename srctype=server desttype=drive
library=tapelibre device=drive-dname
```

- ` drive-dname_` 是驱动器的设备名称
- ` *tapeliborle*` 是您定义的磁带库名称

  对为磁带库定义的每个驱动器重复上述步骤，对每个驱动器使用单独的 ` 驱动器名称 ` 和 ` 驱动器 *-dname*` 。

5. 为驱动器定义设备类。

```
define devclass DeviceClassName devtype=LTO library=tapelibre format=tapettype
```

- ` *DeviceClassName*` 是设备类的名称
- ` lod_` 是连接到服务器的驱动器类型
- ` *tapeliborle*` 是您定义的磁带库名称
- ` *tapettype*` 是磁带类型；例如 ultrium3

6. 将磁带卷添加到库的清单中。

   签入 `libvolume tapelibaler`

   ` *tapeliborle*` 是您定义的磁带库名称。

7. 创建主磁带存储池。

```
define stgpool SGWSTapePool _ _DeviceClassName description=description
m2ate=filespace_maxscrating=_XX
```

- ` *SGWSTapePool*` 是归档节点的磁带存储池的名称。您可以为磁带存储池选择任何名称（只要该名称使用 TSM 服务器预期的语法约定）。
- ` *DeviceClassName*` 是磁带库的设备类名称。
- ` *TSM*` 是存储池的问题描述 ，可使用 `query stgpool` 命令显示在问题描述 服务器上。例如： "`归档节点的磁带存储池。` "
- ` *cowate=filespace*` 指定 TSM 服务器应将同一文件空间中的对象写入单个磁带。
- XX 是以下项之一：
  - 磁带库中的空磁带数量（如果归档节点是唯一使用该库的应用程序）。

- 分配给 StorageGRID 系统使用的磁带数量（在共享磁带库的情况下）。

8. 在 TSM 服务器上，创建磁盘存储池。在 TSM 服务器的管理控制台中，输入

```
define stgpool SGWSDiskPool _ disk description=_description
maxsize=max_file_size nextstgpool=SGWSTapePool _ highmig=_percent_high
lowmig=percent_low
```

   - ` _SGWSDiskPool` 是归档节点磁盘池的名称。您可以为磁盘存储池选择任何名称（只要该名称使用 TSM 预期的语法约定）。
   - ` *TSM*` 是存储池的问题描述 ，可使用 `query stgpool` 命令显示在问题描述 服务器上。例如， " 为归档节点设置 `D` 存储池。 "
   - ` max_max_file_size_` 强制将大于此大小的对象直接写入磁带，而不是缓存在磁盘池中。建议将 ` 最大文件大小 _` 设置为 10 GB 。
   - ` nextstgpool=SGWSTapePool_` 将磁盘存储池引用为归档节点定义的磁带存储池。
   - ` *percent_high*` 设置磁盘池开始将其内容迁移到磁带池的值。建议将 ` *percent_high*` 设置为 0 ，以便立即开始数据迁移
   - ` *percent_low*` 设置停止迁移到磁带池的值。建议将 ` *percent_low*` 设置为 0 以清除磁盘池。

9. 在 TSM 服务器上，创建一个或多个磁盘卷并将其分配给磁盘池。

```
define volume SGWSDiskPool _ _volume_name formatsize=size
```

   - ` _SGWSDiskPool` 是磁盘池名称。
   - ` volume_name_` 是 TSM 服务器上卷位置的完整路径（例如， ` /var/local/arc/stage6.DSM` ），在此服务器上，它会写入磁盘池的内容，以便为传输到磁带做好准备。
   - ` size_` 是磁盘卷的大小，以 MB 为单位。

     例如，要创建一个磁盘卷，使磁盘池的内容填满一个磁带，请在磁带卷的容量为 200 GB 时将大小值设置为 200 ， 000 。

     但是，可能需要创建多个较小大小的磁盘卷，因为 TSM 服务器可以向磁盘池中的每个卷写入数据。例如，如果磁带大小为 250 GB ，请创建 25 个磁盘卷，每个卷的大小为 10 GB （ 10000 ）。

TSM 服务器会在目录中为磁盘卷预先分配空间。此操作可能需要一段时间才能完成（对于 200 GB 磁盘卷，需要三个多小时）。

定义域策略并注册节点

您需要为从归档节点保存的数据定义一个使用 TSM 管理类的域策略，然后注册一个节点以使用此域策略。

如果 Tivoli Storage Manager （ TSM ）中归档节点的客户端密码过期，则归档节点进程可能会泄漏内存。确保已配置 TSM 服务器，以便归档节点的客户端用户名 / 密码永不过期。

在 TSM 服务器上注册节点以使用归档节点（或更新现有节点）时，必须通过在注册节点命令中指定 MAXNUMMP 参数来指定节点可用于写入操作的挂载点数量。挂载点的数量通常等于分配给归档节点的磁带驱动器头的数量。在 TSM 服务器上为 MAXNUMMP 指定的数量必须至少与为归档节点的 * ARC* > * 目标 * > * 配

置 * > * 主 * > * 最大存储会话 * 设置的值相同。 该值设置为 0 或 1 ，因为归档节点不支持并发存储会话。

为 TSM 服务器设置的 MaxSessions 值用于控制所有客户端应用程序可向 TSM 服务器打开的最大会话数。在 TSM 上指定的 MaxSessions 值必须至少与在网格管理器中为归档节点指定的 * ARC* > * 目标 * > * 配置 * > * 主 * > * 会话数 * 的值相同。归档节点会同时为每个挂载点最多创建一个会话，并另外创建少量（ < 5 ）个会话。

分配给归档节点的 TSM 节点使用自定义域策略 `TSM-domain` 。`TSM-domain` 域策略是 "tandard` " 域策略的修改版本，配置为写入磁带，并将归档目标设置为 StorageGRID 系统的存储池（` _SGWSDiskPool s ）。

您必须使用管理权限登录到 TSM 服务器，并使用 dsmadc 工具创建和激活域策略。

创建并激活域策略

您必须创建一个域策略，然后将其激活，以配置 TSM 服务器以保存从归档节点发送的数据。

步骤

1. 创建域策略。

   复制域标准 `TSM-DOMAIN`

2. 如果您使用的不是现有管理类，请输入以下内容之一：

   ```
   define policySet TSM-domain standard

   define mgmtclass tsm-domain standard _default_m
   ```

   ` 默认 _` 是部署的默认管理类。

3. 创建一个副本组到相应的存储池。在一行中输入：

   ```
   define copygroup Tsm-domain standard defaults type=archive
   destination=SGWSDiskPool reinit=event remin=0 rever=0
   ```

   ` *default*` 是归档节点的默认管理类。已选择 `retinit` ， `retmin` 和 `reTver` 的值，以反映归档节点当前使用的保留行为

   请勿将 `retinit` 设置为 `retinit = create` 。设置 `retinit = create` 会阻止归档节点删除内容，因为保留事件用于从 TSM 服务器中删除内容。

4. 将管理类分配为默认值。

   ```
   assign defmgmtclass TSM-domain standard _default_s
   ```

5. 将新策略集设置为活动。

   激活 `policySet TSM-domain standard`

   请忽略输入 activate 命令时显示的 "`no backup copy group` " 警告。

6. 注册一个节点以使用在 TSM 服务器上设置的新策略。在 TSM 服务器上，输入（在一行上）：

re注册节点 arc-user arc-password passexp=0 domain=Tsm-domain MAXNUMMP=number-in-sessions

arc-user 和 arc-password 与您在归档节点上定义的客户端节点名称和密码相同，并且 MAXNUMMP 的值设置为为归档节点存储会话预留的磁带驱动器数量。

默认情况下，注册节点会创建一个由客户端所有者授权的管理用户 ID ，并为此节点定义密码。

将数据迁移到 StorageGRID

您可以将大量数据迁移到 StorageGRID 系统，同时使用 StorageGRID 系统执行日常操作。

下一节将指导您了解并规划将大量数据迁移到 StorageGRID 系统。本指南不是数据迁移的通用指南，也不包括执行迁移的详细步骤。请遵循本节中的准则和说明，确保在不影响日常操作的情况下将数据高效迁移到 StorageGRID 系统中，并确保 StorageGRID 系统能够正确处理迁移的数据。

确认 **StorageGRID** 系统的容量

在将大量数据迁移到 StorageGRID 系统之前，请确认 StorageGRID 系统具有处理预期卷所需的磁盘容量。

如果 StorageGRID 系统包含归档节点，并且已将迁移对象的副本保存到近线存储（例如磁带）中，请确保归档节点的存储具有足够的容量来容纳所迁移数据的预期卷。

在容量评估过程中，请查看计划迁移的对象的数据配置文件，并计算所需的磁盘容量。有关监控 StorageGRID 系统磁盘容量的详细信息，请参见 管理存储节点 和 监控和故障排除。

确定已迁移数据的 **ILM** 策略

StorageGRID 系统的 ILM 策略可确定创建的副本数，副本存储到的位置以及这些副本的保留时间。ILM 策略由一组 ILM 规则组成，这些规则介绍如何筛选对象以及如何随着时间的推移管理对象数据。

根据迁移数据的使用方式以及迁移数据的要求，您可能需要为迁移的数据定义与日常操作所使用的 ILM 规则不同的唯一 ILM 规则。例如，如果日常数据管理的法规要求与迁移中包含的数据的法规要求不同，则您可能需要在不同级别的存储上为迁移的数据创建不同数量的副本。

如果可以唯一区分已迁移数据和通过日常操作保存的对象数据，则可以配置专用于已迁移数据的规则。

如果您可以使用元数据条件之一可靠地区分数据类型，则可以使用此条件定义仅适用于已迁移数据的 ILM 规则。

在开始数据迁移之前，请确保您了解 StorageGRID 系统的 ILM 策略及其如何应用于迁移的数据，并且已对 ILM 策略进行了更改并进行了测试。请参见 使用 ILM 管理对象。

如果未正确指定 ILM 策略发生原因 ，则可能会导致无法恢复的数据丢失。在激活 ILM 策略之前，请仔细查看对该策略所做的所有更改，以确保该策略按预期运行。

迁移对操作的影响

StorageGRID 系统旨在为对象存储和检索提供高效操作，并通过无缝创建对象数据和元数据的冗余副本提供出色的数据保护，防止数据丢失。

但是，必须按照本章中的说明仔细管理数据迁移，以避免对日常系统操作造成影响，或者在极端情况下，在 StorageGRID 系统发生故障时使数据面临丢失风险。

迁移大量数据会给系统带来额外的负载。当 StorageGRID 系统负载过重时，它对存储和检索对象的请求响应速度较慢。这可能会干扰日常操作不可或缺的存储和检索请求。迁移还可以发生原因 解决其他操作问题。例如，当存储节点接近容量时，由于批量载入而产生的大量间歇性负载可以对存储节点进行发生原因 ，使其在只读和读写之间循环，从而生成通知。

如果负载仍然繁重，则可以为 StorageGRID 系统必须执行的各种操作开发队列，以确保对象数据和元数据完全冗余。

必须按照本文档中的准则仔细管理数据迁移，以确保 StorageGRID 系统在迁移期间安全高效地运行。迁移数据时，请批量载入对象或持续限制载入。然后，持续监控 StorageGRID 系统，以确保不超过各种属性值。

计划和监控数据迁移

必须根据需要计划和监控数据迁移，以确保在所需时间内根据 ILM 策略放置数据。

计划数据迁移

避免在核心运行时间迁移数据。将数据迁移限制为晚上，周末以及系统使用率较低的其他时间。

如果可能，请勿在活动频繁期间计划数据迁移。但是，如果完全避免高活动期限不可行，只要您密切监控相关属性并在其超过可接受值时采取措施，就可以安全地继续操作。

监控数据迁移

此表列出了在数据迁移期间必须监控的属性及其所代表的问题。

如果您使用具有速率限制的流量分类策略来限制载入，则可以结合下表所述的统计信息来监控观察到的速率，并根据需要降低这些限制。

监控	**Description**
等待 ILM 评估的对象数量	1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 2. 选择 * ； deployment_* > * 概述 * > * 主要 * 。 3. 在 "ILM Activity" 部分中，监控为以下属性显示的对象数量： ◦ * 正在等待 - 全部（ XQUZ ） *： 等待 ILM 评估的对象总数。 ◦ * 正在等待 - 客户端（ XQZ ） *： 等待通过客户端操作（例如载入）进行 ILM 评估的对象总数。 4. 如果为其中任一属性显示的对象数量超过 100 ， 000 个，请限制对象的载入速率，以减少 StorageGRID 系统上的负载。

监控	Description
目标归档系统的存储容量	如果 ILM 策略将已迁移数据的副本保存到目标归档存储系统（磁带或云），请监控目标归档存储系统的容量，以确保已迁移数据具有足够的容量。
• 归档节点 * > * ARC/ * 存储 *	如果触发了针对 * 存储故障（ ARVF ） * 属性的警报，则目标归档存储系统可能已达到容量。检查目标归档存储系统并解决触发警报的任何问题。

使用 ILM 管理对象

使用 ILM 管理对象：概述

您可以通过配置信息生命周期管理（ ILM ）规则和策略来管理 StorageGRID 系统中的对象。ILM 规则和策略指示 StorageGRID 如何创建和分发对象数据的副本，以及如何随着时间的推移管理这些副本。

关于这些说明

设计和实施 ILM 规则和 ILM 策略需要仔细规划。您必须了解操作要求， StorageGRID 系统的拓扑结构，对象保护需求以及可用存储类型。然后，您必须确定希望如何复制，分发和存储不同类型的对象。

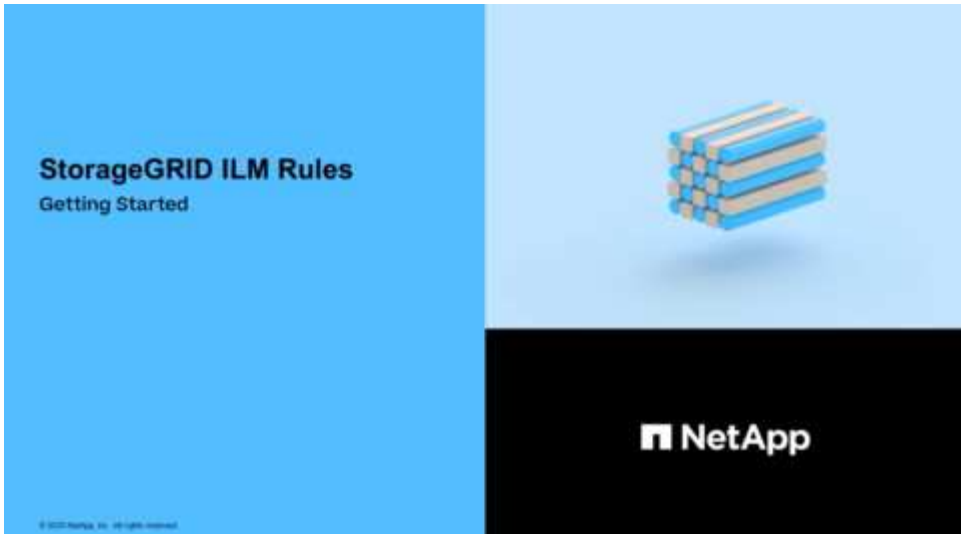
按照以下说明执行以下操作：

- 了解 StorageGRID ILM ，包括 ILM 如何在对象的整个生命周期内运行以及 ILM 策略和规则是什么。
- 了解如何配置存储池，擦除编码配置文件和 ILM 规则。
- 了解如何创建和激活 ILM 策略以保护一个或多个站点上的对象数据。
- 了解如何使用 S3 对象锁定管理对象，这有助于确保特定 S3 分段中的对象在指定时间内不会被删除或覆盖。

了解更多信息。

要了解更多信息，请查看以下视频：

- "视频： StorageGRID ILM 规则：入门"



- "视频： StorageGRID ILM 策略"

ILM 和对象生命周期

ILM 如何在对象的整个生命周期内运行

了解 StorageGRID 如何在对象生命周期的每个阶段使用 ILM 管理对象，有助于您设计更有效的策略。

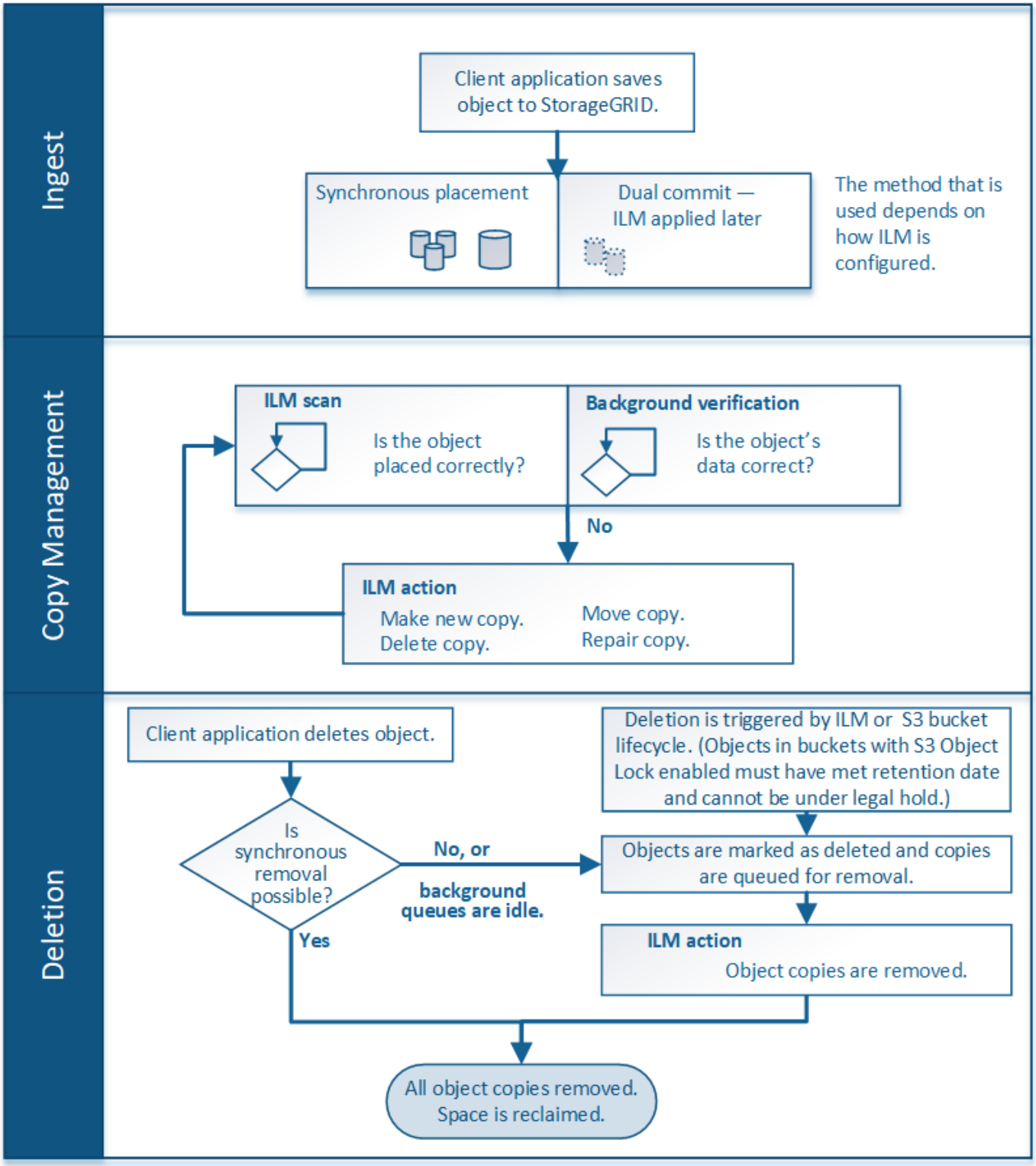
- * 载入 * ： 当 S3 或 Swift 客户端应用程序建立连接以将对象保存到 StorageGRID 系统时，载入开始；当 StorageGRID 向客户端返回 "`ingest successful` " 消息时，载入完成。根据 ILM 要求的指定方式，在载入期间通过立即应用 ILM 指令（同步放置）或创建临时副本并稍后应用 ILM （双提交）来保护对象数据。
- * 副本管理 * ： 创建 ILM 放置说明中指定的对象副本数量和类型后， StorageGRID 可管理对象位置并防止对象丢失。
  - ILM 扫描和评估： StorageGRID 会持续扫描网格中存储的对象列表，并检查当前副本是否符合 ILM 要求。如果需要不同类型，数字或位置的对象副本， StorageGRID 会根据需要创建，删除或移动副本。
  - 后台验证： StorageGRID 持续执行后台验证以检查对象数据的完整性。如果发现问题， StorageGRID 会自动在满足当前 ILM 要求的位置创建一个新的对象副本或替换的擦除编码对象片段。请参见的说明 监

控 StorageGRID 并对其进行故障排除。

- * 对象删除 * ： 从 StorageGRID 系统中删除所有副本后，对象管理将结束。可以根据客户端的删除请求删除对象，也可以通过 ILM 删除对象或因 S3 存储分段生命周期到期而删除对象。

> 如果已启用 S3 对象锁定的存储分段中的对象处于合法保留状态，或者已指定保留日期但尚未满足，则无法删除这些对象。

该图总结了 ILM 在对象的整个生命周期中的运行方式。



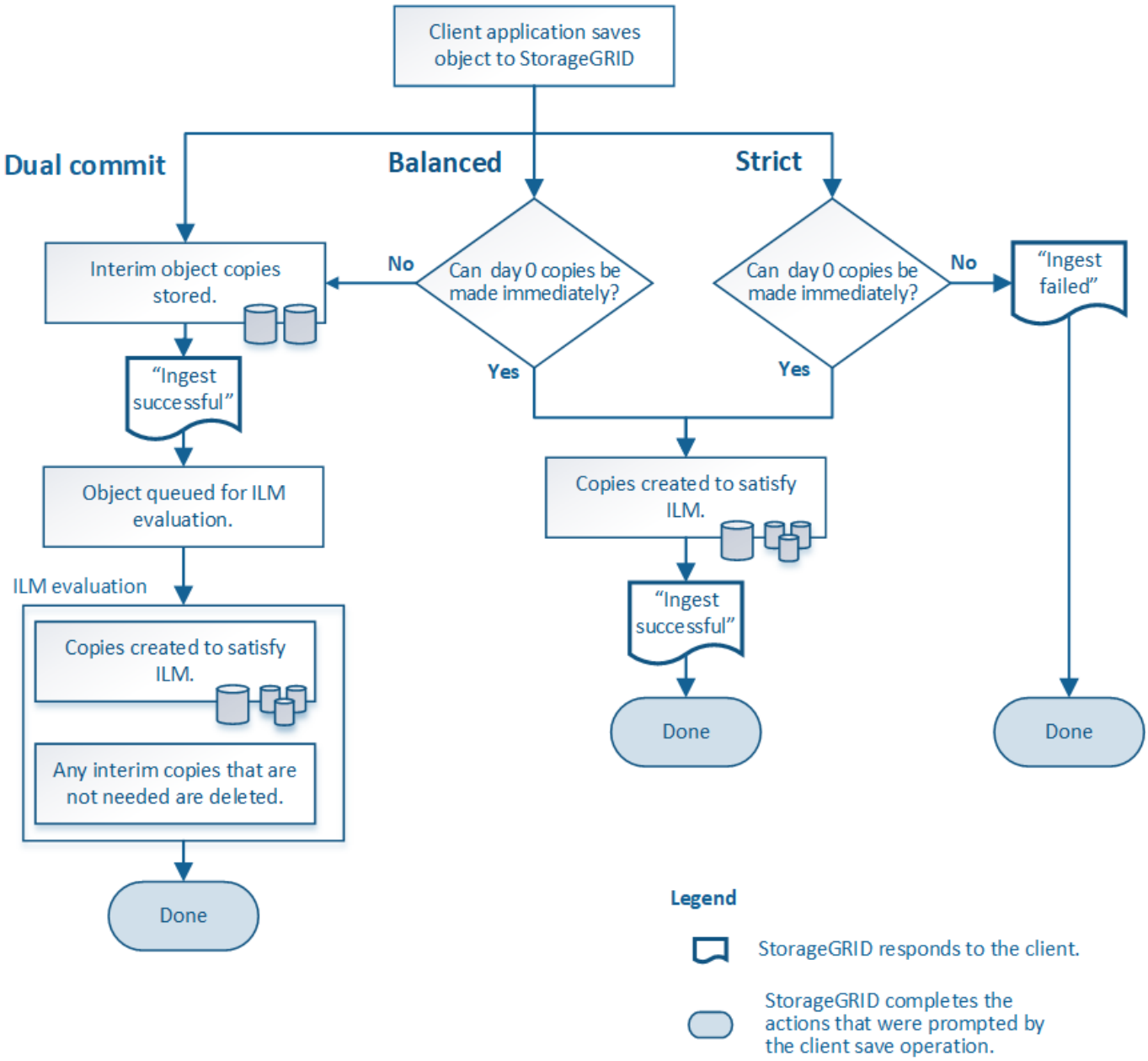
如何载入对象

用于载入的数据保护选项

创建 ILM 规则时，您可以指定以下三个选项之一来在载入时保护对象：双提交，平衡或严格。根据您的选择， StorageGRID 会创建临时副本并将对象排队，以便稍后进行 ILM 评估，或者使用同步放置并立即创建副本以满足 ILM 要求。

三个载入选项的流程图

此流程图显示了在对象与 ILM 规则匹配时会发生的情况，该规则使用三个载入选项中的每一个选项。



双提交

选择双提交选项后， StorageGRID 会立即在两个不同的存储节点上创建临时对象副本，并向客户端返回 "`ingest successful` " 消息。对象将排队等待 ILM 评估，满足规则放置说明的副本将在稍后创建。

何时使用双提交选项

在以下任一情况下，请使用双提交选项：

- 您正在使用多站点 ILM 规则，客户端载入延迟是您的主要考虑因素。使用双提交时，您必须确保网格可以在不满足 ILM 要求的情况下执行创建和删除双提交副本的额外工作。具体而言：

- 网格上的负载必须足够低，以防止 ILM 积压。
- 网格必须具有多余的硬件资源（ IOPS ， CPU ，内存，网络带宽等）。

- 您正在使用多站点 ILM 规则，并且站点之间的 WAN 连接通常具有较高的延迟或有限的带宽。在这种情况下，使用双提交选项有助于防止客户端超时。在选择双提交选项之前，您应使用实际工作负载测试客户端应用程序。

严格

如果选择 strict 选项，则 StorageGRID 会在载入时使用同步放置，并立即创建规则放置说明中指定的所有对象副本。如果 StorageGRID 无法创建所有副本，则载入将失败，例如，因为所需存储位置暂时不可用。客户端必须重试此操作。

何时使用 **strict** 选项

如果您在操作或法规要求中要求仅将对象立即存储在 ILM 规则中所述的位置，请使用 strict 选项。例如，要满足法规要求，您可能需要使用 strict 选项和 Location Constrict 高级筛选器来保证对象永远不会存储在特定数据中心。

示例 5： 用于严格载入行为的 ILM 规则和策略

平衡

选择 Balified 选项时， StorageGRID 还会在载入时使用同步放置，并立即创建规则放置说明中指定的所有副本。与 strict 选项不同，如果 StorageGRID 无法立即创建所有副本，则会改用双提交。

何时使用平衡选项

使用平衡选项可实现数据保护，网格性能和载入成功的最佳组合。平衡是 ILM 规则向导中的默认选项。

数据保护选项的优势，劣势和限制

了解在载入时保护数据的三个选项（平衡，严格或双重提交）中每一个选项的优缺点有助于您确定要为 ILM 规则选择哪个选项。

平衡而严格的选项的优势

与在载入期间创建临时副本的双提交相比，这两个同步放置选项具有以下优势：

- * 更好的数据安全性 * ： 对象数据会按照 ILM 规则放置说明中的说明立即受到保护，可以对其进行配置，以防止出现多种故障情况，包括多个存储位置发生故障。双提交只能防止丢失一个本地副本。
- * 更高效的网格操作 * ： 每个对象仅在载入时进行一次处理。由于 StorageGRID 系统不需要跟踪或删除中间副本，因此处理负载较低，数据库空间占用较少。
- * （平衡）建议 * ： 平衡选项可提供最佳 ILM 效率。除非需要严格的载入行为或网格满足用于双提交的所有标准，否则建议使用 balancired 选项。
- * （严格）对象位置的确定性 * ： strict 选项可确保根据 ILM 规则中的放置说明立即存储对象。

平衡而严格的选项的缺点

与双提交相比，平衡和严格选项存在一些缺点：

- * 客户端载入时间更长 *： 客户端载入延迟可能更长。使用平衡和严格的选项时，在创建和存储所有纠删编码的片段或复制的副本之前，不会向客户端返回 "`ingest successful` " 消息。但是，对象数据很可能会更快地到达最终放置位置。
- * （严格）更高的载入失败率 *： 使用 strict 选项时，只要 StorageGRID 无法立即创建 ILM 规则中指定的所有副本，载入就会失败。如果所需存储位置暂时脱机或网络问题发生原因 在站点之间复制对象时出现延迟，则可能会出现较高的载入失败率。
- 在某些情况下 *（严格） S3 多部分上传放置可能与预期不同 *： 严格地说，您希望对象按照 ILM 规则的说明放置，或者载入操作失败。但是，如果使用 S3 多部分上传，则会在载入对象时对 ILM 的每个部分进行评估，并在多部分上传完成后对整个对象进行评估。在以下情况下，这可能会导致放置方式与您预期不同：
  - * 如果在 S3 多部件上传过程中 ILM 发生变化 *： 由于每个部件都是根据在载入部件时处于活动状态的规则放置的，因此在多部件上传完成后，对象的某些部分可能不符合当前的 ILM 要求。在这些情况下，对象的载入不会失败。相反，未正确放置的任何部件将排队等待 ILM 重新评估，并稍后移动到正确的位置。
  - * 当 ILM 规则按大小筛选时 *： 在评估某个部件的 ILM 时， StorageGRID 会按部件的大小进行筛选，而不是按对象的大小进行筛选。这意味着，对象的某些部分可以存储在不满足整个对象的 ILM 要求的位置。例如，如果规则指定所有 10 GB 或更大的对象都存储在 DC1 中，而所有较小的对象存储在 DC2 中，则在载入时， 10 部分多部分上传的每个 1 GB 部分都存储在 DC2 中。评估对象的 ILM 时，对象的所有部分都会移至 DC1 。
- * （严格）更新对象标记或元数据后，如果无法进行新要求的放置，则载入不会失败 *： 严格地说，您希望按照 ILM 规则的说明放置对象，或者使载入失败。但是，在更新网格中已存储的对象的元数据或标记时，不会重新载入该对象。这意味着，更新触发的任何对象放置更改都不会立即进行。如果通过正常后台 ILM 流程重新评估 ILM ，则会进行放置更改。如果无法进行所需的放置更改（例如，由于新需要的位置不可用），则更新后的对象将保留其当前放置位置，直到可以进行放置更改为止。

具有平衡或严格选项的对象放置限制

对于具有以下任一放置说明的 ILM 规则，不能使用平衡或严格选项：

- 第 0 天放置在云存储池中。
- 在第 0 天放置在归档节点中。
- 当规则将用户定义的创建时间作为参考时间时，将放置在云存储池或归档节点中。

之所以存在这些限制，是因为 StorageGRID 无法同步向云存储池或归档节点创建副本，并且用户定义的创建时间可以解决为当前问题。

ILM 规则和一致性控制如何交互以影响数据保护

ILM 规则和一致性控制选项都会影响对象的保护方式。这些设置可以进行交互。

例如，为 ILM 规则选择的载入行为会影响对象副本的初始放置，而存储对象时使用的一致性控制则会影响对象元数据的初始放置。由于 StorageGRID 需要访问对象的元数据及其数据来满足客户端请求，因此为一致性级别和载入行为选择匹配的保护级别可以提供更好的初始数据保护和更可预测的系统响应。

下面简要总结了 StorageGRID 中提供的一致性控制：

- * 全部 *： 所有节点均立即接收对象元数据，否则请求将失败。
- * 强 - 全局 *： 对象元数据会立即分发到所有站点。保证所有站点中所有客户端请求的写入后读一致性。
- * 强站点 *： 对象元数据会立即分发到站点上的其他节点。保证站点内所有客户端请求的写入后读一致性。

- * 读后新写入 * ： 为新对象提供读后写入一致性，并最终为对象更新提供一致性。提供高可用性和数据保护保证。
- * 可用 * （机头操作的最终一致性）： 与 `read-after-new-write` 一致性级别相同，但仅为机头操作提供最终一致性。

> 在选择一致性级别之前，请阅读的说明中的完整一致性控制问题描述 S3 或 Swift 客户端应用程序。在更改默认值之前，您应了解其优势和限制。

一致性控制和 **ILM** 规则如何交互的示例

假设您有一个双站点网格，其中包含以下 ILM 规则和以下一致性级别设置：

- * ILM 规则 * ： 创建两个对象副本，一个在本地站点，一个在远程站点。此时将选择严格的载入行为。
- * 一致性级别 * ： `strong-global` （对象元数据会立即分发到所有站点。）

当客户端将对象存储到网格时， StorageGRID 会创建两个对象副本并将元数据分发到两个站点，然后再向客户端返回成功。

在载入成功消息时，此对象将受到完全保护，不会丢失。例如，如果本地站点在载入后不久丢失，则远程站点上仍存在对象数据和对象元数据的副本。此对象完全可检索。

如果您改用相同的 ILM 规则和 `strong-site` 一致性级别，则在将对象数据复制到远程站点之后，在将对象元数据分发到该远程站点之前，客户端可能会收到一条成功消息。在这种情况下，对象元数据的保护级别与对象数据的保护级别不匹配。如果本地站点在载入后不久丢失，则对象元数据将丢失。无法检索此对象。

一致性级别和 ILM 规则之间的关系可能很复杂。如需帮助，请联系 NetApp 。

相关信息

- 示例 5： 用于严格载入行为的 ILM 规则和策略

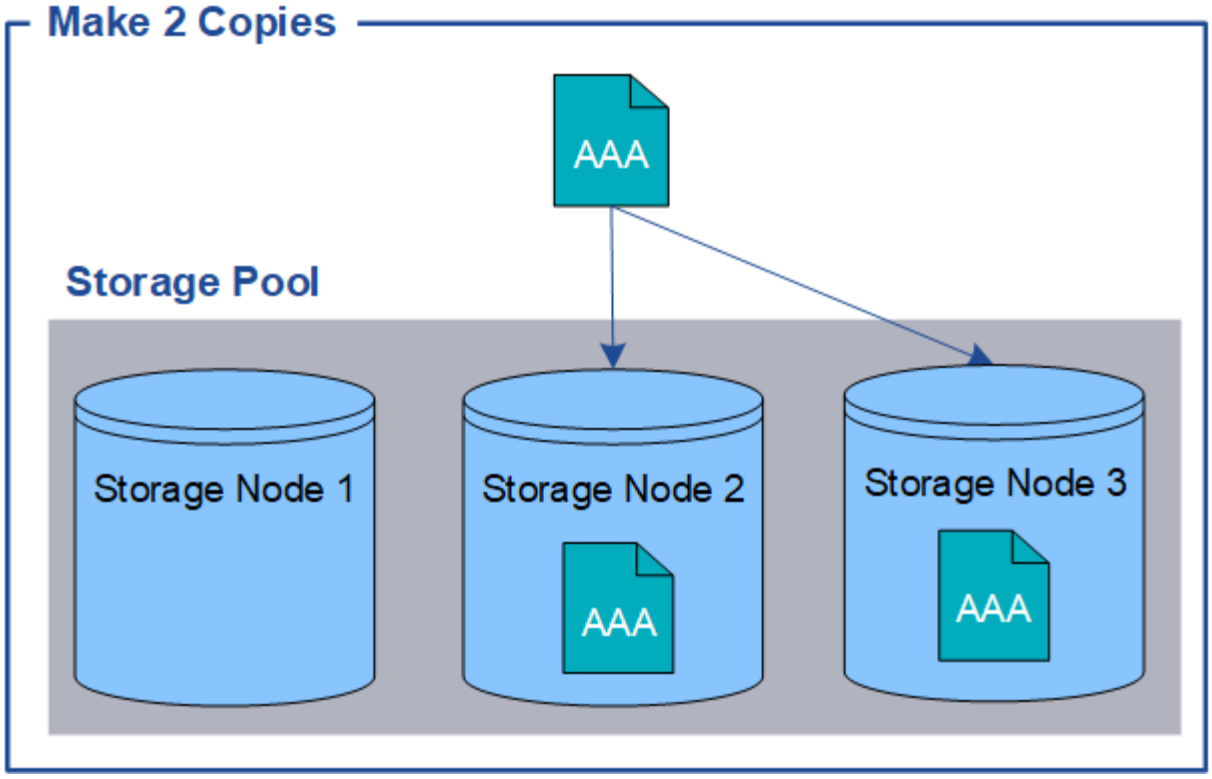
对象的存储方式（复制或纠删编码）

什么是复制

复制是 StorageGRID 用于存储对象数据的两种方法之一。当对象与使用复制的 ILM 规则匹配时，系统会为对象数据创建精确副本，并将这些副本存储在存储节点或归档节点上。

在配置创建复制副本的 ILM 规则时，您可以指定应创建多少个副本，这些副本应放置在何处以及应将这些副本存储在每个位置的时间长度。

在以下示例中， ILM 规则指定将每个对象的两个复制副本放置在包含三个存储节点的存储池中。



当 StorageGRID 将对象与此规则匹配时，它会为该对象创建两个副本，并将每个副本放置在存储池中的不同存储节点上。这两个副本可以放置在三个可用存储节点中的任意两个上。在这种情况下，规则会将对象副本放置在存储节点 2 和 3 上。由于有两个副本，因此，如果存储池中的任何节点出现故障，可以检索此对象。

> StorageGRID 只能在任何给定存储节点上存储一个对象的一个复制副本。如果您的网格包含三个存储节点，并且您创建了一个 4 副本 ILM 规则，则只会创建三个副本—每个存储节点一个副本。系统将触发 * 无法实现 ILM 放置 * 警报，以指示无法完全应用 ILM 规则。

相关信息

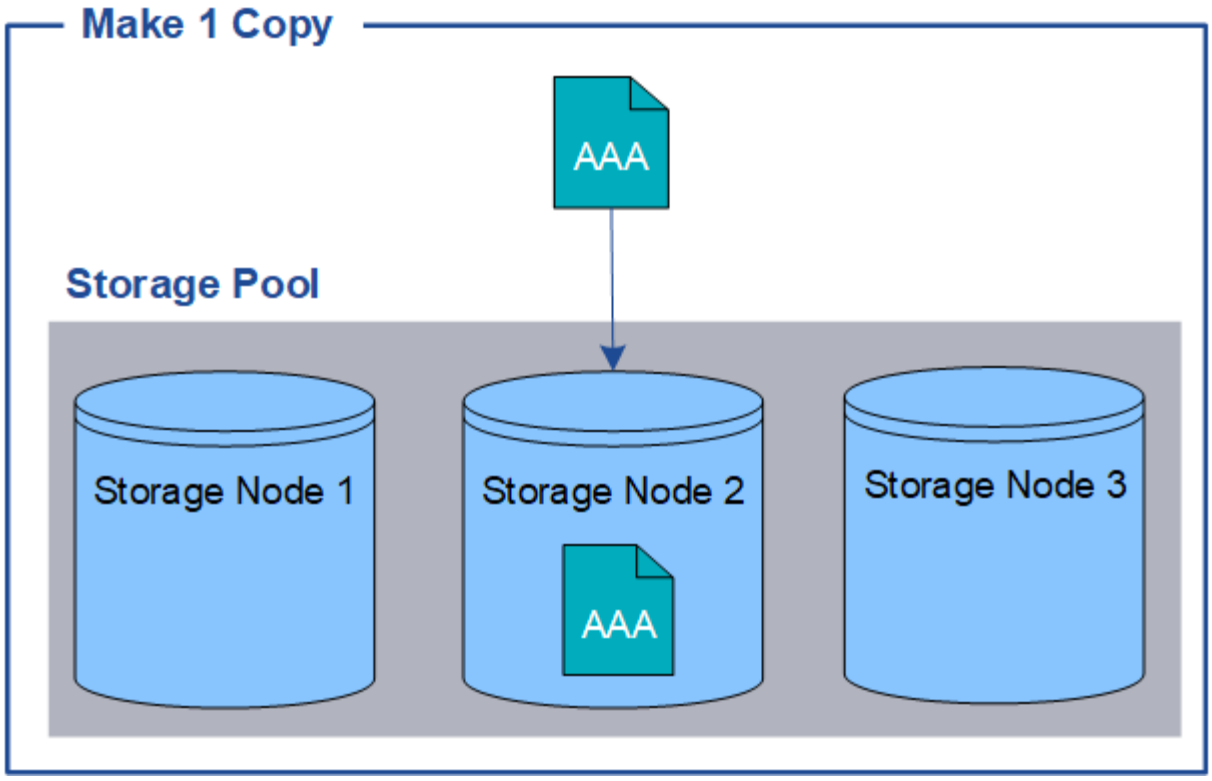
- 什么是存储池
- 使用多个存储池进行跨站点复制

为什么不应使用单副本复制

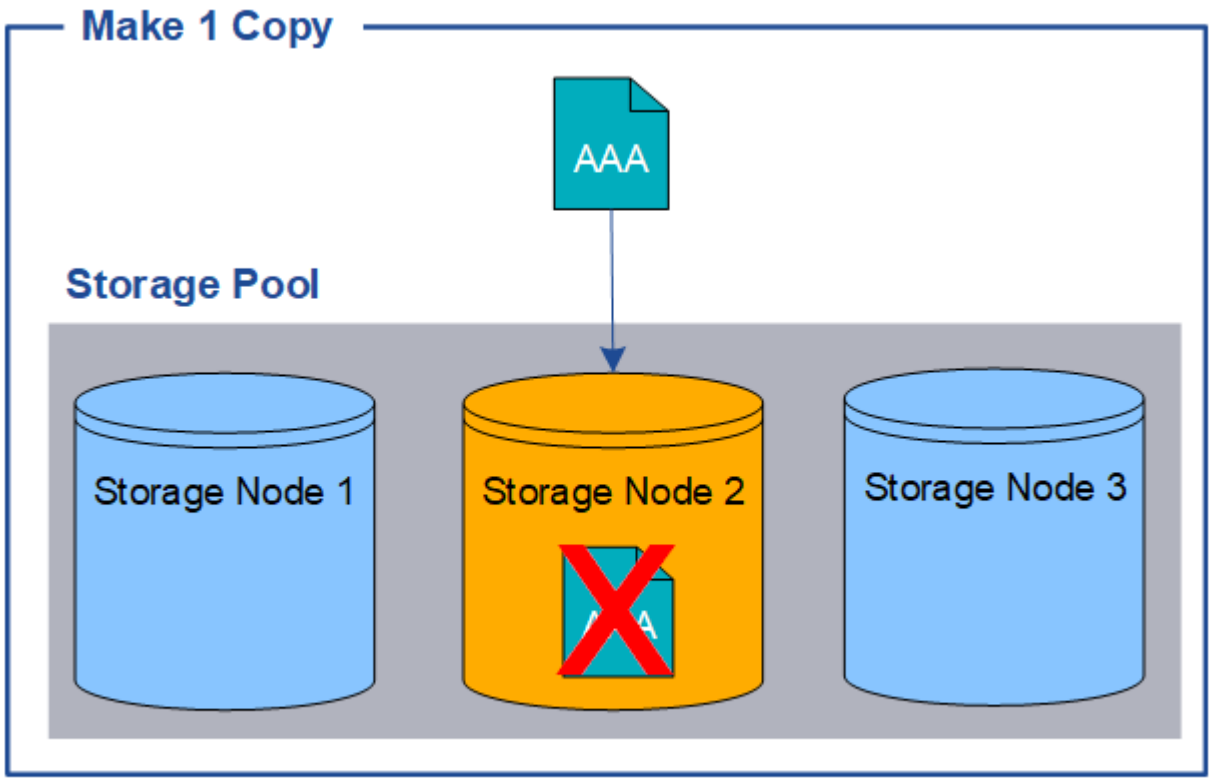
在创建 ILM 规则以创建复制副本时，您应始终在放置说明中指定至少两个副本，以便在任意时间段内使用。

> 请勿使用仅在任意时间段创建一个复制副本的 ILM 规则。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

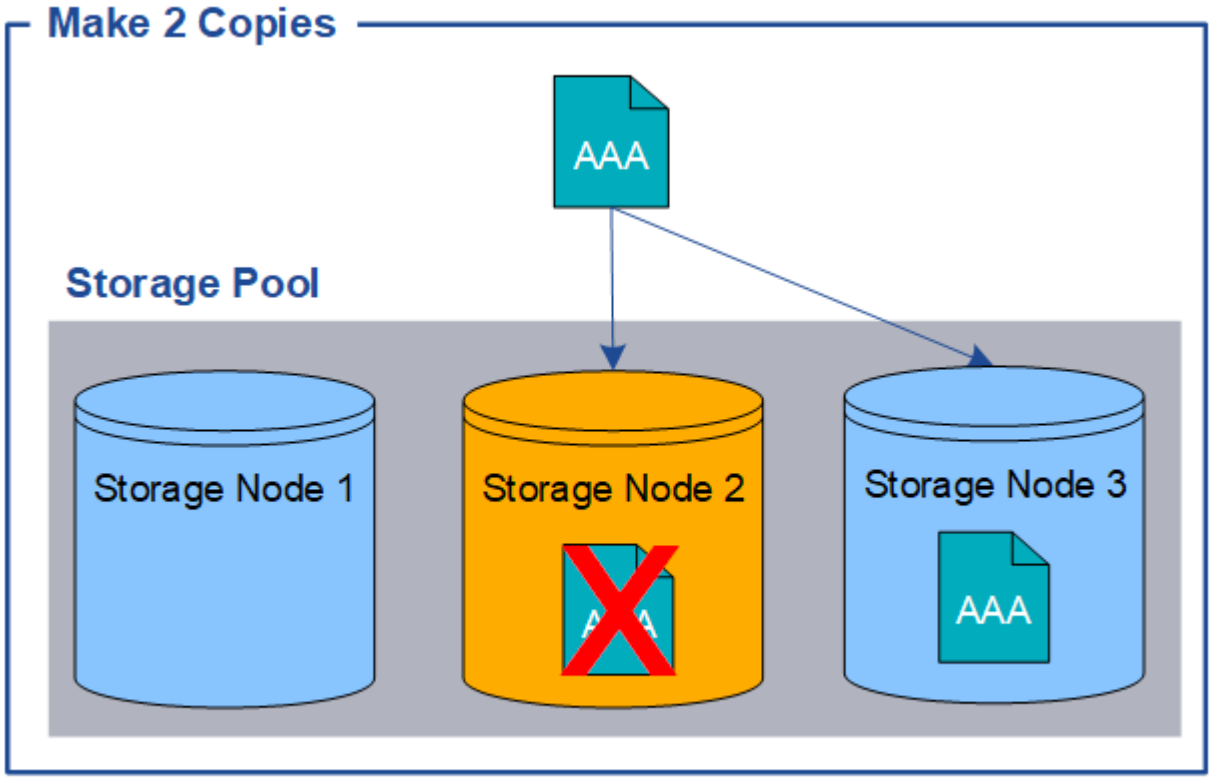
在以下示例中， Make 1 Copy ILM 规则指定将对象的一个复制副本放置在包含三个存储节点的存储池中。如果载入的对象与此规则匹配，则 StorageGRID 仅会在一个存储节点上放置一个副本。



如果 ILM 规则仅创建一个对象的一个复制副本，则在存储节点不可用时，此对象将无法访问。在此示例中，只要存储节点 2 脱机，例如在升级或其他维护操作步骤 期间，您将暂时无法访问对象 AAA 。如果存储节点 2 发生故障，您将完全丢失对象 AAA 。



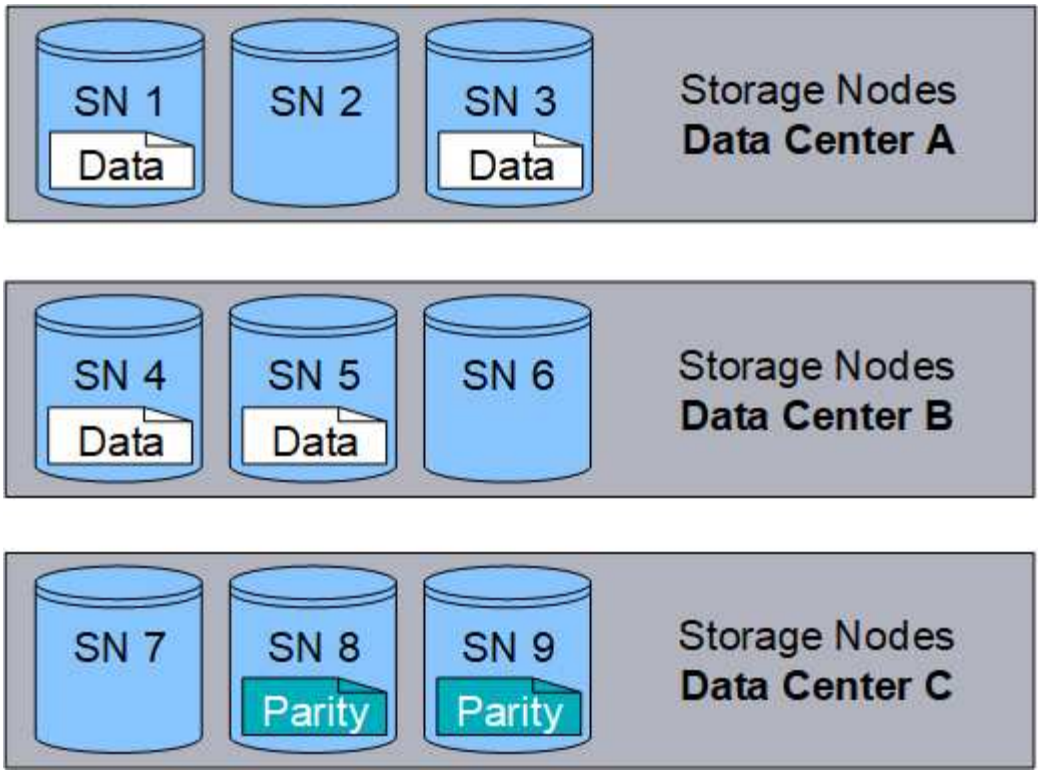
为了避免丢失对象数据，您应始终为要通过复制保护的所有对象创建至少两个副本。如果存在两个或更多副本，则在一个存储节点出现故障或脱机时，您仍可以访问此对象。



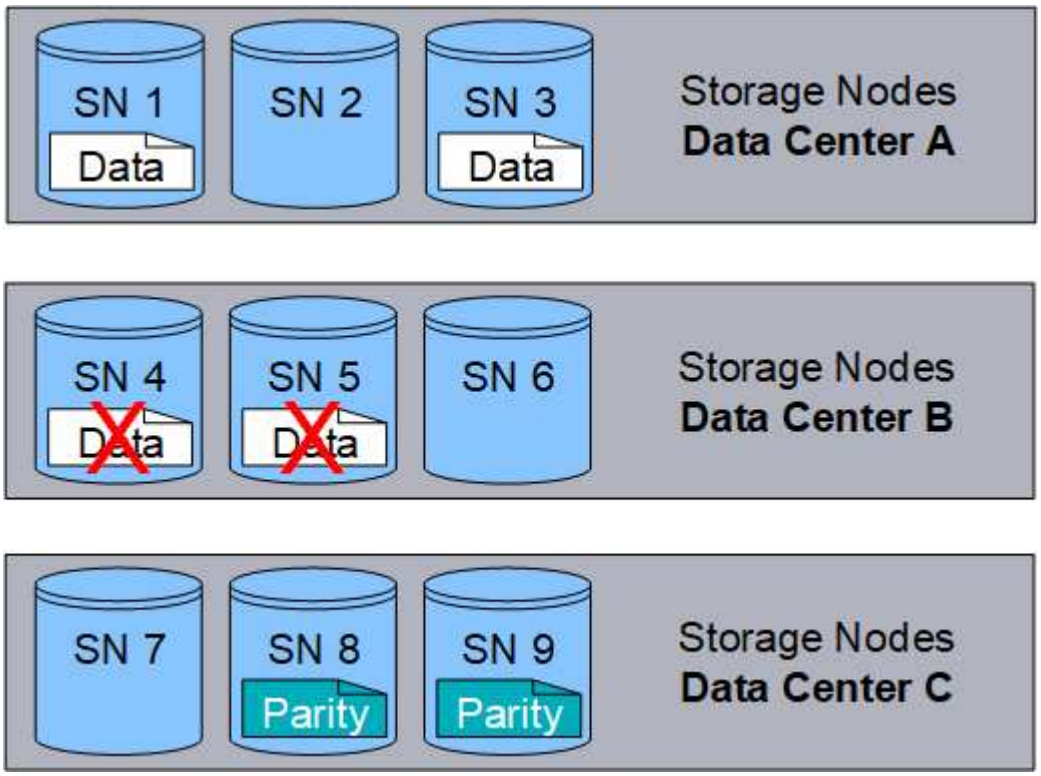
什么是纠删编码

纠删编码是 StorageGRID 存储对象数据的第二种方法。如果 StorageGRID 将对象与配置为创建纠删编码副本的 ILM 规则匹配，则会将对象数据分段为数据片段，计算额外的奇偶校验片段，并将每个片段存储在不同的存储节点上。访问某个对象时，系统会使用存储的片段重新组合该对象。如果数据或奇偶校验片段损坏或丢失，则纠删编码算法可以使用剩余数据和奇偶校验片段的子集重新创建该片段。

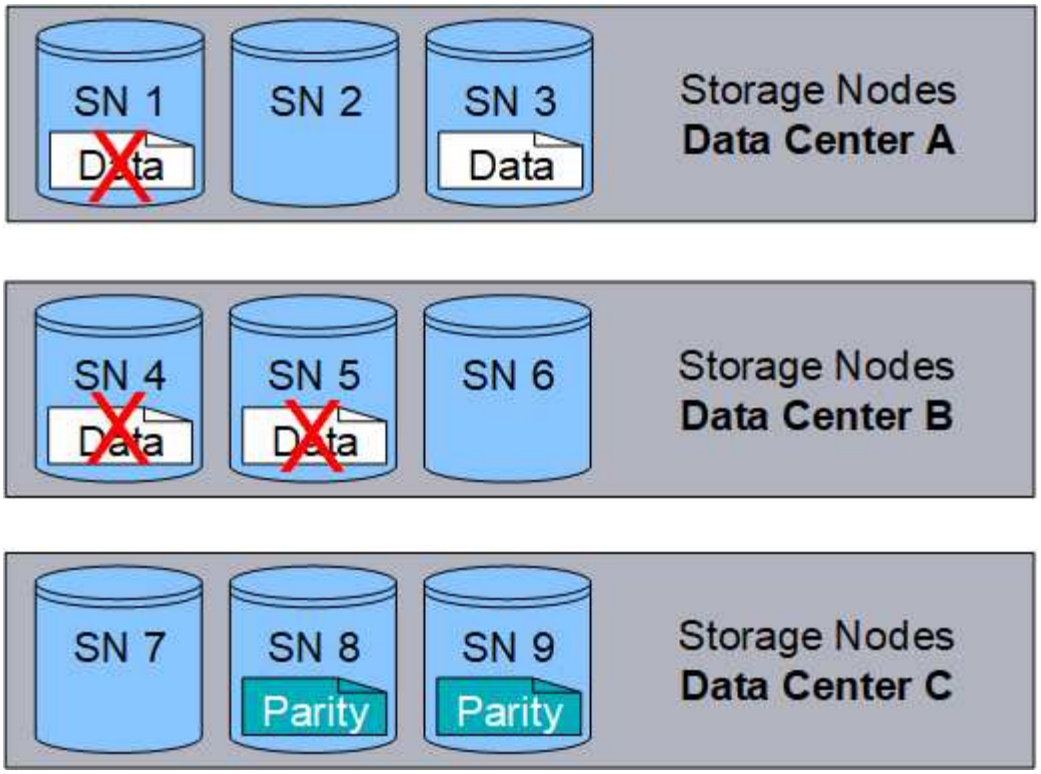
以下示例说明了如何对对象数据使用纠删编码算法。在此示例中， ILM 规则使用 4+2 纠删编码方案。每个对象都会被划分为四个相等的数据片段，并根据对象数据计算两个奇偶校验片段。六个片段中的每个片段都存储在三个数据中心站点的不同节点上，以便为节点故障或站点丢失提供数据保护。



4+2 纠删编码方案至少需要九个存储节点，三个不同站点中的每个站点各有三个存储节点。只要六个片段中的任意四个（数据或奇偶校验）仍然可用，就可以检索对象。最多可以丢失两个片段，而不会丢失对象数据。如果整个数据中心站点丢失，只要所有其他片段仍可访问，仍可检索或修复对象。



如果丢失两个以上的存储节点，则无法检索此对象。



相关信息

- 什么是存储池
- 什么是纠删编码方案
- 创建擦除编码配置文件

什么是纠删编码方案

为 ILM 规则配置纠删编码配置文件时，您可以根据计划使用的存储池中的存储节点和站点数量选择可用的纠删编码方案。纠删编码方案可控制为每个对象创建的数据片段数量和奇偶校验片段数量。

StorageGRID 系统使用 Reed-Solomon 纠删编码算法。该算法会将对象分段为 k 数据片段，并计算 m 奇偶校验片段。k + m = n 个片段分布在 n 个存储节点上，以提供数据保护。一个对象最多可承受丢失或损坏的碎片。检索或修复对象需要 K 个片段。

在配置擦除编码配置文件时，请对存储池遵循以下准则：

- 存储池必须包含三个或更多站点，或者只包含一个站点。

  如果存储池包含两个站点，则无法配置擦除编码配置文件。

  - 包含三个或更多站点的存储池的纠删编码方案
  - 单站点存储池的纠删编码方案
- 请勿使用默认存储池，所有存储节点或包含默认站点的存储池所有站点。
- 存储池应至少包含 *k*+*m*+1 个存储节点。

所需的最小存储节点数为 *k+m* 。但是，如果所需的存储节点暂时不可用，则至少添加一个存储节点有助于防止载入失败或 ILM 回退。

擦除编码方案的存储开销是通过将奇偶校验片段数（ *m* ）除以数据片段数（ *k* ）计算得出的。您可以使用存储开销计算每个擦除编码对象所需的磁盘空间量：

` 磁盘空间 _ = *object size* + （ *object size* * _storage over开销 _ ）`

例如，如果使用 4+2 方案存储一个 10 MB 的对象（存储开销为 50% ），则该对象将占用 15 MB 的网格存储。如果使用 6+2 方案存储同一个 10 MB 对象（存储开销为 33% ），则该对象将占用大约 13.3 MB 的空间。

选择总值最低的纠删编码方案 *k+m* ，以满足您的需求。碎片数量较少的纠删编码方案在计算方面总体上效率更高，因为每个对象创建和分布（或检索）的碎片数量较少，由于碎片大小较大，性能可能会更高，并且在需要更多存储时，扩展中添加的节点可能会更少。（有关规划存储扩展的信息，请参见有关扩展 StorageGRID 的说明。）

包含三个或更多站点的存储池的纠删编码方案

下表介绍了 StorageGRID 当前支持的纠删编码方案，该方案适用于包含三个或更多站点的存储池。所有这些方案均可提供站点丢失保护。一个站点可能会丢失，但对象仍可访问。

对于提供站点丢失保护的纠删编码方案，存储池中的建议存储节点数超过 *k+m*+1 ，因为每个站点至少需要三个存储节点。

纠删编码方案（ *k+m* ）	已部署站点的最小数量	每个站点的建议存储节点数	建议的存储节点总数	站点丢失保护？	存储开销
4+2	3.	3.	9	是的。	50%
6+2	4.	3.	12	是的。	33%
8+2	5.	3.	15	是的。	25%
6+3.	3.	4.	12	是的。	50%
9+3.	4.	4.	16.	是的。	33%
2+1	3.	3.	9	是的。	50%
4+1	5.	3.	15	是的。	25%
6+1	7.	3.	21	是的。	17%
7+5.	3.	5.	15	是的。	71%

StorageGRID 要求每个站点至少有三个存储节点。要使用 7+5 方案，每个站点至少需要四个存储节点。建议每个站点使用五个存储节点。

在选择提供站点保护的纠删编码方案时，请平衡以下因素的相对重要性：

- * 碎片数量 * ： 当碎片总数减少时，性能和扩展灵活性通常会提高。
- * 容错 * ： 容错可通过包含更多奇偶校验分段来提高（即，当 *m* 的值较高时）。
- * 网络流量 * ： 从故障中恢复时，使用包含更多片段的方案（即 *k+m* 的总数更高）会创建更多网络流量。
- * 存储开销 * ： 开销较高的方案需要每个对象更多的存储空间。

例如，在选择 4+2 方案和 6+3 方案（两者都有 50% 的存储开销）时，如果需要额外的容错功能，请选择 6+3 方案。如果网络资源受限，请选择 4+2 方案。如果所有其他因素相等，请选择 4+2 ，因为其碎片总数较低。

如果您不确定要使用的方案，请选择 4+2 或 6+3 ，或者联系技术支持。

单站点存储池的纠删编码方案

单站点存储池支持为三个或更多站点定义的所有纠删编码方案，但前提是该站点具有足够的存储节点。

所需的最小存储节点数为 *k+m* ，但建议使用具有 *k+m*+1 存储节点的存储池。例如， 2+1 纠删编码方案要求一个存储池至少包含三个存储节点，但建议使用四个存储节点。

纠删编码方案（ *k+m* ）	存储节点的最小数量	建议的存储节点数	存储开销
4+2	6.	7.	50%
6+2	8.	9	33%
8+2	10	11.	25%
6+3.	9	10	50%
9+3.	12	13	33%
2+1	3.	4.	50%
4+1	5.	6.	25%
6+1	7.	8.	17%
7+5.	12	13	71%

相关信息

扩展网格

纠删编码的优势，劣势和要求

在决定是使用复制还是纠删编码来保护对象数据不会丢失之前，您应了解纠删编码的优点，缺点和要求。

纠删编码的优势

与复制相比，纠删编码可提高可靠性，可用性和存储效率。

- * 可靠性 * ：可靠性通过容错来衡量—即，在不丢失数据的情况下可以同时发生的故障数量。通过复制，多个相同的副本会存储在不同的节点上以及不同的站点上。通过纠删编码，对象会编码为数据和奇偶校验片段，并分布在多个节点和站点上。这种分散方式可同时提供站点和节点故障保护。与复制相比，纠删编码可提高可靠性，而存储成本相当。
- * 可用性 * ：可用性可定义为在存储节点出现故障或无法访问时检索对象的功能。与复制相比，纠删编码可以以相当的存储成本提高可用性。
- * 存储效率 * ：对于相似级别的可用性和可靠性，通过纠删编码保护的对象比通过复制保护的相同对象占用的磁盘空间更少。例如，复制到两个站点的 10 MB 对象会占用 20 MB 的磁盘空间（两个副本），而采用 6+3 纠删编码方案在三个站点之间进行纠删编码的对象只会占用 15 MB 的磁盘空间。

> 擦除编码对象的磁盘空间计算为对象大小加上存储开销。存储开销百分比是奇偶校验片段数除以数据片段数。

纠删编码的缺点

与复制相比，纠删编码具有以下缺点：

- 需要增加存储节点和站点的数量。例如，如果使用纠删编码方案 6+3 ，则必须在三个不同站点至少有三个存储节点。相比之下，如果只复制对象数据，则每个副本只需要一个存储节点。
- 存储扩展的成本和复杂性增加。要扩展使用复制的部署，只需在创建对象副本的每个位置添加存储容量即可。要扩展使用纠删编码的部署，您必须同时考虑使用的纠删编码方案以及现有存储节点的容量。例如，如果您等待现有节点达到 100% 全满，则必须至少添加 *k+m* 存储节点，但如果在现有节点达到 70% 全满时进行扩展，则可以为每个站点添加两个节点，同时仍可最大程度地提高可用存储容量。有关详细信息，请参见为经过纠删编码的对象添加存储容量。
- 在分布在不同地理位置的站点之间使用纠删编码时，检索延迟会增加。与在本地复制并提供的对象（客户端连接的同一站点）相比，通过 WAN 连接检索经过纠删编码并分布在远程站点上的对象的对象片段所需时间更长。
- 在地理位置分散的站点之间使用纠删编码时，检索和修复的 WAN 网络流量使用率较高，尤其是频繁检索的对象或通过 WAN 网络连接进行对象修复。
- 当您在站点间使用纠删编码时，最大对象吞吐量会随着站点间网络延迟的增加而急剧下降。这一减少是由于 TCP 网络吞吐量相应减少，从而影响 StorageGRID 系统存储和检索对象片段的速度。
- 提高计算资源的利用率。

何时使用纠删编码

纠删编码最适合以下要求：

- 大于 1 MB 的对象。

> 纠删编码最适合大于 1 MB 的对象。请勿对小于 200 KB 的对象使用纠删编码，以避免管理极小的纠删编码片段所产生的开销。

- 长期或冷存储，用于存储不经常检索的内容。

- 高数据可用性和可靠性。
- 防止发生完整的站点和节点故障。
- 存储效率。
- 需要高效数据保护的单站点部署，只需一个纠删编码副本，而不是多个复制副本。
- 站点间延迟小于 100 毫秒的多站点部署。

如何确定对象保留

StorageGRID 为网格管理员和单个租户用户提供了指定对象存储时间的选项。通常，租户用户提供的任何保留指令优先于网格管理员提供的保留指令。

租户用户如何控制对象保留

租户用户可以通过三种主要方式控制其对象在 StorageGRID 中的存储时间：

- 如果为网格启用了全局 S3 对象锁定设置，则 S3 租户用户可以在启用了 S3 对象锁定的情况下创建分段，然后使用 S3 REST API 为添加到该分段的每个对象版本指定保留日期和合法保留设置。
  - 任何方法都不能删除处于合法保留状态的对象版本。
  - 在达到对象版本的保留截止日期之前，无法通过任何方法删除该版本。
  - 启用了 S3 对象锁定的存储分段中的对象由 ILM "`Forever 保留。` 但是，在达到保留截止日期后，可以通过客户端请求或存储分段生命周期到期来删除对象版本。请参见 使用 S3 对象锁定管理对象。
- S3 租户用户可以将生命周期配置添加到其分段中，以指定到期操作。如果存在分段生命周期，则 StorageGRID 会存储一个对象，直到满足到期操作中指定的日期或天数为止，除非客户端先删除该对象。请参见 创建 S3 生命周期配置。
- S3 或 Swift 客户端可以对删除对象请求进行问题描述 处理。在确定是删除还是保留对象时， StorageGRID 始终会优先处理客户端删除请求，而不是 S3 存储分段生命周期或 ILM 。

网格管理员如何控制对象保留

网格管理员可以使用 ILM 放置说明来控制对象的存储时间。如果对象与 ILM 规则匹配，则 StorageGRID 会存储这些对象，直到 ILM 规则中的最后一个时间段结束为止。如果为放置说明指定了 "`forever` " ，则对象将无限期保留。

无论谁控制对象的保留时间， ILM 设置都可控制存储的对象副本类型（复制或擦除编码）以及副本所在位置（存储节点，云存储池或归档节点）。

S3 存储分段生命周期和 **ILM** 如何交互

S3 存储分段生命周期中的到期操作始终会覆盖 ILM 设置。因此，即使有关放置对象的任何 ILM 指令已失效，该对象也可能会保留在网格中。

对象保留示例

要更好地了解 S3 对象锁定，存储分段生命周期设置，客户端删除请求和 ILM 之间的交互，请考虑以下示例。

示例 **1**： **S3** 存储分段生命周期将对象保留的时间超过 **ILM**

ILM

将两个副本存储 1 年（ 365 天）

分段生命周期

对象在 2 年（ 730 天）后过期

结果

StorageGRID 会将对象存储 730 天。StorageGRID 使用存储分段生命周期设置来确定是删除还是保留对象。

> 如果存储分段生命周期指定对象的保留时间应超过 ILM 指定的时间，则 StorageGRID 在确定要存储的副本数量和类型时会继续使用 ILM 放置说明。在此示例中，从第 366 天到第 730 天，此对象的两个副本将继续存储在 StorageGRID 中。

示例 **2**： **S3** 存储分段生命周期将对象在 **ILM** 之前过期

ILM

将两个副本存储 2 年（ 730 天）

分段生命周期

对象在 1 年（ 365 天）后过期

结果

StorageGRID 将在 365 天后删除此对象的两个副本。

示例 **3**：客户端删除将覆盖存储分段生命周期和 **ILM**

ILM

在存储节点 "`Forever` " 上存储两个副本

分段生命周期

对象在 2 年（ 730 天）后过期

客户端删除请求

发布日期：第 400 天

结果

StorageGRID 会在第 400 天删除此对象的两个副本，以响应客户端删除请求。

示例 **4**： **S3** 对象锁定会覆盖客户端删除请求

S3 对象锁定

对象版本的保留截止日期为 2026-03-31 。合法保留无效。

符合 **ILM** 规则

在存储节点 "`Forever 上存储两个副本。`

客户端删除请求

发布日期： 2024-03-31 。

结果

StorageGRID 不会删除此对象版本，因为保留截止日期仍在 2 年后。

如何删除对象

StorageGRID 可以直接响应客户端请求删除对象，也可以因 S3 存储分段生命周期到期或 ILM 策略要求而自动删除对象。了解可删除对象的不同方式以及 StorageGRID 如何处理删除请求有助于您更有效地管理对象。

StorageGRID 可以使用以下两种方法之一删除对象：

- 同步删除：当 StorageGRID 收到客户端删除请求时，将立即删除所有对象副本。删除副本后，系统会通知客户端删除操作成功。
- 对象将排队等待删除：当 StorageGRID 收到删除请求时，该对象将排队等待删除，并且系统会立即通知客户端删除已成功。对象副本稍后将通过后台 ILM 处理进行删除。

删除对象时， StorageGRID 会使用方法来优化删除性能，最大限度地减少潜在的删除积压并以最快的速度释放空间。

下表总结了 StorageGRID 何时使用每种方法。

执行删除的方法	使用时
对象已排队等待删除	当满足以下条件中的 * 任意 * 时： • 以下事件之一已触发自动对象删除： ◦ 已达到 S3 存储分段的生命周期配置中的到期日期或天数。 ◦ ILM 规则中指定的最后一个时间段已过。 • 注意： * 如果已启用 S3 对象锁定的存储分段中的对象处于合法保留状态，或者已指定保留日期但尚未满足，则无法删除这些对象。 • S3 或 Swift 客户端请求删除，但其中一个或多个条件为 true ： ◦ 无法在 30 秒内删除副本，因为对象位置暂时不可用。 ◦ 后台删除队列处于空闲状态。
立即删除对象（同步删除）	当 S3 或 Swift 客户端发出删除请求且满足以下 * 所有 * 条件时： • 可以在 30 秒内删除所有副本。 • 后台删除队列包含要处理的对象。

当 S3 或 Swift 客户端发出删除请求时， StorageGRID 首先会向删除队列添加多个对象。然后，它会切换到执行同步删除。确保后台删除队列包含要处理的对象，这样 StorageGRID 可以更高效地处理删除，尤其是对于低并发性客户端，同时有助于防止客户端删除积压。

删除对象需要多长时间

StorageGRID 删除对象的方式可能会影响系统的执行方式：

- 当 StorageGRID 执行同步删除时， StorageGRID 可能需要长达 30 秒才能将结果返回给客户端。这意味着删除的速度可能会更慢，即使副本的实际删除速度比 StorageGRID 将对象排队等待删除时要快。
- 如果您在批量删除期间密切监控删除性能，则可能会注意到删除了一定数量的对象后，删除率似乎会变慢。当 StorageGRID 从对要删除的对象进行排队转移到执行同步删除时，会发生此更改。删除率明显降低并不意味着删除对象副本的速度较慢。相反，它表明平均而言，空间释放速度更快。

如果要删除大量对象，并且您的优先级是快速释放空间，请考虑使用客户端请求删除对象，而不是使用 ILM 或其他方法删除这些对象。通常，当客户端执行删除时，空间释放速度会更快，因为 StorageGRID 可以使用同步删除。

请注意，删除对象后释放空间所需的时间取决于多种因素：

- 对象副本是同步删除还是稍后排队等待删除（对于客户端删除请求）。
- 其他因素包括网格中的对象数或对象副本排队等待删除时网格资源的可用性（对于客户端删除和其他方法）。

如何删除受版本控制的 **S3** 对象

如果为 S3 存储分段启用了版本控制，则无论这些请求来自 S3 客户端， S3 存储分段生命周期到期还是 ILM 策略要求， StorageGRID 都会在响应删除请求时遵循 Amazon S3 的行为。

对对象进行版本控制时，对象删除请求不会删除对象的当前版本，也不会释放空间。相反，对象删除请求只会创建一个删除标记作为对象的当前版本，从而使先前版本的对象 "`noncurrent.` " 成为非最新版本。

即使尚未删除此对象， StorageGRID 的行为仍会使当前版本的对象不再可用。对该对象的请求将返回 404 NotFound 。但是，由于未删除非当前对象数据，因此指定非当前对象版本的请求可能会成功。

要在删除受版本控制的对象时释放空间，必须执行以下操作之一：

- * S3 客户端请求 * ：在 S3 删除对象请求中指定对象版本号（ `Delete /object ? versionId=ID` ）。请注意，此请求仅删除指定版本的对象副本（其他版本仍占用空间）。
- * 分段生命周期 * ：在分段生命周期配置中使用 `NoncurrentVersionExpiration` 操作。满足指定的非当前磁盘数后， StorageGRID 将永久删除非当前对象版本的所有副本。无法恢复这些对象版本。
- * ILM ：向 ILM 策略添加两个 ILM 规则。在第一个规则中使用 * 非当前时间 * 作为参考时间，以匹配对象的非当前版本。在第二个规则中使用 * 载入时间 * 以匹配当前版本。必须在 * 载入时间 * 规则上方的策略中显示 * 非当前时间 * 规则。

相关信息

- 使用 S3
- 示例 4 ： S3 版本对象的 ILM 规则和策略

什么是 **ILM** 策略

信息生命周期管理（ ILM ）策略是一组有序的 ILM 规则，用于确定 StorageGRID 系统如何在一段时间内管理对象数据。

ILM 策略如何评估对象？

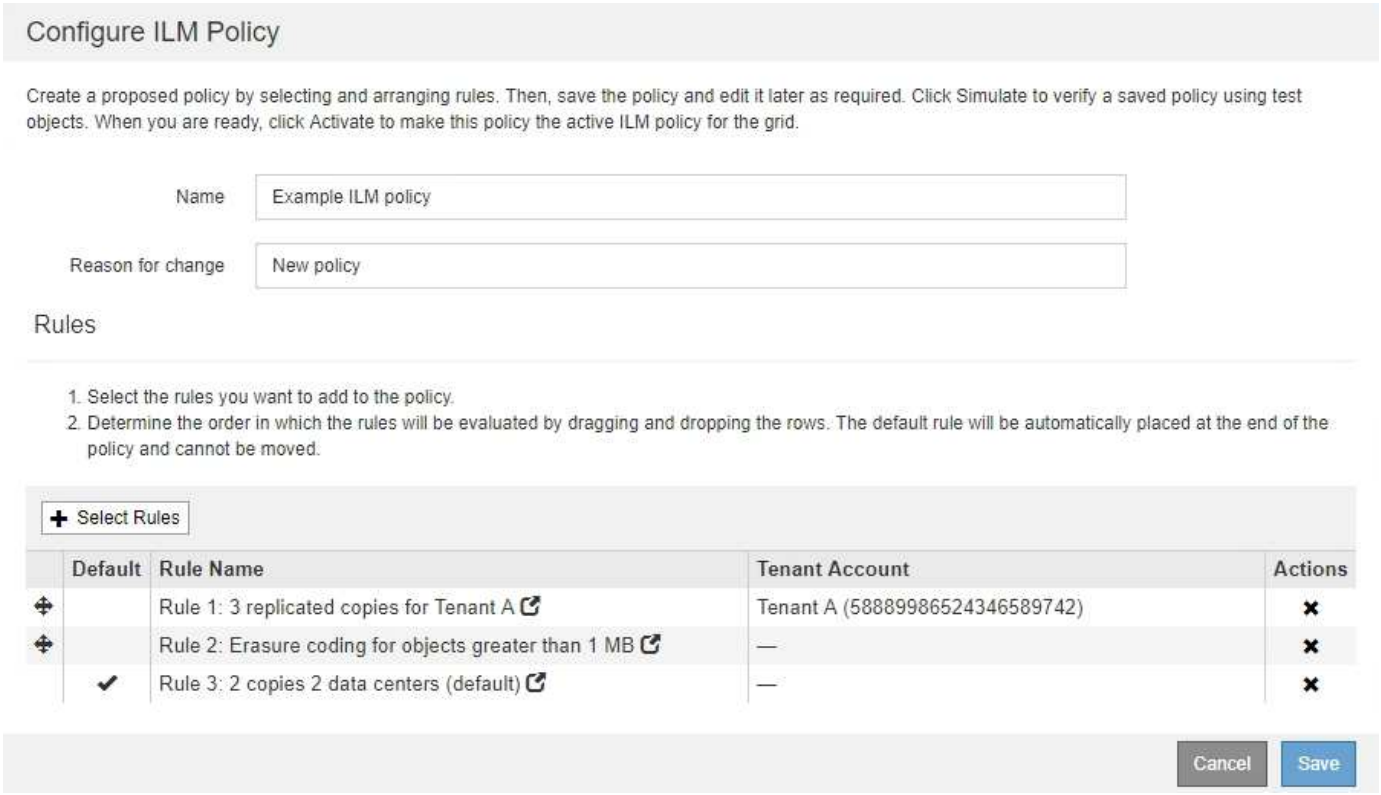
StorageGRID 系统的活动 ILM 策略控制所有对象的放置，持续时间和数据保护。

当客户端将对象保存到 StorageGRID 时，系统会根据活动策略中按顺序排列的一组 ILM 规则对这些对象进行评估，如下所示：

1. 如果策略中第一个规则的筛选器与某个对象匹配，则会根据该规则的载入行为载入该对象，并根据该规则的放置说明进行存储。
2. 如果第一个规则的筛选器与对象不匹配，则会根据策略中的每个后续规则对对象进行评估，直到匹配为止。
3. 如果没有与对象匹配的规则，则会应用策略中默认规则的载入行为和放置说明。默认规则是策略中的最后一个规则。默认规则必须应用于所有租户，所有分段和所有对象版本，并且不能使用任何高级筛选器。

ILM 策略示例

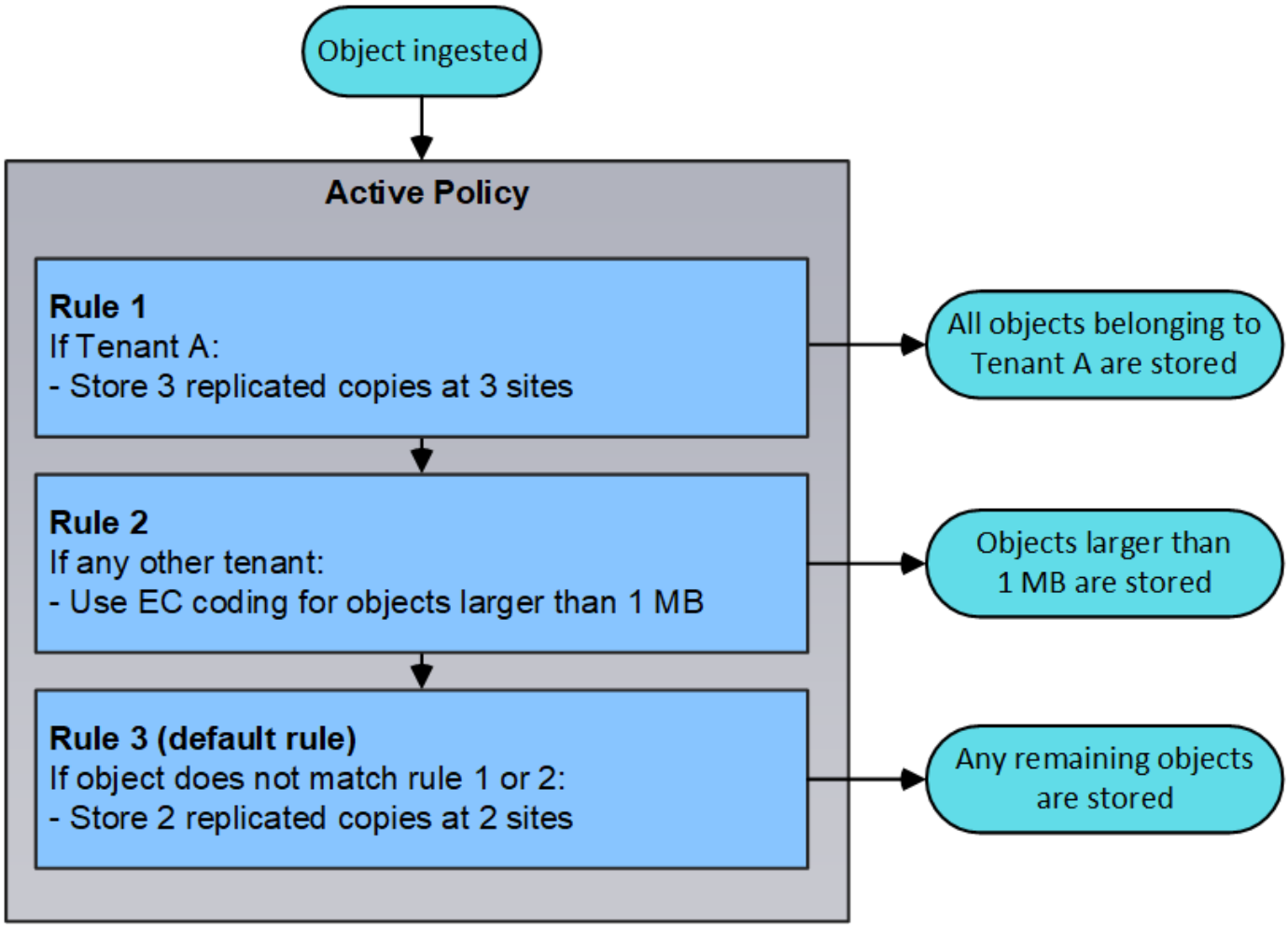
此示例 ILM 策略使用三个 ILM 规则。



在此示例中，规则 1 匹配属于租户 A 的所有对象这些对象会在三个站点上存储为三个复制副本。规则 1 不匹配属于其他租户的对象，因此会根据规则 2 对其进行评估。

规则 2 匹配其他租户的所有对象，但前提是它们大于 1 MB 。这些较大的对象在三个站点上使用 6+3 纠删编码进行存储。规则 2 与 1 MB 或更小的对象不匹配，因此会根据规则 3 评估这些对象。

规则 3 是策略中的最后一条规则和默认规则，不使用筛选器。规则 3 为规则 1 或规则 2 不匹配的所有对象（不属于租户 A 且小于 1 MB 的对象）创建两个复制副本。



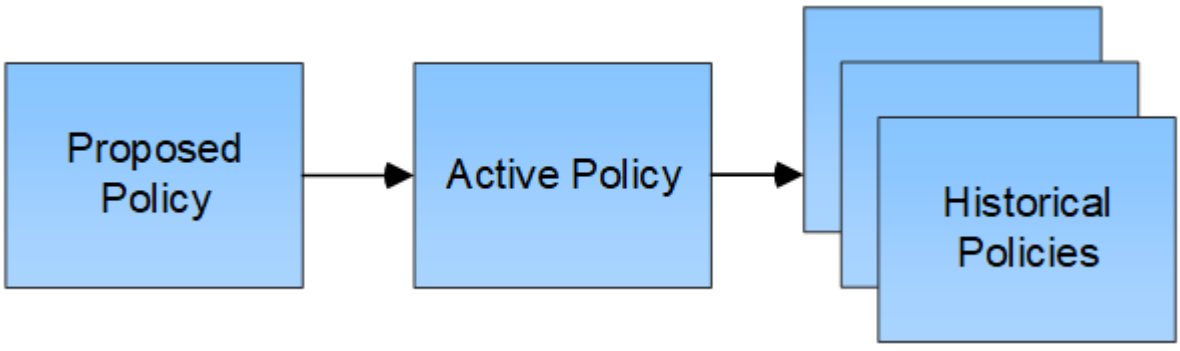
建议的策略，活动策略和历史策略是什么？

每个 StorageGRID 系统都必须有一个活动的 ILM 策略。StorageGRID 系统可能还具有一个建议的 ILM 策略和任意数量的历史策略。

首次创建 ILM 策略时，您可以通过选择一个或多个 ILM 规则并按特定顺序对其进行排列来创建建议的策略。模拟建议的策略以确认其行为后，您可以激活它以创建活动策略。

激活新的 ILM 策略时， StorageGRID 会使用该策略管理所有对象，包括现有对象和新载入的对象。实施新策略中的 ILM 规则后，现有对象可能会移至新位置。

激活建议的策略将导致先前处于活动状态的策略成为历史策略。无法删除历史 ILM 策略。



相关信息

什么是 **ILM** 规则

要管理对象，您需要创建一组信息生命周期管理（ ILM ）规则，并将其组织到 ILM 策略中。系统中载入的每个对象都会根据活动策略进行评估。如果策略中的规则与对象的元数据匹配，则规则中的说明将确定 StorageGRID 复制和存储该对象所采取的操作。

ILM 规则定义：

- 应存储哪些对象。规则可以应用于所有对象，也可以指定筛选器来标识规则适用场景 中的对象。例如，规则只能应用于与特定租户帐户，特定 S3 分段或 Swift 容器或特定元数据值关联的对象。
- 存储类型和位置。对象可以存储在存储节点，云存储池或归档节点上。
- 创建的对象副本的类型。可以复制副本或对副本进行纠删编码。
- 对于复制的副本，为创建的副本数。
- 对于纠删编码副本，使用纠删编码方案。
- 对象的存储位置和副本类型会随时间发生变化。
- 在将对象载入网格时如何保护对象数据（同步放置或双提交）。

请注意，对象元数据不受 ILM 规则管理。而是将对象元数据存储在 Cassandra 数据库中，该数据库称为元数据存储。每个站点会自动维护三个对象元数据副本，以防止数据丢失。这些副本会均匀分布在所有存储节点上。

ILM 规则的要素

ILM 规则包含三个要素：

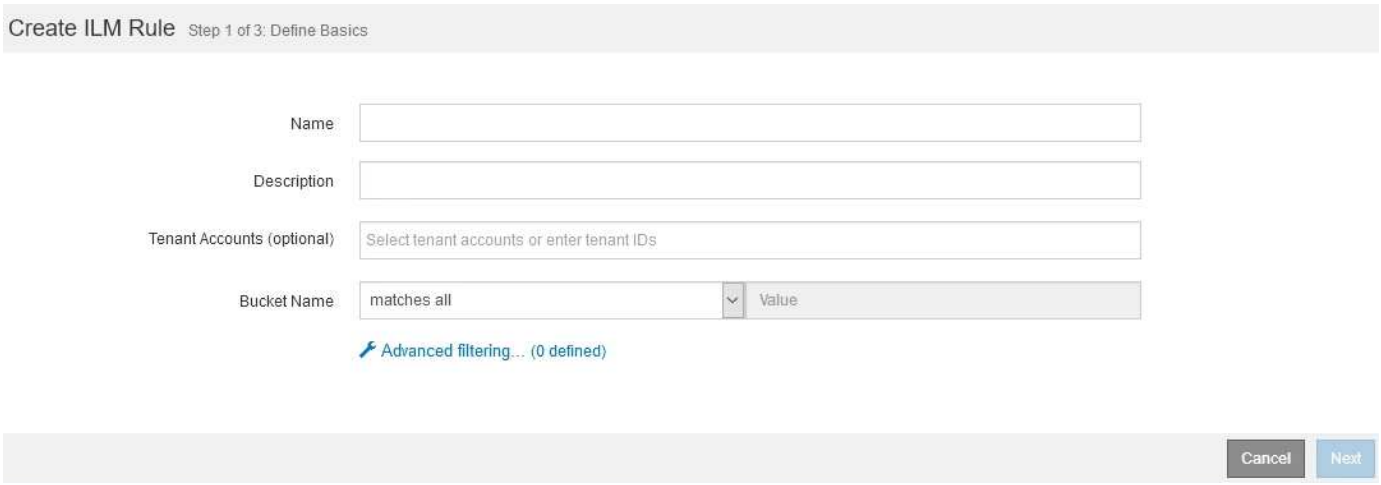
- * 筛选条件 * ： 规则的基本和高级筛选器用于定义规则适用场景 的对象。如果某个对象与所有筛选器匹配，则 StorageGRID 将应用此规则并创建在规则的放置说明中指定的对象副本。
- * 放置说明 * ： 规则的放置说明用于定义对象副本的数量，类型和位置。每个规则都可以包含一系列放置说明，以便随着时间的推移更改对象副本的数量，类型和位置。一个放置的时间段到期后，下一个放置中的说明将自动应用于下一个 ILM 评估。
- * 载入行为 * ： 规则的载入行为定义了 S3 或 Swift 客户端将对象保存到网格时发生的情况。载入行为用于控制是否按照规则中的说明立即放置对象副本，或者是否创建了临时副本并稍后应用放置说明。

什么是 **ILM** 规则筛选

创建 ILM 规则时，您可以指定筛选器来标识规则适用场景 的对象。

最简单的情况是，规则可能不使用任何筛选器。任何不使用筛选器适用场景 all 对象的规则，因此它必须是 ILM 策略中的最后一个（默认）规则。默认规则为与其他规则中的筛选器不匹配的对象提供存储说明。

通过基本筛选器，您可以对不同的大型对象组应用不同的规则。通过创建 ILM 规则向导的定义基础知识页面上的基本筛选器，您可以将规则应用于特定租户帐户，特定 S3 分段或 Swift 容器，或者同时应用于这两者。



通过这些基本筛选器，您可以轻松地将不同规则应用于大量对象。例如，您公司的财务记录可能需要存储以满足法规要求，而营销部门的数据则可能需要存储以方便日常运营。在为每个部门创建单独的租户帐户后，或者将不同部门的数据隔离到单独的 S3 存储分段后，您可以轻松创建适用场景 一个规则来记录所有财务记录，并创建另一个适用场景 规则来记录所有营销数据。

创建 ILM 规则向导的 * 高级筛选 * 页面可提供精细控制。您可以创建筛选器，以便根据以下对象属性选择对象：

- 载入时间
- 上次访问时间
- 全部或部分对象名称（密钥）
- S3 存储分段区域（位置限制）
- 对象大小
- 用户元数据
- S3 对象标记

您可以按非常具体的条件筛选对象。例如，医院成像部门存储的对象在使用不到 30 天时可能会频繁使用，而在使用之后则很少使用，而包含患者就诊信息的对象可能需要复制到健康网络总部的计费部门。您可以创建筛选器，根据对象名称，大小， S3 对象标记或任何其他相关标准来标识每种类型的对象，然后创建单独的规则以适当存储每组对象。

您还可以根据需要在一个规则中组合使用基本筛选器和高级筛选器。例如，营销部门可能希望以不同于供应商记录的方式存储大型映像文件，而人力资源部门可能需要将人员记录集中存储在特定地理位置和策略信息中。在这种情况下，您可以创建规则，按租户帐户进行筛选以将记录与每个部门隔离，同时在每个规则中使用高级筛选器来标识规则适用场景 所使用的特定对象类型。

什么是 **ILM** 规则放置说明

放置说明用于确定对象数据的存储位置，存储时间和存储方式。一个 ILM 规则可以包含一个或多个放置指令。每个放置指令适用场景 都有一段时间。

创建放置说明时：

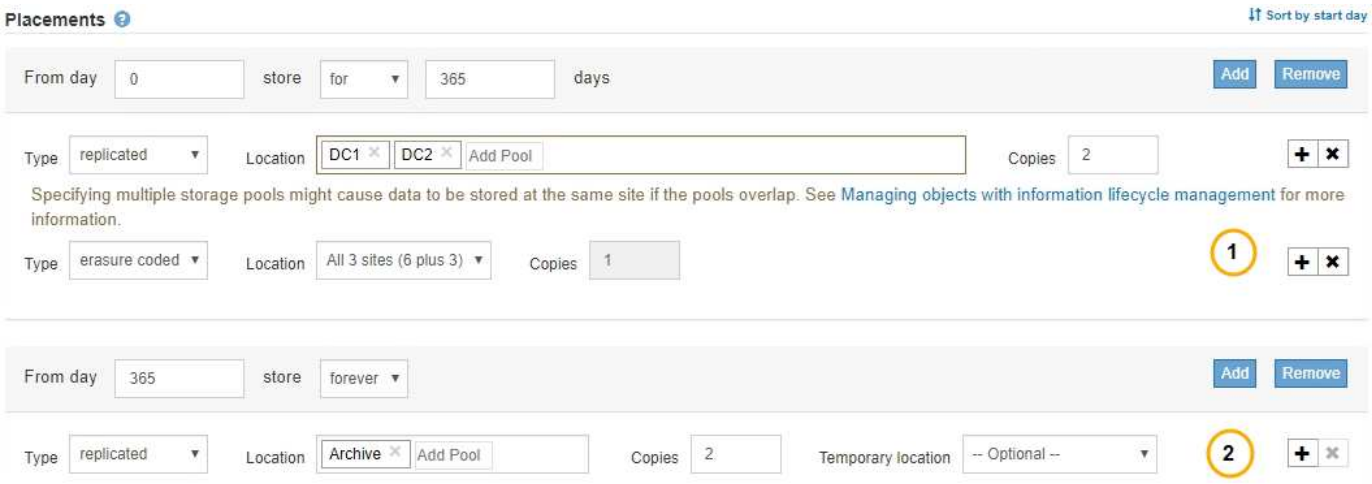
- 首先指定参考时间，该时间决定放置指令的开始时间。参考时间可能是：载入对象时，访问对象时，受版本控制的对象变为非当前状态时或用户定义的时间。

- 接下来，您可以指定相对于参考时间应用放置的时间。例如，放置可能从第 0 天开始，并持续 365 天，与对象载入的时间相关。
- 最后，您可以指定副本的类型（复制或纠删编码）以及副本的存储位置。例如，您可能希望将两个复制副本存储在两个不同的站点上。

每个规则可以定义一个时间段内的多个放置位置，也可以定义不同时间段的不同放置位置。

- 要在一段时间内将对象放置在多个位置，请选择加号图标 ➕ 为该时间段添加多行。
- 要在不同时间段内将对象放置在不同位置，请选择 * 添加 * 按钮以添加下一个时间段。然后，指定时间段内的一个或多个行。

此示例显示了创建 ILM 规则向导的定义放置页面。



1	第一个放置指令在第一年有两行： 1. 第一行会在两个数据中心站点创建两个复制的对象副本。 2. 第二行使用三个数据中心站点创建 6+3 纠删编码副本。
2	第二个放置指令会在一年后创建两个归档副本，并永久保留这些副本。

为规则定义一组放置指令时，必须确保至少有一个放置指令从第 0 天开始，并且定义的时间段之间没有空隙，最终放置指令将永久持续，或者一直持续到您不再需要任何对象副本为止。

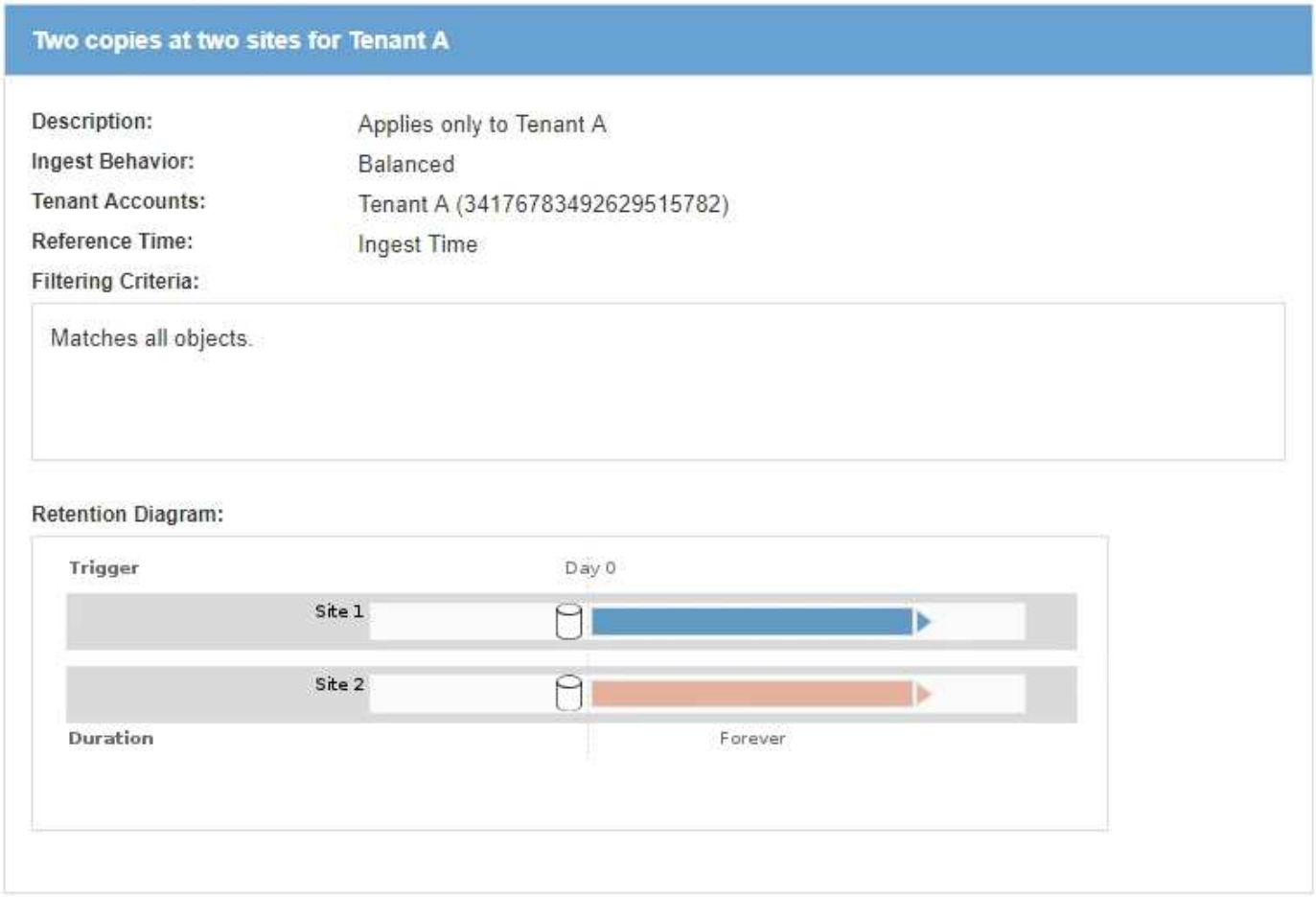
规则中的每个时间段到期后，将应用下一时间段的内容放置说明。此时将创建新的对象副本，并删除任何不需要的副本。

ILM 规则示例

此示例 ILM 规则适用场景 属于租户 A 的对象它会为这些对象创建两个复制副本，并将每个副本存储在不同的站点上。这两个副本会保留 "`Forever ，` " ，这意味着 StorageGRID 不会自动删除它们。相反， StorageGRID 将保留这些对象，直到客户端删除请求或存储分段生命周期到期时将其删除为止。

此规则对载入行为使用平衡选项：租户 A 将对象保存到 StorageGRID 后，系统会立即应用双站点放置指令，除

非无法立即创建所需的两个副本。例如，如果租户 A 保存对象时无法访问站点 2 ，则 StorageGRID 将在站点 1 的存储节点上创建两个临时副本。一旦站点 2 可用， StorageGRID 就会在该站点创建所需的副本。



相关信息

- 用于载入的数据保护选项
- 什么是存储池
- 什么是云存储池

创建存储级别，存储池， EC 配置文件和区域

创建和分配存储级别

存储级别用于确定存储节点使用的存储类型。如果希望 ILM 规则将某些对象放置在特定存储节点上，而不是站点中的所有节点上，则可以创建存储级别。例如，您可能希望某些对象存储在速度最快的存储节点上，例如 StorageGRID 全闪存存储设备。

您需要的内容

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

关于此任务

如果您使用多种类型的存储，则可以选择创建一个存储级别来标识每种类型。通过创建存储级别，您可以在配置

存储池时选择特定类型的存储节点。

如果不考虑存储级别（例如，所有存储节点都相同），则可以跳过此操作步骤，并在配置存储池时使用所有存储节点的默认存储级别。

在扩展中添加新存储节点时，该节点将添加到所有存储节点的默认存储级别。因此：

- 如果 ILM 规则使用具有所有存储节点级别的存储池，则可以在扩展完成后立即使用新节点。
- 如果 ILM 规则使用具有自定义存储级别的存储池，则在手动为节点分配自定义存储级别之前，不会使用此新节点，如下所述。

> 创建存储级别时，创建的存储级别不要超过所需数量。例如，不要为每个存储节点创建一个存储级别。而是将每个存储级别分配给两个或更多节点。如果仅分配给一个节点的存储级别不可用，则发生原因 ILM 会回退日志。

步骤

1. 选择 * ILM * > * 存储级别 * 。
2. 创建存储级别：
   a. 对于需要定义的每个存储级别，选择 * 插入 * 要添加一行并输入存储级别的标签，请执行以下操作：

      无法修改默认存储级别。它是为在 StorageGRID 系统扩展期间添加的新存储节点预留的。

Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

a. 要编辑现有存储级别，请选择 * 编辑 * 并根据需要修改标签。

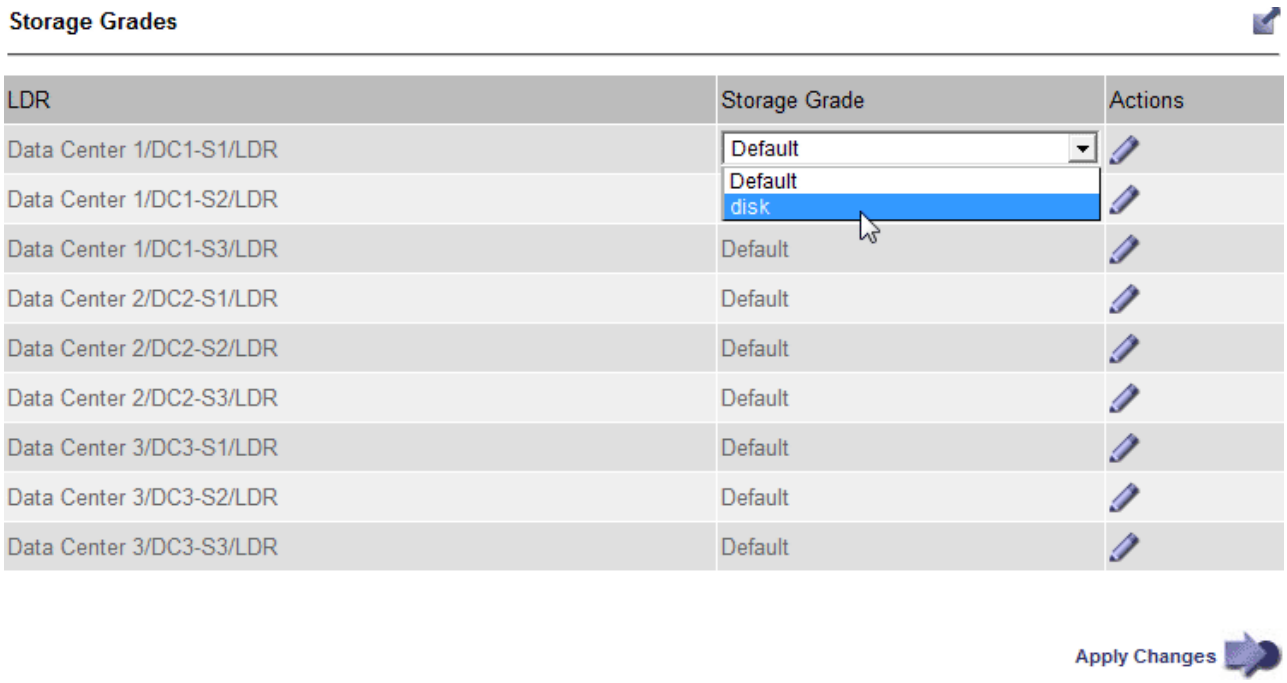
> 您不能删除存储级别。

b. 选择 * 应用更改 * 。

这些存储级别现在可分配给存储节点。

3. 为存储节点分配存储级别：

a. 对于每个存储节点的 LDR 服务，选择 * 编辑 * 并从列表中选择一个存储级别。



只需为给定存储节点分配一次存储级别。从故障中恢复的存储节点将保持先前分配的存储级别。激活 ILM 策略后，请勿更改此分配。如果分配发生更改，则会根据新的存储级别存储数据。

a. 选择 * 应用更改 * 。

配置存储池

什么是存储池

存储池是指存储节点或归档节点的逻辑分组。您可以配置存储池以确定 StorageGRID 系统存储对象数据的位置以及使用的存储类型。

存储池具有两个属性：

- * 存储级别 * ： 对于存储节点，是指后备存储的相对性能。
- * 站点 * ： 要存储对象的数据中心。

存储池用于在 ILM 规则中确定对象数据的存储位置。在为复制配置 ILM 规则时，您可以选择一个或多个包含存储节点或归档节点的存储池。在创建擦除编码配置文件时，您可以选择一个包含存储节点的存储池。

创建存储池的准则

配置和使用存储池时，请遵循以下准则。

所有存储池的准则

- StorageGRID 包括一个默认存储池 " 所有存储节点 " ，该存储池使用默认站点，所有站点以及默认存储级别 " 所有存储节点 " 。每当您添加新的数据中心站点时，系统都会自动更新所有存储节点存储池。

建议不要使用所有存储节点存储池或所有站点站点站点，因为这些项目会自动更新，以包括您在扩展中添加的任何新站点，而这可能不是您希望的行为。在使用所有存储节点存储池或默认站点之前，请仔细阅读有关复制的副本和经过纠删编码的副本的准则。

- 尽可能简化存储池配置。创建的存储池不要超过所需数量。
- 创建具有尽可能多节点的存储池。每个存储池应包含两个或更多节点。如果节点不可用，则节点不足的存储池可以对发生原因 ILM 进行回退。
- 避免创建或使用重叠的存储池（包含一个或多个相同节点）。如果存储池重叠，则可能会在同一节点上保存多个对象数据副本。

用于复制副本的存储池准则

- 为每个站点创建不同的存储池。然后，在每个规则的放置说明中指定一个或多个特定于站点的存储池。对每个站点使用存储池可确保复制的对象副本准确放置在所需位置（例如，每个站点上的每个对象一个副本，以实现站点丢失保护）。
- 如果在扩展中添加站点，请为新站点创建一个新存储池。然后，更新 ILM 规则以控制新站点上存储的对象。
- 通常，不要使用默认存储池，所有存储节点或包含默认站点的任何存储池，即所有站点。

用于擦除编码副本的存储池准则

- 您不能对纠删编码的数据使用归档节点。
- 存储池中包含的存储节点和站点数量决定了可用的纠删编码方案。
- 如果存储池仅包含两个站点，则不能使用该存储池进行纠删编码。对于具有两个站点的存储池，没有可用的纠删编码方案。
- 通常，不要使用默认存储池，所有存储节点或包含默认站点的任何存储池，也不要使用任何擦除编码配置文件中的所有站点。

如果您的网格仅包含一个站点，则系统将阻止您使用擦除编码配置文件中的所有存储节点存储池或所有站点默认站点。此行为可防止添加第二个站点时擦除编码配置文件变得无效。

- 如果您的吞吐量要求较高，则在站点之间的网络延迟超过 100 毫秒时，建议不要创建包含多个站点的存储池。随着延迟增加， StorageGRID 创建，放置和检索对象片段的速率会因 TCP 网络吞吐量降低而大幅下降。吞吐量的下降会影响对象载入和检索的最大可实现速率（如果选择 " 严格 " 或 " 平衡 " 作为 " 载入 " 行为），或者可能导致 ILM 队列回退（如果选择 " 双提交 " 作为 " 载入 " 行为）。
- 如果可能，存储池中的存储节点数应超过您选择的纠删编码方案所需的最小存储节点数。例如，如果您使用 6+3 纠删编码方案，则必须至少有九个存储节点。但是，建议每个站点至少另外配置一个存储节点。
- 尽可能均匀地在各个站点之间分布存储节点。例如，要支持 6+3 纠删编码方案，请配置一个存储池，使其在三个站点中至少包含三个存储节点。

用于归档副本的存储池准则

- 您不能创建同时包含存储节点和归档节点的存储池。归档副本需要一个仅包含归档节点的存储池。
- 如果使用的存储池包含归档节点，则还应在包含存储节点的存储池上至少维护一个已复制或经过纠删编码的副本。
- 如果启用了全局 S3 对象锁定设置，并且您要创建合规的 ILM 规则，则不能使用包含归档节点的存储池。请参见有关使用 S3 对象锁定管理对象的说明。

- 如果归档节点的目标类型为 Cloud Tiering - Simple Storage Service （ S3 ），则归档节点必须位于其自己的存储池中。请参见 管理 StorageGRID。

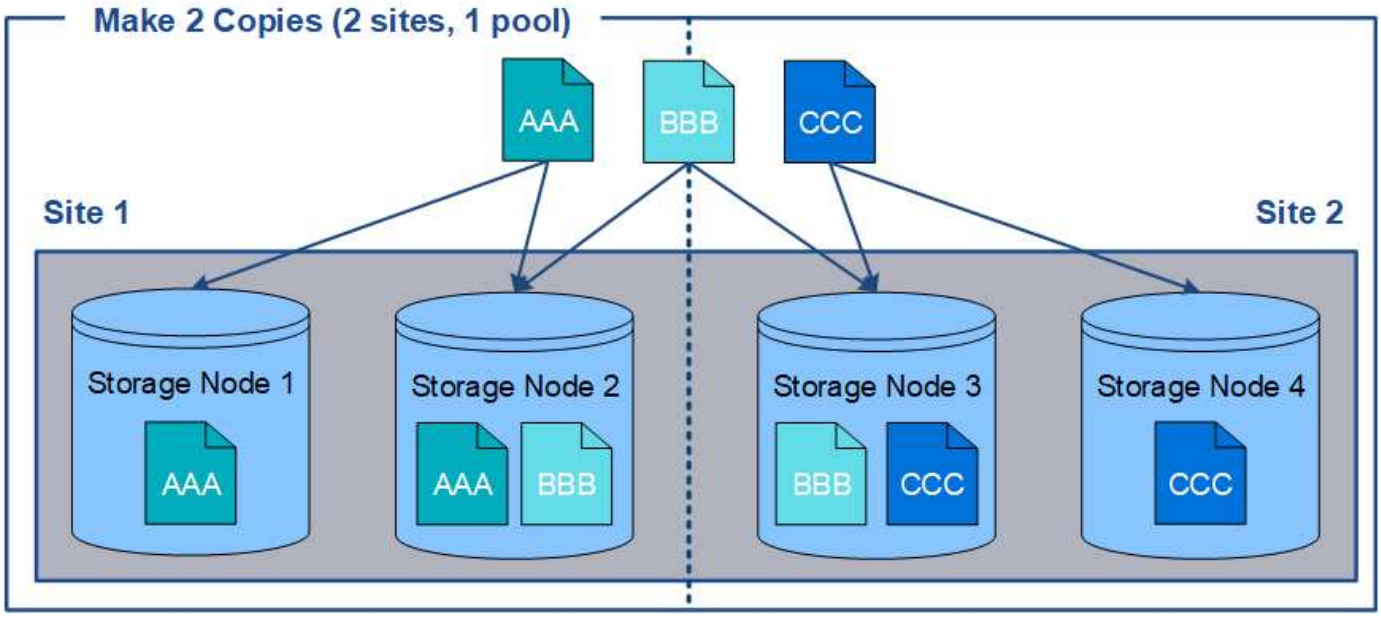
相关信息

- 什么是复制
- 什么是纠删编码
- 什么是纠删编码方案
- 使用多个存储池进行跨站点复制

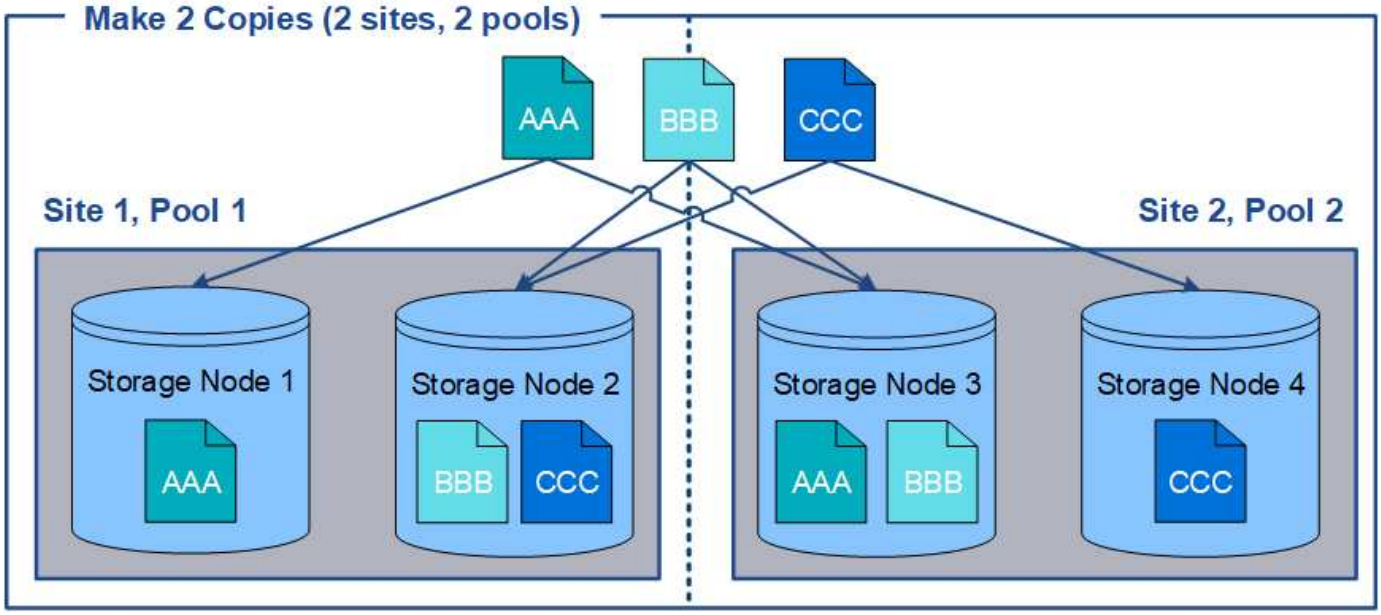
使用多个存储池进行跨站点复制

如果您的 StorageGRID 部署包含多个站点，则可以通过为每个站点创建一个存储池并在规则的放置说明中指定这两个存储池来启用站点丢失保护。例如，如果您将 ILM 规则配置为创建两个复制副本并指定两个站点上的存储池，则每个对象的一个副本将放置在每个站点上。如果您将规则配置为创建两个副本并指定三个存储池，则会分发这些副本以平衡存储池之间的磁盘使用量，同时确保这两个副本存储在不同的站点上。

以下示例说明了在 ILM 规则将复制的对象副本放置到包含两个站点中的存储节点的单个存储池时可能会发生的情况。由于系统在放置复制的副本时会使用存储池中的任何可用节点，因此可能只会将某些对象的所有副本放置在其中一个站点中。在此示例中，系统会在站点 1 的存储节点上存储两个对象 AAA 副本，并在站点 2 的存储节点上存储两个对象 ccc 副本。只有当某个站点发生故障或无法访问时，对象 BBB 才会受到保护。



相比之下，此示例说明了使用多个存储池时对象的存储方式。在此示例中， ILM 规则指定为每个对象创建两个复制副本，并将这些副本分发到两个存储池。每个存储池都包含一个站点上的所有存储节点。由于每个对象的副本存储在每个站点上，因此，可以防止对象数据出现站点故障或无法访问。



使用多个存储池时，请记住以下规则：

- 如果要创建 n 个副本，则必须添加 n 个或更多存储池。例如，如果将规则配置为创建三个副本，则必须指定三个或更多存储池。
- 如果副本数等于存储池数，则每个存储池中将存储一个对象副本。
- 如果副本数小于存储池数，则系统会分发这些副本，以便在池之间保持磁盘使用量的平衡，并确保两个或更多副本不会存储在同一个存储池中。
- 如果存储池重叠（包含相同的存储节点），则对象的所有副本可能只保存在一个站点上。您必须确保选定存储池不包含相同的存储节点。

使用存储池作为临时位置（已弃用）

创建对象放置包含单个存储池的 ILM 规则时，系统会提示您指定要用作临时位置的第二个存储池。

临时位置已弃用，将在未来版本中删除。您不应选择存储池作为新 ILM 规则的临时位置。

如果选择严格的载入行为（创建 ILM 规则向导的第 3 步），则会忽略临时位置。

相关信息

用于载入的数据保护选项

创建存储池

您可以创建存储池来确定 StorageGRID 系统存储对象数据的位置以及使用的存储类型。每个存储池包括一个或多个站点以及一个或多个存储级别。

您需要的内容

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

- 您已查看创建存储池的准则。

关于此任务

存储池用于确定对象数据的存储位置。所需的存储池数量取决于网格中的站点数量以及所需的副本类型：复制副本或经过纠删编码的副本。

- 对于复制和单站点纠删编码，请为每个站点创建一个存储池。例如，如果要将复制的对象副本存储在三个站点上，请创建三个存储池。
- 要在三个或更多站点上进行纠删编码，请创建一个存储池，其中包含每个站点的条目。例如，如果要跨三个站点擦除代码对象，请创建一个存储池。选择加号图标 ➕ 为每个站点添加一个条目。

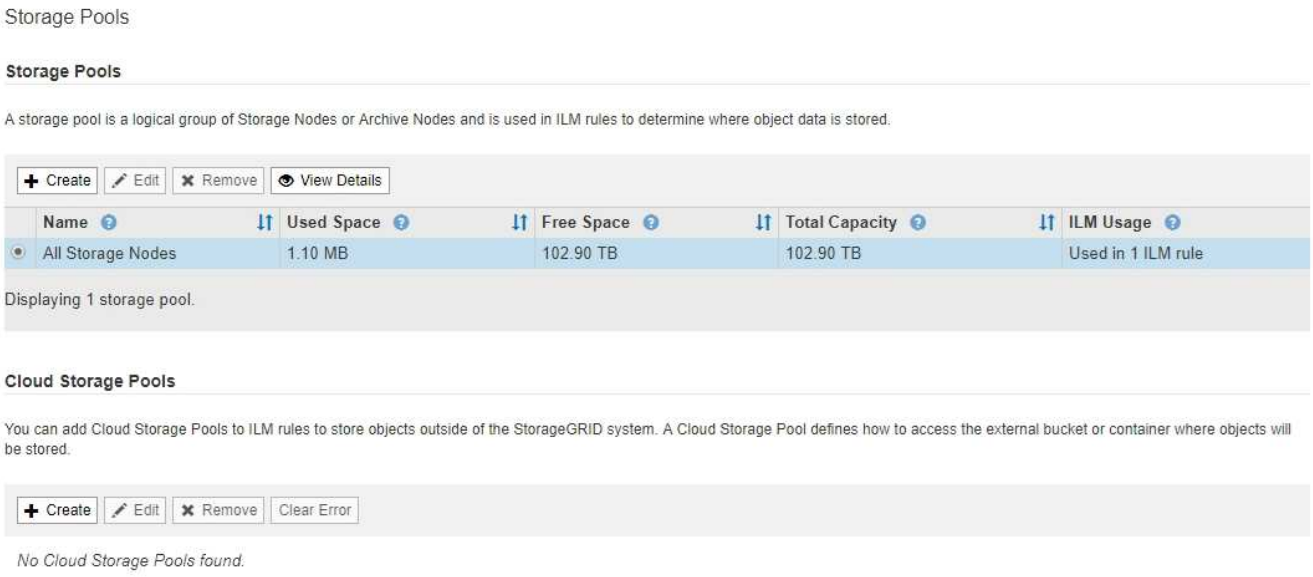
> 请勿将默认的所有站点站点站点包含在要在擦除编码配置文件中使用的存储池中。而是在存储池中为要存储纠删编码数据的每个站点添加一个单独的条目。请参见 此步骤 例如。

- 如果您有多个存储级别，请勿在一个站点上创建包含不同存储级别的存储池。请参见 创建存储池的准则。

步骤

1. 选择 * ILM * > * 存储池 * 。

   此时将显示存储池页面，其中列出了所有已定义的存储池。

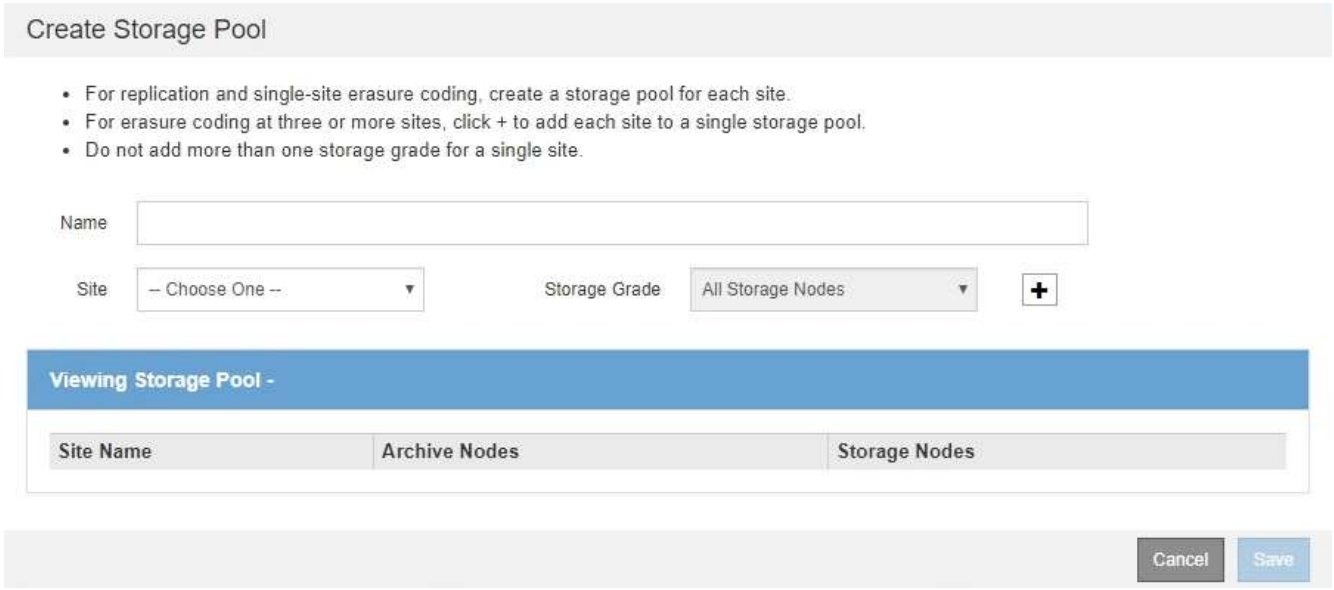


   此列表包括系统默认存储池，使用系统默认站点的所有存储节点，所有站点以及默认存储级别的所有存储节点。

> 由于每当添加新的数据中心站点时，所有存储节点存储池都会自动更新，因此不建议在 ILM 规则中使用此存储池。

2. 要创建新存储池，请选择 * 创建 * 。

   此时将显示创建存储池对话框。



3. 输入存储池的唯一名称。

   在配置纠删编码配置文件和 ILM 规则时，请使用易于识别的名称。

4. 从 * 站点 * 下拉列表中，为此存储池选择一个站点。

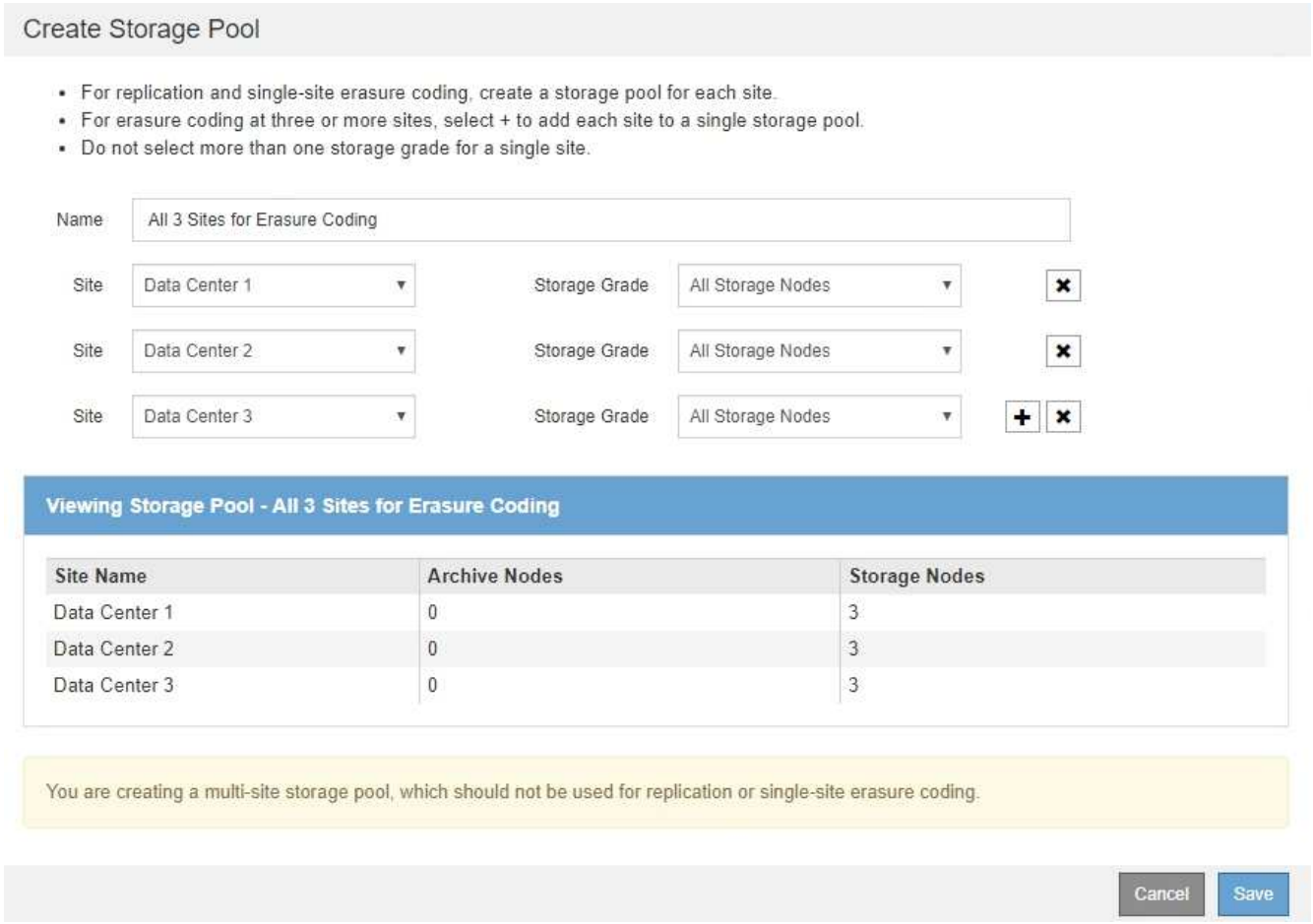
   选择站点时，此表中的存储节点和归档节点数将自动更新。

   通常，不要在任何存储池中使用默认的所有站点站点站点。使用所有站点存储池的 ILM 规则会将对象放置在任何可用站点上，从而减少对对象放置的控制。此外，所有站点存储池会立即使用新站点上的存储节点，这可能不是您所期望的行为。

5. 从 * 存储级别 * 下拉列表中，选择 ILM 规则使用此存储池时要使用的存储类型。

   默认的所有存储节点存储级别包括选定站点上的所有存储节点。默认归档节点存储级别包括选定站点上的所有归档节点。如果您为网格中的存储节点创建了其他存储级别，则这些存储级别将在下拉列表中列出。

6. 【条目】如果要在多站点擦除编码配置文件中使用存储池，请选择 ➕ 将每个站点的条目添加到存储池中。



> 您不能创建重复条目，也不能创建既包含 * 归档节点 * 存储级别又包含存储节点的任何存储级别的存储池。
>
> 如果您为一个站点添加多个条目，但存储级别不同，则系统会向您发出警告。

要删除条目，请选择 ✖。

7. 如果您对所做的选择感到满意，请选择 * 保存 * 。

   此时，新存储池将添加到此列表中。

查看存储池详细信息

您可以查看存储池的详细信息以确定存储池的使用位置，并查看包含哪些节点和存储级别。

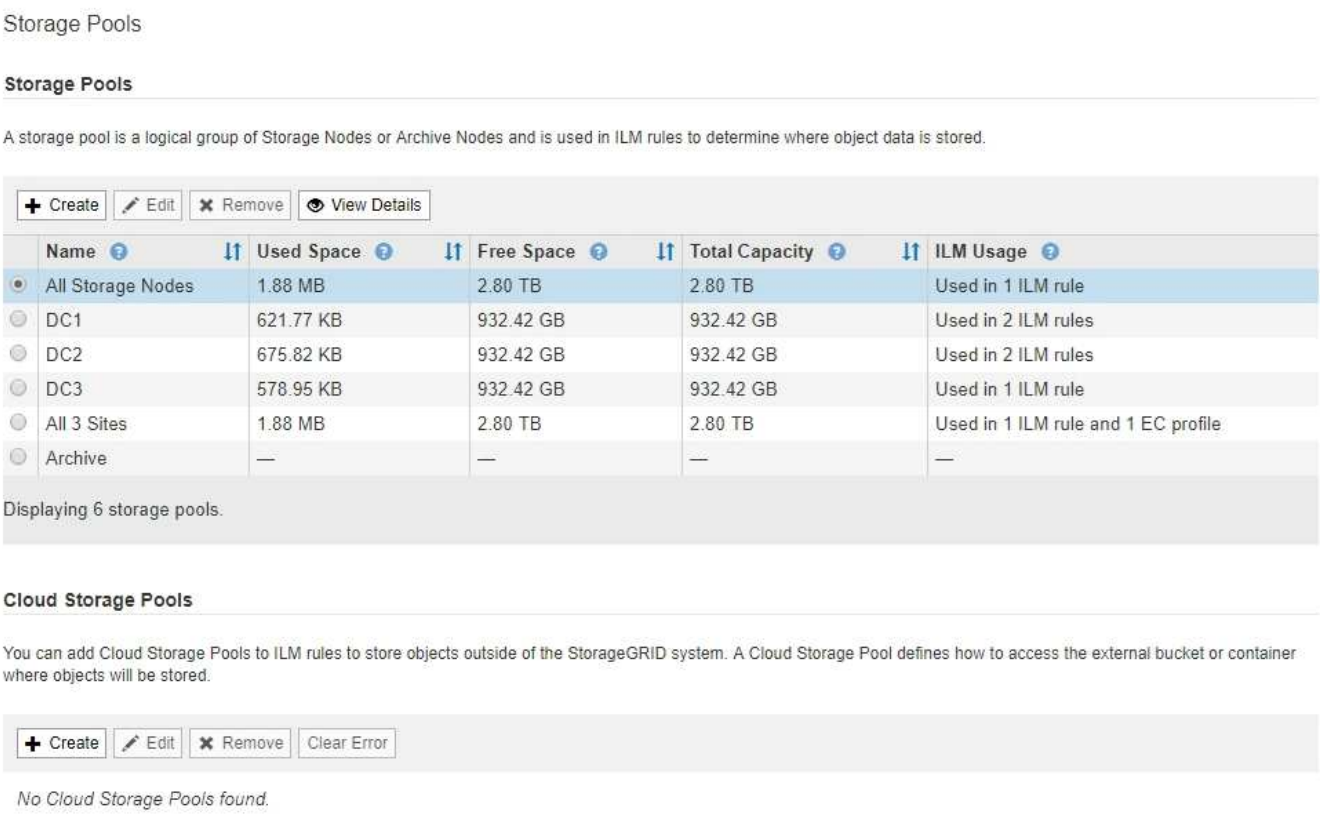
您需要的内容

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

步骤

1. 选择 * ILM * > * 存储池 * 。

此时将显示存储池页面。此页面将列出所有已定义的存储池。



此表包含包含存储节点的每个存储池的以下信息：

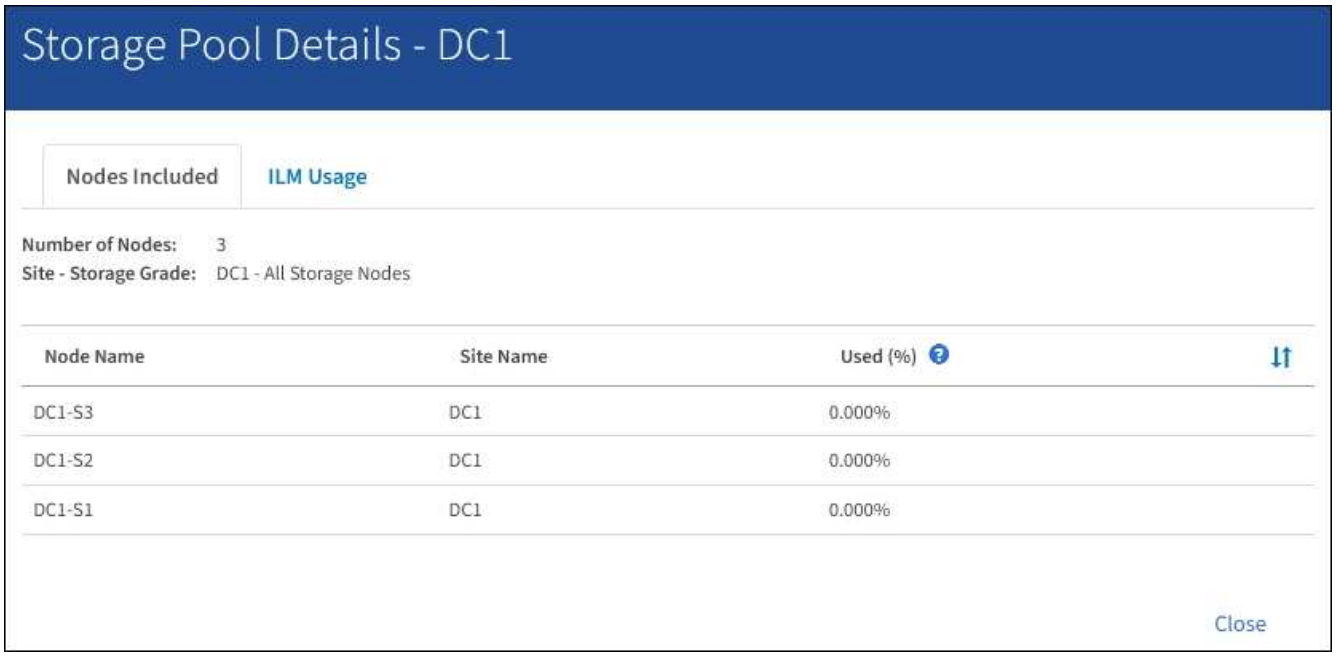
- * 名称 * ： 存储池的唯一显示名称。
- * 已用空间 * ： 当前用于在存储池中存储对象的空间量。
- * 可用空间 * ： 存储池中仍可用于存储对象的空间量。
- * 总容量 * ： 存储池的大小，等于存储池中所有节点的对象数据的总可用空间量。
- * ILM 使用情况 * ： 当前如何使用存储池。存储池可能未使用，也可能在一个或多个 ILM 规则，擦除编码配置文件或这两者中使用。

> 如果正在使用某个存储池，则无法将其删除。

2. 要查看有关特定存储池的详细信息，请选择其单选按钮并选择 * 查看详细信息 * 。

   此时将显示存储池详细信息模式。

3. 查看 * 包含的节点 * 选项卡，了解存储池中包含的存储节点或归档节点。



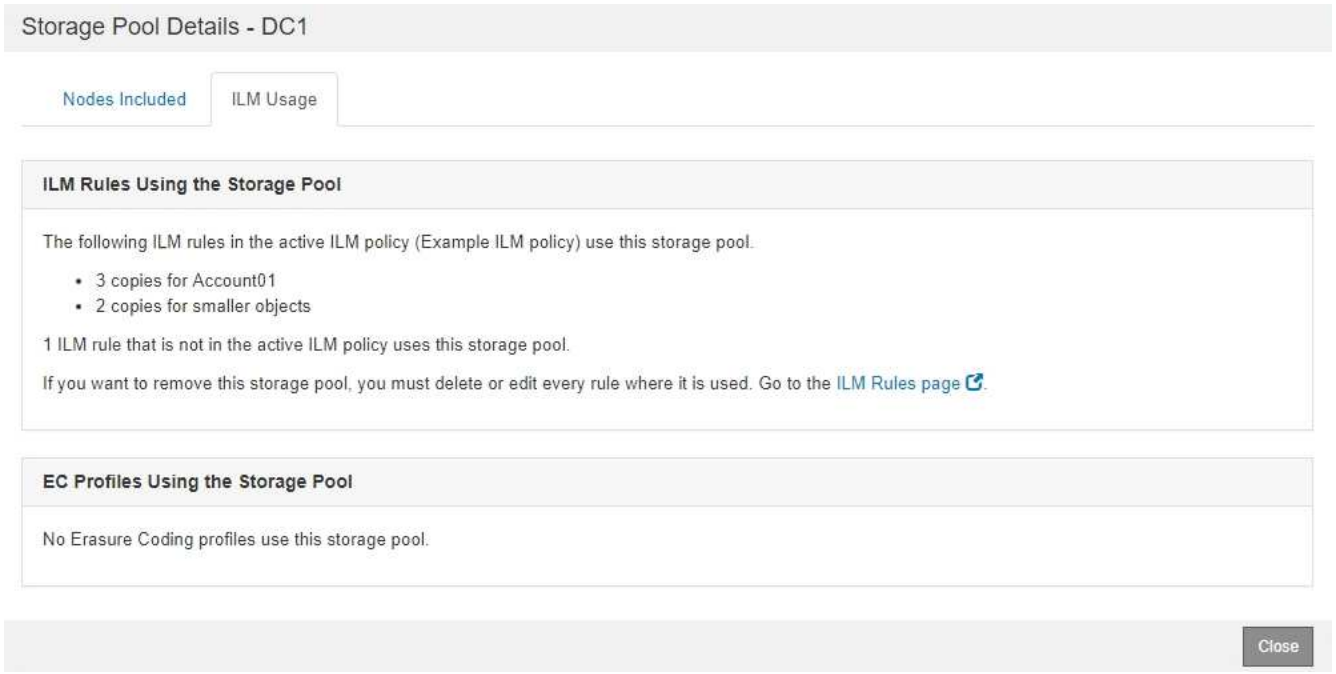
此表包含每个节点的以下信息：

- 节点名称
- 站点名称
- 已用（%）：对于存储节点，已用对象数据总可用空间的百分比。此值不包括对象元数据。

> 每个存储节点的 " 已用存储 - 对象数据 " 图表也显示了相同的已用（%）值（选择 * 节点 * > * 存储节点 _* > * 存储 * ）。

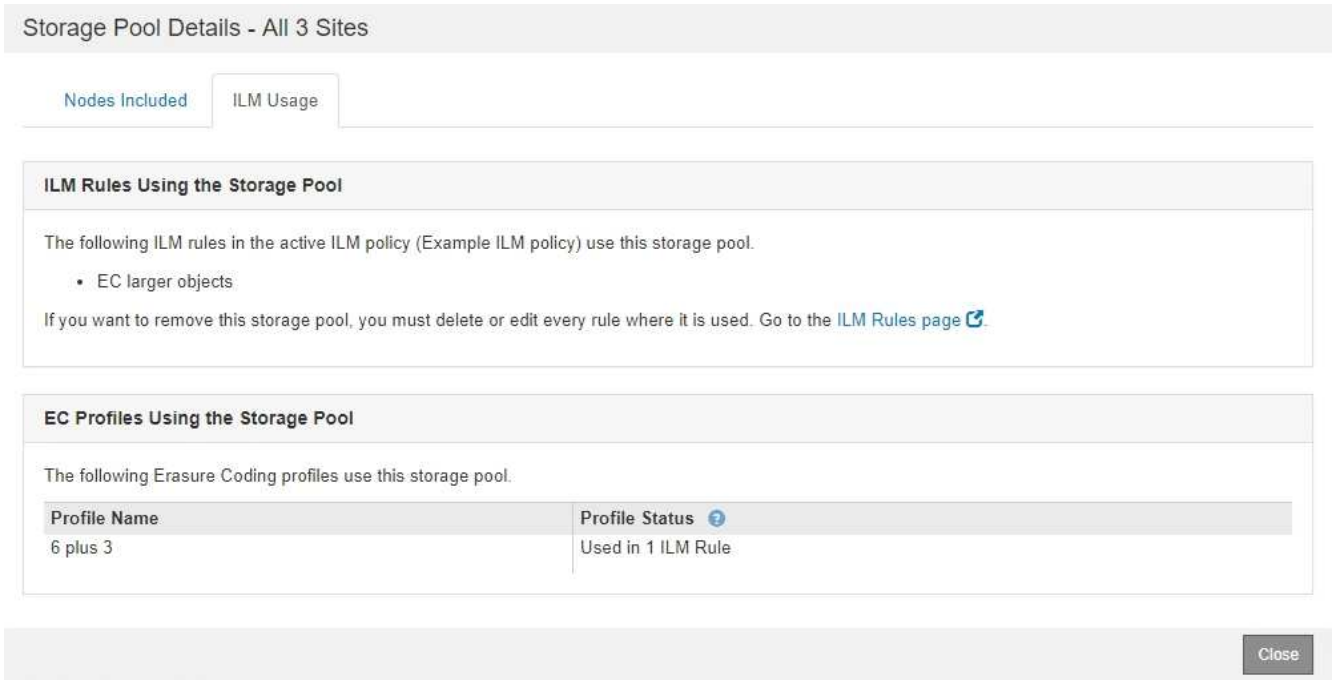
4. 选择 * ILM Usage* 选项卡以确定存储池当前是否正在任何 ILM 规则或擦除编码配置文件中使用。

在此示例中， DC1 存储池用于三个 ILM 规则：两个规则位于活动 ILM 策略中，一个规则不在活动策略中。



如果存储池在 ILM 规则中使用，则不能将其删除。

在此示例中，所有 3 个站点的存储池均用于擦除编码配置文件。反过来，活动 ILM 策略中的一个 ILM 规则也会使用该擦除编码配置文件。



如果存储池在擦除编码配置文件中使用，则无法将其删除。

5. 或者，也可以转到 * ILM 规则页面 * ，了解并管理使用存储池的任何规则。

   请参见有关使用 ILM 规则的说明。

6. 查看完存储池详细信息后，选择 * 关闭 * 。

相关信息

使用 ILM 规则和 ILM 策略

编辑存储池

您可以编辑存储池以更改其名称或更新站点和存储级别。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已查看创建存储池的准则。
- 如果您计划编辑由活动 ILM 策略中的规则使用的存储池，则已考虑所做的更改将如何影响对象数据放置。

关于此任务

如果要向活动 ILM 策略中使用的存储池添加新的存储级别，请注意，不会自动使用新存储级别中的存储节点。要强制 StorageGRID 使用新的存储级别，您必须在保存编辑后的存储池后激活新的 ILM 策略。

步骤

1. 选择 * ILM * > * 存储池 * 。

   此时将显示存储池页面。

2. 选择要编辑的存储池对应的单选按钮。

   您不能编辑所有存储节点存储池。

3. 选择 * 编辑 * 。
4. 根据需要更改存储池名称。
5. 根据需要选择其他站点和存储级别。

   > 如果在擦除编码配置文件中使用存储池，并且此更改会发生原因 使擦除编码方案无效，则您无法更改站点或存储级别。例如、如果在擦除编码配置文件中使用的存储池当前仅包含一个站点的存储级别、则系统会阻止您对两个站点使用存储级别、因为更改会使擦除编码方案无效。

6. 选择 * 保存 * 。

完成后

如果您向活动 ILM 策略中使用的存储池添加了新的存储级别，请激活新的 ILM 策略以强制 StorageGRID 使用新的存储级别。例如，克隆现有 ILM 策略，然后激活此克隆。

删除存储池

您可以删除未使用的存储池。

您需要的内容

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

步骤

1. 选择 * ILM * > * 存储池 * 。

   此时将显示存储池页面。

2. 查看表中的 "ILM Usage" 列，确定是否可以删除存储池。

   如果存储池正在 ILM 规则或纠删编码配置文件中使用，则不能将其删除。根据需要，选择 * 查看详细信息 * > * ILM 使用情况 * 以确定存储池的使用位置。

3. 如果未使用要删除的存储池，请选择单选按钮。
4. 选择 * 删除 * 。
5. 选择 * 确定 * 。

什么是云存储池

通过云存储池，您可以使用 ILM 将对象数据移动到 StorageGRID 系统之外。例如，您可能希望将不常访问的对象移至成本较低的云存储，例如 Amazon S3 Glacier ， S3 Glacier Deep Archive 或 Microsoft Azure Blob 存储中的归档访问层。或者，您可能希望维护 StorageGRID 对象的云备份以增强灾难恢复能力。

从 ILM 角度来看，云存储池与存储池类似。要将对象存储在任一位置，请在为 ILM 规则创建放置说明时选择池。但是，虽然存储池包含 StorageGRID 系统中的存储节点或归档节点，但云存储池包含外部存储分段（ S3 ）或容器（ Azure Blob 存储）。

下表对存储池与云存储池进行了比较，并显示了一些高级相似之处和不同之处。

	存储池	云存储池
如何创建？	使用网格管理器中的 * ILM * > * 存储池 * 选项。 您必须先设置存储级别，然后才能创建存储池。	使用网格管理器中的 * ILM * > * 存储池 * 选项。 您必须先设置外部存储分段或容器，然后才能创建云存储池。
您可以创建多少个池？	无限制。	最多 10 个。
对象存储在何处？	在 StorageGRID 中的一个或多个存储节点或归档节点上。	位于 StorageGRID 系统外部的 Amazon S3 存储分段或 Azure Blob 存储容器中。 如果云存储池是 Amazon S3 存储分段： • 您可以选择配置存储分段生命周期，以便将对象过渡到低成本的长期存储，例如 Amazon S3 Glacier 或 S3 Glacier Deep Archive 。外部存储系统必须支持 Glacier 存储类和 S3 POST 对象还原 API 。 • 您可以创建云存储池，以便与支持 AWS 机密区域的 AWS 商用云服务（ C2S ）结合使用。 如果云存储池是 Azure Blob 存储容器，则 StorageGRID 会将对象过渡到归档层。 • 注意： * 一般情况下，不要为用于云存储池的容器配置 Azure Blob Storage 生命周期管理。对云存储池中的对象执行的后对象还原操作可能会受所配置生命周期的影响。

	存储池	云存储池
什么控制对象放置？	活动 ILM 策略中的 ILM 规则。	活动 ILM 策略中的 ILM 规则。
使用什么数据保护方法？	复制或纠删编码。	复制。
每个对象允许多少个副本？	多个。	一个副本位于云存储池中，一个或多个副本也位于 StorageGRID 中。 • 注意： * 在任何给定时间，不能将对象存储在多个云存储池中。
有哪些优势？	可以随时快速访问对象。	低成本存储。

云存储池对象的生命周期

在实施云存储池之前，请查看存储在每种类型的云存储池中的对象的生命周期。

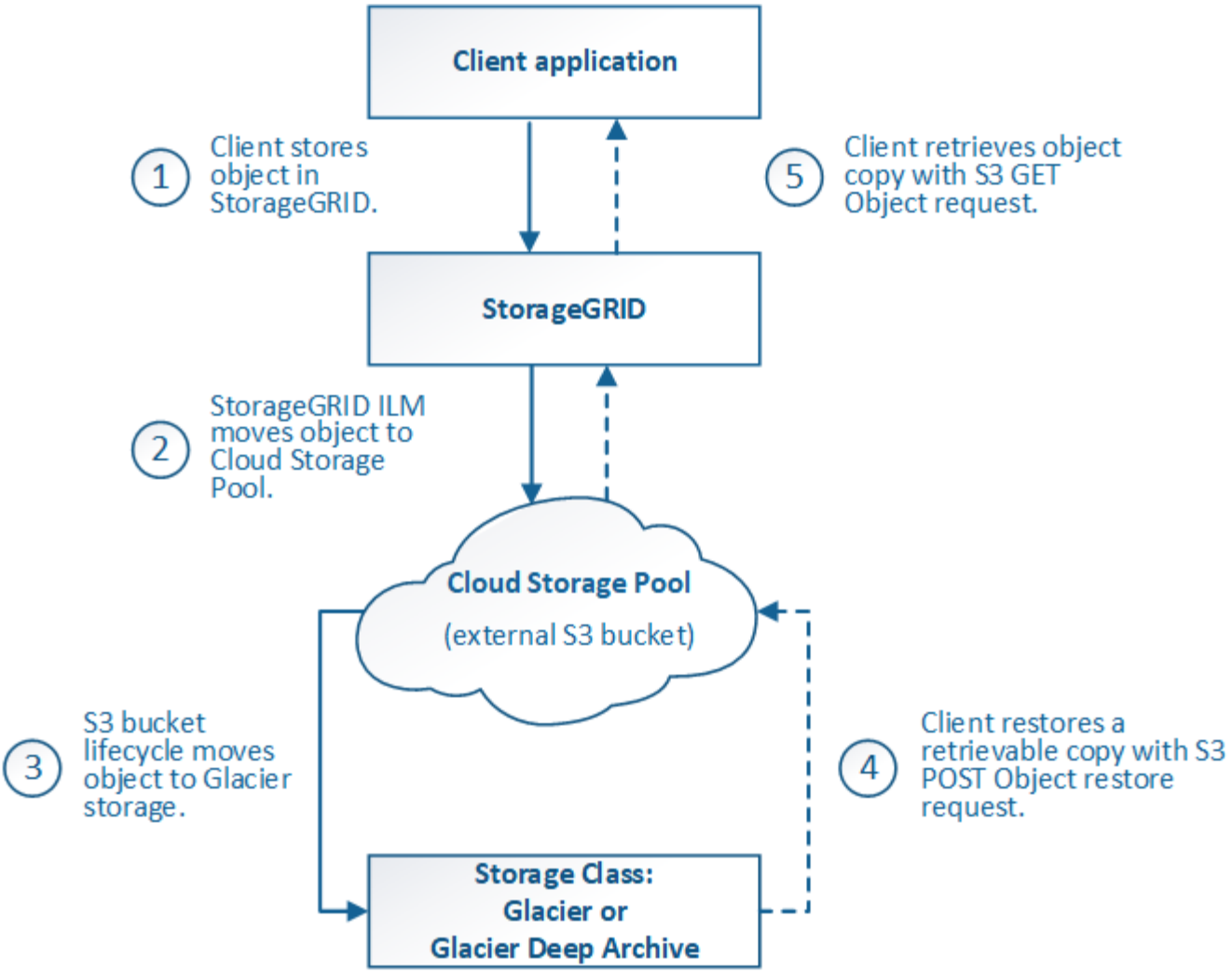
- S3： 云存储池对象的生命周期
- Azure： Cloud Storage Pool 对象的生命周期

S3： 云存储池对象的生命周期

此图显示了存储在 S3 云存储池中的对象的生命周期阶段。

在图和说明中， "`Glacier` " 是指 Glacier 存储类和 Glacier 深度归档存储类，但有一个例外：Glacier 深度归档存储类不支持加急还原层。仅支持批量或标准检索。

Google Cloud Platform （ GCP ）支持从长期存储中检索对象，而无需执行还原后操作。



1. * 存储在 StorageGRID 中的对象 *

   要开始生命周期，客户端应用程序会将对象存储在 StorageGRID 中。

2. * 对象已移至 S3 云存储池 *

   - 如果对象与使用 S3 云存储池作为其放置位置的 ILM 规则匹配，则 StorageGRID 会将此对象移动到云存储池指定的外部 S3 存储分段。
   - 将对象移动到 S3 云存储池后，客户端应用程序可以使用来自 StorageGRID 的 S3 GET 对象请求来检索该对象，除非该对象已过渡到 Glacier 存储。

3. * 已过渡到 Glacier 的对象（无法检索状态） *

   - 也可以将对象过渡到 Glacier 存储。例如，外部 S3 存储分段可能会使用生命周期配置立即或在一定天数后将对象过渡到 Glacier 存储。

   > 如果要过渡对象，必须为外部 S3 存储分段创建生命周期配置，并且必须使用实施 Glacier 存储类并支持 S3 后对象还原 API 的存储解决方案 。

> 不要对 Swift 客户端已载入的对象使用云存储池。Swift 不支持后对象还原请求，因此 StorageGRID 将无法检索已过渡到 S3 Glacier 存储的任何 Swift 对象。发出 Swift GET 对象请求以检索这些对象将失败（ 403 已禁用）。

- 过渡期间，客户端应用程序可以使用 S3 head Object 请求来监控对象的状态。

4. * 对象已从 Glacier 存储还原 *

   如果对象已过渡到 Glacier 存储，则客户端应用程序可以通过问题描述 处理 S3 后对象还原请求，将可检索的副本还原到 S3 云存储池。此请求指定在云存储池和数据访问层中应使用多少天的副本来执行还原操作（加急，标准或批量）。达到可检索副本的到期日期后，该副本将自动恢复为无法检索的状态。

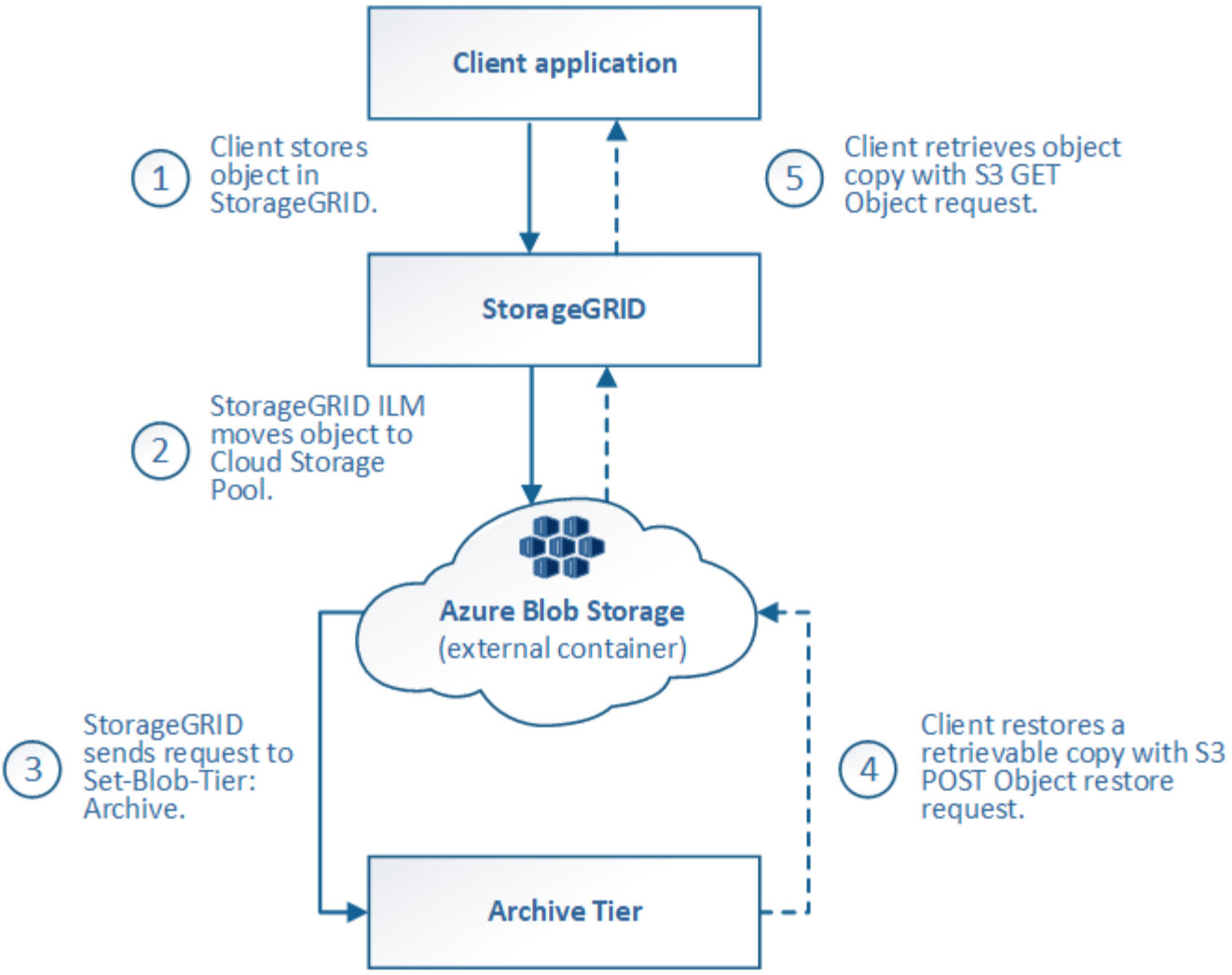
   > 如果 StorageGRID 中的存储节点上也存在对象的一个或多个副本，则无需发出 POST 对象还原请求来从 Glacier 中还原对象。相反，可以使用 GET 对象请求直接检索本地副本。

5. * 已检索对象 *

   还原对象后，客户端应用程序可以通过问题描述 获取对象请求来检索还原的对象。

Azure： Cloud Storage Pool 对象的生命周期

此图显示了存储在 Azure 云存储池中的对象的生命周期阶段。



1. * 存储在 StorageGRID 中的对象 *

   要开始生命周期，客户端应用程序会将对象存储在 StorageGRID 中。

2. * 对象已移至 Azure Cloud Storage Pool*

   如果对象与使用 Azure 云存储池作为其放置位置的 ILM 规则匹配，则 StorageGRID 会将此对象移动到云存储池指定的外部 Azure Blob 存储容器

   > 不要对 Swift 客户端已载入的对象使用云存储池。Swift 不支持后对象还原请求，因此 StorageGRID 将无法检索已过渡到 Azure Blob 存储归档层的任何 Swift 对象。发出 Swift GET 对象请求以检索这些对象将失败（ 403 已禁用）。

3. * 已过渡到归档层的对象（无法检索状态） *

   将对象移动到 Azure 云存储池后， StorageGRID 会立即自动将对象过渡到 Azure Blob 存储归档层。

4. * 对象已从归档层还原 *

   如果某个对象已过渡到归档层，则客户端应用程序可以通过问题描述 处理 S3 后对象还原请求将可检索的副本还原到 Azure 云存储池。

当 StorageGRID 收到后对象还原时，它会暂时将对象过渡到 Azure Blob 存储冷却层。一旦达到 POST 对象还原请求中的到期日期， StorageGRID 就会将该对象过渡回归档层。

如果 StorageGRID 中的存储节点上也存在对象的一个或多个副本，则无需通过发出 POST 对象还原请求从归档访问层还原对象。相反，可以使用 GET 对象请求直接检索本地副本。

5. * 已检索对象 *

   将对象还原到 Azure 云存储池后，客户端应用程序可以通过问题描述 获取对象请求来检索还原的对象。

相关信息

使用 S3

何时使用云存储池

云存储池可以在多种使用情形下提供显著优势。

在外部位置备份 **StorageGRID** 数据

您可以使用云存储池将 StorageGRID 对象备份到外部位置。

如果无法访问 StorageGRID 中的副本，则可以使用云存储池中的对象数据来处理客户端请求。但是，要访问云存储池中的备份对象副本，您可能需要发出问题描述 S3 后对象还原请求。

云存储池中的对象数据也可用于恢复因存储卷或存储节点故障而从 StorageGRID 丢失的数据。如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 会临时还原该对象，并在已恢复的存储节点上创建一个新副本。

要实施备份解决方案 ，请执行以下操作：

1. 创建一个云存储池。
2. 配置一个 ILM 规则，以便在存储节点上同时存储对象副本（以复制或擦除编码的副本的形式），并在云存储池中存储单个对象副本。
3. 将规则添加到 ILM 策略中。然后，模拟并激活策略。

将数据从 **StorageGRID** 分层到外部位置

您可以使用云存储池将对象存储在 StorageGRID 系统之外。例如，假设您需要保留大量对象，但您希望很少访问这些对象（如果有）。您可以使用云存储池将对象分层以降低存储成本并释放 StorageGRID 中的空间。

要实施分层解决方案 ，请执行以下操作：

1. 创建一个云存储池。
2. 配置一个 ILM 规则，以便将很少使用的对象从存储节点移动到云存储池。
3. 将规则添加到 ILM 策略中。然后，模拟并激活策略。

维护多个云端点

如果要将对象数据分层或备份到多个云，则可以配置多个云存储池。您可以通过 ILM 规则中的筛选器指定存储

在每个云存储池中的对象。例如，您可能希望将 Amazon S3 Glacier 中某些租户或分段中的对象以及 Azure Blob 存储中其他租户或分段中的对象存储起来。或者，您可能希望在 Amazon S3 Glacier 和 Azure Blob 存储之间移动数据。使用多个云存储池时，请注意，一个对象一次只能存储在一个云存储池中。

实施多个云端点：

1. 最多创建 10 个云存储池。
2. 配置 ILM 规则，以便在每个云存储池中的适当时间存储相应的对象数据。例如，将存储在云存储池 A 中的存储分段 A 中的对象，并将存储在云存储池 B 中的分段 B 中的对象存储在云存储池 B 中或者，将对象存储在云存储池 A 中一段时间，然后将其移动到云存储池 B
3. 将规则添加到 ILM 策略中。然后，模拟并激活策略。

云存储池注意事项

如果您计划使用云存储池将对象移出 StorageGRID 系统，则必须查看配置和使用云存储池的注意事项。

General considerations

- 通常，云归档存储（例如 Amazon S3 Glacier 或 Azure Blob 存储）是一个存储对象数据的廉价位置。但是，从云归档存储检索数据的成本相对较高。要实现最低的整体成本，您必须考虑何时以及多久访问一次云存储池中的对象。建议仅对预期不常访问的内容使用云存储池。
- 不要对 Swift 客户端已载入的对象使用云存储池。Swift 不支持后对象还原请求，因此 StorageGRID 将无法检索已过渡到 S3 Glacier 存储或 Azure Blob 存储归档层的任何 Swift 对象。发出 Swift GET 对象请求以检索这些对象将失败（ 403 已禁用）。
- 不支持将云存储池与 FabricPool 结合使用，因为从云存储池目标检索对象会增加延迟。

创建云存储池所需的信息

在创建云存储池之前，您必须先创建要用于云存储池的外部 S3 存储分段或外部 Azure Blob 存储容器。然后，在 StorageGRID 中创建云存储池时，必须指定以下信息：

- 提供程序类型： Amazon S3 或 Azure Blob Storage 。
- 如果选择 Amazon S3 ，则说明云存储池是否要与 AWS 机密区域（ * CAP （ C2S 访问门户） * ）结合使用。
- 分段或容器的确切名称。
- 访问存储分段或容器所需的服务端点。
- 访问存储分段或容器所需的身份验证：
  - * S3 ： 可选，访问密钥 ID 和机密访问密钥。
  - * C2S* ： 用于从 CAP 服务器获取临时凭据的完整 URL ；服务器 CA 证书，客户端证书，客户端证书的专用密钥；如果私钥已加密，则用于对其进行解密的密码短语。
  - * Azure Blob Storage* ： 帐户名称和帐户密钥。这些凭据必须具有容器的完全权限。
- （可选）自定义 CA 证书，用于验证与存储分段或容器的 TLS 连接。

用于云存储池的端口的注意事项

要确保 ILM 规则可以将对象移入和移出指定的云存储池，您必须配置包含系统存储节点的一个或多个网络。您必须确保以下端口可以与云存储池进行通信。

默认情况下，云存储池使用以下端口：

- * 80* ： 对于以 http 开头的端点 URI
- * 443 ： 对于以 https 开头的端点 URI

您可以在创建或编辑云存储池时指定其他端口。

如果使用非透明代理服务器，则还必须使用 配置存储代理 允许将消息发送到外部端点，例如 Internet 上的端点。

成本注意事项

使用云存储池访问云中的存储需要通过网络连接到云。您必须根据希望使用云存储池在 StorageGRID 和云之间移动的数据量，考虑用于访问云并适当配置云的网络基础架构的成本。

当 StorageGRID 连接到外部云存储池端点时，它会发出各种请求来监控连接并确保它可以执行所需的操作。虽然这些请求会产生一些额外成本，但监控云存储池的成本只能是在 S3 或 Azure 中存储对象的总成本的一小部分。

如果您需要将对象从外部云存储池端点移回 StorageGRID ，可能会产生更显著的成本。在以下任一情况下，对象可能会移回 StorageGRID ：

- 此对象的唯一副本位于云存储池中，您决定将此对象存储在 StorageGRID 中。在这种情况下，您只需重新配置 ILM 规则和策略即可。进行 ILM 评估时， StorageGRID 会发出多个请求，以便从云存储池中检索对象。然后， StorageGRID 会在本地创建指定数量的复制副本或经过纠删编码的副本。将对象移回 StorageGRID 后，云存储池中的副本将被删除。
- 由于存储节点故障，对象丢失。如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 会临时还原该对象，并在已恢复的存储节点上创建一个新副本。

> 当对象从云存储池移回 StorageGRID 时， StorageGRID 会为每个对象向云存储池端点发出多个请求。在移动大量对象之前，请联系技术支持以帮助估算时间范围和相关成本。

S3 ： 云存储池存储分段所需的权限

用于云存储池的外部 S3 存储分段的分段策略必须授予 StorageGRID 将对象移动到分段，获取对象状态，根据需要从 Glacier 存储还原对象等的权限。理想情况下， StorageGRID 应对存储分段具有完全控制访问权限（ `s3 : *` ）；但是，如果无法访问，存储分段策略必须向 StorageGRID 授予以下 S3 权限：

- `s 3 : AbortMultipartUpload`
- `s 3 : DeleteObject`
- `s 3 : GetObject`
- `s 3 : ListBucket`
- `s 3 : ListBucketMultipartUploads`

- `s 3 ： ListMultipartUploadPart`
- `s 3 ： PutObject`
- `s 3 ： RestoreObject`

S3：外部存储分段的生命周期注意事项

StorageGRID 与云存储池中指定的外部 S3 存储分段之间的对象移动由 StorageGRID 中的 ILM 规则和活动 ILM 策略控制。相比之下，对象从云存储池中指定的外部 S3 存储分段过渡到 Amazon S3 Glacier 或 S3 Glacier 深度归档（或过渡到实施 Glacier 存储类的存储解决方案）则由该分段的生命周期配置控制。

如果要从云存储池过渡对象，必须在外部 S3 存储分段上创建适当的生命周期配置，并且必须使用实施 Glacier 存储类并支持 S3 后对象还原 API 的存储解决方案。

例如，假设您希望将从 StorageGRID 移动到云存储池的所有对象立即过渡到 Amazon S3 Glacier 存储。您应在外部 S3 存储分段上创建一个生命周期配置，用于指定单个操作（* 过渡 *），如下所示：

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

此规则会在创建所有存储分段对象的日期（即从 StorageGRID 迁移到云存储池的日期）将这些对象过渡到 Amazon S3 Glacier。

> 配置外部存储分段的生命周期时，切勿使用 * 到期 * 操作来定义对象何时过期。到期操作发生原因 外部存储系统以删除已过期的对象。如果稍后尝试从 StorageGRID 访问已过期的对象，则无法找到已删除的对象。

如果要将云存储池中的对象过渡到 S3 Glacier 深度归档（而不是 Amazon S3 Glacier），请在存储分段生命周期中指定 ` <StorageClass>Deep_archive</StorageClass>` 。但是，请注意，您不能使用 `Expedited` 层从 S3 Glacier Deep Archive 还原对象。

Azure： 访问层注意事项

配置 Azure 存储帐户时，您可以将默认访问层设置为热或冷。创建用于云存储池的存储帐户时，应使用热层作为默认层。即使 StorageGRID 在将对象移动到云存储池时会立即将层设置为归档，但使用默认设置 " 热 " 可确保在至少 30 天之前从冷层中删除的对象不会收到提前删除费用。

Azure： 不支持生命周期管理

请勿对与云存储池一起使用的容器使用 Azure Blob Storage 生命周期管理。生命周期操作可能会干扰云存储池操作。

相关信息

- 创建云存储池
- S3： 指定云存储池的身份验证详细信息
- C2S S3： 指定云存储池的身份验证详细信息
- Azure： 指定云存储池的身份验证详细信息

比较云存储池和 **CloudMirror** 复制

在开始使用云存储池时，了解云存储池与 StorageGRID CloudMirror 复制服务之间的相似之处和不同之处可能会很有帮助。

	云存储池	**CloudMirror** 复制服务
主要目的是什么？	云存储池充当归档目标。云存储池中的对象副本可以是对象的唯一副本，也可以是其他副本。也就是说，您只能在 StorageGRID 中保留一个副本并将一个副本发送到云存储池，而不是在内部保留两个副本。	通过 CloudMirror 复制服务，租户可以自动将对象从 StorageGRID （源）中的存储分段复制到外部 S3 存储分段（目标）。CloudMirror 复制会在独立的 S3 基础架构中为对象创建一个独立副本。
如何设置？	云存储池的定义方式与存储池相同，可使用网格管理器或网格管理 API 。可以在 ILM 规则中选择云存储池作为放置位置。虽然存储池包含一组存储节点，但云存储池是使用远程 S3 或 Azure 端点（ IP 地址，凭据等）定义的。	租户用户 配置 CloudMirror 复制 通过使用租户管理器或 S3 API 定义 CloudMirror 端点（ IP 地址，凭据等）。设置 CloudMirror 端点后，可以将该租户帐户拥有的任何分段配置为指向 CloudMirror 端点。
谁负责设置？	通常是网格管理员	通常是租户用户
目标是什么？	• 任何兼容的 S3 基础架构（包括 Amazon S3 ） • Azure Blob 归档层	• 任何兼容的 S3 基础架构（包括 Amazon S3 ）
将对象移动到目标的原因是什么？	活动 ILM 策略中的一个或多个 ILM 规则。ILM 规则定义 StorageGRID 将哪些对象移动到云存储池以及何时移动这些对象。	将新对象载入已配置 CloudMirror 端点的源分段的操作。在使用 CloudMirror 端点配置分段之前，源分段中存在的对象不会复制，除非已进行修改。

	云存储池	**CloudMirror** 复制服务
如何检索对象？	应用程序必须向 StorageGRID 发出请求，以检索已移动到云存储池的对象。如果某个对象的唯一副本已过渡到归档存储，则 StorageGRID 会管理还原该对象的过程，以便可以检索该对象。	由于目标存储分段中的镜像副本是一个独立的副本，因此应用程序可以通过向 StorageGRID 或 S3 目标发出请求来检索对象。例如，假设您使用 CloudMirror 复制将对象镜像到合作伙伴组织。配对节点可以使用自己的应用程序直接从 S3 目标读取或更新对象。不需要使用 StorageGRID 。
是否可以直接从目标读取？	否移动到云存储池的对象由 StorageGRID 管理。读取请求必须定向到 StorageGRID （ StorageGRID 将负责从云存储池中检索）。	可以，因为镜像副本是一个独立副本。
如果从源中删除对象，会发生什么情况？	此对象也会在云存储池中删除。	不会复制删除操作。已删除的对象不再位于 StorageGRID 存储分段中，但它仍位于目标存储分段中。同样，可以删除目标分段中的对象而不影响源。
发生灾难后如何访问对象（ StorageGRID 系统无法运行）？	必须恢复发生故障的 StorageGRID 节点。在此过程中，复制对象的副本可能会使用云存储池中的副本进行还原。	CloudMirror 目标中的对象副本独立于 StorageGRID ，因此可以在恢复 StorageGRID 节点之前直接访问这些副本。

创建云存储池

创建云存储池时，您需要指定 StorageGRID 用于存储对象的外部存储分段或容器的名称和位置，云提供程序类型（ Amazon S3 或 Azure Blob Storage ）以及 StorageGRID 访问外部存储分段或容器所需的信息。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已查看配置云存储池的准则。
- 云存储池引用的外部存储分段或容器已存在。
- 您拥有访问存储分段或容器所需的所有身份验证信息。

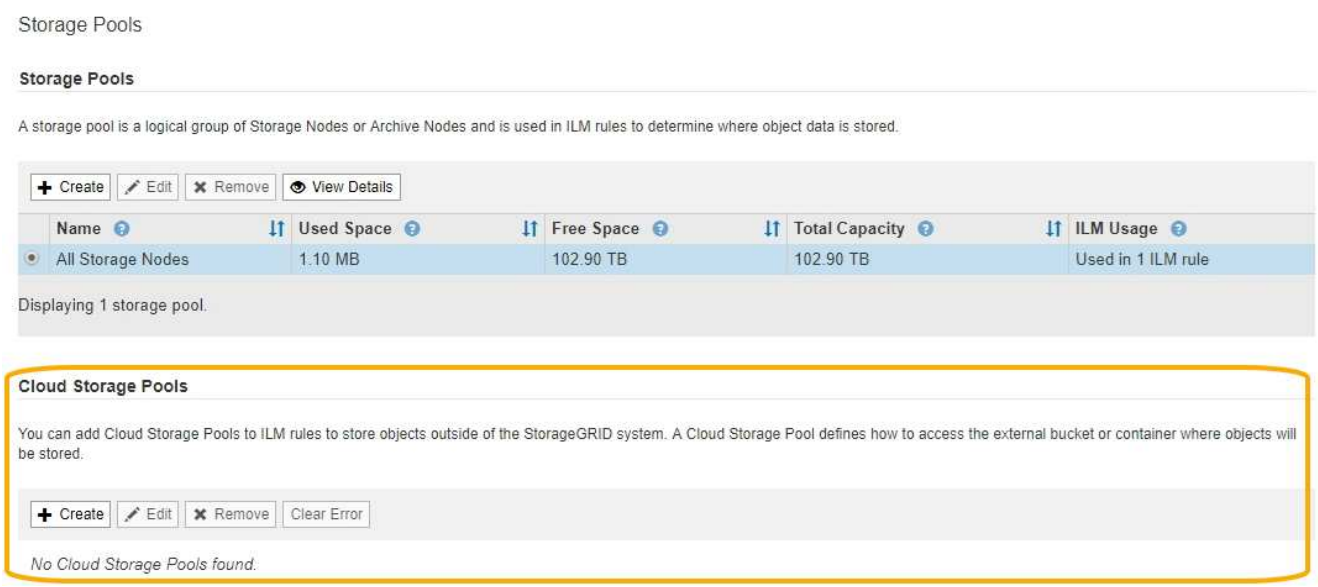
关于此任务

云存储池指定一个外部 S3 存储分段或 Azure Blob 存储容器。StorageGRID 会在您保存云存储池后立即对其进行验证，因此您必须确保云存储池中指定的存储分段或容器存在且可访问。

步骤

1. 选择 * ILM * > * 存储池 * 。

   此时将显示存储池页面。此页面包含两个部分：存储池和云存储池。



2. 在页面的 Cloud Storage Pools 部分中，选择 * 创建 * 。

   此时将显示创建云存储池对话框。

3. 输入以下信息：

字段	Description
显示名称	一个名称，用于简要说明云存储池及其用途。在配置 ILM 规则时，请使用易于识别的名称。
提供程序类型	您将在此云存储池中使用哪个云提供商： • * Amazon S3* ：为 S3 ， C2S S3 或 Google Cloud Platform （ GCP ）端点选择此选项。 • * Azure Blob 存储 * ◦ 注： * 选择提供程序类型时，页面底部将显示服务端点，身份验证和服务器验证部分。

字段	Description
存储分段或容器	为云存储池创建的外部 S3 存储分段或 Azure 容器的名称。此处指定的名称必须与存储分段或容器的名称完全匹配，否则创建云存储池将失败。保存云存储池后，您无法更改此值。

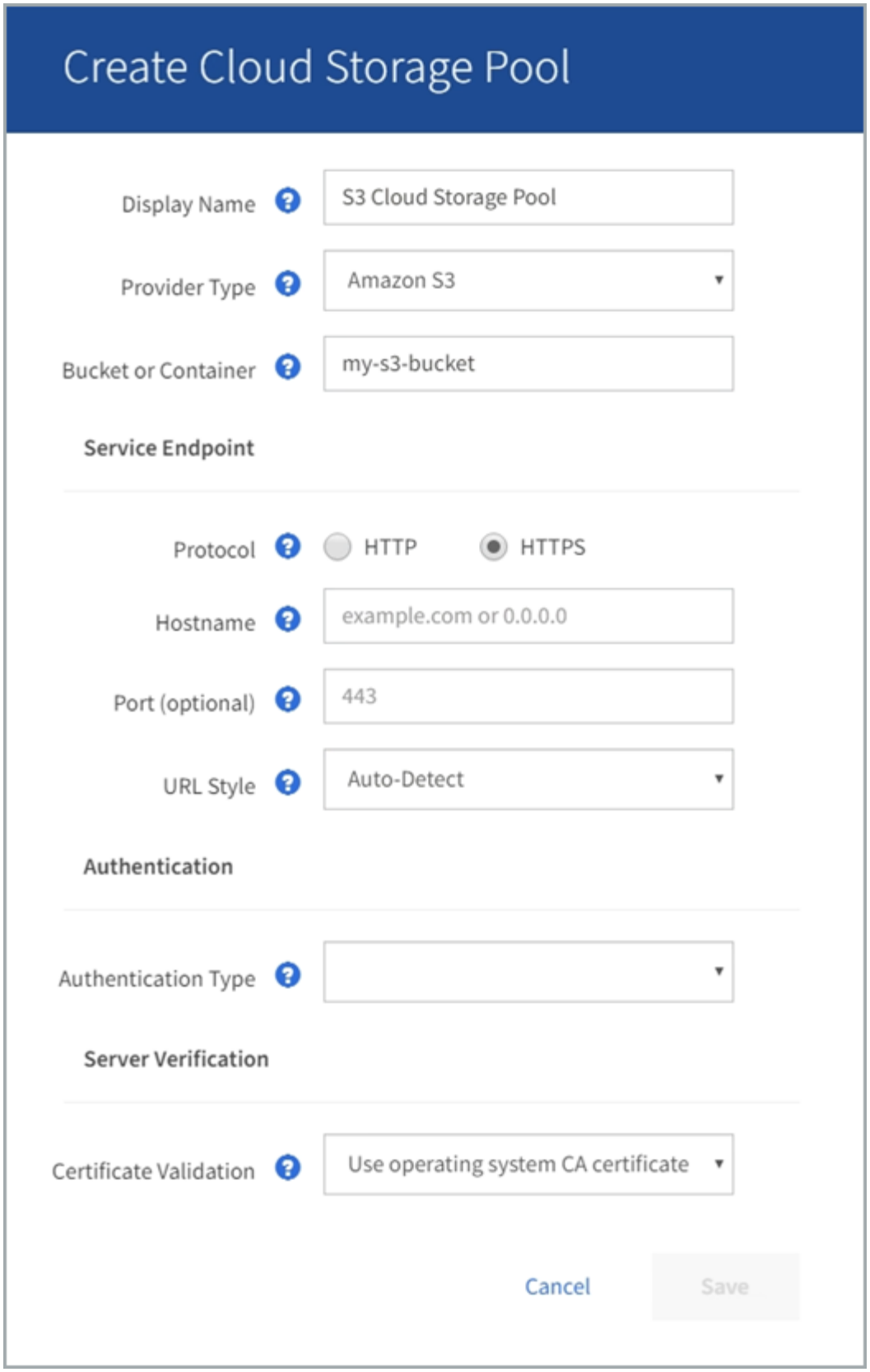
4. 根据选定提供程序类型，完成页面的服务端点，身份验证和服务器验证部分。
   - S3： 指定云存储池的身份验证详细信息
   - C2S S3： 指定云存储池的身份验证详细信息
   - Azure： 指定云存储池的身份验证详细信息

S3： 指定云存储池的身份验证详细信息

在为 S3 创建云存储池时，必须选择云存储池端点所需的身份验证类型。您可以指定匿名或输入访问密钥 ID 和机密访问密钥。

您需要的内容

- 您已输入云存储池的基本信息并指定 * Amazon S3* 作为提供程序类型。



- 如果您使用的是访问密钥身份验证，则知道外部 S3 存储分段的访问密钥 ID 和机密访问密钥。

步骤

1. 在 * 服务端点 * 部分中，提供以下信息：

a. 选择要在连接到云存储池时使用的协议。

   默认协议为 HTTPS 。

b. 输入云存储池的服务器主机名或 IP 地址。

   例如：

   `s3-aws-region.amazonaws.com`

   请勿在此字段中包含存储分段名称。您可以在 * 分段或容器 * 字段中包含分段名称。

a. （可选）指定在连接到云存储池时应使用的端口。

   将此字段留空可使用默认端口：端口 443 用于 HTTPS ，端口 80 用于 HTTP 。

b. 选择 Cloud Storage Pool 存储分段的 URL 模式：

选项	Description
虚拟托管模式	使用虚拟托管模式 URL 访问存储分段。虚拟托管模式 URL 会将存储分段名称包含在域名中，例如 ` + https://bucket-name.s3.company.com/key-name+` 。
路径模式	使用路径模式 URL 访问存储分段。路径模式 URL 的末尾包含分段名称，例如 ` https://s3.company.com/bucket-name/key-name` 。 • 注： * 路径模式 URL 已弃用。
自动检测	尝试根据提供的信息自动检测要使用的 URL 模式。例如，如果指定 IP 地址， StorageGRID 将使用路径模式的 URL 。仅当您不知道要使用哪种特定模式时，才选择此选项。

2. 在 * 身份验证 * 部分中，选择云存储池端点所需的身份验证类型。

选项	Description
访问密钥	要访问云存储池存储分段，需要访问密钥 ID 和机密访问密钥。
匿名	每个人都有权访问云存储池存储分段。不需要访问密钥 ID 和机密访问密钥。
CAP （ C2S 访问门户）	仅用于 C2S S3 。转至 C2S S3 ： 指定云存储池的身份验证详细信息。

3. 如果选择了访问密钥，请输入以下信息：

选项	Description
访问密钥 ID	拥有外部存储分段的帐户的访问密钥 ID 。
机密访问密钥	关联的机密访问密钥。

4. 在服务器验证部分中，选择应使用哪种方法验证与云存储池的 TLS 连接的证书：

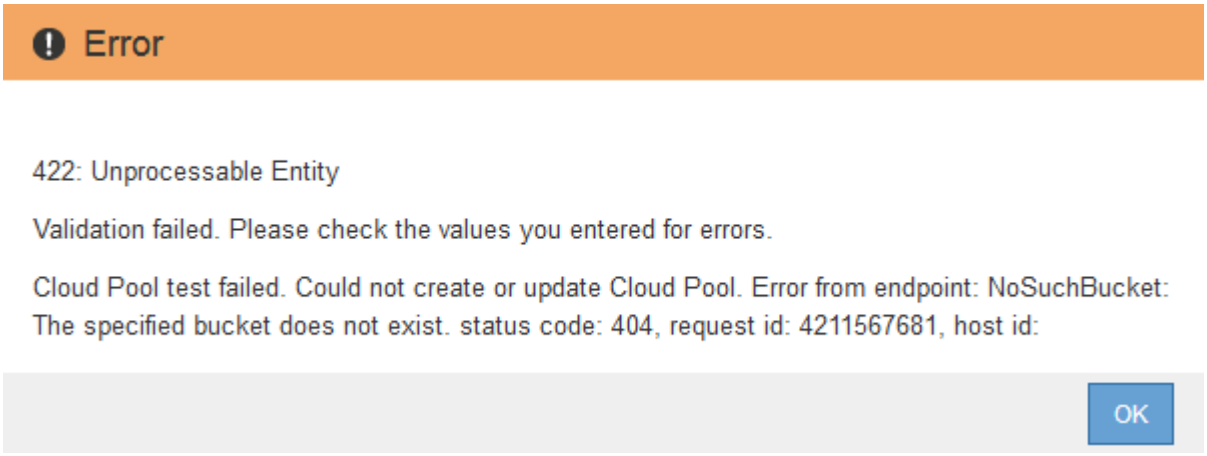
选项	Description
使用操作系统 CA 证书	使用操作系统上安装的默认网格 CA 证书来保护连接。
使用自定义 CA 证书	使用自定义 CA 证书。选择 * 选择新 * ，然后上传 PEM 编码的 CA 证书。
请勿验证证书	未验证用于 TLS 连接的证书。

5. 选择 * 保存 * 。

保存云存储池时， StorageGRID 将执行以下操作：

- 验证存储分段和服务端点是否存在，以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入存储分段，以将存储分段标识为云存储池。切勿删除名为 `x-ntap-sgws-cloud pool-uuid` 的文件。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如，如果存在证书错误或您指定的存储分段不存在，则可能会报告错误。



请参见的说明 对云存储池进行故障排除，解析问题描述 ，然后再次尝试保存云存储池。

C2S S3 ：指定云存储池的身份验证详细信息

要将商用云服务（ C2S ） S3 服务用作云存储池，您必须将 C2S 访问门户（ CAP ）配置为身份验证类型，以便 StorageGRID 可以请求临时凭据来访问 C2S 帐户中的 S3 存储分段。

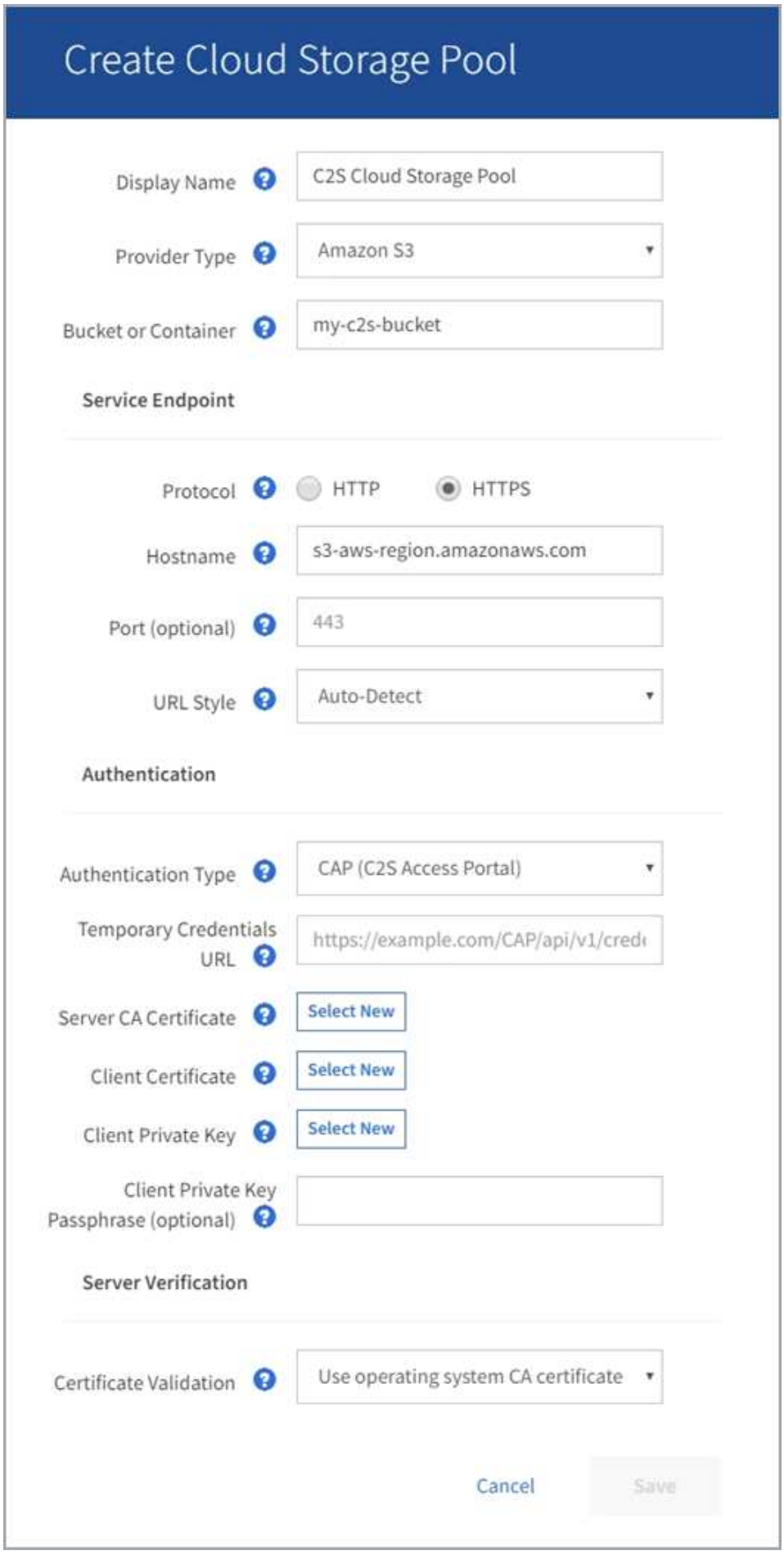
您需要的内容

- 您已输入 Amazon S3 云存储池的基本信息，包括服务端点。
- 您知道 StorageGRID 用于从 CAP 服务器获取临时凭据的完整 URL ，包括分配给 C2S 帐户的所有必需和可选 API 参数。
- 您拥有一个由适当的政府证书颁发机构（ CA ）颁发的服务器 CA 证书。StorageGRID 使用此证书来验证 CAP 服务器的身份。服务器 CA 证书必须使用 PEM 编码。
- 您拥有一个由适当的政府证书颁发机构（ CA ）颁发的客户端证书。StorageGRID 使用此证书向 CAP 服务器标识自身。客户端证书必须使用 PEM 编码，并且必须已授予对 C2S 帐户的访问权限。
- 您已为客户端证书使用 PEM 编码的专用密钥。
- 如果客户端证书的专用密钥已加密，则您可以使用密码短语对其进行解密。

步骤

1. 在 * 身份验证 * 部分中，从 * 身份验证类型 * 下拉列表中选择 * CAP （ C2S Access Portal ） * 。

   此时将显示 CAP C2S 身份验证字段。


Create Cloud Storage Pool
Display Name
C2S Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-c2s-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
URL Style
Auto-Detect
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/cred
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. 请提供以下信息：

   a. 对于 * 临时凭据 URL* ，输入 StorageGRID 从 CAP 服务器获取临时凭据所使用的完整 URL ，包括分配给 C2S 帐户的所有必需和可选 API 参数。

   b. 对于 * 服务器 CA 证书 * ，选择 * 选择新 * ，然后上传 PEM 编码的 CA 证书， StorageGRID 将使用该证书来验证 CAP 服务器。

   c. 对于 * 客户端证书 * ，选择 * 选择新 * ，然后将 StorageGRID 用于标识自身的 PEM 编码证书上传到 CAP 服务器。

   d. 对于 * 客户端专用密钥 * ，选择 * 选择新 * ，然后为客户端证书上传 PEM 编码的专用密钥。

      如果私钥已加密，则必须使用传统格式。（不支持 PKCS 8 加密格式。）

   e. 如果客户端专用密钥已加密，请输入用于对客户端专用密钥进行解密的密码短语。否则，请将 * 客户端专用密钥密码短语 * 字段留空。

3. 在服务器验证部分中，提供以下信息：

   a. 对于 * 证书验证 * ，选择 * 使用自定义 CA 证书 * 。

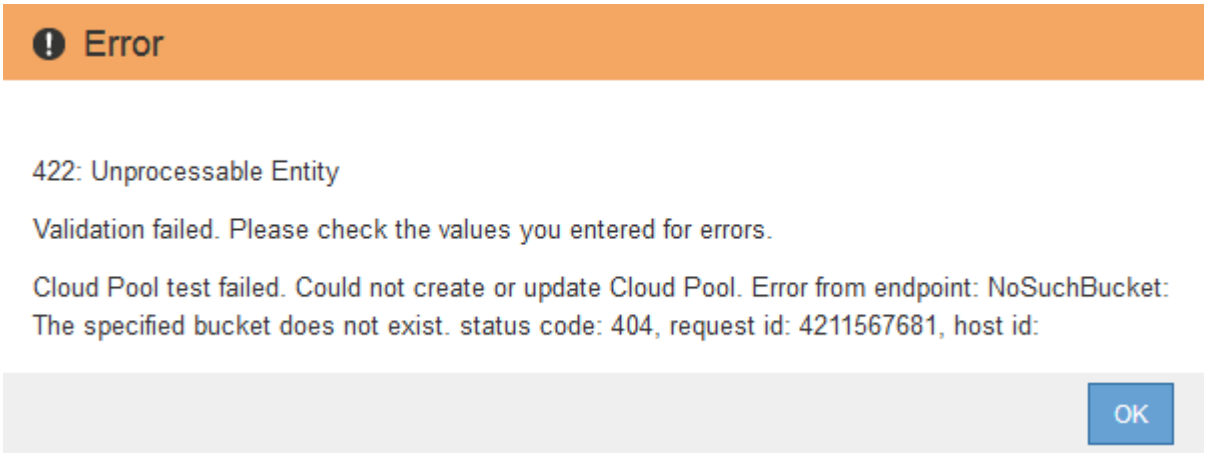
   b. 选择 * 选择新 * ，然后上传 PEM 编码的 CA 证书。

4. 选择 * 保存 * 。

保存云存储池时， StorageGRID 将执行以下操作：

- 验证存储分段和服务端点是否存在，以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入存储分段，以将存储分段标识为云存储池。切勿删除名为 `x-ntap-sgws-cloud pool-uuid` 的文件。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如，如果存在证书错误或您指定的存储分段不存在，则可能会报告错误。



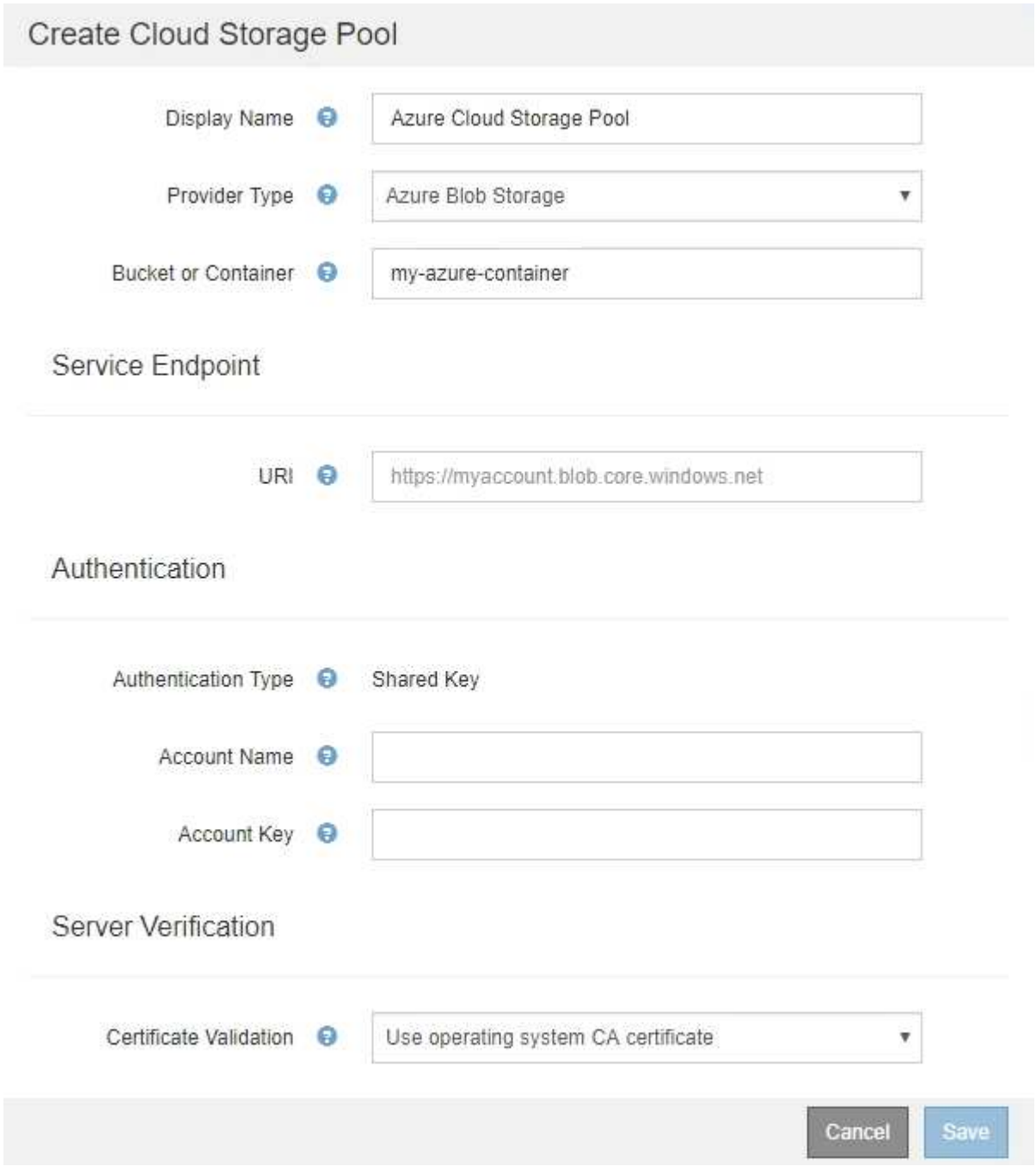
请参见的说明 对云存储池进行故障排除，解析问题描述 ，然后再次尝试保存云存储池。

Azure ： 指定云存储池的身份验证详细信息

为 Azure Blob 存储创建云存储池时，必须为 StorageGRID 用于存储对象的外部容器指定帐户名称和帐户密钥。

您需要的内容

- 您已输入云存储池的基本信息并指定 * Azure Blob Storage* 作为提供程序类型。* 共享密钥 * 显示在 * 身份验证类型 * 字段中。



- 您知道用于访问用于云存储池的 Blob 存储容器的统一资源标识符（ Uniform Resource Identifier ， URI ）。
- 您知道存储帐户的名称和机密密钥。您可以使用 Azure 门户查找这些值。

步骤

1. 在 * 服务端点 * 部分中，输入用于访问用于云存储池的 Blob 存储容器的统一资源标识符（ Uniform Resource Identifier ， URI ）。

   使用以下格式之一指定 URI ：

- ` + https://host:port+`
- ` + http://host:port+`

如果未指定端口，则默认情况下，端口 443 用于 HTTPS URI ，端口 80 用于 HTTP URI 。+ + * Azure Blob 存储容器的示例 URI * ： + `https://myaccount.blob.core.windows.net`

2. 在 * 身份验证 * 部分中，提供以下信息：
   a. 对于 * 帐户名称 * ，输入拥有外部服务容器的 Blob 存储帐户的名称。
   b. 对于 * 帐户密钥 * ，输入 Blob 存储帐户的机密密钥。

   对于 Azure 端点，您必须使用共享密钥身份验证。

3. 在 * 服务器验证 * 部分中，选择应使用哪种方法验证与云存储池的 TLS 连接的证书：

选项	Description
使用操作系统 CA 证书	使用操作系统上安装的网格 CA 证书确保连接安全。
使用自定义 CA 证书	使用自定义 CA 证书。选择 * 选择新 * ，然后上传 PEM 编码的证书。
请勿验证证书	未验证用于 TLS 连接的证书。

4. 选择 * 保存 * 。

保存云存储池时， StorageGRID 将执行以下操作：

- 验证容器和 URI 是否存在，以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入容器，以将其标识为云存储池。切勿删除名为 `x-ntap-sgws-cloud pool-uuid` 的文件。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如，如果存在证书错误或您指定的容器不存在，则可能会报告错误。

请参见的说明 对云存储池进行故障排除，解析问题描述 ，然后再次尝试保存云存储池。

编辑云存储池

您可以编辑云存储池以更改其名称，服务端点或其他详细信息；但是，您不能更改云存储池的 S3 存储分段或 Azure 容器。

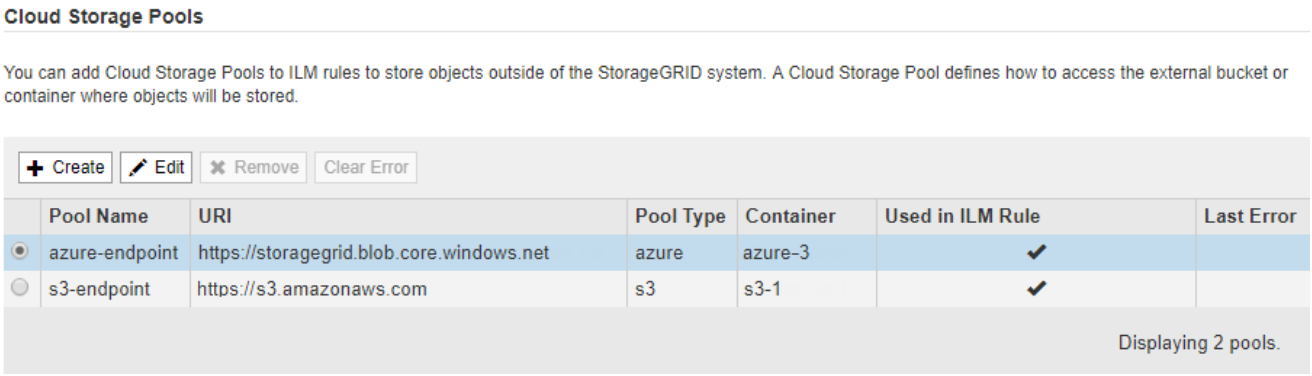
您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已查看 云存储池注意事项。

步骤

1. 选择 * ILM * > * 存储池 * 。

此时将显示存储池页面。" 云存储池 " 表列出了现有的云存储池。



2. 选择要编辑的云存储池的单选按钮。
3. 选择 * 编辑 * 。
4. 根据需要更改显示名称，服务端点，身份验证凭据或证书验证方法。

   您不能更改云存储池的提供程序类型或 S3 存储分段或 Azure 容器。

   如果您先前上传了服务器或客户端证书，则可以选择 * 查看当前 * 来查看当前正在使用的证书。

5. 选择 * 保存 * 。

   保存云存储池时， StorageGRID 会验证存储分段或容器以及服务端点是否存在，以及是否可以使用您指定的凭据访问它们。

   如果云存储池验证失败，则会显示一条错误消息。例如，如果存在证书错误，则可能会报告错误。

   请参见的说明 对云存储池进行故障排除，解析问题描述 ，然后再次尝试保存云存储池。

删除云存储池

您可以删除未在 ILM 规则中使用且不包含对象数据的云存储池。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已确认 S3 存储分段或 Azure 容器不包含任何对象。如果您尝试删除包含对象的云存储池，则会发生错误。请参见 对云存储池进行故障排除。

  创建云存储池时， StorageGRID 会将标记文件写入存储分段或容器，以将其标识为云存储池。请勿删除名为 `x-ntap-sgws-cloud pool-uuid` 的文件。

- 您已删除可能已使用此池的任何 ILM 规则。

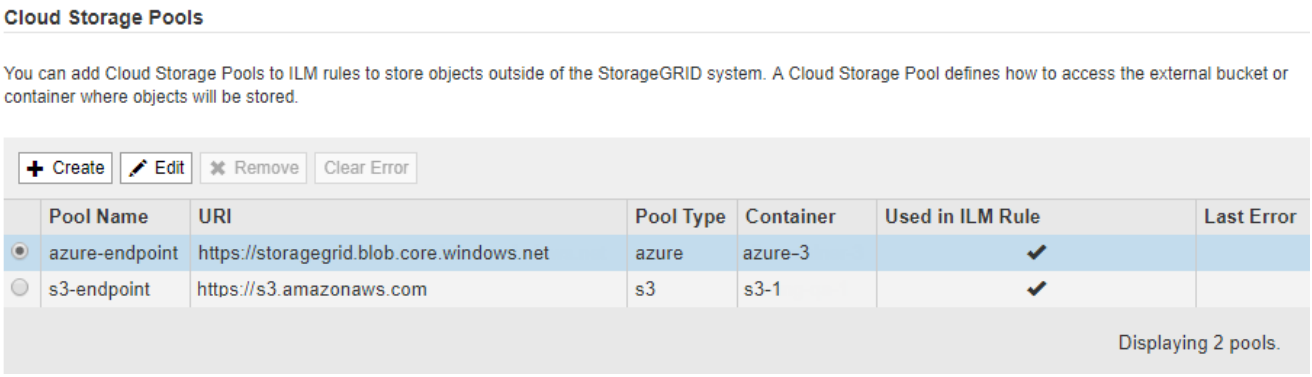
步骤

1. 选择 * ILM * > * 存储池 * 。

此时将显示存储池页面。

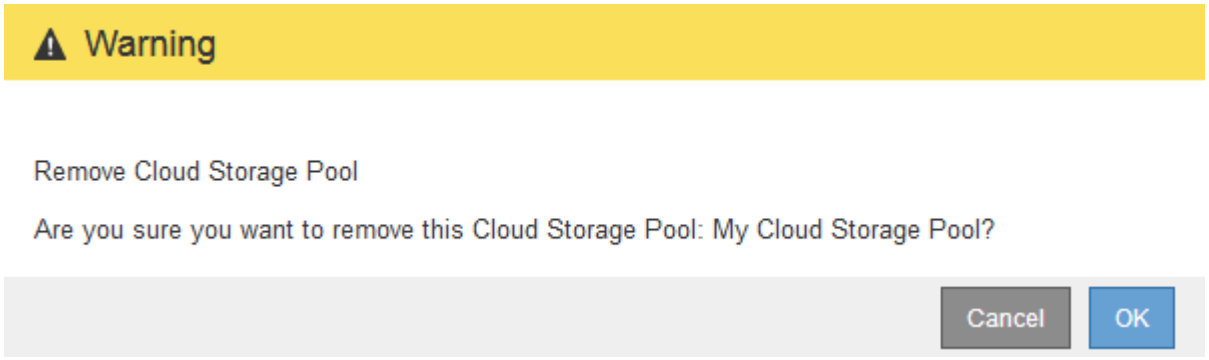
2. 选择 ILM 规则中当前未使用的云存储池的单选按钮。

   如果在 ILM 规则中使用云存储池，则无法将其删除。已禁用 * 删除 * 按钮。



3. 选择 * 删除 * 。

   此时将显示确认警告。



4. 选择 * 确定 * 。

   此时将删除云存储池。

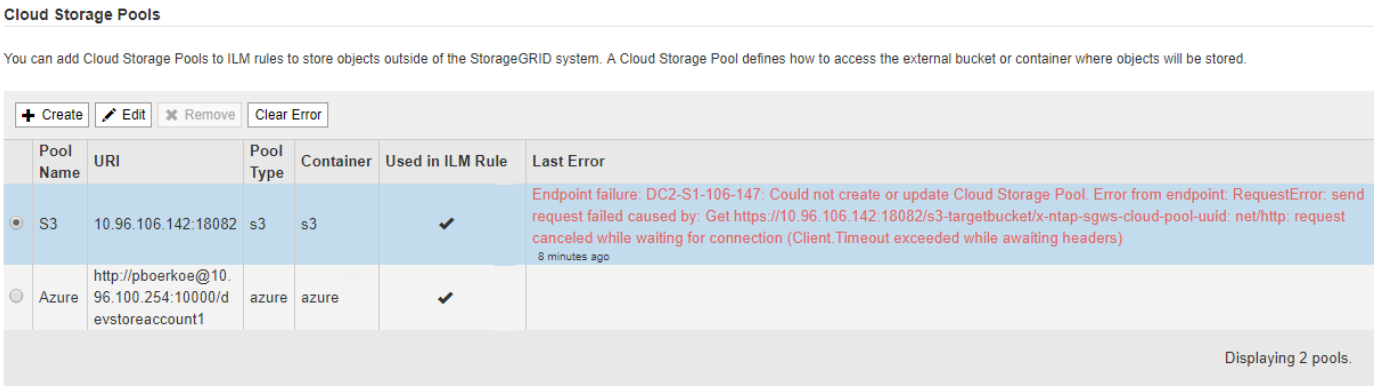
对云存储池进行故障排除

如果在创建，编辑或删除云存储池时遇到错误，请使用以下故障排除步骤帮助解决问题描述 。

确定是否发生错误

StorageGRID 每分钟对每个云存储池执行一次简单的运行状况检查，以确保云存储池可以访问并正常运行。如果运行状况检查检测到问题描述 ，则存储池页面上的云存储池表的最后一个错误列将显示一条消息。

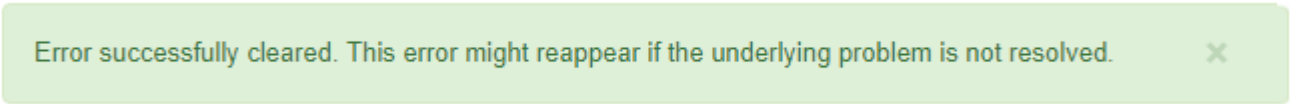
此表显示了为每个云存储池检测到的最新错误，并指示错误发生的时间。



此外，如果运行状况检查检测到在过去 5 分钟内发生了一个或多个新的 Cloud Storage Pool 错误，则会触发 * 云存储池连接错误 * 警报。如果收到有关此警报的电子邮件通知，请转到存储池页面（选择 * ILM * > * 存储池 * ），查看上次错误列中的错误消息，并参考以下故障排除准则。

检查错误是否已解决

解决任何底层问题后，您可以确定错误是否已解决。从云存储池页面中，选择端点的单选按钮，然后选择 * 清除错误 * 。确认消息指示 StorageGRID 已清除云存储池的错误。



如果根本问题已解决，则不再显示此错误消息。但是，如果根本问题尚未修复（或者遇到了不同的错误），则错误消息将在几分钟内显示在 Last Error 列中。

错误：此云存储池包含意外内容

尝试创建，编辑或删除云存储池时，可能会遇到此错误。如果存储分段或容器包含 `x-ntap-sgws-cloud pool-uuid` 标记文件，但该文件没有预期的 UUID ，则会发生此错误。

通常，只有在创建新的云存储池且另一个 StorageGRID 实例已使用同一个云存储池时，您才会看到此错误。

请尝试以下步骤以更正问题描述：

- 请检查以确保您的组织中没有人也在使用此云存储池。
- 删除 `x-ntap-sgws-cloud pool-uuid` 文件，然后尝试重新配置云存储池。

错误：无法创建或更新云存储池。端点出错

在尝试创建或编辑云存储池时，您可能会遇到此错误。此错误表示某种类型的连接或配置问题描述 正在阻止 StorageGRID 写入云存储池。

要更正问题描述 ，请查看来自端点的错误消息。

- 如果错误消息包含 `GET *URL* ： eOF` ，请检查用于云存储池的服务端点是否不对需要 HTTPS 的容器或分段使用 HTTP 协议。
- 如果错误消息包含 `GET *URL* ： net/http ： Request cancelled while waiting for connection` ，请验证网络配置是否允许存储节点访问用于云存储池的服务端点。

- 对于所有其他端点错误消息，请尝试以下一项或多项操作：
  - 创建一个与您为云存储池输入的名称相同的外部容器或存储分段，然后再次尝试保存新的云存储池。
  - 更正为云存储池指定的容器或存储分段名称，然后重新尝试保存新的云存储池。

错误：无法解析 **CA** 证书

在尝试创建或编辑云存储池时，您可能会遇到此错误。如果 StorageGRID 无法解析您在配置云存储池时输入的证书，则会发生此错误。

要更正问题描述 ，请检查您提供的 CA 证书是否存在问题。

错误：未找到具有此 **ID** 的云存储池

尝试编辑或删除云存储池时，可能会遇到此错误。如果端点返回 404 响应，则会发生此错误，这可能表示以下任一项：

- 用于云存储池的凭据不具有此存储分段的读取权限。
- 用于云存储池的存储分段不包括 `x-ntax-sgws-cloud -pool-uuid` 标记文件。

尝试以下一个或多个步骤以更正问题描述 ：

- 检查与配置的访问密钥关联的用户是否具有所需权限。
- 使用具有所需权限的凭据编辑云存储池。
- 如果权限正确，请联系支持部门。

错误：无法检查云存储池的内容。端点出错

在尝试删除云存储池时，您可能会遇到此错误。此错误表示某种类型的连接或配置问题描述 正在阻止 StorageGRID 读取云存储池存储分段的内容。

要更正问题描述 ，请查看来自端点的错误消息。

错误：对象已放置在此存储分段中

在尝试删除云存储池时，您可能会遇到此错误。如果某个云存储池包含通过 ILM 移动到该存储池的数据，在配置云存储池之前存储在存储分段中的数据或在创建云存储池之后某些其他源放置在存储分段中的数据，则不能删除该存储池。

尝试以下一个或多个步骤以更正问题描述 ：

- 按照 "`云存储池对象的生命周期 " 中的说明将对象移回 StorageGRID 。`
- 如果您确定其余对象未被 ILM 放置在云存储池中，请手动从存储分段中删除这些对象。

> 切勿手动删除云存储池中可能已由 ILM 放置的对象。如果稍后尝试从 StorageGRID 访问手动删除的对象，则找不到已删除的对象。

错误：代理尝试访问云存储池时遇到外部错误

如果您在存储节点与用于云存储池的外部 S3 端点之间配置了非透明存储代理，则可能会遇到此错误。如果外部代理服务器无法访问云存储池端点，则会发生此错误。例如， DNS 服务器可能无法解析主机名，或者可能存在外部网络问题描述 。

尝试以下一个或多个步骤以更正问题描述：

- 检查云存储池（ * ILM * > * 存储池 * ）的设置。
- 检查存储代理服务器的网络配置。

相关信息

云存储池对象的生命周期

配置擦除编码配置文件

创建擦除编码配置文件

要创建擦除编码配置文件，请将包含存储节点的存储池与擦除编码方案关联。此关联可确定创建的数据和奇偶校验片段的数量，以及系统将这些片段分布在何处。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已创建一个仅包含一个站点的存储池，或者创建了一个包含三个或更多站点的存储池。对于只有两个站点的存储池，没有可用的纠删编码方案。

关于此任务

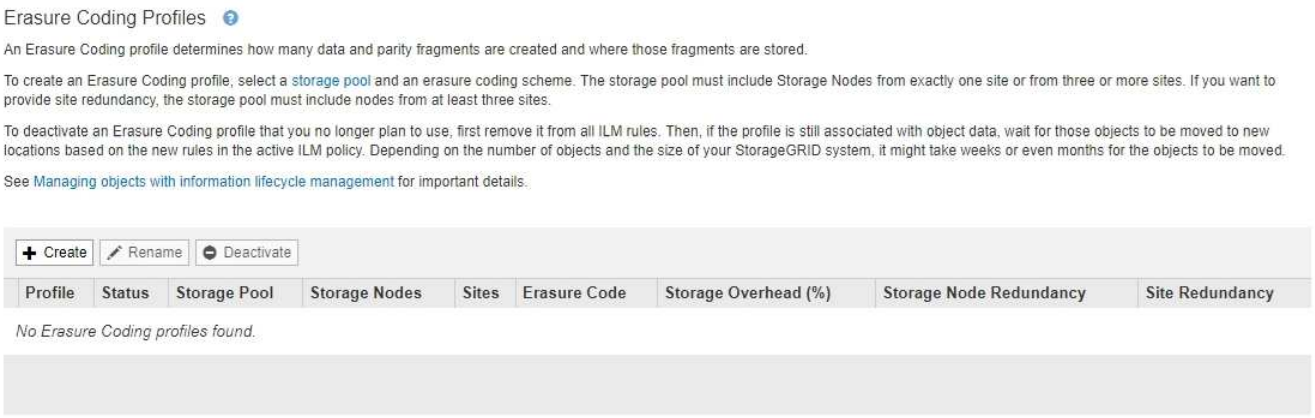
擦除编码配置文件中使用的存储池必须仅包含一个站点或三个或更多站点。如果要提供站点冗余，则存储池必须至少具有三个站点。

> 您必须选择包含存储节点的存储池。您不能对纠删编码的数据使用归档节点。

步骤

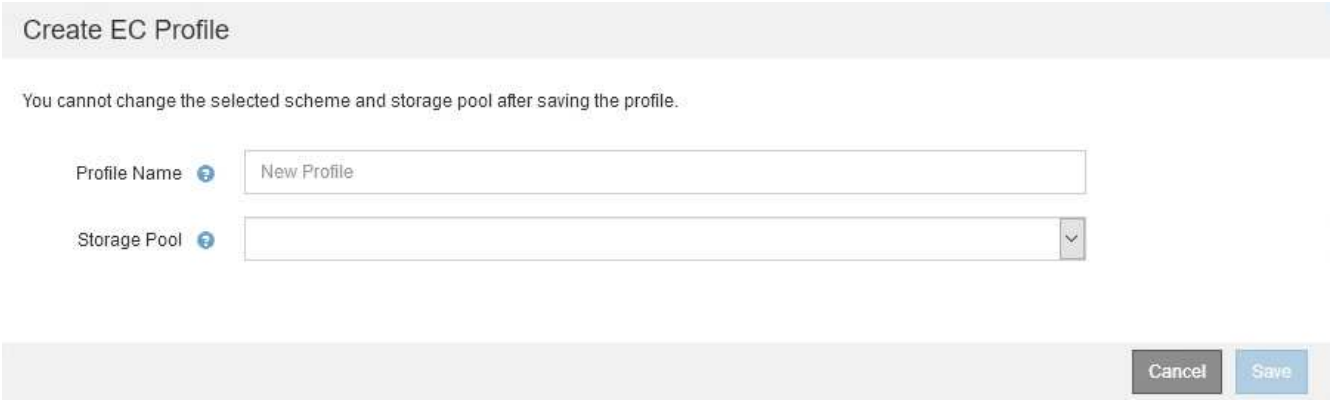
1. 选择 * ILM * > * 擦除编码 * 。

   此时将显示擦除编码配置文件页面。



2. 选择 * 创建 * 。

   此时将显示创建 EC 配置文件对话框。



3. 为擦除编码配置文件输入一个唯一名称。

   纠删编码配置文件名称必须是唯一的。如果您使用现有配置文件的名称，则会发生验证错误，即使该配置文件已停用也是如此。

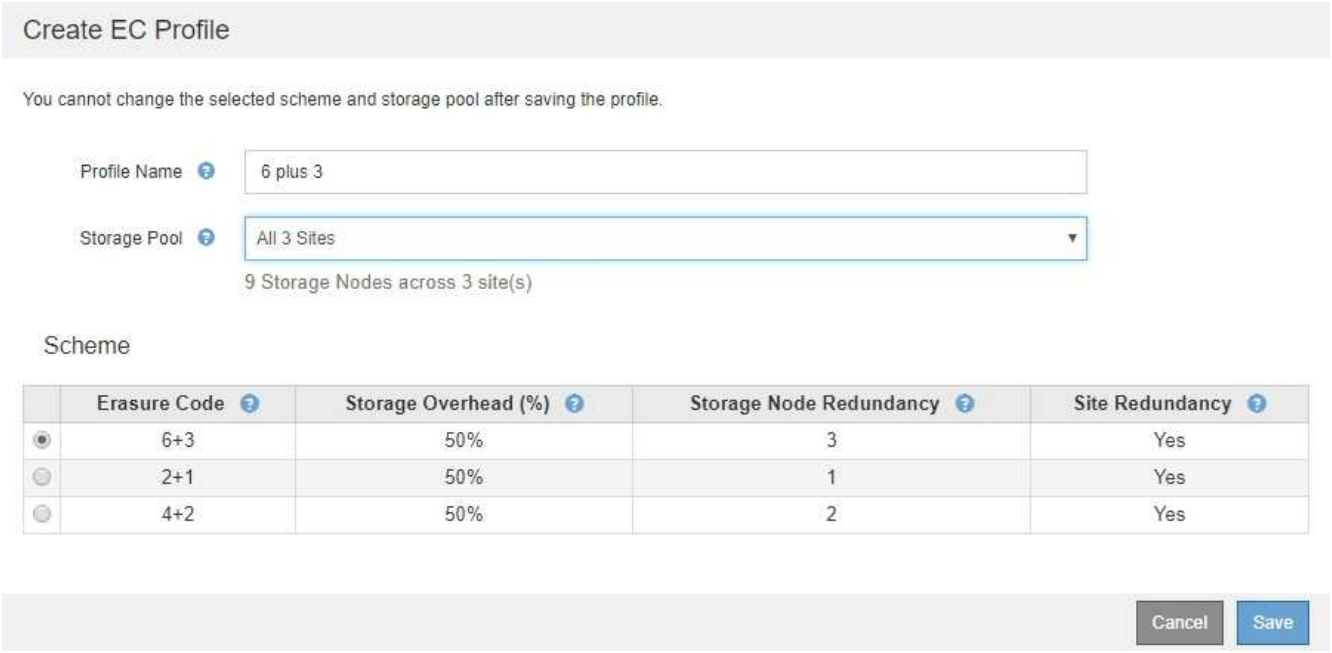
   Erasure Coding 配置文件名称会附加到 ILM 规则放置说明中的存储池名称中。

4. 选择为此擦除编码配置文件创建的存储池。

   如果网格当前仅包含一个站点，则系统将阻止您使用默认存储池，所有存储节点或任何包含默认站点的存储池，所有站点。此行为可防止添加第二个站点时擦除编码配置文件变得无效。

   如果存储池仅包含两个站点，则不能使用该存储池进行纠删编码。对于具有两个站点的存储池，没有可用的纠删编码方案。

选择存储池时，将根据池中的存储节点和站点数量显示可用纠删编码方案的列表。



列出了每个可用纠删编码方案的以下信息：

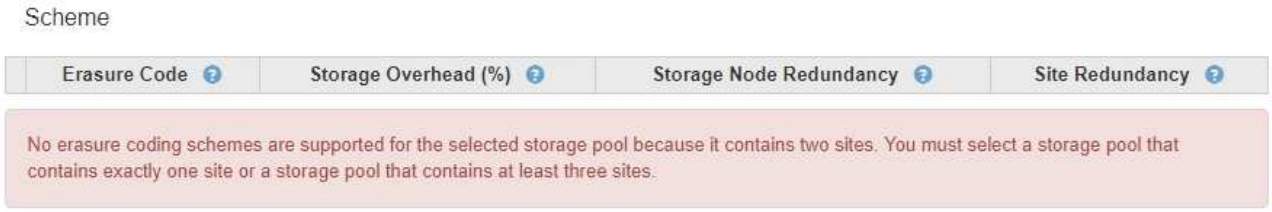
- * 擦除代码 * ： 擦除编码方案的名称，格式如下：数据片段 + 奇偶校验片段。
- * 存储开销（ % ） * ： 相对于对象的数据大小，奇偶校验片段所需的额外存储。存储开销 = 奇偶校验片段的总数 / 数据片段的总数。
- * 存储节点冗余 * ： 在保持检索对象数据的能力的情况下可能丢失的存储节点数。
- * 站点冗余 * ： 选定纠删代码是否允许在站点丢失时检索对象数据。

  要支持站点冗余，选定存储池必须包含多个站点，每个站点都具有足够的存储节点，以允许任何站点丢失。例如，要使用 6+3 纠删编码方案支持站点冗余，选定存储池必须至少包含三个站点，每个站点至少包含三个存储节点。

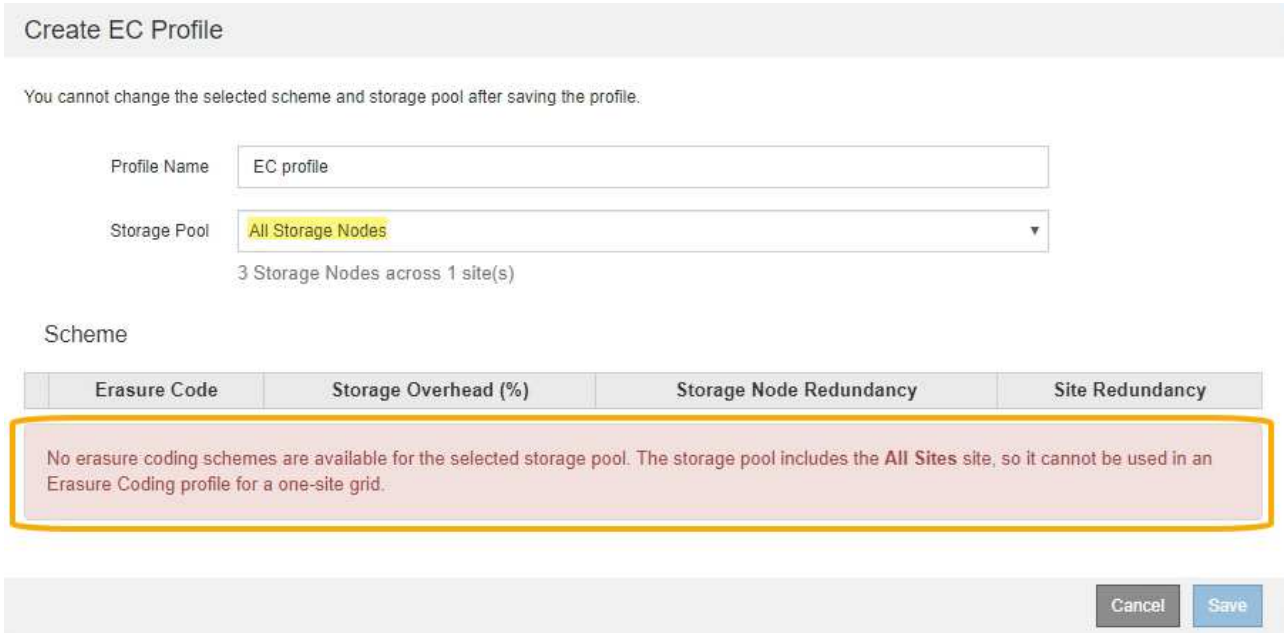
  在以下情况下会显示消息：

- 您选择的存储池不提供站点冗余。如果选定存储池仅包含一个站点，则会显示以下消息。您可以在 ILM 规则中使用此擦除编码配置文件来防止节点故障。

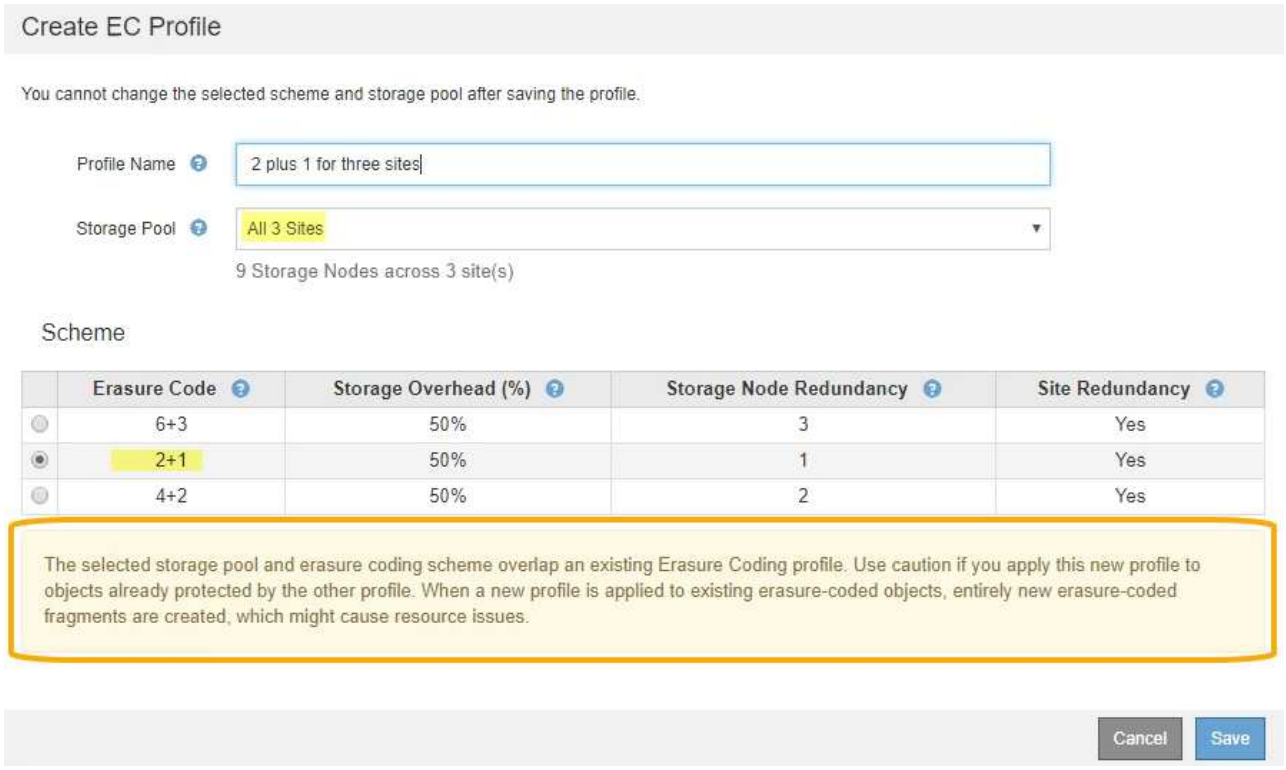
- 您选择的存储池不满足任何纠删编码方案的要求。例如，如果选定存储池仅包含两个站点，则会显示以下消息。如果要使用纠删编码来保护对象数据，则必须选择一个存储池（仅包含一个站点）或一个存储池（包含三个或更多站点）。



- 您的网格仅包含一个站点，并且您选择了默认存储池，所有存储节点或任何包含默认站点的存储池，所有站点。



- 您选择的纠删编码方案和存储池与另一个纠删编码配置文件重叠。



在此示例中，将显示一条警告消息，因为另一个纠删编码配置文件正在使用 2+1 方案，而另一个配置文件的存储池也使用全部 3 个站点存储池中的一个站点。

虽然不会阻止您创建此新配置文件，但在 ILM 策略中开始使用此配置文件时必须非常小心。如果将此新配置文件应用于已受另一个配置文件保护的现有纠删编码对象，则 StorageGRID 将创建一组全新的对象片段。它不会重复使用现有 2+1 片段。从一个纠删编码配置文件迁移到另一个纠删编码配置文件时，可能会出现资源问题，即使纠删编码方案相同也是如此。

5. 如果列出了多个纠删编码方案，请选择要使用的方案。

   在确定要使用的纠删编码方案时，您应根据修复所需的网络流量要求（碎片越多，网络流量越多）平衡容错（通过具有更多奇偶校验分段来实现）。例如，在选择 4+2 方案和 6+3 方案时，如果需要额外的奇偶校验和容错功能，请选择 6+3 方案。如果在节点修复期间网络资源受到限制，从而减少了网络使用量，请选择 4+2 方案。

6. 选择 * 保存 * 。

重命名擦除编码配置文件

您可能需要重命名纠删编码配置文件，以使其更明显地显示该配置文件的功能。

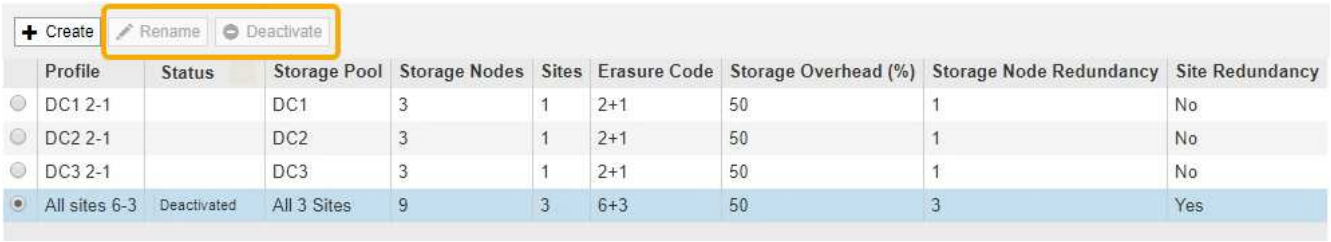
您需要的内容

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

步骤

1. 选择 * ILM * > * 擦除编码 * 。

   此时将显示擦除编码配置文件页面。* 重命名 * 和 * 停用 * 按钮均已禁用。



2. 选择要重命名的配置文件。
   - 重命名 * 和 * 停用 * 按钮将变为启用状态。
3. 选择 * 重命名 * 。

   此时将显示重命名 EC 配置文件对话框。

4. 为擦除编码配置文件输入一个唯一名称。

   Erasure Coding 配置文件名称会附加到 ILM 规则放置说明中的存储池名称中。

> 纠删编码配置文件名称必须是唯一的。如果您使用现有配置文件的名称，则会发生验证错误，即使该配置文件已停用也是如此。

5. 选择 * 保存 * 。

停用擦除编码配置文件

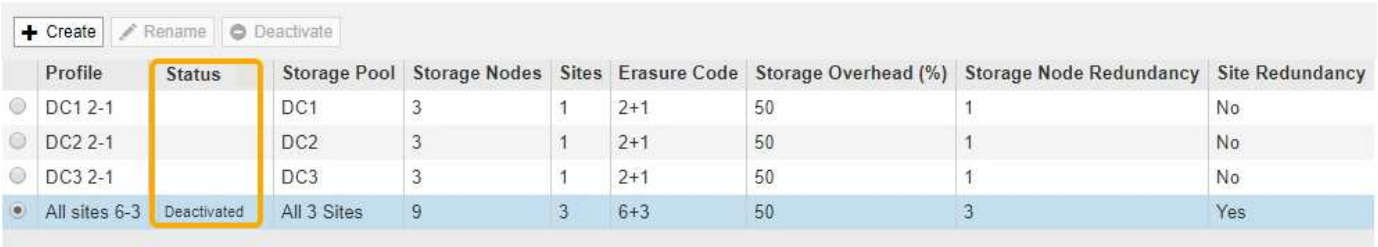
如果您不再计划使用擦除编码配置文件，并且此配置文件当前未在任何 ILM 规则中使用，则可以停用它。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已确认没有正在执行纠删编码的数据修复操作或停用过程。如果您尝试在其中任一操作正在进行时停用擦除编码配置文件，则会返回一条错误消息。

关于此任务

停用擦除编码配置文件时，该配置文件仍会显示在 "Erasure Coding Profiles" 页面上，但其状态为 * 已停用 * 。



您不能再使用已停用的擦除编码配置文件。为 ILM 规则创建放置说明时，不会显示已停用的配置文件。您无法重新激活已停用的配置文件。

如果满足以下任一条件， StorageGRID 将阻止您停用擦除编码配置文件：

- ILM 规则中当前使用擦除编码配置文件。
- Erasure Coding 配置文件不再在任何 ILM 规则中使用，但该配置文件的对象数据和奇偶校验片段仍存在。

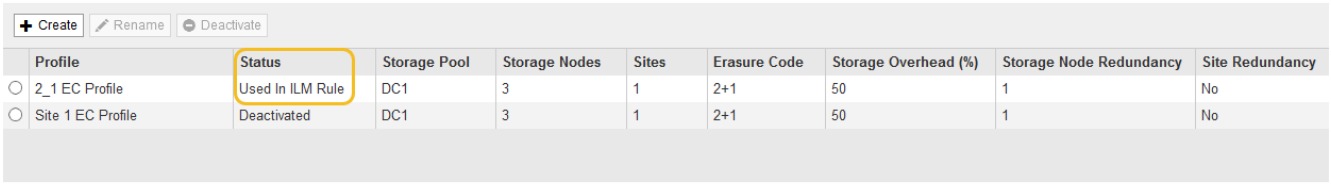
步骤

1. 选择 * ILM * > * 擦除编码 * 。

   此时将显示擦除编码配置文件页面。* 重命名 * 和 * 停用 * 按钮均已禁用。

2. 查看 * 状态 * 列，确认要停用的擦除编码配置文件未在任何 ILM 规则中使用。

   如果擦除编码配置文件在任何 ILM 规则中使用，则无法停用它。在此示例中，至少在一个 ILM 规则中使用了 **2_1 EC Profile** 。

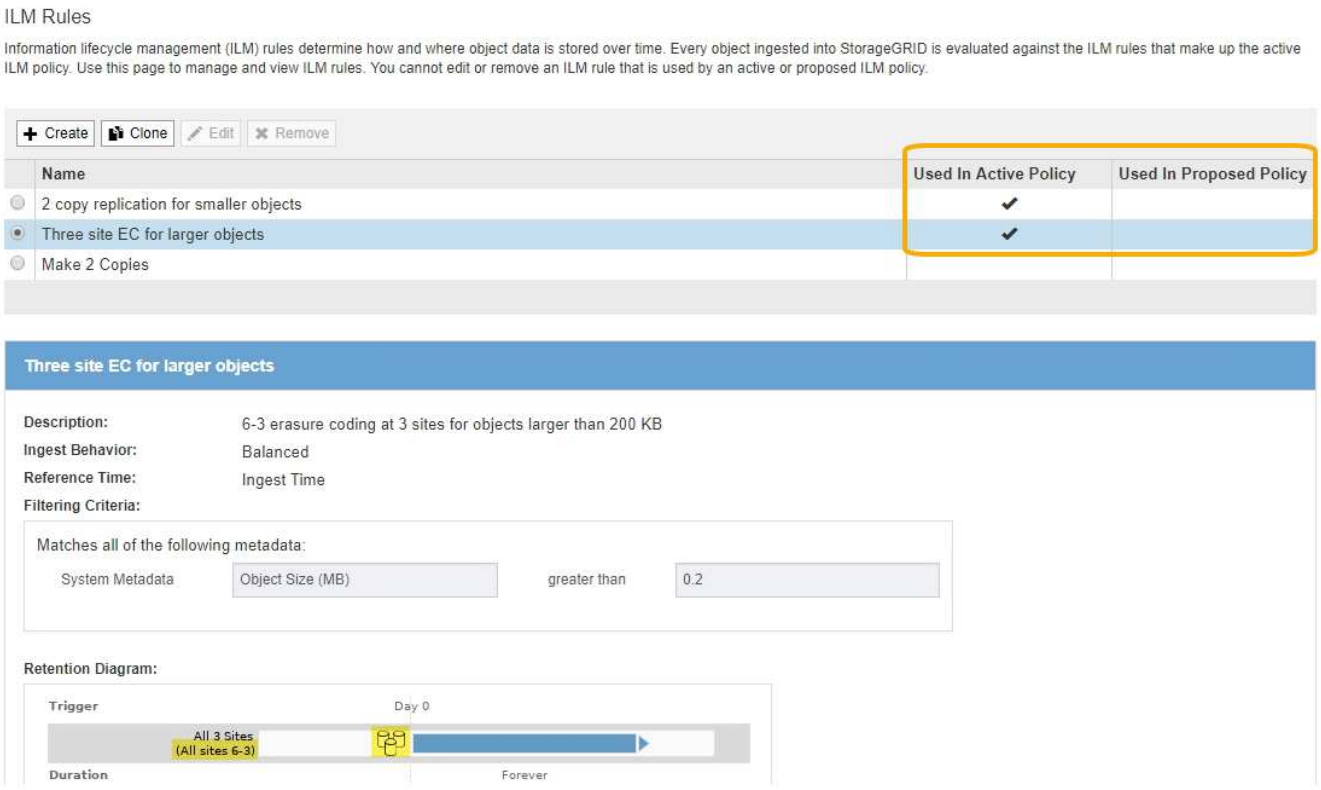


3. 如果在 ILM 规则中使用配置文件，请执行以下步骤：

   a. 选择 * ILM * > * 规则 * 。

   b. 对于列出的每个规则，选择单选按钮并查看保留示意图以确定该规则是否使用要停用的擦除编码配置文件。

      在此示例中， * 三个站点 EC for larger objects* 规则使用名为 * 所有 3 个站点 * 的存储池和 * 所有站点 6-3* 擦除编码配置文件。纠删编码配置文件由以下图标表示：



a. 如果 ILM 规则使用要停用的擦除编码配置文件，请确定该规则是在活动 ILM 策略中使用还是在建议的策略中使用。

   在此示例中，活动 ILM 策略使用了 * 三个站点 EC for larger objects* 规则。

b. 根据纠删编码配置文件的使用位置，完成表中的其他步骤。

此配置文件已在何处使用？	停用配置文件前要执行的其他步骤	请参见这些附加说明
从不在任何 ILM 规则中使用	无需执行其他步骤。继续执行此操作步骤。	无 _
在从未在任何 ILM 策略中使用过的 ILM 规则中	i. 编辑或删除所有受影响的 ILM 规则。如果编辑此规则，请删除使用擦除编码配置文件的所有放置位置。 ii. 继续执行此操作步骤。	使用 ILM 规则和 ILM 策略

此配置文件已在何处使用?	停用配置文件前要执行的其他步骤	请参见这些附加说明
当前处于活动 ILM 策略中的 ILM 规则中	i. 克隆活动策略。 ii. 删除使用擦除编码配置文件的 ILM 规则。 iii. 添加一个或多个新 ILM 规则以确保对象受到保护。 iv. 保存，模拟和激活新策略。 v. 等待应用新策略，并根据添加的新规则将现有对象移动到新位置。 ◦ 注意： * 根据对象数量和 StorageGRID 系统的大小， ILM 操作可能需要数周甚至数月才能根据新的 ILM 规则将对象移动到新位置。 虽然您可以安全地尝试停用擦除编码配置文件，但它仍与数据相关联，但停用操作将失败。如果配置文件尚未准备好停用，则会显示一条错误消息通知您。 vi. 编辑或删除从策略中删除的规则。如果编辑此规则，请删除使用擦除编码配置文件的所有放置位置。 vii. 继续执行此操作步骤。	• 创建 ILM 策略 • 使用 ILM 规则和 ILM 策略
当前在建议的 ILM 策略中的 ILM 规则	i. 编辑建议的策略。 ii. 删除使用擦除编码配置文件的 ILM 规则。 iii. 添加一个或多个新的 ILM 规则以确保所有对象均受保护。 iv. 保存建议的策略。 v. 编辑或删除从策略中删除的规则。如果编辑此规则，请删除使用擦除编码配置文件的所有放置位置。 vi. 继续执行此操作步骤。	• 创建 ILM 策略 • 使用 ILM 规则和 ILM 策略
在历史 ILM 策略中的 ILM 规则中	i. 编辑或删除规则。如果编辑此规则，请删除使用擦除编码配置文件的所有放置位置。（此规则现在将在历史策略中显示为历史规则。） ii. 继续执行此操作步骤。	使用 ILM 规则和 ILM 策略

c. 刷新擦除编码配置文件页面，以确保此配置文件未在 ILM 规则中使用。

4. 如果在 ILM 规则中未使用该配置文件，请选择单选按钮并选择 * 停用 * 。

此时将显示停用 EC 配置文件对话框。

5. 如果确实要停用此配置文件，请选择 * 停用 * 。
   - 如果 StorageGRID 能够停用擦除编码配置文件，则其状态为 * 已停用 * 。您不能再为任何 ILM 规则选择此配置文件。
   - 如果 StorageGRID 无法停用此配置文件，则会显示一条错误消息。例如，如果对象数据仍与此配置文件关联，则会显示一条错误消息。您可能需要等待几周才能再次尝试停用过程。

配置区域（可选，仅 **S3** ）

ILM 规则可以根据创建 S3 存储分段的区域筛选对象，从而可以将不同区域的对象存储在不同存储位置。如果要在规则中使用 S3 分段区域作为筛选器，则必须先创建可由系统中的分段使用的区域。

您需要的内容

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

关于此任务

创建 S3 存储分段时，您可以指定在特定区域创建存储分段。通过指定区域，存储分段可以在地理位置上靠近用户，从而有助于优化延迟，最大限度地降低成本并满足法规要求。

创建 ILM 规则时，您可能需要使用与 S3 存储分段关联的区域作为高级筛选器。例如，您可以设计一个仅适用于在 us-west-2 区域中创建的 S3 存储分段中的对象的规则。然后，您可以指定将这些对象的副本放置在该区域内数据中心站点的存储节点上，以优化延迟。

配置区域时，请遵循以下准则：

- 默认情况下，所有分段均视为属于 us-east-1 区域。
- 在使用租户管理器或租户管理 API 创建存储分段时，或者在使用 LocationConstrcont Request 元素为 S3 PUT 存储分段 API 请求创建存储分段时，您必须先使用网格管理器创建区域，然后才能指定非默认区域。如果 PUT 存储分段请求使用的区域尚未在 StorageGRID 中定义，则会发生错误。
- 创建 S3 存储分段时，必须使用确切的区域名称。区域名称区分大小写，并且必须至少包含 2 个字符，并且不超过 32 个字符。有效字符包括数字，字母和连字符。

  EU-west-1 不视为别名。如果要使用欧盟或 EU-west-1 地区，则必须使用确切的名称。

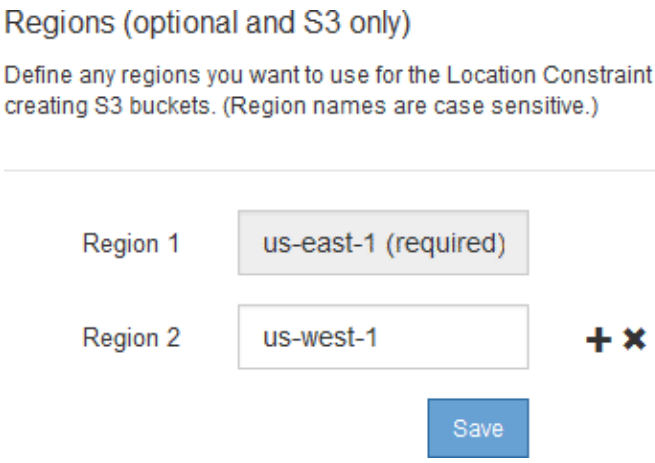
- 如果某个区域当前在活动 ILM 策略或建议的 ILM 策略中使用，则不能删除或修改该区域。

- 如果在 ILM 规则中用作高级筛选器的区域无效，仍可将该规则添加到建议的策略中。但是，如果您尝试保存或激活建议的策略，则会发生错误。（如果您在 ILM 规则中使用某个区域作为高级筛选器，但稍后删除该区域，或者使用网格管理 API 创建规则并指定尚未定义的区域，则可能会导致区域无效。）
- 如果在使用某个区域创建 S3 存储分段后将其删除，则如果您要使用位置限制高级筛选器查找该存储分段中的对象，则需要重新添加该区域。

步骤

1. 选择 * ILM * > * 区域 * 。

   此时将显示区域页面，其中列出了当前定义的区域。* 区域 1* 显示默认区域 `us-east-1` ，无法修改或删除。

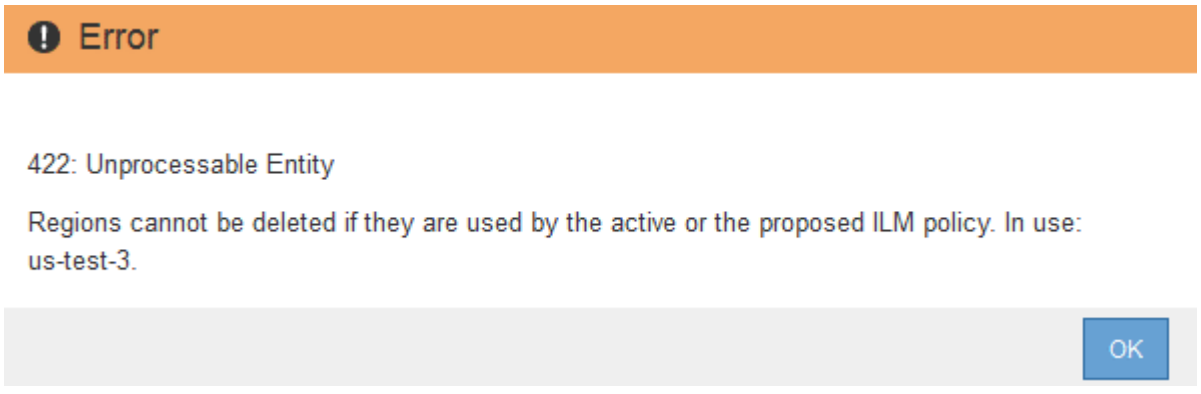
   

2. 要添加区域，请执行以下操作：
   a. 选择插入图标 ✚ 最后一个条目右侧。
   b. 输入要在创建 S3 存储分段时使用的区域名称。

      在创建相应的 S3 存储分段时，您必须使用此确切的区域名称作为 LocationConstraint 请求元素。

3. 要删除未使用的区域，请选择删除图标 ✖。

   如果尝试删除活动策略或建议策略中当前使用的区域，则会显示一条错误消息。

4. 完成更改后，选择 * 保存 * 。

   现在，您可以从创建 ILM 规则向导的 " 高级筛选 " 页面上的 * 位置约束 * 列表中选择这些区域。请参见在 ILM 规则中使用高级筛选器。

创建 **ILM** 规则

访问创建 **ILM** 规则向导

您可以通过 ILM 规则管理对象数据随时间的放置。要创建 ILM 规则，请使用创建 ILM 规则向导。

如果要为策略创建默认 ILM 规则，请改用此操作步骤： 创建默认 ILM 规则。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 如果要指定此规则适用场景 中的租户帐户，您拥有 " 租户帐户 " 权限或知道每个帐户的帐户 ID 。
- 如果您希望规则按上次访问时间元数据筛选对象，则必须通过 S3 的存储分段或 Swift 的容器启用上次访问时间更新。
- 如果要创建复制的副本，则已配置计划使用的任何存储池或云存储池。请参见 创建存储池 和 创建云存储池。
- 如果要创建纠删编码副本，则已配置纠删编码配置文件。请参见 创建擦除编码配置文件。
- 您熟悉 用于载入的数据保护选项。
- 如果您需要创建一个用于 S3 对象锁定的合规规则，您将熟悉 S3 对象锁定的要求。
- 您也可以观看以下视频： "视频： StorageGRID ILM 规则：入门"。

关于此任务

创建 ILM 规则时：

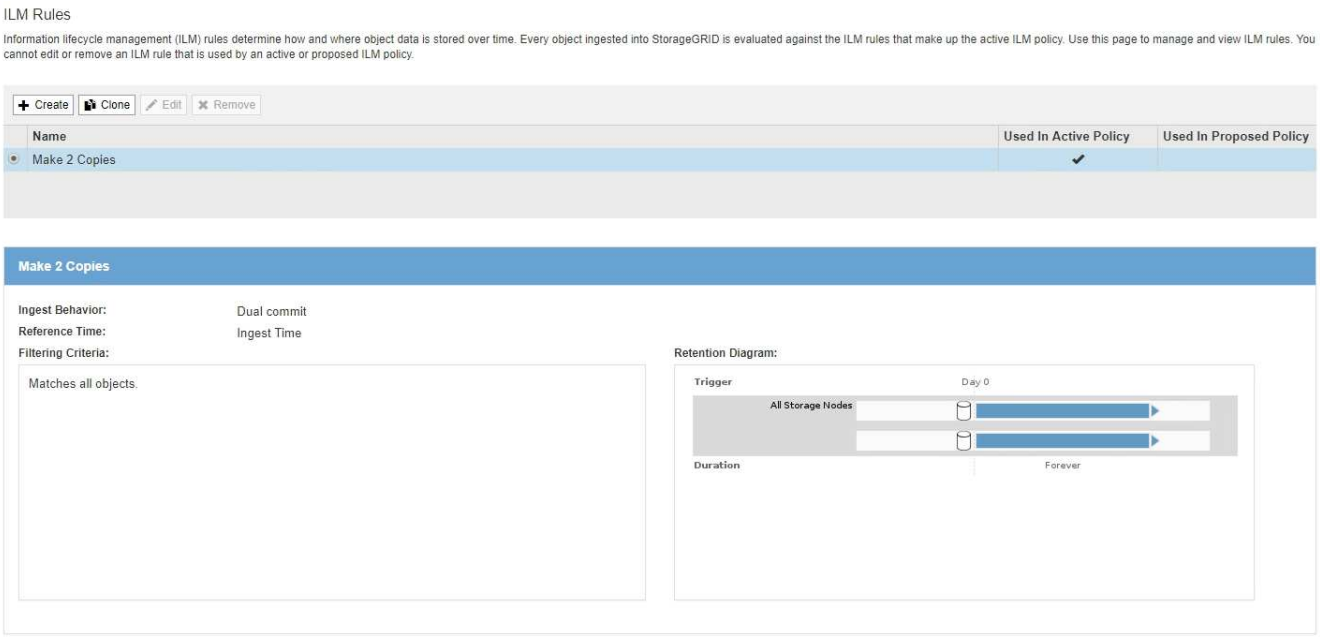
- 请考虑 StorageGRID 系统的拓扑和存储配置。
- 请考虑要创建的对象副本类型（复制或擦除编码）以及所需的每个对象的副本数量。
- 确定连接到 StorageGRID 系统的应用程序中使用的对象元数据类型。ILM 规则根据对象的元数据筛选对象。

- 请考虑随时间推移对象副本的放置位置。
- 确定在载入时使用哪种数据保护选项（均衡，严格或双提交）。

步骤

1. 选择 * ILM * > * 规则 * 。

   此时将显示 "ILM Rules" 页面，其中选中了 "Make 2 copies" 规则。



   如果已为 StorageGRID 系统启用全局 S3 对象锁定设置，则 "ILM 规则 " 页面看起来略有不同。摘要表包含一个 * 符合 * 列，选定规则的详细信息包含一个 * 符合 * 字段。

2. 选择 * 创建 * 。

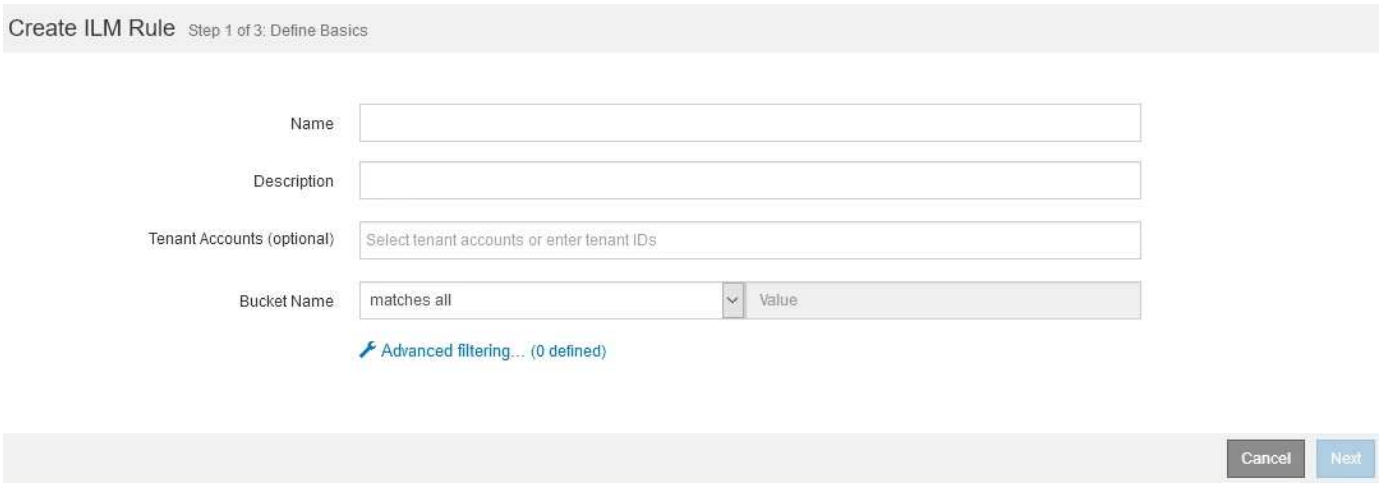
   此时将显示创建 ILM 规则向导的第 1 步（定义基础知识）。您可以使用 " 定义基础知识 " 页面定义规则适用场景 的对象。

第 **1** 步，共 **3** 步：定义基础知识

使用创建 ILM 规则向导的第 1 步（定义基本信息），您可以定义规则的基本和高级筛选器。

关于此任务

根据 ILM 规则评估对象时， StorageGRID 会将对象元数据与规则的筛选器进行比较。如果对象元数据与所有筛选器匹配， StorageGRID 将使用规则放置对象。您可以设计一个规则以应用于所有对象，也可以指定基本筛选器，例如一个或多个租户帐户或分段名称，或者指定高级筛选器，例如对象的大小或用户元数据。



步骤

1. 在 * 名称 * 字段中输入规则的唯一名称。

   必须输入 1 到 64 个字符。

2. 或者，也可以在 * 问题描述 * 字段中为此规则输入一个短问题描述 。

   您应说明此规则的目的或功能，以便稍后识别此规则。

3. 或者，也可以选择一个或多个适用此规则的 S3 或 Swift 租户帐户。如果此规则为所有租户添加适用场景 ，请将此字段留空。

   如果您没有 root 访问权限或租户帐户权限，则无法从列表中选择租户。而是输入租户 ID 或输入多个 ID 作为逗号分隔的字符串。

4. 或者，指定此规则适用的 S3 分段或 Swift 容器。

   如果选择了 * 匹配全部 * （默认），则规则适用场景 all S3 b桶 或 Swift 容器。

5. 或者，选择 * 高级筛选 * 以指定其他筛选器。

   如果不配置高级筛选，则规则适用场景 与基本筛选器匹配的所有对象。

   如果此规则将创建经过擦除编码的副本，请添加 * 对象大小（ MB ） * 高级筛选器并将其设置为 * 大于 1* 。大小筛选器可确保 1 MB 或更小的对象不会进行纠删编码。

   > 纠删编码最适合大于 1 MB 的对象。请勿对小于 200 KB 的对象使用纠删编码，以避免管理极小的纠删编码片段所产生的开销。

6. 选择 * 下一步 * 。

   此时将显示第 2 步（定义放置位置）。

相关信息

- 什么是 ILM 规则
- 在 ILM 规则中使用高级筛选器
- 第 2 步，共 3 步：定义放置位置

在 **ILM** 规则中使用高级筛选器

通过高级筛选功能，您可以创建仅根据特定对象的元数据应用于特定对象的 ILM 规则。为规则设置高级筛选时，您可以选择要匹配的元数据类型，选择运算符并指定元数据值。评估对象时， ILM 规则仅应用于元数据与高级筛选器匹配的对象。

下表显示了您可以在高级筛选器中指定的元数据类型，可用于每种元数据类型的运算符以及预期的元数据值。

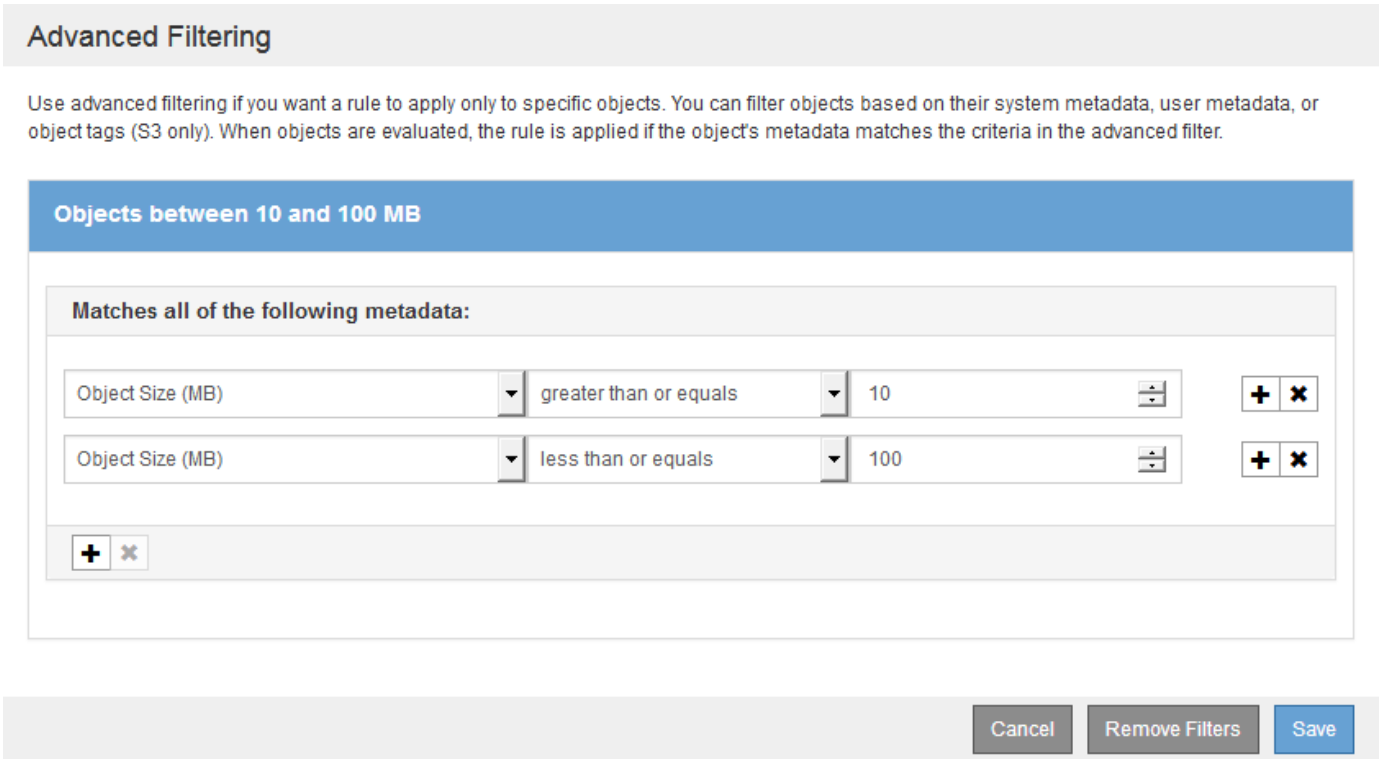
元数据类型	支持的运算符	元数据值
载入时间（微秒）	• 等于 • 不等于 • 小于 • 小于或等于 • 大于 • 大于或等于	载入对象的时间和日期。 • 注意： * 要在激活新 ILM 策略时避免资源问题，您可以在可能更改大量现有对象位置的任何规则中使用 " 载入时间 " 高级筛选器。将载入时间设置为大于或等于新策略生效的大致时间，以确保现有对象不会发生不必要的移动。
密钥	• 等于 • 不等于 • 包含 • 不包含 • 开头为 • 不以开头 • 结尾为 • 结尾不为	唯一 S3 或 Swift 对象密钥的全部或部分内容。 例如，您可能希望匹配以 ` .txt` 或以 `test-object/` 开头的对象。
上次访问时间（微秒）	• 等于 • 不等于 • 小于 • 小于或等于 • 大于 • 大于或等于 • exists • 不存在	上次检索（读取或查看）对象的时间和日期。 • 注意： * 如果您计划使用上次访问时间作为高级筛选器，则必须为 S3 存储分段或 Swift 容器启用上次访问时间更新。 在 ILM 规则中使用上次访问时间

元数据类型	支持的运算符	元数据值
位置限制（仅限 S3 ）	• 等于 • 不等于	创建 S3 存储分段的区域。使用 * ILM * > * 区域 * 定义显示的区域。 • 注： * 值 us-east-1 将匹配在 us-east-1 区域创建的分段中的对象以及未指定区域的分段中的对象。 配置区域（可选，仅 S3 ）
对象大小（ MB ）	• 等于 • 不等于 • 小于 • 小于或等于 • 大于 • 大于或等于	对象的大小（以 MB 为单位）。 纠删编码最适合大于 1 MB 的对象。请勿对小于 200 KB 的对象使用纠删编码，以避免管理极小的纠删编码片段所产生的开销。 • 注： * 要按小于 1 MB 的对象大小进行筛选，请键入一个小数值。您的浏览器类型和区域设置用于控制您是需要使用句点还是逗号作为小数分隔符。
用户元数据	• 包含 • 结尾为 • 等于 • exists • 不包含 • 结尾不为 • 不等于 • 不存在 • 不以开头 • 开头为	键值对，其中 * 用户元数据名称 * 是密钥， * 用户元数据值 * 是值。 例如，要筛选用户元数据为 `color=blue` 的对象，请为 * 用户元数据名称 * 指定 `color` ，为运算符指定 `Equals` ，为 * 用户元数据值 * 指定 `blue` 。 • 注： * 用户元数据名称不区分大小写；用户元数据值区分大小写。
对象标记（仅限 S3 ）	• 包含 • 结尾为 • 等于 • exists • 不包含 • 结尾不为 • 不等于 • 不存在 • 不以开头 • 开头为	键值对，其中 * 对象标记名称 * 是密钥， * 对象标记值 * 是值。 例如，要筛选对象标记为 `Image=True` 的对象，请为 * 对象标记名称 * 指定 `Image` ，为运算符指定 **等于** ，为 * 对象标记值 * 指定 `True` 。 • 注： * 对象标记名称和对象标记值区分大小写。您必须严格按照为对象定义的方式输入这些项。

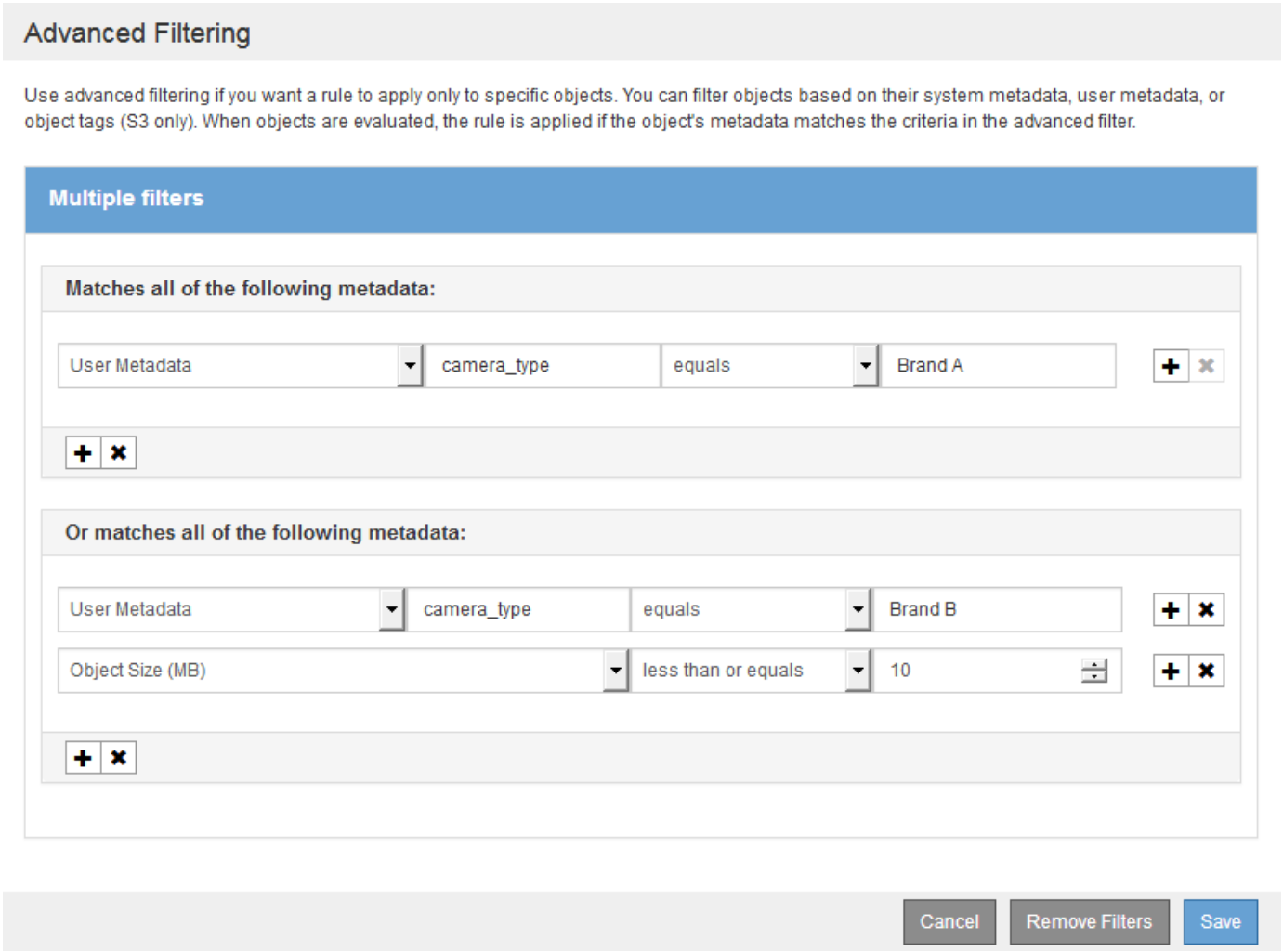
指定多个元数据类型和值

定义高级筛选时，您可以指定多种类型的元数据和多个元数据值。例如，如果您希望某个规则与大小介于 10 MB 到 100 MB 之间的对象匹配，则应选择 * 对象大小 * 元数据类型并指定两个元数据值。

- 第一个元数据值用于指定大于或等于 10 MB 的对象。
- 第二个元数据值用于指定小于或等于 100 MB 的对象。



使用多个条目可以精确控制匹配的对象。在以下示例中，规则适用场景 对象将品牌 A 或品牌 B 作为摄像机类型用户元数据的值。但是，规则仅对小于 10 MB 的品牌 B 对象执行适用场景 。



第 **2** 步，共 **3** 步：定义放置位置

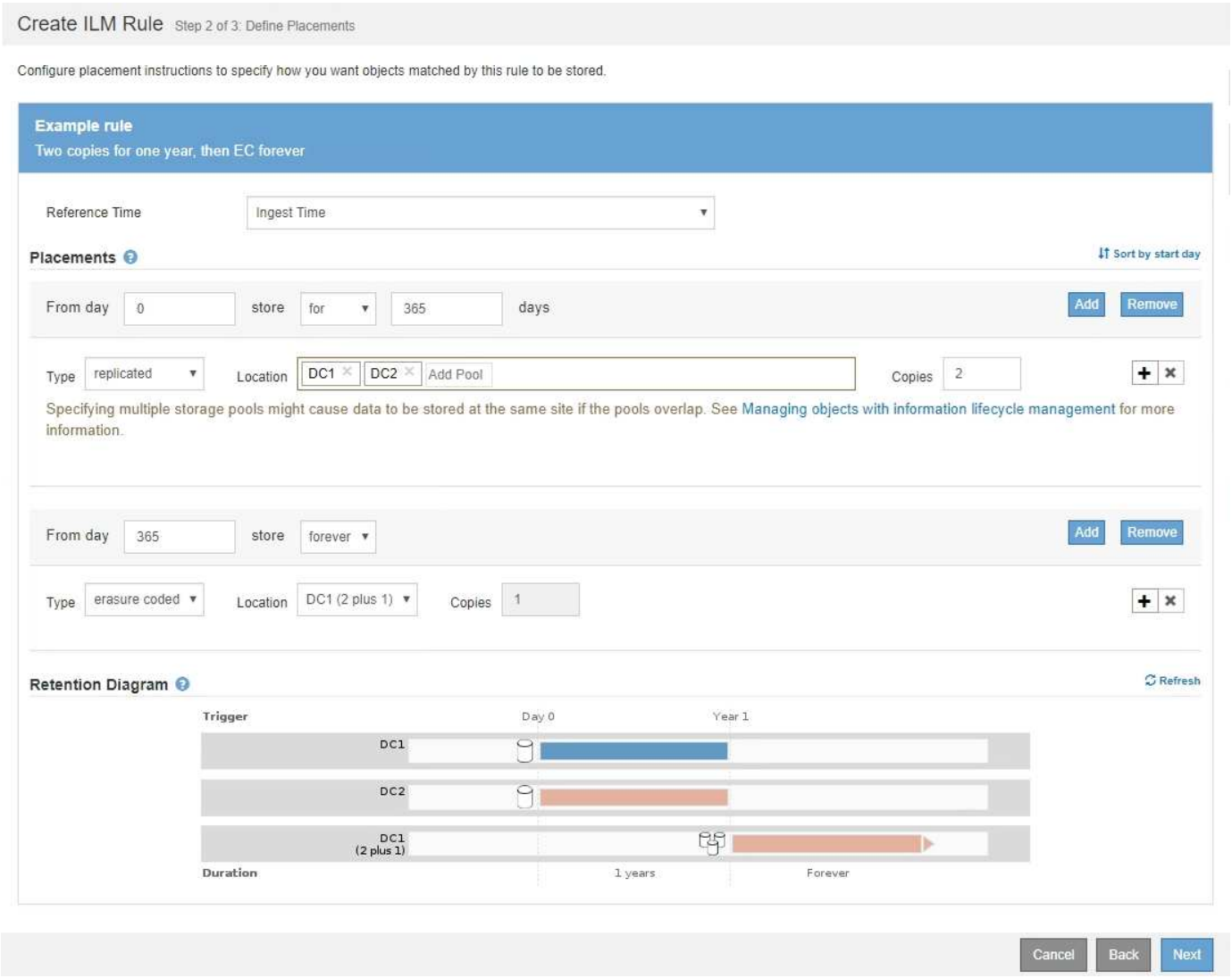
通过创建 ILM 规则向导的第 2 步（定义放置位置），您可以定义放置说明，以确定对象的存储时间，副本的类型（复制或擦除编码），存储位置以及副本数量。

关于此任务

一个 ILM 规则可以包含一个或多个放置指令。每个放置指令适用场景 都有一段时间。如果使用多个指令，则时间段必须是连续的，并且至少有一个指令必须从第 0 天开始。这些说明可以永久继续，也可以一直持续到不再需要任何对象副本为止。

如果要在该时间段内创建不同类型的副本或使用不同的位置，则每个放置指令可以包含多行。

此示例 ILM 规则会为第一年创建两个复制副本。每个副本都保存在不同站点的存储池中。一年后，将创建 2+1 纠删编码副本，并仅保存在一个站点上。



步骤

1. 对于 * 参考时间 * ，选择计算放置指令的开始时间时要使用的时间类型。

选项	Description
载入时间	对象的载入时间。
上次访问时间	上次检索（读取或查看）对象的时间。 • 注意： * 要使用此选项，必须为 S3 存储分段或 Swift 容器启用上次访问时间更新。请参见 在 ILM 规则中使用上次访问时间。
非当前时间	对象版本因载入新版本并替换为当前版本而变为非最新的时间。 • 注： * 非当前时间仅适用于已启用版本控制的存储分段中的 S3 对象。 您可以使用此选项通过筛选非当前对象版本来减少受版本控制的对象的存储影响。请参见 示例 4 ： S3 版本对象的 ILM 规则和策略。

选项	Description
用户定义的创建时间	在用户定义的元数据中指定的时间。

如果要创建合规规则，必须选择 * 载入时间 * 。

2. 在 * 放置位置 * 部分中，选择第一个时间段的开始时间和持续时间。

   例如，您可能需要指定第一年对象的存储位置（ `" day 0 for 365 days "` ）。至少有一个指令必须从第 0 天开始。

3. 如果要创建复制的副本：

   a. 从 * 类型 * 下拉列表中，选择 * 已复制 * 。

   b. 在 * 位置 * 字段中，为要添加的每个存储池选择 * 添加池 * 。

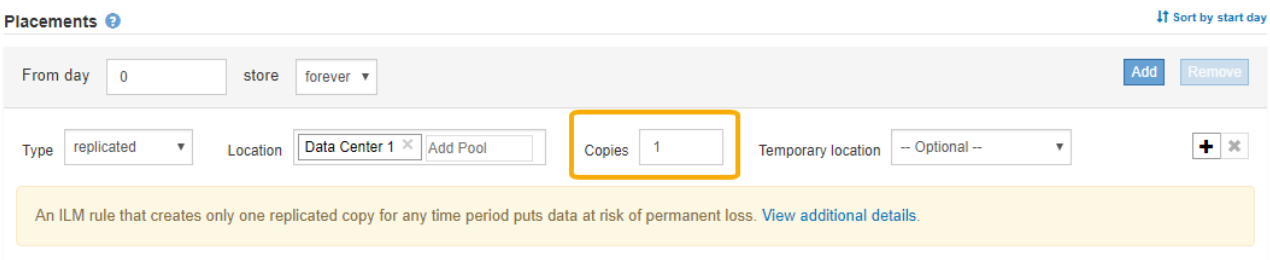
   - 如果仅指定一个存储池 * ，请注意， StorageGRID 只能在任何给定存储节点上存储一个对象的一个复制副本。如果网格包含三个存储节点，并且您选择 4 作为副本数，则只会创建三个副本—每个存储节点一个副本。

     系统将触发 * 无法实现 ILM 放置 * 警报，以指示无法完全应用 ILM 规则。

   - 如果指定多个存储池 * ，请记住以下规则：
     - 副本数量不能大于存储池数量。
     - 如果副本数等于存储池数，则每个存储池中将存储一个对象副本。
     - 如果副本数小于存储池数、则会在载入站点存储一个副本、然后系统会分发其余副本、以保持池中的磁盘使用量保持平衡、同时确保任何站点都不会获得一个对象的多个副本。
     - 如果存储池重叠（包含相同的存储节点），则对象的所有副本可能只保存在一个站点上。因此，请勿指定默认的所有存储节点存储池和另一个存储池。

   c. 选择要创建的副本数。

   如果将副本数更改为 1 ，则会显示一条警告。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。请参见 为什么不应使用单副本复制。



要避免这些风险，请执行以下一项或多项操作：

- 增加时间段内的副本数。
- 选择加号图标 ✚ 在此时间段内创建其他副本。然后，选择其他存储池或云存储池。
- 选择 "Erasure Coded* " 作为 "Type" ，而不是 "* 已复制 * 。如果此规则已在所有时间段创建多个副本，则可以安全地忽略此警告。

d. 如果仅指定一个存储池，请忽略 * 临时位置 * 字段。

> 临时位置已弃用，将在未来版本中删除。请参见 使用存储池作为临时位置（已弃用）。

4. 如果要创建经过纠删编码的副本：

a. 从 * 类型 * 下拉列表中，选择 * 纠删编码 * 。

副本数将更改为 1 。如果规则没有高级筛选器来忽略 200 KB 或更小的对象，则会显示警告。

> Erasure coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to any value greater than 0.2.

> 纠删编码最适合大于 1 MB 的对象。请勿对小于 200 KB 的对象使用纠删编码，以避免管理极小的纠删编码片段所产生的开销。

b. 如果出现对象大小警告，请选择 * 返回 * 以返回到步骤 1 。然后，选择 * 高级筛选 * 并将对象大小（ MB ）筛选器设置为大于 0.2 的任何值。

c. 选择存储位置。

擦除编码副本的存储位置包括存储池的名称，后跟擦除编码配置文件的名称。

5. 或者，也可以在不同位置添加不同的时间段或创建其他副本：

◦ 选择加号图标可在同一时间段内在其他位置创建其他副本。

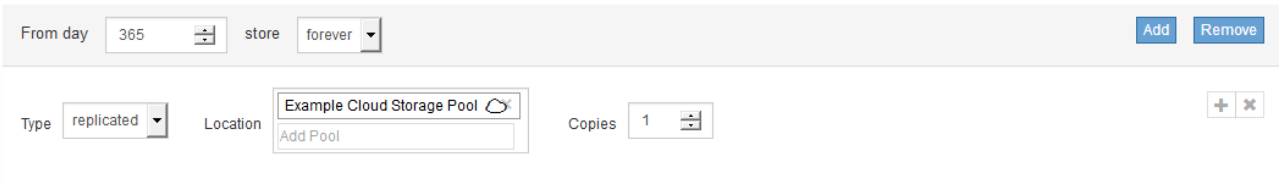
◦ 选择 * 添加 * 可为放置说明添加不同的时间段。

> 除非最后一个时间段以 * 永久 * 结束，否则对象将在最后一个时间段结束时自动删除。

6. 如果要将对象存储在云存储池中：

a. 从 * 类型 * 下拉列表中，选择 * 已复制 * 。

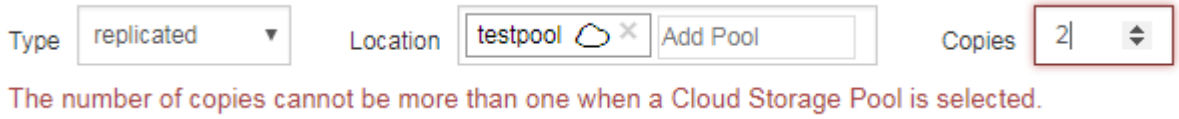
b. 在 * 位置 * 字段中，选择 * 添加池 * 。然后，选择一个云存储池。



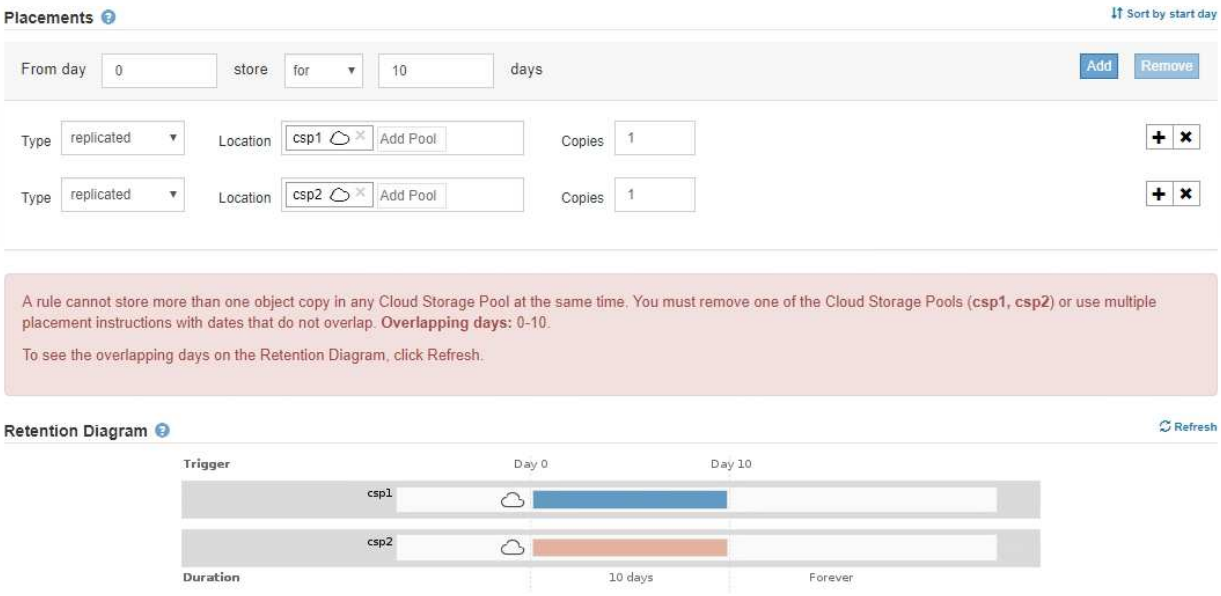
使用云存储池时，请记住以下规则：

- 您不能在一个放置指令中选择多个云存储池。同样，您也不能在同一放置指令中选择云存储池和存储池。

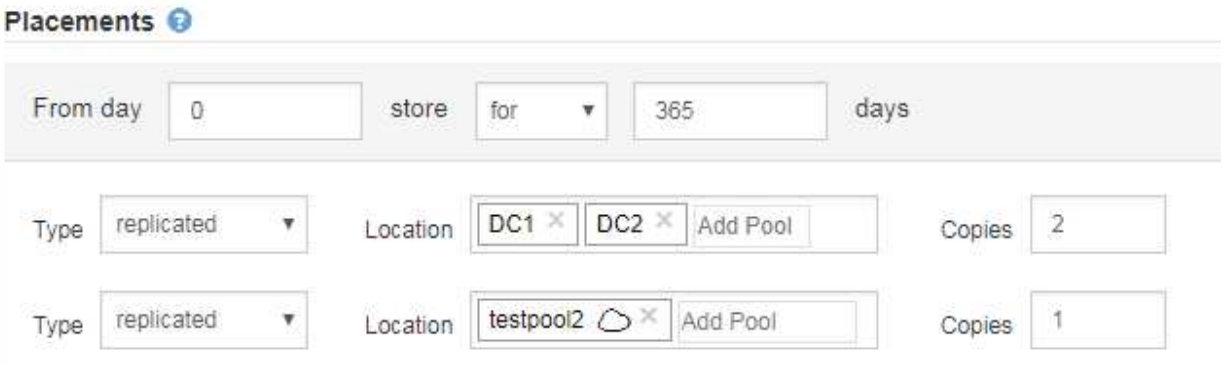
- 您只能在任何给定的云存储池中存储一个对象的一个副本。如果将 * 副本 * 设置为 2 或更多，则会显示一条错误消息。



- 不能同时在任何云存储池中存储多个对象副本。如果使用云存储池的多个放置位置的日期重叠，或者同一放置中的多个行使用云存储池，则会显示错误消息。



- 您可以将对象存储在云存储池中，同时将该对象存储为 StorageGRID 中的复制副本或纠删编码副本。但是，如本示例所示，您必须在时间段的放置说明中包含多行内容，以便为每个位置指定副本的数量和类型。

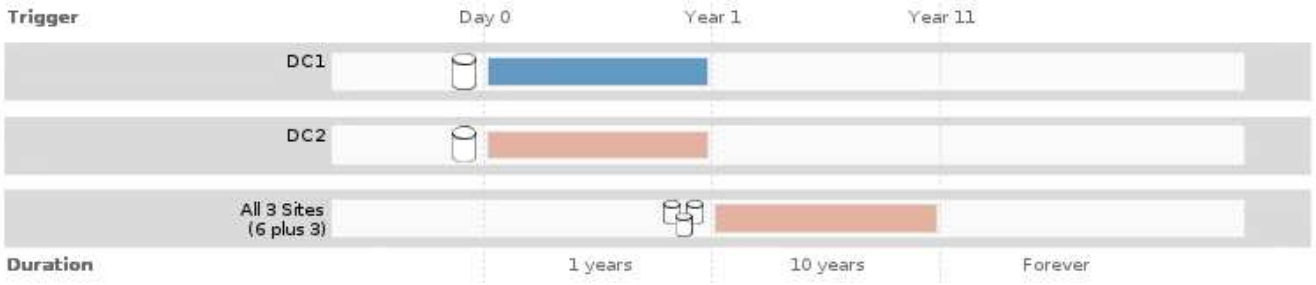


7. 选择 * 刷新 * 以更新保留示意图并确认放置说明。

   图中的每一行都显示了对象副本放置的位置和时间。副本类型由以下图标之一表示：

	复制的副本
	经过纠删编码的副本
	云存储池副本

   在此示例中，两个复制副本将保存到两个存储池（ DC1 和 DC2 ）中一年。然后，在三个站点上使用 6+3 纠删编码方案，再将经过纠删编码的副本保存 10 年。11 年后，这些对象将从 StorageGRID 中删除。



8. 选择 * 下一步 * 。

   此时将显示第 3 步（定义载入行为）。

相关信息

- 什么是 ILM 规则
- 使用 S3 对象锁定管理对象
- 第 3 步，共 3 步：定义载入行为

在 **ILM** 规则中使用上次访问时间

您可以在 ILM 规则中使用上次访问时间作为参考时间。例如，您可能希望将过去三个月查看过的对象保留在本地存储节点上，同时将最近未查看过的对象移动到异地位置。如果您希望 ILM 规则仅应用于上次在特定日期访问的对象，则也可以使用上次访问时间作为高级筛选器。

关于此任务

在 ILM 规则中使用上次访问时间之前，请查看以下注意事项：

- 使用上次访问时间作为参考时间时，请注意，更改对象的上次访问时间不会触发即时 ILM 评估。而是在后台 ILM 评估对象时评估对象的放置位置，并根据需要移动对象。访问对象后，此操作可能需要两周或更长时间。

  在根据上次访问时间创建 ILM 规则时，请考虑此延迟，并避免放置时间较短（不到一个月）。

- 如果将上次访问时间用作高级筛选器或参考时间，则必须为 S3 存储分段启用上次访问时间更新。您可以使用租户管理器或租户管理 API 。

> 对于 Swift 容器，始终会启用上次访问时间更新，但对于 S3 存储分段，默认情况下会禁用上次访问时间更新。

> 请注意，启用上次访问时间更新可能会降低性能，尤其是在对象较小的系统中。之所以会影响性能，是因为每次检索对象时， StorageGRID 都必须使用新的时间戳更新对象。

下表总结了对于不同类型的请求，是否为存储分段中的所有对象更新了上次访问时间。

请求类型	禁用上次访问时间更新时是否更新上次访问时间	启用上次访问时间更新后是否更新上次访问时间
请求检索对象，其访问控制列表或其元数据	否	是的。
请求更新对象的元数据	是的。	是的。
请求将对象从一个存储分段复制到另一个存储分段	• 否，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本
请求完成多部分上传	是，对于已组装的对象	是，对于已组装的对象

相关信息

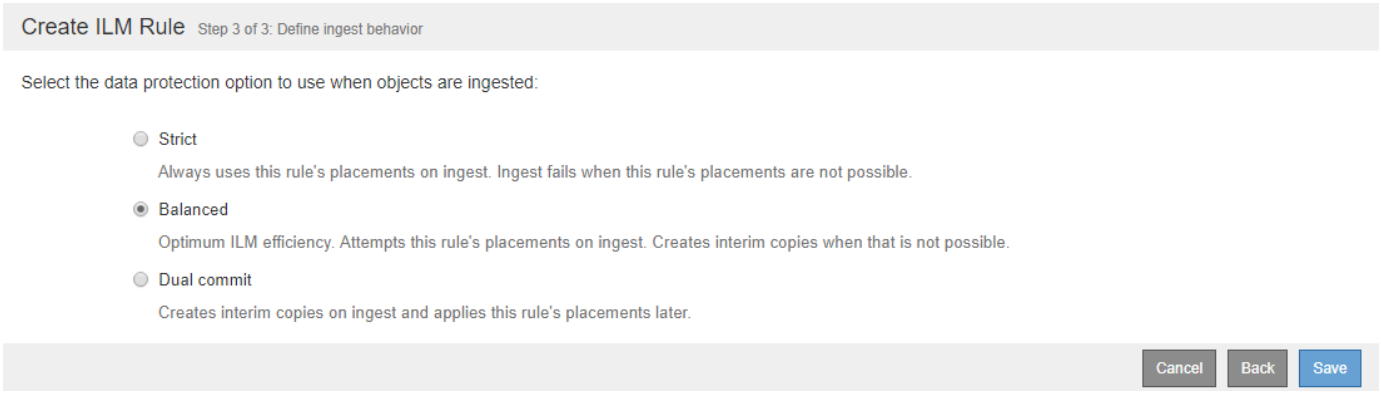
- 使用 S3
- 使用租户帐户

第 **3** 步，共 **3** 步：定义载入行为

通过创建 ILM 规则向导的第 3 步（定义载入行为），您可以选择在载入时如何保护按此规则筛选的对象。

关于此任务

StorageGRID 可以创建临时副本并将对象排入队列，以便稍后进行 ILM 评估，也可以立即创建副本以满足规则的放置说明。



步骤

1. 选择要在载入对象时使用的数据保护选项：

选项	Description
严格	在载入时始终使用此规则的放置位置。如果无法放置此规则，则载入将失败。
平衡	最佳 ILM 效率。尝试在载入时放置此规则。如果无法创建中间副本，请创建此副本。
双提交	在载入时创建中间副本，并稍后应用此规则的放置位置。

Balanced 结合了数据安全性和效率，在大多数情况下都适用。" 严格 " 或 " 双重提交 " 通常用于满足特定要求。

请参见 用于载入的数据保护选项 和 数据保护选项的优势，劣势和限制 有关详细信息 …

如果选择 " 严格 " 或 " 平衡 " 选项，并且规则使用以下放置之一，则会显示一条错误消息：

- 第 0 天的云存储池
- 日期为 0 的归档节点
- 当规则使用用户定义的创建时间作为参考时间时，则为云存储池或归档节点

2. 选择 * 保存 * 。

此时将保存 ILM 规则。在将规则添加到 ILM 策略并激活该策略之前，该规则不会变为活动状态。

相关信息

- 示例 5： 用于严格载入行为的 ILM 规则和策略
- 创建 ILM 策略

创建默认 **ILM** 规则

在创建 ILM 策略之前，您必须创建一个默认规则，以便将其他规则不匹配的任何对象放置

在此策略中。默认规则不能使用任何筛选器。它必须应用于所有租户，所有分段和所有对象版本。

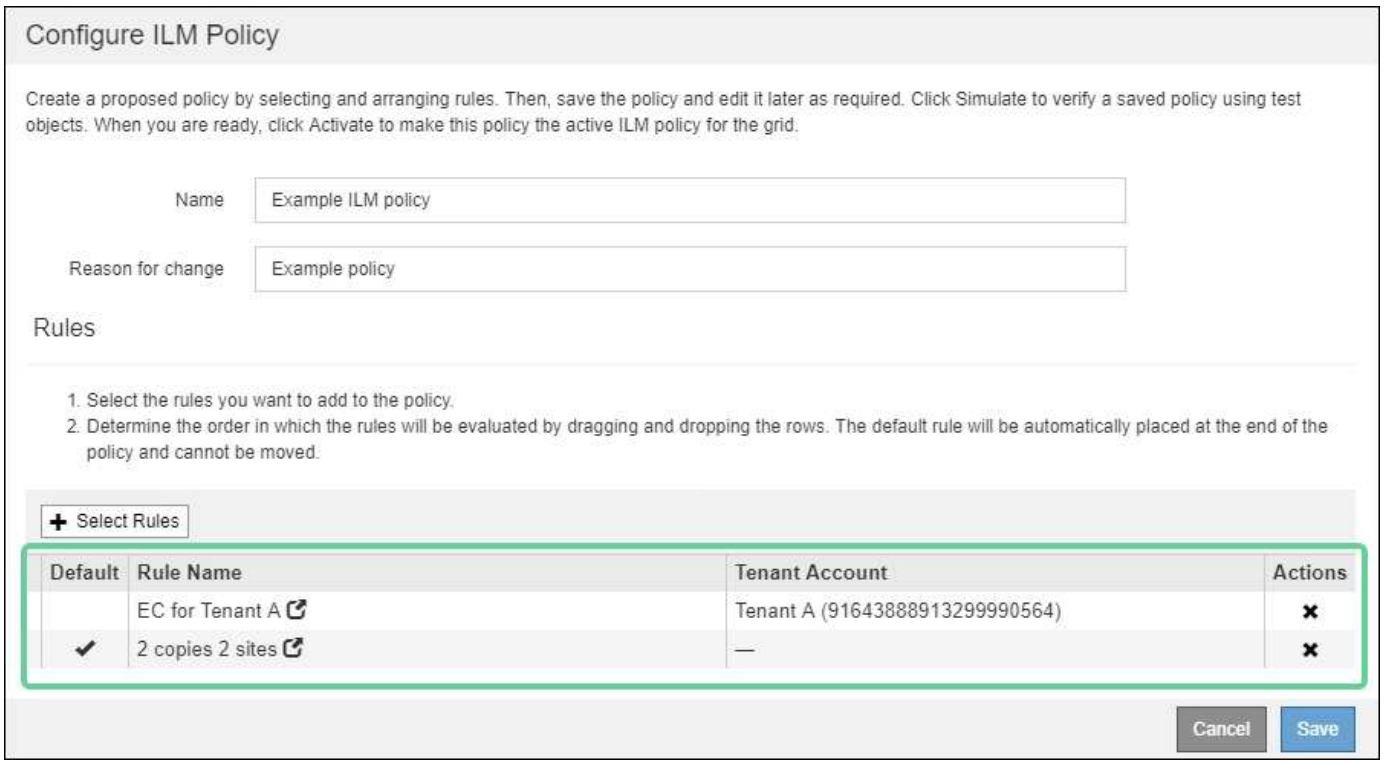
您需要的内容

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

关于此任务

默认规则是 ILM 策略中最后评估的规则，因此它不能使用任何筛选器或非当前参考时间。默认规则的放置说明将应用于策略中其他规则不匹配的任何对象。

在此示例策略中，第一个规则仅适用于属于租户 A 的对象默认规则，即属于所有其他租户帐户的适用场景 对象的最后一个规则。



创建默认规则时，请记住以下要求：

- 默认规则会自动作为策略中的最后一条规则放置。
- 默认规则不能使用任何基本或高级筛选器。
- 默认规则必须应用于所有对象版本，因此不能使用非当前时间参考时间。
- 默认规则应创建复制的副本。

> 请勿使用创建纠删编码副本的规则作为策略的默认规则。纠删编码规则应使用高级筛选器，以防止对较小的对象进行纠删编码。

- 通常，默认规则应永久保留对象。
- 如果您正在使用（或计划启用）全局 S3 对象锁定设置，则活动策略或建议策略的默认规则必须合规。

步骤

1. 选择 * ILM * > * 规则 * 。

   此时将显示 "ILM Rules" 页面。

2. 选择 * 创建 * 。

   此时将显示创建 ILM 规则向导的第 1 步（定义基础知识）。

3. 在 * 名称 * 字段中输入规则的唯一名称。
4. 或者，也可以在 * 问题描述 * 字段中为此规则输入一个短问题描述 。
5. 将 * 租户帐户 * 字段留空。

   默认规则必须应用于所有租户帐户。

6. 将 * 分段名称 * 字段留空。

   默认规则必须应用于所有 S3 分段和 Swift 容器。

7. 请勿选择 * 高级筛选 *

   默认规则不能指定任何筛选器。

8. 选择 * 下一步 * 。

   此时将显示第 2 步（定义放置位置）。

9. 对于 Reference Time ，请选择除 * 非当前时间 * 以外的任何选项。

   默认规则必须应用所有对象版本。

10. 指定默认规则的放置说明。
    - 默认规则应永久保留对象。如果默认规则不会永久保留对象，则在激活新策略时会显示警告。您必须确认这是您期望的行为。
    - 默认规则应创建复制的副本。

      请勿使用创建纠删编码副本的规则作为策略的默认规则。纠删编码规则应包含大于 0.2 * 的 * 对象大小（ MB ）高级筛选器，以防止对较小的对象进行纠删编码。

    - 如果您正在使用（或计划启用）全局 S3 对象锁定设置，则默认规则必须符合：
      - 它必须至少创建两个复制的对象副本或一个经过纠删编码的副本。
      - 这些副本必须在放置说明中每行的整个持续时间内存在于存储节点上。
      - 对象副本无法保存在云存储池中。
      - 无法将对象副本保存在归档节点上。
      - 放置说明中至少有一行必须从第 0 天开始，并使用载入时间作为参考时间。
      - 放置说明中至少一行必须为 "`forever 。` "

11. 选择 * 刷新 * 以更新保留示意图并确认放置说明。
12. 选择 * 下一步 * 。

    此时将显示第 3 步（定义载入行为）。

13. 选择要在载入对象时使用的数据保护选项，然后选择 * 保存 * 。

创建 ILM 策略

创建 ILM 策略：概述

创建 ILM 策略时，首先要选择并排列 ILM 规则。然后，您可以根据先前载入的对象模拟建议的策略，以验证其行为。如果您对建议的策略按预期运行感到满意，则可以激活此策略以创建活动策略。

> 配置不正确的 ILM 策略可能导致无法恢复的数据丢失。激活 ILM 策略之前，请仔细查看 ILM 策略及其 ILM 规则，然后模拟 ILM 策略。请始终确认 ILM 策略将按预期运行。

创建 ILM 策略的注意事项

- 仅在测试系统中使用系统的内置策略基线 2 副本策略。此策略中的 Make 2 Copies 规则使用包含所有站点的所有存储节点存储池。如果 StorageGRID 系统具有多个站点，则一个对象的两个副本可能会放置在同一站点上。
- 在设计新策略时，请考虑可能会输入到网格中的所有不同类型的对象。确保此策略包含与这些对象匹配并根据需要放置这些对象的规则。
- 尽量使 ILM 策略简单。这样可以避免在随时间推移对 StorageGRID 系统进行更改时，对象数据无法按预期得到保护的潜在危险情况。
- 确保策略中的规则顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。例如，如果策略中的第一个规则与某个对象匹配，则任何其他规则都不会评估该规则。
- 每个 ILM 策略中的最后一个规则是默认 ILM 规则，它不能使用任何筛选器。如果某个对象未被其他规则匹配，则默认规则将控制该对象的放置位置以及保留时间。
- 在激活新策略之前，请查看此策略对现有对象的放置所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

创建建议的 ILM 策略

您可以从头开始创建建议的 ILM 策略，也可以克隆当前活动策略（如果要从同一组规则开始）。

> 如果已启用全局 S3 对象锁定设置，请改用此操作步骤： 启用 S3 对象锁定后创建 ILM 策略。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已创建要添加到建议策略的 ILM 规则。您可以根据需要保存建议的策略，创建其他规则，然后编辑建议的

策略以添加新规则。

- 您已拥有 已创建默认 ILM 规则 不包含任何筛选器的策略。
- 您也可以观看以下视频： "视频： StorageGRID ILM 策略"

关于此任务

创建建议 ILM 策略的典型原因包括：

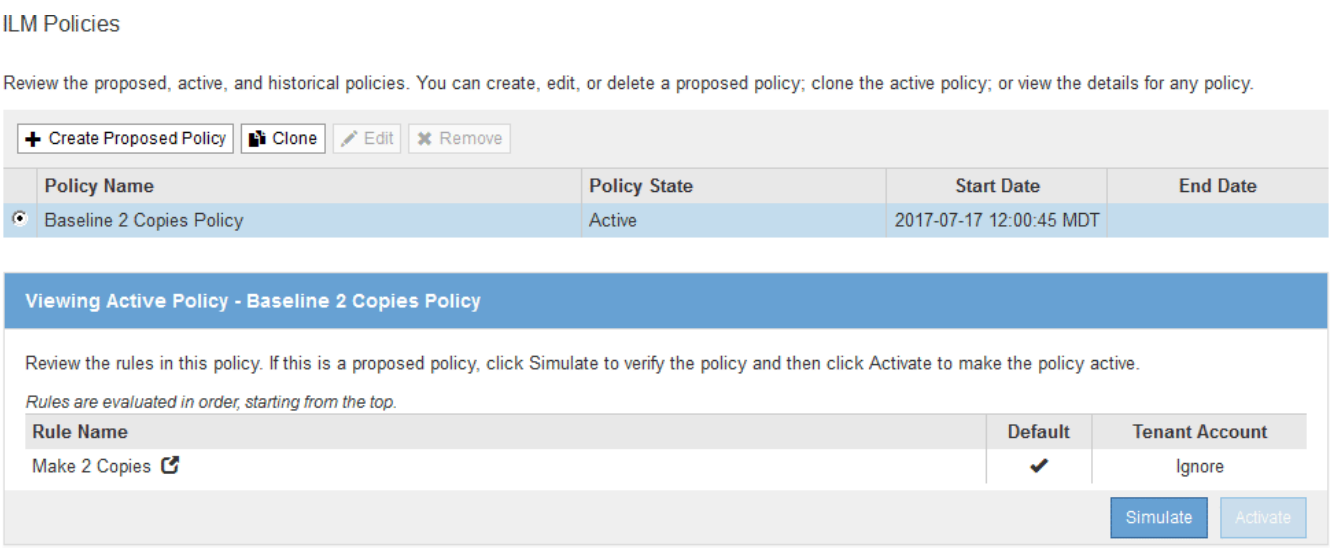
- 您添加了一个新站点，需要使用新的 ILM 规则在该站点上放置对象。
- 您正在停用某个站点，并且需要删除引用此站点的所有规则。
- 您添加了一个具有特殊数据保护要求的新租户。
- 您已开始使用云存储池。

仅在测试系统中使用系统的内置策略基线 2 副本策略。此策略中的 Make 2 Copies 规则使用包含所有站点的所有存储节点存储池。如果 StorageGRID 系统具有多个站点，则一个对象的两个副本可能会放置在同一站点上。

步骤

1. 选择 * ILM * > * 策略 * 。

   此时将显示 "ILM Policies" 页面。在此页面中，您可以查看建议的策略，活动策略和历史策略列表；创建，编辑， 或删除建议的策略；克隆活动策略；或查看任何策略的详细信息。

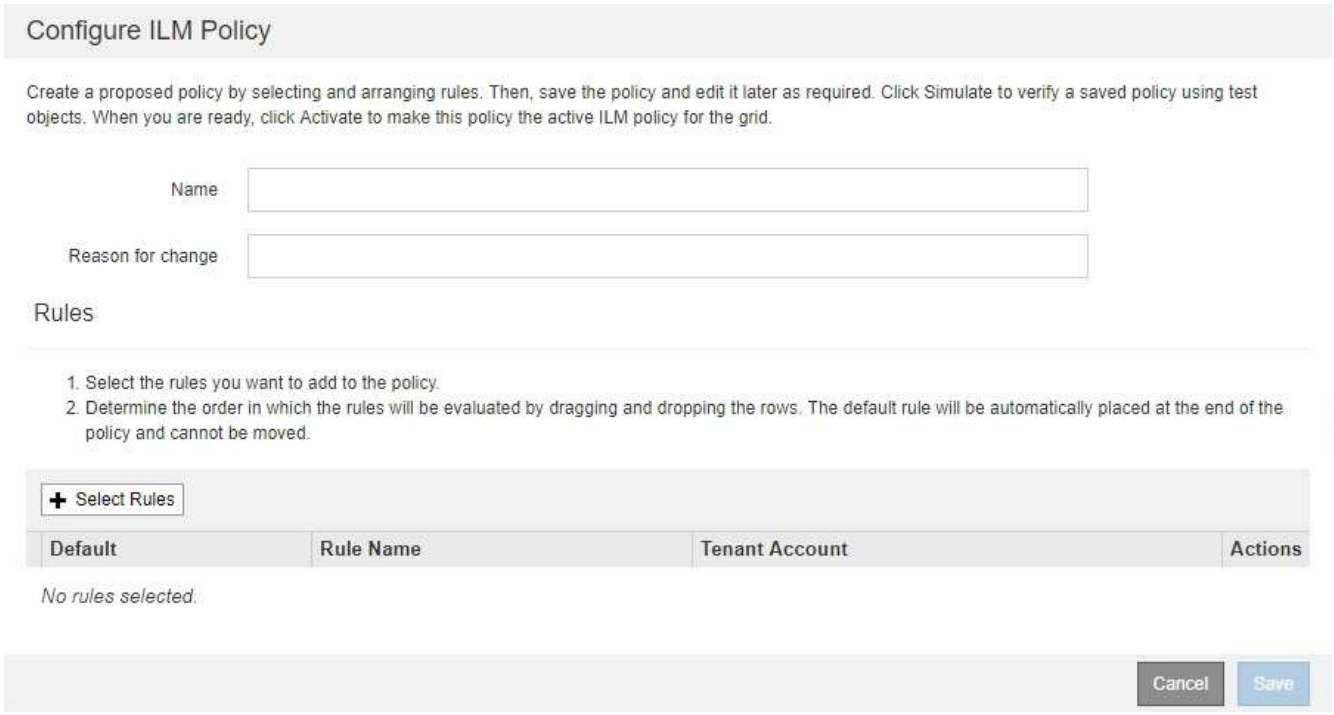


2. 确定要如何创建建议的 ILM 策略。

选项	步骤
创建尚未选择任何规则的新建议策略	a. 如果当前存在建议的 ILM 策略，请选择该策略，然后选择 * 删除 * 。 如果已存在建议的策略，则无法创建新的建议策略。 b. 选择 * 创建建议策略 * 。
根据活动策略创建建议的策略	a. 如果当前存在建议的 ILM 策略，请选择该策略，然后选择 * 删除 * 。 如果已存在建议的策略，则无法克隆活动策略。 b. 从表中选择活动策略。 c. 选择 * 克隆 * 。
编辑现有建议的策略	a. 从表中选择建议的策略。 b. 选择 * 编辑 * 。

此时将显示配置 ILM 策略对话框。

如果要创建新的建议策略，则所有字段均为空，不会选择任何规则。



如果要克隆活动策略，则 * 名称 * 字段将显示活动策略的名称，并附加一个版本号（在示例中为 "`v2` " ）。活动策略中使用的规则将按其当前顺序进行选择和显示。

3. 在 * 名称 * 字段中为建议的策略输入一个唯一名称。

   您必须输入至少 1 个字符，并且不能超过 64 个字符。如果要克隆活动策略，可以使用当前名称并附加版本号，也可以输入新名称。

4. 在 * 更改原因 * 字段中输入创建新建议策略的原因。

   您必须输入至少 1 个字符，并且不能超过 128 个字符。

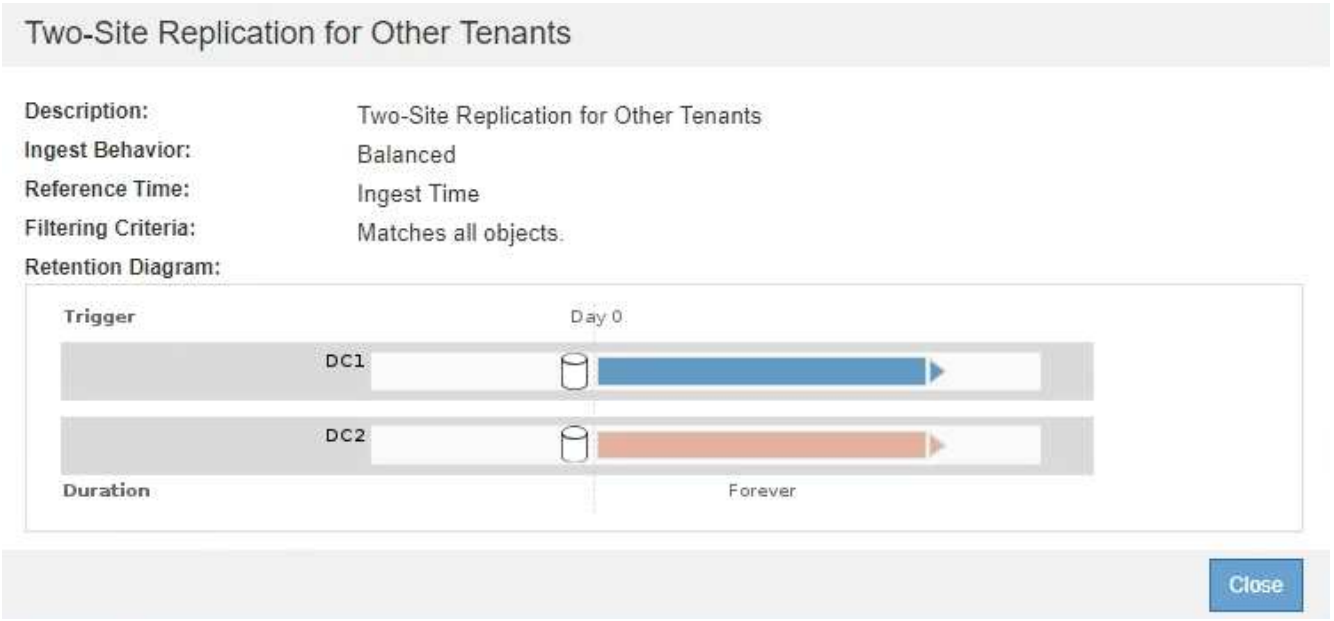
5. 要向策略中添加规则，请选择 * 选择规则 * 。

   此时将显示为策略选择规则对话框，其中列出了所有已定义的规则。如果要克隆策略：

   - 此时将选择要克隆的策略使用的规则。
   - 如果要克隆的策略使用了任何不含筛选器的规则，而这些规则不是默认规则，则系统会提示您删除除其中一个规则之外的所有规则。
   - 如果默认规则使用筛选器或非当前参考时间，系统将提示您选择新的默认规则。
   - 如果默认规则不是最后一条规则，则可以使用按钮将该规则移动到新策略的末尾。

6. 选择规则名称或更多详细信息图标 以查看该规则的设置。

此示例显示了在两个站点创建两个复制副本的 ILM 规则的详细信息。



7. 在 * 选择默认规则 * 部分中，为建议的策略选择一个默认规则。

默认规则适用场景 与策略中的其他规则不匹配的任何对象。默认规则不能使用任何筛选器，并且始终会在最后进行评估。

如果 " 选择默认规则 " 部分未列出任何规则，则必须退出 ILM 策略页面和 创建默认 ILM 规则。

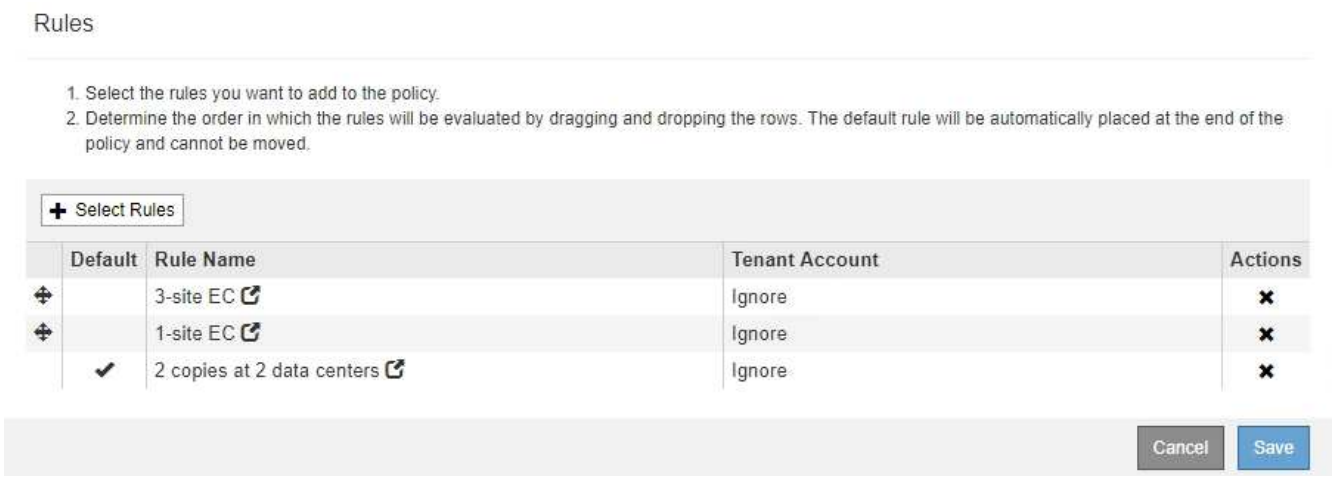
请勿使用 Make 2 copies 常用规则作为策略的默认规则。" 创建 2 个副本 " 规则使用一个存储池 " 所有存储节点 " ，其中包含所有站点。如果 StorageGRID 系统具有多个站点，则一个对象的两个副本可能会放置在同一站点上。

8. 在 * 选择其他规则 * 部分中，选择要包含在策略中的任何其他规则。

   其他规则会在默认规则之前进行评估，并且必须至少使用一个筛选器（租户帐户，分段名称，高级筛选器或非当前参考时间）。

9. 选择完规则后，请选择 * 应用 * 。

   此时将列出您选择的规则。默认规则位于末尾，上面有其他规则。



如果默认规则不会永久保留对象，则会显示警告。激活此策略时，您必须确认希望 StorageGRID 在默认规则的放置说明过后删除对象（除非分段生命周期将对象保留较长时间）。

10. 拖放非默认规则的行以确定评估这些规则的顺序。

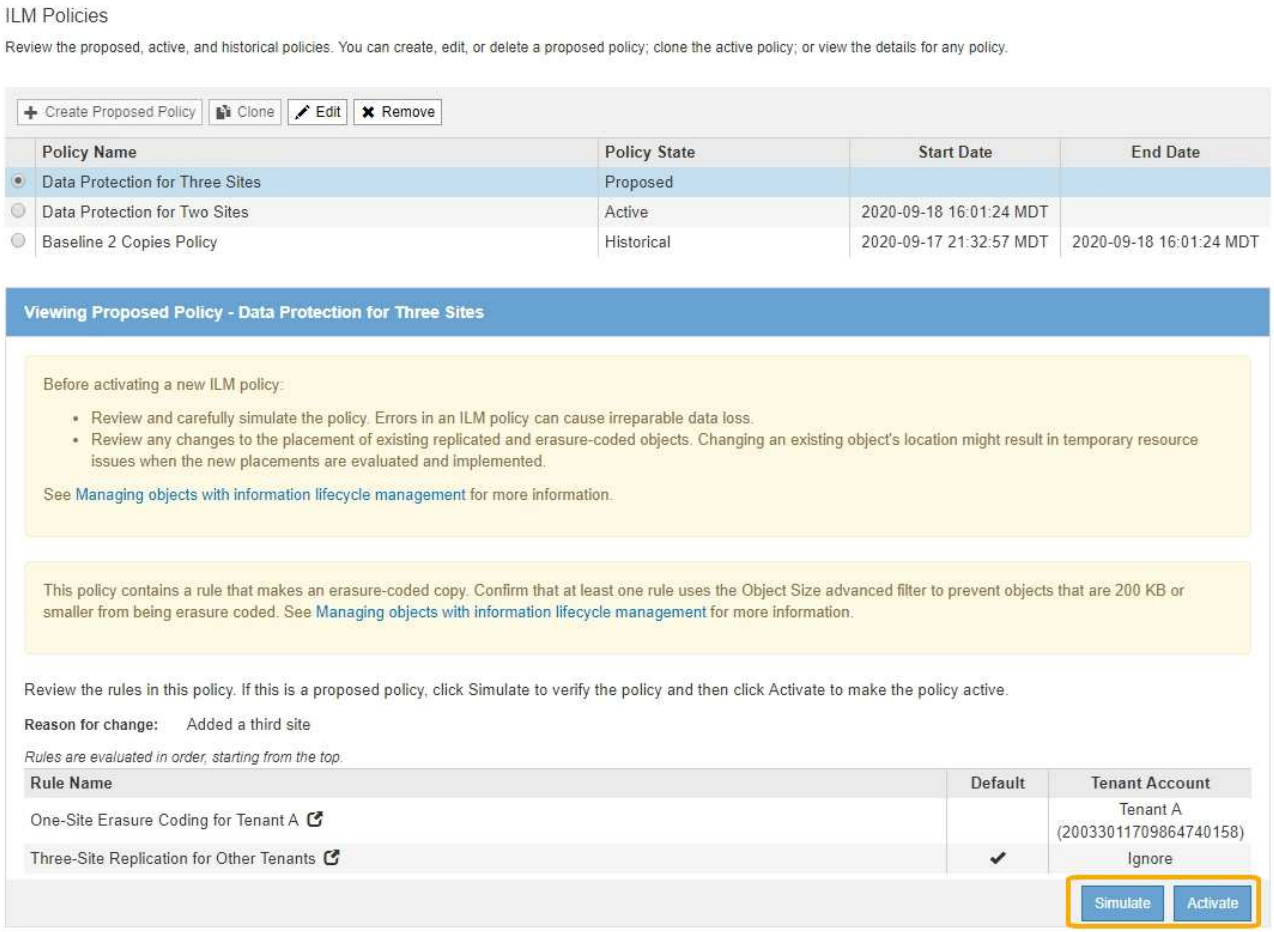
    您不能移动默认规则。

您必须确认 ILM 规则的顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。

11. 根据需要选择删除图标 ✖ 要删除策略中不需要的任何规则，请选择 * 选择规则 * 以添加更多规则。
12. 完成后，选择 * 保存 * 。

    此时将更新 "ILM Policies" 页面：

- 您保存的策略将显示为建议的策略。建议的策略没有开始日期和结束日期。
- 此时将启用 * 模拟 * 和 * 激活 * 按钮。



13. 转至 模拟 ILM 策略。

相关信息

- 什么是 ILM 策略
- 使用 S3 对象锁定管理对象

启用 **S3** 对象锁定后创建 **ILM** 策略

如果启用了全局 S3 对象锁定设置，则创建策略的步骤略有不同。您必须确保 ILM 策略符合已启用 S3 对象锁定的分段的要求。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 已为 StorageGRID 系统启用全局 S3 对象锁定设置。

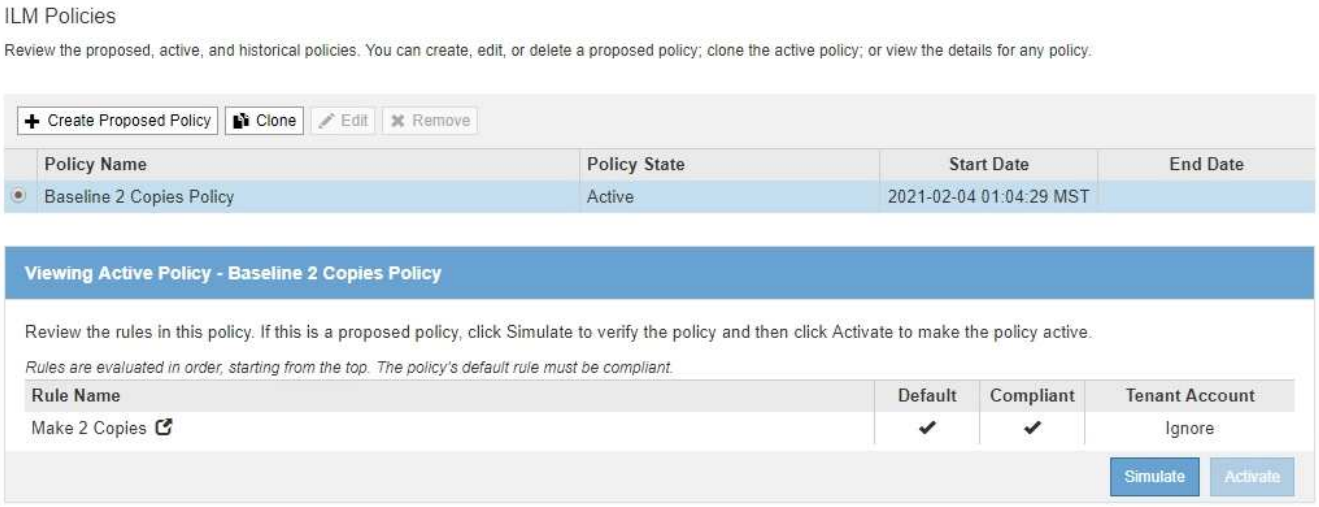
> 如果尚未启用全局 S3 对象锁定设置，请按照的常规说明进行操作 创建建议的 ILM 策略。

- 您已创建要添加到建议策略的合规和不合规 ILM 规则。您可以根据需要保存建议的策略，创建其他规则，然后编辑建议的策略以添加新规则。请参见示例 7： S3 对象锁定的兼容 ILM 策略。
- 您已拥有 已创建默认 ILM 规则 合规策略。
- 您也可以观看以下视频： "视频： StorageGRID ILM 策略"

步骤

1. 选择 * ILM * > * 策略 * 。

   此时将显示 "ILM Policies" 页面。如果启用了全局 S3 对象锁定设置，则 "ILM Policies" 页面将指示符合哪些 ILM 规则。



2. 在 * 名称 * 字段中为建议的策略输入一个唯一名称。

   您必须输入至少 1 个字符，并且不能超过 64 个字符。

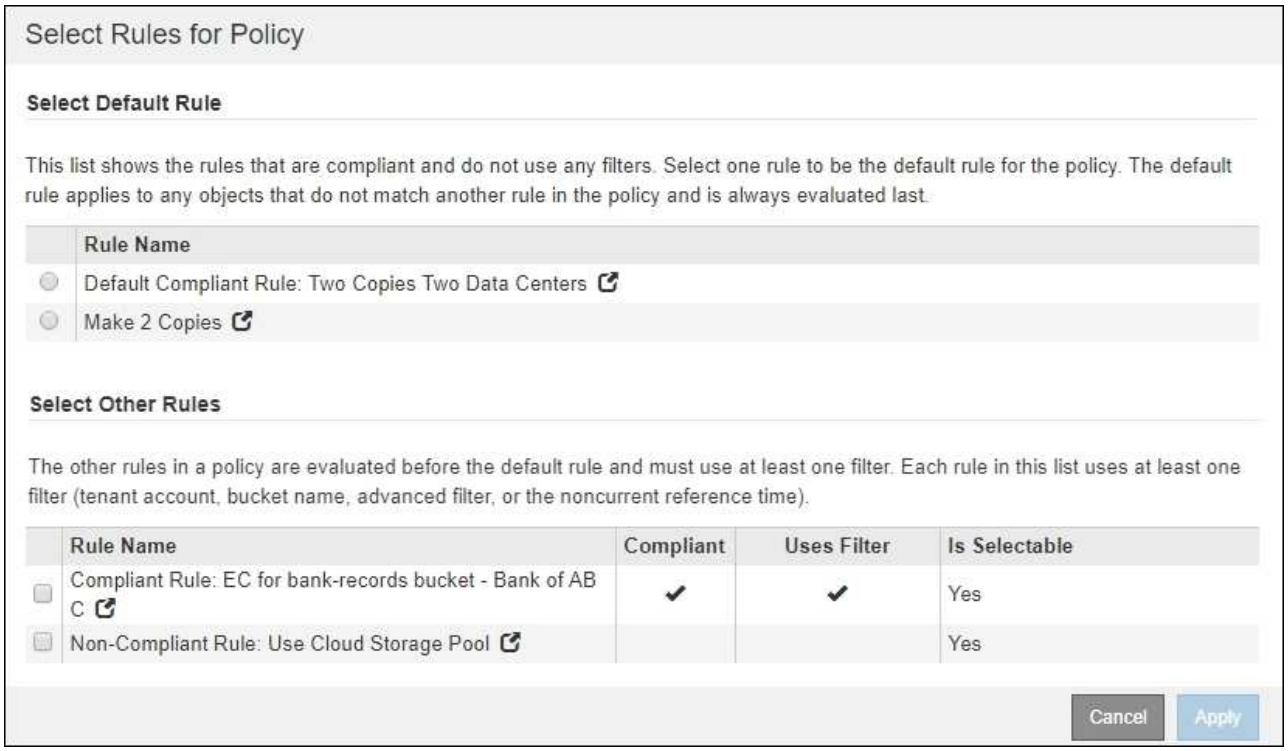
3. 在 * 更改原因 * 字段中输入创建新建议策略的原因。

   您必须输入至少 1 个字符，并且不能超过 128 个字符。

4. 要向策略中添加规则，请选择 * 选择规则 * 。

   此时将显示为策略选择规则对话框，其中列出了所有已定义的规则。

   - " 选择默认规则 " 部分列出了可作为合规策略的默认规则。它包括不使用筛选器或非当前参考时间的合规规则。
   - " 选择其他规则 " 部分列出了可为此策略选择的其他合规和不合规规则。



5. 选择规则名称或更多详细信息图标 以查看该规则的设置。
6. 在 * 选择默认规则 * 部分中，为建议的策略选择一个默认规则。

   本节中的表仅列出了合规的规则，不使用任何筛选器。

   如果 " 选择默认规则 " 部分未列出任何规则，则必须退出 ILM 策略页面和 创建默认 ILM 规则 合规。

   请勿使用 Make 2 copies 常用规则作为策略的默认规则。" 创建 2 个副本 " 规则使用一个存储池 " 所有存储节点 " ，其中包含所有站点。如果使用此规则，则一个对象的多个副本可能会放置在同一站点上。

7. 在 * 选择其他规则 * 部分中，选择要包含在策略中的任何其他规则。

   a. 如果您需要对不合规 S3 存储分段中的对象使用不同的 " 默认 `d` " 规则，则也可以选择一个不使用筛选器的不合规规则。

      例如，您可能希望使用云存储池或归档节点将对象存储在未启用 S3 对象锁定的存储分段中。

您只能选择一个不使用筛选器的不合规规则。选择一个规则后，对于不带筛选器的任何其他不合规规则， * 是可选 * 列将显示 * 否 * 。

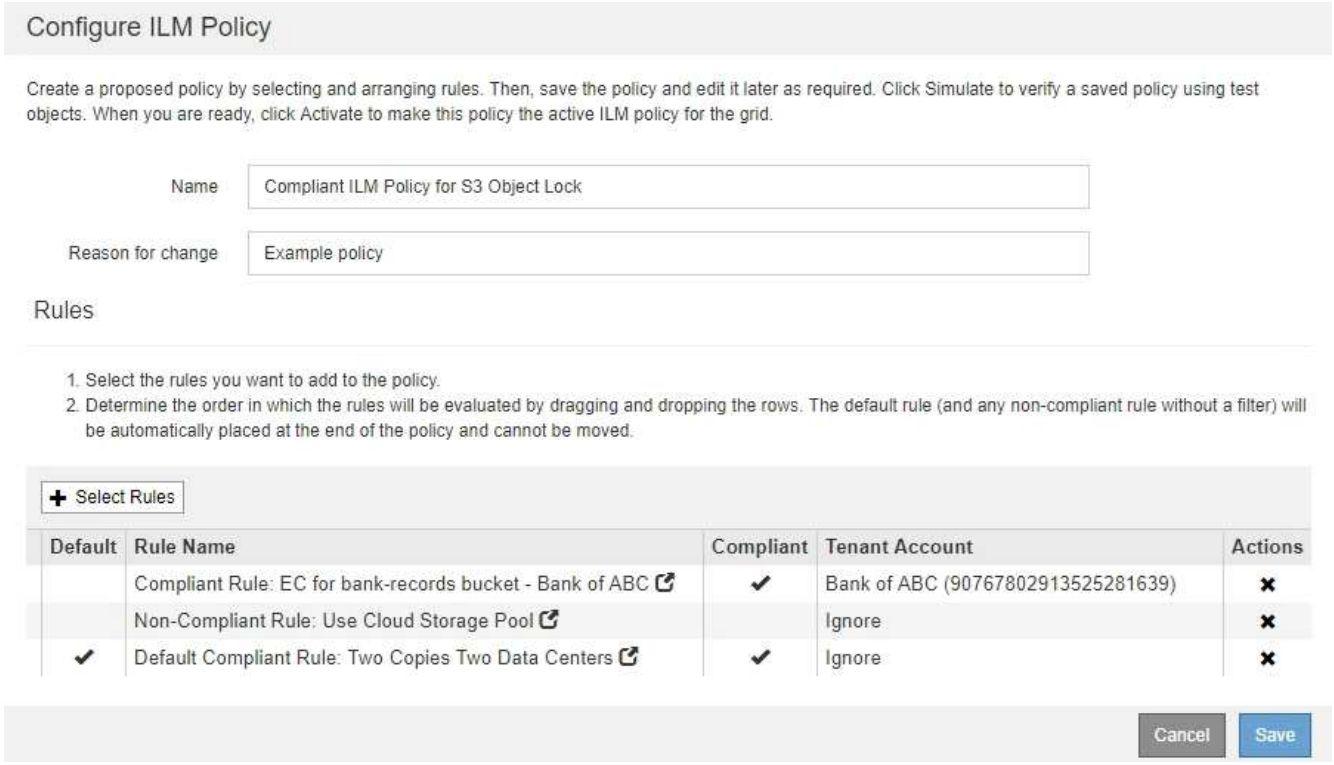
a. 选择要在策略中使用的任何其他合规或不合规规则。

其他规则必须至少使用一个筛选器（租户帐户，分段名称或高级筛选器，例如对象大小）。

8. 选择完规则后，请选择 * 应用 * 。

此时将列出您选择的规则。默认规则位于末尾，上面有其他规则。如果您还选择了一个不合规的 " `default` " 规则，则该规则将添加为策略中的倒数第二规则。

在此示例中，最后一条规则 2 copies 2 Data Center 是默认规则：它合规且不具有筛选器。第二个到最后一个规则 Cloud Storage Pool 也没有筛选器，但它不合规。



9. 拖放非默认规则的行以确定评估这些规则的顺序。

您不能移动默认规则或不合规的 " `default` " 规则。

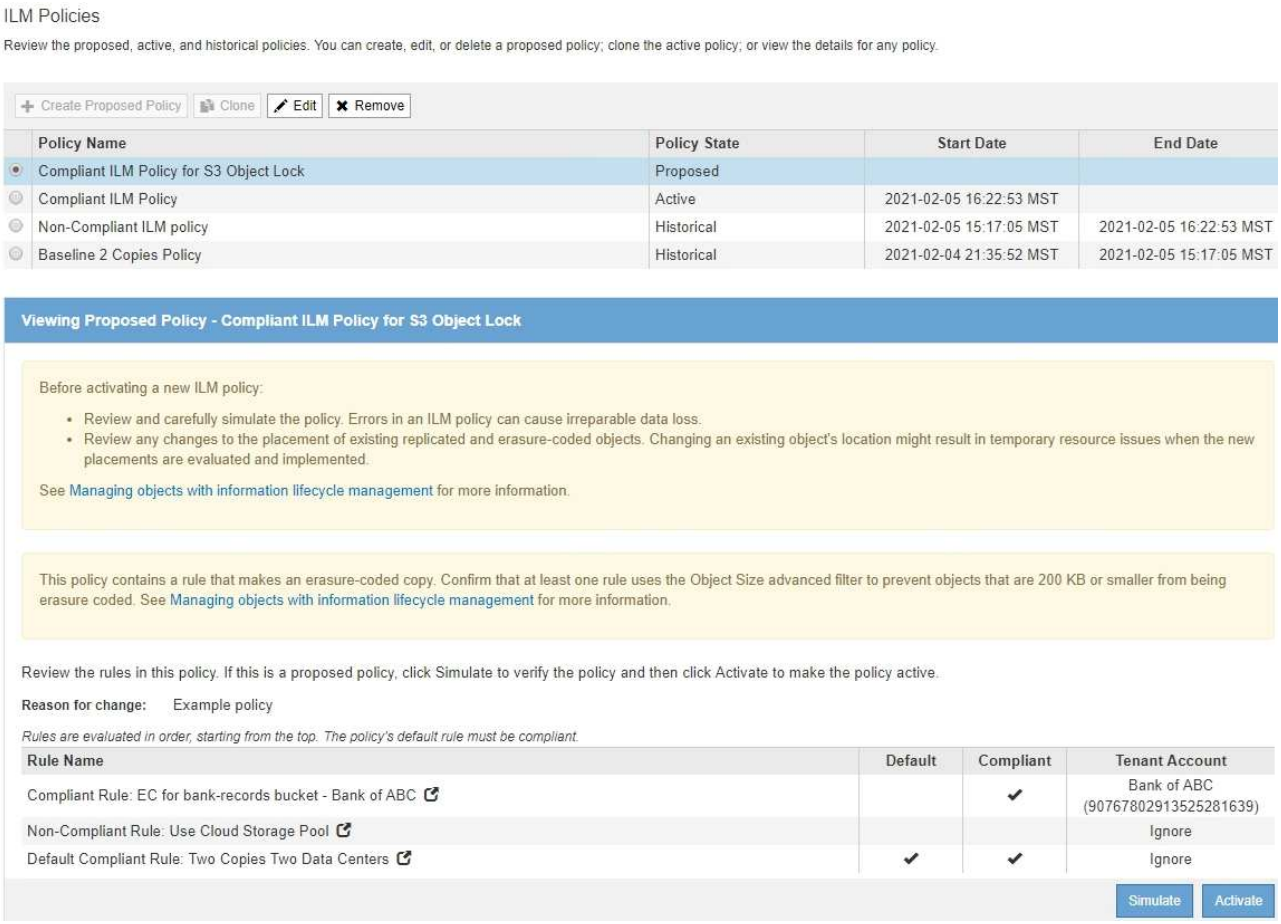
您必须确认 ILM 规则的顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。

10. 根据需要选择删除图标 ✖ 删除策略中不需要的任何规则，或者 * 选择规则 * 添加更多规则。
11. 完成后，选择 * 保存 * 。

此时将更新 "ILM Policies" 页面：

◦ 您保存的策略将显示为建议的策略。建议的策略没有开始日期和结束日期。

◦ 此时将启用 * 模拟 * 和 * 激活 * 按钮。



12. 转至 模拟 ILM 策略。

模拟 **ILM** 策略

在激活测试对象并将其应用于生产数据之前，您应先模拟建议的策略。模拟窗口提供了一个独立的环境，可在激活策略并将其应用于生产环境中的数据之前安全地对策略进行测试。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您知道要测试的每个对象的 S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称，并且您已输入这些对象。

关于此任务

您必须仔细选择要测试建议策略的对象。要全面模拟策略，您应至少为每个规则中的每个筛选器测试一个对象。

例如，如果某个策略包含一个规则来匹配存储分段 A 中的对象，另一个规则来匹配存储分段 B 中的对象，则必须从存储分段 A 中至少选择一个对象，并从存储分段 B 中选择一个对象来全面测试该策略。您还必须从另一个存储分段中至少选择一个对象，以测试默认规则。

模拟策略时，应考虑以下注意事项：

- 更改策略后，保存建议的策略。然后，模拟已保存的建议策略的行为。
- 模拟策略时，策略中的 ILM 规则会筛选测试对象，以便您可以查看对每个对象应用了哪个规则。但是，不会创建任何对象副本，也不会放置任何对象。运行模拟不会以任何方式修改数据，规则或策略。
- "Simulation" 页面会保留您测试的对象，直到您关闭，导航或刷新 "ILM Policies" 页面为止。
- Simulation 将返回匹配规则的名称。要确定哪个存储池或擦除编码配置文件有效，您可以通过选择规则名称或更多详细信息图标来查看保留图。
- 如果启用了 S3 版本控制，则只会根据对象的当前版本模拟策略。

步骤

1. 选择并排列规则，然后保存建议的策略。

   此示例中的策略有三个规则：

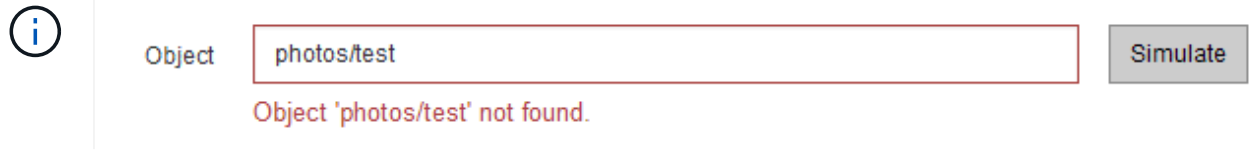
规则名称	筛选器	副本类型	Retention
X-men	• 租户 A • 用户元数据（系列 =x-men ）	在两个数据中心创建 2 个副本	2 年
PNGs	密钥以 .png 结尾	在两个数据中心创建 2 个副本	5 年
两个副本两个数据中心	无 _	在两个数据中心创建 2 个副本	永久

2. 使用 S3 或 Swift 客户端或 S3 控制台处于实验阶段（可在租户管理器中为每个租户提供），载入测试每个规则所需的对象。
3. 选择 * 模拟 * 。

   此时将显示模拟 ILM 策略对话框。

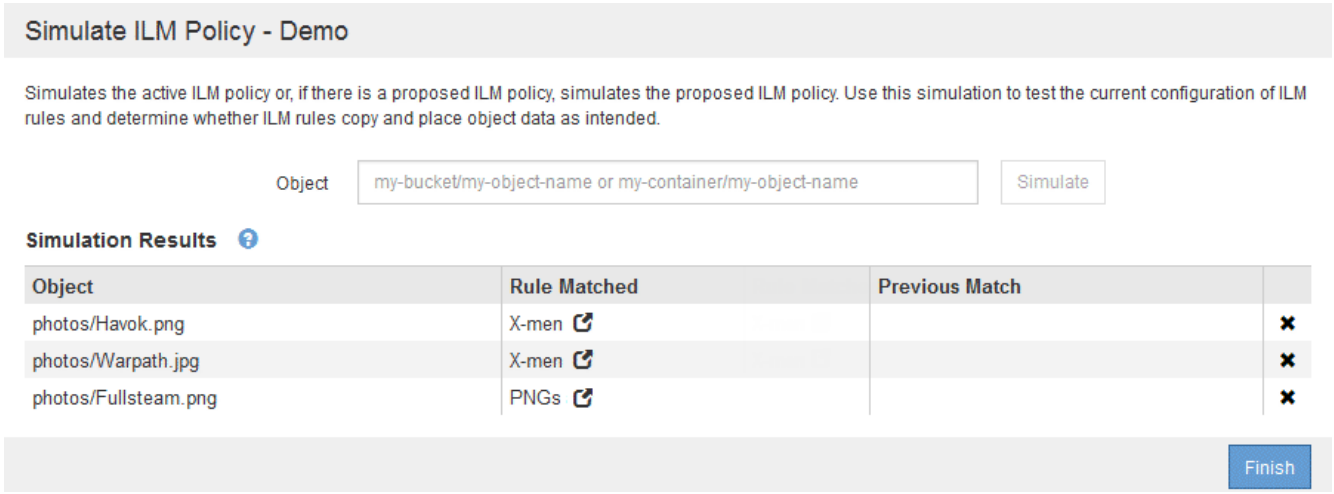
4. 在 * 对象 * 字段中，输入测试对象的 S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称，然后选择 * 模拟 * 。

如果指定的对象尚未被载入，则会显示一条消息。



5. 在 * 模拟结果 * 下，确认每个对象都符合正确的规则。

在此示例中， X-men 规则正确匹配了 `Havok.png` 和 `Warpath.jpg` 对象。不包括 `series=x-men` 用户元数据的 `Fullsteap.png` 对象未与 X-men 规则匹配，但已通过 PNGs 规则正确匹配。未使用默认规则，因为这三个对象都与其他规则匹配。

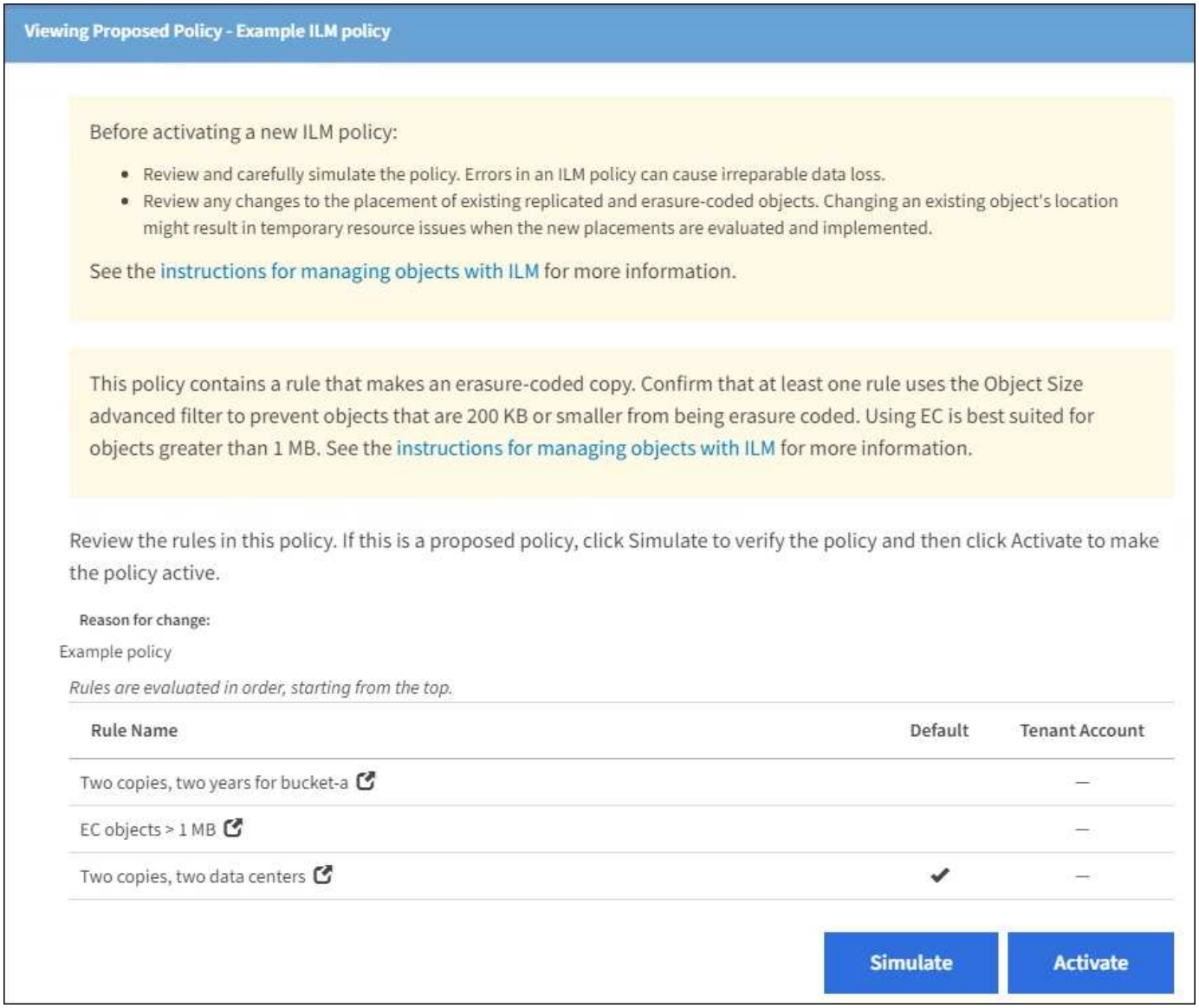


示例 **1** ： 模拟建议的 **ILM** 策略时验证规则

此示例显示了在模拟建议的策略时如何验证规则。

在此示例中，正在针对两个分段中的输入对象模拟 * 示例 ILM 策略 * 。此策略包括三个规则，如下所示：

- 第一条规则 * 两个副本，即 bucket-A* 两年，仅适用于 bucket-a 中的对象
- 第二条规则 * EC 对象 > 1 MB* ，适用场景 all b桶 but filters on objects 大于 1 MB 。
- 第三条规则为 * 两个副本，两个数据中心 * 。它不包含任何筛选器，也不使用非当前参考时间。



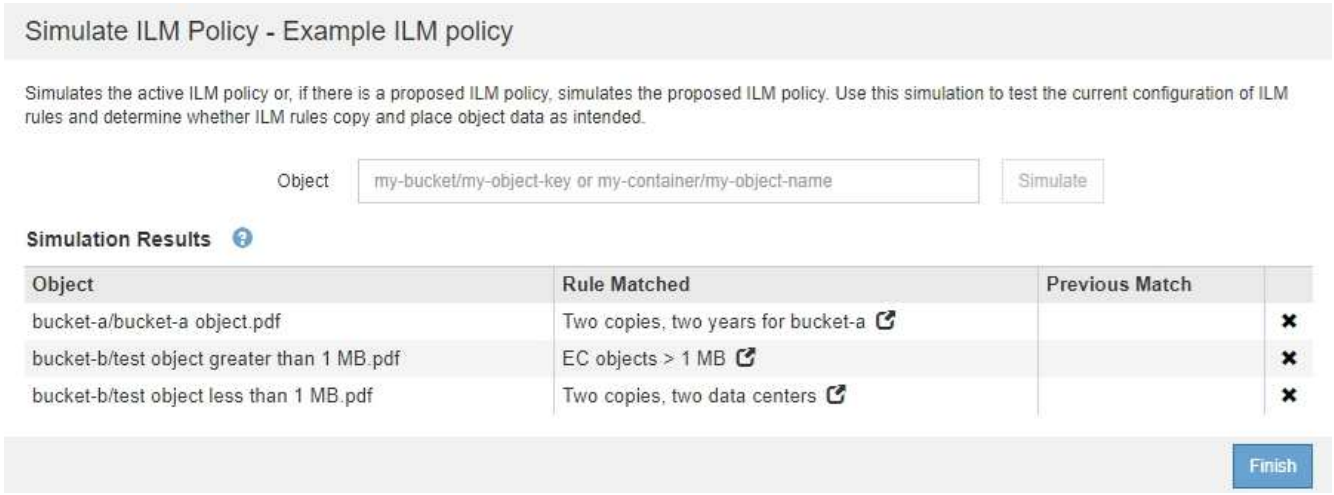
步骤

1. 添加规则并保存策略后，选择 * 模拟 * 。

   此时将显示模拟 ILM 策略对话框。

2. 在 * 对象 * 字段中，输入测试对象的 S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称，然后选择 * 模拟 * 。

   此时将显示模拟结果，其中显示了策略中与您测试的每个对象匹配的规则。



3. 确认每个对象均已使用正确的规则进行匹配。

   在此示例中：

   a. `bucket-A/bucket-a object.pdf` 与第一个规则正确匹配，该规则会对 `bucket-A` 中的对象进行筛选。

   b. `bucket-b/test 对象大于 1 mb.pdf` 位于 `bucket-b` 中，因此与第一条规则不匹配。而是通过第二条规则正确匹配，该规则会对大于 1 MB 的对象进行筛选。

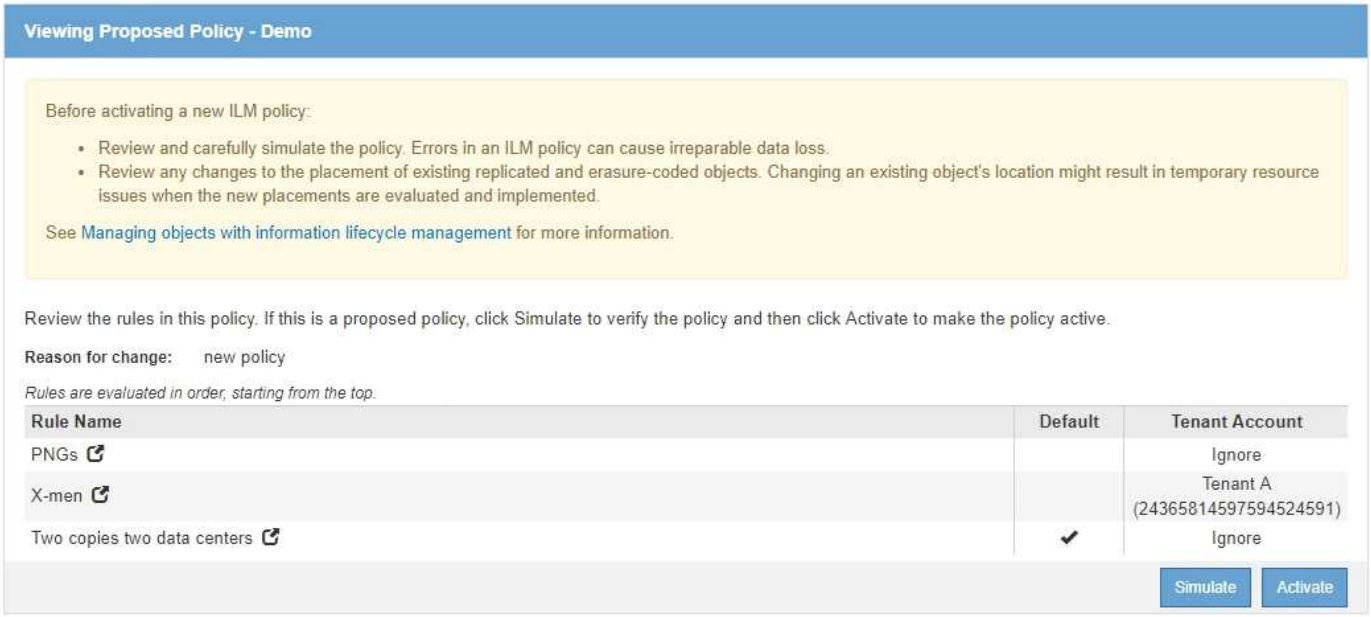
   c. `bucket-b/test 对象小于 1 mB.pdf` 与前两个规则中的筛选器不匹配，因此它将由默认规则放置，该规则不包含任何筛选器。

示例 **2**： 模拟建议的 **ILM** 策略时重新排列规则

此示例显示了在模拟策略时如何重新排列规则以更改结果。

在此示例中，正在模拟 * 演示 * 策略。此策略用于查找具有 series=x-men 用户元数据的对象，它包含以下三个规则：

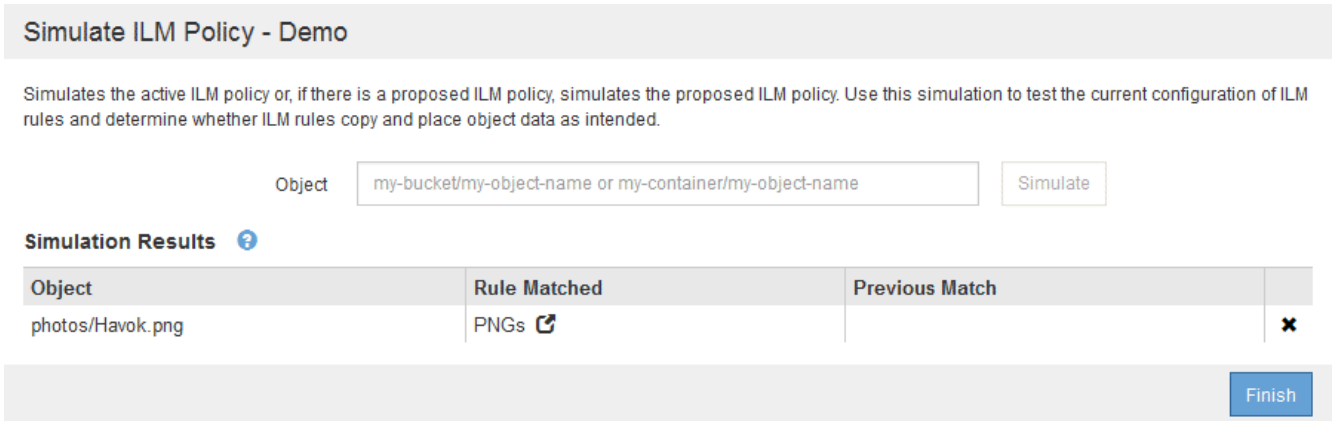
- 第一个规则 * PNGs* 会筛选以 ` .png` 结尾的密钥名称。
- 第二条规则 * X-men* 仅适用于租户 A 的对象以及 `series=x-men` 用户元数据的筛选器。
- 最后一条规则 * 两个副本两个数据中心 * 是默认规则，它匹配与前两个规则不匹配的任何对象。



步骤

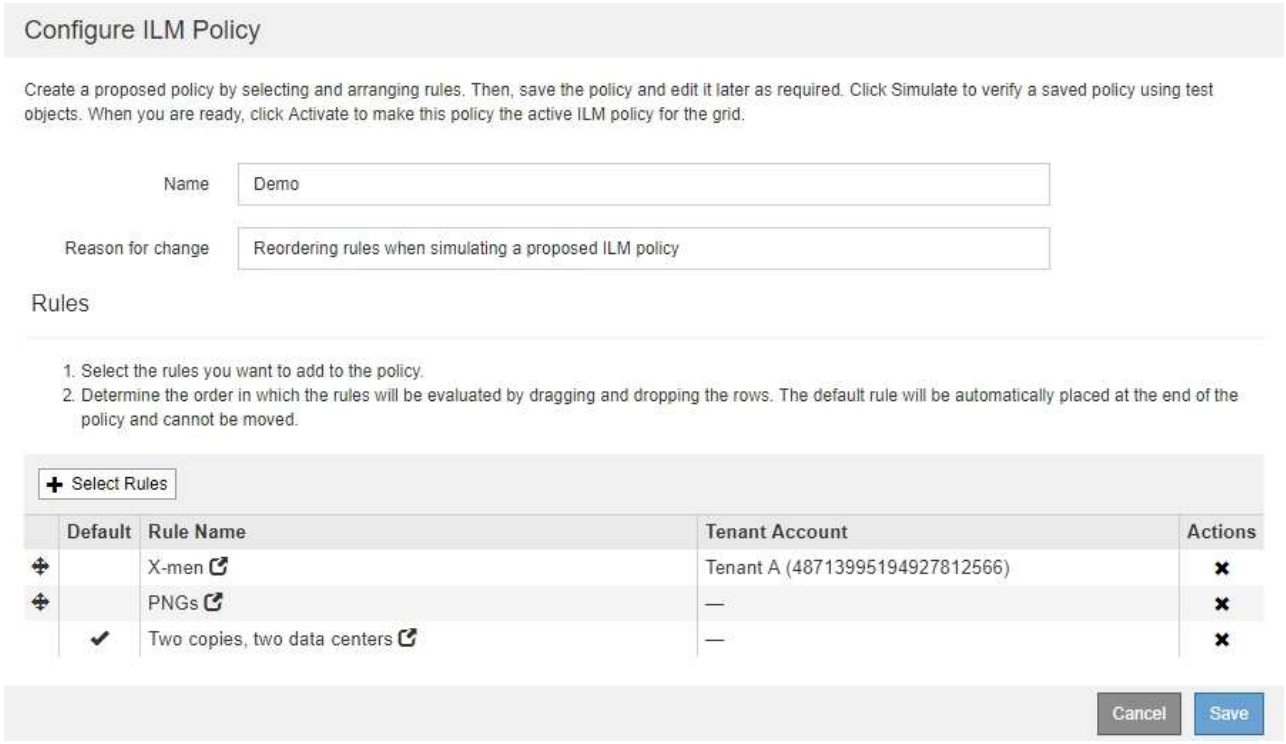
1. 添加规则并保存策略后，选择 * 模拟 * 。
2. 在 * 对象 * 字段中，输入测试对象的 S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称，然后选择 * 模拟 * 。

   此时将显示模拟结果，其中显示 `Havok.png` 对象与 * PNGs* 规则匹配。



   但是， `Havok.png` 对象用于测试的规则是 * X-men* 规则。

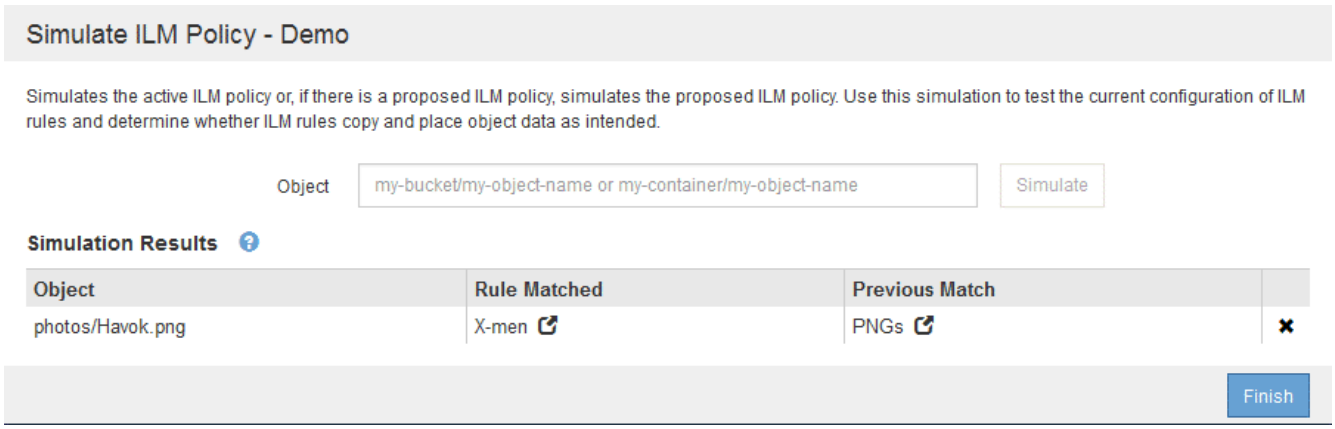
3. 要解析问题描述 ，请对规则重新排序。
   a. 选择 * 完成 * 以关闭模拟 ILM 策略页面。
   b. 选择 * 编辑 * 以编辑策略。
   c. 将 **X-men** 规则拖动到列表顶部。



d. 选择 * 保存 * 。

4. 选择 * 模拟 * 。

系统会根据更新后的策略重新评估先前测试的对象，并显示新的模拟结果。在此示例中， Rule matched 列显示 `Havok.png` 对象现在与 X-men 元数据规则匹配，如预期。上一个匹配列显示 PNGs 规则与上一个模拟中的对象匹配。

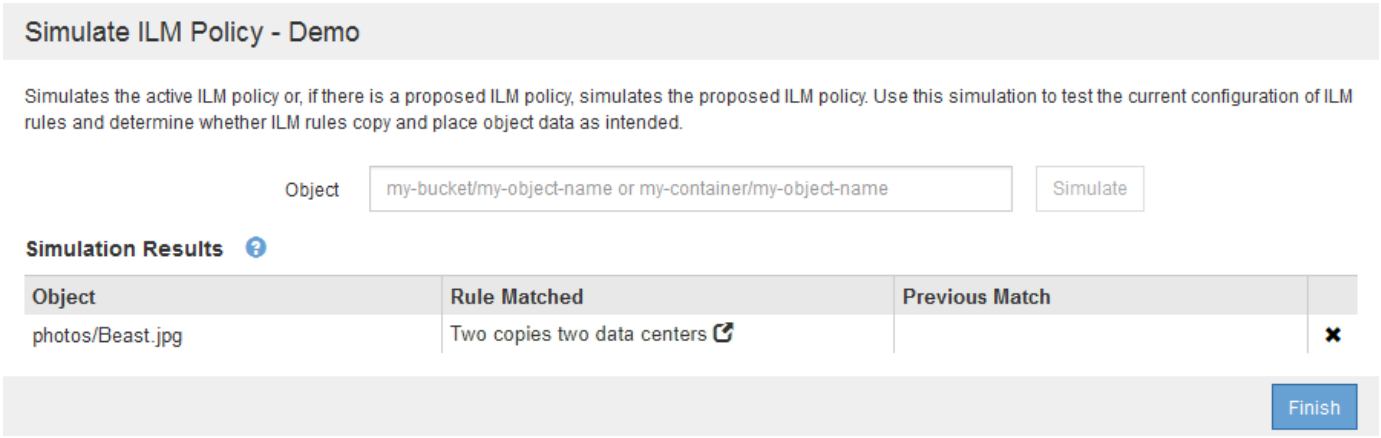


如果您停留在配置策略页面上，则可以在进行更改后重新模拟策略，而无需重新输入测试对象的名称。

示例 **3** ： 模拟建议的 **ILM** 策略时更正规则

此示例显示了如何模拟策略，更正策略中的规则以及继续模拟。

在此示例中，正在模拟 * 演示 * 策略。此策略用于查找具有 `series=x-men` 用户元数据的对象。但是，在针对 `Beast.jpg` 对象模拟此策略时，会出现意外结果。该对象与默认规则匹配，而不是与 X-men 元数据规则匹配，而是复制两个数据中心。

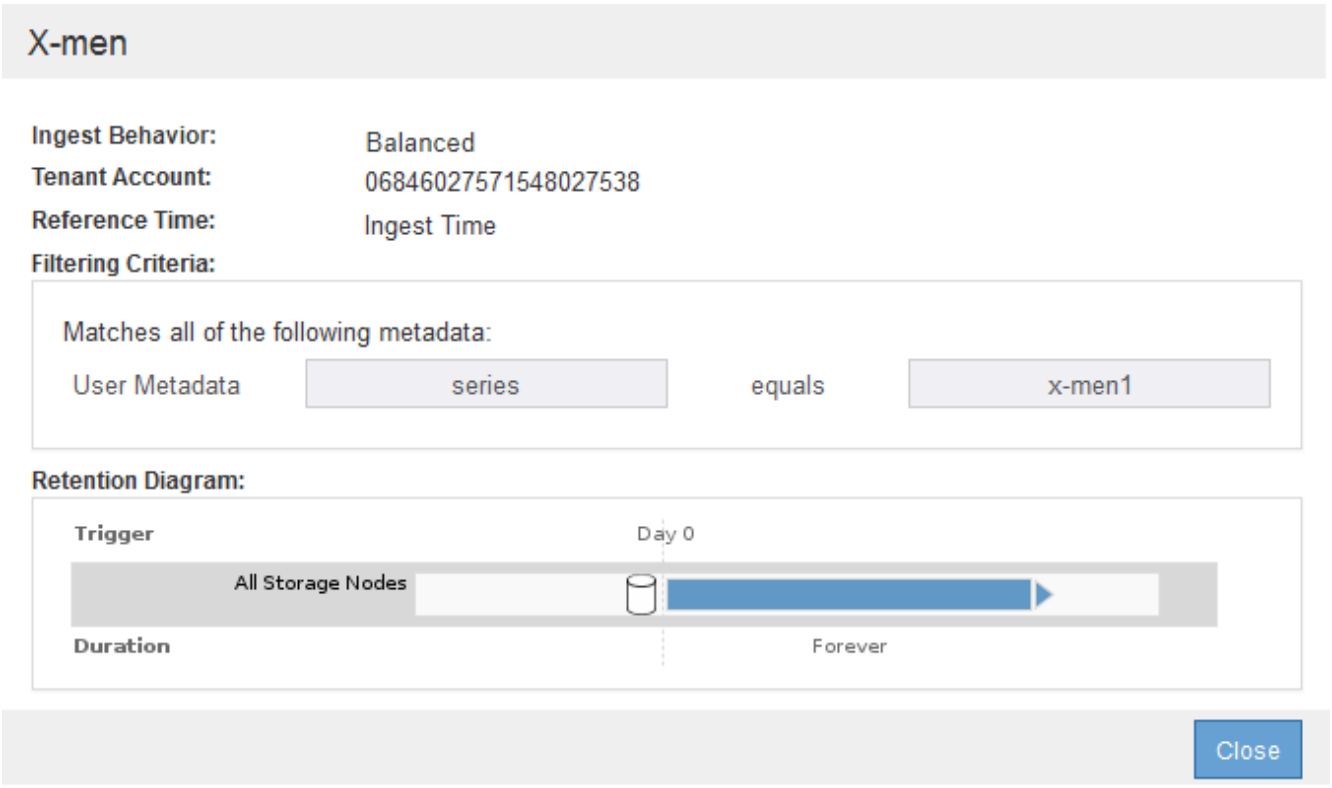


如果测试对象与策略中的预期规则不匹配，则必须检查策略中的每个规则并更正任何错误。

步骤

1. 对于策略中的每个规则，选择规则名称或更多详细信息图标以查看规则设置 显示规则的任何对话框上。
2. 查看规则的租户帐户，参考时间和筛选条件。

   在此示例中， X-men 规则的元数据包含错误。元数据值输入为 "`x-men1` " ，而不是 "`x-men.` "



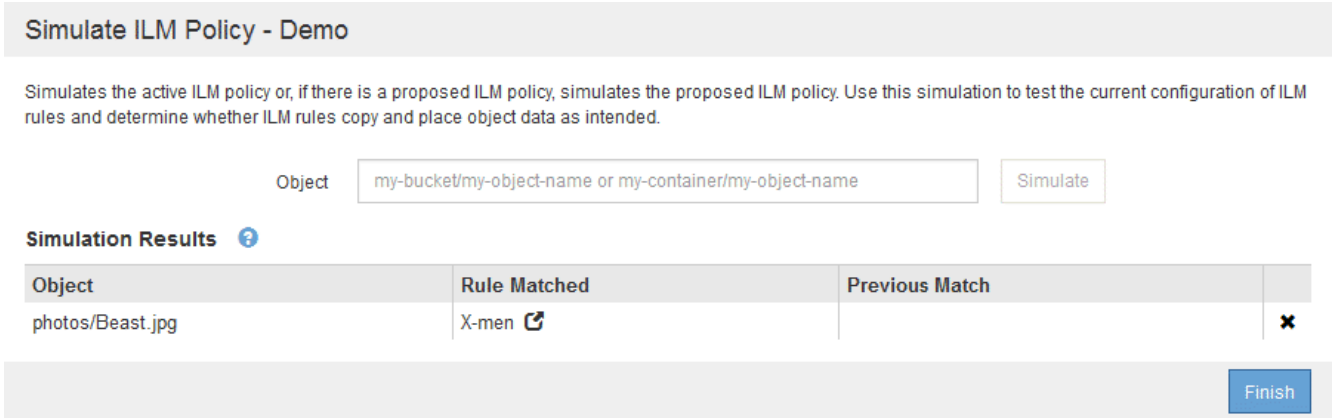
3. 要解决此错误，请按如下所示更正此规则：
   - 如果规则是建议策略的一部分，则可以克隆此规则，也可以从策略中删除此规则，然后对其进行编辑。
   - 如果规则是活动策略的一部分，则必须克隆此规则。您不能编辑活动策略中的规则或将其从活动策略中删除。

选项	Description
克隆规则	i. 选择 * ILM * > * 规则 * 。 ii. 选择不正确的规则，然后选择 * 克隆 * 。 iii. 更改不正确的信息，然后选择 * 保存 * 。 iv. 选择 * ILM * > * 策略 * 。 v. 选择建议的策略，然后选择 * 编辑 * 。 vi. 选择 * 选择规则 * 。 vii. 选中新规则的复选框，取消选中原始规则的复选框，然后选择 * 应用 * 。 viii. 选择 * 保存 * 。
编辑规则	i. 选择建议的策略，然后选择 * 编辑 * 。 ii. 选择删除图标 ✖ 要删除不正确的规则，请选择 * 保存 * 。 iii. 选择 * ILM * > * 规则 * 。 iv. 选择不正确的规则，然后选择 * 编辑 * 。 v. 更改不正确的信息，然后选择 * 保存 * 。 vi. 选择 * ILM * > * 策略 * 。 vii. 选择建议的策略，然后选择 * 编辑 * 。 viii. 选择更正后的规则，选择 * 应用 * ，然后选择 * 保存 * 。

4. 再次执行模拟。

由于您导航出 "ILM Policies" 页面以编辑此规则，因此先前为模拟输入的对象将不再显示。您必须重新输入对象的名称。

在本示例中，更正后的 X-men 规则现在会根据 `series=x-men` 用户元数据与 `Beast.jpg` 对象匹配，如预期。



将 ILM 规则添加到建议的 ILM 策略，模拟该策略并确认其行为符合预期后，您便可激活建议的策略。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您已保存并模拟建议的 ILM 策略。

> ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。在激活策略之前，请仔细查看并模拟策略，以确认策略将按预期运行。

> 激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

关于此任务

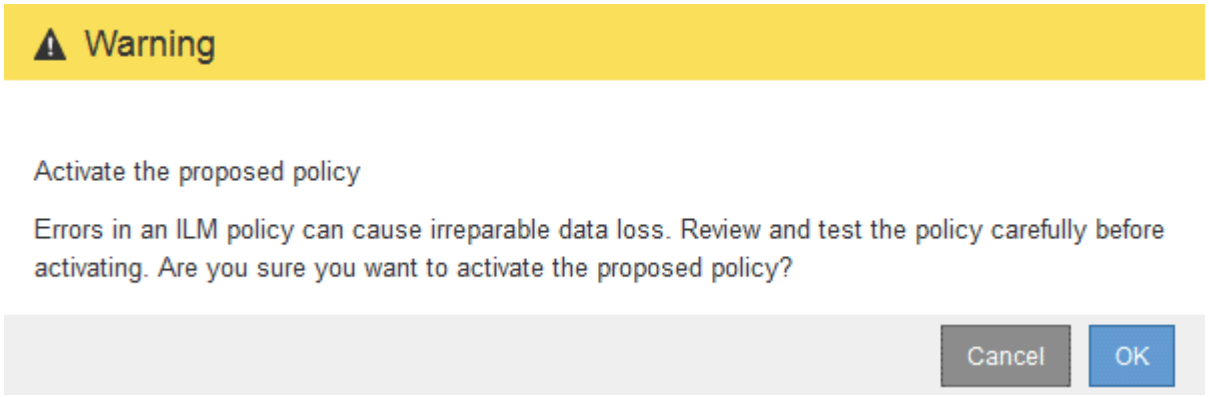
激活 ILM 策略时，系统会将新策略分发到所有节点。但是，只有在所有网格节点均可接收新策略之后，新的活动策略才会实际生效。在某些情况下，系统会等待实施新的活动策略，以确保不会意外删除网格对象。

- 如果进行策略更改以提高数据冗余或持久性，则这些更改将立即实施。例如，如果您激活包含三个副本规则而不是双个副本规则的新策略，则该策略将立即实施，因为它会增加数据冗余。
- 如果进行的策略更改可能会降低数据冗余或持久性，则只有在所有网格节点均可用后，这些更改才会实施。例如，如果您激活的新策略使用的是双副本规则，而不是三副本规则，则新策略将标记为 "`Active ，` " ，但只有在所有节点联机且可用后，它才会生效。

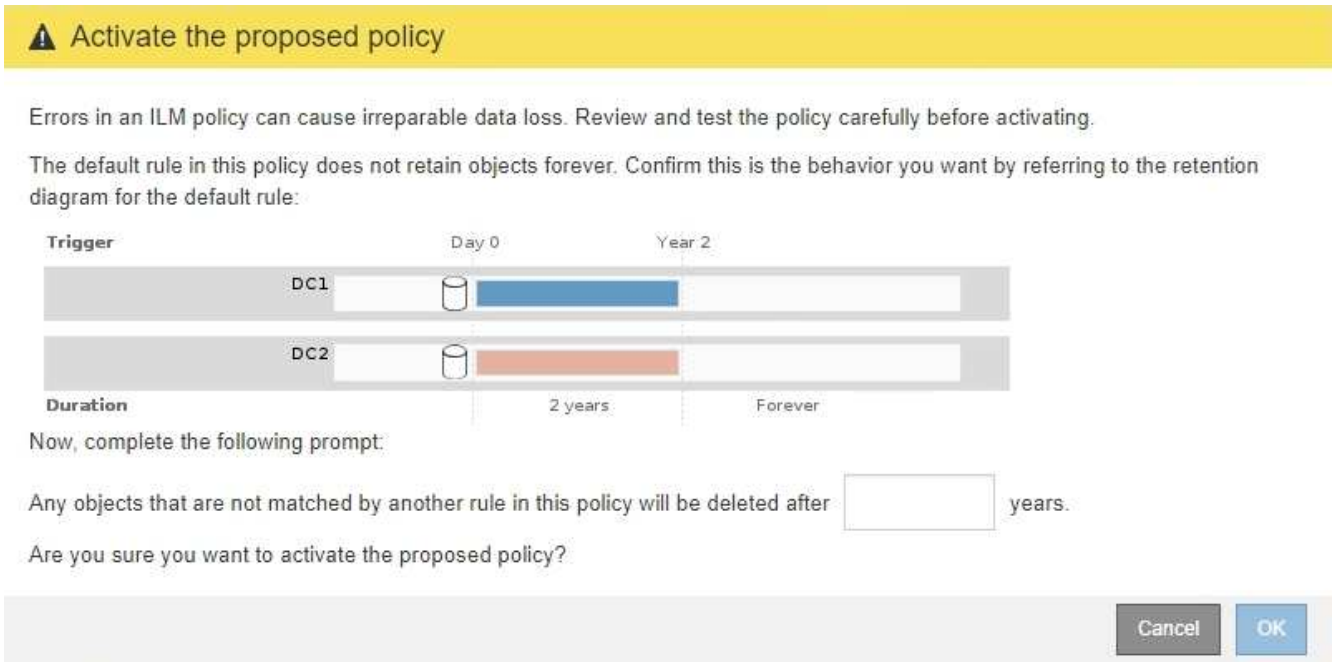
步骤

1. 准备好激活建议的策略后，请在 "ILM Policies" 页面上选择该策略并选择 * 激活 * 。

   此时将显示一条警告消息，提示您确认是否要激活建议的策略。



   如果策略的默认规则不会永久保留对象，则警告消息中会显示一条提示。在此示例中，保留示意图显示默认规则将在 2 年后删除对象。您必须在文本框中键入 **2** ，以确认策略中未与其他规则匹配的任何对象将在 2 年后从 StorageGRID 中删除。

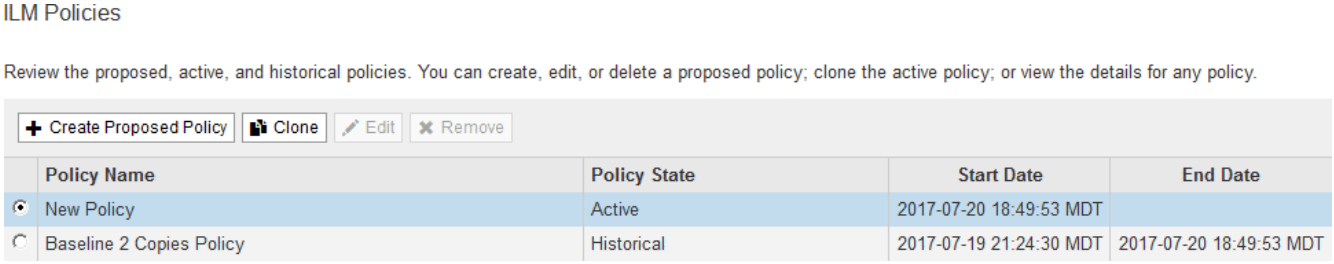


2. 选择 * 确定 * 。

结果

激活新的 ILM 策略后：

- 此策略在 "ILM Policies" 页面上的表中显示为 "Policy State Active" 。" 开始日期 " 条目指示策略的激活日期和时间。



- 此时将显示先前活动的策略，并且策略状态为 " 历史 " 。" 开始日期 " 和 " 结束日期 " 条目用于指示策略何时处于活动状态以及何时不再有效。

相关信息

[示例 6： 更改 ILM 策略]

使用对象元数据查找验证 **ILM** 策略

激活 ILM 策略后，应将代表性测试对象载入 StorageGRID 系统。然后，您应执行对象元数据查找，以确认副本是按预期创建的，并放置在正确的位置。

您需要的内容

- 您有一个对象标识符，可以是以下项之一：
  - * UUID * ： 对象的通用唯一标识符。以全大写形式输入 UUID 。

- * CBID*： StorageGRID 中对象的唯一标识符。您可以从审核日志中获取对象的 CBID 。输入全部大写的 CBID 。
- * S3 存储分段和对象密钥 *：通过 S3 接口载入对象时，客户端应用程序使用存储和标识对象的分段和对象密钥组合。如果 S3 存储分段已版本控制，并且您希望使用存储分段和对象密钥查找特定版本的 S3 对象，则您具有 * 版本 ID* 。
- * Swift 容器和对象名称 *：通过 Swift 界面输入对象时，客户端应用程序将使用容器和对象名称组合来存储和标识对象。

步骤

1. 正在载入对象。
2. 选择 * ILM * > * 对象元数据查找 * 。
3. 在 * 标识符 * 字段中键入对象的标识符。您可以输入 UUID ， CBID ， S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称。
4. 或者，输入对象的版本 ID （仅限 S3 ）。

5. 选择 * 查找 * 。

此时将显示对象元数据查找结果。此页面列出了以下类型的信息：

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

以下示例显示了存储为两个复制副本的 S3 测试对象的对象元数据查找结果。

System Metadata

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

Replicated Copies

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

Raw Metadata


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


6. 确认对象存储在正确的位置，并且是正确的副本类型。

> 如果启用了 Audit 选项，则还可以监控审核日志中是否显示了 "ORLM Object Rules" 消息。ORLM 审核消息可以为您提供有关 ILM 评估过程状态的详细信息，但不能为您提供有关对象数据放置是否正确或 ILM 策略是否完整的信息。您必须自己进行评估。有关详细信息，请参见 查看审核日志。

相关信息

- 使用 S3
- 使用 Swift

使用 ILM 规则和 ILM 策略

创建 ILM 规则和 ILM 策略后，您可以继续使用它们，并随存储需求的变化修改其配置。

您需要的内容

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

删除 **ILM** 规则

要使当前 ILM 规则列表易于管理，请删除不可能使用的任何 ILM 规则。

如果某个 ILM 规则当前已在活动策略或建议的策略中使用，则不能将其删除。如果需要删除使用策略的 ILM 规则，必须先执行以下步骤：

1. 克隆活动策略或编辑建议的策略。
2. 从策略中删除 ILM 规则。
3. 保存，模拟和激活新策略，以确保对象按预期受到保护。

步骤

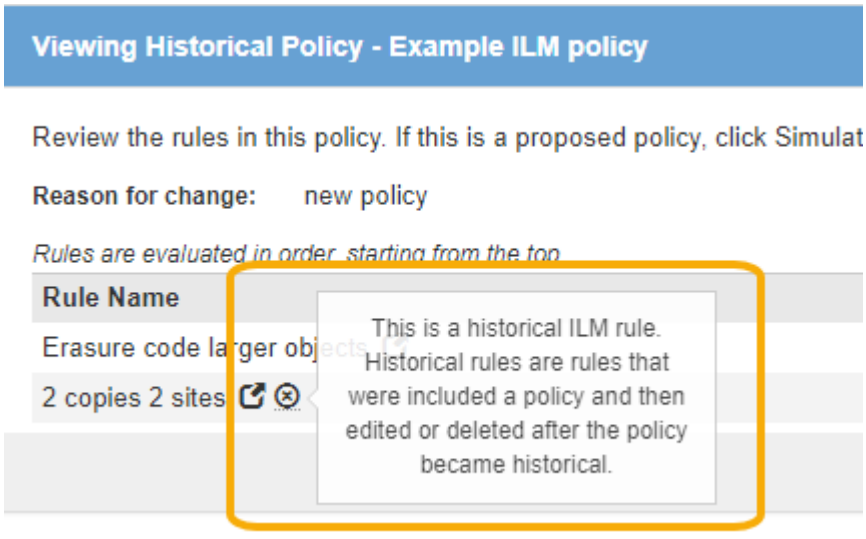
1. 选择 * ILM * > * 规则 * 。
2. 查看要删除的规则的表条目。

   确认此规则未在活动 ILM 策略或建议的 ILM 策略中使用。

3. 如果要删除的规则未在使用中，请选择单选按钮并选择 * 删除 * 。
4. 选择 * 确定 * 确认要删除 ILM 规则。

   此时将删除 ILM 规则。

如果删除历史策略中使用的规则，则会显示 ⊗ 查看策略时会显示规则图标，表示此规则已成为历史规则。



编辑 **ILM** 规则

要更改筛选器或放置指令，您可能需要编辑 ILM 规则。

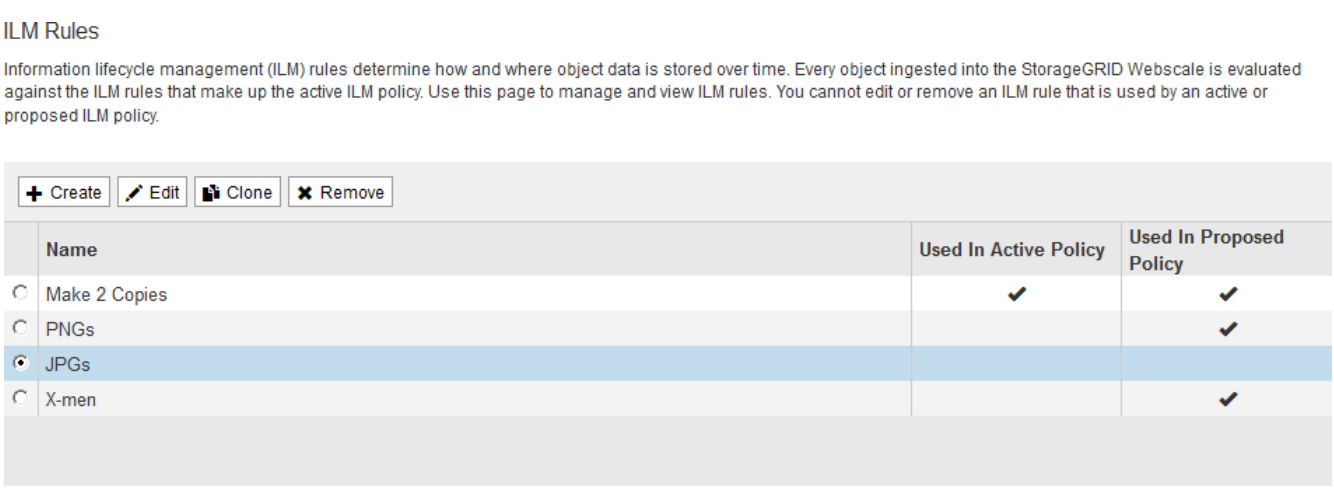
如果某个规则正在建议的 ILM 策略或活动 ILM 策略中使用，则无法编辑该规则。而是可以克隆这些规则并对克隆的副本进行任何必要的更改。您也不能编辑在 StorageGRID 10.3 之前创建的常用 ILM 规则（创建 2 个副本）或 ILM 规则。

> 在将已编辑的规则添加到活动 ILM 策略发生原因 之前，请注意，更改对象的放置指令可能会导致系统负载增加。

步骤

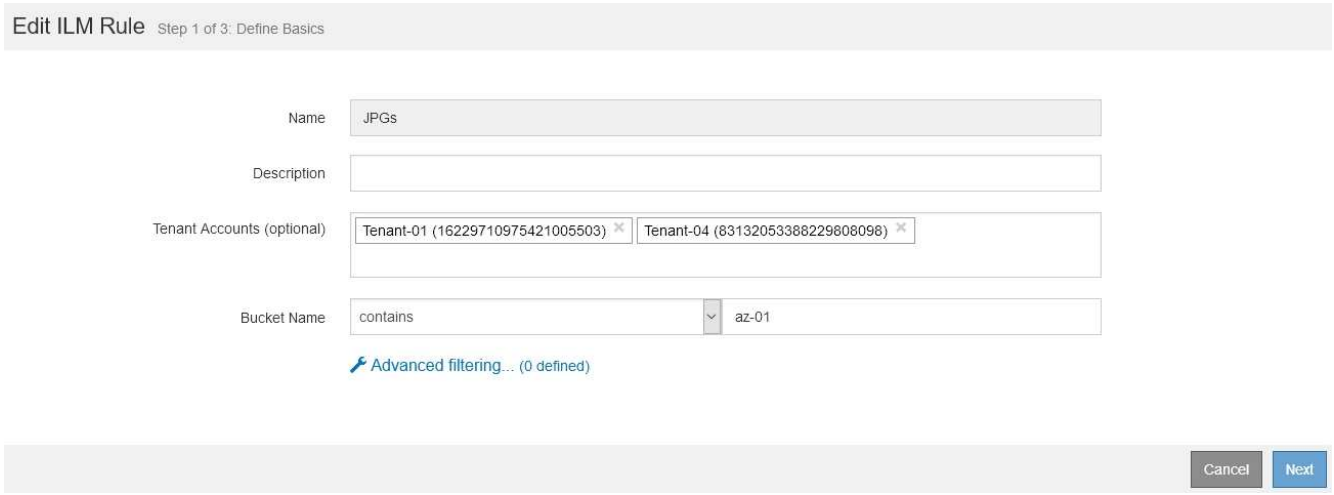
1. 选择 * ILM * > * 规则 * 。

   此时将显示 "ILM Rules" 页面。此页面显示所有可用规则，并指示活动策略或建议策略中正在使用哪些规则。



2. 选择未使用的规则，然后选择 * 编辑 * 。

   此时将打开编辑 ILM 规则向导。

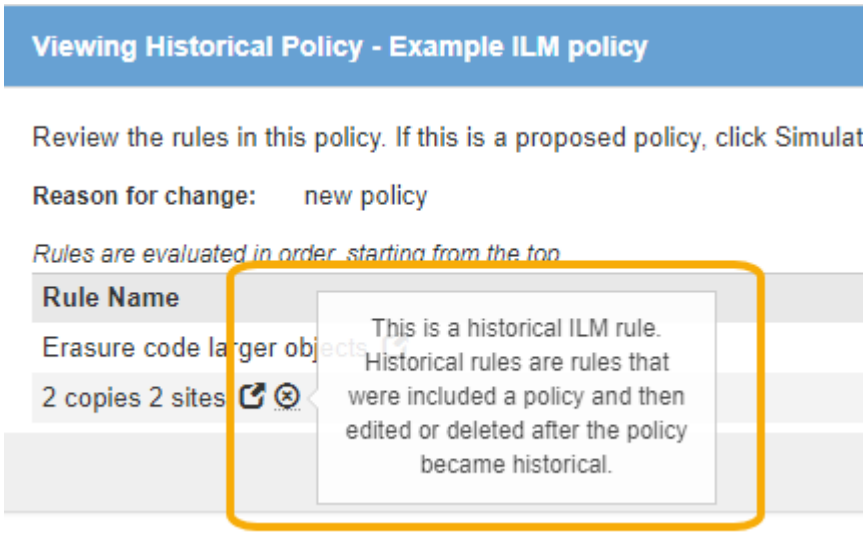


3. 按照的步骤完成编辑 ILM 规则向导中的各个页面 创建 ILM 规则 和 使用高级筛选器根据需要。

   编辑 ILM 规则时，不能更改其名称。

4. 选择 * 保存 * 。

如果编辑历史策略中使用的规则，则可以使用 ⊗ 查看策略时会显示规则图标，表示此规则已成为历史规则。



克隆 **ILM** 规则

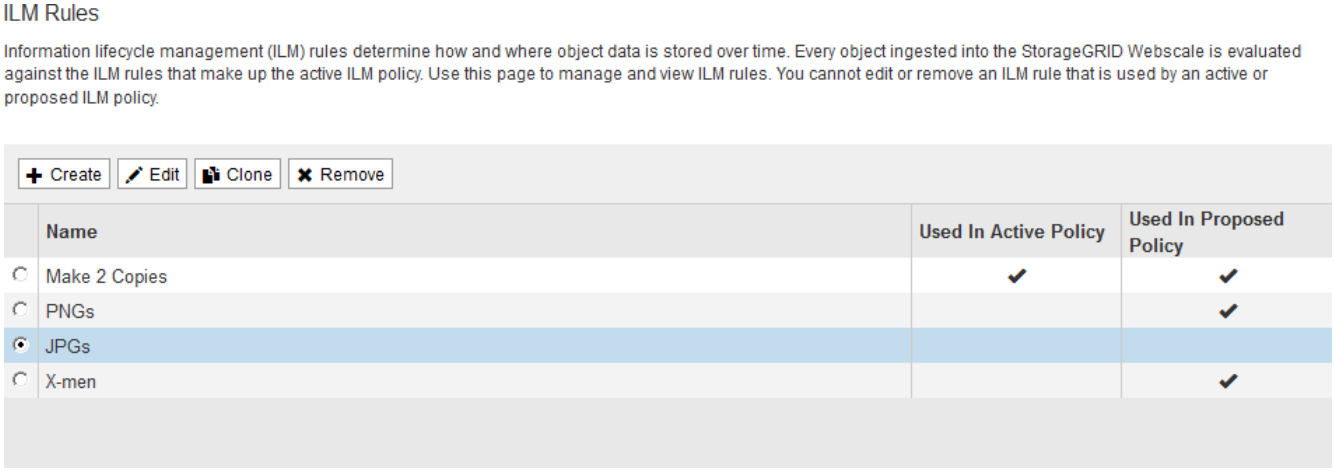
如果某个规则正在建议的 ILM 策略或活动 ILM 策略中使用，则无法编辑该规则。而是可以克隆规则并对克隆的副本进行任何必要的更改。然后，如果需要，您可以从建议的策略中删除原始规则，并将其替换为修改后的版本。如果 ILM 规则是使用 StorageGRID 10.2 或更早版本创建的，则无法克隆该规则。

在将克隆规则添加到活动 ILM 策略发生原因 之前，请注意，更改对象的放置指令可能会导致系统负载增加。

步骤

1. 选择 * ILM * > * 规则 * 。

   此时将显示 "ILM Rules" 页面。



2. 选择要克隆的 ILM 规则，然后选择 * 克隆 * 。

   此时将打开创建 ILM 规则向导。

3. 按照编辑 ILM 规则和使用高级筛选器的步骤更新克隆的规则。

   克隆 ILM 规则时，必须输入新名称。

4. 选择 * 保存 * 。

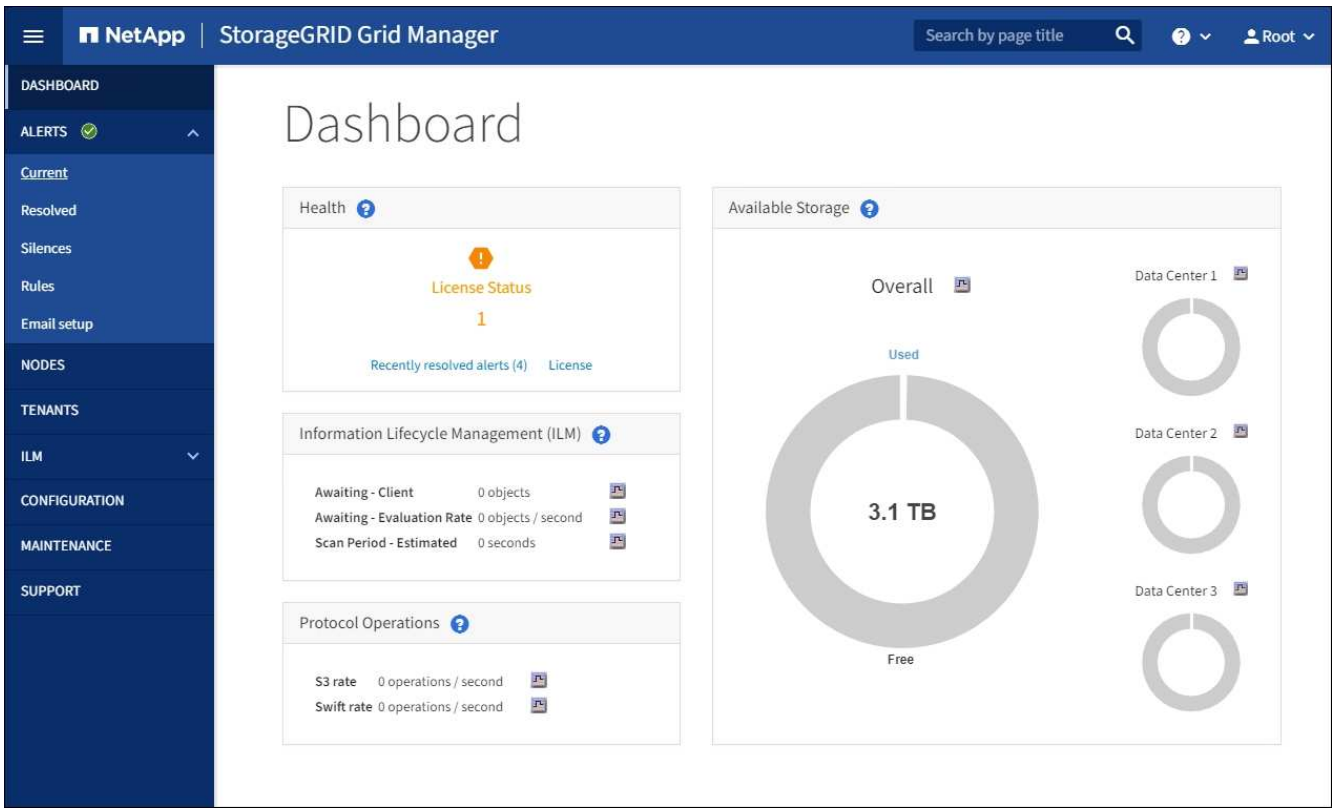
   此时将创建新的 ILM 规则。

查看 ILM 策略活动队列

您可以随时查看队列中要根据 ILM 策略进行评估的对象数量。您可能需要监控 ILM 处理队列以确定系统性能。队列较大可能表示系统无法跟上载入速率的增长，客户端应用程序的负载过大或存在异常情况。

步骤

1. 选择 * 信息板 * 。



2. 监控信息生命周期管理（ ILM ）部分。

   您可以选择问号 以查看本节中各项的问题描述 。

将 S3 对象锁定与 ILM 结合使用

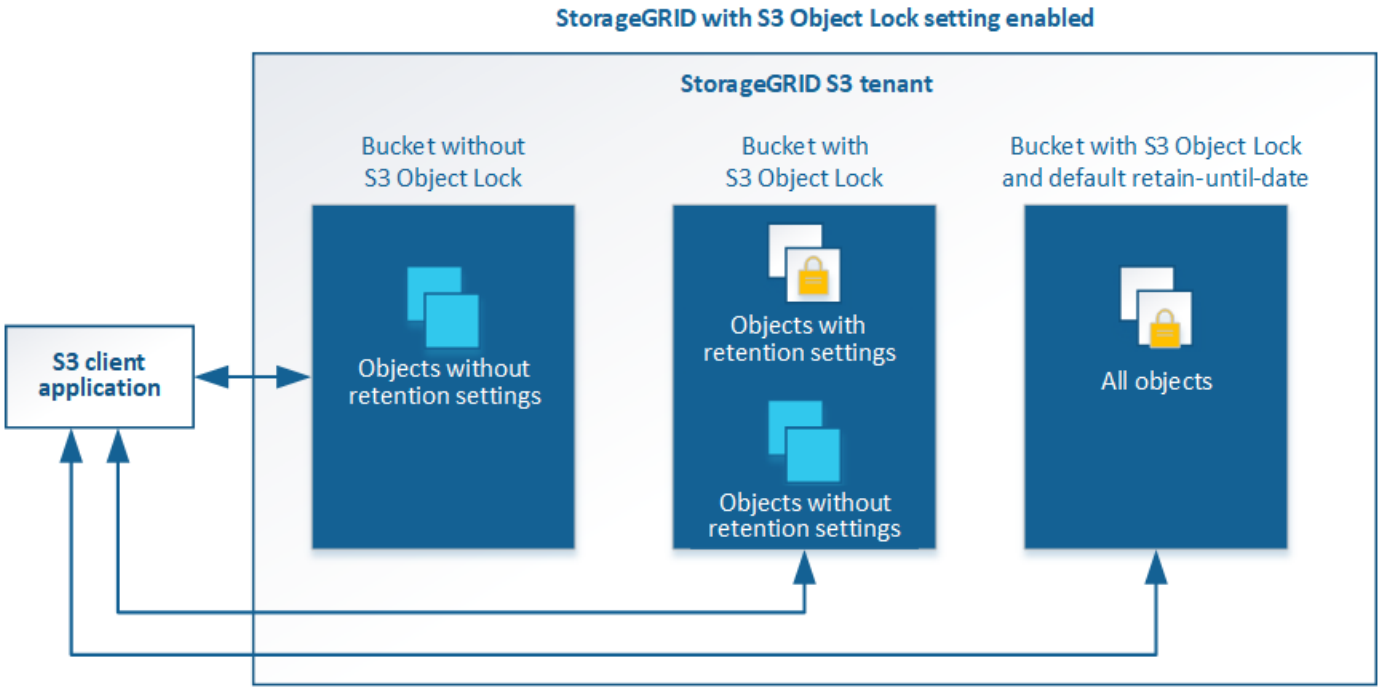
使用 S3 对象锁定管理对象

作为网格管理员，您可以为 StorageGRID 系统启用 S3 对象锁定，并实施合规的 ILM 策略，以确保特定 S3 存储分段中的对象在指定时间内不会被删除或覆盖。

什么是 S3 对象锁定?

StorageGRID S3 对象锁定功能是一种对象保护解决方案，相当于 Amazon Simple Storage Service （Amazon S3 ）中的 S3 对象锁定。

如图所示，如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则 S3 租户帐户可以在启用或不启用 S3 对象锁定的情况下创建存储分段。如果某个存储分段启用了 S3 对象锁定，则 S3 客户端应用程序可以选择为该存储分段中的任何对象版本指定保留设置。对象版本必须具有指定的保留设置，以受 S3 对象锁定的保护。此外，启用了 S3 对象锁定的每个存储分段也可以选择具有默认保留模式和保留期限，如果在没有自身保留设置的情况下将对象添加到存储分段，则此模式和保留期限适用。



StorageGRID S3 对象锁定功能提供了一种保留模式，相当于 Amazon S3 合规模式。默认情况下，任何用户都无法覆盖或删除受保护的对象版本。StorageGRID S3 对象锁定功能不支持监管模式，并且不允许具有特殊权限的用户绕过保留设置或删除受保护的对象。

如果存储分段启用了 S3 对象锁定，则在创建或更新对象时， S3 客户端应用程序可以选择指定以下任一或两个对象级别保留设置：

- * 保留至日期 * ：如果对象版本的保留至日期为未来日期，则可以检索该对象，但无法修改或删除它。可以根据需要增加对象的保留截止日期，但不能缩短此日期。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。合法保留与保留日期无关。

有关对象保留设置的详细信息，请转到 使用 S3 对象锁定。

有关默认存储分段保留设置的详细信息，请转至 使用 S3 对象锁定默认存储分段保留。

比较 S3 对象锁定与原有合规性

S3 对象锁定取代了早期 StorageGRID 版本中提供的合规性功能。由于 S3 对象锁定功能符合 Amazon S3 要求，因此它会弃用专有的 StorageGRID 合规性功能，现在称为 "`原有合规性 " 。`

如果您之前启用了全局合规性设置，则会自动启用全局 S3 对象锁定设置。租户用户无法再在启用了合规性的情况下创建新的分段；但是，根据需要，租户用户可以继续使用和管理任何现有的旧合规分段，其中包括执行以下任务：

- 将新对象载入已启用旧合规性的现有存储分段。
- 增加启用了旧合规性的现有存储分段的保留期限。
- 更改已启用旧合规性的现有存储分段的自动删除设置。
- 对已启用旧合规性的现有存储分段置于合法保留状态。
- 取消合法保留。

请参见 "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段" 有关说明，请参见。

如果您在先前版本的 StorageGRID 中使用了原有的合规性功能，请参见下表，了解它与 StorageGRID 中的 S3 对象锁定功能的比较情况。

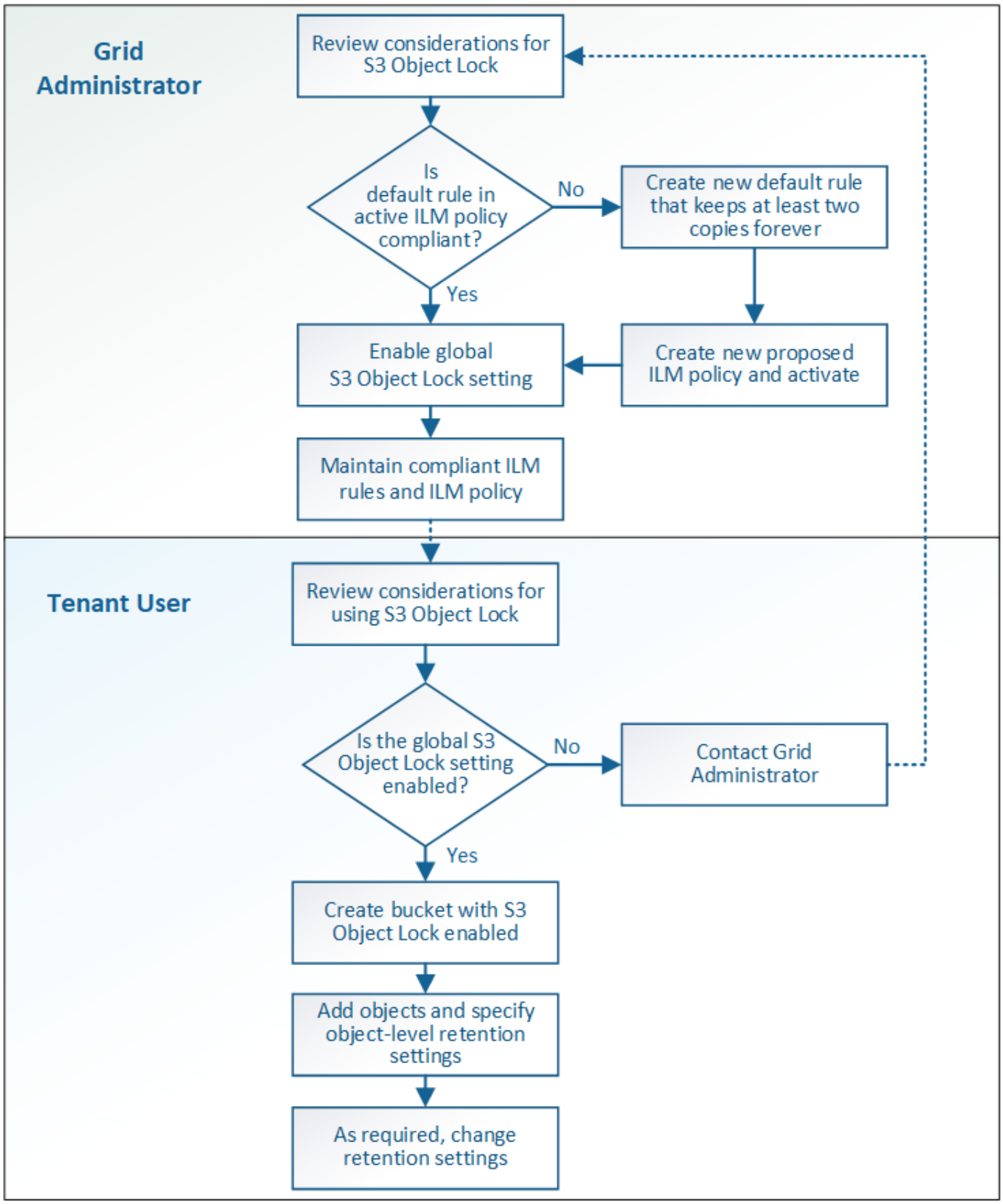
	S3 对象锁定（新增）	合规性（原有）
如何全局启用此功能？	在网格管理器中，选择 * 配置 * > * 系统 * > * S3 对象锁定 * 。	不再支持。 • 注意： * 如果您使用早期版本的 StorageGRID 启用了全局合规性设置，则在 StorageGRID 11.6 中将启用 S3 对象锁定设置。您可以继续使用 StorageGRID 管理现有合规存储分段的设置；但是，您无法创建新的合规存储分段。
如何为存储分段启用此功能？	在使用租户管理器，租户管理 API 或 S3 REST API 创建新存储分段时，用户必须启用 S3 对象锁定。	用户无法再在启用了合规性的情况下创建新的存储分段；但是，他们可以继续向现有合规存储分段添加新对象。
是否支持存储分版本控制？	是的。需要分段版本控制，并且在为分段启用 S3 对象锁定时会自动启用分段版本控制。	否原有的合规性功能不允许分段版本控制。
如何设置对象保留？	用户可以为每个对象版本设置保留截止日期。	用户必须为整个存储分段设置一个保留期限。保留期限适用场景 存储分段中的所有对象。
存储分段是否具有保留和合法保留的默认设置？	是的。启用了 S3 对象锁定的 StorageGRID 存储分段可以具有一个默认保留期限，此保留期限将应用于在载入期间未指定其自己保留设置的对象版本。	是的。

	S3 对象锁定（新增）	合规性（原有）
是否可以更改保留期限？	对象版本的保留日期可以增加，但不能减少。	存储分段的保留期限可以增加，但不能缩短。
合法保留在何处？	用户可以对存储分段中的任何对象版本进行合法保留或取消合法保留。	合法保留放置在存储分段上，并影响存储分段中的所有对象。
何时可以删除对象？	如果对象未处于合法保留状态，则可以在达到保留截止日期后删除该对象版本。	可以在保留期限到期后删除对象，前提是存储分段未处于合法保留状态。可以自动或手动删除对象。
是否支持存储分段生命周期配置？	是的。	否

S3 对象锁定的工作流

作为网格管理员，您必须与租户用户密切协调，以确保对象受到保护，并满足其保留要求。

工作流图显示了使用 S3 对象锁定的高级步骤。这些步骤由网格管理员和租户用户执行。



网格管理任务

如工作流图所示，网格管理员必须执行两项高级任务， S3 租户用户才能使用 S3 对象锁定：

1. 至少创建一个合规的 ILM 规则，并将该规则设置为活动 ILM 策略中的默认规则。

2. 为整个 StorageGRID 系统启用全局 S3 对象锁定设置。

租户用户任务

启用全局 S3 对象锁定设置后，租户可以执行以下任务：

1. 创建已启用 S3 对象锁定的分段。
2. 指定存储分段的默认保留设置，这些设置将应用于添加到存储分段中但未指定其自身保留设置的对象。
3. 向这些存储分段添加对象，并指定对象级别的保留期限和合法保留设置。
4. 根据需要更新单个对象的保留期限或更改合法保留设置。

相关信息

- 使用租户帐户
- 使用 S3
- 使用 S3 对象锁定默认存储分段保留

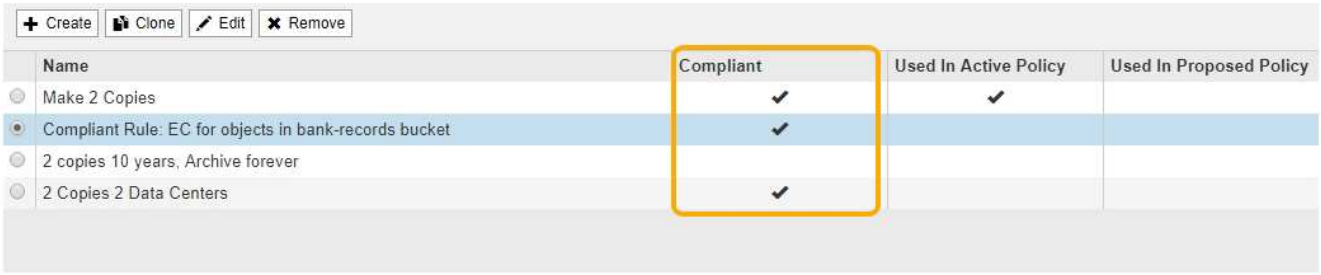
S3 对象锁定的要求

您必须查看启用全局 S3 对象锁定设置的要求，创建合规 ILM 规则和 ILM 策略的要求以及 StorageGRID 对使用 S3 对象锁定的分段和对象所施加的限制。

使用全局 **S3** 对象锁定设置的要求

- 您必须先使用网格管理器或网格管理 API 启用全局 S3 对象锁定设置，然后任何 S3 租户才能创建启用了 S3 对象锁定的分段。
- 启用全局 S3 对象锁定设置后，所有 S3 租户帐户都可以在启用了 S3 对象锁定的情况下创建存储分段。
- 启用全局 S3 对象锁定设置后，您将无法禁用此设置。
- 除非活动 ILM 策略中的默认规则为 *compliant* （即，默认规则必须符合启用了 S3 对象锁定的分段的要求），否则无法启用全局 S3 对象锁定。
- 启用全局 S3 对象锁定设置后，除非策略中的默认规则合规，否则您无法创建新的建议 ILM 策略或激活现有建议的 ILM 策略。启用全局 S3 对象锁定设置后， "ILM 规则 " 和 "ILM 策略 " 页面将指示符合哪些 ILM 规则。

  在以下示例中， "ILM 规则 " 页面列出了与启用了 S3 对象锁定的存储分段兼容的三个规则。

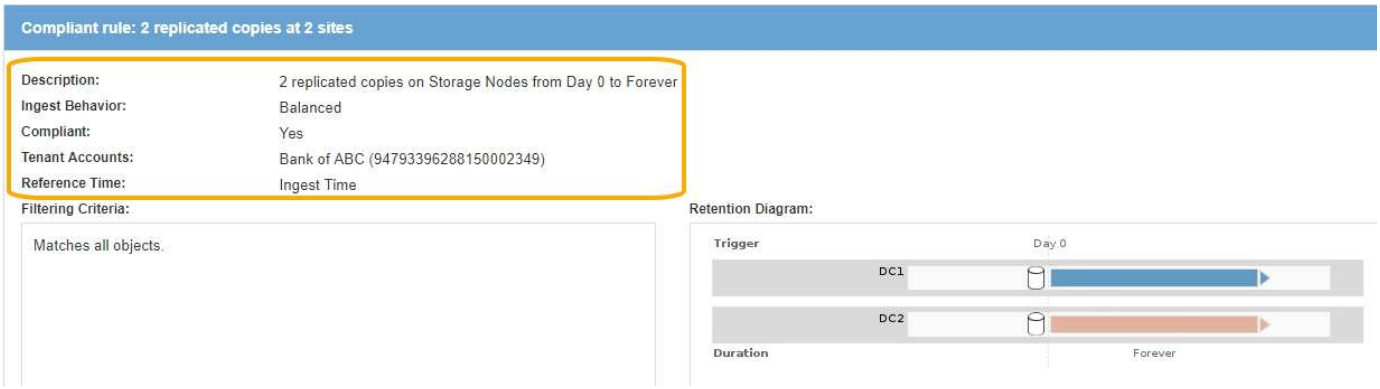


符合 **ILM** 规则的要求

如果要启用全局 S3 对象锁定设置，必须确保活动 ILM 策略中的默认规则合规。合规规则可满足启用了 S3 对象锁定的两个存储分段以及启用了旧合规性的任何现有存储分段的要求：

- 它必须至少创建两个复制的对象副本或一个经过纠删编码的副本。
- 这些副本必须在放置说明中每行的整个持续时间内存在于存储节点上。
- 对象副本无法保存在云存储池中。
- 无法将对象副本保存在归档节点上。
- 放置说明中至少有一行必须从第 0 天开始，并使用 * 载入时间 * 作为参考时间。
- 放置说明中至少一行必须为 "`forever 。` "

例如，此规则满足启用了 S3 对象锁定的分段的要求。它会存储从载入时间（第 0 天）到 "`Forever " 的两个复制对象副本。` 这些对象将存储在两个数据中心的存储节点上。



活动的和建议的 **ILM** 策略的要求

启用全局 S3 对象锁定设置后，活动和建议的 ILM 策略可以同时包含合规和不合规的规则。

- 活动 ILM 策略或任何建议 ILM 策略中的默认规则必须合规。
- 不合规规则仅适用于未启用 S3 对象锁定或未启用原有合规功能的分段中的对象。

- 合规规则可以应用于任何存储分段中的对象；不需要为此存储分段启用 S3 对象锁定或原有合规性。

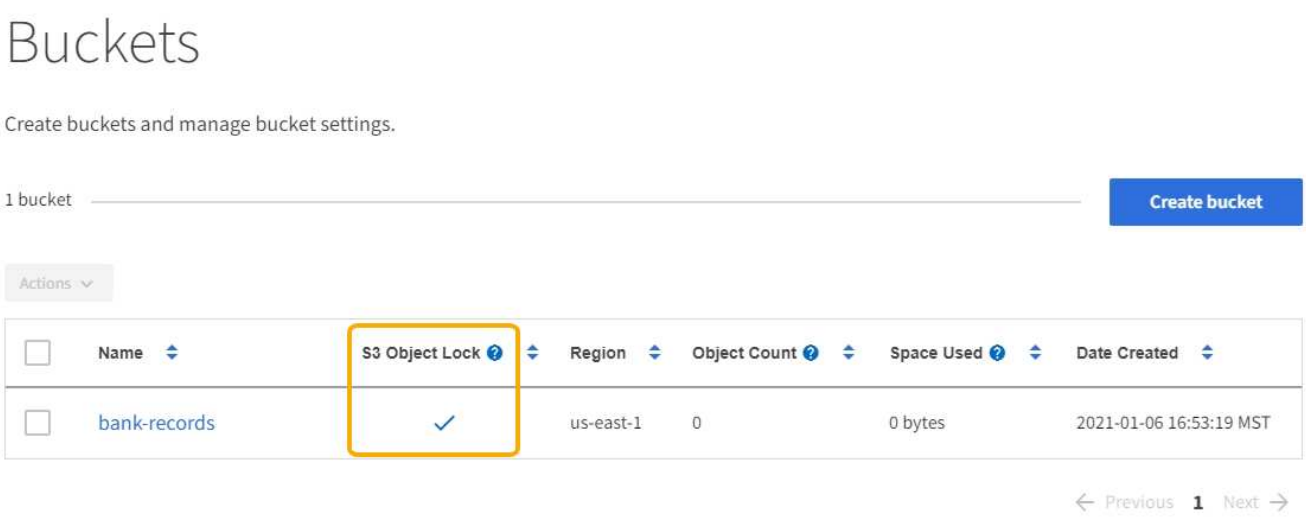
合规的 ILM 策略可能包括以下三个规则：

1. 一种在启用了 S3 对象锁定的情况下为特定分段中的对象创建经过擦除编码的副本的合规规则。EC 副本从第 0 天一直存储在存储节点上。
2. 一种不合规的规则，在存储节点上创建两个复制的对象副本一年，然后将一个对象副本移动到归档节点并永久存储该副本。此规则仅适用于未启用 S3 对象锁定或原有合规性的适用场景 分段，因为它仅永久存储一个对象副本，并且使用归档节点。
3. 一种默认的合规规则，用于在存储节点上创建从 0 天到永久的两个复制对象副本。此规则适用场景 任何分段中未被前两个规则筛选出的任何对象。

启用了 **S3** 对象锁定的存储分段的要求

- 如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以使用租户管理器，租户管理 API 或 S3 REST API 创建启用了 S3 对象锁定的分段。

  此租户管理器示例显示了一个已启用 S3 对象锁定的存储分段。



- 如果您计划使用 S3 对象锁定，则必须在创建存储分段时启用 S3 对象锁定。您不能为现有存储分段启用 S3 对象锁定。
- S3 对象锁定需要分段版本。为存储分段启用 S3 对象锁定后， StorageGRID 会自动为该存储分段启用版本控制。
- 在启用了 S3 对象锁定的情况下创建存储分段后，无法禁用 S3 对象锁定或暂停该存储分段的版本控制。
- 您也可以为存储分段配置默认保留。上传对象版本时，默认保留将应用于对象版本。您可以通过在上传对象版本的请求中指定保留模式和保留至日期来覆盖存储分段默认值。
- S3 对象生命周期分段支持分段生命周期配置。
- 启用了 S3 对象锁定的存储分段不支持 CloudMirror 复制。

启用了 **S3** 对象锁定的分段中的对象的要求

- 要保护对象版本， S3 客户端应用程序必须配置存储分段默认保留，或者在每个上传请求中指定保留设置。
- 您可以增加对象版本的保留截止日期，但不能减小此值。

- 如果您收到有关待定法律诉讼或监管调查的通知，则可以通过对对象版本进行法律保留来保留相关信息。如果对象版本处于合法保留状态，则无法从 StorageGRID 中删除该对象，即使该对象已达到保留日期。一旦取消合法保留，如果已达到保留日期，则可以删除对象版本。
- S3 对象锁定需要使用版本控制的分段。保留设置适用于各个对象版本。对象版本可以同时具有保留截止日期和合法保留设置，但不能具有其他设置，或者两者均不具有。为对象指定保留日期或合法保留设置仅保护请求中指定的版本。您可以创建新版本的对象，而先前版本的对象仍保持锁定状态。

启用了 S3 对象锁定的存储分段中的对象生命周期

保存在启用了 S3 对象锁定的存储分段中的每个对象将经历三个阶段：

1. * 对象载入 *
   - 在启用了 S3 对象锁定的情况下向存储分段添加对象版本时， S3 客户端应用程序可以使用默认存储分段保留设置，也可以指定对象的保留设置（保留至日期，合法保留或两者）。然后， StorageGRID 会为此对象生成元数据，其中包括唯一对象标识符（ UUID ）以及载入日期和时间。
   - 载入具有保留设置的对象版本后，将无法修改其数据和 S3 用户定义的元数据。
   - StorageGRID 存储的对象元数据与对象数据无关。它会为每个站点上的所有对象元数据维护三个副本。
2. * 对象保留 *
   - StorageGRID 会存储该对象的多个副本。副本的确切数量和类型以及存储位置取决于活动 ILM 策略中的合规规则。
3. * 对象删除 *
   - 达到保留截止日期后，可以删除对象。
   - 无法删除处于合法保留状态的对象。

相关信息

- 使用租户帐户
- 使用 S3
- 比较 S3 对象锁定与原有合规性
- 示例 7： S3 对象锁定的兼容 ILM 策略
- 查看审核日志
- 使用 S3 对象锁定默认存储分段保留。

全局启用 S3 对象锁定

如果 S3 租户帐户在保存对象数据时需要遵守法规要求，则必须为整个 StorageGRID 系统启用 S3 对象锁定。启用全局 S3 对象锁定设置后，任何 S3 租户用户都可以使用 S3 对象锁定创建和管理存储分段和对象。

您需要的内容

- 您具有 root 访问权限。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您已查看 S3 对象锁定工作流，必须了解注意事项。

- 活动 ILM 策略中的默认规则合规。
  - 创建默认 ILM 规则
  - 创建 ILM 策略

关于此任务

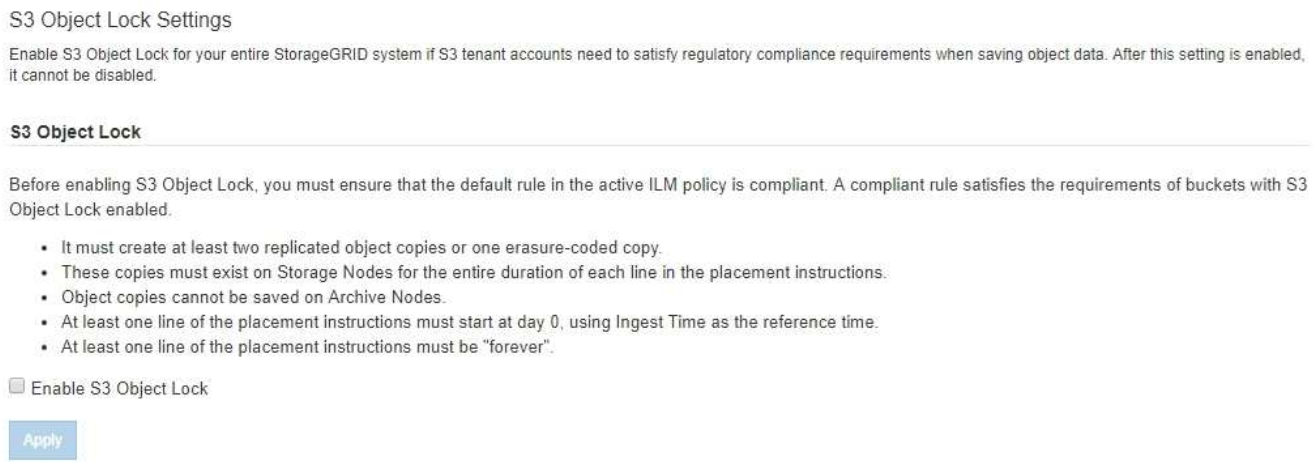
网格管理员必须启用全局 S3 对象锁定设置，以允许租户用户创建启用了 S3 对象锁定的新分段。启用此设置后，便无法将其禁用。

> 如果您使用先前版本的 StorageGRID 启用了全局合规性设置，则 StorageGRID 11.6 中会启用 S3 对象锁定设置。您可以继续使用 StorageGRID 管理现有合规存储分段的设置；但是，您无法创建新的合规存储分段。请参见 "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"。

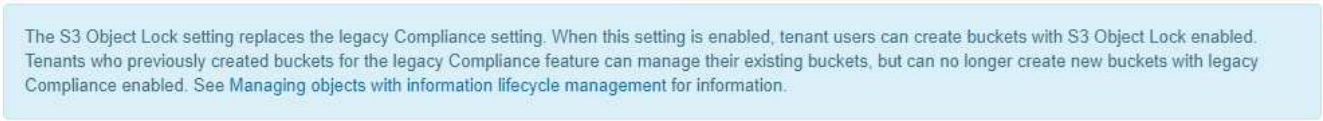
步骤

1. 选择 * 配置 * > * 系统 * > * S3 对象锁定 * 。

   此时将显示 "S3 Object Lock Settings" 页面。

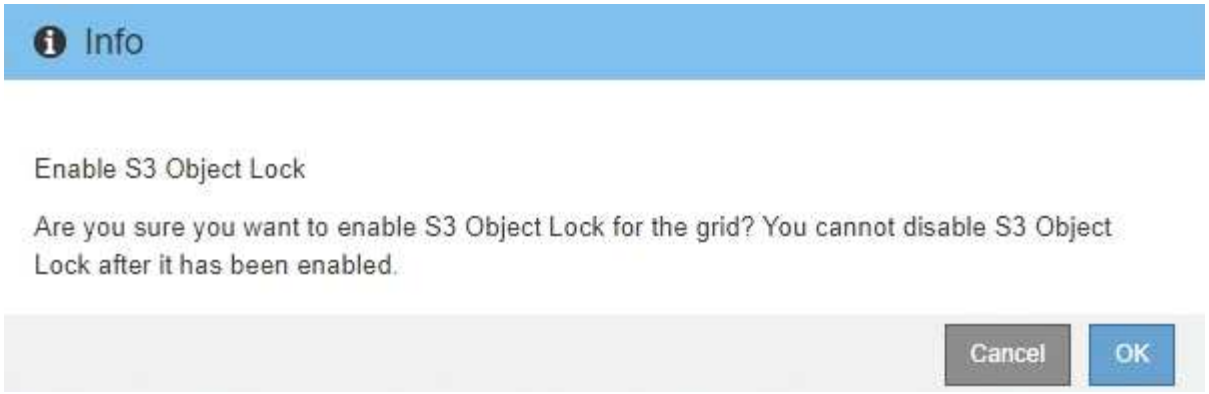


   如果您已使用先前版本的 StorageGRID 启用了全局合规性设置，则此页面将包含以下注意事项：



2. 选择 * 启用 S3 对象锁定 * 。
3. 选择 * 应用 * 。

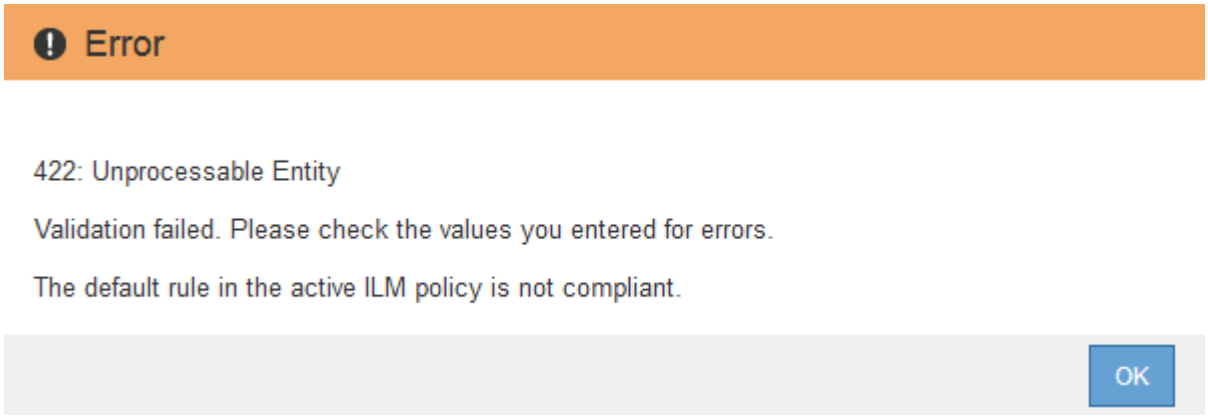
   此时将显示一个确认对话框，提醒您在启用 S3 对象锁定后无法禁用它。



4. 如果确实要为整个系统永久启用 S3 对象锁定，请选择 * 确定 * 。

   选择 * 确定 * 时：

   - 如果活动 ILM 策略中的默认规则合规，则现在将为整个网格启用 S3 对象锁定，并且无法禁用。
   - 如果默认规则不符合要求，则会显示一个错误，指示您必须创建并激活一个新的 ILM 策略，其中包含一个合规规则作为其默认规则。选择 * 确定 * ，然后创建新的建议策略，对其进行模拟并激活。



完成后

启用全局 S3 对象锁定设置后，您可能需要执行此操作 创建默认规则 合规和 创建 ILM 策略 合规。启用此设置后， ILM 策略可以选择同时包含合规的默认规则和不合规的默认规则。例如，您可能希望使用一个不合规规则，该规则不会筛选未启用 S3 对象锁定的分段中的对象。

相关信息

- 比较 S3 对象锁定与原有合规性

解决更新 **S3** 对象锁定或原有合规性配置时出现的一致性错误

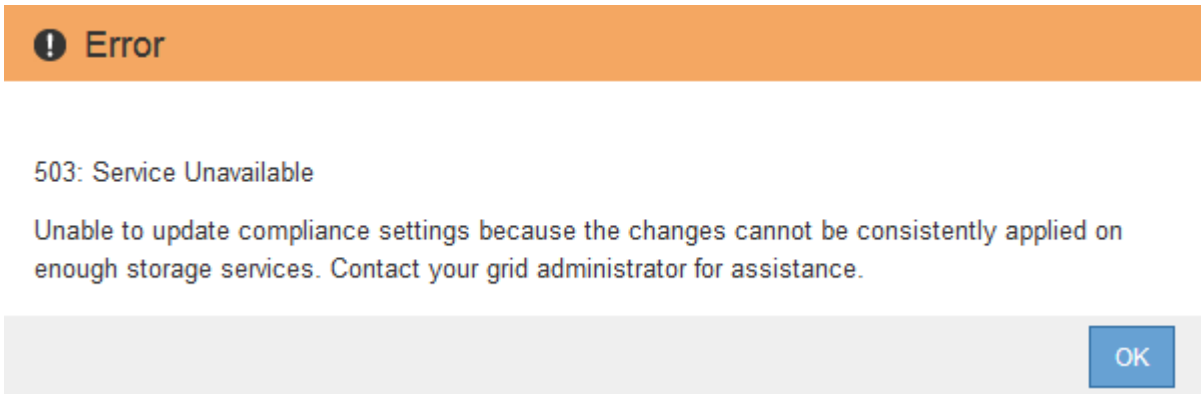
如果一个站点上的一个数据中心站点或多个存储节点不可用，您可能需要帮助 S3 租户用户对 S3 对象锁定或原有合规性配置进行更改。

启用了 S3 对象锁定（或原有合规性）的存储分段的租户用户可以更改某些设置。例如，使用 S3 对象锁定的租户用户可能需要将对象版本置于合法保留状态。

当租户用户更新 S3 存储分段或对象版本的设置时， StorageGRID 会尝试立即更新整个网格中的存储分段或对象元数据。如果系统由于数据中心站点或多个存储节点不可用而无法更新元数据，则会显示一条错误消息。具体

而言：

- 租户管理器用户会看到以下错误消息：



- 租户管理 API 用户和 S3 API 用户收到响应代码 `503 Service unavailable` 并显示类似的消息文本。

要解决此错误，请执行以下步骤：

1. 尝试尽快使所有存储节点或站点重新可用。
2. 如果您无法在每个站点提供足够的存储节点，请联系技术支持，他们可以帮助您恢复节点并确保在网格中一致地应用更改。
3. 解决底层问题描述 后，提醒租户用户重试其配置更改。

相关信息

- 使用租户帐户
- 使用 S3
- 恢复和维护

ILM 规则和策略示例

示例 **1** ： 对象存储的 **ILM** 规则和策略

在定义 ILM 策略以满足对象保护和保留要求时，您可以使用以下示例规则和策略作为起点。

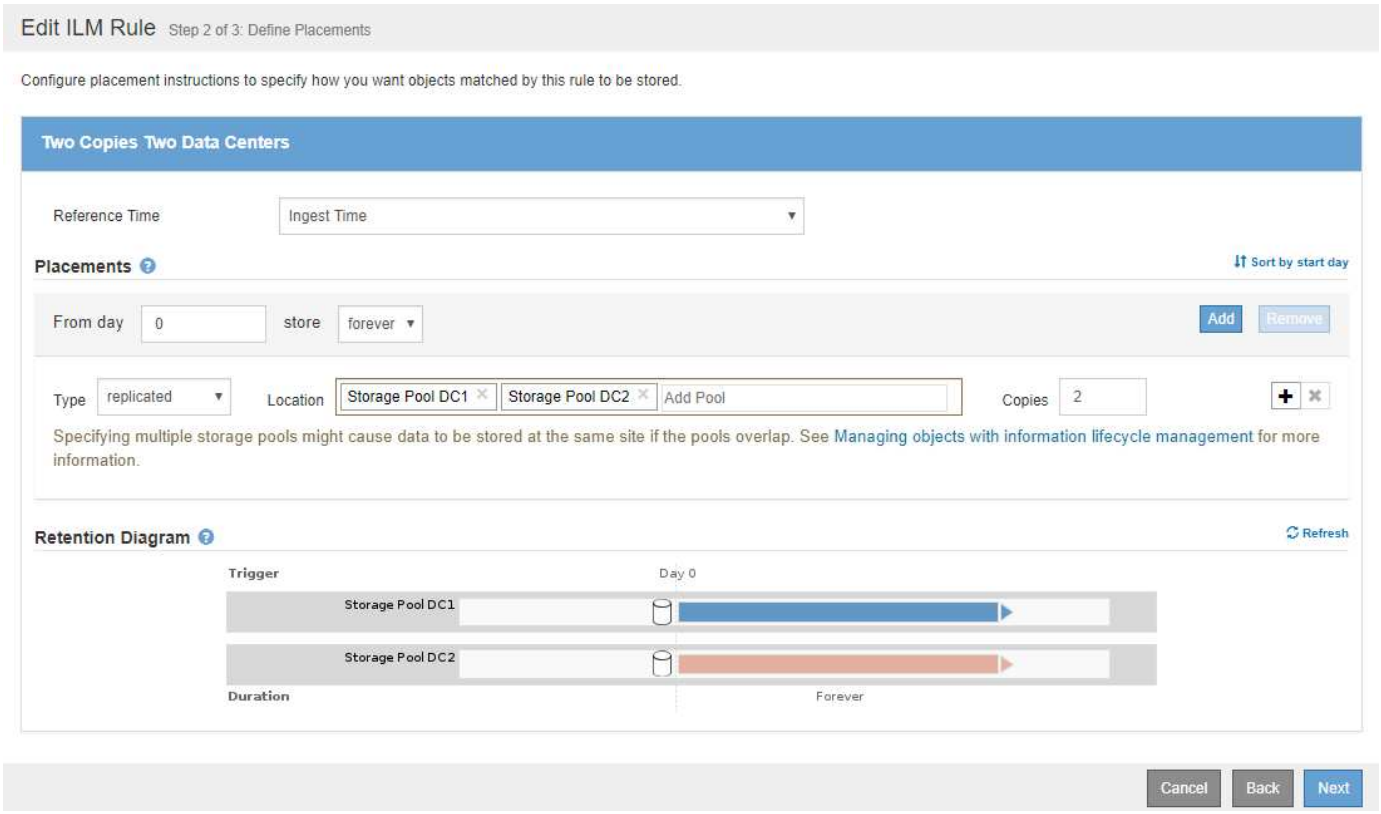
> 以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

ILM 规则 **1** 示例 **1** ： 将对象数据复制到两个数据中心

此示例 ILM 规则会将对象数据复制到两个数据中心中的存储池。

规则定义	示例值
存储池	两个存储池，分别位于不同的数据中心，分别名为存储池 DC1 和存储池 DC2 。

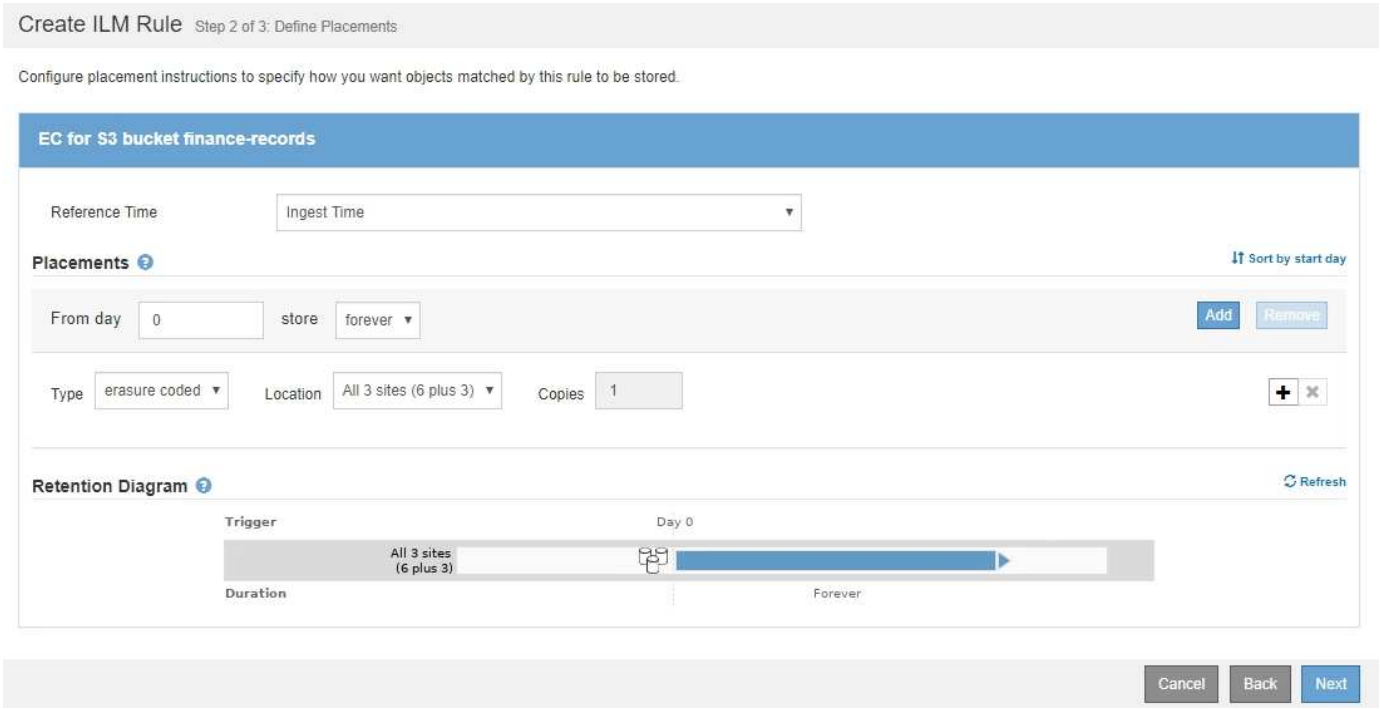
规则定义	示例值
规则名称	两个副本两个数据中心
参考时间	载入时间
内容放置	在第 0 天，永久保留两个复制副本—一个在存储池 DC1 中，一个在存储池 DC2 中。



ILM 规则 **2** 示例 **1**： 使用存储分段匹配的纠删编码配置文件

此示例 ILM 规则使用擦除编码配置文件和 S3 存储分段来确定对象的存储位置和存储时间。

规则定义	示例值
纠删编码配置文件	• 在三个数据中心（全部 3 个站点）之间配置一个存储池 • 使用 6+3 纠删编码方案
规则名称	用于 S3 存储分段财务记录的 EC
参考时间	载入时间
内容放置	对于名为 finance-records 的 S3 存储分段中的对象，请在 Erasure Coding 配置文件指定的池中创建一个经过纠删编码的副本。请永久保留此副本。

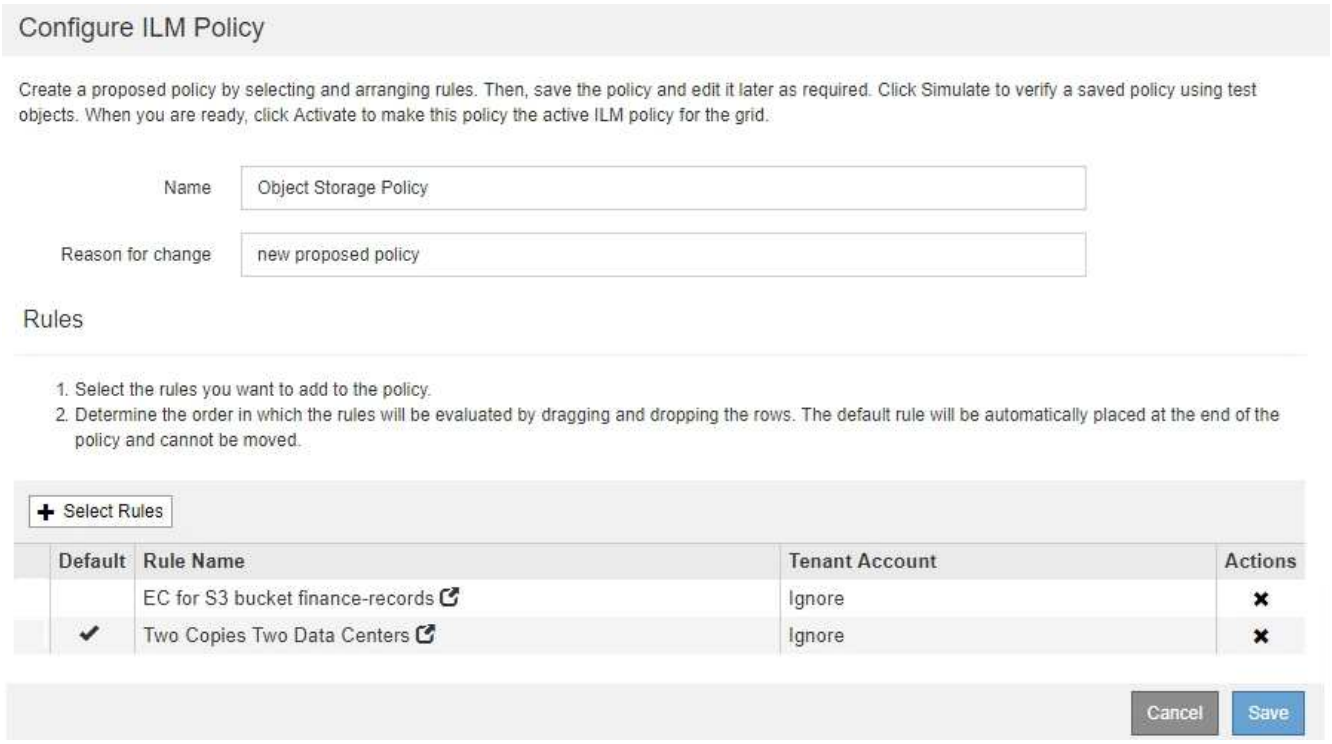


ILM 策略示例 1

您可以通过 StorageGRID 系统设计复杂而复杂的 ILM 策略；但实际上，大多数 ILM 策略都很简单。

多站点拓扑的典型 ILM 策略可能包括以下 ILM 规则：

- 在载入时，使用 6+3 纠删编码将属于名为 `finance-records` 的 S3 存储分段的所有对象存储在三个数据中心中。
- 如果某个对象与第一个 ILM 规则不匹配，请使用该策略的默认 ILM 规则 " 复制两个数据中心 " ，以便将该对象的副本存储在两个数据中心 DC1 和 DC2 中。



示例 2： 用于 EC 对象大小筛选的 ILM 规则和策略

您可以使用以下示例规则和策略作为起点来定义一个 ILM 策略，该策略按对象大小进行筛选以满足建议的 EC 要求。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

ILM 规则 **1** 示例 **2**： 对大于 **1 MB** 的对象使用 **EC**

此示例中的 ILM 规则擦除将对大于 1 MB 的对象进行编码。

纠删编码最适合大于 1 MB 的对象。请勿对小于 200 KB 的对象使用纠删编码，以避免管理极小的纠删编码片段所产生的开销。

规则定义	示例值
规则名称	仅 EC 对象 >1 MB
参考时间	载入时间
对对象大小进行高级筛选	对象大小（ MB ）大于 1
内容放置	使用三个站点创建 2+1 纠删编码副本

ILM 规则 **2** 示例 **2**： 两个复制副本

此示例 ILM 规则将创建两个复制副本，而不按对象大小进行筛选。此规则是策略的默认规则。由于第一个规则会筛选出大于 1 MB 的所有对象，因此此规则仅筛选 1 MB 或更小的适用场景 对象。

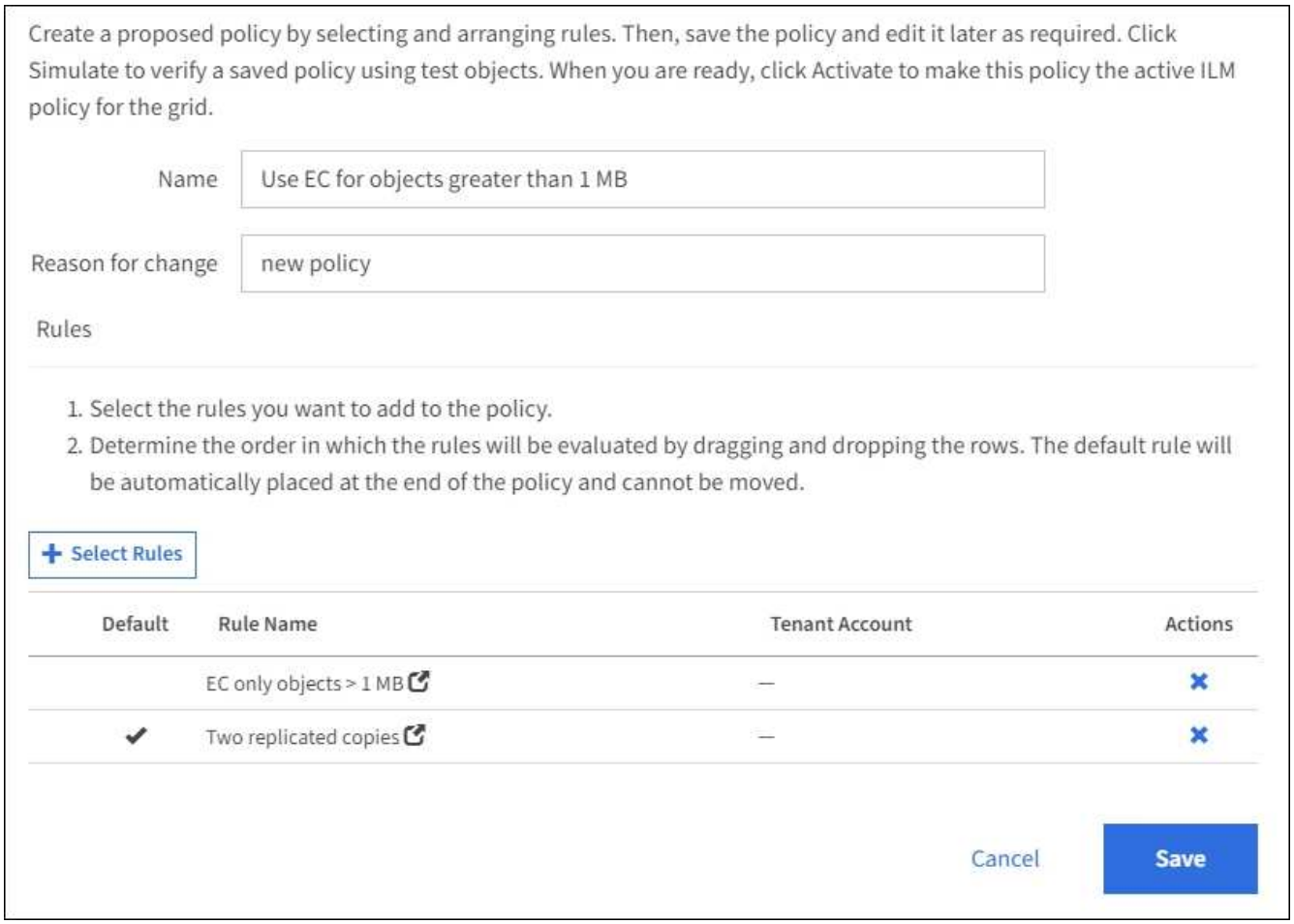
规则定义	示例值
规则名称	两个复制副本
参考时间	载入时间
对对象大小进行高级筛选	无

规则定义	示例值
内容放置	创建两个复制副本并将其保存在两个数据中心 DC1 和 DC2 上

示例 **2** 中的 **ILM** 策略：对大于 **1 MB** 的对象使用 **EC**

此示例 ILM 策略包括两个 ILM 规则：

- 第一个规则擦除将对大于 1 MB 的所有对象进行编码。
- 第二个（默认） ILM 规则会创建两个复制副本。由于规则 1 已筛选出大于 1 MB 的对象，因此规则 2 仅筛选 1 MB 或更小的适用场景 对象。



示例 **3**： 用于更好地保护映像文件的 **ILM** 规则和策略

您可以使用以下示例规则和策略来确保对大于 1 MB 的映像进行纠删编码，并使用较小的映像创建两个副本。

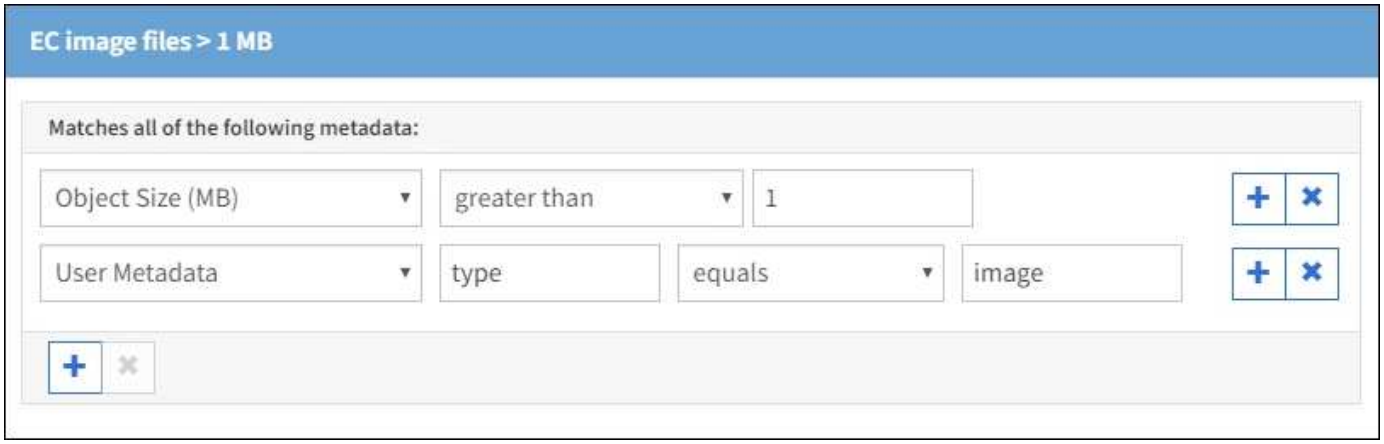
以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

ILM 规则 1 ，例如 3 ： 对大于 1 MB 的映像文件使用 EC

此示例 ILM 规则使用高级筛选功能对大于 1 MB 的所有映像文件进行擦除代码。

> 纠删编码最适合大于 1 MB 的对象。请勿对小于 200 KB 的对象使用纠删编码，以避免管理极小的纠删编码片段所产生的开销。

规则定义	示例值
规则名称	EC 映像文件 > 1 MB
参考时间	载入时间
对对象大小进行高级筛选	对象大小（ MB ）大于 1.0
用户元数据的高级筛选	用户元数据类型等于映像
内容放置	使用三个站点创建 2+1 纠删编码副本



由于此规则已配置为策略中的第一条规则，因此纠删编码放置指令仅会对大于 1 MB 的适用场景 映像执行。

ILM 规则 2 示例 3 ： 为其余所有映像文件创建 2 个复制副本

此示例 ILM 规则使用高级筛选来指定复制较小的映像文件。由于策略中的第一个规则已与大于 1 MB 的映像文件匹配，因此此规则会对 1 MB 或更小的适用场景 映像文件进行匹配。

规则定义	示例值
规则名称	2 个映像文件副本
参考时间	载入时间
用户元数据的高级筛选	用户元数据类型等于映像文件
内容放置	在两个存储池中创建 2 个复制副本

示例 3 中的 ILM 策略：更好地保护映像文件

此示例 ILM 策略包括三个规则：

- 第一个规则擦除会对大于 1 MB 的所有映像文件进行编码。
- 第二条规则会为任何剩余映像文件（即 1 MB 或更小的映像）创建两个副本。
- 默认规则适用场景 所有剩余对象（即任何非映像文件）。

示例 4： S3 版本对象的 ILM 规则和策略

如果您的 S3 存储分段已启用版本控制，则可以通过在 ILM 策略中包含使用 * 非当前时间 * 作为参考时间的规则来管理非当前对象版本。

如本示例所示，您可以通过对非当前对象版本使用不同的放置说明来控制受版本控制的对象使用的存储量。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

如果要创建 ILM 策略来管理非当前对象版本，请注意，要模拟此策略，您必须知道对象版本的 UUID 或 CBID 。要查找对象的 UUID 和 CBID ，请在对象仍为最新状态时使用对象元数据查找。请参见 使用对象元数据查找验证 ILM 策略。

相关信息

- 如何删除对象

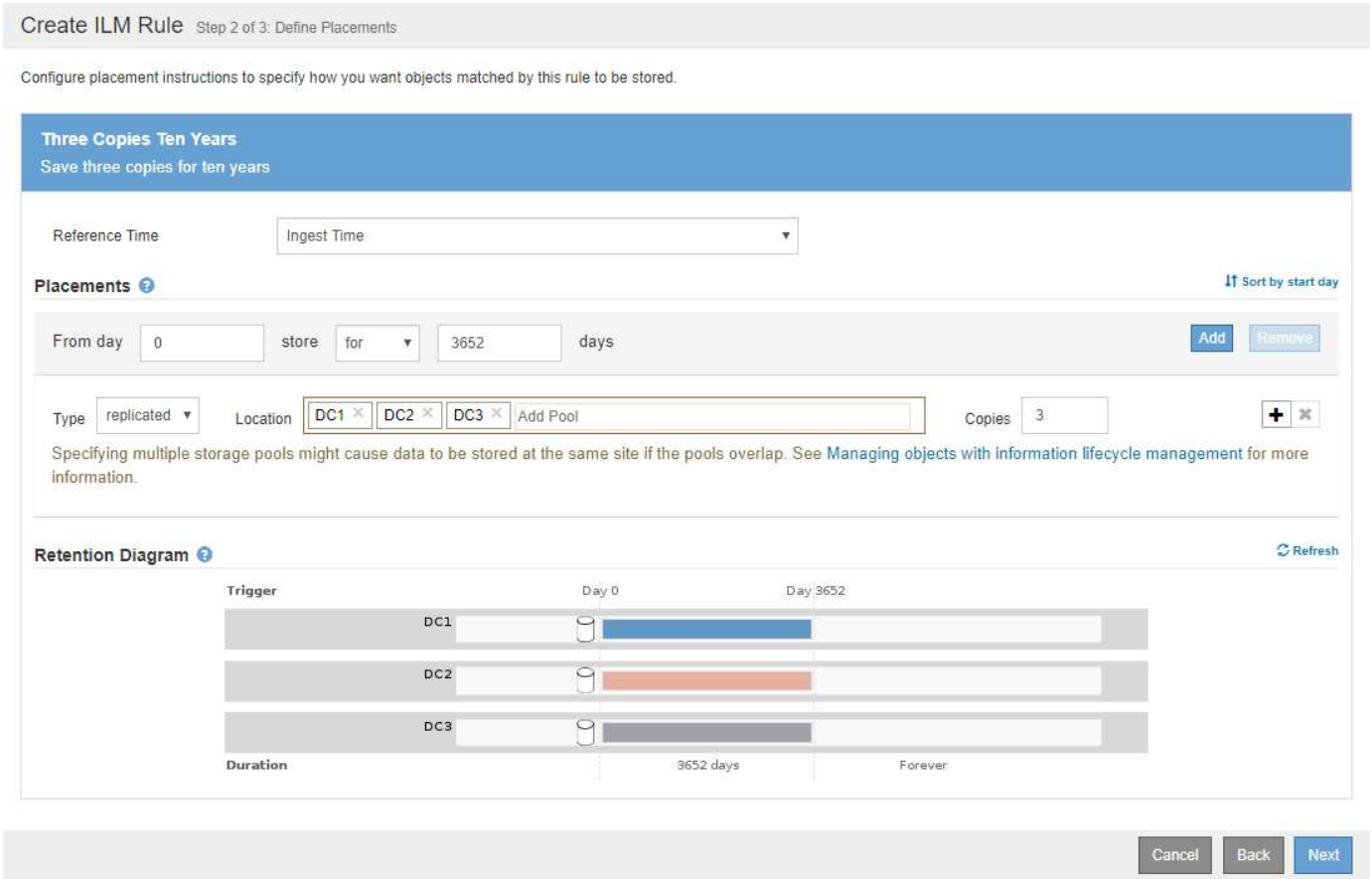
ILM 规则 1 示例 4： 保存三个副本 10 年

此示例 ILM 规则会将每个对象的一个副本存储在三个数据中心，持续 10 年。

此规则将适用场景 所有对象，无论它们是否已受版本控制。

规则定义	示例值
存储池	三个存储池，分别位于不同的数据中心，分别名为 DC1 ， DC2 和 DC3 。
规则名称	三个副本十年

规则定义	示例值
参考时间	载入时间
内容放置	在第 0 天，保留三个复制副本 10 年（ 3 ， 652 天），一个在 DC1 ，一个在 DC2 ，一个在 DC3 。10 年后，删除对象的所有副本。



ILM 规则 **2** 示例 **4**： 将两个非最新版本副本保存 **2** 年

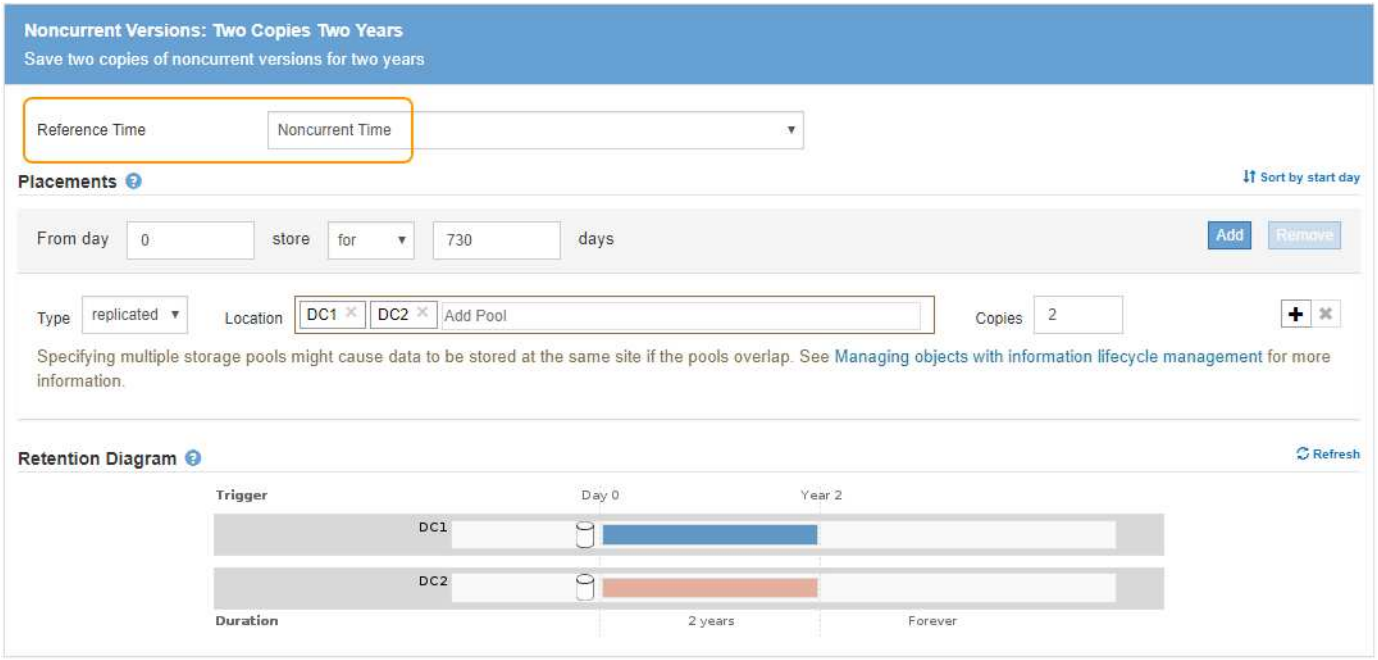
此示例 ILM 规则会将 S3 版本对象的两个非最新版本副本存储 2 年。

由于 ILM 规则 1 会对对象的所有版本进行适用场景 处理，因此您必须创建另一个规则来筛选出任何非最新版本。此规则对参考时间使用 * 非当前时间 * 选项。

在此示例中，仅存储两个非最新版本副本，这些副本将存储两年。

规则定义	示例值
存储池	两个存储池，分别位于不同的数据中心，分别名为 DC1 和 DC2 。
规则名称	非最新版本：两个副本，两年
参考时间	非当前时间

规则定义	示例值
内容放置	在相对于非当前时间（即从对象版本成为非当前版本之日开始）的第 0 天，将两个非当前对象版本的复制副本保留 2 年（ 730 天），一个在 DC1 中，一个在 DC2 中。2 年后，删除非最新版本。



ILM 策略示例 **4**： **S3** 版本对象

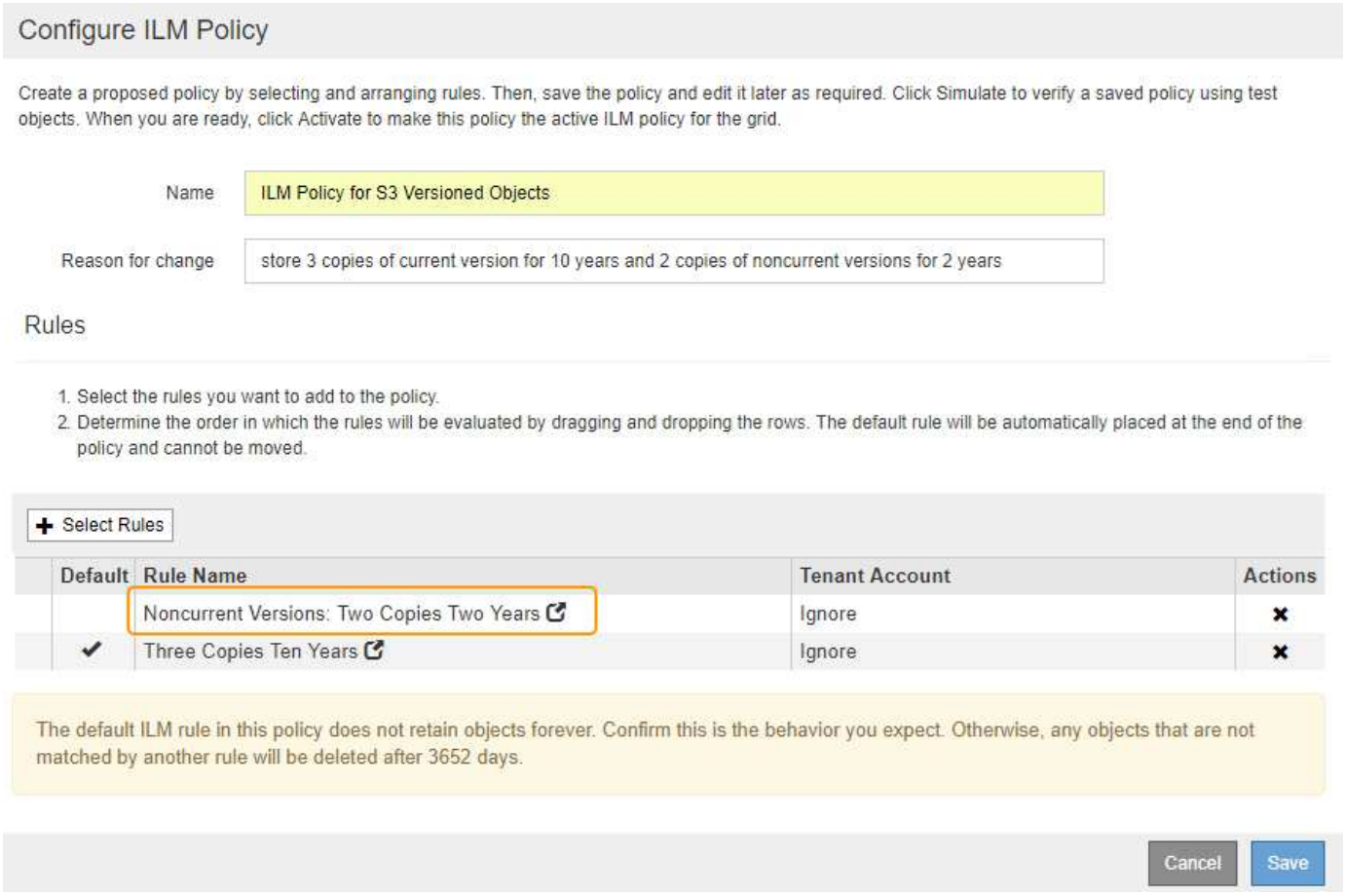
如果要以与当前版本不同的方式管理对象的旧版本，则使用 * 非当前时间 * 作为参考时间的规则必须先显示在 ILM 策略中，然后再显示适用于当前对象版本的规则。

S3 版本对象的 ILM 策略可能包括以下 ILM 规则：

- 从每个对象的任何较旧（非最新）版本变为非最新版本之日起，保留两年。

> 在应用于当前对象版本的规则之前，非当前时间规则必须显示在策略中。否则，非当前对象版本将永远不会与非当前时间规则匹配。

- 载入时，创建三个复制副本，并在三个数据中心中的每个数据中心存储一个副本。将当前对象版本的副本保留 10 年。



模拟此示例策略时，您希望按如下所示评估测试对象：

- 第一个规则将匹配任何非最新的对象版本。如果非当前对象版本超过 2 年，则 ILM 会将其永久删除（非当前版本的所有副本都会从网格中删除）。

> 要模拟非当前对象版本，必须使用该版本的 UUID 或 CBID 。虽然对象仍为最新对象，但您可以使用对象元数据查找来查找其 UUID 和 CBID 。

- 当前对象版本将与第二个规则匹配。当前对象版本存储 10 年后， ILM 过程会添加一个删除标记作为对象的当前版本，并使先前的对象版本 "`` noncurrent." 下次进行 ILM 评估时，此非最新版本将与第一个规则匹配。因此， DC3 上的副本将被清除， DC1 和 DC2 上的两个副本将再存储 2 年。

示例 **5** ： 用于严格载入行为的 **ILM** 规则和策略

您可以在规则中使用位置筛选器和严格的载入行为来防止对象保存在特定数据中心位置。

在本示例中，基于巴黎的租户出于监管方面的考虑，不希望在欧盟以外存储某些对象。其他对象，包括来自其他租户帐户的所有对象，可以存储在巴黎数据中心或美国数据中心。

> 以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

相关信息

- 用于载入的数据保护选项

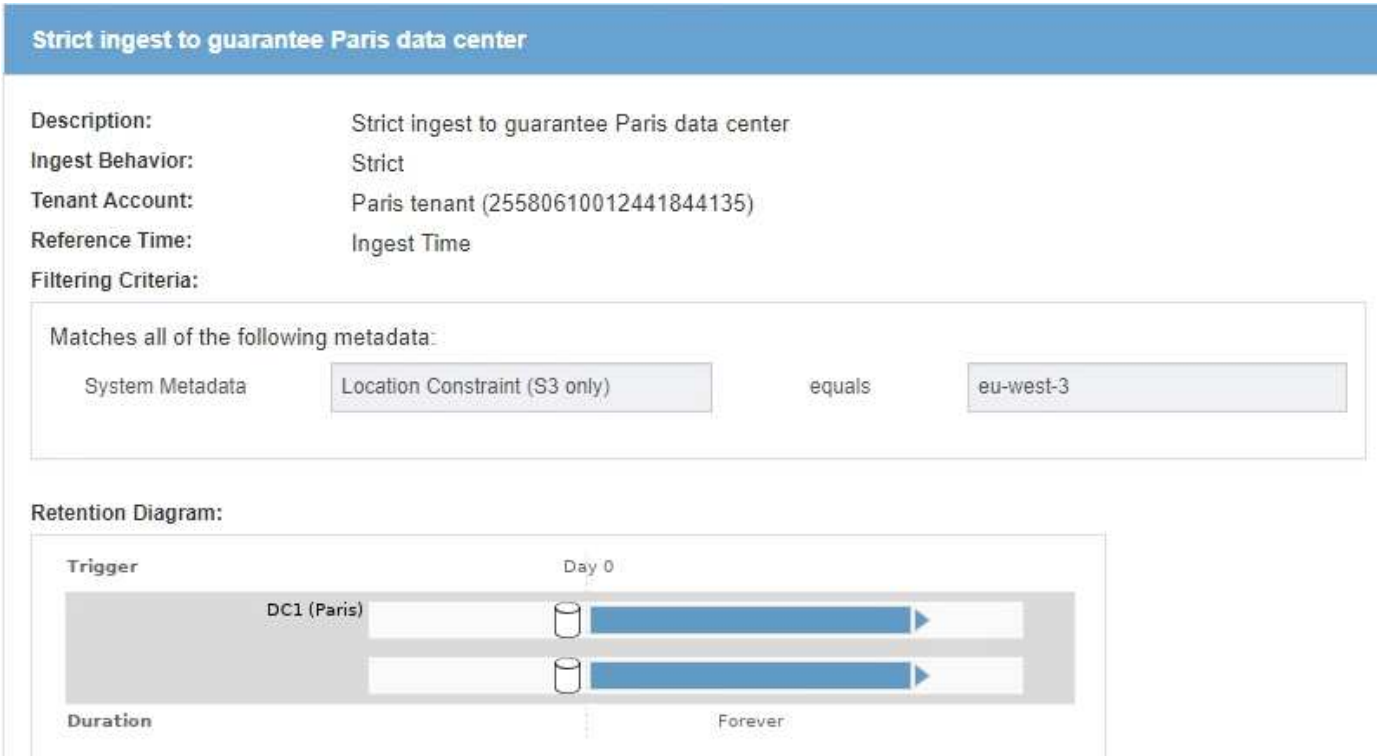
- 第 3 步，共 3 步：定义载入行为

ILM 规则 **1** 示例 **5**： 严格载入以保证巴黎数据中心

此示例 ILM 规则使用严格的载入行为来保证，在将区域设置为 EU-west-3 区域（巴黎）的情况下，基于巴黎的租户保存到 S3 分段的对象永远不会存储在美国数据中心。

此规则属于巴黎租户且 S3 分段区域设置为 EU-west-3 （巴黎）的适用场景 对象。

规则定义	示例值
租户帐户	巴黎租户
高级筛选	位置约束等于 EU-west-3
存储池	DC1 （巴黎）
规则名称	严格载入以保证巴黎数据中心的安全
参考时间	载入时间
内容放置	在第 0 天，在 DC1 （巴黎）中永久保留两个复制副本
载入行为	严格。请始终在载入时使用此规则的放置位置。如果无法在巴黎数据中心存储对象的两个副本，则载入将失败。



ILM 规则 **2** 示例 **5**： 平衡其他对象的载入

此示例 ILM 规则使用平衡载入行为为第一个规则不匹配的任何对象提供最佳 ILM 效率。将存储与此规则匹配的所有对象的两个副本—一个在美国数据中心，一个在巴黎数据中心。如果无法立即满足此规则，则会将临时副本存储在任何可用位置。

此规则适用于属于任何租户和任何区域的适用场景 对象。

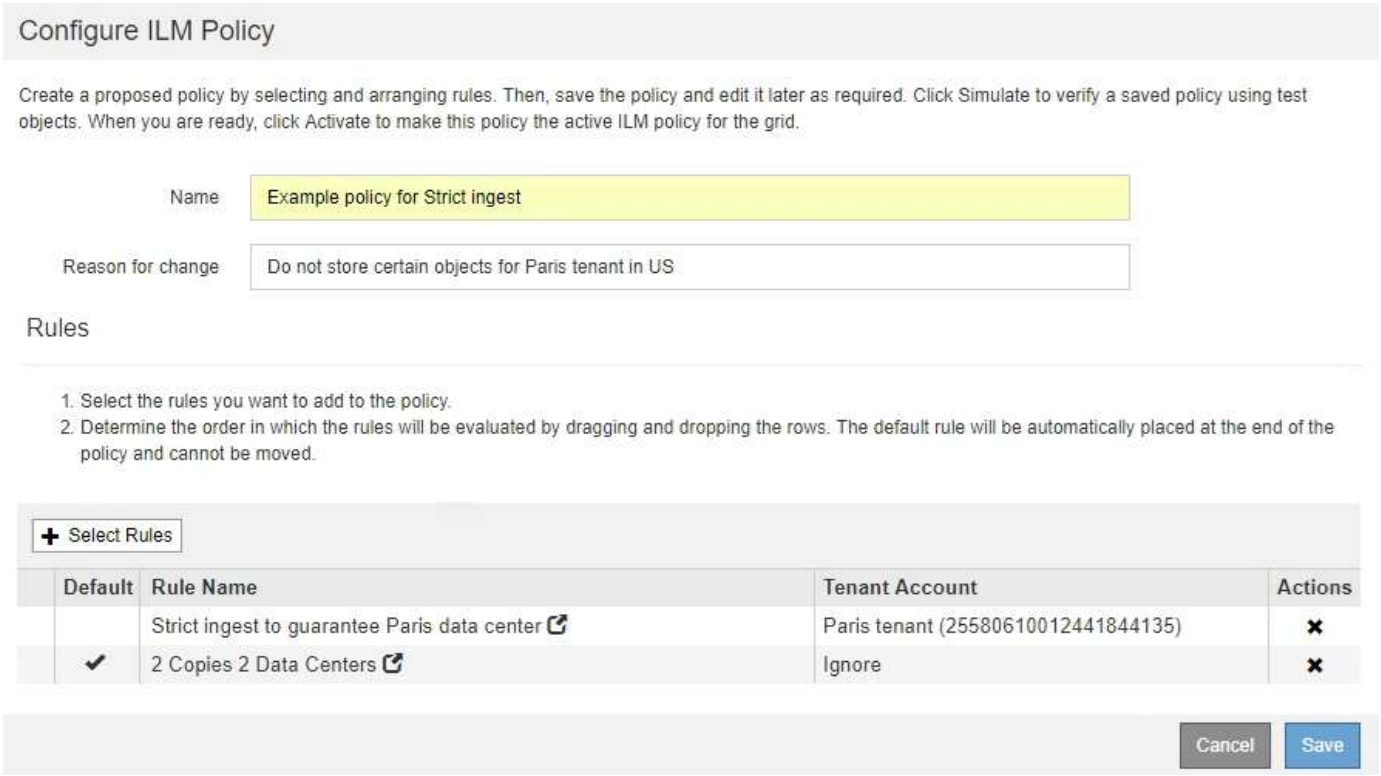
规则定义	示例值
租户帐户	忽略
高级筛选	未指定 _
存储池	DC1 （巴黎）和 DC2 （美国）
规则名称	2 个副本 2 个数据中心
参考时间	载入时间
内容放置	在第 0 天，将两个复制副本永久保留在两个数据中心
载入行为	平衡。如果可能，与此规则匹配的对象将根据规则的放置说明进行放置。否则，会在任何可用位置创建临时副本。

ILM 策略示例 **5** ： 结合载入行为

示例 ILM 策略包括两个具有不同载入行为的规则。

使用两种不同载入行为的 ILM 策略可能包括以下 ILM 规则：

- 仅在巴黎数据中心存储属于 PARIS 租户且 S3 存储分段区域设置为 EU-west-3 （ PARIS ）的对象。如果 PARIS 数据中心不可用，则无法载入。
- 将所有其他对象（包括属于巴黎租户但具有不同分段区域的对象）存储在美国数据中心和巴黎数据中心。如果无法满足放置指令，请在任何可用位置创建临时副本。



模拟示例策略时，您希望按如下所示评估测试对象：

- 属于 PARIS 租户且 S3 存储分段区域设置为 EU-west-3 的任何对象均按第一个规则匹配，并存储在 PARIS 数据中心。由于第一个规则使用严格的载入，因此这些对象永远不会存储在美国数据中心。如果 PARIS 数据中心的存储节点不可用，则载入将失败。
- 所有其他对象均按第二条规则匹配，其中包括属于 PARIS 租户且 S3 分段区域未设置为 EU-west-3 的对象。每个对象的一份副本保存在每个数据中心。但是，由于第二条规则使用平衡载入，因此，如果一个数据中心不可用，则会在任何可用位置保存两个临时副本。

示例 **6** ： 更改 **ILM** 策略

如果需要更改数据保护或添加新站点，您可能需要创建并激活新的 ILM 策略。

在更改策略之前，您必须了解 ILM 放置的更改如何临时影响 StorageGRID 系统的整体性能。

在此示例中，扩展中添加了一个新的 StorageGRID 站点，需要修改活动的 ILM 策略，以便将数据存储在新站点上。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

更改 ILM 策略如何影响性能

激活新的 ILM 策略时， StorageGRID 系统的性能可能会暂时受到影响，尤其是在新策略中的放置说明要求将许多现有对象移动到新位置时。

激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

可能会暂时影响 StorageGRID 性能的 ILM 策略更改类型包括：

- 将不同的擦除编码配置文件应用于现有擦除编码对象。

  StorageGRID 认为每个擦除编码配置文件都是唯一的，使用新配置文件时不会重复使用擦除编码片段。

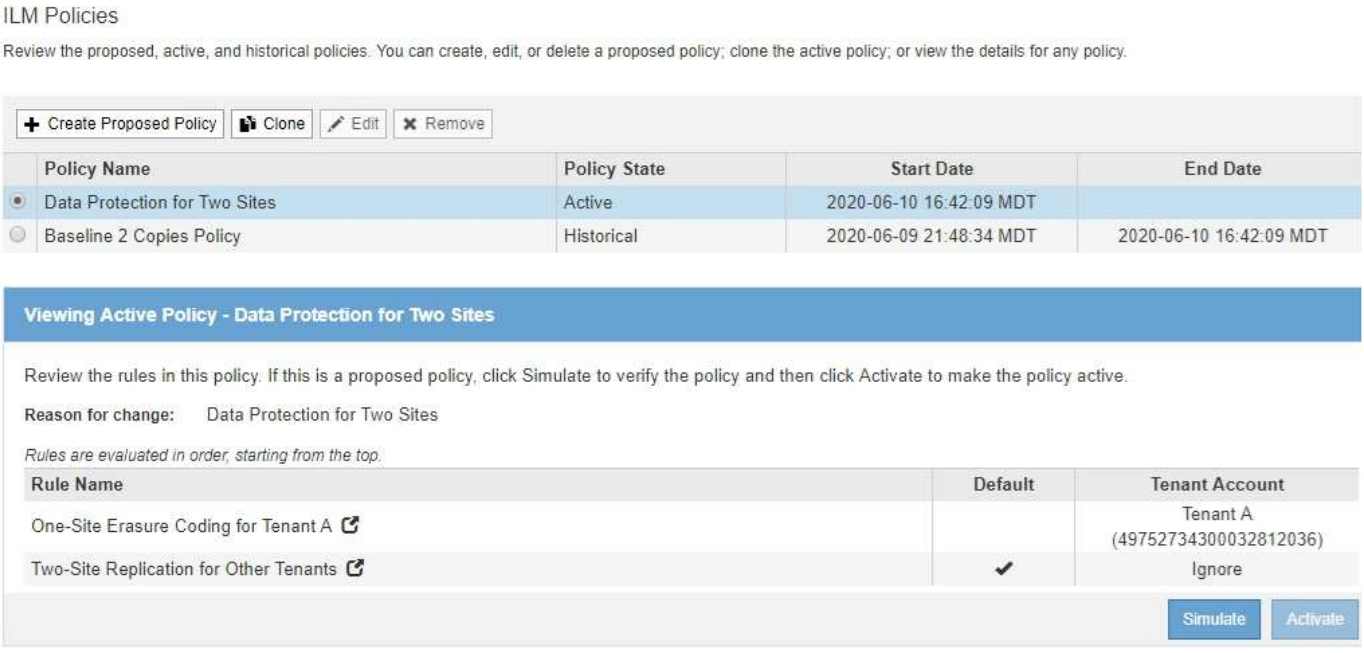
- 更改现有对象所需的副本类型；例如，将大量复制对象转换为经过纠删编码的对象。
- 将现有对象的副本移动到完全不同的位置；例如，将大量对象移入或移出云存储池，或者移动到远程站点或从远程站点移动。

相关信息

创建 ILM 策略

示例 6 中的活动 ILM 策略：两个站点的数据保护

在此示例中，活动 ILM 策略最初是为双站点 StorageGRID 系统设计的，并使用两个 ILM 规则。



在此 ILM 策略中，属于租户 A 的对象在一个站点上通过 2+1 纠删编码进行保护，而属于所有其他租户的对象则

通过双副本复制在两个站点之间进行保护。

> 本示例中的第一个规则使用高级筛选器来确保纠删编码不会用于小型对象。如果租户 A 的任何对象小于 1 MB ，则会受第二个规则的保护，该规则使用复制。

规则 **1** ： 租户 **A** 的单站点纠删编码

规则定义	示例值
规则名称	租户 A 的单站点擦除编码
租户帐户	租户 A
存储池	数据中心 1.
内容放置	从第 0 天到永久，在 Data Center 1 中执行 2+1 纠删编码

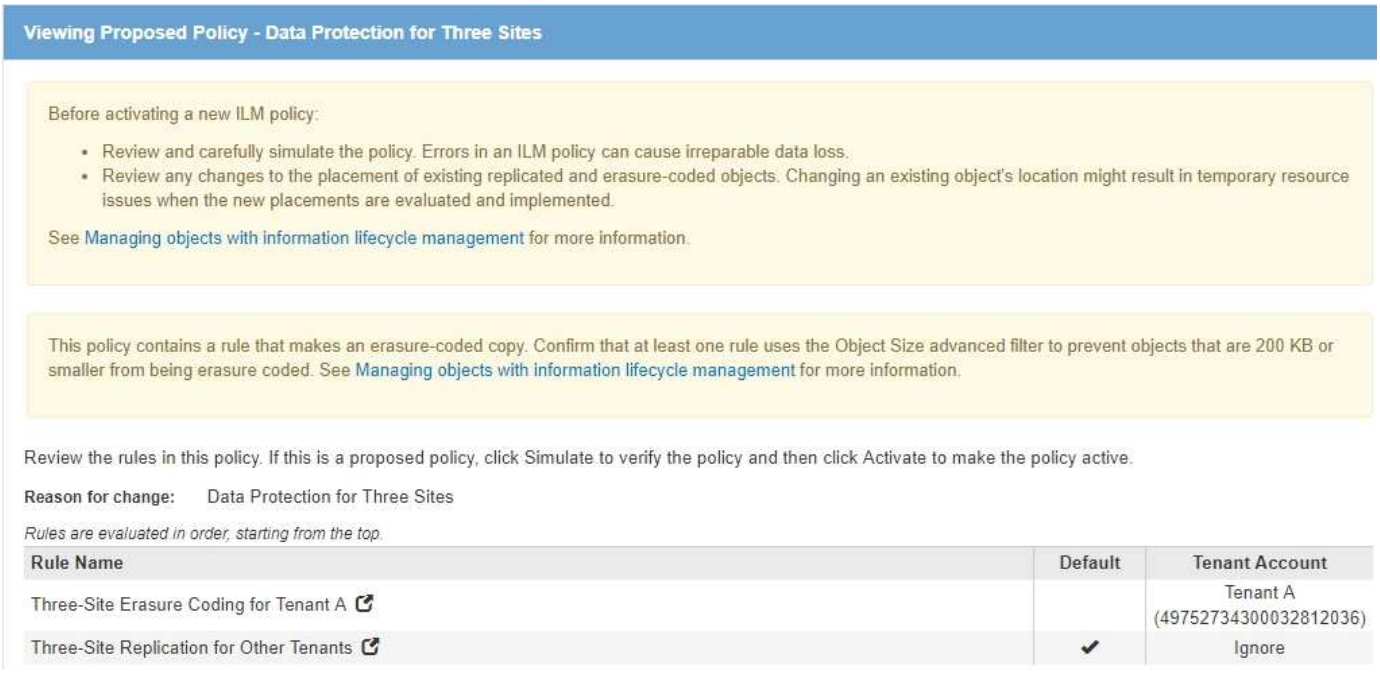
规则 **2** ： 为其他租户进行双站点复制

规则定义	示例值
规则名称	适用于其他租户的双站点复制
租户帐户	忽略
存储池	数据中心 1 和数据中心 2
内容放置	从第 0 天复制到永久的两个副本：一个副本位于数据中心 1 ，一个副本位于数据中心 2 。

示例 **6** 的建议 **ILM** 策略：三个站点的数据保护

在此示例中，正在为三站点 StorageGRID 系统更新 ILM 策略。

执行扩展以添加新站点后，网格管理员创建了两个新存储池：一个用于 Data Center 3 的存储池和一个包含所有三个站点的存储池（与所有存储节点默认存储池不同）。然后，管理员创建了两个新的 ILM 规则和一个新的建议 ILM 策略，该策略旨在保护所有三个站点的数据。



激活此新 ILM 策略后，属于租户 A 的对象将在三个站点上通过 2+1 纠删编码得到保护，而属于其他租户（以及属于租户 A 的较小对象）的对象将通过三个副本复制在三个站点上得到保护。

规则 **1**： 租户 **A** 的三站点纠删编码

规则定义	示例值
规则名称	租户 A 的三站点擦除编码
租户帐户	租户 A
存储池	全部 3 个数据中心（包括数据中心 1 ，数据中心 2 和数据中心 3 ）
内容放置	从第 0 天到永久，在所有 3 个数据中心进行 2+1 纠删编码

规则 **2**： 对其他租户进行三站点复制

规则定义	示例值
规则名称	适用于其他租户的三站点复制
租户帐户	忽略
存储池	数据中心 1 ，数据中心 2 和数据中心 3
内容放置	从第 0 天复制到永久的三个副本：在数据中心 1 复制一个副本，在数据中心 2 复制一个副本，在数据中心 3 复制一个副本。

激活新建议的 ILM 策略时，可能会根据任何新规则或更新的规则中的放置说明将现有对象移动到新位置，或者为现有对象创建新的对象副本。

ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。在激活策略之前，请仔细查看并模拟策略，以确认策略将按预期运行。

激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

擦除编码指令发生变化时会发生什么情况

在本示例的当前活动 ILM 策略中，属于租户 A 的对象将在数据中心 1 使用 2+1 纠删编码进行保护。在新建议的 ILM 策略中，属于租户 A 的对象将在数据中心 1 ， 2 和 3 使用 2+1 纠删编码进行保护。

激活新的 ILM 策略后，将执行以下 ILM 操作：

- 租户 A 输入的新对象将拆分为两个数据片段，并添加一个奇偶校验片段。然后，这三个片段中的每一个都会存储在不同的数据中心。
- 属于租户 A 的现有对象将在进行 ILM 扫描过程中重新评估。由于 ILM 放置说明使用新的纠删编码配置文件，因此会创建全新的纠删编码片段并将其分发到三个数据中心。

不会重复使用 Data Center 1 上的现有 2+1 片段。StorageGRID 认为每个擦除编码配置文件都是唯一的，使用新配置文件时不会重复使用擦除编码片段。

复制指令发生变化时会发生什么情况

在此示例的当前活动 ILM 策略中，属于其他租户的对象将使用数据中心 1 和 2 的存储池中的两个复制副本进行保护。在新建议的 ILM 策略中，属于其他租户的对象将使用数据中心 1 ， 2 和 3 的存储池中的三个复制副本进行保护。

激活新的 ILM 策略后，将执行以下 ILM 操作：

- 如果租户 A 以外的任何租户载入新对象， StorageGRID 将创建三个副本并在每个数据中心保存一个副本。
- 属于这些其他租户的现有对象将在进行中的 ILM 扫描过程中重新评估。由于数据中心 1 和数据中心 2 上的现有对象副本仍然满足新 ILM 规则的复制要求，因此 StorageGRID 只需要为数据中心 3 创建一个新的对象副本。

激活此策略对性能的影响

激活此示例中建议的 ILM 策略后，此 StorageGRID 系统的整体性能将暂时受到影响。要为租户 A 的现有对象创建新的纠删编码片段，并在数据中心 3 为其他租户的现有对象创建新的复制副本，需要的网格资源级别高于正常水平。

由于 ILM 策略发生更改，客户端读取和写入请求可能会暂时出现比正常延迟高的情况。在整个网格中完全实施放置说明后，延迟将恢复到正常水平。

要在激活新 ILM 策略时避免资源问题，您可以在可能更改大量现有对象位置的任何规则中使用 " 载入时间 " 高级

筛选器。将载入时间设置为大于或等于新策略生效的大致时间，以确保现有对象不会发生不必要的移动。

如果在 ILM 策略更改后需要降低或提高对象的处理速度，请联系技术支持。

示例 7： **S3** 对象锁定的兼容 **ILM** 策略

在定义 ILM 策略以满足启用了 S3 对象锁定的存储分段中对象的对象保护和保留要求时，您可以在此示例中使用 S3 存储分段， ILM 规则和 ILM 策略作为起点。

如果您在先前的 StorageGRID 版本中使用了原有合规性功能，则也可以使用此示例来帮助管理启用了原有合规性功能的任何现有存储分段。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。

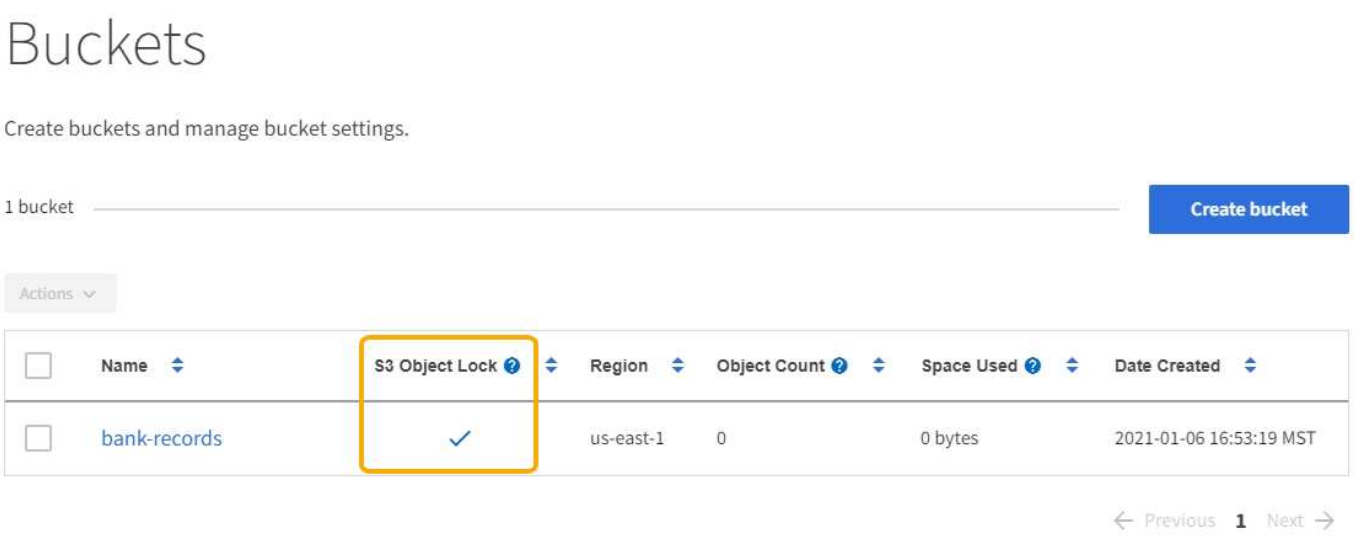
相关信息

- 使用 S3 对象锁定管理对象
- 创建 ILM 策略

S3 对象锁定的分段和对象示例

在此示例中，名为 Bank of ABC 的 S3 租户帐户使用租户管理器创建了一个启用了 S3 对象锁定的存储分段，用于存储重要的银行记录。

存储分段定义	示例值
租户帐户名称	ABC 银行
Bucket Name	银行记录
存储分段区域	us-east-1 （默认）



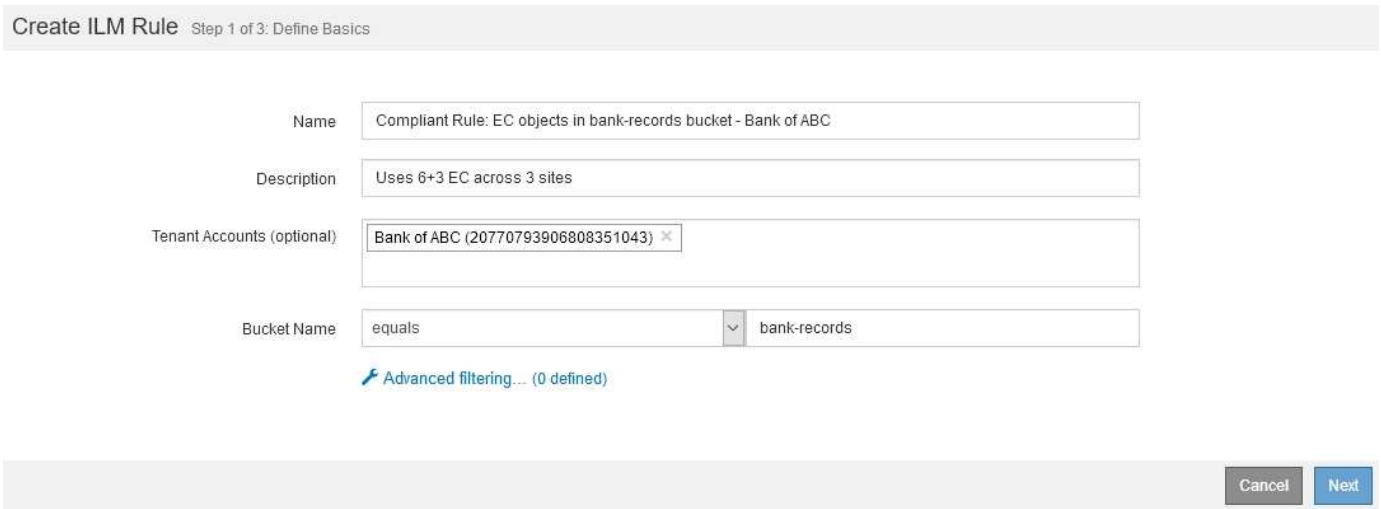
添加到银行记录分段的每个对象和对象版本将对 `redan-until date` 和 `legal hold` 设置使用以下值。

为每个对象设置	示例值
`redan-until date`	`"2030-12-30T23： 59： 59Z"` （ 2030 年 12 月 30 日） 每个对象版本都有自己的 `redy-until date` 设置。此设置可以增加，但不能减少。
法定保留	`" 关闭 "` （未生效） 在保留期限内，可以随时对任何对象版本进行合法保留或取消合法保留。如果对象处于合法保留状态，则即使已达到 `redy-until` **日期**，也无法删除此对象。

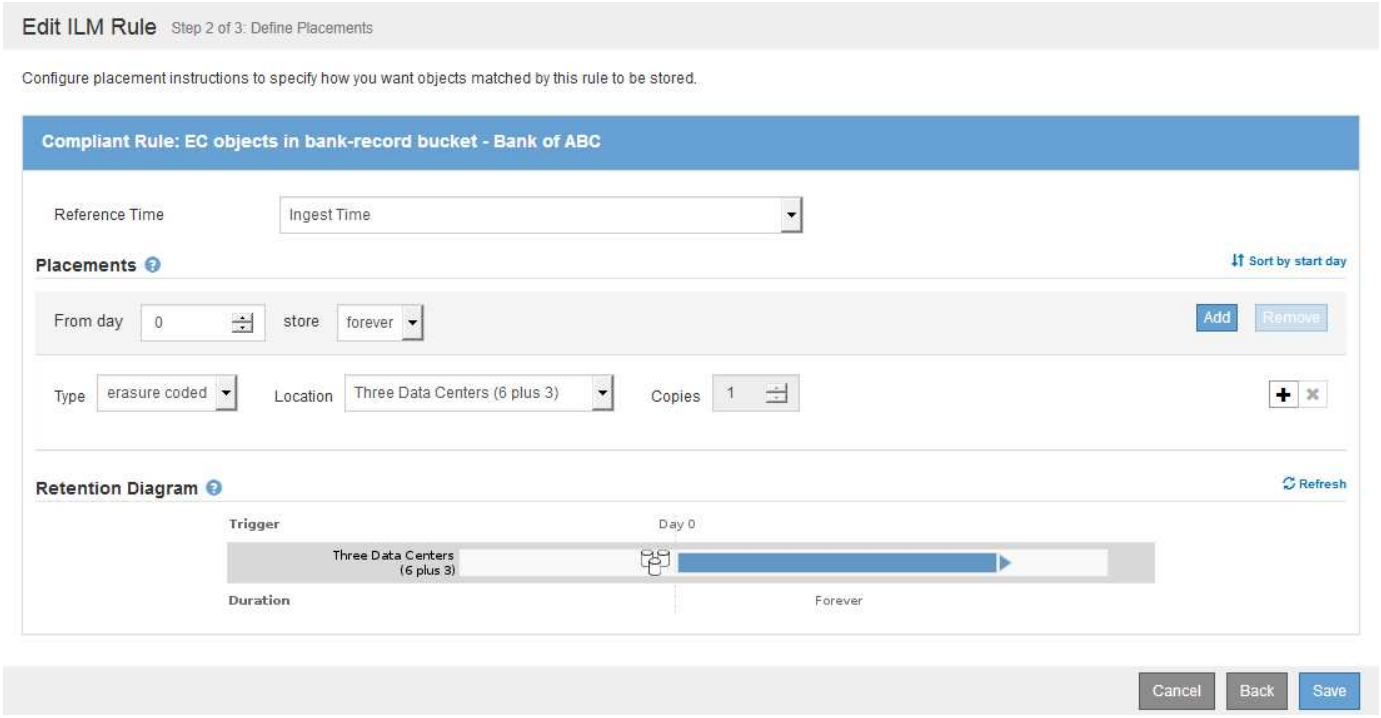
适用于 **S3** 对象锁定的 **ILM** 规则 **1** 示例：使用存储分段匹配的纠删编码配置文件

此示例 ILM 规则仅适用于名为 ABC 银行的 S3 租户帐户。它与 **银行记录** 存储分段中的任何对象匹配，然后使用纠删编码，使用 6+3 擦除编码配置文件将对象存储在三个数据中心站点的存储节点上。此规则满足启用了 S3 对象锁定的存储分段的要求：从 0 天到永久，存储节点上会保留经过擦除编码的副本，并使用载入时间作为参考时间。

规则定义	示例值
规则名称	合规规则：银行记录存储分段中的 EC 对象— ABC 银行
租户帐户	ABC 银行
Bucket Name	**银行记录**
高级筛选	对象大小（ MB ）大于 1 • 注： * 此筛选器可确保擦除编码不会用于 1 MB 或更小的对象。



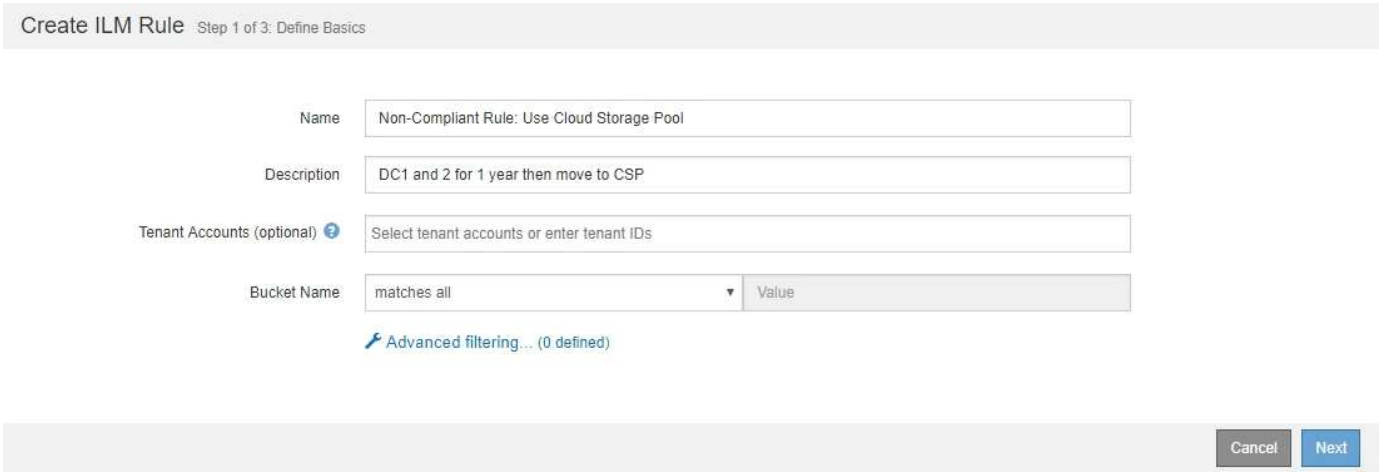
规则定义	示例值
参考时间	载入时间
放置	从 Day 0 存储永久存储
纠删编码配置文件	• 在三个数据中心站点的存储节点上创建经过擦除编码的副本 • 使用 6+3 纠删编码方案



适用于 **S3** 对象锁定的 **ILM** 规则 **2** 示例：不合规规则

此示例 ILM 规则最初会将两个复制的对象副本存储在存储节点上。一年后，它会将一个副本永久存储在云存储池中。由于此规则使用云存储池，因此它不符合要求，并且不会应用于启用了 S3 对象锁定的分段中的对象。

规则定义	示例值
规则名称	不合规规则：使用云存储池
租户帐户	未指定
Bucket Name	未指定，但仅适用于未启用 S3 对象锁定（或原有合规性功能）的分段。
高级筛选	未指定

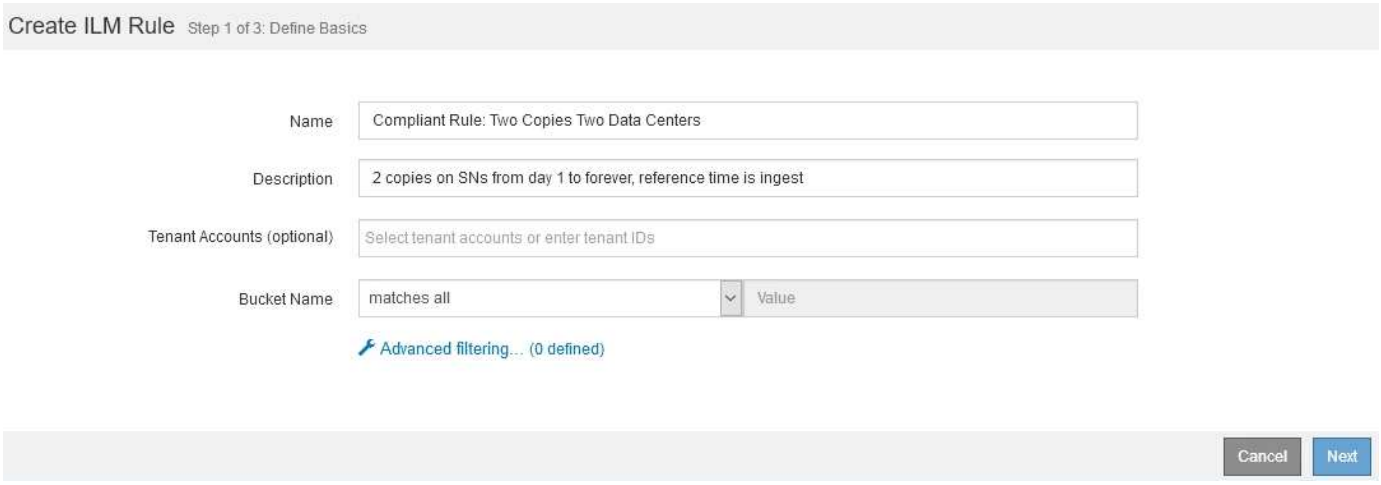


规则定义	示例值
参考时间	载入时间
放置	• 在第 0 天，在数据中心 1 和数据中心 2 的存储节点上保留两个复制副本 365 天 • 1 年后，将一个复制副本永久保留在云存储池中

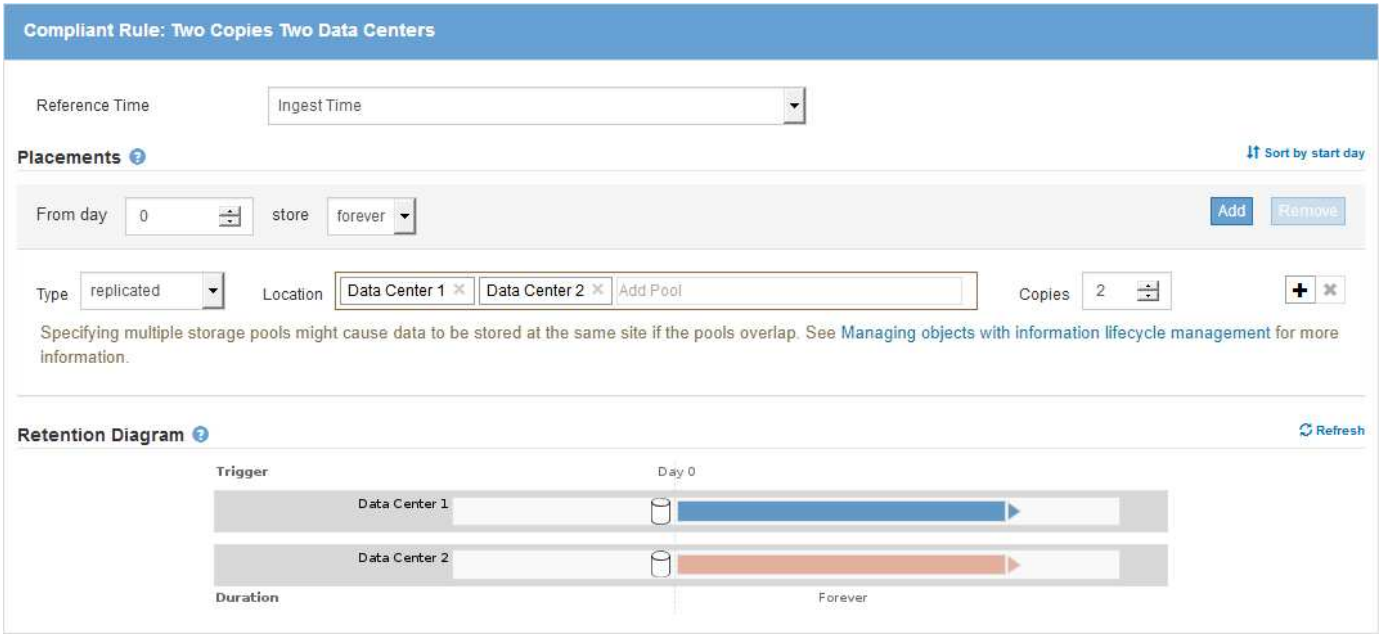
适用于 **S3** 对象锁定的 **ILM** 规则 **3** 示例：默认规则

此示例 ILM 规则会将对象数据复制到两个数据中心中的存储池。此合规规则是 ILM 策略中的默认规则。它不包括任何筛选器，不使用非当前参考时间，并满足启用了 S3 对象锁定的存储分段的要求：从 0 天到永久，存储节点上保留两个对象副本，并使用 Ingest 作为参考时间。

规则定义	示例值
规则名称	默认合规规则：两个副本两个数据中心
租户帐户	未指定
Bucket Name	未指定
高级筛选	未指定



规则定义	示例值
参考时间	载入时间
放置	从 0 天到永久，请保留两个复制副本—一个在数据中心 1 的存储节点上，一个在数据中心 2 的存储节点上。



S3 对象锁定的兼容 **ILM** 策略示例

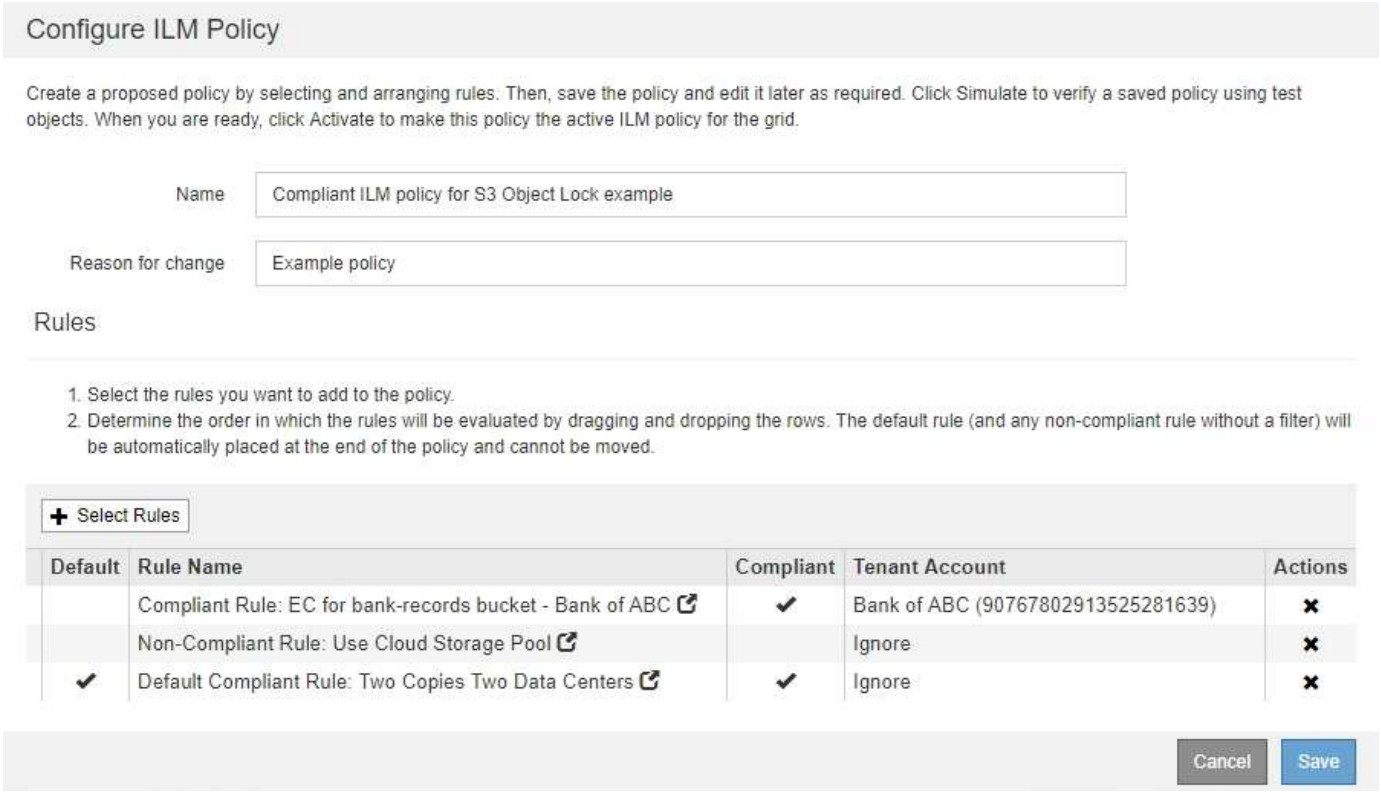
要创建有效保护系统中所有对象的 ILM 策略，包括启用了 S3 对象锁定的分段中的对象，您必须选择满足所有对象存储要求的 ILM 规则。然后，您必须模拟并激活建议的策略。

向策略中添加规则

在此示例中， ILM 策略包括三个 ILM 规则，其顺序如下：

1. 一种使用纠删编码保护启用了 S3 对象锁定的特定分段中大于 1 MB 的对象的合规规则。从 0 天到永久，对象存储在存储节点上。

2. 一种不合规的规则，在存储节点上创建两个复制的对象副本一年，然后将一个对象副本永久移动到云存储池。此规则不适用于启用了 S3 对象锁定的存储分段，因为它使用的是云存储池。
3. 一种默认合规规则，用于在存储节点上创建从 0 天到永久的两个复制对象副本。



模拟建议的策略

在建议的策略中添加规则，选择默认合规规则并排列其他规则后，您应通过测试启用了 S3 对象锁定的存储分段和其他存储分段中的对象来模拟此策略。例如，在模拟示例策略时，您希望按如下所示评估测试对象：

- 第一个规则仅与 ABC 银行租户的存储分段记录中大于 1 MB 的测试对象匹配。
- 第二个规则将匹配所有其他租户帐户的所有不合规分段中的所有对象。
- 默认规则将与以下对象匹配：
  - ABC 银行租户的存储分段库记录中的对象不小于 1 MB 。
  - 为所有其他租户帐户启用了 S3 对象锁定的任何其他分段中的对象。

激活策略

如果您完全确信新策略会按预期保护对象数据，则可以激活此策略。

系统强化

系统强化：概述

系统强化是指尽可能消除 StorageGRID 系统中的安全风险的过程。

本文档概述了特定于 StorageGRID 的强化准则。这些准则是对行业标准系统强化最佳实践的补充。例如，这些准则假定您对 StorageGRID 使用强密码，使用 HTTPS 而不是 HTTP ，并在可用时启用基于证书的身份验证。

在安装和配置 StorageGRID 时，您可以使用这些准则来帮助您实现任何规定的安全目标，以确保信息系统的机密性，完整性和可用性。

StorageGRID 遵循 _NetApp 漏洞处理策略 _ 。报告的漏洞会根据产品安全意外事件响应流程进行验证和解决。

强化 **StorageGRID** 系统的一般注意事项

在强化 StorageGRID 系统时，必须考虑以下几点：

- 您实施了三个 StorageGRID 网络中的哪一个。所有 StorageGRID 系统都必须使用网格网络，但您也可以使用管理网络，客户端网络或这两者。每个网络都有不同的安全注意事项。
- StorageGRID 系统中各个节点使用的平台类型。StorageGRID 节点可以部署在 VMware 虚拟机上， Linux 主机上的容器引擎中或作为专用硬件设备。每种类型的平台都有自己的一套强化最佳实践。
- 租户帐户的受信任程度。如果您是使用不可信租户帐户的服务提供商，则与仅使用可信的内部租户相比，您将面临不同的安全问题。
- 贵组织遵循哪些安全要求和约定。您可能需要遵守特定的法规或企业要求。

相关信息

"漏洞处理策略"

软件升级的强化准则

您必须使 StorageGRID 系统和相关服务保持最新，以抵御攻击。

升级到 **StorageGRID** 软件

您应尽可能将 StorageGRID 软件升级到最新的主要版本或先前的主要版本。使 StorageGRID 保持最新有助于缩短已知漏洞处于活动状态的时间，并减少整体攻击面。此外， StorageGRID 的最新版本通常包含早期版本中不包括的安全强化功能。

如果需要修补程序， NetApp 会优先为最新版本创建更新。某些修补程序可能与早期版本不兼容。

要下载最新的 StorageGRID 版本和修补程序，请转到 StorageGRID 软件下载页面。有关升级 StorageGRID 软件的分步说明，请参见有关升级 StorageGRID 的说明。有关应用修补程序的说明，请参见恢复和维护说明。

升级到外部服务

外部服务可能存在间接影响 StorageGRID 的漏洞。您应确保 StorageGRID 所依赖的服务保持最新。这些服务包括 LDAP ， KMS （或 KMIP 服务器）， DNS 和 NTP 。

使用 NetApp 互操作性表工具可获取受支持版本的列表。

升级到虚拟机管理程序

如果您的 StorageGRID 节点正在 VMware 或其他虚拟机管理程序上运行，则必须确保虚拟机管理程序软件和固件是最新的。

使用 NetApp 互操作性表工具可获取受支持版本的列表。

升级到**Linux**节点

如果 StorageGRID 节点使用的是 Linux 主机平台，则必须确保将安全更新和内核更新应用于主机操作系统。此外，如果存在固件更新，则必须将这些更新应用于容易受到影响的硬件。

使用 NetApp 互操作性表工具可获取受支持版本的列表。

相关信息

"NetApp 下载： StorageGRID"

升级软件

恢复和维护

"NetApp 互操作性表工具"

StorageGRID 网络强化准则

StorageGRID 系统支持每个网格节点最多三个网络接口，使您可以根据安全和访问要求为每个网格节点配置网络。

网格网络准则

您必须为所有内部 StorageGRID 流量配置网格网络。所有网格节点均位于网格网络上，它们必须能够与所有其他节点进行通信。

配置网格网络时，请遵循以下准则：

- 确保网络不受不可信客户端的保护，例如在开放式互联网上的客户端。
- 如果可能，请仅对内部流量使用网格网络。管理网络和客户端网络都具有其他防火墙限制，可阻止外部向内部服务发送流量。支持对外部客户端流量使用网格网络，但这种使用可提供更少的保护层。
- 如果 StorageGRID 部署跨越多个数据中心，请使用网格网络上的虚拟专用网络（ VPN ）或等效网络为内部流量提供额外保护。
- 某些维护过程要求在主管理节点与所有其他网格节点之间的端口 22 上进行安全 Shell （ SSH ）访问。使用外部防火墙将 SSH 访问限制为受信任的客户端。

管理网络准则

管理网络通常用于执行管理任务（使用网格管理器或 SSH 的受信任员工）以及与 LDAP ， DNS ， NTP 或 KMS （或 KMIP 服务器）等其他受信任服务进行通信。但是， StorageGRID 不会在内部强制使用此用法。

如果您使用的是管理网络，请遵循以下准则：

- 阻止管理网络上的所有内部流量端口。请参见适用于您的平台的安装指南中的内部端口列表。
- 如果不可信的客户端可以访问管理网络，请使用外部防火墙阻止对管理网络上 StorageGRID 的访问。

客户端网络准则

客户端网络通常用于租户以及与外部服务（例如 CloudMirror 复制服务或其他平台服务）进行通信。但是，StorageGRID 不会在内部强制使用此用法。

如果您使用的是客户端网络，请遵循以下准则：

- 阻止客户端网络上的所有内部流量端口。请参见适用于您的平台的安装指南中的内部端口列表。
- 仅接受显式配置的端点上的入站客户端流量。请参见 管理不可信客户端网络。

相关信息

网络连接准则

网格入门

管理 StorageGRID

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

安装 VMware

StorageGRID 节点的强化准则

StorageGRID 节点可以部署在 VMware 虚拟机上， Linux 主机上的容器引擎中或作为专用硬件设备。每种类型的平台和每种类型的节点都有自己的一组强化最佳实践。

防火墙配置

在系统强化过程中，您必须查看外部防火墙配置并对其进行修改，以便仅接受来自 IP 地址和严格需要的端口的流量。

StorageGRID 使用自动管理的内部防火墙。虽然此内部防火墙可为应对某些常见威胁提供额外的保护层，但它不会消除对外部防火墙的需求。

有关 StorageGRID 使用的所有内部和外部端口的列表，请参见适用于您的平台的安装指南。

虚拟化，容器和共享硬件

对于所有 StorageGRID 节点，请避免在与不可信软件相同的物理硬件上运行 StorageGRID 。如果 StorageGRID 和恶意软件都位于同一物理硬件上，则不要假定虚拟机管理程序保护将防止恶意软件访问受 StorageGRID 保护的数据。例如， Meltdown 和 Spectre 攻击会利用现代处理器中的关键漏洞，并允许程序在同一台计算机的内存中窃取数据。

禁用未使用的服务

对于所有 StorageGRID 节点，您应禁用或阻止对未使用服务的访问。例如，如果您不打算配置客户端对 CIFS 或 NFS 的审核共享的访问权限，请阻止或禁用对这些服务的访问。

在安装期间保护节点

安装 StorageGRID 节点时，请勿允许不可信的用户通过网络访问这些节点。节点在加入网格之前不会完全安全。

管理节点准则

管理节点可提供系统配置，监控和日志记录等管理服务。登录到网格管理器或租户管理器时，您正在连接到管理节点。

请按照以下准则保护 StorageGRID 系统中的管理节点：

- 保护所有管理节点不受不可信客户端的安全，例如在开放式 Internet 上的客户端。确保任何不可信的客户端都不能访问网格网络，管理网络或客户端网络上的任何管理节点。
- StorageGRID 组控制对网格管理器和租户管理器功能的访问。为每个用户组授予其角色所需的最低权限，并使用只读访问模式防止用户更改配置。
- 在使用 StorageGRID 负载平衡器端点时，请对不可信的客户端流量使用网关节点，而不是管理节点。
- 如果您的租户不可信，请勿允许他们直接访问租户管理器或租户管理 API 。相反，让任何不可信的租户使用与租户管理 API 交互的租户门户或外部租户管理系统。
- 或者，也可以使用管理员代理更好地控制从管理节点到 NetApp 支持的 AutoSupport 通信。请参见管理 StorageGRID 说明中的创建管理员代理的步骤。
- 或者，也可以使用受限的 8443 和 9443 端口分隔 Grid Manager 和租户管理器通信。阻止共享端口 443 并将租户请求限制为端口 9443 以提供额外保护。
- 也可以为网格管理员和租户用户使用单独的管理节点。

有关详细信息，请参见有关管理 StorageGRID 的说明。

存储节点准则

存储节点可管理和存储对象数据和元数据。请按照以下准则保护 StorageGRID 系统中的存储节点。

- 请勿允许不可信的客户端直接连接到存储节点。使用由网关节点或第三方负载平衡器提供服务的负载平衡器端点。
- 请勿为不可信租户启用出站服务。例如，在为不可信租户创建帐户时，请勿允许租户使用自己的身份源，也不允许使用平台服务。请参见管理 StorageGRID 的说明中有关创建租户帐户的步骤。
- 对不可信的客户端流量使用第三方负载平衡器。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。
- 或者，也可以使用存储代理更好地控制云存储池以及从存储节点到外部服务的平台服务通信。请参见管理 StorageGRID 的说明中有关创建存储代理的步骤。
- 也可以使用客户端网络连接到外部服务。然后，选择 * 配置 * > * 网络 * > * 不可信客户端网络 * ，并指示存储节点上的客户端网络不可信。存储节点不再接受客户端网络上的任何传入流量，但仍允许对平台服务发出出站请求。

网关节点准则

网关节点提供了一个可选的负载平衡接口，客户端应用程序可以使用该接口连接到 StorageGRID 。请按照以下准则保护 StorageGRID 系统中的所有网关节点：

- 在网关节点上配置和使用负载平衡器端点，而不是使用 CLB 服务。请参见管理 StorageGRID 说明中的负载平衡管理步骤。

  CLB 服务已弃用。

- 在客户端和网关节点或存储节点之间使用第三方负载平衡器处理不可信的客户端流量。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。如果您使用的是第三方负载平衡器，则仍然可以选择将网络流量配置为通过内部负载平衡器端点或直接发送到存储节点。
- 如果您使用的是负载平衡器端点，则可以选择让客户端通过客户端网络进行连接。然后，选择 * 配置 * > * 网络 * > * 不可信客户端网络 * ，并指示网关节点上的客户端网络不可信。网关节点仅接受显式配置为负载平衡器端点的端口上的入站流量。

硬件设备节点准则

StorageGRID 硬件设备经过专门设计，可在 StorageGRID 系统中使用。某些设备可用作存储节点。其他设备可以用作管理节点或网关节点。您可以将设备节点与基于软件的节点结合使用，也可以部署经过全面设计的全设备网格。

请按照以下准则保护 StorageGRID 系统中的所有硬件设备节点：

- 如果设备使用 SANtricity 系统管理器管理存储控制器，请防止不可信的客户端通过网络访问 SANtricity 系统管理器。
- 如果设备具有基板管理控制器（ Baseboard Management Controller ， BMC ），请注意， BMC 管理端口允许低级别硬件访问。请仅将 BMC 管理端口连接到安全可信的内部管理网络。如果没有此类网络可用，请保持 BMC 管理端口未连接或被阻止，除非技术支持请求 BMC 连接。
- 如果设备支持使用智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）标准通过以太网远程管理控制器硬件，请阻止端口 623 上的不可信流量。
- 如果设备中的存储控制器包含 FDE 或 FIPS 驱动器，并且已启用驱动器安全功能，请使用 SANtricity 配置驱动器安全密钥。
- 对于没有 FDE 或 FIPS 驱动器的设备，请使用密钥管理服务器（ KMS ）启用节点加密。

请参见 StorageGRID 硬件设备的安装和维护说明。

相关信息

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian
- 安装 VMware
- 管理 StorageGRID
- 使用租户帐户
- SG100 和 SG1000 服务设备
- SG5600 存储设备
- SG5700 存储设备
- SG6000 存储设备

服务器证书的强化准则

您应将安装期间创建的默认证书替换为您自己的自定义证书。

对于许多组织来说，用于 StorageGRID Web 访问的自签名数字证书不符合其信息安全策略。在生产系统上，您应安装 CA 签名的数字证书以用于对 StorageGRID 进行身份验证。

具体而言，您应使用自定义服务器证书，而不是这些默认证书：

- * 管理接口证书 * ： 用于确保对网格管理器，租户管理器，网格管理 API 和租户管理 API 的访问安全。
- * S3 和 Swift API 证书 * ： 用于保护对存储节点和网关节点的访问安全， S3 和 Swift 客户端应用程序使用这些节点上传和下载对象数据。

> StorageGRID 单独管理用于负载平衡器端点的证书。要配置负载平衡器证书，请参见管理 StorageGRID 的说明中配置负载平衡器端点的步骤。

使用自定义服务器证书时，请遵循以下准则：

- 证书应具有与 StorageGRID 的 DNS 条目匹配的 ` *subjectAltName*` 。有关详细信息，请参见中的第 4.2.1.6 节 " `SSubject Alternative Name ，` " "RFC 5280： PKIX 证书和 CRL 配置文件"。
- 尽可能避免使用通配符证书。此准则的一个例外是 S3 虚拟托管模式端点的证书，如果事先不知道分段名称，则需要使用通配符。
- 如果必须在证书中使用通配符，则应执行其他步骤以降低风险。请使用通配符模式，例如 ` *.s3.example.com` ，不要对其他应用程序使用 `s3.example.com` 后缀。此模式也适用于路径模式 S3 访问，例如 `dc1-s1.s3.example.com/mybucket` 。
- 将证书到期时间设置为较短（例如 2 个月），并使用网格管理 API 自动轮换证书。这对于通配符证书尤其重要。

此外，客户端在与 StorageGRID 通信时应使用严格的主机名检查。

其他强化准则

除了遵循 StorageGRID 网络和节点的强化准则之外，您还应遵循 StorageGRID 系统其他方面的强化准则。

日志和审核消息

始终以安全的方式保护 StorageGRID 日志和审核消息输出。从支持和系统可用性角度来看， StorageGRID 日志和审核消息可提供宝贵的信息。此外， StorageGRID 日志和审核消息输出中包含的信息和详细信息通常具有敏感性。

将 StorageGRID 配置为向外部系统日志服务器发送安全事件。如果使用系统日志导出，请为传输协议选择 TLS 和 RELP/TLS 。

有关 StorageGRID 日志的详细信息，请参见有关监控和故障排除的说明。有关 StorageGRID 审核消息的详细信息，请参见审核消息的说明。

NetApp AutoSupport

通过 StorageGRID 的 AutoSupport 功能，您可以主动监控系统的运行状况，并自动向 NetApp 技术支持，贵组织的内部支持团队或支持合作伙伴发送消息和详细信息。默认情况下，首次配置 StorageGRID 时，会启用发送给 NetApp 技术支持的 AutoSupport 消息。

可以禁用 AutoSupport 功能。但是， NetApp 建议启用此功能，因为如果您的 StorageGRID 系统上出现问题描述， AutoSupport 有助于加快识别和解决问题的速度。

对于传输协议， AutoSupport 支持 HTTPS ， HTTP 和 SMTP 。由于 AutoSupport 消息的敏感性， NetApp 强烈建议使用 HTTPS 作为向 NetApp 支持部门发送 AutoSupport 消息的默认传输协议。

您也可以配置一个管理员代理，以便更好地控制从管理节点到 NetApp 技术支持的 AutoSupport 通信。请参见管理 StorageGRID 说明中的创建管理员代理的步骤。

跨源资源共享（ **CORS** ）

如果您希望 S3 存储分段中的存储分段和对象可供其他域中的 Web 应用程序访问，则可以为该存储分段配置跨源资源共享（ CORS ）。通常，除非需要，否则请勿启用 CORS 。如果需要 CORS ，请将其限制为可信源。

请参见使用租户帐户说明中的配置跨源资源共享（ CORS ）的步骤。

外部安全设备

全面强化的解决方案 必须解决 StorageGRID 之外的安全机制问题。使用其他基础架构设备筛选和限制对 StorageGRID 的访问是建立和保持严格安全防护的有效方法。这些外部安全设备包括防火墙，入侵防护系统（ IP ）和其他安全设备。

对于不可信的客户端流量，建议使用第三方负载平衡器。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。

相关信息

监控和故障排除

查看审核日志

使用租户帐户

管理 StorageGRID

配置 FabricPool

Configure StorageGRID for FabricPool： 概述

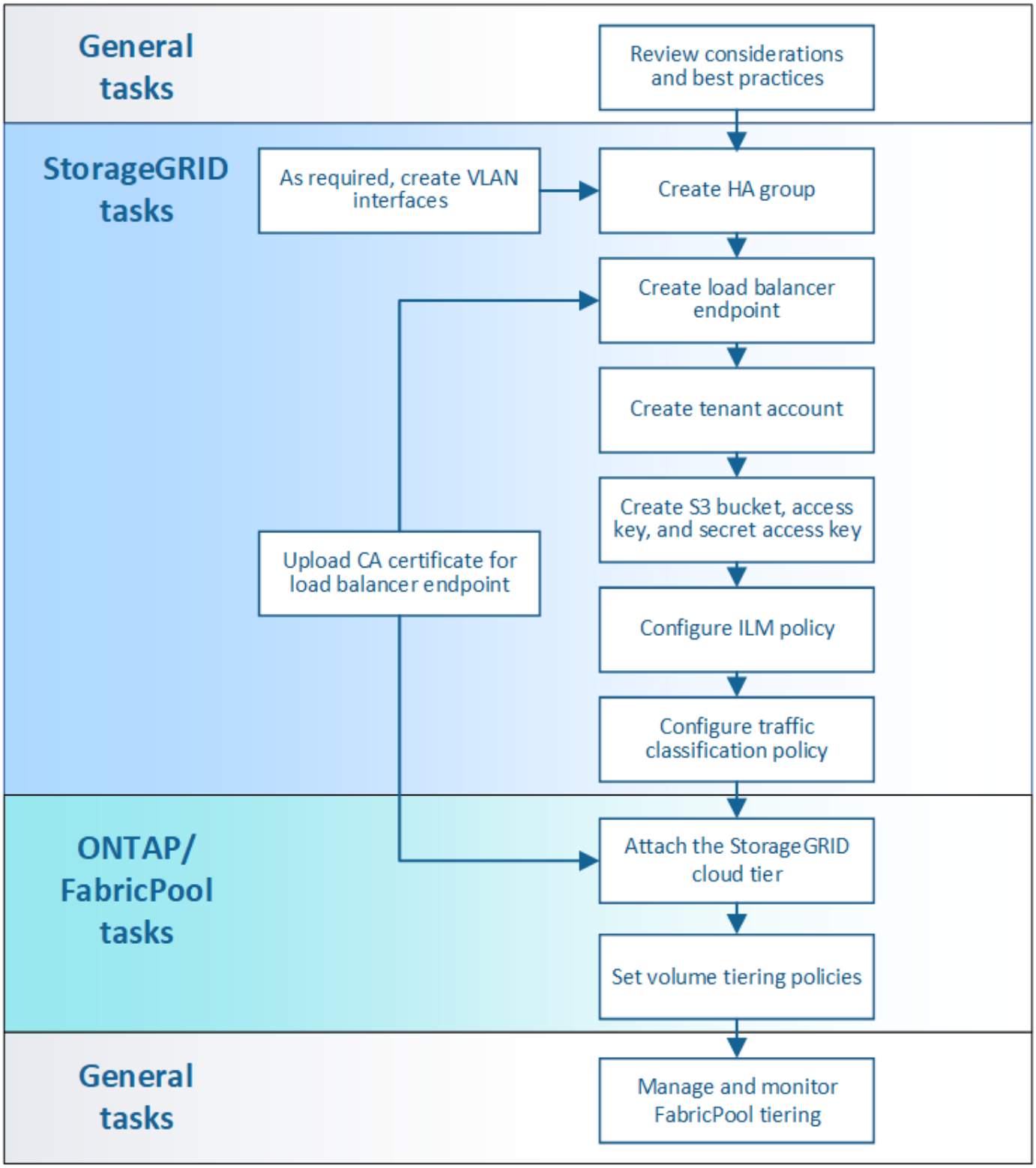
如果您使用的是 NetApp ONTAP 软件，则可以使用 NetApp FabricPool 将非活动或冷数据分层到 NetApp StorageGRID 对象存储系统。

关于这些说明

按照以下说明执行以下操作：

- 简要了解如何配置 StorageGRID 对象存储系统以与 FabricPool 结合使用。
- 了解在将 StorageGRID 附加为 FabricPool 云层时如何获取您提供给 ONTAP 的信息。
- 了解为 FabricPool 工作负载配置 StorageGRID 信息生命周期管理（ ILM ）策略， StorageGRID 流量分类策略和其他 StorageGRID 选项的最佳实践。

配置工作流



开始之前

- 确定要使用哪个 FabricPool 卷分层策略将非活动 ONTAP 数据分层到 StorageGRID 。
- 规划和安装 StorageGRID 系统以满足您的存储容量和性能需求。
- 熟悉 StorageGRID 系统软件，包括网格管理器和租户管理器。
- 查看以下附加资源，其中提供了有关使用和配置 FabricPool 的详细信息：
  - "TR-4598 ： 《 ONTAP 9.9.1 中的 FabricPool 最佳实践》"
  - "ONTAP 9 文档"

什么是 **FabricPool** ？

FabricPool 是一种 ONTAP 混合存储解决方案 ，它使用高性能闪存聚合作为性能层，使用对象存储作为云层。数据存储在主存储介质上或对象数据存储库中，具体取决于是否经常访问。使用启用了 FabricPool 的聚合有助于降低存储成本，而不会影响性能，效率或保护。

无需更改架构，您可以继续从中央 ONTAP 存储系统管理数据和应用程序环境。

什么是 **StorageGRID** ？

StorageGRID 是一种存储架构，可以将数据作为对象进行管理，而不是像文件或块存储这样的其他存储架构。对象保留在一个容器（如分段）中，不会嵌套为其他目录中某个目录中的文件。虽然对象存储的性能通常低于文件或块存储，但其可扩展性明显更高。StorageGRID 存储分段可以容纳数 PB 的数据和数十亿个对象。

为什么使用 **StorageGRID** 作为 **FabricPool** 云层?

FabricPool 可以将 ONTAP 数据分层到多个对象存储提供程序，包括 StorageGRID 。公有 云可能会在存储分段或容器级别设置支持的每秒输入 / 输出操作数上限（ IOPS ），而 StorageGRID 性能则会随系统中的节点数进行扩展。使用 StorageGRID 作为 FabricPool 云层，您可以将冷数据保存在自己的私有云中，以获得最高性能并全面控制数据。

此外，如果使用 StorageGRID 作为云层，则不需要 FabricPool 许可证。

是否可以在 **StorageGRID** 中使用多个 **ONTAP** 集群?

以下说明介绍如何将 StorageGRID 连接到单个 ONTAP 集群。但是，您可能希望将同一个 StorageGRID 系统连接到多个 ONTAP 集群。

将数据从多个 ONTAP 集群分层到一个 StorageGRID 系统的唯一要求是，必须为每个集群使用不同的 S3 存储分段。根据您的要求，您可以对所有集群使用相同的高可用性（ HA ）组，负载平衡器端点和租户帐户，也可以为每个集群配置其中每个项。

将 **StorageGRID** 附加为云层

将 **StorageGRID** 附加为云层所需的信息

在将 StorageGRID 附加为 FabricPool 的云层之前，您必须在 StorageGRID 中执行一些配置步骤并获取某些值。

关于此任务

下表列出了在将 StorageGRID 作为 FabricPool 的云层附加时必须向 ONTAP 提供的信息。本节中的主题介绍如何使用 StorageGRID 网格管理器和租户管理器来获取所需信息。

> 列出的确切字段名称以及用于在 ONTAP 中输入所需值的过程取决于您使用的是 ONTAP 命令行界面（ storage aggregate object-store config create ）还是 ONTAP 系统管理器（ * 存储 * > * 聚合和磁盘 * > * 云层 * ）。

有关详细信息，请参见以下内容：

- "TR-4598 ： 《 ONTAP 9.9.1 中的 FabricPool 最佳实践》"
- "ONTAP 9 文档"

ONTAP 字段	Description
对象存储名称	任何唯一的描述性名称。例如， `StorageGRID_Cloud_Tier` 。
提供程序类型	StorageGRID （ ONTAP 系统管理器）或 `SGWS` （ ONTAP 命令行界面）。
Port	FabricPool 连接到 StorageGRID 时将使用的端口。您可以确定在定义 StorageGRID 负载平衡器端点时要使用的端口号。 为 FabricPool 创建负载平衡器端点
服务器名称	StorageGRID 负载平衡器端点的完全限定域名（ FQDN ）。例如， `s3.storagegrid.company.com` 。 请注意以下事项： • 此处指定的域名必须与您为 StorageGRID 负载平衡器端点上传的 CA 证书上的域名匹配。 • 此域名的 DNS 记录必须映射到要用于连接到 StorageGRID 的每个 IP 地址。 为 DNS 服务器配置 StorageGRID IP 地址

ONTAP 字段	Description
容器名称	要在此 ONTAP 集群中使用的 StorageGRID 存储分段的名称。例如，`fabricpool-bucket` 。您可以在租户管理器中创建此存储分段，也可以从 ONTAP 9.10 System Manager 开始使用 FabricPool 设置向导创建存储分段。 请注意以下事项： • 创建配置后，无法更改存储分段名称。 • 存储分段不能启用版本控制。 • 您必须为每个 ONTAP 集群使用不同的分段，以便将数据分层到 StorageGRID 。 创建 S3 存储分段并获取访问密钥
访问密钥和机密密码	StorageGRID 租户帐户的访问密钥和机密访问密钥。 您可以在租户管理器中生成这些值。 创建 S3 存储分段并获取访问密钥
SSL	必须启用。
对象存储证书	创建 StorageGRID 负载平衡器端点时上传的 CA 证书。 • 注意： * 如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。 为 FabricPool 创建负载平衡器端点

完成后

获取所需的 StorageGRID 信息后，您可以转到 ONTAP 将 StorageGRID 添加为云层，将云层添加为聚合并设置卷分层策略。

负载平衡最佳实践

在将 StorageGRID 附加为 FabricPool 云层之前，您必须使用 StorageGRID 网格管理器至少配置一个负载平衡器端点。

什么是负载平衡？

在将数据从 FabricPool 分层到 StorageGRID 系统时， StorageGRID 会使用负载平衡器来管理载入和检索工作负载。负载平衡通过在多个存储节点之间分布 FabricPool 工作负载，最大限度地提高速度和连接容量。

StorageGRID 负载平衡器服务安装在所有管理节点和所有网关节点上，并提供第 7 层负载平衡。它会终止客户端请求，检查请求并与存储节点建立新的安全连接。

将客户端流量转发到存储节点时，每个节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。

虽然建议使用 StorageGRID 负载平衡器服务来平衡负载，但您可能希望集成第三方负载平衡器。有关信息，请联系您的 NetApp 客户代表或参阅 "TR-4626： StorageGRID 第三方和全局负载平衡器"。

网关节点上的单独连接负载平衡器（ CLB ）服务已弃用，不再建议用于 FabricPool 。

StorageGRID 负载平衡最佳实践

作为一般最佳实践， StorageGRID 系统中的每个站点都应包含两个或更多具有负载平衡器服务的节点。例如，一个站点可能包含两个网关节点，或者同时包含一个管理节点和一个网关节点。无论您使用的是 SG100 或 SG1000 服务设备，裸机节点还是基于虚拟机（ VM ）的节点，确保每个负载平衡节点都有足够的网络，硬件或虚拟化基础架构。

您必须配置 StorageGRID 负载平衡器端点，以定义网关节点和管理节点用于传入和传出 FabricPool 请求的端口。

负载平衡器端点证书的最佳实践

创建用于 FabricPool 的负载平衡器端点时，应使用 HTTPS 作为协议。支持在不使用 TLS 加密的情况下与 StorageGRID 通信，但不建议这样做

然后，您可以上传由公共信任或私有证书颁发机构（ CA ）签名的证书，也可以生成自签名证书。此证书允许 ONTAP 向 StorageGRID 进行身份验证。

作为最佳实践，您应使用 CA 服务器证书来保护连接。由 CA 签名的证书可以无中断地轮换。

请求用于负载平衡器端点的 CA 证书时，请确保此证书上的域名与您在 ONTAP 中为该负载平衡器端点输入的服务器名称匹配。如果可能，请使用通配符（ * ）来支持虚拟主机模式的 URL 。例如：

```
*.s3.storagegrid.company.com
```

在将 StorageGRID 添加为 FabricPool 云层时，必须将同一证书安装到 ONTAP 集群以及根证书颁发机构（ CA ）证书和任何从属证书颁发机构（ CA ）证书。

StorageGRID 将服务器证书用于多种用途。如果要连接到负载平衡器服务，您可以选择使用 S3 和 Swift API 证书。

要了解有关负载平衡端点的服务器证书的详细信息，请执行以下操作：

- 配置负载平衡器端点
- 服务器证书的强化准则

高可用性组的最佳实践

在将 StorageGRID 附加为 FabricPool 云层之前，您应使用 StorageGRID 网格管理器配置高可用性（ HA ）组。

什么是高可用性（ **HA** ）组?

为了确保负载平衡器服务始终可用于管理 FabricPool 数据，您可以将多个管理节点和网关节点的网络接口分组到一个实体中，称为高可用性（ High Availability ， HA ）组。如果 HA 组中的活动节点发生故障，则组中的另一个节点可以继续管理工作负载。

每个 HA 组均可提供对关联节点上共享服务的高可用性访问。例如，如果 HA 组仅包含网关节点上的接口，或者同时包含管理节点和网关节点上的接口，则可以对共享负载平衡器服务进行高可用性访问。

要创建 HA 组，请执行以下常规步骤：

1. 为一个或多个管理节点或网关节点选择网络接口。您可以选择网格网络接口（ eth0 ），客户端网络接口（ eth2 ）或 VLAN 接口。

> ⓘ 如果您计划使用 VLAN 接口隔离 FabricPool 流量，则网络管理员必须先配置中继接口和相应的 VLAN 。每个 VLAN 都通过一个数字 ID 或标记来标识。例如，您的网络可能会使用 VLAN 100 传输 FabricPool 流量。

2. 为组分配一个或多个虚拟 IP （ VIP ）地址。FabricPool 等客户端应用程序可以使用其中任何 VIP 地址连接到 StorageGRID 。
3. 指定一个接口作为主接口，并确定任何备份接口的优先级顺序。主接口是活动接口，除非发生故障。

如果 HA 组包含多个接口，而主接口出现故障，则 VIP 地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。此故障转移过程通常只需几秒钟，并且速度足以使客户端应用程序不会受到任何影响，并且可以依靠正常的重试行为继续运行。

解决故障后，如果更高优先级的接口再次可用，则 VIP 地址会自动移至可用的最高优先级接口。

高可用性（ **HA** ）组的最佳实践

为 FabricPool 创建 StorageGRID HA 组的最佳实践取决于工作负载，如下所示：

- 如果您计划将FabricPool 与主工作负载数据结合使用、则必须创建一个至少包含两个负载平衡节点的HA组、以防止数据检索中断。
- 如果您计划使用 FabricPool snapshot-only 卷分层策略或非主本地性能层（例如，灾难恢复位置或 NetApp SnapMirror ® 目标），则只能为 HA 组配置一个节点。

以下说明介绍如何为主动备份 HA 设置 HA 组（一个节点为活动节点，一个节点为备份节点）。但是，您可能更喜欢使用 DNS 轮循或主动 - 主动 HA 。要了解这些其他 HA 配置的优势，请参见 HA 组的配置选项。

为 **DNS** 服务器配置 **StorageGRID IP** 地址

配置高可用性组和负载平衡器端点后，您必须确保 ONTAP 系统的域名系统（ DNS ）包含一条记录，用于将 StorageGRID 服务器名称（完全限定域名）与 FabricPool 用于建立连接的 IP 地址相关联。

在 DNS 记录中输入的 IP 地址取决于您是否使用的是由负载平衡节点组成的 HA 组：

- 如果已配置HA组、FabricPool 将连接到该HA组的虚拟IP地址。
- 如果您不使用HA组、则FabricPool 可以使用任何网关节点或管理节点的IP地址连接到StorageGRID 负载平

衡器服务。

此外，还必须确保 DNS 记录引用所有必需的端点域名，包括任何通配符名称。

为 **FabricPool** 创建高可用性（ **HA** ）组

在配置 StorageGRID 以与 FabricPool 结合使用时，您可以选择创建一个或多个高可用性（ HA ）组。HA 组由管理节点，网关节点或这两者上的一个或多个网络接口组成。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 如果您计划使用 VLAN ，则已创建 VLAN 接口。请参见 配置 VLAN 接口。

关于此任务

每个 HA 组都使用虚拟 IP 地址（ VIP ）来提供对关联节点上共享服务的高可用性访问。

有关此任务的详细信息，请参见 管理高可用性组。

步骤

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。
2. 选择 * 创建 * 。
3. 输入唯一名称，也可以选择输入问题描述 。
4. 选择一个或多个接口以添加到此 HA 组。

   使用列标题对行进行排序，或者输入搜索词以更快地找到接口。

5. 确定此 HA 组的主接口和任何备份接口。

   拖放行以更改 * 优先级顺序 * 列中的值。

   列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。

   如果 HA 组包含多个接口且活动接口发生故障，则 VIP 地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。解决故障后， VIP 地址将移回可用的最高优先级接口。

6. 以 CIDR 表示法 ##8212 指定 VIP 子网； IPv4 地址后跟斜杠和子网长度（ 0-32 ）。

   网络地址不能设置任何主机位。例如， `192.16.0.0/22` 。

7. 或者，如果用于访问 StorageGRID 的 ONTAP IP 地址与 StorageGRID VIP 地址不在同一子网中，请输入 StorageGRID VIP 本地网关 IP 地址。本地网关 IP 地址必须位于 VIP 子网中。
8. 输入 HA 组的一个或多个虚拟 IP 地址。最多可以添加 10 个 IP 地址。所有 VIP 都必须位于 VIP 子网中。

   您必须至少提供一个 IPv4 地址。您也可以指定其他 IPv4 和 IPv6 地址。

9. 选择 * 创建 HA 组 * ，然后选择 * 完成 * 。

为 **FabricPool** 创建负载平衡器端点

在配置 StorageGRID 以与 FabricPool 结合使用时，您必须配置负载平衡器端点并上传负载平衡器端点证书，此证书用于保护 ONTAP 和 StorageGRID 之间的连接。

您需要的内容

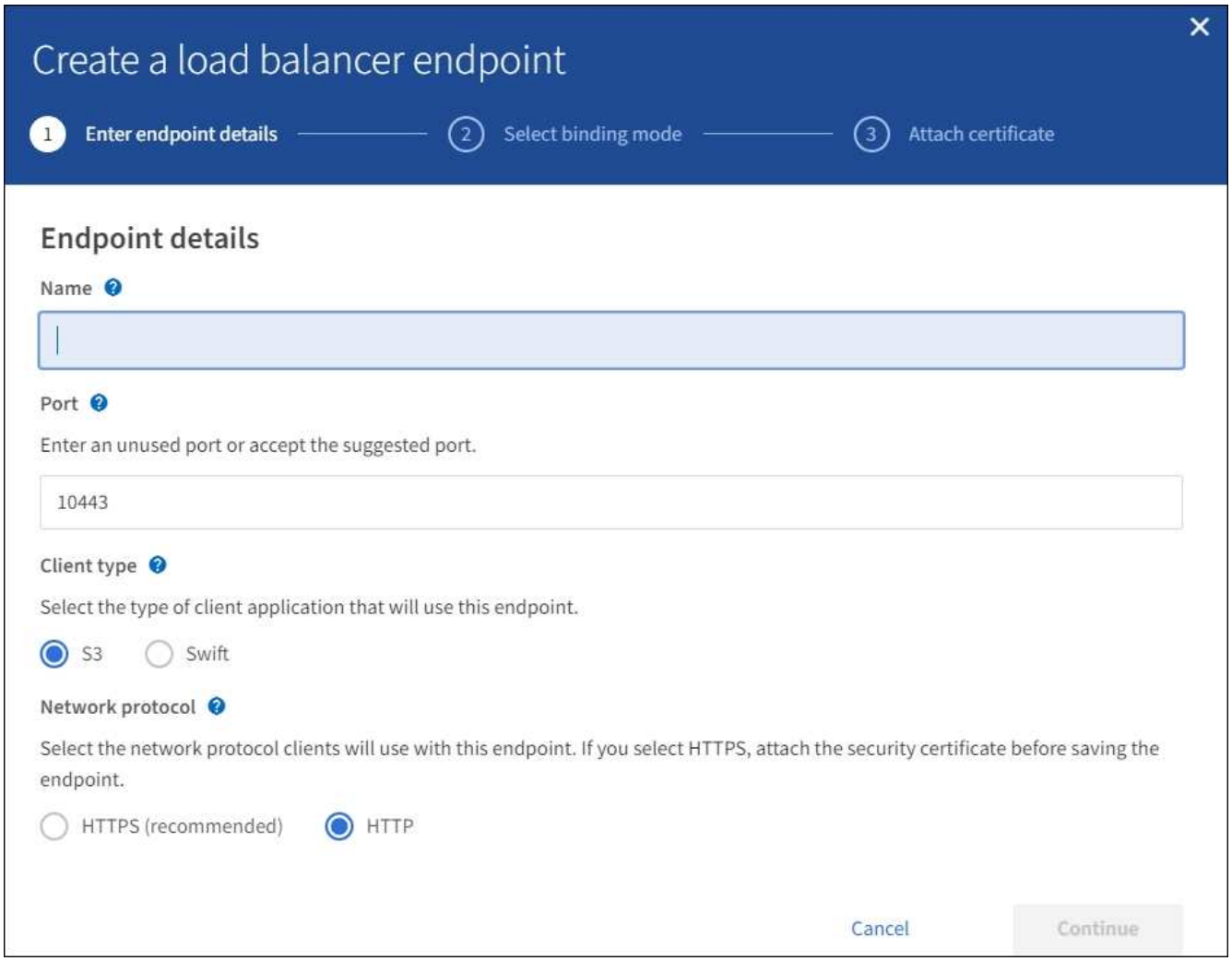
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。
- 您具有以下文件：
  - Server Certificate ： 自定义服务器证书文件。
  - 服务器证书专用密钥：自定义服务器证书专用密钥文件。
  - CA Bundle ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

关于此任务

有关此任务的详细信息，请参见 配置负载平衡器端点。

步骤

1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。
2. 选择 * 创建 * 。



3. 输入端点详细信息。

字段	Description
Name	端点的描述性名称
Port	要用于负载平衡的 StorageGRID 端口。此字段默认为 10433 ，但您可以输入任何未使用的外部端口。如果输入 80 或 443 ，则仅会在网关节点上配置端点，因为这些端口是在管理节点上保留的。 • 注： * 不允许使用其他网格服务使用的端口。请参见网络端口参考。 在将 StorageGRID 附加为 FabricPool 云层时，您必须向 ONTAP 提供此相同端口号。
客户端类型	选择 * 。 s3* 。
网络协议	选择 * HTTPS * 。 • 注 * ： 支持使用 * HTTP * ，但不建议使用。

4. 选择 * 继续 * 。
5. 指定绑定模式。

   使用 * 全局 * 设置（建议）或将此端点的可访问性限制为以下选项之一：

   - 特定节点的特定网络接口。
   - 特定高可用性（ High Availability ， HA ）虚拟 IP 地址（ VIP ）。只有在需要更高级别的工作负载隔离时，才使用此选项。
6. 选择 * 继续 * 。
7. 选择 * 上传证书 * （建议），然后浏览到您的服务器证书，证书专用密钥和可选的 CA 捆绑包。
8. 选择 * 创建 * 。

   对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

为 **FabricPool** 创建租户帐户

您必须在网格管理器中创建一个租户帐户以供 FabricPool 使用。

您需要的内容

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

关于此任务

租户帐户允许客户端应用程序在 StorageGRID 上存储和检索对象。每个租户帐户都有自己的帐户 ID ，授权组和用户，分段和对象。

您可以对多个 ONTAP 集群使用相同的租户帐户。或者，您也可以根据需要为每个 ONTAP 集群创建一个专用租户帐户。

以下说明假定您已为网格管理器配置单点登录（ Single Sign-On ， SSO ）。如果未启用 SSO ，请使用 有关创建租户帐户的说明 而是。

步骤

1. 选择 * 租户 * 。
2. 选择 * 创建 * 。
3. 输入显示名称和问题描述 。
4. 选择 * 。 s3* 。
5. 将 * 存储配额 * 字段留空。
6. 选择 * 允许平台服务 * 可启用平台服务的使用。

   如果启用了平台服务，则租户可以使用 CloudMirror 复制等功能来访问外部服务。

7. 请勿选择 * 使用自己的身份源 * 。
8. 请勿选择 * 允许 S3 选择 * 。

9. 从网格管理器中选择一个现有联合组，以获得租户的初始根访问权限。
10. 选择 * 创建租户 * 。

创建 **S3** 存储分段并获取访问密钥

在将 StorageGRID 与 FabricPool 工作负载结合使用之前，您必须为 FabricPool 数据创建一个 S3 存储分段。您还需要为要用于 FabricPool 的租户帐户获取访问密钥和机密访问密钥。

您需要的内容

- 您已创建一个租户帐户供 FabricPool 使用。

关于此任务

以下说明介绍如何使用 StorageGRID 租户管理器创建存储分段并获取访问密钥。您也可以使用租户管理 API 或 StorageGRID S3 REST API 执行这些任务。或者，如果您使用的是 ONTAP 9.10 ，则可以改用 FabricPool 设置向导创建存储分段。

了解更多信息：

- 使用租户帐户
- 使用 S3

步骤

1. 登录到租户管理器。

   您可以执行以下任一操作：

   - 从网格管理器的租户帐户页面中，选择此租户的 * 登录 * 链接，然后输入您的凭据。
   - 在 Web 浏览器中输入租户帐户的 URL ，然后输入凭据。

2. 为 FabricPool 数据创建 S3 存储分段。

   您必须为计划使用的每个 ONTAP 集群创建一个唯一的存储分段。

   a. 选择 * 存储（ S3 ） * > * 分段 * 。
   b. 选择 * 创建存储分段 * 。
   c. 输入要与 FabricPool 结合使用的 StorageGRID 存储分段的名称。例如， `fabricpool-bucket` 。

      创建存储分段后，您无法更改存储分段名称。

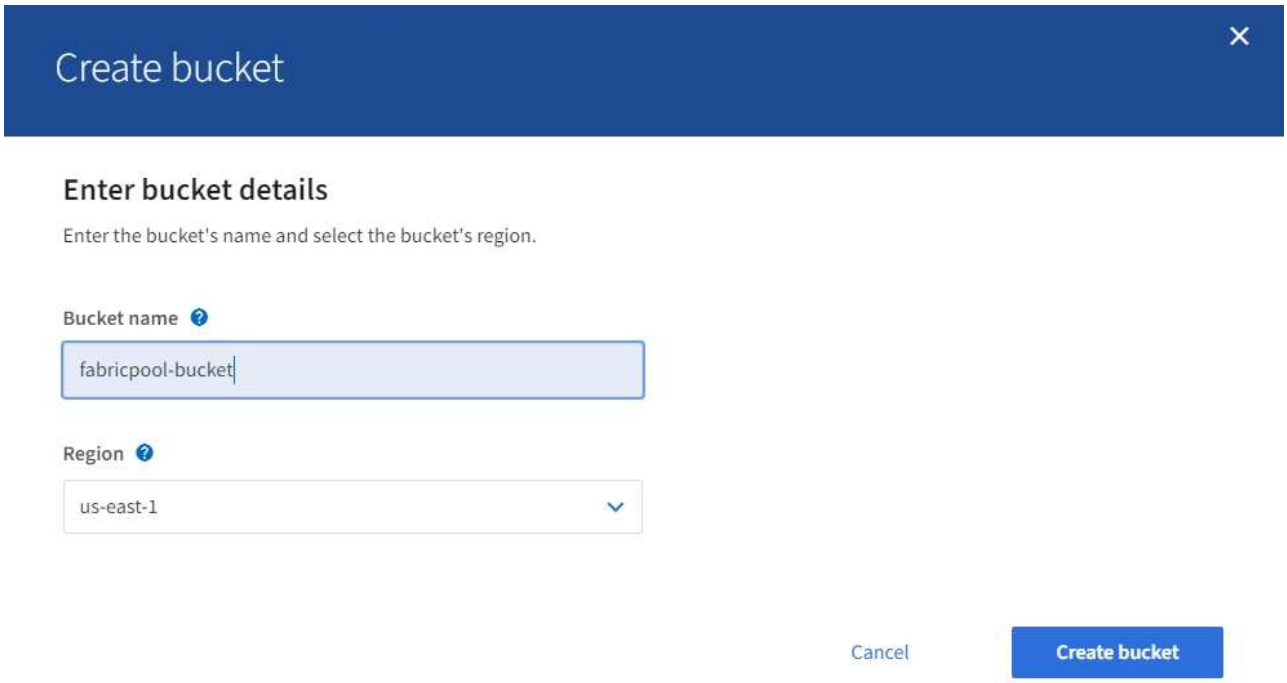
      存储分段名称必须符合以下规则：

      - 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。
      - 必须符合 DNS 要求。
      - 必须至少包含 3 个字符，并且不能超过 63 个字符。
      - 可以是一个或多个标签的序列，并使用一个句点分隔相邻标签。每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。

- 不能与文本格式的 IP 地址类似。
- 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。

d. 为此存储分段选择区域。

默认情况下，所有分段都在 `us-east-1` 区域创建。



e. 选择 * 创建存储分段 * 。

> 对于FabricPool 存储分段、建议的存储分段一致性级别为*读取-后-新-写入*、这是新存储分段的默认设置。请勿将FabricPool 分段编辑为使用*可用*或任何其他一致性级别。

3. 创建访问密钥和机密访问密钥。

a. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

b. 选择 * 创建密钥 * 。

c. 选择 * 创建访问密钥 * 。

d. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

将 StorageGRID 配置为 FabricPool 云层时，您将在 ONTAP 中输入这些值。

> 如果您将来创建新的访问密钥和机密访问密钥，请务必立即更新 ONTAP 中的相应值，以确保 ONTAP 可以在 StorageGRID 中存储和检索数据，而不会造成中断。

将 **StorageGRID** 信息生命周期管理与 **FabricPool** 数据结合使用

如果您使用 FabricPool 将数据分层到 StorageGRID ，则必须了解创建 StorageGRID 信息

生命周期管理（ ILM ）规则和用于管理 FabricPool 数据的 ILM 策略的要求。您必须确保适用于 FabricPool 数据的 ILM 规则不会造成中断。

FabricPool 不了解 StorageGRID ILM 规则或策略。如果 StorageGRID ILM 策略配置不当，可能会发生数据丢失。请参见 使用 ILM 管理对象 有关详细的 ILM 说明。

请查看这些准则，以确保您的 ILM 规则和 ILM 策略适合 FabricPool 数据和业务要求。如果您已经在使用 StorageGRID ILM ，则可能需要更新活动的 ILM 策略以满足这些准则。

- 您可以使用复制和纠删编码规则的任意组合来保护云层数据。

  建议的最佳实践是，在站点内使用 2+1 纠删编码，以实现经济高效的数据保护。纠删编码使用的 CPU 较多，但提供的存储容量明显低于复制。4+1 和 6+1 方案使用的容量小于 2+1 方案。但是，如果您需要在网格扩展期间添加存储节点， 4+1 和 6+1 方案的灵活性将会降低。有关详细信息，请参见 为经过纠删编码的对象添加存储容量。

- 应用于 FabricPool 数据的每个规则都必须使用纠删编码，或者必须至少创建两个复制副本。

  如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

- 请勿使用将使 FabricPool 云层数据过期或删除的 ILM 规则。将每个 ILM 规则中的保留期限设置为 " 永久 " ，以确保 StorageGRID ILM 不会删除 FabricPool 对象。
- 请勿创建将 FabricPool 云层数据从存储分段移至其他位置的规则。您不能使用 ILM 规则使用归档节点将 FabricPool 数据归档到磁带，也不能使用云存储池将 FabricPool 数据移动到其他对象存储。

  不支持将云存储池与 FabricPool 结合使用，因为从云存储池目标检索对象会增加延迟。

- 从 ONTAP 9.8 开始，您可以选择创建对象标记来帮助对分层数据进行分类和排序，以便于管理。例如，您只能在连接到 StorageGRID 的 FabricPool 卷上设置标记。然后，在 StorageGRID 中创建 ILM 规则时，您可以使用对象标记高级筛选器选择并放置此数据。

FabricPool 数据的 **ILM** 策略示例

使用此简单的示例策略作为您自己的 ILM 规则和策略的起点。

本示例假设您正在为一个 StorageGRID 系统设计 ILM 规则和 ILM 策略，该系统在科罗拉多州丹佛的一个数据中心内有四个存储节点。此示例中的 FabricPool 数据使用名为 `fabricpool-bucket` 的存储分段。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前，请模拟建议的策略，以确认它将按预期工作，以防止内容丢失。要了解更多信息，请参见 使用 ILM 管理对象。

步骤

1. 创建一个名为 * 的存储池 * 。选择丹佛站点。
2. 创建一个名为 **2** 加 **1** 的擦除编码配置文件。选择 2+1 纠删编码方案和 * DEN* 存储池。
3. 创建仅适用于 `fabricpool-bucket` 中数据的 ILM 规则。此示例规则用于创建经过擦除编码的副本。

规则定义	示例值
规则名称	2 加上 1 个用于 FabricPool 数据的纠删编码
Bucket Name	`fabricpool-bucket` 您也可以筛选 FabricPool 租户帐户。
高级筛选	对象大小（ MB ）大于 0.2 MB 。 • 注： * FabricPool 仅写入 4 MB 对象，但您必须添加对象大小筛选器，因为此规则使用纠删编码。
参考时间	载入时间
放置	从 Day 0 存储永久存储
Type	已进行纠删编码
位置	DEN （ 2 加 1 ）
载入行为	平衡

4. 创建一个 ILM 规则，以便为第一个规则不匹配的任何对象创建两个复制副本。请勿选择基本筛选器（租户帐户或存储分段名称）或任何高级筛选器。

规则定义	示例值
规则名称	两个复制副本
Bucket Name	无 _
高级筛选	无 _
参考时间	载入时间
放置	从 Day 0 存储永久存储
Type	已复制
位置	DEN
副本	2.

规则定义	示例值
载入行为	平衡

5. 创建建议的 ILM 策略并选择两个规则。由于复制规则不使用任何筛选器，因此它可以是策略的默认（最后）规则。
6. 将测试对象载入网格。
7. 使用测试对象模拟策略以验证此行为。
8. 激活策略。

激活此策略后， StorageGRID 将按如下所示放置对象数据：

- 从 `fabricpool-bucket` 中的 FabricPool 分层的数据将使用 2+1 纠删编码方案进行纠删编码。两个数据片段和一个奇偶校验片段将放置在三个不同的存储节点上。
- 所有其他分段中的所有对象都将被复制。将创建两个副本并将其放置在两个不同的存储节点上。
- 经过纠删编码的副本和复制的副本将保留在 StorageGRID 中，直到 S3 客户端将其删除为止。StorageGRID ILM 不会删除这些项目。

为 FabricPool 创建流量分类策略

您可以选择设计 StorageGRID 流量分类策略，以优化 FabricPool 工作负载的服务质量。

您需要的内容

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

关于此任务

为 FabricPool 创建流量分类策略的最佳实践取决于工作负载，如下所示：

- 如果您计划将 FabricPool 主工作负载数据分层到 StorageGRID ，则应确保 FabricPool 工作负载具有大部分带宽。您可以创建流量分类策略来限制所有其他工作负载。

  一般来说， FabricPool 读取操作比写入操作更重要。

  例如，如果其他 S3 客户端使用此 StorageGRID 系统，则应创建流量分类策略。您可以限制其他分段，租户， IP 子网或负载平衡器端点的网络流量。

- 通常，您不应对任何 FabricPool 工作负载实施服务质量限制；您只应限制其他工作负载。
- 对其他工作负载的限制应考虑这些工作负载的行为。根据网格的规模估算和功能以及预期利用率，施加的限制也会有所不同。

了解更多信息： 管理流量分类策略

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

2. 输入名称和问题描述 。
3. 在匹配规则部分中，至少创建一个规则。
   a. 选择 * 创建 * 。
   b. 选择 * 端点 * ，然后选择为 FabricPool 创建的负载平衡器端点。

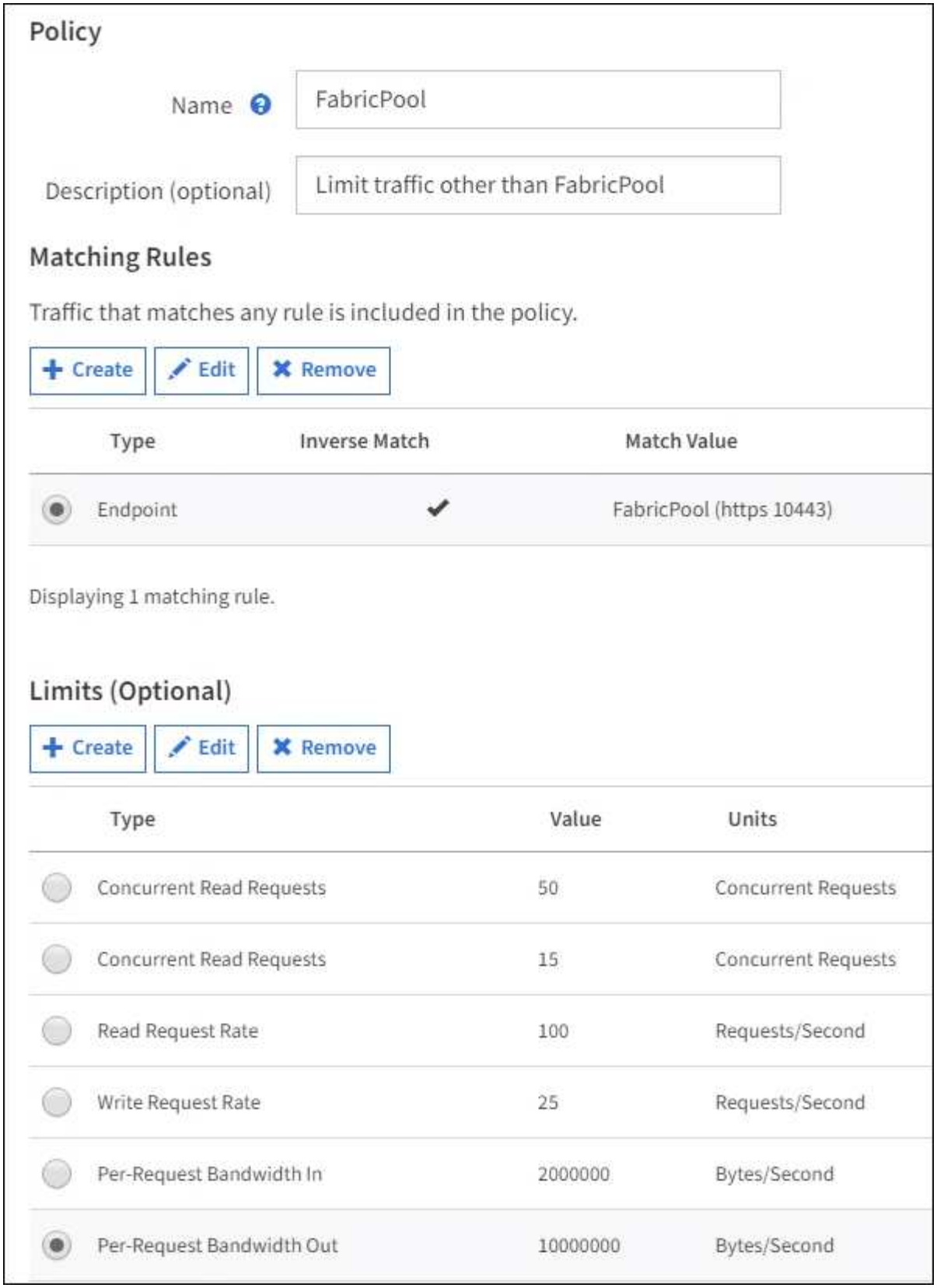
      您也可以选择 FabricPool 租户帐户或存储分段。

   c. 如果希望此流量策略限制其他端点的流量，请选择 * 反向匹配 * 。
4. 或者，也可以创建一个或多个限制。

   即使没有为流量分类策略设置限制，也会收集指标，以便您了解流量趋势。

   a. 选择 * 创建 * 。
   b. 选择要限制的流量类型以及要应用的限制。

      此示例 FabricPool 流量分类策略显示了可以限制的网络流量类型以及可以选择的值类型。实际策略的限制取决于您的特定要求。



5. 创建流量分类策略后，选择该策略，然后选择 * 指标 * 以确定该策略是否按预期限制流量。

StorageGRID 和 FabricPool 的其他最佳实践

在配置要与 FabricPool 结合使用的 StorageGRID 系统时，应避免设置可能影响数据保存方式的全局选项。

对象加密

配置 StorageGRID 时，如果其他 StorageGRID 客户端需要数据加密，您可以选择启用全局 * 存储对象加密 * 设置（ * 配置 * > * 系统 * > * 网格选项 * ）。从 FabricPool 分层到 StorageGRID 的数据已加密，因此不需要启用 StorageGRID 设置。客户端加密密钥归 ONTAP 所有。

对象压缩

配置 StorageGRID 时，请勿启用全局 * 压缩存储的对象 * 设置（ * 配置 * > * 系统 * > * 网格选项 * ）。已对从 FabricPool 分层到 StorageGRID 的数据进行压缩。启用 * 压缩存储的对象 * 不会进一步减小对象的大小。

一致性级别

对于FabricPool 存储分段、建议的存储分段一致性级别为*读取-后-新-写入*、这是新存储分段的默认设置。请勿将FabricPool 分段编辑为使用*可用*或任何其他一致性级别。

FabricPool 分层

如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。例如，如果 StorageGRID 节点正在 VMware 主机上运行，请确保为 StorageGRID 节点的数据存储库提供支持的卷未启用 FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

使用 StorageGRID

使用租户帐户

使用租户帐户：概述

租户帐户允许您使用简单存储服务（ S3 ） REST API 或 Swift REST API 在 StorageGRID 系统中存储和检索对象。

什么是租户帐户？

每个租户帐户都有自己的联合或本地组，用户， S3 分段或 Swift 容器以及对象。

也可以使用租户帐户按不同的实体隔离存储的对象。例如，以下任一使用情形均可使用多个租户帐户：

- * 企业用例： * 如果在企业中使用 StorageGRID 系统，则网格的对象存储可能会被组织中的不同部门隔离。例如，可能存在营销部门，客户支持部门，人力资源部门等的租户帐户。

  > 如果使用 S3 客户端协议，则还可以使用 S3 分段和分段策略在企业中的各个部门之间隔离对象。您无需创建单独的租户帐户。请参见 有关实施 S3 客户端应用程序的说明。

- * 服务提供商用例： * 如果服务提供商正在使用 StorageGRID 系统，则网格的对象存储可能会被租用该存储的不同实体分隔。例如，可能存在公司 A ，公司 B ，公司 C 等的租户帐户。

如何创建租户帐户

租户帐户由创建 使用网格管理器的 StorageGRID 网格管理员。创建租户帐户时，网格管理员会指定以下信息：

- 租户的显示名称（租户的帐户 ID 会自动分配，不能更改）。
- 租户帐户是使用 S3 还是 Swift 。
- 对于 S3 租户帐户：是否允许租户帐户使用平台服务。如果允许使用平台服务，则必须对网格进行配置，以支持使用这些服务。
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。
- 如果为 StorageGRID 系统启用了身份联合，则哪个联合组具有 " 根访问 " 权限来配置租户帐户。
- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。

此外，如果 S3 租户帐户需要符合法规要求，网格管理员可以为 StorageGRID 系统启用 S3 对象锁定设置。启用 S3 对象锁定后，所有 S3 租户帐户均可创建和管理合规的存储分段。

配置 **S3** 租户

在之后 已创建 S3 租户帐户，您可以访问租户管理器以执行以下任务：

- 设置身份联合（除非身份源与网格共享）或创建本地组和用户

- 管理 S3 访问密钥
- 创建和管理 S3 存储分段，包括合规存储分段
- 使用平台服务（如果已启用）
- 监控存储使用情况

> 虽然您可以使用租户管理器创建和管理 S3 存储分段，但您必须具有 S3 访问密钥，并使用 S3 REST API 载入和管理对象。

配置 **Swift** 租户

在 A 之后 已创建 Swift 租户帐户，您可以访问租户管理器以执行以下任务：

- 设置身份联合（除非身份源与网格共享），并创建本地组和用户
- 监控存储使用情况

> Swift 用户必须具有 root 访问权限才能访问租户管理器。但是，" 根访问 " 权限不允许用户在中进行身份验证 Swift REST API 创建容器和载入对象。用户必须具有 Swift 管理员权限才能向 Swift REST API 进行身份验证。

使用租户管理器

租户管理器允许您管理 StorageGRID 租户帐户的所有方面。

您可以使用租户管理器监控租户帐户的存储使用情况，并通过身份联合或创建本地组和用户来管理用户。对于 S3 租户帐户，您还可以管理 S3 密钥，管理 S3 存储分段以及配置平台服务。

如何登录和注销

登录到租户管理器

您可以通过在的地址栏中输入租户的 URL 来访问租户管理器 支持的 Web 浏览器。

您需要的内容

- 您必须拥有登录凭据。
- 您必须具有网格管理员提供的用于访问租户管理器的 URL 。URL 将类似于以下示例之一：

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

此 URL 始终包含用于访问管理节点的完全限定域名（ FQDN ）或 IP 地址，也可以包括端口号， 20 位租户帐户 ID 或这两者。

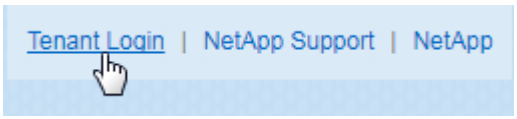
- 如果 URL 不包含租户的 20 位帐户 ID ，则必须具有此帐户 ID 。
- 您必须使用 支持的 Web 浏览器。
- 必须在 Web 浏览器中启用 Cookie 。
- 您必须具有特定的访问权限。

步骤

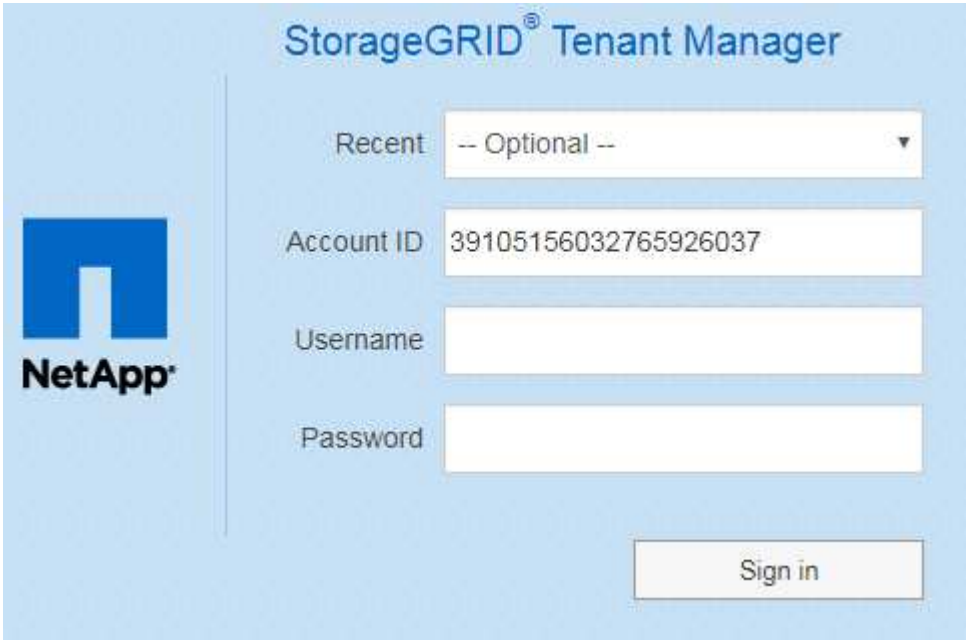
1. 启动 支持的 Web 浏览器。
2. 在浏览器的地址栏中，输入用于访问租户管理器的 URL 。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。
4. 登录到租户管理器。

   您看到的登录屏幕取决于您输入的 URL 以及您的组织是否使用单点登录（ SSO ）。您将看到以下屏幕之一：

   - 网格管理器登录页面。单击右上角的 * 租户登录 * 链接。

   - 租户管理器登录页面。* 帐户 ID* 字段可能已完成，如下所示。

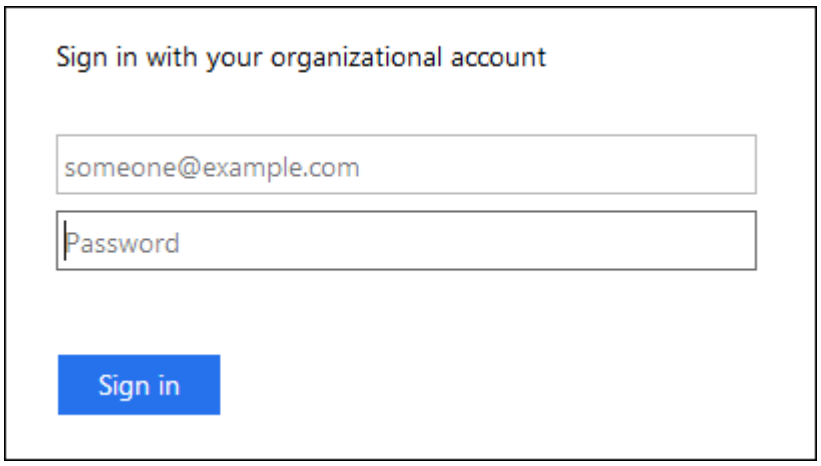
     i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。

ii. 输入用户名和密码。

iii. 单击 * 登录 * 。

此时将显示租户管理器信息板。

- 如果在网格上启用了 SSO ，则为您所在组织的 SSO 页面。例如：



输入标准 SSO 凭据，然后单击 * 登录 * 。

- 租户管理器 SSO 登录页面。

i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。

ii. 单击 * 登录 * 。

iii. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。

此时将显示租户管理器信息板。

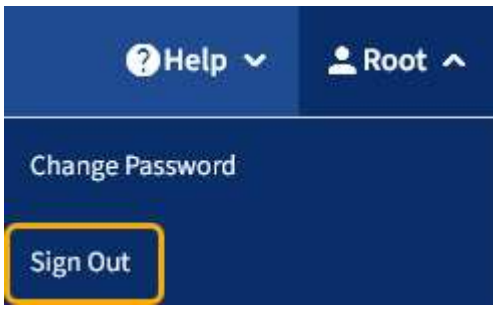
5. 如果您从其他人收到初始密码，请更改密码以保护您的帐户。选择 * 。 username_* > * 更改密码 * 。

如果为 StorageGRID 系统启用了 SSO ，则无法从租户管理器更改密码。

使用租户管理器后，您必须注销以确保未经授权的用户无法访问 StorageGRID 系统。根据浏览器 Cookie 设置，关闭浏览器可能无法将您从系统中注销。

步骤

1. 找到用户界面右上角的用户名下拉列表。



2. 选择用户名，然后选择 * 注销 * 。

   - 如果未使用 SSO：

     您已从管理节点注销。此时将显示租户管理器登录页面。

     如果您已登录到多个管理节点，则必须从每个节点注销。

   - 如果启用了 SSO：

     您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。您刚刚访问的租户帐户的名称将在 * 近期帐户 * 下拉列表中列为默认名称，并显示租户的 * 帐户 ID* 。

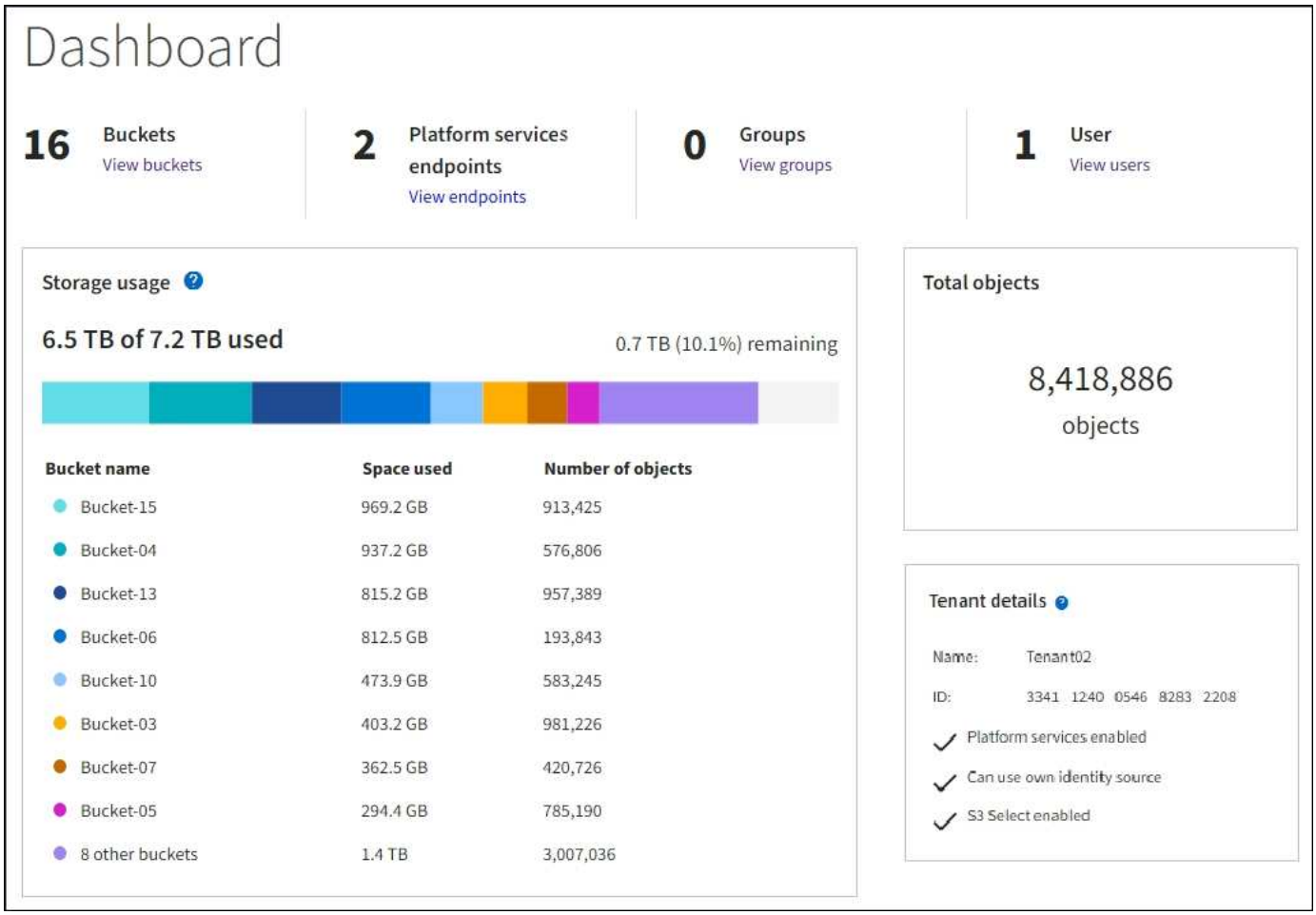
如果启用了 SSO ，并且您还登录到网格管理器，则还必须注销网格管理器才能注销 SSO 。

了解租户管理器信息板

租户管理器信息板概述了租户帐户的配置以及租户分段（ S3 ）或容器（ Swift ）中的对象所使用的空间量。如果租户有配额，信息板将显示配额的已用量和剩余量。如果存在与租户帐户相关的任何错误，则这些错误将显示在信息板上。

" 已用空间 " 值是估计值。这些估计值受载入时间，网络连接和节点状态的影响。

上传对象后，信息板类似于以下示例：



租户帐户摘要

信息板顶部包含以下信息：

- 已配置的分段或容器，组和用户的数量
- 已配置的平台服务端点数量（如果有）

您可以选择这些链接来查看详细信息。

信息板右侧包含以下信息：

- 租户的对象总数。

  对于 S3 帐户，如果尚未载入任何对象，并且您具有 root 访问权限，则会显示入门准则，而不是对象总数。

- 租户详细信息，包括租户帐户名称和 ID 以及租户是否可以使用 平台服务， 自己的身份源或 S3 Select （仅列出已启用的权限）。

存储和配额使用量

存储使用情况面板包含以下信息：

- 租户的对象数据量。

此值表示已上传的对象数据总量，不表示用于存储这些对象及其元数据副本的空间。

- 如果设置了配额，则表示可用于对象数据的总空间量以及剩余空间量和百分比。配额限制了可载入的对象数据量。

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

- 一个条形图，表示最大分段或容器的相对大小。

  您可以将光标置于任何图表区块上方，以查看该分段或容器占用的总空间。

- 要与条形图相对应，需要列出最大的分段或容器，包括对象数据总量以及每个分段或容器的对象数量。

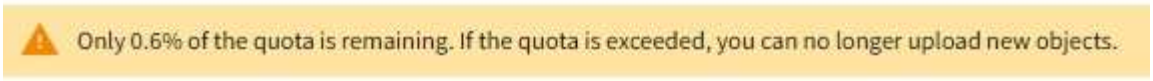
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

如果租户具有九个以上的分段或容器，则所有其他分段或容器将合并到列表底部的一个条目中。

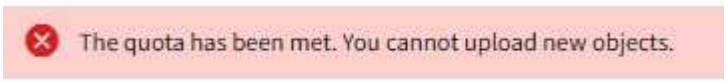
配额使用情况警报

如果已在网格管理器中启用配额使用情况警报，则在配额不足或超过配额时，这些警报将显示在租户管理器中，如下所示：

如果已使用租户配额的 90% 或更多，则会触发 * 租户配额使用量高 * 警报。有关详细信息，请参见 StorageGRID 监控和故障排除说明中的警报参考。



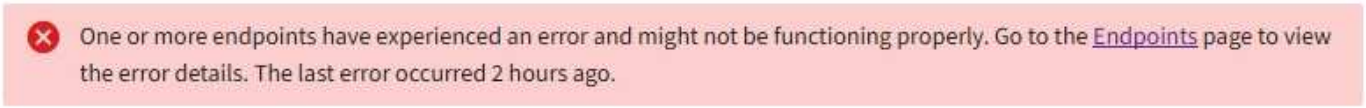
如果超过配额，则无法上传新对象。



要查看其他详细信息以及管理警报规则和通知，请参见有关监控 StorageGRID 和对其进行故障排除的说明。

端点错误

如果您已使用网格管理器配置一个或多个端点以用于平台服务，则如果在过去七天内发生任何端点错误，则租户管理器信息板将显示警报。



要查看有关端点错误的详细信息，请选择端点以显示端点页面。

相关信息

解决平台服务端点错误

监控和故障排除

租户管理 API

了解租户管理 API

您可以使用租户管理 REST API 执行系统管理任务，而不是使用租户管理器用户界面。例如，您可能希望使用 API 来自动执行操作或更快地创建多个实体，例如用户。

租户管理 API：

- 使用 Swagger 开源 API 平台。Swagger 提供了一个直观的用户界面，支持开发人员和非开发人员与 API 进行交互。Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。
- 用途 版本控制以支持无中断升级。

要访问租户管理 API 的 Swagger 文档，请执行以下操作：

步骤

1. 登录到租户管理器。
2. 从租户管理器顶部，选择帮助图标并选择 * API Documentation" 。

API 操作

租户管理 API 将可用的 API 操作组织到以下部分中：

- * 帐户 * - 对当前租户帐户执行的操作，包括获取存储使用情况信息。
- * 身份验证 * —执行用户会话身份验证的操作。

  租户管理 API 支持不承载令牌身份验证方案。对于租户登录，您可以在身份验证请求的 JSON 正文中提供用户名，密码和帐户 ID （即 `post /apI/v3/authorize` ）。如果用户已成功通过身份验证，则会返回一个安全令牌。此令牌必须在后续 API 请求的标题中提供（ " 授权：承载令牌 " ）。

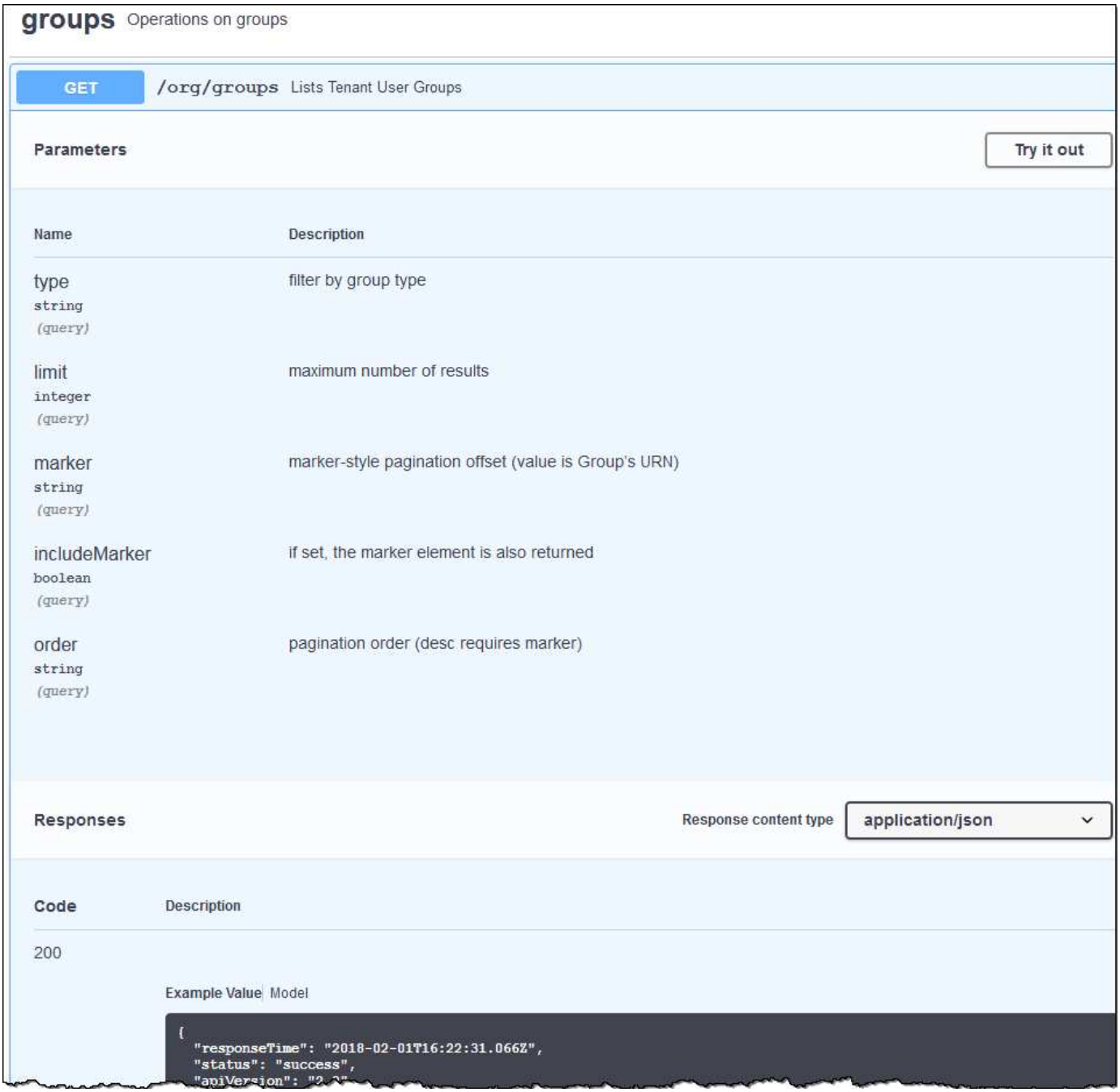
  有关提高身份验证安全性的信息，请参见 防止跨站点请求伪造。

  > 如果为 StorageGRID 系统启用了单点登录（ SSO ），则必须执行不同的步骤进行身份验证。请参见 有关使用网格管理 API 的说明。

- **config** —与租户管理 API 的产品版本和版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- * 容器 * —对 S3 存储分段或 Swift 容器执行的操作如下：
- S3
  - 创建存储分段（启用和不启用 S3 对象锁定）
  - 修改存储分段默认保留（适用于启用了 S3 对象锁定的存储分段）
  - 为对对象执行的操作设置一致性控制
  - 创建，更新和删除存储分段的 CORS 配置
  - 启用和禁用对象的上次访问时间更新
  - 管理平台服务的配置设置，包括 CloudMirror 复制，通知和搜索集成（元数据通知）
  - 删除空分段
- Swift* ： 设置用于容器的一致性级别
- "*deactived-features * - 用于查看可能已停用的功能的操作 " 。
- * 端点 * —用于管理端点的操作。通过端点， S3 存储分段可以使用外部服务进行 StorageGRID CloudMirror 复制，通知或搜索集成。
- * 组 * —用于管理本地租户组和从外部身份源检索联合租户组的操作。
- **identity-source** —用于配置外部身份源以及手动同步联合组和用户信息的操作。
- * 区域 * - 用于确定已为 StorageGRID 系统配置哪些区域的操作。
- * S3 * —用于管理租户用户 S3 访问密钥的操作。
- * s3-object-lock* - 对全局 S3 对象锁定设置执行操作，用于支持合规性。
- * 用户 * —用于查看和管理租户用户的操作。

操作详细信息

展开每个 API 操作时，您可以看到其 HTTP 操作，端点 URL ，任何必需或可选参数的列表，请求正文示例（如果需要）以及可能的响应。



问题描述 **API** 请求

使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

步骤

1. 选择 HTTP 操作以查看请求详细信息。
2. 确定此请求是否需要其他参数，例如组或用户 ID 。然后，获取这些值。您可能需要先对其他 API 请求进行问题描述 处理，以获取所需的信息。
3. 确定是否需要修改示例请求正文。如果是，您可以选择 * 型号 * 来了解每个字段的要求。
4. 选择 * 试用 * 。

5. 提供所需的任何参数，或根据需要修改请求正文。
6. 选择 * 执行 * 。
7. 查看响应代码以确定请求是否成功。

租户管理 API 版本控制

租户管理 API 使用版本控制来支持无中断升级。

例如，此请求 URL 指定 API 版本 3 。

```
https://hostname_or_ip_address/api/v3/authorize
```

如果对旧版本进行了 * 不兼容 _* 的更改，则租户管理 API 的主要版本将发生递增。如果对 * 与旧版本兼容 _* 进行了更改，则租户管理 API 的次要版本将发生递增。兼容的更改包括添加新端点或新属性。以下示例说明了如何根据所做更改的类型对 API 版本进行递增。

API 的更改类型	旧版本	新版本
与旧版本兼容	2.1	2.2
与旧版本不兼容	2.1	3.0

首次安装 StorageGRID 软件时，仅会启用最新版本的租户管理 API 。但是，在将 StorageGRID 升级到新功能版本后，您仍可访问至少一个 StorageGRID 功能版本的旧版 API 。

已过时的请求将通过以下方式标记为已弃用：

- 响应标头为 "depression: true"
- JSON 响应正文包含 "depressioned" ： true

确定当前版本支持哪些 API 版本

请使用以下 API 请求返回受支持的 API 主要版本列表：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

指定请求的 API 版本

您可以使用路径参数（` API/v3` ）或标头（`API-Version ： 3`）指定 API 版本。如果同时提供这两个值，则标头值将覆盖路径值。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

防止跨站点请求伪造（ CSRF ）

您可以通过使用 CSRF 令牌增强使用 Cookie 的身份验证，帮助防止 StorageGRID 受到跨站点请求伪造（ CSRF ）攻击。网格管理器和租户管理器会自动启用此安全功能；其他 API 客户端可以选择在登录时是否启用此功能。

如果攻击者可能触发对其他站点的请求（例如使用 HTTP 表单发布），则可以对使用已登录用户的 cookie 发出的某些请求进行发生原因 处理。

StorageGRID 可通过使用 CSRF 令牌帮助防止 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标题或特定后处理正文参数的内容匹配。

要启用此功能，请在身份验证期间将 `csrfToken` 参数设置为 `true` 。默认值为 `false` 。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果为 true ，则使用随机值为 `GridCsrfToken` cookie 设置网格管理器登录，并使用随机值为 `AccountCsrfToken` cookie 设置为登录租户管理器。

如果存在 Cookie ，则可以修改系统状态的所有请求（ POST ， PUT ， patch ， delete ）都必须包括以下项之一：

- `X-CSRF-Token` 标头，标头的值设置为 CSRF 令牌 cookie 的值。
- 对于接受表单编码正文的端点： a `csrfToken` form-enc编码 请求正文参数。

要配置 CSRF 保护，请使用 网格管理 API 或 租户管理 API。

> 设置了 CSRF 令牌 cookie 的请求还会对任何希望 JSON 请求正文作为额外保护来抵御 CSRF 攻击的请求强制使用 ` "Content-Type ： application/json"` 标头。

管理系统访问

使用身份联合

使用身份联合可以加快租户组和用户的设置速度，并允许租户用户使用熟悉的凭据登录到租户帐户。

为租户管理器配置身份联合

如果您希望在 Active Directory ， Azure Active Directory （ Azure AD ） ， OpenLDAP 或 Oracle Directory Server 等其他系统中管理租户组和用户，则可以为租户管理器配置身份联合。

您需要的内容

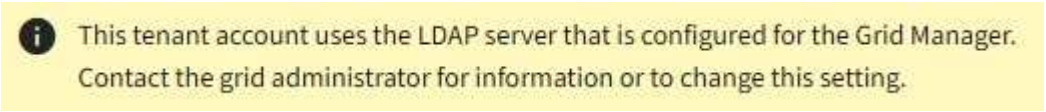
- 您将使用登录到租户管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。
- 您正在使用 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  如果要使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参见 配置 OpenLDAP 服务器的准则。
- 如果您计划使用传输层安全（ Transport Layer Security ， TLS ）与 LDAP 服务器进行通信，则身份提供程序必须使用 TLS 1.2 或 1.3 。请参见 支持传出 TLS 连接的密码。

关于此任务

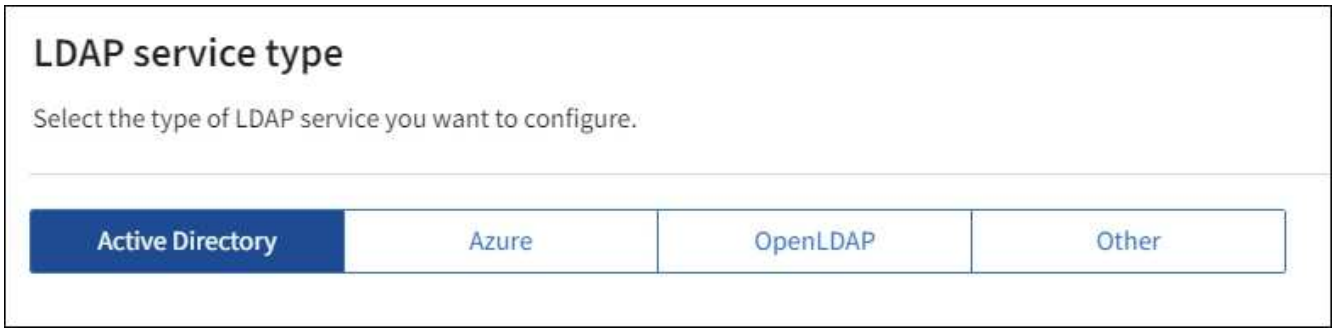
是否可以为租户配置身份联合服务取决于租户帐户的设置方式。您的租户可能会共享为网格管理器配置的身份联合服务。如果您在访问身份联合页面时看到此消息，则无法为此租户配置单独的联合身份源。



进入配置

步骤

1. 选择 * 访问管理 * > * 身份联合 * 。
2. 选择 * 启用身份联合 * 。
3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - * 用户唯一名称 * ： 包含 LDAP 用户唯一标识符的属性的名称。此属性相当于 `sAMAccountName` 用于 Active Directory ， `uid` 用于 OpenLDAP 。如果要配置 Oracle Directory Server ，请输入 `uid` 。
   - * 用户 UID* ： 包含 LDAP 用户的永久唯一标识符的属性的名称。此属性等效于 Active Directory 的 `objectGUID` 和 OpenLDAP 的 `entryUUID` 。如果要配置 Oracle Directory Server ，请输入 `nssuniqueid` 。每个用户在指定属性中的值都必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
   - * 组唯一名称 * ： 包含 LDAP 组唯一标识符的属性的名称。对于 Active Directory ，此属性相当于 `sAMAccountName` ；对于 OpenLDAP ，此属性相当于 `CN` 。如果要配置 Oracle Directory Server ，请输入 `CN` 。
   - * 组 UID* ： 包含 LDAP 组的永久唯一标识符的属性的名称。此属性等效于 Active Directory 的 `objectGUID` 和 OpenLDAP 的 `entryUUID` 。如果要配置 Oracle Directory Server ，请输入 `nssuniqueid` 。每个组在指定属性中的值必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
5. 对于所有 LDAP 服务类型，请在配置 LDAP 服务器部分中输入所需的 LDAP 服务器和网络连接信息。
   - * 主机名 * ： LDAP 服务器的完全限定域名（ FQDN ）或 IP 地址。
   - * 端口 * ： 用于连接到 LDAP 服务器的端口。

     STARTTLS 的默认端口为 389 ， LDAPS 的默认端口为 636 。但是，只要防火墙配置正确，您就可以使用任何端口。

   - * 用户名 * ： 要连接到 LDAP 服务器的用户的可分辨名称（ DN ）的完整路径。

     对于 Active Directory ，您还可以指定低级别的登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

     - `sAMAccountName` 或 `uid`
     - `objectGUID` ， `entryUUID` 或 `nssuniqueid`
     - `CN`
     - `memberOf` 或 `isMemberOf`
     - * Active Directory* ： `objectSid` ， `primaryGroupID` ， `userAccountControl` 和 `userPrincipalName`
     - * Azure * ： `accountEnabled` 和 `userPrincipalName`
   - * 密码 * ： 与用户名关联的密码。
   - * 组基本 DN* ： 要搜索组的 LDAP 子树的可分辨名称（ DN ）的完整路径。在 Active Directory 示例（如下）中，可分辨名称相对于基础 DN （ DC=storagegrid ， DC=example ， DC=com ）的所有组均可用作联合组。

     * 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

   - * 用户基础 DN* ： 要搜索用户的 LDAP 子树的可分辨名称（ DN ）的完整路径。

用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

- * 绑定用户名格式 *（可选）：如果无法自动确定模式， StorageGRID 应使用默认用户名模式。

  建议提供 * 绑定用户名格式 * ，因为如果 StorageGRID 无法绑定到服务帐户，它可以允许用户登录。

  输入以下模式之一：

  - * 用户 PrincipalName 模式（ Active Directory 和 Azure ）*： `` 用户名@*example*.com
  - * 低级登录名称模式（ Active Directory 和 Azure ）*： ` 示例 _\[ 用户名 ]`
  - * 可分辨名称模式 *： `CN=[ 用户名 ] ， CN=Users ， DC=example ， DC=com`

    与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   - * 使用 STARTTLS *：使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是建议的 Active Directory ， OpenLDAP 或其他选项，但 Azure 不支持此选项。
   - * 使用 LDAPS*： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。您必须为 Azure 选择此选项。
   - * 请勿使用 TLS*： StorageGRID 系统与 LDAP 服务器之间的网络流量将不会受到保护。Azure 不支持此选项。

     如果 Active Directory 服务器强制实施 LDAP 签名，则不支持使用 * 不使用 TLS* 选项。您必须使用 STARTTLS 或 LDAPS 。

7. 如果选择 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。
   - * 使用操作系统 CA 证书 *：使用操作系统上安装的默认网格 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 *：使用自定义安全证书。

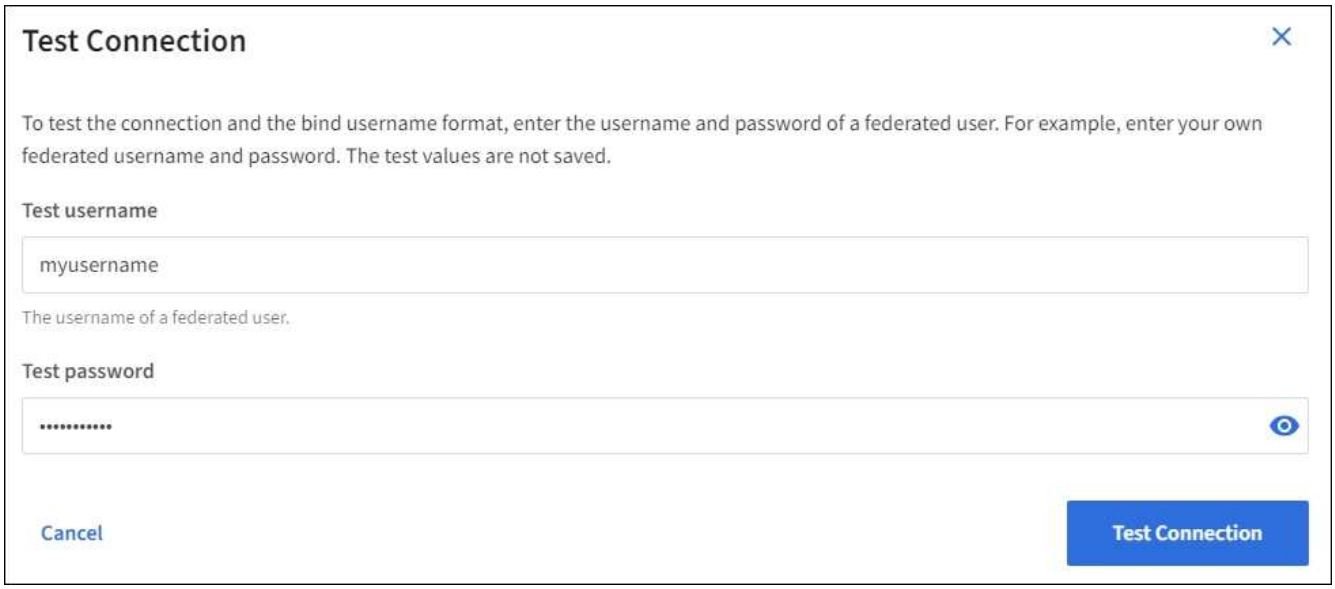
     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

1. 选择 * 测试连接 * 。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效，则会显示 "`test connection could not be established` " 消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

   例如，输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符，例如 @ 或 / 。



- 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
- 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到身份联合页面。
2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以临时或永久禁用组和用户的身份联合。禁用身份联合后， StorageGRID 与身份源之间不会进行通信。但是，您配置的任何设置都将保留下来，以便将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，并且不会为尚未同步的帐户发出警报或警报。
- 如果单点登录（ SSO ）设置为 * 已启用 * 或 * 沙盒模式 * ，则 * 启用身份联合 * 复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 * 已禁用 * 。请参见 禁用单点登录。

步骤

1. 转到身份联合页面。
2. 取消选中 * 启用身份联合 * 复选框。

配置 OpenLDAP 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于非 ActiveDirectory 或 Azure 身份源， StorageGRID 不会自动阻止外部禁用的用户进行 S3 访问。要阻止 S3 访问，请删除该用户的任何 S3 密钥，并从所有组中删除该用户。

memberOf 和 fint 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex ： objectclass` 均衡器
- `olcDbIndex ： UID eq ， pres ， sub`
- `olcDbIndex ： CN eq ， pres ， sub`
- `olcDbIndex ： entryUUID` 均衡器

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

管理组

为 S3 租户创建组

您可以通过导入联合组或创建本地组来管理 S3 用户组的权限。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。请参见 租户管理权限。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

有关 S3 的信息，请参见 使用 S3。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选择 * 创建组 * 。
3. 选择 * 本地组 * 选项卡以创建本地组，或者选择 * 联合组 * 选项卡以从先前配置的身份源导入组。

   如果为 StorageGRID 系统启用了单点登录（ SSO ），则属于本地组的用户将无法登录到租户管理器，但他们可以根据组权限使用客户端应用程序管理租户的资源。

4. 输入组的名称。
   - * 本地组 * ： 输入显示名称和唯一名称。您可以稍后编辑显示名称。
   - * 联合组 * ： 输入唯一名称。对于 Active Directory ，唯一名称是与 `sAMAccountName` 属性关联的名称。对于 OpenLDAP ，唯一名称是与 `uid` 属性关联的名称。
5. 选择 * 继续 * 。
6. 选择访问模式。如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。
   - * 读写 * （默认）： 用户可以登录到租户管理器并管理租户配置。
   - * 只读 * ： 用户只能查看设置和功能。他们不能在租户管理器或租户管理 API 中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。
7. 选择此组的组权限。

   请参见有关租户管理权限的信息。

8. 选择 * 继续 * 。
9. 选择组策略以确定此组的成员将拥有哪些 S3 访问权限。
   - * 无 S3 访问 * ： 默认值。此组中的用户无权访问 S3 资源，除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
   - * 只读访问 * ： 此组中的用户对 S3 资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您不能编辑此字符串。

- * 完全访问 * ： 此组中的用户对 S3 资源（包括分段）具有完全访问权限。选择此选项后，完全访问组策略的 JSON 字符串将显示在文本框中。您不能编辑此字符串。
- * 自定义 * ： 组中的用户将获得您在文本框中指定的权限。有关组策略的详细信息，包括语言语法和示例，请参见实施 S3 客户端应用程序的说明。

10. 如果选择 * 自定义 * ，请输入组策略。每个组策略的大小限制为 5 ， 120 字节。您必须输入有效的 JSON 格式字符串。

    在此示例中，只允许组成员列出和访问指定存储分段中与其用户名（密钥前缀）匹配的文件夹。请注意，在确定其他组策略和存储分段策略的隐私时，应考虑这些文件夹的访问权限。

11. 根据要创建的是联合组还是本地组，选择显示的按钮：

    - 联合组： * 创建组 *
    - 本地组： * 继续 *

    如果要创建本地组，请在选择 * 继续 * 后显示步骤 4 （添加用户）。对于联合组，不会显示此步骤。

12. 选中要添加到组的每个用户对应的复选框，然后选择 * 创建组 * 。

    或者，您也可以在不添加用户的情况下保存组。您可以稍后将用户添加到组中，也可以在添加新用户时选择组。

13. 选择 * 完成 * 。

    您创建的组将显示在组列表中。由于缓存，更改可能需要长达 15 分钟才能生效。

您可以通过导入联合组或创建本地组来管理 Swift 租户帐户的访问权限。至少有一个组必须具有 Swift 管理员权限，这是管理 Swift 租户帐户的容器和对象所必需的。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选择 * 创建组 * 。
3. 选择 * 本地组 * 选项卡以创建本地组，或者选择 * 联合组 * 选项卡以从先前配置的身份源导入组。

   如果为 StorageGRID 系统启用了单点登录（ SSO ），则属于本地组的用户将无法登录到租户管理器，但他们可以根据组权限使用客户端应用程序管理租户的资源。

4. 输入组的名称。
   - * 本地组 * ： 输入显示名称和唯一名称。您可以稍后编辑显示名称。
   - * 联合组 * ： 输入唯一名称。对于 Active Directory ，唯一名称是与 `sAMAccountName` 属性关联的名称。对于 OpenLDAP ，唯一名称是与 `uid` 属性关联的名称。
5. 选择 * 继续 * 。
6. 选择访问模式。如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。
   - * 读写 * （默认）： 用户可以登录到租户管理器并管理租户配置。

- * 只读 * ： 用户只能查看设置和功能。他们不能在租户管理器或租户管理 API 中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

7. 设置组权限。
   - 如果用户需要登录到租户管理器或租户管理 API ，请选中 * 根访问 * 复选框。（默认）
   - 如果用户不需要访问租户管理器或租户管理 API ，请取消选中 * 根访问 * 复选框。例如，取消选中不需要访问租户的应用程序对应的复选框。然后，分配 * Swift 管理员 * 权限，以允许这些用户管理容器和对象。
8. 选择 * 继续 * 。
9. 如果用户需要能够使用 Swift REST API ，请选中 * Swift administrator* 复选框。

   Swift 用户必须具有 root 访问权限才能访问租户管理器。但是， " 根访问 " 权限不允许用户向 Swift REST API 进行身份验证以创建容器和载入对象。用户必须具有 Swift 管理员权限才能向 Swift REST API 进行身份验证。

10. 根据要创建的是联合组还是本地组，选择显示的按钮：
    - 联合组： * 创建组 *
    - 本地组： * 继续 *

      如果要创建本地组，请在选择 * 继续 * 后显示步骤 4 （添加用户）。对于联合组，不会显示此步骤。

11. 选中要添加到组的每个用户对应的复选框，然后选择 * 创建组 * 。

    或者，您也可以在不添加用户的情况下保存组。您可以稍后将用户添加到组中，也可以在创建新用户时选择组。

12. 选择 * 完成 * 。

    您创建的组将显示在组列表中。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

租户管理权限

使用 Swift

租户管理权限

在创建租户组之前，请考虑要分配给该组的权限。租户管理权限用于确定用户可以使用租户管理器或租户管理 API 执行的任务。一个用户可以属于一个或多个组。如果用户属于多个组，则权限是累积的。

要登录到租户管理器或使用租户管理 API ，用户必须属于至少具有一个权限的组。所有可以登录的用户均可执行以下任务：

- 查看信息板
- 更改自己的密码（适用于本地用户）

对于所有权限，组的访问模式设置将确定用户是否可以更改设置并执行操作，或者是否只能查看相关设置和功能。

如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。

您可以为组分配以下权限。请注意， S3 租户和 Swift 租户具有不同的组权限。由于缓存，更改可能需要长达 15 分钟才能生效。

权限	Description
根访问	提供对租户管理器和租户管理 API 的完全访问权限。 • 注： * Swift 用户必须具有 root 访问权限才能登录到租户帐户。
管理员	仅限 Swift 租户。提供对此租户帐户的 Swift 容器和对象的完全访问权限 • 注： * Swift 用户必须具有 Swift 管理员权限才能使用 Swift REST API 执行任何操作。
管理您自己的 S3 凭据	仅限 S3 租户。允许用户创建和删除自己的 S3 访问密钥。没有此权限的用户不会看到 * 存储（ S3 ） * > * 我的 S3 访问密钥 * 菜单选项。
管理所有分段	• S3 租户：允许用户使用租户管理器和租户管理 API 创建和删除 S3 存储分段，并管理租户帐户中所有 S3 存储分段的设置，而不管 S3 存储分段或组策略如何。 没有此权限的用户不会看到 * 分段 * 菜单选项。 • Swift 租户：允许 Swift 用户使用租户管理 API 控制 Swift 容器的一致性级别。 • 注意： * 您只能通过租户管理 API 为 Swift 组分配 " 管理所有分段 " 权限。您不能使用租户管理器将此权限分配给 Swift 组。
管理端点	仅限 S3 租户。允许用户使用租户管理器或租户管理 API 创建或编辑端点，这些端点用作 StorageGRID 平台服务的目标。 没有此权限的用户不会看到 * 平台服务端点 * 菜单选项。

相关信息

使用 S3

使用 Swift

查看和编辑组详细信息

查看组的详细信息时，您可以更改组的显示名称，权限，策略以及属于该组的用户。

您需要的内容

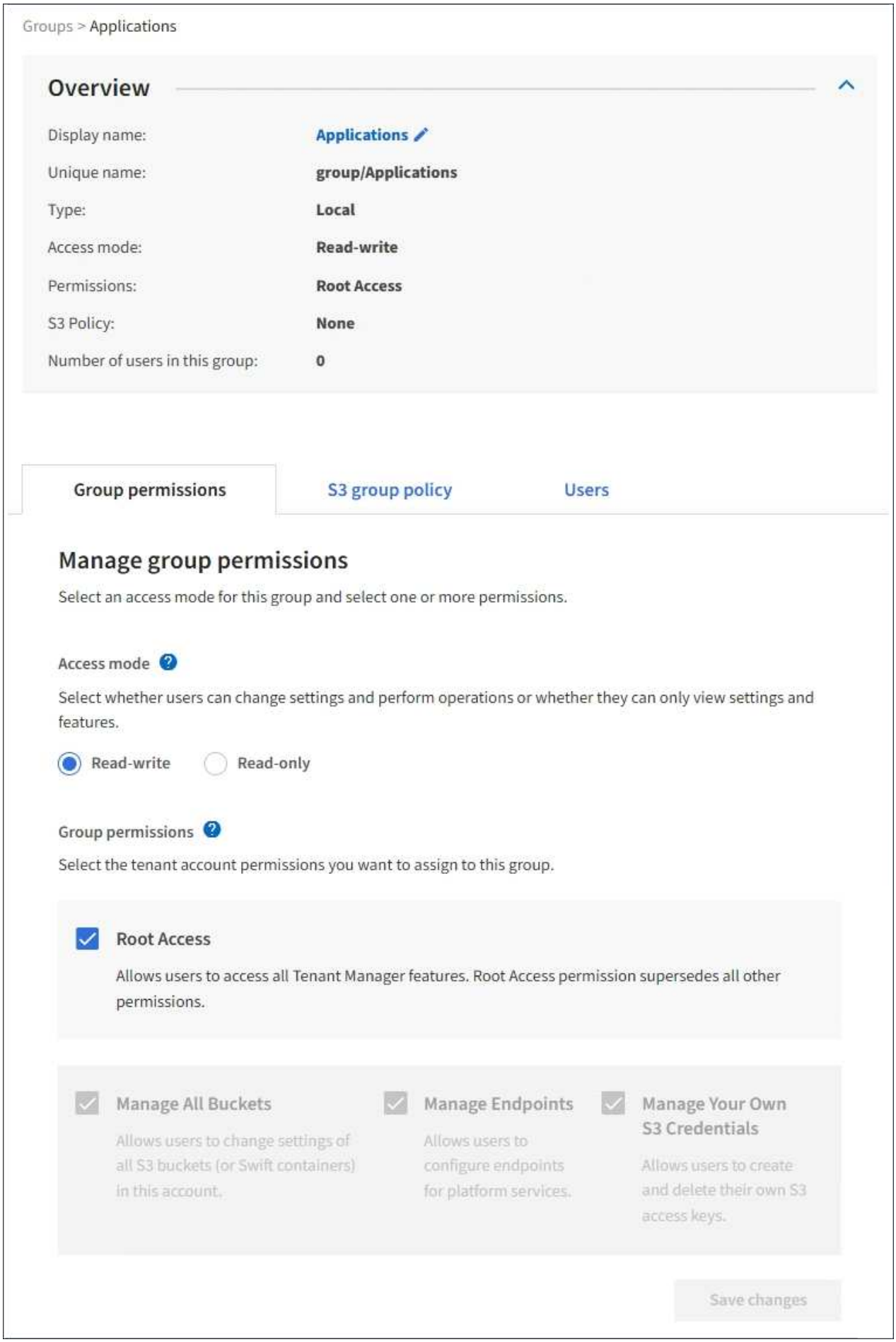
- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选择要查看或编辑其详细信息的组的名称。

   或者，您也可以选择 * 操作 * > * 查看组详细信息 * 。

   此时将显示组详细信息页面。以下示例显示了 S3 组详细信息页面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 根据需要更改组设置。

   要确保更改已保存，请在每个部分进行更改后选择 * 保存更改 * 。保存所做的更改后，页面右上角将显示一条确认消息。

   a. 也可以选择显示名称或编辑图标 更新显示名称。

      您不能更改组的唯一名称。您不能编辑联合组的显示名称。

   b. 也可以更新权限。

   c. 对于组策略，请为 S3 或 Swift 租户进行相应的更改。

      - 如果要编辑 S3 租户的组，也可以选择其他 S3 组策略。如果选择自定义 S3 策略，请根据需要更新 JSON 字符串。
      - 如果要编辑 Swift 租户的组，也可以选中或取消选中 * Swift 管理员 * 复选框。

        有关 Swift 管理员权限的详细信息，请参见有关为 Swift 租户创建组的说明。

   d. 也可以添加或删除用户。

4. 确认您已为更改的每个部分选择 * 保存更改 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

为 S3 租户创建组

为 Swift 租户创建组

将用户添加到本地组

您可以根据需要将用户添加到本地组。

您需要的内容

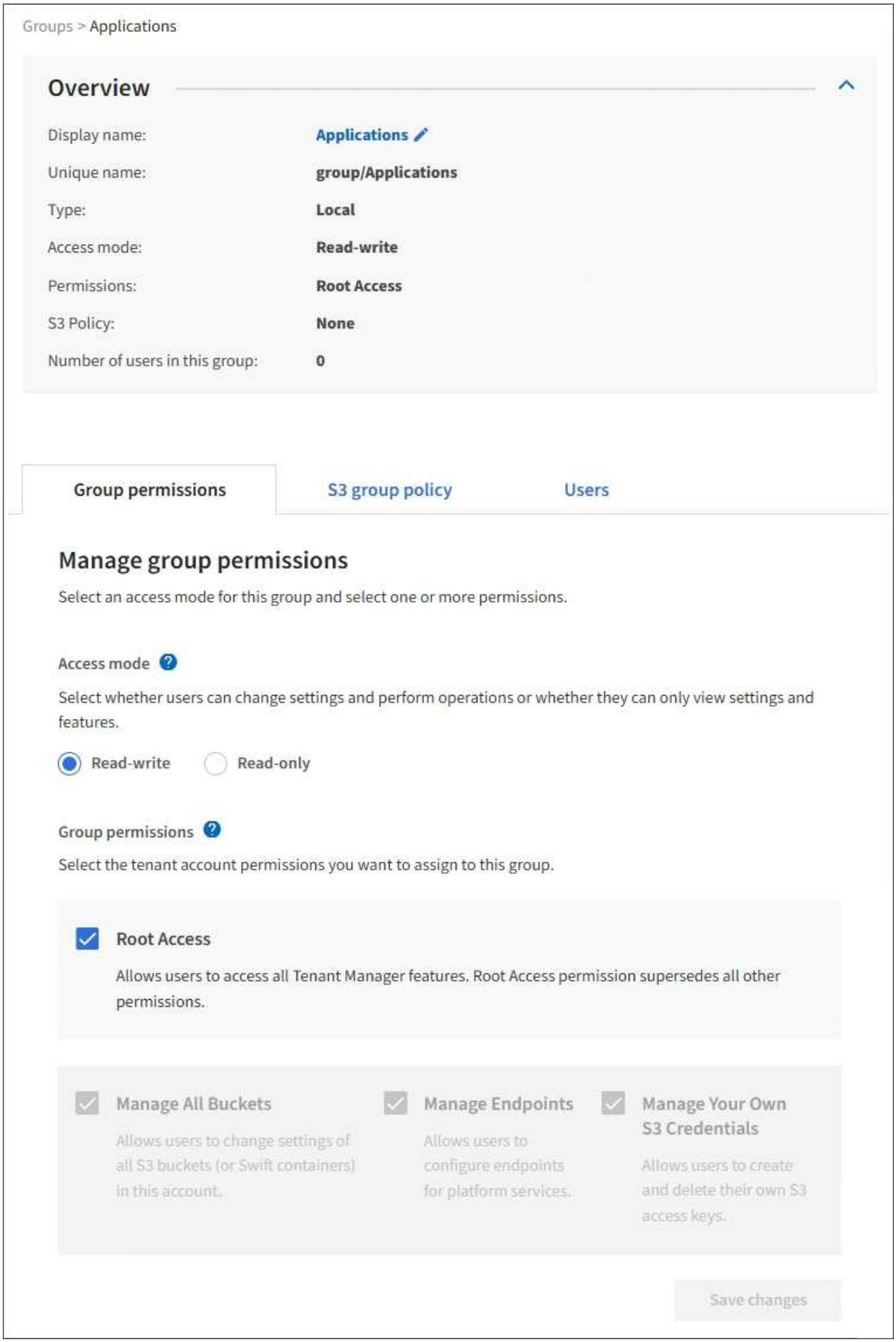
- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。

步骤

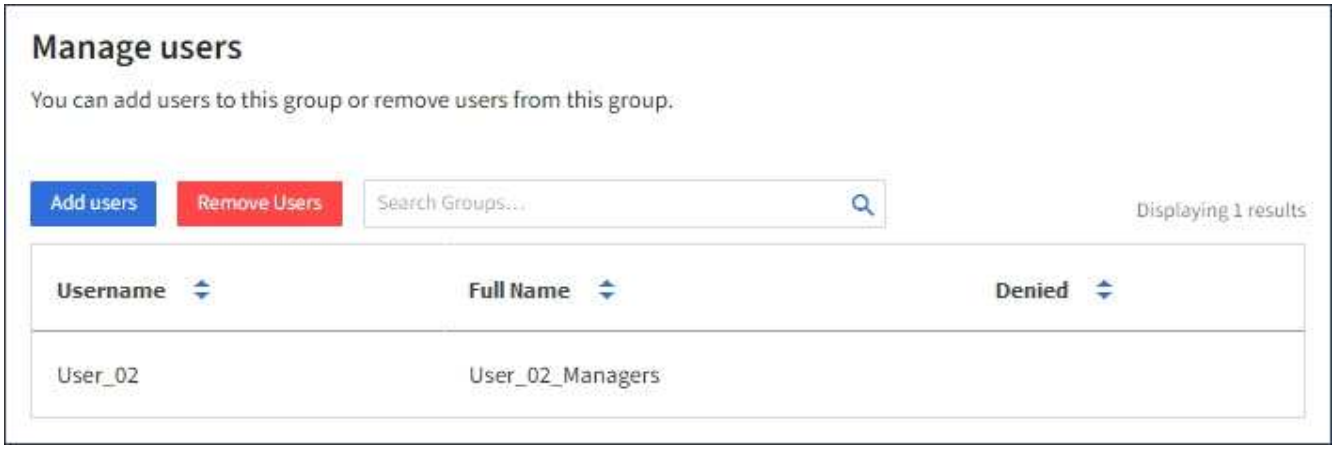
1. 选择 * 访问管理 * > * 组 * 。
2. 选择要将用户添加到的本地组的名称。

   或者，您也可以选择 * 操作 * > * 查看组详细信息 * 。

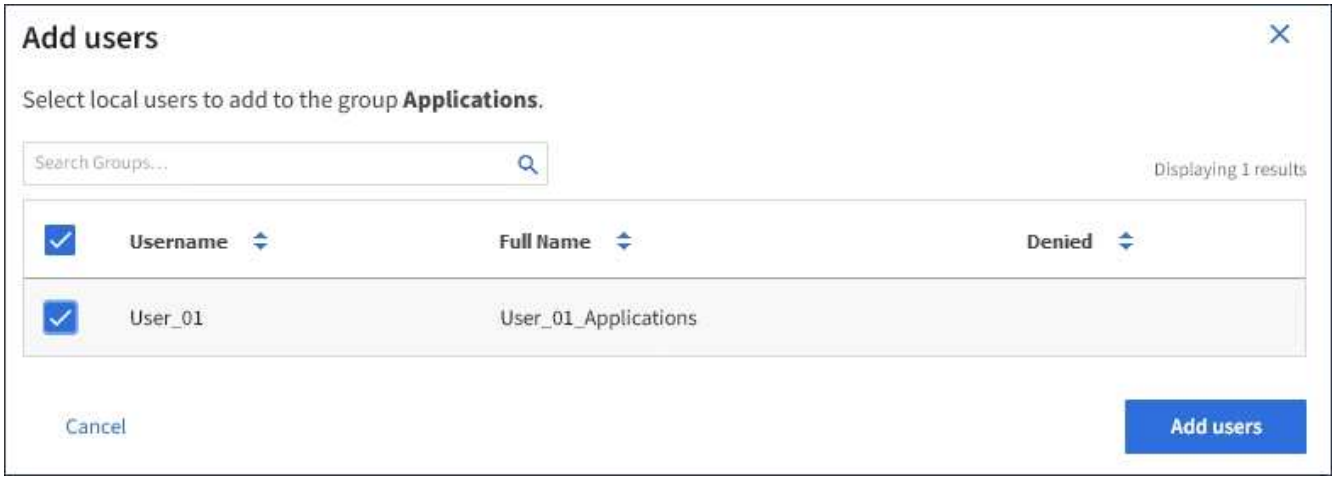
   此时将显示组详细信息页面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 选择 * 用户 * ，然后选择 * 添加用户 * 。



4. 选择要添加到组中的用户，然后选择 * 添加用户 * 。



页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

编辑组名称

您可以编辑组的显示名称。您不能编辑组的唯一名称。

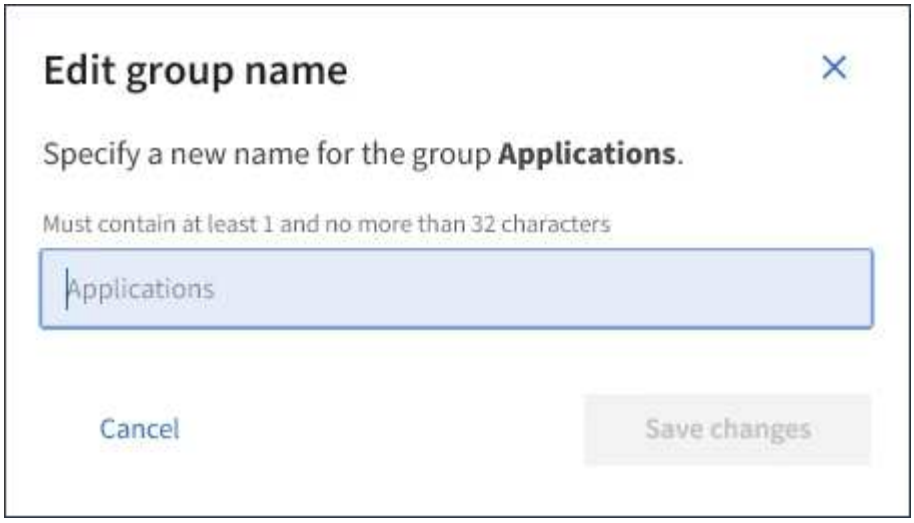
您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。请参见 租户管理权限。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要编辑其显示名称的组对应的复选框。
3. 选择 * 操作 * > * 编辑组名称 * 。

   此时将显示编辑组名称对话框。



4. 如果要编辑本地组，请根据需要更新显示名称。

   您不能更改组的唯一名称。您不能编辑联合组的显示名称。

5. 选择 * 保存更改 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

重复的组

您可以通过复制现有组来更快地创建新组。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。请参见 租户管理权限。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要复制的组对应的复选框。
3. 选择 * 复制组 * 。有关创建组的其他详细信息，请参见创建组的说明 S3 租户 或 Swift 租户。
4. 选择 * 本地组 * 选项卡以创建本地组，或者选择 * 联合组 * 选项卡以从先前配置的身份源导入组。

   如果为 StorageGRID 系统启用了单点登录（ SSO ），则属于本地组的用户将无法登录到租户管理器，尽管他们可以使用客户端应用程序管理租户的资源， 基于组权限。

5. 输入组的名称。
   - * 本地组 * ： 输入显示名称和唯一名称。您可以稍后编辑显示名称。
   - * 联合组 * ： 输入唯一名称。对于 Active Directory ，唯一名称是与 `sAMAccountName` 属性关联的名称。对于 OpenLDAP ，唯一名称是与 `uid` 属性关联的名称。
6. 选择 * 继续 * 。
7. 根据需要修改此组的权限。

8. 选择 * 继续 * 。
9. 如果要为 S3 租户复制组，可以根据需要从 * 添加 S3 策略 * 单选按钮中选择其他策略。如果选择了自定义策略，请根据需要更新 JSON 字符串。
10. 选择 * 创建组 * 。

删除组

您可以从系统中删除组。仅属于该组的任何用户将无法再登录到租户管理器或使用租户帐户。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的用户组。请参见 租户管理权限。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选中要删除的组对应的复选框。
3. 选择 * 操作 * > * 删除组 * 。

   此时将显示一条确认消息。

4. 选择 * 删除组 * 确认要删除确认消息中指示的组。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

管理本地用户

您可以创建本地用户并将其分配给本地组，以确定这些用户可以访问哪些功能。租户管理

器包括一个名为 "`root" 的预定义本地用户。` 虽然您可以添加和删除本地用户，但不能删除 root 用户。

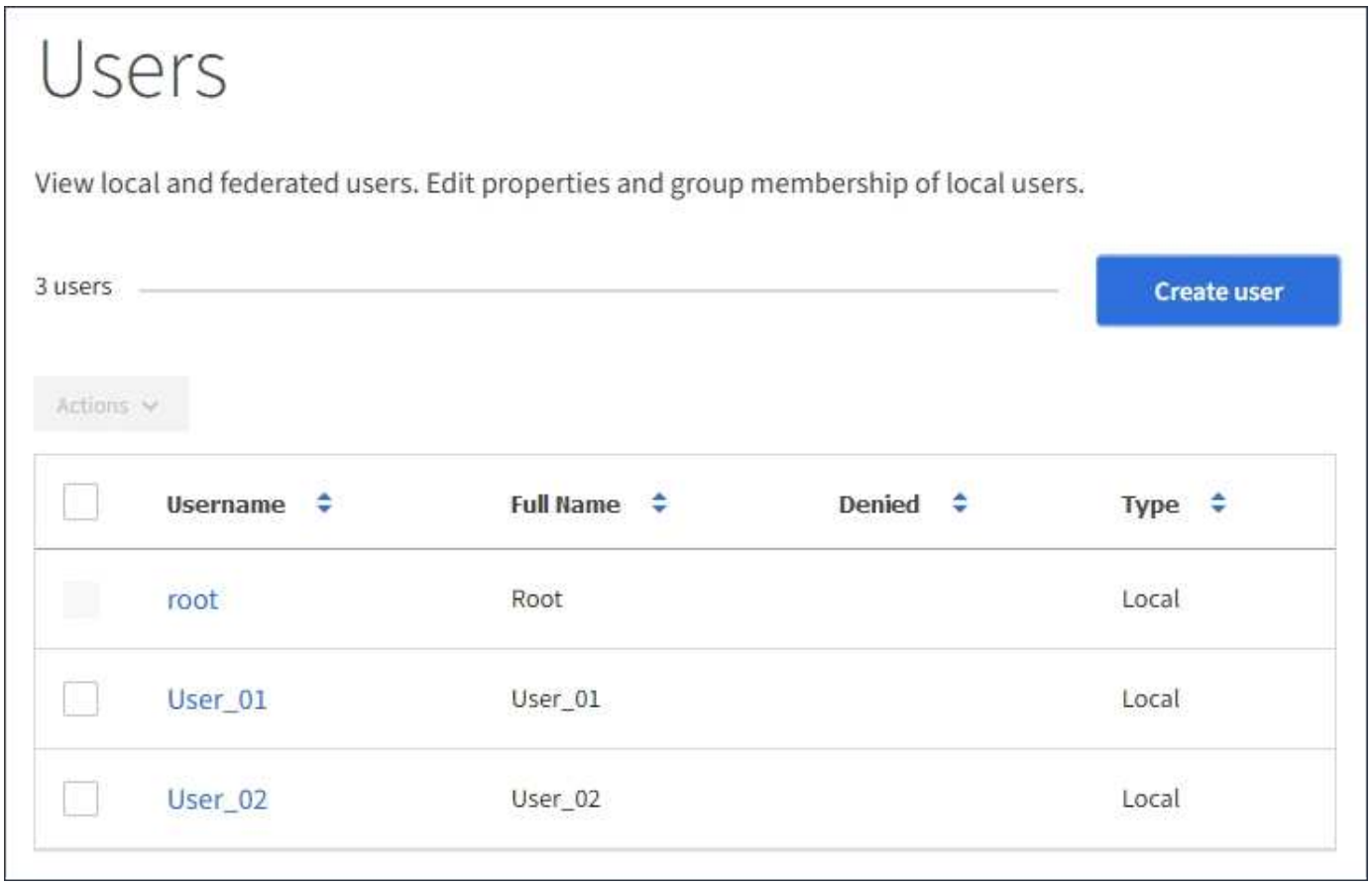
您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 root 访问权限的读写用户组。请参见 租户管理权限。

> 如果为 StorageGRID 系统启用了单点登录（ SSO ），则本地用户将无法登录到租户管理器或租户管理 API ，但他们可以根据组权限使用 S3 或 Swift 客户端应用程序访问租户的资源。

访问用户页面

选择 * 访问管理 * > * 用户 * 。



创建本地用户

您可以创建本地用户并将其分配给一个或多个本地组以控制其访问权限。

不属于任何组的 S3 用户没有应用管理权限或 S3 组策略。这些用户可能已通过存储分段策略授予 S3 存储分段访问权限。

不属于任何组的 Swift 用户不具有管理权限或 Swift 容器访问权限。

步骤

1. 选择 * 创建用户 * 。

2. 填写以下字段。
   - * 全名 * ： 此用户的全名，例如，人员的名字和姓氏或应用程序的名称。
   - * 用户名 * ： 此用户用于登录的名称。用户名必须是唯一的，不能更改。
   - * 密码 * ： 用户登录时使用的密码。
   - * 确认密码 * ： 键入您在密码字段中键入的相同密码。
   - * 拒绝访问 * ： 如果选择 * 是 * ，则此用户无法登录到租户帐户，即使此用户可能仍属于一个或多个组。

     例如，您可以使用此功能暂时暂停用户的登录能力。
3. 选择 * 继续 * 。
4. 将用户分配给一个或多个本地组。

   不属于任何组的用户将无管理权限。权限是累积的。用户将对其所属的所有组拥有所有权限。
5. 选择 * 创建用户 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

编辑用户详细信息

编辑用户的详细信息时，您可以更改用户的全名和密码，将用户添加到不同的组并阻止用户访问租户。

步骤

1. 在用户列表中，选择要查看或编辑其详细信息的用户的名称。

   或者，您也可以选中用户的复选框，然后选择 * 操作 * > * 查看用户详细信息 * 。
2. 根据需要更改用户设置。
   a. 选择全名或编辑图标，根据需要更改用户的全名 在概述部分。

      您不能更改用户名。
   b. 在 * 密码 * 选项卡上，根据需要更改用户的密码。
   c. 在 * 访问 * 选项卡上，允许用户登录（选择 * 否 * ），或者根据需要阻止用户登录（选择 * 是 * ）。
   d. 在 * 组 * 选项卡上，根据需要将用户添加到组或从组中删除该用户。
   e. 根据需要为每个部分选择 * 保存更改 * 。

      由于缓存，更改可能需要长达 15 分钟才能生效。

本地用户重复

您可以复制本地用户以更快地创建新用户。

步骤

1. 在用户列表中，选择要复制的用户。

2. 选择 * 复制用户 * 。
3. 修改新用户的以下字段。
   - * 全名 * ： 此用户的全名，例如，人员的名字和姓氏或应用程序的名称。
   - * 用户名 * ： 此用户用于登录的名称。用户名必须是唯一的，不能更改。
   - * 密码 * ： 用户登录时使用的密码。
   - * 确认密码 * ： 键入您在密码字段中键入的相同密码。
   - * 拒绝访问 * ： 如果选择 * 是 * ，则此用户无法登录到租户帐户，即使此用户可能仍属于一个或多个组。

     例如，您可以使用此功能暂时暂停用户的登录能力。
4. 选择 * 继续 * 。
5. 选择一个或多个本地组。

   不属于任何组的用户将无管理权限。权限是累积的。用户将对其所属的所有组拥有所有权限。
6. 选择 * 创建用户 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

删除本地用户

您可以永久删除不再需要访问 StorageGRID 租户帐户的本地用户。

使用租户管理器，您可以删除本地用户，但不能删除联合用户。您必须使用联合身份源删除联合用户。

步骤

1. 在用户列表中，选中要删除的本地用户对应的复选框。
2. 选择 * 操作 * > * 删除用户 * 。
3. 在确认对话框中，选择 * 删除用户 * 以确认要从系统中删除此用户。

   由于缓存，更改可能需要长达 15 分钟才能生效。

管理 S3 租户帐户

管理 S3 访问密钥

S3 租户帐户的每个用户都必须具有访问密钥，才能在 StorageGRID 系统中存储和检索对象。访问密钥由访问密钥 ID 和机密访问密钥组成。

关于此任务

S3 访问密钥可按如下方式进行管理：

- 具有 * 管理自己的 S3 凭据 * 权限的用户可以创建或删除自己的 S3 访问密钥。
- 具有 * 根访问 * 权限的用户可以管理 S3 根帐户和所有其他用户的访问密钥。除非存储分段策略明确禁用，否则根访问密钥可为租户提供对所有存储分段和对象的完全访问权限。

StorageGRID 支持签名版本 2 和签名版本 4 身份验证。除非存储分段策略明确启用，否则不允许跨帐户访问。

创建您自己的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以创建自己的 S3 访问密钥。要访问 S3 租户帐户中的分段和对象，您必须具有访问密钥。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须具有管理自己的 S3 凭据权限。请参见 租户管理权限。

关于此任务

您可以创建一个或多个 S3 访问密钥，以便为租户帐户创建和管理存储分段。创建新的访问密钥后，使用新的访问密钥 ID 和机密访问密钥更新应用程序。为安全起见，请勿创建超出您需要的密钥，并删除您未使用的密钥。如果只有一个密钥，并且该密钥即将到期，请在旧密钥到期之前创建一个新密钥，然后删除旧密钥。

每个密钥可以有特定的到期时间，也可以无到期时间。请遵循以下到期时间准则：

- 为密钥设置到期时间，以将访问权限限制为特定时间段。设置较短的到期时间有助于降低访问密钥 ID 和机密访问密钥意外暴露时的风险。过期密钥将自动删除。
- 如果环境中的安全风险较低，并且您不需要定期创建新密钥，则无需为密钥设置到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。

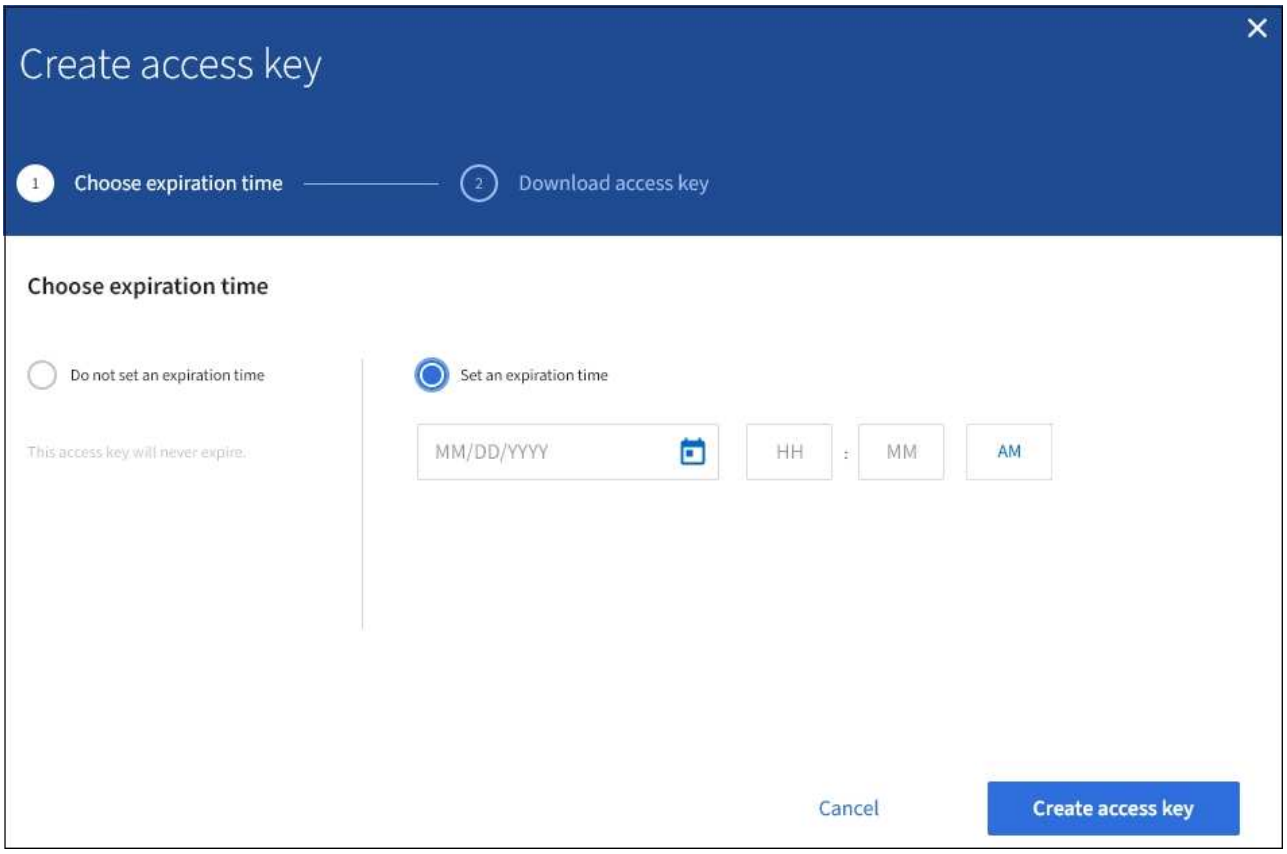
> 您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

   此时将显示 My access keys 页面，其中列出了所有现有访问密钥。

2. 选择 * 创建密钥 * 。
3. 执行以下操作之一：
   - 选择 * 不设置到期时间 * 可创建不会过期的密钥。（默认）
   - 选择 * 设置到期时间 * ，然后设置到期日期和时间。

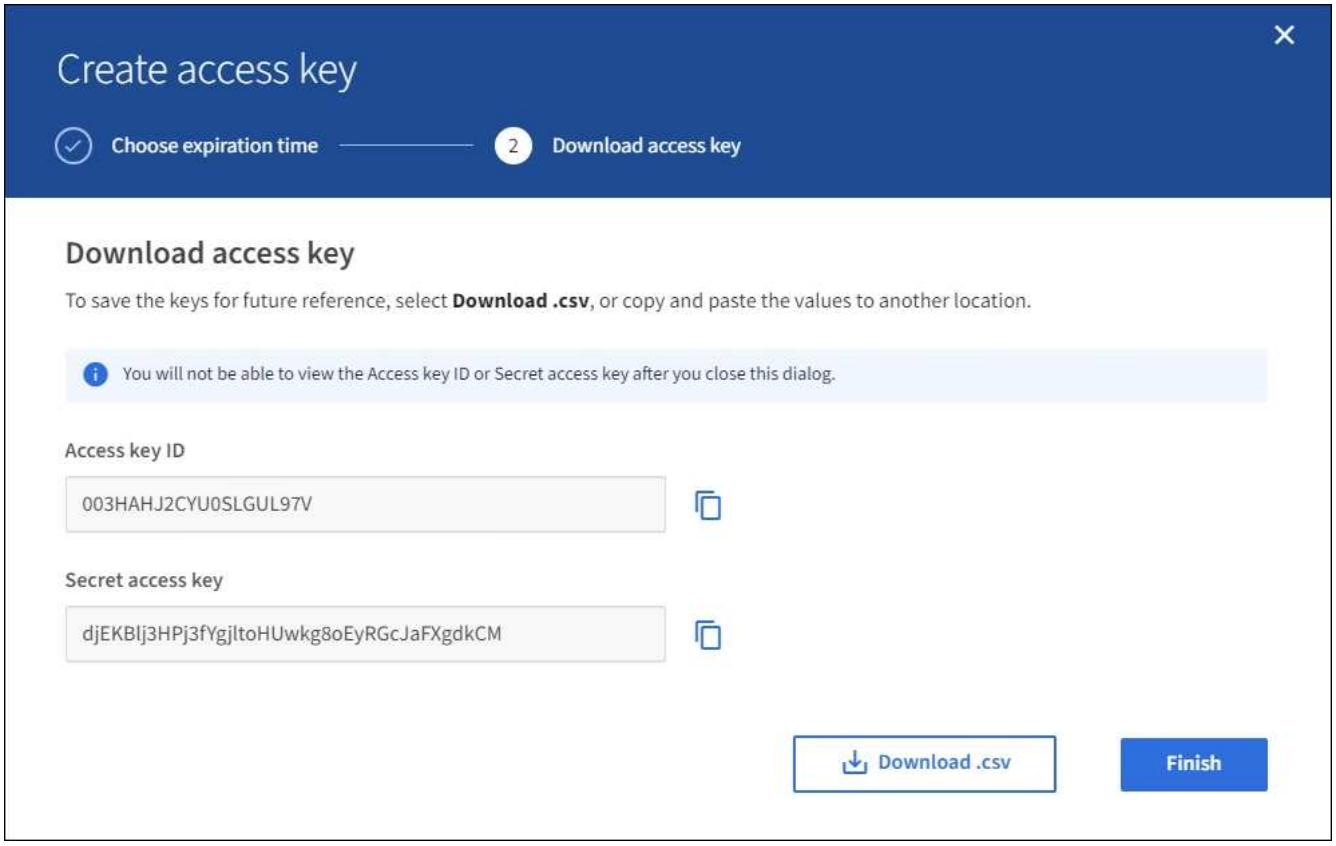


4. 选择 * 创建访问密钥 * 。

   此时将显示 Download access key 对话框，其中列出了您的访问密钥 ID 和机密访问密钥。

5. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

   在复制或下载此信息之前，请勿关闭此对话框。关闭此对话框后，您将无法复制或下载密钥。



6. 选择 * 完成 * 。

   新密钥将列在 " 我的访问密钥 " 页面上。由于缓存，更改可能需要长达 15 分钟才能生效。

查看 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以查看 S3 访问密钥列表。您可以按到期时间对列表进行排序，以便确定哪些密钥不久将过期。您可以根据需要创建新密钥或删除不再使用的密钥。

您需要的内容

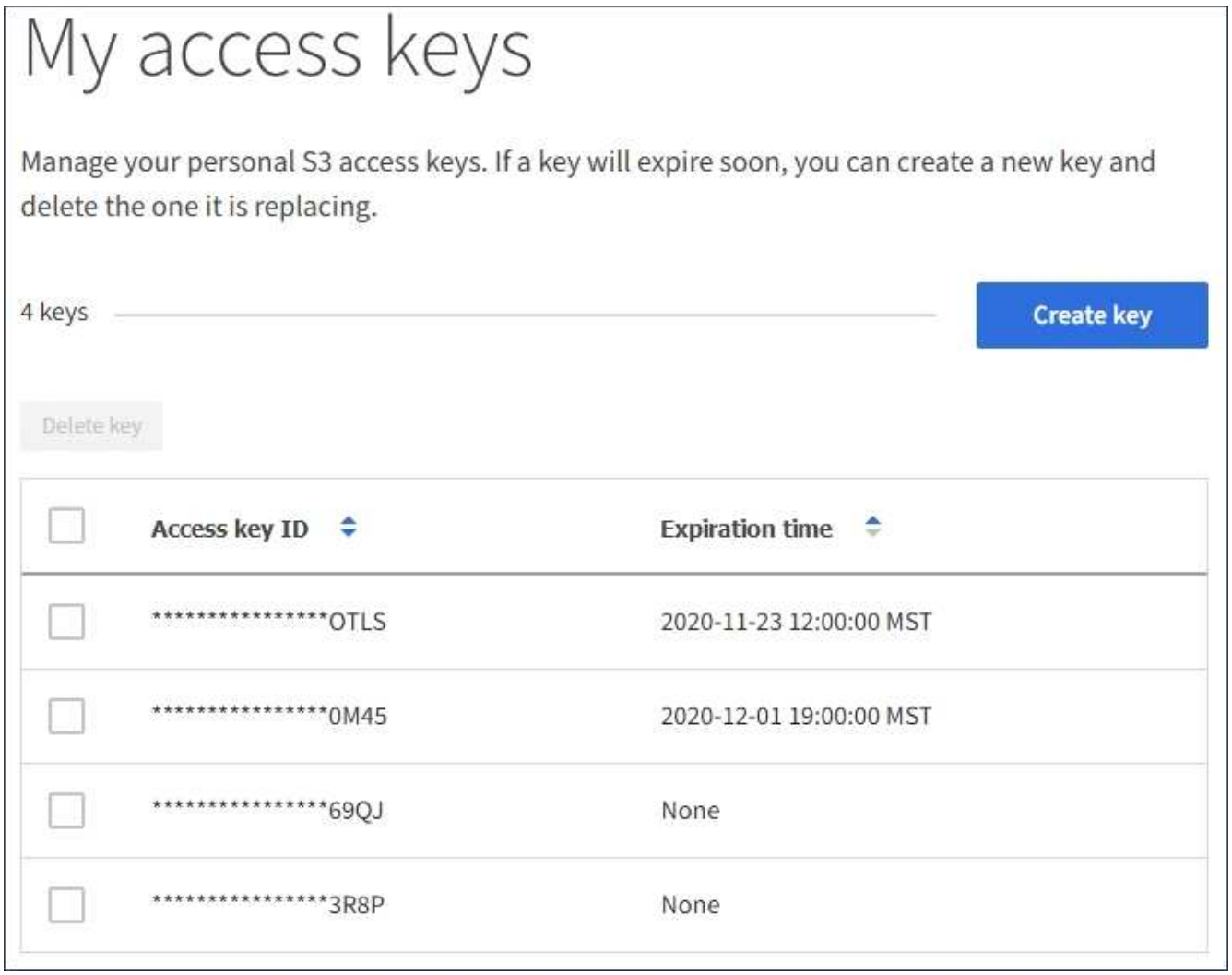
- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须具有管理自己的 S3 凭据权限。

> 您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

   此时将显示 My access keys 页面，其中列出了所有现有访问密钥。



2. 按 * 到期时间 * 或 * 访问密钥 ID* 对密钥进行排序。
3. 根据需要创建新密钥并手动删除不再使用的密钥。

   如果在现有密钥到期之前创建新密钥，则可以开始使用新密钥，而不会暂时丢失对帐户中对象的访问权限。

   过期密钥将自动删除。

相关信息

创建您自己的 S3 访问密钥

删除您自己的 S3 访问密钥

删除您自己的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以删除您自己的 S3 访问密钥。删除访问密钥后，无法再使用它访问租户帐户中的对象和分段。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。

- 您必须具有管理自己的 S3 凭据权限。请参见 租户管理权限。

> 您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

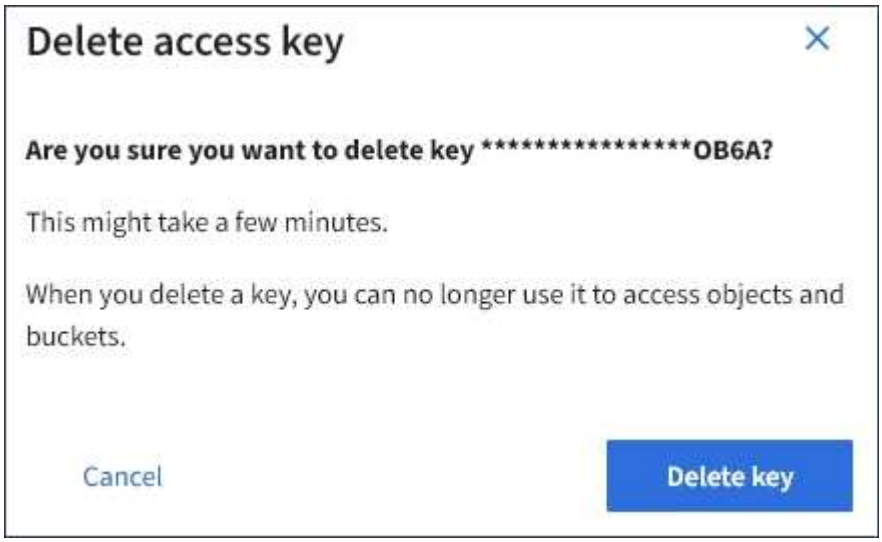
步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

   此时将显示 My access keys 页面，其中列出了所有现有访问密钥。

2. 选中要删除的每个访问密钥对应的复选框。
3. 选择 * 删除密钥 * 。

   此时将显示确认对话框。



4. 选择 * 删除密钥 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

创建其他用户的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以为其他用户创建 S3 访问密钥，例如需要访问存储分段和对象的应用程序。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须具有 root 访问权限。

关于此任务

您可以为其他用户创建一个或多个 S3 访问密钥，以便他们可以为其租户帐户创建和管理存储分段。创建新的访问密钥后，使用新的访问密钥 ID 和机密访问密钥更新应用程序。为安全起见，请勿创建超出用户需求的密钥，并删除未使用的密钥。如果只有一个密钥，并且该密钥即将到期，请在旧密钥到期之前创建一个新密钥，然后删

除旧密钥。

每个密钥可以有特定的到期时间，也可以无到期时间。请遵循以下到期时间准则：

- 设置密钥的到期时间，以将用户的访问限制为特定时间段。如果访问密钥 ID 和机密访问密钥意外暴露，则设置较短的到期时间有助于降低风险。过期密钥将自动删除。
- 如果环境中的安全风险较低，并且您不需要定期创建新密钥，则无需为密钥设置到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。

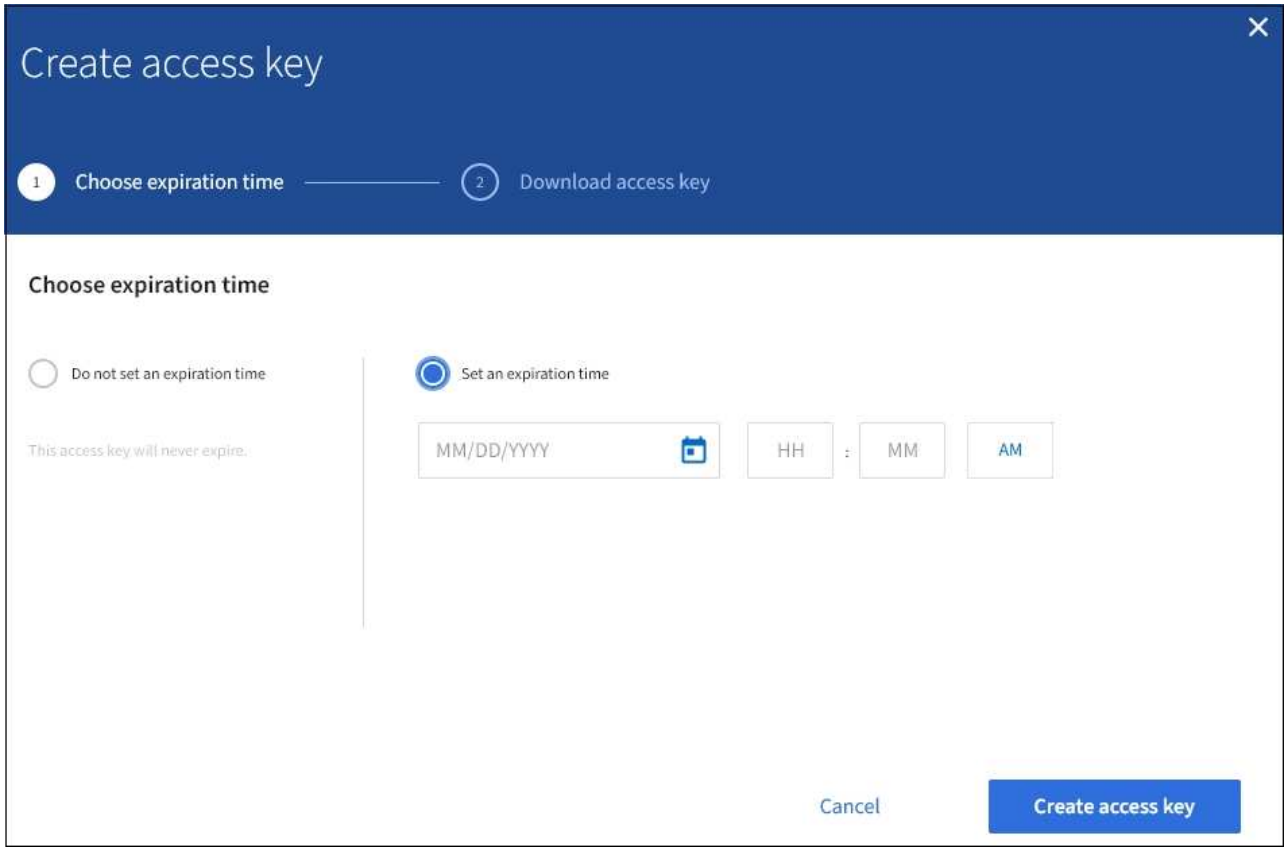
> 可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 访问管理 * > * 用户 * 。
2. 选择要管理其 S3 访问密钥的用户。

   此时将显示用户详细信息页面。

3. 选择 * 访问密钥 * ，然后选择 * 创建密钥 * 。
4. 执行以下操作之一：
   - 选择 * 不设置到期时间 * 可创建未过期的密钥。（默认）
   - 选择 * 设置到期时间 * ，然后设置到期日期和时间。

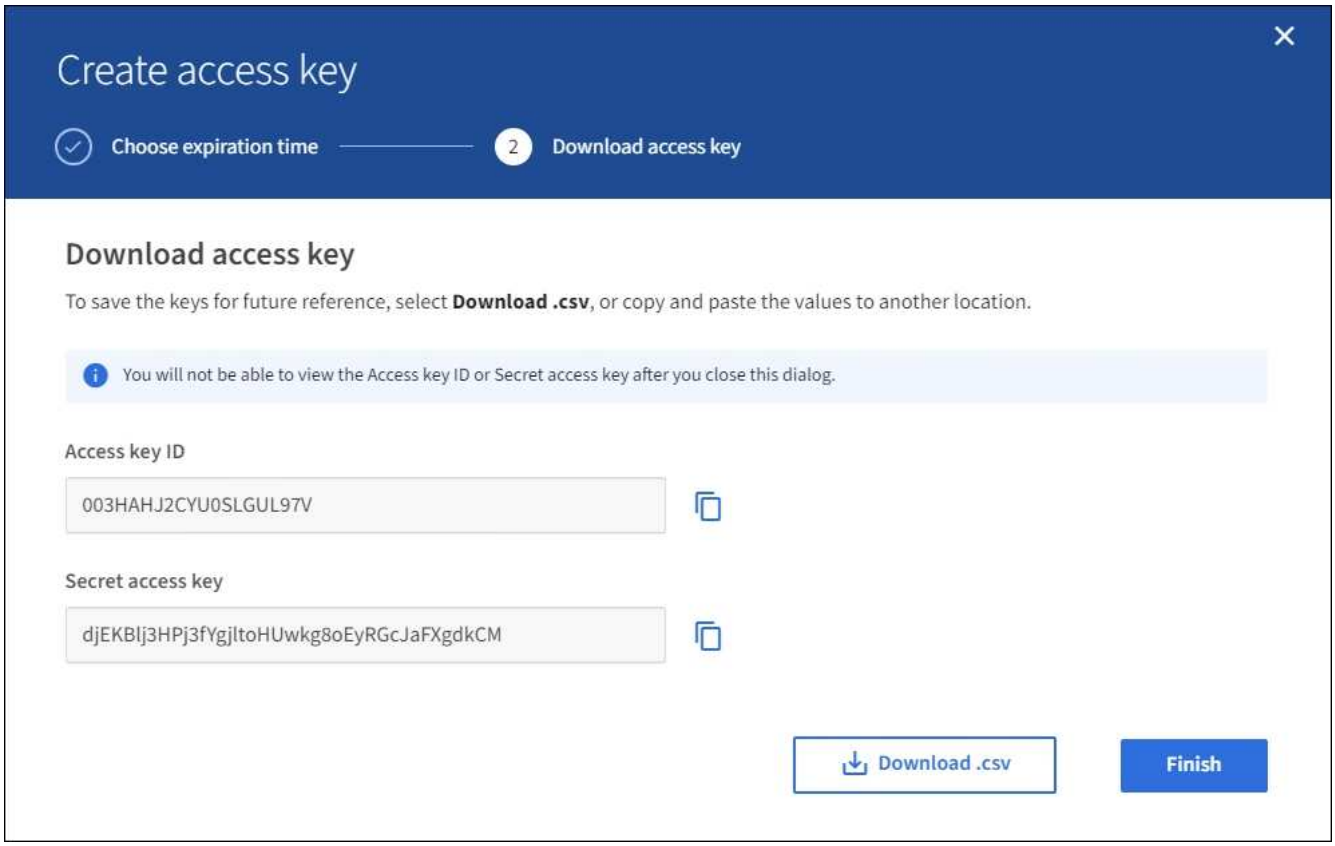


5. 选择 * 创建访问密钥 * 。

此时将显示 Download access key 对话框，其中列出了访问密钥 ID 和机密访问密钥。

6. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

   在复制或下载此信息之前，请勿关闭此对话框。关闭此对话框后，您将无法复制或下载密钥。



7. 选择 * 完成 * 。

   新密钥将列在用户详细信息页面的访问密钥选项卡中。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

租户管理权限

查看其他用户的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以查看其他用户的 S3 访问密钥。您可以按到期时间对列表进行排序，以便确定哪些密钥不久将过期。您可以根据需要创建新密钥并删除不再使用的密钥。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须具有 root 访问权限。

可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

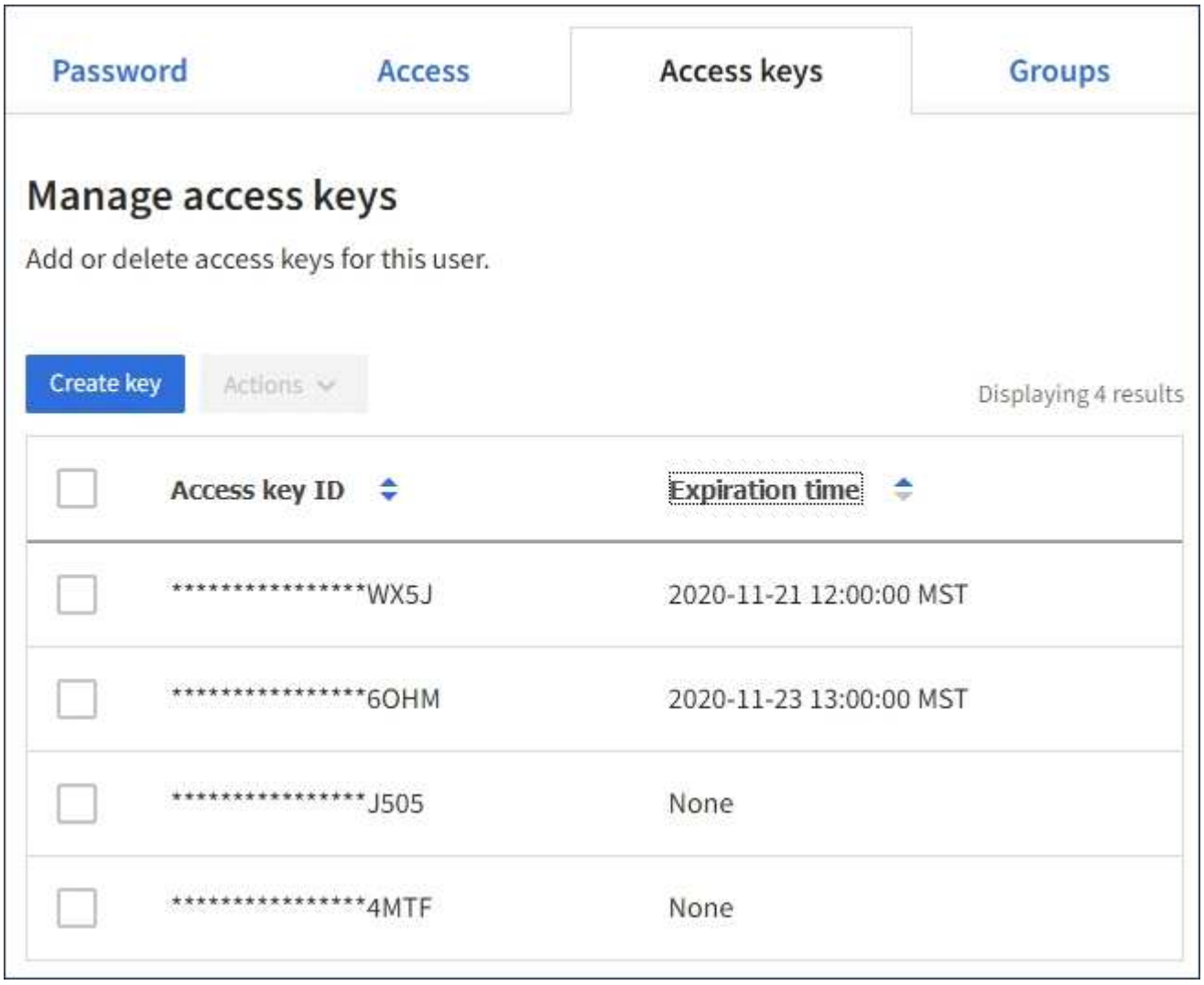
1. 选择 * 访问管理 * > * 用户 * 。

   此时将显示 "Users" 页面，其中列出了现有用户。

2. 选择要查看其 S3 访问密钥的用户。

   此时将显示用户详细信息页面。

3. 选择 * 访问密钥 * 。



4. 按 * 到期时间 * 或 * 访问密钥 ID* 对密钥进行排序。
5. 根据需要创建新密钥并手动删除不再使用的密钥。

   如果在现有密钥到期之前创建新密钥，则用户可以开始使用新密钥，而不会暂时丢失对帐户中对象的访问权限。

过期密钥将自动删除。

相关信息

创建其他用户的 S3 访问密钥

删除其他用户的 S3 访问密钥

删除其他用户的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以删除其他用户的 S3 访问密钥。删除访问密钥后，无法再使用它访问租户帐户中的对象和分段。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须具有 root 访问权限。请参见 租户管理权限。

> 可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 访问管理 * > * 用户 * 。

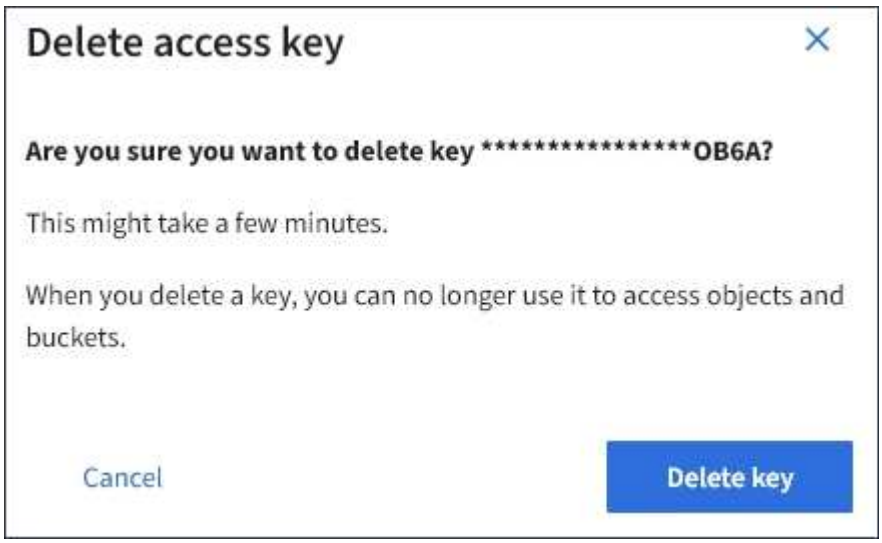
   此时将显示 "Users" 页面，其中列出了现有用户。

2. 选择要管理其 S3 访问密钥的用户。

   此时将显示用户详细信息页面。

3. 选择 * 访问密钥 * ，然后选中要删除的每个访问密钥对应的复选框。
4. 选择 * 操作 * > * 删除选定密钥 * 。

   此时将显示确认对话框。



5. 选择 * 删除密钥 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

管理 S3 存储分段

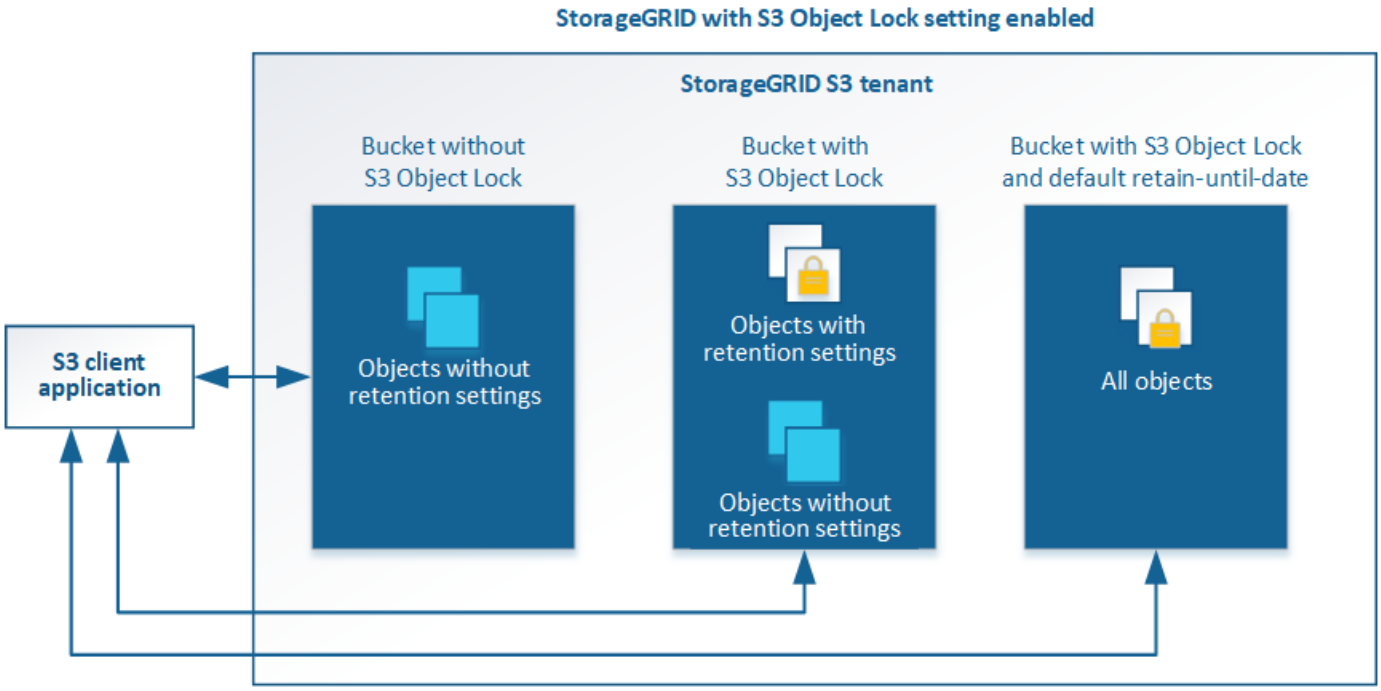
对租户使用 S3 对象锁定

如果您的对象必须符合保留方面的法规要求，则可以使用 StorageGRID 中的 S3 对象锁定功能。

什么是 S3 对象锁定?

StorageGRID S3 对象锁定功能是一种对象保护解决方案 ，相当于 Amazon Simple Storage Service （ Amazon S3 ）中的 S3 对象锁定。

如图所示，如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则 S3 租户帐户可以在启用或不启用 S3 对象锁定的情况下创建存储分段。如果某个存储分段启用了 S3 对象锁定，则 S3 客户端应用程序可以选择为该存储分段中的任何对象版本指定保留设置。对象版本必须具有指定的保留设置，以受 S3 对象锁定的保护。



StorageGRID S3 对象锁定功能提供了一种保留模式，相当于 Amazon S3 合规模式。默认情况下，任何用户都无法覆盖或删除受保护的对象版本。StorageGRID S3 对象锁定功能不支持监管模式，并且不允许具有特殊权限的用户绕过保留设置或删除受保护的对象。

如果存储分段启用了 S3 对象锁定，则在创建或更新对象时， S3 客户端应用程序可以选择指定以下任一或两个对象级别保留设置：

- * 保留至日期 * ：如果对象版本的保留至日期为未来日期，则可以检索该对象，但无法修改或删除它。可以根据需要增加对象的保留截止日期，但不能缩短此日期。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。合法保留与保留日期无关。

您也可以 指定存储分段的默认保留模式和默认保留期限。这些设置将应用于添加到存储分段中但不指定其自身保留设置的每个对象。

有关这些设置的详细信息，请参见 使用 S3 对象锁定。

管理旧版合规存储分段

S3 对象锁定功能取代了先前 StorageGRID 版本中提供的合规性功能。如果您使用早期版本的 StorageGRID 创建了合规的存储分段，则可以继续管理这些存储分段的设置；但是，您无法再创建新的合规存储分段。有关说明，请参见 NetApp 知识库文章。

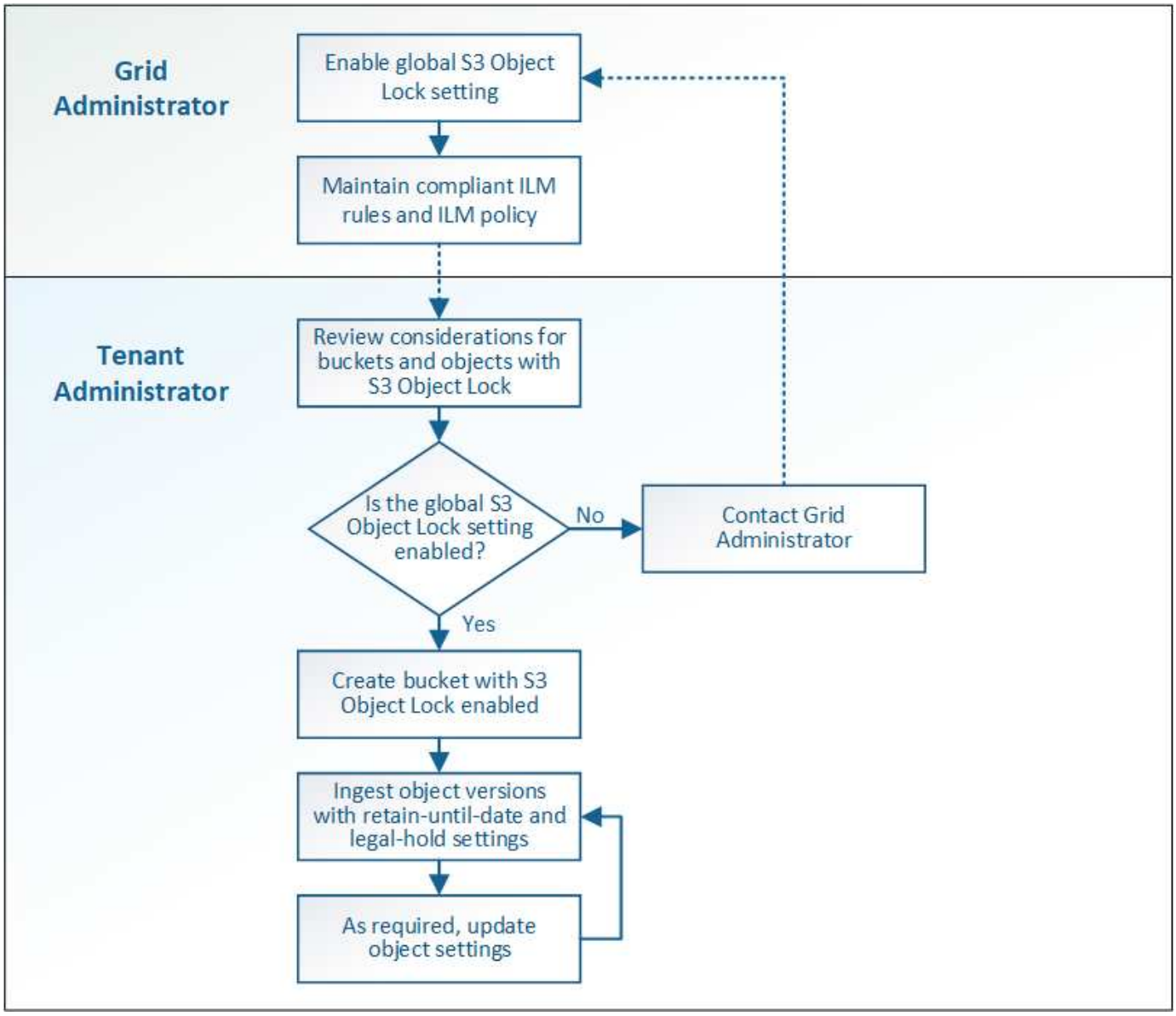
"NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

S3 对象锁定工作流

工作流图显示了在 StorageGRID 中使用 S3 对象锁定功能的高级步骤。

在启用了 S3 对象锁定的情况下创建分段之前，网格管理员必须为整个 StorageGRID 系统启用全局 S3 对象锁定设置。网格管理员还必须确保 信息生命周期管理（ ILM ）策略 符合 "`合规` "；它必须满足启用了 S3 对象锁定的分段的要求。有关详细信息，请联系网格管理员或查看有关通过信息生命周期管理来管理对象的说明。

启用全局 S3 对象锁定设置后，您可以在启用了 S3 对象锁定的情况下创建存储分段。然后，您可以使用 S3 客户端应用程序为每个对象版本指定保留设置。



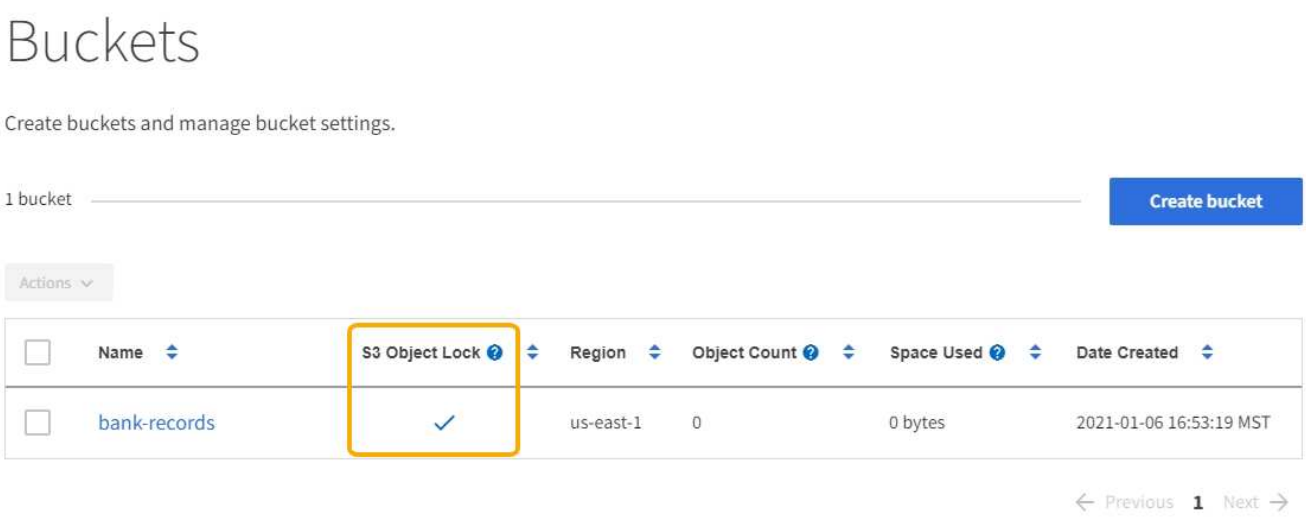
S3 对象锁定的要求

在为存储分段启用 S3 对象锁定之前，请查看 S3 对象锁定存储分段和对象的要求以及启用了 S3 对象锁定的存储分段中对象的生命周期。

启用了 **S3** 对象锁定的存储分段的要求

- 如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以使用租户管理器，租户管理 API 或 S3 REST API 创建启用了 S3 对象锁定的分段。

  此租户管理器示例显示了一个已启用 S3 对象锁定的存储分段。



- 如果您计划使用 S3 对象锁定，则必须在创建存储分段时启用 S3 对象锁定。您不能为现有存储分段启用 S3 对象锁定。
- S3 对象锁定需要分段版本。为存储分段启用 S3 对象锁定后， StorageGRID 会自动为该存储分段启用版本控制。
- 在启用了 S3 对象锁定的情况下创建存储分段后，无法禁用 S3 对象锁定或暂停该存储分段的版本控制。
- 您也可以为存储分段配置默认保留。上传对象版本时，默认保留将应用于对象版本。您可以通过在上传对象版本的请求中指定保留模式和保留至日期来覆盖存储分段默认值。
- S3 对象生命周期分段支持分段生命周期配置。
- 启用了 S3 对象锁定的存储分段不支持 CloudMirror 复制。

启用了 **S3** 对象锁定的分段中的对象的要求

- 要保护对象版本， S3 客户端应用程序必须配置存储分段默认保留，或者在每个上传请求中指定保留设置。
- 您可以增加对象版本的保留截止日期，但不能减小此值。
- 如果您收到有关待定法律诉讼或监管调查的通知，则可以通过对对象版本进行法律保留来保留相关信息。如果对象版本处于合法保留状态，则无法从 StorageGRID 中删除该对象，即使该对象已达到保留日期。一旦取消合法保留，如果已达到保留日期，则可以删除对象版本。
- S3 对象锁定需要使用版本控制的分段。保留设置适用于各个对象版本。对象版本可以同时具有保留截止日期和合法保留设置，但不能具有其他设置，或者两者均不具有。为对象指定保留日期或合法保留设置仅保护请求中指定的版本。您可以创建新版本的对象，而先前版本的对象仍保持锁定状态。

启用了 **S3** 对象锁定的存储分段中的对象生命周期

保存在启用了 S3 对象锁定的存储分段中的每个对象将经历三个阶段：

1. * 对象载入 *
    - 在启用了 S3 对象锁定的情况下，将对象版本添加到存储分段时， S3 客户端应用程序可以选择为此对象指定保留设置（ retene-until date ， legal hold 或两者）。然后， StorageGRID 会为此对象生成元数据，其中包括唯一对象标识符（ UUID ）以及载入日期和时间。
    - 载入具有保留设置的对象版本后，将无法修改其数据和 S3 用户定义的元数据。
    - StorageGRID 存储的对象元数据与对象数据无关。它会为每个站点上的所有对象元数据维护三个副本。

2. * 对象保留 *
    - StorageGRID 会存储该对象的多个副本。副本的确切数量和类型以及存储位置取决于活动 ILM 策略中的合规规则。
3. * 对象删除 *
    - 达到保留截止日期后，可以删除对象。
    - 无法删除处于合法保留状态的对象。

创建 **S3** 存储分段

您可以使用租户管理器为对象数据创建 S3 分段。创建存储分段时，必须指定存储分段的名称和区域。如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以选择为存储分段启用 S3 对象锁定。

您需要的内容

- 您将使用登录到租户管理器 支持的 Web 浏览器。
- 您属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。

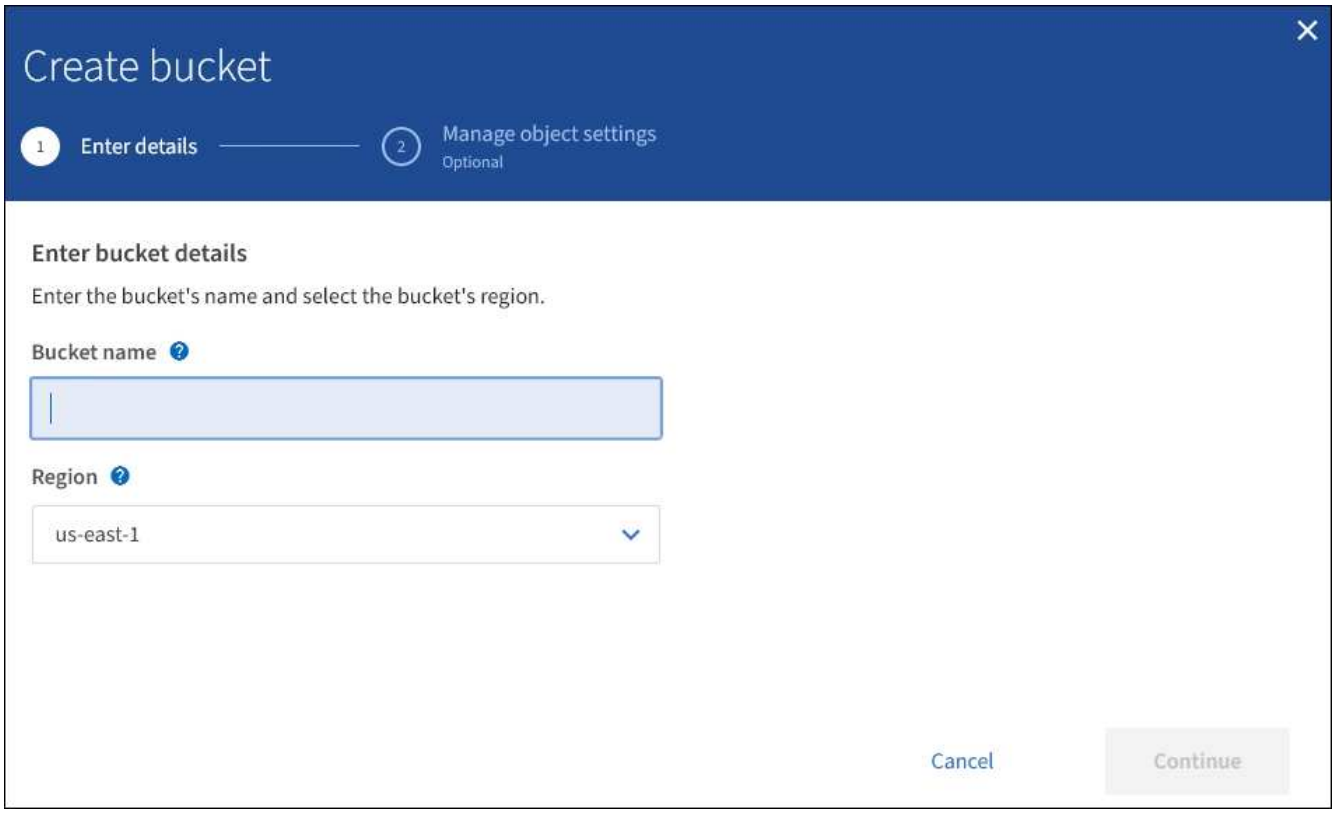
  可以授予设置或修改存储分段或对象的 S3 对象锁定属性的权限 存储分段策略或组策略。

- 如果您计划使用 S3 对象锁定创建存储分段，则已为 StorageGRID 系统启用全局 S3 对象锁定设置，并已查看 S3 对象锁定存储分段和对象的要求。

  使用 S3 对象锁定

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。
2. 选择 * 创建存储分段 * 。



3. 输入存储分段的唯一名称。

   创建存储分段后，您无法更改存储分段名称。

   存储分段名称必须符合以下规则：

   - 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。
   - 必须符合 DNS 要求。
   - 必须至少包含 3 个字符，并且不能超过 63 个字符。
   - 每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。
   - 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。

   有关详细信息，请参见 "有关存储分段命名规则的 Amazon Web Services （ AWS ）文档"。

4. 为此存储分段选择区域。

   StorageGRID 管理员负责管理可用的区域。存储分段的区域可能会影响应用于对象的数据保护策略。默认情况下，所有分段都在 `us-east-1` 区域创建。

   创建存储分段后，您无法更改此区域。

5. 选择 * 继续 * 。
6. （可选）为存储分段启用对象版本控制。

   如果要将每个对象的每个版本存储在此存储分段中，请启用对象版本控制。然后，您可以根据需要检索对象

的先前版本。

7. 如果显示 "S3 Object Lock" 部分，则可以选择为存储分段启用 S3 Object Lock 。

   创建存储分段后，您无法启用或禁用 S3 对象锁定。

   只有在启用了全局 S3 对象锁定设置的情况下，才会显示 S3 对象锁定部分。

   必须为存储分段启用 S3 对象锁定， S3 客户端应用程序才能为添加到存储分段的对象指定保留日期和合法保留设置。

   如果为存储分段启用 S3 对象锁定，则会自动启用存储分段版本控制。您也可以 指定存储分段的默认保留模式和默认保留期限 应用于输入到存储分段中但未指定其自身保留设置的每个对象。

8. 选择 * 创建存储分段 * 。

   此时将创建存储分段并将其添加到 " 存储分段 " 页面上的表中。

相关信息

使用 ILM 管理对象

了解租户管理 API

使用 S3

查看 **S3** 存储分段详细信息

您可以查看租户帐户中的分段和分段设置列表。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。

   此时将显示 " 分段 " 页面，其中列出了租户帐户的所有分段。

2. 查看每个存储分段的信息。

   您可以根据需要按任何列对信息进行排序，也可以在列表中向前和向后翻页。

   - name ： 存储分段的唯一名称，不能更改。
   - S3 对象锁定：是否为此存储分段启用了 S3 对象锁定。

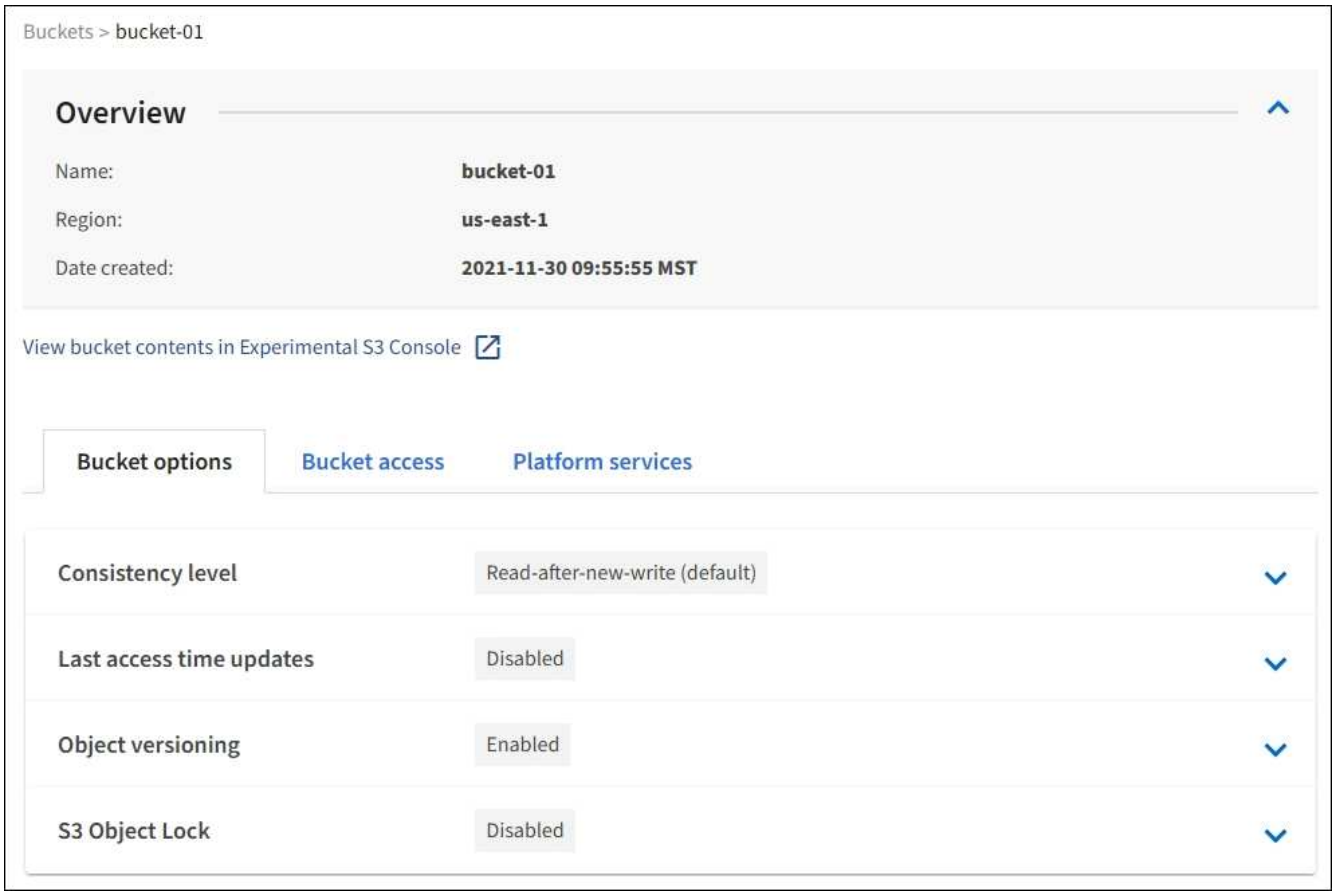
     如果禁用全局 S3 对象锁定设置，则不会显示此列。此列还会显示任何旧版合规存储分段的信息。

   - 区域：分段的区域，无法更改。
   - Object Count ： 此分段中的对象数。
   - 已用空间：此分段中所有对象的逻辑大小。逻辑大小不包括复制的或经过纠删编码的副本或对象元数据所需的实际空间。
   - Date created ： 创建存储分段的日期和时间。

   > 显示的对象计数和已用空间值为估计值。这些估计值受载入时间，网络连接和节点状态的影响。如果分段启用了版本控制，则删除的对象版本将包含在对象计数中。

3. 要查看和管理存储分段的设置，请选择存储分段名称。

   您可以通过存储分段详细信息页面查看和编辑存储分段选项，存储分段访问和的设置 平台服务。



更改一致性级别

如果您使用的是 S3 租户，则可以使用租户管理器或租户管理 API 来更改对 S3 分段中的对象执行的操作的一致性控制。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。请参见 租户管理权限。

关于此任务

一致性级别可在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。通常，您应该对存储分段使用 * 读 - 后 - 新 - 写 * 一致性级别。

如果*读后新写入*一致性级别不符合客户端应用程序的要求、则可以通过设置存储分段一致性级别或使用来更改一致性级别 `Consistency-Control` 标题。。 `Consistency-Control` 标题将覆盖存储分段一致性级别。

更改存储分段的一致性级别时，只会保证更改后载入的对象符合修订后的级别。

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。
2. 从列表中选择存储分段名称。

此时将显示存储分段详细信息页面。

3. 选择 * 分段选项 * > * 一致性级别 * 。
4. 为此存储分段中的对象选择一个一致性级别。
   - 全部：提供最高级别的一致性。所有节点都会立即接收数据，否则请求将失败。
   - 强-全局：保证所有站点中所有客户端请求的写入后读一致性。
   - 强站点：保证站点内所有客户端请求的写入后读一致性。
   - 读后新写入(默认)：为新对象提供读后写入一致性、并最终为对象更新提供一致性。提供高可用性和数据保护保证。建议用于大多数情况。
   - 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅根据需要使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行head或get操作)。S3 FabricPool 存储分段不支持。
5. 选择 * 保存更改 * 。

启用或禁用上次访问时间更新

当网格管理员为 StorageGRID 系统创建信息生命周期管理（ ILM ）规则时，他们可以选择指定对象的最后访问时间来确定是否将该对象移动到其他存储位置。如果您使用的是 S3 租户，则可以通过为 S3 存储分段中的对象启用上次访问时间更新来利用此类规则。

这些说明仅适用于至少包含一个在放置说明中使用 * 上次访问时间 * 选项的 ILM 规则的 StorageGRID 系统。如果您的 StorageGRID 系统不包含此类规则，则可以忽略这些说明。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。请参见 租户管理权限。

对于 ILM 规则， * 上次访问时间 * 是 * 参考时间 * 放置说明可用的选项之一。通过将规则的参考时间设置为上次访问时间，网格管理员可以根据上次检索（读取或查看）对象的时间指定将对象放置在某些存储位置。

例如，为了确保最近查看的对象保持在较快的存储上，网格管理员可以创建一个 ILM 规则，指定以下内容：

- 过去一个月检索到的对象应保留在本地存储节点上。
- 过去一个月未检索到的对象应移至异地位置。

请参见有关通过信息生命周期管理来管理对象的说明。

默认情况下，对上次访问时间的更新处于禁用状态。如果您的 StorageGRID 系统包含使用 * 上次访问时间 * 选项的 ILM 规则，并且您希望此选项应用于此存储分段中的对象，则必须为该规则中指定的 S3 存储分段启用对上次访问时间的更新。

在检索对象时更新上次访问时间会降低 StorageGRID 性能，尤其是对于小型对象。

上次访问时间更新会影响性能，因为每次检索对象时， StorageGRID 都必须执行以下附加步骤：

- 使用新的时间戳更新对象
- 将对象添加到 ILM 队列，以便根据当前 ILM 规则和策略对其进行重新评估

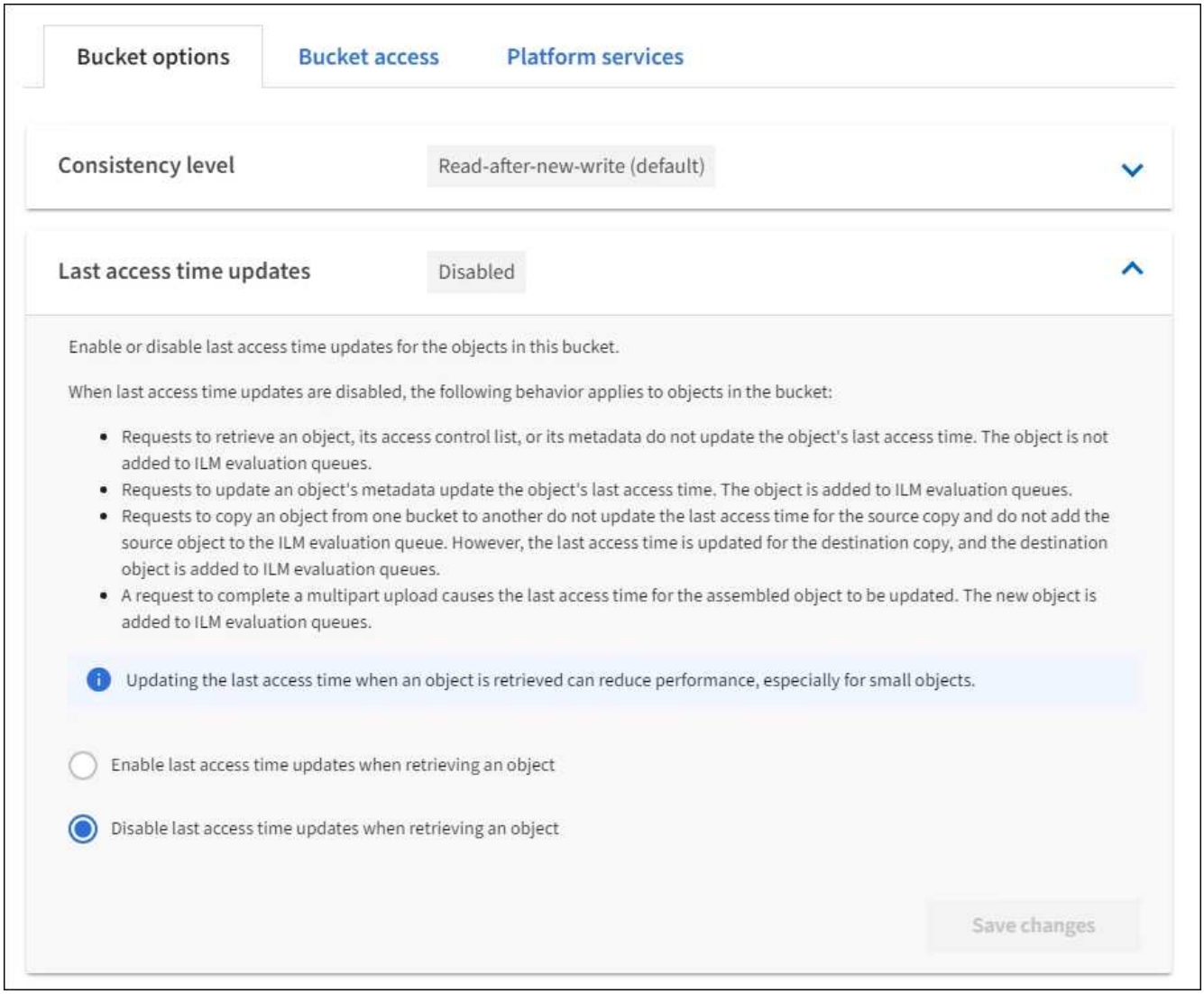
下表汇总了禁用或启用上次访问时间时应用于存储分段中所有对象的行为。

请求类型	禁用上次访问时间时的行为（默认）		启用上次访问时间时的行为	
	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?
请求检索对象，其访问控制列表或其元数据	否	否	是的。	是的。
请求更新对象的元数据	是的。	是的。	是的。	是的。
请求将对象从一个存储分段复制到另一个存储分段	• 否，对于源副本 • 是，对于目标副本	• 否，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本
请求完成多部分上传	是，对于已组装的对象	是，对于已组装的对象	是，对于已组装的对象	是，对于已组装的对象

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。
2. 从列表中选择存储分段名称。

   此时将显示存储分段详细信息页面。
3. 选择 * 分段选项 * > * 上次访问时间更新 * 。
4. 选择相应的单选按钮以启用或禁用上次访问时间更新。



5. 选择 * 保存更改 * 。

相关信息

租户管理权限

使用 ILM 管理对象

更改存储分段的对象版本控制

如果您使用的是 S3 租户，则可以使用租户管理器或租户管理 API 更改 S3 分段的版本控制状态。

您需要的内容

- 您将使用登录到租户管理器 支持的 Web 浏览器。
- 您属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。

  租户管理权限

关于此任务

您可以为存储分段启用或暂停对象版本控制。为存储分段启用版本控制后，它将无法恢复为未版本控制状态。但是，您可以暂停存储分段的版本控制。

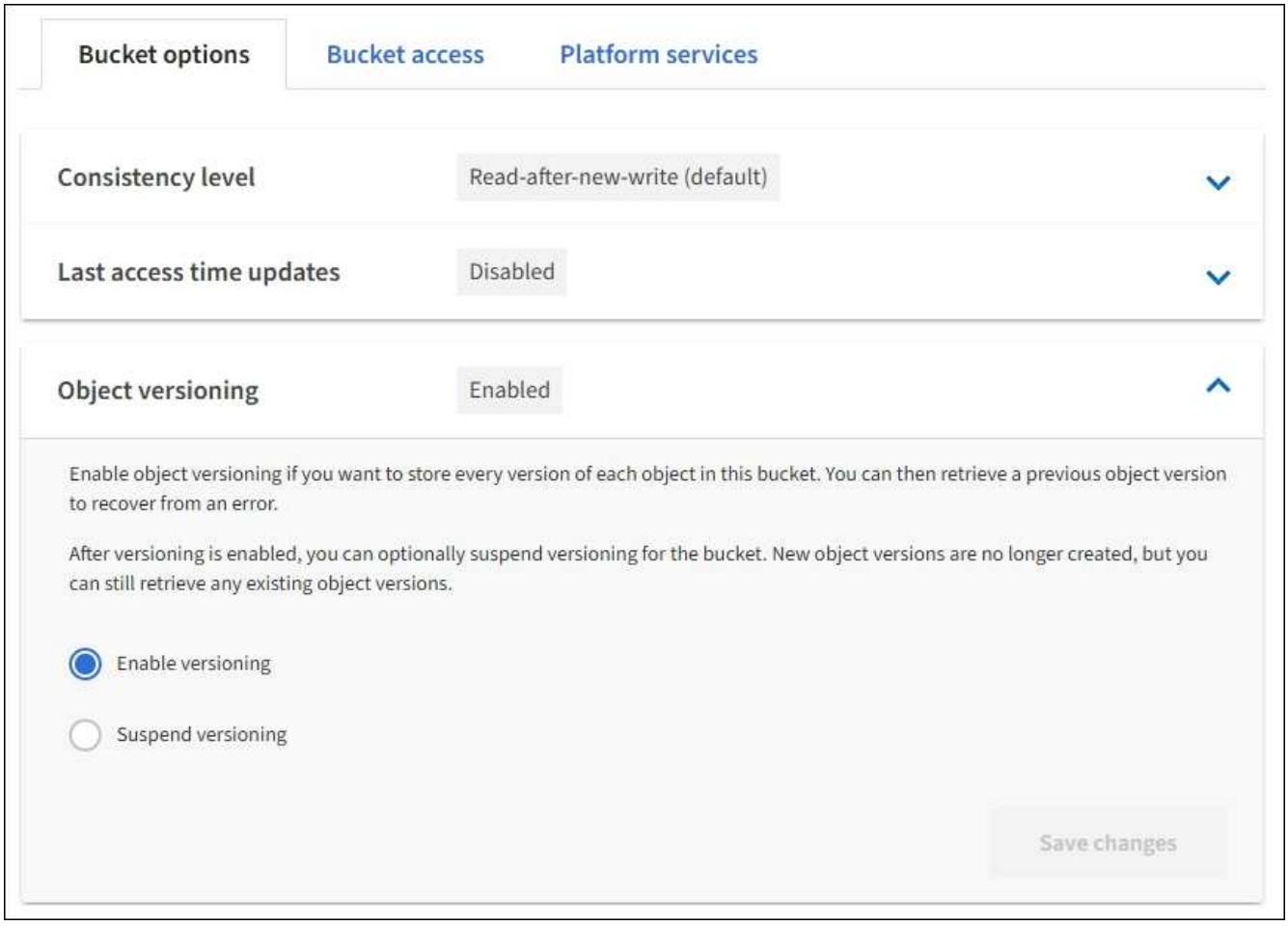
- Disabled ： 从未启用版本控制
- Enabled ： 已启用版本控制
- suspended ： 先前已启用版本控制并已暂停

S3 对象版本控制

S3 版本对象的 ILM 规则和策略（示例 4 ）

步骤

1. 选择 * 存储（ S3 ） * > * 分段 * 。
2. 从列表中选择存储分段名称。
3. 选择 * 分段选项 * > * 对象版本控制 * 。



4. 为此存储分段中的对象选择版本控制状态。

如果启用了 S3 对象锁定或原有合规性，则会禁用 * 对象版本控制 * 选项。

选项	Description
启用版本控制	如果要将每个对象的每个版本存储在此存储分段中，请启用对象版本控制。然后，您可以根据需要检索对象的先前版本。 用户修改存储分段中已存在的对象时，这些对象将进行版本控制。
暂停版本控制	如果您不再需要创建新的对象版本，请暂停对象版本控制。您仍然可以检索任何现有对象版本。

5. 选择 * 保存更改 * 。

配置跨源资源共享（ **CORS** ）

如果您希望 S3 存储分段中的存储分段和对象可供其他域中的 Web 应用程序访问，则可以为该存储分段配置跨源资源共享（ CORS ）。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。

关于此任务

跨源资源共享（ CORS ）是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如，假设您使用名为 `images` 的 S3 存储分段来存储图形。通过为 `images` 存储分段配置 CORS ，您可以允许该存储分段中的图像显示在网站 `http://www.example.com` 上。

步骤

1. 使用文本编辑器创建启用 CORS 所需的 XML 。

   此示例显示了用于为 S3 存储分段启用 CORS 的 XML 。此 XML 允许任何域向存储分段发送 GET 请求，但它仅允许 ` + http://www.example.com+` 域发送 POST 和 DELETE 请求。允许使用所有请求标头。

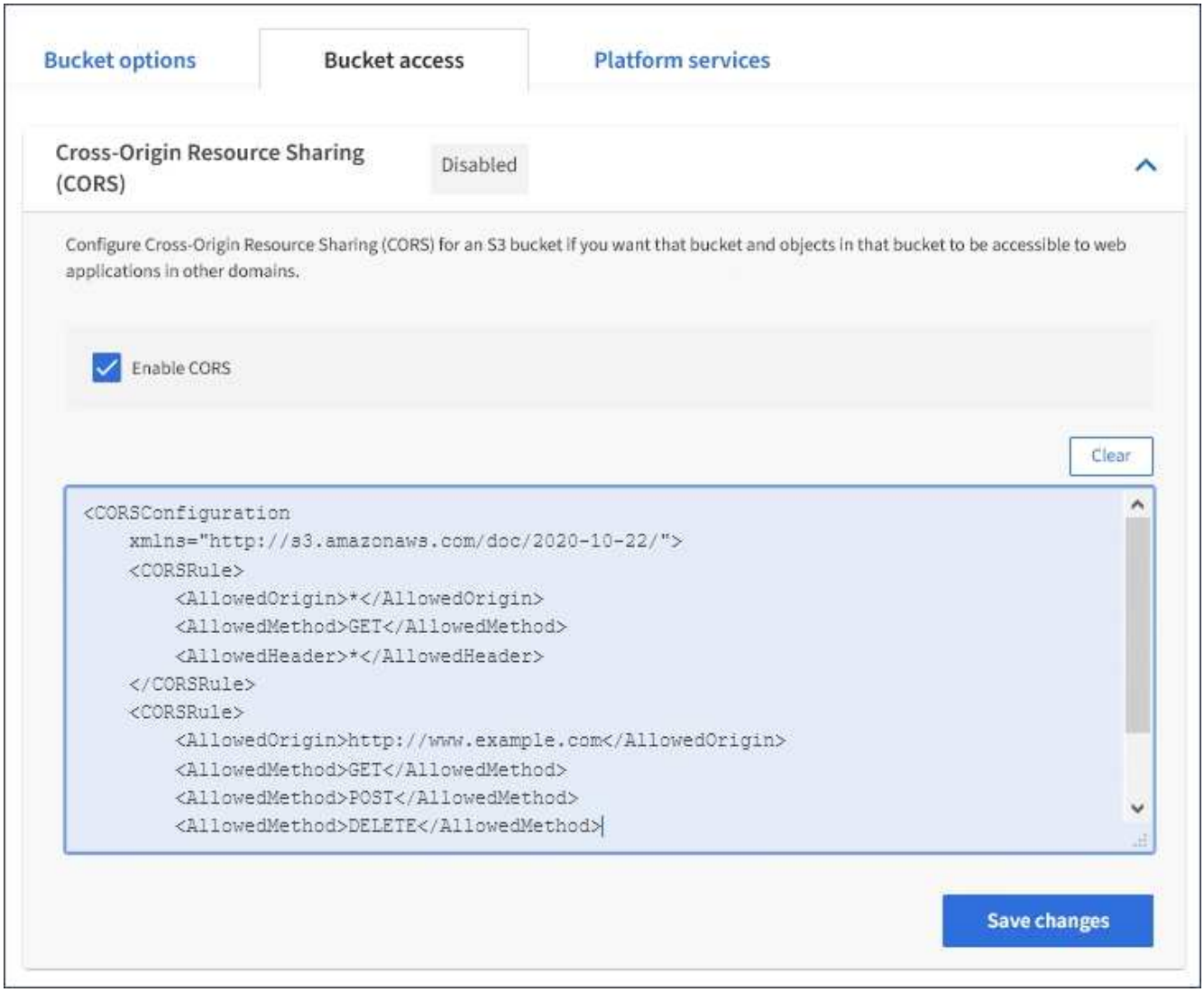
```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

有关 CORS 配置 XML 的详细信息，请参见 "Amazon Web Services （AWS ）文档：《 Amazon Simple Storage Service 开发人员指南》"。

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 从列表中选择存储分段名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 分段访问 * > * 跨源资源共享（ CORS ） * 。
5. 选中 * 启用 CORS* 复选框。
6. 将 CORS 配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。



7. 要修改存储分段的 CORS 设置，请在文本框中更新 CORS 配置 XML ，或者选择 * 清除 * 重新开始。然后选择 * 保存更改 * 。
8. 要为存储分段禁用 CORS ，请取消选中 * 启用 CORS* 复选框，然后选择 * 保存更改 * 。

删除 **S3** 存储分段

您可以使用租户管理器删除一个或多个空的 S3 分段。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组。这些权限将覆盖组或存储分段策略中的权限设置。请参见 租户管理权限。
- 要删除的存储分段为空。

关于此任务

以下说明介绍如何使用租户管理器删除 S3 存储分段。您也可以使用删除 S3 存储分段 租户管理 API 或 S3 REST API。

如果 S3 存储分段包含对象或非当前对象版本，则不能删除该存储分段。有关如何删除 S3 版本对象的信息，请

参见 有关通过信息生命周期管理来管理对象的说明。

步骤

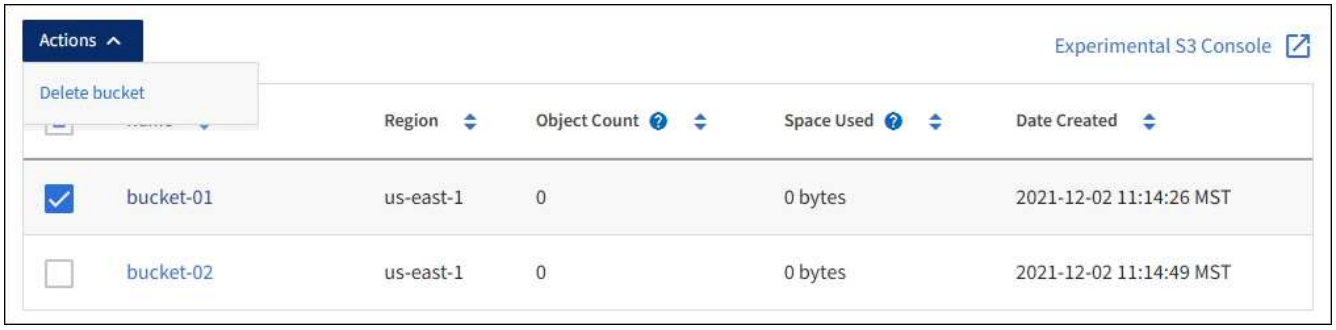
1. 选择 * 存储（ S3 ） * > * 分段 * 。

   此时将显示 " 分段 " 页面，其中会显示所有现有的 S3 分段。

2. 选中要删除的空存储分段对应的复选框。您可以一次选择多个存储分段。

   此时将启用操作菜单。

3. 从操作菜单中，选择 * 删除存储分段 * （或者如果选择了多个存储分段 * ，则选择 * 删除存储分段 * ）。



4. 显示确认对话框时，选择 * 是 * 可删除您选择的所有存储分段。

   StorageGRID 会确认每个存储分段均为空，然后删除每个存储分段。此操作可能需要几分钟时间。

   如果存储分段不为空，则会显示一条错误消息。必须先删除所有对象，然后才能删除存储分段。

使用试验性 **S3** 控制台

您可以使用 S3 控制台查看 S3 存储分段中的对象。

您也可以使用 S3 控制台执行以下操作：

- 添加和删除对象，对象版本和文件夹
- 重命名对象
- 在分段和文件夹之间移动和复制对象
- 管理对象标记
- 查看对象元数据
- 下载对象

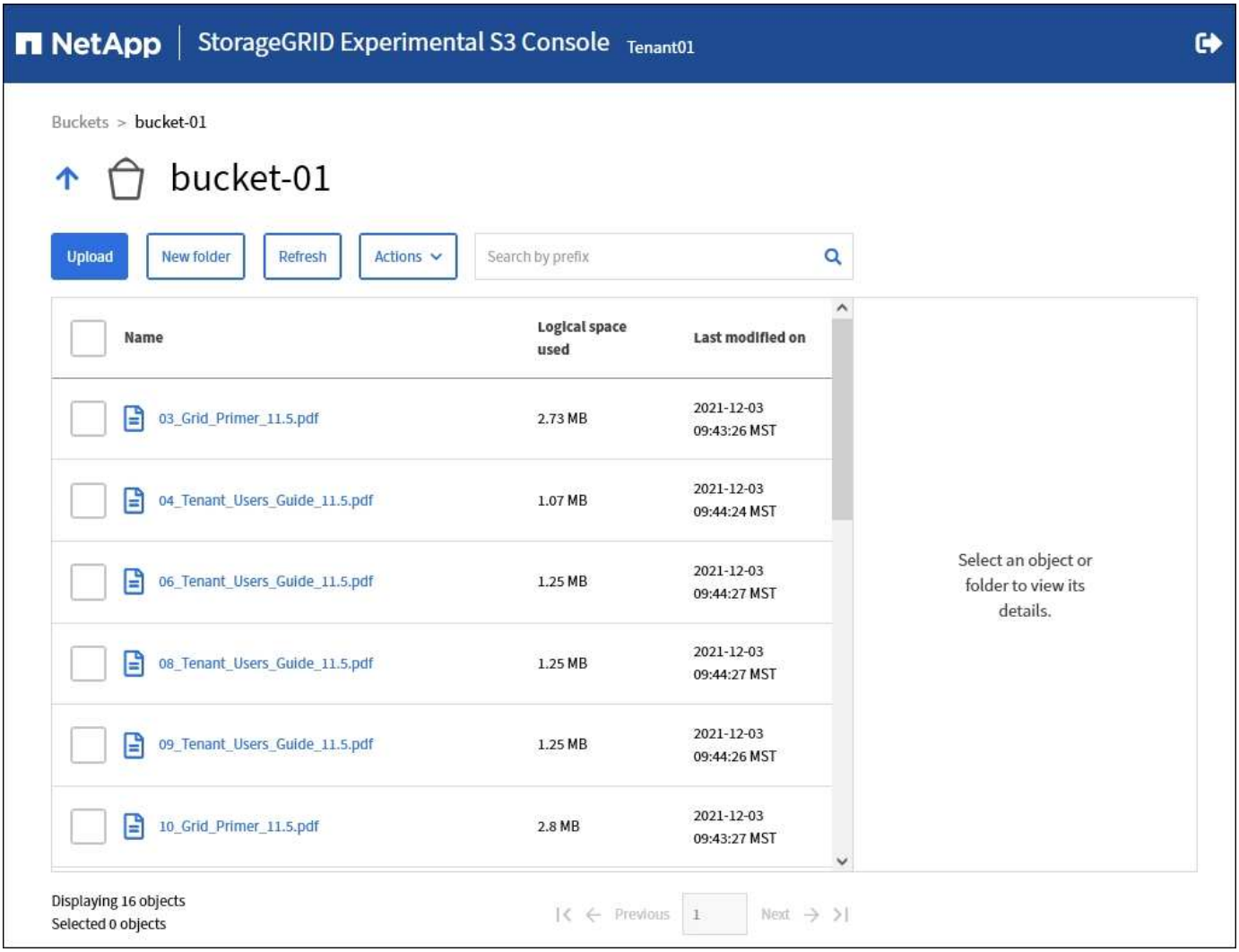
S3 控制台尚未经过全面测试，并标记为 " 试验 " 。 它不适用于对象的批量管理或在生产环境中使用。只有在为少量对象执行功能时，租户才应使用 S3 控制台，例如上传对象以模拟新的 ILM 策略，排除载入问题或使用概念验证或非生产网格。

您需要的内容

- 您将使用登录到租户管理器 支持的 Web 浏览器。
- 您具有管理自己的 S3 凭据权限。
- 您已创建存储分段。
- 您知道用户的访问密钥 ID 和机密访问密钥。您也可以使用包含此信息的 ` .csv` 文件。请参见 创建访问密钥的说明。

步骤

1. 选择 * 分段 * 。
2. 选择 … Experimental S3 Console 。您也可以从存储分段详细信息页面访问此链接。
3. 在试验性 S3 控制台登录页面上，将访问密钥 ID 和机密访问密钥粘贴到字段中。否则，请选择 * 上传访问密钥 * 并选择您的 ` .csv` 文件。
4. 选择 * 登录 * 。
5. 根据需要管理对象。



管理 S3 平台服务

什么是平台服务?

StorageGRID 平台服务可以帮助您实施混合云战略。

如果您的租户帐户允许使用平台服务，则可以为任何 S3 存储分段配置以下服务：

- * CloudMirror 复制 *： StorageGRID CloudMirror 复制服务 用于将特定对象从 StorageGRID 存储分段镜像到指定的外部目标。

  例如，您可以使用 CloudMirror 复制将特定客户记录镜像到 Amazon S3 ，然后利用 AWS 服务对数据执行分析。

  > 如果源存储分段启用了 S3 对象锁定，则不支持 CloudMirror 复制。

- * 通知 *： 每个存储分段的事件通知 用于向指定的外部 Amazon Simple Notification Service （ SNS ）发送有关对对象执行的特定操作的通知。

  例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

虽然可以在启用了 S3 对象锁定的存储分段上配置事件通知，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留至日期和合法保留状态）。

- * 搜索集成服务 * ： 搜索集成服务 用于将 S3 对象元数据发送到指定的 Elasticsearch 索引，在此索引中可以使用外部服务搜索或分析元数据。

  例如，您可以将存储分段配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 跨存储分段执行搜索，并对对象元数据中存在的模式执行复杂的分析。

  虽然可以在启用了 S3 对象锁定的情况下在存储分段上配置 Elasticsearch 集成，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留截止日期和合法保留状态）。

由于平台服务的目标位置通常不在 StorageGRID 部署中，因此平台服务可以为您提供使用外部存储资源，通知服务以及数据搜索或分析服务所带来的强大功能和灵活性。

可以为一个 S3 存储分段配置任何平台服务组合。例如，您可以在 StorageGRID S3 存储分段上配置 CloudMirror 服务和通知，以便将特定对象镜像到 Amazon Simple Storage Service ，同时向第三方监控应用程序发送有关每个此类对象的通知，以帮助您跟踪 AWS 支出。

StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。

如何配置平台服务

平台服务与您使用租户管理器或租户管理 API 配置的外部端点进行通信。每个端点都代表一个外部目标，例如 StorageGRID S3 存储分段， Amazon Web 服务分段，简单通知服务（ SNS ）主题或本地托管， AWS 或其他位置的 Elasticsearch 集群。

创建端点后，您可以通过向存储分段添加 XML 配置来为存储分段启用平台服务。XML 配置可确定存储分段应处理的对象，存储分段应执行的操作以及存储分段应用于服务的端点。

您必须为要配置的每个平台服务添加单独的 XML 配置。例如：

1. 如果要将密钥以 ` 或 images` 开头的所有对象复制到 Amazon S3 存储分段，则必须向源存储分段添加复制配置。
2. 如果您还希望在这些对象存储到存储分段时发送通知，则必须添加通知配置。
3. 最后，如果要为这些对象的元数据编制索引，则必须添加用于实施搜索集成的元数据通知配置。

配置 XML 的格式由用于实施 StorageGRID 平台服务的 S3 REST API 控制：

平台服务	**S3 REST API**
CloudMirror 复制	• 获取存储分段复制 • PUT 存储分段复制
通知	• 获取存储分段通知 • PUT 存储分段通知

平台服务	**S3 REST API**
搜索集成	• 获取存储分段元数据通知配置 • PUT 存储分段元数据通知配置 这些操作是 StorageGRID 的自定义操作。

有关 StorageGRID 如何实施这些 API 的详细信息，请参见有关实施 S3 客户端应用程序的说明。

相关信息

使用平台服务的注意事项

使用 S3

CloudMirror 复制服务

如果您希望 StorageGRID 将添加到 S3 存储分段的指定对象复制到一个或多个目标存储分段，则可以为该存储分段启用 CloudMirror 复制。

CloudMirror 复制独立于网格的活动 ILM 策略运行。CloudMirror 服务会在将对象存储到源存储分段时复制这些对象，并尽快将其交付到目标存储分段。对象载入成功后，系统将触发复制对象的传送。

如果为现有存储分段启用 CloudMirror 复制，则只会复制添加到该存储分段的新对象。不会复制存储分段中的任何现有对象。要强制复制现有对象，您可以通过执行对象复制来更新现有对象的元数据。

> 如果您使用 CloudMirror 复制将对象复制到 AWS S3 目标，请注意 Amazon S3 将每个 PUT 请求标头中用户定义的元数据的大小限制为 2 KB 。如果对象的用户定义元数据大于 2 KB ，则不会复制该对象。

在 StorageGRID 中，您可以将单个存储分段中的对象复制到多个目标存储分段。为此，请为复制配置 XML 中的每个规则指定目标。不能将对象同时复制到多个存储分段。

此外，您还可以在受版本控制或未受版本控制的分段上配置 CloudMirror 复制，并可以指定受版本控制或未受版本控制的分段作为目标。您可以使用版本控制和未版本控制的分段的任意组合。例如，您可以将版本控制的存储分段指定为未版本控制的源存储分段的目标，反之亦然。您还可以在未版本控制的存储分段之间进行复制。

CloudMirror 复制服务的删除行为与 Amazon S3 提供的跨区域复制（ CRR ）服务的删除行为相同—删除源存储分段中的对象绝不会删除目标中的复制对象。如果源和目标存储分段都已进行版本控制，则会复制删除标记。如果目标分段未进行版本控制，则删除源分段中的对象不会将删除标记复制到目标分段或删除目标对象。

当对象复制到目标存储分段时， StorageGRID 会将其标记为 `replicas` 。 目标 StorageGRID 存储分段不会再次复制标记为副本的对象，从而防止意外复制环路。此副本标记是 StorageGRID 的内部标记，不会阻止您在使用 Amazon S3 存储分段作为目标时利用 AWS CRR 。

> 用于标记副本的自定义标头为 `x-ntap-sg-replica` 。此标记可防止级联镜像。StorageGRID 确实支持在两个网格之间使用双向 CloudMirror 。

无法保证目标存储分段中事件的唯一性和顺序。由于为确保成功交付而执行的操作，可能会将一个源对象的多个相同副本传送到目标。在极少数情况下，如果从两个或更多不同的 StorageGRID 站点同时更新同一对象，则目标存储分段上的操作顺序可能与源存储分段上的事件顺序不匹配。

CloudMirror 复制通常配置为使用外部 S3 存储分段作为目标。但是，您也可以将复制配置为使用另一个 StorageGRID 部署或任何与 S3 兼容的服务。

了解存储分段通知

如果您希望 StorageGRID 向目标 Amazon Simple Notification Service （ SNS ）发送有关指定事件的通知，则可以为 S3 存储分段启用事件通知。

您可以 配置事件通知 通过将通知配置 XML 与源存储分段相关联。通知配置 XML 遵循 S3 配置存储分段通知的约定，并将目标 SNS 主题指定为端点的 URN 。

事件通知在通知配置中指定的源存储分段处创建，并传送到目标。如果与某个对象关联的事件成功，则会创建有关该事件的通知并排队等待传送。

不保证通知的唯一性和顺序。由于为保证成功交付而执行的操作，可能会向目标发送多个事件通知。由于交付是异步的，因此无法保证目标上通知的时间顺序与源存储分段上事件的顺序一致，尤其是对于来自不同 StorageGRID 站点的操作。您可以在事件消息中使用 `sEquencer` 键来确定特定对象的事件顺序，如 Amazon S3 文档中所述。

支持的通知和消息

StorageGRID 事件通知遵循 Amazon S3 API ，但存在以下限制：

- 您不能为以下事件类型配置通知。这些事件类型 * 不 * 受支持。
  - `s 3 ：异径冗余 LostObject`
  - `s 3 ： ObjectRestore ：已完成`
- 从 StorageGRID 发送的事件通知使用标准 JSON 格式，只是它们不包含某些密钥，而对其他密钥使用特定值，如下表所示：

密钥名称	**StorageGRID** 值
事件源	`sGWS ： S3`
awsRegion	不包括
X-AMZ-ID-2	不包括
ARN	`urn ： sgws ： s3 ：：： bucket_name`

了解搜索集成服务

如果要对对象元数据使用外部搜索和数据分析服务，则可以为 S3 存储分段启用搜索集成。

搜索集成服务是一种自定义 StorageGRID 服务，每当更新对象或其元数据时，该服务都会自动异步地将 S3 对象元数据发送到目标端点。然后，您可以使用目标服务提供的复杂搜索，数据分析，可视化或机器学习工具来搜索，分析对象数据并从中获得洞察力。

您可以为任何版本控制或未版本控制的存储分段启用搜索集成服务。搜索集成是通过将元数据通知配置 XML 与用于指定要对哪些对象执行操作的存储分段以及对象元数据的目标进行关联来配置的。

通知以 JSON 文档的形式生成，该文档使用分段名称，对象名称和版本 ID （如果有）命名。除了对象的所有标记和用户元数据之外，每个元数据通知还包含一组标准的对象系统元数据。

> 对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后，您无法在索引中编辑文档的字段类型。

每当出现以下情况时，都会生成通知并将其排队以供传送：

- 已创建对象。
- 删除对象，包括因网格的 ILM 策略操作而删除对象的时间。
- 添加，更新或删除对象元数据或标记。更新时始终会发送一组完整的元数据和标记，而不仅仅是更改后的值。

将元数据通知配置 XML 添加到存储分段后，系统会为您创建的任何新对象以及您通过更新其数据，用户元数据或标记来修改的任何对象发送通知。但是，不会为存储分段中已有的任何对象发送通知。要确保将存储分段中所有对象的对象元数据发送到目标，应执行以下任一操作：

- 创建存储分段后以及添加任何对象之前，请立即配置搜索集成服务。
- 对存储分段中已有的所有对象执行操作，此操作将触发元数据通知消息以发送到目标。

StorageGRID 搜索集成服务支持将 Elasticsearch 集群作为目标。与其他平台服务一样，目标也会在端点中指定，而此端点的 URN 会在该服务的配置 XML 中使用。使用 "NetApp 互操作性表工具" 确定支持的 Elasticsearch 版本。

相关信息

用于搜索集成的配置 XML

元数据通知中包含的对象元数据

由搜索集成服务生成的 JSON

配置搜索集成服务

使用平台服务的注意事项

在实施平台服务之前，请查看有关使用这些服务的建议和注意事项。

有关 S3 的信息，请参见 使用 S3。

使用平台服务的注意事项

注意事项	详细信息
目标端点监控	您必须监控每个目标端点的可用性。如果与目标端点的连接长时间断开，并且存在大量请求积压，则向 StorageGRID 发出的其他客户端请求（例如 PUT 请求）将失败。当端点可访问时，您必须重试这些失败的请求。
目标端点限制	如果发送请求的速率超过目标端点接收请求的速率， StorageGRID 软件可能会限制传入的存储分段 S3 请求。只有在等待发送到目标端点的请求积压时，才会发生限制。 唯一明显的影响是，传入的 S3 请求执行时间较长。如果您开始检测到性能明显较慢，则应降低载入速率或使用容量较高的端点。如果积压的请求持续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。 CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求所涉及的数据传输通常多于搜索集成或事件通知请求。
订购担保	StorageGRID 保证对站点中的对象执行操作的顺序。只要针对某个对象的所有操作都位于同一站点内，最终对象状态（用于复制）就始终等于 StorageGRID 中的状态。 在跨 StorageGRID 站点执行操作时， StorageGRID 会尽力订购请求。例如，如果您先将某个对象写入站点 A ，然后覆盖站点 B 上的同一个对象，则 CloudMirror 复制到目标分段的最终对象不能保证为较新的对象。
ILM 驱动的对象删除	为了匹配 AWS CRR 和 SNS 服务的删除行为，如果因 StorageGRID ILM 规则而删除源存储分段中的对象，则不会发送 CloudMirror 和事件通知请求。例如，如果 ILM 规则在 14 天后删除某个对象，则不会发送 CloudMirror 或事件通知请求。 相反，在因 ILM 而删除对象时，系统会发送搜索集成请求。

使用 **CloudMirror** 复制服务的注意事项

注意事项	详细信息
复制状态	StorageGRID 不支持 `x-AMZ-reply-status` 标头。
对象大小	CloudMirror 复制服务可复制到目标分段的对象的最大大小为 5 TiB ，与最大 _supported 对象大小相同。 • 注 * ： 单个 PUT 对象操作的最大 _recommended_size 为 5 GiB （ 5 ， 368 ， 709 ， 120 字节）。如果对象大于 5 GiB ，请改用多部分上传。

注意事项	详细信息
存储分段版本控制和版本 ID	如果 StorageGRID 中的源 S3 存储分段已启用版本控制，则还应为目标存储分段启用版本控制。 使用版本控制时，请注意，由于 S3 协议的限制，在目标存储分段中排列对象版本是尽力而为的， CloudMirror 服务无法保证这一点。 • 注意 *： StorageGRID 中源存储分段的版本 ID 与目标存储分段的版本 ID 无关。
标记对象版本	由于 S3 协议的限制， CloudMirror 服务不会复制任何提供版本 ID 的 PUT 对象标记或删除对象标记请求。由于源和目标的版本 ID 不相关，因此无法确保复制对特定版本 ID 的标记更新。 相反， CloudMirror 服务会复制不指定版本 ID 的 PUT 对象标记请求或删除对象标记请求。这些请求会更新最新密钥的标记（如果分段已受版本控制，则更新最新版本的标记）。此外，还会复制具有标记（而不是标记更新）的常规载入。
多部分上传和 `ETag` 值	镜像使用多部分上传方式上传的对象时， CloudMirror 服务不会保留这些部分。因此，镜像对象的 `ETag` 值将与原始对象的 `ETag` 值不同。
使用 SSI-C 加密的对象（使用客户提供的密钥进行服务器端加密）	CloudMirror 服务不支持使用 SSI-C 加密的对象如果您尝试将对象载入源存储分段以进行 CloudMirror 复制，并且此请求包含 SSI-C 请求标头，则此操作将失败。
已启用 S3 对象锁定的存储分段	如果用于 CloudMirror 复制的目标 S3 存储分段已启用 S3 对象锁定，则配置存储分段复制（ PUT 存储分段复制）的尝试将失败，并显示 AccessDenied 错误。

配置平台服务端点

在为存储分段配置平台服务之前，必须至少将一个端点配置为平台服务的目标。

StorageGRID 管理员可以按租户访问平台服务。要创建或使用平台服务端点，您必须是具有 " 管理端点 " 或 " 根访问 " 权限的租户用户，并且此用户所在的网格已配置为允许存储节点访问外部端点资源。有关详细信息，请与 StorageGRID 管理员联系。

什么是平台服务端点?

创建平台服务端点时，您可以指定 StorageGRID 访问外部目标所需的信息。

例如，如果要将对象从 StorageGRID 存储分段复制到 AWS S3 存储分段，则可以创建一个平台服务端点，其中包含 StorageGRID 访问 AWS 上的目标存储分段所需的信息和凭据。

每种类型的平台服务都需要自己的端点，因此您必须为计划使用的每个平台服务至少配置一个端点。定义平台服务端点后，您可以在用于启用此服务的配置 XML 中使用此端点的 URN 作为目标。

您可以对多个源存储分段使用与目标相同的端点。例如，您可以配置多个源分段，将对象元数据发送到同一搜索集成端点，以便可以跨多个分段执行搜索。您还可以将源分段配置为使用多个端点作为目标，这样您可以执行以下操作：向一个 SNS 主题发送有关对象创建的通知，向另一个 SNS 主题发送有关对象删除的通知。

用于 **CloudMirror** 复制的端点

StorageGRID 支持表示 S3 存储分段的复制端点。这些存储分段可能托管在 Amazon Web Services ，相同或远程 StorageGRID 部署或其他服务上。

通知的端点

StorageGRID 支持简单通知服务（ SNS ）端点。不支持简单队列服务（ SQS ）或 AWS Lambda 端点。

搜索集成服务的端点

StorageGRID 支持表示 Elasticsearch 集群的搜索集成端点。这些 Elasticsearch 集群可以位于本地数据中心，也可以托管在 AWS 云或其他位置。

搜索集成端点是指特定的 Elasticsearch 索引和类型。您必须先在 Elasticsearch 中创建索引，然后才能在 StorageGRID 中创建端点，否则端点创建将失败。在创建端点之前，您无需创建类型。如果需要，StorageGRID 将在向端点发送对象元数据时创建此类型。

相关信息

管理 StorageGRID

为平台服务端点指定 **URN**

创建平台服务端点时，必须指定唯一资源名称（ URN ）。在为平台服务创建配置 XML 时，您将使用 URN 引用此端点。每个端点的 URN 必须是唯一的。

StorageGRID 会在您创建平台服务端点时对其进行验证。在创建平台服务端点之前，请确认此端点中指定的资源存在且可访问。

urn 元素

平台服务端点的 URN 必须以 `arn ： AWS` 或 `urn ： mysite` 开头，如下所示：

- 如果此服务托管在 Amazon Web Services （ AWS ）上，请使用 `arn ： AWS` 。
- 如果此服务托管在 Google Cloud Platform （ GCP ）上，请使用 `arn ： AWS` 。
- 如果服务托管在本地，请使用 `urn ： mysite`

例如，如果要为 StorageGRID 上托管的 CloudMirror 端点指定 URN ，则 URN 可能以 `urn ： sgws` 开头。

URN 的下一个元素用于指定平台服务的类型，如下所示：

服务	**Type**
CloudMirror 复制	S3
通知	SnS
搜索集成	ES

例如，要继续为 StorageGRID 上托管的 CloudMirror 端点指定 URN ，您应添加 `s 3` 以获取 `urn ： sgws ： S3` 。

URN 的最后一个元素用于标识目标 URI 上的特定目标资源。

服务	特定资源
CloudMirror 复制	分段名称
通知	Sns-topic-name
搜索集成	`domain-name/index-name/type-name` • 注意： * 如果 Elasticsearch 集群已配置为 * 不 * 自动创建索引，则必须在创建端点之前手动创建索引。

AWS 和 **GCP** 上托管的服务的 **urns**

对于 AWS 和 GCP 实体，完整的 URN 是有效的 AWS ARN 。例如：

- CloudMirror 复制：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 搜索集成：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> 对于 AWS 搜索集成端点， `domain-name` 必须包含文字字符串 `domain/` ，如下所示。

用于本地托管服务的 **urns**

使用本地托管的服务而非云服务时，只要 URN 在第三个和最后一个位置包含所需的元素，您就可以以任何方式指定 URN 以创建有效且唯一的 URN 。您可以将可选元素留空，也可以通过任何方式指定这些元素，以帮助您标识资源并使 URN 具有唯一性。例如：

- CloudMirror 复制：

```
urn:mysite:s3:optional:optional:bucket-name
```

对于 StorageGRID 上托管的 CloudMirror 端点，您可以指定以 `urn ： sgws` 开头的有效 URN ：

```
urn:sgws:s3:optional:optional:bucket-name
```

- 通知：

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- 搜索集成：

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> 对于本地托管的搜索集成端点，只要端点的 URN 是唯一的， `domain-name` element 就可以是任意字符串。

创建平台服务端点

必须至少创建一个正确类型的端点，然后才能启用平台服务。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须属于具有管理端点权限的用户组。
- 必须已创建平台服务端点引用的资源：
  - CloudMirror 复制： S3 存储分段
  - 事件通知： SnS 主题
  - 搜索通知： Elasticsearch index ，如果目标集群未配置为自动创建索引。
- 您必须具有有关目标资源的信息：
  - 统一资源标识符（ URI ）的主机和端口

    > 如果您计划使用 StorageGRID 系统上托管的存储分段作为 CloudMirror 复制的端点，请联系网格管理员以确定需要输入的值。

  - 唯一资源名称（ URN ）

    为平台服务端点指定 URN

  - 身份验证凭据（如果需要）：
    - 访问密钥：访问密钥 ID 和机密访问密钥
    - 基本 HTTP ： 用户名和密码

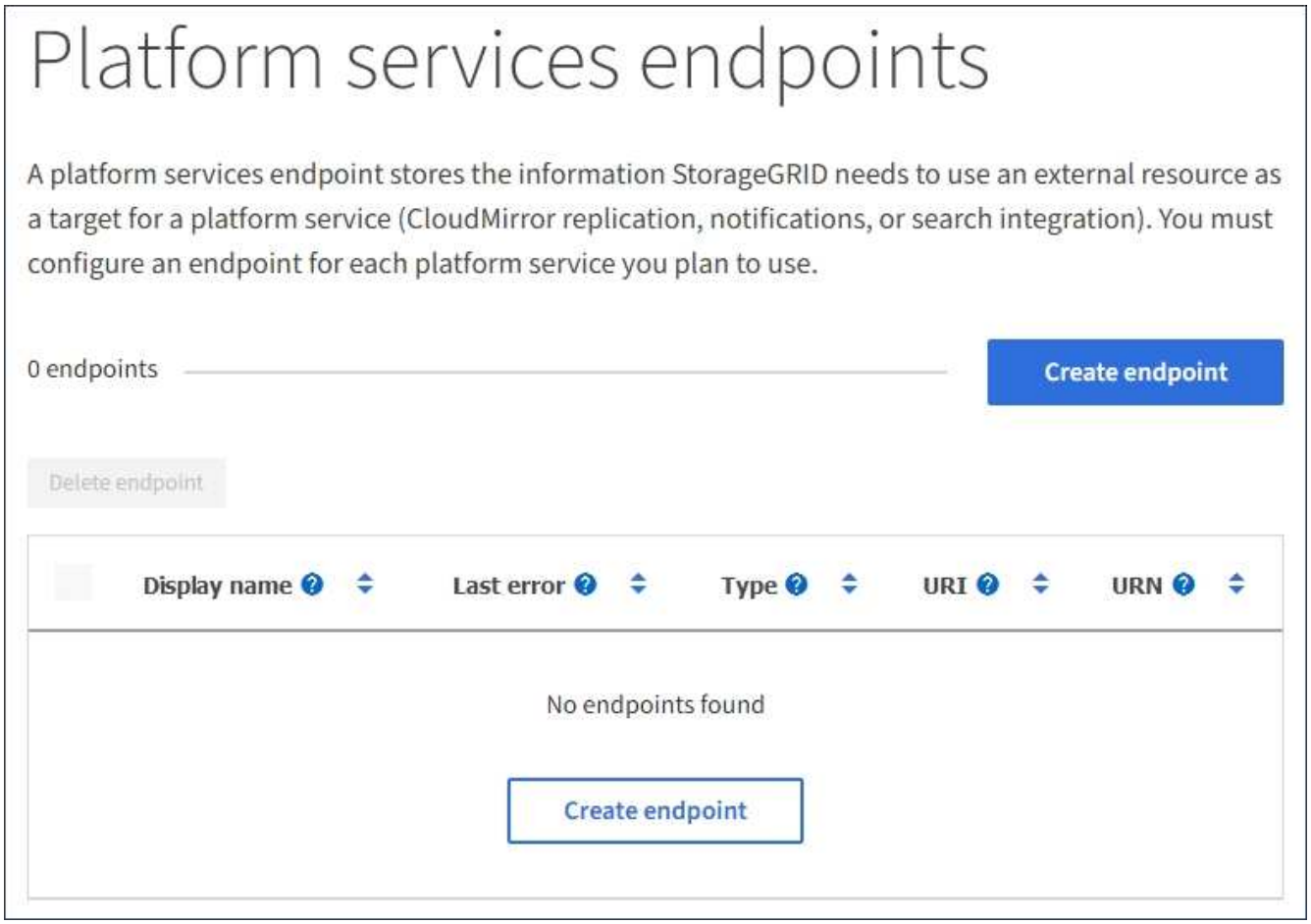
- CAP （ C2S 访问门户）：临时凭据 URL ，服务器和客户端证书，客户端密钥以及可选的客户端专用密钥密码短语。

◦ 安全证书（如果使用自定义 CA 证书）

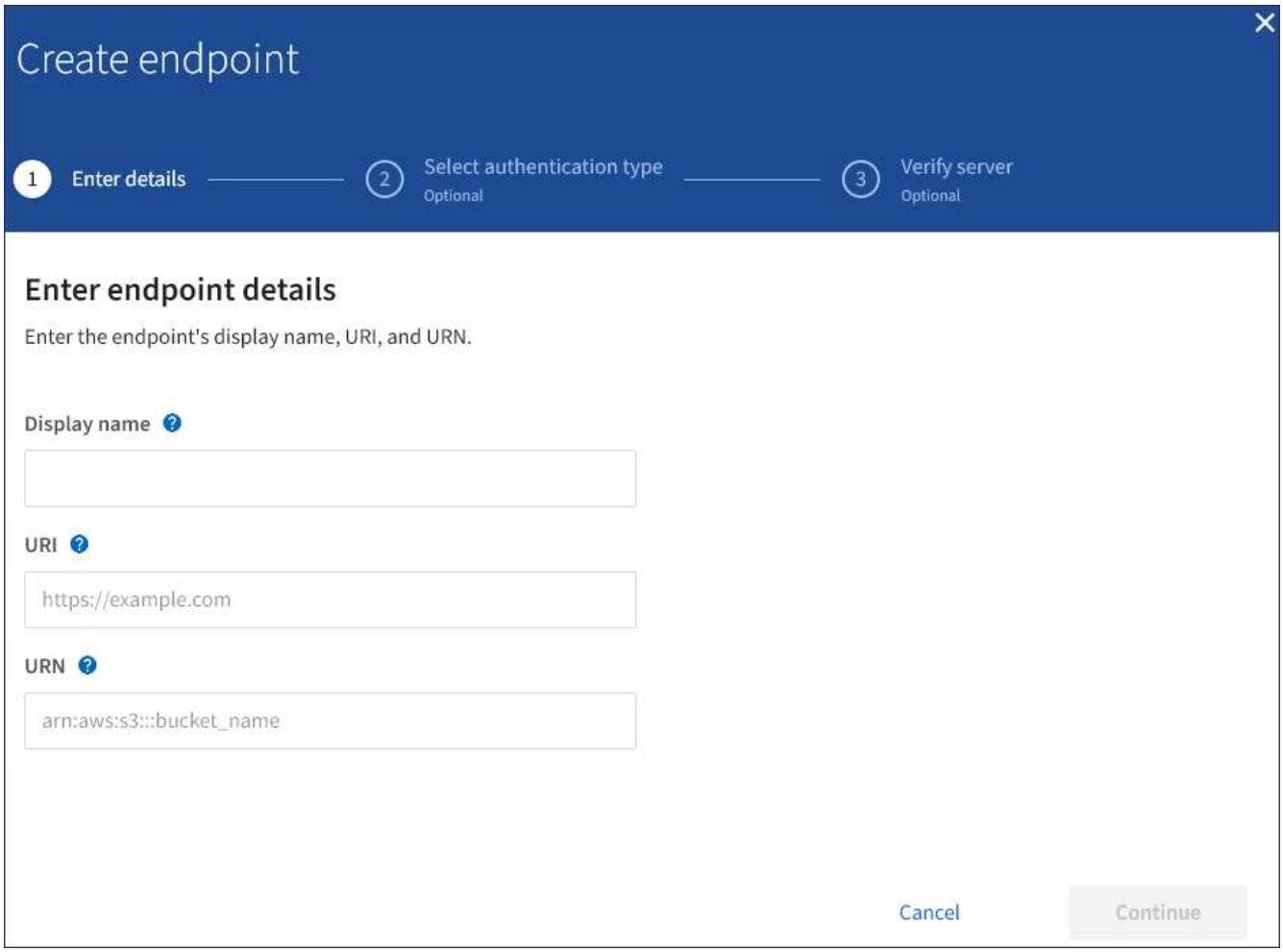
步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面。



2. 选择 * 创建端点 * 。



3. 输入显示名称以简要说明端点及其用途。

   端点支持的平台服务类型会显示在端点页面上列出的端点名称旁边，因此您无需在此名称中包含此信息。

4. 在 * URI * 字段中，指定端点的唯一资源标识符（ URI ）。

   请使用以下格式之一：

   ```
   https://host:port
   http://host:port
   ```

   如果未指定端口，则端口 443 用于 HTTPS URI ，端口 80 用于 HTTP URI 。

   例如， StorageGRID 上托管的存储分段的 URI 可能为：

   ```
   https://s3.example.com:10443
   ```

   在此示例中， `s3.example.com` 表示 StorageGRID 高可用性（ HA ）组的虚拟 IP （ VIP ）的 DNS 条目， `10443` 表示负载平衡器端点中定义的端口。

应尽可能连接到负载平衡节点的HA组、以避免单点故障。

同样， AWS 上托管的存储分段的 URI 可能为：

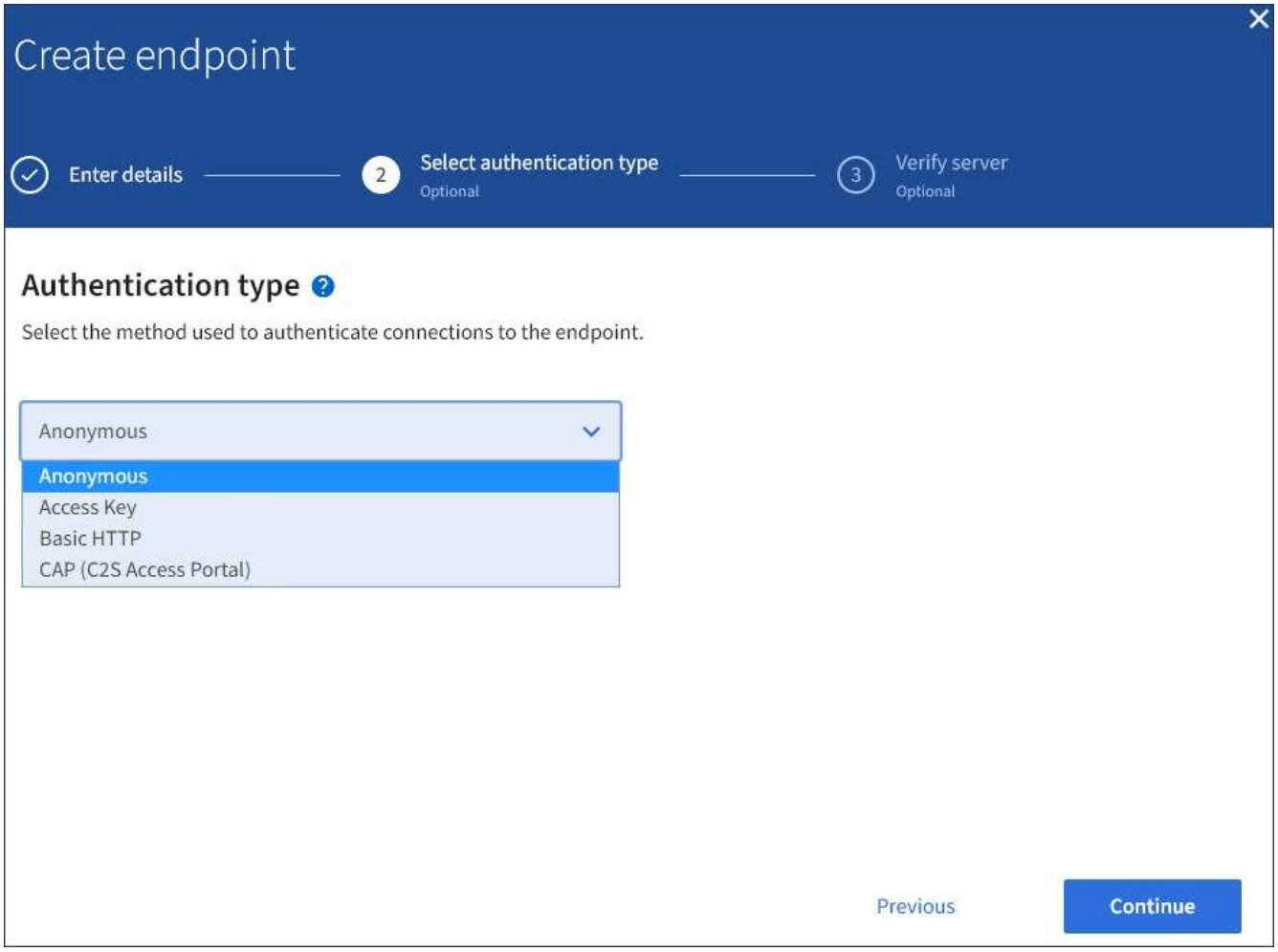
```
https://s3-aws-region.amazonaws.com
```

如果端点用于 CloudMirror 复制服务，请勿在 URI 中包含分段名称。您可以在 * URN* 字段中包含分段名称。

5. 输入端点的唯一资源名称（ URN ）。

创建端点后，您无法更改端点的 URN 。

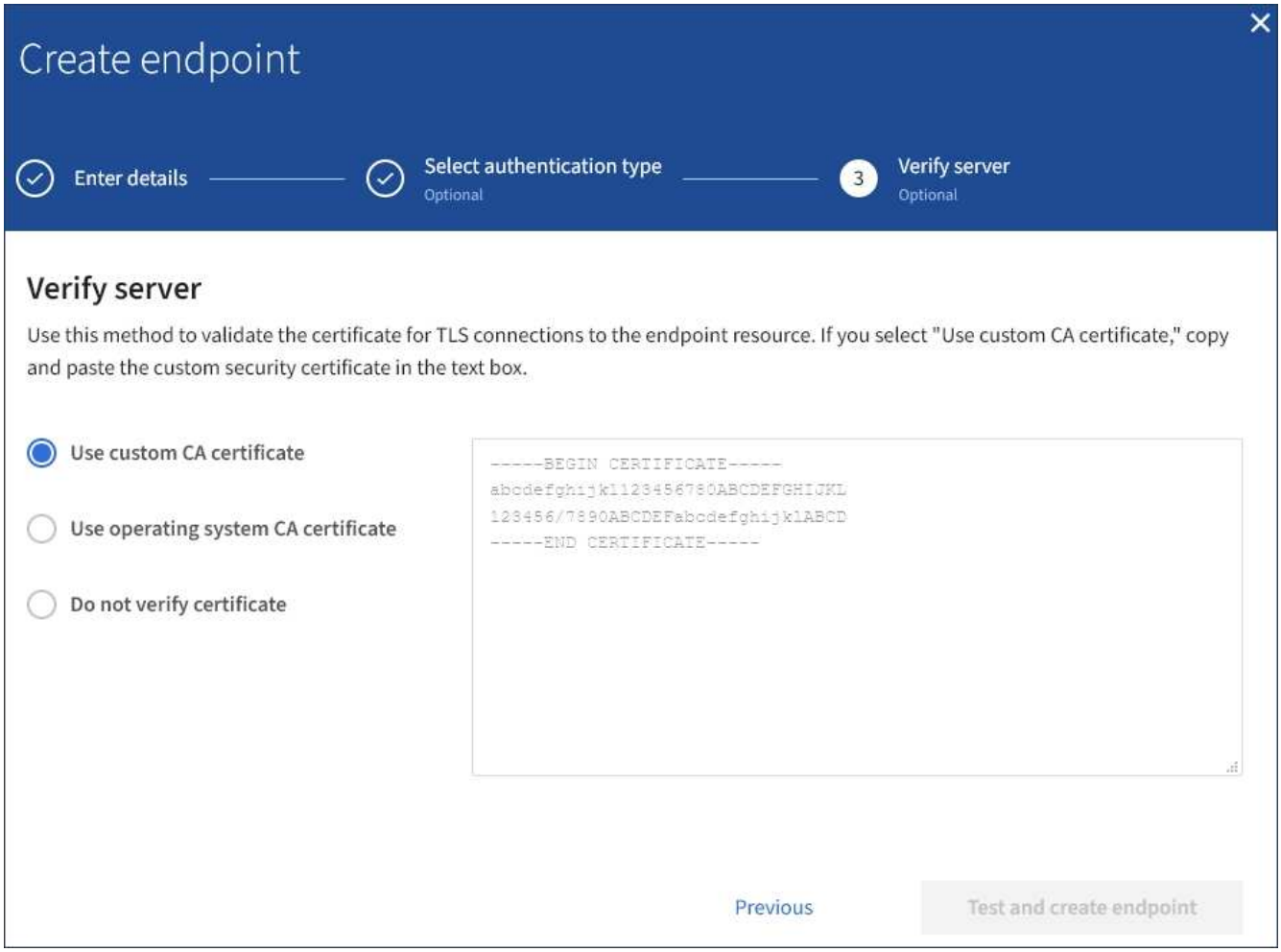
6. 选择 * 继续 * 。
7. 为 * 身份验证类型 * 选择一个值，然后输入或上传所需的凭据。



您提供的凭据必须具有目标资源的写入权限。

Authentication type	Description	凭据
匿名	提供对目标的匿名访问。仅适用于已禁用安全性的端点。	无身份验证。
访问密钥	使用 AWS 模式的凭据对与目标的连接进行身份验证。	• 访问密钥 ID • 机密访问密钥
基本 HTTP	使用用户名和密码对目标连接进行身份验证。	• Username • Password
CAP （ C2S 访问门户）	使用证书和密钥对目标连接进行身份验证。	• 临时凭据 URL • 服务器 CA 证书（ PEM 文件上传） • 客户端证书（ PEM 文件上传） • 客户端专用密钥（ PEM 文件上传，OpenSSL 加密格式或未加密的专用密钥格式） • 客户端专用密钥密码短语（可选）

8. 选择 * 继续 * 。
9. 选择 * 验证服务器 * 单选按钮以选择如何验证与端点的 TLS 连接。



证书验证的类型	Description
使用自定义 CA 证书	使用自定义安全证书。如果选择此设置，请在 * CA 证书 * 文本框中复制并粘贴自定义安全证书。
使用操作系统 CA 证书	使用操作系统上安装的默认网格 CA 证书来保护连接。
请勿验证证书	未验证用于 TLS 连接的证书。此选项不安全。

10. 选择 * 测试并创建端点 * 。
    - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
    - 如果端点验证失败，则会显示一条错误消息。如果需要修改端点以更正错误，请选择 * 返回到端点详细信息 * 并更新此信息。然后，选择 * 测试并创建端点 * 。

> 如果未为租户帐户启用平台服务，则端点创建将失败。请与 StorageGRID 管理员联系。

配置端点后，您可以使用其 URN 配置平台服务。

相关信息

为平台服务端点指定 URN

配置 CloudMirror 复制

配置事件通知

配置搜索集成服务

测试平台服务端点的连接

如果与平台服务的连接发生更改，您可以测试端点的连接，以验证目标资源是否存在以及是否可以使用您指定的凭据访问它。

您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有管理端点权限的用户组。

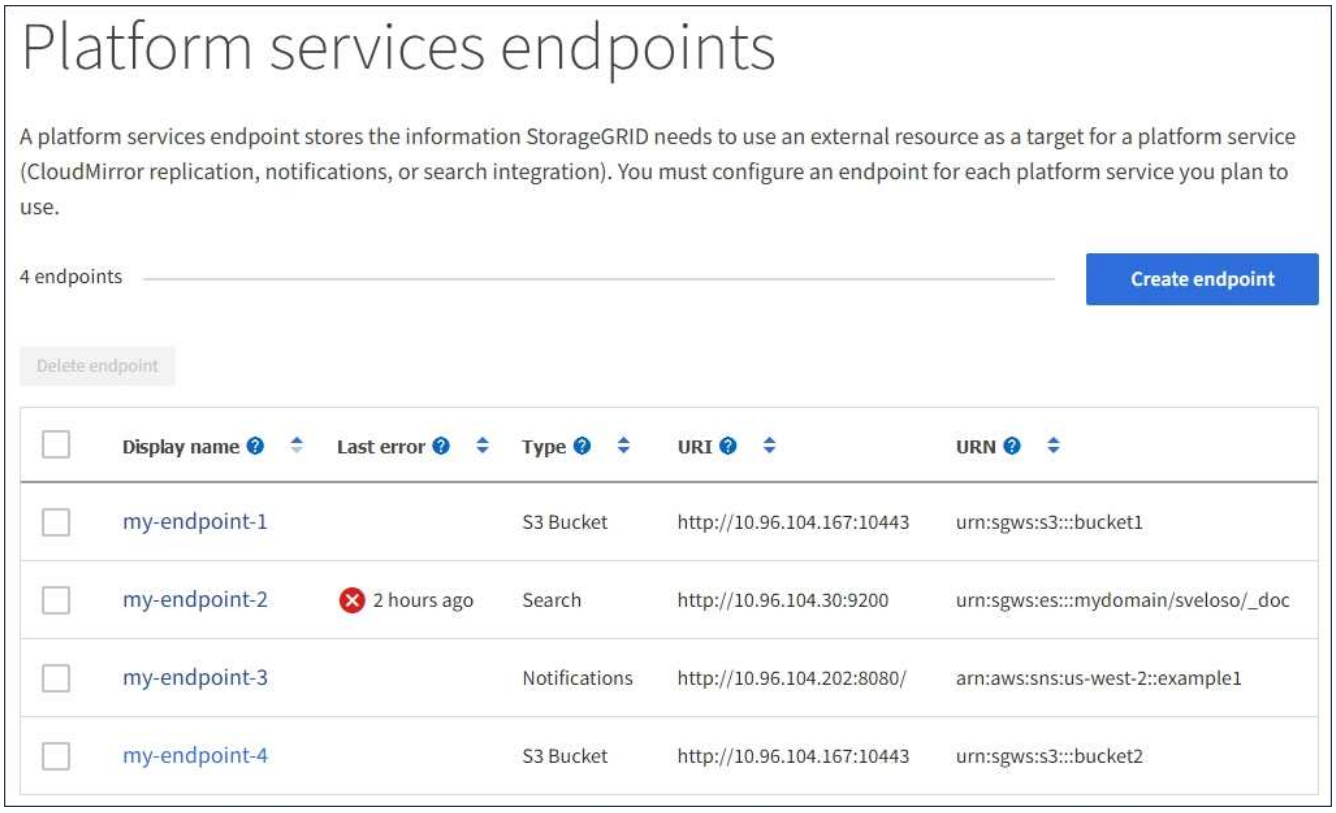
关于此任务

StorageGRID 不会验证这些凭据是否具有正确的权限。

步骤

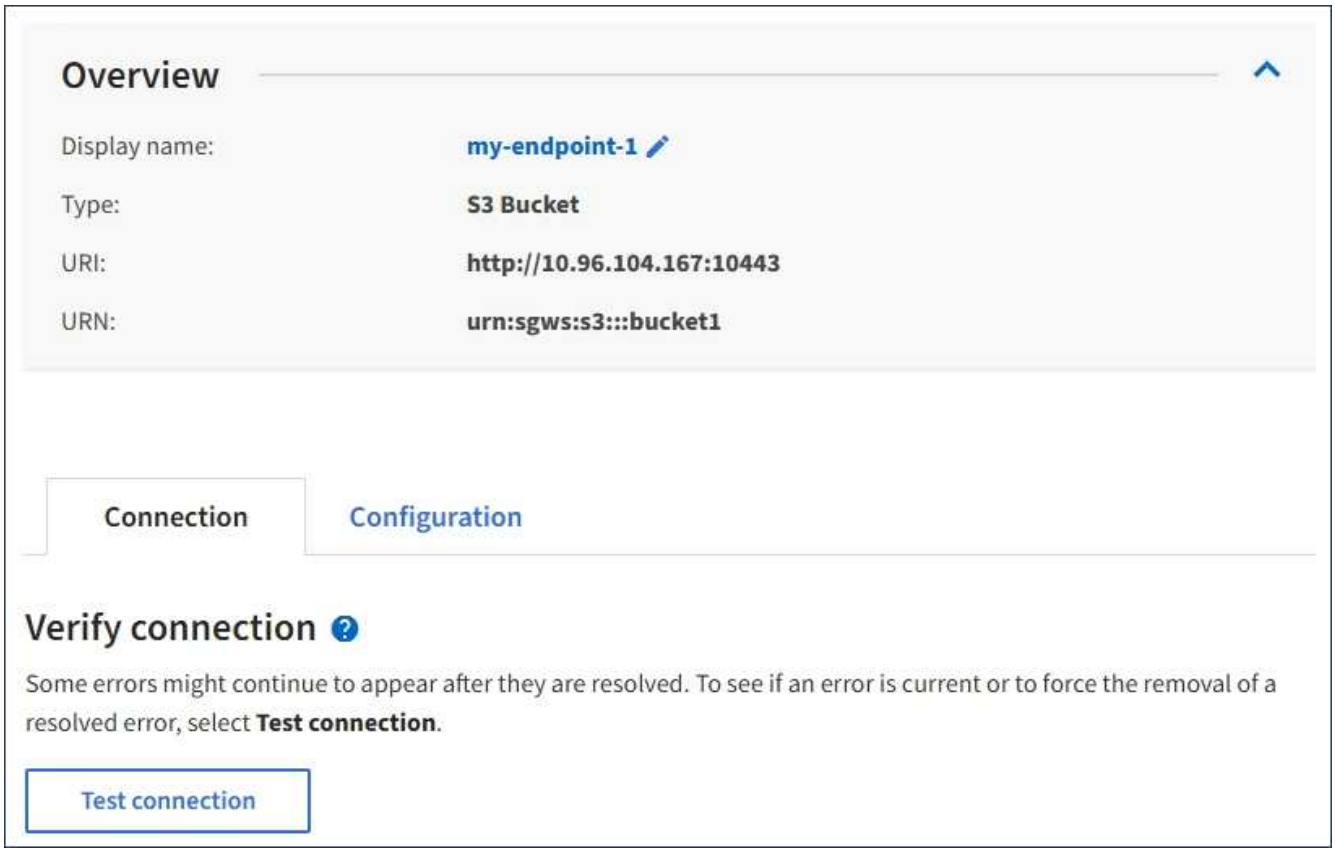
1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。



2. 选择要测试其连接的端点。

此时将显示端点详细信息页面。



3. 选择 * 测试连接 * 。
   - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
   - 如果端点验证失败，则会显示一条错误消息。如果需要修改端点以更正错误，请选择 * 配置 * 并更新信息。然后，选择 * 测试并保存更改 * 。

编辑平台服务端点

您可以编辑平台服务端点的配置以更改其名称， URI 或其他详细信息。例如，您可能需要更新已过期的凭据或更改 URI 以指向备份 Elasticsearch 索引以进行故障转移。您不能更改平台服务端点的 URN 。

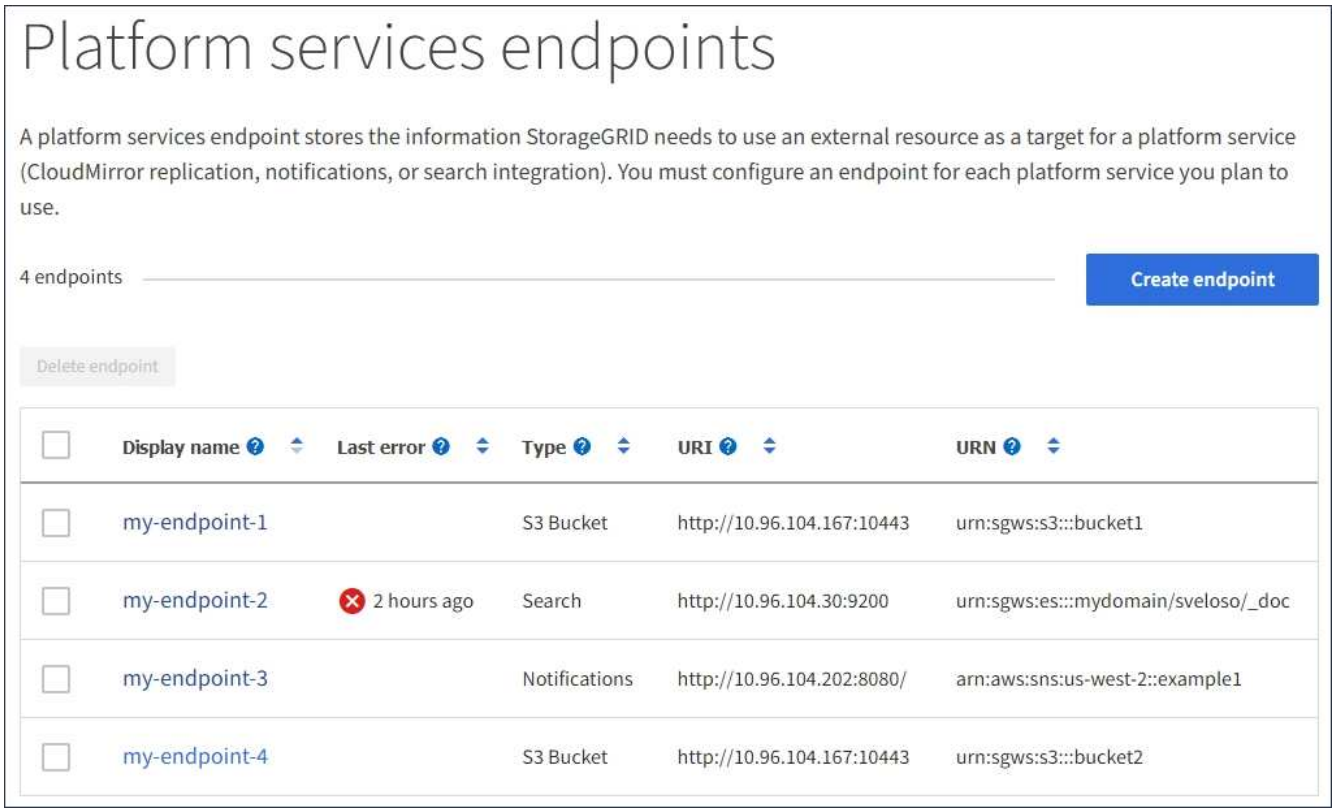
您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有管理端点权限的用户组。请参见 租户管理权限。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

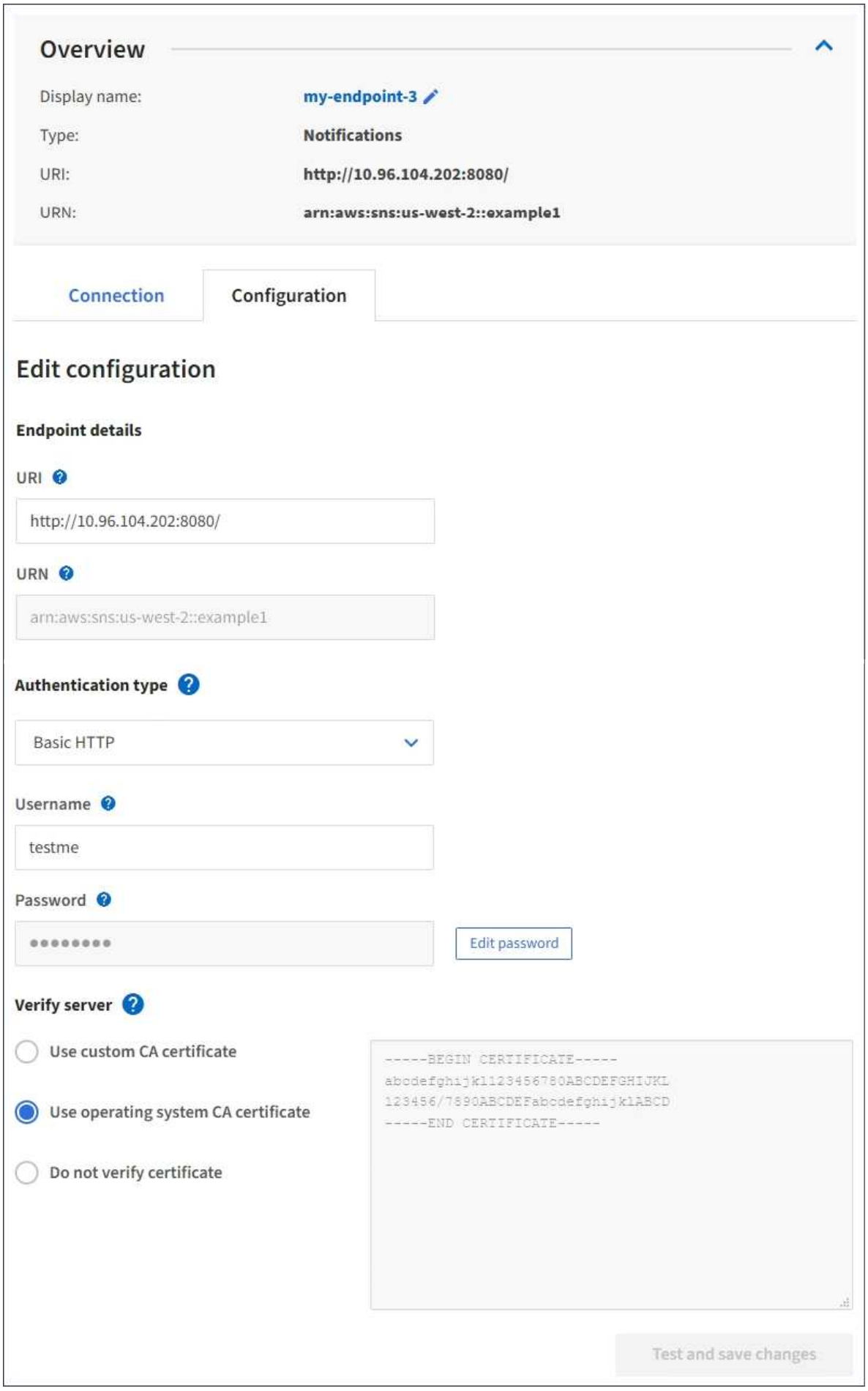
   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。



2. 选择要编辑的端点。

   此时将显示端点详细信息页面。

3. 选择 * 配置 * 。


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. 根据需要更改端点的配置。

   创建端点后，您无法更改端点的 URN 。

   a. 要更改端点的显示名称，请选择编辑图标 。

   b. 根据需要更改 URI 。

   c. 根据需要更改身份验证类型。

      - 对于访问密钥身份验证，请根据需要更改密钥，方法是选择 * 编辑 S3 密钥 * 并粘贴新的访问密钥 ID 和机密访问密钥。如果需要取消所做的更改，请选择 * 还原 S3 密钥编辑 * 。
      - 对于基本 HTTP 身份验证，请根据需要更改用户名。根据需要更改密码，方法是选择 * 编辑密码 * 并输入新密码。如果需要取消所做的更改，请选择 * 还原密码编辑 * 。
      - 对于 CAP （ C2S 访问门户）身份验证，更改临时凭据 URL 或可选客户端专用密钥密码短语，并根据需要上传新的证书和密钥文件。

        客户端专用密钥必须采用 OpenSSL 加密格式或未加密的专用密钥格式。

   d. 根据需要更改用于验证服务器的方法。

5. 选择 * 测试并保存更改 * 。

   - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
   - 如果端点验证失败，则会显示一条错误消息。修改端点以更正错误，然后选择 * 测试并保存更改 * 。

删除平台服务端点

如果您不想再使用关联的平台服务，可以删除端点。

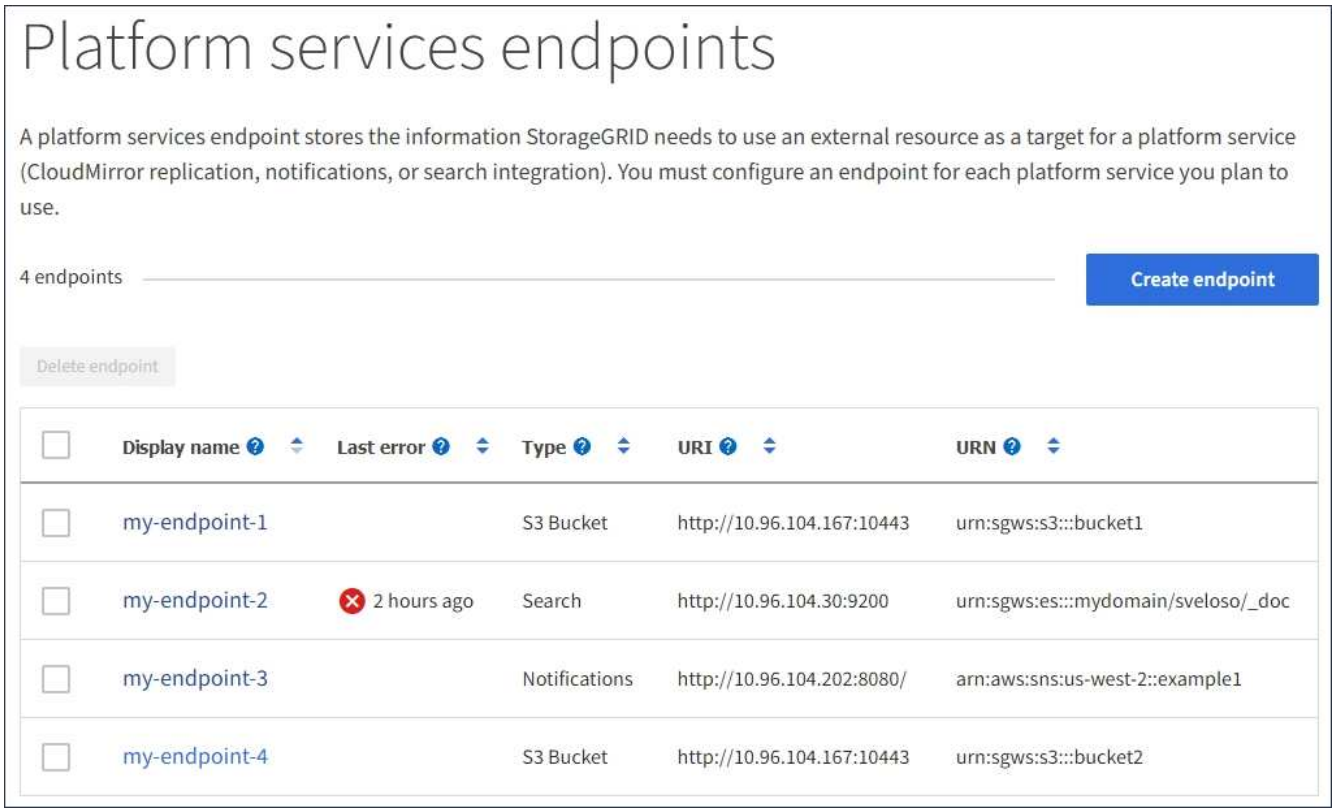
您需要的内容

- 您必须使用登录到租户管理器 支持的 Web 浏览器。
- 您必须属于具有 * 管理端点 * 权限的用户组。请参见 租户管理权限。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。

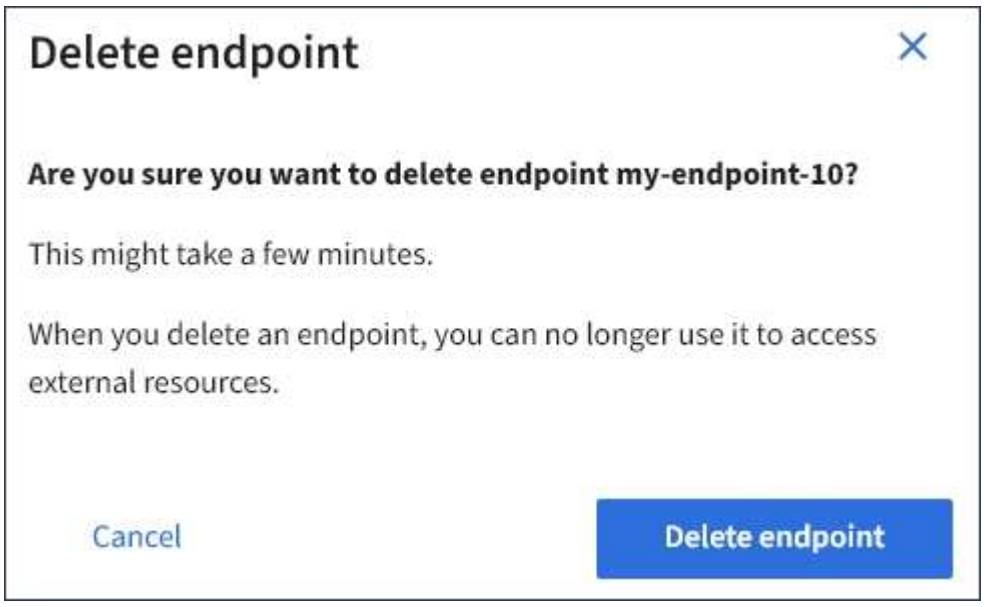


2. 选中要删除的每个端点对应的复选框。

> 如果删除正在使用的平台服务端点，则使用此端点的任何分段都将禁用关联的平台服务。任何尚未完成的请求都将被丢弃。所有新请求都将继续生成，直到您更改存储分段配置以不再引用已删除的 URN 为止。StorageGRID 会将这些请求报告为不可恢复的错误。

3. 选择 * 操作 * > * 删除端点 * 。

此时将显示一条确认消息。

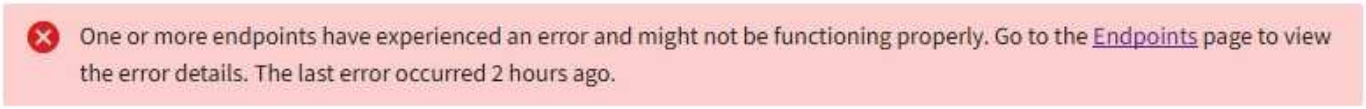


4. 选择 * 删除端点 * 。

如果在 StorageGRID 尝试与平台服务端点通信时发生错误，信息板上将显示一条消息。在平台服务端点页面上，最后一个错误列指示错误发生多长时间前。如果与端点凭据关联的权限不正确，则不会显示任何错误。

确定是否发生错误

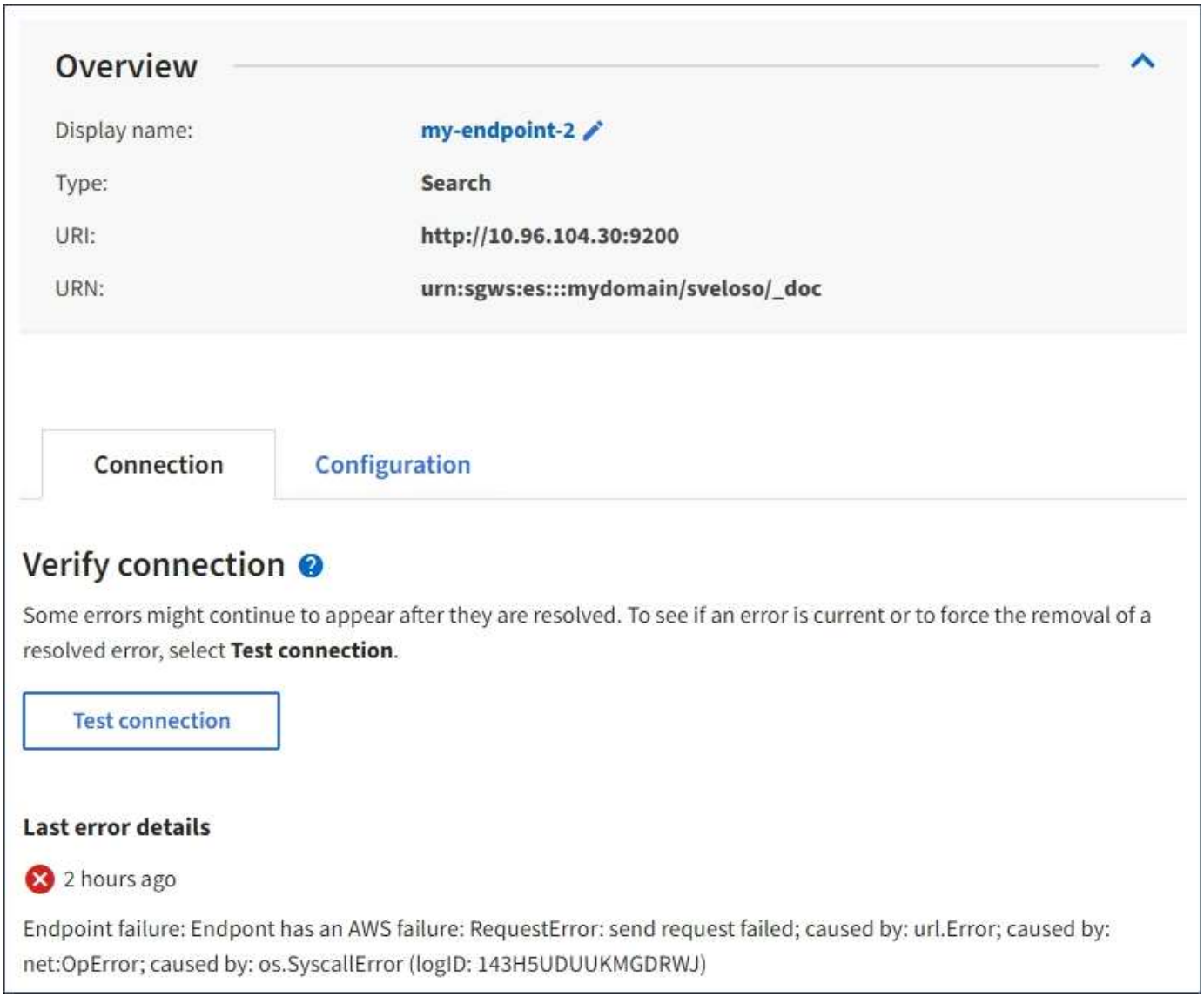
如果在过去 7 天内发生任何平台服务端点错误，则租户管理器信息板将显示一条警报消息。您可以转到平台服务端点页面以查看有关此错误的更多详细信息。



信息板上显示的同一错误也会显示在平台服务端点页面的顶部。要查看更详细的错误消息，请执行以下操作：

步骤

1. 从端点列表中，选择出现错误的端点。
2. 在端点详细信息页面上，选择 * 连接 * 。此选项卡仅显示端点的最新错误，并指示错误发生的时间。包含红色 X 图标的错误 发生在过去 7 天内。



检查错误是否仍然是最新的

即使解决了某些错误， * 最后一个错误 * 列也可能会继续显示这些错误。要查看错误是否为当前错误或强制从表中删除已解决的错误，请执行以下操作：

步骤

1. 选择端点。

   此时将显示端点详细信息页面。

2. 选择 * 连接 * > * 测试连接 * 。

选择 * 测试连接 * 将使 StorageGRID 验证平台服务端点是否存在以及是否可以使用当前凭据访问它。系统会从每个站点的一个节点验证与端点的连接。

解决端点错误

您可以使用端点详细信息页面上的 * 最后一个错误 * 消息来帮助确定导致错误的原因。某些错误可能需要编辑端点才能解决问题描述 。例如，如果 StorageGRID 由于没有正确的访问权限或访问密钥已过期而无法访问目标

S3 存储分段，则可能会发生 CloudMirrorbuc2 错误。消息为 "`需要更新端点凭据或目标访问，` "，详细信息为 "`AccessDenied` " 或 "`InvalidAccessKeyId 。` "

如果您需要编辑端点以解决错误，则选择 * 测试并保存更改 * 会使 StorageGRID 验证更新后的端点，并确认可以使用当前凭据访问它。系统会从每个站点的一个节点验证与端点的连接。

步骤

1. 选择端点。
2. 在端点详细信息页面上，选择 * 配置 * 。
3. 根据需要编辑端点配置。
4. 选择 * 连接 * > * 测试连接 * 。

权限不足的端点凭据

当 StorageGRID 验证平台服务端点时，它会确认端点的凭据可用于联系目标资源，并执行基本权限检查。但是， StorageGRID 不会验证某些平台服务操作所需的所有权限。因此，如果您在尝试使用平台服务（例如 "`403 For禁用` " ）时收到错误，请检查与此端点凭据关联的权限。

其他平台服务故障排除

有关追加信息 对平台服务进行故障排除的信息，请参见有关管理 StorageGRID 的说明。

管理 StorageGRID

相关信息

创建平台服务端点

测试平台服务端点的连接

编辑平台服务端点

配置 **CloudMirror** 复制

。 CloudMirror 复制服务 是三种 StorageGRID 平台服务之一。您可以使用 CloudMirror 复制将对象自动复制到外部 S3 存储分段。

您需要的内容

- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须已创建一个分段，才能用作复制源。
- 要用作 CloudMirror 复制目标的端点必须已存在，并且必须具有其 URN 。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组，此权限允许您管理租户帐户中所有 S3 分段的设置。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

CloudMirror 复制会将对象从源存储分段复制到端点中指定的目标存储分段。要为存储分段启用 CloudMirror 复制，必须创建并应用有效的存储分段复制配置 XML 。复制配置 XML 必须对每个目标使用 S3 存储分段端点的 URN 。

启用了 S3 对象锁定的源或目标分段不支持复制。

有关存储分段复制以及如何配置的一般信息，请参见 Amazon Simple Storage Service （ S3 ）有关跨区域复制（ CRR ）的文档。有关 StorageGRID 如何实施 S3 存储分段复制配置 API 的信息，请参见 有关实施 S3 客户端应用程序的说明。

如果在包含对象的存储分段上启用 CloudMirror 复制，则会复制添加到存储分段中的新对象，但不会复制存储分段中的现有对象。您必须更新现有对象才能触发复制。

如果在复制配置 XML 中指定存储类，则 StorageGRID 在对目标 S3 端点执行操作时会使用该类。目标端点还必须支持指定的存储类。请务必遵循目标系统供应商提供的任何建议。

步骤

1. 为源存储分段启用复制：

   使用文本编辑器创建在 S3 复制 API 中指定的启用复制所需的复制配置 XML 。配置 XML 时：

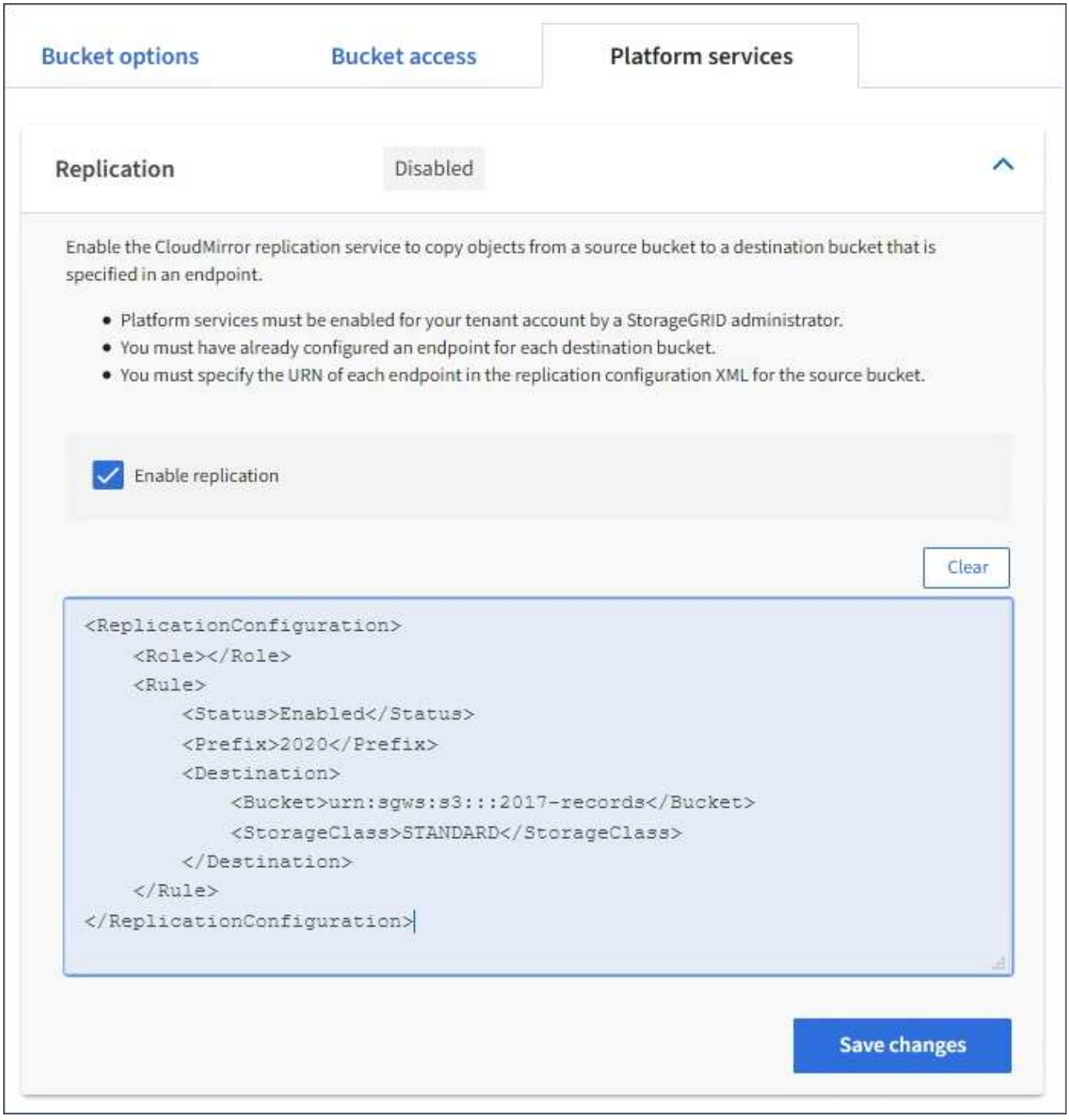
   - 请注意， StorageGRID 仅支持复制配置的 V1 。这意味着， StorageGRID 不支持使用 `Filter` 元素作为规则，并遵循 V1 约定删除对象版本。有关详细信息，请参见有关复制配置的 Amazon 文档。
   - 使用 S3 存储分段端点的 URN 作为目标。
   - 也可以添加 ` <StorageClass>` 元素，并指定以下项之一：
     - `standard` ：默认存储类。如果在上传对象时未指定存储类，则会使用 `Standard` storage class 。
     - `standard_IA` ：（标准 - 不常访问。） 对于访问频率较低但仍需要在需要时快速访问的数据，请使用此存储类。
     - `re`介绍冗余：将此存储类用于非关键，可重现的数据，这些数据的存储冗余程度低于 `S` 标准存储类。
   - 如果在配置 XML 中指定 `role` ，则会忽略该角色。StorageGRID 不使用此值。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 复制 * 。
5. 选中 * 启用复制 * 复选框。
6. 将复制配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。



StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证复制配置是否正确：
   a. 向源存储分段添加一个对象，以满足复制配置中指定的复制要求。

在前面显示的示例中，复制与前缀 "`2020` " 匹配的对象。

b. 确认对象已复制到目标存储分段。

对于小型对象，复制操作会快速进行。

相关信息

使用 S3

创建平台服务端点

配置事件通知

通知服务是三种 StorageGRID 平台服务之一。您可以为存储分段启用通知，以便将有关指定事件的信息发送到支持 AWS Simple Notification Service （ SNS ）的目标服务。

您需要的内容

- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须已创建一个存储分段，才能用作通知源。
- 要用作事件通知目标的端点必须已存在，并且必须具有其 URN 。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组，此权限允许您管理租户帐户中所有 S3 分段的设置。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

配置事件通知后，每当源存储分段中的某个对象发生指定事件时，都会生成一个通知，并将其发送到用作目标端点的简单通知服务（ SNS ）主题。要为存储分段启用通知，必须创建并应用有效的通知配置 XML 。通知配置 XML 必须使用每个目标的事件通知端点的 URN 。

有关事件通知以及如何配置这些通知的一般信息，请参见 Amazon 文档。有关 StorageGRID 如何实施 S3 存储分段通知配置 API 的信息，请参见实施 S3 客户端应用程序的说明。

如果为包含对象的存储分段启用事件通知，则仅会为保存通知配置后执行的操作发送通知。

步骤

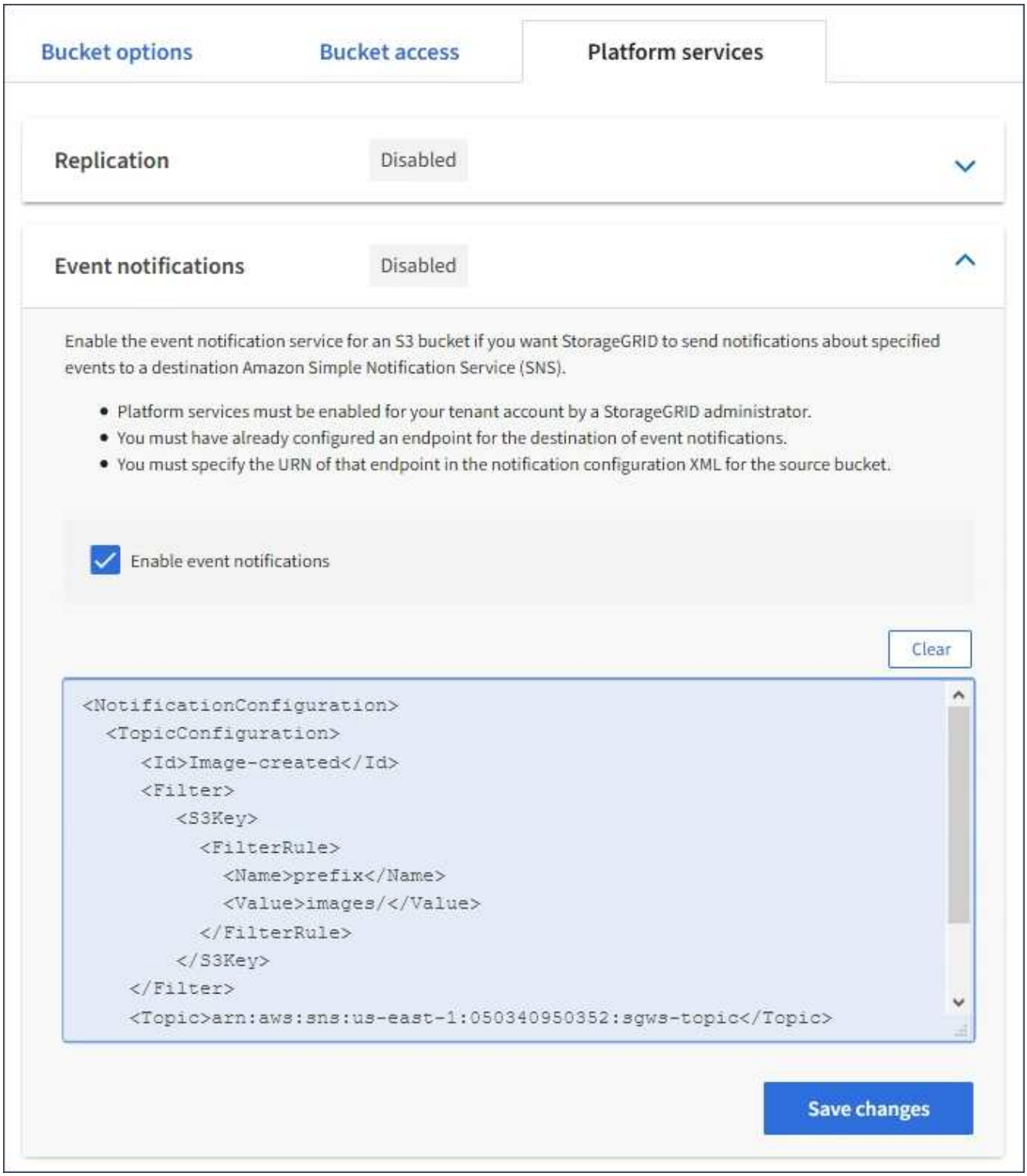
1. 为源存储分段启用通知：
    - 使用文本编辑器创建启用 S3 通知 API 中指定的事件通知所需的通知配置 XML 。
    - 配置 XML 时，请使用事件通知端点的 URN 作为目标主题。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 事件通知 * 。
5. 选中 * 启用事件通知 * 复选框。
6. 将通知配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。



StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证是否已正确配置事件通知：

   a. 对源存储分段中符合配置 XML 中配置的触发通知要求的对象执行操作。

      在此示例中，每当创建具有 `images/` 前缀的对象时，都会发送事件通知。

b. 确认已向目标 SNS 主题发送通知。

例如，如果您的目标主题托管在 AWS 简单通知服务（ SNS ）上，则可以将此服务配置为在发送通知时向您发送电子邮件。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

如果在目标主题收到通知，则表示您已成功为 StorageGRID 通知配置源存储分段。

相关信息

了解存储分段通知

使用 S3

创建平台服务端点

使用搜索集成服务

搜索集成服务是三种 StorageGRID 平台服务之一。您可以启用此服务，以便在创建，删除对象或更新其元数据或标记时将对象元数据发送到目标搜索索引。

您可以使用租户管理器将自定义 StorageGRID 配置 XML 应用于存储分段来配置搜索集成。

由于搜索集成服务会将对象元数据发送到目标，因此其配置 XML 称为 *metadata notification configuration xml* 。此配置 XML 与用于启用事件通知的 *notification* 配置 *xml* 不同。

请参见 有关实施 S3 客户端应用程序的说明 有关以下自定义 StorageGRID S3 REST API 操作的详细信息：

- 删除存储分段元数据通知配置请求
- 获取存储分段元数据通知配置请求
- PUT 存储分段元数据通知配置请求

相关信息

用于搜索集成的配置 XML

元数据通知中包含的对象元数据

由搜索集成服务生成的 JSON

配置搜索集成服务

使用 S3

用于搜索集成的配置 **XML**

搜索集成服务使用 ` <MetadataNotificationConfiguration>` 和 ` </MetadataNotificationConfiguration>` 标记中包含的一组规则进行配置。每个规则都指定规则适用场景 所对应的对象以及 StorageGRID 应将这些对象的元数据发送到的目标。

可以按对象名称的前缀筛选对象。例如，您可以将前缀为 `images` 的对象的元数据发送到一个目标，将前缀为 `videos` 的对象的元数据发送到另一个目标。前缀重叠的配置无效，在提交时会被拒绝。例如，不允许对前缀为 `test` 的对象使用一个规则，而对前缀为 `test2` 的对象使用另一个规则。

必须使用为搜索集成服务创建的 StorageGRID 端点的 URN 指定目标。这些端点是指 Elasticsearch 集群上定义的索引和类型。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表介绍了元数据通知配置 XML 中的元素。

Name	Description	Required
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是的。
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是的。
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
Status	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是的。

Name	Description	Required
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是的。
目标	规则目标的容器标记。 包含在 Rule 元素中。	是的。
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN ： • `es` 必须是第三个元素。 • URN 必须以 `domain-name/myindex/mytype` 形式的索引和元数据存储类型结尾。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn ： AWS ： es ： Region ： account-ID ： domain/mydomain/myindex/mytype` • `urn ： mysite ： es ： ： ： mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是的。

使用示例元数据通知配置 XML 了解如何构建自己的 XML 。

用于适用场景 所有对象的元数据通知配置

在此示例中，所有对象的对象元数据都将发送到同一目标。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

具有两个规则的元数据通知配置

在此示例中，与前缀 ` /images` 匹配的对象的对象元数据将发送到一个目标，而与前缀 ` /videos` 匹配的对象的对象元数据则发送到另一个目标。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相关信息

使用 S3

元数据通知中包含的对象元数据

由搜索集成服务生成的 JSON

配置搜索集成服务

每当创建，删除对象或更新其元数据或标记时，搜索集成服务都会将对象元数据发送到目标搜索索引。

您需要的内容

- StorageGRID 管理员必须为您的租户帐户启用平台服务。
- 您必须已创建要为其内容编制索引的 S3 存储分段。
- 要用作搜索集成服务目标的端点必须已存在，并且必须具有其 URN 。
- 您必须属于具有 " 管理所有分段 " 或 " 根访问 " 权限的用户组，此权限允许您管理租户帐户中所有 S3 分段的设置。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

为源存储分段配置搜索集成服务后，创建对象或更新对象的元数据或标记会触发要发送到目标端点的对象元数据。如果为已包含对象的存储分段启用搜索集成服务，则不会自动为现有对象发送元数据通知。您必须更新这些现有对象，以确保其元数据已添加到目标搜索索引中。

步骤

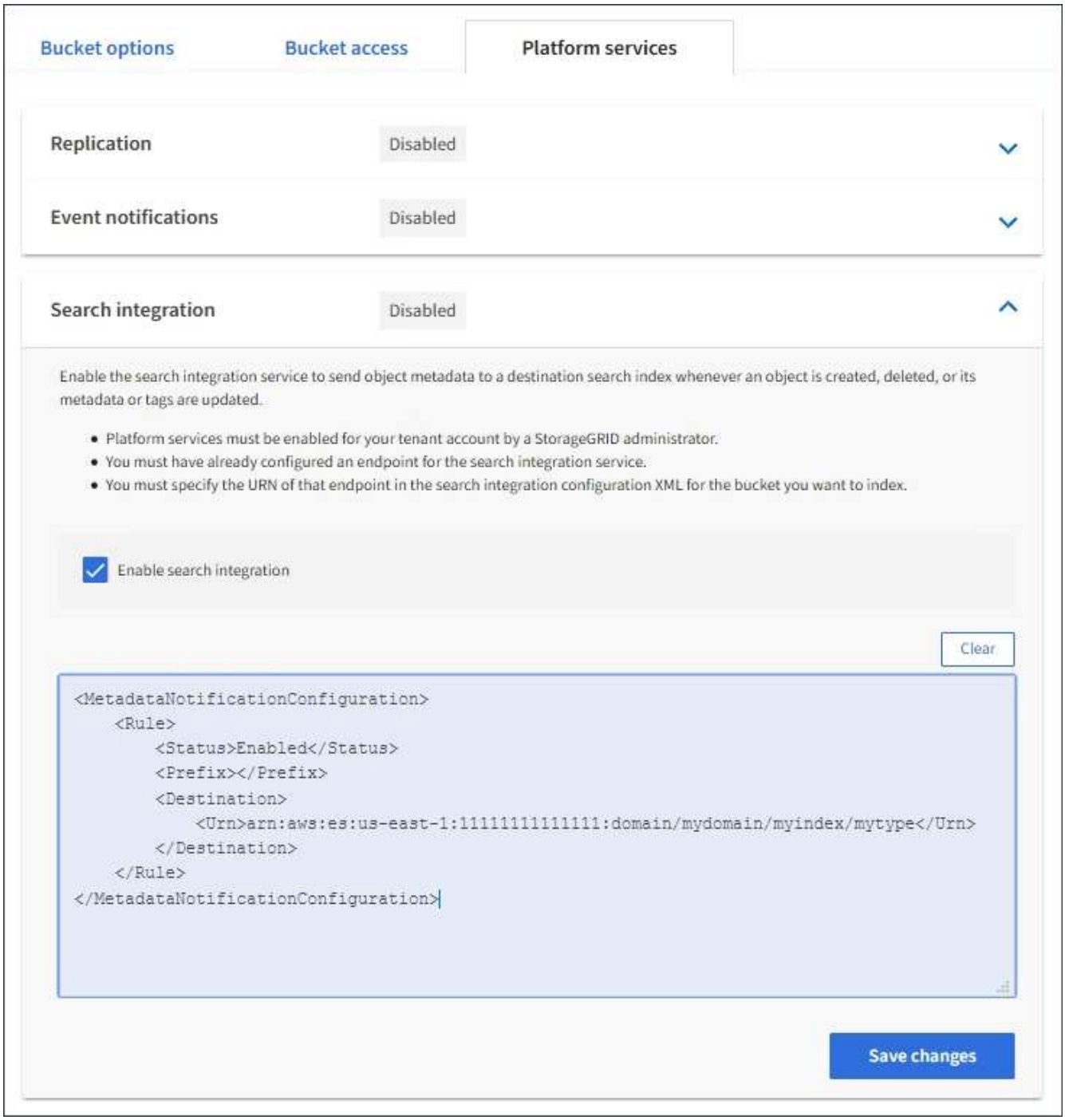
1. 使用文本编辑器创建启用搜索集成所需的元数据通知 XML 。
   - 请参见有关用于搜索集成的配置 XML 的信息。
   - 配置 XML 时，请使用搜索集成端点的 URN 作为目标。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 搜索集成 *
5. 选中 * 启用搜索集成 * 复选框。
6. 将元数据通知配置粘贴到文本框中，然后选择 * 保存更改 * 。



StorageGRID 管理员必须使用网格管理器或管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证是否已正确配置搜索集成服务：
   a. 向源存储分段添加一个对象，以满足配置 XML 中指定的元数据通知触发要求。

      在前面显示的示例中，添加到存储分段的所有对象都会触发元数据通知。

   b. 确认包含对象元数据和标记的 JSON 文档已添加到端点中指定的搜索索引中。

完成后

根据需要，您可以使用以下任一方法禁用存储分段的搜索集成：

- 选择 * 存储（ S3 ） * > * 分段 * ，然后取消选中 * 启用搜索集成 * 复选框。
- 如果您直接使用 S3 API ，请使用删除分段元数据通知请求。请参见有关实施 S3 客户端应用程序的说明。

相关信息

了解搜索集成服务

用于搜索集成的配置 XML

使用 S3

创建平台服务端点

由搜索集成服务生成的 **JSON**

为存储分段启用搜索集成服务后，每次添加，更新或删除对象元数据或标记时，系统都会生成一个 JSON 文档并将其发送到目标端点。

此示例显示了在名为 `test` 的存储分段中创建具有密钥 `SGWS/Tagging.txt` 的对象时可能生成的 JSON 示例。`test` 存储分段未进行版本控制，因此 `veversionId` 标记为空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

元数据通知中包含的对象元数据

下表列出了启用搜索集成后发送到目标端点的 JSON 文档中包含的所有字段。

文档名称包括存储分段名称，对象名称和版本 ID （如果存在）。

Type	项目名称和问题描述
存储分段和对象信息	`Bucket` ： 存储分段的名称

Type	项目名称和问题描述
`key` ： 对象密钥名称	`veversionID` ： 版本控制分段中的对象的对象版本
`reGion` ： 桶区，例如 `us-east-1`	系统元数据
`size` ： HTTP 客户端可以看到的对象大小（以字节为单位）	`mD5` ： 对象哈希
用户元数据	`metadata` ： 对象的所有用户元数据，作为键值对 键：值
Tags	`tags` ： 为对象定义的所有对象标记，作为键值对 键：值

对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后，您无法在索引中编辑文档的字段类型。

使用 S3

使用 S3 ： 概述

StorageGRID 支持简单存储服务（ S3 ） API ，该 API 作为一组表示状态传输（ Representational State Transfer ， REST ） Web 服务来实施。通过对 S3 REST API 的支持，您可以将为 S3 Web 服务开发的面向服务的应用程序与使用 StorageGRID 系统的内部对象存储连接起来。这需要对客户端应用程序当前使用 S3 REST API 调用的情况进行最少的更改。

对 S3 REST API 支持的更改

您应了解 StorageGRID 系统对 S3 REST API 的支持发生了哪些变化。

版本。	注释
11.6.	• 增加了对在 GET 对象和 HEAD 对象请求中使用 `partnumber` request 参数的支持。 • 增加了对 S3 对象锁定的默认保留模式和存储分段级别的默认保留期限的支持。 • 增加了对 `s 3 ： object-lock-real-retention-days` 策略条件密钥的支持，用于设置对象允许的保留期限范围。 • 现在，单个 PUT 对象操作的最大 _recommended_size 为 5 GiB （ 5 ， 368 ， 709 ， 120 字节）。如果对象大于 5 GiB ，请改用多部分上传。 在 StorageGRID 11.6 中，单个 PUT 对象操作的最大 _supported _ 大小仍为 5 TiB （ 5 ， 497 ， 552 ， 138 ， 880 字节）。但是，如果您尝试上传超过 5 GiB 的对象，则会触发 * S3 PUT Object Size Too large* 警报。
11.5	• 增加了对管理存储分段加密的支持。 • 增加了对 S3 对象锁定和已弃用旧合规性请求的支持。 • 增加了对在版本控制的存储分段上使用删除多个对象的支持。 • 现在可以正确支持 `Content-MD5` 请求标头。
11.4	• 增加了对删除存储分段标记，获取存储分段标记和放置存储分段标记的支持。不支持成本分配标记。 • 对于在 StorageGRID 11.4 中创建的分段，不再需要限制对象密钥名称以满足性能最佳实践。 • 增加了对 `s 3 ： ObjectRestore ： POST` 事件类型的存储分段通知的支持。 • 现在，多部件的 AWS 大小限制已强制实施。多部分上传中的每个部件必须介于 5 MiB 和 5 GiB 之间。最后一个部件可以小于 5 MiB 。 • 增加了对 TLS 1.3 的支持，并更新了支持的 TLS 密码套件列表。 • CLB 服务已弃用。
11.3	• 增加了对使用客户提供的密钥（ SSI-C ）对对象数据进行服务器端加密的支持。 • 增加了对删除，获取和放置分段生命周期操作（仅限到期操作）以及 `x-AMZ-expiration` 响应标头的支持。 • 更新了 PUT 对象， PUT 对象 - 复制和多部件上传，以说明在载入时使用同步放置的 ILM 规则的影响。 • 更新了支持的 TLS 密码套件列表。不再支持 TLS 1.1 密码。

版本。	注释
11.2.	增加了对用于云存储池的后对象还原的支持。增加了对在组和存储分段策略中使用 AWS 语法来处理 ARN ，策略条件密钥和策略变量的支持。仍支持使用 StorageGRID 语法的现有组和存储分段策略。 • 注意： * 在其他配置 JSON/XML 中使用 ARN/URN 的情况没有改变，包括在自定义 StorageGRID 功能中使用的情况。
11.1	增加了对跨源资源共享（ CORS ）， S3 客户端到网格节点连接的 HTTP 以及存储分段上的合规性设置的支持。
11.0	增加了对为存储分段配置平台服务（ CloudMirror 复制，通知和 Elasticsearch 搜索集成）的支持。此外，还增加了对存储分段的对象标记位置约束以及可用一致性控制设置的支持。
10.4.	增加了对版本控制，端点域名页面更新，策略中的条件和变量，策略示例以及 PutOverwriteObject 权限的 ILM 扫描更改的支持。
10.3	增加了对版本控制的支持。
10.2	增加了对组和存储分段访问策略以及多部件副本（上传部件 - 复制）的支持。
10.1	增加了对多部分上传，虚拟托管模式请求和 v4 身份验证的支持。
10.0	StorageGRID 系统最初支持 S3 REST API 。当前支持的 _Simple Storage Service API 参考版本为 2006-03-01 。

支持的版本

StorageGRID 支持以下特定版本的 S3 和 HTTP 。

项目	**version**
S3 规范	_Simple Storage Service API 参考 _ 2006-03-01
HTTP	1.1 有关 HTTP 的详细信息，请参见 HTTP/1.1 （ RFC 7230-35 ）。 • 注 * ： StorageGRID 不支持 HTTP/1.1 管道化。

相关信息

"IETF RFC 2616 ： 超文本传输协议（ HTTP/1.1 ）"

"Amazon Web Services （ AWS ）文档： Amazon Simple Storage Service API 参考"

支持 **StorageGRID** 平台服务

通过 StorageGRID 平台服务， StorageGRID 租户帐户可以利用远程 S3 存储分段，简单通知服务（ SNS ）端点或 Elasticsearch 集群等外部服务来扩展网格提供的服务。

下表总结了可用的平台服务以及用于配置这些服务的 S3 API 。

平台服务	目的	用于配置服务的 **S3 API**
CloudMirror 复制	将对象从源 StorageGRID 存储分段复制到已配置的远程 S3 存储分段。	PUT 存储分段复制
通知	将有关源 StorageGRID 存储分段中事件的通知发送到已配置的简单通知服务（ Simple Notification Service ， SNS ）端点。	PUT 存储分段通知
搜索集成	将存储在 StorageGRID 存储分段中的对象的对象元数据发送到已配置的 Elasticsearch 索引。	PUT 存储分段元数据通知 • 注： * 这是 StorageGRID 自定义 S3 API 。

网格管理员必须先为租户帐户启用平台服务，然后才能使用这些服务。然后，租户管理员必须在租户帐户中创建一个表示远程服务的端点。要配置服务，必须执行此步骤。

使用平台服务的建议

在使用平台服务之前，您必须了解以下建议：

- NetApp 建议，对于需要进行 CloudMirror 复制，通知和搜索集成的 S3 请求，您允许的活动租户不超过 100 个。如果活动租户超过 100 个，则可能会导致 S3 客户端性能下降。
- 如果 StorageGRID 系统中的 S3 存储分段同时启用了版本控制和 CloudMirror 复制， NetApp 建议目标端点也启用 S3 存储分段版本控制。这样， CloudMirror 复制就可以在端点上生成类似的对象版本。
- 如果源存储分段启用了 S3 对象锁定，则不支持 CloudMirror 复制。
- 如果目标存储分段启用了原有合规性，则 CloudMirror 复制将失败并显示 AccessDenied 错误。

相关信息

使用租户帐户

管理 StorageGRID

对存储分段执行的操作

PUT 存储分段元数据通知配置请求

配置租户帐户和连接

要将 StorageGRID 配置为接受来自客户端应用程序的连接，需要创建一个或多个租户帐户

并设置连接。

创建和配置 **S3** 租户帐户

S3 API 客户端必须先具有 S3 租户帐户，然后才能在 StorageGRID 上存储和检索对象。每个租户帐户都有自己的帐户 ID ，组和用户以及容器和对象。

S3 租户帐户由 StorageGRID 网格管理员使用网格管理器或网格管理 API 创建。创建 S3 租户帐户时，网格管理员会指定以下信息：

- 租户的显示名称（租户的帐户 ID 会自动分配，不能更改）。
- 是否允许租户帐户使用平台服务。如果允许使用平台服务，则必须对网格进行配置，以支持使用这些服务。
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。
- 如果为 StorageGRID 系统启用了身份联合，则哪个联合组具有 " 根访问 " 权限来配置租户帐户。
- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。

创建 S3 租户帐户后，租户用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享），并创建本地组和用户
- 管理 S3 访问密钥
- 创建和管理 S3 存储分段，包括启用了 S3 对象锁定的存储分段
- 使用平台服务（如果已启用）
- 监控存储使用情况

> S3 租户用户可以使用租户管理器创建和管理 S3 存储分段，但他们必须具有 S3 访问密钥，并使用 S3 REST API 载入和管理对象。

相关信息

管理 StorageGRID

使用租户帐户

如何配置客户端连接

网格管理员可以选择影响 S3 客户端连接到 StorageGRID 以存储和检索数据的配置。建立连接所需的具体信息取决于所选的配置。

客户端应用程序可以通过连接到以下任一项来存储或检索对象：

- 管理节点或网关节点上的负载平衡器服务，或者也可以是管理节点或网关节点高可用性（ HA ）组的虚拟 IP 地址
- 网关节点上的 CLB 服务，或者也可以是网关节点高可用性组的虚拟 IP 地址

CLB 服务已弃用。在 StorageGRID 11.3 版本之前配置的客户端可以继续在网关节点上使用 CLB 服务。所有其他依靠 StorageGRID 提供负载平衡的客户端应用程序都应使用负载平衡器服务进行连接。

- 存储节点，具有或不具有外部负载平衡器

配置 StorageGRID 时，网格管理员可以使用网格管理器或网格管理 API 执行以下步骤，所有这些步骤均为可选步骤：

1. 为负载平衡器服务配置端点。

   您必须配置端点才能使用负载平衡器服务。管理节点或网关节点上的负载平衡器服务会将传入的网络连接从客户端应用程序分发到存储节点。创建负载平衡器端点时， StorageGRID 管理员会指定端口号，端点是否接受 HTTP 或 HTTPS 连接，将使用此端点的客户端类型（ S3 或 Swift ）以及用于 HTTPS 连接的证书（如果适用）。

2. 配置不可信客户端网络。

   如果 StorageGRID 管理员将节点的客户端网络配置为不可信，则节点仅接受客户端网络上显式配置为负载平衡器端点的端口上的入站连接。

3. 配置高可用性组。

   如果管理员创建了一个 HA 组，则多个管理节点或网关节点的网络接口将置于主动备份配置中。客户端连接使用 HA 组的虚拟 IP 地址进行。

有关每个选项的详细信息，请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

摘要：客户端连接的 **IP** 地址和端口

客户端应用程序使用网格节点的 IP 地址以及该节点上服务的端口号连接到 StorageGRID 。如果配置了高可用性（ HA ）组，则客户端应用程序可以使用 HA 组的虚拟 IP 地址进行连接。

建立客户端连接所需的信息

下表总结了客户端连接到 StorageGRID 的不同方式以及每种连接类型所使用的 IP 地址和端口。有关详细信息，请与 StorageGRID 管理员联系，或者参见有关管理问题描述 StorageGRID 的说明，了解如何在网格管理器中查找此信息。

建立连接的位置	客户端连接到的服务	**IP** 地址	**Port**
HA 组	负载平衡器	HA 组的虚拟 IP 地址	• 负载平衡器端点端口
HA 组	CLB • 注： * CLB 服务已弃用。	HA 组的虚拟 IP 地址	默认 S3 端口： • HTTPS： 8082 • HTTP： 8084

建立连接的位置	客户端连接到的服务	IP 地址	Port
管理节点	负载平衡器	管理节点的 IP 地址	• 负载平衡器端点端口
网关节点	负载平衡器	网关节点的 IP 地址	• 负载平衡器端点端口
网关节点	CLB • 注： * CLB 服务已弃用。	网关节点的 IP 地址 • 注： * 默认情况下，CLB 和 LDR 的 HTTP 端口未启用。	默认 S3 端口： • HTTPS： 8082 • HTTP： 8084
存储节点	LDR	存储节点的 IP 地址	默认 S3 端口： • HTTPS： 18082 • HTTP： 18084

示例

要将 S3 客户端连接到网关节点 HA 组的负载平衡器端点，请使用以下结构化 URL：

- `https://VIP-of-HA-group:_LB-endpoint-port_`

例如，如果 HA 组的虚拟 IP 地址为 192.0.2.5 ，而 S3 负载平衡器端点的端口号为 10443 ，则 S3 客户端可以使用以下 URL 连接到 StorageGRID：

- `https://192.0.2.5:10443`

可以为客户端用于连接到 StorageGRID 的 IP 地址配置 DNS 名称。请与本地网络管理员联系。

相关信息

管理 StorageGRID

决定使用 **HTTPS** 或 **HTTP** 连接

使用负载平衡器端点建立客户端连接时，必须使用为此端点指定的协议（ HTTP 或 HTTPS ）进行连接。要使用 HTTP 连接到存储节点或网关节点上的 CLB 服务，必须启用 HTTP 。

默认情况下，当客户端应用程序连接到存储节点或网关节点上的 CLB 服务时，它们必须对所有连接使用加密 HTTPS 。您也可以选择网格管理器中的 * 启用 HTTP 连接 * 网格选项来启用不太安全的 HTTP 连接。例如，在非生产环境中测试与存储节点的连接时，客户端应用程序可能会使用 HTTP 。

> 为生产网格启用 HTTP 时要小心，因为请求将以未加密方式发送。

> CLB 服务已弃用。

如果选择了 * 启用 HTTP 连接 * 选项，则客户端对 HTTP 使用的端口必须与对 HTTPS 使用的端口不同。请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

活动，空闲和并发 HTTP 连接的优势

S3 请求的端点域名

在对客户端请求使用 S3 域名之前， StorageGRID 管理员必须将系统配置为接受在 S3 路径模式和 S3 虚拟托管模式请求中使用 S3 域名的连接。

关于此任务

要使用 S3 虚拟托管模式请求，网格管理员必须执行以下任务：

- 使用网格管理器将 S3 端点域名添加到 StorageGRID 系统。
- 确保客户端用于与 StorageGRID 的 HTTPS 连接的证书已针对客户端所需的所有域名进行签名。

  例如，如果端点为 `s3.company.com` ，则网格管理员必须确保用于 HTTPS 连接的证书包含 `s3.company.com` 端点和端点的通配符使用者备用名称（ SAN ）： `*.s3.company.com` 。

- 配置客户端使用的 DNS 服务器，使其包含与端点域名匹配的 DNS 记录，包括任何所需的通配符记录。

如果客户端使用负载平衡器服务进行连接，则网格管理员配置的证书是客户端使用的负载平衡器端点的证书。

每个负载平衡器端点都有自己的证书，并且可以对每个端点进行配置以识别不同的端点域名。

如果客户端连接到存储节点或网关节点上的 CLB 服务，则网格管理员配置的证书是用于网格的单个自定义服务器证书。

CLB 服务已弃用。

有关详细信息，请参见有关管理 StorageGRID 的说明。

完成这些步骤后，您可以使用虚拟托管模式请求（例如， `bucket.s3.company.com` ）。

相关信息

管理 StorageGRID

配置 REST API 的安全性

测试 S3 REST API 配置

您可以使用 Amazon Web Services 命令行界面（ AWS 命令行界面）测试与系统的连接，并验证是否可以向系统读取和写入对象。

您需要的内容

- 您已从下载并安装 AWS 命令行界面 "aws.amazon.com/cli"。
- 您已在 StorageGRID 系统中创建 S3 租户帐户。

步骤

1. 配置 Amazon Web Services 设置以使用您在 StorageGRID 系统中创建的帐户：
   a. 进入配置模式： `AWS configure`
   b. 输入您创建的帐户的 AWS 访问密钥 ID 。
   c. 输入您创建的帐户的 AWS 机密访问密钥。
   d. 输入要使用的默认区域，例如 us-east-1 。
   e. 输入要使用的默认输出格式，或者按 * 输入 * 选择 JSON 。
2. 创建存储分段。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

   如果已成功创建存储分段，则会返回存储分段的位置，如以下示例所示：

```
"Location": "/testbucket"
```

1. 上传对象。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

   如果对象上传成功，则返回一个 Etag ，该 Etag 是对象数据的哈希。

2. 列出存储分段的内容以验证是否已上传此对象。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

3. 删除对象。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

4. 删除存储分段。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID 如何实施 S3 REST API

客户端应用程序可以使用 S3 REST API 调用连接到 StorageGRID 来创建，删除和修改存储分段以及存储和检索对象。

客户端请求冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。

" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

一致性控制

一致性控制可以根据应用程序的要求、在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。

默认情况下， StorageGRID 保证新创建的对象的写入后读一致性。成功完成 PUT 后的任何 GET 都将能够读取新写入的数据。对现有对象的覆盖，元数据更新和删除最终保持一致。覆盖通常需要几秒钟或几分钟才能传播，但可能需要长达 15 天的时间。

如果要在不同的一致性级别执行对象操作，可以为每个分段或每个 API 操作指定一致性控制。

一致性控制

一致性控制会影响 StorageGRID 用于跟踪对象的元数据在节点之间的分布方式，从而影响对象用于客户端请求的可用性。

您可以将存储分段或 API 操作的一致性控制设置为以下值之一：

- 全部：所有节点均立即接收数据、否则请求将失败。
- * 强 - 全局 * ：保证所有站点中所有客户端请求的写入后读一致性。
- * 强站点 * ：保证站点内所有客户端请求的写入后读一致性。
- 读后新写入：(默认)为新对象提供读后写入一致性、并最终为对象更新提供一致性。提供高可用性和数据保护保证。建议用于大多数情况。
- 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅根据需要使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行head或get操作)。S3 FabricPool 存储分段不支持。

使用"`read-after-new-write`"和"`available`"一致性控制

如果 head 或 get 操作使用 `read-after-new-write` 一致性控制，则 StorageGRID 将执行多个步骤的查找，如下所示：

- 它首先使用低一致性查找对象。
- 如果该查找失败、则会在下一个一致性级别重复执行该查找、直到达到与强全局行为等效的一致性级别为止。

如果head或get操作使用`read-after-new-write`一致性控制、但对象不存在、则对象查找将始终达到与强全局行为等效的一致性级别。由于此一致性级别要求在每个站点上提供多个对象元数据副本、因此、如果同一站点上的

一个或多个存储节点不可用、您可能会收到大量500个内部服务器错误。

除非您需要与 Amazon S3 类似的一致性保证，否则您可以通过将一致性控制设置为 "`Available" 来防止机头和 GET 操作出现这些错误。` 当机头或 GET 操作使用 "`Available` " 一致性控制时， StorageGRID 仅提供最终一致性。它不会在一致性级别提高时重试失败的操作、因此不要求对象元数据的多个副本可用。

为 API 操作指定一致性控制

要为单个 API 操作设置一致性控制，此操作必须支持一致性控制，并且必须在请求标题中指定一致性控制。此示例将 GET 对象操作的一致性控制设置为 `strong-site` 。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

PUT 对象和 GET 对象操作必须使用相同的一致性控制。

为存储分段指定一致性控制

要为存储分段设置一致性控制，您可以使用 StorageGRID PUT 存储分段一致性请求和 GET 存储分段一致性请求。或者，您也可以使用租户管理器或租户管理 API 。

为存储分段设置一致性控制时，请注意以下事项：

- 设置存储分段的一致性控制可确定对存储分段中的对象或存储分段配置执行 S3 操作时使用的一致性控制。它不会影响存储分段本身的操作。
- 单个 API 操作的一致性控制将覆盖存储分段的一致性控制。
- 通常，存储分段应使用默认一致性控制 `read-after-new-write` 。 如果请求无法正常工作，请尽可能更改应用程序客户端的行为。或者，配置客户端以指定每个 API 请求的一致性控制。请仅作为最后一种方法在存储分段级别设置一致性控制。

一致性控制和 ILM 规则如何交互以影响数据保护

您选择的一致性控制和 ILM 规则都会影响对象的保护方式。这些设置可以进行交互。

例如，存储对象时使用的一致性控制会影响对象元数据的初始放置，而为 ILM 规则选择的载入行为会影响对象副本的初始放置。由于 StorageGRID 需要访问对象的元数据及其数据来满足客户端请求，因此为一致性级别和载入行为选择匹配的保护级别可以提供更好的初始数据保护和更可预测的系统响应。

ILM 规则可以使用以下载入行为：

- * 严格 * ：必须创建 ILM 规则中指定的所有副本，才能将成功返回给客户端。
- * 平衡 * ： StorageGRID 尝试在载入时创建 ILM 规则中指定的所有副本；如果无法创建，则创建临时副本并将成功返回给客户端。在可能的情况下，将创建 ILM 规则中指定的副本。
- * 双提交 * ： StorageGRID 会立即为对象创建临时副本，并将成功返回给客户端。如果可能，将创建 ILM 规则中指定的副本。

在为ILM规则选择载入行为之前、请阅读中这些设置的完整问题描述 使用 ILM 管理对象。

一致性控制和 **ILM** 规则如何交互的示例

假设您有一个双站点网格，其中包含以下 ILM 规则和以下一致性级别设置：

- * ILM 规则 * ：创建两个对象副本，一个在本地站点，一个在远程站点。此时将选择严格的载入行为。
- * 一致性级别 * ： `strong-global` （对象元数据会立即分发到所有站点。）

当客户端将对象存储到网格时， StorageGRID 会创建两个对象副本并将元数据分发到两个站点，然后再向客户端返回成功。

在载入成功消息时，此对象将受到完全保护，不会丢失。例如，如果本地站点在载入后不久丢失，则远程站点上仍存在对象数据和对象元数据的副本。此对象完全可检索。

如果您改用相同的 ILM 规则和 `strong-site` 一致性级别，则在将对象数据复制到远程站点之后，在将对象元数据分发到该远程站点之前，客户端可能会收到一条成功消息。在这种情况下，对象元数据的保护级别与对象数据的保护级别不匹配。如果本地站点在载入后不久丢失，则对象元数据将丢失。无法检索此对象。

一致性级别和 ILM 规则之间的关系可能很复杂。如需帮助，请联系 NetApp 。

相关信息

获取存储分段一致性请求

PUT 存储分段一致性请求

StorageGRID ILM 规则如何管理对象

网格管理员创建信息生命周期管理（ ILM ）规则，用于管理从 S3 REST API 客户端应用程序输入到 StorageGRID 系统中的对象数据。然后，这些规则将添加到 ILM 策略中，以确定随着时间的推移对象数据的存储方式和存储位置。

ILM 设置可确定对象的以下方面：

- * 地理位置 *

  对象数据在 StorageGRID 系统（存储池）或云存储池中的位置。

- * 存储级别 *

  用于存储对象数据的存储类型：例如闪存或旋转磁盘。

- * 损失保护 *

  创建的副本数量以及创建的副本类型：复制，纠删编码或两者。

- * 保留 *

  随着时间的推移，对象数据的管理方式，存储位置以及保护数据免受丢失的方式会发生变化。

- * 载入期间的保护 *

  用于在载入期间保护对象数据的方法：同步放置（使用平衡或严格的 InGest 行为选项）或创建中间副本（使用双提交选项）。

ILM 规则可以筛选和选择对象。对于使用 S3 载入的对象， ILM 规则可以根据以下元数据筛选对象：

- 租户帐户
- Bucket Name
- 载入时间
- 密钥
- 上次访问时间

> 默认情况下，对所有 S3 分段禁用上次访问时间更新。如果您的 StorageGRID 系统包含使用上次访问时间选项的 ILM 规则，则必须为该规则中指定的 S3 分段启用对上次访问时间的更新。您可以使用租户管理器中的 PUT 分段上次访问时间请求， * S3* > * 分段 * > * 配置上次访问时间 * 复选框或租户管理 API 启用上次访问时间更新。启用上次访问时间更新时，请注意 StorageGRID 性能可能会降低，尤其是在具有小型对象的系统中。

- 位置限制
- 对象大小
- 用户元数据
- 对象标记

有关 ILM 的详细信息，请参见有关通过信息生命周期管理管理对象的说明。

相关信息

使用租户帐户

使用 ILM 管理对象

PUT 分段上次访问时间请求

对象版本控制

您可以使用版本控制来保留一个对象的多个版本，从而防止意外删除对象，并可用于检索和还原对象的早期版本。

StorageGRID 系统实施版本控制，并支持大多数功能，但存在一些限制。StorageGRID 最多支持 1 ， 000 个对象版本。

对象版本控制可以与 StorageGRID 信息生命周期管理（ ILM ）或 S3 存储分段生命周期配置结合使用。要为每个存储分段启用此功能，您必须明确启用版本控制。存储分段中的每个对象都分配有一个版本 ID ，该 ID 由 StorageGRID 系统生成。

不支持使用 MFA （多因素身份验证） Delete 。

只能在使用 StorageGRID 10.3 或更高版本创建的存储分段上启用版本控制。

ILM 和版本控制

ILM 策略将应用于对象的每个版本。ILM 扫描过程会持续扫描所有对象，并根据当前 ILM 策略重新评估这些对象。对 ILM 策略所做的任何更改都会应用于先前载入的所有对象。如果启用了版本控制，则包括先前载入的版本。ILM 扫描会将新的 ILM 更改应用于先前输入的对象。

对于启用了版本控制的分段中的 S3 对象，版本控制支持允许您创建使用非当前时间作为参考时间的 ILM 规则。对象更新后，其先前版本将变为非最新版本。使用非当前时间筛选器可以创建策略，以减少先前版本的对象对存储的影响。

使用多部分上传操作上传新版本的对象时，原始版本对象的非当前时间反映为新版本创建多部分上传的时间，而不是多部分上传完成的时间。在有限情况下，原始版本的非当前时间可能比当前版本的时间早数小时或数天。

有关 S3 版本控制对象的示例 ILM 策略，请参见有关通过信息生命周期管理管理对象的说明。

相关信息

使用 ILM 管理对象

实施 **S3 REST API** 的建议

在实施用于 StorageGRID 的 S3 REST API 时，应遵循以下建议。

针对不存在的对象的建议

如果您的应用程序定期检查某个对象是否位于您不希望该对象实际存在的路径上，则应使用 "`available` " 一致性控制。例如，如果您的应用程序在放置到某个位置之前一直位于某个位置，则应使用 "`Available` " 一致性控制。

否则，如果 head 操作未找到对象，则在一个或多个存储节点不可用时，可能会收到大量 500 个内部服务器错误。

您可以使用 PUT 存储分段一致性请求为每个存储分段设置 "`Available` " 一致性控制，也可以在单个 API 操作的请求标题中指定一致性控制。

对象密钥建议

对于在 StorageGRID 11.4 或更高版本中创建的分段，不再需要限制对象密钥名称以满足性能最佳实践。例如，现在可以对对象密钥名称的前四个字符使用随机值。

对于在 StorageGRID 11.4 之前的版本中创建的分段，请继续对对象密钥名称遵循以下建议：

- 不应使用随机值作为对象密钥的前四个字符。这与 AWS 以前针对密钥前缀的建议不同。而应使用非随机的非唯一前缀，例如 `image` 。
- 如果您按照以前的 AWS 建议在密钥前缀中使用随机和唯一字符，则应在对象密钥前添加目录名称。也就是说，请使用以下格式：

```
mybucket/mydir/f8e3-image3132.jpg
```

而不是以下格式：

```
mybucket/f8e3-image3132.jpg
```

关于"`范围读取`"的建议

如果选择了 * 压缩存储的对象 * 选项（ * 配置 * > * 系统 * > * 网格选项 * ），则 S3 客户端应用程序应避免执行指定要返回的字节数范围的 GET 对象操作。这些 "`range read` " 操作效率低下，因为 StorageGRID 必须有效解压缩对象以访问请求的字节。从非常大的对象请求少量字节的 GET 对象操作效率尤其低下；例如，从 50 GB 压缩对象读取 10 MB 范围的操作效率非常低。

如果从压缩对象读取范围，则客户端请求可能会超时。

如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

相关信息

- 一致性控制
- PUT 存储分段一致性请求
- 管理 StorageGRID

S3 REST API 支持的操作和限制

StorageGRID 系统实施简单存储服务 API （API 版本 2006-03-01 ），支持大多数操作，但有一些限制。在集成 S3 REST API 客户端应用程序时，您需要了解实施详细信息。

StorageGRID 系统既支持虚拟托管模式请求，也支持路径模式请求。

日期处理

S3 REST API 的 StorageGRID 实施仅支持有效的 HTTP 日期格式。

对于接受日期值的任何标头， StorageGRID 系统仅支持有效的 HTTP 日期格式。日期的时间部分可以使用格林威治标准时间（ GMT ）格式或通用协调时间（ UTC ）格式指定，并且不存在时区偏移（必须指定 +0000 ）。如果您在请求中包含 `x-AMZ-date` 标题，则此标题将覆盖日期请求标题中指定的任何值。使用 AWS 签名版本 4 时，签名请求中必须包含 `x-AMZ-date` 标头，因为不支持日期标头。

通用请求标头

StorageGRID 系统支持由定义的通用请求标头 "Amazon Web Services （AWS ）文档： Amazon Simple Storage Service API 参考"，但有一个例外。

请求标题	实施
Authorization	完全支持 AWS 签名版本 2 支持 AWS 签名版本 4 ，但以下情况除外： • 不会为请求正文计算 SHA256 值。接受用户提交的值而不进行验证，就好像为 `x-AMZ-content-SHA256` 标头提供了值 `unsigned-load` 一样。
X-AMZ-securation-token	未实施。返回 `XNotImplemented"` 。

通用响应标头

StorageGRID 系统支持由 _Simple Storage Service API 参考 _ 定义的所有通用响应标头，但有一个例外。

响应标头	实施
X-AMZ-ID-2	未使用

对请求进行身份验证

StorageGRID 系统支持使用 S3 API 对对象进行身份验证和匿名访问。

S3 API 支持签名版本 2 和签名版本 4 对 S3 API 请求进行身份验证。

经过身份验证的请求必须使用您的访问密钥 ID 和机密访问密钥进行签名。

StorageGRID 系统支持两种身份验证方法： HTTP `Authorization` header 和使用查询参数。

使用 **HTTP** 授权标头

HTTP `Authorization` 标头由所有 S3 API 操作使用，但在存储分段策略允许的情况下，匿名请求除外。`Authorization` 标头包含对请求进行身份验证所需的所有签名信息。

使用查询参数

您可以使用查询参数向 URL 添加身份验证信息。这称为对 URL 进行预签名，可用于授予对特定资源的临时访问权限。使用预签名 URL 的用户无需知道机密访问密钥即可访问资源，这样您就可以为资源提供第三方受限访问权限。

对服务执行的操作

StorageGRID 系统支持对该服务执行以下操作。

操作	实施
获取服务	在所有 Amazon S3 REST API 行为下实施。

操作	实施
获取存储使用量	" 获取存储使用量 " 请求会告知您帐户正在使用的存储总量以及与帐户关联的每个存储分段的存储总量。这是对服务执行的操作，其中添加了路径 / 和自定义查询参数（`？ x-ntap-sg-usage`）。
选项 /	客户端应用程序可以在不提供 S3 身份验证凭据的情况下对存储节点上的 S3 端口发出问题描述 `options /` 请求，以确定存储节点是否可用。您可以使用此请求进行监控，也可以允许外部负载平衡器确定存储节点何时关闭。

相关信息

获取存储使用情况请求

对存储分段执行的操作

对于每个 S3 租户帐户， StorageGRID 系统最多支持 1 ， 000 个分段。

存储分段名称限制遵循 AWS US 标准区域限制，但您应进一步将其限制为 DNS 命名约定，以便支持 S3 虚拟托管模式请求。

"Amazon Web Services （ AWS ）文档：存储分段限制"

配置 S3 API 端点域名

获取分段（列出对象）和获取分段版本操作支持 StorageGRID 一致性控制。

您可以检查是否已为各个存储分段启用上次访问时间更新。

下表介绍了 StorageGRID 如何实施 S3 REST API 存储分段操作。要执行其中任何操作，必须为帐户提供必要的访问凭据。

操作	实施
删除存储分段	在所有 Amazon S3 REST API 行为下实施。
删除存储分段或	此操作将删除存储分段的 CORS 配置。
删除存储分段加密	此操作将从存储分段中删除默认加密。现有加密对象保持加密状态，但添加到存储分段中的任何新对象不会加密。
删除存储分段生命周期	此操作将从存储分段中删除生命周期配置。
删除存储分段策略	此操作将删除附加到存储分段的策略。
删除存储分段复制	此操作将删除附加到存储分段的复制配置。

操作	实施
删除存储分段标记	此操作使用 `tagging` Subresource 从存储分段中删除所有标记。
获取分段（列出对象）版本 1 和版本 2	此操作将返回一个存储分段中的部分或全部（最多 1 ， 000 个）对象。对象的存储类可以具有两个值中的任一值，即使使用 `refastore_redundancy` storage class 选项载入对象也是如此： • `standard` ，表示对象存储在由存储节点组成的存储池中。 • `Glacier` ，表示对象已移至云存储池指定的外部存储分段。 如果存储分段包含大量前缀相同的已删除密钥，则响应可能包括一些不包含密钥的 `CommonPrefixes` 。
获取分段 ACL	此操作将返回肯定响应以及存储分段所有者的 ID ， DisplayName 和权限，指示所有者对存储分段具有完全访问权限。
获取分段存储器	此操作将返回存储分段的 `cors` 配置。
获取存储分段加密	此操作将返回存储分段的默认加密配置。
获取存储分段生命周期	此操作将返回存储分段的生命周期配置。
获取存储分段位置	此操作将返回在 PUT Bucket 请求中使用 `LocationConstrcont` 元素设置的区域。如果存储分段的区域为 `us-east-1` ，则会为该区域返回一个空字符串。
获取存储分段通知	此操作将返回附加到存储分段的通知配置。
获取 Bucket 对象版本	通过在存储分段上进行读取访问，此操作会使用 `versions` Subresource 列出存储分段中所有版本对象的元数据。
获取存储分段策略	此操作将返回附加到存储分段的策略。
获取存储分段复制	此操作将返回附加到存储分段的复制配置。
获取存储分段标记	此操作使用 `tagging` Subresource 返回存储分段的所有标记。
获取存储分段版本控制	此实施会使用 `ve`**决策** 子资源返回存储分段的版本控制状态。 • *blank* ： 从未启用版本控制（存储分段为 "`未版本控制` " ） • Enabled ： 已启用版本控制 • suspended ： 先前已启用版本控制并已暂停

操作	实施
获取对象锁定配置	此操作将返回存储分段默认保留模式和默认保留期限（如果已配置）。 请参见 获取对象锁定配置 了解详细信息。
头存储分段	此操作将确定某个存储分段是否存在，并且您有权访问该存储分段。 此操作将返回： • `x-ntap-sg-bucket-id`： UUID 格式的存储分段 UUID 。 • `x-ntap-sg-trace-id`：关联请求的唯一跟踪 ID 。
放入存储分段	此操作将创建一个新存储分段。创建存储分段后，您就会成为存储分段所有者。 • 存储分段名称必须符合以下规则： ◦ 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。 ◦ 必须符合 DNS 要求。 ◦ 必须至少包含 3 个字符，并且不能超过 63 个字符。 ◦ 可以是一个或多个标签的序列，并使用一个句点分隔相邻标签。每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。 ◦ 不能与文本格式的 IP 地址类似。 ◦ 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。 • 默认情况下，会在 `us-east-1` 区域中创建分段；但是，您可以使用请求正文中的 `LocationConstrcont` Request 元素来指定其他区域。使用 `LocationConstrcont` 元素时，必须指定已使用网格管理器或网格管理 API 定义的区域的确切名称。如果您不知道应使用的区域名称，请联系您的系统管理员。 • 注 * ：如果 PUT 存储分段请求使用的区域尚未在 StorageGRID 中定义，则会发生错误。 • 您可以使用 `x-AMZ-bucket-object-lock-enabled` 请求标头来创建启用了 S3 对象锁定的存储分段。请参见 使用 S3 对象锁定。 创建存储分段时，必须启用 S3 对象锁定。创建存储分段后，您无法添加或禁用 S3 对象锁定。S3 对象锁定需要分段版本控制，在创建分段时会自动启用分段版本控制。
放入存储分段箱	此操作会为存储分段设置 CORS 配置，以便存储分段可以处理跨源请求。跨源资源共享（ CORS ）是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如，假设您使用名为 `images` 的 S3 存储分段来存储图形。通过为 `images` 存储分段设置 CORS 配置，您可以允许在网站 ` + http://www.example.com+` 上显示该存储分段中的图像。

操作	实施
PUT 存储分段加密	此操作将设置现有存储分段的默认加密状态。启用存储分段级别加密后，添加到存储分段中的任何新对象都会进行加密。 StorageGRID 支持使用 StorageGRID 管理的密钥进行服务器端加密。指定服务器端加密配置规则时，请将 `SSEAlgorithm` 参数设置为 `AES256` ，不要使用 `KMSMasterKeyID` 参数。 如果对象上传请求已指定加密（即，如果请求包含 `x-AMZ-server-side encryption-*` 请求标头），则存储分段默认加密配置将被忽略。
PUT 存储分段生命周期	此操作将为存储分段创建新的生命周期配置或替换现有的生命周期配置。StorageGRID 在一个生命周期配置中最多支持 1 ， 000 条生命周期规则。每个规则可以包含以下 XML 元素： • 到期日期（天，日期） • 非当前版本到期（非当前日期） • 筛选器（前缀，标记） • Status • ID StorageGRID 不支持以下操作： • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • 过渡 要了解存储分段生命周期中的到期操作如何与 ILM 放置说明交互，请参见使用信息生命周期管理功能管理对象的说明中的 "`ILM 如何在对象的整个生命周期内运行` "。 • 注 *：存储分段生命周期配置可用于启用了 S3 对象锁定的存储分段，但传统合规存储分段不支持存储分段生命周期配置。

操作	实施

PUT 存储分段通知	此操作将使用请求正文中包含的通知配置 XML 为存储分段配置通知。您应了解以下实施详细信息：
	
	• StorageGRID 支持将简单通知服务（ SNS ）主题作为目标。不支持简单队列服务（ SQS ）或 Amazon Lambda 端点。
	• 必须将通知目标指定为 StorageGRID 端点的 URN 。可以使用租户管理器或租户管理 API 创建端点。
	
	要成功配置通知，端点必须存在。如果端点不存在，则返回 `400 bad request` 错误，并显示代码 `InvalidArgument` 。
	
	• 您不能为以下事件类型配置通知。这些事件类型 * 不 * 受支持。
	
	◦ `s 3` ：异径冗余 `LostObject`
	
	◦ `s 3` ： `ObjectRestore` ：已完成
	
	• 从 StorageGRID 发送的事件通知使用标准 JSON 格式，只是它们不包含某些密钥，而对其他密钥使用特定值，如以下列表所示：
	• * 事件源 *
	
	`sGWS` ： `S3`
	
	• * awsRegion*
	
	不包括
	
	• * 。 x-AMZ-id-2*
	
	不包括
	
	• * arn*
	
	`urn` ： `sgws` ： `s3` ：：： `bucket_name`

PUT 存储分段策略	此操作将设置附加到存储分段的策略。

操作	实施
PUT 存储分段复制	此操作将使用请求正文中提供的复制配置 XML 为存储分段配置 StorageGRID CloudMirror 复制。对于 CloudMirror 复制，您应了解以下实施详细信息： • StorageGRID 仅支持复制配置的 V1 。这意味着， StorageGRID 不支持使用 `Filter` 元素作为规则，并遵循 V1 约定删除对象版本。有关详细信息，请参见 "有关复制配置的 Amazon S3 文档"。 • 分段复制可以在分版本或未分版本的分段上配置。 • 您可以在复制配置 XML 的每个规则中指定不同的目标存储分段。一个源存储分段可以复制到多个目标存储分段。 • 必须将目标分段指定为租户管理器或租户管理 API 中指定的 StorageGRID 端点的 URN 。 要成功进行复制配置，必须存在此端点。如果此端点不存在，则此请求将失败，并显示 `400` 错误请求 。错误消息显示： `Unable to save the replication policy` 。指定的端点 `URN` 不存在： *`URN`* 。 • 您不需要在配置 XML 中指定 `role` 。StorageGRID 不使用此值，如果提交，则会忽略此值。 • 如果在配置 XML 中省略存储类，则 StorageGRID 默认使用 `Standard` storage class 。 • 如果从源存储分段中删除对象或删除源存储分段本身，则跨区域复制行为如下： ◦ 如果在复制对象或存储分段之前将其删除，则不会复制此对象 / 存储分段，您也不会收到通知。 ◦ 如果您在复制对象或存储分段后将其删除，则 StorageGRID 会对跨区域复制的 V1 遵循标准 Amazon S3 删除行为。
放置存储分段标记	此操作使用 `tagging` Subresource 为存储分段添加或更新一组标记。添加存储分段标记时，请注意以下限制： • StorageGRID 和 Amazon S3 为每个存储分段最多支持 50 个标签。 • 与存储分段关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可包含 128 个 Unicode 字符。 • 标记值的长度最多可以为 256 个 Unicode 字符。 • 密钥和值区分大小写。
PUT 存储分版本	此实施使用 `ve`决策 子资源来设置现有存储分段的版本控制状态。您可以使用以下值之一设置版本控制状态： • Enabled ： 为存储分段中的对象启用版本控制。添加到存储分段中的所有对象都会收到唯一的版本 ID 。 • suspended ： 为存储分段中的对象禁用版本控制。添加到存储分段的所有对象都会收到版本 ID `null` 。

操作	实施
PUT 对象锁定配置	此操作将配置或删除存储分段默认保留模式和默认保留期限。 如果修改了默认保留期限，则现有对象版本的保留日期将保持不变，不会使用新的默认保留期限重新计算。 请参见 PUT 对象锁定配置 了解详细信息。

相关信息

一致性控制

获取分段上次访问时间请求

存储分段和组访问策略

在审核日志中跟踪 S3 操作

使用 ILM 管理对象

使用租户帐户

创建 **S3** 生命周期配置

您可以创建 S3 生命周期配置，以控制何时从 StorageGRID 系统中删除特定对象。

本节中的简单示例说明了 S3 生命周期配置如何控制从特定 S3 存储分段中删除（过期）某些对象的时间。本节中的示例仅供说明。有关创建 S3 生命周期配置的完整详细信息，请参见 "《Amazon Simple Storage Service 开发人员指南：对象生命周期管理》"。请注意， StorageGRID 仅支持到期操作，不支持过渡操作。

什么是生命周期配置

生命周期配置是一组应用于特定 S3 分段中的对象的规则。每个规则都指定受影响的对象以及这些对象的到期时间（在特定日期或一定天数后）。

StorageGRID 在一个生命周期配置中最多支持 1 ， 000 条生命周期规则。每个规则可以包含以下 XML 元素：

- 到期日期：从对象载入开始，在达到指定日期或达到指定天数时删除对象。
- NoncurrentVersionExpiration ：从对象变为非最新状态开始，在达到指定天数时删除对象。
- 筛选器（前缀，标记）
- Status
- ID

如果将生命周期配置应用于某个存储分段，则存储分段的生命周期设置始终会覆盖 StorageGRID ILM 设置。StorageGRID 使用存储分段的 " 到期 " 设置（而不是 ILM ）来确定是删除还是保留特定对象。

因此，即使 ILM 规则中的放置说明仍适用于某个对象，该对象也可能会从网格中删除。或者，即使对象的任何 ILM 放置指令已失效，该对象也可能会保留在网格中。有关详细信息，请参见 ILM 如何在对象的整个生命周期内运行。

存储分段生命周期配置可用于启用了 S3 对象锁定的存储分段，但旧版合规存储分段不支持存储分段生命周期配置。

StorageGRID 支持使用以下存储分段操作来管理生命周期配置：

- 删除存储分段生命周期
- 获取存储分段生命周期
- PUT 存储分段生命周期

创建生命周期配置

作为创建生命周期配置的第一步，您需要创建一个包含一个或多个规则的 JSON 文件。例如，此 JSON 文件包含三个规则，如下所示：

1. 规则 1 仅适用于与前缀 `category1` / 匹配且 `key2` 值为 `ag2` 的对象。`Expiration` 参数指定与筛选器匹配的对象将在 2020 年 8 月 22 日午夜到期。
2. 规则 2 仅适用于与前缀 `category2` / 匹配的对象。`Expiration` 参数指定与筛选器匹配的对象将在载入后 100 天后过期。

   指定天数的规则与对象的载入时间相关。如果当前日期超过载入日期加上天数，则在应用生命周期配置后，可能会立即从存储分段中删除某些对象。

3. 规则 3 仅适用于与前缀 `category3` / 匹配的对象。`Expiration` 参数指定任何非最新版本的匹配对象将在其变为非最新状态 50 天后过期。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

将生命周期配置应用于存储分段

创建生命周期配置文件后，您可以通过发出 PUT 存储分段生命周期请求将其应用于存储分段。

此请求会将示例文件中的生命周期配置应用于名为 `testbucket` 的存储分段中的对象。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

要验证是否已成功将生命周期配置应用于存储分段，请发送问题描述 获取存储分段生命周期请求。例如：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功的响应将列出您刚刚应用的生命周期配置。

验证存储分段生命周期到期适用场景 对象

在发出 PUT 对象， HEAD 对象或 GET 对象请求时，您可以确定生命周期配置适用场景 中的到期规则是否为特定对象。如果适用某条规则，响应将包含一个 `Expiration` 参数，用于指示对象何时到期以及匹配的到期规则。

> 由于存储分段生命周期会覆盖 ILM ，因此显示的 `expiry-date` 是删除对象的实际日期。有关详细信息，请参见 如何确定对象保留。

例如，此 PUT 对象请求是在 2020 年 6 月 22 日发出的，并将一个对象放置在 `testbucket` 存储分段中。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功响应表示此对象将在 100 天后（ 2020 年 10 月 1 日）过期，并且与生命周期配置的规则 2 匹配。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

例如，此 head Object 请求用于获取测试分段中同一对象的元数据。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功响应包括对象的元数据，并指示对象将在 100 天后过期，并且与规则 2 匹配。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

使用 **S3** 对象锁定默认存储分段保留

如果存储分段启用了 S3 对象锁定，则可以指定应用于添加到存储分段中的每个对象的默认保留模式和默认保留期限。

- 在创建存储分段期间，可以为存储分段启用或禁用 S3 对象锁定。
- 如果为存储分段启用了 S3 对象锁定，则可以为存储分段配置默认保留。
- 默认保留配置指定：
  - 默认保留模式： StorageGRID 仅支持 " 合规 " 模式。
  - 默认保留期限，以天或年为单位。

获取对象锁定配置

通过获取对象锁定配置请求，您可以确定是否为存储分段启用了对象锁定，如果已启用，请查看是否为存储分段配置了默认保留模式和保留期限。

将新对象版本载入存储分段后，如果未指定 `x-AMZ-object-lock-mode` ，则会应用默认保留模式。如果未指定 `x-AMZ-object-lock-retain-until date` ，则使用默认保留期限计算 retene-until 日期。

要完成此操作，您必须具有 S3： GetBucketObjectLockConfiguration 权限或帐户 root 。

请求示例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization string
Authorization: authorization string
```

响应示例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

PUT 对象锁定配置

使用 PUT 对象锁定配置请求，您可以修改已启用对象锁定的存储分段的默认保留模式和默认保留期限。您还可以删除先前配置的默认保留设置。

将新对象版本载入存储分段后，如果未指定 `x-AMZ-object-lock-mode` ，则会应用默认保留模式。如果未指定 `x-AMZ-object-lock-retain-until date` ，则使用默认保留期限计算 retene-until 日期。

如果在载入对象版本后修改了默认保留期限，则对象版本的保留日期将保持不变，不会使用新的默认保留期限重新计算。

要完成此操作，您必须具有 S3： PutBucketObjectLockConfiguration 权限或帐户 root 。

必须在 PUT 请求中指定 `Content-MD5` 请求标头。

请求示例

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization string
Authorization: authorization string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

对存储分段执行自定义操作

StorageGRID 系统支持添加到 S3 REST API 中且特定于系统的自定义存储分段操作。

下表列出了 StorageGRID 支持的自定义存储分段操作。

操作	Description	有关详细信息 ...
获取存储分段一致性	返回应用于特定存储分段的一致性级别。	获取存储分段一致性请求
PUT 存储分段一致性	设置应用于特定存储分段的一致性级别。	PUT 存储分段一致性请求
获取存储分段上次访问时间	返回为特定存储分段启用还是禁用上次访问时间更新。	获取分段上次访问时间请求
PUT 分段上次访问时间	用于启用或禁用特定存储分段的上次访问时间更新。	PUT 分段上次访问时间请求
删除存储分段元数据通知配置	删除与特定存储分段关联的元数据通知配置 XML 。	删除存储分段元数据通知配置请求

操作	Description	有关详细信息 ...
获取存储分段元数据通知配置	返回与特定存储分段关联的元数据通知配置 XML 。	获取存储分段元数据通知配置请求
PUT 存储分段元数据通知配置	配置存储分段的元数据通知服务。	PUT 存储分段元数据通知配置请求
使用合规设置放置存储分段	已弃用且不支持：您无法再在启用合规性的情况下创建新存储分段。	已弃用：使用合规性设置放置存储分段
获取存储分段合规性	已弃用但受支持：返回当前对现有旧版合规存储分段有效的合规性设置。	已弃用：获取存储分段合规性请求
PUT 存储分段合规性	已弃用但受支持：允许您修改现有旧版合规存储分段的合规性设置。	已弃用： PUT 存储分段合规性请求

相关信息

审核日志中跟踪的 S3 操作

对对象执行的操作

本节介绍 StorageGRID 系统如何对对象实施 S3 REST API 操作。

以下条件适用于所有对象操作：

- StorageGRID 一致性控制 支持对对象执行的所有操作，但以下操作除外：
  - 获取对象 ACL
  - 选项 /
  - PUT 对象合法保留
  - 放置对象保留
  - 选择对象内容
- 冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。
- StorageGRID 存储分段中的所有对象均归存储分段所有者所有，包括由匿名用户或其他帐户创建的对象。
- 无法通过 S3 访问通过 Swift 载入到 StorageGRID 系统的数据对象。

下表介绍了 StorageGRID 如何实施 S3 REST API 对象操作。

操作	实施
删除对象	不支持多因素身份验证（ Multi-Factor Authentication ， MFA ）和响应标头 `x-AMZ-MFA` 。 在处理删除对象请求时， StorageGRID 会尝试立即从所有存储位置删除此对象的所有副本。如果成功， StorageGRID 会立即向客户端返回响应。如果无法在 30 秒内删除所有副本（例如，由于某个位置暂时不可用），则 StorageGRID 会将这些副本排队等待删除，然后指示客户端成功删除。 • 版本控制 * 要删除特定版本，请求者必须是存储分段所有者，并使用 `veversionId` Subresource 。使用此子资源将永久删除此版本。如果 `veversionId` 对应于删除标记，则返回的响应标头 `x-AMZ-delete-marker` 将设置为 `true` 。 • 如果在已启用版本的存储分段上删除不带 `veversionId` Subresource 的对象，则会生成删除标记。使用 `x-AMZ-version-id` 响应标头返回删除标记的 `veversionId` ，返回的 `x-AMZ-delete-marker` response 标头设置为 `true` 。 • 如果在版本暂停的分段上删除了不带 `veversionId` Subresource 的对象，则会永久删除已存在的 "null" 版本或 "null" 删除标记，并生成新的 "null" 删除标记。返回的 `x-AMZ-delete-marker` 响应标头设置为 `true` 。 • 注意 *： 在某些情况下，一个对象可能存在多个删除标记。
删除多个对象	不支持多因素身份验证（ Multi-Factor Authentication ， MFA ）和响应标头 `x-AMZ-MFA` 。 可以在同一请求消息中删除多个对象。
删除对象标记	使用 `tagging` Subresource 从对象中删除所有标记。在所有 Amazon S3 REST API 行为下实施。 • 版本控制 * 如果未在此请求中指定 `veversionId` query 参数，则此操作将删除受版本控制的存储分段中最新版本对象的所有标记。如果对象的当前版本为删除标记，则返回 "n `MethodNotAllowed` " 状态，并将 `x-AMZ-delete-marker` response 标头设置为 `true` 。
获取对象	获取对象
获取对象 ACL	如果为帐户提供了必要的访问凭据，则此操作将返回肯定响应以及对象所有者的 ID ， DisplayName 和权限，指示所有者对对象具有完全访问权限。

操作	实施
获取对象合法保留	使用 S3 对象锁定
获取对象保留	使用 S3 对象锁定
获取对象标记	使用 `tagging` Subresource 返回对象的所有标记。在所有 Amazon S3 REST API 行为下实施 • 版本控制 * 如果在请求中未指定 `veversionId` query 参数，则此操作将返回受版本控制的存储分段中最新版本对象的所有标记。如果对象的当前版本为删除标记，则返回 "n `MethodNotAllowed` " 状态，并将 `x-AMZ-delete-marker` response 标头设置为 `true` 。
HEAD 对象	HEAD 对象
后对象还原	后对象还原
PUT 对象	PUT 对象
PUT 对象—复制	PUT 对象—复制
PUT 对象合法保留	使用 S3 对象锁定
放置对象保留	使用 S3 对象锁定

操作	实施
PUT 对象标记	使用 `tagging` Subresource 向现有对象添加一组标记。在所有 Amazon S3 REST API 行为下实施 • 对象标记限制 * 您可以在上传新对象时为其添加标记，也可以将其添加到现有对象中。StorageGRID 和 Amazon S3 对每个对象最多支持 10 个标记。与对象关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可以是 128 个 Unicode 字符，而标记值的长度最多可以是 256 个 Unicode 字符。密钥和值区分大小写。 • 标记更新和载入行为 * 使用 PUT 对象标记更新对象的标记时， StorageGRID 不会重新载入对象。这意味着不会使用匹配 ILM 规则中指定的 " 载入行为 " 选项。通过正常后台 ILM 进程重新评估 ILM 时，更新触发的任何对象放置更改都会进行。 这意味着，如果 ILM 规则对载入行为使用严格选项，则在无法放置所需对象时（例如，由于新需要的位置不可用），不会执行任何操作。更新后的对象会保留其当前位置，直到可以进行所需的位置为止。 • 解决冲突 * 冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。 • 版本控制 * 如果在请求中未指定 `veversionId` query 参数，则该操作会向受版本控制的存储分段中的对象的最新版本添加标记。如果对象的当前版本为删除标记，则返回 "n `MethodNotAllowed` " 状态，并将 `x-AMZ-delete-marker` response 标头设置为 `true` 。

相关信息

在审核日志中跟踪 S3 操作

使用 **S3** 对象锁定

如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以在启用了 S3 对象锁定的情况下创建存储分段，然后为每个存储分段指定默认保留期限，或者为添加到存储分段的每个对象版本指定特定的保留截止日期和合法保留设置。

通过 S3 对象锁定，您可以指定对象级别的设置，以防止对象在固定时间内或无限期地被删除或覆盖。

StorageGRID S3 对象锁定功能提供了一种保留模式，相当于 Amazon S3 合规模式。默认情况下，任何用户都无法覆盖或删除受保护的对象版本。StorageGRID S3 对象锁定功能不支持监管模式，并且不允许具有特殊权限的用户绕过保留设置或删除受保护的对象。

为存储分段启用 S3 对象锁定

如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以选择在创建每个分段时启用 S3 对象锁定。您可以使用以下任一方法：

- 使用租户管理器创建存储分段。

  使用租户帐户

- 使用具有 `x-AMZ-bucket-object-lock-enabled` 请求标题的 PUT Bucket 请求创建存储分段。

  对存储分段执行的操作

创建存储分段后，您无法添加或禁用 S3 对象锁定。S3 对象锁定需要分段版本控制，在创建分段时会自动启用分段版本控制。

启用了 S3 对象锁定的存储分段可以包含具有和不具有 S3 对象锁定设置的对象组合。StorageGRID 支持 S3 对象锁定分段中的对象的默认保留期限，并支持 PUT 对象锁定配置分段操作。`s 3 ： object-lock-remaing-retention-days` 策略条件键可设置对象允许的最小和最大保留期限。

确定是否为存储分段启用了 S3 对象锁定

要确定是否已启用 S3 对象锁定，请使用 获取对象锁定配置 请求。

使用 S3 对象锁定设置创建对象

要在将对象版本添加到启用了 S3 对象锁定的存储分段时指定 S3 对象锁定设置，请问题描述 对 PUT 对象，PUT 对象 - 复制或启动多部件上传请求。请使用以下请求标头。

> 创建存储分段时，必须启用 S3 对象锁定。创建存储分段后，您无法添加或禁用 S3 对象锁定。

- `x-AMZ-object-lock-mode` ，必须符合要求（区分大小写）。

  > 如果指定 `x-AMZ-object-lock-mode` ，则还必须指定 `x-AMZ-object-lock-retain-until date` 。

- `x-AMZ-object-lock-retain-until date`
  - 保留日期值的格式必须为 `2020-08-10T21 ： 46 ： 00Z` 。允许使用小数秒，但仅保留 3 位小数（精确度为毫秒）。不允许使用其他 ISO 8601 格式。
  - 保留截止日期必须为未来日期。
- `x-AMZ-object-lock-legal-hold`

  如果处于合法保留状态（区分大小写），则对象将置于合法保留状态。如果关闭了合法保留，则不会进行合法保留。任何其他值都会导致 400 错误请求（ InvalidArgument ）错误。

如果您使用上述任一请求标头，请注意以下限制：

- 如果 PUT 对象请求中存在任何 `x-AMZ-object-lock-*` 请求标头，则需要提供 `Content-MD5` 请求标头。PUT 对象 - 复制或启动多部件上传不需要 `Content-MD5` 。

- 如果存储分段未启用 S3 对象锁定，并且存在 `x-AMZ-object-lock-*` 请求标头，则会返回 400 错误请求（ InvalidRequest ）错误。
- PUT 对象请求支持使用 `x-AMZ-storage-class ： reduced _redundancy` 来匹配 AWS 行为。但是，如果在启用了 S3 对象锁定的情况下将对象载入存储分段，则 StorageGRID 将始终执行双提交载入。
- 如果已配置标题 `x-AMZ-object-lock-mode ， x-AMZ-object-lock-retain-tilt-date` 和 `x-AMZ-object-lock-legal-hold` ，并且请求发送方具有正确的 `s 3 ： get*` 权限，则后续 GET 或 HEAD 对象版本响应将包括标题 x-AMZ-object-lock-legal-hold 。
- 如果后续的删除对象版本或删除对象版本请求早于保留截止日期或处于合法保留状态，则此请求将失败。

更新 **S3** 对象锁定设置

如果需要更新现有对象版本的合法保留或保留设置，可以执行以下对象子资源操作：

- `PUT` 对象合法保留

  如果新的合法保留值为 on ，则对象将置于合法保留状态。如果合法保留值为 off ，则取消合法保留。

- 放置对象保留
  - 模式值必须符合要求（区分大小写）。
  - 保留日期值的格式必须为 `2020-08-10T21 ： 46 ： 00Z` 。允许使用小数秒，但仅保留 3 位小数（精确度为毫秒）。不允许使用其他 ISO 8601 格式。
  - 如果对象版本具有现有的保留日期，则只能增加此保留日期。新的价值必须是未来的。

相关信息

使用 ILM 管理对象

使用租户帐户

PUT 对象

PUT 对象—复制

启动多部件上传

对象版本控制

"《 Amazon Simple Storage Service 用户指南：使用 S3 对象锁定》"

使用 **S3 Select**

StorageGRID 支持以下 AWS S3 Select 子句，数据类型和运算符 SelectObjectContent 命令。

> 不支持未列出的任何项目。

有关语法，请参见 SelectObjectContent。有关 S3 Select 的详细信息，请参见 "适用于 S3 Select 的 AWS 文档"。

只有启用了 S3 Select 的租户帐户才能进行问题描述 SelectObjectContent 查询。请参见 使用 S3 Select 的注意事项和要求。

条款

- 选择列表
- from 子句
- Where 子句
- Limit 子句

数据类型

- 池
- 整型
- string
- 浮点
- 小数点，数字
- timestamp

运算符

逻辑运算符

- 和
- 不是
- 或

比较运算符

- <
- >
- &lt； =
- &gt； =
- =
- =
- <>
- ！ =
- 介于之间
- 在中

模式匹配运算符

- 例如
- _
- %

统一运算符

- 为空
- 不为空

数学运算符

- +
- -
- *
- /
- %

StorageGRID 遵循 AWS S3 Select 运算符优先级。

聚合函数

- 平均（）
- 计数（ * ）
- 最大值（）
- 最小值（）
- sum（ ）

条件函数

- 案例
- 合并
- NULLIF

转换函数

- cast （用于受支持的数据类型）

date 函数

- 日期添加
- 日期差异
- 提取

- to_string
- to_timestamp
- UTCNOW

字符串函数

- char_length ， character_length
- 更低
- 子字符串
- 剪切
- 上限

使用服务器端加密

服务器端加密可用于保护空闲对象数据。StorageGRID 会在写入对象时对数据进行加密，并在您访问对象时对数据进行解密。

如果要使用服务器端加密，可以根据加密密钥的管理方式从两个互斥选项中选择任一选项：

- *SSE （使用 StorageGRID 管理的密钥进行服务器端加密） *： 在问题描述 S3 请求以存储对象时， StorageGRID 会使用唯一密钥对对象进行加密。在问题描述 S3 请求以检索对象时， StorageGRID 会使用存储的密钥对对象进行解密。
- * SSI-C （使用客户提供的密钥进行服务器端加密） *： 在问题描述 S3 请求以存储对象时，您可以提供自己的加密密钥。检索对象时，您可以在请求中提供相同的加密密钥。如果这两个加密密钥匹配，则会对对象进行解密，并返回您的对象数据。

  虽然 StorageGRID 负责管理所有对象加密和解密操作，但您必须管理提供的加密密钥。

  您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。

  如果使用 SSE 或 SSI-C 对对象进行加密，则会忽略任何分段级别或网格级别的加密设置。

使用 **SS**

要使用 StorageGRID 管理的唯一密钥对对象进行加密，请使用以下请求标头：

```
x-AMZ-server-side encryption
```

以下对象操作支持此命令头：

- PUT 对象
- PUT 对象—复制
- 启动多部件上传

使用 **SSI-C**

要使用您管理的唯一密钥对对象进行加密，请使用三个请求标头：

请求标题	**Description**
`x-AMZ-server-side encryption -customer-运算 法则`	指定加密算法。标题值必须为 `AES256` 。
`x-AMZ-server-side encryption -customer -key`	指定用于对对象进行加密或解密的加密密钥。密钥的值必须为 256 位 base64 编码。
`x-AMZ-server-side -m ü s-customer-key-md5 encryption`	根据 RFC 1321 指定加密密钥的 MD5 摘要，用于确保加密密钥的传输没有错误。MD5 摘要的值必须为 base64 编码的 128 位。

以下对象操作支持 SSI-C 请求标头：

- 获取对象
- HEAD 对象
- PUT 对象
- PUT 对象—复制
- 启动多部件上传
- 上传部件
- 上传部件—复制

将服务器端加密与客户提供的密钥（ **SSI-C** ）结合使用的注意事项

在使用 SSI-C 之前，请注意以下注意事项：

- 必须使用 https 。

> 使用 SSI-C 时， StorageGRID 会拒绝通过 http 发出的任何请求出于安全考虑，您应考虑使用 http 意外发送的任何密钥受到损坏。丢弃该密钥，并根据需要旋转。

- 响应中的 ETag 不是对象数据的 MD5 。
- 您必须管理加密密钥到对象的映射。StorageGRID 不存储加密密钥。您负责跟踪为每个对象提供的加密密钥。
- 如果您的存储分段已启用版本控制，则每个对象版本都应具有自己的加密密钥。您负责跟踪每个对象版本使用的加密密钥。
- 由于您在客户端上管理加密密钥，因此您还必须在客户端上管理任何其他保护措施，例如密钥轮换。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。

- 如果为存储分段配置了 CloudMirror 复制，则无法载入 SSI-C 对象。载入操作将失败。

相关信息

获取对象

HEAD 对象

PUT 对象

PUT 对象—复制

启动多部件上传

上传部件

上传部件—复制

"Amazon S3 开发人员指南：使用客户提供的加密密钥（ SSI-C ）使用服务器端加密保护数据"

获取对象

您可以使用 S3 GET 对象请求从 S3 存储分段检索对象。

获取对象和多部分对象

您可以使用 `partnumber` request 参数检索多部分或分段对象的特定部分。`x-AMZ-MP-parts-count` 响应元素指示对象包含的部件数。

对于已分段 / 多部分对象和未分段 / 非多部分对象，您可以将 `partnumber` 设置为 1 ；但是，仅对于已分段或多部分对象，才会返回 `x-AMZ-MP-parts-count` response 元素。

使用客户提供的加密密钥（ **SSI-C** ）进行服务器端加密的请求标头

如果使用您提供的唯一密钥对对象进行加密，请使用所有三个标头。

- `x-AMZ-server-side encrypt-customer-all` ：指定 `AES256` 。
- `x-AMZ-server-side encrypt-customer-key` ：指定对象的加密密钥。
- `x-AMZ-server-side encrypt-customer-key-md5` ：指定对象加密密钥的 MD5 摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`

用户元数据中的 **UTF-8** 字符

StorageGRID 不会解析或解释用户定义的元数据中的转义 UTF-8 字符。如果密钥名称或值包含不可打印的字符，则对用户定义的元数据中包含转义 UTF-8 字符的对象的获取请求不会返回 `x-AMZ-MISSING-meta` 标头。

请求标头不受支持

不支持以下请求标头，并返回 `XNotImplemented"` ：

- `x-AMZ-website-redirect-location`

版本控制

如果未指定 `veversionId` Subresource ，则此操作将提取受版本控制的存储分段中的对象的最新版本。如果对象的当前版本为删除标记，则返回 "`not found` " 状态，并将 `x-AMZ-delete-marker` response 标头设置为 `true` 。

Cloud Storage Pool 对象的 **GET** 对象行为

如果某个对象已存储在云存储池中（请参见有关通过信息生命周期管理来管理对象的说明），则 GET 对象请求的行为取决于对象的状态。有关详细信息，请参见 "`head Object` " 。

如果某个对象存储在云存储池中，并且该对象的一个或多个副本也位于网格中，则获取对象请求将尝试从网格中检索数据，然后再从云存储池中检索数据。

对象的状态	**GET** 对象的行为
对象已载入 StorageGRID 但尚未通过 ILM 进行评估，或者存储在传统存储池中的对象或使用纠删编码	`200` 正常 检索对象的副本。
云存储池中的对象，但尚未过渡到无法检索的状态	`200` 正常 检索对象的副本。
对象已过渡到无法检索的状态	`403 For`禁用， `InvalidObjectState` 使用 POST 对象还原请求将对象还原到可检索的状态。
正在从不可检索状态还原的对象	`403 For`禁用， `InvalidObjectState` 等待 POST 对象还原请求完成。
对象已完全还原到云存储池	`200` 正常 检索对象的副本。

云存储池中的多部分或分段对象

如果您上传的是多部分对象或 StorageGRID 将一个大型对象拆分为多个区块，则 StorageGRID 会通过取样该对象的部分或区块来确定该对象是否在云存储池中可用。在某些情况下，如果对象的某些部分已过渡到不可检索的状态或对象的某些部分尚未还原，则获取对象请求可能会错误地返回 `200` 正常 。

在这些情况下：

- GET 对象请求可能会返回一些数据，但会在传输过程中停止。

- 后续的 GET 对象请求可能会返回 `403 For禁用` 。

相关信息

使用服务器端加密

使用 ILM 管理对象

后对象还原

在审核日志中跟踪 S3 操作

HEAD 对象

您可以使用 S3 head Object 请求从对象检索元数据，而无需返回对象本身。如果对象存储在云存储池中，则可以使用 head 对象确定对象的过渡状态。

head 对象和多部分对象

您可以使用 `partnumber` request 参数检索多部分或已分段对象的特定部分的元数据。`x-AMZ-MP-parts-count` 响应元素指示对象包含的部件数。

对于已分段 / 多部分对象和未分段 / 非多部分对象，您可以将 `partnumber` 设置为 1 ；但是，仅对于已分段或多部分对象，才会返回 `x-AMZ-MP-parts-count` response 元素。

使用客户提供的加密密钥（ **SSI-C** ）进行服务器端加密的请求标头

如果对象使用您提供的唯一密钥进行加密，请使用所有这三个标头。

- `x-AMZ-server-side encrypt-customer-all` ： 指定 `AES256` 。
- `x-AMZ-server-side encrypt-customer-key` ： 指定对象的加密密钥。
- `x-AMZ-server-side encrypt-customer-key-md5` ： 指定对象加密密钥的 MD5 摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`

用户元数据中的 **UTF-8** 字符

StorageGRID 不会解析或解释用户定义的元数据中的转义 UTF-8 字符。如果密钥名称或值包含不可打印的字符，则对用户定义的元数据中包含转义 UTF-8 字符的对象发出的 HEAD 请求不会返回 `x-AMZ-MISSING-meta` 标头。

请求标头不受支持

不支持以下请求标头，并返回 `XNotImplemented"` ：

- `x-AMZ-website-redirect-location`

Cloud Storage Pool 对象的响应标头

如果对象存储在云存储池中（请参见有关通过信息生命周期管理来管理对象的说明），则返回以下响应标头：

- `X-AMZ-storage-class ： Glacier`
- `x-AMZ-restore`

响应标头提供了有关对象移动到云存储池，可选择过渡到不可检索状态并已还原时的状态的信息。

对象的状态	对 **head** 对象的响应
对象已载入 StorageGRID 但尚未通过 ILM 进行评估，或者存储在传统存储池中的对象或使用纠删编码	`200 正常` （不返回任何特殊响应标头。）

云存储池中的对象，但尚未过渡到无法检索的状态	`200 正常`
	
	`X-AMZ-storage-class ： Glacier`
	
	`x-AMZ-restore ： ongoing-request="false" ， expiry-date="Sat" ， 20 年 7 月 23 日 20300000000000000000000"`
	
	在将对象过渡到不可检索的状态之前， `expiry-date` 的值将设置为未来的某个远程时间。确切的过渡时间不受 StorageGRID 系统控制。

对象已过渡到不可检索状态，但网格上至少也存在一个副本	`200 正常`
	
	`X-AMZ-storage-class ： Glacier`
	
	`x-AMZ-restore ： ongoing-request="false" ， expiry-date="Sat" ， 20 年 7 月 23 日 20300000000000000000000"`
	
	`expiry-date` 的值将设置为未来的某个距离时间。
	
	• 注意 *： 如果网格上的副本不可用（例如，存储节点已关闭），则必须先对后对象还原请求进行问题描述 处理，以便从云存储池还原此副本，然后才能成功检索此对象。

对象已过渡到无法检索的状态，网格上不存在任何副本	`200 正常`
	
	`X-AMZ-storage-class ： Glacier`

对象的状态	对 **head** 对象的响应

正在从不可检索状态还原的对象	`200` 正常
	
	`X-AMZ-storage-class ： Glacier`
	
	`x-AMZ-restore ： ongoing-request="true"`

对象已完全还原到云存储池	`200` 正常
	
	`X-AMZ-storage-class ： Glacier`
	
	`x-AMZ-restore ： ongoing-request="false" ， expiry-date="Sat" ， 2018 年 7 月 23 日 00 ： 00 ： 00 GMT"`
	
	`expiry-date` 指示何时将云存储池中的对象返回到不可检索的状态。

云存储池中的多部分或分段对象

如果您上传的是多部分对象或 StorageGRID 将一个大型对象拆分为多个区块，则 StorageGRID 会通过取样该对象的部分或区块来确定该对象是否在云存储池中可用。在某些情况下，如果对象的某些部分已过渡到不可检索的状态或对象的某些部分尚未还原，则 HEAD 对象请求可能会错误地返回 `x-AMZ-restore ： ongoing-request="false"` 。

版本控制

如果未指定 `veversionId` Subresource ，则此操作将提取受版本控制的存储分段中的对象的最新版本。如果对象的当前版本为删除标记，则返回 "`not found` " 状态，并将 `x-AMZ-delete-marker` response 标头设置为 `true` 。

相关信息

使用服务器端加密

使用 ILM 管理对象

后对象还原

在审核日志中跟踪 S3 操作

后对象还原

您可以使用 S3 后对象还原请求还原存储在云存储池中的对象。

支持的请求类型

StorageGRID 仅支持后对象还原请求来还原对象。它不支持 `Select` 类型的还原。选择 Requests return `XNotImplement`已 执行 。

版本控制

或者，指定 `veversionId` 以还原受版本控制的存储分段中特定版本的对象。如果未指定 `veversionId` ，则会还原对象的最新版本

对云存储池对象执行后对象还原的行为

如果某个对象存储在云存储池中（请参见有关通过信息生命周期管理管理来管理对象的说明），则根据对象的状态，后对象还原请求具有以下行为。有关详细信息，请参见 "`head Object` " 。

> 如果某个对象存储在云存储池中，并且该对象的一个或多个副本也位于网格中，则无需发出后对象还原请求来还原该对象。相反，可以使用 GET 对象请求直接检索本地副本。

对象的状态	**POST** 对象还原的行为
对象已载入 StorageGRID ，但尚未通过 ILM 进行评估，或者对象不在云存储池中	`403 For`禁用， `InvalidObjectState`
云存储池中的对象，但尚未过渡到无法检索的状态	`200` 正常 不进行任何更改。 • 注 * ：在将对象过渡到不可检索状态之前，您不能更改其 到期日期 。
对象已过渡到无法检索的状态	`202` 已接受 在请求正文中指定的天数内将对象的可检索副本还原到云存储池。在此期间结束时，对象将返回到无法检索的状态。 或者，也可以使用 `Tier` Request 元素来确定完成还原作业所需的时间（`Expedited` ， `Standard` 或 `Bulk` ）。如果未指定 `Tier` ，则会使用 `Standard` Tier 。 • 注意 * ：如果对象已过渡到 S3 Glacier 深度归档或云存储池使用 Azure Blob Storage ，则无法使用 `Expedited` 层还原它。返回以下错误 `403 For`禁用， `InvalidTier` ： 此存储类不支持检索选项 。
正在从不可检索状态还原的对象	`409 conflict` ，`RestoreAlreadyInProProgress`
对象已完全还原到云存储池	`200` 正常 • 注： * 如果对象已还原到可检索状态，您可以通过重新发出 POST 对象还原请求并为 `Days` 提供新值来更改其 `expiry-date` 。还原日期将相对于请求时间进行更新。

相关信息

使用 ILM 管理对象

[HEAD 对象]

[在审核日志中跟踪 S3 操作]

PUT 对象

您可以使用 S3 PUT 对象请求将对象添加到存储分段中。

解决冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

对象大小

单个 PUT 对象操作的最大 _recommended_size 为 5 GiB （ 5 ， 368 ， 709 ， 120 字节）。如果对象大于 5 GiB ，请改用多部分上传。

> 在 StorageGRID 11.6 中，单个 PUT 对象操作的最大 _supported _ 大小为 5 TiB （ 5 ， 497 ， 554 ， 138 ， 880 字节）。但是，如果您尝试上传超过 5 GiB 的对象，则会触发 * S3 PUT Object Size Too large* 警报。

用户元数据大小

Amazon S3 将每个 PUT 请求标头中用户定义的元数据的大小限制为 2 KB 。StorageGRID 将用户元数据限制为 24 KiB 。用户定义的元数据的大小是通过采用 UTF-8 编码的每个键和值的字节数之和来衡量的。

用户元数据中的 **UTF-8** 字符

如果某个请求在用户定义的元数据的密钥名称或值中包含（未转义） UTF-8 值，则会未定义 StorageGRID 行为。

StorageGRID 不会解析或解释用户定义的元数据的密钥名称或值中包含的转义 UTF-8 字符。转义的 UTF-8 字符被视为 ASCII 字符：

- 如果用户定义的元数据包含转义的 UTF-8 字符，则 PUT ， PUT 对象副本， GET 和 HEAD 请求将成功。
- 如果对密钥名称或值的解释值包含不可打印的字符，则 StorageGRID 不会返回 `x-AMZ-MISSING-meta` 标头。

对象标记限制

您可以在上传新对象时为其添加标记，也可以将其添加到现有对象中。StorageGRID 和 Amazon S3 对每个对象最多支持 10 个标记。与对象关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可以是 128 个 Unicode 字符，而标记值的长度最多可以是 256 个 Unicode 字符。密钥和值区分大小写。

对象所有权

在 StorageGRID 中，所有对象均归存储分段所有者帐户所有，包括由非所有者帐户或匿名用户创建的对象。

支持的请求标头

支持以下请求标头：

- 缓存控制
- 内容处置
- 内容编码

  如果为 内容编码StorageGRID 指定 `AWS-chunked` ，则不会验证以下项：

  - StorageGRID 不会根据区块数据验证 `chunk-signature` 。
  - StorageGRID 不会验证为对象提供的 `x-AMZ-解码  内容长度` 值。
- 内容语言
- 内容长度
- 内容 `-MD5`
- 内容类型
- 到期
- 传输编码

  如果同时使用 `AWS-chunked` 有效负载签名，则支持分块传输编码。

- `x-AMZ-meta-` ，后跟一个名称 - 值对，其中包含用户定义的元数据。

  为用户定义的元数据指定名称 - 值对时，请使用以下通用格式：

  ```
  x-amz-meta-name: value
  ```

  如果要使用 * 用户定义的创建时间 * 选项作为 ILM 规则的参考时间，则必须使用 `creation-time` 作为创建对象时记录的元数据的名称。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  自 1970 年 1 月 1 日以来， `creation-time` 的值将以秒为单位进行评估。

  > ILM 规则不能同时使用 * 用户定义的创建时间 * 作为参考时间，也不能使用平衡或严格选项来执行载入行为。创建 ILM 规则时返回错误。

- `X-AMZ-Tagging`
- S3 对象锁定请求标头

  - `x-AMZ-object-lock-mode`
  - `x-AMZ-object-lock-retain-until date`

- x-AMZ-object-lock-legal-hold

  如果在不使用这些标题的情况下发出请求，则存储分段默认保留设置用于计算对象版本 retain-until 日期。

使用 S3 对象锁定

- SSA 请求标头：
  - x-AMZ-server-side encryption
  - x-AMZ-server-side encrypt-customer-key-md5
  - x-AMZ-server-side encrypt-customer-key
  - x-AMZ-server-side encrypt-customer-encryption

    请参见 [服务器端加密的请求标头]

请求标头不受支持

不支持以下请求标头：

- 不支持 x-AMZ-ACL 请求标头。
- 不支持 x-AMZ-website-redirect-location 请求标头并返回 XNotImplemented 。

存储类选项

支持 x-AMZ-storage-class 请求标头。为 x-AMZ-storage-class 提交的值会影响 StorageGRID 在载入期间保护对象数据的方式，而不会影响 StorageGRID 系统中存储对象的永久性副本的数量（由 ILM 决定）。

如果与已载入对象匹配的 ILM 规则对载入行为使用 strict 选项，则 x-AMZ-storage-class 标头将不起作用。

以下值可用于 x-AMZ-storage-class ：

- standard （默认）
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则在载入对象后，系统会立即创建该对象的第二个副本并将其分发到其他存储节点（双提交）。评估 ILM 后， StorageGRID 将确定这些初始临时副本是否满足规则中的放置说明。否则，可能需要在不同位置创建新的对象副本，并且可能需要删除初始中间副本。
  - * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，而 StorageGRID 无法立即创建规则中指定的所有副本，则 StorageGRID 会在不同的存储节点上创建两个临时副本。

    如果 StorageGRID 可以立即创建 ILM 规则（同步放置）中指定的所有对象副本，则 x-AMZ-storage-class 标头将不起作用。
- re介绍冗余
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则 StorageGRID 会在载入对象时创建一个临时副本（单个提交）。
  - * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，则只有在系统无法立即创建规则中指定的所有副本时，

StorageGRID 才会创建一个临时副本。如果 StorageGRID 可以执行同步放置，则此标头不起作用。re 与对象匹配的 ILM 规则创建一个复制副本时，最好使用 " 已复制 " 选项。在这种情况下，使用 recreated_redundancy 可以避免在每次载入操作中不必要地创建和删除额外的对象副本。

在其他情况下，不建议使用 reincluster_redundancy 选项。re介绍冗余 增加了载入期间对象数据丢失的风险。例如，如果最初将单个副本存储在发生故障的存储节点上，而此存储节点未能进行 ILM 评估，则可能会丢失数据。

- 注意 * ：在任意时间段内只复制一个副本会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

指定 recreated_redundancy 仅会影响首次载入对象时创建的副本数。它不会影响在活动 ILM 策略评估对象时创建的对象副本数，也不会导致数据在 StorageGRID 系统中以较低的冗余级别存储。

- 注 * ：如果要在启用了 S3 对象锁定的情况下将对象载入存储分段，则会忽略 re区冗余 选项。如果要将对象载入旧的合规存储分段，则 re区冗余 选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

服务器端加密的请求标头

您可以使用以下请求标头通过服务器端加密对对象进行加密。SSE 和 SSI-C 选项是互斥的。

- * SSE* ：如果要使用 StorageGRID 管理的唯一密钥对对象进行加密，请使用以下标题。
  - x-AMZ-server-side encryption
- * SSI-C* ：如果要使用您提供和管理的唯一密钥对对象进行加密，请使用所有这三个标头。
  - x-AMZ-server-side encrypt-customer-all ：指定 AES256 。
  - x-AMZ-server-side encrypt-customer-key ：为新对象指定加密密钥。
  - x-AMZ-server-side encrypt-customer-key-md5 ：指定新对象加密密钥的 MD5 摘要。
- 注意： * 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`
- 注： * 如果对象使用 SSE 或 SSI-C 进行加密，则会忽略任何分段级别或网格级别的加密设置。

版本控制

如果为存储分段启用了版本控制，则会自动为所存储的对象版本生成唯一的 veversionId 。此 veversionId 也会在响应中使用 x-AMZ-version-id 响应标头返回。

如果版本控制已暂停，则存储的对象版本为 null veversionId ，如果已存在空版本，则该版本将被覆盖。

相关信息

使用 ILM 管理对象

对存储分段执行的操作

在审核日志中跟踪 S3 操作

使用服务器端加密

PUT 对象—复制

您可以使用 S3 PUT 对象 - 复制请求为已存储在 S3 中的对象创建副本。PUT 对象 - 复制操作与执行 GET ，然后执行 PUT 操作相同。

解决冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

对象大小

单个 PUT 对象操作的最大 _recommended_size 为 5 GiB （ 5 ， 368 ， 709 ， 120 字节）。如果对象大于 5 GiB ，请改用多部分上传。

> 在 StorageGRID 11.6 中，单个 PUT 对象操作的最大 _supported _ 大小为 5 TiB （ 5 ， 497 ， 554 ， 138 ， 880 字节）。但是，如果您尝试上传超过 5 GiB 的对象，则会触发 * S3 PUT Object Size Too large* 警报。

用户元数据中的 **UTF-8** 字符

如果某个请求在用户定义的元数据的密钥名称或值中包含（未转义） UTF-8 值，则会未定义 StorageGRID 行为。

StorageGRID 不会解析或解释用户定义的元数据的密钥名称或值中包含的转义 UTF-8 字符。转义的 UTF-8 字符被视为 ASCII 字符：

- 如果用户定义的元数据包含转义的 UTF-8 字符，则请求将成功。
- 如果对密钥名称或值的解释值包含不可打印的字符，则 StorageGRID 不会返回 `x-AMZ-MISSING-meta` 标头。

支持的请求标头

支持以下请求标头：

- 内容类型
- `x-AMZ-copy-source`
- `x-AMZ-copy-source-if-match`
- `x-AMZ-copy-source-if-none-match`
- `x-AMZ-copy-source-if-modified - since`
- `x-AMZ-copy-source-if-modified-since`
- `x-AMZ-meta-` ，后跟一个名称 - 值对，其中包含用户定义的元数据
- `x-AMZ-metadata-directive` ：默认值为 `copy` ，可用于复制对象和关联元数据。

  您可以指定 `replace` 以在复制对象时覆盖现有元数据，或更新对象元数据。

- `x-AMZ-storage-class`
- `x-AMZ-tagging-directive` ：默认值为 `copy` ，可用于复制对象和所有标记。

  您可以指定 `replace` 以在复制对象时覆盖现有标记，或更新标记。

- S3 对象锁定请求标头：
  - `x-AMZ-object-lock-mode`
  - `x-AMZ-object-lock-retain-until date`
  - `x-AMZ-object-lock-legal-hold`

    如果在不使用这些标题的情况下发出请求，则存储分段默认保留设置用于计算对象版本 retain-until 日期。

  使用 S3 对象锁定

- SSA 请求标头：
  - `x-AMZ-copy-source -server-side -customer-zr encryption`
  - `x-AMZ-copy-source -server-side encrypt-customer-key`
  - `x-AMZ-copy-source -server-side encryption - customer-key-MD5`
  - `x-AMZ-server-side encryption`
  - `x-AMZ-server-side encrypt-customer-key-md5`
  - `x-AMZ-server-side encrypt-customer-key`
  - `x-AMZ-server-side encrypt-customer-encryption`

    请参见 [服务器端加密的请求标头]

请求标头不受支持

不支持以下请求标头：

- 缓存控制
- 内容处置
- 内容编码
- 内容语言
- 到期
- `x-AMZ-website-redirect-location`

存储类选项

支持 `x-AMZ-storage-class` 请求标头，如果匹配的 ILM 规则指定了双重提交或平衡的载入行为，则会影响 StorageGRID 创建的对象副本数。

- s标准

  （默认）指定在 ILM 规则使用双提交选项或 balanced-option 回退到创建中间副本时执行双提交载入操作。

- re介绍冗余

  指定在 ILM 规则使用双提交选项或 balanced-option 回退为创建中间副本时执行单提交载入操作。

  > 如果要在启用了 S3 对象锁定的情况下将对象载入存储分段，则会忽略 re区冗余 选项。如果要将对象载入旧的合规存储分段，则 re区冗余 选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

在 **PUT** 对象中使用 **x-AMZ-copy-source —**复制

如果在 x-AMZ-copy-source 标头中指定的源分段和密钥与目标分段和密钥不同，则会向目标写入源对象数据的副本。

如果源和目标匹配，并且将 x-AMZ-metada-directive 标头指定为 replace ，则对象的元数据将使用请求中提供的元数据值进行更新。在这种情况下， StorageGRID 不会重新载入对象。这有两个重要后果：

- 您不能使用 PUT 对象 - 复制对现有对象进行原位加密，也不能更改现有对象的加密。如果您提供了 x-AMZ-server-side encryption 标头或 x-AMZ-server-side encrypt-customer-encryption 标头，则 StorageGRID 将拒绝此请求并返回 XNotImplemented 。
- 不会使用匹配 ILM 规则中指定的 " 载入行为 " 选项。通过正常后台 ILM 进程重新评估 ILM 时，更新触发的任何对象放置更改都会进行。

  这意味着，如果 ILM 规则对载入行为使用严格选项，则在无法放置所需对象时（例如，由于新需要的位置不可用），不会执行任何操作。更新后的对象会保留其当前位置，直到可以进行所需的位置为止。

服务器端加密的请求标头

如果使用服务器端加密，则您提供的请求标头取决于源对象是否已加密以及是否计划对目标对象加密。

- 如果源对象使用客户提供的密钥（ SSI-C ）进行加密，则必须在 PUT Object - Copy 请求中包含以下三个标头，以便可以解密并复制此对象：
  - x-AMZ-copy-source server-side -customer-all 指定 AES256 encryption 。
  - x-AMZ-copy-source -server-side encrypt-customer-key 指定您在创建源对象时提供的加密密钥。
  - x-AMZ-copy-source -server-side encryption - customer-key-MD5 ： 指定您在创建源对象时提供的 MD5 摘要。
- 如果要使用您提供和管理的唯一密钥对目标对象（副本）进行加密，请包含以下三个标题：
  - x-AMZ-server-side encrypt-customer-all ： 指定 AES256 。
  - x-AMZ-server-side encrypt-customer-key ： 为目标对象指定新的加密密钥。
  - x-AMZ-server-side encrypt-customer-key-md5 ： 指定新加密密钥的 MD5 摘要。
- 注意： * 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`

- 如果要使用由 StorageGRID （ SSE ）管理的唯一密钥对目标对象（副本）进行加密，请将此标头包括在 PUT 对象 - 复制请求中：
  - `x-AMZ-server-side encryption`
- 注： * 无法更新对象的 s服务器端加密 值。相反，请使用 `sx-AMZ-metada-directive： replace` 使用新的 服务器端加密 值创建副本。

版本控制

如果源存储分段已版本控制，则可以使用 `x-AMZ-copy-source` 标头复制对象的最新版本。要复制对象的特定版本，必须使用 `veversionId` Subresource 明确指定要复制的版本。如果目标存储分段已版本控制，则生成的版本将在 `x-AMZ-version-id` 响应标题中返回。如果目标分段的版本控制已暂停，则 `x-AMZ-version-id` 将返回 "`null` " 值。

相关信息

使用 ILM 管理对象

使用服务器端加密

在审核日志中跟踪 S3 操作

PUT 对象

SelectObjectContent

您可以使用 S3 SelectObjectContent 请求根据简单的 SQL 语句筛选 S3 对象的内容。

有关详细信息，请参见 "适用于 SelectObjectContent 的 AWS 文档"。

您需要的内容

- 此租户帐户具有 S3 Select 权限。
- 您对要查询的对象具有 `s 3 ： GetObject` 权限。
- 要查询的对象为 CSV 格式，或者为包含 CSV 格式文件的 GZIP 或 bzip 2 压缩文件。
- SQL 表达式的最大长度为 256 KB 。
- 输入或结果中的任何记录的最大长度为 1 MiB 。

请求语法示例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL 查询示例

此查询可从美国人口统计数据中获取状态名称， 2010 年人口， 2015 年估计人口以及变更百分比。文件中不属于状态的记录将被忽略。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

要查询的文件的前几行 `SUB-EST2020_all.csv` 如下所示：

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLI 使用示例

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

输出文件的前几行 `changes.csv` 如下所示：

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

多部分上传操作

本节介绍 StorageGRID 如何支持多部件上传操作。

以下条件和注释适用于所有多部件上传操作：

- 一个存储分段的并发多部件上传数不应超过 1 ， 000 次，因为该存储分段的 List Multipart uploads 查询结果可能会返回不完整的结果。
- StorageGRID 对多部件部件强制实施 AWS 大小限制。S3 客户端必须遵循以下准则：
  - 多部分上传中的每个部分必须介于 5 MiB （ 5 ， 242 ， 880 字节）和 5 GiB （ 5 ， 368 ， 709 ， 120 字节）之间。
  - 最后一部分可以小于 5 MiB （ 5 ， 242 ， 880 字节）。
  - 通常，部件大小应尽可能大。例如，对于 100 GiB 对象，请使用部件大小 5 GiB 。由于每个部件都被视为唯一对象，因此使用较大的部件大小可降低 StorageGRID 元数据开销。
  - 对于小于 5 GiB 的对象，请考虑使用非多部分上传。
- 如果 ILM 规则使用严格或平衡的载入行为，则会在载入多部分对象时对其每个部分进行评估，并在多部分上传完成后对该对象作为一个整体进行评估。您应了解这会对对象和部件放置产生何种影响：
  - 如果在 S3 多部分上传过程中 ILM 发生更改，则在多部分上传完成后，对象的某些部分可能无法满足当前的 ILM 要求。任何放置不正确的部件都会排队等待 ILM 重新评估，并稍后移至正确的位置。
  - 在评估某个部件的 ILM 时， StorageGRID 会筛选该部件的大小，而不是对象的大小。这意味着，对象的某些部分可以存储在不满足整个对象的 ILM 要求的位置。例如，如果规则指定所有 10 GB 或更大的对象都存储在 DC1 中，而所有较小的对象存储在 DC2 中，则在载入时， 10 部分多部分上传的每个 1 GB 部分都存储在 DC2 中。在对对象整体进行 ILM 评估时，对象的所有部分都将移至 DC1 。
- 所有多部分上传操作均支持 StorageGRID 一致性控制。
- 您可以根据需要对多部分上传使用服务器端加密。要使用 SSE （服务器端加密与 StorageGRID 管理的密钥），请仅在启动多部件上传请求中包含 `x-AMZ-server-side encryption` request 标头。要对客户提供的密钥使用 SSI-C （服务器端加密），您可以在 " 启动多部件上传请求 " 和后续的每个 " 上传部件请求 " 中指定相同的三个加密密钥请求标头。

操作	实施
列出多部件上传	请参见 列出多部件上传
启动多部件上传	请参见 启动多部件上传
上传部件	请参见 上传部件

操作	实施
上传部件—复制	请参见 上传部件—复制
完成多部件上传	请参见 完成多部件上传
中止多部分上传	在所有 Amazon S3 REST API 行为下实施
列出部件	在所有 Amazon S3 REST API 行为下实施

相关信息

- 一致性控制
- 使用服务器端加密

列出多部件上传

" 列出多部件上传 " 操作会列出某个存储分段正在进行的多部件上传。

支持以下请求参数：

- 编码类型
- `m`轴向上传
- 键标记
- 前缀
- `upload-id-marker`

不支持 `delimiter` request 参数。

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。执行完 " 多部分上传 " 操作后，即创建对象（并在适用情况下进行版本控制）。

启动多部件上传

" 启动多部件上传 " 操作将为对象启动多部件上传，并返回上传 ID 。

支持 `x-AMZ-storage-class` 请求标头。为 `x-AMZ-storage-class` 提交的值会影响 StorageGRID 在载入期间保护对象数据的方式，而不会影响 StorageGRID 系统中存储对象的永久性副本的数量（由 ILM 决定）。

如果与已载入对象匹配的 ILM 规则对载入行为使用 strict 选项，则 `x-AMZ-storage-class` 标头将不起作用。

以下值可用于 `x-AMZ-storage-class` ：

- `standard` （默认）
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则在载入对象后，系统会立即创建该对象的

第二个副本并将其分发到其他存储节点（双提交）。评估 ILM 后， StorageGRID 将确定这些初始临时副本是否满足规则中的放置说明。否则，可能需要在不同位置创建新的对象副本，并且可能需要删除初始中间副本。

- * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，而 StorageGRID 无法立即创建规则中指定的所有副本，则 StorageGRID 会在不同的存储节点上创建两个临时副本。

  如果 StorageGRID 可以立即创建 ILM 规则（同步放置）中指定的所有对象副本，则 `x-AMZ-storage-class` 标头将不起作用。

- `re`介绍冗余

  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则 StorageGRID 会在载入对象时创建一个临时副本（单个提交）。
  - * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，则只有在系统无法立即创建规则中指定的所有副本时，StorageGRID 才会创建一个临时副本。如果 StorageGRID 可以执行同步放置，则此标头不起作用。`re` 与对象匹配的 ILM 规则创建一个复制副本时，最好使用 " 已复制 " 选项。在这种情况下，使用 `recreated_redundancy` 可以避免在每次载入操作中不必要地创建和删除额外的对象副本。

  在其他情况下，不建议使用 `reincluster_redundancy` 选项。`re`介绍冗余 增加了载入期间对象数据丢失的风险。例如，如果最初将单个副本存储在发生故障的存储节点上，而此存储节点未能进行 ILM 评估，则可能会丢失数据。

- 注意 * ： 在任意时间段内只复制一个副本会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

指定 `recreated_redundancy` 仅会影响首次载入对象时创建的副本数。它不会影响在活动 ILM 策略评估对象时创建的对象副本数，也不会导致数据在 StorageGRID 系统中以较低的冗余级别存储。

- 注 * ： 如果要在启用了 S3 对象锁定的情况下将对象载入存储分段，则会忽略 `re`区冗余 选项。如果要将对象载入旧的合规存储分段，则 `re`区冗余 选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

支持以下请求标头：

- 内容类型
- `x-AMZ-meta-` ，后跟一个名称 - 值对，其中包含用户定义的元数据

  为用户定义的元数据指定名称 - 值对时，请使用以下通用格式：

  ```
  x-amz-meta-_name_: `value`
  ```

  如果要使用 * 用户定义的创建时间 * 选项作为 ILM 规则的参考时间，则必须使用 `creation-time` 作为创建对象时记录的元数据的名称。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  自 1970 年 1 月 1 日以来， `creation-time` 的值将以秒为单位进行评估。

如果要将对象添加到启用了旧合规性的存储分段，则不允许将 `create-time` 添加为用户定义的元数据。此时将返回错误。

- S3 对象锁定请求标头：
  - `x-AMZ-object-lock-mode`
  - `x-AMZ-object-lock-retain-until date`
  - `x-AMZ-object-lock-legal-hold`

  如果在不使用这些标题的情况下发出请求，则存储分段默认保留设置用于计算对象版本 retain-until 日期。

使用 S3 对象锁定

- SSA 请求标头：
  - `x-AMZ-server-side encryption`
  - `x-AMZ-server-side encrypt-customer-key-md5`
  - `x-AMZ-server-side encrypt-customer-key`
  - `x-AMZ-server-side encrypt-customer-encryption`

  [服务器端加密的请求标头]

有关 StorageGRID 如何处理 UTF-8 字符的信息，请参见 PUT 对象的文档。

服务器端加密的请求标头

您可以使用以下请求标头通过服务器端加密对多部分对象进行加密。SSE 和 SSI-C 选项是互斥的。

- * SSE* ： 如果要使用 StorageGRID 管理的唯一密钥对对象进行加密，请在 " 启动多部分上传请求 " 中使用以下标题。请勿在任何上传部件请求中指定此标题。
  - `x-AMZ-server-side encryption`
- * SSI-C* ： 如果要使用您提供和管理的唯一密钥对对象进行加密，请在 " 启动多部件上传请求 " （以及后续的每个 " 上传部件请求 " ）中使用所有这三个标头。
  - `x-AMZ-server-side encrypt-customer-all` ： 指定 `AES256` 。
  - `x-AMZ-server-side encrypt-customer-key` ： 为新对象指定加密密钥。
  - `x-AMZ-server-side encrypt-customer-key-md5` ： 指定新对象加密密钥的 MD5 摘要。
- 注意： * 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`

请求标头不受支持

不支持以下请求标头，并返回 `XNotImplemented"`

- `x-AMZ-website-redirect-location`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。在执行完整的多部件上传操作时，系统会创建对象（如果适用，还会进行版本控制）。

相关信息

使用 ILM 管理对象

使用服务器端加密

PUT 对象

上传部件

" 上传部件 " 操作会通过多部件上传方式为对象上传部件。

支持的请求标头

支持以下请求标头：

- 内容长度
- 内容 `-MD5`

服务器端加密的请求标头

如果您为启动多部件上传请求指定了 SSI-C 加密，则还必须在每个上传部件请求中包含以下请求标头：

- `x-AMZ-server-side encrypt-customer-all` ：指定 `AES256` 。
- `x-AMZ-server-side encrypt-customer-key` ：指定您在启动多部件上传请求中提供的相同加密密钥。
- `x-AMZ-server-side encrypt-customer-key-MD5` ：指定您在启动多部分上传请求中提供的相同 MD5 摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。在执行完整的多部件上传操作时，系统会创建对象（如果适用，还会进行版本控制）。

相关信息

使用服务器端加密

上传部件—复制

上传部件 - 复制操作通过将现有对象中的数据复制为数据源来上传对象的一部分。

上传部件 - 复制操作可在所有 Amazon S3 REST API 行为下实施。

此请求会读取和写入 StorageGRID 系统中 `x-AMZ-copy-source-range` 中指定的对象数据。

支持以下请求标头：

- `x-AMZ-copy-source-if-match`
- `x-AMZ-copy-source-if-none-match`
- `x-AMZ-copy-source-if-modified - since`
- `x-AMZ-copy-source-if-modified-since`

服务器端加密的请求标头

如果您为启动多部件上传请求指定了 SSI-C 加密，则还必须在每个上传部件 - 复制请求中包含以下请求标头：

- `x-AMZ-server-side encrypt-customer-all`：指定 `AES256` 。
- `x-AMZ-server-side encrypt-customer-key`：指定您在启动多部件上传请求中提供的相同加密密钥。
- `x-AMZ-server-side encrypt-customer-key-MD5`：指定您在启动多部分上传请求中提供的相同 MD5 摘要。

如果源对象使用客户提供的密钥（ SSI-C ）进行加密，则必须在上传部件 - 复制请求中包含以下三个标题，以便可以解密并复制此对象：

- `x-AMZ-copy-source server-side -customer-all`：指定 `AES256 encryption` 。
- `x-AMZ-copy-source -server-side encryption -customer-key`：指定您在创建源对象时提供的加密密钥。
- `x-AMZ-copy-source -server-side encryption - customer-key-MD5`：指定您在创建源对象时提供的 MD5 摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "`使用服务器端加密 " 中的注意事项。`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。在执行完整的多部件上传操作时，系统会创建对象（如果适用，还会进行版本控制）。

完成多部件上传

完整的多部件上传操作通过整合先前上传的部件来完成对象的多部分上传。

解决冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

请求标题

支持 `x-AMZ-storage-class` 请求标头，如果匹配的 ILM 规则指定了双重提交或平衡的载入行为，则会影响 StorageGRID 创建的对象副本数。

- `s`标准

  （默认）指定在 ILM 规则使用双提交选项或 balanced-option 回退到创建中间副本时执行双提交载入操作。

- `re`介绍冗余

  指定在 ILM 规则使用双提交选项或 balanced-option 回退为创建中间副本时执行单提交载入操作。

> 如果要在启用了 S3 对象锁定的情况下将对象载入存储分段，则会忽略 `re`区冗余 选项。如果要将对象载入旧的合规存储分段，则 `re`区冗余 选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

> 如果多部分上传未在 15 天内完成，则此操作将标记为非活动，并从系统中删除所有关联数据。

> 返回的 `ETag` 值不是数据的 MD5 之和，而是遵循 Amazon S3 API 实施的多部分对象的 `ETag` 值。

版本控制

此操作将完成多部分上传。如果为存储分段启用了版本控制，则在完成多部分上传后会创建对象版本。

如果为存储分段启用了版本控制，则会自动为所存储的对象版本生成唯一的 `veversionId` 。此 `veversionId` 也会在响应中使用 `x-AMZ-version-id` 响应标头返回。

如果版本控制已暂停，则存储的对象版本为 null `veversionId` ，如果已存在空版本，则该版本将被覆盖。

> 如果为存储分段启用了版本控制，则完成多部分上传始终会创建新版本，即使在同一对象密钥上同时完成多部分上传也是如此。如果某个存储分段未启用版本控制，则可以先启动多部分上传，然后再对同一对象密钥启动并完成另一个多部分上传。在非版本控制的存储分段上，最后完成的多部分上传将优先。

复制，通知或元数据通知失败

如果为平台服务配置了进行多部分上传的存储分段，则即使关联的复制或通知操作失败，多部分上传也会成功。

如果发生这种情况，则会在网格管理器中针对总事件（ SMT ）发出警报。最后一个事件消息显示 "`failed to publish notifications for bucket-nameobject key` " for the last object whose notification failed.（要查看此消息，请选择 * 节点 * > * 存储节点 _* > * 事件 * 。在表顶部查看上次事件。） 事件消息也会在 `/var/local/log/byncast-err.log` 中列出。

租户可以通过更新对象的元数据或标记来触发失败的复制或通知。租户可以重新提交现有值，以避免进行不必要的更改。

相关信息

使用 ILM 管理对象

StorageGRID 系统支持所有适用的标准 S3 REST API 错误响应。此外， StorageGRID 实施还添加了多个自定义响应。

支持的 **S3 API** 错误代码

Name	**HTTP** 状态
ACCESSDENIED	403 已禁用
BadDigest	400 个错误请求
BucketAlreadyExists	409 冲突
BucketNotEmpagty	409 冲突
实体不完整	400 个错误请求
内部错误	500 内部服务器错误
InvalidAccessKeyId	403 已禁用
InvalidArgument	400 个错误请求
InvalidBucketName	400 个错误请求
InvalidBucketState	409 冲突
InvalidDigest	400 个错误请求
InvalidEncryptionAlgorithmError	400 个错误请求
InvalidPart	400 个错误请求
InvalidPartOrder	400 个错误请求
InvalidRange	416 无法满足请求的范围
InvalidRequest	400 个错误请求
InvalidStorageClass	400 个错误请求
InvalidTag	400 个错误请求

Name	HTTP 状态
InvalidURI	400 个错误请求
KeyTooLong	400 个错误请求
MalformedXML	400 个错误请求
MetadataTooLarge	400 个错误请求
方法未使用	不允许使用 405 方法
MissingContent长度	411 需要长度
MissingRequestBodyError	400 个错误请求
MissingSecurityHeader	400 个错误请求
NoSuchBucket	未找到 404
NoSuchKey	未找到 404
NoSuchUpload	未找到 404
未实施	501 未实施
NoSuchBucketPolicy	未找到 404
ObjectLockConfigurationNotFoundError	未找到 404
预条件已启用	412- 前提条件失败
已请求超时	403 已禁用
服务不可用	503 服务不可用
SignatureDoesNotMatch	403 已禁用
TooMany桶	400 个错误请求
用户密钥已规范	400 个错误请求

Name	Description	HTTP 状态
XBucketLifeycleNotAllowed	旧版合规存储分段不支持存储分段生命周期配置	400 个错误请求
XBucketPolicyParseException	无法解析收到的存储分段策略 JSON 。	400 个错误请求
XComplianceConflict	操作因原有合规性设置而被拒绝。	403 已禁用
XComplianceReducedRedundancyFor禁用	原有的合规存储分段不允许减少冗余	400 个错误请求
XMaxBucketPolicyLengthExceeded	您的策略超出了允许的最大存储分段策略长度。	400 个错误请求
XMissingInternalRequestHeader	缺少内部请求的标题。	400 个错误请求
XNoSuchBucketCompliance	指定的存储分段未启用原有合规性。	未找到 404
XNotAcceptable	此请求包含一个或多个无法满足的接受标头。	406 不可接受
未实施	您提供的请求意味着未实施的功能。	501 未实施

StorageGRID S3 REST API 操作

S3 REST API 中添加了特定于 StorageGRID 系统的操作。

- 获取存储分段一致性请求

  使用获取存储分段一致性请求，您可以确定应用于特定存储分段的一致性级别。

- PUT 存储分段一致性请求

  通过 PUT 分段一致性请求，您可以指定要应用于对分段执行的操作的一致性级别。

- 获取分段上次访问时间请求

  通过获取分段上次访问时间请求，您可以确定是为单个分段启用还是禁用了上次访问时间更新。

- PUT 分段上次访问时间请求

  通过 PUT 分段上次访问时间请求，您可以为各个分段启用或禁用上次访问时间更新。禁用上次访问时间更新可提高性能，它是使用 10.3.0 或更高版本创建的所有存储分段的默认设置。

- 删除存储分段元数据通知配置请求

  通过删除存储分段元数据通知配置请求，您可以通过删除配置 XML 来禁用各个存储分段的搜索集成服务。

- 获取存储分段元数据通知配置请求

  使用获取分段元数据通知配置请求，您可以检索用于为各个分段配置搜索集成的配置 XML 。

- PUT 存储分段元数据通知配置请求

  通过 PUT Bucket 元数据通知配置请求，您可以为各个存储分段启用搜索集成服务。您在请求正文中提供的元数据通知配置 XML 用于指定将其元数据发送到目标搜索索引的对象。

- 获取存储使用情况请求

  " 获取存储使用量 " 请求会告知您帐户正在使用的存储总量以及与帐户关联的每个存储分段的存储总量。

- 已弃用旧合规性的存储分段请求

  您可能需要使用 StorageGRID S3 REST API 来管理使用原有合规性功能创建的分段。

获取存储分段一致性请求

使用获取存储分段一致性请求，您可以确定应用于特定存储分段的一致性级别。

默认一致性控制设置为保证新创建的对象的写入后读。

要完成此操作，您拥有 S3： GetBucketConsistency 权限或帐户 root 。

请求示例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

响应

在响应 XML 中，`< 一致性 >` 将返回以下值之一：

一致性控制	Description
全部	所有节点都会立即接收数据，否则请求将失败。
强大的全局功能	保证所有站点中所有客户端请求的写入后读一致性。
强大的站点	保证站点内所有客户端请求的写入后读一致性。

一致性控制	Description
读后写	（默认）为新对象提供写入后读一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。最符合 Amazon S3 一致性保证。 • 注意： * 如果应用程序对不存在的对象使用 head 请求，则在一个或多个存储节点不可用时，可能会收到大量 500 个内部服务器错误。要防止出现这些错误，请将一致性控制设置为 "`Available` "，除非您需要类似于 Amazon S3 的一致性保证。
可用（机头操作的最终一致性）	与 `read-after-new-write` 一致性级别相同，但仅为机头操作提供最终一致性。如果存储节点不可用，则为机头操作提供的可用性比 " `read-after-new-write` " 更高。与 Amazon S3 一致性保证不同，仅适用于机头操作。

响应示例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

相关信息

一致性控制

PUT 存储分段一致性请求

通过 PUT 分段一致性请求，您可以指定要应用于对分段执行的操作的一致性级别。

默认一致性控制设置为保证新创建的对象的写入后读。

要完成此操作，您拥有 S3： PutBucketConsistency 权限或帐户 root 。

请求

`x-ntap-sg-consistency` 参数必须包含以下值之一：

一致性控制	Description
全部	所有节点都会立即接收数据，否则请求将失败。
强大的全局功能	保证所有站点中所有客户端请求的写入后读一致性。
强大的站点	保证站点内所有客户端请求的写入后读一致性。
读后写	（默认）为新对象提供写入后读一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。最符合 Amazon S3 一致性保证。 • 注意： * 如果应用程序对不存在的对象使用 head 请求，则在一个或多个存储节点不可用时，可能会收到大量 500 个内部服务器错误。要防止出现这些错误，请将一致性控制设置为 "`Available` "，除非您需要类似于 Amazon S3 的一致性保证。
可用（机头操作的最终一致性）	与 `read-after-new-write` 一致性级别相同，但仅为机头操作提供最终一致性。如果存储节点不可用，则为机头操作提供的可用性比 " `read-after-new-write` " 更高。与 Amazon S3 一致性保证不同，仅适用于机头操作。

• 注： * 通常，您应使用 `read-after-new-write` 一致性控制值。如果请求无法正常工作，请尽可能更改应用程序客户端的行为。或者，配置客户端以指定每个 API 请求的一致性控制。请仅作为最后一种方法在存储分段级别设置一致性控制。

请求示例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

相关信息

一致性控制

获取分段上次访问时间请求

通过获取分段上次访问时间请求，您可以确定是为单个分段启用还是禁用了上次访问时间更新。

要完成此操作，您拥有 S3： GetBucketLastAccessTime 权限或帐户 root 。

请求示例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

响应示例

此示例显示已为存储分段启用上次访问时间更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT 分段上次访问时间请求

通过 PUT 分段上次访问时间请求，您可以为各个分段启用或禁用上次访问时间更新。禁用上次访问时间更新可提高性能，它是使用 10.3.0 或更高版本创建的所有存储分段的默认设置。

要完成此操作，您对某个存储分段拥有 S3： PutBucketLastAccessTime 权限，或者您是帐户的 root 用户。

> 从 StorageGRID 10.3 版开始，默认情况下，所有新存储分段都会禁用对上次访问时间的更新。如果您的存储分段是使用早期版本的 StorageGRID 创建的，并且您希望与新的默认行为匹配，则必须明确禁用上述每个存储分段的上次访问时间更新。您可以使用租户管理器中的 PUT 分段上次访问时间请求， * S3 > * 分段 * > * 更改上次访问设置 * 复选框或租户管理 API 启用或禁用对最后访问时间的更新。

如果禁用了某个存储分段的上次访问时间更新，则会对存储分段上的操作应用以下行为：

- GET 对象， GET 对象 ACL ， GET 对象标记和 HEAD 对象请求不会更新上次访问时间。此对象不会添加到用于信息生命周期管理（ ILM ）评估的队列中。
- PUT 对象—仅更新元数据的复制和 PUT 对象标记请求也会更新上次访问时间。对象将添加到队列中以进行 ILM 评估。
- 如果对源存储分段禁用了对最后访问时间的更新，则 PUT Object - Copy Requests 不会更新源存储分段的最后访问时间。复制的对象不会添加到源存储分段的 ILM 评估队列中。但是，对于目标， PUT 对象 - 复制请求始终更新上次访问时间。对象副本将添加到队列中以进行 ILM 评估。

- 完成多部件上传请求更新上次访问时间。已完成的对象将添加到队列中以进行 ILM 评估。

请求示例

此示例将为存储分段启用上次访问时间。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

此示例将禁用存储分段的上次访问时间。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

相关信息

使用租户帐户

删除存储分段元数据通知配置请求

通过删除存储分段元数据通知配置请求，您可以通过删除配置 XML 来禁用各个存储分段的搜索集成服务。

要完成此操作，您对某个存储分段拥有 S3： DeleteBucketMetadataNotification 权限，或者您是帐户的 root 用户。

请求示例

此示例显示了禁用存储分段的搜索集成服务。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

获取存储分段元数据通知配置请求

使用获取分段元数据通知配置请求，您可以检索用于为各个分段配置搜索集成的配置 XML 。

要完成此操作，您拥有 S3： GetBucketMetadataNotification 权限，或者帐户为 root 。

请求示例

此请求将检索名为 `bucket` 的存储分段的元数据通知配置。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

响应

响应正文包括存储分段的元数据通知配置。通过元数据通知配置，您可以确定如何配置存储分段以进行搜索集成。也就是说，您可以通过它确定哪些对象已编制索引，以及将其对象元数据发送到哪些端点。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

每个元数据通知配置都包含一个或多个规则。每个规则都指定其适用场景 的对象以及 StorageGRID 应将对象元数据发送到的目标。必须使用 StorageGRID 端点的 URN 指定目标。

Name	Description	Required
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是的。

Name	Description	Required
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是的。
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
Status	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是的。
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是的。
目标	规则目标的容器标记。 包含在 Rule 元素中。	是的。

Name	Description	Required
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN： • `es` 必须是第三个元素。 • URN 必须以 `domain-name/myindex/mytype` 形式的索引和元数据存储类型结尾。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn ： AWS ： es ： *Region* ： *account-ID* ： domain/mydomain/myindex/mytype` • `urn ： mysite ： es ： ： mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是的。

响应示例

在 ` <MetadataNotificationConfiguration>/MetadataNotificationConfiguration>` 标记之间包含的 XML 显示了如何为存储分段配置与搜索集成端点的集成。在此示例中，对象元数据将发送到名为 `current` 且类型为 `2017` 的 Elasticsearch 索引，该索引托管在名为 `records` 的 AWS 域中。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相关信息

使用租户帐户

PUT 存储分段元数据通知配置请求

通过 PUT Bucket 元数据通知配置请求，您可以为各个存储分段启用搜索集成服务。您在请求正文中提供的元数据通知配置 XML 用于指定将其元数据发送到目标搜索索引的对象。

要完成此操作，您对某个存储分段拥有 S3： PutBucketMetadataNotification 权限，或者您是帐户的 root 用户。

请求

此请求必须在请求正文中包含元数据通知配置。每个元数据通知配置都包含一个或多个规则。每个规则都指定其适用场景 的对象以及 StorageGRID 应将对象元数据发送到的目标。

可以按对象名称的前缀筛选对象。例如，您可以将前缀为 ` /images` 的对象的元数据发送到一个目标，将前缀为 ` /videos` 的对象发送到另一个目标。

前缀重叠的配置无效，在提交时会被拒绝。例如，不允许在配置中为前缀为 `test` 的对象包含一个规则，而为前缀为 `test2` 的对象包含另一个规则。

必须使用 StorageGRID 端点的 URN 指定目标。当提交元数据通知配置时，此端点必须存在，否则此请求会因 `400` **错误请求** 而失败。错误消息显示： `Unable to save the metadata notification （ search ） policy 。指定的端点 URN 不存在： URN 。`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表介绍了元数据通知配置 XML 中的元素。

Name	Description	Required
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是的。
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是的。
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
Status	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是的。

Name	Description	Required
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是的。
目标	规则目标的容器标记。 包含在 Rule 元素中。	是的。
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN： • `es` 必须是第三个元素。 • URN 必须以 `domain-name/myindex/mytype` 形式的索引和元数据存储类型结尾。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn ： AWS ： es ： Region ： account-ID ： domain/mydomain/myindex/mytype` • `urn ： mysite ： es ： ： ： mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是的。

请求示例

此示例显示了为存储分段启用搜索集成。在此示例中，所有对象的对象元数据都将发送到同一目标。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

在此示例中，与前缀 ` /images` 匹配的对象的对象元数据将发送到一个目标，而与前缀 ` /videos` 匹配的对象的对象元数据则发送到另一个目标。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

由搜索集成服务生成的 **JSON**

为存储分段启用搜索集成服务后，每次添加，更新或删除对象元数据或标记时，系统都会生成一个 JSON 文档并将其发送到目标端点。

此示例显示了在名为 `test` 的存储分段中创建具有密钥 `SGWS/Tagging.txt` 的对象时可能生成的 JSON 示例。`test` 存储分段未进行版本控制，因此 `veversionId` 标记为空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

元数据通知中包含的对象元数据

下表列出了启用搜索集成后发送到目标端点的 JSON 文档中包含的所有字段。

文档名称包括存储分段名称，对象名称和版本 ID （如果存在）。

Type	项目名称	Description
存储分段和对象信息	存储分段	存储分段的名称
存储分段和对象信息	key	对象密钥名称
存储分段和对象信息	版本 ID	对象版本，用于受版本控制的分段中的对象
存储分段和对象信息	region	分段区域，例如 `us-east-1`
系统元数据	size	HTTP 客户端可见的对象大小（以字节为单位）
系统元数据	MD5	对象哈希

Type	项目名称	Description
用户元数据	元数据 ` 键：值 _ `	对象的所有用户元数据，作为键值对
Tags	标记 ` *key* ： *value* `	为对象定义的所有对象标记，作为键值对

- 注： * 对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后，您无法在索引中编辑文档的字段类型。

相关信息

使用租户帐户

获取存储使用情况请求

" 获取存储使用量 " 请求会告知您帐户正在使用的存储总量以及与帐户关联的每个存储分段的存储总量。

帐户及其存储分段使用的存储量可通过修改后的 GET 服务请求获得，该请求可使用 `x-ntap-sg-usage` 查询参数。存储分段使用量与系统处理的 PUT 和 DELETE 请求分开跟踪。根据请求处理情况，使用量值与预期值匹配可能会有一定的延迟，尤其是在系统负载较重时。

默认情况下， StorageGRID 会尝试使用强全局一致性检索使用情况信息。如果无法实现强全局一致性， StorageGRID 将尝试以强站点一致性检索使用情况信息。

要完成此操作，您拥有 S3 ： ListAllMy桶 权限或帐户 root 。

请求示例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

响应示例

此示例显示了一个帐户，该帐户在两个存储分段中包含四个对象和 12 字节的数据。每个存储分段包含两个对象和六个字节的数据。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

版本控制

存储的每个对象版本都会在响应中生成 `ObjectCount` 和 `DataBytes` 值。删除标记不会添加到 `ObjectCount` Total 中。

相关信息

一致性控制

已弃用旧合规性存储分段请求

您可能需要使用 StorageGRID S3 REST API 来管理使用原有合规性功能创建的分段。

已弃用合规性功能

先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。

如果您之前启用了全局合规性设置，则会在 StorageGRID 11.6 中启用全局 S3 对象锁定设置。您不能再在启用了合规性的情况下创建新的存储分段；但是，您可以根据需要使用 StorageGRID S3 REST API 管理任何现有的旧合规存储分段。

- 使用 S3 对象锁定
- 使用 ILM 管理对象
- "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

已弃用的合规性请求：

- 已弃用 - 为符合性修改存储分段请求

  SGCompliance XML 元素已弃用。以前，您可以将此 StorageGRID 自定义元素包含在 PUT 存储分段请求的可选 XML 请求正文中，以创建合规存储分段。

- 已弃用—获取存储分段合规性请求

  获取存储分段合规性请求已弃用。但是，您可以继续使用此请求来确定当前对现有旧版合规存储分段有效的合规性设置。

- 已弃用— PUT 存储分段合规性请求

  PUT 存储分段合规性请求已弃用。但是，您可以继续使用此请求修改现有旧版合规存储分段的合规性设置。例如，您可以将现有存储分段置于合法保留状态或延长其保留期限。

已弃用：为满足合规性而修改存储分段请求

SGCompliance XML 元素已弃用。以前，您可以将此 StorageGRID 自定义元素包含在 PUT 存储分段请求的可选 XML 请求正文中，以创建合规存储分段。

先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。

使用 S3 对象锁定

使用 ILM 管理对象

"NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

您不能再在已启用合规性的情况下创建新存储分段。如果您尝试使用 PUT 分段请求修改以满足合规性要求来创建新的合规分段，则会返回以下错误消息：

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

相关信息

使用 ILM 管理对象

使用租户帐户

获取存储分段合规性请求已弃用。但是，您可以继续使用此请求来确定当前对现有旧版合规存储分段有效的合规性设置。

先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。

使用 S3 对象锁定

使用 ILM 管理对象

"NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

要完成此操作，您拥有 S3： GetBucketCompliance 权限或帐户 root 。

请求示例

通过此示例请求，您可以确定名为 `mybucket` 的存储分段的合规性设置。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

响应示例

在响应 XML 中，` <SGCompliance>` 列出了对存储分段有效的合规性设置。此示例响应显示了一个存储分段的合规性设置，从将对象载入网格开始，每个对象将保留一年（ 525600 分钟）。此存储分段当前没有法律上的保留。每个对象将在一年后自动删除。

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	Description
RetentionPeriodMinutes	添加到此存储分段的对象的保留期限长度，以分钟为单位。保留期限从将对象载入网格时开始。
乐高积木	• true ： 此存储分段当前处于合法保留状态。除非取消合法保留，否则无法删除此存储分段中的对象，即使其保留期限已过期也是如此。 • false ： 此存储分段当前未处于合法保留状态。此存储分段中的对象可以在保留期限到期时删除。
自动删除	• true ： 此存储分段中的对象将在保留期限到期时自动删除，除非此存储分段处于合法保留状态。 • false ： 保留期限到期后，不会自动删除此存储分段中的对象。如果需要删除这些对象，必须手动将其删除。

错误响应

如果未创建符合要求的存储分段，则响应的 HTTP 状态代码为 `404 Not Found` ， S3 错误代码为 `XNoSuchBucketCompliance` 。

相关信息

使用 ILM 管理对象

使用租户帐户

已弃用： **PUT** 存储分段合规性请求

PUT 存储分段合规性请求已弃用。但是，您可以继续使用此请求修改现有旧版合规存储分段的合规性设置。例如，您可以将现有存储分段置于合法保留状态或延长其保留期限。

先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。

使用 S3 对象锁定

使用 ILM 管理对象

"NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

要完成此操作，您拥有 S3 ： PutBucketCompliance 权限或帐户 root 。

发出 PUT 存储分段合规性请求时，必须为合规性设置的每个字段指定一个值。

请求示例

此示例请求修改名为 `mybucket` 的存储分段的合规性设置。在此示例中， `mybucket` 中的对象现在将保留两年（ 1 ， 051 ， 200 分钟），而不是一年，从将对象载入网格开始。此存储分段没有法律上的保留。每个对象将

在两年后自动删除。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	Description
RetentionPeriodMinutes	添加到此存储分段的对象的保留期限长度，以分钟为单位。保留期限从将对象载入网格时开始。 • 注意： * 为 RetentionPeriodMinutes 指定新值时，必须指定一个等于或大于存储分段当前保留期限的值。设置存储分段的保留期限后，您不能减小该值；您只能增加该值。
乐高积木	• true ： 此存储分段当前处于合法保留状态。除非取消合法保留，否则无法删除此存储分段中的对象，即使其保留期限已过期也是如此。 • false ： 此存储分段当前未处于合法保留状态。此存储分段中的对象可以在保留期限到期时删除。
自动删除	• true ： 此存储分段中的对象将在保留期限到期时自动删除，除非此存储分段处于合法保留状态。 • false ： 保留期限到期后，不会自动删除此存储分段中的对象。如果需要删除这些对象，必须手动将其删除。

合规性设置的一致性级别

当您使用 PUT 存储分段合规性请求更新 S3 存储分段的合规性设置时， StorageGRID 会尝试更新整个网格中存储分段的元数据。默认情况下， StorageGRID 使用 * 强 - 全局 * 一致性级别来保证所有数据中心站点以及包含存储分段元数据的所有存储节点在更改的合规性设置中具有读 - 写一致性。

如果 StorageGRID 由于某个站点上的数据中心站点或多个存储节点不可用而无法达到 * 强 - 全局 * 一致性级别，则响应的 HTTP 状态代码为 `503 Service unavailable` 。

如果收到此响应，您必须联系网格管理员，以确保所需的存储服务尽快可用。如果网格管理员无法在每个站点提供足够的存储节点，技术支持可能会指示您通过强制执行 * 强站点 * 一致性级别来重试失败的请求。

除非技术支持指示您这样做，并且您了解使用此级别可能产生的后果，否则切勿强制使用 * 强站点 * 一致性级别来满足 PUT 存储分段合规性要求。

当一致性级别降低到 * 强站点 * 时， StorageGRID 保证更新后的合规性设置仅对站点中的客户端请求具有读写后一致性。这意味着，在所有站点和存储节点均可用之前， StorageGRID 系统可能会暂时为此存储分段设置多个不一致的设置。设置不一致可能导致意外和意外的行为。例如，如果您将某个存储分段置于合法保留状态并强制降低一致性级别，则某些数据中心站点上可能仍会继续使用存储分段先前的合规性设置（即合法保留）。因此，您认为处于合法保留状态的对象可能会在保留期限到期时被用户删除，或者如果启用了自动删除，也可以删除。

要强制使用 * 强站点 * 一致性级别，请重新发出 PUT 分段合规性请求，并包含 `consistency Control` HTTP 请求标头，如下所示：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

错误响应

- 如果未创建符合要求的存储分段，则响应的 HTTP 状态代码为 `404 not found`。
- 如果请求中的 `RetentionPeriodMinutes` 小于存储分段的当前保留期限，则 HTTP 状态代码为 `400 bad request`。

相关信息

已弃用：为满足合规性而修改存储分段请求

使用租户帐户

使用 ILM 管理对象

存储分段和组访问策略

StorageGRID 使用 Amazon Web Services （ AWS ）策略语言允许 S3 租户控制对这些存储分段和对象的访问。StorageGRID 系统实施 S3 REST API 策略语言的一个子集。S3 API 的访问策略以 JSON 格式写入。

访问策略概述

StorageGRID 支持两种访问策略。

- * 分段策略 * ，使用 GET 分段策略， PUT 分段策略和 DELETE 分段策略 S3 API 操作进行配置。存储分段策略附加到存储分段，因此，可以对其进行配置，以控制存储分段所有者帐户或其他帐户中的用户对存储分段及其对象的访问。一个存储分段策略适用场景 只能包含一个存储分段，并且可能包含多个组。
- * 组策略 * ，使用租户管理器或租户管理 API 配置。组策略会附加到帐户中的某个组，因此，这些策略会配置为允许该组访问该帐户拥有的特定资源。一个组策略只对一个组进行适用场景 ，并且可能对多个存储分段进行。

StorageGRID 存储分段和组策略遵循由 Amazon 定义的特定语法。每个策略中都包含一组策略语句，每个语句都包含以下元素：

- 语句 ID （ SID ）（可选）
- 影响
- 主体 / 不重要
- 资源 /NotResource
- 操作 / 未操作
- 条件（可选）

策略语句是使用此结构构建的，用于指定权限： Grant <Effic> to allow/deny <Principe> to Perform <Action> on <Resource> when <condition> applies 。

每个策略元素都用于特定功能：

Element	Description
SID	Sid 元素是可选的。SID 仅用作用户的问题描述 。它会被存储，但不会被 StorageGRID 系统解释。
影响	使用 Effect 元素确定是否允许或拒绝指定的操作。您必须使用支持的 Action Element 关键字来确定允许（或拒绝）对存储分段或对象执行的操作。
主体 / 不重要	您可以允许用户，组和帐户访问特定资源并执行特定操作。如果请求中不包含 S3 签名，则可以通过指定通配符（ * ）作为主体来进行匿名访问。默认情况下，只有帐户 root 有权访问该帐户拥有的资源。 您只需要在存储分段策略中指定主体元素。对于组策略，附加该策略的组为隐式主体元素。
资源 /NotResource	资源元素用于标识分段和对象。您可以使用 Amazon 资源名称（ ARN ）来标识资源，从而允许或拒绝对存储分段和对象的权限。
操作 / 未操作	操作和效果元素是权限的两个组成部分。当组请求资源时，它们会被授予或拒绝访问该资源。除非您明确分配权限，否则访问将被拒绝，但您可以使用显式拒绝覆盖由其他策略授予的权限。
条件	条件元素是可选的。通过条件，您可以构建表达式以确定何时应用策略。

在 Action 元素中，您可以使用通配符（ * ）指定所有操作或部分操作。例如，此操作与 S3： GetObject ， S3 ： PutObject 和 S3： DeleteObject 等权限匹配。

```
s3:*Object
```

在资源元素中，可以使用通配符（ * ）和（？ ）。星号（ * ）与 0 个或更多字符匹配时，问号（？ ） 匹配任意单个字符。

在 Principal 元素中，除了设置匿名访问权限之外，不支持使用通配符，此权限会授予所有人权限。例如，您将

通配符（ * ）设置为 Principal 值。

```
"Principal":"*"
```

在以下示例中，该语句使用的是 " 影响 " ， " 主体 " ， " 操作 " 和 " 资源 " 元素。此示例显示了一个完整的存储分段策略语句，该语句使用 " 允许 " 的效果为 Principals ，管理组 联合组 / 管理员 和财务组 联合组 / 财务在名为 `mybucket` 的存储分段上执行操作 `s 3 ： ListBucket` 以及对该存储分段中的所有对象执行操作 `s 3 ： GetObject` 。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

存储分段策略的大小限制为 20 ， 480 字节，而组策略的大小限制为 5 ， 120 字节。

相关信息

使用租户帐户

策略的一致性控制设置

默认情况下，对组策略所做的任何更新最终都是一致的。由于策略缓存，一旦组策略保持一致，所做的更改可能还需要 15 分钟才能生效。默认情况下，对存储分段策略进行的任何更新最终也会保持一致。

您可以根据需要更改存储分段策略更新的一致性保证。例如，出于安全原因，您可能希望对存储分段策略所做的更改尽快生效。

在这种情况下，您可以在 PUT 存储分段策略请求中设置 `consistency Control` 标头，也可以使用 PUT 存储分段一致性请求。更改此请求的一致性控制时，必须使用值 * 全部 * ，这可以为读写一致性提供最高保证。如果

在 PUT 存储分段一致性请求的标题中指定任何其他一致性控制值，则此请求将被拒绝。如果为 PUT 存储分段策略请求指定任何其他值，则此值将被忽略。存储分段策略保持一致后，由于策略缓存，更改可能需要额外 8 秒才能生效。

> 如果将一致性级别设置为 "**all** " 以强制新的存储分段策略更快生效，请确保在完成后将存储分段级别控制设置回其原始值。否则，所有未来的存储分段请求将使用 * 全部 * 设置。

在策略语句中使用 **ARN**

在策略语句中， ARN 用于 Principal 和 Resource Element 。

- 使用以下语法指定 S3 资源 ARN ：

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 使用以下语法指定身份资源 ARN （用户和组）：

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

其他注意事项：

- 您可以使用星号（ * ）作为通配符，以匹配对象密钥中的零个或多个字符。
- 可以在对象密钥中指定的国际字符应使用 JSON UTF-8 或 JSON \u 转义序列进行编码。不支持百分比编码。

  "RFC 2141 URN 语法"

  PUT 存储分段策略操作的 HTTP 请求正文必须使用 charset=UTF-8 进行编码。

在策略中指定资源

在策略语句中，您可以使用资源元素指定允许或拒绝权限的分段或对象。

- 每个策略语句都需要一个资源元素。在策略中，资源由元素 `Resource` 或 `NotResource` 表示以表示排除。
- 您可以使用 S3 资源 ARN 指定资源。例如：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 您也可以在对象密钥中使用策略变量。例如：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 资源值可以指定创建组策略时尚不存在的存储分段。

相关信息

[指定策略中的变量]

指定策略中的主体

使用 Principal 元素标识策略语句允许 / 拒绝访问资源的用户，组或租户帐户。

- 存储分段策略中的每个策略语句都必须包含一个主体元素。组策略中的策略语句不需要主体元素，因为组被理解为主体。
- 在策略中，主体由元素 "`Principal ，` " 或 "`NotPrincipal` " 表示以表示排除。
- 必须使用 ID 或 ARN 指定基于帐户的身份：

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 此示例使用租户帐户 ID 27233906934684427525 ，其中包括帐户 root 和帐户中的所有用户：

```
 "Principal": { "AWS": "27233906934684427525" }
```

- 您只能指定帐户 root ：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 您可以指定一个特定的联合用户（ "Alex" ）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 您可以指定特定的联合组（ "Managers" ）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- 您可以指定匿名主体：

```
"Principal": "*"
```

- 为避免歧义，您可以使用用户 UUID ，而不是用户名：

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  例如，假设 Alex 离开该组织，并且用户名 `Alex` 已被删除。如果新的 Alex 加入组织并获得相同的 `Alex` 用户名，则新用户可能会无意中继承授予给原始用户的权限。

- 主体值可以指定在创建存储分段策略时尚不存在的组 / 用户名称。

在策略中指定权限

在策略中， Action 元素用于允许 / 拒绝对资源的权限。您可以在策略中指定一组权限，这些权限由元素 "Action" 或 "NotAction" 表示以表示排除。其中每个元素都映射到特定的 S3 REST API 操作。

下表列出了应用于存储分段的权限以及应用于对象的权限。

> Amazon S3 现在对 PUT 和 DELETE 分段复制操作使用 S3： PutReplicationConfiguration 权限。StorageGRID 对每个操作使用单独的权限，这些权限与原始 Amazon S3 规范匹配。

> 如果使用 PUT 覆盖现有值，则会执行删除。

应用于存储分段的权限

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： CreateBucket	放入存储分段	
S3： DeleteBucket	删除存储分段	
S3： DeleteBucketMetadataNotification	删除存储分段元数据通知配置	是的。
S3： DeleteBucketPolicy	删除存储分段策略	
S3： DeleteReplicationConfiguration	删除存储分段复制	是， PUT 和 DELETE 的权限不同 *
S3： GetBucketAcl	获取分段 ACL	
S3： GetBucketCompliance	获取存储分段合规性（已弃用）	是的。

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： GetBucketConsistency	获取存储分段一致性	是的。
S3： GetBucketCORS	获取分段存储器	
S3： GetEncryptionConfiguration	获取存储分段加密	
S3： GetBucketLastAccessTime	获取存储分段上次访问时间	是的。
S3： GetBucketLocation	获取存储分段位置	
S3： GetBucketMetadataNotification	获取存储分段元数据通知配置	是的。
S3： GetBucketNotification	获取存储分段通知	
S3： GetBucketObjectLockConfiguration	获取对象锁定配置	
S3： GetBucketPolicy	获取存储分段策略	
S3： GetBucketTagging	获取存储分段标记	
S3： GetBucketVersioning	获取存储分段版本控制	
S3： GetLifeycleConfiguration	获取存储分段生命周期	
S3： GetReplicationConfiguration	获取存储分段复制	
S3： ListAllMy桶	• 获取服务 • 获取存储使用量	是，适用于获取存储使用量
S3： ListBucket	• 获取存储分段（列出对象） • 头存储分段 • 后对象还原	
S3： ListBucketMultipartUploads	• 列出多部件上传 • 后对象还原	
S3： ListBucketVersions	获取存储分段版本	
S3： PutBucketCompliance	PUT 存储分段合规性（已弃用）	是的。

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： PutBucketConsistency	PUT 存储分段一致性	是的。
S3： PutBucketCORS	• 删除存储分段或† • 放入存储分段箱	
S3： PutEncryptionConfiguration	• 删除存储分段加密 • PUT 存储分段加密	
S3： PutBucketLastAccessTime	PUT 分段上次访问时间	是的。
S3： PutBucketMetadataNotification	PUT 存储分段元数据通知配置	是的。
S3： PutBucketNotification	PUT 存储分段通知	
S3： PutBucketObjectLockConfiguration	• PUT Bucket with the `x-AMZ-bucket-object-lock-enabled ： true` request header （ also requires the S3： CreateBucket permission ） • PUT 对象锁定配置	
S3： PutBucketPolicy	PUT 存储分段策略	
S3： PutBucketTagging	• 删除存储分段标记† • 放置存储分段标记	
S3： PutBucketVersioning	PUT 存储分版本	
S3： PutLifeycleConfiguration	• 删除存储分段生命周期† • PUT 存储分段生命周期	
S3： PutReplicationConfiguration	PUT 存储分段复制	是， PUT 和 DELETE 的权限不同 *

应用于对象的权限

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： AbortMultipartUpload	• 中止多部分上传 • 后对象还原	

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： DeleteObject	• 删除对象 • 删除多个对象 • 后对象还原	
S3： DeleteObjectTagging	删除对象标记	
S3： DeleteObjectVersionTagging	删除对象标记（对象的特定版本）	
S3： DeleteObjectVersion	删除对象（对象的特定版本）	
S3： GetObject	• 获取对象 • HEAD 对象 • 后对象还原 • 选择对象内容	
S3： GetObjectAcl	获取对象 ACL	
S3： GetObjectLegend	获取对象合法保留	
S3： GetObjectRetention	获取对象保留	
S3： GetObjectTagging	获取对象标记	
S3： GetObjectVersionTagging	获取对象标记（对象的特定版本）	
S3： GetObjectVersion	GET 对象（对象的特定版本）	
S3： ListMultipartUploadPart	列出部件， POST 对象还原	
S3： PutObject	• PUT 对象 • PUT 对象—复制 • 后对象还原 • 启动多部件上传 • 完成多部件上传 • 上传部件 • 上传部件—复制	
S3： PutObjectLegend	PUT 对象合法保留	

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： PutObjectRetention	放置对象保留	
S3： PutObjectTagging	放置对象标记	
S3： PutObjectVersionTagging	PUT 对象标记（对象的特定版本）	
S3： PutOverwriteObject	• PUT 对象 • PUT 对象—复制 • PUT 对象标记 • 删除对象标记 • 完成多部件上传	是的。
S3： RestoreObject	后对象还原	

使用 **PutOverwriteObject** 权限

S3： PutOverwriteObject 权限是一种自定义 StorageGRID 权限，适用场景 可通过此权限创建或更新对象。此权限的设置可确定客户端是否可以覆盖对象的数据，用户定义的元数据或 S3 对象标记。

此权限的可能设置包括：

- * 允许 *：客户端可以覆盖对象。这是默认设置。
- * 拒绝 *：客户端无法覆盖对象。如果设置为 deny ，则 PutOverwriteObject 权限的工作原理如下：
  - 如果在同一路径中找到现有对象：
    - 无法覆盖对象的数据，用户定义的元数据或 S3 对象标记。
    - 正在执行的任何载入操作均会取消，并返回错误。
    - 如果启用了 S3 版本控制，则 deny 设置将阻止 PUT 对象标记或删除对象标记操作修改对象及其非最新版本的标记集。
  - 如果未找到现有对象，此权限将不起作用。
- 如果不存在此权限，则效果与设置了 allow 时相同。

> 如果当前 S3 策略允许覆盖，并且 PutOverwriteObject 权限设置为 deny ，则客户端无法覆盖对象的数据，用户定义的元数据或对象标记。此外，如果选中了 * 阻止客户端修改 * 复选框（ * 配置 * > * 系统 * > * 网格选项 * ），则该设置将覆盖 PutOverwriteObject 权限的设置。

相关信息

S3 组策略示例

指定策略中的条件

条件用于定义策略何时生效。条件包括运算符和键值对。

条件使用键值对进行评估。一个条件元素可以包含多个条件，每个条件可以包含多个键值对。条件块使用以下格式：

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

在以下示例中， ipaddress 条件使用 SourceIp 条件密钥。

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

支持的条件运算符

条件运算符分为以下几类：

- string
- 数字
- 布尔值
- IP 地址
- 空检查

条件运算符	**Description**
StringEquals	根据完全匹配（区分大小写）将键与字符串值进行比较。
StringNotEquals	根据否定匹配（区分大小写）将键与字符串值进行比较。
StringEqualsIgnoreCase	根据完全匹配将键与字符串值进行比较（忽略大小写）。
StringNotEqualsIgnoreCase	根据否定的匹配将键与字符串值进行比较（忽略大小写）。
StringLike	根据完全匹配（区分大小写）将键与字符串值进行比较。可以包括 * 和？通配符。

条件运算符	Description
StringNotLike	根据否定匹配（区分大小写）将键与字符串值进行比较。可以包括 * 和？通配符。
数值方程式	根据精确匹配将键与数字值进行比较。
NumericNotEquals	根据否定匹配将键与数字值进行比较。
数值 GreaterThan	根据 "`大于` " 匹配将键与数值进行比较。
NumericGreaterThals.	根据 "`大于或等于` " 匹配将键与数值进行比较。
数值细小	根据 "`小于` " 匹配将键与数值进行比较。
数值 ThalEquals	根据 "`小于或等于` " 匹配将键与数值进行比较。
池	根据 "`true 或 false` " 匹配将键与布尔值进行比较。
IP 地址	将密钥与 IP 地址或 IP 地址范围进行比较。
NotIpAddress	根据否定匹配将密钥与 IP 地址或 IP 地址范围进行比较。
空	检查当前请求上下文中是否存在条件密钥。

支持的条件密钥

类别	适用的条件密钥	Description
IP 运算符	AWS ： 源 Ip	将与发送请求的 IP 地址进行比较。可用于存储分段或对象操作。 • 注意： * 如果 S3 请求是通过管理节点和网关节点上的负载平衡器服务发送的，则此请求将与负载平衡器服务上游的 IP 地址进行比较。 • 注 * ： 如果使用第三方非透明负载平衡器，则此负载平衡器将与该负载平衡器的 IP 地址进行比较。任何 `X-forwarded-for` 标头都将被忽略，因为无法确定其有效性。

类别	适用的条件密钥	Description
资源 / 身份	AWS： 用户名	将与发送请求的发件人用户名进行比较。可用于存储分段或对象操作。
S3： ListBucket 和 S3： ListBucketVersions 权限	S3： 分隔符	将与 GET 分段或 GET 分段对象版本请求中指定的分隔符参数进行比较。
S3： ListBucket 和 S3： ListBucketVersions 权限	S3： 最大密钥	将与获取分段或获取分段对象版本请求中指定的 max-keys 参数进行比较。
S3： ListBucket 和 S3： ListBucketVersions 权限	S3： 前缀	将与获取分段或获取分段对象版本请求中指定的前缀参数进行比较。
S3： PutObject	S3： object-lock-real-retenation-days	与 `x-AMZ-object-lock-retain-until date` 请求标题中指定的或根据存储分段默认保留期限计算得出的保留日期进行比较，以确保这些值在以下请求允许的范围内： • PUT 对象 • PUT 对象—复制 • 启动多部件上传
S3： PutObjectRetention	S3： object-lock-real-retenation-days	与 PUT 对象保留请求中指定的保留截止日期进行比较，以确保其在允许的范围内。

指定策略中的变量

您可以在策略中使用变量填充可用的策略信息。您可以在 `Resource` 元素中使用策略变量，也可以在 `Condition` 元素中使用字符串比较。

在此示例中，变量 ` $ ｛AWS： username｝ ` 是资源元素的一部分：

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

在此示例中，变量 ` $ ｛AWS： username｝ ` 是条件块中条件值的一部分：

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

变量	Description
`$ {AWS： SourceIp}`	使用 SourceIp 键作为提供的变量。
`$ {AWS： username}`	使用 username 密钥作为提供的变量。
`$ {S3： prefix}`	使用特定于服务的前缀密钥作为提供的变量。
`$ {S3： max-keys}`	使用特定于服务的 max-keys 键作为提供的变量。
`$ {*}`	特殊字符。使用字符作为文字 * 字符。
`$ {？ }`	特殊字符。使用字符作为文字？字符。
`$ {$}`	特殊字符。使用字符作为文字 $ 字符。

创建需要特殊处理的策略

有时，策略可能会授予对安全性有危险或对持续操作（例如锁定帐户的 root 用户）有危险的权限。在策略验证期间， StorageGRID S3 REST API 实施的限制性要低于 Amazon ，但在策略评估期间同样严格。

策略问题描述	Policy type	Amazon 行为	StorageGRID 行为
拒绝向自己授予对 root 帐户的任何权限	存储分段	有效且强制实施，但 root 用户帐户保留所有 S3 存储分段策略操作的权限	相同
拒绝用户 / 组的任何权限	组	有效且强制实施	相同
允许外部帐户组拥有任何权限	存储分段	主体无效	有效，但如果某个策略允许，则所有 S3 存储分段策略操作的权限均会返回 405 Method not allowed 错误

策略问题描述	**Policy type**	**Amazon** 行为	**StorageGRID** 行为
允许外部帐户 root 或用户拥有任何权限	存储分段	有效，但如果某个策略允许，则所有 S3 存储分段策略操作的权限均会返回 405 Method not allowed 错误	相同
允许所有人对所有操作拥有权限	存储分段	有效，但对所有 S3 存储分段策略操作的权限会为外部帐户 root 和用户返回 405 Method not allowed 错误	相同
拒绝任何人对所有操作的权限	存储分段	有效且强制实施，但 root 用户帐户保留所有 S3 存储分段策略操作的权限	相同
主体是不存在的用户或组	存储分段	主体无效	有效
资源不是 S3 存储分段	组	有效	相同
主体是一个本地组	存储分段	主体无效	有效
策略授予非所有者帐户（包括匿名帐户）放置对象的权限	存储分段	有效。对象由创建者帐户拥有，并且存储分段策略不适用。创建者帐户必须使用对象 ACL 为对象授予访问权限。	有效。对象由存储分段所有者帐户拥有。存储分段策略适用。

一次写入多读（**WORM**）保护

您可以创建一次写入多读（Write Once Read-Many ， WORM ）分段来保护数据，用户定义的对象元数据和 S3 对象标记。您可以配置 WORM 分段，以便创建新对象并防止覆盖或删除现有内容。请使用此处所述的方法之一。

为了确保覆盖始终被拒绝，您可以：

- 在网格管理器中，转到 * 配置 * > * 系统 * > * 网格选项 * ，然后选中 * 阻止客户端修改 * 复选框。
- 应用以下规则和 S3 策略：
  - 向 S3 策略添加 PutOverwriteObject deny 操作。
  - 将 DeleteObject deny 操作添加到 S3 策略中。
  - 向 S3 策略添加 PUT 对象允许操作。

> 在 S3 策略中将 DeleteObject 设置为 deny 不会阻止 ILM 在存在 "`zero copies after 30 days` " 等规则时删除对象。

即使应用了所有这些规则和策略，它们也不会防止并发写入（请参见情况 A ）。它们可以防止顺序完成的覆盖（请参见情况 B ）。

- 情形 A*： 并发写入（不受保护）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 情形 B*： 顺序完成的覆盖（防止）

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

相关信息

使用 ILM 管理对象

[创建需要特殊处理的策略]

StorageGRID ILM 规则如何管理对象

S3 组策略示例

S3 策略示例

使用本节中的示例为分段和组构建 StorageGRID 访问策略。

S3 存储分段策略示例

存储分段策略用于指定附加此策略的存储分段的访问权限。存储分段策略使用 S3 PutBucketPolicy API 进行配置。

可以按照以下命令使用 AWS 命令行界面配置存储分段策略：

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

示例：允许每个人对某个存储分段进行只读访问

在此示例中，允许包括匿名用户在内的所有人列出存储分段中的对象，并对存储分段中的所有对象执行 GET Object 操作。所有其他操作都将被拒绝。请注意，此策略可能不会特别有用，因为除了帐户 root 之外，没有其他人有权写入存储分段。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

示例：允许一个帐户中的每个人完全访问某个存储分段，而另一帐户中的每个人只读访问某个存储分段

在此示例中，一个指定帐户中的每个人都可以完全访问某个存储分段，而另一个指定帐户中的每个人只能列出存储分段并对存储分段中以 `shared/` 对象密钥前缀开头的对象执行 GetObject 操作。

> 在 StorageGRID 中，非所有者帐户创建的对象（包括匿名帐户）归存储分段所有者帐户所有。存储分段策略适用场景 这些对象。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

示例：允许每个人对某个存储分段进行只读访问，并允许指定组进行完全访问

在此示例中，允许包括 anonymous 在内的所有人列出存储分段并对存储分段中的所有对象执行 GET Object 操作，而仅允许指定帐户中属于组 `Marketing` 的用户进行完全访问。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

示例：如果客户端位于 **IP** 范围内，则允许每个人对存储分段进行读写访问

在此示例中，允许包括匿名用户在内的所有人列出存储分段并对存储分段中的所有对象执行任何对象操作，前提是这些请求来自指定的 IP 范围（ 54.240.143.0 到 54.240.143.255 ，但 54.240.143.188 除外）。所有其他操作都将被拒绝，并且 IP 范围以外的所有请求都将被拒绝。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

示例：允许指定的联合用户完全访问某个存储分段

在此示例中，允许联合用户 Alex 对 `examplebucket` 存储分段及其对象进行完全访问。包括 "`root` " 在内的所有其他用户均被明确拒绝所有操作。但请注意， "`root` " 从不会被拒绝 PUT ， Get/DeleteBucketPolicy 的权限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

示例： **PutOverwriteObject** 权限

在此示例中， PutOverwriteObject 和 DeleteObject 的 `Deny` Effect 可确保任何人都无法覆盖或删除对象的数据，用户定义的元数据和 S3 对象标记。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

相关信息

对存储分段执行的操作

S3 组策略示例

组策略用于指定附加此策略的组的访问权限。此策略中没有 `Principal` 元素，因为它是隐式的。组策略可使用租户管理器或 API 进行配置。

示例：使用租户管理器设置组策略

使用租户管理器添加或编辑组时，您可以选择要如何创建组策略，以定义此组的成员将具有的 S3 访问权限，如

下所示：

- * 无 S3 访问 * ：默认选项。此组中的用户无权访问 S3 资源，除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
- * 只读访问 * ：此组中的用户对 S3 资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您不能编辑此字符串。
- * 完全访问 * ：此组中的用户对 S3 资源（包括分段）具有完全访问权限。选择此选项后，完全访问组策略的 JSON 字符串将显示在文本框中。您不能编辑此字符串。
- * 自定义 * ：组中的用户将获得您在文本框中指定的权限。

  在此示例中，组成员只能列出并访问指定存储分段中的特定文件夹（密钥前缀）。

示例：允许组完全访问所有存储分段

在此示例中，除非 bucket 策略明确拒绝，否则允许组中的所有成员对租户帐户拥有的所有分段进行完全访问。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

示例：允许组对所有分段进行只读访问

在此示例中，组的所有成员都对 S3 资源具有只读访问权限，除非 bucket 策略明确拒绝。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

示例：仅允许组成员对存储分段中的**"`folder`"**具有完全访问权限

在此示例中，组成员只能列出并访问指定存储分段中的特定文件夹（密钥前缀）。请注意，在确定其他组策略和存储分段策略的隐私时，应考虑这些文件夹的访问权限。

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

相关信息

使用租户帐户

配置 REST API 的安全性

您应查看为 REST API 实施的安全措施，并了解如何保护系统安全。

StorageGRID 如何为 REST API 提供安全性

您应了解 StorageGRID 系统如何为 REST API 实施安全性，身份验证和授权。

StorageGRID 使用以下安全措施。

- 如果为负载平衡器端点配置了 HTTPS ，则客户端与负载平衡器服务的通信将使用 HTTPS 。

  配置负载平衡器端点时，可以选择启用 HTTP 。例如，您可能希望将 HTTP 用于测试或其他非生产目的。有关详细信息，请参见有关管理 StorageGRID 的说明。

- 默认情况下， StorageGRID 使用 HTTPS 与存储节点进行客户端通信，并在网关节点上使用 CLB 服务。

  可以选择为这些连接启用 HTTP 。例如，您可能希望将 HTTP 用于测试或其他非生产目的。有关详细信息，请参见有关管理 StorageGRID 的说明。

  CLB 服务已弃用。

- StorageGRID 与客户端之间的通信使用 TLS 进行加密。
- 无论将负载平衡器端点配置为接受 HTTP 或 HTTPS 连接，网格中的负载平衡器服务和存储节点之间的通信都会进行加密。
- 客户端必须向 StorageGRID 提供 HTTP 身份验证标头，才能执行 REST API 操作。

安全证书和客户端应用程序

客户端可以连接到网关节点或管理节点上的负载平衡器服务，直接连接到存储节点或网关节点上的 CLB 服务。

在所有情况下，客户端应用程序都可以使用网格管理员上传的自定义服务器证书或 StorageGRID 系统生成的证书进行 TLS 连接：

- 当客户端应用程序连接到负载平衡器服务时，它们会使用为用于建立连接的特定负载平衡器端点配置的证书来执行此操作。每个端点都有自己的证书，此证书可以是网格管理员上传的自定义服务器证书，也可以是网格管理员在配置端点时在 StorageGRID 中生成的证书。
- 当客户端应用程序直接连接到存储节点或网关节点上的 CLB 服务时，它们会使用安装 StorageGRID 系统时为存储节点生成的系统生成的服务器证书（由系统证书颁发机构签名）， 或网格管理员为网格提供的一个自定义服务器证书。

应将客户端配置为信任对用于建立 TLS 连接的任何证书签名的证书颁发机构。

有关配置负载平衡器端点的信息，请参见管理 StorageGRID 的说明，以及有关为直接连接到存储节点或网关节点上的 CLB 服务添加单个自定义服务器证书的说明。

摘要

下表显示了如何在 S3 和 Swift REST API 中实施安全问题：

Security 问题描述	实施 **REST API**
连接安全性	TLS
服务器身份验证	系统 CA 签名的 X.509 服务器证书或管理员提供的自定义服务器证书
客户端身份验证	• S3： S3 帐户（访问密钥 ID 和机密访问密钥） • Swift： Swift 帐户（用户名和密码）
客户端授权	• S3： 存储分段所有权和所有适用的访问控制策略 • Swift： 管理员角色访问

相关信息

管理 StorageGRID

支持 **TLS** 库的哈希和加密算法

StorageGRID 系统支持一组有限的密码套件，客户端应用程序可在建立传输层安全（ TLS ）会话时使用这些密码套件。

支持的 **TLS** 版本

StorageGRID 支持 TLS 1.2 和 TLS 1.3 。

不再支持 SSLv3 和 TLS 1.1 （或更早版本）。

支持的密码套件

TLS 版本	密码套件的 **IANA** 名称
1.2	tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384
1.2	tls_ECDHE_RSA_WIT_CHACHA20_POLY1305_SHA256
1.2	tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256
1.3	tls_aes_256_gcm_SHA384
1.3	tls_chacHA20_POLY1305_SHA256
1.3	tls_aes_128_gcm_SHA256

已弃用密码套件

以下密码套件已弃用。未来版本将删除对这些密码的支持。

IANA 名称
tls_rsa_and_aes_128_gcm_SHA256
tls_rsa_and_aes_256_gcm_SHA384

相关信息

如何配置客户端连接

监控和审核操作

您可以通过查看整个网格或特定节点的事务趋势来监控客户端操作的工作负载和效率。您可以使用审核消息监控客户端操作和事务。

监控对象载入和检索速率

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

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 在信息板上，找到协议操作部分。

   本节总结了 StorageGRID 系统执行的客户端操作的数量。协议速率是过去两分钟的平均值。

3. 选择 * 节点 * 。
4. 从节点主页（部署级别）中，单击 * 负载平衡器 * 选项卡。

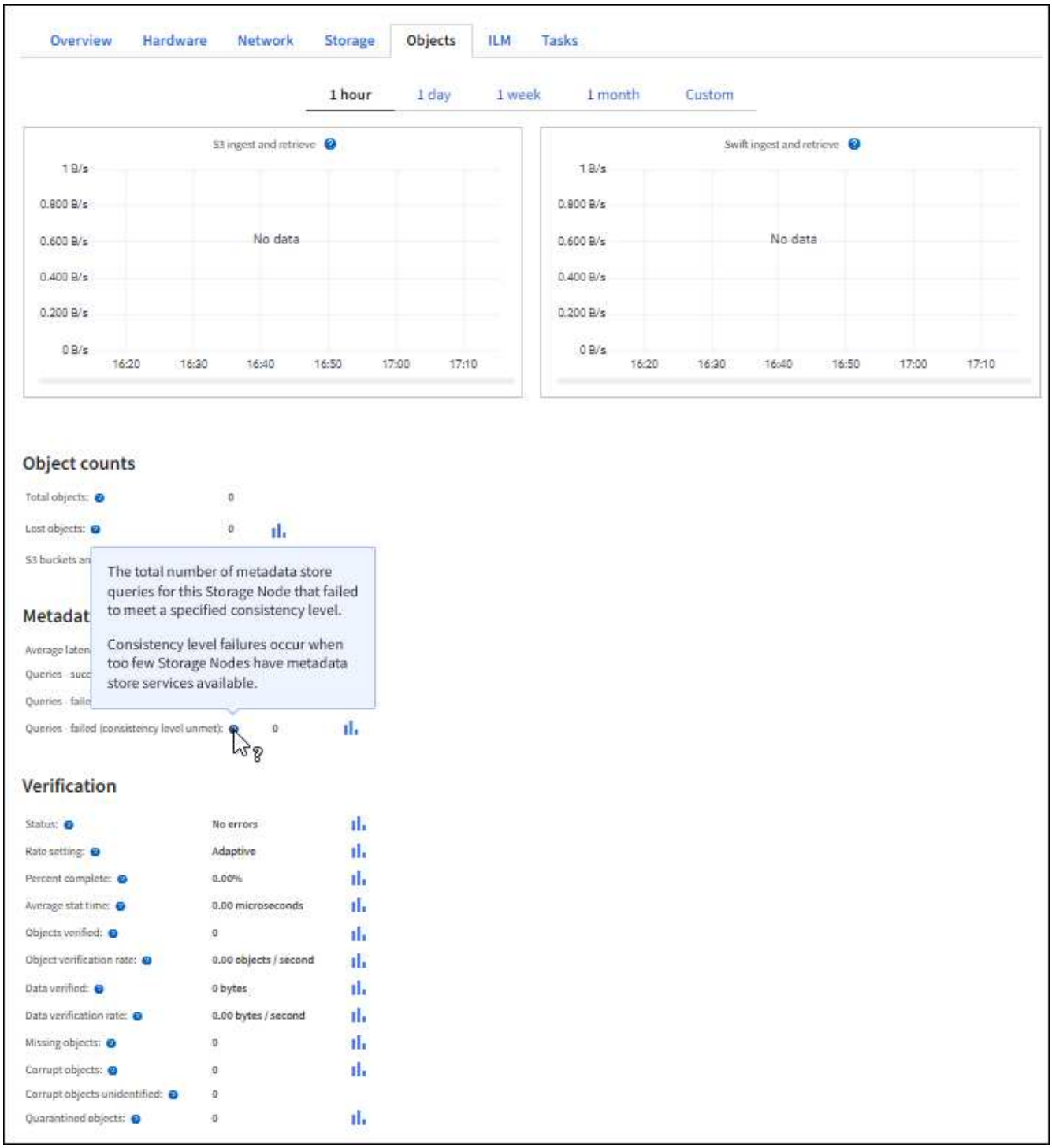
   这些图表显示了定向到网格中负载平衡器端点的所有客户端流量的趋势。您可以选择以小时，天，周，月或年为单位的时间间隔， 或者，您也可以应用自定义间隔。

5. 从节点主页（部署级别）中，单击 * 对象 * 选项卡。

   此图表显示了整个 StorageGRID 系统的载入和检索速率，以每秒字节数和总字节数为单位。您可以选择以小时，天，周，月或年为单位的时间间隔， 或者，您也可以应用自定义间隔。

6. 要查看特定存储节点的信息，请从左侧列表中选择该节点，然后单击 * 对象 * 选项卡。

   此图表显示了此存储节点的对象载入速率和检索速率。此选项卡还包括对象计数，查询和验证的指标。您可以单击这些标签以查看这些指标的定义。



7. 如果您需要更多详细信息：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 概述 * > * 主要 * 。

      API Operations 部分显示整个网格的摘要信息。

   c. 选择 * 存储节点 _* > * LDR* > * 客户端应用程序 _* > * 概述 * > * 主 *

      操作部分显示选定存储节点的摘要信息。

访问和查看审核日志

审核消息由 StorageGRID 服务生成并存储在文本日志文件中。审核日志中特定于 API 的审核消息提供关键的安全性，操作和性能监控数据，可帮助您评估系统的运行状况。

您需要的内容

- 您具有特定的访问权限。
- 您已有 `passwords.txt` 文件。
- 您知道管理节点的 IP 地址。

关于此任务

活动审核日志文件名为 `audit.log` ，并存储在管理节点上。

每天保存一次活动的 audit.log 文件，并启动一个新的 `audit.log` 文件。已保存文件的名称以 ` yyyy-mm-dd.txt_` 的格式指示其保存时间。

一天后，保存的文件将按 ` yyyy-mm-dd.txt.gz_` 格式进行压缩和重命名，从而保留原始日期。

此示例显示了活动的 `audit.log` 文件，前一天的文件（`2018-04-15.txt` ）和前一天的压缩文件（`2018-04-14.txt.gz` ）。

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

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 转到包含审核日志文件的目录：

   ```
   cd /var/local/audit/export
   ```

3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

审核日志中跟踪的 **S3** 操作

StorageGRID 审核日志会跟踪多个存储分段操作和对象操作。

审核日志中跟踪的存储分段操作

- 删除存储分段
- 删除存储分段标记

- 删除多个对象
- 获取存储分段（列出对象）
- 获取 Bucket 对象版本
- 获取存储分段标记
- 头存储分段
- 放入存储分段
- PUT 存储分段合规性
- 放置存储分段标记
- PUT 存储分版本

审核日志中跟踪的对象操作

- 完成多部件上传
- 上传部件（ ILM 规则使用严格或平衡的载入行为时）
- 上传部件—复制（当 ILM 规则使用严格或平衡的载入行为时）
- 删除对象
- 获取对象
- HEAD 对象
- 后对象还原
- PUT 对象
- PUT 对象—复制

相关信息

对存储分段执行的操作

对对象执行的操作

活动，空闲和并发 **HTTP** 连接的优势

如何配置 HTTP 连接可能会影响 StorageGRID 系统的性能。根据 HTTP 连接是活动连接还是空闲连接，或者您有多个并发连接，配置会有所不同。

您可以确定以下类型的 HTTP 连接的性能优势：

- 空闲 HTTP 连接
- 活动 HTTP 连接
- 并发 HTTP 连接

保持空闲 **HTTP** 连接处于打开状态的优势

即使客户端应用程序处于闲置状态，您也应保持 HTTP 连接处于打开状态，以允许客户端

应用程序通过打开的连接执行后续事务。根据系统测量结果和集成经验，您应将闲置的 HTTP 连接保持打开状态最多 10 分钟。StorageGRID 可能会自动关闭保持打开和闲置超过 10 分钟的 HTTP 连接。

开放式和空闲 HTTP 连接具有以下优势：

- 从 StorageGRID 系统确定必须执行 HTTP 事务的时间缩短到 StorageGRID 系统可以执行此事务的时间

  缩短延迟是主要优势，尤其是在建立 TCP/IP 和 TLS 连接所需的时间方面。

- 通过在先前执行的传输中填充 TCP/IP 慢速启动算法来提高数据传输速率
- 瞬时通知多种中断客户端应用程序与 StorageGRID 系统之间连接的故障情况

- 保持闲置连接打开多长时间是对与现有连接相关的慢速启动优势与将连接分配给内部系统资源的理想平衡。

活动 **HTTP** 连接的优势

要直接连接到存储节点或网关节点上的 CLB 服务（已弃用），您应将活动 HTTP 连接的持续时间限制为最多 10 分钟，即使 HTTP 连接持续执行事务也是如此。

- 连接应保持打开状态的最长持续时间是为了权衡连接持久性的优势与将连接分配给内部系统资源的理想方式。

对于客户端与存储节点或 CLB 服务的连接，限制活动 HTTP 连接具有以下优势：

- 在 StorageGRID 系统之间实现最佳负载平衡。

  使用 CLB 服务时，您应防止使用长 - 寿命的 TCP/IP 连接，以优化整个 StorageGRID 系统的负载平衡。您应将客户端应用程序配置为跟踪每个 HTTP 连接的持续时间，并在设置的时间后关闭 HTTP 连接，以便可以重新建立和重新平衡 HTTP 连接。

  在客户端应用程序建立 HTTP 连接时， CLB 服务会在整个 StorageGRID 系统中平衡负载。随着时间的推移，随着负载平衡要求的变化， HTTP 连接可能不再是最佳连接。当客户端应用程序为每个事务建立单独的 HTTP 连接时，系统会执行最佳的负载平衡，但这会抵消与持久连接相关的更有价值的收益。

  CLB 服务已弃用。

- 允许客户端应用程序将 HTTP 事务定向到具有可用空间的 LDR 服务。
- 允许开始维护过程。

  某些维护过程仅在所有正在进行的 HTTP 连接完成后才会启动。

对于客户端与负载平衡器服务的连接，限制打开连接的持续时间对于允许某些维护过程立即启动非常有用。如果客户端连接的持续时间不受限制，则自动终止活动连接可能需要几分钟的时间。

并发 **HTTP** 连接的优势

您应保持与 StorageGRID 系统的多个 TCP/IP 连接处于开放状态，以实现并行处理，从而提高性能。并行连接的最佳数量取决于多种因素。

并发 HTTP 连接具有以下优势：

- 缩短延迟

  事务可以立即启动，而不是等待其他事务完成。

- 提高吞吐量

  StorageGRID 系统可以执行并行事务并提高聚合事务吞吐量。

客户端应用程序应建立多个 HTTP 连接。当客户端应用程序必须执行事务时，它可以选择并立即使用当前未处理事务的任何已建立连接。

在性能开始下降之前，每个 StorageGRID 系统的拓扑对于并发事务和连接具有不同的峰值吞吐量。峰值吞吐量取决于计算资源，网络资源，存储资源和 WAN 链路等因素。服务器和服务的数量以及 StorageGRID 系统支持的应用程序的数量也是因素。

StorageGRID 系统通常支持多个客户端应用程序。在确定客户端应用程序所使用的最大并发连接数时，应牢记这一点。如果客户端应用程序包含多个软件实体，每个软件实体都与 StorageGRID 系统建立连接，则应添加这些实体之间的所有连接。在以下情况下，您可能需要调整并发连接的最大数量：

- StorageGRID 系统的拓扑会影响系统可以支持的并发事务和连接的最大数量。
- 如果客户端应用程序通过带宽有限的网络与 StorageGRID 系统进行交互，则可能需要降低并发程度，以确保各个事务在合理时间内完成。
- 当许多客户端应用程序共享 StorageGRID 系统时，您可能需要降低并发程度，以避免超过系统限制。

为读取和写入操作分隔 **HTTP** 连接池

您可以使用单独的 HTTP 连接池执行读写操作，并控制每个连接池要使用的池容量。通过单独的 HTTP 连接池，您可以更好地控制事务并平衡负载。

客户端应用程序可以创建检索占主导地位（读取）或存储占主导地位（写入）的负载。由于读取和写入事务使用单独的 HTTP 连接池，因此您可以调整每个池中用于读取或写入事务的数量。

使用 **Swift**

使用 **Swift**： 概述

客户端应用程序可以使用 OpenStack Swift API 与 StorageGRID 系统相连接。

StorageGRID 支持以下特定版本的 Swift 和 HTTP 。

项目	**version**
Swift 规格	截至 2015 年 11 月的 OpenStack Swift 对象存储 API v1

项目	**version**
HTTP	1.1 有关 HTTP 的详细信息，请参见 HTTP/1.1 （ RFC 7230-35 ）。 • 注 * ： StorageGRID 不支持 HTTP/1.1 管道化。

相关信息

"OpenStack ： 对象存储 API"

StorageGRID 中的 **Swift API** 支持历史记录

您应了解 StorageGRID 系统对 Swift REST API 的支持发生了哪些变化。

版本。	注释
11.6.	少量编辑更改。
11.5	消除了弱一致性控制。此时将改用可用的一致性级别。
11.4	增加了对 TLS 1.3 的支持，并更新了支持的 TLS 密码套件列表。CLB 已弃用。增加了 ILM 与一致性设置之间的关系问题描述 。
11.3	更新了 PUT 对象操作，以描述在载入时使用同步放置的 ILM 规则的影响（适用于载入行为的平衡而严格的选项）。添加了使用负载平衡器端点或高可用性组的客户端连接的问题描述 。更新了支持的 TLS 密码套件列表。不再支持 TLS 1.1 密码。
11.2.	对文档进行了少量编辑更改。
11.1	增加了对使用 HTTP 与网格节点建立 Swift 客户端连接的支持。更新了一致性控制的定义。
11.0	增加了对每个租户帐户 1 ， 000 个容器的支持。
10.3	对文档进行管理更新和更正。删除了用于配置自定义服务器证书的部分。
10.2	StorageGRID 系统对 Swift API 的初始支持。当前支持的版本为 OpenStack Swift 对象存储 API v1 。

StorageGRID 如何实施 **Swift REST API**

客户端应用程序可以使用 Swift REST API 调用连接到存储节点和网关节点以创建容器以及

存储和检索对象。这样，为 OpenStack Swift 开发的面向服务的应用程序便可与 StorageGRID 系统提供的内部对象存储相连接。

Swift 对象管理

将 Swift 对象载入 StorageGRID 系统后，这些对象将通过系统活动 ILM 策略中的信息生命周期管理（ ILM ）规则进行管理。ILM 规则和策略可确定 StorageGRID 如何创建和分发对象数据副本，以及它如何在一段时间内管理这些副本。例如， ILM 规则可能适用于特定 Swift 容器中的对象，并可能指定在一定年数内将多个对象副本保存到多个数据中心。

如果您需要了解网格的 ILM 规则和策略将如何影响您的 Swift 租户帐户中的对象，请联系您的 StorageGRID 管理员。

客户端请求冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 Swift 客户端何时开始操作。

一致性保证和控制

默认情况下， StorageGRID 为新创建的对象提供读写一致性，并为对象更新和机头操作提供最终一致性。成功完成 PUT 后的任何 GET 都将能够读取新写入的数据。对现有对象的覆盖，元数据更新和删除最终保持一致。覆盖通常需要几秒钟或几分钟才能传播，但可能需要长达 15 天的时间。

此外，您还可以通过 StorageGRID 控制每个容器的一致性。您可以根据应用程序的需要更改一致性控制、以便在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。

相关信息

使用 ILM 管理对象

获取容器一致性请求

提交容器一致性请求

实施 **Swift REST API** 的建议

在实施用于 StorageGRID 的 Swift REST API 时，应遵循以下建议。

针对不存在的对象的建议

如果您的应用程序定期检查某个对象是否位于您不希望该对象实际存在的路径上，则应使用 "`available` " 一致性控制。例如，如果应用程序在对某个位置执行 PUT 操作之前对该位置执行 HEAD 操作，则应使用 "`Available` " 一致性控制。

否则，如果 head 操作未找到对象，则在一个或多个存储节点不可用时，可能会收到大量 500 个内部服务器错误。

您可以使用 PUT 容器一致性请求为每个容器设置 "`Available` " 一致性控制。

对象名称建议

对于在 StorageGRID 11.4 或更高版本中创建的容器，不再需要限制对象名称以满足性能最佳实践。例如，现在

可以对对象名称的前四个字符使用随机值。

对于在 StorageGRID 11.4 之前的版本中创建的容器，请继续对对象名称遵循以下建议：

- 不应使用随机值作为对象名称的前四个字符。这与 AWS 以前针对名称前缀的建议不同。而应使用非随机的非唯一前缀，例如 `image` 。
- 如果您按照以前的 AWS 建议在名称前缀中使用随机和唯一字符，则应在对象名称前添加目录名称。也就是说，请使用以下格式：

```
mycontainer/mydir/f8e3-image3132.jpg
```

而不是以下格式：

```
mycontainer/f8e3-image3132.jpg
```

关于"`范围读取`"的建议

如果选择了 * 压缩存储的对象 * 选项（ * 配置 * > * 系统 * > * 网格选项 * ），则 Swift 客户端应用程序应避免执行指定要返回的字节数范围的 GET 对象操作。这些 "`range read` " 操作效率低下，因为 StorageGRID 必须有效解压缩对象以访问请求的字节。从非常大的对象请求少量字节的 GET 对象操作效率尤其低下；例如，从 50 GB 压缩对象读取 10 MB 范围的操作效率非常低。

如果从压缩对象读取范围，则客户端请求可能会超时。

如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

相关信息

获取容器一致性请求

提交容器一致性请求

管理 StorageGRID

配置租户帐户和连接

要将 StorageGRID 配置为接受来自客户端应用程序的连接，需要创建一个或多个租户帐户并设置连接。

创建和配置 **Swift** 租户帐户

要使 Swift API 客户端能够在 StorageGRID 上存储和检索对象，需要使用 Swift 租户帐户。每个租户帐户都有自己的帐户 ID ，组和用户以及容器和对象。

Swift 租户帐户由 StorageGRID 网格管理员使用网格管理器或网格管理 API 创建。

创建 Swift 租户帐户时，网格管理员会指定以下信息：

- 租户的显示名称（租户的帐户 ID 会自动分配，不能更改）
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。
- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。
- 如果启用了 SSO ，则哪个联合组具有 root 访问权限来配置租户帐户。

创建 Swift 租户帐户后，具有 root 访问权限的用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享），并创建本地组和用户
- 监控存储使用情况

> Swift 用户必须具有 root 访问权限才能访问租户管理器。但是， " 根访问 " 权限不允许用户向 Swift REST API 进行身份验证以创建容器和载入对象。用户必须具有 Swift 管理员权限才能向 Swift REST API 进行身份验证。

相关信息

管理 StorageGRID

使用租户帐户

支持的 Swift API 端点

如何配置客户端连接

网格管理员可以选择影响 Swift 客户端连接到 StorageGRID 以存储和检索数据的配置。建立连接所需的具体信息取决于所选的配置。

客户端应用程序可以通过连接到以下任一项来存储或检索对象：

- 管理节点或网关节点上的负载平衡器服务，或者也可以是管理节点或网关节点高可用性（ HA ）组的虚拟 IP 地址
- 网关节点上的 CLB 服务，或者也可以是网关节点高可用性组的虚拟 IP 地址

> CLB 服务已弃用。在 StorageGRID 11.3 版本之前配置的客户端可以继续在网关节点上使用 CLB 服务。所有其他依靠 StorageGRID 提供负载平衡的客户端应用程序都应使用负载平衡器服务进行连接。

- 存储节点，具有或不具有外部负载平衡器

配置 StorageGRID 时，网格管理员可以使用网格管理器或网格管理 API 执行以下步骤，所有这些步骤均为可选步骤：

1. 为负载平衡器服务配置端点。

   您必须配置端点才能使用负载平衡器服务。管理节点或网关节点上的负载平衡器服务会将传入的网络连接从客户端应用程序分发到存储节点。创建负载平衡器端点时， StorageGRID 管理员会指定端口号，端点是否接受 HTTP 或 HTTPS 连接，将使用此端点的客户端类型（ S3 或 Swift ）以及用于 HTTPS 连接的证书（如果适用）。

2. 配置不可信客户端网络。

   如果 StorageGRID 管理员将节点的客户端网络配置为不可信，则节点仅接受客户端网络上显式配置为负载平衡器端点的端口上的入站连接。

3. 配置高可用性组。

   如果管理员创建了一个 HA 组，则多个管理节点或网关节点的网络接口将置于主动备份配置中。客户端连接使用 HA 组的虚拟 IP 地址进行。

有关每个选项的详细信息，请参见有关管理 StorageGRID 的说明。

摘要：客户端连接的 **IP** 地址和端口

客户端应用程序使用网格节点的 IP 地址以及该节点上服务的端口号连接到 StorageGRID 。如果配置了高可用性（ HA ）组，则客户端应用程序可以使用 HA 组的虚拟 IP 地址进行连接。

建立客户端连接所需的信息

下表总结了客户端连接到 StorageGRID 的不同方式以及每种连接类型所使用的 IP 地址和端口。有关详细信息，请与 StorageGRID 管理员联系，或者参见有关管理问题描述 StorageGRID 的说明，了解如何在网格管理器中查找此信息。

建立连接的位置	客户端连接到的服务	**IP** 地址	**Port**
HA 组	负载平衡器	HA 组的虚拟 IP 地址	• 负载平衡器端点端口
HA 组	CLB • 注： * CLB 服务已弃用。	HA 组的虚拟 IP 地址	默认 Swift 端口： • HTTPS： 8083 • HTTP： 8085
管理节点	负载平衡器	管理节点的 IP 地址	• 负载平衡器端点端口
网关节点	负载平衡器	网关节点的 IP 地址	• 负载平衡器端点端口
网关节点	CLB • 注： * CLB 服务已弃用。	网关节点的 IP 地址 • 注意： * 默认情况下，CLB 和 LDR 的 HTTP 端口未启用。	默认 Swift 端口： • HTTPS： 8083 • HTTP： 8085
存储节点	LDR	存储节点的 IP 地址	默认 Swift 端口： • HTTPS： 18083 • HTTP： 18085

示例

要将 Swift 客户端连接到网关节点 HA 组的负载平衡器端点，请使用以下结构化 URL：

- `https://VIP-of-HA-group:LB-endpoint-port`

例如，如果 HA 组的虚拟 IP 地址为 192.0.2.6 ， Swift 负载平衡器端点的端口号为 10444 ，则 Swift 客户端可以使用以下 URL 连接到 StorageGRID：

- ` https://192.0.2.6:10444`

可以为客户端用于连接到 StorageGRID 的 IP 地址配置 DNS 名称。请与本地网络管理员联系。

决定使用 **HTTPS** 或 **HTTP** 连接

使用负载平衡器端点建立客户端连接时，必须使用为此端点指定的协议（ HTTP 或 HTTPS ）进行连接。要使用 HTTP 连接到存储节点或网关节点上的 CLB 服务，必须启用 HTTP 。

默认情况下，当客户端应用程序连接到存储节点或网关节点上的 CLB 服务时，它们必须对所有连接使用加密 HTTPS 。您也可以选择网格管理器中的 * 启用 HTTP 连接 * 网格选项来启用不太安全的 HTTP 连接。例如，在非生产环境中测试与存储节点的连接时，客户端应用程序可能会使用 HTTP 。

> 为生产网格启用 HTTP 时要小心，因为请求将以未加密方式发送。

> CLB 服务已弃用。

如果选择了 * 启用 HTTP 连接 * 选项，则客户端对 HTTP 使用的端口必须与对 HTTPS 使用的端口不同。请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

在 **Swift API** 配置中测试连接

您可以使用 Swift 命令行界面测试与 StorageGRID 系统的连接，并验证是否可以向系统读取和写入对象。

您需要的内容

- 您必须已下载并安装 python swiftclient ，即 Swift 命令行客户端。

  "SwiftStack： Python-swiftclient"

- 您必须在 StorageGRID 系统中具有 Swift 租户帐户。

关于此任务

如果尚未配置安全性，则必须在每个命令中添加 ` -insecure` 标志。

步骤

1. 查询 StorageGRID Swift 部署的信息 URL：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

这足以测试您的 Swift 部署是否正常运行。要通过存储对象进一步测试帐户配置，请继续执行其他步骤。

2. 将对象放入容器中：

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. 获取用于验证对象的容器：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. 删除对象：

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. 删除容器：

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

相关信息

创建和配置 Swift 租户帐户

配置 REST API 的安全性

Swift REST API 支持的操作

StorageGRID 系统在 OpenStack Swift API 中支持大多数操作。在将 Swift REST API 客户端与 StorageGRID 集成之前，请查看帐户，容器和对象操作的实施详细信息。

StorageGRID 中支持的操作

支持以下 Swift API 操作：

- 帐户操作
- 容器操作
- 对象操作

所有操作的通用响应标头

StorageGRID 系统可为 OpenStack Swift 对象存储 API v1 定义的受支持操作实施所有通用标头。

相关信息

"OpenStack： 对象存储 API"

支持的 Swift API 端点

StorageGRID 支持以下 Swift API 端点：信息 URL ，身份验证 URL 和存储 URL 。

信息 URL

您可以通过向带有 /info 路径的 Swift 基础 URL 发出 GET 请求来确定 StorageGRID Swift 实施的功能和限制。

`https://FQDN _ 节点 IP ： Swift Port_/info/`

在请求中：

- ` fqdn_` 是完全限定域名。
- ` 节点 IP_` 是 StorageGRID 网络上存储节点或网关节点的 IP 地址。
- ` *Swift Port*` 是用于存储节点或网关节点上的 Swift API 连接的端口号。

例如，以下信息 URL 将从 IP 地址为 10.99.106.103 且使用端口 18083 的存储节点请求信息。

` https://10.99.106.103:18083/info/`

此响应包括 Swift 实施的功能，可用作 JSON 词典。客户端工具可以解析 JSON 响应以确定实施的功能，并将其用作后续存储操作的约束。

通过实施 StorageGRID ， Swift 可以对信息 URL 进行未经身份验证的访问。

身份验证 URL

客户端可以使用 Swift 身份验证 URL 作为租户帐户用户进行身份验证。

`https://FQDN _ 节点 IP ： Swift Port_/auth/v1.0/`

您必须在 `X-Auth-User` 和 `X-Auth-Key` Request 标头中提供租户帐户 ID ，用户名和密码作为参数，如下所示：

`X-Auth-User ： Tenant 帐户 ID ： Username`

`X-Auth-Key ： Password`

在请求标题中：

- ` 租户帐户 ID` 是创建 Swift 租户时 StorageGRID 分配的帐户 ID 。这与租户管理器登录页面上使用的租户帐户 ID 相同。
- ` 用户名 _` 是已在租户管理器中创建的租户用户的名称。此用户必须属于具有 Swift 管理员权限的组。无法将租户的 root 用户配置为使用 Swift REST API 。

  如果为租户帐户启用了身份联合，请从 LDAP 服务器提供联合用户的用户名和密码。或者，也可以提供 LDAP 用户的域名。例如：

  `X-Auth-User ： Tenant 帐户 ID ： 用户名@Domain_Name`

- ` 密码 _` 是租户用户的密码。用户密码在租户管理器中创建和管理。

对成功的身份验证请求的响应将返回存储 URL 和身份验证令牌，如下所示：

<code>X-Storage-URL： https://FQDN _ 节点 IP： Swift_Port/v1/_Tenant 帐户 ID</code>

`X-Auth-Token ： token`

`X-Storage-Token ： token`

默认情况下，令牌在生成后 24 小时内有效。

为特定租户帐户生成令牌。一个帐户的有效令牌不会授权用户访问另一个帐户。

存储 URL

客户端应用程序可以通过问题描述 Swift REST API 调用对网关节点或存储节点执行支持的帐户，容器和对象操作。存储请求会发送到身份验证响应中返回的存储 URL 。此请求还必须包含从身份验证请求返回的 X-Auth-Token 标头和值。

` https://FQDN _ IP： Swift_Port_/v1/_Tenant 帐户 ID`

` _ 容器 ]/object_]`

`X-Auth-Token : token`

某些包含使用情况统计信息的存储响应标头可能无法反映最近修改的对象的准确数字。准确的数字可能需要几分钟才能显示在这些标题中。

帐户和容器操作的以下响应标头是包含使用情况统计信息的示例：

- `X-Account-bytes-used`
- `X-Account-Object-Count`
- `X-Container-bytes-used`
- `X-Container-Object-Count`

相关信息

配置租户帐户和连接

帐户操作

容器操作

对象操作

帐户操作

对帐户执行以下 Swift API 操作。

获取帐户

此操作将检索与帐户和帐户使用情况统计信息关联的容器列表。

以下请求参数为必填项：

- 帐户

以下请求标头为必填项：

- `X-Auth-Token`

以下支持的请求查询参数是可选的：

- `delimiter`
- `End_marker`
- 格式
- 限制
- `marker`
- 前缀

如果成功执行，则会返回以下标头，并在该帐户未找到容器或容器列表为空时返回 "`HTTP/1.1 204 No Content` " 响应；如果找到该帐户且容器列表不为空，则返回 "`HTTP/1.1 200 OK` " 响应：

- `Accept-ranges`
- 内容长度
- 内容类型
- `dATE`
- `X-Account-bytes-used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-ID`

主帐户

此操作将从 Swift 帐户检索帐户信息和统计信息。

以下请求参数为必填项：

- 帐户

以下请求标头为必填项：

- `X-Auth-Token`

成功执行将返回以下标头，并显示 "`HTTP/1.1 204 No Content` " 响应：

- `Accept-ranges`
- 内容长度
- `dATE`
- `X-Account-bytes-used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-ID`

相关信息

监控和审核操作

容器操作

每个 Swift 帐户最多支持 1 ， 000 个容器。 StorageGRID对容器执行以下 Swift API 操作。

删除容器

此操作会从 StorageGRID 系统中的 Swift 帐户中删除一个空容器。

需要以下请求参数：

- 帐户
- 容器

以下请求标头为必填项：

- `X-Auth-Token`

成功执行将返回以下标头并显示 "HTTP/1.1 204 No Content" 响应：

- 内容长度
- 内容类型
- `dATE`
- `X-Trans-ID`

获取容器

此操作将检索与此容器关联的对象列表以及 StorageGRID 系统中的容器统计信息和元数据。

需要以下请求参数：

- 帐户
- 容器

以下请求标头为必填项：

- `X-Auth-Token`

以下支持的请求查询参数是可选的：

- `delimiter`
- `End_marker`
- 格式
- 限制
- `marker`
- 路径
- 前缀

成功执行将返回以下标头，并显示 "HTTP/1.1 200 successful" 或 "HTTP/1.1 204 No Content" 响应：

- `Accept-ranges`

- 内容长度
- 内容类型
- dATE
- X-Container-bytes-used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-ID

机头容器

此操作将从 StorageGRID 系统检索容器统计信息和元数据。

需要以下请求参数：

- 帐户
- 容器

以下请求标头为必填项：

- X-Auth-Token

成功执行将返回以下标头并显示 "HTTP/1.1 204 No Content" 响应：

- Accept-ranges
- 内容长度
- dATE
- X-Container-bytes-used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-ID

放入容器

此操作将为 StorageGRID 系统中的帐户创建一个容器。

需要以下请求参数：

- 帐户
- 容器

以下请求标头为必填项：

- X-Auth-Token

成功执行将返回以下标头，并显示 "HTTP/1.1 201 Created " 或 "HTTP/1.1 202 Accept" （如果此帐户下已存在

此容器）响应：

- 内容长度
- `dATE`
- `X-Timestamp`
- `X-Trans-ID`

容器名称在 StorageGRID 命名空间中必须是唯一的。如果容器位于其他帐户下，则返回以下标头： "HTTP/1.1 409 conflict 。 "

相关信息

监控和审核操作

对象操作

对对象执行以下 Swift API 操作。

删除对象

此操作将从 StorageGRID 系统中删除对象的内容和元数据。

需要以下请求参数：

- 帐户
- 容器
- 对象

以下请求标头为必填项：

- `X-Auth-Token`

成功执行将返回以下响应标头，并显示 `HTTP/1.1 204 No Content` response：

- 内容长度
- 内容类型
- `dATE`
- `X-Trans-ID`

在处理删除对象请求时， StorageGRID 会尝试立即从所有存储位置删除此对象的所有副本。如果成功， StorageGRID 会立即向客户端返回响应。如果无法在 30 秒内删除所有副本（例如，由于某个位置暂时不可用），则 StorageGRID 会将这些副本排队等待删除，然后指示客户端成功删除。

有关如何删除对象的详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

获取对象

此操作将检索对象内容并从 StorageGRID 系统获取对象元数据。

需要以下请求参数：

- 帐户
- 容器
- 对象

以下请求标头为必填项：

- `X-Auth-Token`

以下请求标头是可选的：

- 接受编码
- 如果匹配
- 如果修改 - 自
- 如果 - 无 - 匹配
- `If - Unmodify-since`
- 范围

成功执行将返回以下标头，并显示 `HTTP/1.1 200 OK` 响应：

- `Accept-ranges`
- `Content-Disposition` ，仅当设置了 `Content-Disposition` 元数据时才返回
- `Content-Encoding` ，仅在设置了 `Content-Encoding` 元数据时才返回
- 内容长度
- 内容类型
- `dATE`
- `ETag`
- 最后修改日期
- `X-Timestamp`
- `X-Trans-ID`

head 对象

此操作将从 StorageGRID 系统检索所载入对象的元数据和属性。

需要以下请求参数：

- 帐户
- 容器
- 对象

以下请求标头为必填项：

- `X-Auth-Token`

成功执行将返回以下标头并显示 "HTTP/1.1 200 OK" 响应：

- `Accept-ranges`
- `Content-Disposition` ，仅当设置了 `Content-Disposition` 元数据时才返回
- `Content-Encoding` ，仅在设置了 `Content-Encoding` 元数据时才返回
- 内容长度
- 内容类型
- `dATE`
- `ETag`
- 最后修改日期
- `X-Timestamp`
- `X-Trans-ID`

PUT 对象

此操作将使用数据和元数据创建新对象，或者将现有对象替换为 StorageGRID 系统中的数据和元数据。

StorageGRID 支持大小高达 5 TiB （ 5 ， 497 ， 556 ， 138 ， 880 字节）的对象。

> 冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 Swift 客户端何时开始操作。

需要以下请求参数：

- 帐户
- 容器
- 对象

以下请求标头为必填项：

- `X-Auth-Token`

以下请求标头是可选的：

- 内容处置
- 内容编码

  如果 ILM 规则要求适用场景 对象根据大小筛选对象并在载入时使用同步放置（即用于载入行为的平衡或严格选项），请勿使用分块 内容编码 。

- 传输编码

  如果 ILM 规则要求适用场景 对象根据大小筛选对象并在载入时使用同步放置（即用于载入行为的平衡或严

格选项），请勿使用压缩或分块 `Transfer-Encoding` 。

- 内容长度

  如果 ILM 规则按大小筛选对象并在载入时使用同步放置，则必须指定 `Content-L`长度 。

  > 如果您未遵循 内容编码 ， 传输编码 和 内容长度 的这些准则，则 StorageGRID 必须先保存此对象，然后才能确定对象大小并应用 ILM 规则。换言之， StorageGRID 必须默认为在载入时创建对象的临时副本。也就是说， StorageGRID 必须对载入行为使用双提交选项。

  有关同步放置和 ILM 规则的详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

- 内容类型
- `ETag`
- `X-Object-Meta-<` 名称 `\>` （对象相关元数据）

  如果要使用 * 用户定义的创建时间 * 选项作为 ILM 规则的参考时间，则必须将该值存储在名为 `X-Object-Meta-creation-time` 的用户定义标题中。例如：

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  自 1970 年 1 月 1 日以来，此字段的评估值为秒。

- `X-Storage-Class` ： `reduced` 冗余

  如果与所载入对象匹配的 ILM 规则指定了双重提交或平衡的载入行为，则此标头会影响 StorageGRID 创建的对象副本数。

  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则 StorageGRID 会在载入对象时创建一个临时副本（单个提交）。
  - * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，则只有在系统无法立即创建规则中指定的所有副本时，StorageGRID 才会创建一个临时副本。如果 StorageGRID 可以执行同步放置，则此标头不起作用。

    如果与 `re`匹配的 `ILM` 规则创建了一个复制副本，则最好使用 created_redundancy 标头。在这种情况下，使用 `recreated_redundancy` 可以避免在每次载入操作中不必要地创建和删除额外的对象副本。

    在其他情况下，不建议使用 `re`部冗余 标头，因为这样会增加载入期间丢失对象数据的风险。例如，如果最初将单个副本存储在发生故障的存储节点上，而此存储节点未能进行 ILM 评估，则可能会丢失数据。

    > 在任何一段时间内只复制一个副本会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

  请注意，指定 `recreated_redundancy` 仅会影响首次载入对象时创建的副本数。它不会影响在活动 ILM 策略评估对象时创建的对象副本数，也不会导致数据在 StorageGRID 系统中以较低的冗余级别存储。

成功执行将返回以下标头，并显示 "HTTP/1.1 201 Created " 响应：

- 内容长度
- 内容类型
- dATE
- ETag
- 最后修改日期
- X-Trans-ID

相关信息

使用 ILM 管理对象

监控和审核操作

选项请求

选项请求会检查单个 Swift 服务的可用性。选项请求由 URL 中指定的存储节点或网关节点处理。

options 方法

例如，客户端应用程序可以在不提供 Swift 身份验证凭据的情况下将选项请求问题描述 到存储节点上的 Swift 端口，以确定存储节点是否可用。您可以使用此请求进行监控，也可以允许外部负载平衡器确定存储节点何时关闭。

与信息 URL 或存储 URL 结合使用时， options 方法将返回给定 URL 支持的动词列表（例如 head ， get ， options 和 put ）。选项方法不能与身份验证 URL 结合使用。

以下请求参数为必填项：

- 帐户

以下请求参数是可选的：

- 容器
- 对象

成功执行将返回以下标头，并显示 "`HTTP/1.1 204 No Content` " 响应。对存储 URL 的选项请求不要求目标存在。

- allow （给定 URL 支持的动词列表，例如 head ， get ， options ， 和 PUT ）
- 内容长度
- 内容类型
- dATE
- X-Trans-ID

相关信息

支持的 Swift API 端点

对 **Swift API** 操作的错误响应

了解可能的错误响应有助于您对操作进行故障排除。

如果操作期间发生错误，可能会返回以下 HTTP 状态代码：

Swift 错误名称	**HTTP** 状态
AccountNameTooLong， ContainerNameTooLong， HeaderTooBig， InContainvaliderName， InvalidRequest， InvalidURI， MetadataNameTooLong， MetadataValueTooBig， MissingSecurityHeader， ObjectNameTooLong， TooManyContainers， TooManyMetadataItems， TotalMetadataTooLarge	400 个错误请求
ACCESSDENIED	403 已禁用
ContainerNotEmpty， ContainerAlreadyExists	409 冲突
内部错误	500 内部服务器错误
InvalidRange	416 无法满足请求的范围
方法未使用	不允许使用 405 方法
MissingContent长度	411 需要长度
未找到	未找到 404
未实施	501 未实施
预条件已启用	412- 前提条件失败
ResourceNotFound	未找到 404
未授权	401 未授权
UnprocessableEntity	422 不可处理实体

StorageGRID Swift REST API 操作

在 Swift REST API 中添加了特定于 StorageGRID 系统的操作。

获取容器一致性请求

一致性级别可在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。使用获取容器一致性请求，您可以确定应用于特定容器的一致性级别。

请求

请求 **HTTP** 标头	**Description**
`X-Auth-Token`	指定要用于请求的帐户的 Swift 身份验证令牌。
`x-ntap-sg-consistency`	指定请求的类型，其中 `true` = 获取容器一致性，`false` = 获取容器。
主机	请求所定向到的主机名。

请求示例

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

响应

响应 **HTTP** 标头	**Description**
`dATE`	响应的日期和时间。
连接	与服务器的连接是打开还是关闭。
`X-Trans-ID`	请求的唯一事务标识符。
内容长度	响应正文的长度。

响应 HTTP 标头	Description
x-ntap-sg-consistency	应用于容器的一致性控制级别。支持以下值： • * 全部 * ： 所有节点均立即接收数据，否则请求将失败。 • * 强 - 全局 * ： 保证所有站点中所有客户端请求的写入后读一致性。 • * 强站点 * ： 保证站点内所有客户端请求的写入后读一致性。 • * 读后新写入 * ： 为新对象提供读后写入一致性，并最终为对象更新提供一致性。提供高可用性和数据保护保证。 • 注意 * ： 如果应用程序对不存在的对象使用 head 请求，则在一个或多个存储节点不可用时，可能会收到大量 500 个内部服务器错误。要防止出现这些错误，请使用 "`Available` " 级别。 • * 可用 * （机头操作的最终一致性）：与 read-after-new-write 一致性级别相同，但仅为机头操作提供最终一致性。如果存储节点不可用，则为机头操作提供的可用性比 " read-after-new-write " 更高。

响应示例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

相关信息

使用租户帐户

提交容器一致性请求

使用 PUT 容器一致性请求可以指定要应用于对容器执行的操作的一致性级别。默认情况下，使用 read-after-new-write 一致性级别创建新容器。

请求

请求 HTTP 标头	Description
X-Auth-Token	要用于请求的帐户的 Swift 身份验证令牌。

请求 **HTTP** 标头	**Description**
`x-ntap-sg-consistency`	要应用于容器上的操作的一致性控制级别。支持以下值： • * 全部 *：所有节点均立即接收数据，否则请求将失败。 • * 强 - 全局 *：保证所有站点中所有客户端请求的写入后读一致性。 • * 强站点 *：保证站点内所有客户端请求的写入后读一致性。 • * 读后新写入 *：为新对象提供读后写入一致性，并最终为对象更新提供一致性。提供高可用性和数据保护保证。 • 注意 *：如果应用程序对不存在的对象使用 head 请求，则在一个或多个存储节点不可用时，可能会收到大量 500 个内部服务器错误。要防止出现这些错误，请使用 "`Available` " 级别。 • * 可用 *（机头操作的最终一致性）：与 `read-after-new-write` 一致性级别相同，但仅为机头操作提供最终一致性。如果存储节点不可用，则为机头操作提供的可用性比 " `read-after-new-write` " 更高。
主机	请求所定向到的主机名。

一致性控制和 **ILM** 规则如何交互以影响数据保护

您选择的一致性控制和 ILM 规则都会影响对象的保护方式。这些设置可以进行交互。

例如，存储对象时使用的一致性控制会影响对象元数据的初始放置，而为 ILM 规则选择的载入行为会影响对象副本的初始放置。由于 StorageGRID 需要访问对象的元数据及其数据来满足客户端请求，因此为一致性级别和载入行为选择匹配的保护级别可以提供更好的初始数据保护和更可预测的系统响应。

ILM 规则可以使用以下载入行为：

- * 严格 *：必须创建 ILM 规则中指定的所有副本，才能将成功返回给客户端。
- * 平衡 *： StorageGRID 尝试在载入时创建 ILM 规则中指定的所有副本；如果无法创建，则创建临时副本并将成功返回给客户端。在可能的情况下，将创建 ILM 规则中指定的副本。
- * 双提交 *： StorageGRID 会立即为对象创建临时副本，并将成功返回给客户端。如果可能，将创建 ILM 规则中指定的副本。

> 在为 ILM 规则选择载入行为之前，请阅读有关通过信息生命周期管理管理对象的说明中有关这些设置的完整问题描述 。

一致性控制和 **ILM** 规则如何交互的示例

假设您有一个双站点网格，其中包含以下 ILM 规则和以下一致性级别设置：

- * ILM 规则 * ：创建两个对象副本，一个在本地站点，一个在远程站点。此时将选择严格的载入行为。
- * 一致性级别 * ： `strong-global` （对象元数据会立即分发到所有站点。）

当客户端将对象存储到网格时， StorageGRID 会创建两个对象副本并将元数据分发到两个站点，然后再向客户端返回成功。

在载入成功消息时，此对象将受到完全保护，不会丢失。例如，如果本地站点在载入后不久丢失，则远程站点上仍存在对象数据和对象元数据的副本。此对象完全可检索。

如果您改用相同的 ILM 规则和 `strong-site` 一致性级别，则在将对象数据复制到远程站点之后，在将对象元数据分发到该远程站点之前，客户端可能会收到一条成功消息。在这种情况下，对象元数据的保护级别与对象数据的保护级别不匹配。如果本地站点在载入后不久丢失，则对象元数据将丢失。无法检索此对象。

一致性级别和 ILM 规则之间的关系可能很复杂。如需帮助，请联系 NetApp 。

请求示例

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

响应

响应 **HTTP** 标头	**Description**
`dATE`	响应的日期和时间。
连接	与服务器的连接是打开还是关闭。
`X-Trans-ID`	请求的唯一事务标识符。
内容长度	响应正文的长度。

响应示例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

相关信息

使用租户帐户

配置 REST API 的安全性

您应查看为 REST API 实施的安全措施，并了解如何保护系统安全。

StorageGRID 如何为 REST API 提供安全性

您应了解 StorageGRID 系统如何为 REST API 实施安全性，身份验证和授权。

StorageGRID 使用以下安全措施。

- 如果为负载平衡器端点配置了 HTTPS ，则客户端与负载平衡器服务的通信将使用 HTTPS 。

  配置负载平衡器端点时，可以选择启用 HTTP 。例如，您可能希望将 HTTP 用于测试或其他非生产目的。有关详细信息，请参见有关管理 StorageGRID 的说明。

- 默认情况下， StorageGRID 使用 HTTPS 与存储节点进行客户端通信，并在网关节点上使用 CLB 服务。

  可以选择为这些连接启用 HTTP 。例如，您可能希望将 HTTP 用于测试或其他非生产目的。有关详细信息，请参见有关管理 StorageGRID 的说明。

  CLB 服务已弃用。

- StorageGRID 与客户端之间的通信使用 TLS 进行加密。
- 无论将负载平衡器端点配置为接受 HTTP 或 HTTPS 连接，网格中的负载平衡器服务和存储节点之间的通信都会进行加密。
- 客户端必须向 StorageGRID 提供 HTTP 身份验证标头，才能执行 REST API 操作。

安全证书和客户端应用程序

客户端可以连接到网关节点或管理节点上的负载平衡器服务，直接连接到存储节点或网关节点上已弃用的 CLB 服务。

在所有情况下，客户端应用程序都可以使用网格管理员上传的自定义服务器证书或 StorageGRID 系统生成的证书进行 TLS 连接：

- 当客户端应用程序连接到负载平衡器服务时，它们会使用为用于建立连接的特定负载平衡器端点配置的证书来执行此操作。每个端点都有自己的证书，此证书可以是网格管理员上传的自定义服务器证书，也可以是网格管理员在配置端点时在 StorageGRID 中生成的证书。
- 当客户端应用程序直接连接到存储节点或网关节点上的 CLB 服务时，它们会使用安装 StorageGRID 系统时为存储节点生成的系统生成的服务器证书（由系统证书颁发机构签名）， 或网格管理员为网格提供的一个自定义服务器证书。

应将客户端配置为信任对用于建立 TLS 连接的任何证书签名的证书颁发机构。

有关配置负载平衡器端点的信息，请参见管理 StorageGRID 的说明，以及有关为直接连接到存储节点或网关节点上的 CLB 服务添加单个自定义服务器证书的说明。

摘要

下表显示了如何在 S3 和 Swift REST API 中实施安全问题：

Security 问题描述	实施 **REST API**
连接安全性	TLS
服务器身份验证	系统 CA 签名的 X.509 服务器证书或管理员提供的自定义服务器证书
客户端身份验证	• S3： S3 帐户（访问密钥 ID 和机密访问密钥） • Swift： Swift 帐户（用户名和密码）
客户端授权	• S3： 存储分段所有权和所有适用的访问控制策略 • Swift： 管理员角色访问

相关信息

管理 StorageGRID

支持 **TLS** 库的哈希和加密算法

StorageGRID 系统支持一组有限的密码套件，客户端应用程序可在建立传输层安全（ TLS ）会话时使用这些密码套件。

支持的 **TLS** 版本

StorageGRID 支持 TLS 1.2 和 TLS 1.3 。

不再支持 SSLv3 和 TLS 1.1 （或更早版本）。

支持的密码套件

TLS 版本	密码套件的 **IANA** 名称
1.2	tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384
tls_ECDHE_RSA_WIT_CHACHA20_POLY1305_SHA256	tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256
1.3	tls_aes_256_gcm_SHA384
tls_chacHA20_POLY1305_SHA256	tls_aes_128_gcm_SHA256

已弃用密码套件

以下密码套件已弃用。未来版本将删除对这些密码的支持。

IANA 名称
tls_rsa_and_aes_128_gcm_SHA256
tls_rsa_and_aes_256_gcm_SHA384

相关信息

配置租户帐户和连接

监控和审核操作

您可以通过查看整个网格或特定节点的事务趋势来监控客户端操作的工作负载和效率。您可以使用审核消息监控客户端操作和事务。

监控对象载入和检索速率

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

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 在信息板上，找到协议操作部分。

   本节总结了 StorageGRID 系统执行的客户端操作的数量。协议速率是过去两分钟的平均值。

3. 选择 * 节点 * 。
4. 从节点主页（部署级别）中，单击 * 负载平衡器 * 选项卡。

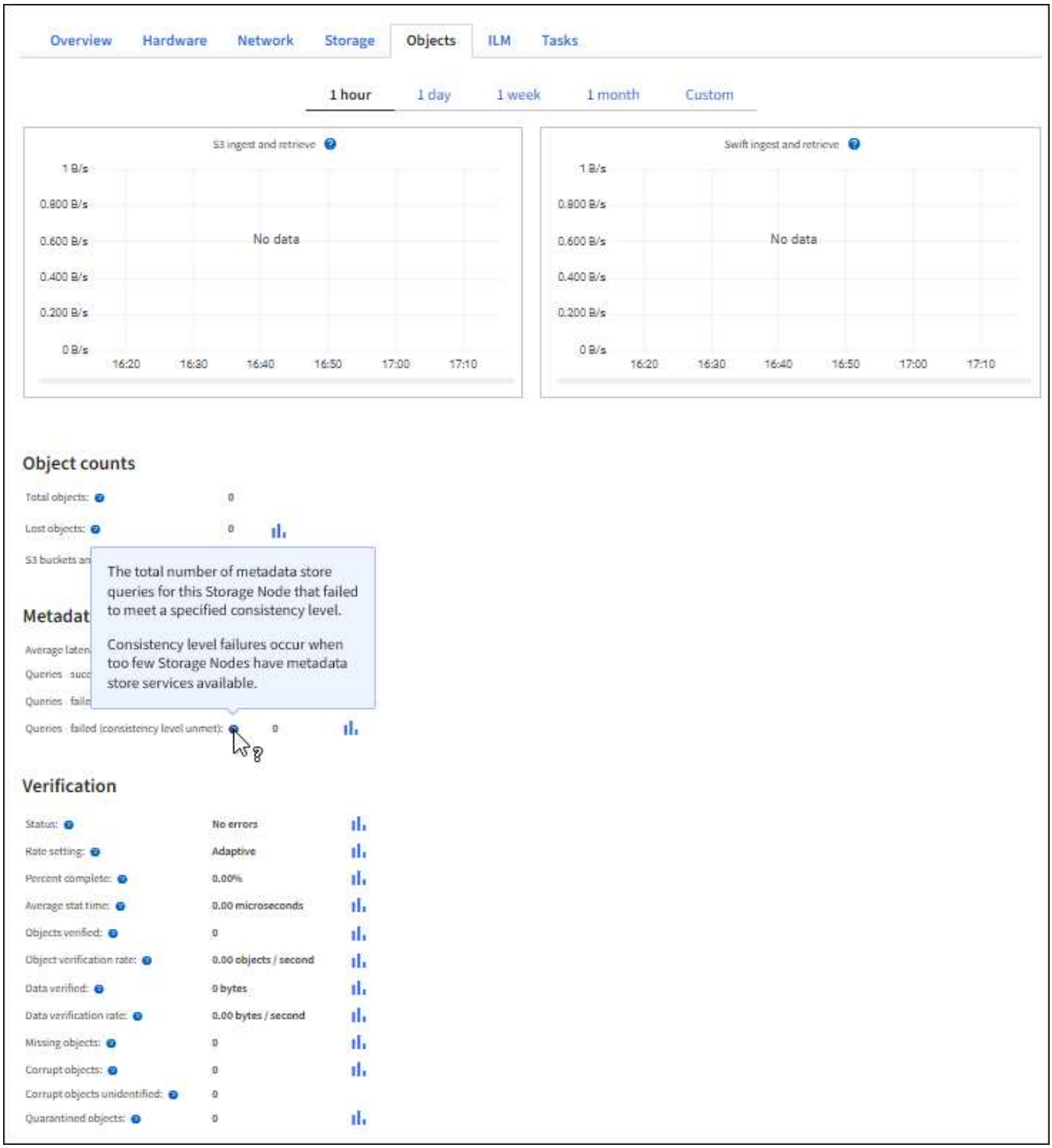
   这些图表显示了定向到网格中负载平衡器端点的所有客户端流量的趋势。您可以选择以小时，天，周，月或年为单位的时间间隔， 或者，您也可以应用自定义间隔。

5. 从节点主页（部署级别）中，单击 * 对象 * 选项卡。

   此图表显示了整个 StorageGRID 系统的载入和检索速率，以每秒字节数和总字节数为单位。您可以选择以小时，天，周，月或年为单位的时间间隔， 或者，您也可以应用自定义间隔。

6. 要查看特定存储节点的信息，请从左侧列表中选择该节点，然后单击 * 对象 * 选项卡。

   此图表显示了此存储节点的对象载入速率和检索速率。此选项卡还包括对象计数，查询和验证的指标。您可以单击这些标签以查看这些指标的定义。



7. 如果您需要更多详细信息：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 概述 * > * 主要 * 。

      API Operations 部分显示整个网格的摘要信息。

   c. 选择 * 存储节点 _* > * LDR* > * 客户端应用程序 _* > * 概述 * > * 主 *

      操作部分显示选定存储节点的摘要信息。

访问和查看审核日志

审核消息由 StorageGRID 服务生成并存储在文本日志文件中。审核日志中特定于 API 的审核消息提供关键的安全性，操作和性能监控数据，可帮助您评估系统的运行状况。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。
- 您必须知道管理节点的 IP 地址。

关于此任务

活动审核日志文件名为 `audit.log` ，并存储在管理节点上。

每天保存一次活动的 audit.log 文件，并启动一个新的 audit.log 文件。已保存文件的名称以 `yyyy-mm-dd.txt` 格式指示其保存时间。

一天之后，保存的文件将被压缩并重命名，格式为 `yyyy-mm-dd.txt.gz` ，从而保留原始日期。

此示例显示了活动的 audit.log 文件，前一天的文件（ 2018-04-15.txt ）以及前一天的压缩文件（`2018-04-14.txt.gz` ）。

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

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 转到包含审核日志文件的目录：`cd /var/local/audit/export`
3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

相关信息

查看审核日志

审核日志中跟踪的 **Swift** 操作

所有成功的存储删除， GET ， HEAD ， POST 和 PUT 操作都会在 StorageGRID 审核日志中进行跟踪。不会记录故障，也不会记录信息，身份验证或选项请求。

有关为以下 Swift 操作跟踪的信息的详细信息，请参见 _ 了解审核消息 _ 。

帐户操作

- 获取帐户

- 主帐户

容器操作

- 删除容器
- 获取容器
- 机头容器
- 放入容器

对象操作

- 删除对象
- 获取对象
- head 对象
- PUT 对象

相关信息

查看审核日志

帐户操作

容器操作

对象操作

监控和维护 StorageGRID

监控和故障排除

监控和故障排除：概述

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

关于这些说明

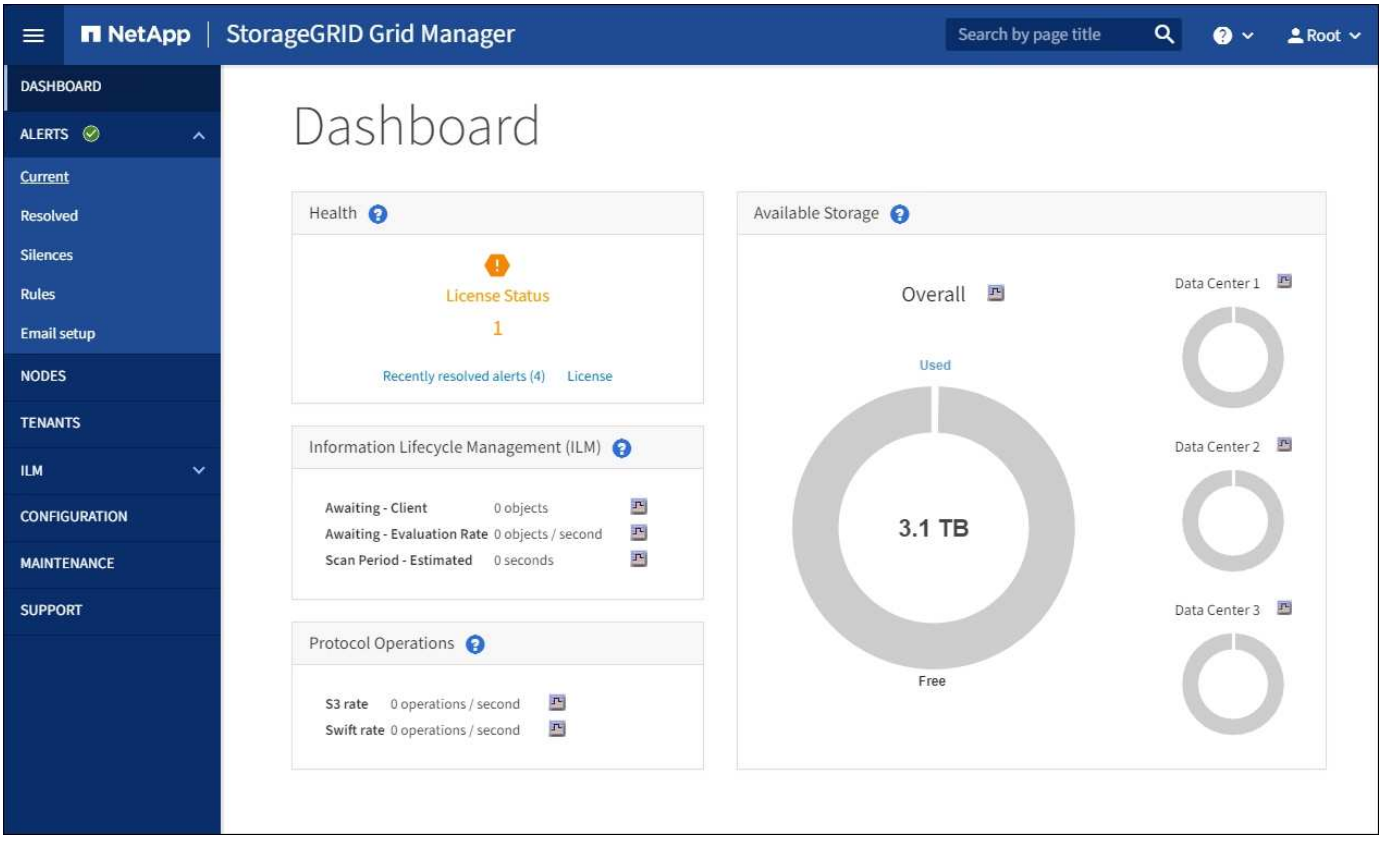
以下说明介绍如何使用网格管理器监控 StorageGRID 系统。您将了解应定期监控哪些信息，如何管理警报和旧警报，如何使用 SNMP 进行监控以及如何获取其他 StorageGRID 数据，包括指标和诊断。

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

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

查看信息板

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



搜索字段

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

钥 * 以访问密钥管理服务器页面。

运行状况面板

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

可用存储面板

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

信息生命周期管理（ **ILM** ）面板

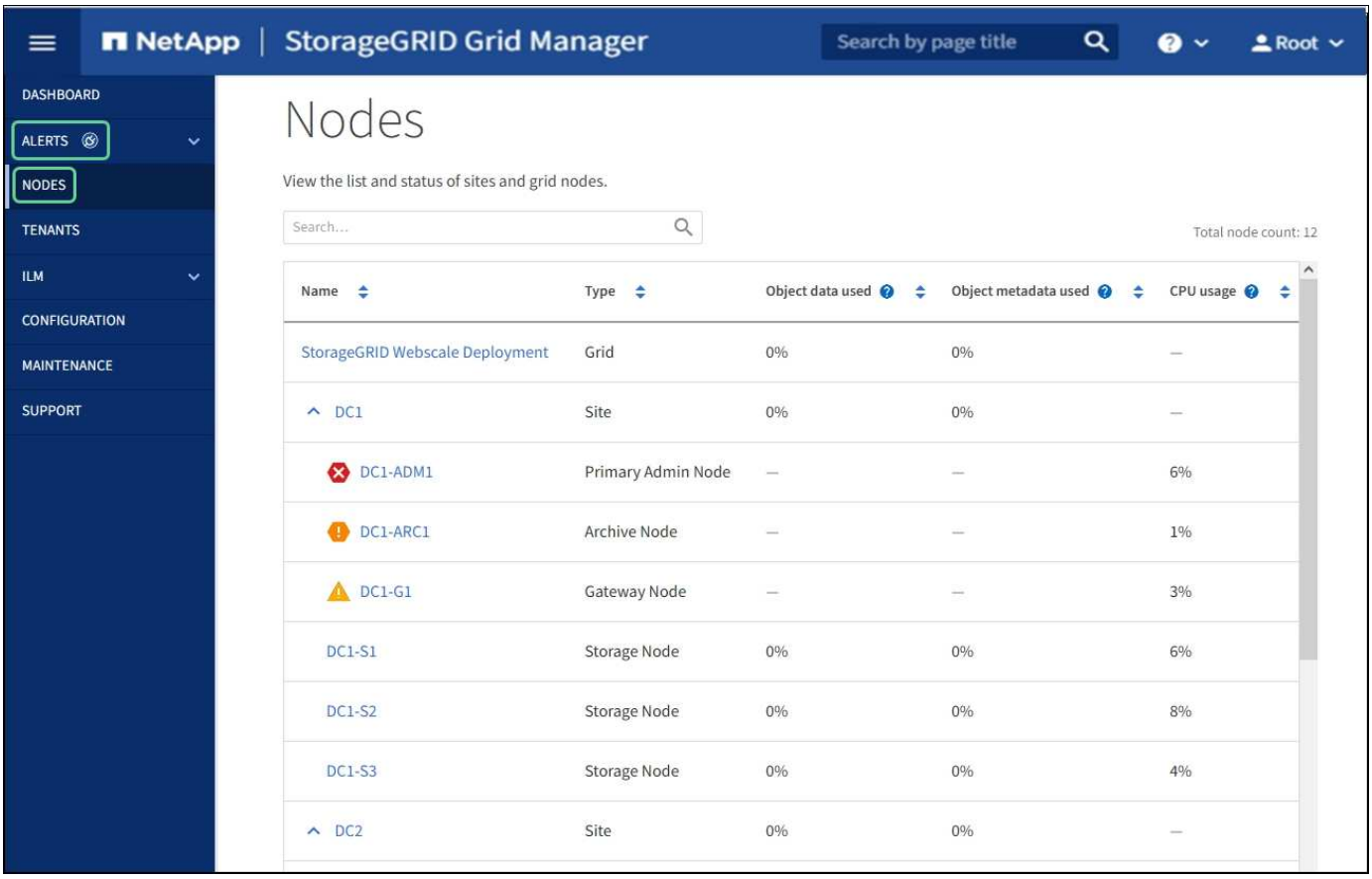
Description	查看其他详细信息	了解更多信息。
显示系统的当前 ILM 操作和 ILM 队列。您可以使用此信息监控系统的工作负载。 • * 正在等待 - 客户端 * ： 等待通过客户端操作（例如载入）进行 ILM 评估的对象总数。 • * 等待 - 评估速率 * ： 根据网格中的 ILM 策略评估对象的当前速率。 • * 扫描期间 - 估计 * ： 完成对所有对象的完整 ILM 扫描的估计时间。* 注意： * 完全扫描并不能保证 ILM 已应用于所有对象。	• 要查看详细信息，请选择 * 节点 * 。然后，查看整个网格，整个站点或单个存储节点的 ILM 选项卡。 • 要查看现有 ILM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

协议操作面板

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

查看节点页面

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



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

连接状态图标

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

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

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

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

警报图标

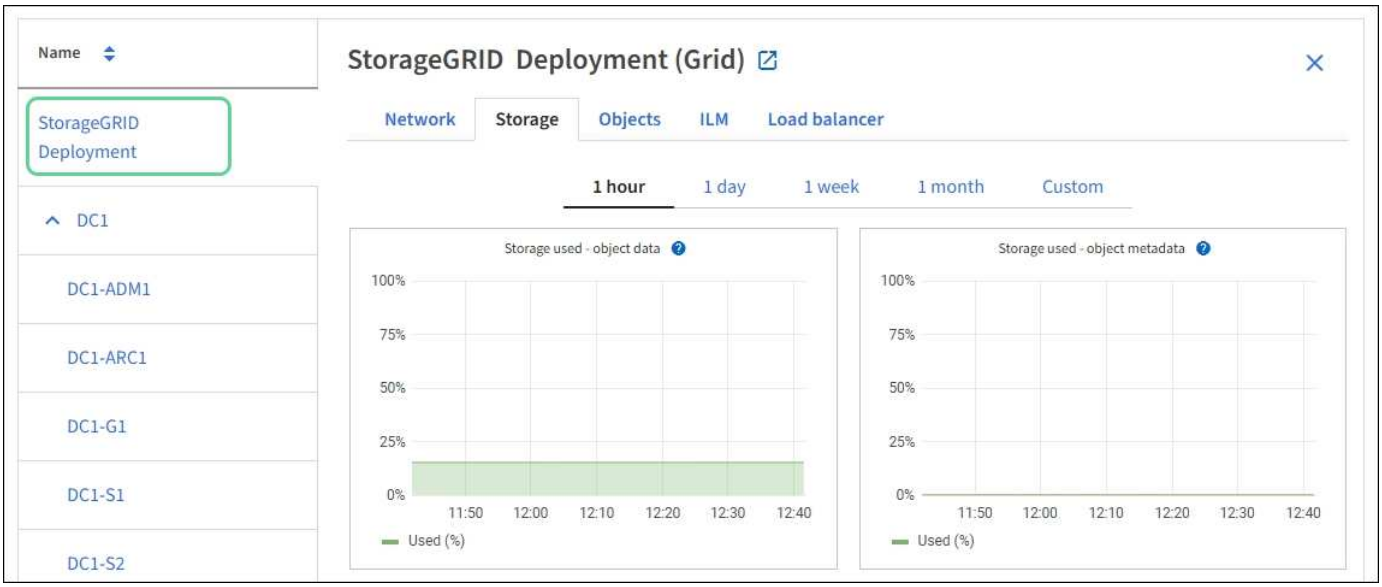
如果节点存在活动警报，则节点名称旁边会显示以下图标之一：

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

查看系统，站点或节点的详细信息

要查看可用信息，请按如下所示选择网格，站点或节点的名称：

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



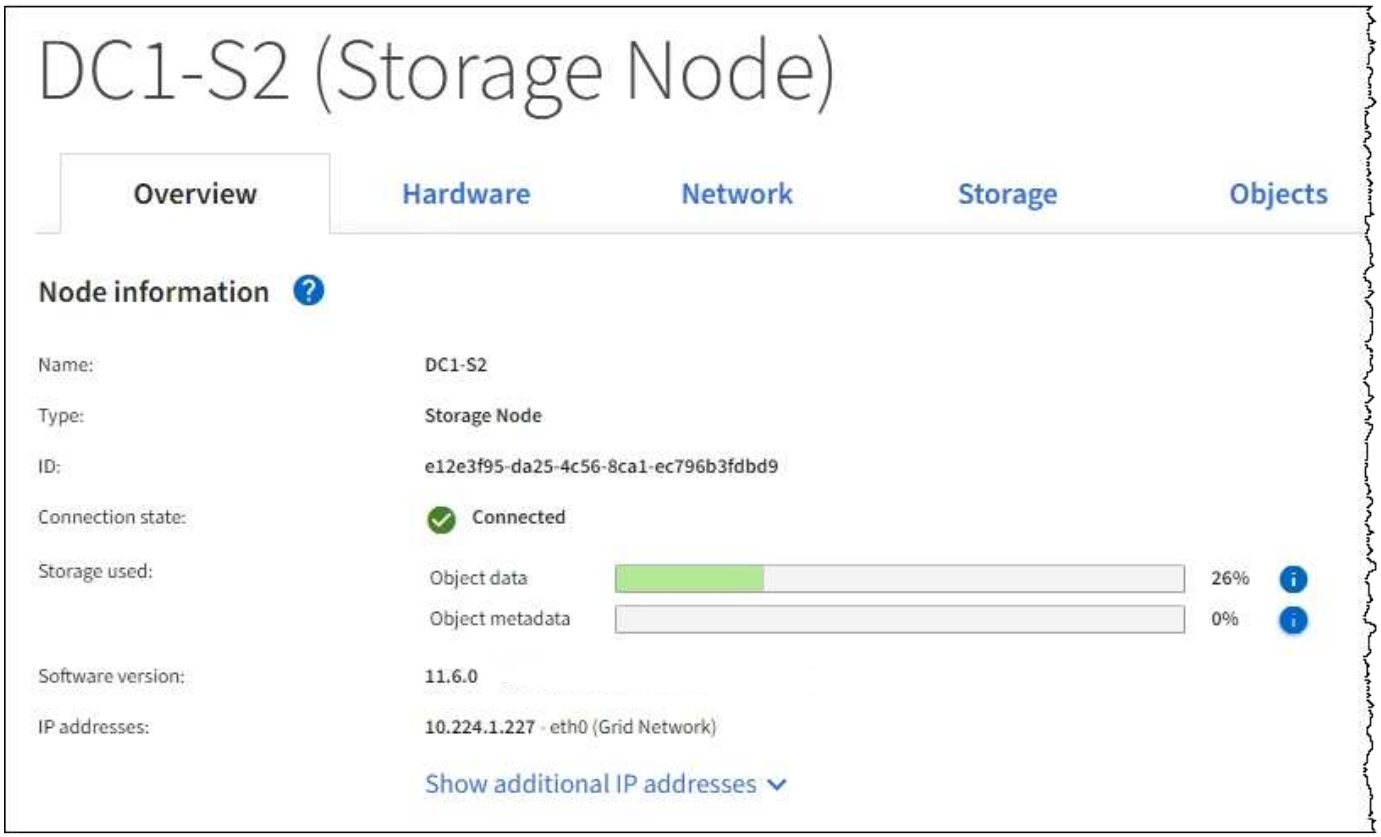
查看概述选项卡

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

此时将显示所有节点的概述选项卡。

节点信息

概述选项卡的节点信息部分列出了有关网格节点的基本信息。



节点的概述信息包括：

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

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

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

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

警报

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

相关信息

监控节点连接状态

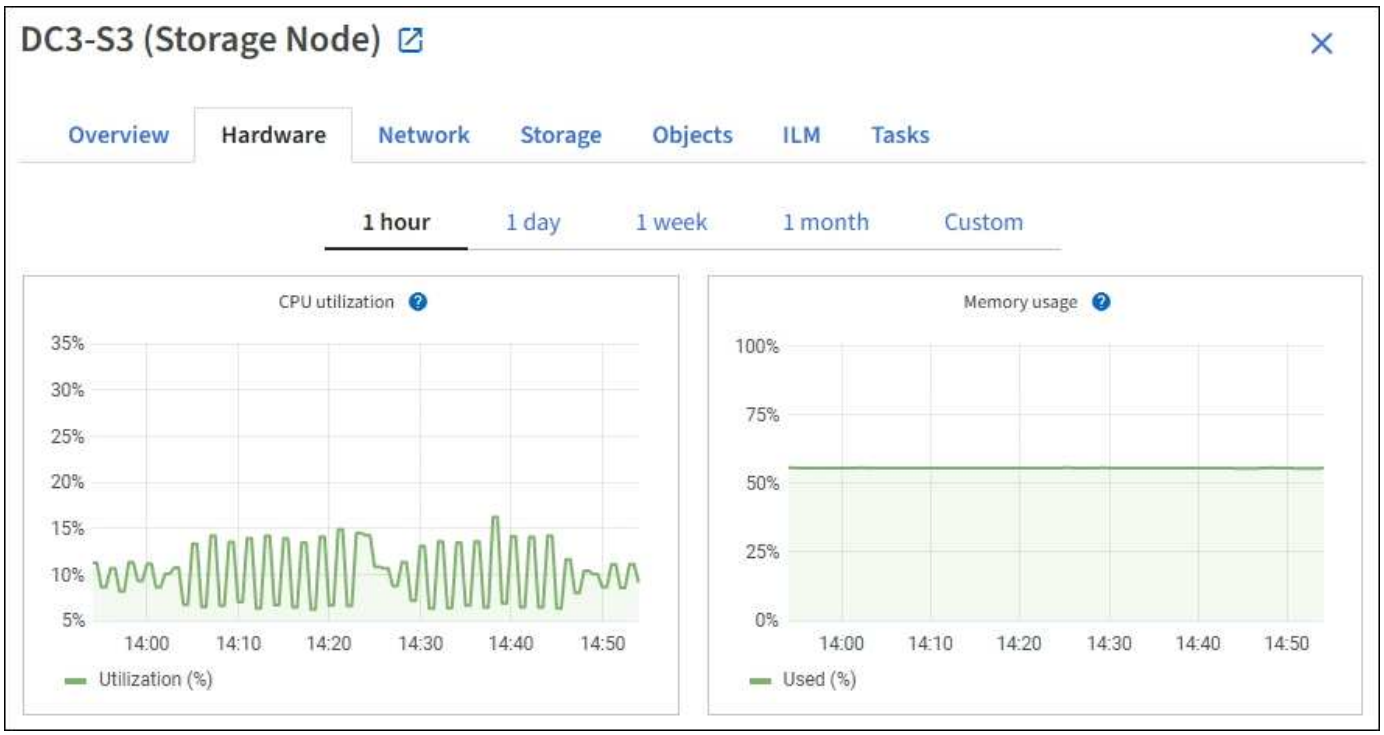
查看当前警报

查看特定警报

查看硬件选项卡

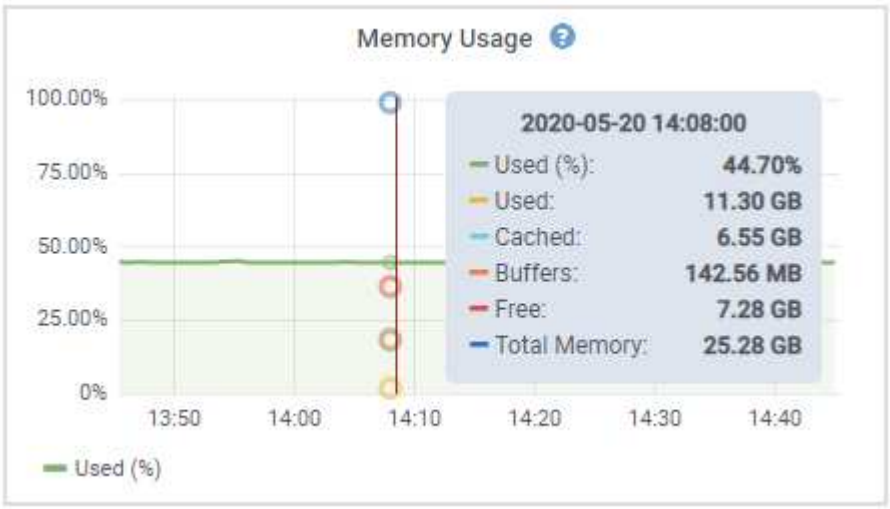
硬件选项卡可显示每个节点的 CPU 利用率和内存使用情况，以及有关设备的其他硬件信息。

此时将显示所有节点的硬件选项卡。



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

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



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

查看有关设备存储节点的信息

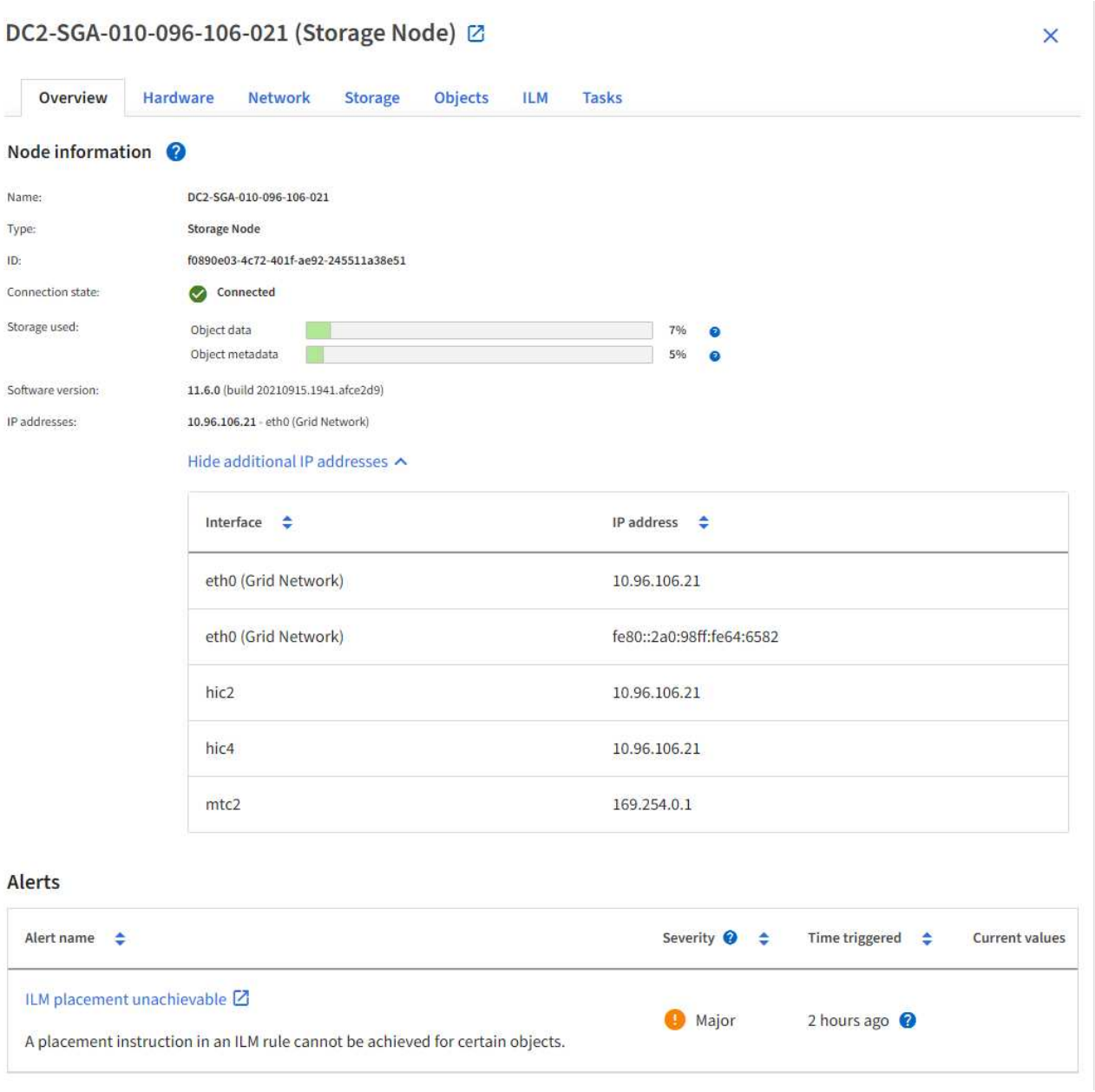
节点页面列出了有关每个设备存储节点的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，控制器固件版本，网络资源，网络接口， 网络地址以及接收和传输数据。

步骤

1. 从节点页面中，选择设备存储节点。
2. 选择 * 概述 * 。

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

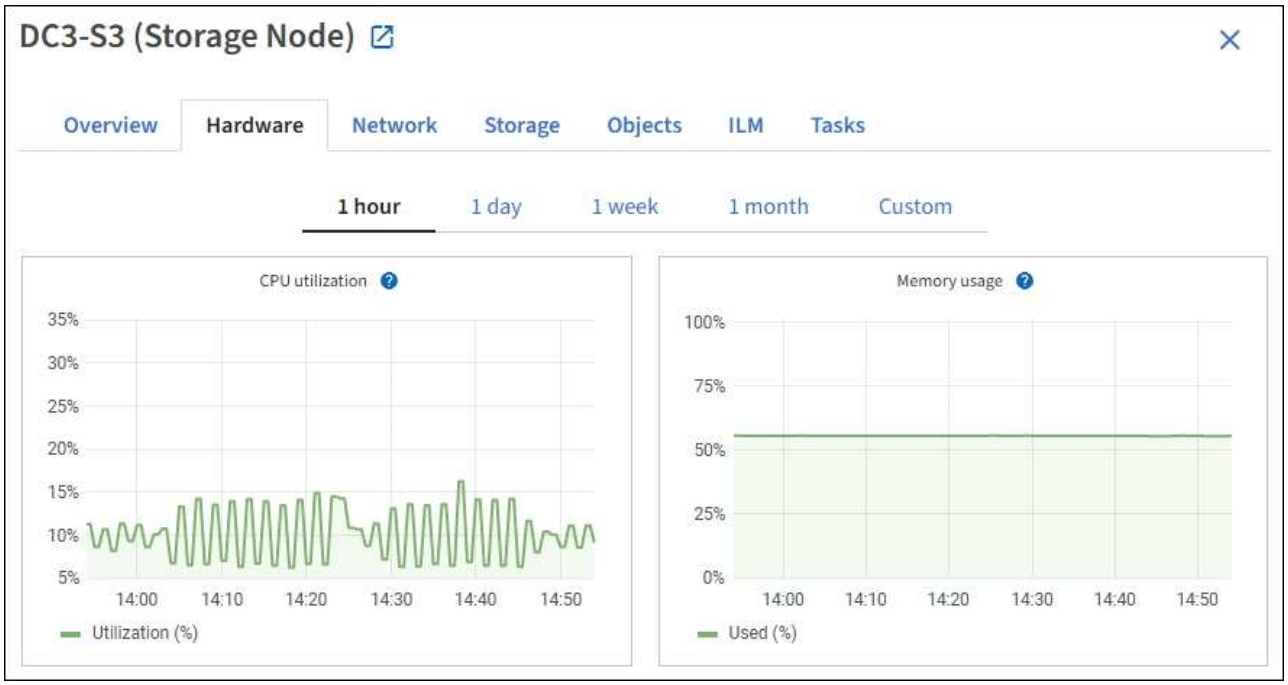
   - * eth * ： 网格网络，管理网络或客户端网络。
   - * hic* ： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
   - * MTC* ： 设备上的一个物理 1 GbE 端口。一个或多个 MTC 接口已绑定，以构成 StorageGRID 管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。



" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

3. 选择 * 硬件 * 可查看有关此设备的详细信息。

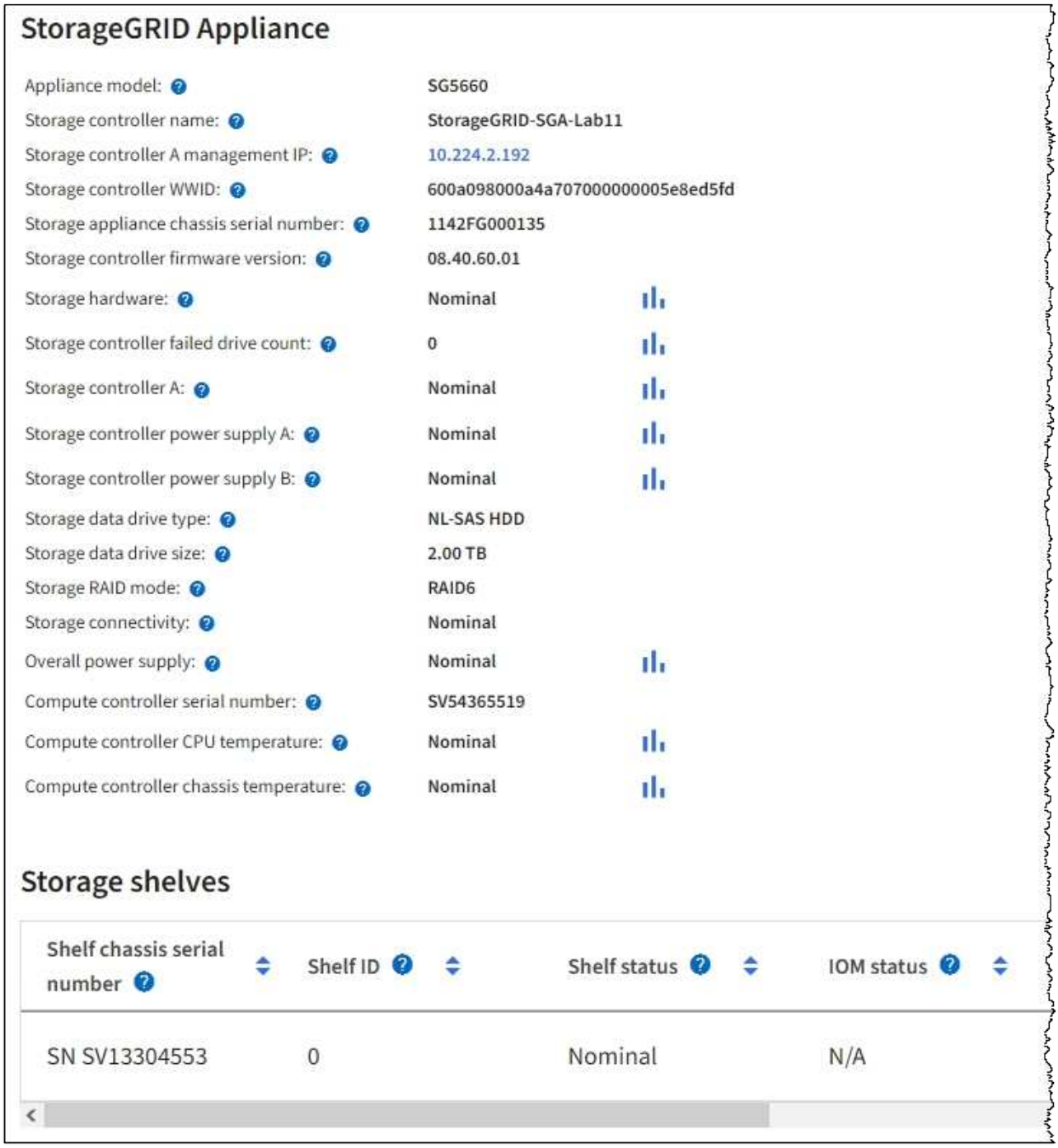
   a. 查看 CPU 利用率和内存图形，确定 CPU 和内存使用量随时间的变化所占百分比。要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。



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

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

存储架和扩展架（如果是安装的一部分）的组件会显示在设备表下方的单独表中。



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

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

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

+

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

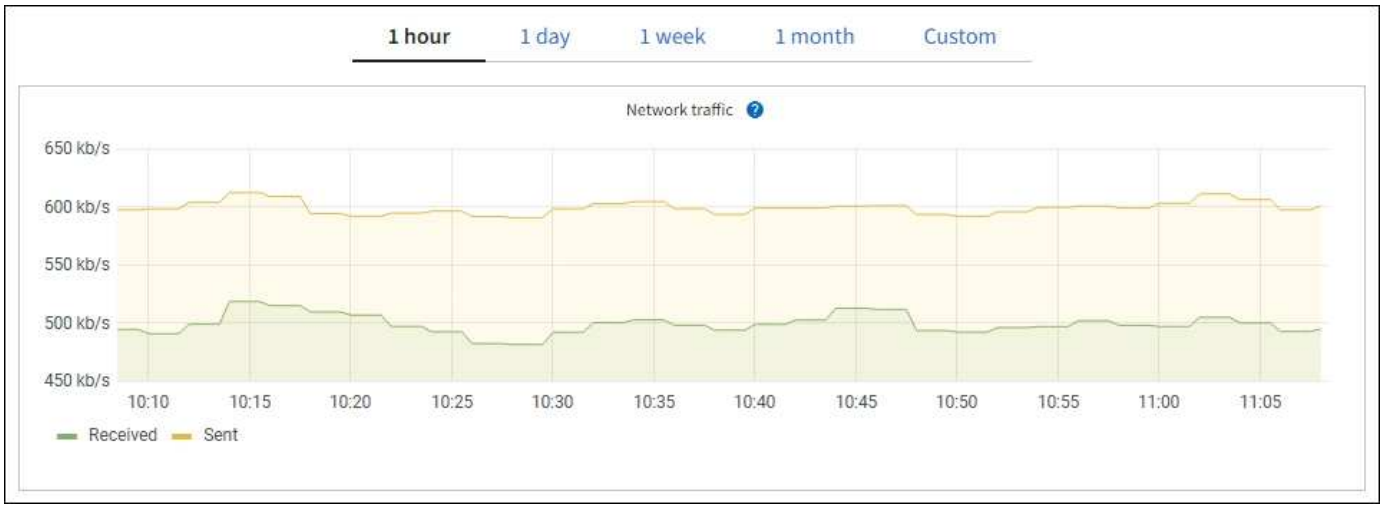
存储架表中的列	Description
【磁盘架数据驱动器大小】数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储架中用作缓存的驱动器数量。
缓存驱动器大小	存储架中最小缓存驱动器的大小。通常，缓存驱动器的大小相同。
配置状态	存储架的配置状态。

4. 确认所有状态均为 "`标称值。` "

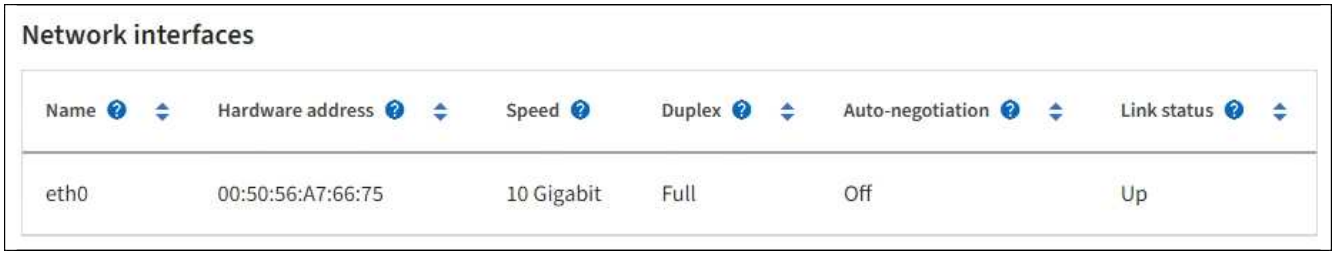
   如果状态不是 "`标称，` " ，请查看任何当前警报。您还可以使用 SANtricity 系统管理器详细了解其中一些硬件值。请参见有关安装和维护设备的说明。

5. 选择 * 网络 * 可查看每个网络的信息。

网络流量图提供了整体网络流量的摘要。



1. 查看网络接口部分。



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

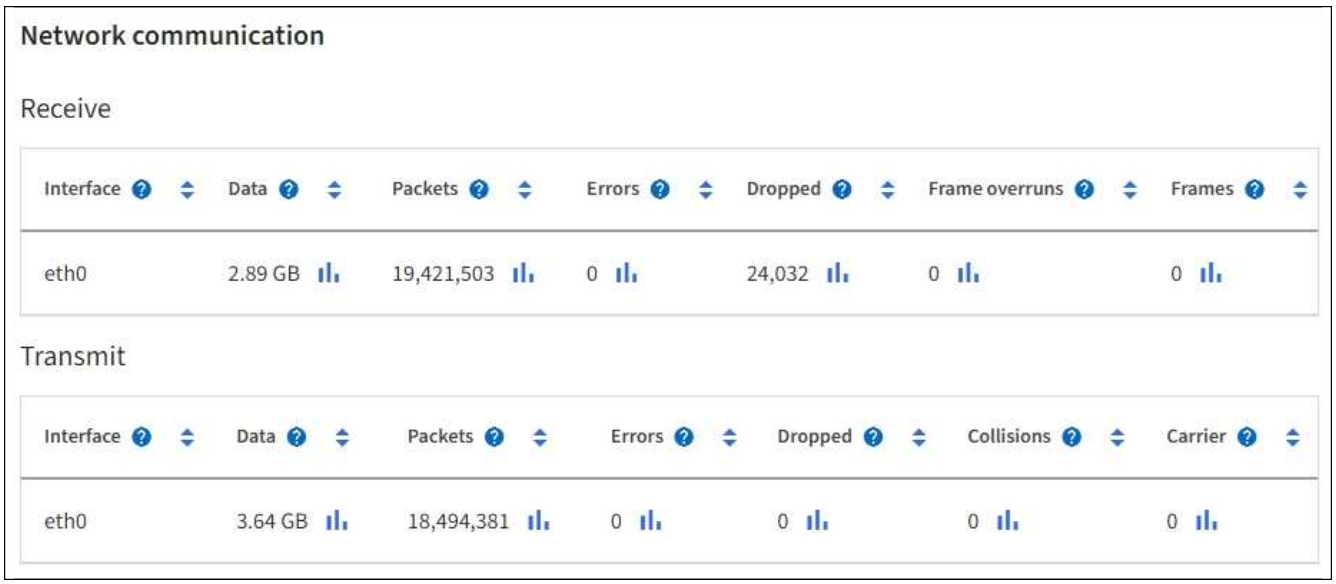
表中显示的值假定使用了所有四个链路。

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

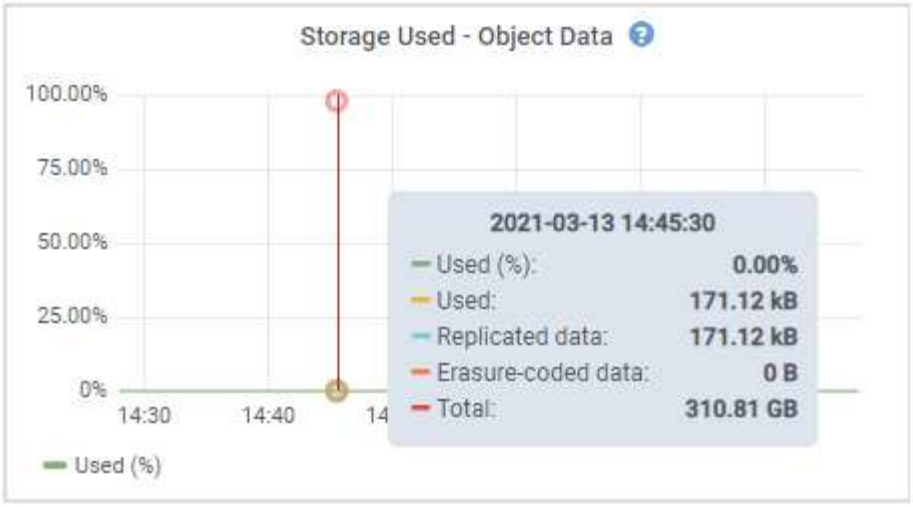
有关配置 10/225-GbE 端口的详细信息，请参见设备的安装和维护说明。

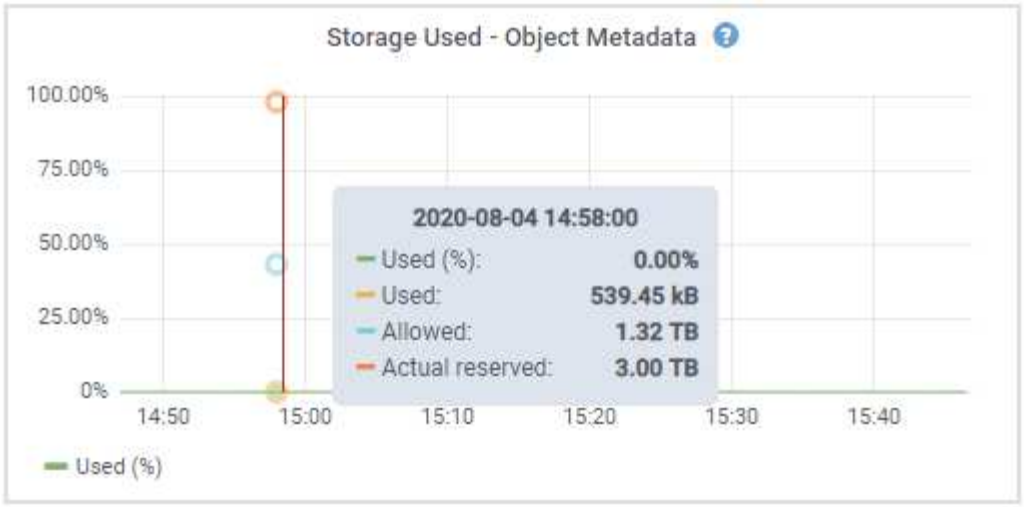
2. 查看网络通信部分。

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



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

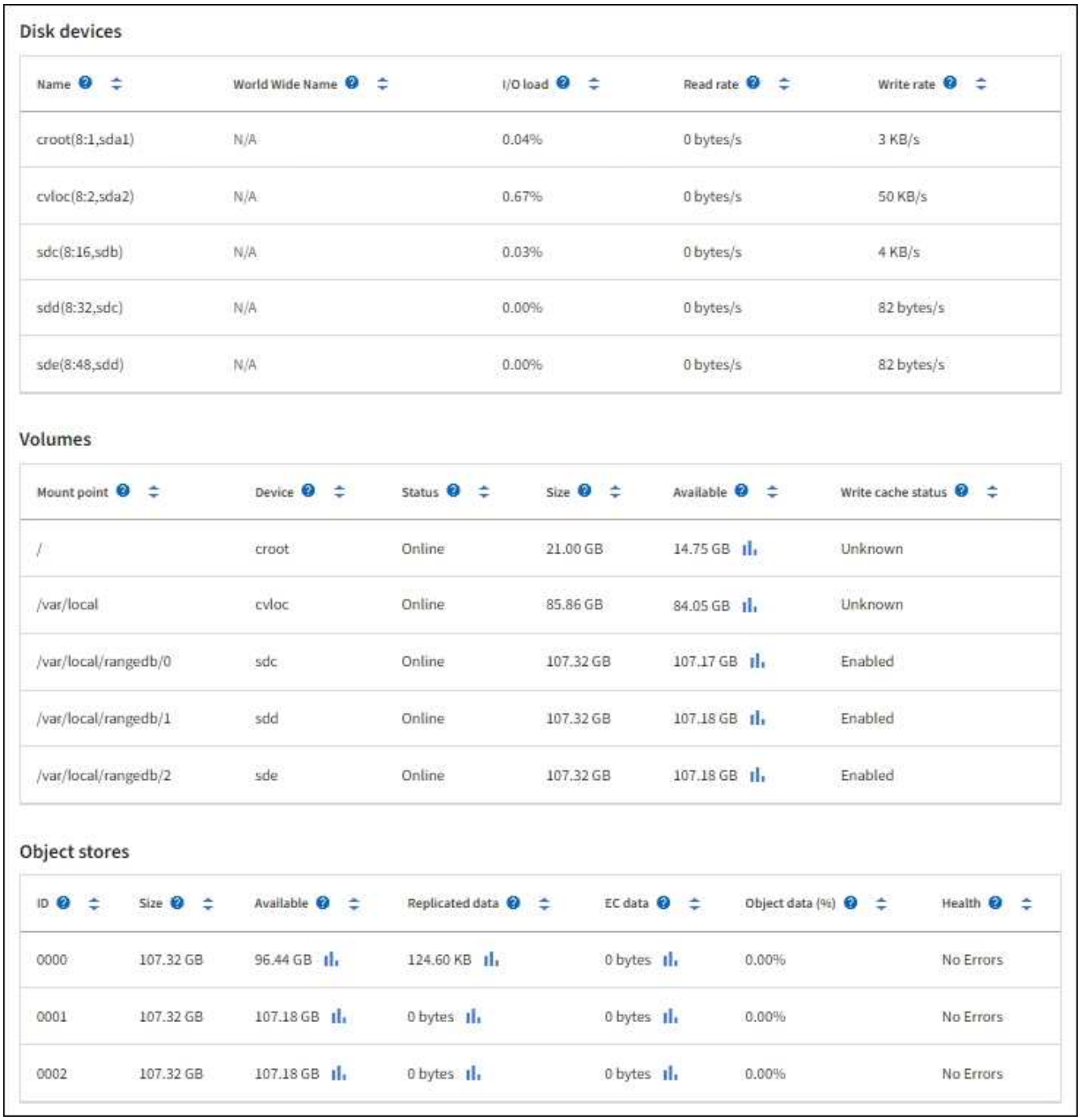




a. 向下滚动以查看每个卷和对象存储的可用存储容量。

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

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



Disk devices

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

Volumes

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

Object stores

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

相关信息

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

查看有关设备管理节点和网关节点的信息

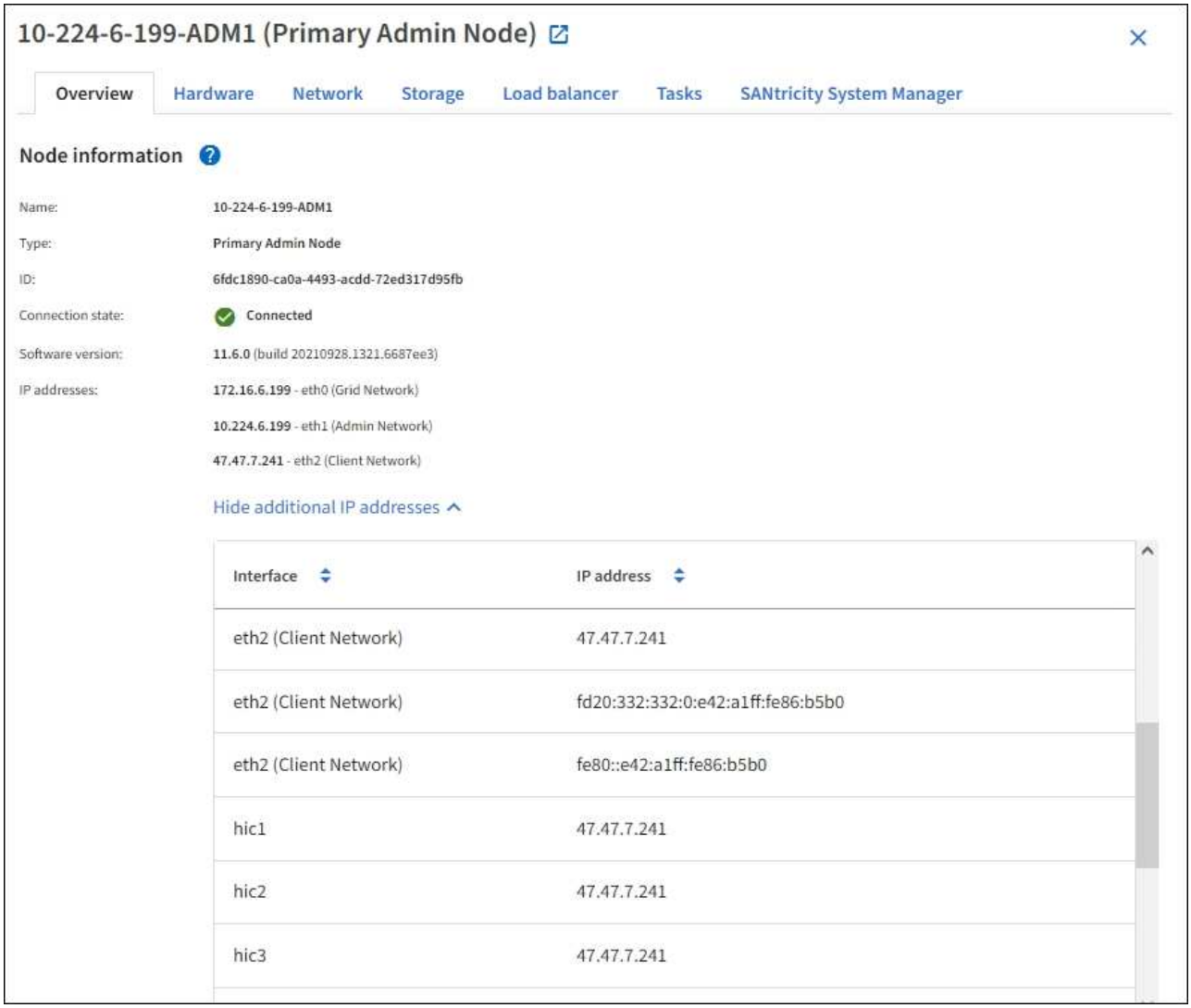
节点页面列出了有关用作管理节点或网关节点的每个服务设备的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，网络资源，网络接口，网络地址， 以及接收和传输数据。

步骤

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

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

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

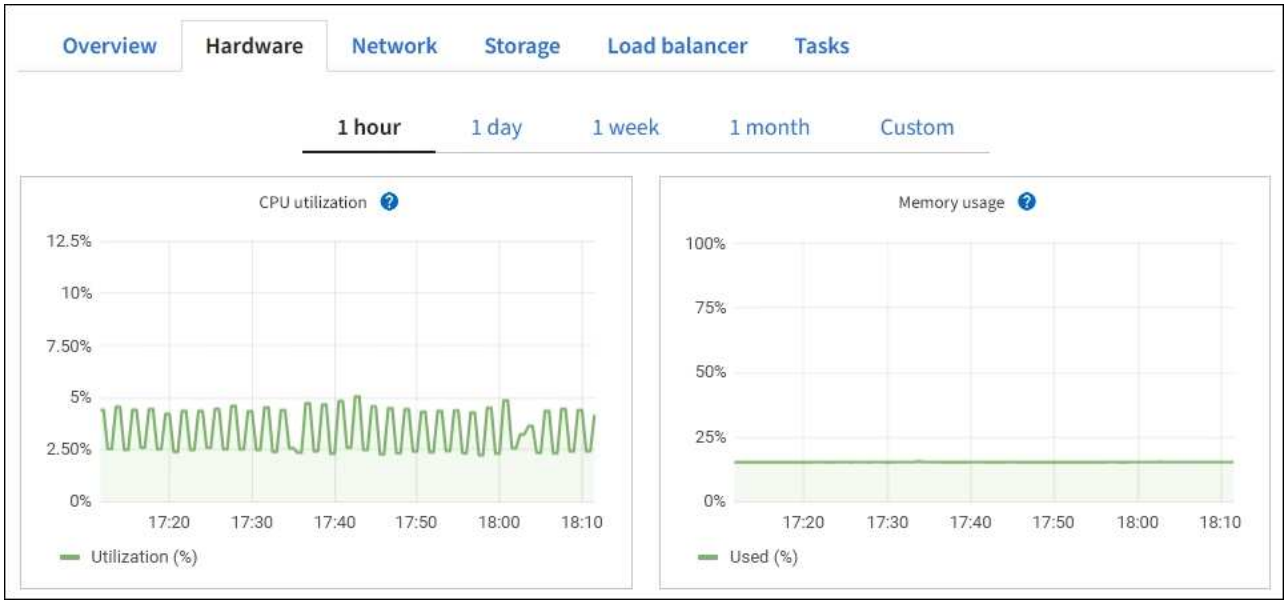


   " 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

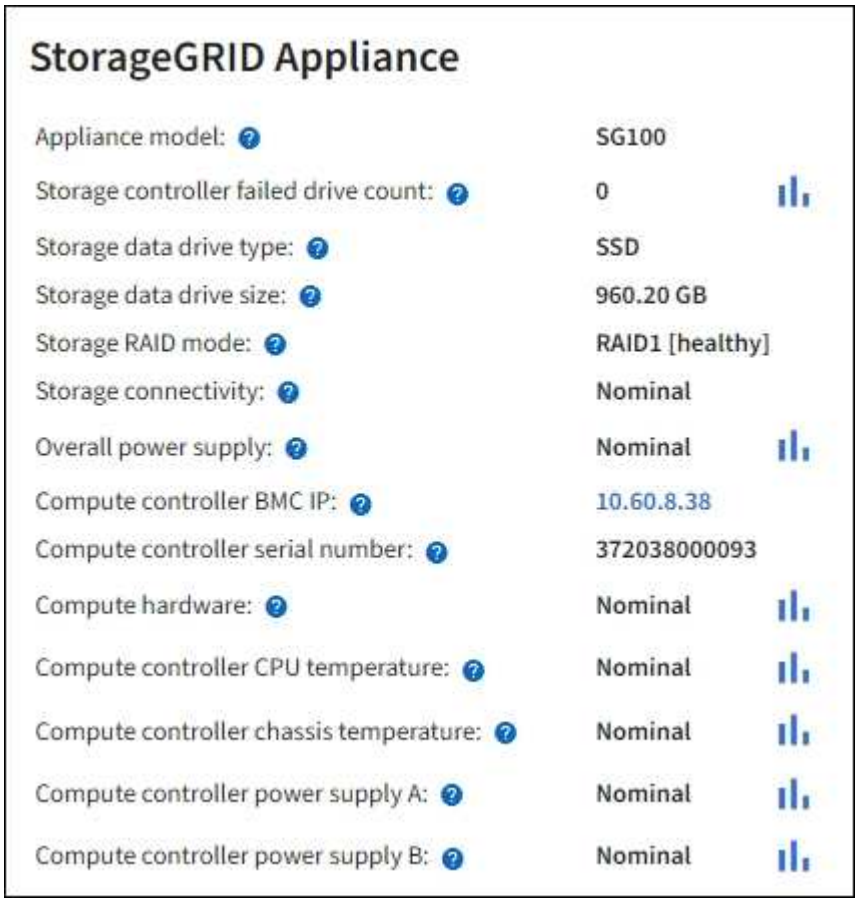
3. 选择 * 硬件 * 可查看有关此设备的详细信息。

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

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



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



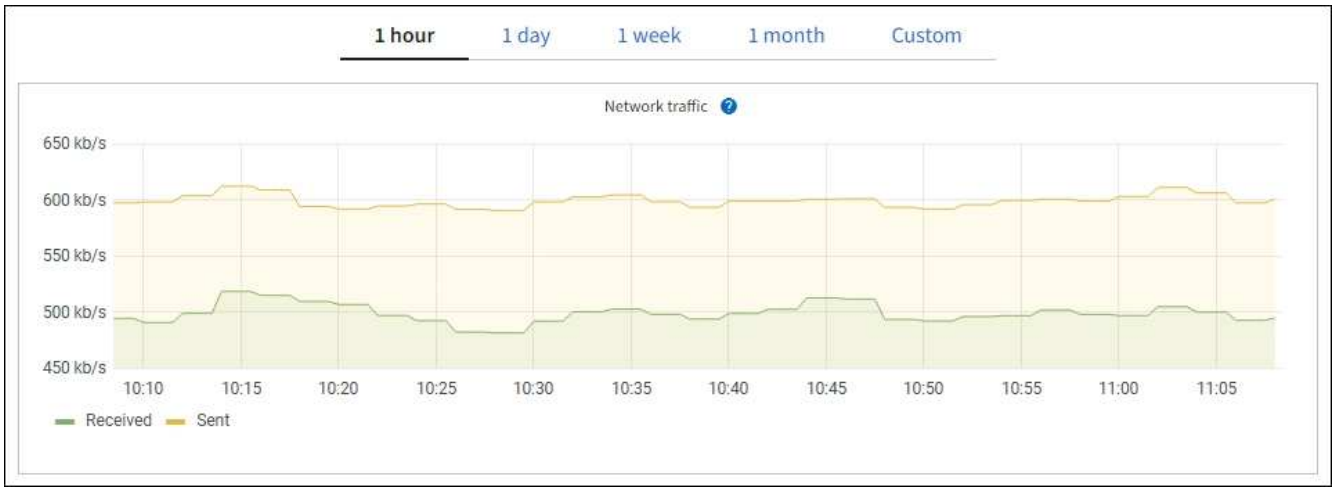
字段	Description
设备型号	此 StorageGRID 设备的型号。
存储控制器故障驱动器计数	非最佳驱动器的数量。
存储数据驱动器类型	设备中的驱动器类型，例如 HDD （硬盘驱动器）或 SSD （固态驱动器）。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller ， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含 BMC 的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

a. 确认所有状态均为 "`标称值。` "

如果状态不是 "`标称，` " ，请查看任何当前警报。

4. 选择 * 网络 * 可查看每个网络的信息。

网络流量图提供了整体网络流量的摘要。



a. 查看网络接口部分。

Network interfaces

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

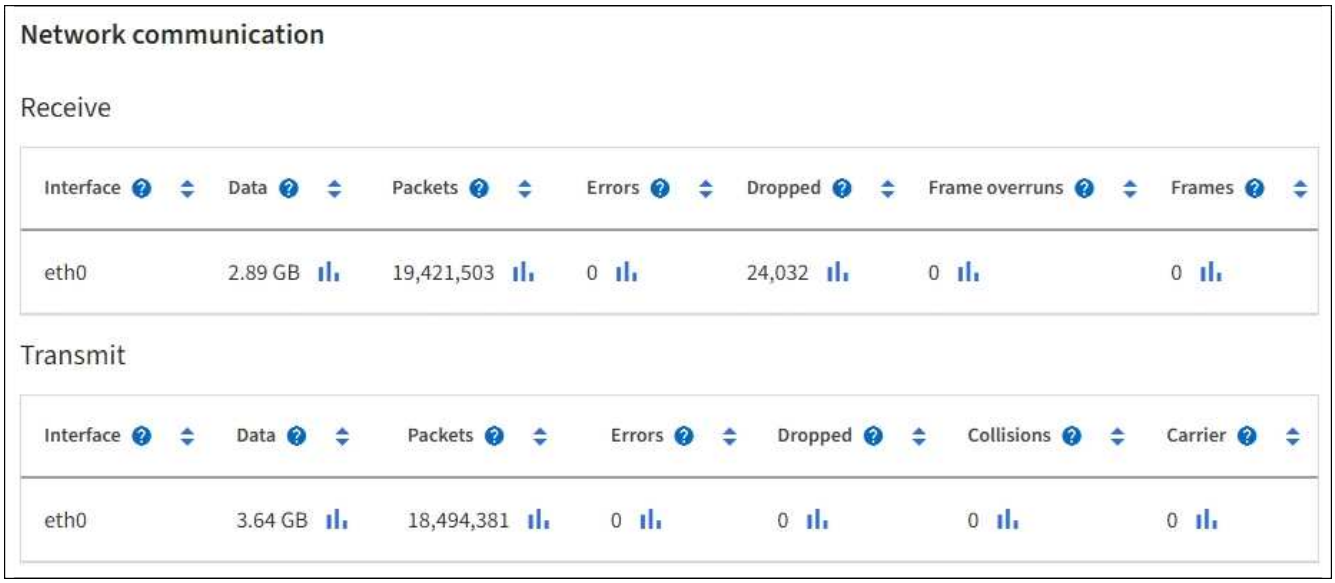
使用下表以及网络接口表中 * 速度 * 列中的值确定设备上的四个 40/100-GbE 网络端口是否配置为使用主动 / 备份模式或 LACP 模式。

表中显示的值假定使用了所有四个链路。

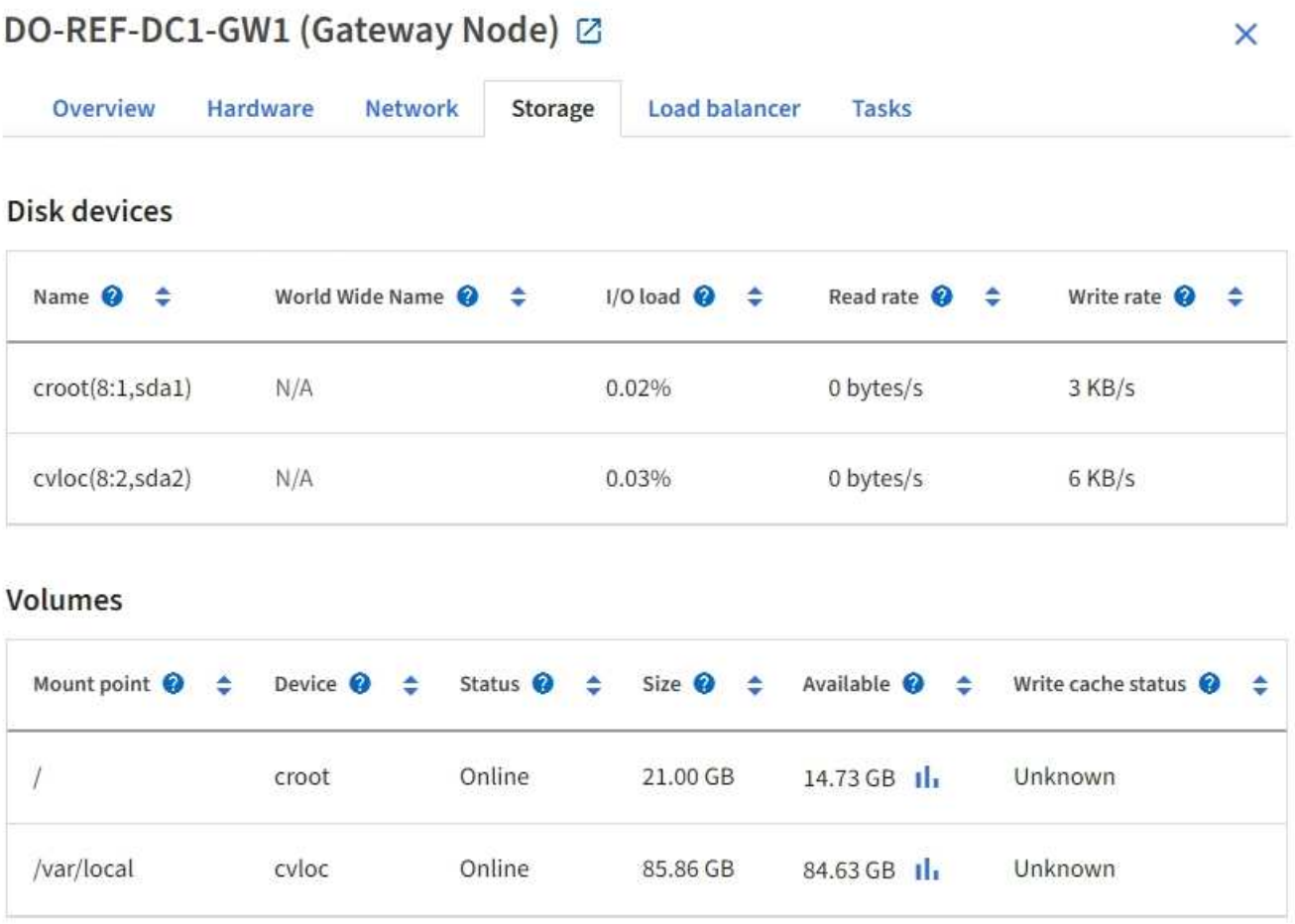
链路模式	绑定模式	单个 **HIC** 链路速度（ **hic1** ， **hic2** ， **hic3** ， **hic4** ）	预期网格 **/** 客户端网络速度（ **eth0** ， **eth2** ）
聚合	LACP	100	400
已修复	LACP	100	200
已修复	主动 / 备份	100	100
聚合	LACP	40	160
已修复	LACP	40	80
已修复	主动 / 备份	40	40

b. 查看网络通信部分。

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



5. 选择 * 存储 * 可查看有关服务设备上的磁盘设备和卷的信息。



相关信息

SG100 和 SG1000 服务设备

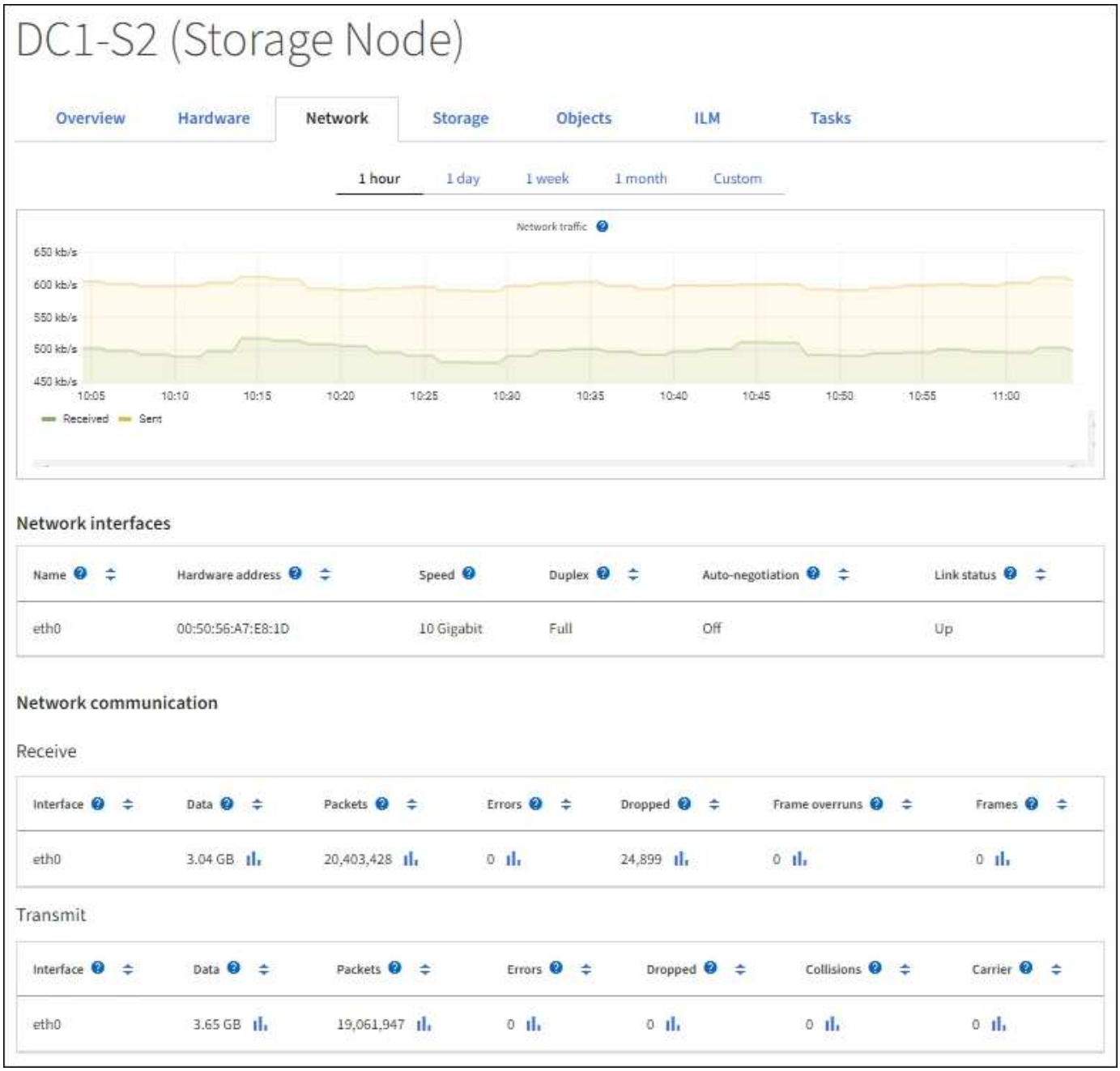
查看网络选项卡

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

此时将显示所有节点，每个站点和整个网格的网络选项卡。

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

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



相关信息

监控网络连接和性能

查看存储选项卡

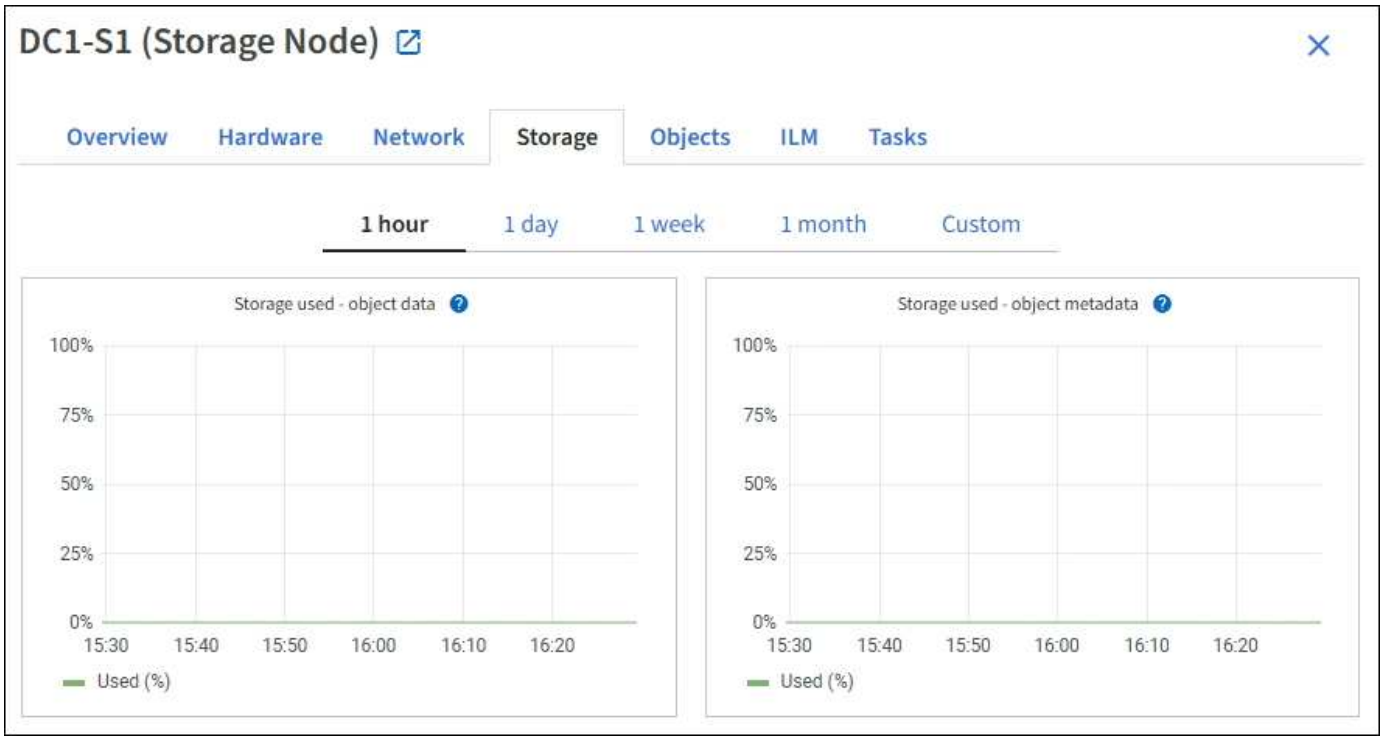
存储选项卡汇总了存储可用性和其他存储指标。

此时将显示所有节点，每个站点和整个网格的存储选项卡。

已用存储图

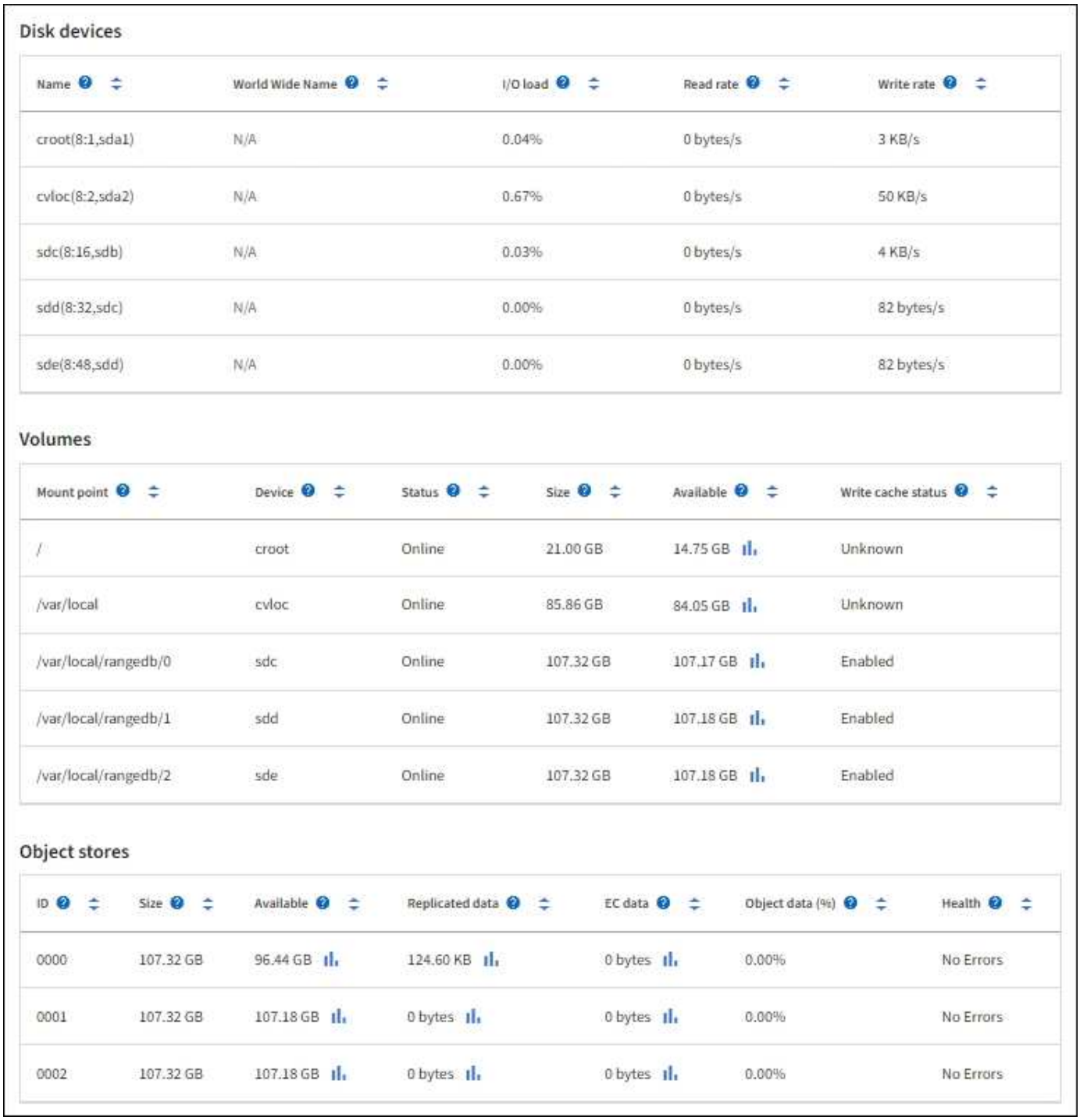
对于存储节点，每个站点和整个网格， " 存储 " 选项卡包含一些图形，用于显示对象数据和对象元数据在一段时间内使用了多少存储。

站点或网格的总值不包括至少在五分钟内未报告指标的节点，例如脱机节点。



磁盘设备，卷和对象存储表

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



Disk devices

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

Volumes

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

Object stores

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

相关信息

监控存储容量

使用任务选项卡重新启动网格节点

通过任务选项卡，您可以重新启动选定节点。此时将显示所有节点的任务选项卡。

您需要的内容

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

- 您具有配置密码短语。

关于此任务

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

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

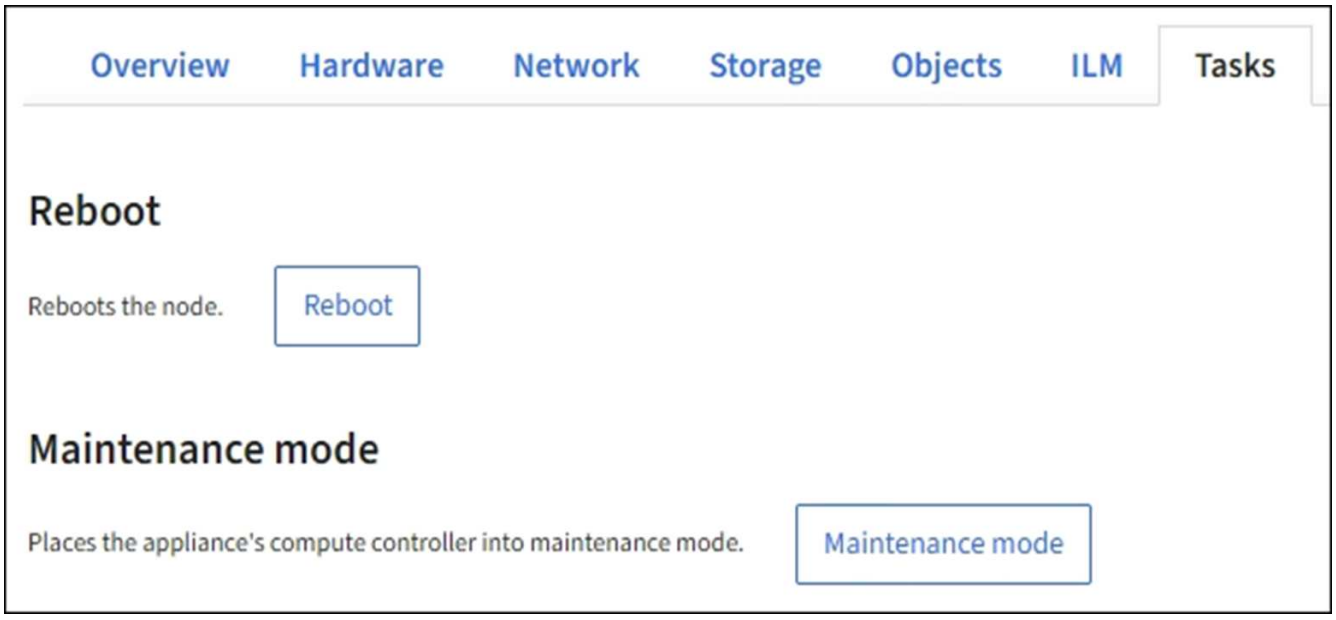
  如果您计划重新启动存储节点，请注意以下事项：

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

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

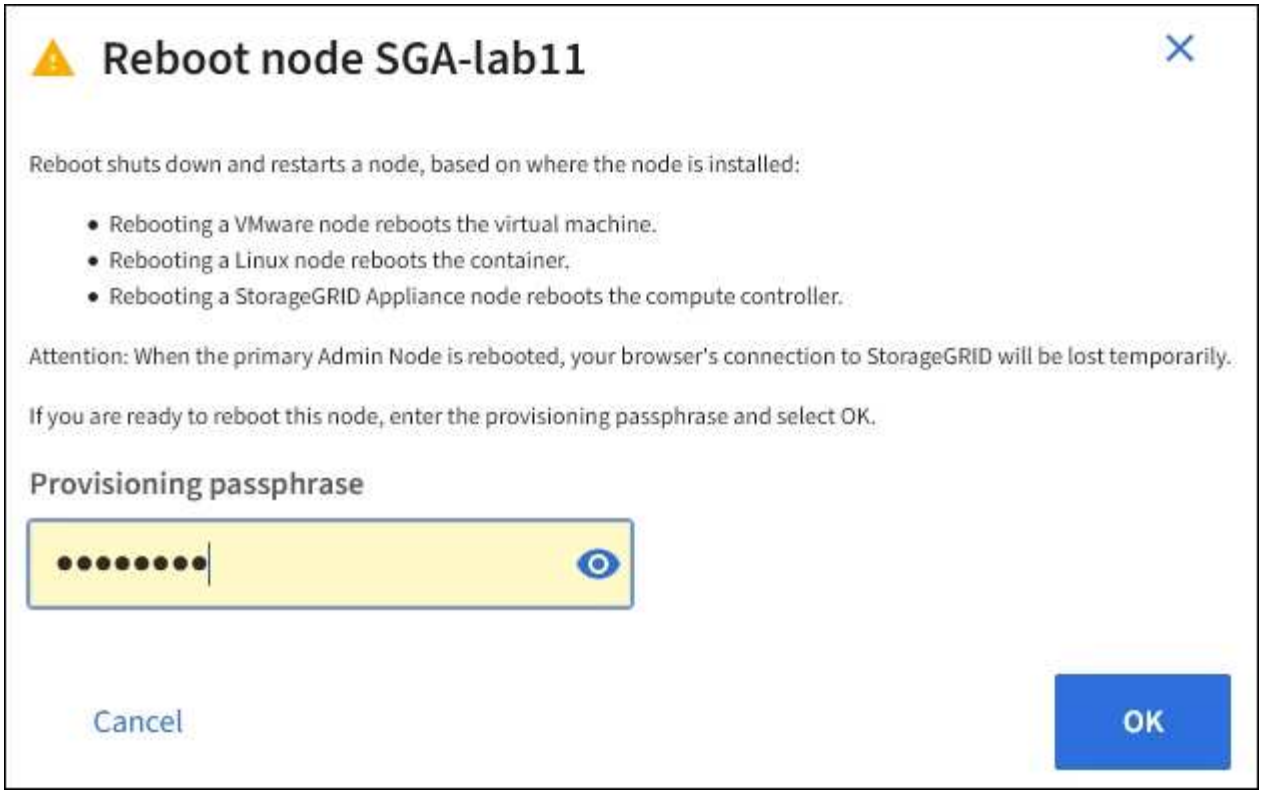
步骤

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



4. 选择 * 重新启动 * 。

   此时将显示确认对话框。



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

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

   关闭服务可能需要一些时间。

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

相关信息

SG6000 存储设备

SG5700 存储设备

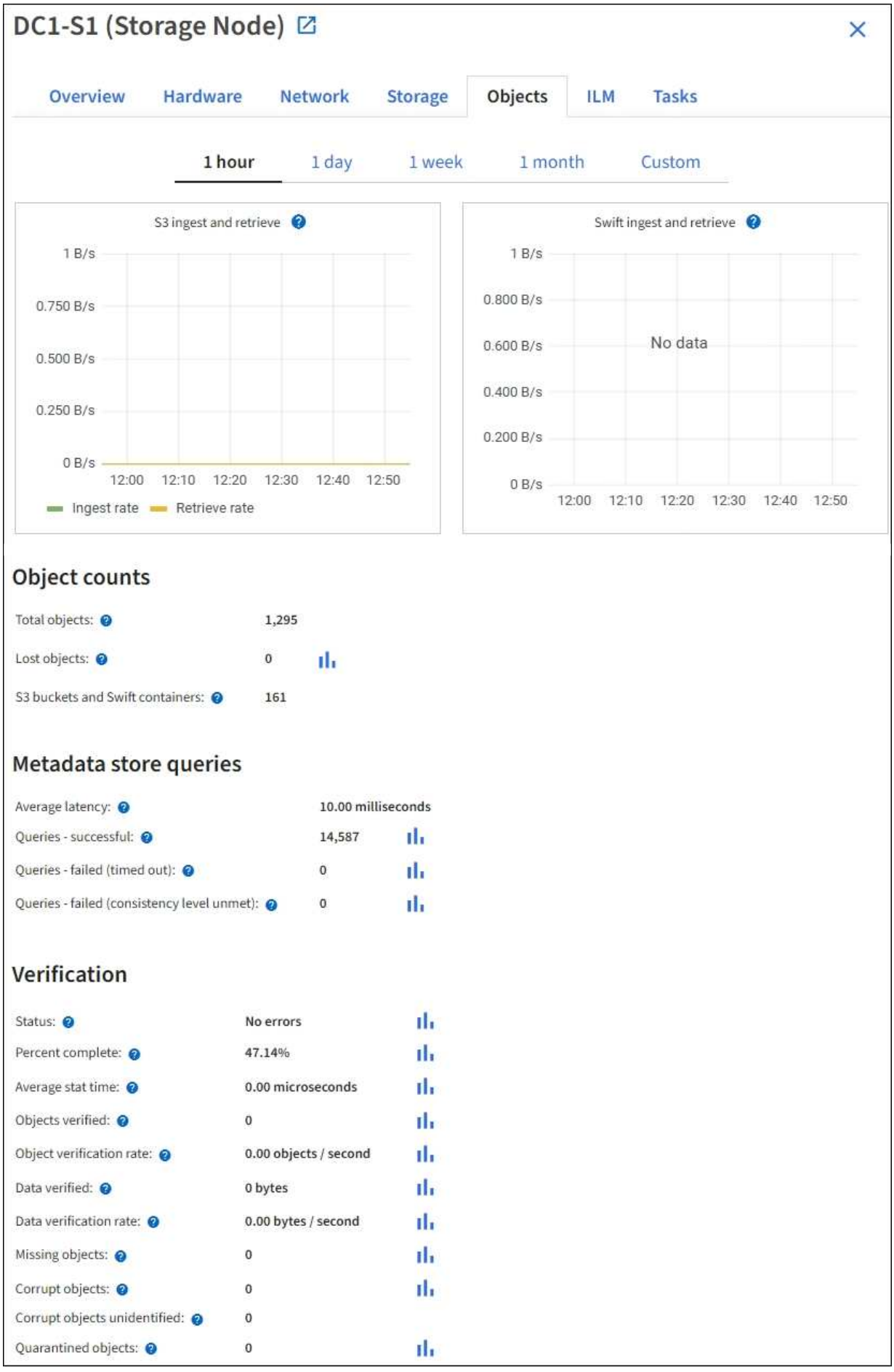
SG5600 存储设备

SG100 和 SG1000 服务设备

查看对象选项卡

对象选项卡提供了有关的信息 S3 和 Swift 载入和检索速率。

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

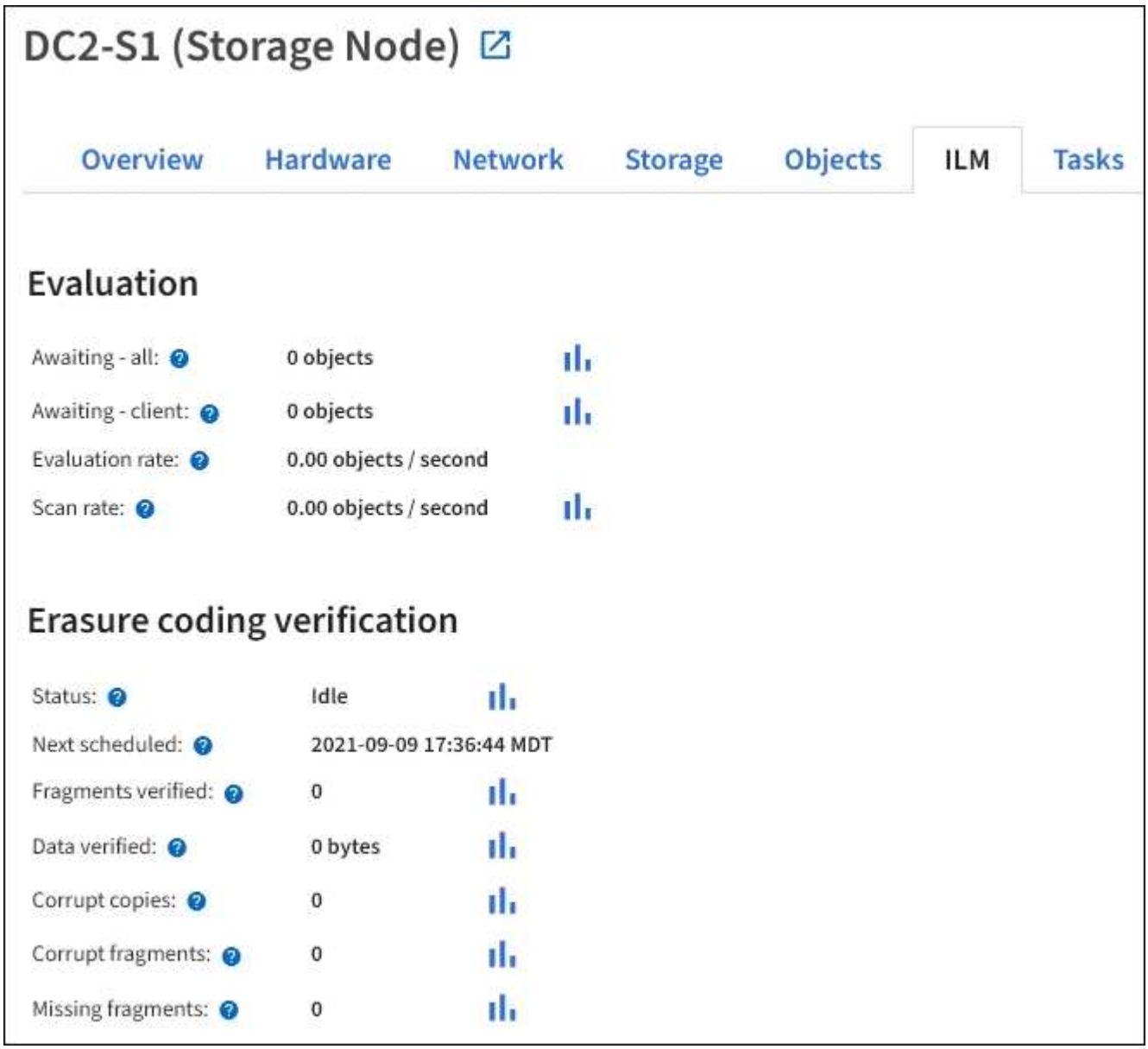

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200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

查看 **ILM** 选项卡

ILM 选项卡提供了有关信息生命周期管理（ ILM ）操作的信息。

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

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



相关信息

监控信息生命周期管理

管理 StorageGRID

查看负载平衡器选项卡

" 负载平衡器 " 选项卡包含与负载平衡器服务的运行相关的性能和诊断图。

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

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

请求流量

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

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

传入请求速率

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

平均请求持续时间（非错误）

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

错误响应率

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

相关信息

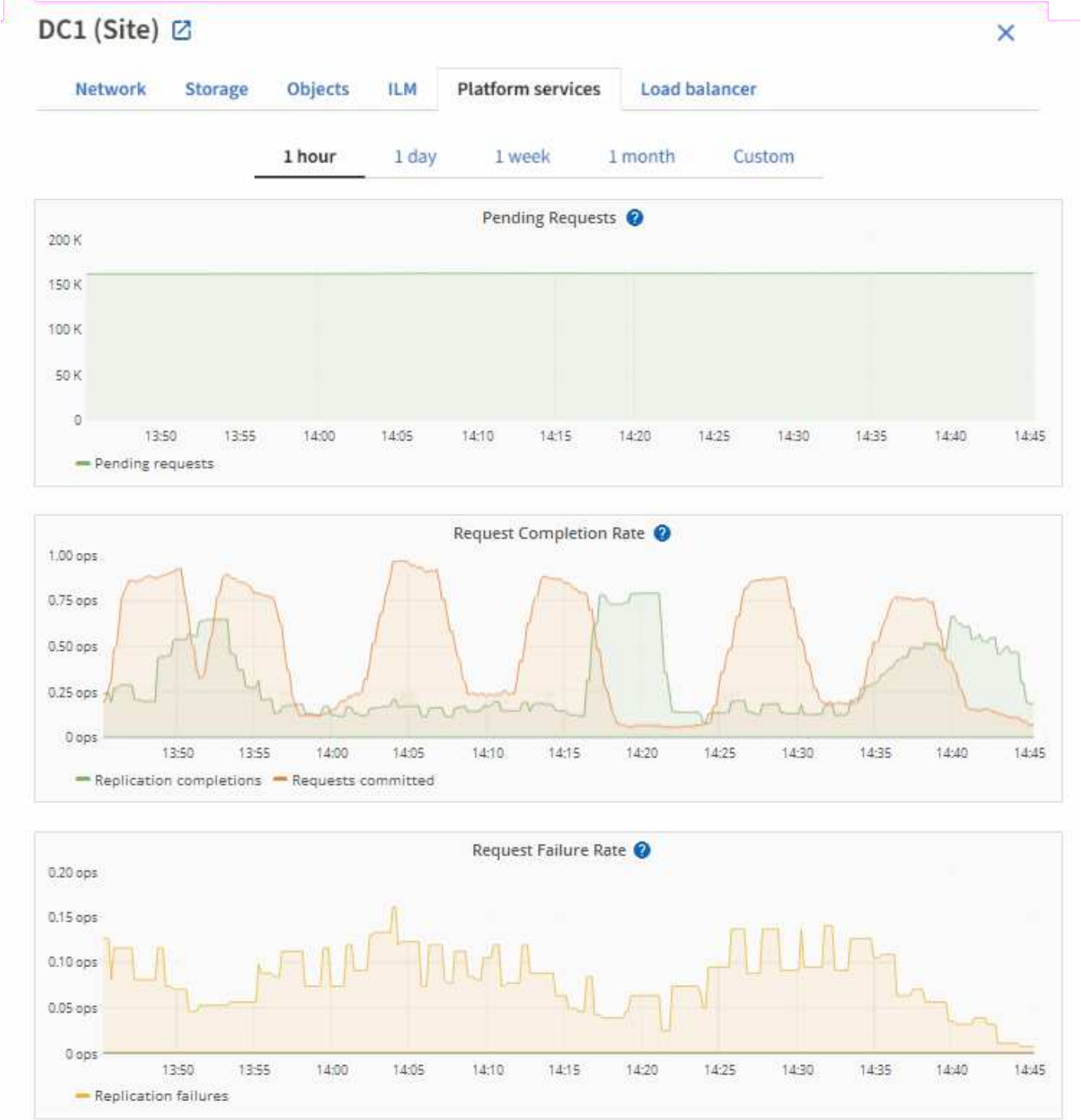
监控负载平衡操作

管理 StorageGRID

查看平台服务选项卡

平台服务选项卡提供了有关站点上任何 S3 平台服务操作的信息。

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



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

查看 **SANtricity** 系统管理器选项卡

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

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

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

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

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

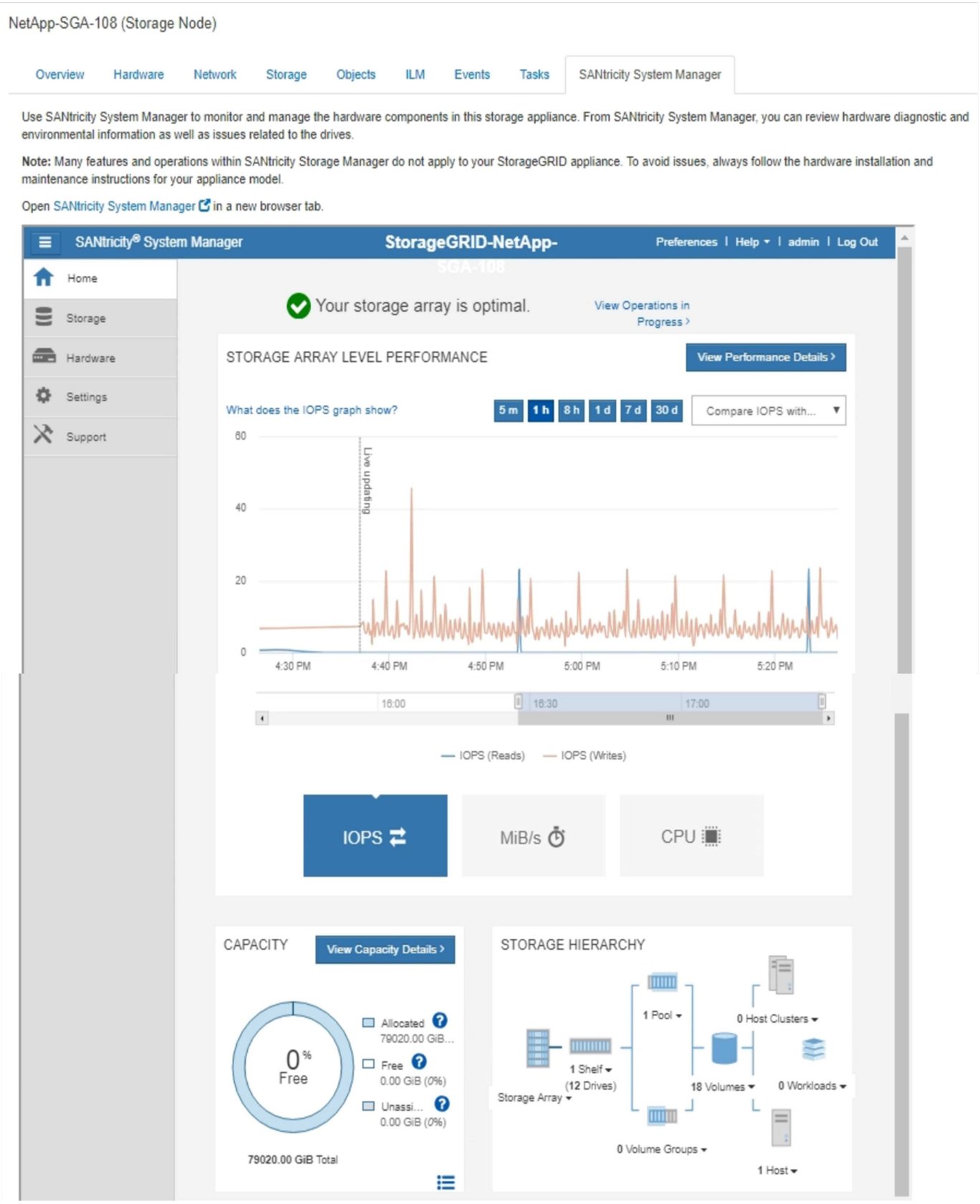
管理 StorageGRID

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

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

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

此选项卡将显示 SANtricity 系统管理器的主页。



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

要查看存储阵列级别性能和容量使用情况的详细信息，请将光标悬停在每个图形上。

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

您应定期监控的信息

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

繁忙的系统会生成大量信息。本节提供了有关持续监控的最重要信息的指导。

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

监控系统运行状况

您应每天监控 StorageGRID 系统的整体运行状况。

关于此任务

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

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

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

步骤

1. 登录到网格管理器以查看信息板。
2. 查看运行状况面板中的信息。

如果存在问题，则会显示一些链接，您可以通过这些链接查看其他详细信息：

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

相关信息

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

监控节点连接状态

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

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

节点可以具有以下三种连接状态之一：

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

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

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

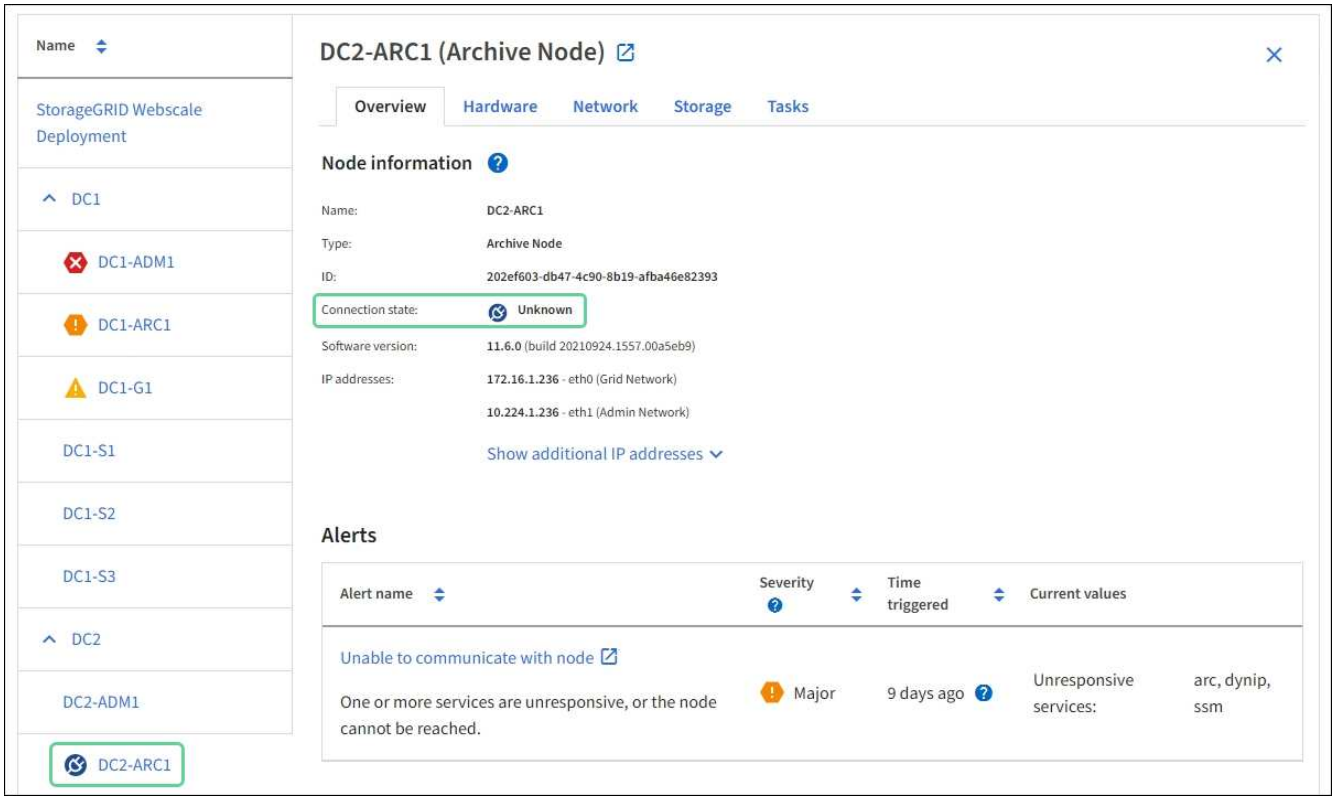
- * 已连接 * ：节点已连接到网格。

步骤

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

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

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



2. 如果节点有蓝色图标，请按照以下步骤操作：

   a. 选择表中的每个警报，然后按照建议的操作进行操作。

例如，您可能需要重新启动已停止的服务或重新启动节点的主机。

b. 如果无法使节点恢复联机，请联系技术支持。

3. 如果节点有灰色图标，请执行以下步骤：

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

a. 查看警报部分，并确定是否有任何警报影响此节点。

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

c. 如果无法使节点恢复联机，请联系技术支持。

相关信息

警报参考

恢复和维护

查看当前警报

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

您需要的内容

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

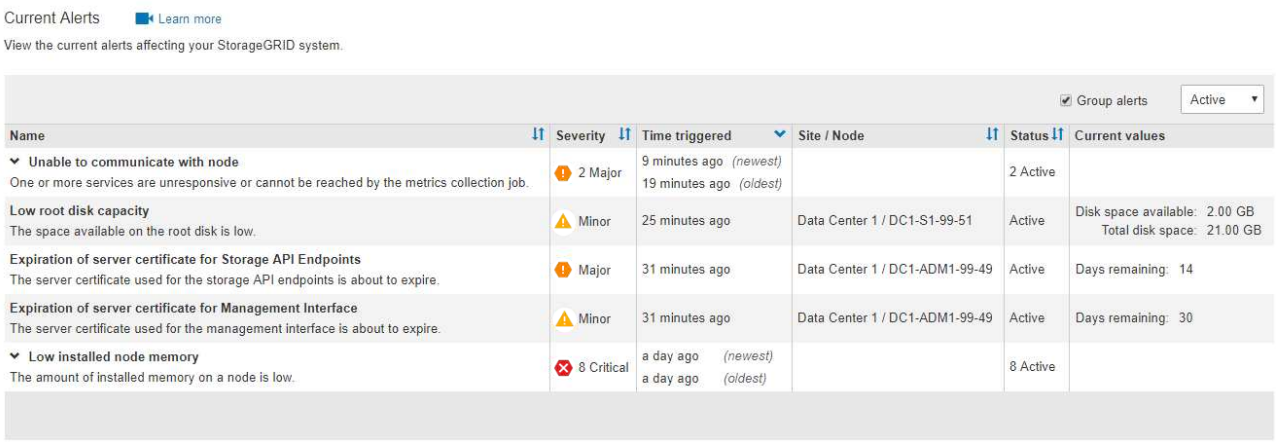
步骤

1. 如果一个或多个警报处于活动状态，请执行以下操作之一：

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

◦ 选择 * 警报 * > * 当前 * 。

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



默认情况下，警报显示如下：

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

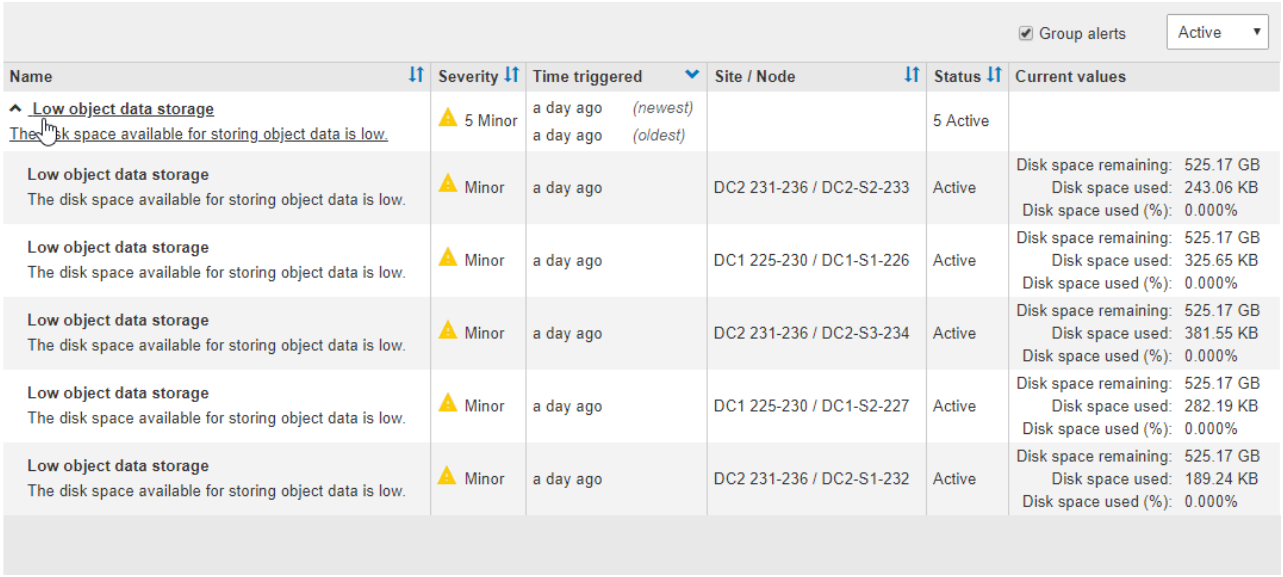
" 当前警报 " 页面每两分钟刷新一次。

2. 查看表中的信息。

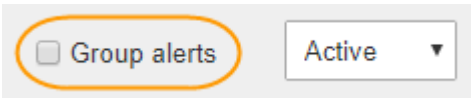
列标题	**Description**
Name	警报及其问题描述 的名称。
severity	警报的严重性。如果对多个警报进行了分组，则标题行将显示每个严重性发生的警报实例数。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 • * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影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

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

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



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



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

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

7. 要查看特定警报的详细信息，请从表中选择该警报。

   此时将显示警报对话框。请参见 查看特定警报。

查看已解决的警报

您可以搜索和查看已解决的警报历史记录。

您需要的内容

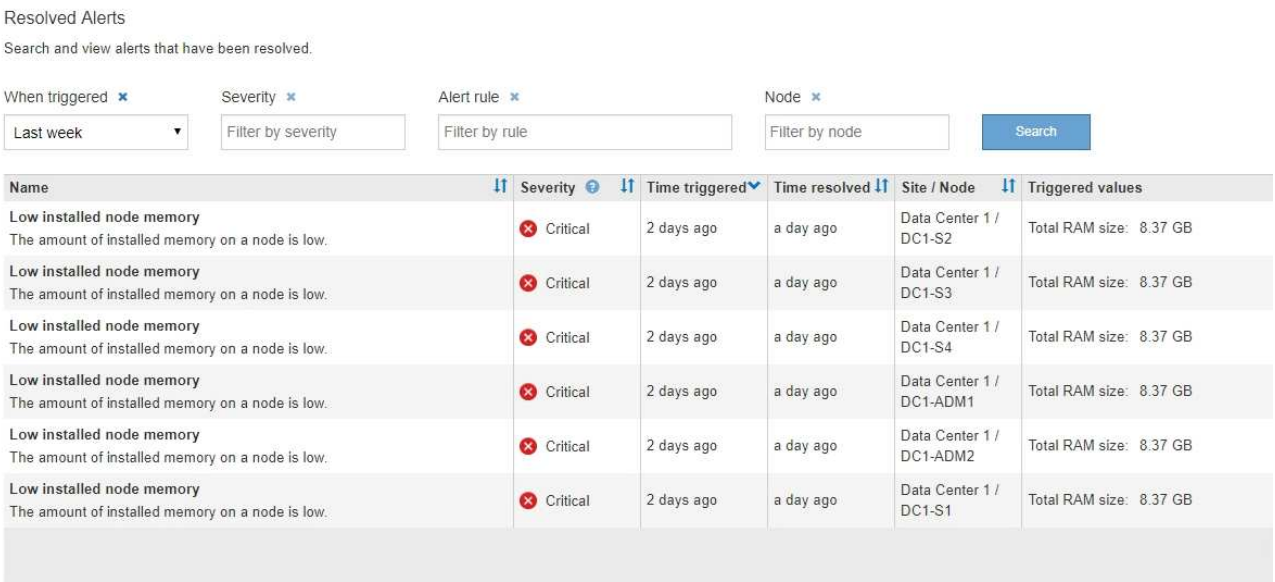
- 您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

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

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

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



2. 查看表中的信息。

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

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

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

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

      您可以搜索在以下时间段内触发的警报：

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

- 自定义（用于指定时间段的开始日期和结束日期）

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

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

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

e. 单击 * 搜索 * 。

5. 要查看特定已解决警报的详细信息，请从表中选择该警报。

此时将显示警报对话框。请参见 查看特定警报。

查看特定警报

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

您也可以选择 静默当前警报 或 更新警报规则。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

步骤

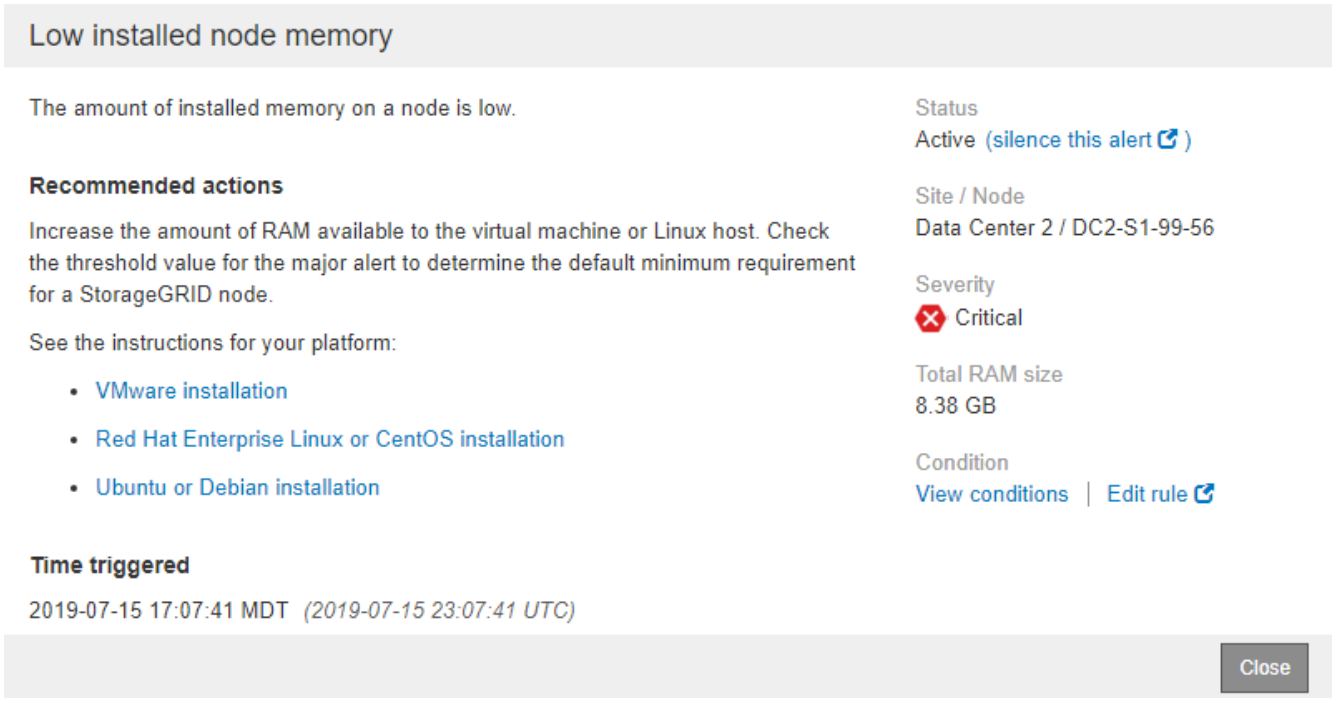
1. 根据您要查看当前警报还是已解决警报，执行以下操作之一：

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

2. 根据需要展开一组警报，然后选择要查看的警报。

选择警报，而不是一组警报的标题。

此时将显示一个对话框，其中提供了选定警报的详细信息。



3. 查看警报详细信息。

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

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

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

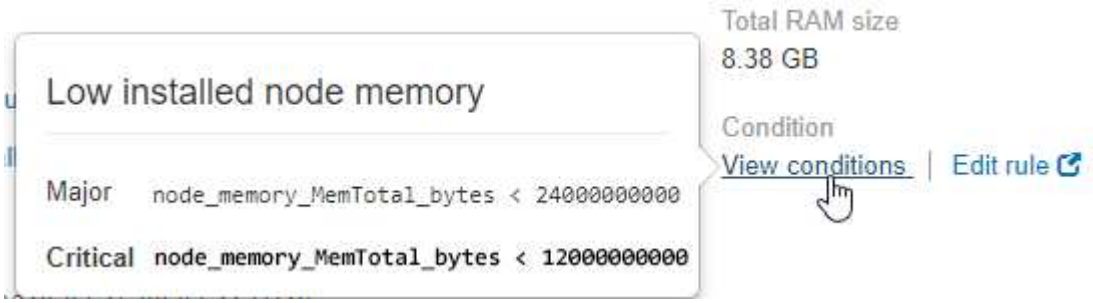
   要使警报规则静默，您必须具有管理警报或 root 访问权限。

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

5. 要查看警报规则的当前条件，请执行以下操作：

   a. 在警报详细信息中，单击 * 查看条件 * 。

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



   a. 要关闭此弹出窗口，请单击此弹出窗口以外的任意位置。

6. 或者，也可以单击 * 编辑规则 * 来编辑导致触发此警报的警报规则：

   要编辑警报规则，您必须具有管理警报或 root 访问权限。

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

7. 要关闭警报详细信息，请单击 * 关闭 * 。

查看旧警报

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

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

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

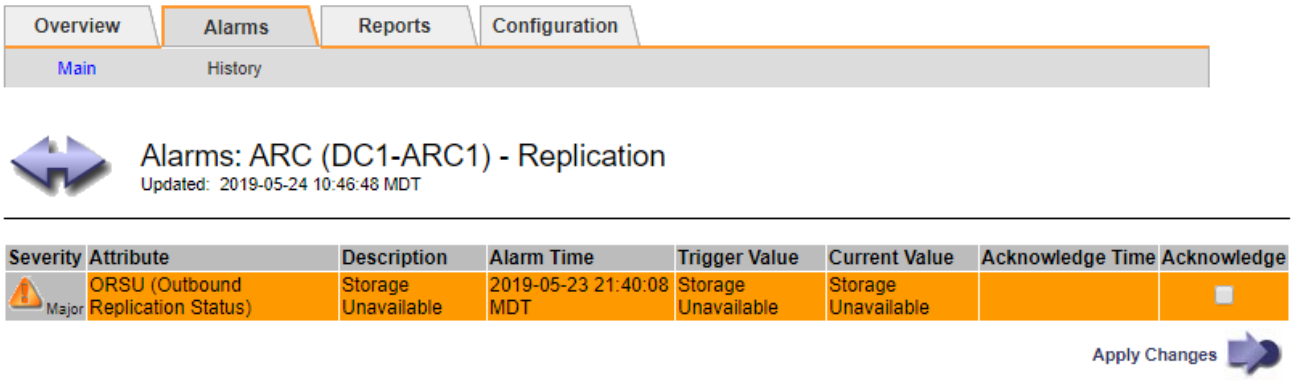
警报图标指示每个警报的严重性，如下所示：

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

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

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

）。



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

相关信息

警报参考（旧系统）

确认当前警报（旧系统）

禁用警报（旧系统）

监控存储容量

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

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

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

监控整个网格的存储容量

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

您需要的内容

您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

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

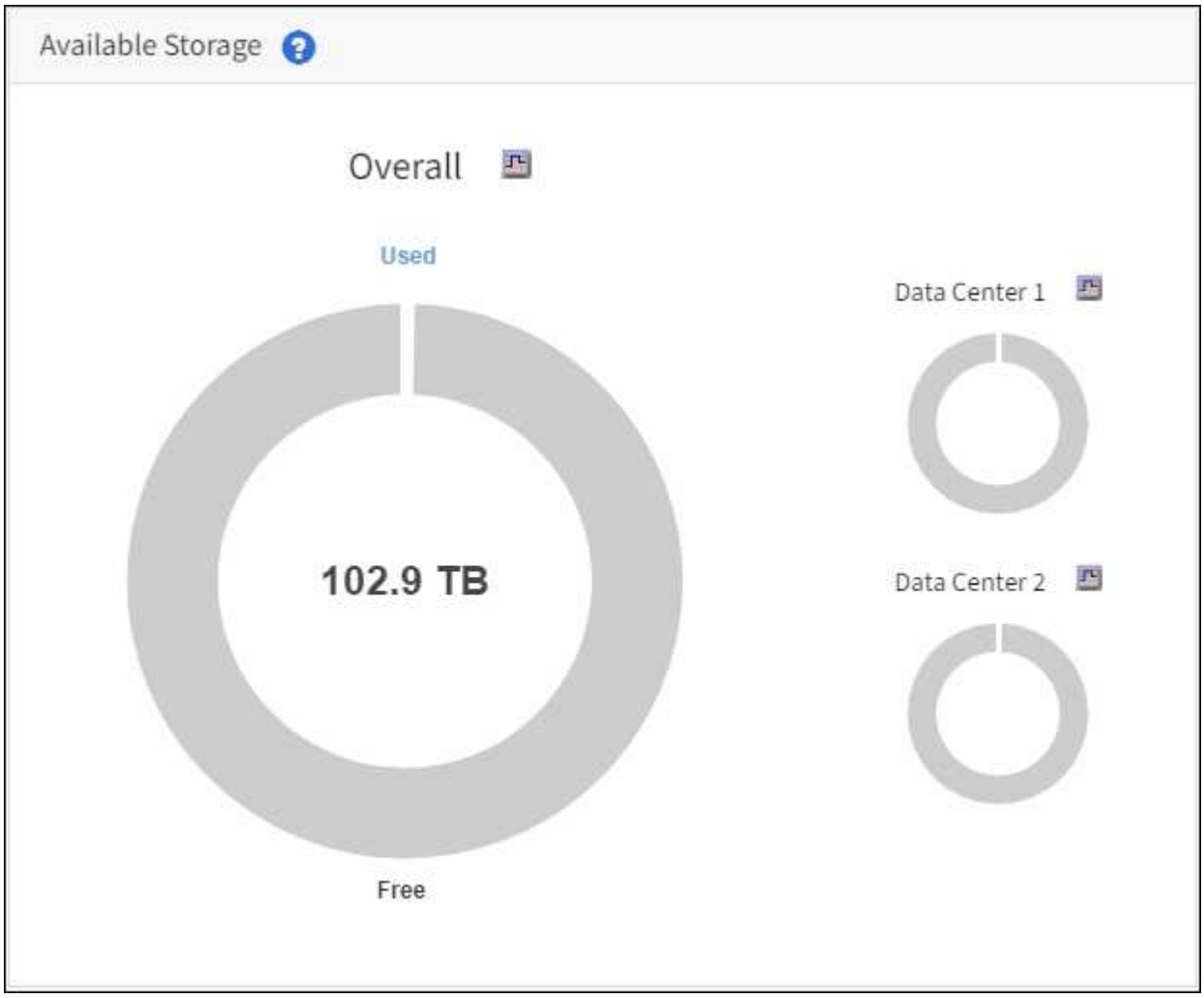
步骤

1. 评估可用于整个网格和每个数据中心的存储量。

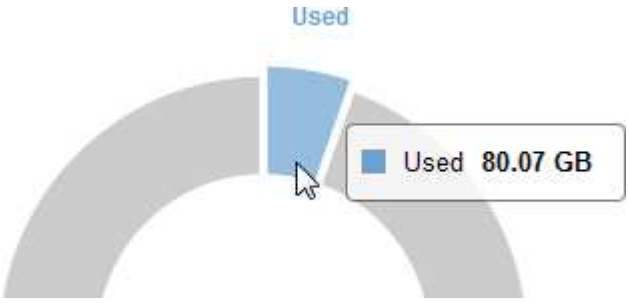
a. 选择 * 信息板 * 。

b. 在可用存储面板中，记下可用存储容量和已用存储容量的总体摘要。

此摘要不包括归档介质。



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

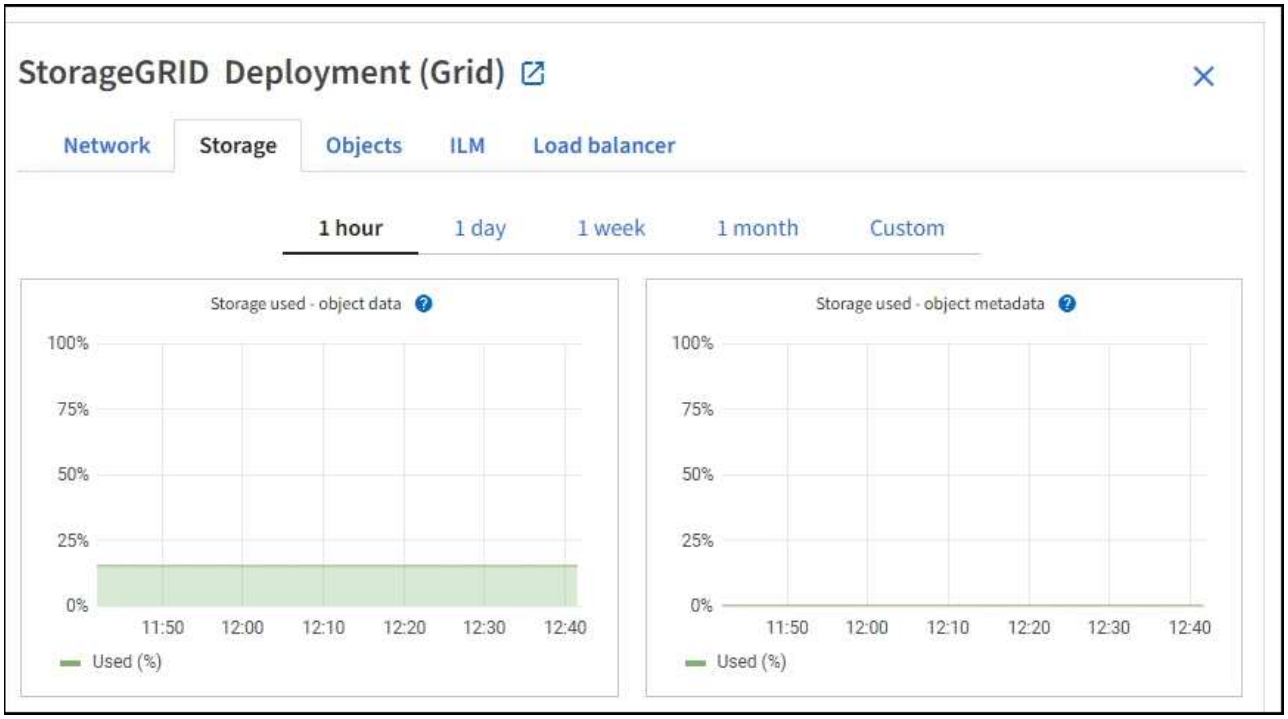


b. 对于多站点网格，请查看每个数据中心的图表。

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

显示已用存储容量百分比（ % ）与的图形此时将显示时间。

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



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

> 站点或网格的总值不包括至少在五分钟内未报告指标的节点，例如脱机节点。

3. 计划执行扩展，以便在占用网格的可用存储容量之前添加存储节点或存储卷。

   在规划扩展时间时，请考虑购买和安装额外存储需要多长时间。

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

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

监控每个存储节点的存储容量

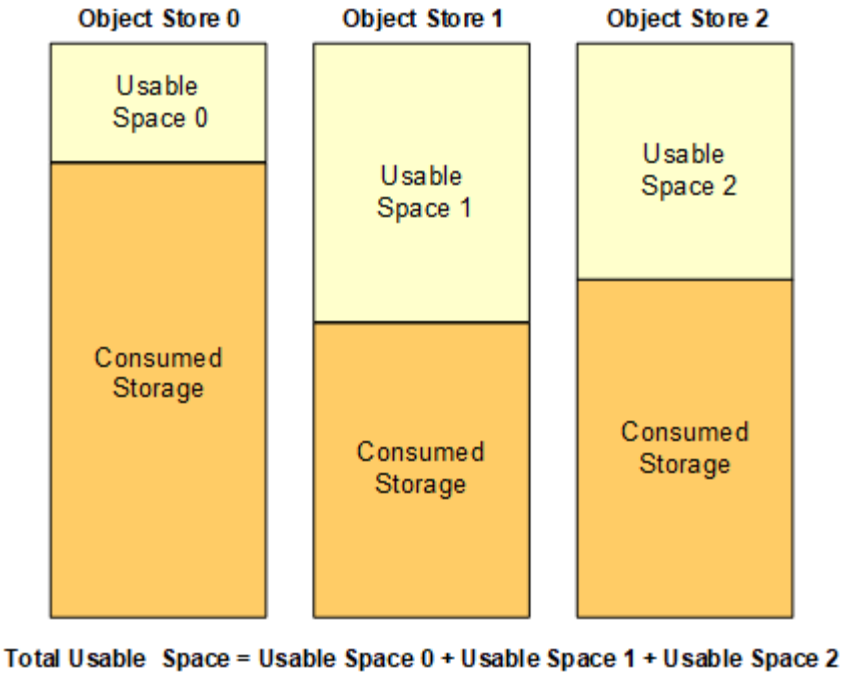
监控每个存储节点的总可用空间，以确保该节点具有足够的空间来容纳新对象数据。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

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



步骤

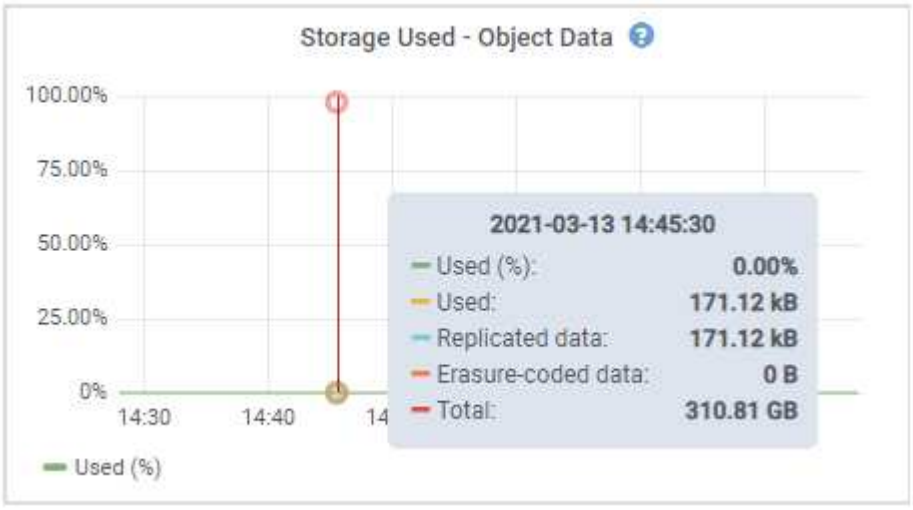
1. 选择 * 节点 * > * 存储节点 _* > * 存储 * 。

   此时将显示节点的图形和表。

2. 将光标悬停在已用存储 - 对象数据图上。

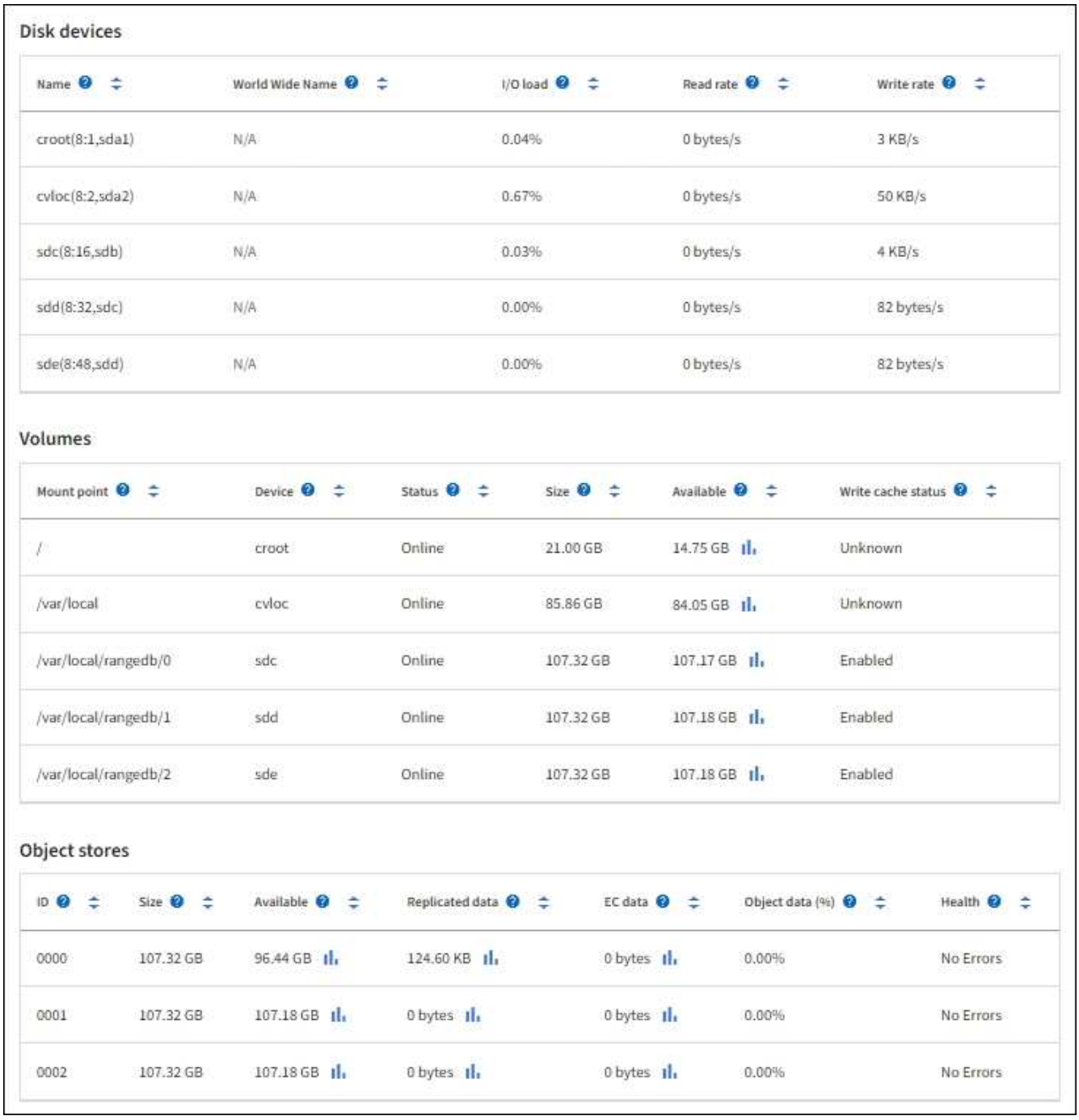
   此时将显示以下值：

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



3. 查看图形下方的卷和对象存储表中的可用值。

要查看这些值的图形，请单击图表图标 在可用列中。



Disk devices

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

Volumes

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

Object stores

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

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

   在规划扩展时间时，请考虑购买和安装额外存储需要多长时间。

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

有关规划存储扩展的详细信息，请参见 扩展 StorageGRID 的说明。

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

监控每个存储节点的对象元数据容量

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

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

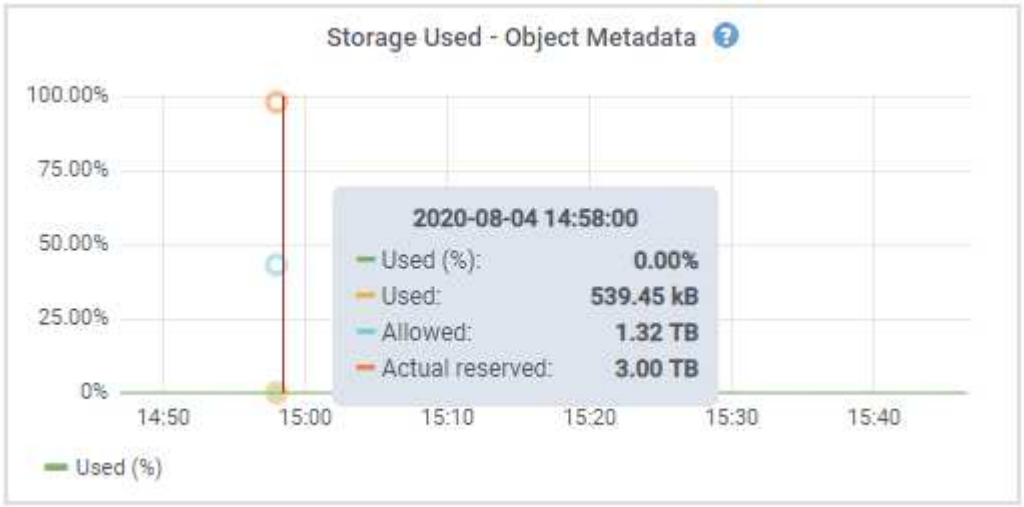
StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并防止对象元数据丢失。这三个副本会使用每个存储节点的存储卷 0 上为元数据预留的空间均匀分布在每个站点的所有存储节点上。

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

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

步骤

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



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

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

站点或网格的总值不包括至少在五分钟内未报告指标的节点，例如脱机节点。

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

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

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

监控信息生命周期管理

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

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

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

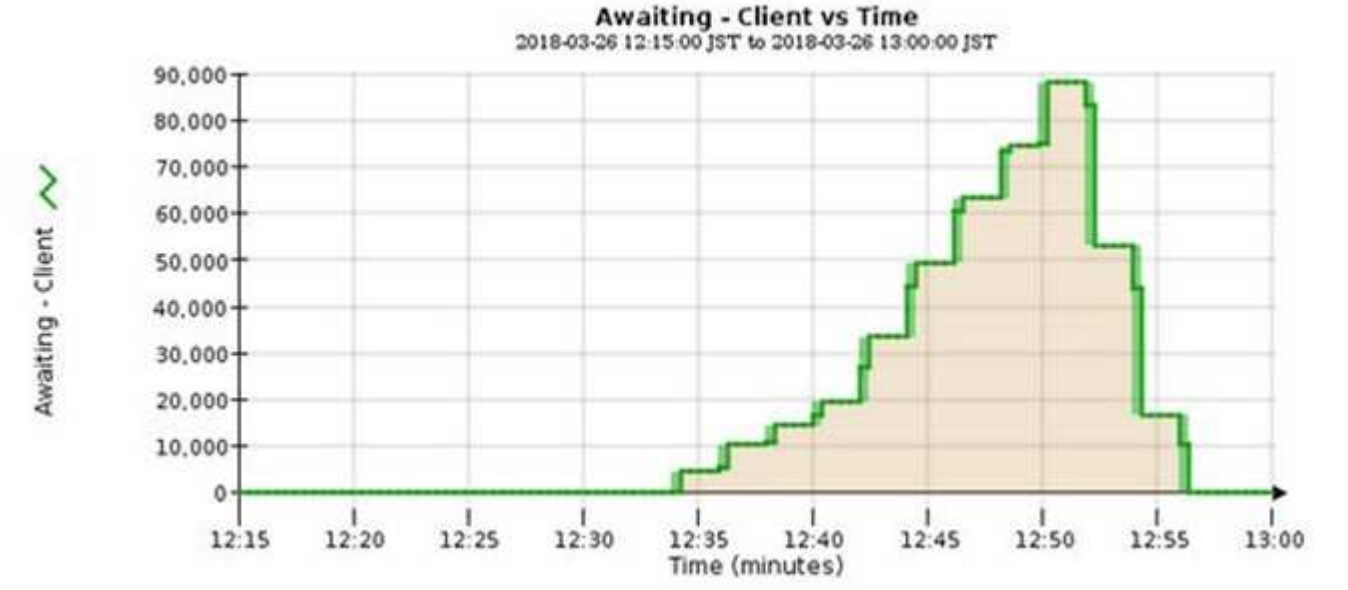
对象载入和其他与对象相关的活动可能会超过 StorageGRID 评估 ILM 的速率，从而导致系统对无法近乎实时地执行 ILM 放置指令的对象进行排队。您可以通过绘制 waiting - Client 属性来监控 StorageGRID 是否与客户端操作保持一致。

要对此属性进行绘制，请执行以下操作：

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

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

表明， ILM 暂时未近乎实时地完成。



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

您可以使用 * 节点 * 页面进一步调查 ILM 队列。

步骤

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

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

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

     完全扫描并不能保证 ILM 已应用于所有对象。

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

     如果修复后复制失败，则同一对象修复可能会再次增加。

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

扫描，则修复可能已完成。

监控网络连接和性能

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

您需要的内容

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

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

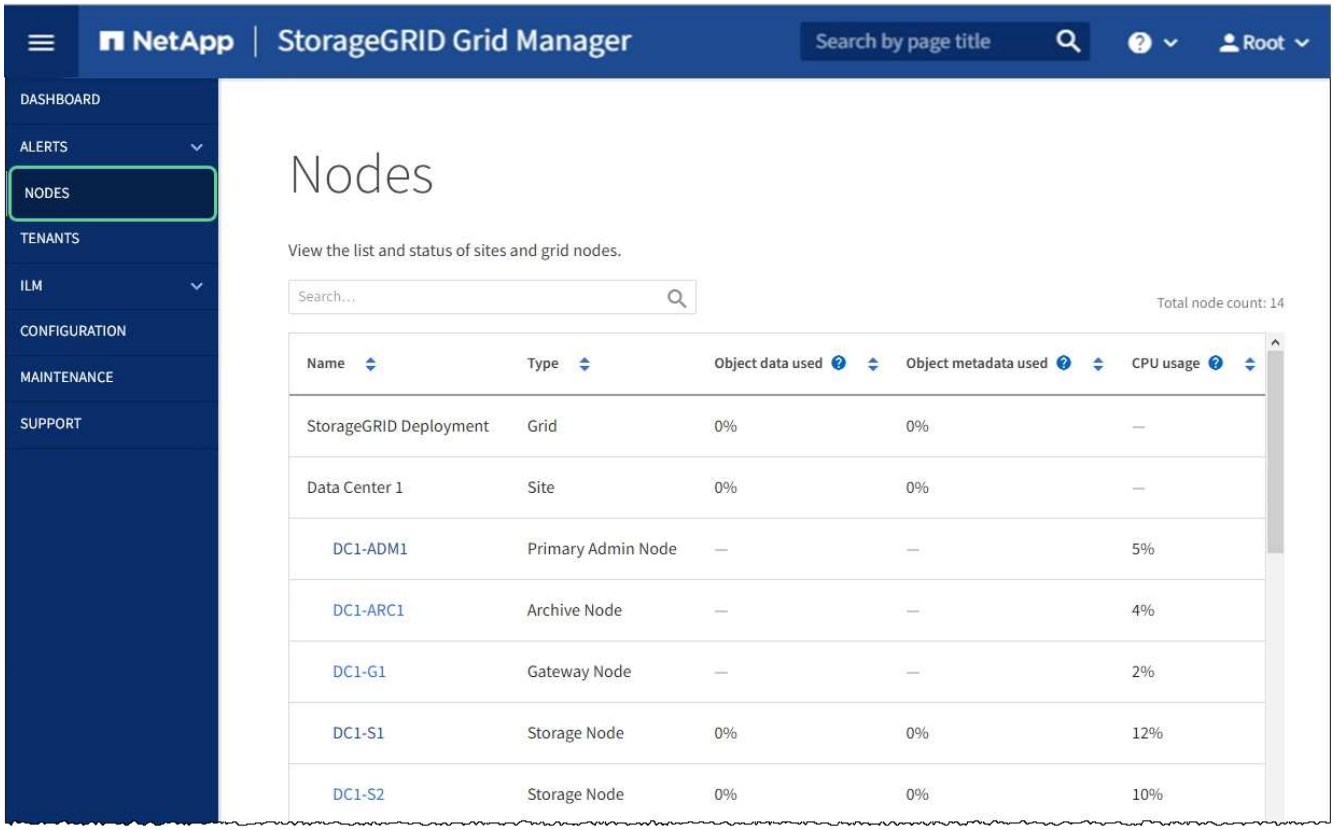
您可以使用网格管理器监控连接和网络性能，以便及时解决任何问题。

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

步骤

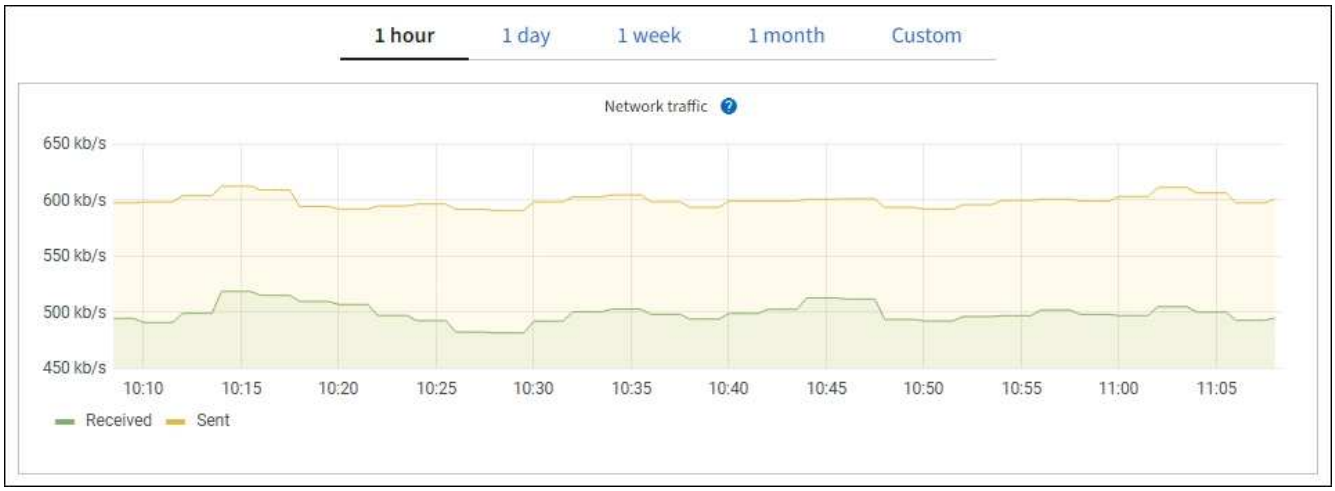
1. 选择 * 节点 * 。

   此时将显示节点页面。网格中的每个节点均以表格式列出。

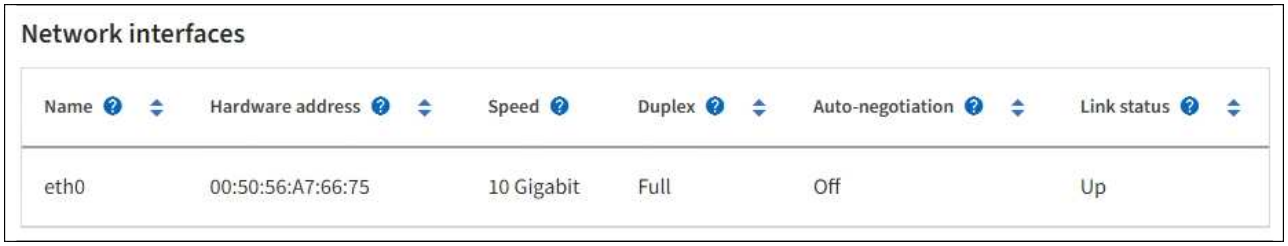


2. 选择网格名称，特定数据中心站点或网格节点，然后选择 * 网络 * 选项卡。

   网络流量图提供了整个网格，数据中心站点或节点的整体网络流量摘要。



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

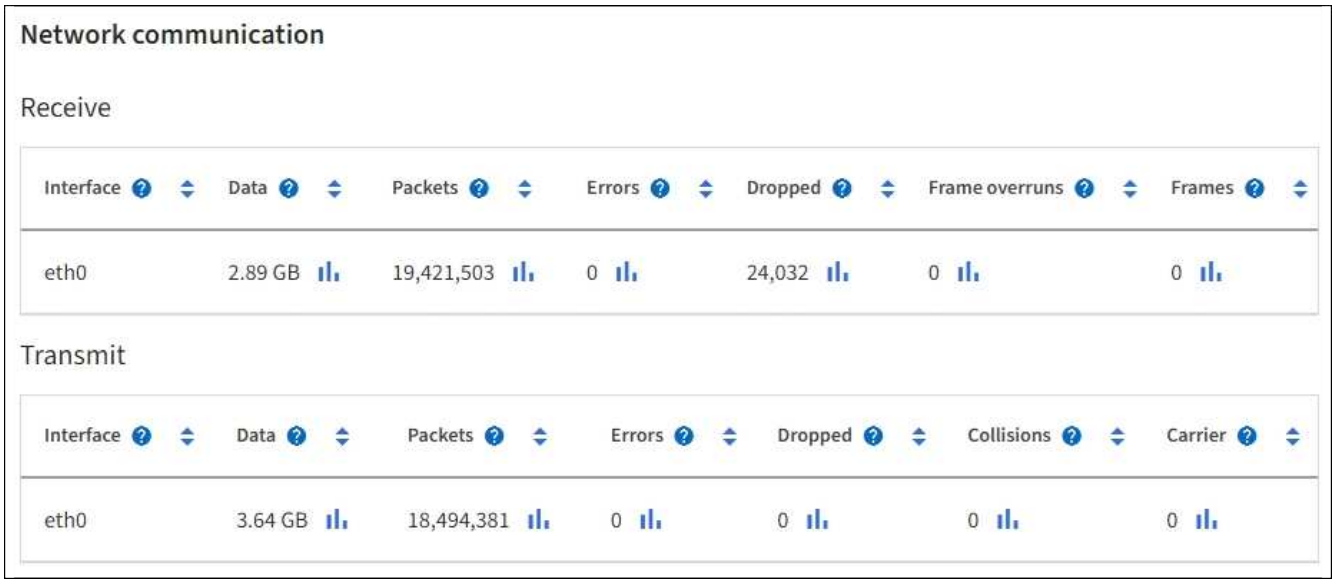


Network interfaces

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

   b. 对于网格节点，向下滚动以查看页面的 * 网络通信 * 部分。

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



Network communication

Receive

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

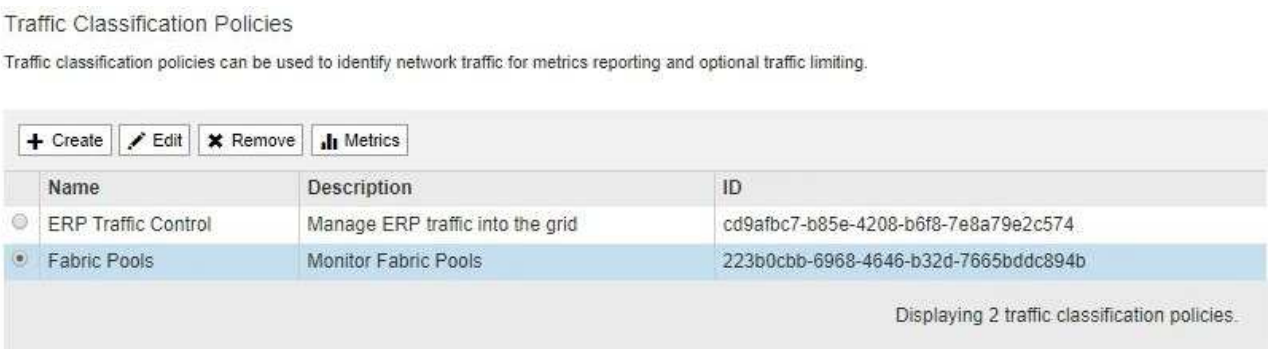
Transmit

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

3. 使用与流量分类策略关联的指标监控网络流量。

   a. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



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

c. 查看图形以了解与策略关联的网络流量。

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

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

相关信息

查看网络选项卡

监控节点连接状态

监控节点级资源

您应监控各个网格节点以检查其资源利用率级别。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

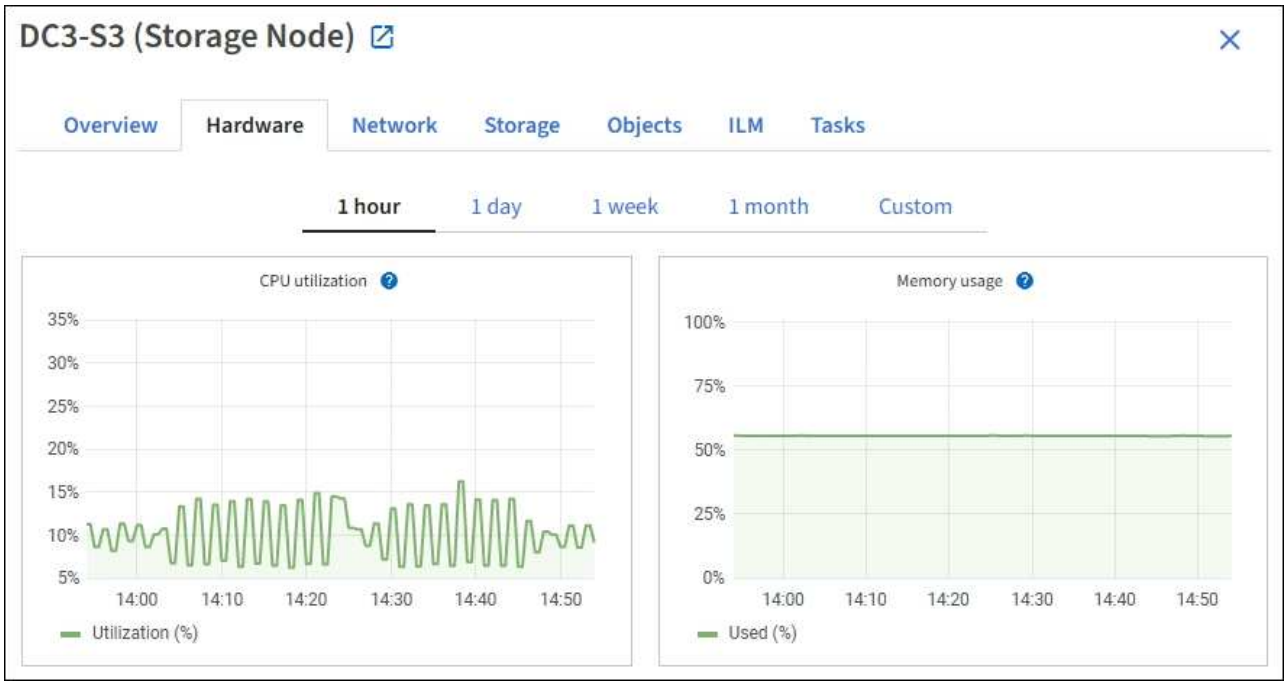
如果节点始终过载，则可能需要更多节点才能高效运行。

步骤

1. 要查看有关网格节点硬件利用率的信息，请执行以下操作：

a. 从 * 节点 * 页面中，选择节点。

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



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

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

相关信息

查看有关设备存储节点的信息

查看有关设备管理节点和网关节点的信息

监控租户活动

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

您需要的内容

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

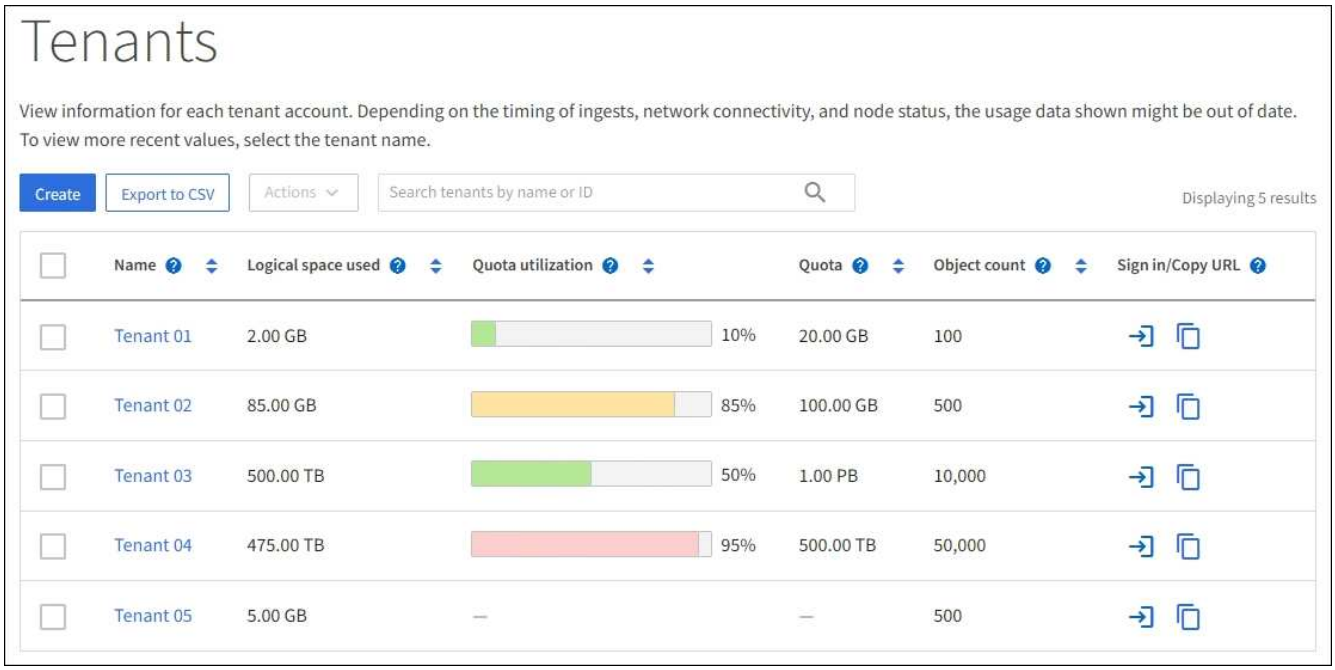
关于此任务

已用空间值是估计值。这些估计值受载入时间，网络连接和节点状态的影响。

步骤

1. 选择 * 租户 * 可查看所有租户使用的存储量。

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



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

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

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

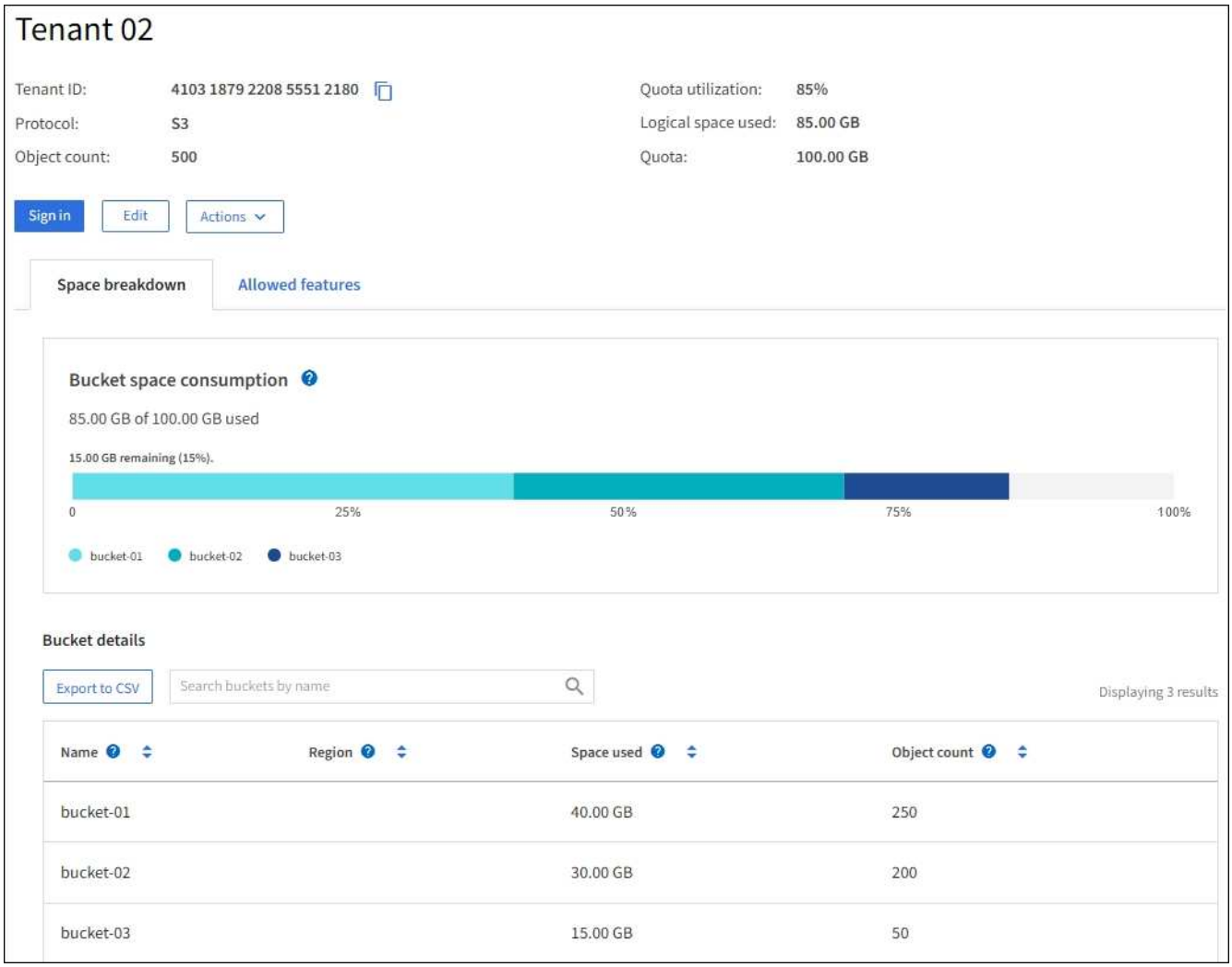
   系统会提示您打开或保存 ` .csv` 文件。

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

图 **1. csv** 文件的内容如下所示：

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

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



◦ * 租户概述 *

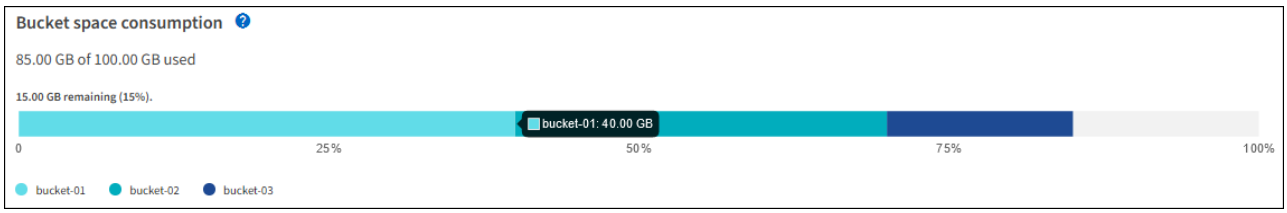
租户的概述区域包含对象计数，配额利用率，已用逻辑空间和配额设置的值。

◦ * 空间细分 - 空间消耗 *

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

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

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



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

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

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

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

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

   单个 S3 租户的 .csv 文件的内容如下所示：

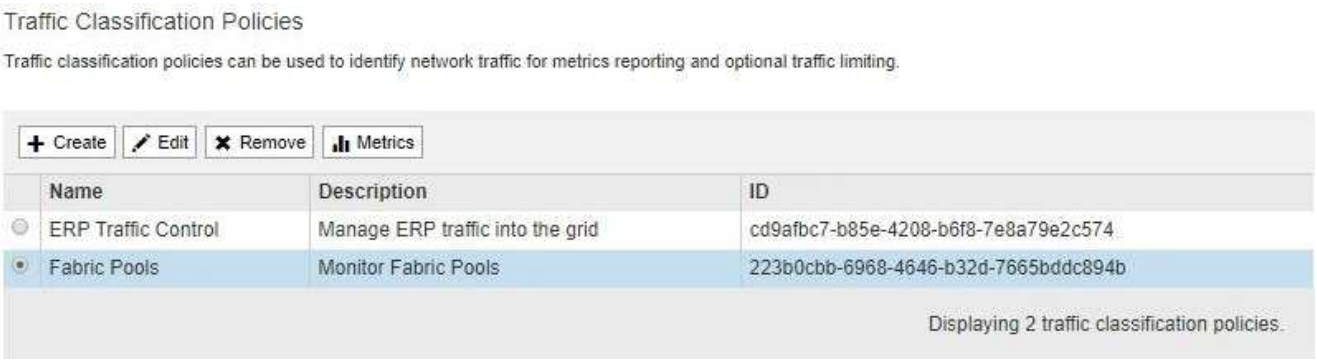
Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

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

5. 如果某个租户已设置流量分类策略，请查看该租户的网络流量。

   a. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

      此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



   a. 查看策略列表以确定适用于特定租户的策略。

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

   c. 分析图形以确定策略限制流量的频率以及是否需要调整策略。

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

6. 或者，也可以使用审核日志更精细地监控租户的活动。

   例如，您可以监控以下类型的信息：

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

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

   有关详细信息，请参见了解审核消息的说明。

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

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

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

相关信息

警报参考

查看审核日志

管理 StorageGRID

查看支持指标

监控归档容量

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

您需要的内容

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

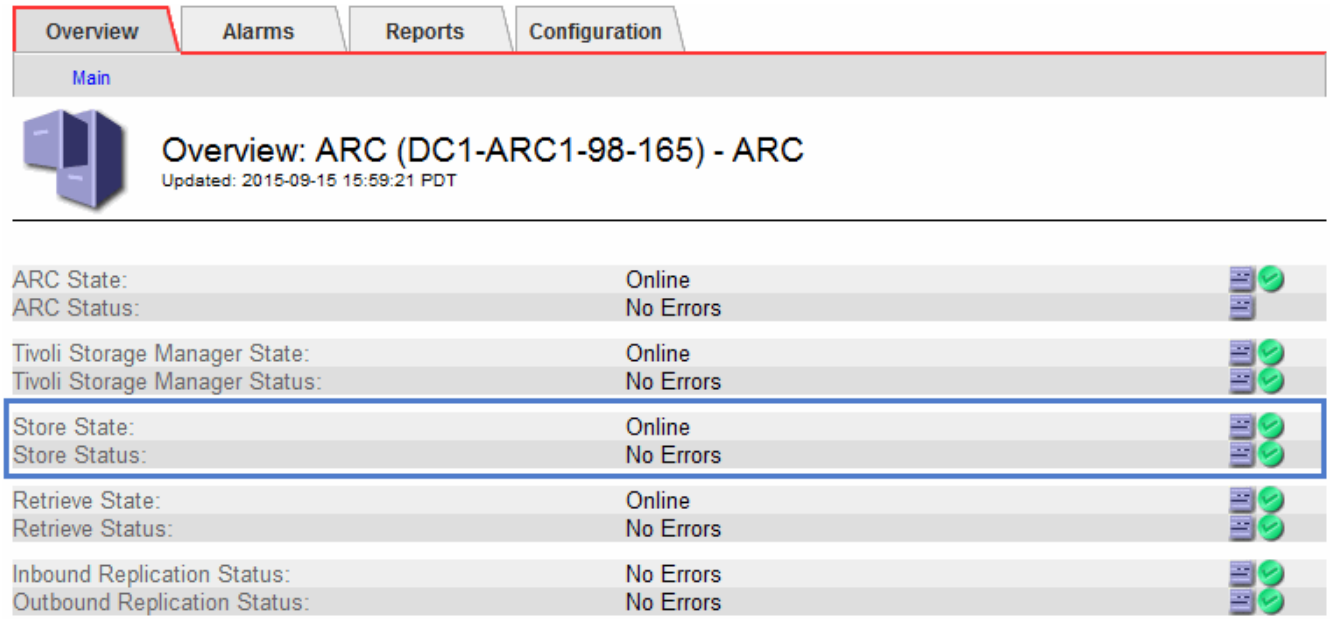
关于此任务

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

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

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



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

监控负载平衡操作

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

您需要的内容

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

关于此任务

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

CLB 服务已弃用。

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

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

请参见有关管理 StorageGRID 的说明中有关配置客户端连接的章节。

步骤

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

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

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

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

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

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

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

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

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

      所有存储节点的会话数应大致相等。

相关信息

管理 StorageGRID

查看负载平衡器选项卡

如有必要，应用修补程序或升级软件

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

关于此任务

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

步骤

1. 转到 StorageGRID 的 "NetApp 下载 " 页面。

   "NetApp 下载： StorageGRID"

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

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

     ▪ 相关信息 *

升级软件

恢复和维护

管理警报和警报

管理警报和警报：概述

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

警报系统

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

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

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

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

传统警报系统

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

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

触发警报后，将执行以下操作：

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

比较警报和警报

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

请参见下表，了解如何执行类似操作。

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

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

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

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

管理警报

管理警报：概述

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

关于 **StorageGRID** 警报

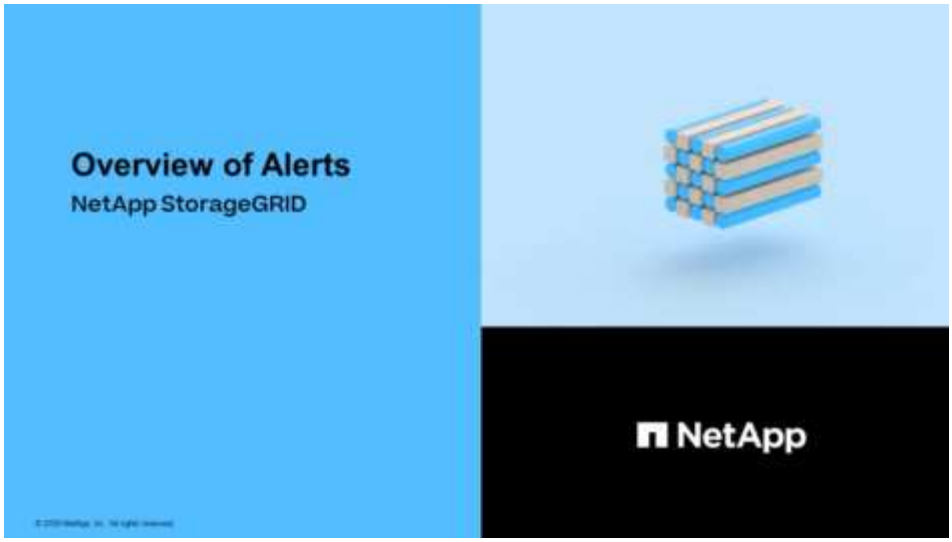
警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

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

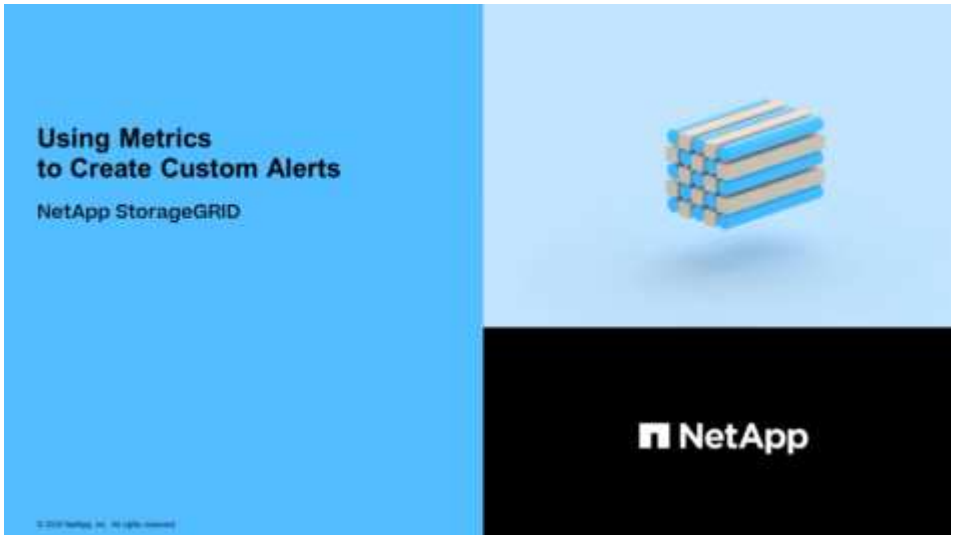
了解更多信息。

要了解更多信息，请查看以下视频：

- "视频：警报概述"



- "视频：使用指标创建自定义警报"



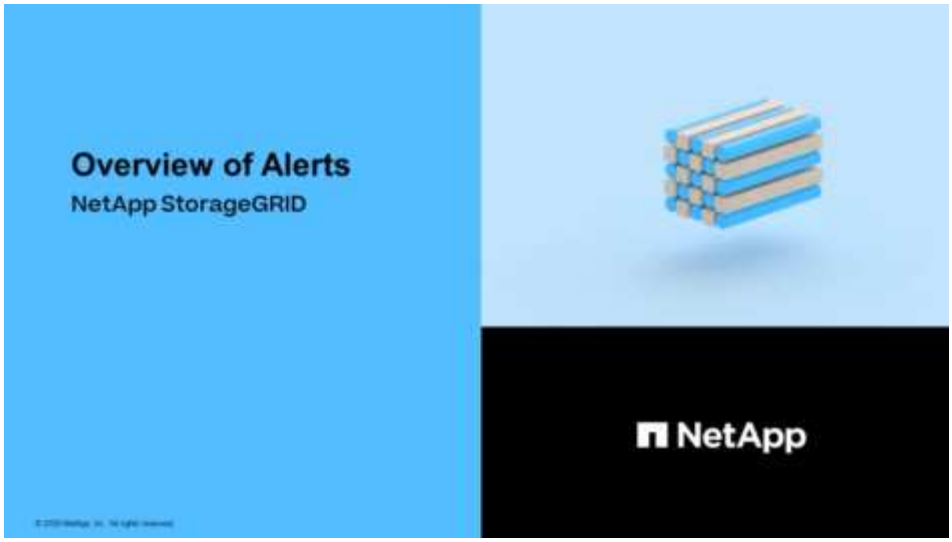
查看警报规则

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

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

您需要的内容

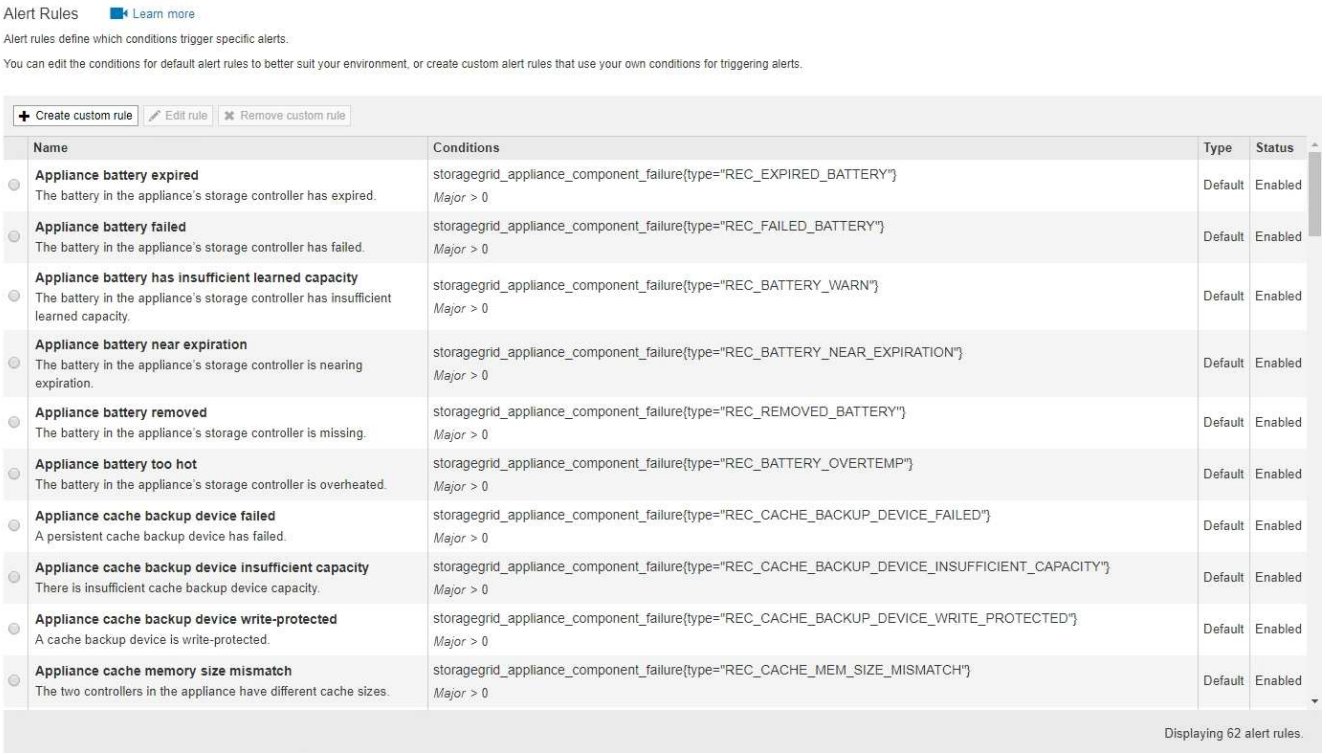
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 " 管理警报 " 或 " 根访问 " 权限。
- 您也可以观看以下视频： "视频：警报概述"



步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。



2. 查看警报规则表中的信息：

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

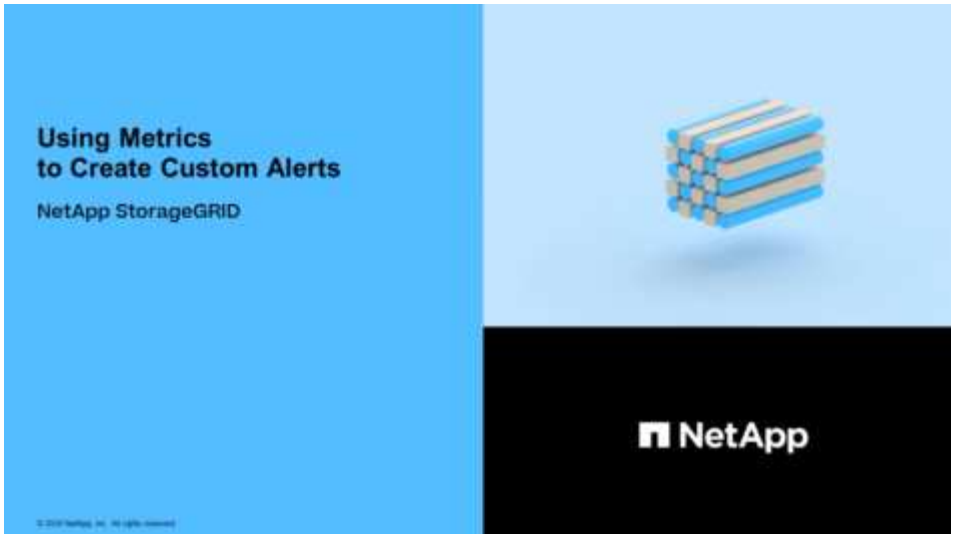
列标题	Description
条件	用于确定何时触发此警报的 Prometheus 表达式。可以在以下一个或多个严重性级别触发警报，但不需要为每个严重性设置一个条件。 • * 严重 * ：存在已停止 StorageGRID 节点或服务正常运行的异常情况。您必须立即解决底层问题描述 。如果未解决问题描述 ，可能会导致服务中断和数据丢失。 • * 主要 * ：存在影响当前操作或接近严重警报阈值的异常情况。您应调查主要警报并解决任何根本问题，以确保异常情况不会停止 StorageGRID 节点或服务的正常运行。 • * 次要 * ：系统运行正常，但存在异常情况，如果系统继续运行，可能会影响系统的运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

创建自定义警报规则

您可以创建自定义警报规则来定义自己触发警报的条件。

您需要的内容

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



关于此任务

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

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

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

- 除非您验证警报是在预期时间触发的，否则请勿假定自定义警报正在运行。

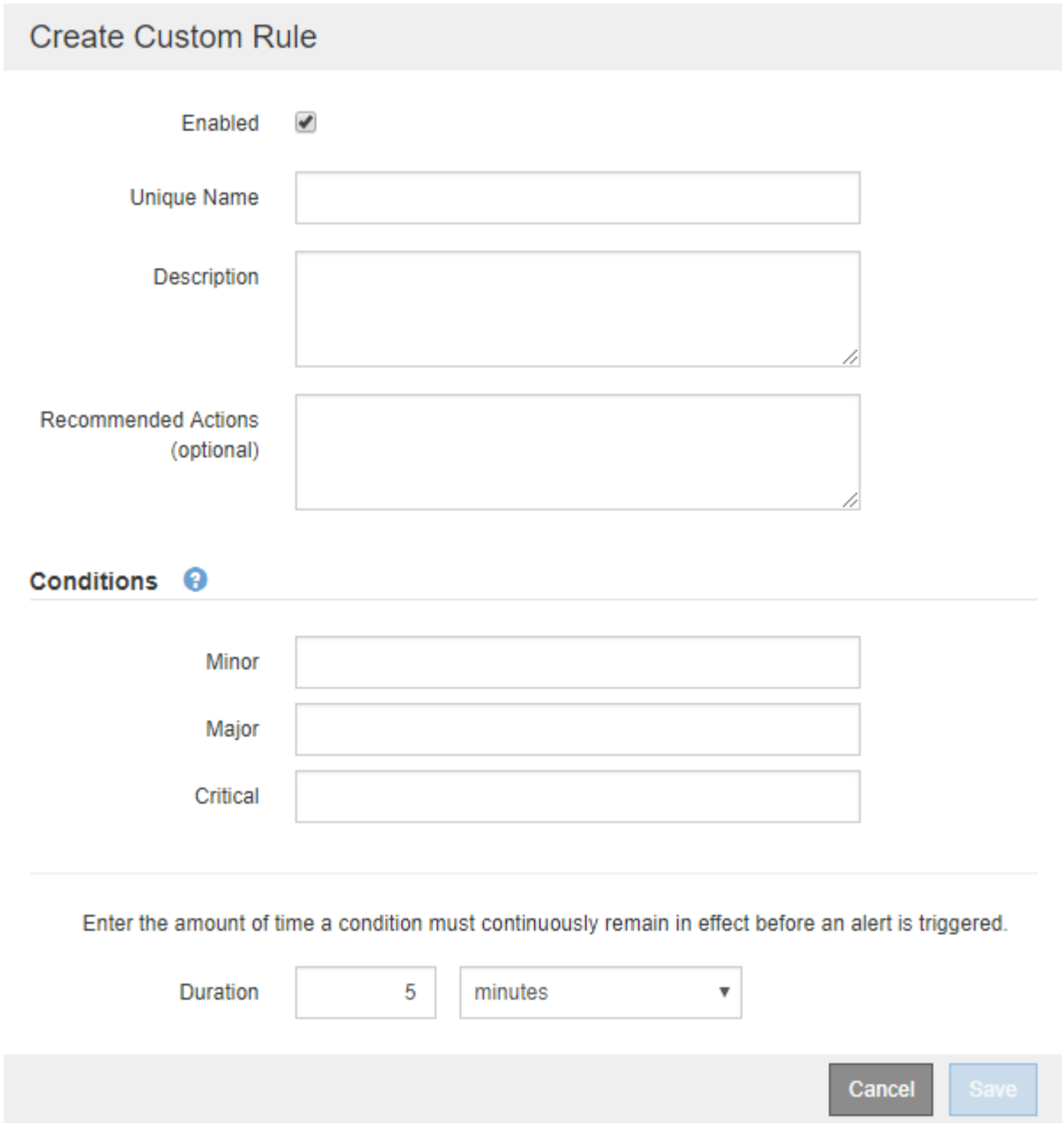
步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

2. 选择 * 创建自定义规则 * 。

   此时将显示创建自定义规则对话框。



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

   如果禁用了警报规则，则不会评估其表达式，也不会触发任何警报。

4. 输入以下信息：

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

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

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

   基本表达式通常采用以下形式：

   `，指标，运算符，值，`

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

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

   ```
   node_memory_MemTotal_bytes < 240000000
   ```

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

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

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

   默认值为 5 分钟。

7. 选择 * 保存 * 。

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

编辑警报规则

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

您需要的内容

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

关于此任务

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

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

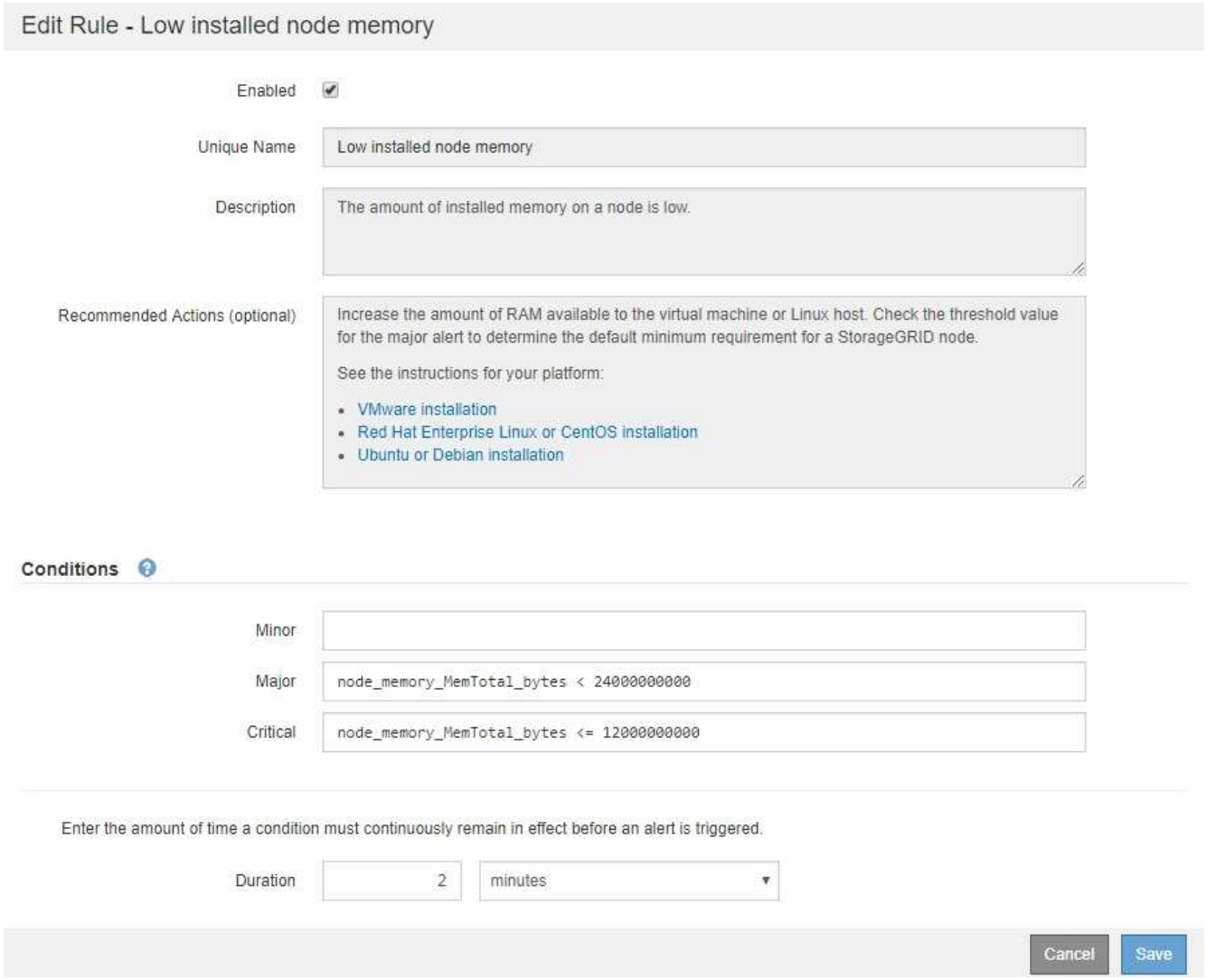
步骤

1. 选择 * 警报 * > * 规则 * 。

此时将显示 "Alert Rules" 页面。

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

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



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

   如果禁用了警报规则，则不会评估其表达式，也不会触发任何警报。

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

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

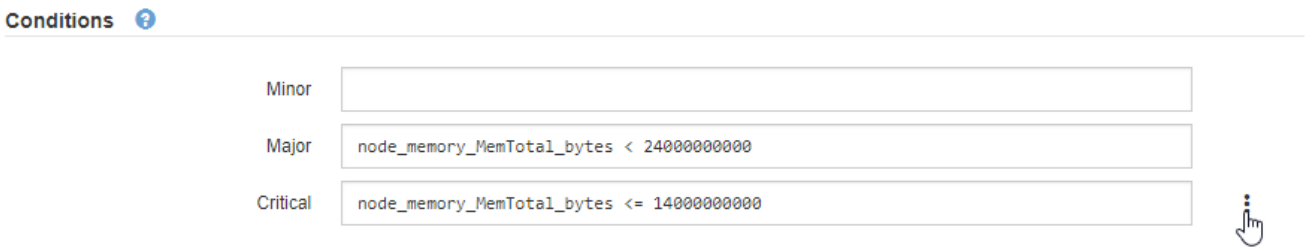
5. 对于自定义警报规则，请根据需要更新以下信息。

您不能为默认警报规则编辑此信息。

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

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

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



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

基本表达式通常采用以下形式：

`，指标，运算符，值，`

表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

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

```
node_memory_MemTotal_bytes < 240000000
```

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

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

默认值为 5 分钟。

8. 选择 * 保存 * 。

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

禁用警报规则

您可以更改默认或自定义警报规则的启用 / 禁用状态。

您需要的内容

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

关于此任务

禁用警报规则后，不会评估其表达式，也不会触发任何警报。

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

步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

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

   此时将显示编辑规则对话框。

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

   如果禁用了警报规则，则不会评估其表达式，也不会触发任何警报。

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

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

删除自定义警报规则

如果您不想再使用自定义警报规则，可以将其删除。

您需要的内容

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

步骤

1. 选择 * 警报 * > * 规则 * 。

   此时将显示 "Alert Rules" 页面。

2. 选择要删除的自定义警报规则对应的单选按钮。

您不能删除默认警报规则。

3. 选择 * 删除自定义规则 * 。

   此时将显示确认对话框。

4. 选择 * 确定 * 以删除警报规则。

   任何处于活动状态的警报实例将在 10 分钟内得到解决。

管理警报通知

为警报设置 **SNMP** 通知

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

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

要了解如何配置 SNMP 代理，请参见 使用 SNMP 监控。

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

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

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

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

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

为警报设置电子邮件通知

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

您需要的内容

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

关于此任务

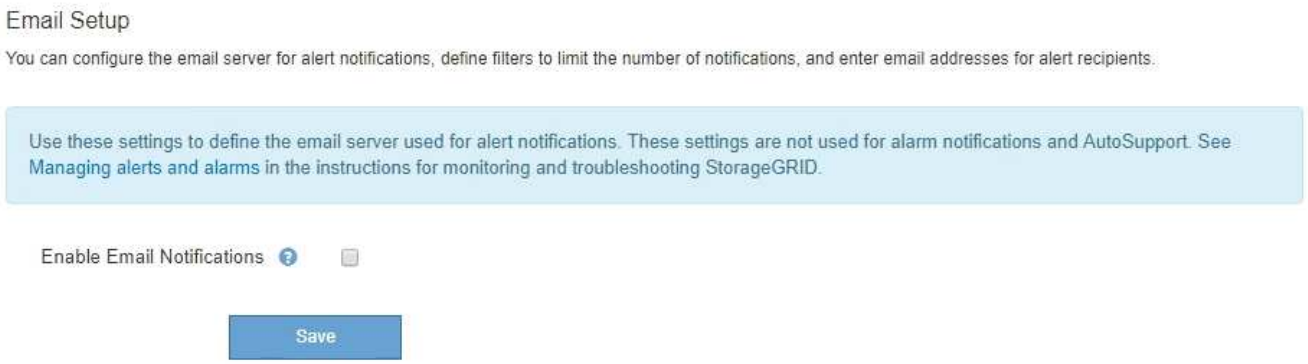
由于警报和警报是独立的系统，因此用于警报通知的电子邮件设置不会用于警报通知和 AutoSupport 消息。但是，您可以对所有通知使用同一个电子邮件服务器。

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

步骤

1. 选择 * 警报 * > * 电子邮件设置 * 。

   此时将显示电子邮件设置页面。



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

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

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

   如果 SMTP 服务器需要身份验证，则必须同时提供用户名和密码。

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

4. 在电子邮件地址部分中，输入发件人和每个收件人的电子邮件地址。

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

      例如： `storagegrid-alerts@example.com`

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

      选择加号图标 ✚ 以添加收件人。

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

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

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

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

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

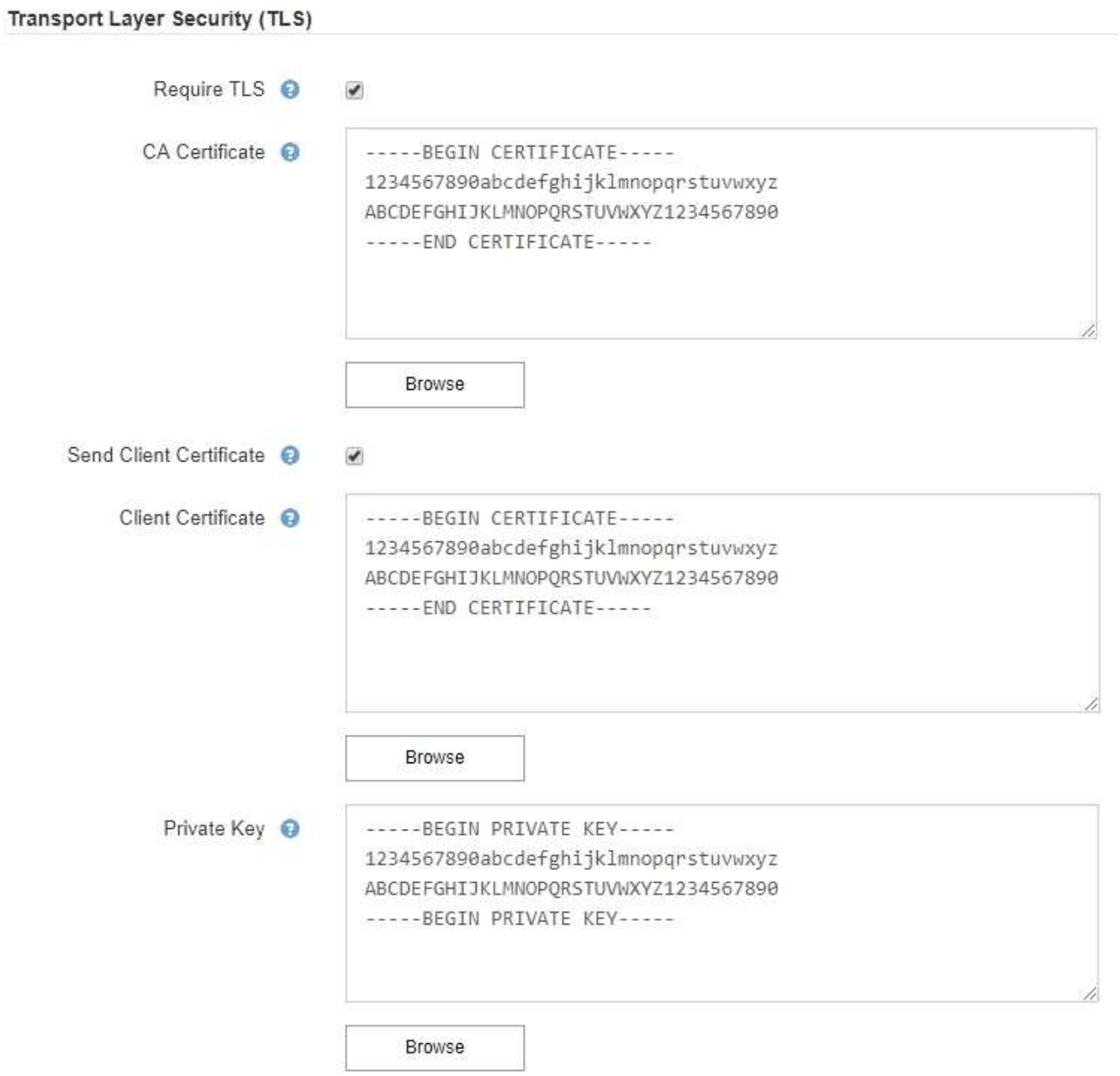
   c. 在 * 客户端证书 * 字段中，提供 PEM 编码的客户端证书以发送到 SMTP 服务器。

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

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

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

      如果需要编辑电子邮件设置，请选择铅笔图标以更新此字段。



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

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

7. 准备好测试电子邮件设置后，请执行以下步骤：
   a. 选择 * 发送测试电子邮件 * 。

      此时将显示一条确认消息，指示已发送测试电子邮件。

   b. 检查所有电子邮件收件人的收件箱，确认已收到测试电子邮件。

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

   c. 登录到任何其他管理节点并发送测试电子邮件以验证所有站点的连接。

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

8. 选择 * 保存 * 。

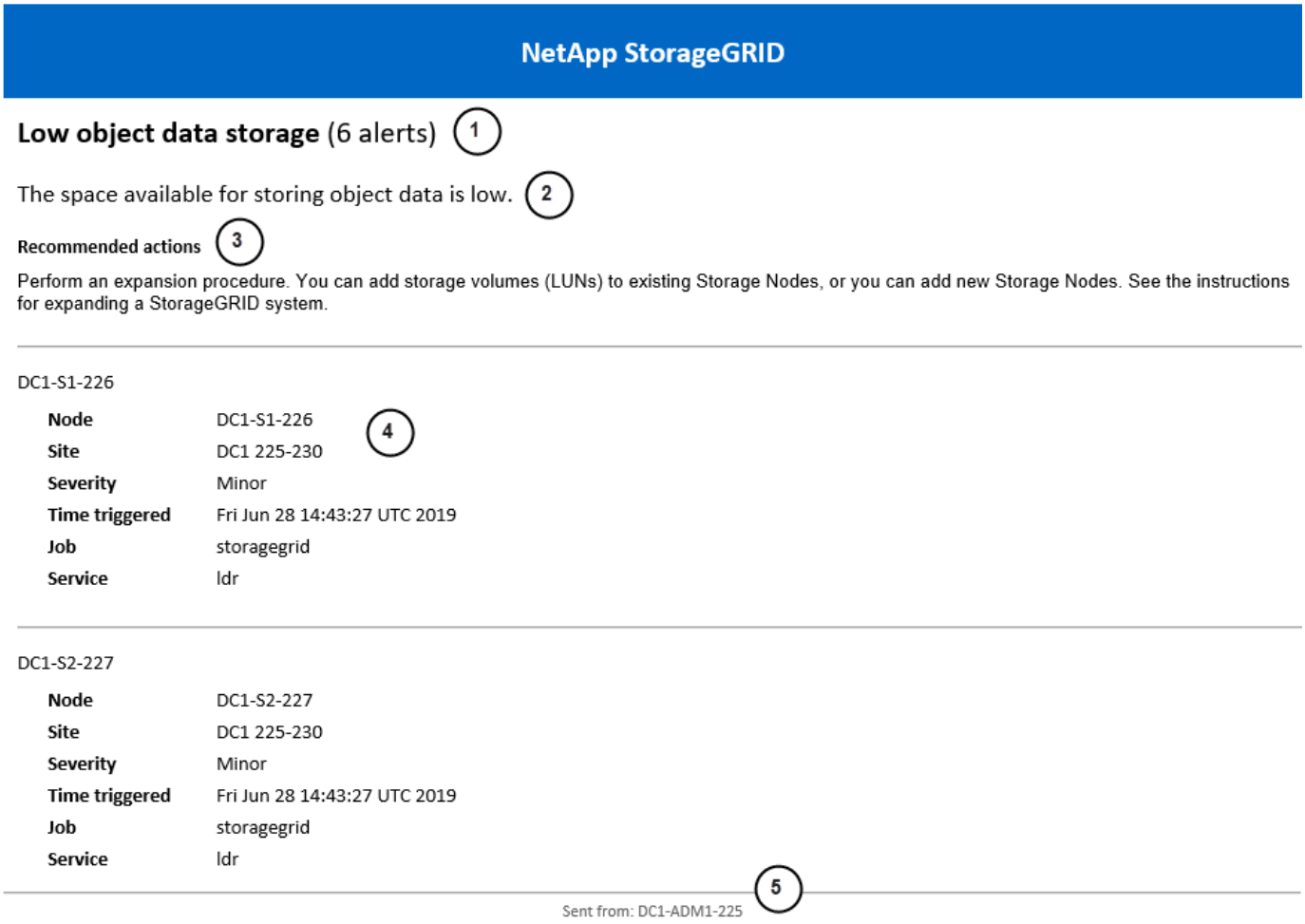
   发送测试电子邮件不会保存您的设置。您必须选择 * 保存 * 。

   此时将保存电子邮件设置。

警报电子邮件通知中包含的信息

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

电子邮件通知包括以下信息：



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

如何对警报进行分组

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

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

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

对警报电子邮件通知进行故障排除

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

您需要的内容

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

步骤

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

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

   请参见 收集日志文件和系统数据。

静默警报通知

或者，您也可以配置静音以临时禁止警报通知。

您需要的内容

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

关于此任务

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

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

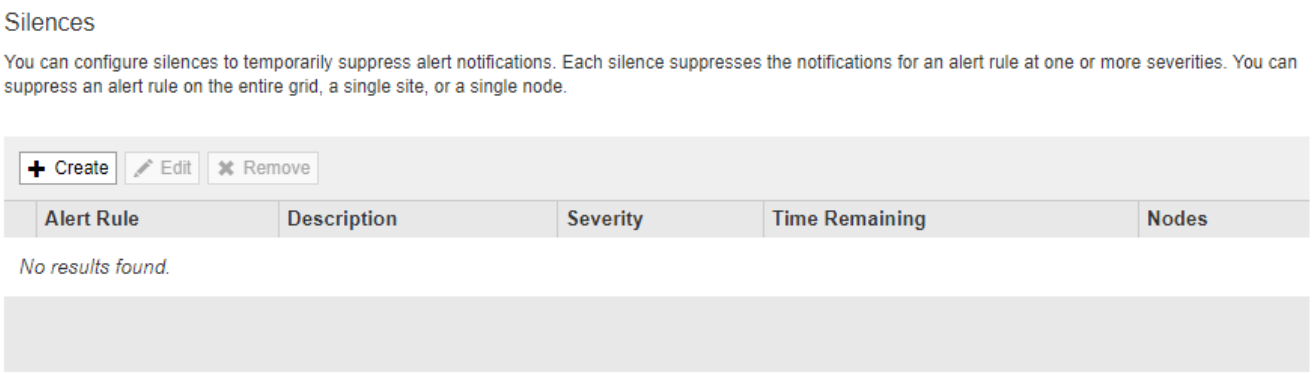
> 在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

> 由于警报和警报是独立的系统，因此不能使用此功能禁止警报通知。

步骤

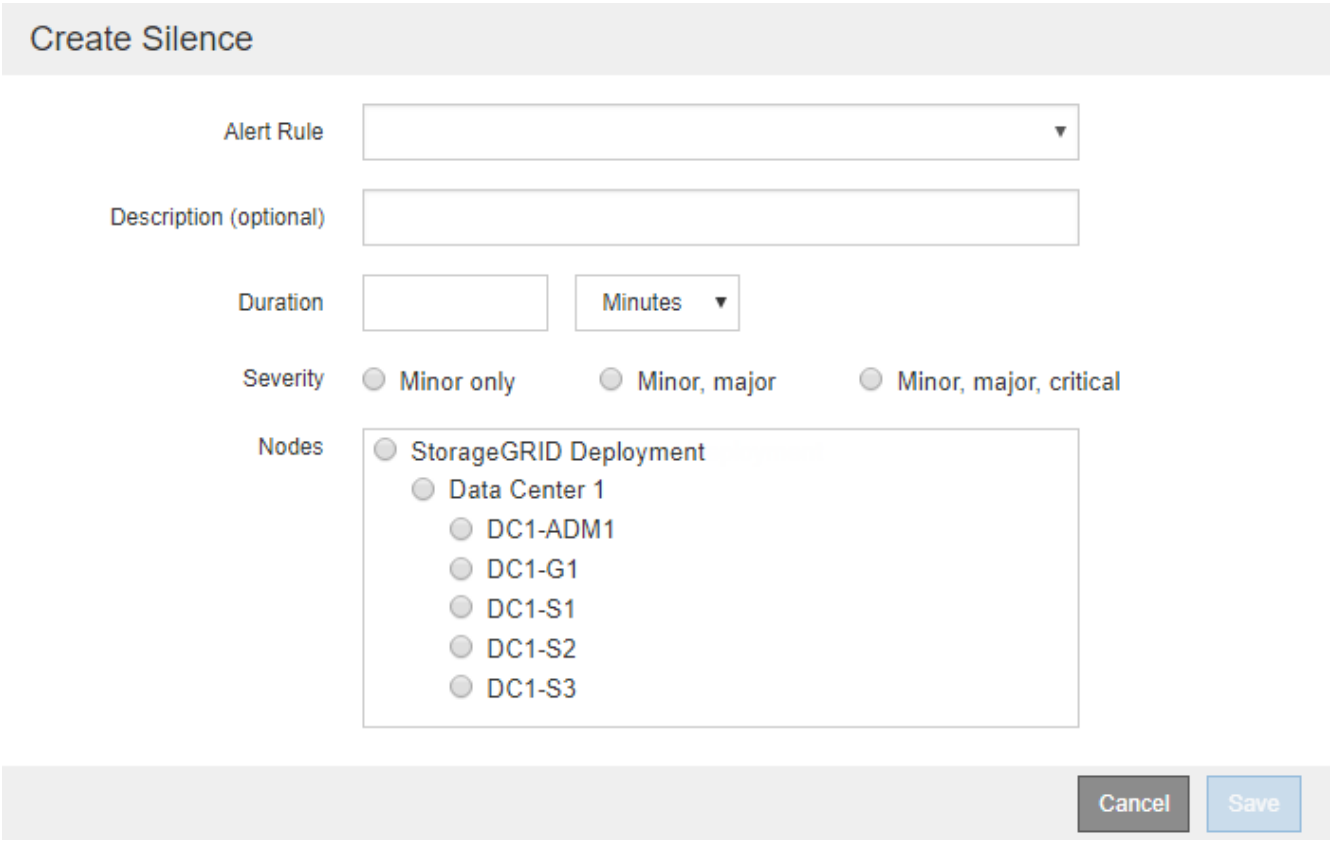
1. 选择 * 警报 * > * 静音 * 。

   此时将显示 Silences 页面。



2. 选择 * 创建 * 。

   此时将显示创建静默对话框。



3. 选择或输入以下信息：

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

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

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

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

相关信息

- 配置 SNMP 代理

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

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

警报类（旧系统）

旧警报可以属于两个相互排斥的警报类之一。

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

警报触发逻辑（旧系统）

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

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

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

请注意，严重性级别为 " 正常 " 不会触发警报。

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

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

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

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

警报触发示例

您可以使用此示例了解如何触发全局自定义警报和默认警报。

对于以下示例，属性定义并启用了全局自定义警报和默认警报，如下表所示。

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

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

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

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

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

严重性相同的警报

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

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

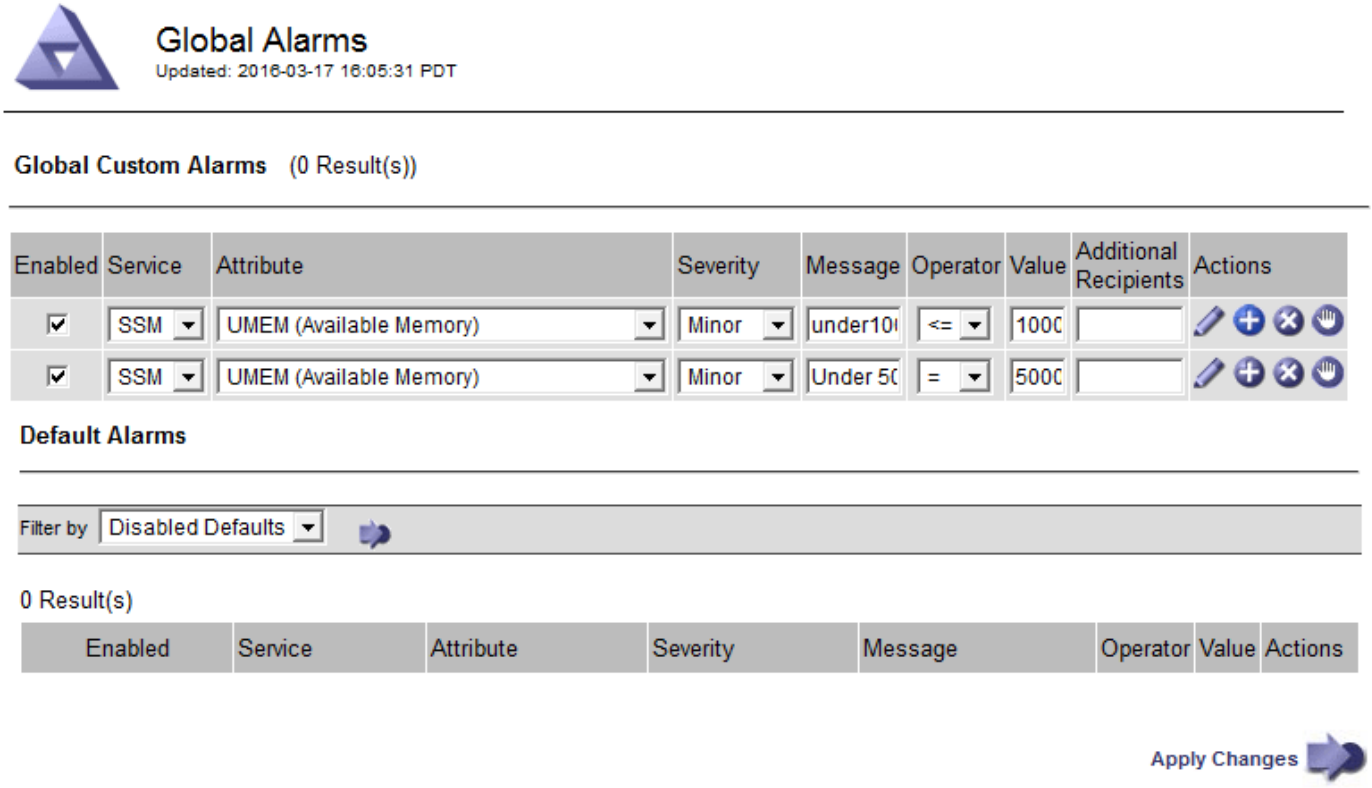
Global Alarms

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

Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
☑	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
☑	SSM	UMEM (Available Memory)	Minor	under10	<=	1000		

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



通知

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

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

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

新服务

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

警报和表

表中显示的警报属性可以在系统级别禁用。不能为表中的各个行禁用警报。

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

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

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

确认当前警报（旧系统）

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

您需要的内容

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

关于此任务

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

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

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

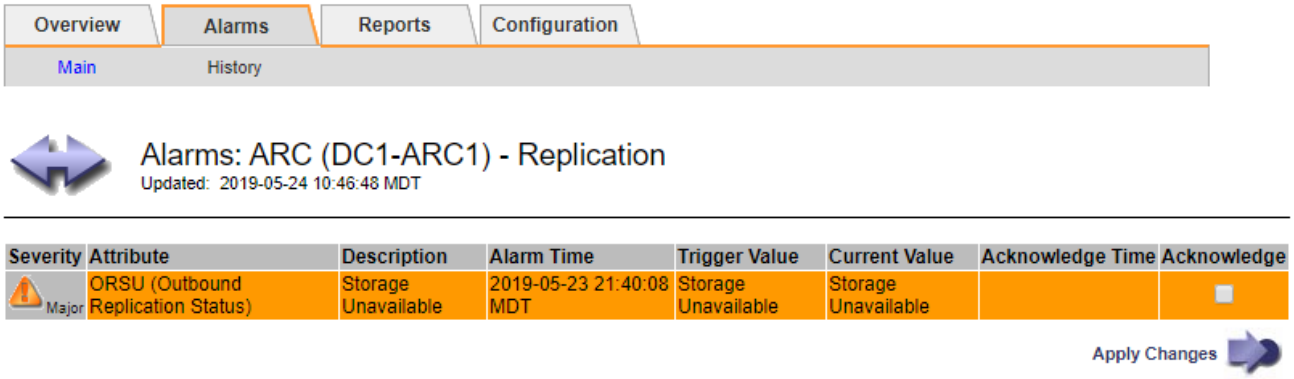
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

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

2. 在表中选择服务名称。

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



3. 选中警报的 * 确认 * 复选框，然后单击 * 应用更改 * 。

   警报不再显示在信息板或当前警报页面上。

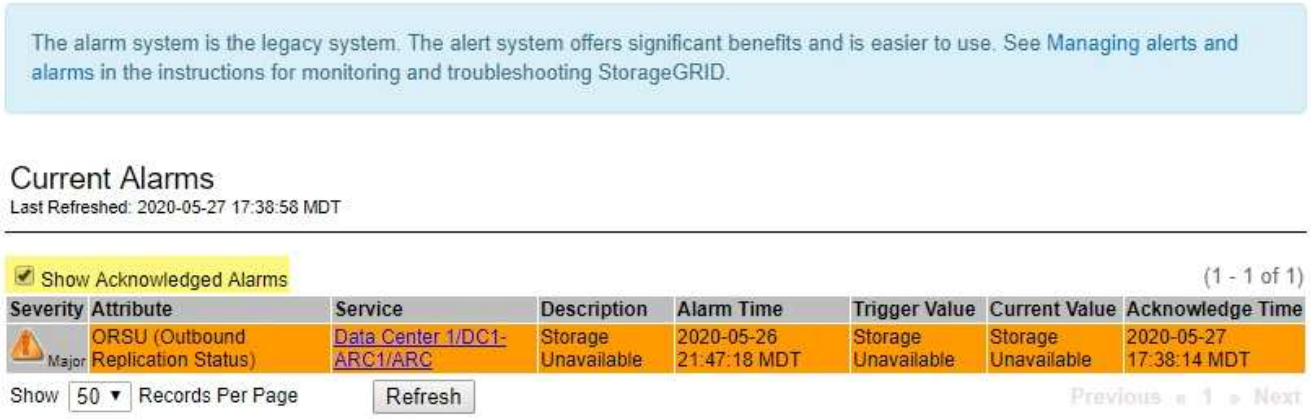
   确认警报后，确认不会复制到其他管理节点。因此，如果您从另一个管理节点查看信息板，则可能仍会看到活动警报。

4. 根据需要查看已确认的警报。

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

   b. 选择 * 显示已确认警报 * 。

      此时将显示任何已确认的警报。



查看默认警报（旧系统）

您可以查看所有默认旧警报的列表。

您需要的内容

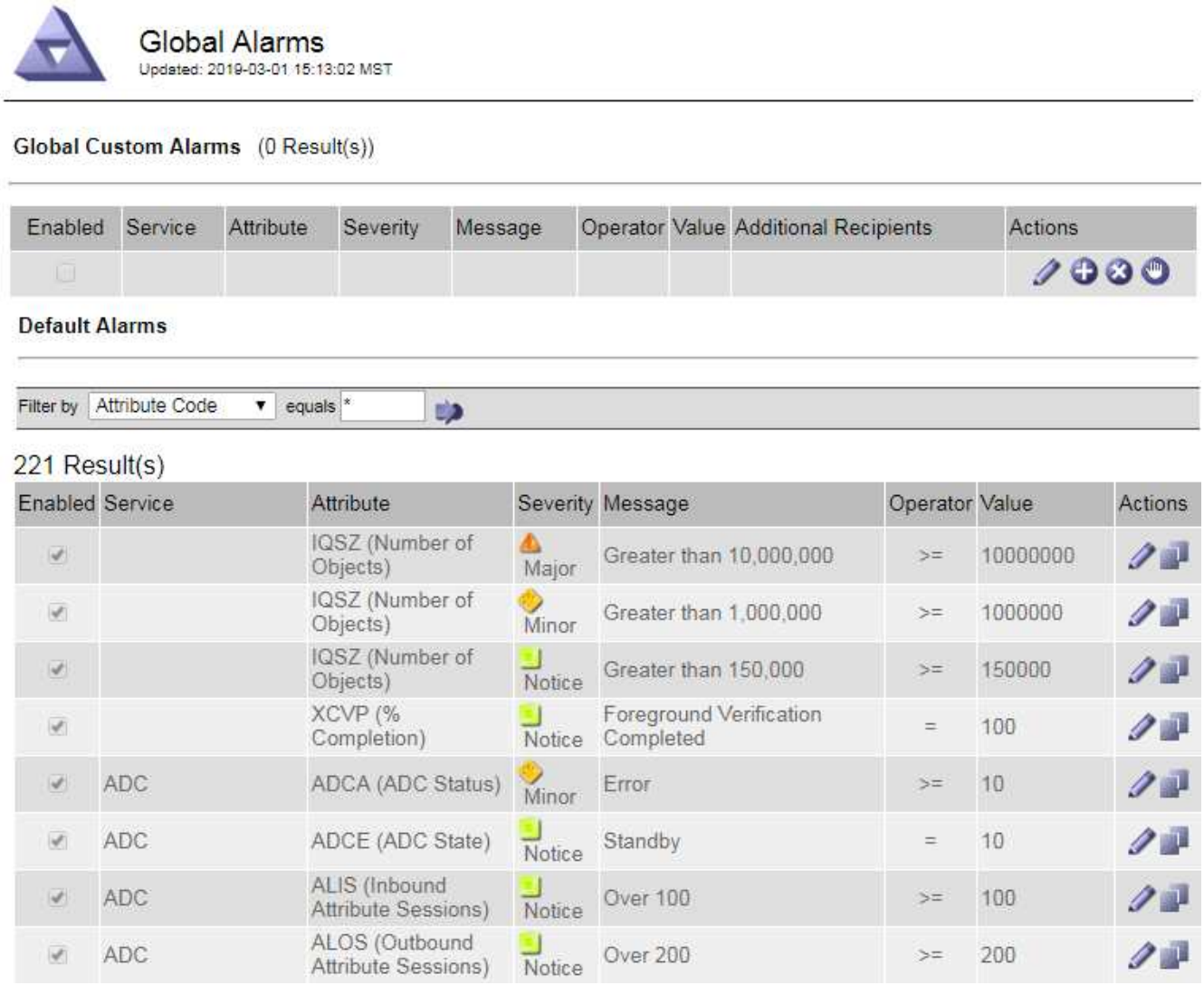
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

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

   此时将列出所有默认警报。



查看历史警报和警报频率（传统系统）

对问题描述 进行故障排除时，您可以查看过去触发传统警报的频率。

您需要的内容

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

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

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

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

创建全局自定义警报（旧系统）

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

您需要的内容

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

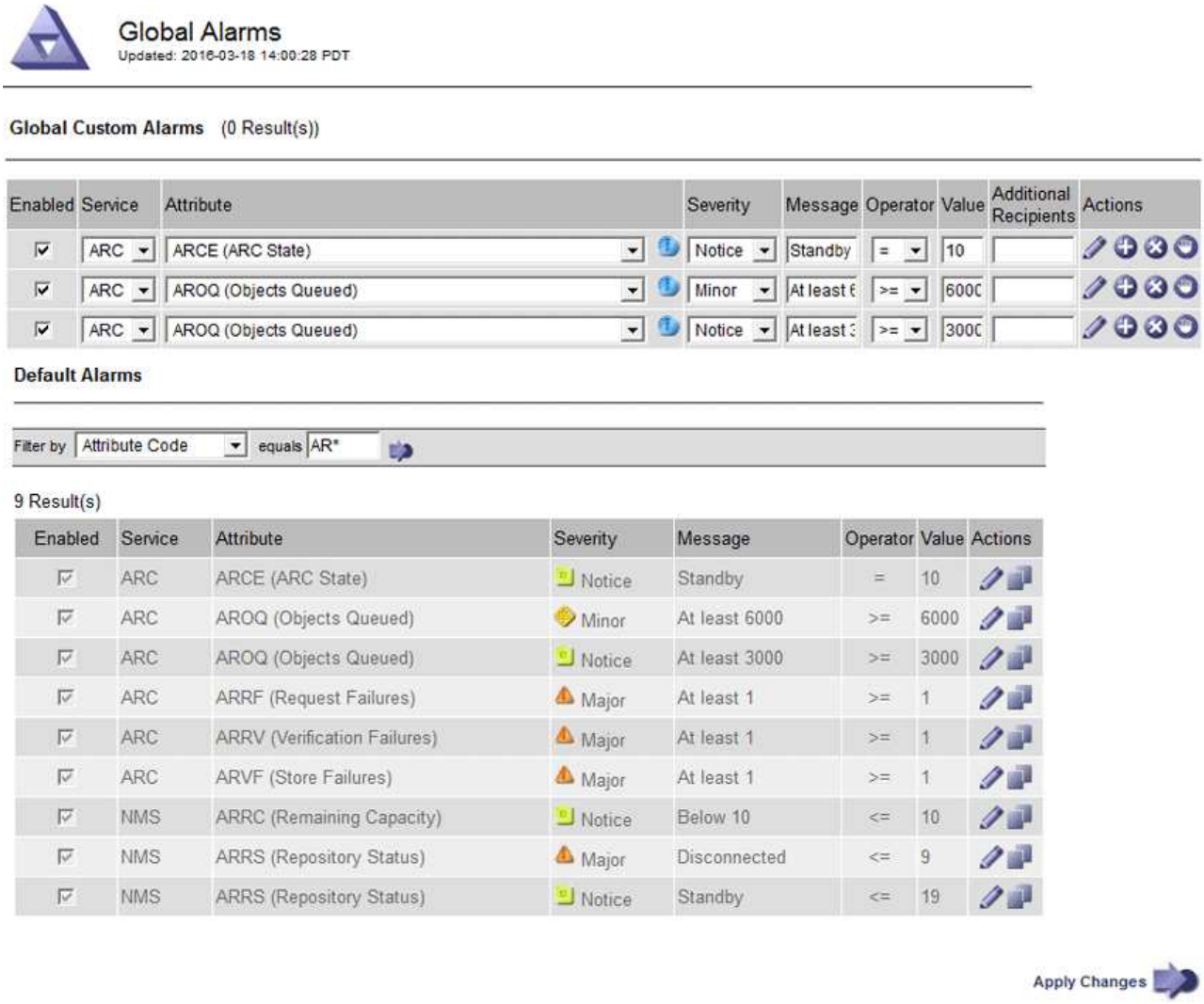
虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

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

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

步骤

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



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

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

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

  默认警报将复制到全局自定义警报表。

3. 对全局自定义警报设置进行任何必要的更改：

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

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

4. 单击 * 应用更改 * 。

禁用警报（旧系统）

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

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

禁用默认警报（传统系统）

您可以为整个系统禁用一个原有的默认警报。

您需要的内容

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

关于此任务

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

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

步骤

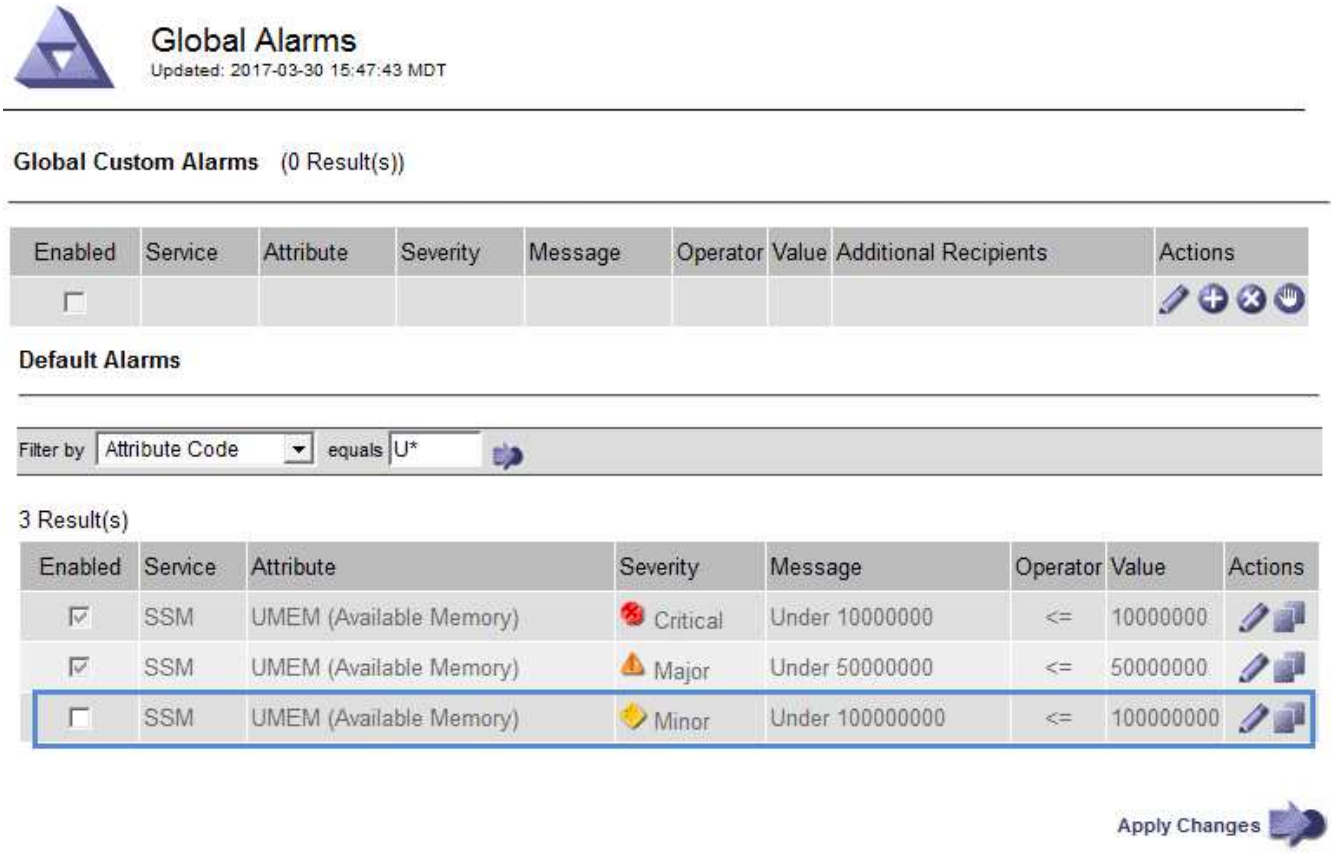
1. 选择 * 支持 * > * 警报（原有） * > * 全局警报 * 。
2. 搜索要禁用的默认警报。
   a. 在默认警报部分中，选择 * 筛选依据 * > * 属性代码 * 或 * 属性名称 * 。
   b. 键入搜索字符串。

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

   c. 单击箭头 ，或按 * 输入 * 。

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

3. 在搜索结果表中，单击编辑图标 要禁用的警报。



选定警报的 * 已启用 * 复选框将变为活动状态。

4. 取消选中 * 已启用 * 复选框。
5. 单击 * 应用更改 * 。

默认警报已禁用。

禁用全局自定义警报（旧系统）

您可以为整个系统禁用旧版全局自定义警报。

您需要的内容

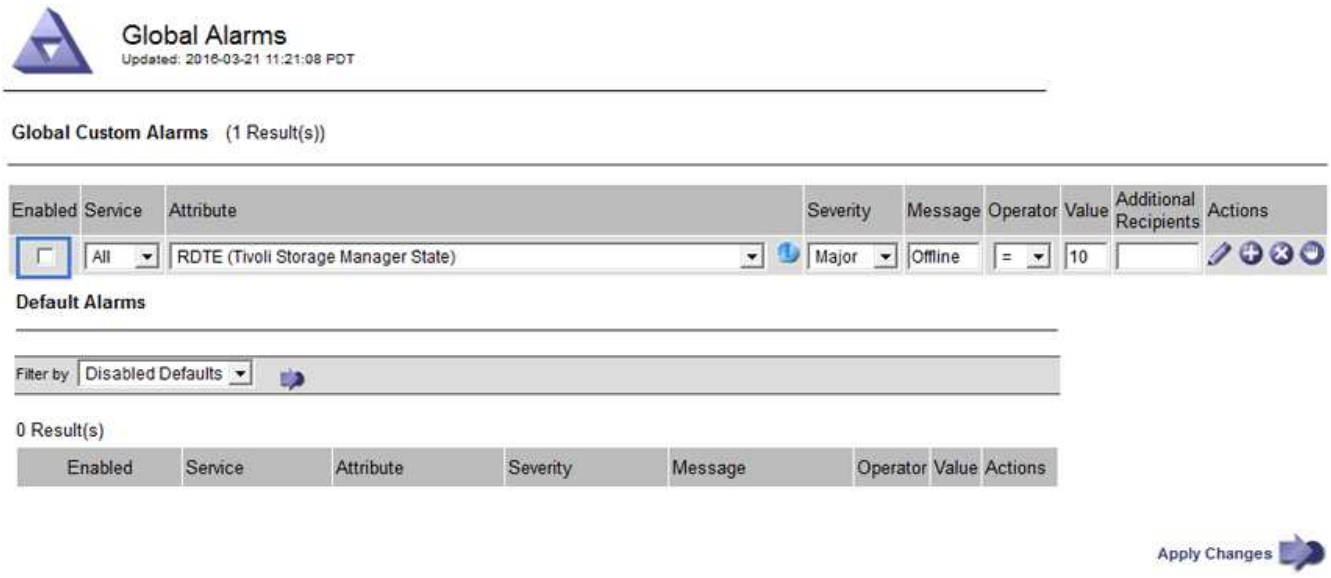
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

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

步骤

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



4. 单击 * 应用更改 * 。

   已禁用全局自定义警报。

清除触发的警报（旧系统）

如果触发了旧警报，您可以清除它，而不是确认它。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

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

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

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

   警报已清除。

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

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

警报通知类型（旧系统）

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

严重性级别通知

在选定严重性级别触发旧警报时，系统会发送警报电子邮件通知：

- 通知
- 次要
- major
- 严重

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

服务状态通知

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

- 未知
- 已管理员关闭

邮件列表将接收与选定状态下的更改相关的所有通知。

为警报配置电子邮件服务器设置（旧系统）

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

您需要的内容

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

关于此任务

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

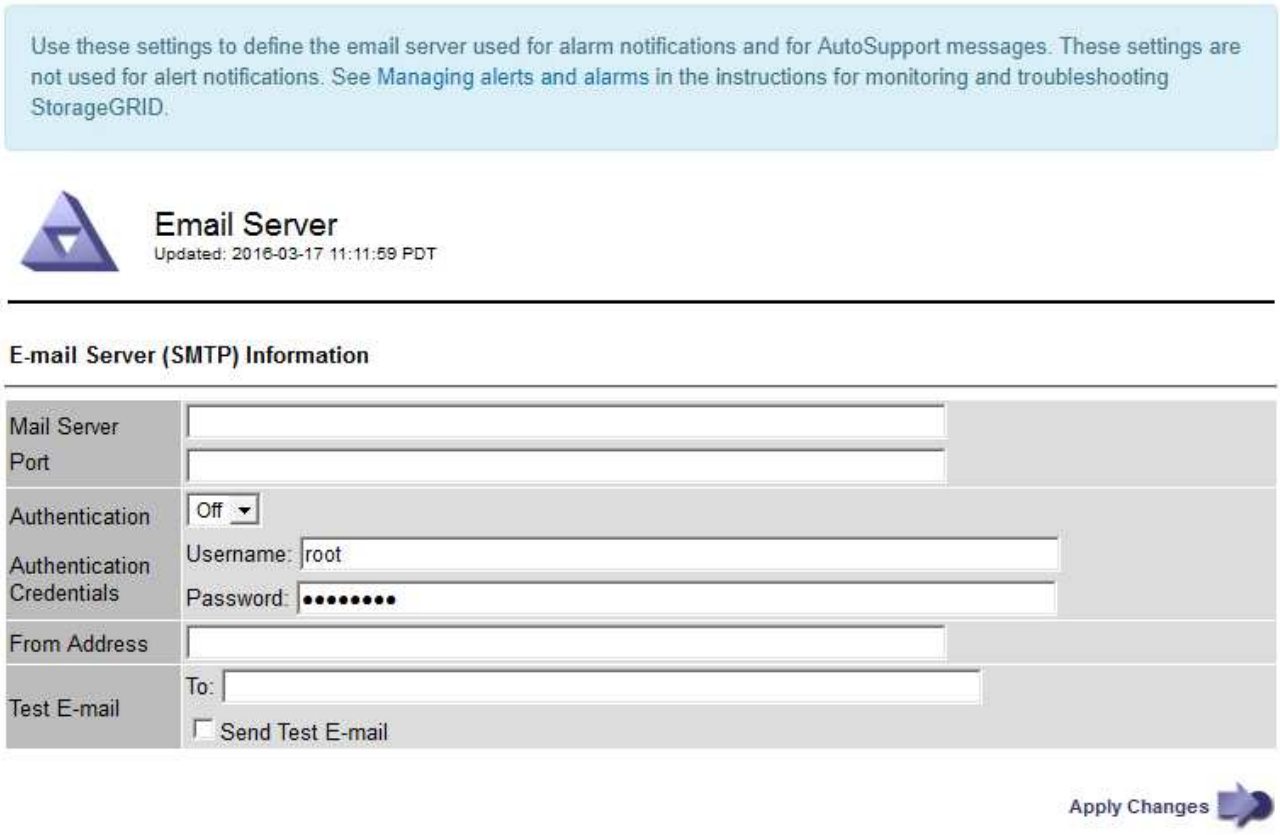
> 如果使用 SMTP 作为 AutoSupport 消息的协议，则可能已配置 SMTP 邮件服务器。同一个 SMTP 服务器用于警报电子邮件通知，因此您可以跳过此操作步骤 。请参见 有关管理 StorageGRID 的说明。

SMTP 是唯一支持发送电子邮件的协议。

步骤

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

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



3. 添加以下 SMTP 邮件服务器设置：

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

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

5. （可选）发送测试电子邮件以确认 SMTP 邮件服务器设置正确无误。
   a. 在 * 测试电子邮件 * > * 至 * 框中，添加一个或多个可访问的地址。

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

   b. 选择 * 发送测试电子邮件 * 。
6. 单击 * 应用更改 * 。

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

创建警报电子邮件模板（旧系统）

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

您需要的内容

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

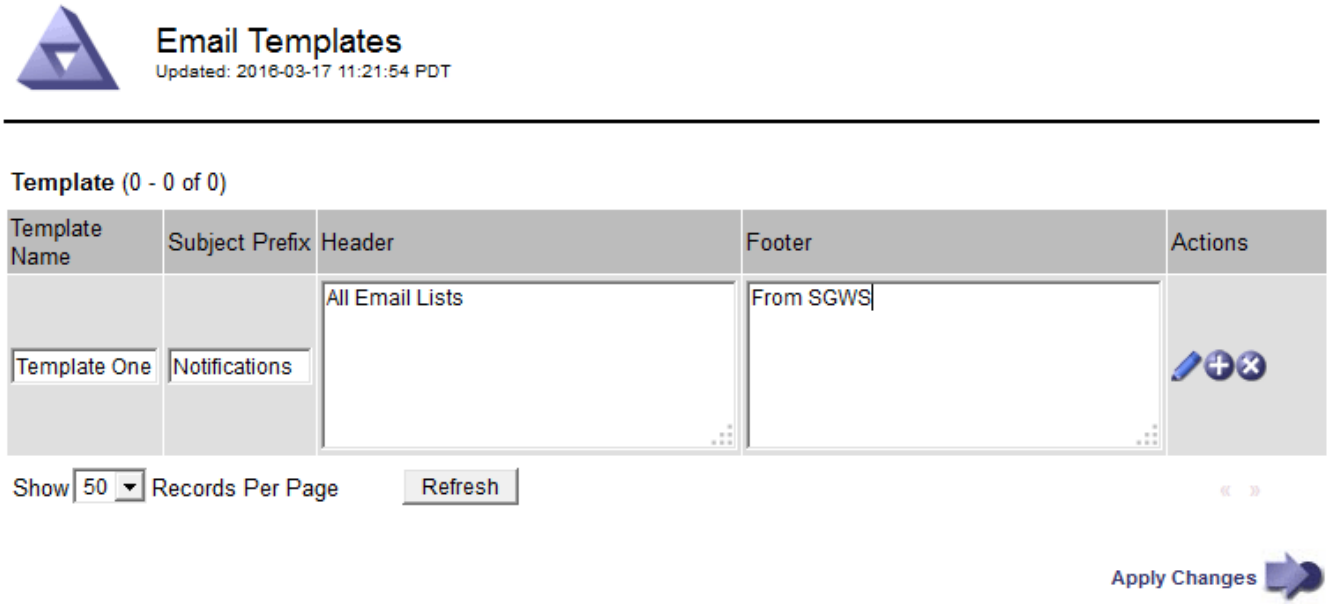
关于此任务

使用这些设置可以定义用于旧警报通知的电子邮件模板。这些设置不用于警报通知。

不同的邮件列表可能需要不同的联系信息。模板不包含电子邮件的正文。

步骤

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



4. 在新行中添加以下内容：

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

5. 单击 * 应用更改 * 。

   此时将为通知添加一个新模板。

为警报通知创建邮件列表（旧系统）

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

您需要的内容

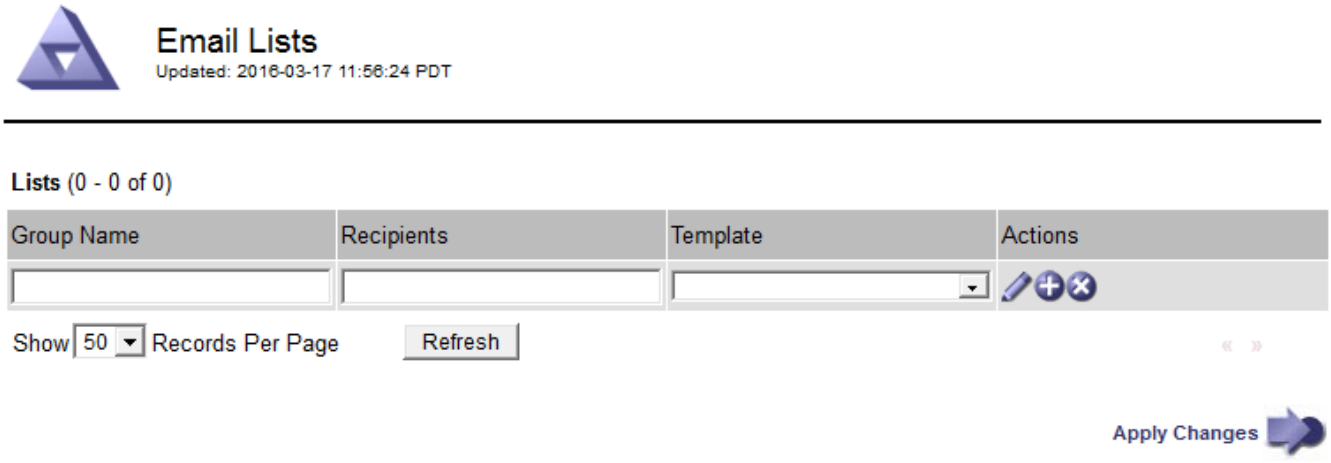
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 如果要为邮件列表指定电子邮件模板（自定义页眉，页脚和主题行），则必须已创建此模板。

关于此任务

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

步骤

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



4. 在新行中，添加以下内容：

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

5. 单击 * 应用更改 * 。

   此时将创建一个新的邮件列表。

配置警报电子邮件通知（旧系统）

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

您需要的内容

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

关于此任务

使用这些设置为旧警报配置通知。这些设置不用于警报通知。

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

步骤

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

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

禁止发送邮件列表的警报通知（旧系统）

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

您需要的内容

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

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

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

步骤

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

   选定邮件列表将禁止使用旧警报通知。

在系统范围内禁止电子邮件通知

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

您需要的内容

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

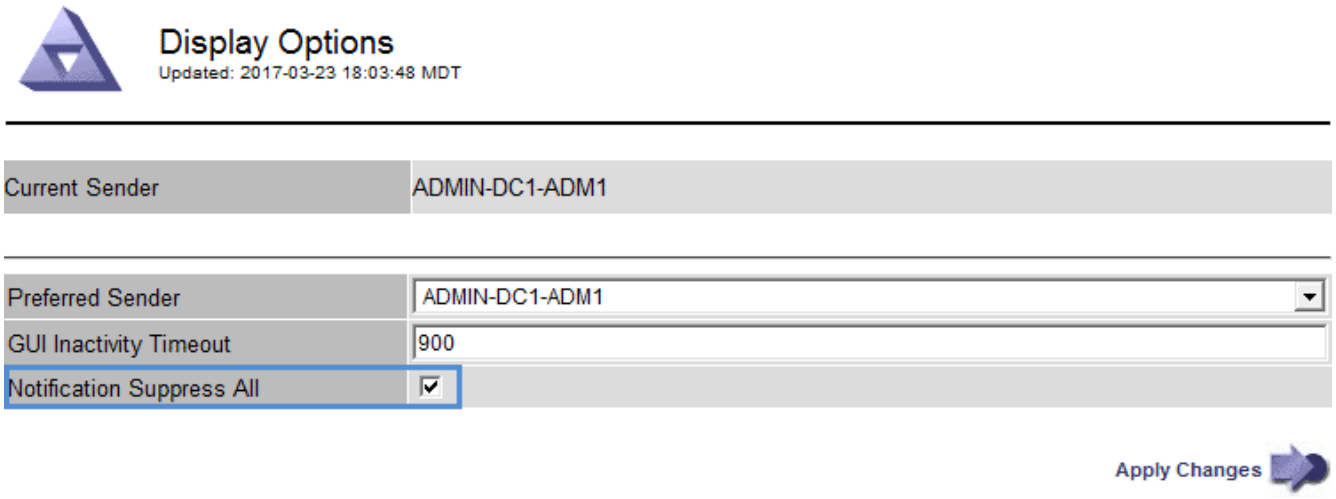
关于此任务

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

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

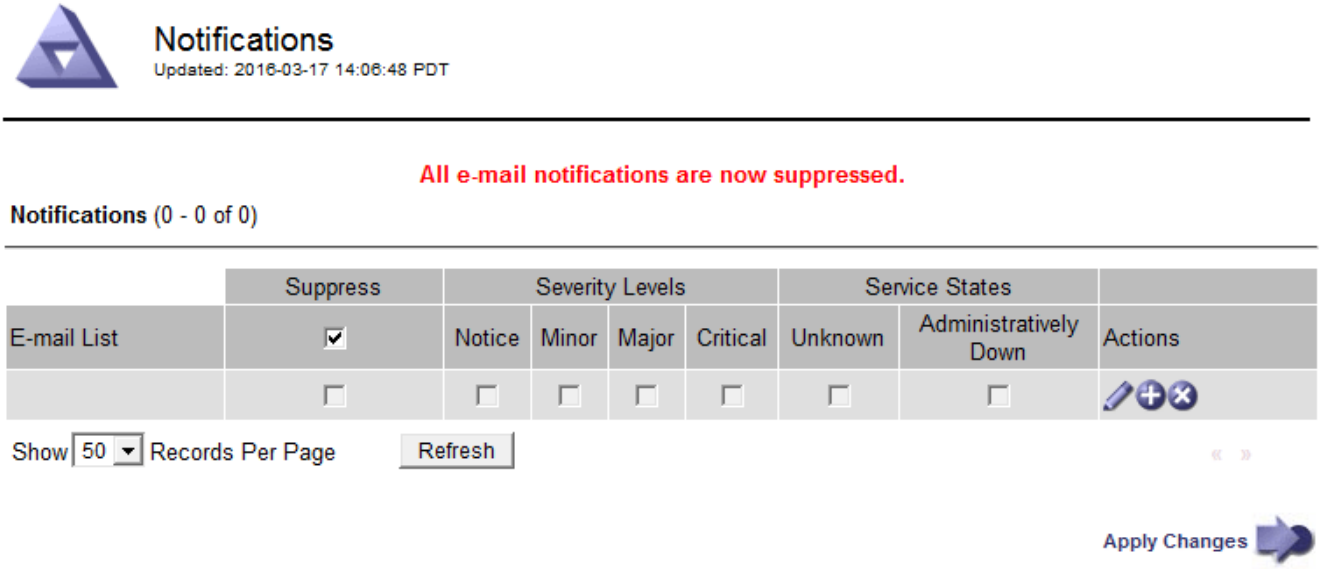
步骤

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



4. 单击 * 应用更改 * 。

通知页面（ * 配置 * > * 通知 * ）显示以下消息：



配置审核消息和日志目标

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

有关审核消息的详细信息，请参见 查看审核日志。

您需要的内容

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

关于此任务

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

更改审核日志中的审核消息级别

您可以为审核日志中的以下每种消息设置不同的审核级别：

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

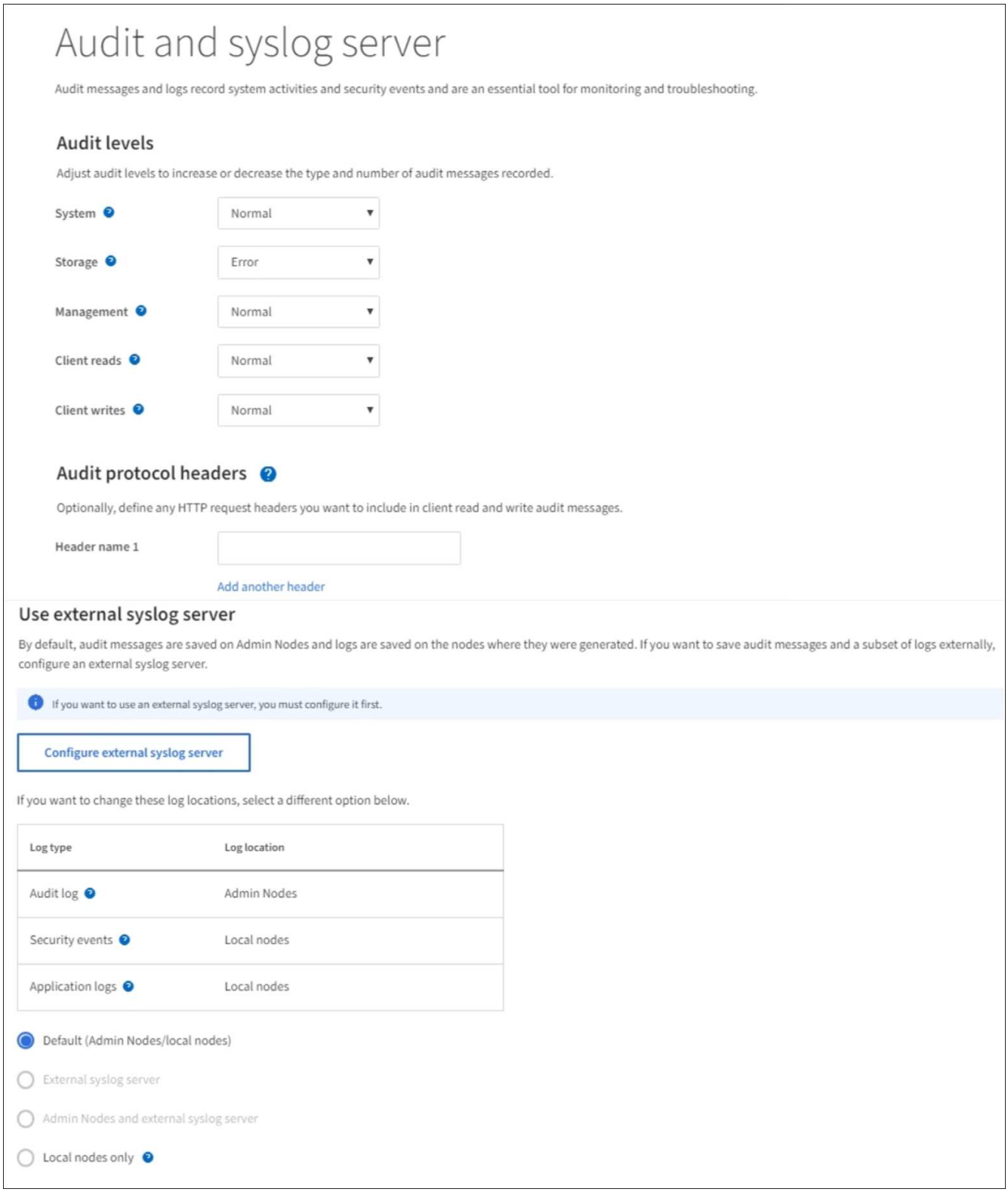
审核类别	Description
客户端写入	默认情况下，此级别设置为 " 正常 " 。请参见 客户端写入审核消息。

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

升级期间，审核级别配置不会立即生效。

步骤

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



2. 对于每个审核消息类别，从下拉列表中选择一个审核级别：

审核级别	Description
关闭	不会记录此类别中的任何审核消息。

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

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

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

   审核协议标头仅适用于 S3 和 Swift 请求。

4. 如果需要，选择 * 添加另一个标题 * 以创建其他标题。

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

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

5. 选择 * 保存 *

   此时将显示一个绿色横幅，指示您的配置已成功保存。

使用外部系统日志服务器

如果要远程保存审核信息，可以配置外部系统日志服务器。

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

选择审核信息目标

您可以指定将审核日志，安全事件日志和应用程序日志发送到何处。

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

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

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

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

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

1. 选择 * 保存 * 。

此时将显示一条警告消息：

是否更改日志目标?

1. 选择 * 确定 * 以确认要更改审核信息的目标。

   此时将显示一个绿色横幅，通知您已成功保存审核配置。

   新日志将发送到选定的目标。现有日志将保留在其当前位置。

相关信息

外部系统日志服务器的注意事项

管理 StorageGRID

对外部系统日志服务器进行故障排除

使用外部系统日志服务器

外部系统日志服务器的注意事项

请按照以下准则估算所需外部系统日志服务器的大小。

什么是外部系统日志服务器?

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

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

如何估算外部系统日志服务器的大小

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

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

在估计公式中使用每秒 **S3** 操作数

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

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

审核日志的估计公式

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

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

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

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

称）：

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

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

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

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

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

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

非默认审核级别的估计公式

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

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

安全事件的估计公式

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

应用程序日志的估计公式

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

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

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

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

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

规模估算示例

本节介绍了如何使用网格估算公式和以下数据保护方法的示例案例：

- Replication
- 纠删编码

如果使用复制来保护数据

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

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

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

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

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

如果您使用纠删编码进行数据保护

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

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

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

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

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

有关配置审核消息级别和外部系统日志服务器的详细信息，请参见以下内容：

- 配置外部系统日志服务器
- 配置审核消息和日志目标

配置外部系统日志服务器

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

您需要的内容

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

关于此任务

如果要将审核信息发送到外部系统日志服务器，则必须先配置外部服务器。

通过将审核信息发送到外部系统日志服务器，您可以：

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

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

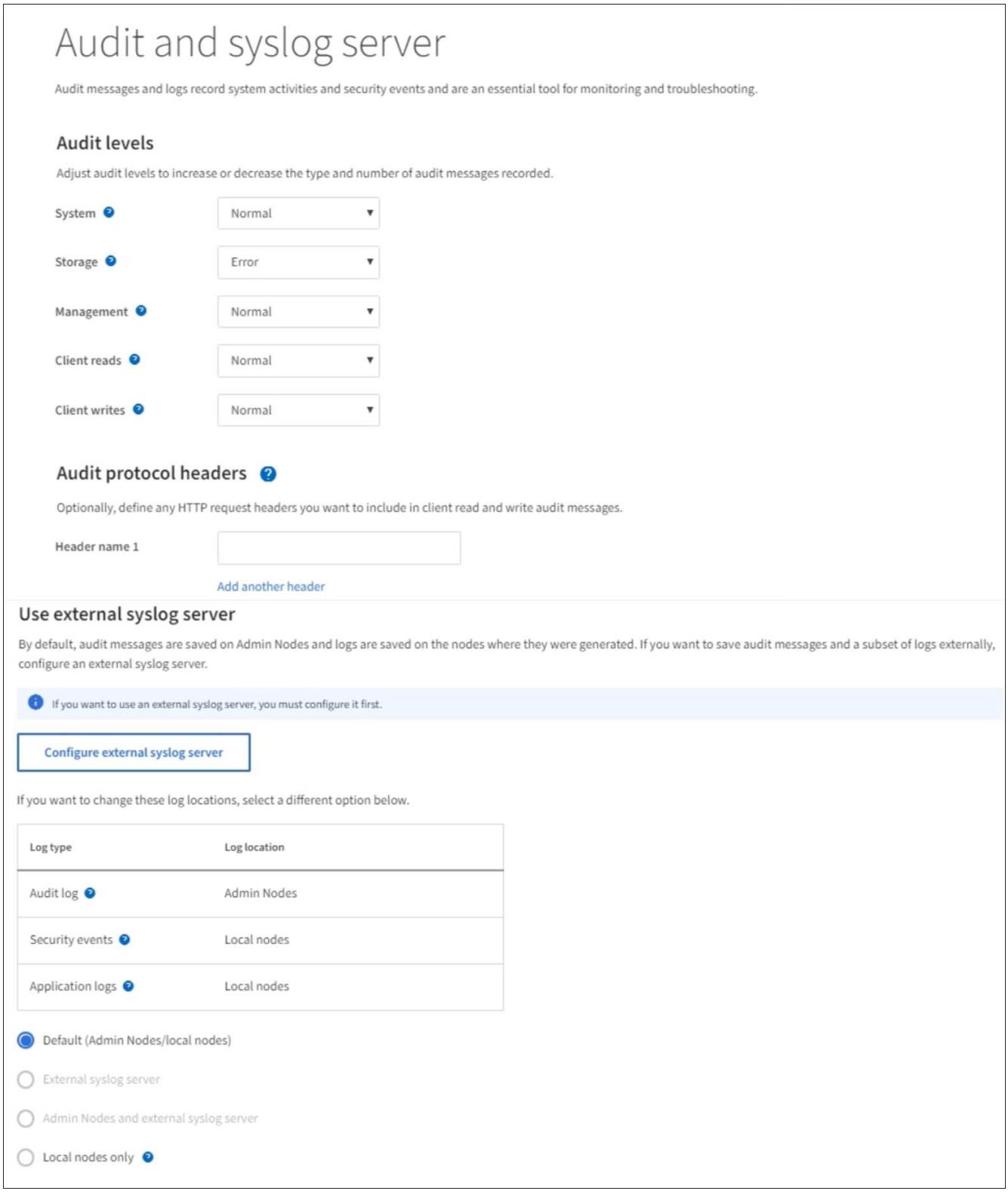
> 为了在外部系统日志服务器发生故障时最大程度地提高完整数据恢复的选项，每个节点上最多会保留 20 GB 的本地审核记录日志（ localaudit.log ）。

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

访问系统日志服务器配置向导

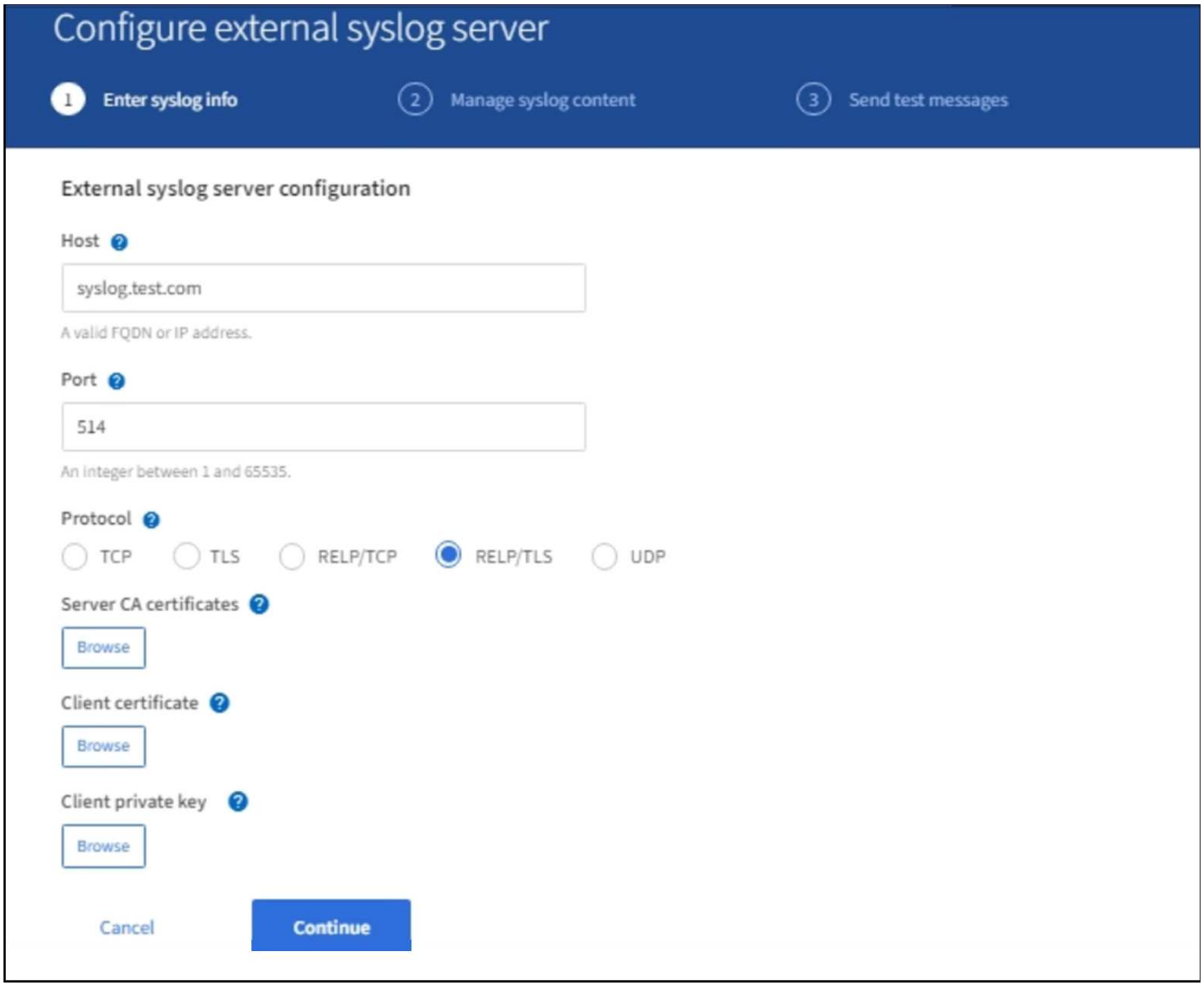
步骤

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



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

输入系统日志信息



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

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

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

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

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

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

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

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

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

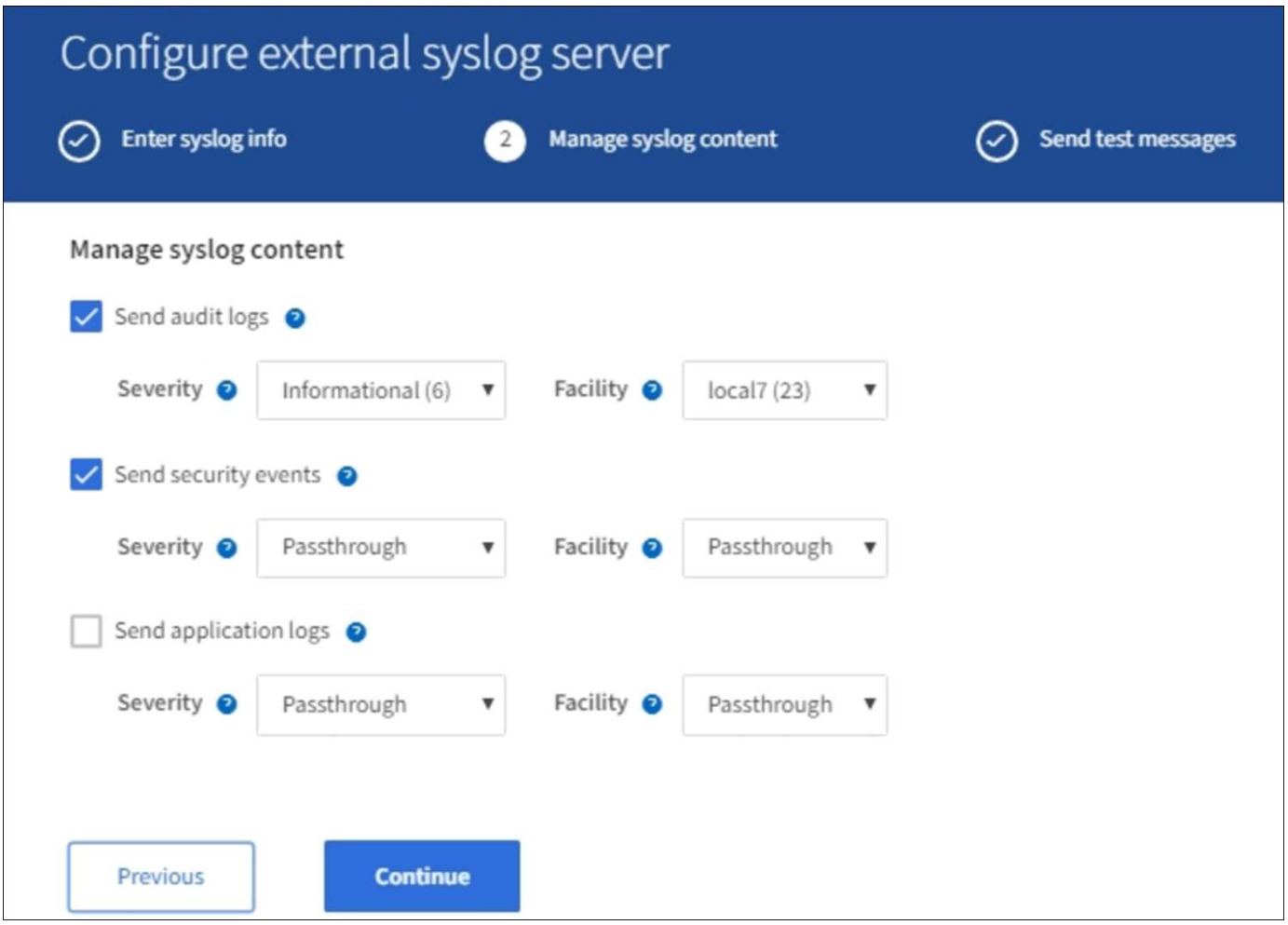
> 如果使用客户端证书，则还必须使用客户端专用密钥。如果您提供加密的私钥，则还必须提供密码短语。使用加密的私钥不会带来显著的安全优势，因为必须存储密钥和密码短语；为了简化操作，建议使用未加密的私钥（如果可用）。

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

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

6. 选择 * 继续 * 。

管理系统日志内容



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

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

2. 使用下拉菜单为要发送的审核信息类别选择严重性和工具（消息类型）。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

d. 如果不想使用直通值，请选择 0 到 23 之间的设施值。

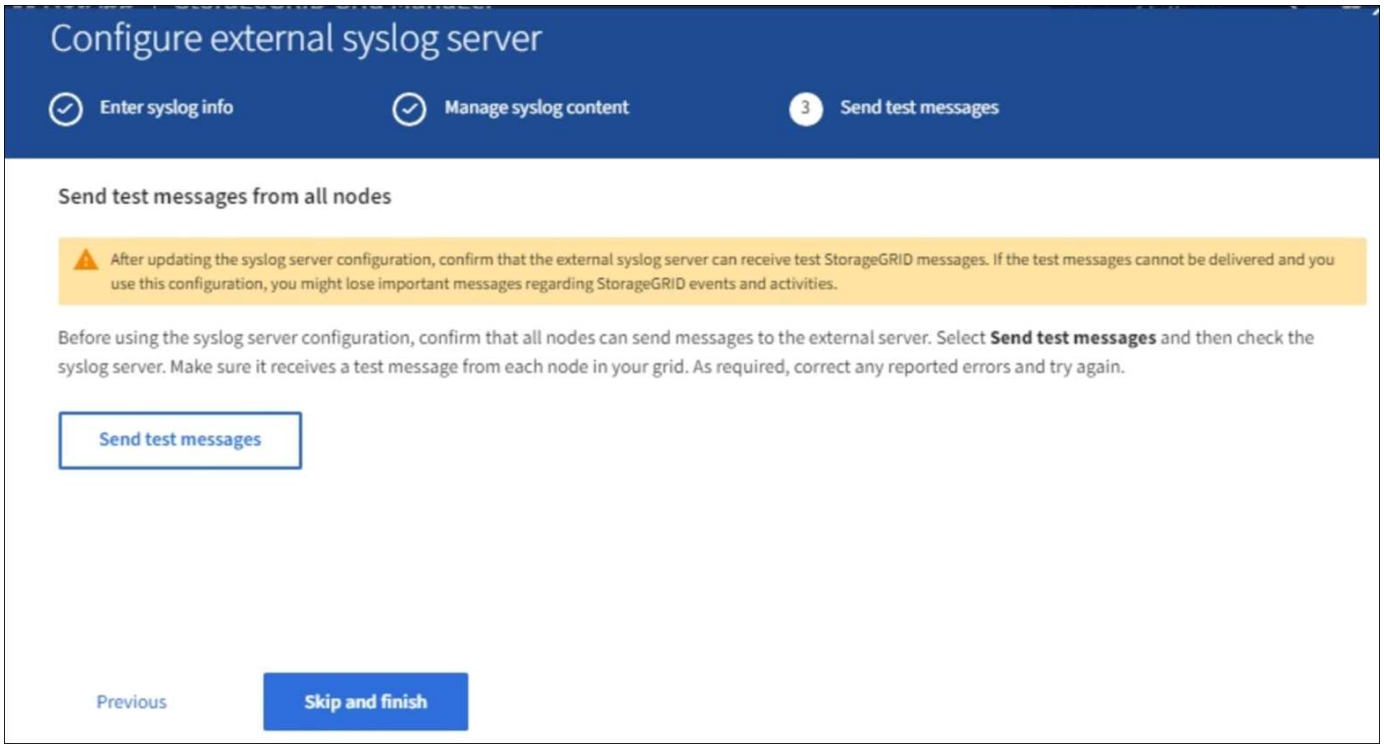
选定值将应用于此类型的所有消息。如果您选择使用固定值覆盖设施，则有关不同设施的信息将丢失。

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

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

3. 选择 * 继续 * 。

发送测试消息



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

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

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

   此时将显示一个绿色横幅，指示您的配置已成功保存。

2. 否则，请选择 * 发送测试消息 * 。

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

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

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

6. 选择 * 停止并完成 * 。

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

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

选择审核信息目标

您可以指定将安全事件日志，应用程序日志和审核消息日志发送到何处。

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

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

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

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

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

您必须确认外部系统日志服务器可以接收测试 StorageGRID 消息。

1. 选择 * 确定 * 以确认要更改审核信息的目标。

   此时将显示一个绿色横幅，通知您已成功保存审核配置。

新日志将发送到选定的目标。现有日志将保留在其当前位置。

相关信息

审核消息概述

配置审核消息和日志目标

系统审核消息

对象存储审核消息

管理审核消息

客户端读取审核消息

管理 StorageGRID

使用 **SNMP** 监控

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

- 配置 SNMP 代理
- 更新 SNMP 代理

功能

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

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

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

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

  所有三个版本的 SNMP 均支持陷阱。

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

  SNMPv2c 和 SNMPv3 支持 INFORM 。

在以下情况下会发送陷阱和通知通知通知：

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

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

- 某些警报（旧系统）会在指定的严重性级别或更高级别触发。

> 不会针对每个警报或每个警报严重性发送 SNMP 通知。

SNMP 版本支持

下表简要总结了每个 SNMP 版本支持的功能。

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

限制

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

访问 **MIB**

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

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

相关信息

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

配置 **SNMP** 代理

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

您需要的内容

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

关于此任务

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

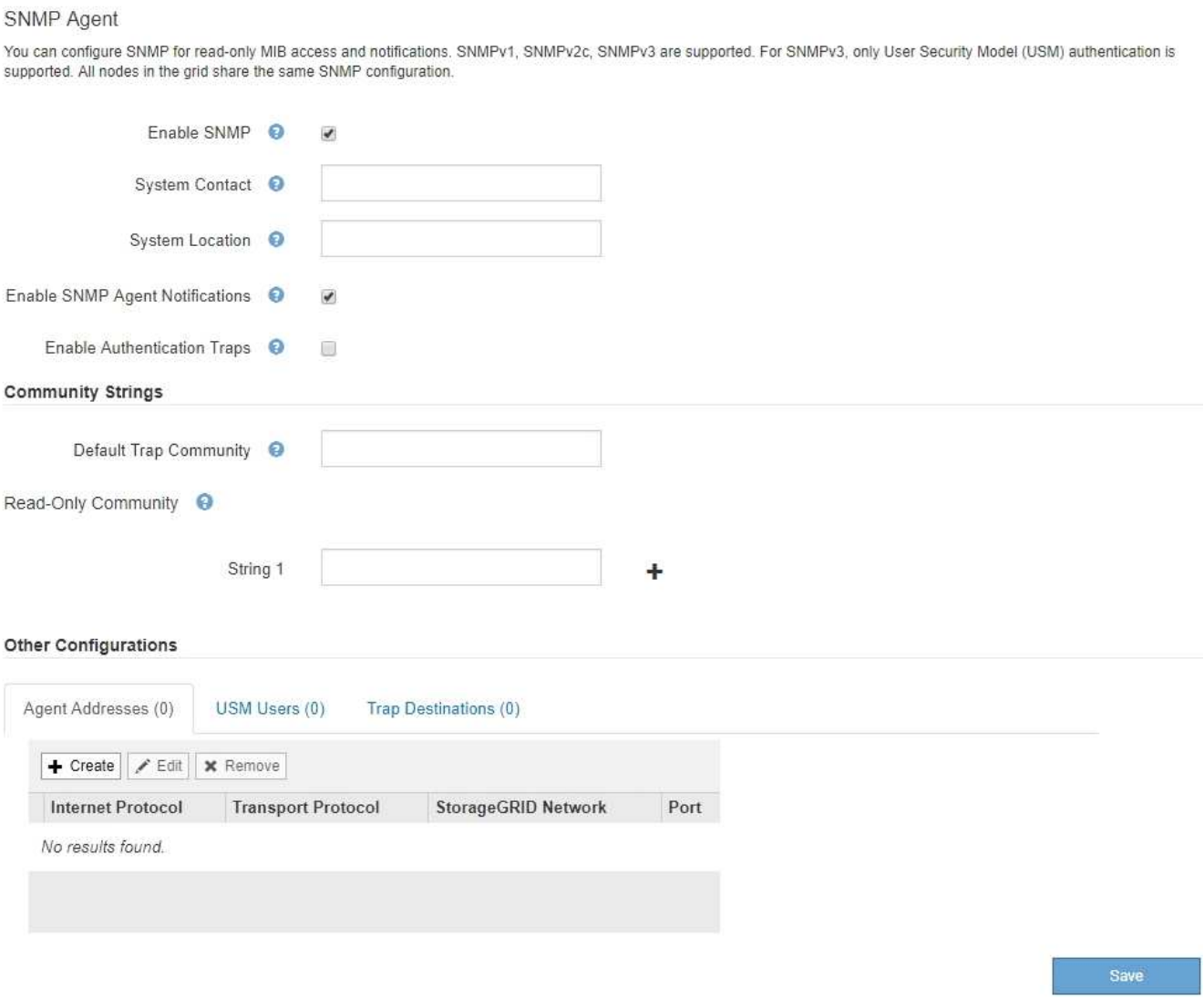
步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

   此时将显示 SNMP 代理页面。

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

   此时将显示用于配置 SNMP 代理的字段。



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

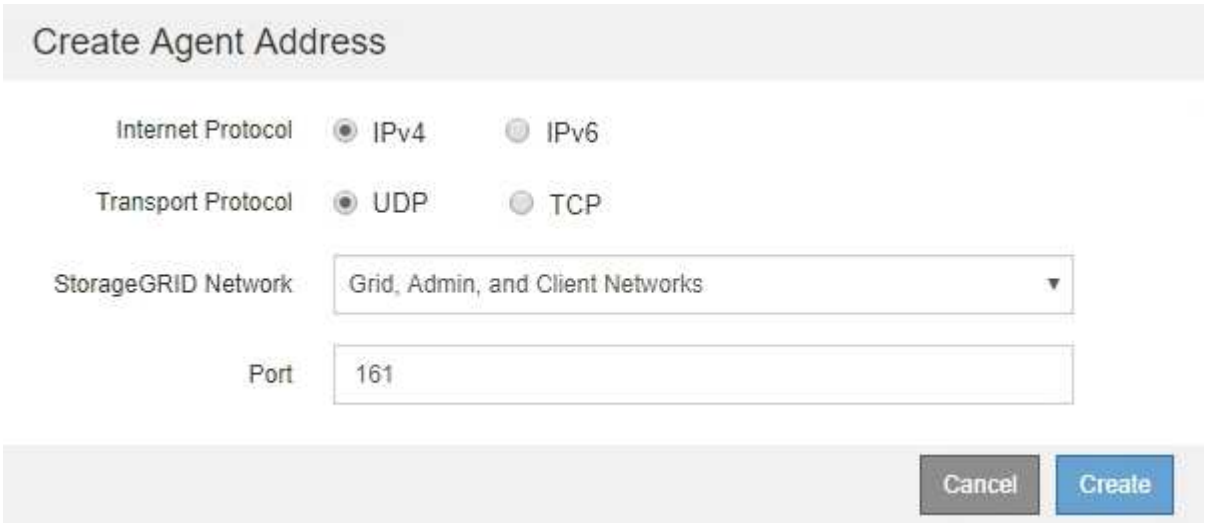
8. 也可以选择其他配置部分中的代理地址选项卡。

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

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

a. 单击 * 创建 * 。

   此时将显示创建代理地址对话框。



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

   默认情况下， SNMP 使用 IPv4 。

c. 对于 * 传输协议 * ，选择此地址是使用 UDP 还是 TCP 。

   默认情况下， SNMP 使用 UDP 。

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

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

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

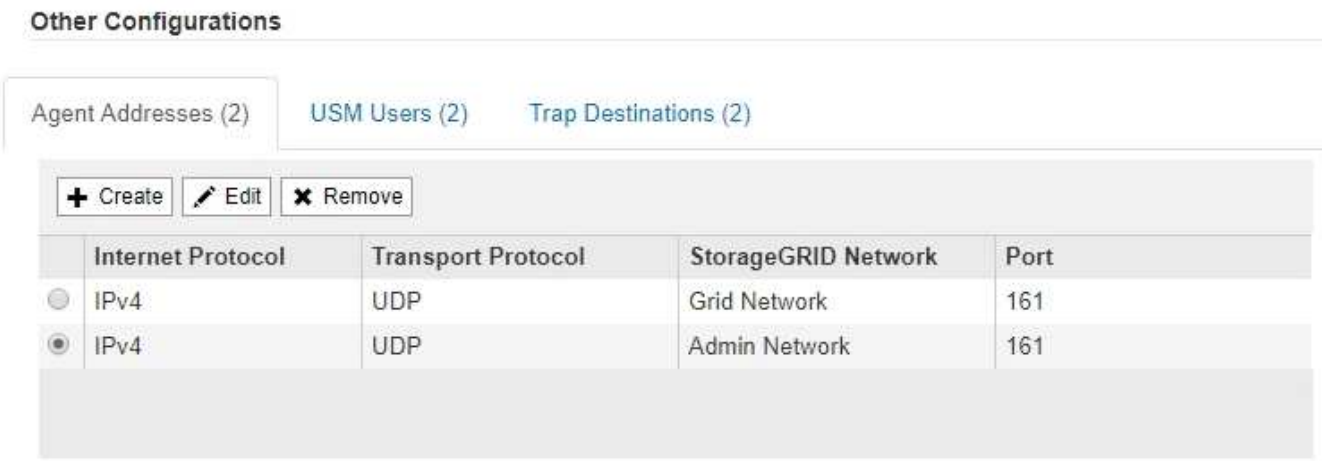
e. 在 * 端口 * 字段中，也可以输入 SNMP 代理应侦听的端口号。

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

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

f. 单击 * 创建 * 。

此时将创建代理地址并将其添加到表中。



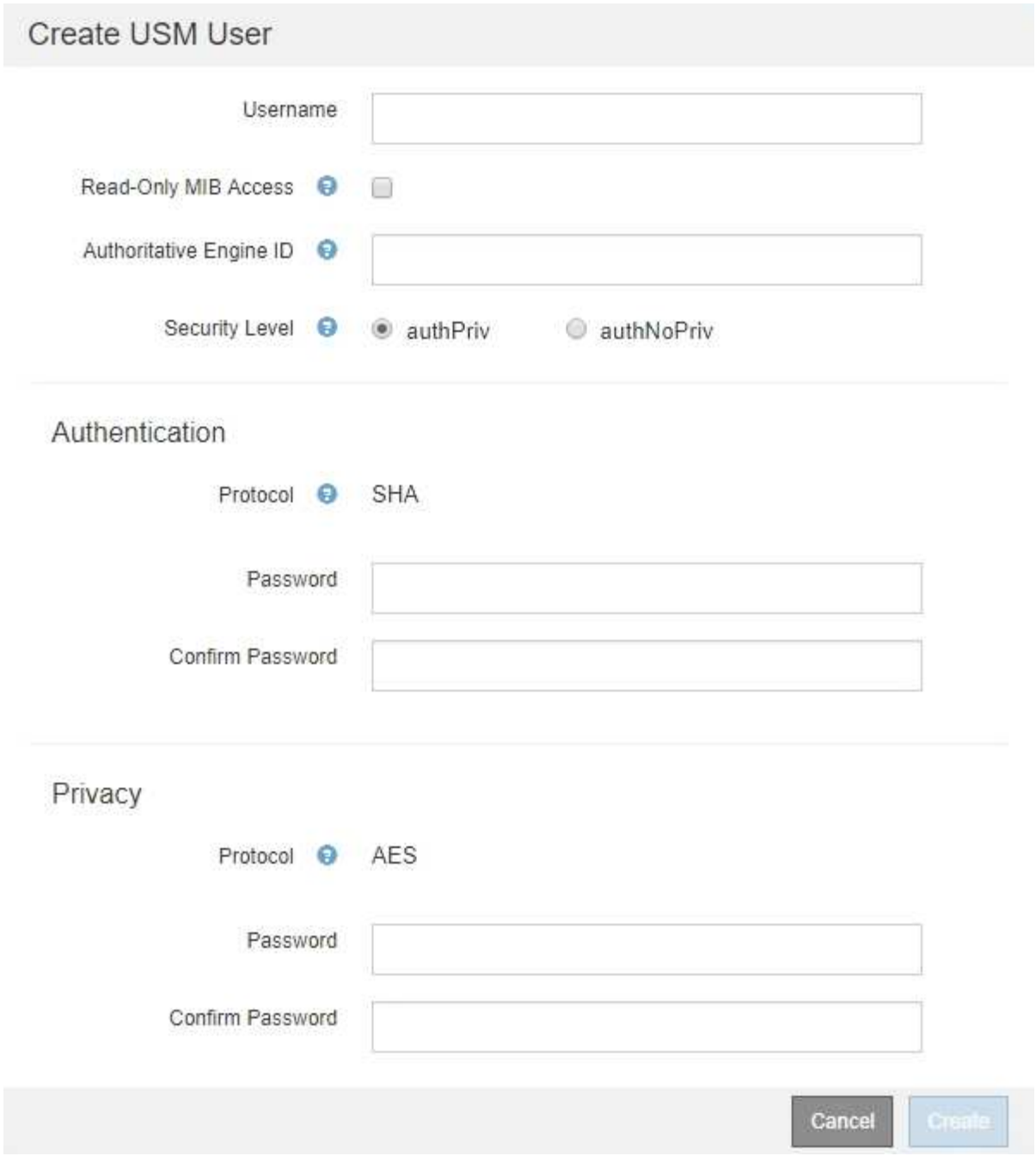
9. 如果您使用的是 SNMPv3 ，请在其他配置部分中选择 USM 用户选项卡。

使用此选项卡可定义有权查询 MIB 或接收陷阱并通知的 USM 用户。

> 如果您仅使用 SNMPv1 或 SNMPv2c ，则此步骤不适用。

a. 单击 * 创建 * 。

此时将显示创建 USM 用户对话框。



b. 为此 USM 用户输入唯一的 * 用户名 * 。

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

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

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

具有只读 MIB 访问权限的 USM 用户不能具有引擎 ID 。

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

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

权威引擎 ID 可以是 5 到 32 字节，以十六进制表示。

e. 为 USM 用户选择一个安全级别。

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

f. 输入并确认此用户将用于身份验证的密码。

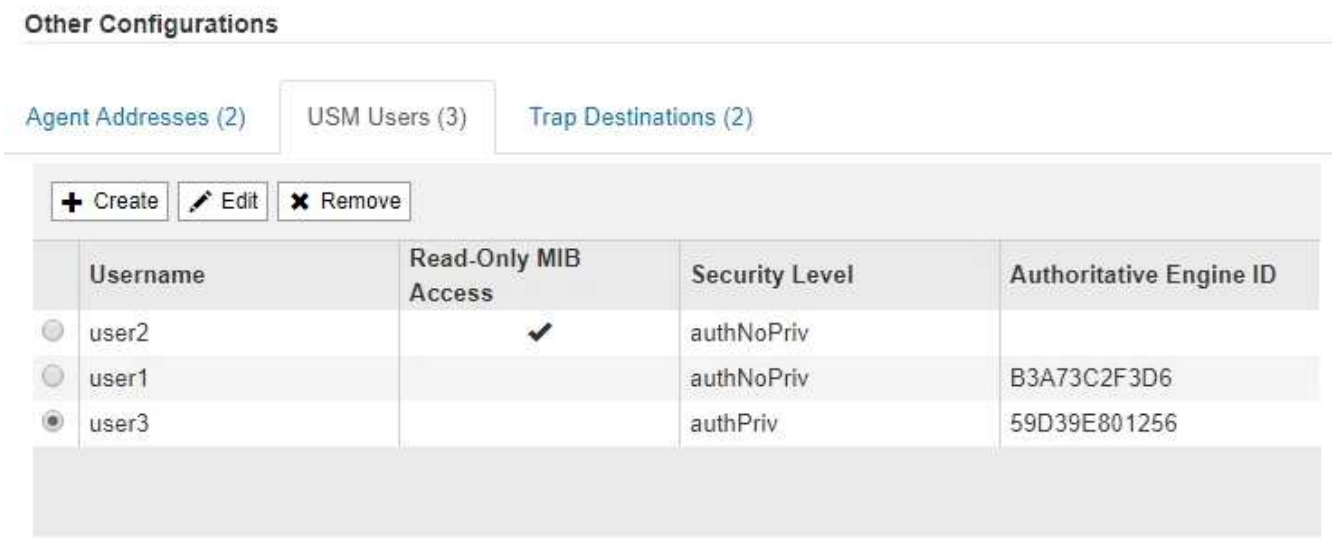
唯一支持的身份验证协议是 SHA （ HMAC-SHA-96 ）。

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

唯一支持的隐私协议是 AES 。

h. 单击 * 创建 * 。

此时将创建 USM 用户并将其添加到表中。

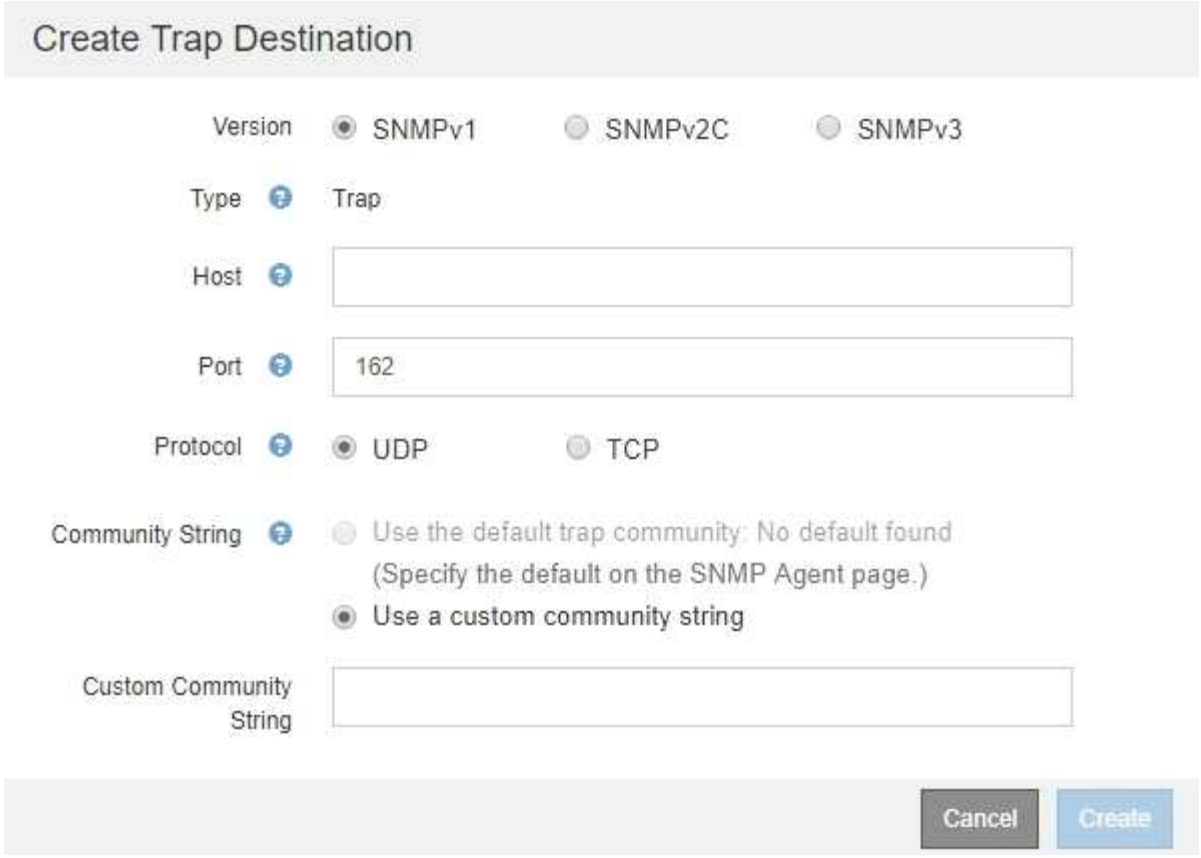


10. 在其他配置部分中，选择陷阱目标选项卡。

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

a. 单击 * 创建 * 。

此时将显示创建陷阱目标对话框。



b. 在 * 版本 * 字段中，选择要用于此通知的 SNMP 版本。

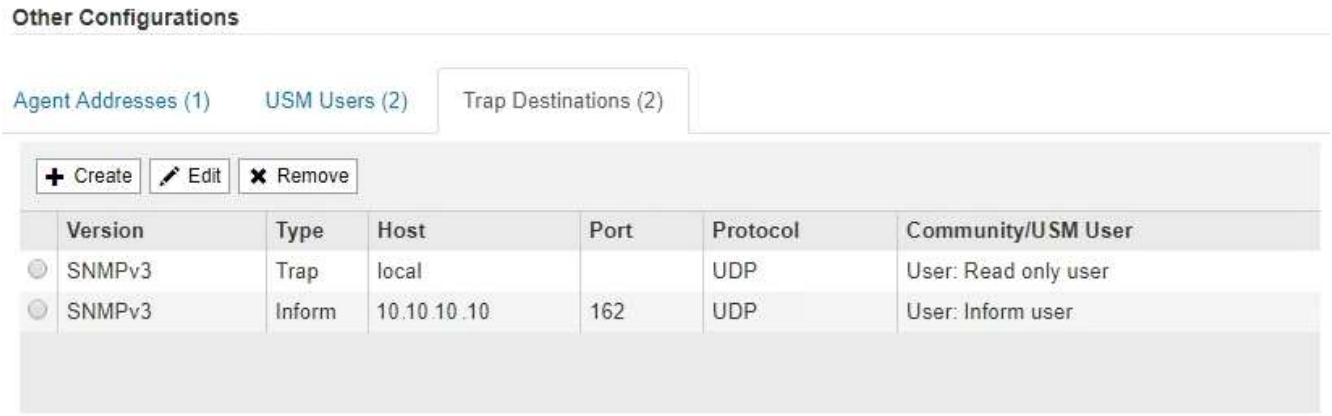
c. 根据您选择的版本填写此表单

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

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

d. 单击 * 创建 * 。

此时将创建陷阱目标并将其添加到表中。



11. 完成 SNMP 代理配置后，单击 * 保存 *

    新的 SNMP 代理配置将变为活动状态。

相关信息

静默警报通知

更新 **SNMP** 代理

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

您需要的内容

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

关于此任务

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

步骤

1. 选择 * 配置 * > * 监控 * > * SNMP 代理 * 。

   此时将显示 SNMP 代理页面。

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

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

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

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

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

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

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

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

7. 如果要更新代理地址，请选择其他配置部分中的代理地址选项卡。

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

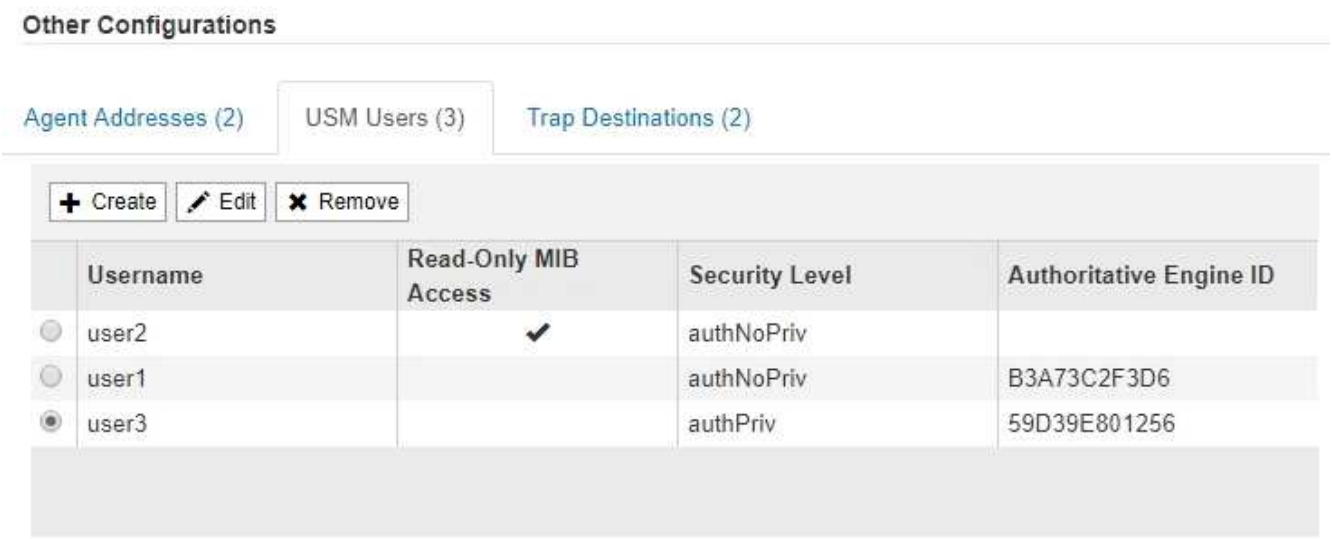
   a. 要添加代理地址，请单击 * 创建 * 。然后，请参见有关配置 SNMP 代理的说明中的代理地址步骤。

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

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

   d. 要提交更改，请单击 SNMP 代理页面底部的 * 保存 * 。

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



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

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

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

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

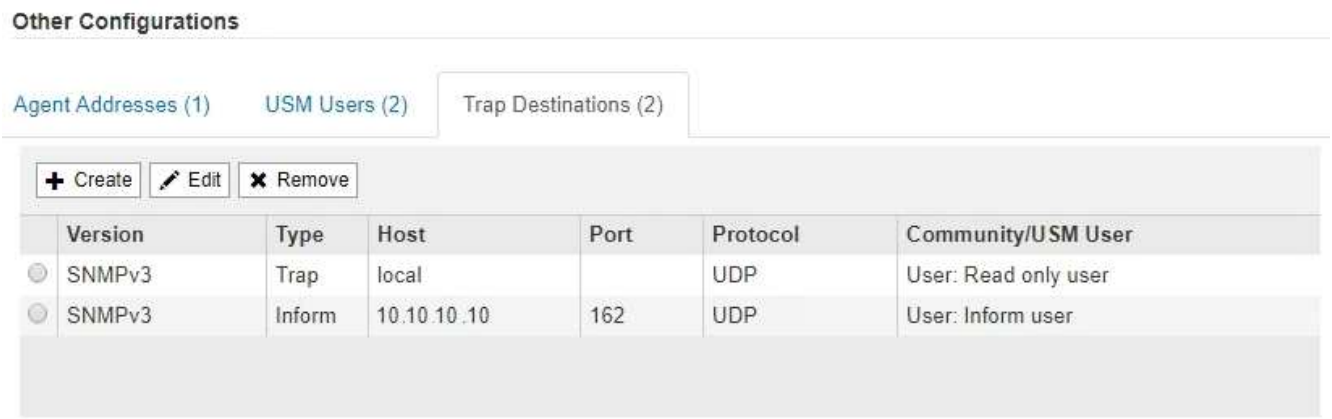
> 如果您添加或删除用户的权威引擎 ID ，并且当前已选择该用户作为目标，则必须按照步骤中所述编辑或删除该目标 SNMP 陷阱目标。否则，在保存 SNMP 代理配置时会发生验证错误。

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

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

a. 要提交更改，请单击 SNMP 代理页面底部的 * 保存 * 。

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



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

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

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

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

d. 要提交更改，请单击 SNMP 代理页面底部的 * 保存 * 。

10. 更新 SNMP 代理配置后，单击 * 保存 * 。

收集其他 **StorageGRID** 数据

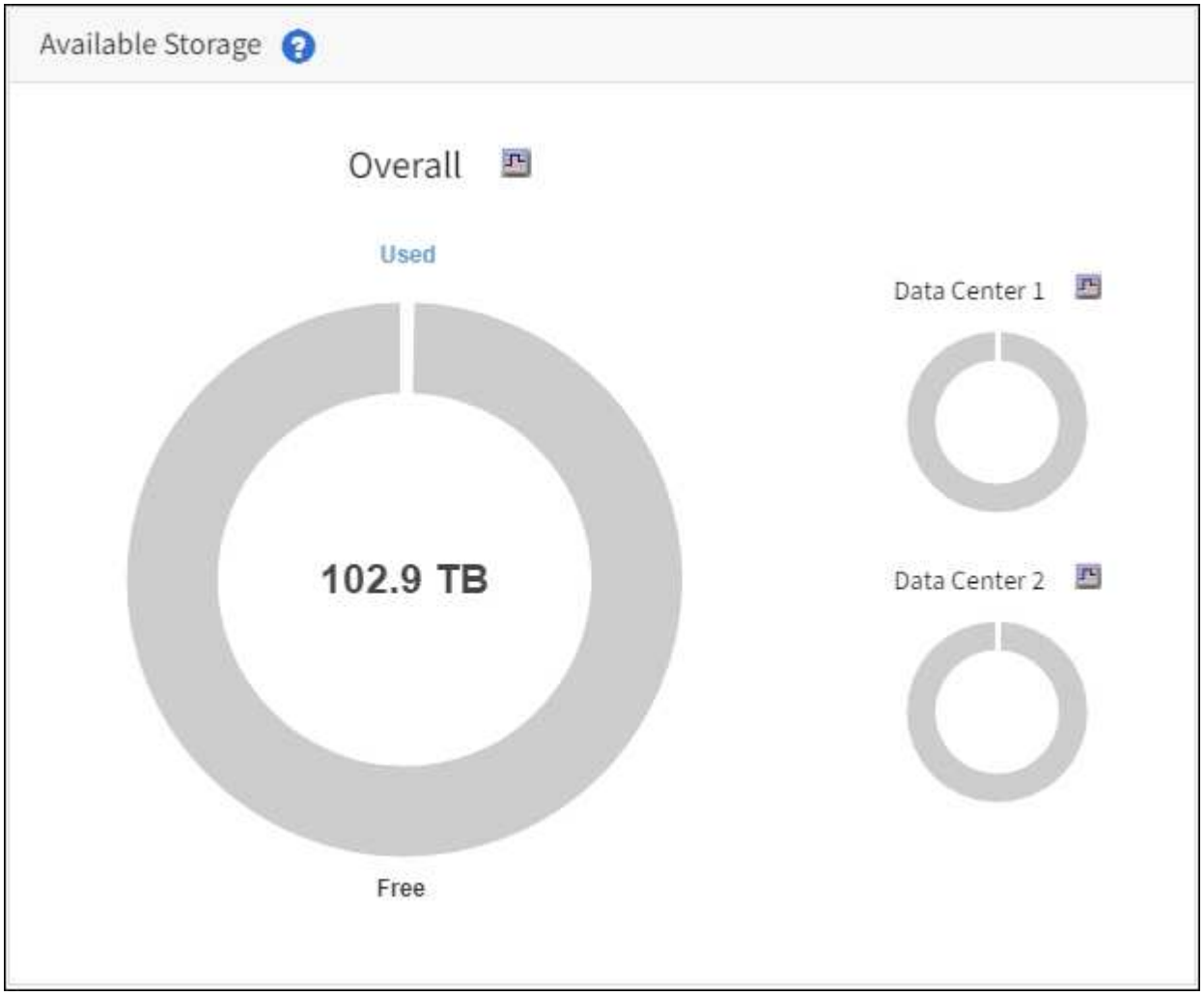
使用图表和图形

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

图表类型

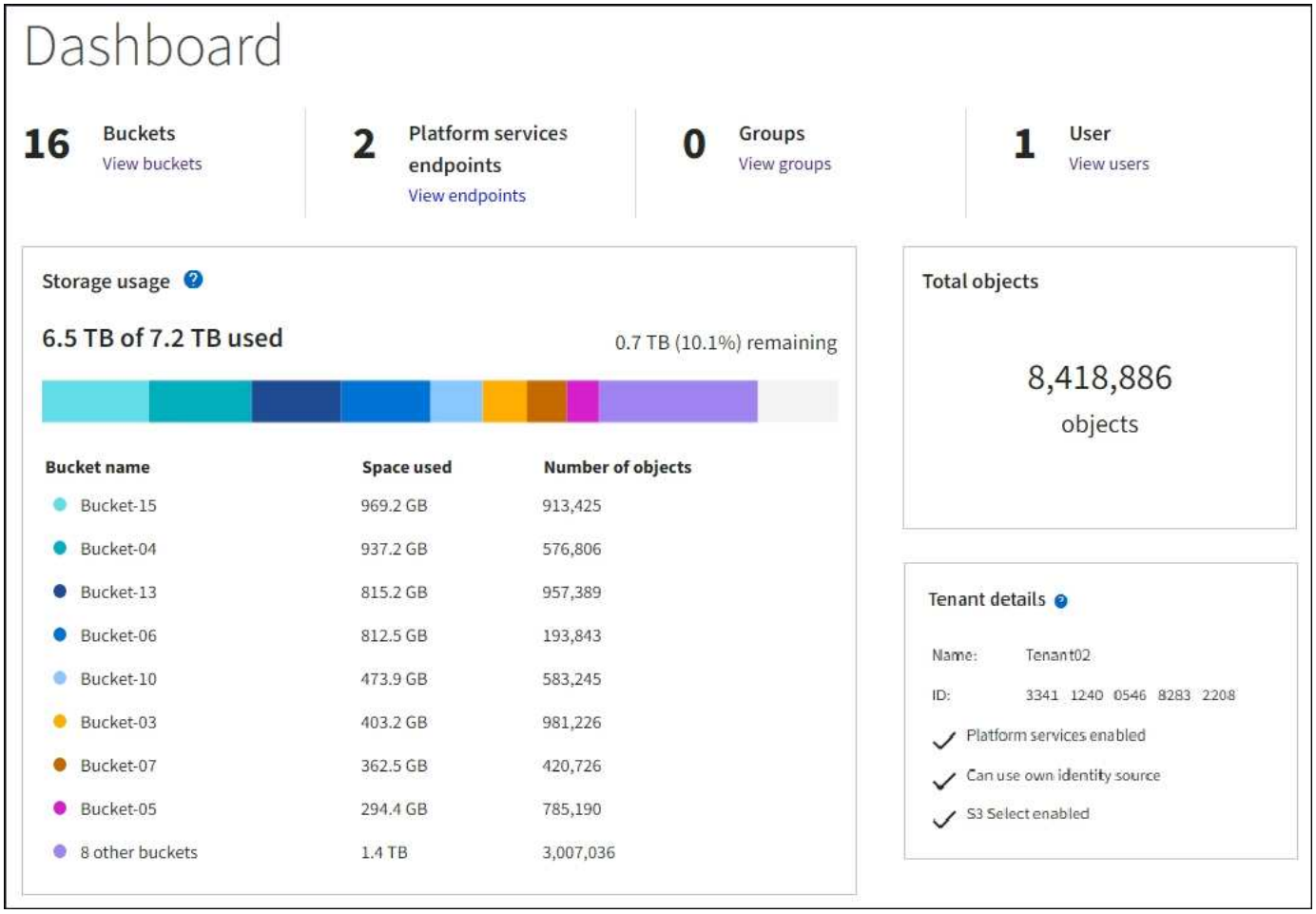
图表和图形汇总了特定 StorageGRID 指标和属性的值。

网格管理器信息板包含圆环图表，用于汇总网格和每个站点的可用存储。



租户管理器信息板上的存储使用情况面板显示以下内容：

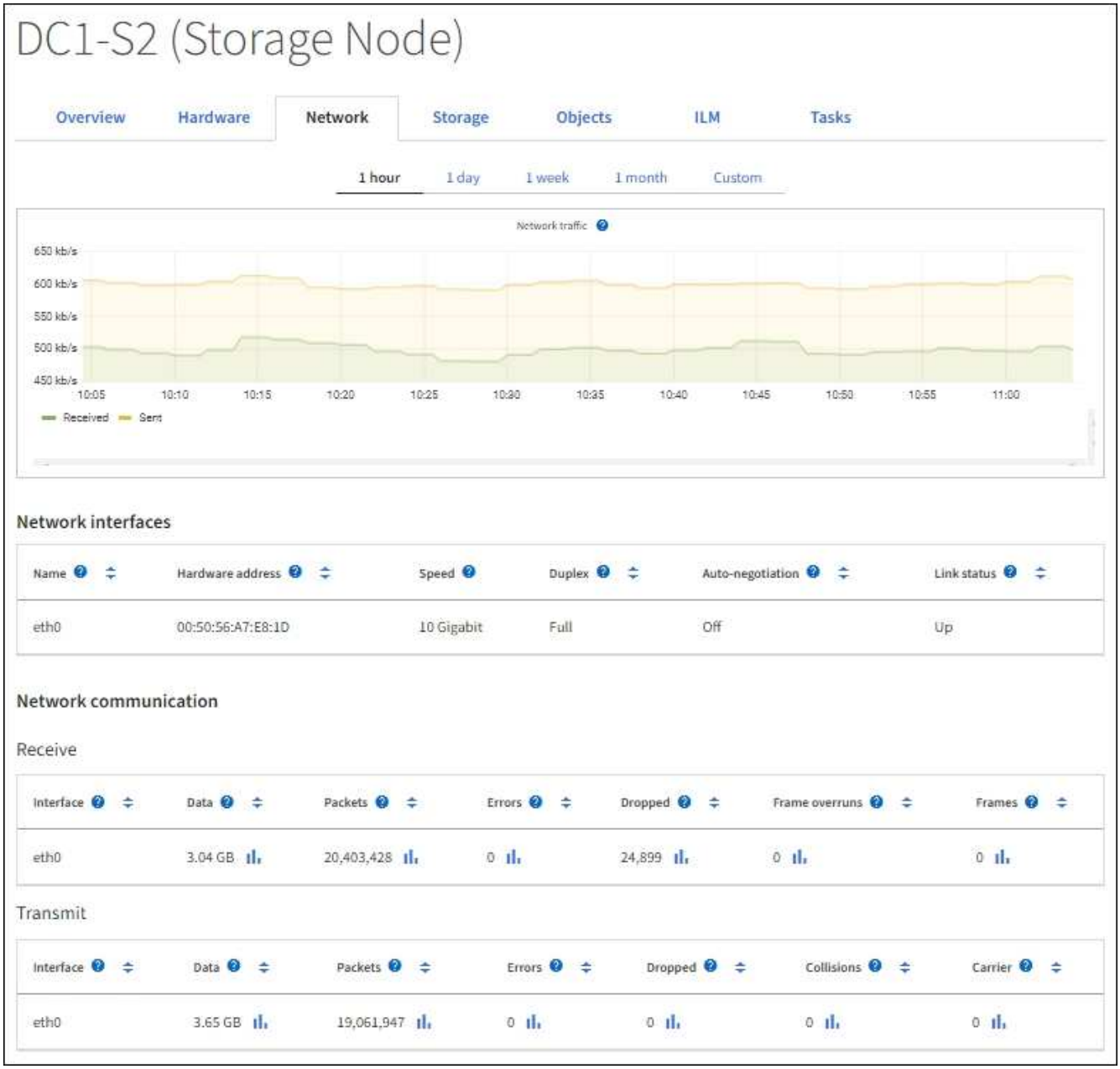
- 租户最大的分段（ S3 ）或容器（ Swift ）列表
- 一个条形图，表示最大分段或容器的相对大小
- 已用总空间量，如果设置了配额，则还会显示剩余空间量和百分比



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

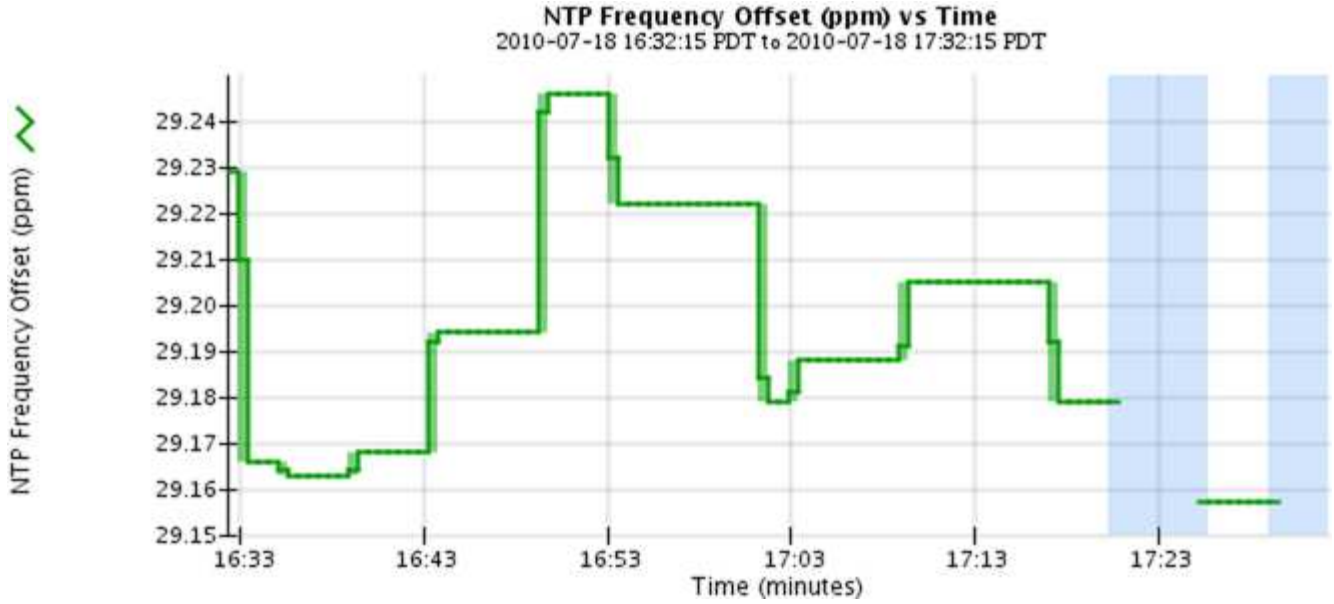
图形有四种类型：

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

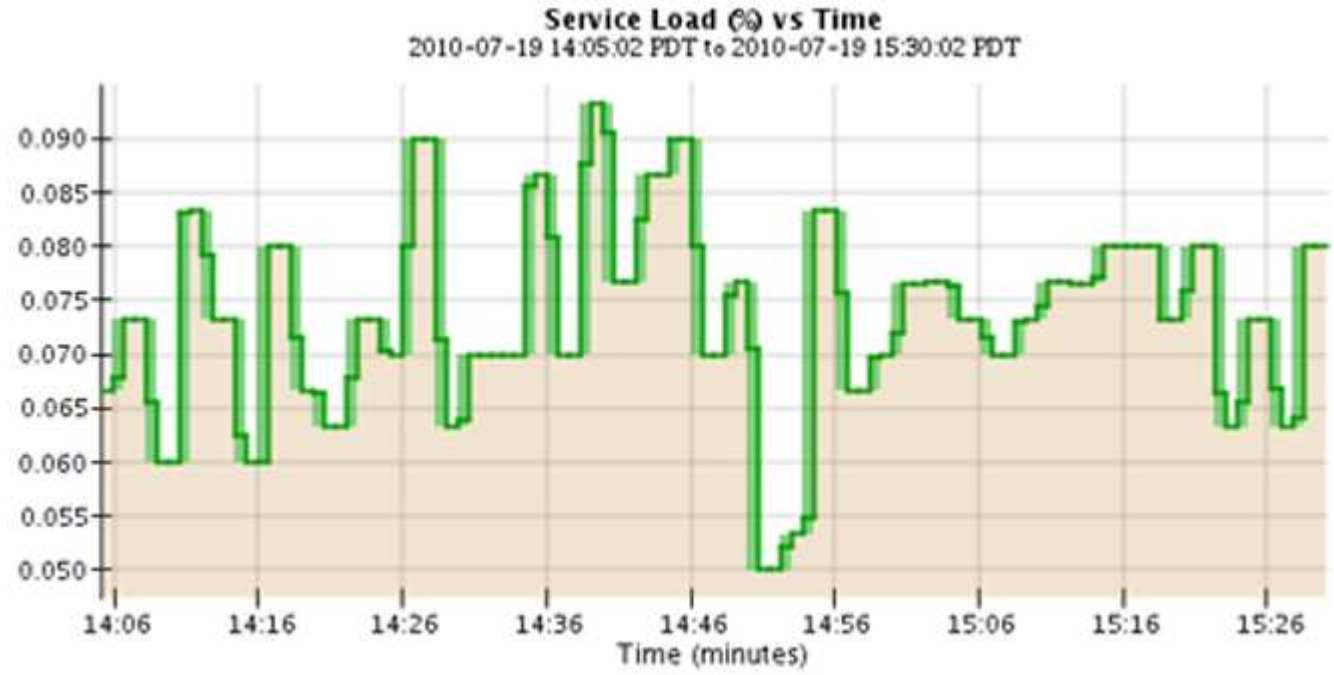


Grafana 图表也包含在预构建的信息板中，这些信息板可从 * 支持 * > * 工具 * > * 指标 * 页面获得。

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

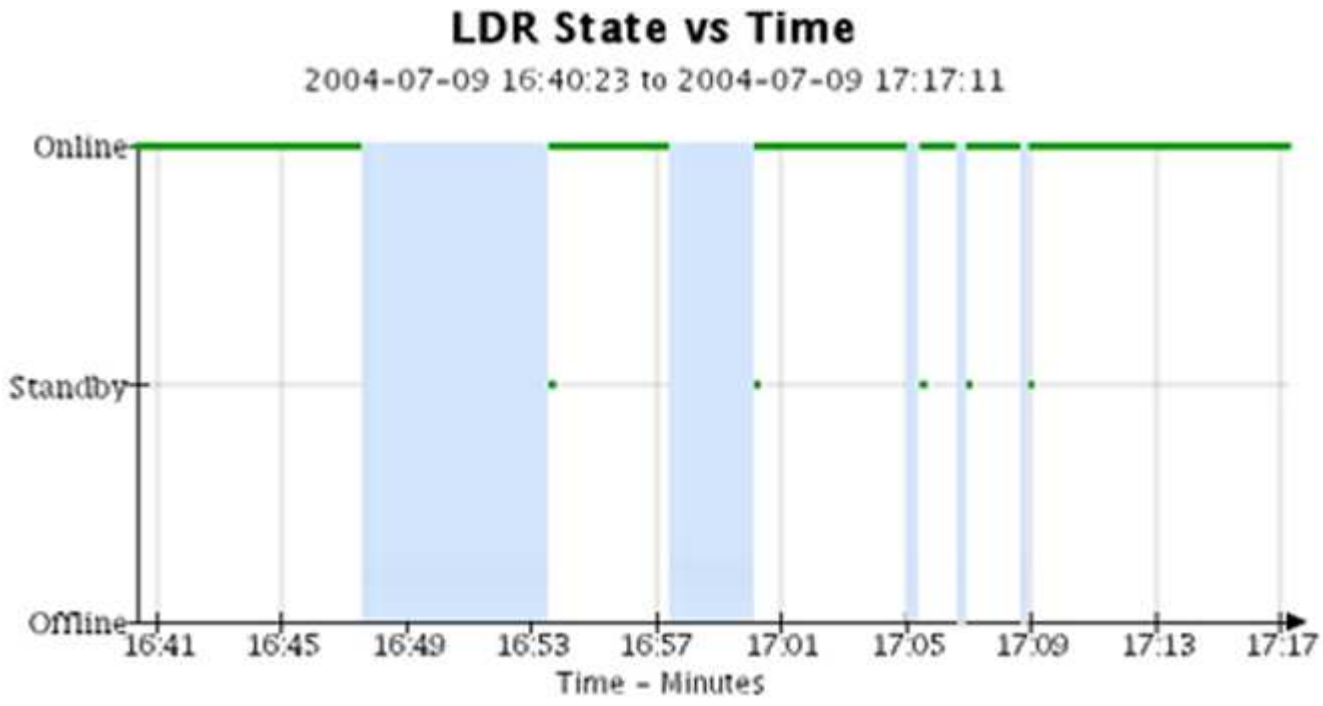


- * 区域图形 * ： 可从节点页面和 * 支持 * > * 工具 * > * 网格拓扑 * 页面（选择图表图标 在数据值之后，使用分区图绘制容量属性数量，例如对象计数或服务负载值。区域图形与折线图类似，但在折线下方会显示浅棕色阴影。值的更改会按定期数据间隔（箱）绘制。



- 某些图形使用不同类型的图表图标表示 格式不同：

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



相关信息

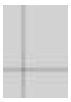
查看节点页面

查看网格拓扑树

查看支持指标

图表图例

用于绘制图表的线条和颜色具有特定的含义。

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

显示图表和图形

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

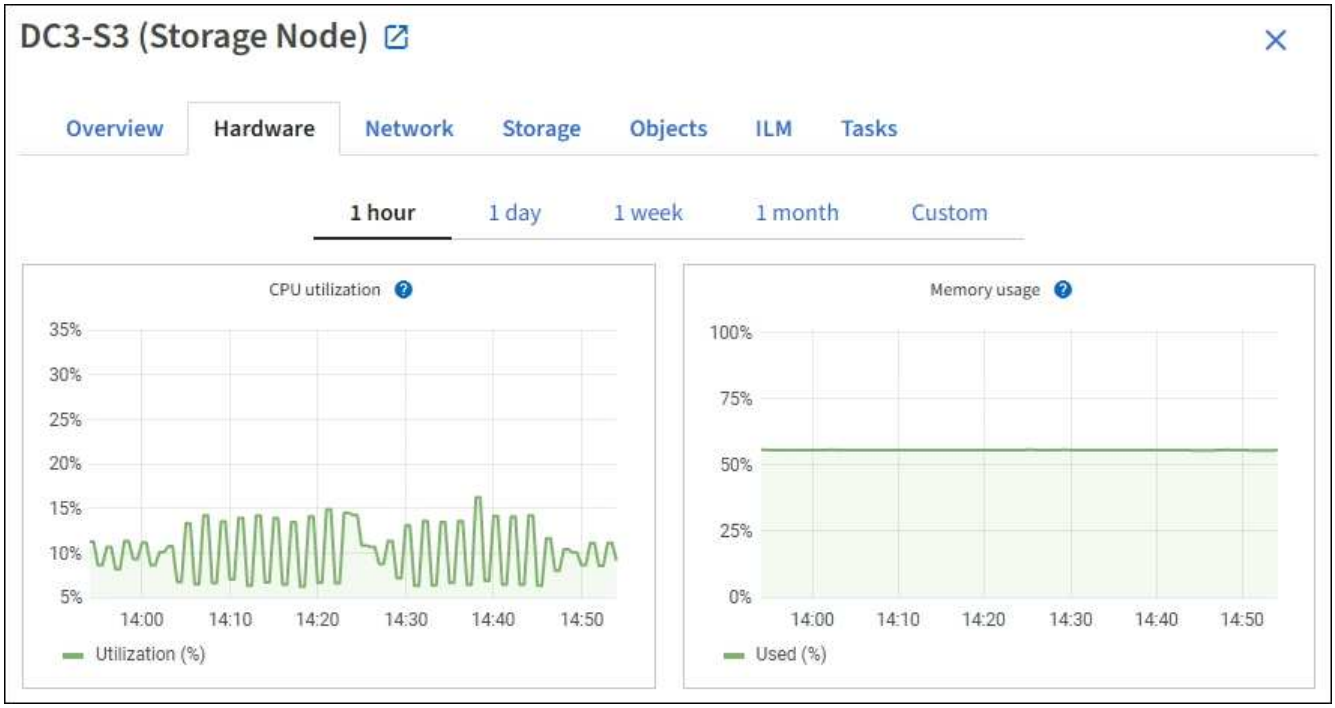
您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

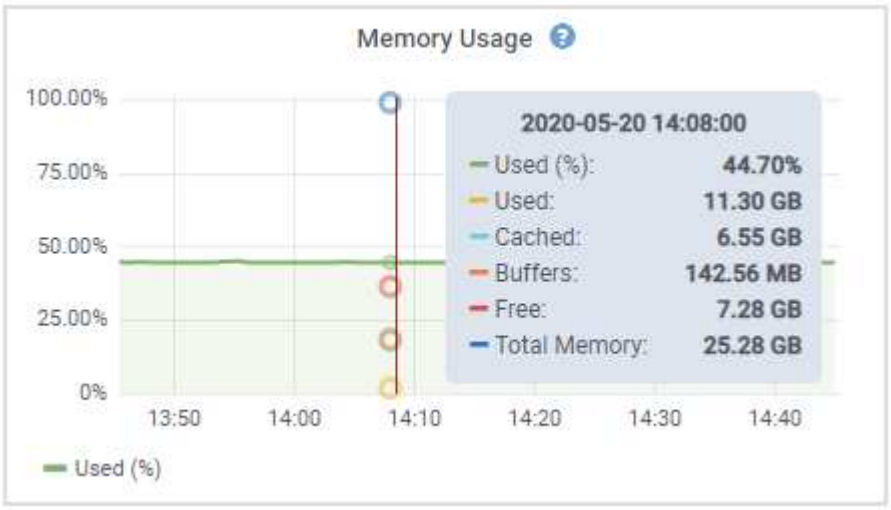
步骤

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

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



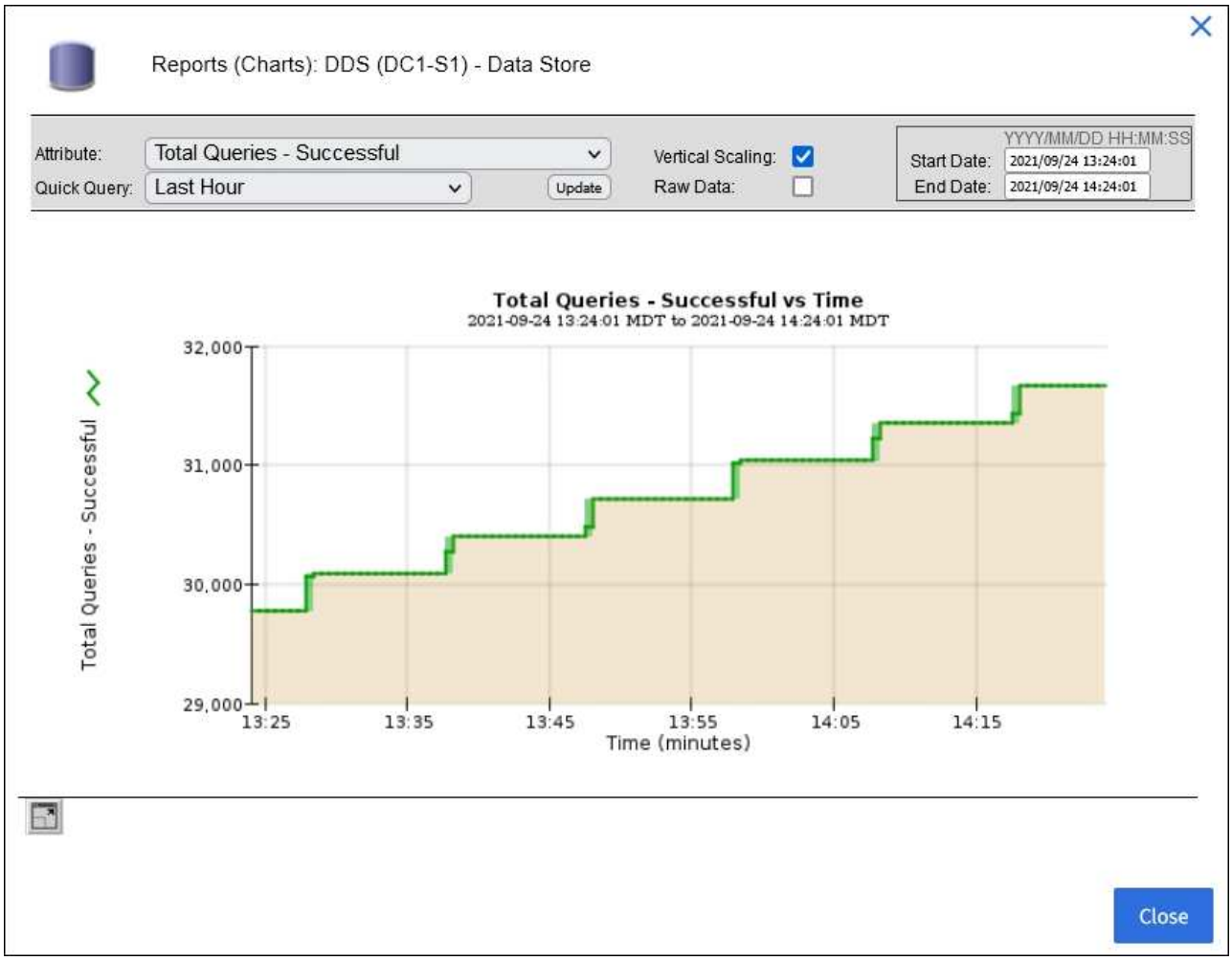
3. 或者，将光标悬停在图表上方可查看特定时间点的更详细值。

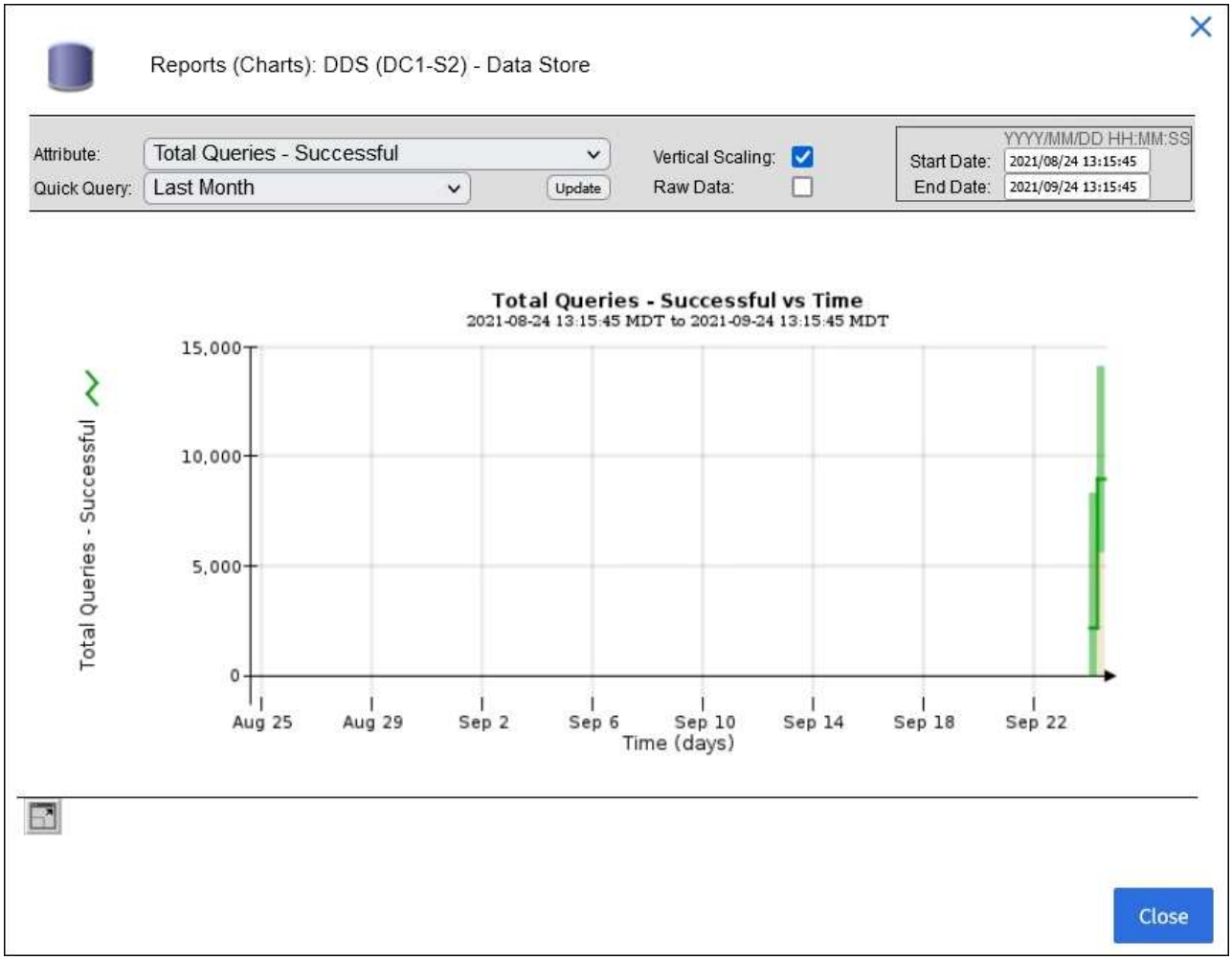


4. 您通常可以根据需要显示特定属性或指标的图表。从节点页面上的表中，选择图表图标 属性名称右侧。

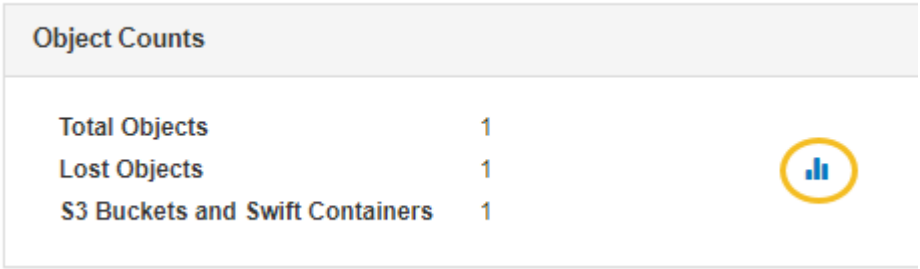
   并非所有指标和属性都有图表。

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

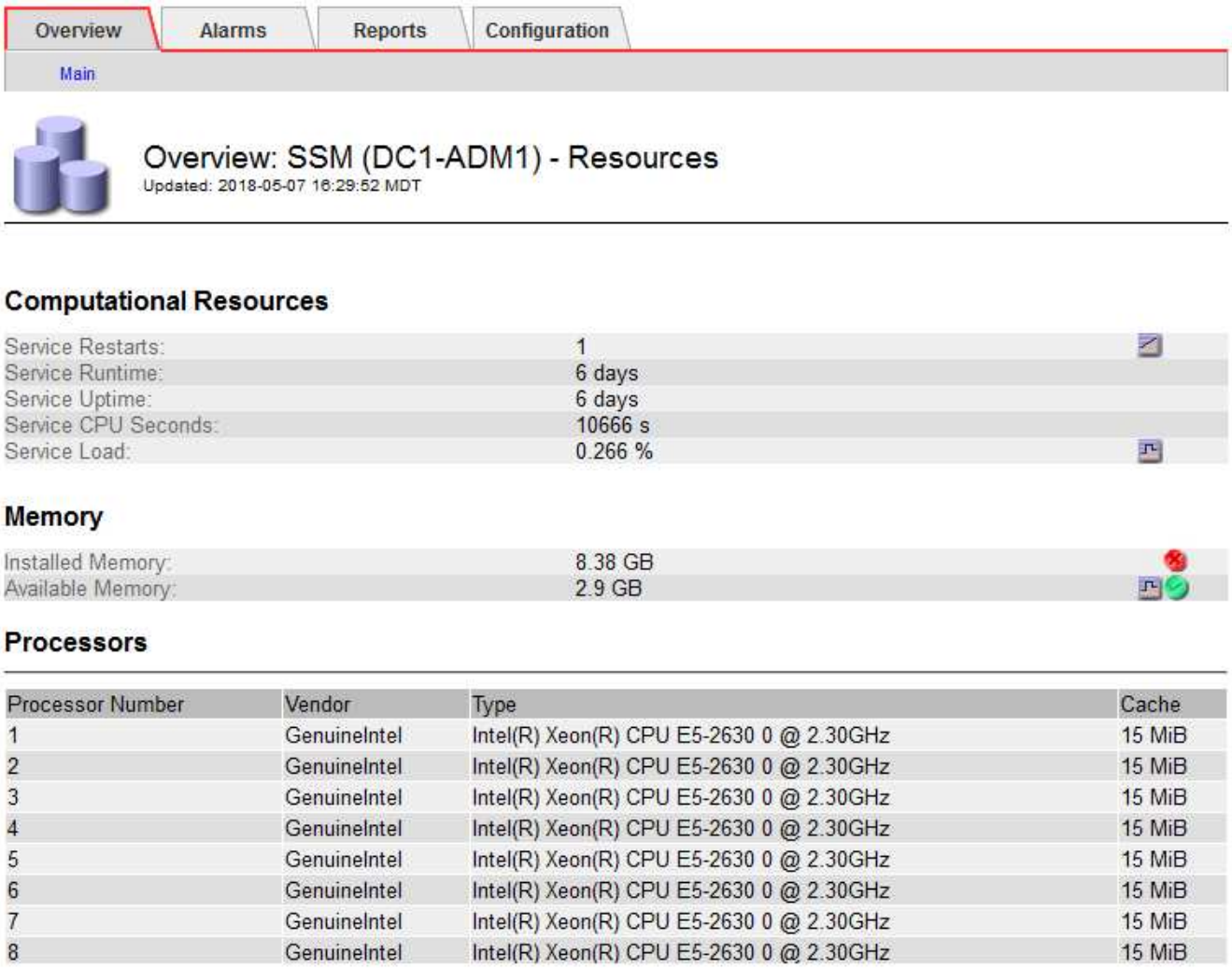

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01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



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



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



7. 选择图表图标 属性旁边。

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

生成图表

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

您需要的内容

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

步骤

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

6. 从 * 快速查询 * 下拉列表中选择要报告的时间段。

   选择自定义查询选项以选择特定的时间范围。

   稍后，图表将显示。请留出几分钟时间，以表格形式列出较长的时间范围。

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

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

8. 选择 * 更新 * 。

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

使用文本报告

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

原始文本报告

原始文本报告显示有关选定属性的详细信息：

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

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

聚合文本报告

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

每个条目都会显示以下信息：

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

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

生成文本报告

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

您需要的内容

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

关于此任务

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

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

灰色文本表示服务在取样期间被管理员关闭。蓝色文本表示服务处于未知状态。

步骤

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

   选择自定义查询选项以选择特定的时间范围。

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

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

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

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

8. 单击 * 更新 * 。

   稍后将生成一个文本报告。请留出几分钟时间，以表格形式列出较长的时间范围。根据为查询设置的时间长度，将显示原始文本报告或聚合文本报告。

导出文本报告

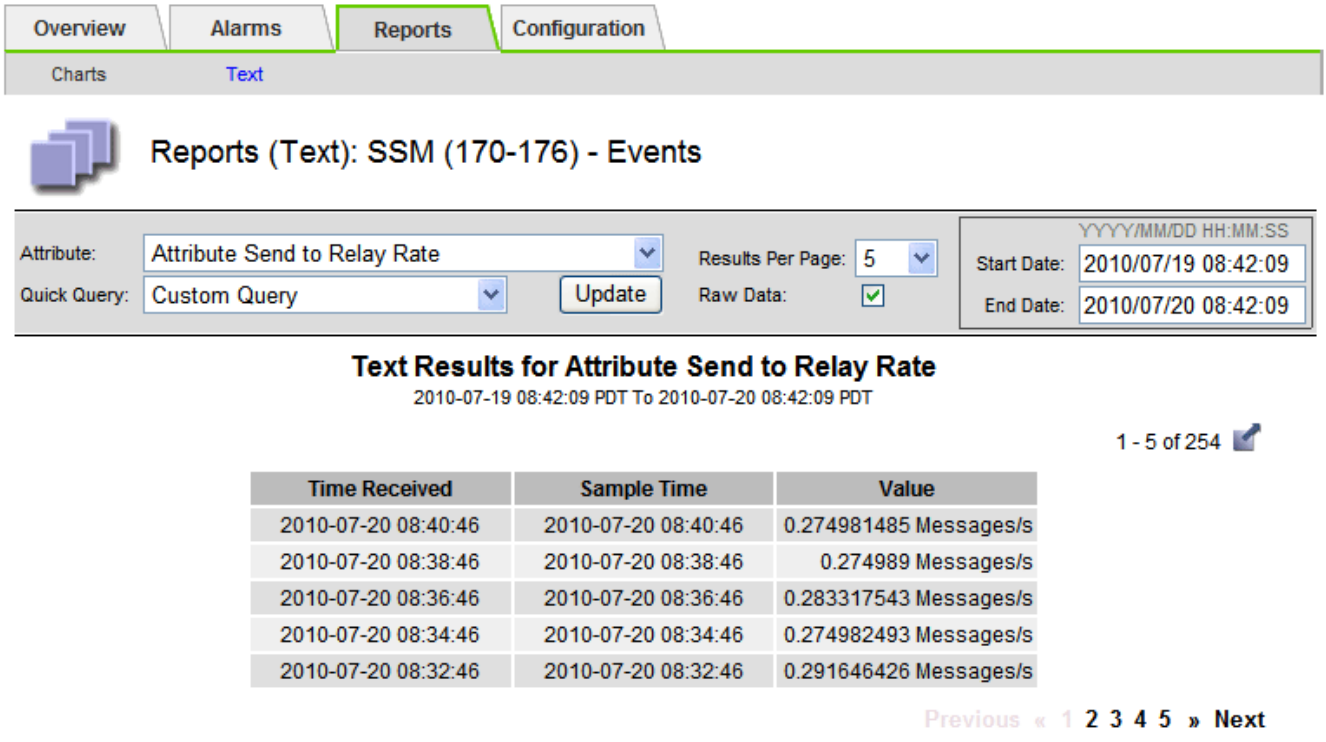
导出的文本报告将打开一个新的浏览器选项卡，在此可以选择和复制数据。

关于此任务

然后，可以将复制的数据保存到新文档（例如电子表格）中，并用于分析 StorageGRID 系统的性能。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 创建文本报告。
3. 单击 * 导出 * 。



   此时将打开导出文本报告窗口，其中显示了此报告。

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. 选择并复制导出文本报告窗口的内容。

   现在，可以将此数据粘贴到电子表格等第三方文档中。

监控 **PUT** 和 **GET** 性能

您可以监控某些操作的性能，例如对象存储和检索，以帮助确定可能需要进一步调查的更改。

关于此任务

要监控 PUT 和 GET 性能，您可以直接从工作站或使用开源 S3tester 应用程序运行 S3 和 Swift 命令。使用这些方法可以独立于 StorageGRID 外部因素（例如客户端应用程序问题或外部网络问题）评估性能。

对 PUT 和 GET 操作执行测试时，请遵循以下准则：

- 使用与通常载入到网格中的对象相当的对象大小。
- 对本地站点和远程站点执行操作。

中的消息 审核日志 指示运行某些操作所需的总时间。例如，要确定 S3 GET 请求的总处理时间，您可以查看 SGET 审核消息中的时间属性值。您还可以在以下操作的审核消息中找到时间属性：

- * S3： delete， get， head， Metadata updated， post， PUT
- * Swift*： delete， get， head， put

在分析结果时，请查看满足请求所需的平均时间以及可以实现的总吞吐量。定期重复相同的测试并记录结果，以便确定可能需要调查的趋势。

- 您可以 "从 GitHub 下载 S3tester"。

StorageGRID 系统可以验证存储节点上对象数据的完整性，并检查是否存在损坏和缺失的对象。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。

关于此任务

两个 验证过程 协同工作以确保数据完整性：

- * 后台验证 * 会自动运行，并持续检查对象数据的正确性。

  后台验证会自动持续检查所有存储节点，以确定复制的和经过纠删编码的对象数据是否存在损坏的副本。如果发现问题， StorageGRID 系统会自动尝试替换存储在系统其他位置的副本中损坏的对象数据。后台验证不会在归档节点或云存储池中的对象上运行。

  如果系统检测到无法自动更正的损坏对象，则会触发 * 检测到未标识的损坏对象 * 警报。

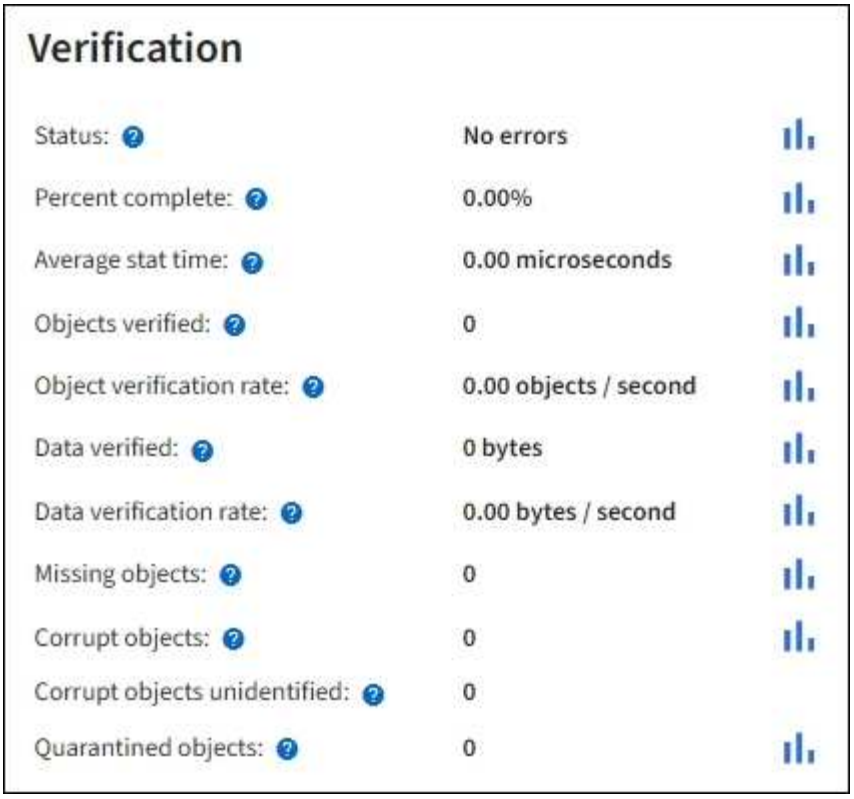
- 用户可以触发 * 对象存在检查 * ，以便更快速地验证对象数据是否存在（尽管不是正确）。

  对象存在检查可验证存储节点上是否存在所有预期复制的对象副本以及经过纠删编码的片段。对象存在检查提供了一种验证存储设备完整性的方法，尤其是在最新的硬件问题描述 可能会影响数据完整性的情况下。

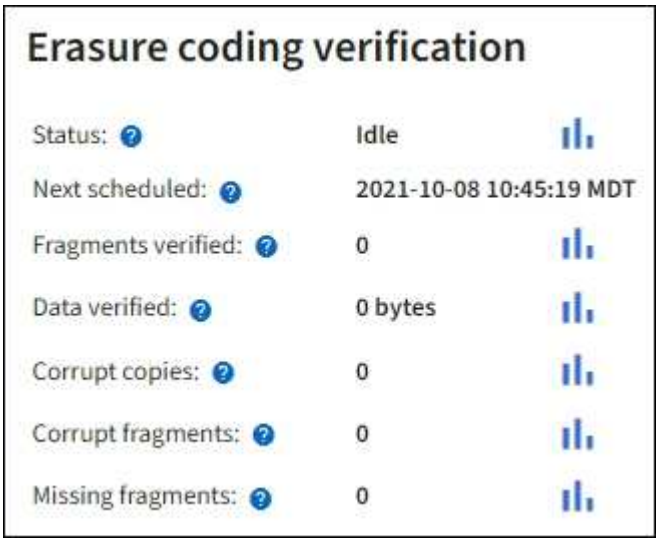
您应定期查看后台验证和对象存在检查的结果。立即调查任何对象数据损坏或丢失的实例，以确定根发生原因。

步骤

1. 查看后台验证的结果：
   a. 选择 * 节点 * > * 存储节点 _* > * 对象 * 。
   b. 检查验证结果：
      - 要检查复制的对象数据验证，请查看验证部分中的属性。

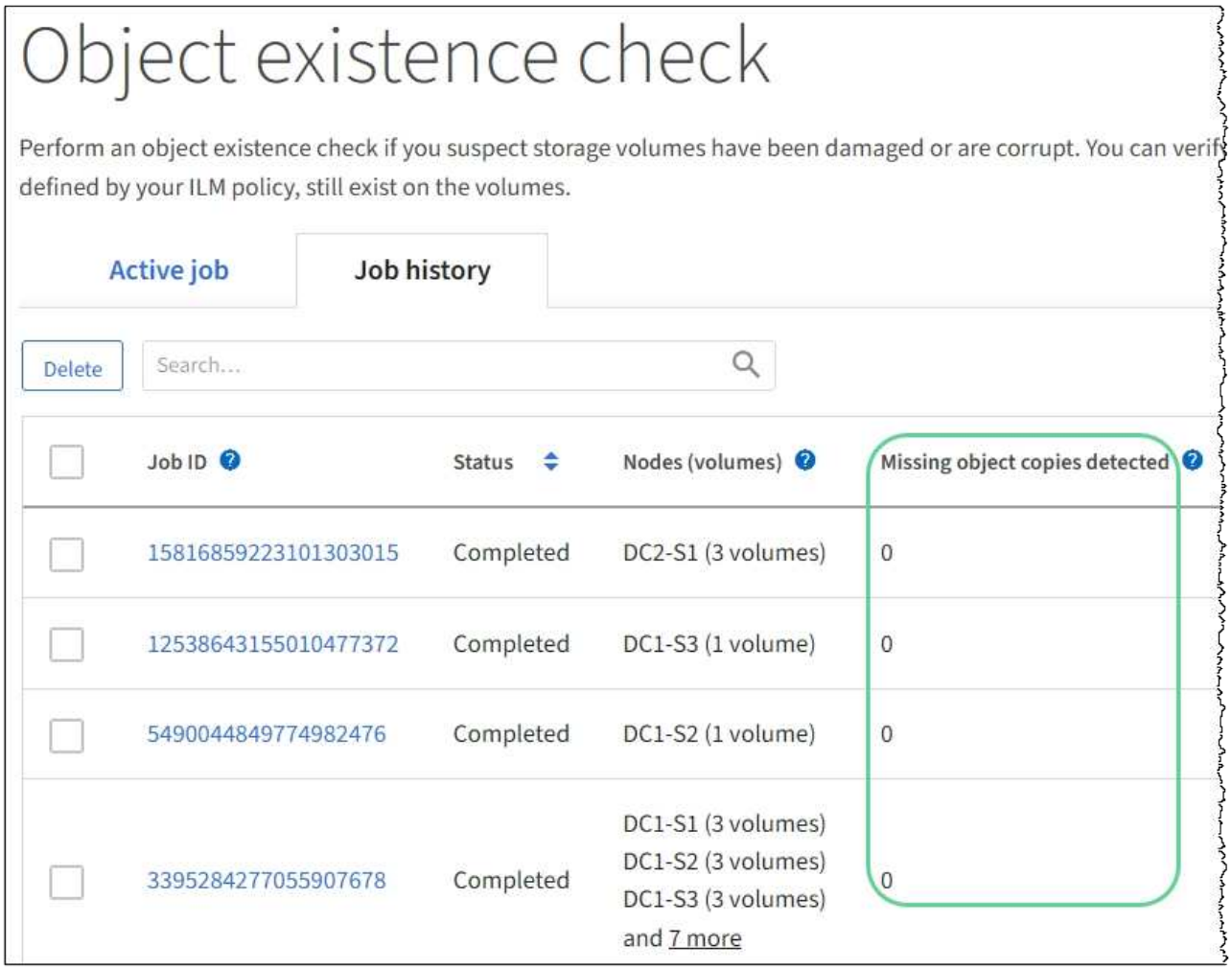


- 要检查擦除编码的片段验证，请选择 * 存储节点 _* > * ILM * ，然后查看擦除编码验证部分中的属性。



选择问号 在属性名称旁边显示帮助文本。

2. 查看对象存在检查作业的结果：
   a. 选择 * 维护 * > * 对象存在检查 * > * 作业历史记录 * 。
   b. 扫描检测到的缺少对象副本列。如果任何作业导致缺少 100 个或更多对象副本和 对象丢失警报 已触发，请联系技术支持。



监控事件

您可以监控网格节点检测到的事件，包括您为跟踪记录到系统日志服务器的事件而创建的自定义事件。网格管理器中显示的最后一个事件消息提供了有关最新事件的详细信息。

事件消息也会列在 ` /var/local/log/byncast-err.log` 日志文件中。请参见 日志文件参考。

网络问题，断电或升级等问题可能会重复触发 SMTT" （事件总数） " 警报。本节介绍了有关调查事件的信息，以便您更好地了解发生这些警报的原因。如果由于已知问题描述 而发生事件，则可以安全地重置事件计数器。

步骤

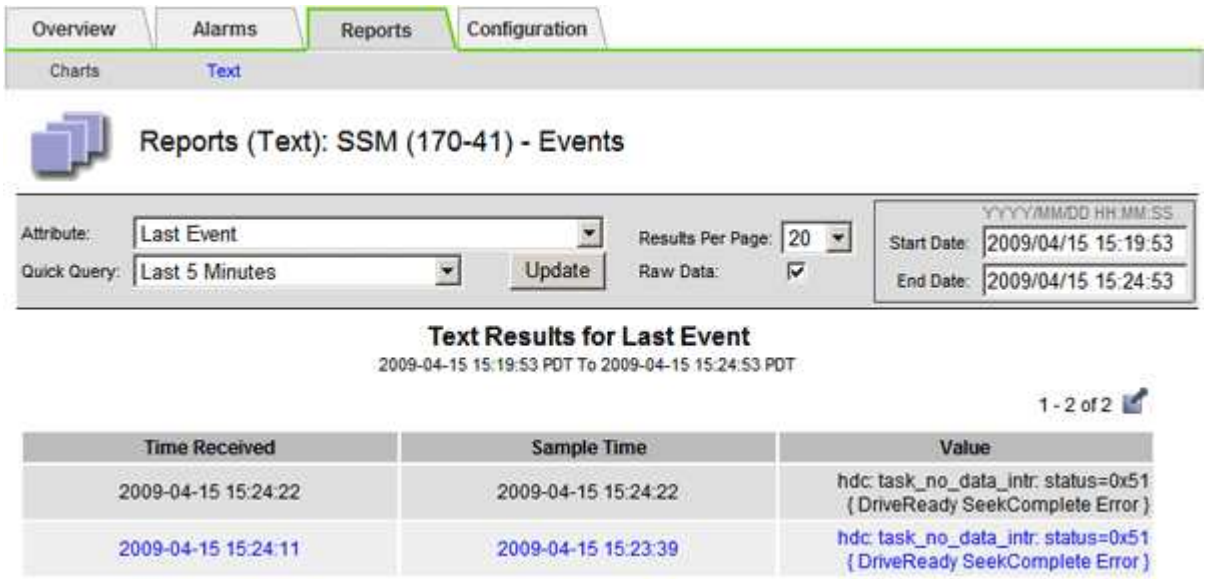
1. 查看每个网格节点的系统事件：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 概述 * > * 主 * 。
2. 生成先前事件消息的列表，以帮助隔离过去发生的问题：
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * > * 报告 * 。
   c. 选择 * 文本 * 。

中未显示 * 最后一个事件 * 属性 图表视图。要查看它，请执行以下操作：

d. 将 * 属性 * 更改为 * 最后一个事件 * 。

e. 也可以选择 * 快速查询 * 的时间段。

f. 选择 * 更新 * 。



创建自定义系统日志事件

通过自定义事件，您可以跟踪记录到系统日志服务器的所有内核，守护进程，错误和严重级别的用户事件。自定义事件可用于监控系统日志消息的发生情况（进而监控网络安全事件和硬件故障）。

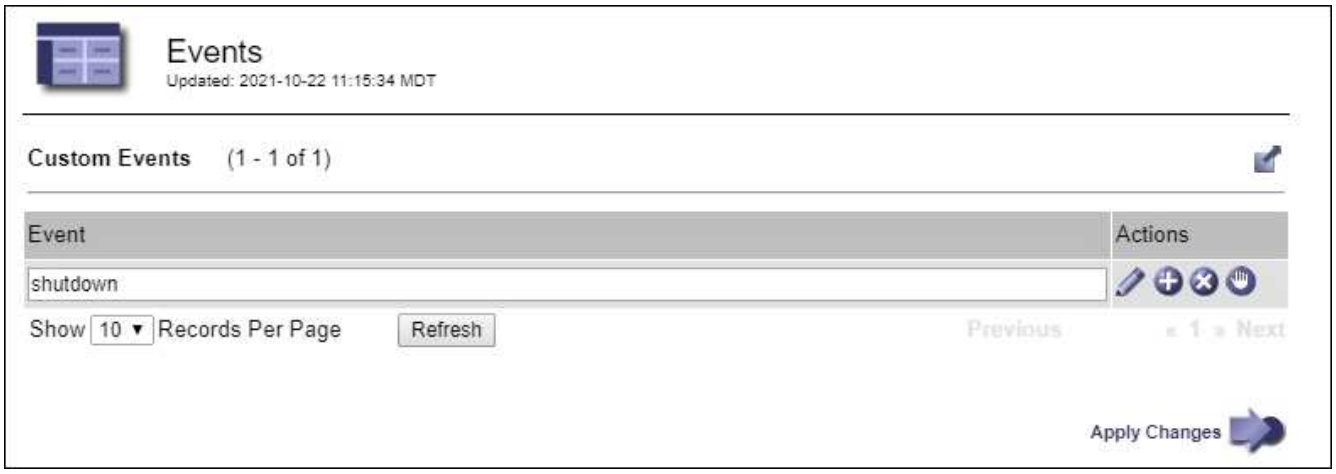
关于此任务

请考虑创建自定义事件以监控重复出现的问题。以下注意事项适用于自定义事件。

- 创建自定义事件后，系统会监控其每次发生情况。
- 要基于 ` /var/local/log/messages` 文件中的关键字创建自定义事件，这些文件中的日志必须为：
  - 由内核生成
  - 由守护进程或用户程序在错误或严重级别生成
- 注： * ` /var/local/log/messages` 文件中的所有条目不会匹配，除非它们满足上述要求。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 自定义事件 * 。
2. 单击 * 编辑 * 。 （或 * 插入 * 如果这不是第一个事件）。
3. 输入自定义事件字符串，例如 shutdown



4. 选择 * 应用更改 * 。
5. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
6. 选择 ***GRID NODE*** > * 。 ssm * > * 事件 * 。
7. 在事件表中找到自定义事件条目，并监控 * 计数 * 的值。

   如果计数增加，则会在该网格节点上触发您正在监控的自定义事件。

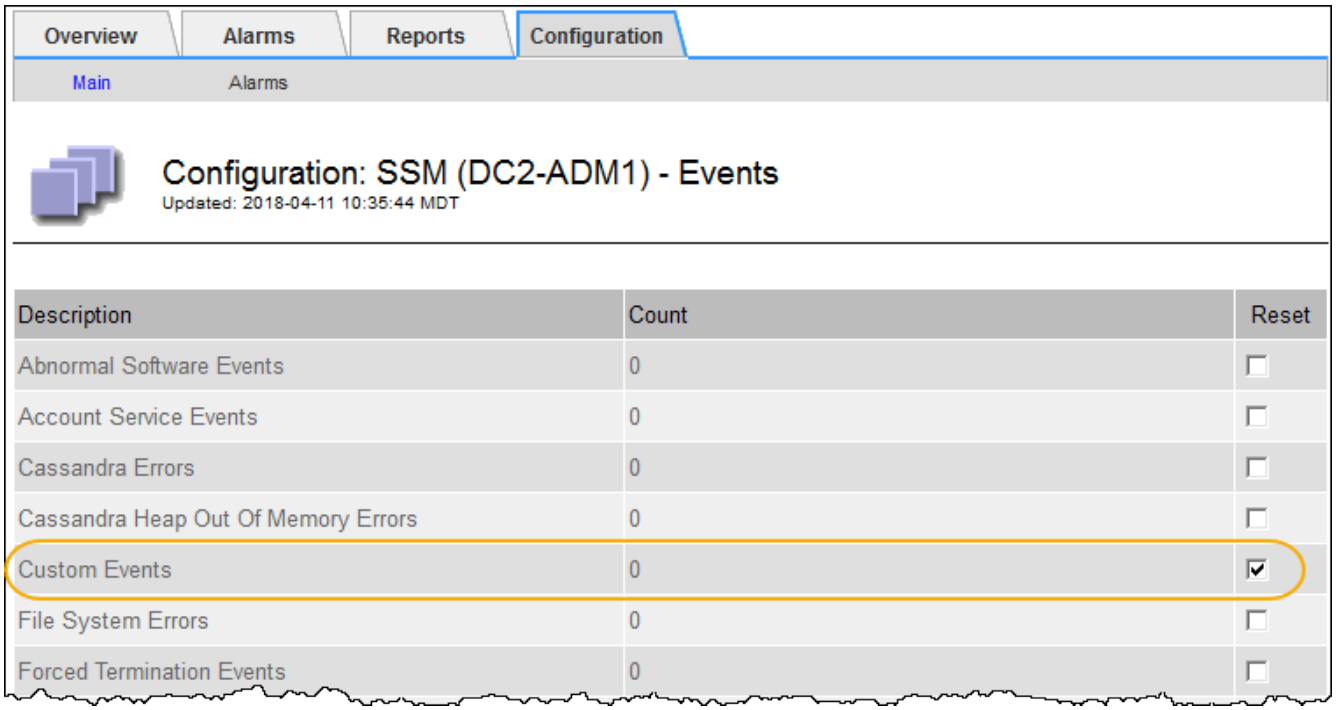
将自定义事件计数重置为零

如果只想重置自定义事件的计数器，则必须使用支持菜单中的网格拓扑页面。

关于此任务

重置计数器会导致下一个事件触发警报。相反，确认警报时，只有在达到下一阈值级别时才会重新触发该警报。

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 ***GRID NODE*** > * SSM* > * 事件 * > * 配置 * > * 主 * 。
3. 选中自定义事件的 * 重置 * 复选框。



4. 选择 * 应用更改 * 。

查看审核消息

审核消息可帮助您更好地了解 StorageGRID 系统的详细操作。您可以使用审核日志对问题进行故障排除并评估性能。

在系统正常运行期间，所有 StorageGRID 服务都会生成审核消息，如下所示：

- 系统审核消息与审核系统本身，网格节点状态，系统范围的任务活动和服务备份操作相关。
- 对象存储审核消息与 StorageGRID 中对象的存储和管理相关，包括对象存储和检索，网格节点到网格节点的传输以及验证。
- 当 S3 或 Swift 客户端应用程序请求创建，修改或检索对象时，系统会记录客户端读写审核消息。
- 管理审核消息会将用户请求记录到管理 API 。

每个管理节点都会将审核消息存储在文本文件中。审核共享包含活动文件（ audit.log ）以及前几天压缩的审核日志。网格中的每个节点还会存储在该节点上生成的审核信息的副本。

为了便于访问审核日志，您可以为 NFS 和 CIFS 配置客户端对审核共享的访问权限（ CIFS 已弃用）。您也可以直接从管理节点的命令行访问审核日志文件。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

有关审核日志文件的详细信息，审核消息的格式，审核消息的类型以及可用于分析审核消息的工具，请参见审核消息的说明。要了解如何配置审核客户端访问，请参见有关管理 StorageGRID 的说明。

相关信息

查看审核日志

收集日志文件和系统数据

您可以使用网格管理器检索 StorageGRID 系统的日志文件和系统数据（包括配置数据）。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须具有配置密码短语。

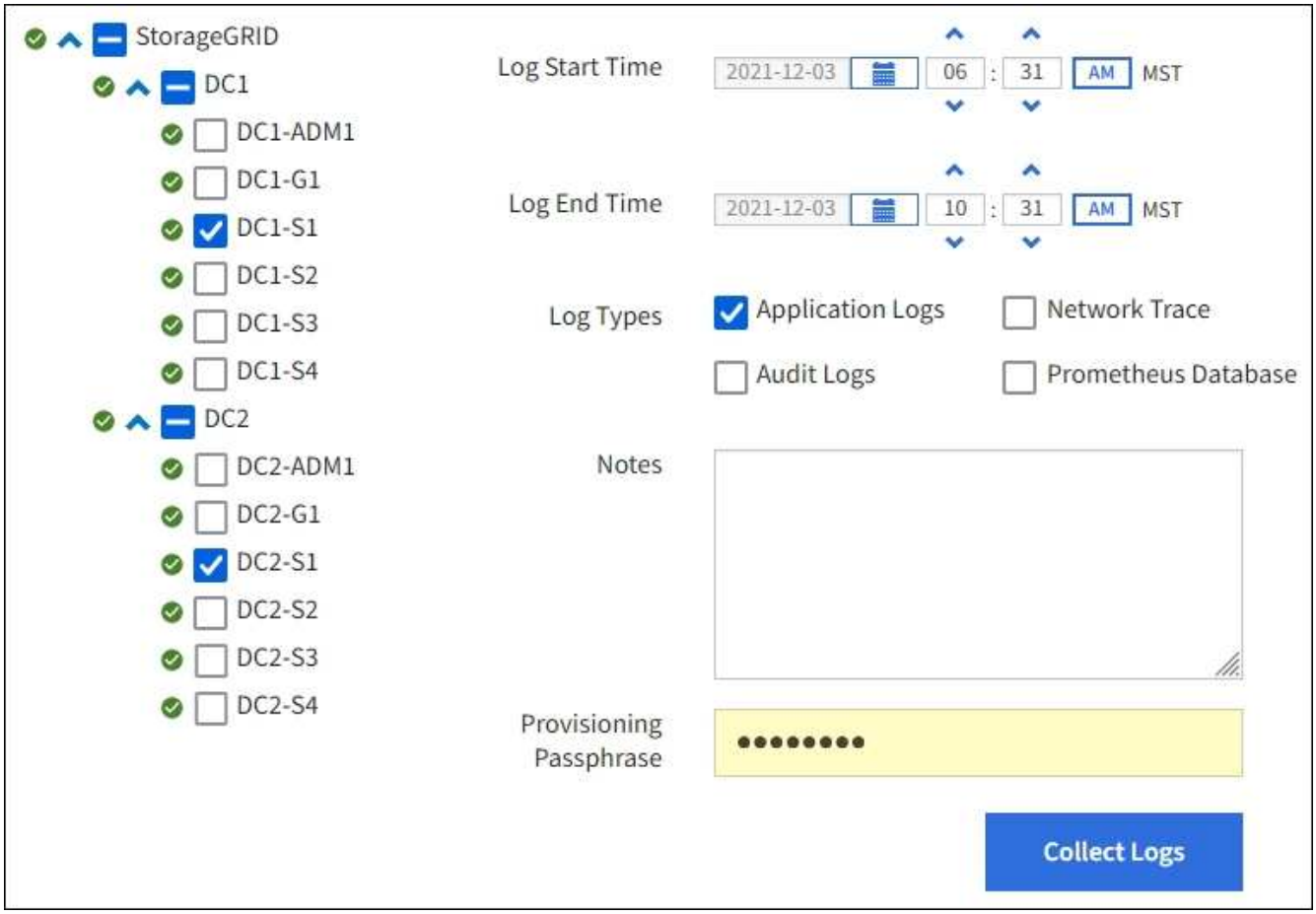
关于此任务

您可以使用网格管理器收集 日志文件选定时间段内任何网格节点的系统数据和配置数据。数据会收集并归档在 .tar.gz 文件中，然后可下载到本地计算机。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

步骤

1. 选择 * 支持 * > * 工具 * > * 日志 * 。



2. 选择要收集日志文件的网格节点。

   您可以根据需要收集整个网格或整个数据中心站点的日志文件。

3. 选择 * 开始时间 * 和 * 结束时间 * 以设置要包含在日志文件中的数据的时间范围。

   如果选择很长的时间段或从大型网格中的所有节点收集日志，则日志归档可能会变得过大，无法存储在节点上，或者可能会变得过大，无法收集到主管理节点以供下载。如果发生这种情况，您必须使用一组较小的数据重新启动日志收集。

4. 选择要收集的日志类型。
   - * 应用程序日志 * ： 技术支持最常用于故障排除的应用程序特定日志。收集的日志是可用应用程序日志的一部分。
   - * 审核日志 * ： 包含在正常系统操作期间生成的审核消息的日志。
   - * 网络跟踪 * ： 用于网络调试的日志。
   - * Prometheus Database* ： 所有节点上的服务的时间序列指标。
5. 或者，也可以在 * 注释 * 文本框中输入有关要收集的日志文件的注释。

   您可以使用这些注释提供有关提示您收集日志文件的问题的技术支持信息。您的注释以及有关日志文件收集的其他信息将添加到名为 `info.txt` 的文件中。`info.txt` 文件保存在日志文件归档包中。

6. 在 * 配置密码短语 * 文本框中输入 StorageGRID 系统的配置密码短语。
7. 选择 * 收集日志 * 。

   提交新请求时，系统将删除先前收集的日志文件。

   您可以使用日志页面监控每个网格节点的日志文件收集进度。

   如果您收到有关日志大小的错误消息，请尝试收集较短时间段或较少节点的日志。

8. 日志文件收集完成后，选择 * 下载 * 。

   .tar.gz 文件包含成功收集日志的所有网格节点中的所有日志文件。在组合的 *.tar.gz* 文件中，每个网格节点有一个日志文件归档。

完成后

如果需要，您可以稍后重新下载日志文件归档包。

您也可以选择 * 删除 * 以删除日志文件归档软件包并释放磁盘空间。下次收集日志文件时，系统会自动删除当前日志文件归档包。

手动触发 **AutoSupport** 消息

为了帮助技术支持解决 StorageGRID 系统的问题，您可以手动触发要发送的 AutoSupport 消息。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

2. 选择 * 发送用户触发的 AutoSupport * 。

   StorageGRID 尝试向技术支持发送 AutoSupport 消息。如果尝试成功，则会更新 * 结果 * 选项卡上的 * 最新结果 * 和 * 最后成功时间 * 值。如果出现问题， * 最新结果 * 值将更新为 " 失败 " ， StorageGRID 不会再尝试发送 AutoSupport 消息。

   发送用户触发的 AutoSupport 消息后，请在 1 分钟后刷新浏览器中的 AutoSupport 页面以访问最新结果。

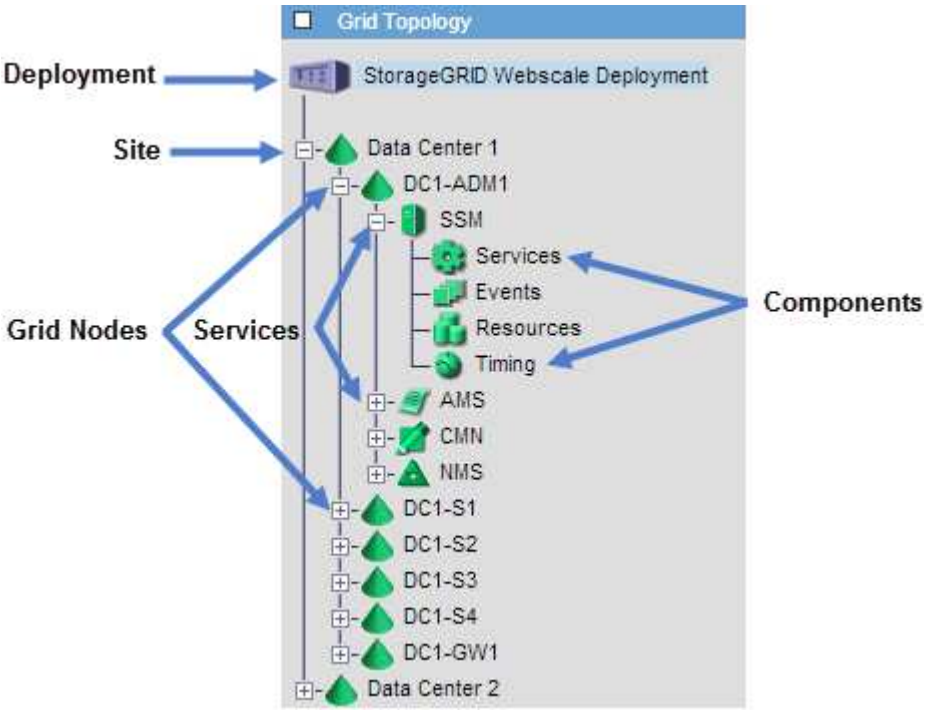
相关信息

为警报配置电子邮件服务器设置（旧系统）

查看网格拓扑树

通过网格拓扑树，您可以访问有关 StorageGRID 系统元素的详细信息，包括站点，网格节点，服务和组件。在大多数情况下，只有在文档中说明或与技术支持合作时，您才需要访问网格拓扑树。

要访问网格拓扑树，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。



要展开或折叠网格拓扑树，请单击 ⊞ 或 ⊟ 在站点，节点或服务级别。要展开或折叠整个站点或每个节点中的所有项，请按住 * 键 * 并单击。

查看支持指标

对问题描述 进行故障排除时，您可以与技术支持人员一起查看 StorageGRID 系统的详细

指标和图表。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

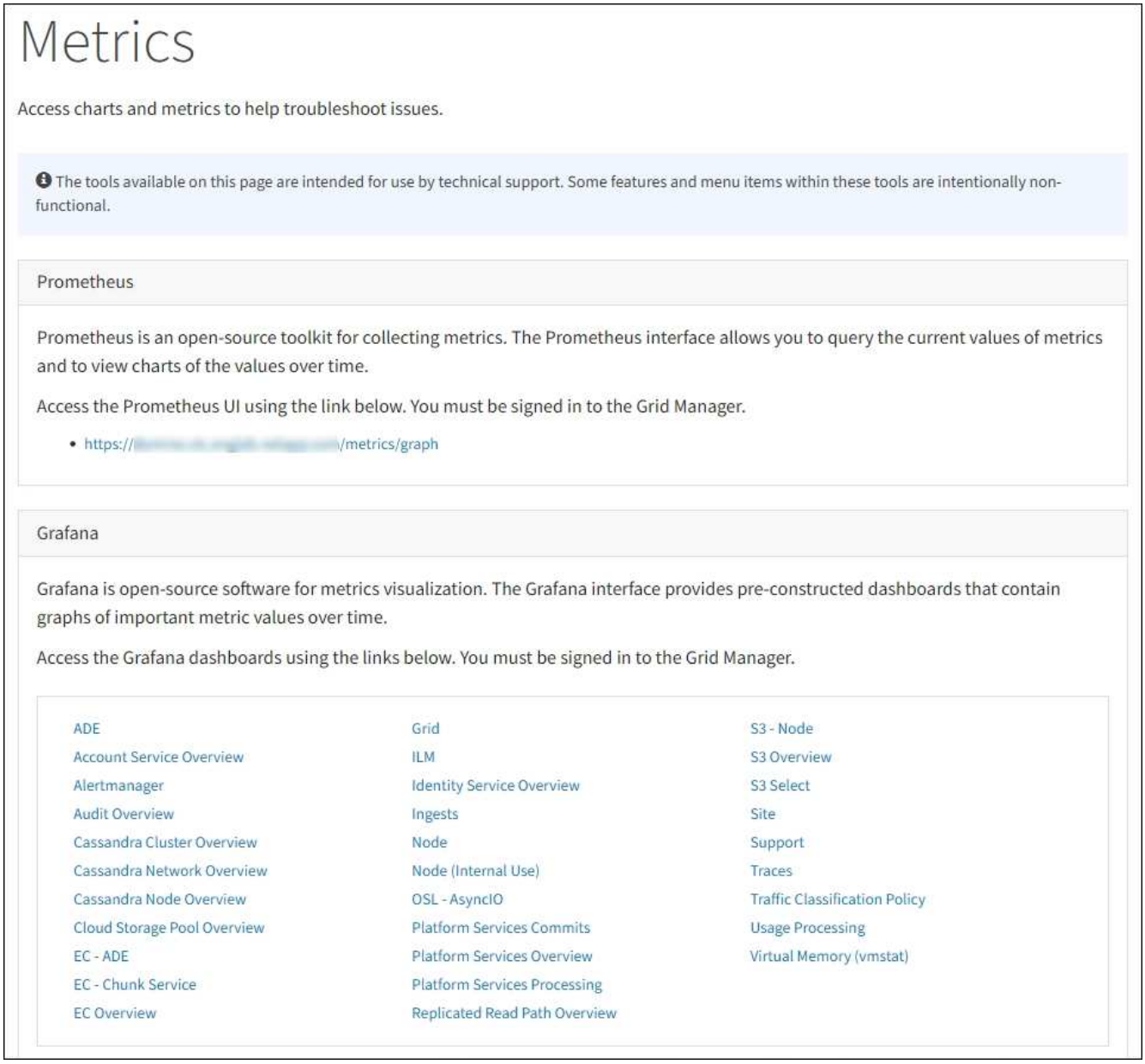
您可以通过指标页面访问 Prometheus 和 Grafana 用户界面。Prometheus 是用于收集指标的开源软件。Grafana 是用于可视化指标的开源软件。

> 指标页面上提供的工具供技术支持使用。这些工具中的某些功能和菜单项有意不起作用，可能会发生更改。请参见列表 常用的 Prometheus 指标。

步骤

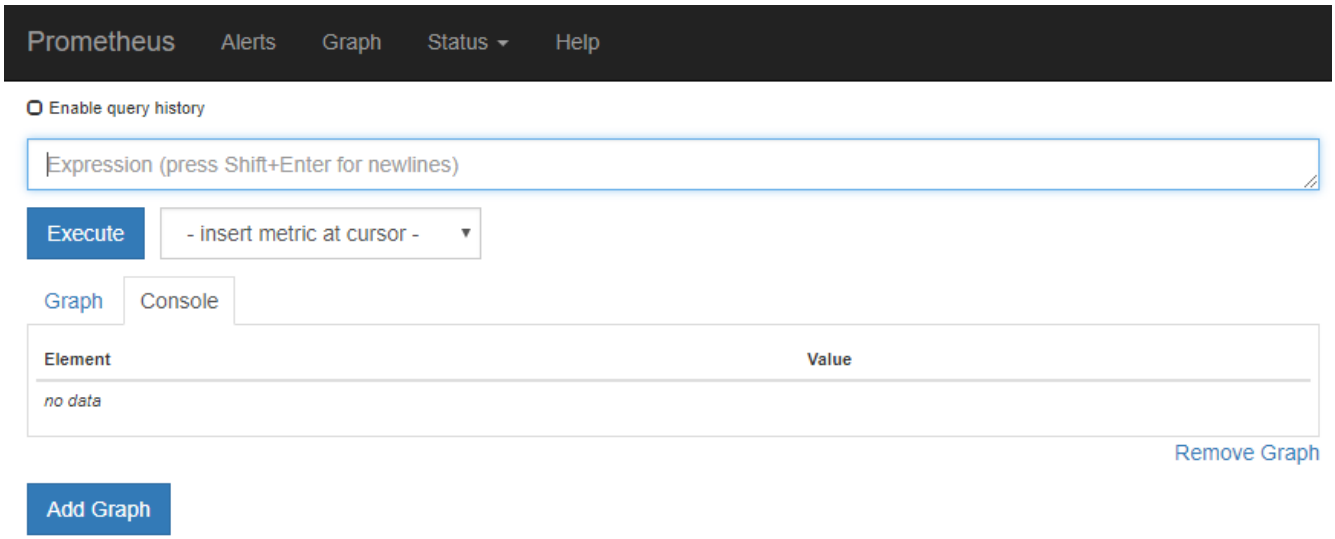
1. 根据技术支持的指示，选择 * 支持 * > * 工具 * > * 指标 * 。

   下面显示了 " 指标 " 页面的一个示例：



2. 要查询 StorageGRID 指标的当前值并查看随时间变化的值图形，请单击 Prometheus 部分中的链接。

   此时将显示 Prometheus 界面。您可以使用此界面对可用的 StorageGRID 指标执行查询，并绘制一段时间内的 StorageGRID 指标图。



名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间可能会发生更改，恕不另行通知。

3. 要访问包含一段时间内 StorageGRID 指标图的预构建信息板，请单击 Grafana 部分中的链接。

   此时将显示选定链接的 Grafana 界面。

Run diagnostics

在对问题描述 进行故障排除时，您可以与技术支持一起在 StorageGRID 系统上运行诊断并查看结果。

- 查看支持指标
- 常用的 Prometheus 指标

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有特定的访问权限。

关于此任务

" 诊断 " 页面会对网格的当前状态执行一组诊断检查。每个诊断检查可以具有以下三种状态之一：

-

- * 正常 * ： 所有值均在正常范围内。
- * 注意 * ： 一个或多个值超出正常范围。
- * 小心 * ： 一个或多个值明显超出正常范围。

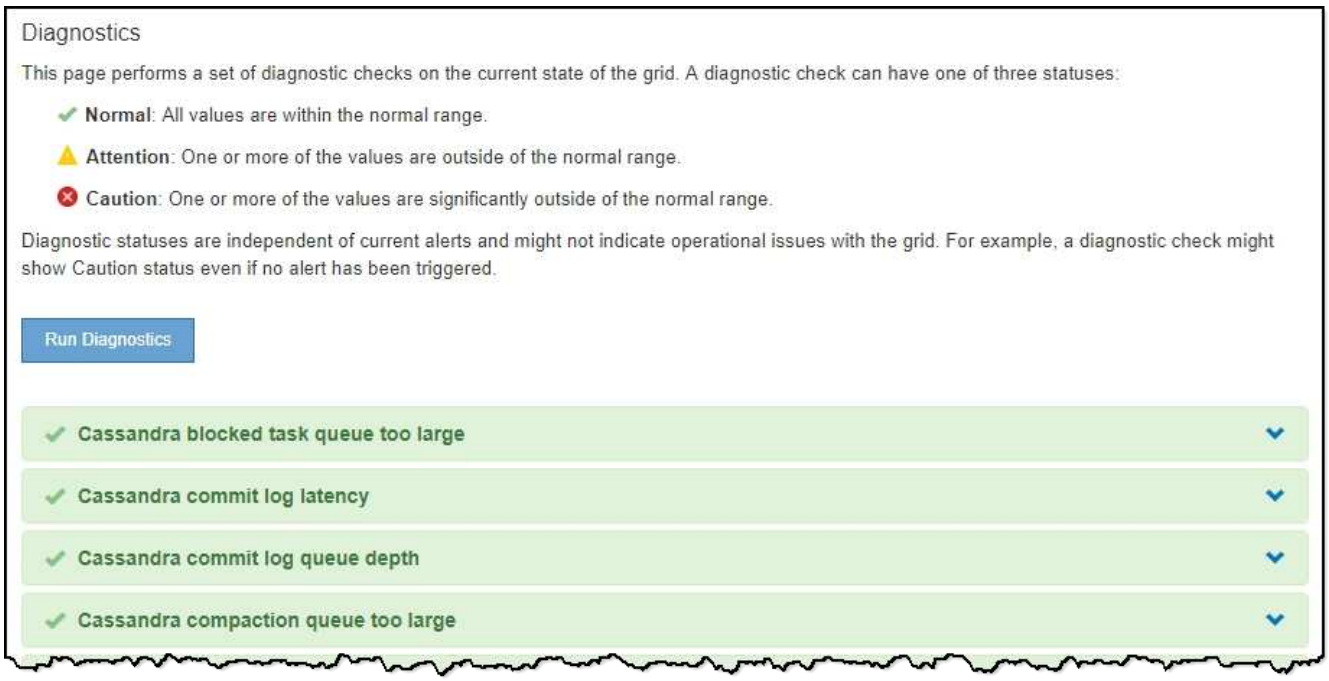
诊断状态与当前警报无关，可能并不表示网格存在操作问题。例如，即使未触发任何警报，诊断检查也可能会显示 " 小心 " 状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 诊断 * 。

   此时将显示 "Diagnostics " 页面，其中列出了每个诊断检查的结果。结果将按严重性（ " 小心 " ， " 注意 " 和 " 正常 " ）进行排序。在每个严重性范围内，结果按字母顺序排序。

   在此示例中，所有诊断均处于正常状态。



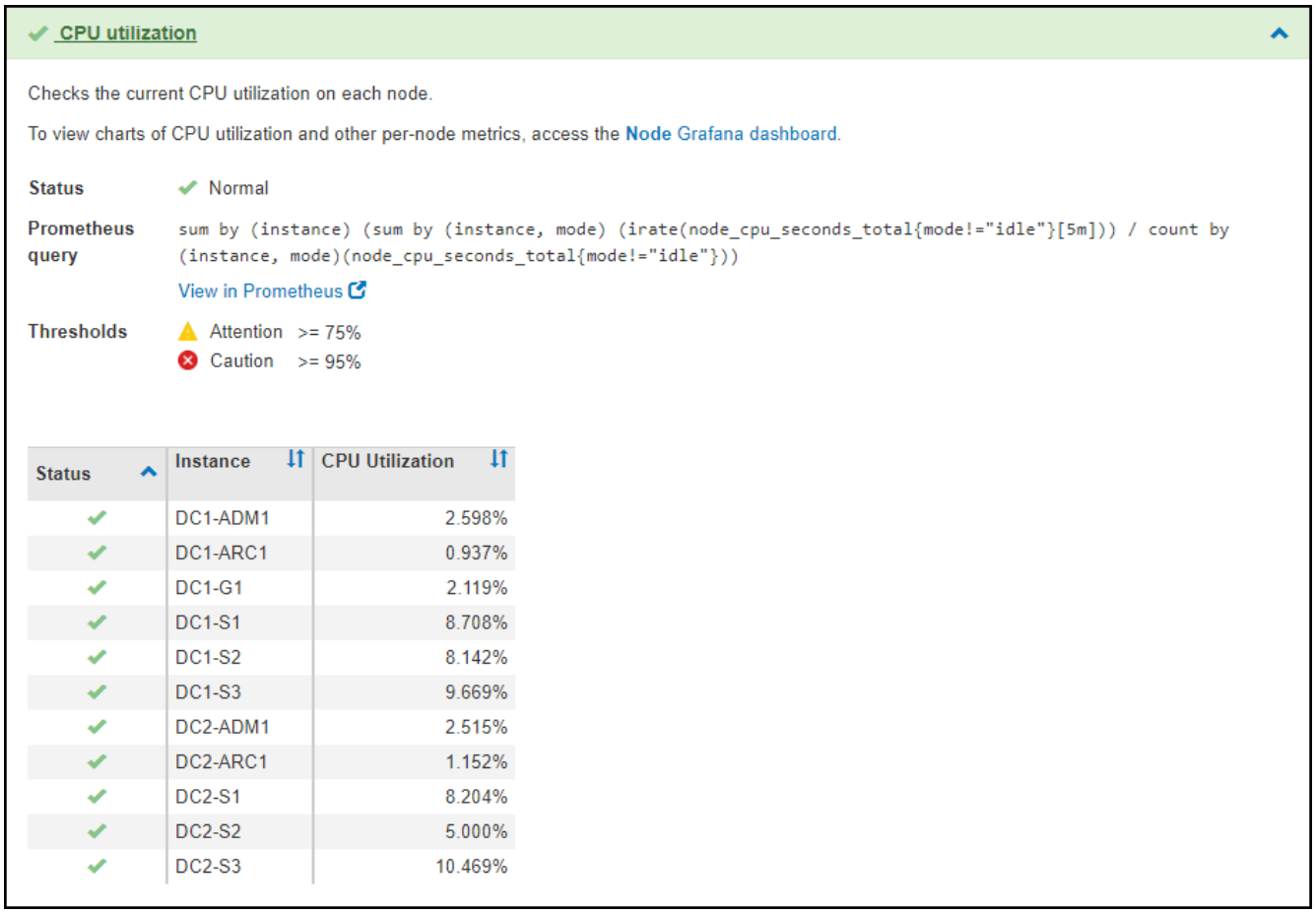
2. 要了解有关特定诊断的详细信息，请单击行中的任意位置。

   此时将显示有关此诊断及其当前结果的详细信息。此时将列出以下详细信息：

   - * 状态 * ： 此诊断的当前状态：正常，注意或小心。
   - * 项目查询 * ： 如果用于诊断，则为用于生成状态值的 Prometheus 表达式。（并非所有诊断都使用 Prometheus 表达式。）
   - * 阈值 * ： 如果可用于诊断，则为每个异常诊断状态提供系统定义的阈值。（并非所有诊断都使用阈值。）

     您不能更改这些阈值。

   - * 状态值 * ： 显示整个 StorageGRID 系统中诊断的状态和值的表。在此示例中，显示了 StorageGRID 系统中每个节点的当前 CPU 利用率。所有节点值均低于警示和警示阈值，因此诊断的整体状态为正常。



3. * 可选 * ： 要查看与此诊断相关的 Grafana 图表，请单击 * Grafana dashboard* 链接。

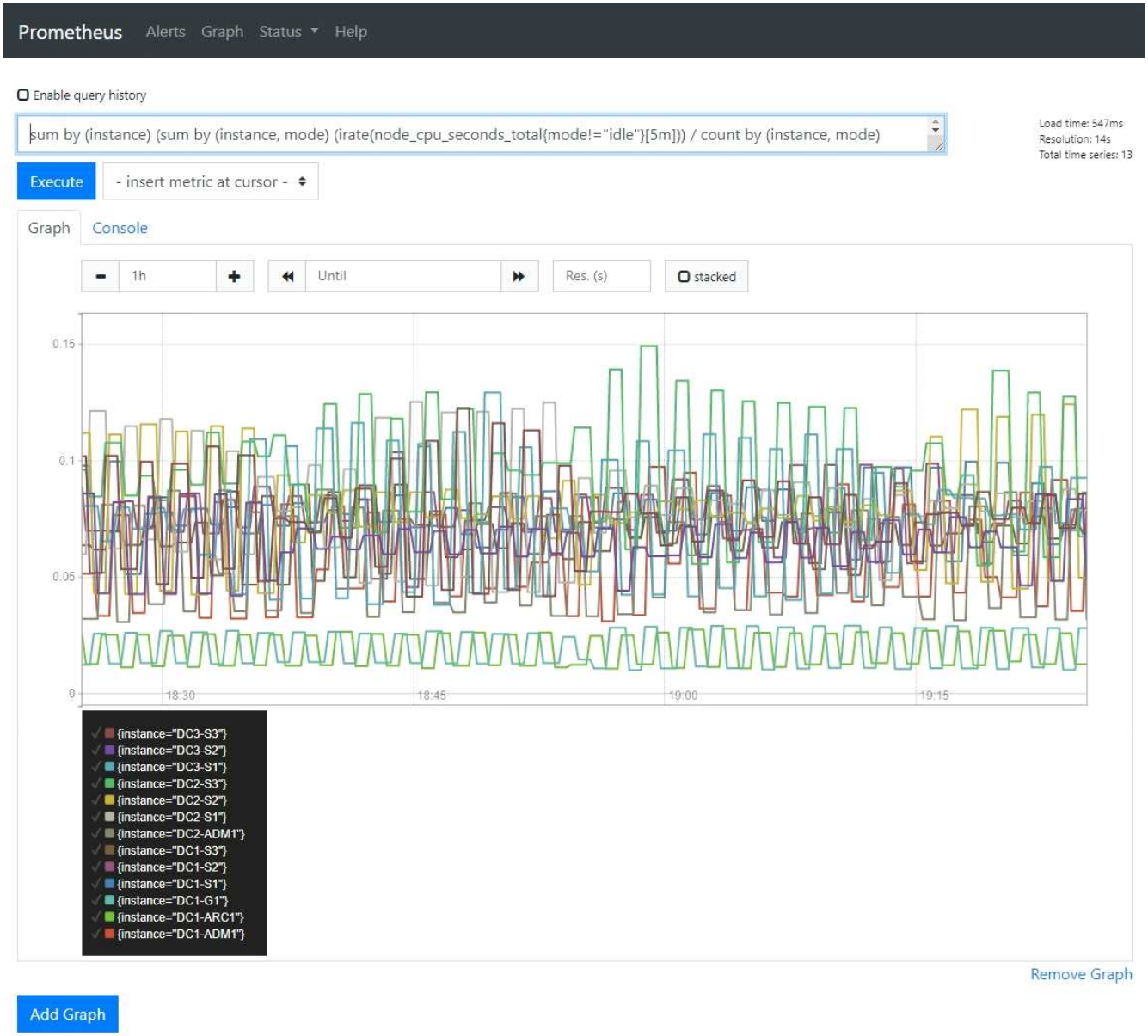
   并非所有诊断都显示此链接。

   此时将显示相关的 Grafana 信息板。在此示例中，将显示节点信息板，其中显示了此节点的 CPU 利用率随时间变化以及此节点的其他 Grafana 图表。

   > 您也可以从 * 支持 * > * 工具 * > * 指标 * 页面的 Grafana 部分访问预构建的 Grafana 信息板。

4. * 可选 * ： 要查看一段时间内的 Prometheus 表达式图表，请单击 * 在 Prometheus* 中查看。

   此时将显示诊断中使用的表达式的 Prometheus 图形。



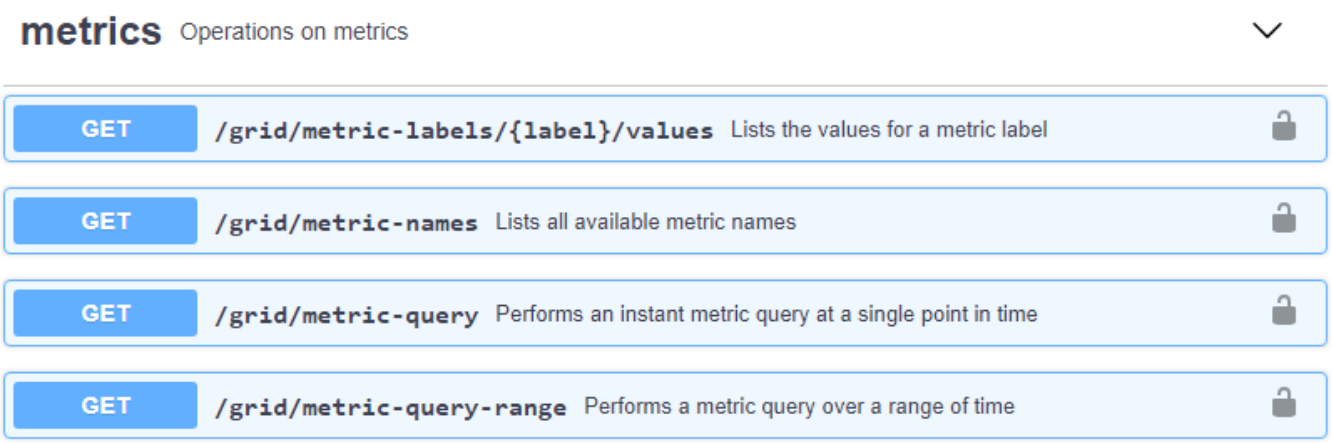
创建自定义监控应用程序

您可以使用网格管理 API 提供的 StorageGRID 指标构建自定义监控应用程序和信息板。

如果要监控网格管理器的现有页面上未显示的指标，或者要为 StorageGRID 创建自定义信息板，则可以使用网格管理 API 查询 StorageGRID 指标。

您还可以直接使用外部监控工具（例如 Grafana ）访问 Prometheus 指标。使用外部工具时，您需要上传或生成管理客户端证书，以使 StorageGRID 能够对该工具进行身份验证以确保安全性。请参见 有关管理 StorageGRID 的说明。

要查看指标 API 操作，包括可用指标的完整列表，请转到网格管理器。从页面顶部，选择帮助图标并选择 * API Documentation* > * 指标 * 。



本文档不会详细介绍如何实施自定义监控应用程序。

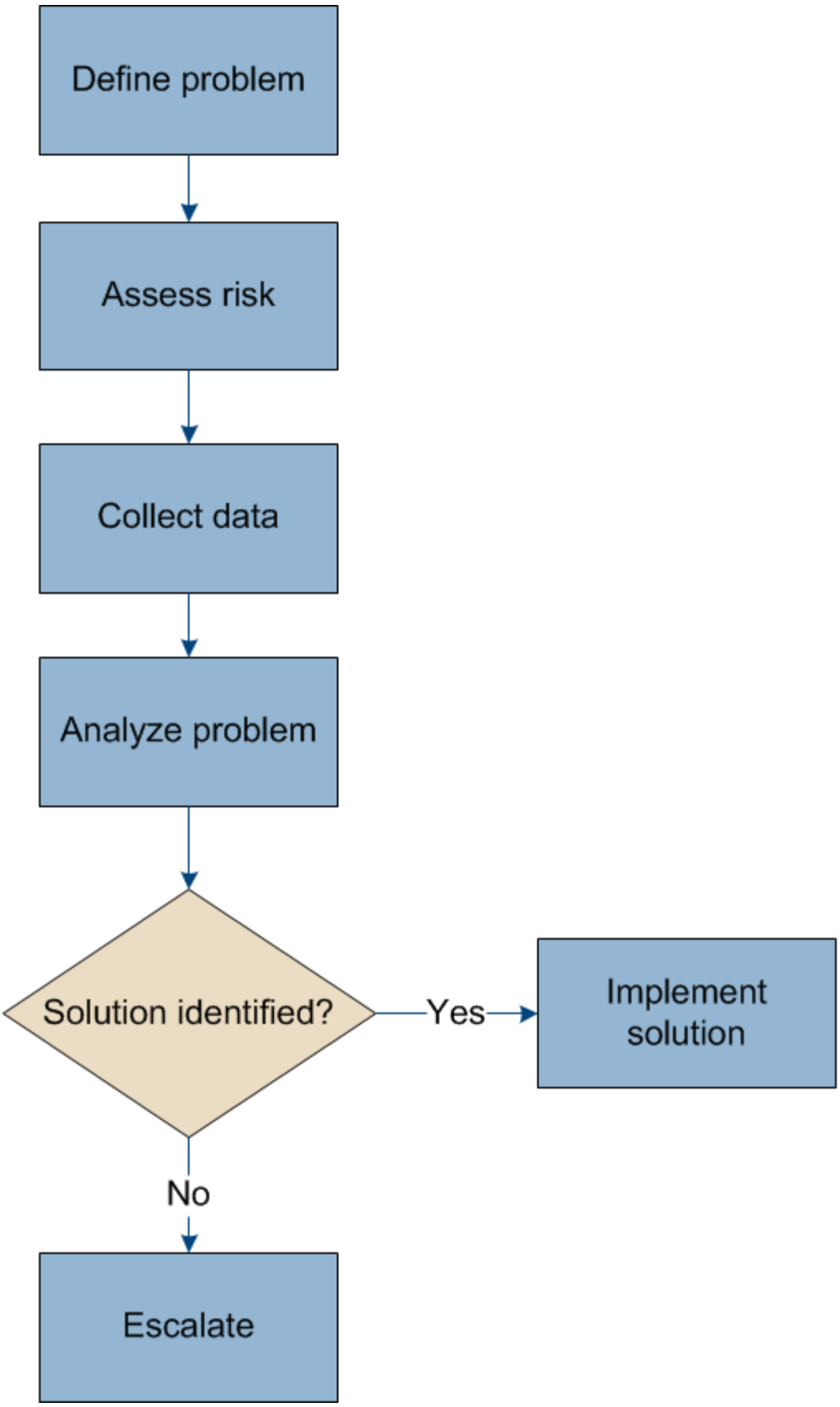
对 StorageGRID 系统进行故障排除

对 **StorageGRID** 系统进行故障排除

如果在使用 StorageGRID 系统时遇到问题，请参阅本节中的提示和准则，以帮助确定和解决问题描述 。

问题确定概述

如果遇到问题，请执行此操作 管理 StorageGRID 系统，您可以使用此图中概述的过程来识别和分析问题描述 。在许多情况下，您可以自行解决问题；但是，您可能需要将某些问题上报给技术支持。



定义问题

解决问题的第一步是明确定义问题。

下表提供了定义问题时可能收集的信息类型示例：

问题	响应示例
StorageGRID 系统正在执行什么操作或不执行什么操作？其症状是什么？	客户端应用程序报告无法将对象载入 StorageGRID 。
问题是从何时开始的？	对象载入于 2020 年 1 月 8 日 14： 50 时被首次拒绝。
您是如何首次注意到该问题的？	客户端应用程序已通知。同时还收到警报电子邮件通知。
问题是持续发生还是仅偶尔发生？	问题仍在继续。
如果此问题经常发生，则说明发生发生原因 的步骤是什么	每次客户端尝试载入对象时都会发生问题。
如果此问题间歇性发生，何时发生？记录您所知的每个意外事件的时间。	问题不是间歇性的。
您以前是否遇到过此问题？您过去遇到此问题的频率如何？	这是我第一次看到此问题描述 。

评估风险和对系统的影响

定义问题后，请评估其对 StorageGRID 系统的风险和影响。例如，存在严重警报并不一定意味着系统不提供核心服务。

下表总结了示例问题对系统操作的影响：

问题	响应示例
StorageGRID 系统是否可以载入内容？	否
客户端应用程序是否可以检索内容？	可以检索某些对象，而不能检索其他对象。
数据是否存在风险？	否
开展业务的能力是否受到严重影响？	可以，因为客户端应用程序无法将对象存储到 StorageGRID 系统，并且无法一致地检索数据。

收集数据

定义问题并评估其风险和影响后，收集数据以供分析。最有用的数据类型取决于问题的性质。

要收集的数据类型	为什么收集此数据	说明
创建最近更改的时间线	对 StorageGRID 系统，其配置或环境进行更改可以发生原因 新行为。	• 创建最近更改的时间线
查看警报和警报	警报和警报可通过提供有关可能导致问题的根本问题的重要线索，帮助您快速确定问题的根本发生原因 。 查看当前警报和警报列表，查看 StorageGRID 是否已确定问题的根发生原因 。 查看过去触发的警报和警报，以获得更多见解。	• 查看当前警报 • 查看旧警报 • 查看已解决的警报 • 查看历史警报和警报频率（传统系统）
监控事件	事件包括节点的任何系统错误或故障事件，包括网络错误等错误。监控事件以了解有关问题的更多信息或帮助进行故障排除。	• 监控事件
使用图表和文本报告确定趋势	趋势可以提供有关问题首次出现的宝贵线索，并有助于您了解事情发生的速度。	• 使用图表和图形 • 使用文本报告
建立基线	收集有关各种运行值的正常级别的信息。这些基线值以及与这些基线的偏差可以提供有价值的线索。	• 建立基线
执行载入和检索测试	要解决载入和检索的性能问题，请使用工作站存储和检索对象。将结果与使用客户端应用程序时看到的结果进行比较。	• 监控 PUT 和 GET 性能
查看审核消息	查看审核消息以详细了解 StorageGRID 操作。审核消息中的详细信息对于排除包括性能问题在内的多种类型的问题非常有用。	• 查看审核消息
检查对象位置和存储完整性	如果存在存储问题，请验证对象是否已放置在预期位置。检查存储节点上对象数据的完整性。	• 监控对象验证操作 • 确认对象数据位置 • 验证对象完整性
为技术支持收集数据	技术支持可能会要求您收集数据或查看特定信息，以帮助您解决问题。	• 收集日志文件和系统数据 • 手动触发 AutoSupport 消息 • 查看支持指标

【create_timeline】创建最近更改的时间线

出现问题时，您应考虑最近发生了哪些更改以及何时发生了这些更改。

- 对 StorageGRID 系统，其配置或环境进行更改可以发生原因 新行为。

- 更改时间线可以帮助您确定哪些更改可能会对问题描述 造成影响，以及每个更改可能会对其开发产生何种影响。

创建一个系统近期更改的表，其中包含有关每次更改发生时间的信息以及有关更改的任何相关详细信息，以及有关更改进行期间发生的其他情况的信息：

更改时间	更改类型	详细信息
例如： • 您何时开始节点恢复？ • 软件升级何时完成？ • 您是否中断了此过程？	发生什么事了？您做了什么？	记录有关变更的任何相关详细信息。例如： • 网络更改的详细信息。 • 安装了哪个修补程序。 • 客户端工作负载如何更改。 请务必注意，如果同时发生多个更改。例如，是否在升级过程中进行了此更改？

近期重大变更的示例

以下是一些可能会发生重大变化的示例：

- StorageGRID 系统是最近安装，扩展还是恢复的？
- 系统近期是否已升级？是否应用了修补程序？
- 最近是否修复或更改过任何硬件？
- 是否已更新 ILM 策略？
- 客户端工作负载是否已更改？
- 客户端应用程序或其行为是否发生变化？
- 您是否更改了负载平衡器，添加或删除了管理节点或网关节点的高可用性组？
- 是否已启动可能需要很长时间才能完成的任务？示例包括：
  - 恢复发生故障的存储节点
  - 存储节点停用
- 是否对用户身份验证进行了任何更改，例如添加租户或更改 LDAP 配置？
- 是否正在进行数据迁移？
- 最近是否启用或更改了平台服务？
- 最近是否启用了合规性？
- 是否已添加或删除云存储池？
- 是否对存储压缩或加密进行了任何更改？
- 网络基础架构是否有任何变化？例如， VLAN ，路由器或 DNS 。
- 是否对 NTP 源进行了任何更改？

- 是否对网格，管理员或客户端网络接口进行了任何更改？
- 是否对归档节点进行了任何配置更改？
- 是否对 StorageGRID 系统或其环境进行了任何其他更改？

【建立基线】建立基线

您可以通过记录各种运行值的正常级别来为系统建立基线。将来，您可以将当前值与这些基线进行比较，以帮助检测和解决异常值。

属性	价值	如何获取
平均存储消耗	GB 已用 / 天 每日消耗百分比	转到网格管理器。在节点页面上，选择整个网格或站点，然后转到存储选项卡。 在 " 已用存储 - 对象数据 " 图表上，找到一个线相当稳定的句点。将光标悬停在图表上方可估计每天占用的存储空间量 您可以收集整个系统或特定数据中心的此信息。
平均元数据消耗	GB 已用 / 天 每日消耗百分比	转到网格管理器。在节点页面上，选择整个网格或站点，然后转到存储选项卡。 在 " 已用存储 - 对象元数据 " 图表上，找到一个线相当稳定的句点。将光标悬停在图表上方，可估算每天占用的元数据存储量 您可以收集整个系统或特定数据中心的此信息。
S3/Swift 操作速率	操作数 / 秒	转到网格管理器中的信息板。在协议操作部分中，查看 S3 速率和 Swift 速率的值。 要查看特定站点或节点的载入率和检索率以及计数，请选择 * 节点 * > * 站点或存储节点 _* > * 对象 * 。将光标悬停在 Insest and retrieve 图表上，查看 S3 或 Swift 的图表。
S3/Swift 操作失败	操作	选择 * 支持 * > * 工具 * > * 网格拓扑 * 。在 API Operations 部分的 Overview 选项卡上，查看 S3 Operations - Failed 或 Swift Operations - Failed 的值。

属性	价值	如何获取
ILM 评估率	对象 / 秒	从节点页面中，选择 * ； grid_* > * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标悬停在图表上方可估算系统的 * 评估速率 * 基线值。
ILM 扫描速率	对象 / 秒	选择 * 节点 * > * 网格 _* > * ILM * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标悬停在图表上方可估算系统的 * 扫描速率 * 基线值。
从客户端操作排队的对象	对象 / 秒	选择 * 节点 * > * 网格 _* > * ILM * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标悬停在图表上方，可估算系统中 * 已排队（从客户端操作） * 的对象的基线值。
平均查询延迟	毫秒	选择 * 节点 * > * 存储节点 _* > * 对象 * 。在查询表中，查看平均延迟的值。

分析数据

使用您收集的信息确定问题的发生原因 以及可能的解决方案。

分析与问题 - 相关，但一般而言：

- 使用警报查找故障点和瓶颈。
- 使用警报历史记录和图表重建问题历史记录。
- 使用图表查找异常并将问题情况与正常运行进行比较。

上报信息检查清单

如果您无法自行解决此问题，请联系技术支持。在联系技术支持之前，请收集下表中列出的信息，以便于解决问题。

✔	项目	注释：
	问题陈述	问题症状是什么？问题是从何时开始的？是否持续或间歇性发生？如果间歇性发生，发生过什么时间？ 定义问题
	影响评估	问题的严重性是什么？对客户端应用程序有何影响？ • 客户端以前是否已成功连接？ • 客户端是否可以载入，检索和删除数据？
	StorageGRID 系统 ID	选择 * 维护 * > * 系统 * > * 许可证 * 。StorageGRID 系统 ID 显示为当前许可证的一部分。
	软件版本	从网格管理器顶部，选择帮助图标并选择 * 关于 * 以查看 StorageGRID 版本。
	自定义	总结 StorageGRID 系统的配置方式。例如，列出以下内容： • 网格是否使用存储压缩，存储加密或合规性？ • ILM 是否会创建复制或擦除编码对象？ILM 是否可确保站点冗余？ILM 规则是否使用严格，平衡或双重提交载入行为？
	日志文件和系统数据	收集系统的日志文件和系统数据。选择 * 支持 * > * 工具 * > * 日志 * 。 您可以收集整个网格或选定节点的日志。 如果仅收集选定节点的日志，请确保至少包含一个具有此 ADA 服务的存储节点。（一个站点的前三个存储节点包含此 ADC-Service 。） 收集日志文件和系统数据
	基线信息	收集有关载入操作，检索操作和存储消耗的基线信息。 建立基线
	最近更改的时间线	创建一个时间线，用于汇总系统或其环境的所有近期更改。 创建最近更改的时间线

✔	项目	注释：
	诊断问题描述 的工作历史记录	如果您已自行采取步骤对问题描述 进行诊断或故障排除，请务必记录所采取的步骤和结果。

对对象和存储问题进行故障排除

确认对象数据位置

根据问题，您可能需要确认对象数据的存储位置。例如，您可能需要验证 ILM 策略是否按预期执行，以及对象数据是否按预期存储。

您需要的内容

- 您必须具有一个对象标识符，该标识符可以是以下项之一：
  - * UUID * ： 对象的通用唯一标识符。以全大写形式输入 UUID 。
  - * CBID* ： StorageGRID 中对象的唯一标识符。您可以从审核日志中获取对象的 CBID 。输入全部大写的 CBID 。
  - * S3 存储分段和对象密钥 * ： 通过 S3 接口载入对象时，客户端应用程序使用存储和标识对象的分段和对象密钥组合。
  - * Swift 容器和对象名称 * ： 通过 Swift 界面输入对象时，客户端应用程序将使用容器和对象名称组合来存储和标识对象。

步骤

1. 选择 * ILM * > * 对象元数据查找 * 。
2. 在 * 标识符 * 字段中键入对象的标识符。

   您可以输入 UUID ， CBID ， S3 存储分段 / 对象密钥或 Swift 容器 / 对象名称。

3. 如果要查找对象的特定版本，请输入版本 ID （可选）。

4. 选择 * 查找 * 。

此时将显示对象元数据查找结果。此页面列出了以下类型的信息：

- 系统元数据，包括对象 ID （ UUID ），版本 ID （可选），对象名称，容器名称，租户帐户名称或 ID ，对象的逻辑大小，首次创建对象的日期和时间以及上次修改对象的日期和时间。
- 与对象关联的任何自定义用户元数据键值对。
- 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
- 对于复制的对象副本，为每个副本提供当前存储位置。
- 对于经过擦除编码的对象副本，为每个片段的当前存储位置。
- 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。
- 对于分段对象和多部分对象，包含分段标识符和数据大小的对象分段列表。对于包含 100 个以上区块的对象，仅显示前 100 个区块。
- 所有对象元数据均采用未处理的内部存储格式。此原始元数据包括内部系统元数据，不能保证这些元数据在版本之间持续存在。

  以下示例显示了存储为两个复制副本的 S3 测试对象的对象元数据查找结果。

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


相关信息

使用 ILM 管理对象

使用 S3

使用 Swift

对象存储（存储卷）故障

存储节点上的底层存储分为多个对象存储。对象存储也称为存储卷。

您可以查看每个存储节点的对象存储信息。对象存储显示在 * 节点 * > * 存储节点 _* > * 存储 * 页面的底部。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

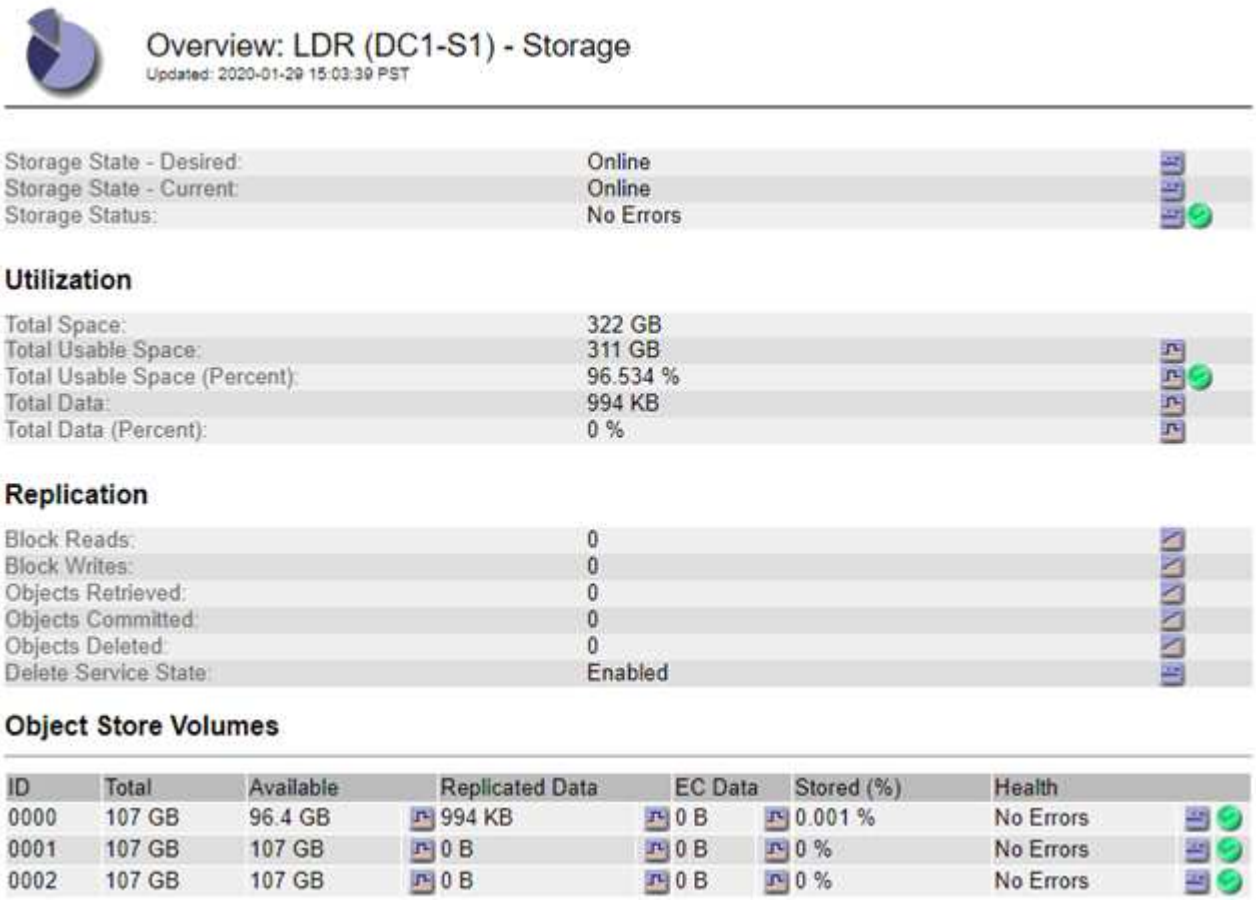
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

要查看有关每个存储节点的更多详细信息，请执行以下步骤：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 存储 * > * 概述 * > * 主 * 。



根据故障的性质，存储卷的故障可能会反映在有关存储状态或对象存储运行状况的警报中。如果存储卷发生故障，您应尽快修复故障存储卷，以将存储节点还原到完整功能。如有必要，您可以转到 * 配置 * 选项卡并将存储节点置于只读 - 状态，以便 StorageGRID 系统可以在准备服务器完全恢复时使用它进行数据检索。

相关信息

恢复和维护

验证对象完整性

StorageGRID 系统会验证存储节点上对象数据的完整性，并检查是否存在损坏和缺失的对象。

验证过程有两个：后台验证和对象存在检查（以前称为前台验证）。它们协同工作，确保数据完整性。后台验证会自动运行，并持续检查对象数据的正确性。用户可以触发对象存在检查，以便更快速地验证对象是否存在（尽管不是正确）。

什么是后台验证？

后台验证过程会自动持续检查存储节点中是否存在损坏的对象数据副本，并自动尝试修复发现的任何问题。

后台验证将检查复制对象和经过纠删编码的对象的完整性，如下所示：

- * 复制对象 *：如果后台验证过程发现复制的对象已损坏，则损坏的副本将从其位置中删除，并隔离到存储节点上的其他位置。然后，系统将生成一个未损坏的新副本并放置该副本以满足活动 ILM 策略的要求。新副本可能不会放置在用于原始副本的存储节点上。

> 损坏的对象数据将被隔离而不是从系统中删除，以便仍可访问。有关访问隔离对象数据的详细信息，请联系技术支持。

- * 擦除编码对象 *：如果后台验证过程检测到擦除编码对象的片段已损坏，则 StorageGRID 会自动尝试使用剩余的数据和奇偶校验片段在同一个存储节点上原位重建缺失的片段。如果损坏的片段无法重建，则会尝试检索对象的另一个副本。如果检索成功，则会执行 ILM 评估以创建经过纠删编码的对象的替代副本。

  后台验证过程仅检查存储节点上的对象。它不会检查归档节点或云存储池中的对象。对象必须超过四天，才能进行后台验证。

后台验证以连续速率运行，不会干扰普通系统活动。无法停止后台验证。但是，如果您怀疑存在问题，则可以提高后台验证率，以便更快地验证存储节点的内容。

与后台验证相关的警报和警报（传统）

如果系统检测到某个损坏的对象，而该对象无法自动更正（因为该损坏会阻止识别该对象），则会触发 * 检测到未标识的损坏对象 * 警报。

如果后台验证无法替换损坏的对象，因为它找不到其他副本，则会触发 * 对象丢失 * 警报。

更改后台验证速率

如果您担心数据完整性，可以更改后台验证检查存储节点上复制的对象数据的速率。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

您可以更改存储节点上用于后台验证的验证速率：

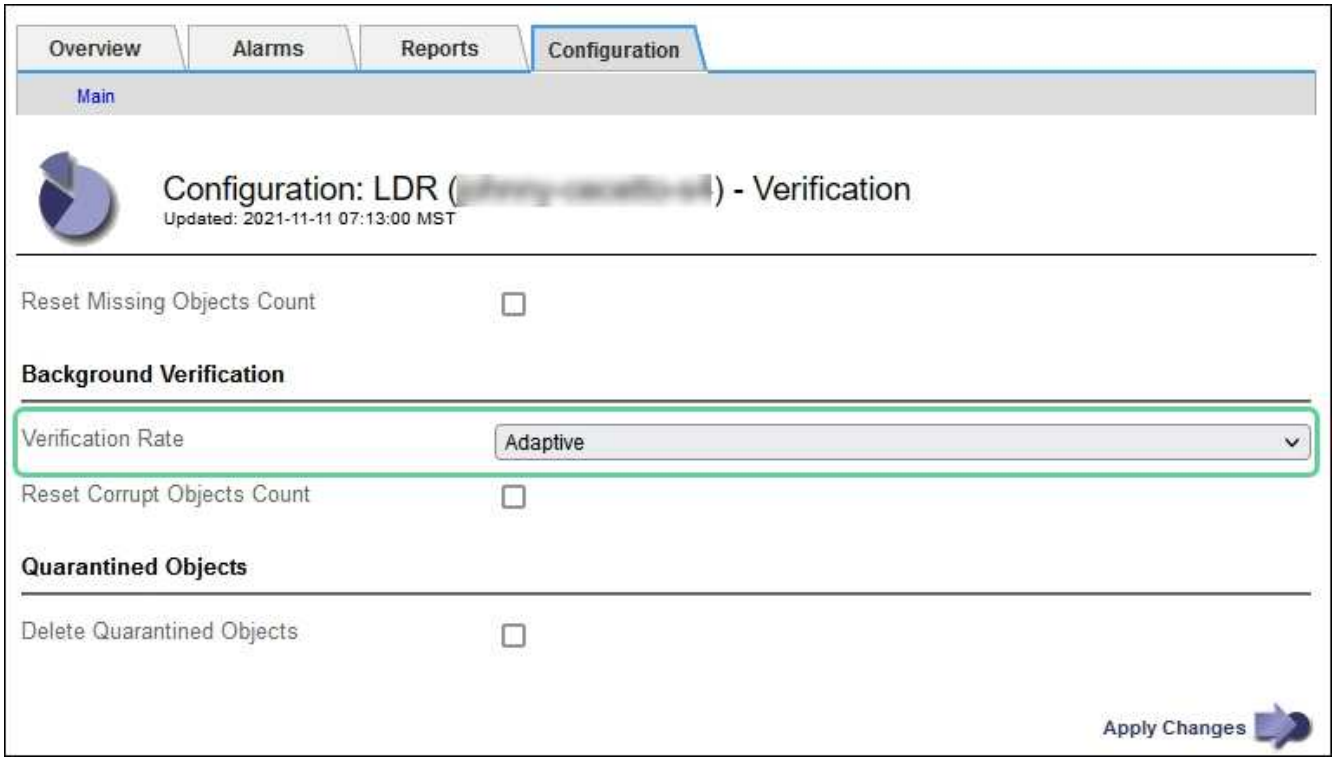
- Adaptive：默认设置。此任务用于验证速度最多为 4 MB/ 秒或 10 个对象 / 秒（以先超过者为准）。
- high：存储验证进展迅速，速度可能会减慢常规系统活动。

只有当您怀疑硬件或软件故障可能包含损坏的对象数据时，才使用 " 高 " 验证率。高优先级后台验证完成后，验证率将自动重置为自适应。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 存储节点 _* > * LDR* > * 验证 * 。
3. 选择 * 配置 * > * 主 * 。
4. 转至 * LDR* > * 验证 * > * 配置 * > * 主 * 。

5. 在后台验证下，选择 * 验证速率 * > * 高 * 或 * 验证速率 * > * 自适应 * 。



将验证速率设置为高会在通知级别触发 VPRi （验证速率）传统警报。

6. 单击 * 应用更改 * 。
7. 监控复制对象的后台验证结果。
   a. 转至 * 节点 * > * 存储节点 _* > * 对象 * 。
   b. 在验证部分中，监控 * 损坏对象 * 和 * 未标识的损坏对象 * 的值。

      如果后台验证发现复制的对象数据损坏，则 * 损坏的对象 * 指标将递增， StorageGRID 将尝试从数据中提取对象标识符，如下所示：

      - 如果可以提取对象标识符， StorageGRID 会自动为对象数据创建一个新副本。可以在 StorageGRID 系统中满足活动 ILM 策略的任何位置创建新副本。
      - 如果无法提取对象标识符（因为它已损坏），则会增加 "Corrupt Objects Unidentifited" 指标，并触发 "* Unidentified Corrupt object detected* " 警报。

   c. 如果发现复制的对象数据损坏，请联系技术支持以确定损坏的根发生原因 。
8. 监控纠删编码对象的后台验证结果。

   如果后台验证发现擦除编码对象数据的损坏片段，则检测到的损坏片段属性将递增。StorageGRID 通过在同一存储节点上原位重建损坏的片段来恢复。

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 存储节点 _* > * LDR* > * 擦除编码 * 。
   c. 在验证结果表中，监控已检测到损坏的碎片 （ ECCD ） 属性。

9. 在 StorageGRID 系统自动还原损坏的对象后，重置损坏的对象计数。
   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 存储节点 _* > * LDR* > * 验证 * > * 配置 * 。
   c. 选择 * 重置损坏的对象计数 * 。
   d. 单击 * 应用更改 * 。
10. 如果您确信不需要隔离对象，可以将其删除。

> 如果触发了 * 对象丢失 * 警报或丢失（对象丢失）旧警报，技术支持可能希望访问隔离的对象以帮助调试底层问题描述 或尝试数据恢复。

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 存储节点 _* > * LDR* > * 验证 * > * 配置 * 。
   c. 选择 * 删除隔离的对象 * 。
   d. 选择 * 应用更改 * 。

什么是对象存在检查?

对象存在检查可验证存储节点上是否存在所有预期复制的对象副本以及经过纠删编码的片段。对象存在检查不会验证对象数据本身（后台验证会验证）；相反，它可以提供一种验证存储设备完整性的方法，尤其是在最新的硬件问题描述 可能会影响数据完整性的情况下。

与自动执行的后台验证不同，您必须手动启动对象存在检查作业。

对象存在检查会读取存储在 StorageGRID 中的每个对象的元数据，并验证是否存在复制的对象副本和经过纠删编码的对象片段。任何缺失的数据将按以下方式处理：

- * 复制的副本 * ： 如果缺少已复制对象数据的副本， StorageGRID 会自动尝试替换存储在系统其他位置的副本中的副本。存储节点通过 ILM 评估运行现有副本，该评估将确定此对象不再符合当前 ILM 策略，因为缺少另一个副本。系统会生成并放置一个新副本以满足系统的活动 ILM 策略。此新副本可能不会放置在存储缺失副本的同一位置。
- * 擦除编码片段 * ： 如果缺少擦除编码对象的片段， StorageGRID 会自动尝试使用剩余片段在同一存储节点上原位重建缺失的片段。如果无法重建缺少的片段（因为丢失了太多的片段）， ILM 将尝试查找对象的另一个副本，以便生成经过纠删编码的新片段。

运行对象存在检查

一次创建并运行一个对象存在检查作业。创建作业时，您可以选择要验证的存储节点和卷。您还可以为作业选择一致性控制。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或根访问权限。
- 您已确保要检查的存储节点处于联机状态。选择 * 节点 * 以查看节点表。确保要检查的节点的节点名称旁边未显示任何警报图标。
- 您已确保要检查的节点上 * 未 * 运行以下过程：

- 网格扩展以添加存储节点
- 存储节点停用
- 恢复发生故障的存储卷
- 恢复系统驱动器出现故障的存储节点
- EC 重新平衡
- 设备节点克隆

在这些过程中，对象存在检查不会提供有用的信息。

关于此任务

根据网格中的对象数量，选定存储节点和卷以及选定一致性控制，完成对象存在检查作业可能需要数天或数周时间。一次只能运行一个作业，但可以同时选择多个存储节点和卷。

步骤

1. 选择 * 维护 * > * 任务 * > * 对象存在检查 * 。
2. 选择 * 创建作业 * 。此时将显示创建对象存在检查作业向导。
3. 选择包含要验证的卷的节点。要选择所有联机节点，请选中列标题中的 * 节点名称 * 复选框。

   您可以按节点名称或站点进行搜索。

   您不能选择未连接到网格的节点。

4. 选择 * 继续 * 。
5. 为列表中的每个节点选择一个或多个卷。您可以使用存储卷编号或节点名称搜索卷。

   要为选定的每个节点选择所有卷，请选中列标题中的 * 存储卷 * 复选框。

6. 选择 * 继续 * 。
7. 选择作业的一致性控制。

   一致性控制用于确定对象存在检查所使用的对象元数据副本数。

   - * 强站点 * ： 在一个站点上创建两个元数据副本。
   - * 强 - 全局 * ： 每个站点上有两个元数据副本。
   - * 全部 * （默认）： 每个站点上的所有三个元数据副本。

     有关一致性控制的详细信息，请参见向导中的说明。

8. 选择 * 继续 * 。
9. 查看并验证您的选择。您可以选择 * 上一步 * 以转到向导中的上一步以更新所做的选择。

   此时将生成并运行对象存在检查作业，直到出现以下情况之一：

   - 作业完成。
   - 暂停或取消作业。您可以恢复已暂停的作业，但无法恢复已取消的作业。

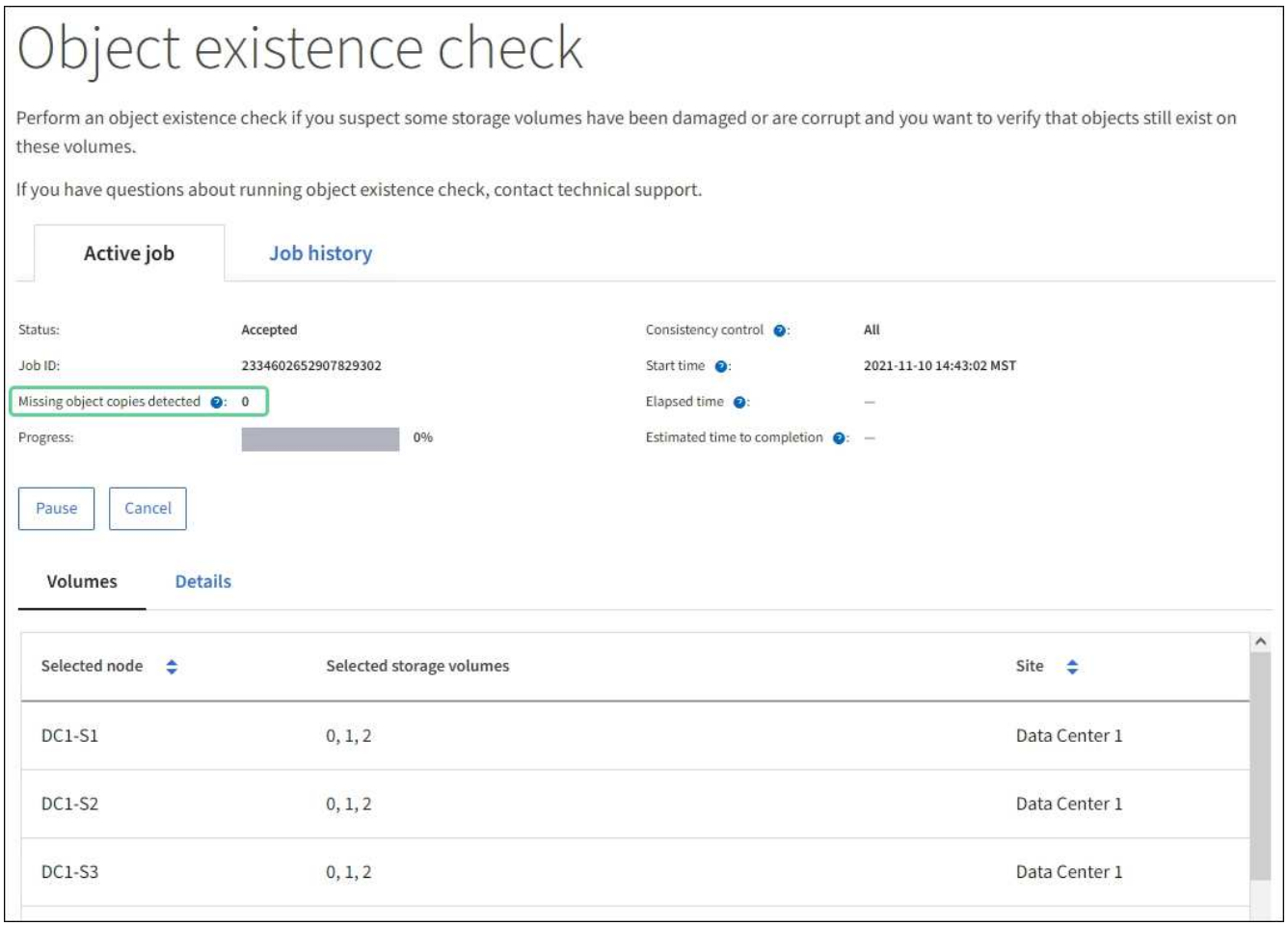
- 作业停止。此时将触发 * 对象存在检查已停止 * 警报。按照为警报指定的更正操作进行操作。
- 作业失败。触发 * 对象存在检查失败 * 警报。按照为警报指定的更正操作进行操作。
- 此时将显示 " 服务不可用` " 或 "`内部服务器错误 `S` " 消息。一分钟后，刷新页面以继续监控作业。

> 您可以根据需要离开对象存在检查页面并返回以继续监控作业。

10. 在作业运行时，查看 * 活动作业 * 选项卡，并记下检测到的缺少对象副本的值。

    此值表示缺少一个或多个片段的复制对象和经过纠删编码的对象的副本总数。

    如果检测到的缺少对象副本数大于 100 ，则可能存在存储节点存储的问题描述 。



11. 作业完成后，执行任何其他所需操作：
    - 如果检测到缺少对象副本为零，则未发现任何问题。无需执行任何操作。
    - 如果检测到缺少对象副本大于零，并且未触发 * 对象丢失 * 警报，则系统会修复所有缺少的副本。验证是否已更正任何硬件问题，以防止将来对对象副本造成损坏。
    - 如果检测到缺少对象副本大于零，并且已触发 * 对象丢失 * 警报，则数据完整性可能会受到影响。请联系技术支持。
    - 您可以使用 grep 提取 LLST 审核消息来调查丢失的对象副本： `grep LLST audit_file_name` 。

      此操作步骤 类似于的 调查丢失的对象，尽管对于对象副本，您搜索的是 `LLST` 而不是 `OLST` 。

12. 如果您为作业选择了强站点一致性或强全局一致性控制，请等待大约三周以保持元数据一致性，然后在相同卷上重新运行此作业。

    如果 StorageGRID 有时间为作业中包含的节点和卷实现元数据一致发生原因 性，则重新运行作业可能会错误地清除报告的缺失对象副本，或者如果未选中其他对象副本，则重新运行作业可能会清除这些副本。

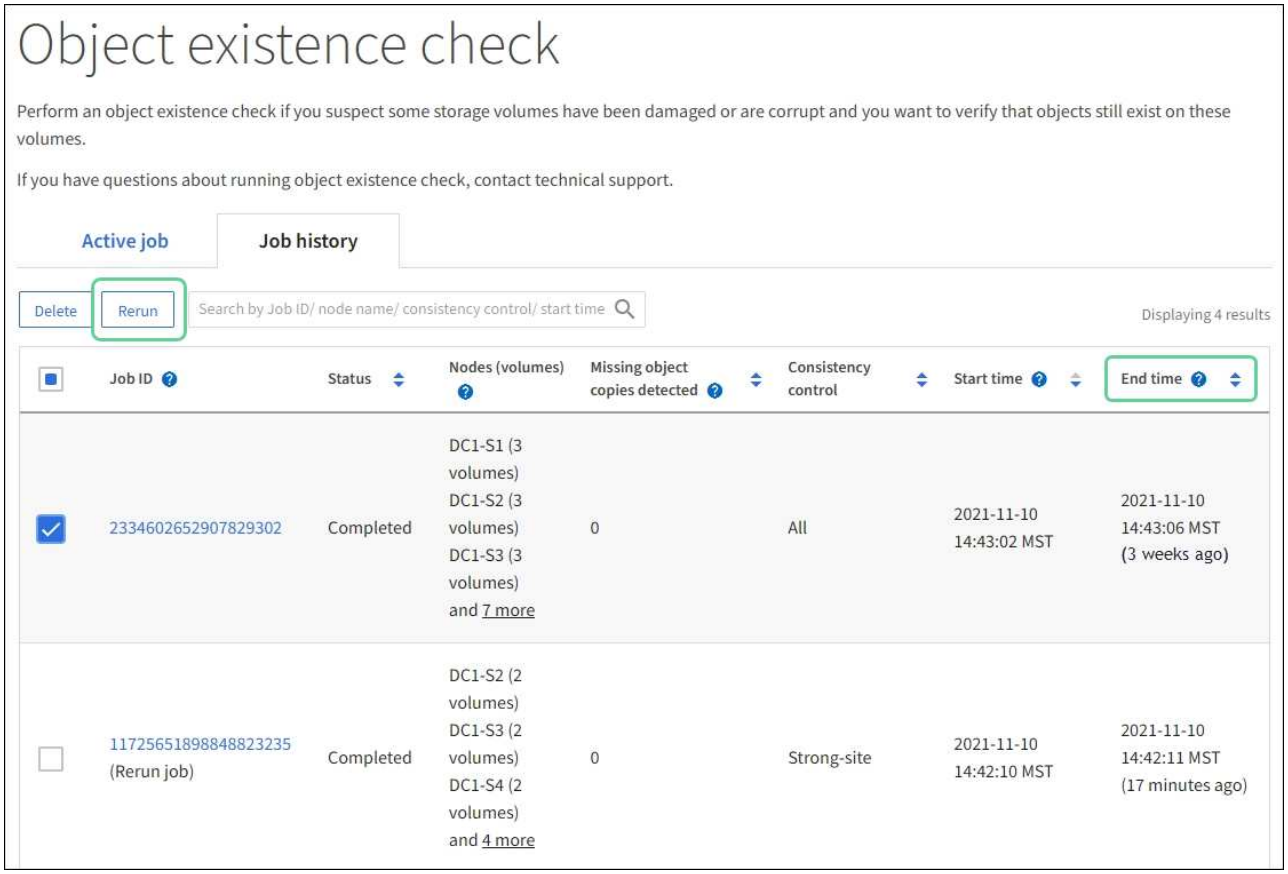
    a. 选择 * 维护 * > * 对象存在检查 * > * 作业历史记录 * 。

    b. 确定哪些作业已准备好重新运行：

        i. 查看 * 结束时间 * 列，确定三周前运行的作业。

        ii. 对于这些作业，请扫描一致性控制列中的强站点或强全局。

    c. 选中要重新运行的每个作业对应的复选框，然后选择 * 重新运行 * 。



    d. 在重新运行作业向导中，查看选定节点和卷以及一致性控制。

    e. 准备好重新运行作业后，请选择 * 重新运行 * 。

此时将显示活动作业选项卡。您选择的所有作业都将在强站点的一致性控制下作为一个作业重新运行。详细信息部分中的 * 相关作业 * 字段列出了原始作业的作业 ID 。

完成后

如果您仍对数据完整性有顾虑，请转到 * 支持 * > * 工具 * > * 网格拓扑 * > * 站点 _ * > * 存储节点 _ * > * LDR* > * 验证 * > * 配置 * > * 主 * 并提高验证后台速率。后台验证会检查所有已存储对象数据的准确性，并修复发现的任何问题。尽快发现并修复潜在问题可降低数据丢失的风险。

可以出于多种原因检索对象，包括从客户端应用程序读取请求，对复制的对象数据进行后台验证， ILM 重新评估以及在存储节点恢复期间还原对象数据。

StorageGRID 系统使用对象元数据中的位置信息来确定从哪个位置检索对象。如果在预期位置未找到对象的副本，则系统会尝试从系统中的其他位置检索该对象的另一个副本，前提是 ILM 策略包含一条规则，用于为该对象创建两个或更多副本。

如果此检索成功， StorageGRID 系统将替换缺少的对象副本。否则，系统将触发 * 对象丢失 * 警报，如下所示：

- 对于复制的副本，如果无法检索到另一个副本，则会将对象视为丢失，并触发警报。
- 对于经过擦除编码的副本，如果无法从预期位置检索到副本，则在尝试从其他位置检索副本之前，检测到的损坏副本（ DECOR ）属性会递增 1 。如果未找到其他副本，则会触发警报。

您应立即调查所有 * 对象丢失 * 警报，以确定丢失的根发生原因 ，并确定对象是否仍位于脱机存储节点或归档节点中，或者当前是否不可用。

如果没有副本的对象数据丢失，则不存在恢复解决方案 。但是，您必须重置丢失对象计数器，以防止已知丢失的对象屏蔽任何新的丢失对象。

相关信息

调查丢失的对象

重置丢失和缺失的对象计数

调查丢失的对象

触发 * 对象丢失 * 警报时，您必须立即进行调查。收集有关受影响对象的信息并联系技术支持。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。

关于此任务

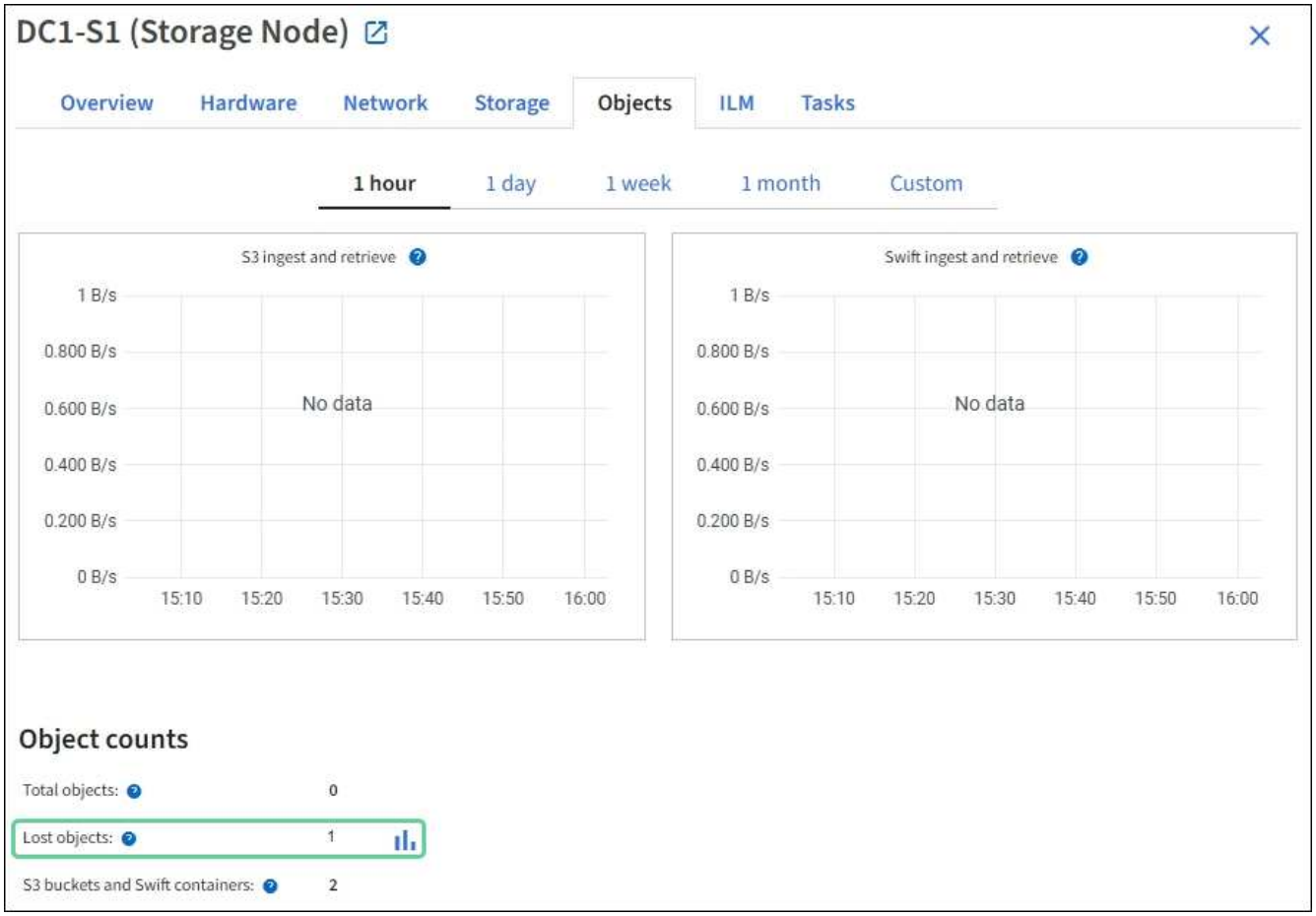
"* 对象丢失 * " 警报表示 StorageGRID 认为网格中没有对象副本。数据可能已永久丢失。

立即调查丢失的对象警报。您可能需要采取措施以防止进一步数据丢失。在某些情况下，如果您立即采取措施，则可能能够还原丢失的对象。

步骤

1. 选择 * 节点 * 。
2. 选择 * 存储节点 _* > * 对象 * 。
3. 查看对象计数表中显示的丢失对象的数量。

此数字表示此网格节点在整个 StorageGRID 系统中检测到缺少的对象总数。该值是 LDR 和 DDS 服务中数据存储组件的丢失对象计数器之和。



4. 从管理节点访问审核日志，以确定触发 * 对象丢失 * 警报的对象的唯一标识符（ UUID ）：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 更改为审核日志所在的目录。输入： `cd /var/local/audit/export/`
   c. 使用 grep 提取对象丢失（ OLST ）审核消息。输入： `grep OLST audit_file_name`
   d. 记下消息中包含的 UUID 值。

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. 使用 `ObjectByUUID` 命令按对象标识符（ UUID ）查找对象，然后确定数据是否存在风险。

   a. Telnet 到 localhost 1402 以访问 LDR 控制台。

   b. 输入： ` /proc/obrp/ObjectByUUID UID_Value`

      在第一个示例中， `UUID` 为 `926026C4-00A4-449B-AC72-BCCA72DD1311` 的对象列出了两个位置。

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
```

```
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

在第二个示例中， `UUID` 为 `926026C4-00A4-449B-AC72-BCCA72DD1311` 的对象没有列出任何位置。

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. 查看 /proc/obrp/ObjectByUUID 的输出，并采取相应的操作：

元数据	结论
未找到对象（ "error" ： "" ）	如果未找到对象，则返回消息 "error" ： "" 。 如果未找到此对象，您可以重置 * 丢失的对象 * 计数以清除警报。缺少对象表示该对象已被有意删除。
位置 > 0	如果输出中列出了一些位置，则 * 对象丢失 * 警报可能为误报。 确认对象存在。使用输出中列出的节点 ID 和文件路径确认对象文件位于列出的位置。 （的操作步骤 正在搜索可能丢失的对象 介绍如何使用节点 ID 查找正确的存储节点。） 如果对象存在，您可以重置 * 丢失的对象 * 计数以清除警报。
位置 = 0	如果输出中未列出任何位置，则此对象可能会丢失。您可以尝试 搜索并还原对象 您也可以联系技术支持。 技术支持可能会要求您确定是否正在进行存储恢复操作步骤 。也就是说，是否已在任何存储节点上发出 *repair-data* 命令，并且恢复是否仍在进行中？请参见有关的信息 将对象数据还原到存储卷。

相关信息

查看审核日志

搜索并还原可能丢失的对象

可能会找到并还原已触发 " 对象丢失（丢失） " 警报和 " 对象丢失 * " 警报且您已确定可能丢失的对象。

您需要的内容

- 您必须具有 "`调查丢失的对象 " 中标识的任何丢失对象的 UUID 。`
- 您必须具有 `passwords.txt` 文件。

关于此任务

您可以按照此操作步骤 在网格中其他位置查找丢失对象的复制副本。在大多数情况下，找不到丢失的对象。但是，在某些情况下，如果您立即采取措施，则可能能够找到并还原丢失的复制对象。

请联系技术支持以获得有关此操作步骤 的帮助。

步骤

1. 在管理节点中，搜索审核日志以查找可能的对象位置：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 `$` 更改为 `#` 。

b. 更改为审核日志所在的目录： `cd /var/local/audit/export/`

c. 使用 grep 提取与可能丢失的对象关联的审核消息并将其发送到输出文件。输入： `grep uuid-valueaudit_file_name > output_file_name`

例如：

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_lost_object.txt
```

d. 使用 grep 从此输出文件中提取丢失位置（ LLLST ）审核消息。输入： `grep LLST output_file_name`

例如：

```
Admin: # grep LLST messages_about_lost_objects.txt
```

LLST 审核消息类似于此示例消息。

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. 在 LLST 消息中找到 PCLD 字段和 NOID 字段。

如果存在，则 PCLD 的值为磁盘上缺少复制对象副本的完整路径。NOID 的值是可能找到对象副本的 LDR 的节点 ID 。

如果找到对象位置，您可能能够还原该对象。

f. 找到此 LDR 节点 ID 的存储节点。

使用节点 ID 查找存储节点的方法有两种：

- 在网格管理器中，选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 。 Data Center_* > * 。 Storage Node_* > * 。LDR 节点 ID 位于 Node Information 表中。查看每个存储节点的信息，直到找到托管此 LDR 的存储节点为止。

- 下载并解压缩网格的恢复软件包。该软件包中有一个 *\docs* 目录。如果打开 index.html 文件， " 服务器摘要 " 将显示所有网格节点的所有节点 ID 。

2. 确定对象是否位于审核消息中指示的存储节点上：

   a. 登录到网格节点：

      i. 输入以下命令： `ssh admin@grid_node_ip`

      ii. 输入 `passwords.txt` 文件中列出的密码。

      iii. 输入以下命令切换到 root： `su -`

      iv. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

1. 确定对象的文件路径是否存在。

对于对象的文件路径，请使用 LLST 审核消息中的 PCLD 值。

例如，输入：

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

- 注 * ：在命令中，始终用单引号将对象文件路径括起来，以转义任何特殊字符。
- 如果未找到对象路径，则此对象将丢失，无法使用此操作步骤 进行还原。请联系技术支持。
- 如果找到对象路径，请继续执行步骤 将对象还原到 StorageGRID。您可以尝试将找到的对象还原回 StorageGRID 。

   a. 【还原对象到 StorageGRID ， start=3]] 如果找到对象路径，请尝试将对象还原到 StorageGRID ：

      i. 从同一个存储节点中，更改对象文件的所有权，以便可通过 StorageGRID 进行管理。输入： `chown LDR 用户： byncast 'file_path_of_object'`

      ii. Telnet 到 localhost 1402 以访问 LDR 控制台。输入： `telnet 0 1402`

      iii. 输入： `cd /proc/stor`

      iv. 输入： `object_found 'file_path_of_object"`

      例如，输入：

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      +
      发出 `objection\_found` 命令，向网格通知对象的位置。它还会触发活动的 ILM 策略，该策略会根据策略中的指定创建其他副本。

- 注 * ：如果发现对象所在的存储节点脱机，则可以将该对象复制到任何联机存储节点。将对象放置在联机存储节点的任何 /var/local/rangedb 目录中。然后，使用该对象的文件路径问题描述 `Object\\_found` 命令。

- 如果无法还原此对象，则 `Object\\_found` 命令将失败。请联系技术支持。
- 如果对象已成功还原到 StorageGRID ，则会显示一条成功消息。例如：

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

继续执行步骤 验证是否已创建新位置

i. 如果对象已成功还原到 StorageGRID ，请验证是否已创建新位置。

A. 输入： `cd /proc/obRP`

B. 输入： `ObjectByUUID UID_Value`

以下示例显示 UUID 为 926026C4-00A4-449B-AC72-BCCA72DD1311 的对象有两个位置。

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
```

```
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

1. 从 LDR 控制台注销。输入： `exit`
   a. 在管理节点中，搜索此对象的 ORLM 审核消息的审核日志，以确认信息生命周期管理（ ILM ）已根据需要放置副本。
2. 登录到网格节点：
   a. 输入以下命令： `ssh admin@grid_node_ip`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
3. 更改为审核日志所在的目录： `cd /var/local/audit/export/`
4. 使用 grep 将与对象关联的审核消息提取到输出文件中。输入： `grep uuid-valueaudit_file_name > output_file_name`

   例如：

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

5. 使用 grep 从此输出文件中提取对象规则已满足（ ORLM ）审核消息。输入： `grep ORLM output_file_name`

   例如：

   ```
   Admin: # grep ORLM messages_about_restored_object.txt
   ```

   ORLM 审核消息类似于此示例消息。

   ```
   [AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
   [STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
   BCCA72DD1311"]
   [LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
   [RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
   69]
   [ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
   ```

6. 在审核消息中找到 LOC 字段。

   如果存在，则在 LOM 中的 CLDI 值为节点 ID 和创建对象副本的卷 ID 。此消息显示已应用 ILM ，并且已在网格中的两个位置创建两个对象副本。。在网格管理器中重置丢失对象的计数。

相关信息

调查丢失的对象

重置丢失和缺失的对象计数

查看审核日志

重置丢失和缺失的对象计数

在调查 StorageGRID 系统并验证所有记录的丢失对象是否永久丢失或是否为虚假警报之后，您可以将丢失对象属性的值重置为零。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

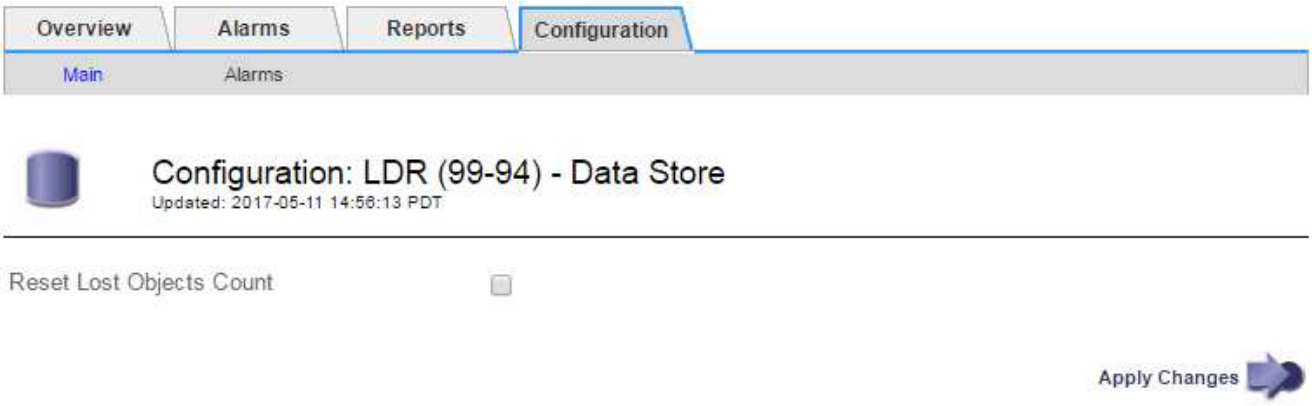
您可以从以下任一页面重置丢失的对象计数器：

- * 支持 * > * 工具 * > * 网格拓扑 * > * 站点 _* > * 存储节点 _* > * LDR* > * 数据存储 * > * 概述 * > * 主 *
- * 支持 * > * 工具 * > * 网格拓扑 * > * 站点 _* > * 存储节点 _* > * DDS* > * 数据存储 * > * 概述 * > * 主 *

以下说明显示了如何从 * LDR* > * 数据存储 * 页面重置计数器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 对于出现 "* 对象丢失 " 警报或 " 丢失 " 警报的存储节点，选择 * 站点 _* > * 存储节点 _* > * * 存储节点 * > * 数据存储 * > * 配置 * 。
3. 选择 * 重置丢失的对象计数 * 。



4. 单击 * 应用更改 * 。

   丢失的对象属性将重置为 0 ，并且 * 对象丢失 * 警报和丢失警报将清除，这可能需要几分钟的时间。

5. 或者，也可以重置在识别丢失的对象过程中可能会递增的其他相关属性值。

   a. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 擦除编码 * > * 配置 * 。
   b. 选择 * 重置读取失败计数 * 和 * 重置检测到的损坏副本计数 * 。
   c. 单击 * 应用更改 * 。
   d. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 验证 * > * 配置 * 。
   e. 选择 * 重置缺少的对象计数 * 和 * 重置损坏的对象计数 * 。
   f. 如果您确信不需要隔离对象，则可以选择 * 删除隔离对象 * 。

      在后台验证发现复制的对象副本损坏时，将创建隔离的对象。在大多数情况下， StorageGRID 会自动替换损坏的对象，并且可以安全地删除隔离的对象。但是，如果触发 * 对象丢失 * 警报或丢失警报，技术支持可能需要访问隔离的对象。

   g. 单击 * 应用更改 * 。

   单击 * 应用更改 * 后，可能需要几分钟时间才能重置属性。

对对象数据存储不足警报进行故障排除

对象数据存储空间 * 不足警报可监控每个存储节点上可用于存储对象数据的空间量。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

如果存储节点上复制和擦除编码的对象数据总量满足警报规则中配置的条件之一，则会触发 * 对象数据存储空间不足 * 警报。

默认情况下，如果此情况评估为 true ，则会触发重大警报：

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

在这种情况下：

- `storagegRid_storage_utilization_data_bytes` 是对存储节点的已复制和擦除编码对象数据总大小的估计值。
- `storagegRid_storage_utilization_usable_space_bytes` 是存储节点剩余的对象存储空间总量。

如果触发主要或次要的 * 对象数据存储空间不足 * 警报，则应尽快执行扩展操作步骤 。

步骤

1. 选择 * 警报 * > * 当前 * 。

   此时将显示警报页面。

2. 如果需要，从警报表中展开 * 对象数据存储空间不足 * 警报组，然后选择要查看的警报。

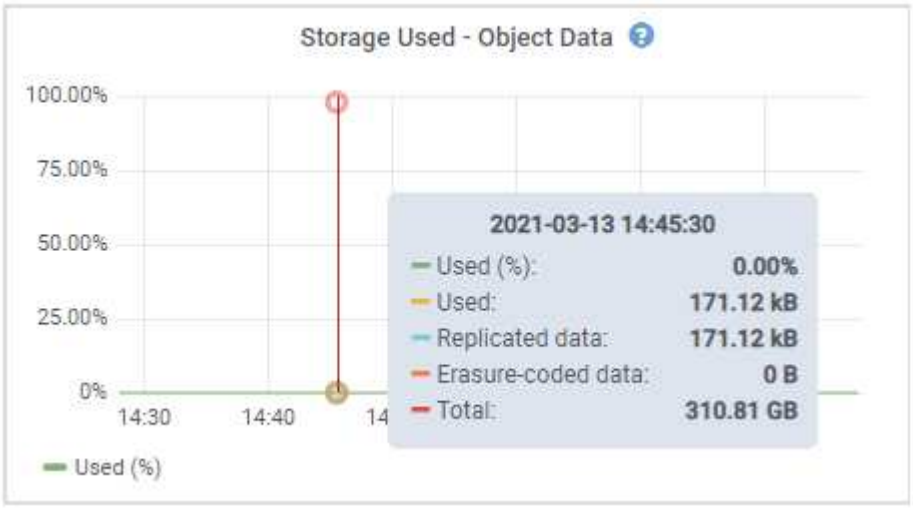
   选择警报，而不是一组警报的标题。

3. 查看对话框中的详细信息，并注意以下事项：
   - 时间已触发
   - 站点和节点的名称
   - 此警报的指标的当前值
4. 选择 * 节点 * > * 存储节点或站点 _* > * 存储 * 。
5. 将光标悬停在 "Storage Used - Object Data" 图上。

   此时将显示以下值：

   - * 已用（ % ） * ： 已用于对象数据的总可用空间的百分比。
   - * 已用 * ： 已用于对象数据的总可用空间量。
   - * 复制数据 * ： 此节点，站点或网格上复制的对象数据量的估计值。
   - * 擦除编码数据 * ： 此节点，站点或网格上经过擦除编码的对象数据量的估计值。

◦ * 总计 * ： 此节点，站点或网格上的可用空间总量。使用的值是 `storagegRid_storage_utilization _data_bytes` 指标。



6. 选择图形上方的时间控件可查看不同时间段的存储使用情况。

   查看一段时间内的存储使用量有助于您了解触发警报前后的存储使用量，并有助于您估计节点的剩余空间可能需要多长时间才能达到全满状态。

7. 请尽快执行扩展操作步骤 以添加存储容量。

   您可以向现有存储节点添加存储卷（ LUN ），也可以添加新的存储节点。

   要管理完整的存储节点，请参见有关管理 StorageGRID 的说明。

相关信息

对存储状态（ SSTS ）警报进行故障排除

扩展网格

管理 StorageGRID

对低只读水印覆盖警报进行故障排除

如果对存储卷水印使用自定义值，则可能需要解决 * 低只读水印覆盖 * 警报。如果可能，您应更新系统以开始使用优化值。

在先前版本中，这三个 存储卷水印 为全局设置 &#8212 ； 应用于每个存储节点上的每个存储卷的值相同。从 StorageGRID 11.6 开始，软件可以根据存储节点的大小和卷的相对容量为每个存储卷优化这些水印。

升级到 StorageGRID 11.6 时，经过优化的只读和读写水印会自动应用于所有存储卷，除非满足以下条件之一：

- 您的系统容量已接近，如果应用了优化的水印，则无法接受新数据。在这种情况下， StorageGRID 不会更改水印设置。
- 您先前已将任何存储卷水印设置为自定义值。StorageGRID 不会使用优化值覆盖自定义水印设置。但是，如果您对存储卷软只读水印的自定义值太小，则 StorageGRID 可能会触发 * 低只读水印覆盖 * 警报。

了解警报

如果对存储卷水印使用自定义值，则可能会为一个或多个存储节点触发 * 低只读水印覆盖 * 警报。

每个警报实例都指示 * 存储卷软只读水印 * 的自定义值小于该存储节点的最小优化值。如果您继续使用自定义设置，则存储节点可能会在空间严重不足的情况下运行，然后才能安全地过渡到只读状态。当节点达到容量时，某些存储卷可能无法访问（自动卸载）。

例如，假设您先前已将 * 存储卷软只读水印 * 设置为 5 GB 。现在，假设 StorageGRID 已为存储节点 A 中的四个存储卷计算出以下优化值：

卷 0	12 GB
卷 1	12 GB
第 2 卷	11 GB
第 3 卷	15 GB

为存储节点 A 触发 * 低只读水印覆盖 * 警报，因为您的自定义水印（ 5 GB ）小于该节点中所有卷的最小优化值（ 11 GB ）。如果继续使用自定义设置，则节点可能会在空间严重不足的情况下运行，然后才能安全过渡到只读状态。

解决警报

如果触发了一个或多个 * 低只读水印覆盖 * 警报，请执行以下步骤。如果您当前正在使用自定义水印设置，并且希望开始使用优化设置，即使未触发任何警报，也可以使用这些说明。

您需要的内容

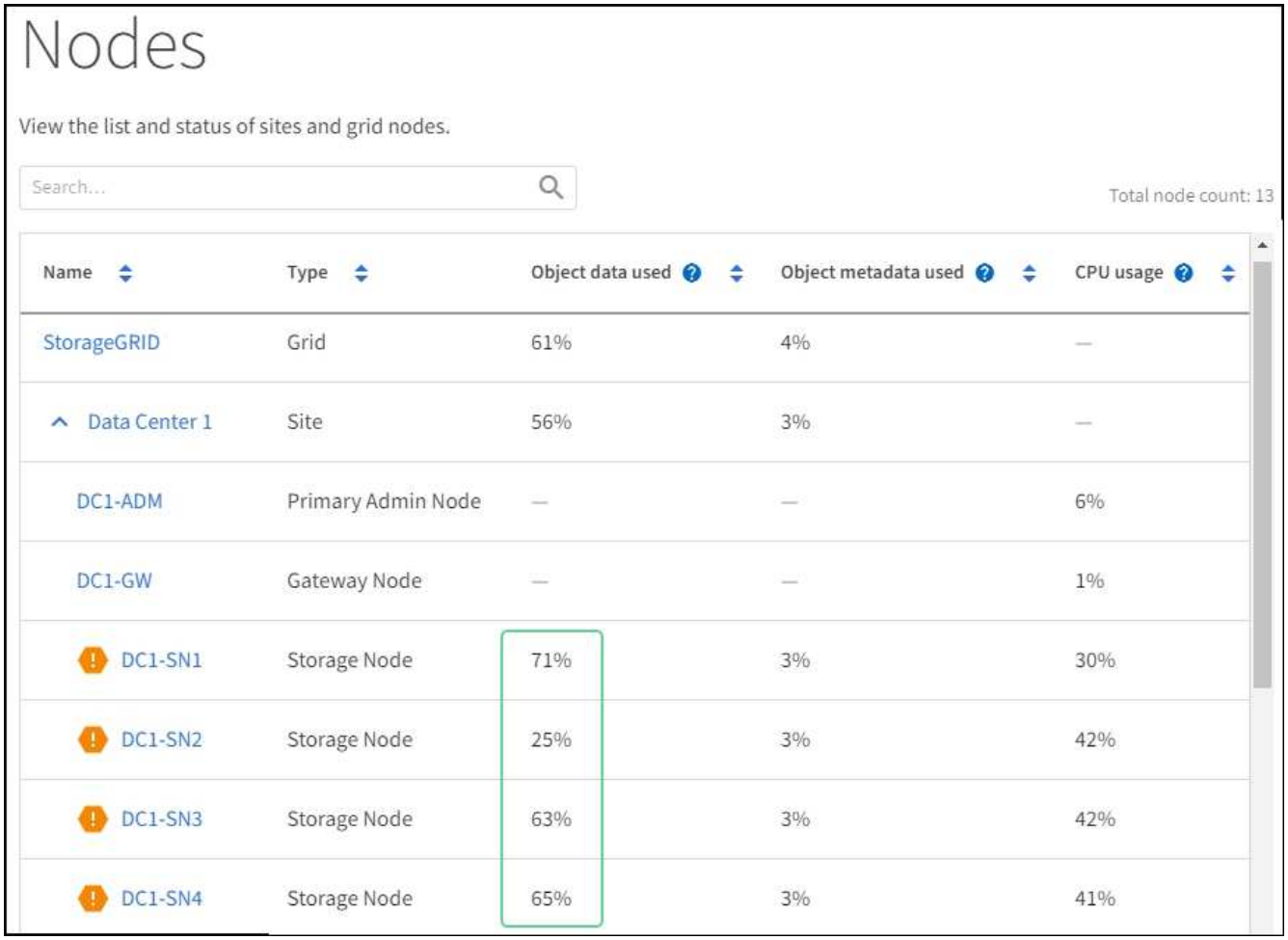
- 您已完成 StorageGRID 11.6 的升级。
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有 root 访问权限。

关于此任务

您可以通过将自定义水印设置更新为新的水印覆盖来解决 * 低只读水印覆盖 * 警报。但是，如果一个或多个存储节点接近全满或您有特殊的 ILM 要求，则应首先查看优化的存储水印并确定使用它们是否安全。

评估整个网格的对象数据使用情况

1. 选择 * 节点 * 。
2. 对于网格中的每个站点，展开节点列表。
3. 查看每个站点的每个存储节点的 * 对象数据已用 * 列中显示的百分比值。



4. 如果所有存储节点均未接近全满（例如，所有 * 已使用的对象数据 * 值均小于 80% ），则可以开始使用覆盖设置。转至 [使用优化的水印]。

> 此一般规则存在一些例外情况。例如，如果 ILM 规则使用严格的载入行为或特定存储池接近全满，则应首先执行中的步骤 [查看优化的存储水印] 和 [确定是否可以使用优化的水印]。

5. 如果还有一个存储节点接近全满，请执行中的步骤 [查看优化的存储水印] 和 [确定是否可以使用优化的水印]。

查看优化的存储水印

StorageGRID 使用两个 Prometheus 指标来显示它为 * 存储卷软只读水印 * 计算的优化值。您可以查看网格中每个存储节点的最小和最大优化值。

1. 选择 * 支持 * > * 工具 * > * 指标 * 。
2. 在 Prometheus 部分中，选择用于访问 Prometheus 用户界面的链接。
3. 要查看建议的最小软只读水印，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegRid_storage_volume_minimum_optimized_soft_readonly_slogm
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最小优化值。如果此值大于 * 存储卷软只读水印 * 的自定义设置，则会为存储节点触发 * 低只读水印覆盖 * 警报。

4. 要查看建议的最大软只读水印数，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegRid_storage_volume_max_optimized_soft_readonly_slogm
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

5. 【最大优化值】记下每个存储节点的最大优化值。

确定是否可以使用优化的水印

1. 选择 * 节点 * 。
2. 对每个联机存储节点重复上述步骤：
   a. 选择 * 存储节点 _* > * 存储 * 。
   b. 向下滚动到对象存储表。
   c. 将每个对象存储（卷）的 * 可用 * 值与您为该存储节点记下的最大优化水印进行比较。
3. 如果每个联机存储节点上至少有一个卷的可用空间超过该节点的最大优化水印容量，请转至 [使用优化的水印] 开始使用经过优化的水印。

   否则， 扩展网格 请尽快。向现有节点添加存储卷或添加新的存储节点。然后，转到 [使用优化的水印] 更新水印设置。

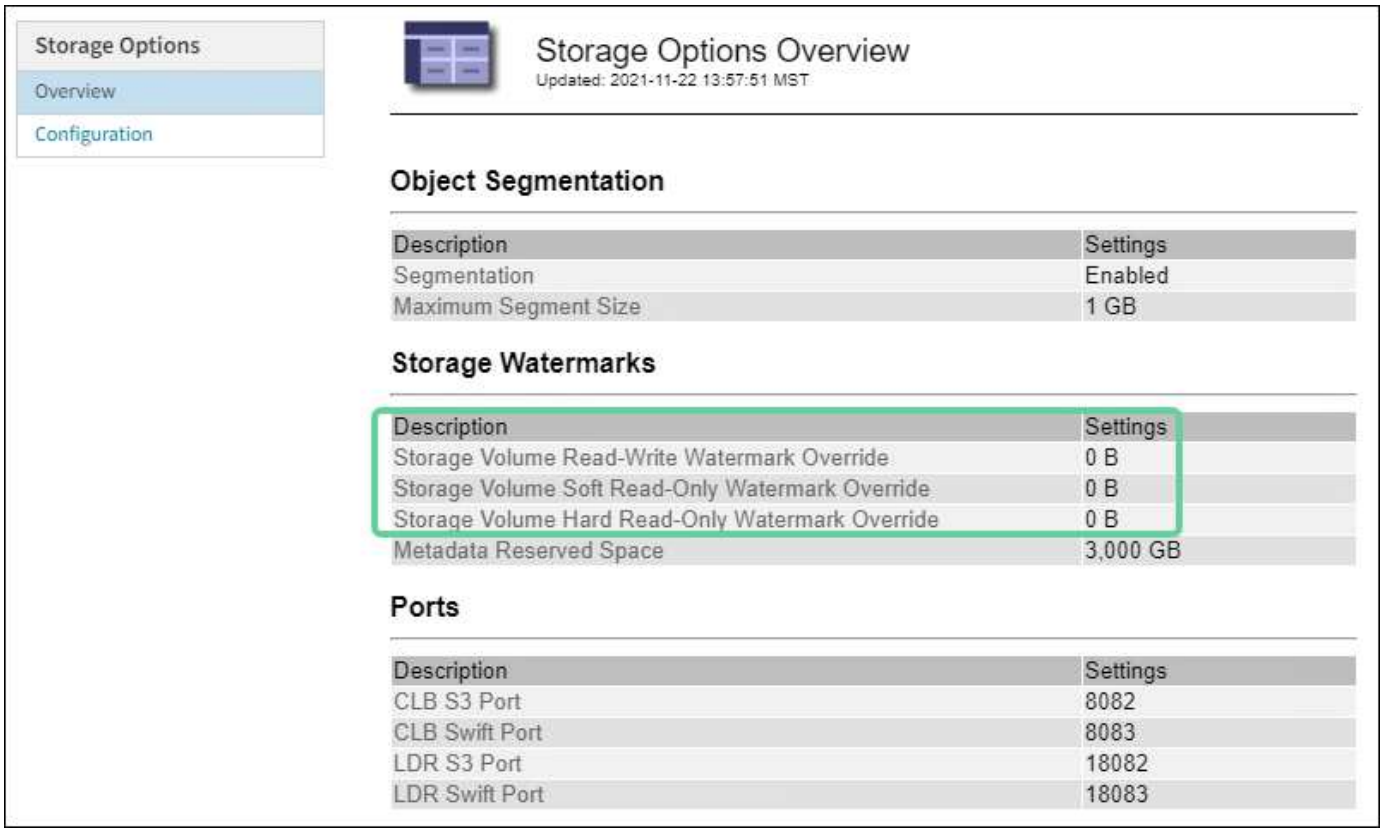
4. 如果需要继续对存储卷水印使用自定义值， 静默 或 -disable * 低只读水印覆盖 * 警报。

   相同的自定义水印值将应用于每个存储节点上的每个存储卷。对存储卷水印使用小于建议值可能发生原因 会导致某些存储卷在节点达到容量时无法访问（自动卸载）。

使用优化的水印

1. 转至 * 配置 * > * 系统 * > * 存储选项 * 。
2. 从存储选项菜单中选择 * 配置 * 。
3. 将所有三个 " 水印覆盖 " 更改为 0 。
4. 选择 * 应用更改 * 。

现在，根据存储节点的大小和卷的相对容量，优化的存储卷水印设置将对每个存储卷生效。



对存储状态（ **SSTS** ）警报进行故障排除

如果存储节点的对象存储剩余可用空间不足，则会触发存储状态（ SSTS ）警报。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。

关于此任务

当存储节点中每个卷上的可用空间量降至存储卷软只读水印（ * 配置 * > * 系统 * > * 存储选项 * ）的值以下时，SSTS （存储状态）警报将在通知级别触发。

Storage Options Overview
Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

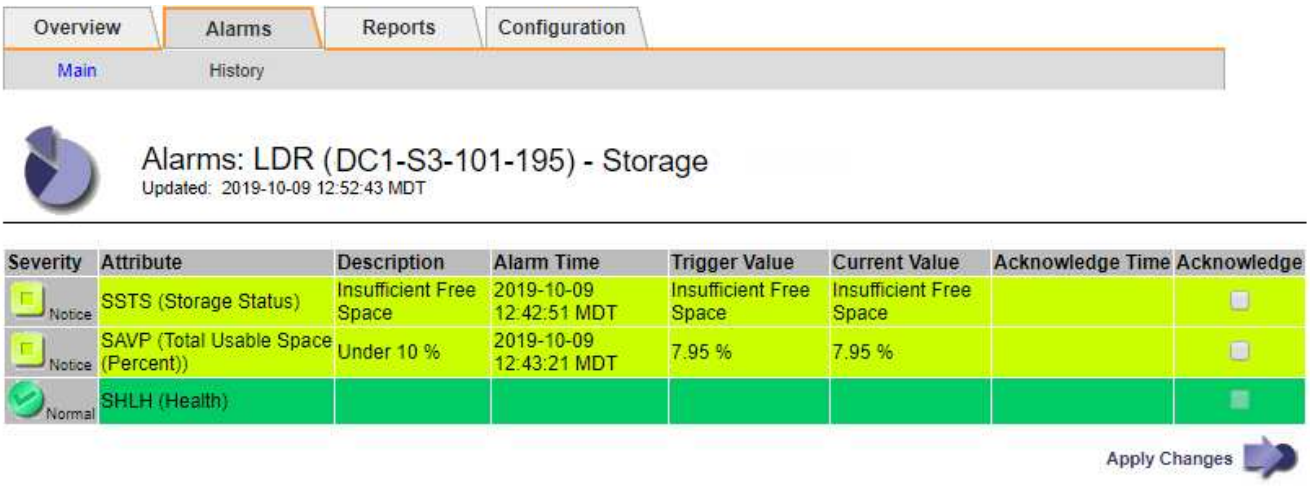
例如，假设存储卷软只读水印设置为 10 GB ，这是其默认值。如果存储节点中的每个存储卷上的可用空间不足 10 GB ，则会触发 SSTS 警报。如果任何卷具有 10 GB 或更大的可用空间，则不会触发警报。

如果已触发 SSTS 警报，您可以按照以下步骤更好地了解问题描述 。

步骤

1. 选择 * 支持 * > * 警报（原有） * > * 当前警报 * 。
2. 从服务列中，选择与 SSTS 警报关联的数据中心，节点和服务。

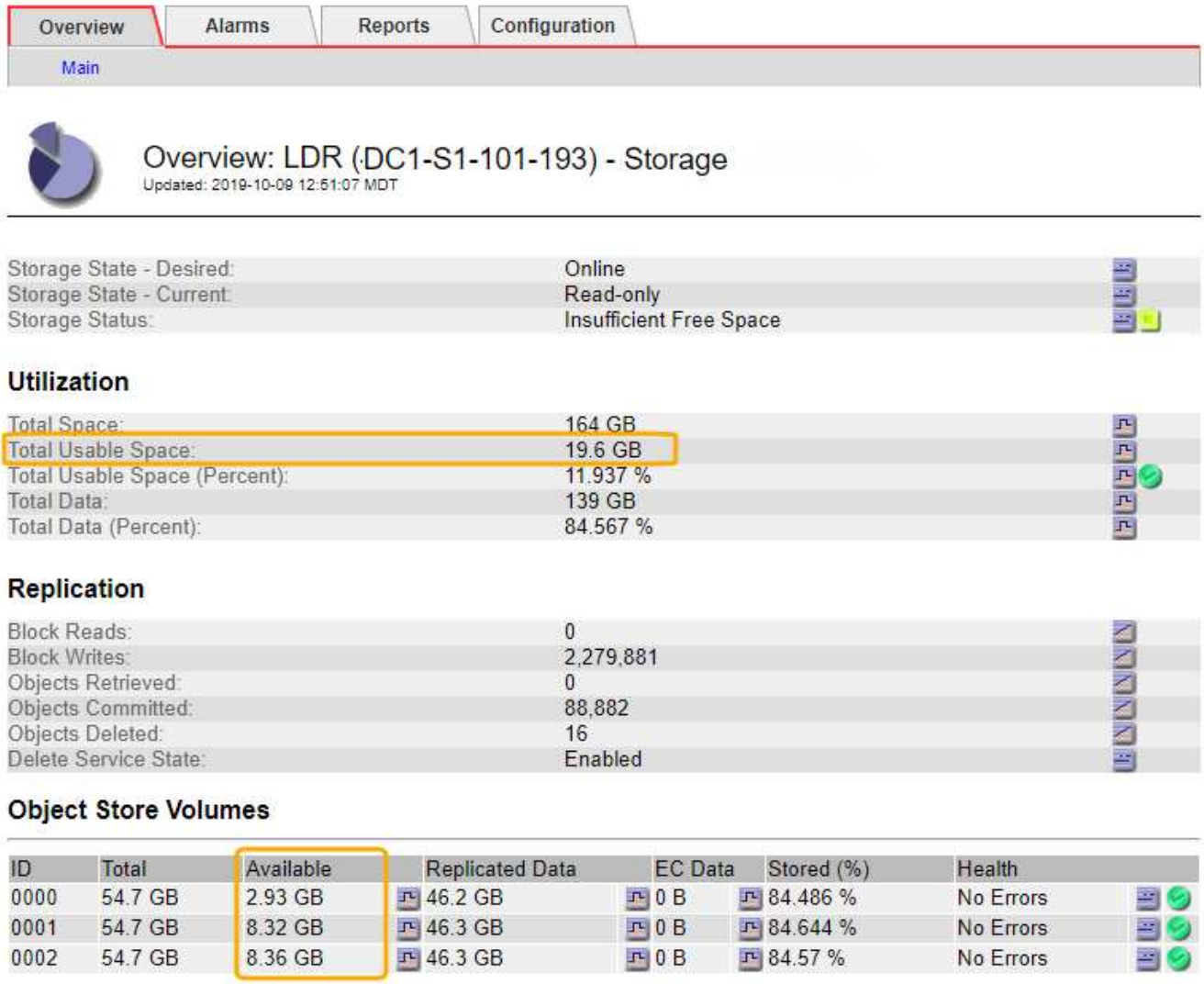
   此时将显示网格拓扑页面。警报选项卡显示选定节点和服务的活动警报。



   在此示例中，已在通知级别触发 SSTS （存储状态）和 SAVP （总可用空间（百分比））警报。

   通常， SSTS 警报和 SAVP 警报会同时触发；但是，是否同时触发这两个警报取决于以 GB 为单位的水印设置和以百分比表示的 SAVP 警报设置。

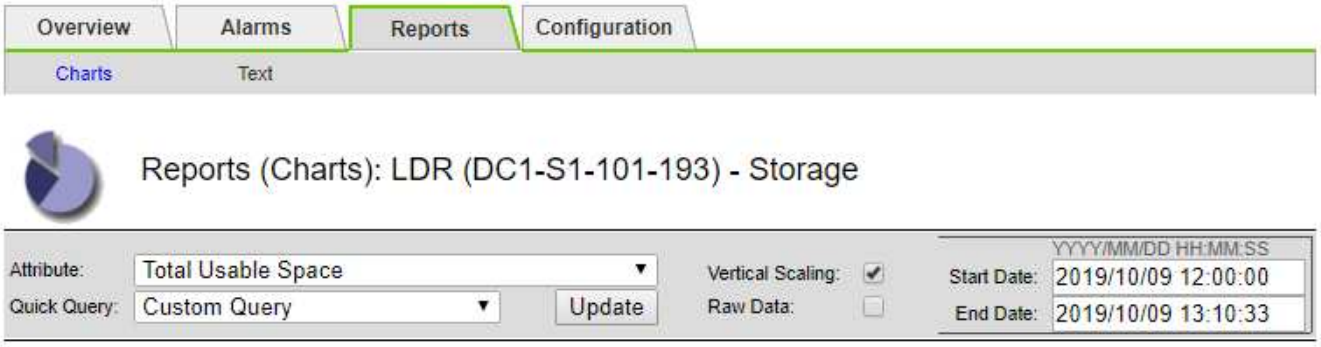
3. 要确定实际可用空间量，请选择 * LDR* > * 存储 * > * 概述 * ，然后找到总可用空间（ STAMP ）属性。

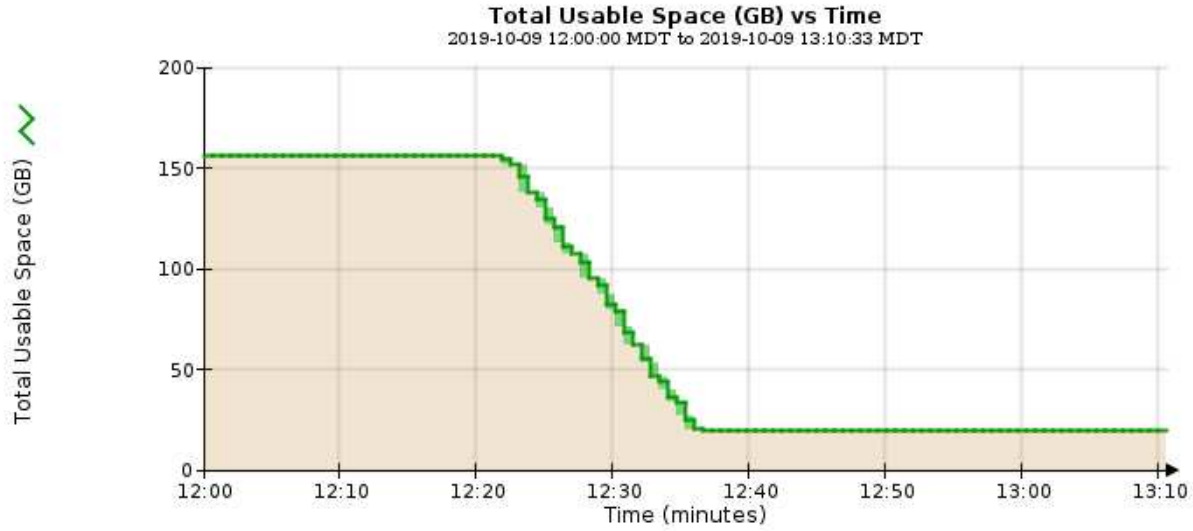


在此示例中，此存储节点上 164 GB 空间中只有 19.6 GB 可用。请注意，总计值是三个对象存储卷的 * 可用 * 值之和。之所以触发 SSTS 警报，是因为这三个存储卷中的每个卷的可用空间均小于 10 GB 。

4. 要了解存储在一段时间内的使用情况，请选择 * 报告 * 选项卡，然后绘制过去几小时的总可用空间。

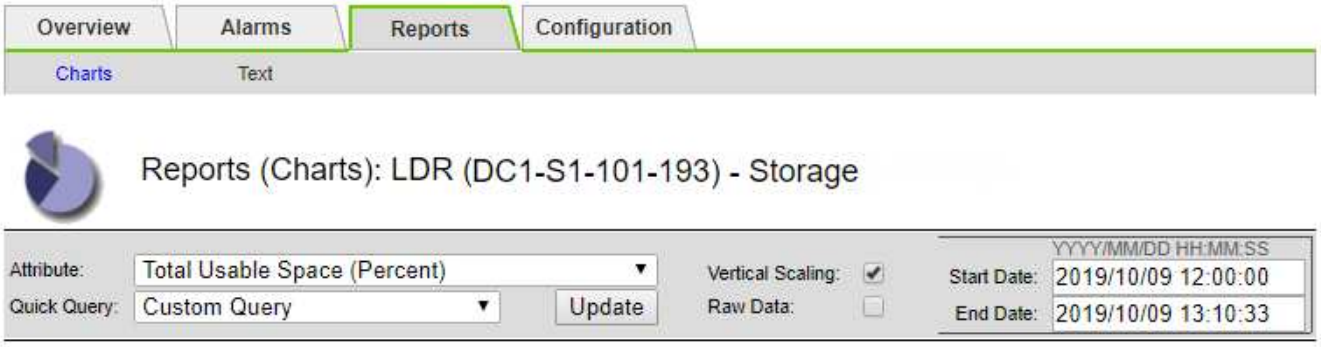
   在此示例中，总可用空间从 12： 00 处的大约 155 GB 降至 12： 35 处的 20 GB ，这与触发 SSTS 警报的时间相对应。

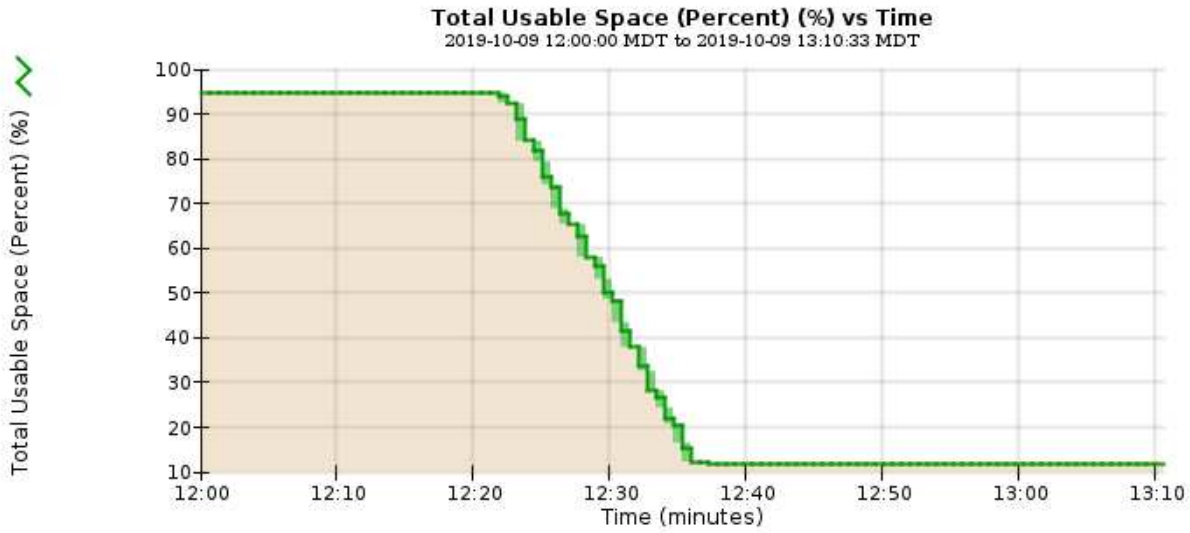




5. 要了解存储的使用情况占总空间的百分比，请绘制过去几小时的总可用空间（百分比）。

   在此示例中，总可用空间大约同时从 95% 下降到 10% 以上。





6. 根据需要添加存储容量 扩展 StorageGRID 系统。

   有关如何管理完整存储节点的过程，请参见 有关管理 StorageGRID 的说明。

对平台服务消息的传送进行故障排除（ **SMTTT** 警报）

如果平台服务消息传送到无法接受数据的目标，则会在网格管理器中触发总事件（ SMT ）警报。

关于此任务

例如，即使无法将关联的复制或通知消息传送到已配置的端点， S3 多部分上传也可以成功。或者，如果元数据过长，则可能无法传送有关 CloudMirror 复制的消息。

SMT 警报包含最后一条事件消息，其中显示： `failed to publish notifications for bucket-name object key` for the last object whose notification failed.

事件消息也会列在 ` /var/local/log/byncast-err.log` 日志文件中。请参见 日志文件参考。

有关追加信息 对平台服务进行故障排除的信息，请参见 有关管理 StorageGRID 的说明。您可能需要 从租户管理器访问租户 调试平台服务错误。

步骤

1. 要查看警报，请选择 * 节点 * > * 站点 _* > * 网格节点 _* > * 事件 * 。

2. 在表顶部查看上次事件。

   事件消息也会在 ` /var/local/log/byncast-err.log` 中列出。

3. 按照 SMT 警报内容中提供的指导更正问题描述 。
4. 选择 * 重置事件计数 * 。
5. 将尚未传送平台服务消息的对象通知租户。
6. 指示租户通过更新对象的元数据或标记来触发失败的复制或通知。

对元数据问题进行故障排除

您可以执行多项任务来帮助确定元数据问题的根源。

对 " 低元数据存储 " 警报进行故障排除

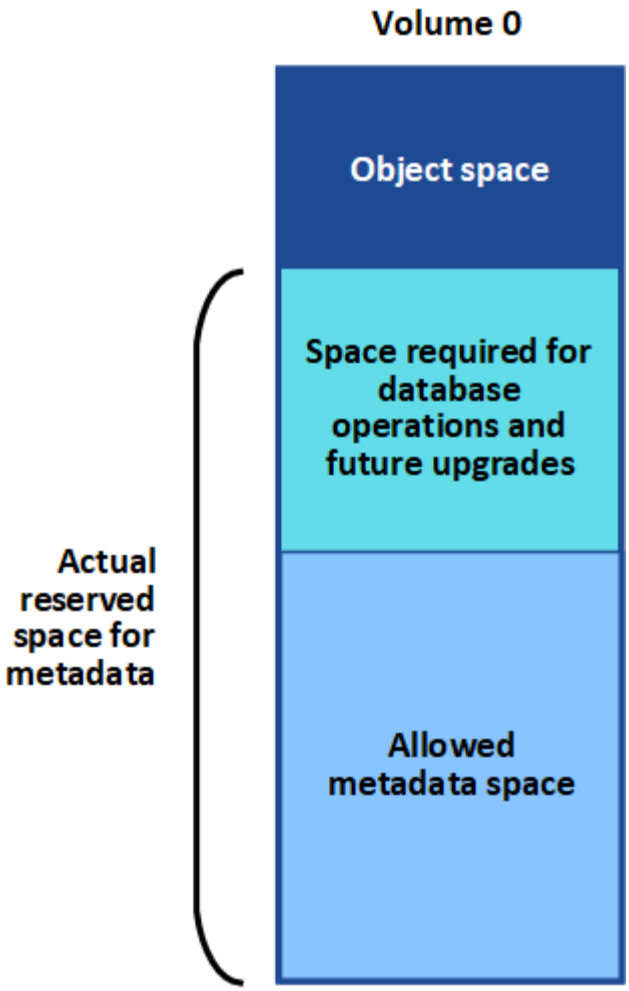
如果触发 * 低元数据存储 * 警报，则必须添加新的存储节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

StorageGRID 会在每个存储节点的卷 0 上为对象元数据预留一定数量的空间。此空间称为实际预留空间，并细分为对象元数据允许的空间（允许的元数据空间）以及数据缩减和修复等基本数据库操作所需的空间。允许的元数据空间用于控制整体对象容量。



如果对象元数据占用的空间超过元数据允许的 100% ，则数据库操作将无法高效运行，并会发生错误。

您可以 监控每个存储节点的对象元数据容量 帮助您预测错误并在发生错误之前予以更正。

StorageGRID 使用以下 Prometheus 指标来衡量允许的元数据空间的容量：

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

当此 Prometheus 表达式达到特定阈值时，将触发 * 低元数据存储 * 警报。

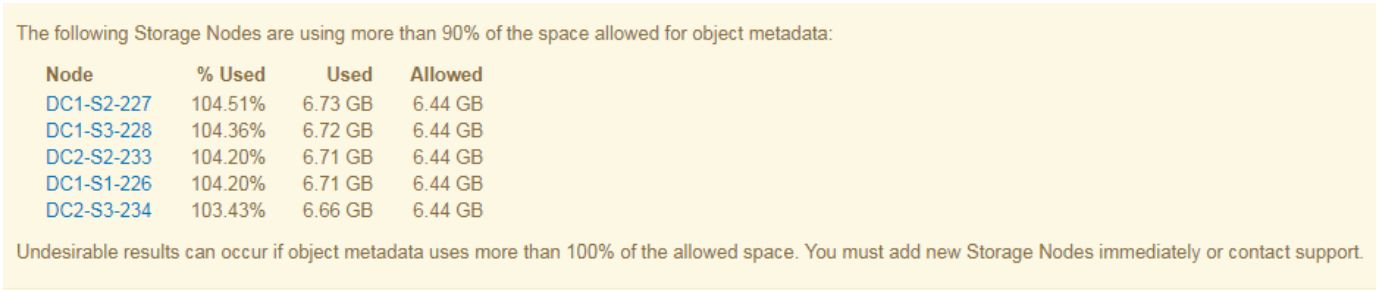
- * 次要 * ： 对象元数据正在使用允许的元数据空间的 70% 或更多。您应尽快添加新的存储节点。
- * 主要 * ： 对象元数据正在使用允许的元数据空间的 90% 或更多。您必须立即添加新的存储节点。

> 当对象元数据使用 90% 或更多的允许元数据空间时，信息板上会显示一条警告。如果显示此警告，则必须立即添加新的存储节点。绝不能允许对象元数据使用超过允许空间的 100% 。

- * 严重 * ： 对象元数据正在使用 100% 或更多的允许元数据空间，并且开始占用基本数据库操作所需的空间。您必须停止载入新对象，并且必须立即添加新的存储节点。

在以下示例中，对象元数据使用的元数据空间超过允许的 100% 。这是一种严重情况，会导致数据库运行效率

低下和出现错误。



如果卷 0 的大小小于元数据预留空间存储选项（例如，在非生产环境中），则计算 * 低元数据存储 * 警报可能不准确。

步骤

1. 选择 * 警报 * > * 当前 * 。
2. 如果需要，从警报表中展开 * 低元数据存储 * 警报组，然后选择要查看的特定警报。
3. 查看警报对话框中的详细信息。
4. 如果触发了主要或关键的 * 低元数据存储 * 警报，请执行扩展以立即添加存储节点。

由于 StorageGRID 会在每个站点保留所有对象元数据的完整副本，因此整个网格的元数据容量受最小站点的元数据容量限制。如果需要向一个站点添加元数据容量，则还应添加元数据容量 扩展任何其他站点 相同数量的存储节点。

执行扩展后， StorageGRID 会将现有对象元数据重新分发到新节点，从而增加网格的整体元数据容量。无需用户操作。已清除 * 低元数据存储 * 警报。

对服务进行故障排除：状态 - **Cassandra** （ **SVST** ）警报进行故障排除

服务：状态 - Cassandra （ SVST ）警报指示您可能需要为存储节点重建 Cassandra 数据库。Cassandra 用作 StorageGRID 的元数据存储。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。

关于此任务

如果 Cassandra 停止超过 15 天（例如，存储节点已关闭），则在节点恢复联机后， Cassandra 将无法启动。您必须为受影响的 DDS 服务重建 Cassandra 数据库。

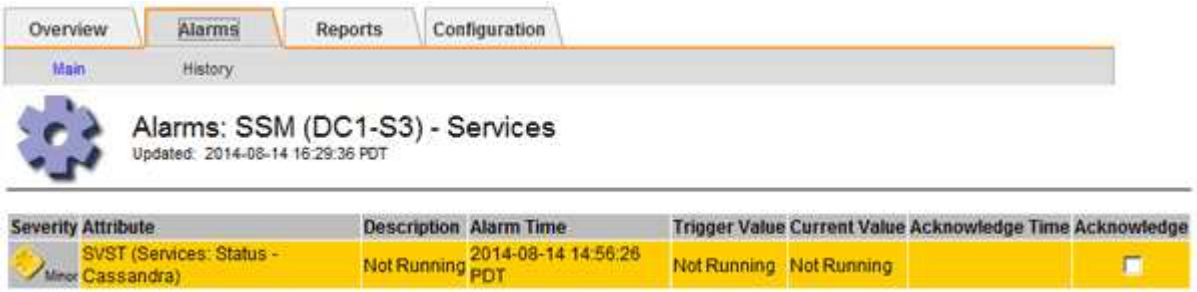
您可以 运行诊断 获取网格当前状态的追加信息 。

如果两个或多个 Cassandra 数据库服务关闭超过 15 天，请联系技术支持，不要继续执行以下步骤。

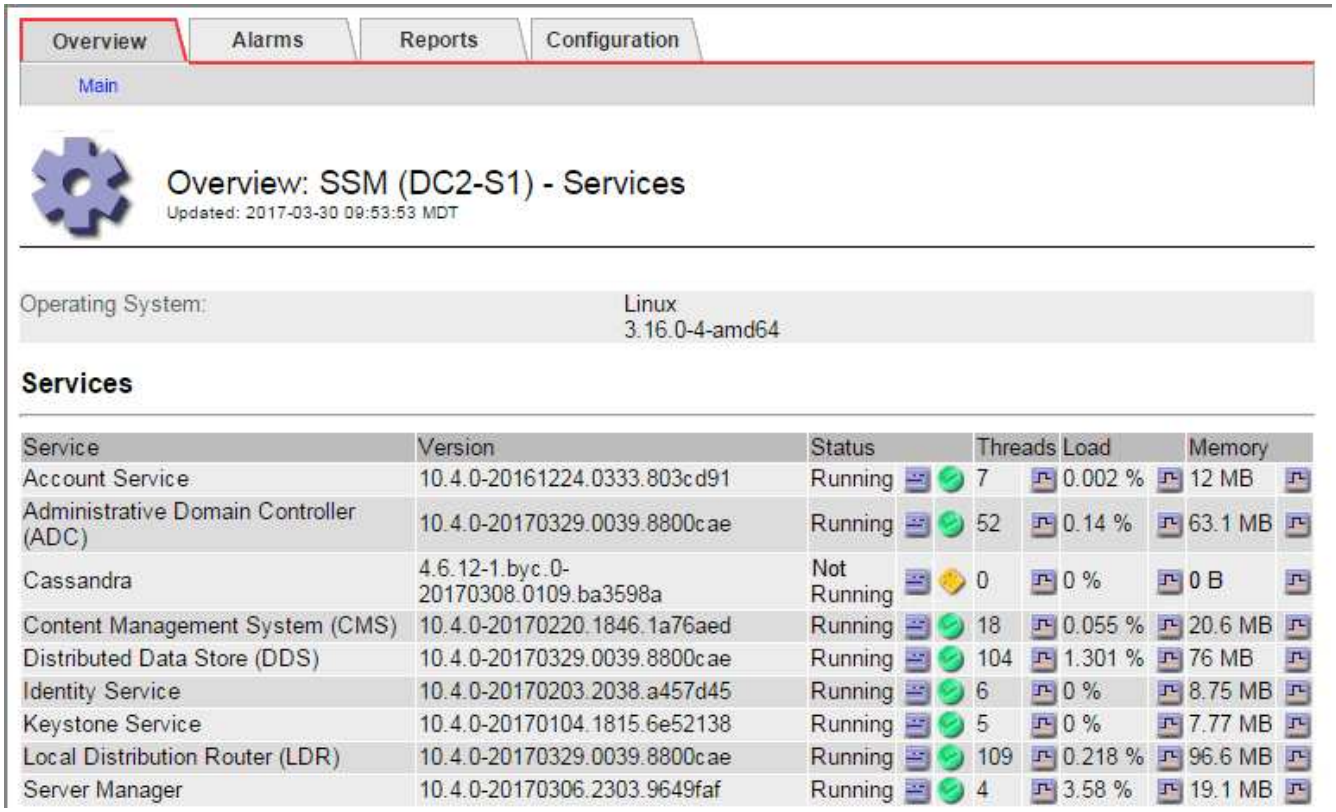
步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* > * SSM* > * 服务 * > * 警报 * > * 主 * 以显示警报。

   此示例显示已触发 SVST 警报。



   "SSM 服务主页 " 页面还指示 Cassandra 未运行。



3. 【重新启动 Cassandra_from_the_Storage_Node ， start=3]] 尝试从存储节点重新启动 Cassandra ：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_ip`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root ： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
   b. 输入： ` /etc/init.d/Cassandra status`
   c. 如果 Cassandra 未运行，请重新启动它： ` /etc/init.d/Cassandra restart`

4. 如果 Cassandra 未重新启动，请确定 Cassandra 已关闭多长时间。如果 Cassandra 已关闭超过 15 天，则必须重建 Cassandra 数据库。

   如果两个或更多 Cassandra 数据库服务已关闭，请联系技术支持，不要继续执行以下步骤。

   您可以通过绘制 Cassandra 图表或查看 servermanager.log 文件来确定 Cassandra 已关闭多长时间。

5. 绘制 Cassandra 图表：

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 存储节点 _* > * SSM* > * 服务 * > * 报告 * > * 图表 * 。

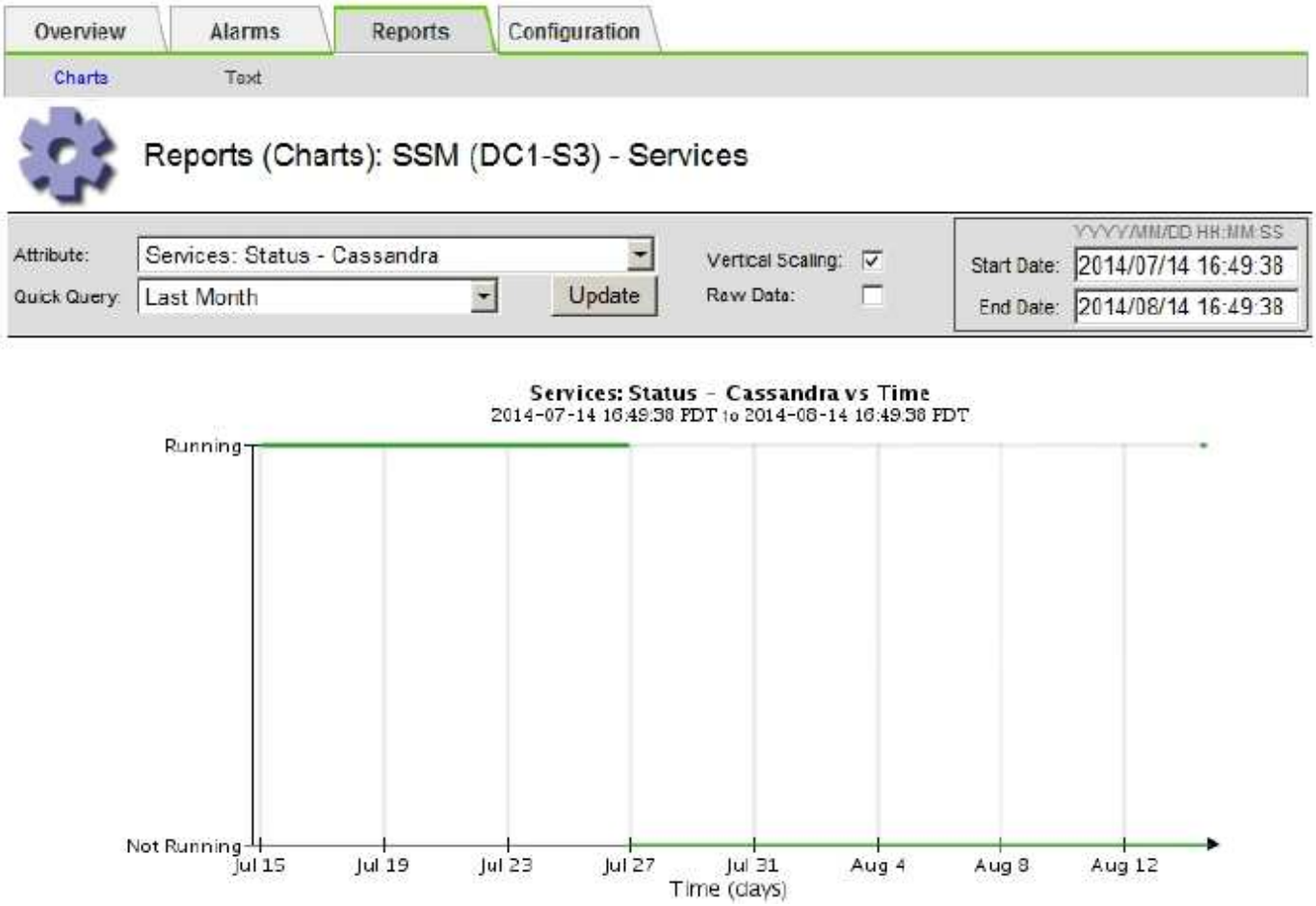
   b. 选择 * 属性 * > * 服务：状态 - Cassandra* 。

   c. 对于 * 开始日期 * ，请输入至少早于当前日期 16 天的日期。对于 * 结束日期 * ，输入当前日期。

   d. 单击 * 更新 * 。

   e. 如果图表显示 Cassandra 关闭超过 15 天，请重建 Cassandra 数据库。

以下图表示例显示 Cassandra 已关闭至少 17 天。



1. 查看存储节点上的 servermanager.log 文件：

   a. 登录到网格节点：

      i. 输入以下命令： `ssh admin@grid_node_ip`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

b. 输入： `cat /var/local/log/servermanager.log`

此时将显示 servermanager.log 文件的内容。

如果 Cassandra 已关闭超过 15 天，则 servermanager.log 文件中将显示以下消息：

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

a. 确保此消息的时间戳是您按照步骤中的说明尝试重新启动 Cassandra 的时间 从存储节点重新启动 Cassandra。

Cassandra 可以有多个条目；您必须找到最新的条目。

b. 如果 Cassandra 已关闭超过 15 天，则必须重建 Cassandra 数据库。

有关说明，请参见 将存储节点恢复到关闭状态超过 15 天。

c. 如果重建 Cassandra 后无法清除警报，请联系技术支持。

对 **Cassandra** 内存不足错误（ **SMTTT** 警报）进行故障排除

如果 Cassandra 数据库出现内存不足错误，则会触发总计事件（ SMT ）警报。如果发生此错误，请联系技术支持以使用问题描述 。

关于此任务

如果 Cassandra 数据库发生内存不足错误，则会创建堆转储，触发总事件（ SMT ）警报， Cassandra 堆内存不足错误计数将增加 1 。

步骤

1. 要查看事件，请选择 * 支持 * > * 工具 * > * 网格拓扑 * > * 配置 * 。
2. 验证 Cassandra 堆内存不足错误计数是否为 1 或更高。

   您可以 运行诊断 获取网格当前状态的追加信息 。
3. 转至 ` /var/local/core/` ，压缩 `Cassandra.hprof` 文件，然后将其发送给技术支持。
4. 备份 `Cassandra.hprof` 文件，然后将其从 ` /var/local/core/ 目录` 中删除。

   此文件最大可达 24 GB ，因此您应将其删除以释放空间。
5. 解决问题描述 后，选中 Cassandra 堆内存不足错误计数的 * 重置 * 复选框。然后选择 * 应用更改 * 。

要重置事件计数，您必须具有网格拓扑页面配置权限。

对证书错误进行故障排除

如果您在尝试使用 Web 浏览器， S3 或 Swift 客户端或外部监控工具连接到 StorageGRID 时看到安全或证书问题描述 ，则应检查此证书。

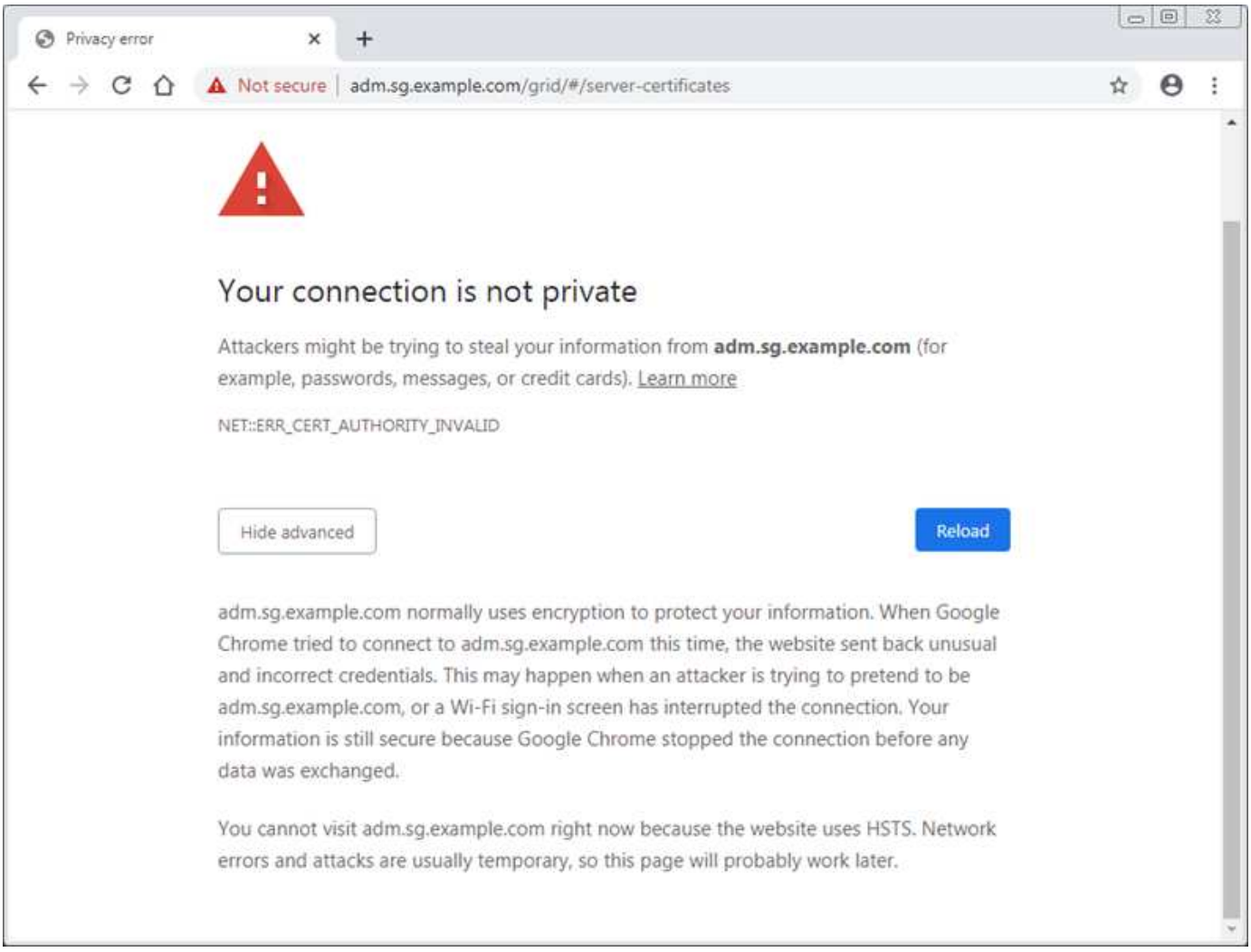
关于此任务

尝试使用网格管理器，网格管理 API ，租户管理器或租户管理 API 连接到 StorageGRID 时，证书错误可能会出现发生原因 问题。尝试连接到 S3 或 Swift 客户端或外部监控工具时，也可能发生证书错误。

如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：

- 您的自定义管理接口证书将过期。
- 您可以从自定义管理接口证书还原到默认服务器证书。

以下示例显示了自定义管理接口证书过期时的证书错误：



为了确保操作不会因服务器证书失败而中断，当服务器证书即将过期时，将触发 * 管理接口的服务器证书到期 *

警报。

在使用客户端证书进行外部 Prometheus 集成时，证书错误可能是由 StorageGRID 管理接口证书或客户端证书引起的。当客户端证书即将过期时，将触发 " 证书 " 页面上配置的 * 客户端证书到期 * 警报。

步骤

如果您收到有关证书已过期的警报通知，请访问证书详细信息：。选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 选择相应的证书选项卡。

1. 检查证书的有效期。+ 某些 Web 浏览器以及 S3 或 Swift 客户端不接受有效期超过 398 天的证书。
2. 如果证书已过期或即将过期，请上传或生成新证书。
   - 有关服务器证书，请参见的步骤 为网格管理器和租户管理器配置自定义服务器证书。
   - 有关客户端证书，请参见的步骤 配置客户端证书。
3. 对于服务器证书错误，请尝试以下任一或两个选项：
   - 确保已填充证书的使用者备用名称（ SAN ），并且 SAN 与要连接到的节点的 IP 地址或主机名匹配。
   - 如果您尝试使用域名连接到 StorageGRID ：
     i. 输入管理节点的 IP 地址，而不是域名，以绕过连接错误并访问网格管理器。
     ii. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 选择相应的证书选项卡 安装新的自定义证书或继续使用默认证书。
     iii. 在管理 StorageGRID 的说明中，请参见的步骤 为网格管理器和租户管理器配置自定义服务器证书。

对管理节点和用户界面问题进行故障排除

您可以执行多项任务来帮助确定与管理节点和 StorageGRID 用户界面相关的问题的根源。

对登录错误进行故障排除

如果您在登录到 StorageGRID 管理节点时遇到错误，则您的系统可能具有身份联合配置的问题描述 ，网络或硬件问题，具有管理节点服务的问题描述 或连接的存储节点上具有 Cassandra 数据库的问题描述 。

您需要的内容

- 您必须具有 `passwords.txt` 文件。
- 您必须具有特定的访问权限。

关于此任务

如果在尝试登录到管理节点时看到以下任何错误消息，请遵循以下故障排除准则：

- 您的此帐户凭据无效。请重试。
- 正在等待服务启动 ...
- 内部服务器错误。服务器遇到错误，无法完成您的请求。请重试。如果问题仍然存在，请联系技术支持。
- 无法与服务器通信。正在重新加载页面 ...

步骤

1. 等待 10 分钟，然后重新尝试登录。

如果此错误未自动解决，请转至下一步。

2. 如果您的 StorageGRID 系统具有多个管理节点，请尝试从另一个管理节点登录到网格管理器。
   - 如果您能够登录，则可以使用 * 信息板 * ， * 节点 * ， * 警报 * 和 * 支持 * 选项来帮助确定错误的发生原因 。
   - 如果只有一个管理节点，或者您仍然无法登录，请转至下一步。
3. 确定节点的硬件是否脱机。
4. 如果为 StorageGRID 系统启用了单点登录（ SSO ），请参见 StorageGRID 管理说明中的配置单点登录步骤。

   要解决任何问题，您可能需要暂时禁用并重新启用单个管理节点的 SSO 。

   > 如果启用了 SSO ，则无法使用受限端口登录。必须使用端口 443 。

5. 确定您正在使用的帐户是否属于联合用户。

   如果此联合用户帐户不起作用，请尝试以本地用户（例如 root ）身份登录到网格管理器。

   - 如果本地用户可以登录：
     i. 查看显示的任何警报。
     ii. 选择 * 配置 * > * 访问控制 * > * 身份联合 * 。
     iii. 单击 * 测试连接 * 以验证 LDAP 服务器的连接设置。
     iv. 如果测试失败，请解决任何配置错误。
   - 如果本地用户无法登录，并且您确信凭据正确无误，请转至下一步。
6. 使用安全 Shell （ ssh ）登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
7. 查看网格节点上运行的所有服务的状态： `storagegRid-status`

   确保 NMS ， Mi ， nginx 和 mgmt API 服务均已运行。

   如果服务状态发生变化，输出将立即更新。

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. 确认 nginx gw 服务正在运行 ` # service nginx gw status`
9. 【使用 _lumberjack_to_collect_logs ， start=9]] 使用 lumberjack 收集日志： ` # /usr/local/sbin/lumberjack.rb`

   如果身份验证在过去失败，您可以使用 -start 和 -end Lumberjack 脚本选项指定适当的时间范围。有关这些选项的详细信息，请使用 lumberjack -h 。

   终端的输出指示日志归档的复制位置。

10. 【 review_logs ， start=10]] 查看以下日志：
    - ` /var/local/log/byncast.log`
    - ` /var/local/log/byncast-err.log`
    - ` /var/local/log/NMS.log`

◦ ` //* 命令 .txt`

11. 如果您无法确定管理节点存在任何问题问题描述，请执行以下任一命令来确定在您的站点上运行此 ADA 服务的三个存储节点的 IP 地址。通常，这些存储节点是站点上安装的前三个存储节点。

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

管理节点会在身份验证过程中使用此 ADC 服务。

12. 从管理节点中，使用您确定的 IP 地址登录到每个 ADC 存储节点。
    a. 输入以下命令： `ssh admin@grid_node_ip`
    b. 输入 `passwords.txt` 文件中列出的密码。
    c. 输入以下命令切换到 root： `su -`
    d. 输入 `passwords.txt` 文件中列出的密码。

    以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

13. 查看网格节点上运行的所有服务的状态： `storagegRid-status`

    确保 idnt ， Acct ， nginx 和 Cassandra 服务均已运行。

14. 重复步骤 使用 Lumberjack 收集日志 和 查看日志 查看存储节点上的日志。
15. If you are unable to resolve the issue, contact technical support.

    将收集的日志提供给技术支持。另请参见 日志文件参考。

对用户界面问题进行故障排除

升级到新版本的 StorageGRID 软件后，您可能会看到网格管理器或租户管理器出现问题。

Web 界面未按预期响应

升级 StorageGRID 软件后，网格管理器或租户管理器可能无法按预期做出响应。

如果您在使用 Web 界面时遇到问题：

- 确保您使用的是 支持的 Web 浏览器。

  StorageGRID 11.5 的浏览器支持已更改。确认您使用的是受支持的版本。

- 清除 Web 浏览器缓存。

  清除缓存将删除先前版本的 StorageGRID 软件所使用的过时资源，并允许用户界面再次正常运行。有关说明，请参见 Web 浏览器的文档。

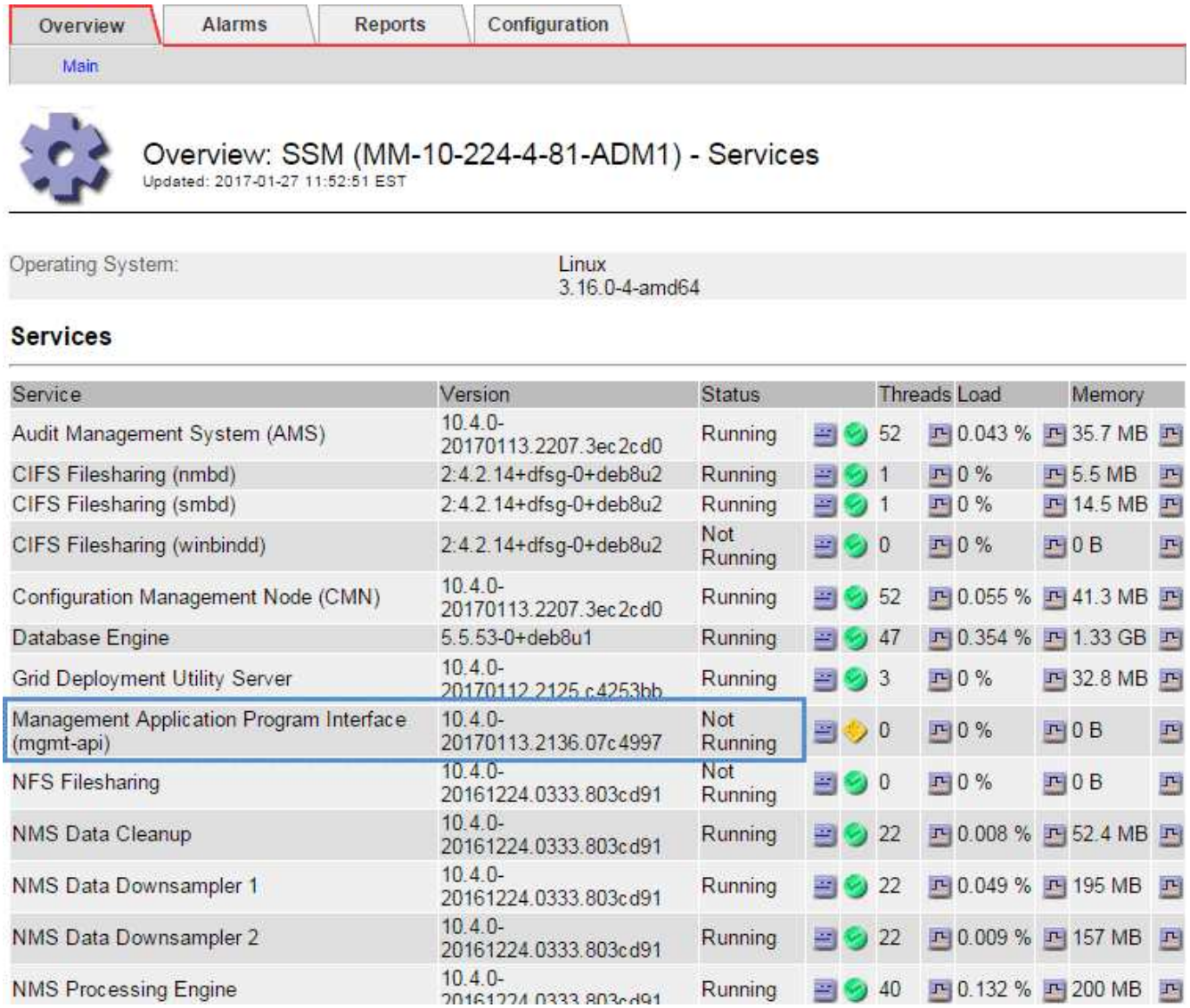
如果 StorageGRID 系统包含多个管理节点，则可以使用另一个管理节点检查不可用管理节点的状态。

您需要的内容

您必须具有特定的访问权限。

步骤

1. 从可用的管理节点中，使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
3. 选择 * 站点 * > * 不可用管理节点 _* > * SSM* > * 服务 * > * 概述 * > * 主 * 。
4. 查找状态为未运行且可能也显示为蓝色的服务。



5. 确定是否已触发警报。
6. 采取适当的操作解决问题描述 。

相关信息

对网络，硬件和平台问题进行故障排除

您可以执行多项任务来帮助确定与 StorageGRID 网络，硬件和平台问题相关的问题的根源。

对"`422：Unprocessable Entity`"错误进行故障排除

错误 422 ： 在许多情况下可能会出现 Unprocessable Entity 。检查错误消息以确定导致问题描述 的原因。

如果您看到列出的错误消息之一，请采取建议的操作。

错误消息	根发生原因 和更正操作

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	如果在使用 Windows Active Directory （ AD ）配置身份联合时为传输层安全（ TLS ）选择 * 不使用 TLS* 选项，则可能会出现此消息。
	
	不支持对强制执行 LDAP 签名的 AD 服务器使用 * 不使用 TLS* 选项。您必须为 TLS 选择 * 使用 STARTTL* 选项或 * 使用 LDAPS* 选项。

错误消息	根发生原因 和更正操作

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	如果您尝试使用不受支持的密码从 StorageGRID 到用于标识联合或云存储池的外部系统建立传输层安全（ TLS ）连接，则会显示此消息。
	
	检查外部系统提供的密码。系统必须使用 StorageGRID 支持的其中一个密码进行传出 TLS 连接，如 StorageGRID 管理说明所示。

相关信息

管理 StorageGRID

【故障排除_MTU_ALERT]]对网格网络MTU不匹配警报进行故障排除

如果网格网络接口（ eth0 ）的最大传输单元（ MTU ）设置在网格中的各个节点之间差别很大，则会触发 * 网格网络 MTU 不匹配 * 警报。

关于此任务

MTU 设置的差异可能表明，某些（但并非所有） eth0 网络配置了巨型帧。如果 MTU 大小不匹配大于 1000 ，则可能会出现发生原因 网络性能问题。

步骤

1. 列出所有节点上 eth0 的 MTU 设置。
   - 使用网格管理器中提供的查询。
   - 导航到 ` 主管理节点 IP 地址 _/metrics/graph` 并输入以下查询： `node_network_mtu` 字节 `{interface="eth0' }`
2. 根据需要修改 MTU 设置，以确保所有节点上的网格网络接口（ eth0 ）设置相同。
   - 对于设备节点，请参见适用于您的设备的安装和维护说明。
   - 对于基于 Linux 和 VMware 的节点，请使用以下命令： ` +/usr/sbin/change-ip.py （ -h] （ -n 节点） MTU 网络（ network…） +`
     - 示例 * ： `change-ip.py -n node 1500 grid admin`
     - 注 * ： 在基于 Linux 的节点上，如果容器中网络所需的 MTU 值超过主机接口上已配置的值，则必须先将主机接口配置为具有所需的 MTU 值， 然后，使用 `change-ip.py` 脚本更改容器中网络的 MTU 值。

   使用以下参数修改基于 Linux 或 VMware 的节点上的 MTU 。

定位参数	Description
`mtu`	要设置的 MTU 。必须介于 1280 到 9216 之间。
网络	要应用 MTU 的网络。包括以下一种或多种网络类型： • 网格 • 管理员 • 客户端

+

可选参数	Description
` h ，–帮助`	显示帮助消息并退出。
` -n node ， -node node`	节点。默认值为本地节点。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

对网络接收错误（ NRER ）警报进行故障排除

StorageGRID 与网络硬件之间的连接问题可能会导致网络接收错误（ NRER ）警报。在某些情况下，无需手动干预即可清除 NRER 错误。如果未清除这些错误，请执行建议的操作。

关于此任务

与 StorageGRID 连接的网络硬件出现以下问题可能会导致 NRER 警报：

- 需要正向错误更正（ FEC ），但不在使用中
- 交换机端口和 NIC MTU 不匹配
- 链路错误率较高
- NIC 环缓冲区溢出

步骤

1. 根据您的网络配置，对 NRER 警报的所有潜在原因执行故障排除步骤。
    - 如果此错误是由 FEC 不匹配引起的，请执行以下步骤：

- 注 * ： 这些步骤仅适用于 StorageGRID 设备上 FEC 不匹配导致的 NRER 错误。

  i. 检查连接到 StorageGRID 设备的交换机中端口的 FEC 状态。

  ii. 检查从设备到交换机的缆线的物理完整性。

  iii. 如果要更改 FEC 设置以尝试解决 NRER 警报，请首先确保在 StorageGRID 设备安装程序的 " 链路配置 " 页面上将设备配置为 * 自动 * 模式（请参见适用于您设备的安装和维护说明）。然后，更改交换机端口上的 FEC 设置。如果可能， StorageGRID 设备端口会调整其 FEC 设置以匹配。

  （您不能在 StorageGRID 设备上配置 FEC 设置。相反，设备会尝试发现并镜像其所连接的交换机端口上的 FEC 设置。如果强制链路达到 25 GbE 或 100 GbE 网络速度，则交换机和 NIC 可能无法协商通用 FEC 设置。如果没有通用的 FEC 设置，网络将回退到 "`no-FEC` " 模式。如果未启用 FEC ，则连接更容易受到电气噪声引起的错误的影响。）

- 注 * ： StorageGRID 设备支持光纤节点（ FC ）和 Reed Solomon （ RS ） FEC ，并且不支持 FEC 。

◦ 如果此错误是由于交换机端口和 NIC MTU 不匹配导致的，请检查节点上配置的 MTU 大小是否与交换机端口的 MTU 设置相同。

节点上配置的 MTU 大小可能小于节点所连接的交换机端口上的设置。如果 StorageGRID 节点收到的以太网帧大于其 MTU ，则可能会报告 NRER 警报。如果您认为发生了这种情况，请根据端到端 MTU 目标或要求更改交换机端口的 MTU 以匹配 StorageGRID 网络接口 MTU ，或者更改 StorageGRID 网络接口的 MTU 以匹配交换机端口。

> 为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都相同。

> 要更改 MTU 设置，请参见适用于您的设备的安装和维护指南。

◦ 如果此错误是由高链路错误率引起的，请执行以下步骤：

  i. 启用 FEC （如果尚未启用）。

  ii. 确认网络布线质量良好，并且未损坏或连接不正确。

  iii. 如果电缆似乎不存在问题，请联系技术支持。

  > 在具有高电噪声的环境中，您可能会发现错误率较高。

◦ 如果错误是 NIC 环缓冲区溢出，请联系技术支持。

如果 StorageGRID 系统过载且无法及时处理网络事件，则环缓冲区可能会溢出。

2. 解决基本问题后，重置错误计数器。

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

   b. 选择 * 站点 _* > * 网格节点 _* > * SSM* > * 资源 * > * 配置 * > * 主 * 。

   c. 选择 * 重置接收错误计数 * ，然后单击 * 应用更改 * 。

相关信息

对网格网络 MTU 不匹配警报进行故障排除

警报参考（旧系统）

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

SG100 和 SG1000 服务设备

对时间同步错误进行故障排除

您可能会在网格中看到时间同步问题。

如果遇到时间同步问题，请确认您至少指定了四个外部 NTP 源，每个源均提供 Stratum 3 或更好的参考，并且所有外部 NTP 源均正常运行且可由 StorageGRID 节点访问。

> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。

相关信息

恢复和维护

Linux： 网络连接问题

您可能会看到 Linux 主机上托管的 StorageGRID 网格节点的网络连接问题。

MAC 地址克隆

在某些情况下，可以使用 MAC 地址克隆来解决网络问题。如果使用的是虚拟主机，请在节点配置文件中将每个网络的 MAC 地址克隆密钥值设置为 "true" 。此设置会使 StorageGRID 容器的 MAC 地址使用主机的 MAC 地址。要创建节点配置文件，请参见适用于您的平台的安装指南中的说明。

> 创建单独的虚拟网络接口，以供 Linux 主机操作系统使用。如果发生原因 虚拟机管理程序未启用混杂模式，则对 Linux 主机操作系统和 StorageGRID 容器使用相同的网络接口可能会使主机操作系统无法访问。

有关启用 MAC 克隆的详细信息，请参见适用于您的平台的安装指南中的说明。

混杂模式

如果您不希望使用 MAC 地址克隆，而希望允许所有接口接收和传输非虚拟机管理程序分配的 MAC 地址的数据， 对于配置模式， MAC 地址更改和伪造传输，请确保虚拟交换机和端口组级别的安全属性设置为 * 接受 * 。虚拟交换机上设置的值可以被端口组级别的值覆盖，因此请确保这两个位置的设置相同。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

Linux：节点状态为"`孤立`"

处于孤立状态的 Linux 节点通常表示控制节点容器的 StorageGRID 服务或 StorageGRID 节点守护进程意外终止。

关于此任务

如果 Linux 节点报告其处于孤立状态，您应：

- 检查日志中的错误和消息。
- 尝试重新启动节点。
- 如有必要，请使用 container engine 命令停止现有节点容器。
- 重新启动节点。

步骤

1. 检查服务守护进程和孤立节点的日志，查看是否存在明显的错误或有关意外退出的消息。
2. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
3. 运行以下命令，尝试重新启动节点： ` $sudo StorageGRID node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   如果节点已孤立，则响应为

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. 在 Linux 中，停止容器引擎以及任何控制存储节点进程。例如：`sudo Docker stop -time secondscontainer-name`

   对于 `seconds` ，输入要等待容器停止的秒数（通常为 15 分钟或更短）。例如：

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. 重新启动节点： `StorageGRID node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

Linux： 对 **IPv6** 支持进行故障排除

如果您在 Linux 主机上安装了 StorageGRID 节点，并且注意到尚未按预期为节点容器分配 IPv6 地址，则可能需要在内核中启用 IPv6 支持。

关于此任务

您可以在网格管理器的以下位置查看已分配给网格节点的 IPv6 地址：

- 选择 * 节点 * ，然后选择节点。然后，在概述选项卡上选择 * IP 地址 * 旁边的 * 显示更多 * 。
- 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * ； node_* > * 。 ssm * > * 资源 * 。如果已分配 IPv6 地址，则此地址将列在 * 网络地址 * 部分的 IPv4 地址下方。

如果未显示 IPv6 地址且节点安装在 Linux 主机上，请按照以下步骤在内核中启用 IPv6 支持。

步骤

1. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
2. 运行以下命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

结果应为 0 。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

如果结果不是 0 ，请参见适用于您的操作系统的文档，了解如何更改 `sysctl` 设置。然后，将此值更改为 0 ，然后再继续。

3. 输入 StorageGRID 节点容器： `StorageGRID node enter node-name`
4. 运行以下命令： `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

结果应为 1 。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

如果结果不是 1 ，则此操作步骤 不适用。请联系技术支持。

5. 退出容器： `exit`

```
root@DC1-S1:~ # exit
```

6. 以 root 用户身份编辑以下文件： ` /var/lib/storaggrid/settings/sysctl.d/net.conf` 。

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 找到以下两行并删除注释标记。然后，保存并关闭该文件。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 运行以下命令重新启动 StorageGRID 容器：

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

对外部系统日志服务器进行故障排除

下表介绍了外部系统日志服务器错误消息并列出了更正操作。

错误消息	问题描述 和建议的操作
无法解析主机名	您为系统日志服务器输入的 FQDN 无法解析为 IP 地址。 1. 检查输入的主机名。如果输入了 IP 地址，请确保其为 w.x.y.z （ " 点分十进制 " ）表示法中的有效 IP 地址。 2. 检查 DNS 服务器是否配置正确。 3. 确认每个节点均可访问 DNS 服务器的 IP 地址。
连接被拒绝	拒绝与系统日志服务器建立 TCP 或 TLS 连接。可能没有服务在侦听主机的 TCP 或 TLS 端口，或者防火墙可能正在阻止访问。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 2. 确认系统日志服务的主机正在运行侦听指定端口的系统日志守护进程。 3. 确认防火墙不会阻止从节点到系统日志服务器的 IP 和端口的 TCP/TLS 连接访问。

错误消息	问题描述 和建议的操作
无法访问网络	系统日志服务器不在直连子网上。路由器返回 ICMP 失败消息，指示它无法将测试消息从列出的节点转发到系统日志服务器。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 对于列出的每个节点，请检查网格网络子网列表，管理网络子网列表和客户端网络网关。确认这些配置已通过预期网络接口和网关（网格，管理员或客户端）将流量路由到系统日志服务器。
无法访问主机	系统日志服务器位于直连子网上（列出的节点用于其网格，管理员或客户端 IP 地址的子网）。节点尝试发送测试消息，但未收到对系统日志服务器 MAC 地址的 ARP 请求的响应。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 检查运行系统日志服务的主机是否已启动。
连接超时	已尝试进行 TCP/TLS 连接，但系统日志服务器长时间未收到任何响应。可能存在路由配置不当或防火墙在未发送任何响应的情况下丢弃流量（通用配置）。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 对于列出的每个节点，请检查网格网络子网列表，管理网络子网列表和客户端网络网关。确认已将这些配置为通过网络接口和网关（网格，管理员或客户端）将流量路由到系统日志服务器，而您希望通过该网关访问系统日志服务器。 3. 确认防火墙未阻止从列出的节点到系统日志服务器的 IP 和端口访问 TCP/TLS 连接。
配对节点已关闭连接	已成功建立与系统日志服务器的 TCP 连接，但稍后关闭。原因可能包括： • 系统日志服务器可能已重新启动或重新启动。 • 节点和系统日志服务器可能具有不同的 TCP/TLS 设置。 • 中间防火墙可能正在关闭闲置的 TCP 连接。 • 侦听系统日志服务器端口的非系统日志服务器可能已关闭连接。 a. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 b. 如果您使用的是 TLS ，请确认系统日志服务器也使用 TLS 。如果您使用的是 TCP ，请确认系统日志服务器也使用 TCP 。 c. 检查中间防火墙是否未配置为关闭空闲 TCP 连接。

错误消息	问题描述 和建议的操作
TLS 证书错误	从系统日志服务器收到的服务器证书与您提供的 CA 证书包和客户端证书不兼容。 1. 确认 CA 证书包和客户端证书（如果有）与系统日志服务器上的服务器证书兼容。 2. 确认系统日志服务器的服务器证书中的身份包含预期的 IP 或 FQDN 值。
转发已暂停	系统日志记录不再转发到系统日志服务器， StorageGRID 无法检测到原因。 查看随此错误提供的调试日志，尝试确定根发生原因 。
TLS 会话已终止	系统日志服务器已终止 TLS 会话， StorageGRID 无法检测到原因。 1. 查看随此错误提供的调试日志，尝试确定根发生原因 。 2. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 3. 如果您使用的是 TLS ，请确认系统日志服务器也使用 TLS 。如果您使用的是 TCP ，请确认系统日志服务器也使用 TCP 。 4. 确认 CA 证书包和客户端证书（如果有）与系统日志服务器的服务器证书兼容。 5. 确认系统日志服务器的服务器证书中的身份包含预期的 IP 或 FQDN 值。
结果查询失败	用于系统日志服务器配置和测试的管理节点无法从列出的节点请求测试结果。一个或多个节点可能已关闭。 1. 按照标准故障排除步骤操作，确保节点联机且所有预期服务均正在运行。 2. 在列出的节点上重新启动 miscd 服务。

警报参考

下表列出了所有默认 StorageGRID 警报。您可以根据需要创建自定义警报规则，以适合您的系统管理方法。

请参见有关的信息 常用的 Prometheus 指标 了解其中某些警报中使用的指标。

警报名称	问题描述 和建议的操作
设备电池已过期	设备存储控制器中的电池已过期。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池出现故障	设备存储控制器中的电池出现故障。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池的已学习容量不足	设备存储控制器中的电池已获取容量不足。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池即将过期	设备存储控制器中的电池即将过期。 1. 请尽快更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。

警报名称	问题描述 和建议的操作
已取出设备电池	设备存储控制器中的电池缺失。 1. 安装电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
设备电池过热	设备存储控制器中的电池过热。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 调查可能导致温度升高的原因，例如风扇或暖通空调出现故障。 3. 如果此警报仍然存在，请联系技术支持。
设备 BMC 通信错误	与基板管理控制器（ BMC ）的通信已丢失。 1. 确认 BMC 运行正常。选择 * 节点 * ，然后选择设备节点的 * 硬件 * 选项卡。找到 Compute Controller BMC IP 字段，然后浏览到此 IP 。 2. 尝试将节点置于维护模式，然后关闭并重新打开设备电源，以恢复 BMC 通信。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG6000 存储设备 3. 如果此警报仍然存在，请联系技术支持。
设备缓存备份设备失败	永久性缓存备份设备出现故障。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 请联系技术支持。
设备缓存备份设备容量不足	缓存备份设备容量不足。 请联系技术支持。
设备缓存备份设备已写保护	缓存备份设备受写保护。 请联系技术支持。

警报名称	问题描述 和建议的操作
设备缓存内存大小不匹配	设备中的两个控制器具有不同的缓存大小。 请联系技术支持。
设备计算控制器机箱温度过高	StorageGRID 设备中计算控制器的温度已超过额定阈值。 1. 检查硬件组件是否过热，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备计算控制器 CPU 温度过高	StorageGRID 设备中计算控制器的 CPU 温度已超过额定阈值。 1. 检查硬件组件是否过热，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备

警报名称	问题描述 和建议的操作
设备计算控制器需要引起注意	在 StorageGRID 设备的计算控制器中检测到硬件故障。 1. 检查硬件组件是否存在错误，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备
设备计算控制器电源 A 出现问题	计算控制器中的电源 A 存在问题。此警报可能指示电源出现故障或无法供电。 1. 检查硬件组件是否存在错误，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备

警报名称	问题描述 和建议的操作
设备计算控制器电源 B 出现问题	计算控制器中的电源 B 出现问题。 此警报可能指示电源出现故障或无法供电。 1. 检查硬件组件是否存在错误，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG100 和 SG1000 服务设备 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备
设备计算硬件监控服务已停止	监控存储硬件状态的服务已停止报告数据。 1. 在基础操作系统中检查 EOS 系统状态服务的状态。 2. 如果此服务处于 stopped 或 error 状态，请重新启动此服务。 3. 如果此警报仍然存在，请联系技术支持。
检测到设备光纤通道故障	检测到设备存储控制器和计算控制器之间存在光纤通道链路问题。 此警报可能指示设备中存储控制器和计算控制器之间的光纤通道连接出现问题。 1. 检查硬件组件是否存在错误（ * 节点 * > * 设备节点 _* > * 硬件 * ）。如果任何组件的状态不是 "`标称，` "，请执行以下操作： a. 验证控制器之间的光纤通道缆线是否已完全连接。 b. 确保光纤通道缆线没有过度弯曲。 c. 确认 SFP+ 模块已正确就位。 ▪ 注： * 如果此问题仍然存在，则 StorageGRID 系统可能会自动使有问题的连接脱机。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG5700 存储设备 ◦ SG6000 存储设备
设备光纤通道 HBA 端口故障	光纤通道 HBA 端口出现故障或出现故障。 请联系技术支持。

警报名称	问题描述 和建议的操作
设备闪存缓存驱动器非最佳	用于 SSD 缓存的驱动器并非最佳驱动器。 1. 更换 SSD 缓存驱动器。请参见适用于您的设备的说明： ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
已卸下设备互连 / 电池箱	互连 / 电池箱缺失。 1. 更换电池。在更换存储控制器时，操作步骤 中提供了电池的拆卸和更换步骤。请参见适用于您的存储设备的说明。 ◦ SG5600 存储设备 ◦ SG5700 存储设备 ◦ SG6000 存储设备 2. 如果此警报仍然存在，请联系技术支持。
缺少设备 LACP 端口	StorageGRID 设备上的端口不参与 LACP 绑定。 1. 检查交换机的配置。确保接口配置在正确的链路聚合组中。 2. 如果此警报仍然存在，请联系技术支持。
设备整体电源性能下降	StorageGRID 设备的电源已偏离建议的工作电压。 1. 检查电源 A 和 B 的状态以确定哪个电源运行异常，并按照建议的操作进行操作： ◦ 如果您使用的是 SG100 ， SG1000 或 SG6000 ，请使用 BMC 。 ◦ 如果您使用的是 SG5600 或 SG5700 ，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ SG100 和 SG1000 服务设备

警报名称	问题描述 和建议的操作
设备存储控制器 A 出现故障	StorageGRID 设备中的存储控制器 A 出现故障。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器 B 故障	StorageGRID 设备中的存储控制器 B 出现故障。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器驱动器故障	StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器硬件问题描述	SANtricity 软件报告 StorageGRID 设备中的某个组件 " 需要关注 " 。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备

警报名称	问题描述 和建议的操作
设备存储控制器电源 A 出现故障	StorageGRID 设备中的电源 A 与建议的工作电压不同。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储控制器电源 B 故障	StorageGRID 设备中的电源 B 与建议的工作电压不同。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
设备存储硬件监控服务已停止	监控存储硬件状态的服务已停止报告数据。 1. 在基础操作系统中检查 EOS 系统状态服务的状态。 2. 如果此服务处于 stopped 或 error 状态，请重新启动此服务。 3. 如果此警报仍然存在，请联系技术支持。
设备存储架降级	存储设备存储架中某个组件的状态为已降级。 1. 使用 SANtricity 系统管理器检查硬件组件，并按照建议的操作进行操作。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
已超过设备温度	已超过设备存储控制器的额定或最大温度。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 调查可能导致温度升高的原因，例如风扇或暖通空调出现故障。 3. 如果此警报仍然存在，请联系技术支持。

警报名称	问题描述 和建议的操作
已卸下设备温度传感器	已卸下温度传感器。请联系技术支持。
Cassandra auto-compactor 错误	Cassandra 自动 compactor 出现错误。 Cassandra 自动 compactor 位于所有存储节点上，用于管理 Cassandra 数据库的大小，以覆盖和删除繁重的工作负载。虽然此情况持续存在，但某些工作负载的元数据消耗量会异常高。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 请联系技术支持。
正在将审核日志添加到内存队列中	节点无法将日志发送到本地系统日志服务器，并且内存队列正在填满。 1. 确保 rsyslog 服务正在节点上运行。 2. 如有必要，请使用命令 `service rsyslog restart` 在节点上重新启动 rsyslog 服务。 3. 如果无法重新启动 rsyslog 服务，并且您未在管理节点上保存审核消息，请联系技术支持。如果不更正此情况，审核日志将丢失。
Cassandra 自动数据压缩器指标已过期	描述 Cassandra 自动数据压缩器的指标已过时。 Cassandra 自动 compactor 位于所有存储节点上，用于管理 Cassandra 数据库的大小，以覆盖和删除繁重的工作负载。尽管此警报持续存在，但某些工作负载的元数据消耗量会异常高。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 请联系技术支持。

警报名称	问题描述 和建议的操作
Cassandra 通信错误	运行 Cassandra 服务的节点无法彼此通信。 此警报表示存在干扰节点到节点通信的情况。一个或多个存储节点上可能存在网络问题描述 或 Cassandra 服务已关闭。 1. 确定是否存在其他影响一个或多个存储节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 检查是否存在可能影响一个或多个存储节点的网络问题描述 。 3. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 4. 对于系统中的每个存储节点，选择 * SSM* > * 服务 * 。确保 Cassandra 服务的状态为 "running" 。 5. 如果 Cassandra 未运行，请按照的步骤进行操作 启动或重新启动服务。 6. 如果 Cassandra 服务的所有实例现在都在运行，并且警报未得到解决，请联系技术支持。
Cassandra compActions 已过载	Cassandra 数据缩减过程过载。 如果数据缩减过程过载，读取性能可能会下降， RAM 可能会用尽。Cassandra 服务也可能无响应或崩溃。 1. 按照的步骤重新启动 Cassandra 服务 正在重新启动服务。 2. 如果此警报仍然存在，请联系技术支持。
Cassandra 修复指标已过期	描述 Cassandra 修复作业的指标已过时。如果此情况持续 48 小时以上，则存储分段列表等客户端查询可能会显示已删除的数据。 1. 重新启动节点。在网格管理器中，转到 * 节点 * ，选择节点，然后选择任务选项卡。 2. 如果此警报仍然存在，请联系技术支持。
Cassandra 修复进度缓慢	Cassandra 数据库修复进度缓慢。 当数据库修复速度较慢时， Cassandra 数据一致性操作会受到阻碍。如果此情况持续 48 小时以上，则存储分段列表等客户端查询可能会显示已删除的数据。 1. 确认所有存储节点均已联机，并且没有与网络相关的警报。 2. 监控此警报最多 2 天，查看问题描述 是否自行解决。 3. 如果数据库修复继续缓慢进行，请联系技术支持。

警报名称	问题描述 和建议的操作
Cassandra 修复服务不可用	Cassandra 修复服务不可用。 Cassandra 修复服务位于所有存储节点上，可为 Cassandra 数据库提供关键修复功能。如果此情况持续 48 小时以上，则存储分段列表等客户端查询可能会显示已删除的数据。 1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 2. 对于系统中的每个存储节点，选择 * SSM* > * 服务 * 。确保 Cassandra Reaper 服务的状态为 "running" 。 3. 如果 Cassandra Reaper 未运行，请按照中的步骤进行操作 启动或重新启动服务。 4. 如果 Cassandra Reaper 服务的所有实例现在都在运行，并且警报未得到解决，请联系技术支持。
Cassandra 表损坏	Cassandra 检测到表损坏。 如果 Cassandra 检测到表损坏，则它会自动重新启动。 请联系技术支持。
云存储池连接错误	云存储池的运行状况检查检测到一个或多个新错误。 1. 转到 " 存储池 " 页面的 " 云存储池 " 部分。 2. 查看 Last Error 列以确定哪个 Cloud Storage Pool 存在错误。 3. 请参见的说明 通过信息生命周期管理管理对象。
DHCP 租约已过期	网络接口上的 DHCP 租约已过期。如果 DHCP 租约已过期，请执行建议的操作： 1. 确保此节点与受影响接口上的 DHCP 服务器之间存在连接。 2. 确保 DHCP 服务器上的受影响子网中有可分配的 IP 地址。 3. 确保为 DHCP 服务器中配置的 IP 地址预留了永久空间。或者，使用 StorageGRID 更改 IP 工具在 DHCP 地址池之外分配静态 IP 地址。请参见 恢复和维护说明。

警报名称	问题描述 和建议的操作
DHCP 租约即将到期	网络接口上的 DHCP 租约即将到期。 要防止 DHCP 租约到期，请执行建议的操作： 1. 确保此节点与受影响接口上的 DHCP 服务器之间存在连接。 2. 确保 DHCP 服务器上的受影响子网中有可分配的 IP 地址。 3. 确保为 DHCP 服务器中配置的 IP 地址预留了永久空间。或者，使用 StorageGRID 更改 IP 工具在 DHCP 地址池之外分配静态 IP 地址。请参见 恢复和维护说明。
DHCP 服务器不可用	DHCP 服务器不可用。 StorageGRID 节点无法联系您的 DHCP 服务器。无法验证节点 IP 地址的 DHCP 租约。 1. 确保此节点与受影响接口上的 DHCP 服务器之间存在连接。 2. 确保 DHCP 服务器上的受影响子网中有可分配的 IP 地址。 3. 确保为 DHCP 服务器中配置的 IP 地址预留了永久空间。或者，使用 StorageGRID 更改 IP 工具在 DHCP 地址池之外分配静态 IP 地址。请参见 恢复和维护说明。
磁盘 I/O 速度非常慢	磁盘 I/O 非常慢可能会影响 StorageGRID 性能。 1. 如果问题描述 与存储设备节点相关，请使用 SANtricity 系统管理器检查是否存在故障驱动器，存在预测故障的驱动器或正在进行的驱动器修复。此外，还应检查设备计算控制器和存储控制器之间的光纤通道或 SAS 链路的状态，以查看是否有任何链路已关闭或显示的错误率过高。 2. 检查托管此节点的卷的存储系统，以确定并更正慢速 I/O 的根发生原因 3. 如果此警报仍然存在，请联系技术支持。 ◦ 注意： * 受影响的节点可能会禁用服务并自行重新启动，以避免影响整体网格性能。如果清除了底层条件，并且这些节点检测到正常 I/O 性能，则它们将自动恢复到完全服务状态。

警报名称	问题描述 和建议的操作

EC 重新平衡失败	在存储节点之间重新平衡擦除编码的数据的作业失败或已被用户暂停。
	1. 确保要重新平衡的站点上的所有存储节点均已联机且可用。
	2. 确保要重新平衡的站点上没有卷故障。如果存在，请终止 EC 重新平衡作业，以便您可以运行修复作业。
	`"rebalance-data terminate -job-id <ID>"`
	3. 确保要重新平衡的站点上没有服务故障。如果服务未运行，请按照恢复和维护说明中有关启动或重新启动服务的步骤进行操作。
	4. 解决任何问题后，请在主管理节点上运行以下命令以重新启动作业：
	`"rebalance-data start -job-id <ID>"`
	5. 如果无法解决此问题，请联系技术支持。

EC 修复失败	擦除编码数据的修复作业失败或已停止。 1. 确保有足够的可用存储节点或卷来替代发生故障的存储节点或卷。 2. 确保有足够的可用存储节点来满足活动 ILM 策略的要求。 3. 确保没有网络连接问题。 4. 解决任何问题后，请在主管理节点上运行以下命令以重新启动作业： `"repair-data start-EC-node-repair -repair-id <ID>"` 5. 如果无法解决此问题，请联系技术支持。
EC 修复已停止	擦除编码数据的修复作业已停止。 1. 确保有足够的可用存储节点或卷来替代发生故障的存储节点或卷。 2. 确保没有网络连接问题。 3. 解决任何问题后，请检查警报是否已解决。要查看有关修复进度的更详细报告，请在主管理节点上运行以下命令： `"repair-data show-EC-repair-status -repair-id <ID>"` 4. 如果无法解决此问题，请联系技术支持。

警报名称	问题描述 和建议的操作
电子邮件通知失败	无法发送警报电子邮件通知。 如果警报电子邮件通知失败或无法传送测试电子邮件（从 * 警报 * > * 电子邮件设置 * 页面发送），则会触发此警报。 1. 从警报的 * 站点 / 节点 * 列中列出的管理节点登录到网格管理器。 2. 转到 * 警报 * > * 电子邮件设置 * 页面，检查设置，并根据需要进行更改。 3. 单击 * 发送测试电子邮件 * ，然后检查测试收件人的收件箱中是否存在此电子邮件。如果无法发送测试电子邮件，则可能会触发此警报的新实例。 4. 如果无法发送测试电子邮件，请确认您的电子邮件服务器已联机。 5. 如果服务器正在运行，请选择 * 支持 * > * 工具 * > * 日志 * ，然后收集管理节点的日志。指定警报时间前后 15 分钟的时间段。 6. 提取下载的归档并查看 `Prometheus.log` （ _/GID<time_stamp>/<site_node>/<time_stamp>/metrics/Prometheus.log ）` 的内容。 7. 如果无法解决此问题，请联系技术支持。
在 " 证书 " 页面上配置的客户端证书到期	在 " 证书 " 页面上配置的一个或多个客户端证书即将过期。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。 2. 选择一个即将到期的证书。 3. 选择 * 附加新证书 * 上传或生成新证书。 4. 对即将过期的每个证书重复上述步骤。
负载平衡器端点证书到期	一个或多个负载平衡器端点证书即将过期。 1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。 2. 选择证书即将过期的端点。 3. 选择 * 编辑端点 * 可上传或生成新证书。 4. 对证书已过期或即将过期的每个端点重复上述步骤。 有关管理负载平衡器端点的详细信息，请参见 有关管理 StorageGRID 的说明。

警报名称	问题描述 和建议的操作
管理接口的服务器证书到期	用于管理接口的服务器证书即将过期。 1. 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。 3. 上传新的管理接口证书。
S3 和 Swift API 的全局服务器证书到期	用于访问存储 API 端点的服务器证书即将过期。 1. 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。 3. 上传新的 S3 和 Swift API 证书。
外部系统日志 CA 证书到期	用于签署外部系统日志服务器证书的证书颁发机构（ CA ）证书即将过期。 1. 更新外部系统日志服务器上的 CA 证书。 2. 获取更新后的 CA 证书的副本。 3. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 4. 选择 * 编辑外部系统日志服务器 * 。 5. 选择 * 浏览 * 以上传新证书。 6. 完成配置向导以保存新证书和密钥。
外部系统日志客户端证书到期	外部系统日志服务器的客户端证书即将过期。 1. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 2. 选择 * 编辑外部系统日志服务器 * 。 3. 选择 * 浏览 * 以上传新证书。 4. 选择 * 浏览 * 以上传新的私钥。 5. 完成配置向导以保存新证书和密钥。
外部系统日志服务器证书到期	外部系统日志服务器提供的服务器证书即将过期。 1. 更新外部系统日志服务器上的服务器证书。 2. 如果您之前使用网格管理器 API 提供用于证书验证的服务器证书，请使用 API 上传更新后的服务器证书。

警报名称	问题描述 和建议的操作
外部系统日志服务器转发错误	节点无法将日志转发到外部系统日志服务器。 1. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 2. 选择 * 编辑外部系统日志服务器 * 。 3. 继续执行配置向导，直到您能够选择 * 发送测试消息 * 。 4. 选择 * 发送测试消息 * 以确定无法将日志转发到外部系统日志服务器的原因。 5. 解决报告的任何问题。
网格网络 MTU 不匹配	网格网络接口（ eth0 ）的最大传输单元（ MTU ）设置在网格中的各个节点之间差别很大。 MTU 设置的差异可能表明，某些（但并非所有） eth0 网络配置了巨型帧。如果 MTU 大小不匹配大于 1000 ，则可能会出现发生原因 网络性能问题。 请参见中有关网格网络 MTU 不匹配警报的说明 对网络，硬件和平台问题进行故障排除。
Java 堆使用率较高	正在使用的 Java 堆空间百分比很高。 如果 Java 堆已满，则元数据服务可能不可用，客户端请求可能会失败。 1. 查看信息板上的 ILM 活动。当 ILM 工作负载减少时，此警报可能会自行解决。 2. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 3. 如果此警报仍然存在，请联系技术支持。
元数据查询延迟较长	Cassandra 元数据查询的平均时间过长。 查询延迟增加的原因可能包括硬件更改，例如更换磁盘，工作负载更改（例如载入量突然增加）或网络更改（例如节点和站点之间的通信问题）。 1. 确定查询延迟增加前后是否发生任何硬件，工作负载或网络更改。 2. 如果无法解决此问题，请联系技术支持。

警报名称	问题描述 和建议的操作
身份联合同步失败	无法从身份源同步联合组和用户。 1. 确认已配置的 LDAP 服务器已联机且可用。 2. 查看身份联合页面上的设置。确认所有值均为最新值。请参见 使用身份联合 在管理 StorageGRID 的说明中。 3. 单击 * 测试连接 * 以验证 LDAP 服务器的设置。 4. 如果无法解决此问题描述 ，请联系技术支持。
租户的身份联合同步失败	无法从租户配置的身份源同步联合组和用户。 1. 登录到租户管理器。 2. 确认租户配置的 LDAP 服务器已联机且可用。 3. 查看身份联合页面上的设置。确认所有值均为最新值。请参见 使用身份联合 在使用租户帐户的说明中。 4. 单击 * 测试连接 * 以验证 LDAP 服务器的设置。 5. 如果无法解决此问题描述 ，请联系技术支持。
无法实现 ILM 放置	无法为某些对象实现 ILM 规则中的放置指令。 此警报表示放置指令所需的节点不可用或 ILM 规则配置不当。例如，规则可能指定的复制副本数可能多于存储节点数。 1. 确保所有节点均已联机。 2. 如果所有节点均处于联机状态，请查看使用活动 ILM 策略的所有 ILM 规则中的放置说明。确认所有对象都有有效的说明。请参见 有关通过信息生命周期管理来管理对象的说明。 3. 根据需要更新规则设置并激活新策略。 ◦ 注意： * 清除警报可能需要长达 1 天的时间。 4. 如果问题仍然存在，请联系技术支持。 ◦ 注意： * 此警报可能会在升级期间出现，并且可能会在升级成功完成后持续 1 天。当此警报由升级触发时，它将自行清除。

警报名称	问题描述 和建议的操作
ILM 扫描周期过长	扫描，评估对象和应用 ILM 所需的时间过长。 如果完成对所有对象的完整 ILM 扫描的估计时间过长（请参见信息板上的 * 扫描时间段 - 估计值 * ），则活动 ILM 策略可能不会应用于新载入的对象。对 ILM 策略所做的更改可能不会应用于现有对象。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 确认所有存储节点均已联机。 3. 临时减少客户端流量。例如，在网格管理器中，选择 * 配置 * > * 网络 * > * 流量分类 * ，然后创建一个限制带宽或请求数量的策略。 4. 如果磁盘 I/O 或 CPU 过载，请尝试减少负载或增加资源。 5. 如有必要，请更新 ILM 规则以使用同步放置（对于在 StorageGRID 11.3 之后创建的规则，默认设置）。 6. 如果此警报仍然存在，请联系技术支持。 管理 StorageGRID
ILM 扫描速率低	ILM 扫描速率设置为每秒不到 100 个对象。 此警报表示有人已将系统的 ILM 扫描速率更改为每秒不到 100 个对象（默认值： 400 个对象 / 秒）。活动 ILM 策略可能不会应用于新载入的对象。此后对 ILM 策略所做的更改不会应用于现有对象。 1. 在持续支持调查中，确定是否临时更改了 ILM 扫描速率。 2. 请联系技术支持。 请勿在未联系技术支持的情况下更改 ILM 扫描速率。
Kms CA 证书到期	用于对密钥管理服务器（ KMS ）证书进行签名的证书颁发机构（ CA ）证书即将过期。 1. 使用 KMS 软件更新密钥管理服务器的 CA 证书。 2. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 3. 选择证书状态警告的 KMS 。 4. 选择 * 编辑 * 。 5. 选择 * 下一步 * 转到步骤 2 （上传服务器证书）。 6. 选择 * 浏览 * 以上传新证书。 7. 选择 * 保存 * 。 管理 StorageGRID

警报名称	问题描述 和建议的操作
Kms 客户端证书到期	密钥管理服务器的客户端证书即将过期。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 2. 选择证书状态警告的 KMS 。 3. 选择 * 编辑 * 。 4. 选择 * 下一步 * 转到步骤 3 （上传客户端证书）。 5. 选择 * 浏览 * 以上传新证书。 6. 选择 * 浏览 * 以上传新的私钥。 7. 选择 * 保存 * 。 管理 StorageGRID
无法加载 Kms 配置	密钥管理服务器的配置存在，但无法加载。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 如果此警报仍然存在，请联系技术支持。
Kms 连接错误	设备节点无法连接到其站点的密钥管理服务器。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 2. 确认端口和主机名条目正确无误。 3. 确认服务器证书，客户端证书和客户端证书专用密钥正确且未过期。 4. 确保防火墙设置允许设备节点与指定的 KMS 进行通信。 5. 更正任何网络或 DNS 问题。 6. 如果您需要帮助或此警报持续存在，请联系技术支持。
未找到 Kms 加密密钥名称	配置的密钥管理服务器没有与提供的名称匹配的加密密钥。 1. 确认分配给站点的 KMS 使用的加密密钥名称以及任何先前版本正确无误。 2. 如果您需要帮助或此警报持续存在，请联系技术支持。
Kms 加密密钥轮换失败	所有设备卷均已解密，但一个或多个卷无法轮换到最新密钥。请联系技术支持。

警报名称	问题描述 和建议的操作
未配置公里	此站点不存在密钥管理服务器。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。 2. 为此站点添加 KMS 或添加默认 KMS 。 管理 StorageGRID
Kms 密钥无法对设备卷进行解密	无法使用当前 KMS 密钥对启用了节点加密的设备上的一个或多个卷进行解密。 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 确保密钥管理服务器（ KMS ）已配置加密密钥以及任何先前的密钥版本。 3. 如果您需要帮助或此警报持续存在，请联系技术支持。
Kms 服务器证书到期	密钥管理服务器（ KMS ）使用的服务器证书即将过期。 1. 使用 KMS 软件更新密钥管理服务器的服务器证书。 2. 如果您需要帮助或此警报持续存在，请联系技术支持。 管理 StorageGRID
审核队列较大	审核消息的磁盘队列已满。 1. 检查系统上的负载—如果事务数量很多，则警报应逐渐自行解决，您可以忽略此警报。 2. 如果警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。 3. 通过将客户端写入和客户端读取的审核级别更改为 " 错误 " 或 " 关闭 "（ * 配置 * > * 监控 * > * 审核和系统日志服务器 * ），降低客户端操作速率或减少记录的审核消息数量。 查看审核日志

警报名称	问题描述 和建议的操作
检测到原有 CLB 负载平衡器活动	某些客户端可能正在使用默认 S3 和 Swift API 证书连接到已弃用的 CLB 负载平衡器服务。 1. 要简化未来升级，请在 * 证书 * 页面的 * 全局 * 选项卡上安装自定义 S3 和 Swift API 证书。然后，确保连接到原有 CLB 的所有 S3 或 Swift 客户端都具有新证书。 2. 创建一个或多个负载平衡器端点。然后，将所有现有 S3 和 Swift 客户端定向到这些端点。如果需要重新映射客户端端口，请联系技术支持。 其他活动可能会触发此警报，包括端口扫描。要确定当前是否正在使用已弃用的 CLB 服务，请查看 `storagegRid_private_clb_http_connection_established_successful` Prometheus 指标。 如果不再使用 CLB 服务，请根据需要静默或禁用此警报规则。
正在将日志添加到磁盘队列中	节点无法将日志转发到外部系统日志服务器，并且磁盘队列正在填满。 1. 在网格管理器中，转到 * 配置 * > * 监控 * > * 审核和系统日志服务器 * 。 2. 选择 * 编辑外部系统日志服务器 * 。 3. 继续执行配置向导，直到您能够选择 * 发送测试消息 * 。 4. 选择 * 发送测试消息 * 以确定无法将日志转发到外部系统日志服务器的原因。 5. 解决报告的任何问题。
审核日志磁盘容量低	可用于审核日志的空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
可用节点内存不足	节点上的可用 RAM 量较低。 可用 RAM 不足可能表示工作负载发生变化或一个或多个节点发生内存泄漏。 1. 监控此警报以查看问题描述 是否自行解决。 2. 如果可用内存低于主要警报阈值，请联系技术支持。

警报名称	问题描述 和建议的操作
存储池可用空间不足	可用于在存储池中存储对象数据的空间量较低。 1. 选择 * ILM * > * 存储池 * 。 2. 选择警报中列出的存储池，然后选择 * 查看详细信息 * 。 3. 确定需要额外存储容量的位置。您可以向存储池中的每个站点添加存储节点，也可以向一个或多个现有存储节点添加存储卷（ LUN ）。 4. 执行扩展操作步骤 以增加存储容量。 扩展网格
节点内存不足	节点上安装的内存量不足。 增加虚拟机或 Linux 主机可用的 RAM 量。检查主要警报的阈值，以确定 StorageGRID 节点的默认最低要求。请参见适用于您的平台的安装说明： • 安装 Red Hat Enterprise Linux 或 CentOS • 安装 Ubuntu 或 Debian • 安装 VMware
元数据存储不足	可用于存储对象元数据的空间不足。 • 严重警报 * 1. 停止载入对象。 2. 立即在扩展操作步骤 中添加存储节点。 • 主要警报 * 立即在扩展操作步骤 中添加存储节点。 • 次要警报 * 1. 监控对象元数据空间的使用速率。选择 * 节点 * > * 存储节点 _* > * 存储 * ，然后查看已用存储 - 对象元数据图。 2. 在中添加存储节点 扩展操作步骤 请尽快。 添加新存储节点后，系统会自动在所有存储节点之间重新平衡对象元数据，并清除警报。 请参见中有关 " 低元数据存储 " 警报的说明 对元数据问题进行故障排除。
低指标磁盘容量	可用于指标数据库的空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。

警报名称	问题描述 和建议的操作
对象数据存储不足	可用于存储对象数据的空间不足。 执行扩展操作步骤 。您可以向现有存储节点添加存储卷（ LUN ），也可以添加新的存储节点。 对对象数据存储不足警报进行故障排除 扩展网格
低只读水印覆盖	存储卷软只读水印覆盖小于存储节点的最小优化水印。 要了解如何解决此警报，请转至 对低只读水印覆盖警报进行故障排除。
根磁盘容量低	根磁盘的可用空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
系统数据容量低	在 ` /var/local` 文件系统上可用于 StorageGRID 系统数据的空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
tmp 目录可用空间不足	/tmp 目录中的可用空间不足。 1. 监控此警报，查看问题描述 是否自行解析且磁盘空间是否再次可用。 2. 如果可用空间继续减少，请联系技术支持。
节点网络连接错误	在节点之间传输数据时出错。 网络连接错误可能会在无需手动干预的情况下清除。如果错误无法清除，请联系技术支持。 请参见中的网络接收错误（ NRER ）警报说明 对网络，硬件和平台问题进行故障排除。
节点网络接收帧错误	节点收到的网络帧中有很高比例出现错误。 此警报可能指示硬件问题描述 ，例如以太网连接任一端的缆线损坏或收发器出现故障。 1. 如果您使用的是设备，请尝试更换每个 SFP+ 或 SFP28 收发器和缆线，一次更换一个，以查看警报是否清除。 2. 如果此警报仍然存在，请联系技术支持。

警报名称	问题描述 和建议的操作
节点与 NTP 服务器不同步	节点的时间与网络时间协议（ NTP ）服务器不同步。 1. 验证您是否已指定至少四个外部 NTP 服务器，每个服务器均提供 Stratum 3 或更好的参考。 2. 检查所有 NTP 服务器是否均正常运行。 3. 验证与 NTP 服务器的连接。确保它们未被防火墙阻止。
节点未使用 NTP 服务器锁定	节点未锁定到网络时间协议（ NTP ）服务器。 1. 验证您是否已指定至少四个外部 NTP 服务器，每个服务器均提供 Stratum 3 或更好的参考。 2. 检查所有 NTP 服务器是否均正常运行。 3. 验证与 NTP 服务器的连接。确保它们未被防火墙阻止。
非设备节点网络已关闭	一个或多个网络设备已关闭或断开连接。此警报表示无法访问虚拟机或 Linux 主机上安装的节点的网络接口（ eth ）。 请联系技术支持。
对象存在检查失败	对象存在检查作业失败。 1. 选择 * 维护 > 对象存在检查 * 。 2. 记下错误消息。执行相应的更正操作： ◦ 无法启动 * ， * 连接断开 * ， * 未知错误 * a. 确保作业中包含的存储节点和卷处于联机状态且可用。 b. 确保存储节点上没有服务或卷故障。如果某个服务未运行，请启动或重新启动该服务。请参见 恢复和维护说明。 c. 确保可以满足选定的一致性控制。 d. 解决任何问题后，选择 * 重试 * 。作业将从最后一个有效状态恢复。 卷中的 * 严重存储错误 * a. 恢复故障卷。请参见 恢复和维护说明。 b. 选择 * 重试 * 。 c. 作业完成后，为节点上的其余卷创建另一个作业，以检查是否存在其他错误。 3. 如果无法解决这些问题，请联系技术支持。

警报名称	问题描述 和建议的操作
对象存在检查已停止	对象存在检查作业已停止。 对象存在检查作业无法继续。作业中包含的一个或多个存储节点或卷脱机或无响应，或者由于节点过多或不可用，无法再满足选定一致性控制。 1. 确保所有要检查的存储节点和卷均处于联机状态且可用（选择 * 节点 * ）。 2. 确保有足够的存储节点处于联机状态且可用，以使当前协调者节点能够使用选定一致性控制读取对象元数据。如有必要，启动或重新启动服务。请参见 恢复和维护说明。 解决步骤 1 和 2 后，作业将自动从停止位置开始。 3. 如果无法满足选定的一致性控制，请取消作业并使用较低的一致性控制启动另一个作业。 4. 如果无法解决这些问题，请联系技术支持。
对象丢失	一个或多个对象已从网格中丢失。 此警报可能指示数据已永久丢失，无法检索。 1. 立即调查此警报。您可能需要采取措施以防止进一步数据丢失。如果您立即采取措施，则还可以还原丢失的对象。 对丢失和丢失的对象数据进行故障排除 2. 解决底层问题后，重置计数器： a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 b. 对于发出警报的存储节点，请选择 * ； site_* > * ； grid node_* > * LDR* > * 数据存储 * > * 配置 * > * 主 * 。 c. 选择 * 重置丢失的对象计数 * ，然后单击 * 应用更改 * 。
平台服务不可用	具有 RSM 服务的存储节点在站点上运行或可用的数量太少。 确保受影响站点上拥有 RSM 服务的大多数存储节点均处于运行状态且无错误状态。 请参见中的 "`解决平台服务问题` " 有关管理 StorageGRID 的说明。

警报名称	问题描述 和建议的操作
S3 PUT 对象大小太大	S3 客户端正在尝试执行超过 S3 大小限制的 PUT 对象操作。 1. 使用警报详细信息中显示的租户 ID 来标识租户帐户。 2. 转至 * 支持 * > * 工具 * > * 日志 * ，然后收集警报详细信息中显示的存储节点的应用程序日志。指定警报时间前后 15 分钟的时间段。 3. 提取下载的归档，然后导航到 `byncast.log` 的位置（` /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/byncast.log` ）。 4. 在 `byncast.log` 的内容中搜索 ` "method =pt"` ，并通过查看 `clientIP` 字段确定 S3 客户端的 IP 地址。 5. 通知所有客户端用户， PUT 对象大小上限为 5 GiB 。 6. 对大于 5 GiB 的对象使用多部分上传。
管理网络端口 1 上的服务设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。 1. 检查连接到管理网络端口 1 的缆线和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG100 和 SG1000 服务设备 ◦ 禁用警报规则
管理网络（或客户端网络）上的服务设备链接已关闭	管理网络（ eth1 ）或客户端网络（ eth2 ）的设备接口已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG100 和 SG1000 服务设备 ◦ 禁用警报规则

警报名称	问题描述 和建议的操作
网络端口 1 ， 2 ， 3 或 4 上的服务设备链路已关闭	设备上的网络端口 1 ， 2 ， 3 或 4 已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG100 和 SG1000 服务设备 ◦ 禁用警报规则
服务设备存储连接已降级	服务设备中的两个 SSD 之一出现故障或与另一个 SSD 不同步。 设备功能不受影响，但您应立即解决问题描述 。如果两个驱动器都发生故障，则设备将无法再正常运行。 1. 在网格管理器中，选择 * 节点 * > ***services appliage*** ，然后选择 " 硬件 " 选项卡。 2. 查看 * 存储 RAID 模式 * 字段中的消息。 3. 如果此消息显示重新同步操作的进度，请等待此操作完成，然后确认警报已解决。重新同步消息表示 SSD 最近已更换，或者由于其他原因正在重新同步。 4. 如果此消息指示其中一个 SSD 发生故障，请尽快更换发生故障的驱动器。 有关如何更换服务设备中的驱动器的说明，请参见 SG100 和 SG1000 设备安装和维护指南。 SG100 和 SG1000 服务设备
管理网络端口 1 上的存储设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。 1. 检查连接到管理网络端口 1 的缆线和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ 禁用警报规则

警报名称	问题描述 和建议的操作
管理网络（或客户端网络）上的存储设备链接已关闭	管理网络（ eth1 ）或客户端网络（ eth2 ）的设备接口已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ 禁用警报规则
网络端口 1 ， 2 ， 3 或 4 上的存储设备链路已关闭	设备上的网络端口 1 ， 2 ， 3 或 4 已关闭或断开连接。 1. 检查与 StorageGRID 网络的缆线， SFP 和物理连接。 2. 解决任何连接问题。请参见适用于您的设备硬件的安装和维护说明。 3. 如果此端口已按目的断开连接，请禁用此规则。在网格管理器中，选择 * 警报 * > * 规则 * ，选择规则，然后单击 * 编辑规则 * 。然后，取消选中 * 已启用 * 复选框。 ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备 ◦ 禁用警报规则
存储设备存储连接已降级	计算控制器和存储控制器之间的一个或多个连接出现问题。 1. 转至设备以检查端口指示灯。 2. 如果端口指示灯不亮，请确认缆线已正确连接。根据需要更换缆线。 3. 最多等待五分钟。 ◦ 注： * 如果需要更换另一根缆线，请至少拔下 5 分钟。否则，根卷可能会变为只读，这需要重新启动硬件。 4. 在网格管理器中，选择 * 节点 * 。然后，选择出现问题的节点的硬件选项卡。验证警报条件是否已解决。

警报名称	问题描述 和建议的操作
无法访问存储设备	无法访问存储设备。 此警报表示由于底层存储设备出现问题，无法挂载或访问卷。 1. 检查用于此节点的所有存储设备的状态： ◦ 如果节点安装在虚拟机或 Linux 主机上，请按照您的操作系统的说明运行硬件诊断或执行文件系统检查。 ▪ 安装 Red Hat Enterprise Linux 或 CentOS ▪ 安装 Ubuntu 或 Debian ▪ 安装 VMware ◦ 如果节点安装在 SG100 ， SG1000 或 SG6000 设备上，请使用 BMC 。 ◦ 如果此节点安装在 SG5600 或 SG5700 设备上，请使用 SANtricity 系统管理器。 2. 如有必要，请更换组件。请参见适用于您的设备的说明： ◦ SG6000 存储设备 ◦ SG5700 存储设备 ◦ SG5600 存储设备
租户配额使用量高	正在使用的租户配额空间百分比很高。如果租户超过其配额，则新的载入将被拒绝。 • 注： * 默认情况下，此警报规则处于禁用状态，因为它可能会生成大量通知。 1. 在网格管理器中，选择 * 租户 * 。 2. 按 * 配额利用率 * 对表进行排序。 3. 选择配额利用率接近 100% 的租户。 4. 执行以下操作之一或同时执行这两项操作： ▪ 选择 * 编辑 * 以增加租户的存储配额。 ▪ 通知租户其配额利用率较高。

警报名称	问题描述 和建议的操作
无法与节点通信	一个或多个服务无响应，或者无法访问节点。 此警报表示节点已因未知原因断开连接。例如，节点上的服务可能已停止，或者节点可能已因电源故障或意外中断而丢失网络连接。 监控此警报以查看问题描述 是否自行解决。如果问题描述 仍然存在： 1. 确定是否存在其他影响此节点的警报。解决另一个警报后，此警报可能会得到解决。 2. 确认此节点上的所有服务均已运行。如果某个服务已停止，请尝试启动它。请参见 恢复和维护说明。 3. 确保节点的主机已启动。如果不是，请启动主机。 ◦ 注： * 如果关闭了多个主机，请参见 恢复和维护说明。 4. 确定此节点与管理节点之间是否存在网络连接问题描述 。 5. 如果无法解决此警报，请联系技术支持。
节点意外重新启动	节点在过去 24 小时内意外重新启动。 1. 监控此警报。此警报将在 24 小时后清除。但是，如果节点再次意外重新启动，则会再次触发此警报。 2. 如果无法解决此警报，则可能存在硬件故障。请联系技术支持。
检测到未标识的损坏对象	在复制的对象存储中找到无法标识为复制对象的文件。 1. 确定存储节点上的底层存储是否存在任何问题。例如，运行硬件诊断或执行文件系统检查。 2. 解决任何存储问题后， 运行对象存在检查 确定是否缺少 ILM 策略定义的任何复制副本。 3. 监控此警报。此警报将在 24 小时后清除，但如果问题描述 未修复，则会再次触发。 4. 如果无法解决此警报，请联系技术支持。

常用的 **Prometheus** 指标

管理节点上的 Prometheus 服务从所有节点上的服务收集时间序列指标。虽然 Prometheus 收集的指标超过 1000 个，但监控最关键的 StorageGRID 操作需要的指标相对较少。

指标会存储在每个管理节点上，直到为 Prometheus 数据预留的空间已满为止。当 ` /var/local/mysql_ibdata/` 卷达到容量时，首先删除最旧的指标。

要获取完整的指标列表，请使用网格管理 API 。

1. 从网格管理器的顶部，选择帮助图标并选择 * API Documentation" 。

2. 找到 * 指标 * 操作。
3. 执行 `GET /grid/metric-names` 操作。
4. 下载结果。

下表列出了最常用的 Prometheus 指标。您可以参考此列表来更好地了解默认警报规则中的条件，或者为自定义警报规则构建条件。

> 名称中包含 *private* 的指标仅供内部使用，在 StorageGRID 版本之间可能会发生更改，恕不另行通知。

Prometheus 指标	**Description**
alertmanager_notifications _failed_total	失败警报通知的总数。
node_filesystem_avail_bytes	非 root 用户可用的文件系统空间量（以字节为单位）。
node_memory_MemAvailable_bytes	内存信息字段 MemAvailable_bytes 。
node_network_Carrier	/sys/class/net/<iface> 的托架值。
node_network_receive ； errs_total	网络设备统计信息 Receive _errs 。
node_network_transmit_errs_total	网络设备统计信息 transmit_errs 。
storaggrid_administratively 关闭	由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。
storagegrid_appliage_compute_controller_hardware_status	设备中计算控制器硬件的状态。
storagegrid_appliation_failed_disks	对于设备中的存储控制器，是指不是最佳的驱动器数量。
storagegrid_appliage_storage_controller_hardware_status	设备中存储控制器硬件的整体状态。
storagegrid_content_bages_and_containers	此存储节点已知的 S3 存储分段和 Swift 容器总数。
storaggrid_content_objects	此存储节点已知的 S3 和 Swift 数据对象总数。计数仅适用于通过 S3 或 Swift 与系统连接的客户端应用程序创建的数据对象。

Prometheus 指标	Description
storaggrid_content_objects_lost	此服务在 StorageGRID 系统中检测到缺失的对象总数。应采取措施确定丢失的发生原因 以及是否可以恢复。 对丢失和丢失的对象数据进行故障排除
storagegRid_http_sessions_incoming_attempted	尝试访问存储节点的 HTTP 会话总数。
storaggrid_http_sessions_incoming_currently 已建立	存储节点上当前处于活动状态（已打开）的 HTTP 会话数。
storagegRid_http_sessions_incoming_failed	由于 HTTP 请求格式错误或在处理操作时失败而无法成功完成的 HTTP 会话总数。
storagegRid_http_sessions_incoming_successful	已成功完成的 HTTP 会话总数。
storaggrid_ilm_awaiting 背景对象	此节点上等待通过扫描进行 ILM 评估的对象总数。
storaggrid_ilm_awaiting 客户端评估对象每秒对象数	根据此节点上的 ILM 策略评估对象的当前速率。
storaggrid_ilm_awaiting 客户端对象	此节点上等待通过客户端操作进行 ILM 评估的对象总数（例如，载入）。
storaggrid_ilm_awaing_total_objects	等待 ILM 评估的对象总数。
storagegrid_ilm_scanne_objects_per_second	此节点拥有的对象在 ILM 中进行扫描和排队的速率。
storaggrid_ilm_scann_period_estimated_minutes	在此节点上完成完整 ILM 扫描的估计时间。 • 注： * 完全扫描并不能保证 ILM 已应用于此节点拥有的所有对象。
storagegRid_load_Balancer_endpoint_ct_expiry_time	负载平衡器端点证书自 Epoch 以来的到期时间（以秒为单位）。
storaggrid_metadata_queries_average ； latency ；毫秒	通过此服务对元数据存储运行查询所需的平均时间。
storaggrid_network_received_bytes	自安装以来接收的总数据量。
storaggrid_network_transmated_bytes	自安装以来发送的总数据量。

Prometheus 指标	Description
storagegrid_node_cpu_utilization 百分比	此服务当前正在使用的可用 CPU 时间的百分比。指示服务的繁忙程度。可用 CPU 时间量取决于服务器的 CPU 数量。
storaggrid_ntp_chosed_time_source_offset_mms	选定时间源提供的系统时间偏移。如果到达某个时间源的延迟与该时间源到达 NTP 客户端所需的时间不相等，则会引入偏移。
storaggrid_ntp_locked	节点未锁定到网络时间协议（ NTP ）服务器。
storaggrid_s3_data_transfers_bytes_ingested	自上次重置属性以来从 S3 客户端载入到此存储节点的总数据量。
已检索 storagegRid_s3_data_transfers_bytes_reRetrieved	自上次重置属性以来 S3 客户端从此存储节点检索的总数据量。
storaggrid_s3_operations_failed	S3 操作失败的总数（ HTTP 状态代码 4xx 和 5xx ），不包括因 S3 授权失败而导致的操作。
storaggrid_s3_operations_successful	成功执行 S3 操作的总数（ HTTP 状态代码 2xx ）。
storaggrid_s3_operations_unauthorized	授权失败导致的 S3 操作失败的总数。
storagegRid_servercertificate_management_interface_cert_expiry_days	管理接口证书到期前的天数。
storagegRid_servercertificate_storage_api_Endpoints " 证书到期日 "	对象存储 API 证书到期前的天数。
storaggrid_service_cpu_seconds	自安装以来此服务使用 CPU 的累积时间。
storagegrid_service_memory_usage_bytes	此服务当前正在使用的内存量（ RAM ）。此值与 Linux 顶部实用程序显示的值相同，即 Res 。
storaggrid_service_network_received_bytes	自安装以来此服务收到的总数据量。
storaggrid_service_network_transmated_bytes	此服务发送的总数据量。
storagegrid_service_Restart	重新启动服务的总次数。
storaggrid_service_runtime_seconds	自安装以来服务一直运行的总时间量。
storaggrid_service_uptime_seconds	服务自上次重新启动以来的总运行时间。

Prometheus 指标	Description
storaggrid_storage_state_current	存储服务的当前状态。属性值为： • 10 = 脱机 • 15 = 维护 • 20 = 只读 • 30 = 联机
storagegrid_storage_status	存储服务的当前状态。属性值为： • 0 = 无错误 • 10 = 正在过渡 • 20 = 可用空间不足 • 30 = 卷不可用 • 40 = 错误
storaggrid_storage_utilization字节	存储节点上复制和擦除编码的对象数据的估计总大小。
storaggrid_storage_utilization metadata_allowed_bytes	每个存储节点的卷 0 上允许用于对象元数据的总空间。此值始终小于为节点上的元数据预留的实际空间，因为必要的数据库操作（如数据缩减和修复）以及未来的硬件和软件升级都需要预留部分空间。对象元数据允许的空间控制整体对象容量。
storaggrid_storage_utilization metadata_bytes	存储卷 0 上的对象元数据量，以字节为单位。
storaggrid_storage_utilization 总空间字节	分配给所有对象存储的存储空间总量。
storagegRid_storage_utilization_usable_space_bytes	剩余的对象存储空间总量。计算方法是将存储节点上所有对象存储的可用空间量相加。
storagegrid_swif_data_transfers_bytes_ingested	自上次重置属性以来从 Swift 客户端载入到此存储节点的总数据量。
已检索 storaggrid_swif_data_transfers_bytes_reRetrieved	自上次重置属性以来 Swift 客户端从此存储节点检索的总数据量。
storaggrid_swif_operations_failed	Swift 操作失败的总数（ HTTP 状态代码 4xx 和 5xx ），不包括因 Swift 授权失败而导致的操作。
storagegrid_swif_operations_successful	成功的 Swift 操作总数（ HTTP 状态代码 2xx ）。

Prometheus 指标	Description
storaggrid_swif_operations_unauthorized	授权失败导致的 Swift 操作失败的总数（ HTTP 状态代码 401 ， 403 ， 405 ）。
storagegrid_tenant_usage_data_bytes	租户的所有对象的逻辑大小。
storagegrid_tenant_usage_object_count	租户的对象数。
storagegRid_tenant_usage_quota_bytes	可用于租户对象的最大逻辑空间量。如果未提供配额指标，则可用空间量不受限制。

警报参考（旧系统）

下表列出了所有原有的默认警报。如果触发了警报，您可以在此表中查找警报代码以查找建议的操作。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

代码	Name	服务	建议的操作
ABRL	可用属性中继	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BSSM ， BDDS	尽快恢复与运行属性中继服务的服务（一种模数转换器服务）的连接。如果没有连接的属性中继，则网格节点无法向 NMS 服务报告属性值。因此， NMS 服务无法再监控服务的状态，也无法更新服务的属性。 如果问题仍然存在，请联系技术支持。
ACMS	可用元数据服务	BARR ， BLDR ， BCMN	如果 LDR 或 ARC-Service 与 DDS 服务断开连接，则会触发警报。如果发生这种情况，则无法处理载入或检索事务。如果 DDS 服务不可用只是一个短暂的瞬时问题描述 ，则事务可能会延迟。 检查并还原与 DDS 服务的连接，以清除此警报并使此服务恢复完整功能。
行为	云分层服务状态	圆弧	仅适用于目标类型为 Cloud Tiering 的归档节点 - 简单存储服务（ S3 ）。 如果归档节点的 "Acts " 属性设置为 "Read-Only Enabled" 或 "Read-Write Disabled" ，则必须将此属性设置为 "Read-Write Enabled" 。 如果因身份验证失败而触发重大警报，请验证与目标存储分段关联的凭据，并根据需要更新值。 如果因任何其他原因触发重大警报，请联系技术支持。

代码	**Name**	服务	建议的操作
ADCA	模数转换器状态	模数转换器	如果触发警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ADC* > * 概述 * > * 主要 * 和 * ADC* > * 警报 * > * 主要 * 来确定警报的发生原因 。 如果问题仍然存在，请联系技术支持。
ADCE	模数转换器状态	模数转换器	如果 "ADC-State" 的值为 "Standby" ，请继续监控此服务，如果问题仍然存在，请联系技术支持。 如果 "ADC" 状态的值为脱机，请重新启动此服务。如果问题仍然存在，请联系技术支持。
AITE	检索状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果检索状态值正在等待目标，请检查 TSM 中间件服务器并确保其正常运行。如果刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置归档节点与目标外部归档存储系统的连接。 如果 " 归档检索状态 " 的值为 " 脱机 " ，请尝试将此状态更新为 " 联机 " 。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主要 * ，选择 * 归档检索状态 * > * 联机 * ，然后单击 * 应用更改 * 。 如果问题仍然存在，请联系技术支持。
AITU-A	检索状态	BARC-B	如果检索状态的值为目标错误，请检查目标外部归档存储系统是否存在错误。 如果归档检索状态的值为会话丢失，请检查目标外部归档存储系统以确保其联机并正常运行。检查与目标的网络连接。 如果 " 归档检索状态 " 的值为未知错误，请联系技术支持。
Alis	入站属性会话	模数转换器	如果属性中继上的入站属性会话数增长得太大，则可能表示 StorageGRID 系统已变得不平衡。在正常情况下，属性会话应均匀分布在各个模块转换服务之间。不平衡可能导致性能问题。 如果问题仍然存在，请联系技术支持。
ALOS	出站属性会话	模数转换器	此 ADE 服务具有大量属性会话，并且正在过载。如果触发此警报，请联系技术支持。

代码	**Name**	服务	建议的操作
Alur	无法访问的属性存储库	模数转换器	检查与 NMS 服务的网络连接，以确保此服务可以与属性存储库联系。 如果触发此警报且网络连接良好，请联系技术支持。
AMQS	已排队的审核消息	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BDDS	如果无法将审核消息立即转发到审核中继或存储库，则这些消息将存储在磁盘队列中。如果磁盘队列已满，则可能发生中断。 为了及时做出响应以防止中断，当磁盘队列中的消息数量达到以下阈值时，系统将触发 AMQS 警报： • 注意：超过 100 ， 000 条消息 • 次要：至少 500 ， 000 条消息 • 主要：至少 2 ， 000 ， 000 条消息 • 严重：至少 5 ， 000 ， 000 条消息 如果触发了 AMQS 警报，请检查系统上的负载—如果存在大量事务，则该警报应随着时间的推移自行解决。在这种情况下，您可以忽略警报。 如果警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 配置审核消息和日志目标。
AOTE	存储状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果 "Store State" 的值为 Waiting for Target" ，请检查外部归档存储系统并确保其正常运行。如果刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置归档节点与目标外部归档存储系统的连接。 如果 " 存储状态 " 的值为 " 脱机 " ，请检查 " 存储状态 " 的值。在将存储状态移回联机之前更正所有问题。
AOTU	存储状态	BARC-B	如果 "Store Status" （存储状态）的值为 "Session lost" （会话丢失），请检查外部归档存储系统是否已连接并联机。 如果 "Target Error" 的值为，请检查外部归档存储系统是否存在错误。 如果 "Store Status" 的值为 "Unknown" 错误，请联系技术支持。

代码	**Name**	服务	建议的操作
APM	存储多路径连接	SSM	如果多路径状态警报显示为 `Degraded` （选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 事件 * ），请执行以下操作： 1. 插入或更换不显示任何指示灯的缆线。 2. 等待一到五分钟。 在插入另一根缆线至少五分钟后，再拔下另一根缆线。过早拔出可能会使根卷发生原因 变为只读，这要求重新启动硬件。 3. 返回到 * SSM* > * 资源 * 页面，并验证存储硬件部分中的 `Degraded` 多路径状态是否已更改为 "`nominal` " 。
Arce	弧状态	圆弧	在所有旋转组件（复制，存储，检索，目标）启动之前，此旋转式应用程序服务的状态均为 " 备用 " 。然后过渡到联机。 如果 "ARC-State" 值未从 " 备用 " 过渡到 " 联机 " ，请检查这些组件的状态。 如果 "ARC-State" 的值为 "Offlin" ，请重新启动此服务。如果问题仍然存在，请联系技术支持。
AROQ	已排队的对象	圆弧	如果可移动存储设备由于目标外部归档存储系统出现问题而运行缓慢，或者遇到多个读取错误，则可能会触发此警报。检查外部归档存储系统是否存在错误，并确保其正常运行。 在某些情况下，此错误可能是由于数据请求率较高而导致的。监控在系统活动减少时排队的对象数量。

代码	**Name**	服务	建议的操作
ARRF	请求失败	圆弧	如果从目标外部归档存储系统检索失败，则归档节点会重试检索，因为此失败可能是由于瞬时问题描述 造成的。但是，如果对象数据已损坏或已标记为永久不可用，则检索不会失败。相反，归档节点会持续重试检索，而请求失败的值会继续增加。 此警报可能指示保存所请求数据的存储介质已损坏。检查外部归档存储系统以进一步诊断此问题。 如果确定对象数据不再位于归档中，则必须从 StorageGRID 系统中删除该对象。有关详细信息，请联系技术支持。 触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主 * ，选择 * 重置请求失败计数 * 并单击 * 应用更改 * 。
ARRV	验证失败	圆弧	要诊断并更正此问题，请联系技术支持。 触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主 * ，选择 * 重置验证失败计数 * 并单击 * 应用更改 * 。
ARVF	存储故障	圆弧	如果目标外部归档存储系统出错，可能会出现此警报。检查外部归档存储系统是否存在错误，并确保其正常运行。 触发此警报的问题解决后，重置故障计数。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 检索 * > * 配置 * > * 主 * ，选择 * 重置存储故障计数 * ，然后单击 * 应用更改 * 。
ASXP	审核共享	AMS	如果审核共享的值为未知，则会触发警报。此警报可能指示管理节点的安装或配置出现问题。 如果问题仍然存在，请联系技术支持。
AUMA	AMS 状态	AMS	如果 AMS Status 的值为 DB Connectivity Error ，请重新启动网格节点。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
AUME	AMS 状态	AMS	如果 AMS State 的值为 "Standby" ，请继续监控 StorageGRID 系统。如果问题仍然存在，请联系技术支持。 如果 AMS State 的值为 Offline ，请重新启动服务。如果问题仍然存在，请联系技术支持。
AUXS	审核导出状态	AMS	如果触发警报，请更正根本问题，然后重新启动 AMS 服务。 如果问题仍然存在，请联系技术支持。
badd	存储控制器故障驱动器计数	SSM	如果 StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器，则会触发此警报。根据需要更换驱动器。
BASF	可用对象标识符	CMN	配置 StorageGRID 系统后，系统会为 CMN 服务分配固定数量的对象标识符。当 StorageGRID 系统开始用尽其对象标识符时，会触发此警报。 要分配更多标识符，请联系技术支持。
重声	标识符块分配状态	CMN	默认情况下，如果无法分配对象标识符，因为无法达到模数转换仲裁，则会触发警报。 要在 CMN 服务上分配标识符块，需要使模拟学习中心服务达到联机和连接的仲裁（ 50% + 1 ）。如果仲裁不可用，则 CMN 服务将无法分配新的标识符块，直到重新建立了模板仲裁为止。如果丢失了模块转换仲裁，通常不会对 StorageGRID 系统产生任何即时影响（客户端仍可载入和检索内容），因为大约一个月的标识符会缓存在网格中的其他位置； 但是，如果此情况持续存在，则 StorageGRID 系统将无法载入新内容。 如果触发警报，请调查丢失 ADC 仲裁的原因（例如，可能是网络或存储节点故障）并采取更正措施。 如果问题仍然存在，请联系技术支持。
BRDT	计算控制器机箱温度	SSM	如果 StorageGRID 设备中计算控制器的温度超过额定阈值，则会触发警报。 检查硬件组件和环境问题是否过热。如有必要，请更换组件。

代码	**Name**	服务	建议的操作
BTOF	Offset	BADC ， BLDR ， BNMS ， BAMS ， BCLB ， BCMN ， BARC-A	如果服务时间（秒）与操作系统时间相差很大，则会触发警报。在正常情况下，服务应自行重新同步。如果服务时间偏离操作系统时间太远，则可能会影响系统操作。确认 StorageGRID 系统的时间源正确无误。 如果问题仍然存在，请联系技术支持。
BTSE	时钟状态	BADC ， BLDR ， BNMS ， BAMS ， BCLB ， BCMN ， BARC-A	如果服务的时间与操作系统跟踪的时间不同步，则会触发警报。在正常情况下，服务应自行重新同步。如果时间偏离操作系统时间太远，则可能会影响系统操作。确认 StorageGRID 系统的时间源正确无误。 如果问题仍然存在，请联系技术支持。
CAHP	Java 堆使用量百分比	DDS	如果 Java 无法以允许有足够堆空间使系统正常运行的速率执行垃圾收集，则会触发警报。警报可能指示用户工作负载超出整个系统可用于 DDS 元数据存储的资源。检查信息板中的 ILM 活动，或者选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * DDS * > * 资源 * > * 概述 * > * 主 * 。 如果问题仍然存在，请联系技术支持。
CAIH	可用的载入目标的数量	CLB	此警报已弃用。
CAQH	可用目标的数量	CLB	当可用 LDR 服务的基本问题得到更正时，此警报将清除。确保 LDR 服务的 HTTP 组件处于联机状态并正常运行。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
CASA	数据存储状态	DDS	如果 Cassandra 元数据存储不可用，则会发出警报。 检查 Cassandra 的状态： 1. 在存储节点上，使用 Passwords.txt 文件中列出的密码以 admin 和 `su` 登录到 root 。 2. 输入： `sservice Cassandra status` 3. 如果 Cassandra 未运行，请重新启动它： `sservice Cassandra restart` 此警报还可能指示存储节点的元数据存储（ Cassandra 数据库）需要重建。 请参见中有关对服务进行故障排除的信息：状态 - Cassandra （ SVST ）警报 对元数据问题进行故障排除。 如果问题仍然存在，请联系技术支持。
案例	数据存储状态	DDS	安装或扩展期间会触发此警报，以指示新的数据存储正在加入网格。
CCE	传入会话—已建立	CLB	如果网关节点上当前有 20 ， 000 个或更多 HTTP 会话处于活动状态（已打开），则会触发此警报。如果客户端的连接太多，您可能会看到连接失败。您应减少工作负载。
CCNA	计算硬件	SSM	如果需要注意 StorageGRID 设备中计算控制器硬件的状态，则会触发此警报。

代码	Name	服务	建议的操作
CDLP	元数据已用空间（百分比）	DDS	当元数据有效空间（ Metadata Effective Space ，CEMS ）达到 70% 全满（次要警报）， 90% 全满（主要警报）和 100% 全满（严重警报）时，将触发此警报。 如果此警报达到 90% 阈值，则网格管理器的信息板上将显示一条警告。要尽快添加新的存储节点，您必须执行扩展操作步骤 。请参见 扩展网格。 如果此警报达到 100% 阈值，则必须停止载入对象并立即添加存储节点。Cassandra 需要一定的空间来执行诸如压实和修复等基本操作。如果对象元数据使用的空间超过允许的 100% ，则这些操作将受到影响。可能会出现不希望的结果。 • 注 * ： 如果无法添加存储节点，请联系技术支持。 添加新存储节点后，系统会自动在所有存储节点之间重新平衡对象元数据，并清除警报。 另请参见中有关对 " 低元数据存储 " 警报进行故障排除的信息 对元数据问题进行故障排除。
CLBA	CLB 状态	CLB	如果触发警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * CLB* > * 概述 * > * 主 * 和 * CLB* > * 警报 * > * 主 * 以确定警报的发生原因 并解决问题。 如果问题仍然存在，请联系技术支持。
CLBE	CLB 状态	CLB	如果 CLB 状态的值为 " 备用 " ，请继续监控此情况，如果问题仍然存在，请联系技术支持。 如果此状态为脱机，并且没有已知的服务器硬件问题（例如，服务器已拔出）或计划的停机，请重新启动此服务。如果问题仍然存在，请联系技术支持。
CMNA	CMN 状态	CMN	如果 CMN Status 的值为 Error ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * CMN* > * 概述 * > * 主 * 和 * CMN* > * 警报 * > * 主 * 以确定错误的发生原因 并对问题进行故障排除。 切换 CMNS 后，在主管理节点硬件刷新期间会触发警报，并且 CMN 状态值为无联机 CMN （旧的 CMN 状态值为 " 备用 " ，新的 " 联机 " ）。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
CPRC	剩余容量	NMS	如果剩余容量（可打开到 NMS 数据库的可用连接数）降至配置的警报严重性以下，则会触发警报。 如果触发了警报，请联系技术支持。
CPSA	计算控制器电源 A	SSM	如果 StorageGRID 设备的计算控制器中存在电源为 A 的问题描述 ，则会触发警报。 如有必要，请更换组件。
cPSB	计算控制器电源 B	SSM	如果 StorageGRID 设备的计算控制器中存在电源为 B 的问题描述 ，则会触发警报。 如有必要，请更换组件。
CPUT	计算控制器 CPU 温度	SSM	如果 StorageGRID 设备中计算控制器中的 CPU 温度超过额定阈值，则会触发警报。 如果存储节点是 StorageGRID 设备，则 StorageGRID 系统指示需要关注控制器。 检查硬件组件和环境问题是否存在过热情况。如有必要，请更换组件。
DNST	DNS 状态	SSM	安装完成后，将在 SSM 服务中触发 DNST 警报。配置 DNS 并将新服务器信息访问到所有网格节点后，警报将被取消。
ECCD	检测到损坏的片段	LDR	当后台验证过程检测到损坏的纠删编码片段时，将触发警报。如果检测到损坏的片段，则会尝试重建该片段。重置检测到的损坏片段，并将丢失的属性复制到零，然后对其进行监控，以查看计数是否再次增加。如果计数增加，则存储节点的底层存储可能会出现问题。除非丢失或损坏的碎片数量违反纠删代码的容错能力，否则不会认为缺少纠删编码对象数据的副本；因此，可能存在损坏的碎片，并且仍能检索对象。 如果问题仍然存在，请联系技术支持。
ECST	验证状态	LDR	此警报指示此存储节点上经过纠删编码的对象数据的后台验证过程的当前状态。 如果后台验证过程出现错误，则会触发重大警报。

代码	**Name**	服务	建议的操作
FWPN	打开文件描述符	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BSSM ， BDDS	在活动高峰期间， FWPN 可能会变大。如果在活动缓慢期间不会减少，请联系技术支持。
HSTE	HTTP 状态	BLDR	请参见建议的 HSTU 操作。
HSTU	HTTP 状态	BLDR	HSTE 和 HSTU 与所有 LDR 流量的 HTTP 协议相关，包括 S3 ， Swift 和其他内部 StorageGRID 流量。警报表示已发生以下情况之一： • HTTP 协议已手动脱机。 • 已禁用自动启动 HTTP 属性。 • LDR 服务正在关闭。 默认情况下，自动启动 HTTP 属性处于启用状态。如果更改此设置， HTTP 可能会在重新启动后保持脱机状态。 如有必要，请等待 LDR 服务重新启动。 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 存储节点 _* > * LDR* > * 配置 * 。如果 HTTP 协议处于脱机状态，请将其置于联机状态。验证是否已启用自动启动 HTTP 属性。 如果 HTTP 协议仍处于脱机状态，请联系技术支持。
HTA	自动启动 HTTP	LDR	指定是否在启动时自动启动 HTTP 服务。这是用户指定的配置选项。
IRSU	入站复制状态	BLDR ， BARR	警报指示已禁用入站复制。确认配置设置：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 复制 * > * 配置 * > * 主 * 。

代码	**Name**	服务	建议的操作
延迟	平均延迟	NMS	检查连接问题。 检查系统活动以确认系统活动有所增加。系统活动增加将导致属性数据活动增加。这种增加的活动将导致属性数据处理延迟。这可以是正常的系统活动，也可以是次要活动。 检查是否存在多个警报。触发的警报数量过多可能表明平均延迟时间增加。 如果问题仍然存在，请联系技术支持。
LDRE	LDR 状态	LDR	如果 LDR 状态值为 " 备用 " ，请继续监控此情况，如果问题仍然存在，请联系技术支持。 如果 LDR 状态值为脱机，请重新启动服务。如果问题仍然存在，请联系技术支持。
已丢失	对象丢失	DDS ， LDR	当 StorageGRID 系统无法从系统中的任何位置检索所请求对象的副本时触发。在触发 " 丢失（丢失的对象） " 警报之前，系统会尝试从系统中的其他位置检索并更换缺失的对象。 对象丢失表示数据丢失。只要对象的位置数降至零，并且 DDS 服务未特意清除内容以满足 ILM 策略， " 丢失对象 " 属性就会递增。 立即调查丢失（对象丢失）警报。如果问题仍然存在，请联系技术支持。 对丢失和丢失的对象数据进行故障排除
MCEP	管理接口证书到期	CMN	用于访问管理接口的证书即将过期时触发。 1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。 3. 上传新的管理接口证书。
分钟	电子邮件通知已排队	NMS	检查托管 NMS 服务的服务器和外部邮件服务器的网络连接。另外，请确认电子邮件服务器配置正确。 为警报配置电子邮件服务器设置（旧系统）

代码	**Name**	服务	建议的操作
分钟	电子邮件通知状态	BNMS	如果 NMS 服务无法连接到邮件服务器，则会触发一个小警报。检查托管 NMS 服务的服务器和外部邮件服务器的网络连接。另外，请确认电子邮件服务器配置正确。 为警报配置电子邮件服务器设置（旧系统）
等	NMS 接口引擎状态	BNMS	如果管理节点上用于收集和生成接口内容的 NMS 接口引擎与系统断开连接，则会触发警报。检查服务器管理器以确定服务器单个应用程序是否已关闭。
Nang	网络自动协商设置	SSM	检查网络适配器配置。此设置必须与您的网络路由器和交换机的首选项匹配。 设置不正确可能会严重影响系统性能。
NDUP	网络双工设置	SSM	检查网络适配器配置。此设置必须与您的网络路由器和交换机的首选项匹配。 设置不正确可能会严重影响系统性能。
NLNK	网络链路检测	SSM	检查端口和交换机上的网络缆线连接。 检查网络路由器，交换机和适配器配置。 重新启动服务器。 如果问题仍然存在，请联系技术支持。
NRER	接收错误	SSM	以下可能是 NRER 警报的原因： • 正向错误更正（ FEC ）不匹配 • 交换机端口和 NIC MTU 不匹配 • 链路错误率较高 • NIC 环缓冲区溢出 请参见中有关对网络接收错误（ NRER ）警报进行故障排除的信息 对网络，硬件和平台问题进行故障排除。

代码	**Name**	服务	建议的操作
NRLY	可用的审核中继	BADC ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BDDS	如果审核中继未连接到 ADC- 服务，则无法报告审核事件。它们将排队，在连接恢复之前不可供用户使用。 请尽快恢复与模数转换器服务的连接。 如果问题仍然存在，请联系技术支持。
NSCA	NMS 状态	NMS	如果 NMS Status 的值为 DB Connectivity Error ，请重新启动此服务。如果问题仍然存在，请联系技术支持。
NSCE	NMS 状态	NMS	如果 NMS 状态的值为 " 备用 " ，请继续监控，如果问题仍然存在，请联系技术支持。 如果 NMS 状况的值为脱机，请重新启动服务。如果问题仍然存在，请联系技术支持。
NSPD	速度	SSM	这可能是由于网络连接或驱动程序兼容性问题造成的。如果问题仍然存在，请联系技术支持。
NBR	可用表空间	NMS	如果触发警报，请检查数据库使用量变化的速度。突然下降（而不是随着时间的推移逐渐变化）表示出现错误情况。如果问题仍然存在，请联系技术支持。 通过调整警报阈值，您可以主动管理何时需要分配更多存储。 如果可用空间达到较低阈值（请参见警报阈值），请联系技术支持以更改数据库分配。
NTER	传输错误	SSM	可以在不手动重置的情况下清除这些错误。如果未清除，请检查网络硬件。检查适配器硬件和驱动程序是否已正确安装并配置，以便与网络路由器和交换机配合使用。 解决底层问题后，重置计数器。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 资源 * > * 配置 * > * 主 * ，选择 * 重置传输错误计数 * ，然后单击 * 应用更改 * 。
NTFQ	NTP 频率偏移	SSM	如果频率偏移超过配置的阈值，则本地时钟可能存在硬件问题。如果问题仍然存在，请联系技术支持以安排更换。
NTLK	NTP 锁定	SSM	如果 NTP 守护进程未锁定到外部时间源，请检查与指定外部时间源的网络连接，这些时间源的可用性及其稳定性。

代码	**Name**	服务	建议的操作
NTOF	NTP 时间偏移	SSM	如果时间偏移超过配置的阈值，则本地时钟的振铃器可能存在硬件问题。如果问题仍然存在，请联系技术支持以安排更换。
NTSJ	选定时间源抖动	SSM	此值表示本地服务器上的 NTP 用作参考的时间源的可靠性和稳定性。 如果触发警报，则可能表示时间源的振荡器有缺陷，或者与时间源的 WAN 链路出现问题。
Ntlu	NTP 状态	SSM	如果 "NTP Status" 的值未运行，请联系技术支持。
OPST	整体电源状态	SSM	如果 StorageGRID 设备的电源与建议的工作电压不同，则会触发警报。 检查电源 A 或 B 的状态以确定哪个电源运行异常。 如有必要，请更换电源。
OQRT	已隔离对象	LDR	在 StorageGRID 系统自动还原对象后，可以从隔离目录中删除隔离的对象。 1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 2. 选择 * 站点 * > * 存储节点 * > * LDR* > * 验证 * > * 配置 * > * 主 * 。 3. 选择 * 删除隔离的对象 * 。 4. 单击 * 应用更改 * 。 隔离的对象将被删除，计数将重置为零。
ORSU	出站复制状态	BLDR ， BARR	警报指示无法进行出站复制：存储处于无法检索对象的状态。如果手动禁用了出站复制，则会触发警报。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 复制 * > * 配置 * 。 如果 LDR 服务不可用于复制，则会触发警报。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 存储 * 。
OSLF	磁盘架状态	SSM	如果存储设备存储架中某个组件的状态为已降级，则会触发警报。存储架组件包括 IOM ，风扇，电源和驱动器抽盒。如果触发此警报，请参见设备的维护说明。

代码	**Name**	服务	建议的操作
PMEM	服务内存使用量（百分比）	BADC ， BAMS ， BARC ， BCLB ， BCMN ， BLDR ， BNMS ， BSSM ， BDDS	可以具有大于 Y% RAM 的值，其中 Y 表示服务器正在使用的内存百分比。 低于 80% 的数字是正常的。超过 90% 被视为问题。 如果一项服务的内存使用率较高，请监控情况并进行调查。 如果问题仍然存在，请联系技术支持。
PSAS	电源 A 状态	SSM	如果 StorageGRID 设备中的电源 A 与建议的工作电压不同，则会触发警报。 如有必要，请更换电源 A
PSB	电源 B 状态	SSM	如果 StorageGRID 设备中的电源 B 与建议的工作电压不同，则会触发警报。 如有必要，请更换电源 B
RTTE	Tivoli Storage Manager 状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果 Tivoli Storage Manager State 的值为脱机，请检查 Tivoli Storage Manager 状态并解决任何问题。 使组件重新联机。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * ARC* > * 目标 * > * 配置 * > * 主要 * ，选择 * Tivoli Storage Manager State* > * 联机 * ，然后单击 * 应用更改 * 。

代码	**Name**	服务	建议的操作
RDTU	Tivoli Storage Manager 状态	BARC-B	仅适用于目标类型为 Tivoli Storage Manager （ TSM ）的归档节点。 如果 Tivoli Storage Manager 状态的值为配置错误，并且刚刚将归档节点添加到 StorageGRID 系统，请确保已正确配置 TSM 中间件服务器。 如果 Tivoli Storage Manager Status 的值为 Connection Failure 或 Connection Failure ，请重试，请检查 TSM 中间件服务器上的网络配置以及 TSM 中间件服务器和 StorageGRID 系统之间的网络连接。 如果 Tivoli Storage Manager 状态的值为身份验证失败或身份验证失败并重新连接，则 StorageGRID 系统可以连接到 TSM 中间件服务器，但无法对连接进行身份验证。检查 TSM 中间件服务器是否配置了正确的用户，密码和权限，然后重新启动服务。 如果 Tivoli Storage Manager Status 的值为 session failure ，则表示已建立的会话已意外丢失。检查 TSM 中间件服务器与 StorageGRID 系统之间的网络连接。检查中间件服务器是否存在错误。 如果 Tivoli Storage Manager Status 的值为未知错误，请联系技术支持。
RIRF	入站复制—失败	BLDR ， BARR	入站复制—在负载较高或网络临时中断期间，可能会发生故障警报。系统活动减少后，应清除此警报。如果失败的复制计数持续增加，请查找网络问题，并验证源和目标 LDR 以及 ARR 服务是否联机且可用。 要重置计数，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 复制 * > * 配置 * > * 主 * 。选择 * 重置入站复制失败计数 * ，然后单击 * 应用更改 * 。
RIRQ	入站复制—已排队	BLDR ， BARR	在高负载或临时网络中断期间，可能会发生警报。系统活动减少后，应清除此警报。如果排队复制的数量继续增加，请查找网络问题，并验证源和目标 LDR 以及 ARR 服务是否联机且可用。
RORQ	出站复制—已排队	BLDR ， BARR	出站复制队列包含要复制的对象数据，以满足客户端请求的 ILM 规则和对象。 系统过载可能会导致警报。等待系统活动下降时警报是否清除。如果警报再次出现，请通过添加存储节点来添加容量。

代码	**Name**	服务	建议的操作
SAVP	总可用空间（百分比）	LDR	如果可用空间达到较低阈值，则可选择扩展 StorageGRID 系统或通过归档节点将对象数据移动到归档。
SCA	Status	CMN	如果活动网格任务的状态值为错误，请查找网格任务消息。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * CMN* > * 网格任务 * > * 概述 * > * 主 * 。网格任务消息会显示有关此错误的信息（例如， "`check failed on node 12130011` " ）。 调查并更正问题后，重新启动网格任务。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * CMN* > * 网格任务 * > * 配置 * > * 主 * ，然后选择 * 操作 * > * 运行 * 。 如果要中止的网格任务的状态值为错误，请重试中止网格任务。 如果问题仍然存在，请联系技术支持。
SCEP	存储 API 服务端点证书过期	CMN	用于访问存储 API 端点的证书即将过期时触发。 1. 选择 * 配置 * > * 安全性 * > * 证书 * 。 2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。 3. 上传新的 S3 和 Swift API 证书。
SCHR	Status	CMN	如果历史网格任务的状态值已中止，请调查原因并在需要时再次运行此任务。 如果问题仍然存在，请联系技术支持。
SCSA	存储控制器 A	SSM	如果 StorageGRID 设备中存在存储控制器 A 的问题描述 ，则会触发警报。 如有必要，请更换组件。
SCSB	存储控制器 B	SSM	如果 StorageGRID 设备中存在存储控制器 B 的问题描述 ，则会触发警报。 如有必要，请更换组件。 某些设备型号没有存储控制器 B

代码	**Name**	服务	建议的操作
SHLH	运行状况	LDR	如果对象存储的 " 运行状况 " 值为 " 错误 " ，请检查并更正： • 正在挂载的卷出现问题 • 文件系统错误
SLSA	CPU 负载平均值	SSM	值越高，系统就越繁忙。 如果 CPU 负载平均值保持在较高的值，则应调查系统中的事务数，以确定这是否是由于当时的负载过重所致。查看 CPU 负载平均值图表：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 资源 * > * 报告 * > * 图表 * 。 如果系统上的负载不大，但问题仍然存在，请联系技术支持。
SMST	日志监控状态	SSM	如果日志监控状态值在一段时间内未连接，请联系技术支持。
SMTT	事件总数	SSM	如果总事件的值大于零，请检查是否存在已知事件（例如网络故障），这些事件可以是发生原因 。除非清除了这些错误（即，计数已重置为 0 ），否则可以触发事件总数警报。 解决问题描述 后，重置计数器以清除警报。选择 * 节点 * > * 站点 _* > * 网格节点 _* > * 事件 * > * 重置事件计数 * 。 要重置事件计数，您必须具有网格拓扑页面配置权限。 如果事件总数值为零，或者数量增加且问题仍然存在，请联系技术支持。
SNST	Status	CMN	警报表示存储网格任务包时出现问题。如果 " 状态 " 值为 " 检查点错误 " 或 " 未达到仲裁 " ，请确认大多数的 StorageGRID 服务已连接到系统（ 50% 加 1 ），然后等待几分钟。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
SOSS	存储操作系统状态	SSM	如果 SANtricity 软件指示 StorageGRID 设备中存在组件 "`Needs Attention` " 问题描述 ，则会触发警报。 选择 * 节点 * 。然后选择 * 设备存储节点 * > * 硬件 * 。向下滚动以查看每个组件的状态。在 SANtricity 软件中，检查其他设备组件以隔离问题描述 。
SSMA	SSM 状态	SSM	如果 SSM Status 的值为 Error ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * ，然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 概述 * 和 * SSM* > * 概述 * > * 警报 * 以确定警报的发生原因 。 如果问题仍然存在，请联系技术支持。
SSME	SSM 状态	SSM	如果 "SSM State" 的值为 "Standby" ，请继续监控，如果问题仍然存在，请联系技术支持。 如果 "SSM State" 的值为 "Offlin" ，请重新启动此服务。如果问题仍然存在，请联系技术支持。
SST	存储状态	BLDR	如果 "Storage Status" 的值为 "Ininsufficient Available Space" ，则此存储节点上没有更多可用存储，并且数据载入将重定向到其他可用存储节点。可以继续从此网格节点传送检索请求。 应添加更多存储。它不会影响最终用户的功能，但警报会持续存在，直到添加更多存储为止。 如果 "Storage Status" （存储状态）的值为 "Volume Unavailage" （卷不可用），则表示部分存储不可用。无法从这些卷进行存储和检索。有关详细信息，请检查卷的运行状况：选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 存储 * > * 概述 * > * 主 * 。卷的运行状况列在对象存储下。 如果 "Storage Status" 的值为 "Error" ，请联系技术支持。 对存储状态（ SSTS ）警报进行故障排除

代码	**Name**	服务	建议的操作
SVST	Status	SSM	解决与未运行的服务相关的其他警报后，此警报将清除。跟踪源服务警报以还原操作。 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * SSM* > * 服务 * > * 概述 * > * 主 * 。如果某个服务的状态显示为未运行，则其状态为 administratively down 。此服务的状态可能会列为未运行，原因如下： • 已手动停止此服务（` /etc/init.d/<service\> stop` ）。 • 有一个包含 MySQL 数据库的问题描述 ，并且 Server Manager 会关闭 MI 服务。 • 已添加网格节点，但尚未启动。 • 在安装期间，网格节点尚未连接到管理节点。 如果某个服务列为未运行，请重新启动此服务（` /etc/init.d/<service\> restart` ）。 此警报还可能指示存储节点的元数据存储（ Cassandra 数据库）需要重建。 如果问题仍然存在，请联系技术支持。 对服务进行故障排除：状态 - Cassandra （ SVST ）警报进行故障排除
TMEM	已安装内存	SSM	如果节点运行的已安装内存小于 24 GiB ，则可能会导致性能问题和系统不稳定。系统上安装的内存量应至少增加到 24 GiB 。
TPOP	待定操作	模数转换器	消息队列可以指示此 ADA 服务过载。可以连接到 StorageGRID 系统的 ADC 服务太少。在大型部署中，可能需要添加计算资源，或者系统可能需要更多的模数转换服务。
UMEM	可用内存	SSM	如果可用 RAM 较低，请确定这是硬件问题描述 还是软件。如果不是硬件问题描述 ，或者可用内存降至 50 MB 以下（默认警报阈值），请联系技术支持。
VMFI	条目可用	SSM	这表示需要额外存储。请联系技术支持。
VMFR	可用空间	SSM	如果可用空间值过低（请参见警报阈值），则需要调查是否存在超出比例的日志文件，或者对象占用的磁盘空间过多（请参见警报阈值）需要减少或删除。 如果问题仍然存在，请联系技术支持。

代码	**Name**	服务	建议的操作
VMST	Status	SSM	如果挂载的卷的状态值为未知，则会触发警报。如果值为未知或脱机，则表示由于底层存储设备出现问题，无法挂载或访问此卷。
VPRI.	验证优先级	BLDR ， BARR	默认情况下，验证优先级的值为自适应。如果验证优先级设置为高，则会触发警报，因为存储验证可能会减慢服务的正常运行速度。
VSTU	对象验证状态	BLDR	选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 网格节点 _* > * LDR* > * 存储 * > * 概述 * > * 主 * 。 检查操作系统是否存在任何块设备或文件系统错误的迹象。 如果对象验证状态的值为未知错误，则通常表示文件系统或硬件问题（ I/O 错误）级别较低，从而使存储验证任务无法访问存储的内容。请联系技术支持。
XAMS	无法访问审核存储库	BADC ， BARC ， BCLB ， BCMN ， BLDR ， BNMS	检查与托管管理节点的服务器的网络连接。 如果问题仍然存在，请联系技术支持。

生成 **SNMP** 通知的警报（旧系统）

下表列出了生成 SNMP 通知的原有警报。与警报不同，并非所有警报都会生成 SNMP 通知。只有列出的警报才会生成 SNMP 通知，并且严重性仅为指示值或更高。

虽然传统警报系统仍受支持，但警报系统具有显著优势，并且更易于使用。

代码	**Name**	**severity**
ACMS	可用元数据服务	严重
AITE	检索状态	次要
AITU-A	检索状态	major
AMQS	已排队的审核消息	通知
AOTE	存储状态	次要
AOTU	存储状态	major

代码	Name	severity
AROQ	已排队的对象	次要
ARRF	请求失败	major
ARRV	验证失败	major
ARVF	存储故障	major
ASXP	审核共享	次要
AUMA	AMS 状态	次要
AUXS	审核导出状态	次要
BTOF	Offset	通知
CAHP	Java 堆使用量百分比	major
CAQH	可用目标的数量	通知
CASA	数据存储状态	major
CDLP	元数据已用空间（百分比）	major
CLBE	CLB 状态	严重
DNST	DNS 状态	严重
ECST	验证状态	major
HSTE	HTTP 状态	major
HTA	自动启动 HTTP	通知
已丢失	对象丢失	major
分钟	电子邮件通知已排队	通知
分钟	电子邮件通知状态	次要
Nang	网络自动协商设置	通知

代码	Name	severity
NDUP	网络双工设置	次要
NLNK	网络链路检测	次要
NRER	接收错误	通知
NSPD	速度	通知
NTER	传输错误	通知
NTFQ	NTP 频率偏移	次要
NTLK	NTP 锁定	次要
NTOF	NTP 时间偏移	次要
NTSJ	选定时间源抖动	次要
Ntlu	NTP 状态	major
OPST	整体电源状态	major
ORSU	出站复制状态	通知
PSAS	电源 A 状态	major
PSB	电源 B 状态	major
RTTE	Tivoli Storage Manager 状态	通知
RDTU	Tivoli Storage Manager 状态	major
SAVP	总可用空间（百分比）	通知
SHLH	运行状况	通知
SLSA	CPU 负载平均值	通知
SMTT	事件总数	通知
SNST	Status	

代码	Name	severity
SOSS	存储操作系统状态	通知
SST	存储状态	通知
SVST	Status	通知
TMEM	已安装内存	次要
UMEM	可用内存	次要
VMST	Status	次要
VPRI.	验证优先级	通知
VSTU	对象验证状态	通知

日志文件参考

StorageGRID 提供了用于捕获事件，诊断消息和错误情况的日志。系统可能会要求您收集日志文件并将其转发给技术支持以协助进行故障排除。

这些日志分为以下几类：

- StorageGRID 软件日志
- 部署和维护日志
- 第三方软件的日志
- 关于 bycast.log

> 为每种日志类型提供的详细信息仅供参考。这些日志可供技术支持进行高级故障排除。使用审核日志和应用程序日志文件重建问题历史记录的高级技术不在本说明的范围之内。

要访问日志，您可以将日志文件和系统数据作为一个日志文件归档（ * 支持 * > * 工具 * > * 日志 * ）从一个或多个节点收集。或者，如果主管理节点不可用或无法访问特定节点，您可以按如下所示访问每个网格节点的各个日志文件：

1. 输入以下命令： `ssh admin@grid_node_ip`
2. 输入 `passwords.txt` 文件中列出的密码。
3. 输入以下命令切换到 root： `su -`
4. 输入 `passwords.txt` 文件中列出的密码。

StorageGRID 日志文件归档包含为每个类别描述的日志以及包含指标和调试命令输出的其他文件。

归档位置	Description
审核	在正常系统操作期间生成的审核消息。
基础操作系统日志	基本操作系统信息，包括 StorageGRID 映像版本。
捆绑包	全局配置信息（捆绑包）。
Cassandra	Cassandra 数据库信息和 Reaper 修复日志。
EC	按配置文件 ID 显示有关当前节点和 EC 组的 vCSs 信息。
网格	常规网格日志，包括调试（`byncast.log`）和 `servermanager` 日志。
grid.xml	网格配置文件在所有节点之间共享。
hagroup	高可用性组指标和日志。
安装	`Gdu-server` 和安装日志。
lumberjack.log	与日志收集相关的调试消息。
lambda-arbitrator	与 S3 Select 代理请求相关的日志。
指标	Grafana ， Jaeger ，节点导出程序和 Prometheus 的服务日志。
错误	其他访问和错误日志。
MySQL	MariaDB 数据库配置和相关日志。
网络	网络相关脚本和动态 IP 服务生成的日志。
nginx	负载平衡器配置文件和日志。还包括 Grid Manager 和租户管理器流量日志。
nginx 网关	负载平衡器配置文件和日志。
NTP	NTP 配置文件和日志。
os	节点和网格状态文件，包括服务 `pid` 。
其他	` /var/local/log` 下未在其他文件夹中收集的日志文件。
性能	CPU ，网络和磁盘 I/O 的性能信息

归档位置	Description
Prometheus-data	当前 Prometheus 指标（如果日志收集包含 Prometheus 数据）。
配置	与网格配置过程相关的日志。
草稿	来自平台服务中使用的 raft 集群的日志。
SNMP	用于发送 SNMP 通知的 SNMP 代理配置和警报允许 / 拒绝列表。
套接字数据	用于网络调试的套接字数据。
system-commands.txt	StorageGRID 容器命令的输出。包含系统信息，例如网络连接和磁盘使用情况。

相关信息

收集日志文件和系统数据

StorageGRID 软件日志

您可以使用 StorageGRID 日志对问题进行故障排除。

如果要将日志发送到外部系统日志服务器或更改 `byncast.log` 和 `NMS.log` 等审核信息的目标，请参见 配置审核消息和日志目标。

常规 StorageGRID 日志

文件名	注释：	在上找到
` /var/local/log/byncast.log`	主 StorageGRID 故障排除文件。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。	所有节点
` /var/local/log/byncast-err.log`	包含一个子集 `byncast.log` （严重性错误和严重的消息）。系统中也会显示严重消息。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。	所有节点
` /var/local/core/`	包含在程序异常终止时创建的任何核心转储文件。可能的原因包括断言失败，违规或线程超时。 文件 ` /var/local/core/kexec_cmd` 通常位于设备节点上，并不表示存在错误。	所有节点

Server Manager 日志

文件名	注释：	在上找到
` /var/local/log/servermanager.log`	服务器上运行的 Server Manager 应用程序的日志文件。	所有节点
` /var/local/log/GridstatBackend.errlog`	Server Manager GUI 后端应用程序的日志文件。	所有节点
` /var/local/log/gridstat.errlog`	Server Manager 图形用户界面的日志文件。	所有节点

StorageGRID 服务的日志

文件名	注释：	在上找到
` /var/local/log/Acct.errlog`		运行此 ADC 服务的存储节点
` /var/local/log/ADC.errlog`	包含相应服务的标准错误（ stderr ）流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	运行此 ADC 服务的存储节点
` /var/local/log/AMS.errlog`		管理节点
` /var/local/log/arc.errlog`		归档节点
` /var/local/log/Cassandra/system.log`	元数据存储（ Cassandra 数据库）的信息，如果添加新存储节点时出现问题或节点池修复任务停止，则可以使用这些信息。	存储节点
` /var/local/log/Cassandra-reaper.log`	Cassandra Reaper 服务的信息，用于修复 Cassandra 数据库中的数据。	存储节点
` /var/local/log/Cassandra-reaper.errlog`	Cassandra Reaper 服务的错误信息。	存储节点
` /var/local/log/chun.errlog`		存储节点
` /var/local/log/CLB.errlog`	CLB 服务的错误信息。 • 注： * CLB 服务已弃用。	网关节点
` /var/local/log/CMN.errlog`		管理节点

文件名	注释：	在上找到
` /var/local/log/cms.errlog`	此日志文件可能存在于已从旧版 StorageGRID 升级的系统上。它包含旧信息。	存储节点
` /var/local/log/CTS.errlog`	只有当目标类型为 * 云分层 - 简单存储服务（ S3 ） * 时，才会创建此日志文件	归档节点
` /var/local/log/dds.errlog`		存储节点
` /var/local/log/DMV.errlog`		存储节点
` /var/local/log/dynip*`	包含与 dynip 服务相关的日志，该日志可监控网格中的动态 IP 更改并更新本地配置。	所有节点
` /var/local/log/grafana.log`	与 Grafana 服务关联的日志，用于在网格管理器中显示指标。	管理节点
` /var/local/log/hagroups.log`	与高可用性组关联的日志。	管理节点和网关节点
` /var/local/log/hagroup_events.log`	跟踪状态更改，例如从备份过渡到主节点或故障。	管理节点和网关节点
` /var/local/log/idnt.errlog`		运行此 ADC 服务的存储节点
` /var/local/log/jaeger.log`	与 jaeger 服务关联的日志，用于收集跟踪。	所有节点
` /var/local/log/kstn.errlog`		运行此 ADC 服务的存储节点
` /var/local/log/lambda/*`	包含 S3 Select 服务的日志。	管理节点和网关节点 只有某些管理节点和网关节点才包含此日志。请参见 S3 Select 管理节点和网关节点的要求和限制。
` /var/local/log/LDer.errlog`		存储节点

文件名	注释：	在上找到
` /var/local/log/miscd/* 。 log`	包含 MISCd 服务（信息服务控制守护进程）的日志，此服务提供一个界面，用于查询和管理其他节点上的服务以及管理节点上的环境配置，例如查询其他节点上运行的服务的状态。	所有节点
` /var/local/log/nginx/* 。 log`	包含 nginx 服务的日志，此服务可充当各种网格服务（例如 Prometheus 和动态 IP ）的身份验证和安全通信机制，以便能够通过 HTTPS API 与其他节点上的服务进行通信。	所有节点
` /var/local/log/nginx gw/* 。 log`	包含管理节点上受限管理端口和负载平衡器服务的日志，该服务可对从客户端到存储节点的 S3 和 Swift 流量进行负载平衡。	管理节点和网关节点
` /var/local/log/persistence *`	包含永久性服务的日志，该服务用于管理根磁盘上需要在重新启动后持续存在的文件。	所有节点
` /var/local/log/Prometheus.log`	对于所有节点，包含节点导出程序服务日志和 ade-exporter指标 服务日志。 对于管理节点，还包含 Prometheus 和警报管理器服务的日志。	所有节点
` /var/local/log/raf.log`	包含用于 raft 协议的 RSM 服务所使用的库的输出。	具有 RSM 服务的存储节点
` /var/local/log/rms.errlog`	包含用于 S3 平台服务的复制状态机服务（ RSM ）服务的日志。	具有 RSM 服务的存储节点
` /var/local/log/sSM.errlog`		所有节点
` /var/local/log/update-s3vs-domains.log`	包含与处理 S3 虚拟托管域名配置的更新相关的日志。请参见实施 S3 客户端应用程序的说明。	管理节点和网关节点
` /var/local/log/update-snmp-firewall.*`	包含与为 SNMP 管理的防火墙端口相关的日志。	所有节点
` /var/local/log/update-sysl.log`	包含与对系统系统系统日志配置所做更改相关的日志。	所有节点

文件名	注释：	在上找到
` /var/local/log/update-traffic 类 .log`	包含与流量分类器配置更改相关的日志。	管理节点和网关节点
` /var/local/log/update-utcn/log`	包含与此节点上的不可信客户端网络模式相关的日志。	所有节点

NMS 日志

文件名	注释：	在上找到
` /var/local/log/NMS.log`	• 从网格管理器和租户管理器捕获通知。 • 捕获与 NMS 服务运行相关的事件，例如警报处理，电子邮件通知和配置更改。 • 包含因系统中的配置更改而导致的 XML 包更新。 • 包含与每天执行一次的属性缩减采样相关的错误消息。 • 包含 Java Web 服务器错误消息，例如页面生成错误和 HTTP 状态 500 错误。	管理节点
` /var/local/log/NMS.errlog`	包含与 MySQL 数据库升级相关的错误消息。 包含相应服务的标准错误（ stderr ）流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	管理节点
` /var/local/log/nms.requestlog`	包含有关从管理 API 到内部 StorageGRID 服务的传出连接的信息。	管理节点

相关信息

关于 bycast.log

使用 S3

部署和维护日志

您可以使用部署和维护日志对问题进行故障排除。

文件名	注释：	在上找到
` /var/local/log/install.log`	在软件安装期间创建。包含安装事件的记录。	所有节点

文件名	注释：	在上找到
` /var/local/log/expand-progress.log`	在扩展操作期间创建。包含扩展事件的记录。	存储节点
` /var/local/log/gdu-server.log`	由 GDU 服务创建。包含与主管理节点管理的配置和维护过程相关的事件。	主管理节点
` /var/local/log/send_admin_hw.log`	在安装期间创建。包含与节点与主管理节点的通信相关的调试信息。	所有节点
` /var/local/log/upgrade.log`	在软件升级期间创建。包含软件更新事件的记录。	所有节点

第三方软件的日志

您可以使用第三方软件日志对问题进行故障排除。

类别	文件名	注释：	在上找到
归档	/var/local/log/dsierror.log	TSM 客户端 API 的错误信息。	归档节点
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	MySQL 生成的日志文件。 文件 `mysql.err` 可捕获数据库错误和事件，例如启动和关闭。 文件 `mysql-slow.log` （查询日志较慢）可捕获执行时间超过 10 秒的 SQL 语句。	管理节点
操作系统	/var/local/log/messages	此目录包含操作系统的日志文件。这些日志中包含的错误也会显示在网格管理器中。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 拓扑 * > * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。	所有节点
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntstats	` /var/local/log/ntp.log` 包含 NTP 错误消息的日志文件。 ` /var/lib/ntp/var/log/ntpstats /` 目录包含 NTP 时间统计信息。 `loopstats` 记录环路筛选器统计信息。 `peerstats` 记录对等统计信息。	所有节点

类别	文件名	注释：	在上找到
SAMBA	/var/local/log/samba/	Samba 日志目录包含每个 Samba 进程（ SMB， nmb 和 winbind ）以及每个客户端主机名 /IP 的日志文件。	已配置管理节点，用于通过 CIFS 导出审核共享

关于 bycast.log

文件 ` /var/local/log/byncast.log` 是 StorageGRID 软件的主要故障排除文件。每个网格节点都有一个 `byncast.log` 文件。该文件包含特定于该网格节点的消息。

文件 ` /var/local/log/byncast-err.log` 是 `byncast.log` 的子集。它包含严重性错误和严重的消息。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

bycast.log 的文件轮换

当 `byncast.log` 文件达到 1 GB 时，将保存现有文件并启动新的日志文件。

保存的文件将重命名为 `byncast.log.1` ，新文件名为 `byncast.log` 。当新的 `byncast.log` 达到 1 GB 时， `byncast.log.1` 将重命名并压缩为 `byncast.log.2.gz` ，而 `byncast.log` 将重命名为 `byncast.log.1` 。

`byncast.log` 的轮换限制为 21 个文件。创建 `byncast.log` 文件的第 22 个版本时，将删除最旧的文件。

`byncast-err.log` 的轮换限制为七个文件。

> 如果日志文件已被压缩，则不能将其解压缩到写入该文件的同一位置。将文件解压缩到同一位置可能会干扰日志轮换脚本。

您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

相关信息

收集日志文件和系统数据

bycast.log 中的消息

`byncast.log` 中的消息由 ADE （异步分布式环境）写入。ADE 是每个网格节点的服务所使用的运行时环境。

ADE 消息示例：

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE 消息包含以下信息：

消息段	示例中的值
节点 ID	12455685
ADE 进程 ID	0357819531
模块名称	SVMR
消息标识符	EVHR
UTC 系统时间	2019-05-05T27T17： 10： 29.784677 （YYYY-MM-DDTHH： MM： SS.uuuuu ）
严重性级别	error
内部跟踪编号	0906
message	SVMR： 卷 3 的运行状况检查失败，原因为 "Tut"

bycast.log 中的消息严重性

已为 `byncast.log` 中的消息分配严重性级别。

例如：

- * 通知 * —发生了应记录的事件。大多数日志消息都处于此级别。
- * 警告 * - 发生意外情况。
- * 错误 * —发生了一个会影响操作的重大错误。
- * 严重 * —发生异常情况，导致正常操作停止。您应立即解决基本情况。网格管理器中也会显示严重消息。选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后选择 * 站点 * > * 节点 * > * SSM* > * 事件 * 。

中的错误代码 `bycast.log`

`byncast.log` 中的大多数错误消息都包含错误代码。

下表列出了 `byncast.log` 中的常见非数字代码。非数字代码的确切含义取决于报告该代码的上下文。

错误代码	含义
SUC	无错误
GERR	未知

错误代码	含义
已完成	已取消
异常	已中止
输出	超时
调用	无效
NFND	未找到
服务器	version
配置	Configuration
失败	失败
ICPL	未完成
完成	完成
SUNV	服务不可用

下表列出了 `byncast.log` 中的数字错误代码。

错误编号	错误代码	含义
001	EPERM	不允许执行此操作
002	已执行	没有此类文件或目录
003	ESRCH	无此过程
004	EINTR	系统调用中断
005.	EIO	I/O 错误
006	ENXIO	没有此类设备或地址
007	E2BIG	参数列表太长
008	ENOExec	Exec 格式错误

错误编号	错误代码	含义
009.	EBADF	文件编号错误
010	ECHILD	无子进程
011	EAGAIN	请重试
012	ENOMEM	内存不足
013	EACCE	权限被拒绝
014	默认	地址错误
015	ENOTBLK	需要块设备
016	EBUSY	设备或资源繁忙
017	EEXIST	文件已存在
018	EXDEV	跨设备链路
019	ENODEV	没有此类设备
020	ENOTDIR	不是目录
21	EISDIR	是一个目录
0222	EINVAL	参数无效
023	ENFILE	文件表溢出
024	EMFILE	打开的文件过多
025	ENOTTY	不是一种打字机
026	ETXTBSY	文本文件繁忙
027	EFBIG	文件太大
028	ENOSPC	设备上没有剩余空间
029	ESPIPE	非法寻道

错误编号	错误代码	含义
030	EROFS	只读文件系统
0331	EMLINK	链路太多
032	EPIPE	管道已断开
033	以登	数学参数不在功能域中
034	电子书	数学结果不可代表
035	EDEADLK	可能会发生资源死锁
036	ENAMETOOLONG	文件名太长
037	ENOLCK	没有可用的记录锁定
038	ENOSYS	未实施功能
039	ENOTEMPTY	目录不为空
40	ELOOP	遇到的符号链接太多
041		
042	ENOMSG	没有所需类型的消息
043	EIDRM	已删除标识符
044	ECHRNG	通道编号超出范围
045	EL2NSync	2 级未同步
046	EL3HLT	3 级已暂停
047	EL3RST	3 级重置
048	ELNRNG	链路编号超出范围
049	EUNATCH	未连接协议驱动程序
050	ENOCSI	没有可用的 CSI 结构

错误编号	错误代码	含义
051	EL2HLT	级别 2 已暂停
052	EBADE	交换无效
053	EBADR	请求描述符无效
054	EXFULL	Exchange 已满
055	ENOANO	无阳极
056	EBADRQC	请求代码无效
057	EBADLT	插槽无效
058		
059	EBFNT	字体文件格式错误
060	ENOSTR	设备不是流
061	ENODATA	无可用数据
062	时间	计时器已过期
063	ENOSR	流资源不足
064	ENONET	计算机不在网络上
065	ENOPK	未安装软件包
066	EREMOTE	对象为远程对象
067	ENOLINK	链路已切断
068	EADV	公布错误
069	ESRMNT	Srmount 错误
070	eComm	发送时出现通信错误
071	EPROTO	协议错误

错误编号	错误代码	含义
072	EMULTIHOP	已尝试多跃点
073	EDOTDOT	RFS 专用错误
074	EBADMSG	不是数据消息
075	超越	对于定义的数据类型，值太大
076	ENOTUNIQ	名称在网络上不唯一
077	EBADFD	文件描述符处于错误状态
078	错误	已更改远程地址
079	EIBAcc	无法访问所需的共享库
080	EIBBAD	访问损坏的共享库
081	ELIBSCN	
082	ELIBMAX	正在尝试链接过多的共享库
083	ELIBExec	无法直接执行共享库
084	EILSEQ	字节序列非法
085	错误	应重新启动中断的系统调用
086	ESTRPIPE	流管道错误
087	EUSERs.	用户过多
088	ENOTSOCK	在非套接字上执行套接字操作
089	EDESTADDRREQ	目标地址为必填项
090	EMSSIZE	消息太长
091	EPROTOTYPE	套接字的协议类型错误
092	ENOPROTOOPT	协议不可用

错误编号	错误代码	含义
093	产品说明	不支持协议
094	ESOCKTNOSUPPORT	不支持套接字类型
095	EOPNOTSUPP	传输端点上不支持此操作
096	EPFNOSUPPORT	不支持协议系列
097	EAFNOSUPPORT	协议不支持地址系列
098	EADDRINUSE	地址已在使用中
099	EADDRNOTAVAIL	无法分配请求的地址
100	ENETDOWN	网络已关闭
101.	ENETUNREACH	无法访问网络
102.	ENETRESET	由于重置，网络已断开连接
103.	已完成	软件导致连接中止
104	ECONNRESET	对等方重置连接
105.	ENOBUFS	无可用缓冲区空间
106.	EISCONN	传输端点已连接
107.	ENOTCONN	传输端点未连接
108.	ESHUTDOWN	传输端点关闭后无法发送
109.	ETOOMANYREFS	引用过多：无法接合
110	ETIMEDOUT	连接超时
111.	ECONNREFUSED	连接被拒绝
112	EHOSTDOWN	主机已关闭
113	EHOSTUNREACH	没有到主机的路由

错误编号	错误代码	含义
114	EALREADY	操作已在进行中
115	EINPROGRESS	操作正在进行中
116		
117	EUC	结构需要清理
118	ENOTCAM	不是名为 type 的 Xenix 文件
119	ENAVAIL	没有可用的 Xenix 信号
120	EISNAM	是一个命名类型的文件
121.	EREMOTEIO	远程 I/O 错误
122.	EDQUOT	已超过配额
123.	ENOMINDIUM	未找到介质
124.	EMeduMTYPE	介质类型错误
125.	ECANCELED	操作已取消
126.	ENOKEY	所需密钥不可用
127.	EKEYEXPIRED	密钥已过期
128.	EKBREVOKED	密钥已撤销
129.	已完成	密钥已被服务拒绝
130	终止	对于稳定可靠的 mMutexes： owner died
131.	ENOTRECOVERABLE	对于强大的 mutexes：状态不可恢复

扩展网格

扩展网格：概述

按照以下说明扩展 StorageGRID 系统的容量或功能，而不会中断系统操作。

关于这些说明

以下说明介绍如何执行 StorageGRID 扩展，以便向存储节点，现有站点或整个新站点添加新网格节点。

本说明适用于安装 StorageGRID 系统后负责配置和支持该系统的技术人员。

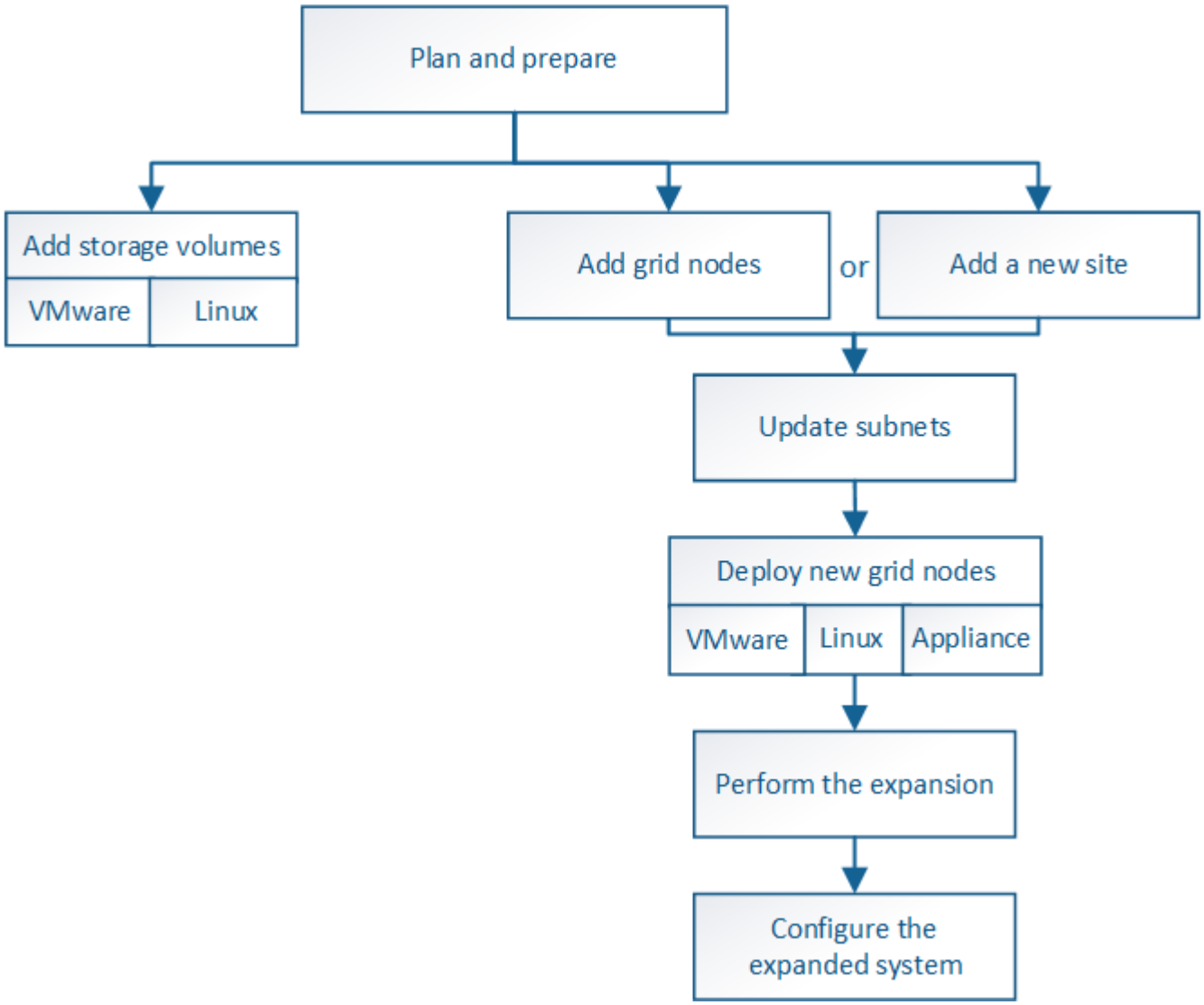
扩展操作步骤 概述

执行扩展的原因决定了您必须添加的每种类型的新节点数以及这些新节点的位置。例如，如果要执行扩展以增加存储容量，添加元数据容量或添加冗余或新功能，则节点要求会有所不同。

如工作流图所示，执行扩展的步骤取决于是向存储节点添加存储卷，向现有站点添加新节点还是添加新站点。无论哪种情况，您都可以在不中断当前系统运行的情况下执行扩展。

添加节点的步骤还取决于您是添加 StorageGRID 设备还是添加运行 VMware 或 Linux 的主机。

"`Linux`" 是指 Red Hat ® Enterprise Linux ® ， Ubuntu ® ， CentOS 或 Debian ® 部署。使用 "NetApp 互操作性表工具（ IMT ）" 以获取支持的版本列表。



规划 StorageGRID 扩展

添加存储容量

添加对象容量的准则

您可以通过向现有存储节点添加存储卷或向现有站点添加新存储节点来扩展 StorageGRID 系统的对象存储容量。添加存储容量时，必须满足信息生命周期管理（ ILM ）策略的要求。

添加存储卷的准则

在将存储卷添加到现有存储节点之前，请查看以下准则和限制：

- 您必须检查当前的 ILM 规则，以确定在何处以及何时添加存储卷以增加可用于复制或擦除编码对象的存储。请参见的说明 通过信息生命周期管理管理对象。
- 您不能通过添加存储卷来增加系统的元数据容量，因为对象元数据仅存储在卷 0 上。
- 每个基于软件的存储节点最多可支持 16 个存储卷。如果您需要添加的容量超出此范围，则必须添加新的存储节点。
- 您可以向每个SG6060或SG6060X设备添加一个或两个扩展架。每个扩展架可添加 16 个存储卷。如果安装了这两个扩展架、则SG6060和SG6060X每个扩展架总共可支持48个存储卷。
- 您不能将存储卷添加到任何其他存储设备。
- 您不能增加现有存储卷的大小。
- 您不能在执行系统升级，恢复操作或其他扩展的同时向存储节点添加存储卷。

在决定添加存储卷并确定必须扩展哪些存储节点以满足 ILM 策略后，请按照适用于您的存储节点类型的说明进行操作：

- 要向SG6060或SG60X存储设备添加一个或两个扩展架、请转至 将扩展架添加到已部署的SG6060或SG60X。
- 对于基于软件的节点，请按照的说明进行操作将存储卷添加到存储节点。

添加存储节点的准则

在将存储节点添加到现有站点之前，请查看以下准则和限制：

- 您必须检查当前的 ILM 规则，以确定在何处以及何时添加存储节点以增加可用于复制或擦除编码对象的存储。请参见的说明 通过信息生命周期管理管理对象。
- 在一个扩展操作步骤 中添加的存储节点不应超过 10 个。
- 您可以在一个扩展操作步骤 中将存储节点添加到多个站点。
- 您可以在一个扩展操作步骤 中添加存储节点和其他类型的节点。
- 在启动扩展操作步骤 之前，您必须确认在恢复过程中执行的所有数据修复操作均已完成。请参见 检查数据修复作业。
- 如果在执行扩展之前或之后需要删除存储节点，则在一个 " 停用节点 " 操作步骤 中停用的存储节点不应超过 10 个。

存储节点上的模块转换服务准则

配置扩展时，必须选择是否在每个新存储节点上包含管理域控制器（ADA）服务。此 ADA 服务可跟踪网格服务的位置和可用性。

- StorageGRID 系统需要 ADC 服务的仲裁 可在每个站点和任何时间使用。
- 每个站点至少有三个存储节点必须包含此 ADC-Service 。
- 不建议将此 ADA 服务添加到每个存储节点。包含过多的 ADC 服务可能会因节点间通信量增加而导致发生原因 速度变慢。
- 一个网格中包含的存储节点不应超过 48 个，而是使用了此 ADA 服务。这相当于 16 个站点，每个站点有三个模块转换服务。
- 通常，在为新节点选择 * 数字转换服务 * 设置时，应选择 * 自动 * 。仅当新节点将替换包含此 ADC-Service 的另一个存储节点时，才选择 * 是 * 。由于如果仍会保留的 ADD 服务太少，则无法停用存储节点，因此，这样可以确保在删除旧服务之前新的 ADD 服务可用。
- 在部署此节点后，您不能将此 ADC 服务添加到该节点中。

为复制的对象添加存储容量

如果您的部署的信息生命周期管理（ ILM ）策略包含一条规则，用于创建对象的复制副本，则必须考虑要添加的存储容量以及要添加新存储卷或存储节点的位置。

有关在何处添加额外存储的指导，请查看创建复制副本的 ILM 规则。如果 ILM 规则创建两个或更多对象副本，请计划在创建对象副本的每个位置添加存储。例如，如果您有一个双站点网格和一个 ILM 规则，在每个站点创建一个对象副本，则必须向每个站点添加存储，以增加网格的整体对象容量。请参见的说明 通过信息生命周期管理管理对象。

出于性能原因，您应尝试在各个站点之间保持存储容量和计算能力的平衡。因此，在此示例中，您应向每个站点添加相同数量的存储节点或在每个站点添加更多存储卷。

如果您的 ILM 策略更加复杂，其中包括根据存储分段名称等标准将对象放置在不同位置的规则，或者随着时间的推移更改对象位置的规则，则您对扩展所需存储位置的分析将类似，但更为复杂。

绘制整体存储容量的消耗速度图表有助于您了解要在扩展中添加多少存储以及何时需要额外存储空间。您可以使用网格管理器监控和绘制存储容量图表，如的说明所述 监控 StorageGRID 并对其进行故障排除。

在规划扩展的时间时，请务必考虑购买和安装额外存储可能需要多长时间。

为经过纠删编码的对象添加存储容量

如果 ILM 策略包含创建纠删编码副本的规则，则必须计划在何处添加新存储以及何时添加新存储。您添加的存储量和添加的时间可能会影响网格的可用存储容量。

规划存储扩展的第一步是，检查 ILM 策略中用于创建纠删编码对象的规则。由于 StorageGRID 会为每个纠删编码对象创建 *k+m_fragments* ，并将每个片段存储在不同的存储节点上，因此您必须确保在扩展后至少 *_k+m* 存储节点具有用于存储新纠删编码数据的空间。如果纠删编码配置文件提供站点丢失保护，则必须向每个站点添加存储。请参见 使用 ILM 管理对象。

您需要添加的节点数还取决于执行扩展时现有节点的容量。

有关为经过纠删编码的对象添加存储容量的一般建议

如果要避免详细计算，可以在现有存储节点容量达到 70% 时为每个站点添加两个存储节点。

对于单站点网格和纠删编码可提供站点丢失保护的网格，此一般建议可在多种纠删编码方案中提供合理的结果。

要更好地了解导致此建议的因素或为您的站点制定更精确的计划，请查看下一节。有关针对您的情况优化的自定义建议，请联系您的 NetApp 客户代表。

计算要为擦除编码对象添加的扩展存储节点数

要优化存储纠删编码对象的部署扩展方式，您必须考虑许多因素：

- 正在使用纠删编码方案
- 用于纠删编码的存储池的特征，包括每个站点上的节点数和每个节点上的可用空间量
- 网格之前是否已扩展（因为每个存储节点上的可用空间量可能并非所有节点上的大致相同）
- ILM 策略的确切性质，例如 ILM 规则是否同时创建复制的对象和经过纠删编码的对象

以下示例可帮助您了解纠删编码方案的影响，存储池中的节点数以及每个节点上的可用空间量。

类似的注意事项会影响存储复制数据和纠删编码数据的 ILM 策略的计算以及先前扩展的网格的计算。

> 本节中的示例介绍了向 StorageGRID 系统添加存储容量的最佳实践。如果无法添加建议的节点数，则可能需要运行 EC 重新平衡操作步骤 ，以便存储其他经过纠删编码的对象。请参见 重新平衡经过纠删编码的数据。

示例 **1** ： 扩展使用 **2+1** 纠删编码的单站点网格

此示例显示了如何扩展仅包含三个存储节点的简单网格。

> 为了简单起见，此示例仅使用三个存储节点。但是，不建议仅使用三个存储节点：实际生产网格应至少使用 *k*+*m* + 1 个存储节点来实现冗余，此值等于本示例中的四个存储节点（ 2+1+1 ）。

假设满足以下条件：

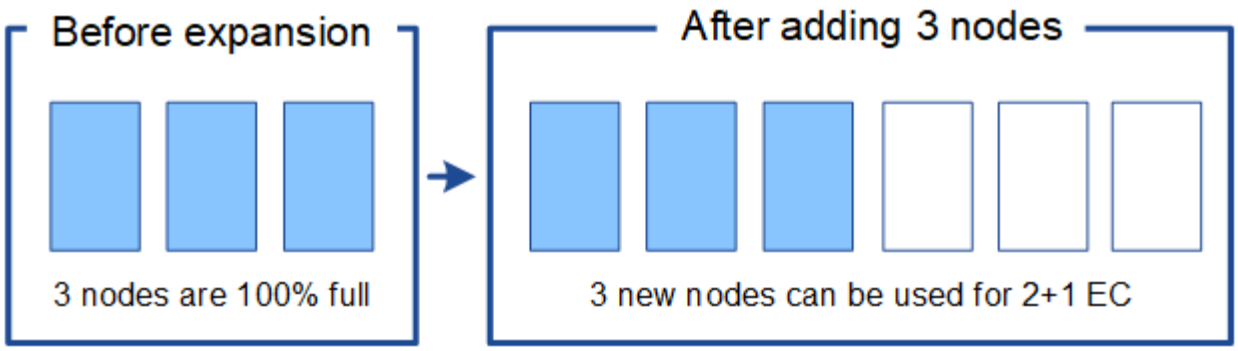
- 所有数据均使用 2+1 纠删编码方案进行存储。使用 2+1 纠删编码方案时，每个对象都存储为三个片段，每个片段保存在不同的存储节点上。
- 您有一个站点包含三个存储节点。每个存储节点的总容量为 100 TB 。
- 要通过添加新的 100 TB 存储节点进行扩展。
- 您希望最终在新旧节点之间平衡经过纠删编码的数据。

根据执行扩展时存储节点的容量，您可以选择多种方法。

- * 如果现有节点已满，请添加三个 100 TB 存储节点 *

  在此示例中，现有节点已满 100% 。由于没有可用容量，您必须立即添加三个节点以继续 2+1 纠删编码。

  扩展完成后，对对象进行纠删编码后，所有片段都将放置在新节点上。

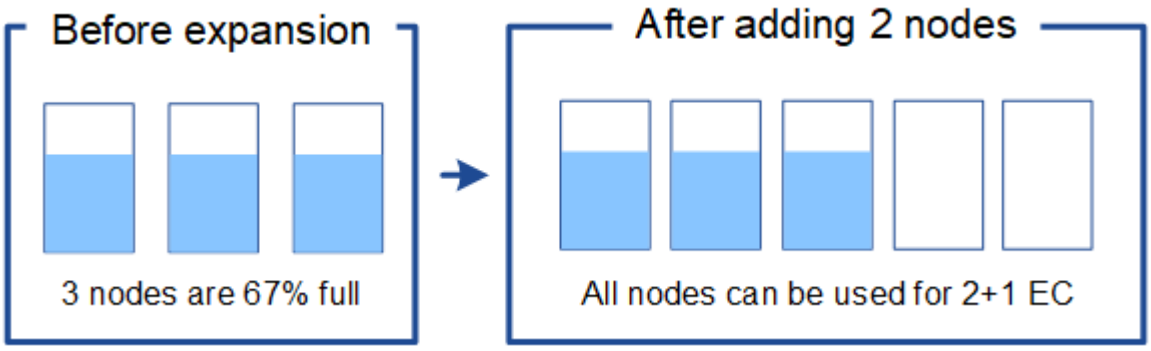


此扩展可添加 _k+m_nodes 。为实现冗余，建议添加四个节点。如果在现有节点已满 100% 时仅添加 _k+m_expansion Storage Node ，则所有新对象都会存储在扩展节点上。如果任何新节点变得不可用，即使是暂时不可用， StorageGRID 也无法满足 ILM 要求。

- * 如果现有存储节点已满 67% ，请添加两个 100 TB 存储节点 *

  在此示例中，现有节点已满 67% 。由于现有节点上有 100 TB 的可用容量（每个节点 33 TB ），因此，如果您现在执行扩展，则只需添加两个节点。

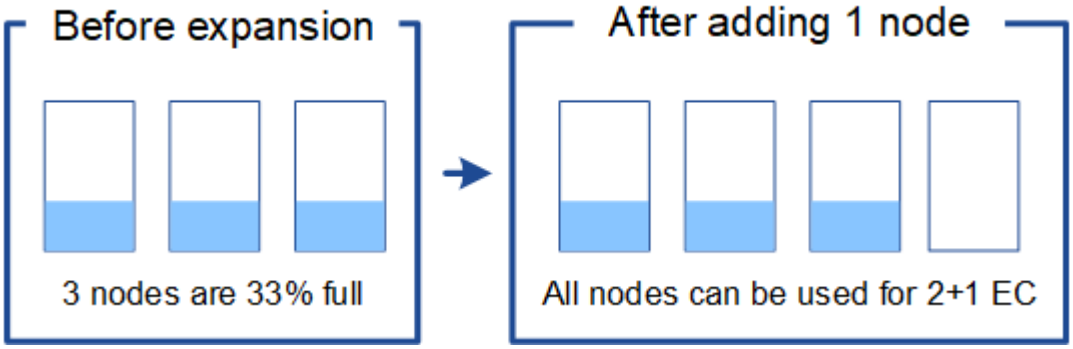
  添加 200 TB 的额外容量后，您可以继续 2+1 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。



- * 如果现有存储节点已满 33% ，请添加一个 100 TB 存储节点 *

  在此示例中，现有节点已满 33% 。由于现有节点上有 200 TB 的可用容量（每个节点 67 TB ），因此，如果您现在执行扩展，则只需要添加一个节点。

  添加 100 TB 的额外容量后，您可以继续 2+1 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。



示例 **2** ： 扩展使用 **6+3** 纠删编码的三站点网格

此示例显示了如何为多站点网格制定扩展计划，该网格采用的纠删编码方案包含更多片段。尽管这些示例之间存在差异，但建议的扩展计划非常相似。

假设满足以下条件：

- 所有数据均使用 6+3 纠删编码方案进行存储。使用 6+3 纠删编码方案时，每个对象将存储为 9 个片段，每个片段将保存到不同的存储节点。
- 您有三个站点，每个站点有四个存储节点（共 12 个节点）。每个节点的总容量为 100 TB 。
- 要通过添加新的 100 TB 存储节点进行扩展。
- 您希望最终在新旧节点之间平衡经过纠删编码的数据。

根据执行扩展时存储节点的容量，您可以选择多种方法。

- * 如果现有节点已满，请添加九个 100 TB 存储节点（每个站点三个） *

  在此示例中， 12 个现有节点已满。由于没有可用容量，您必须立即添加九个节点（ 900 TB 的额外容量），才能继续 6+3 纠删编码。

  扩展完成后，对对象进行纠删编码后，所有片段都将放置在新节点上。

  > 此扩展可添加 _k+m_nodes 。为了实现冗余，建议添加 12 个节点（每个站点四个）。如果在现有节点已满 100% 时仅添加 _k+m_expansion Storage Node ，则所有新对象都会存储在扩展节点上。如果任何新节点变得不可用，即使是暂时不可用， StorageGRID 也无法满足 ILM 要求。

- * 如果现有节点已满 75% ，请添加六个 100 TB 存储节点（每个站点两个） *

  在此示例中， 12 个现有节点已满 75% 。由于可用容量为 300 TB （每个节点 25 TB ），因此，如果您现在执行扩展，则只需添加六个节点。您应向这三个站点中的每个站点添加两个节点。

  添加 600 TB 的存储容量后，您可以继续 6+3 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。

- * 如果现有节点已满 50% ，请添加三个 100 TB 存储节点（每个站点一个） *

  在此示例中， 12 个现有节点已满 50% 。由于可用容量为 600 TB （每个节点 50 TB ），因此，如果您现在执行扩展，则只需添加三个节点。您应向这三个站点中的每个站点添加一个节点。

  添加 300 TB 的存储容量后，您可以继续 6+3 纠删编码，并最终在所有节点之间平衡经过纠删编码的数据。

重新平衡经过纠删编码的数据的注意事项

如果要执行扩展以添加存储节点，并且 ILM 策略包含一个或多个用于擦除代码数据的 ILM 规则，则可能需要在扩展完成后执行 EC 重新平衡操作步骤 。

例如，如果您无法为所使用的纠删编码方案添加建议数量的存储节点，则可能需要运行 EC 重新平衡操作步骤以存储其他经过纠删编码的对象。

查看这些注意事项后，请执行扩展，然后转到 添加存储节点后重新平衡经过纠删编码的数据 以运行操作步骤 。

什么是 **EC** 重新平衡?

EC 重新平衡是扩展存储节点后可能需要的 StorageGRID 操作步骤 。操作步骤 将作为主管理节点上的命令行脚本运行。运行 EC 重新平衡操作步骤 时， StorageGRID 会在站点的现有存储节点和新扩展的存储节点之间重新分布经过擦除编码的片段。

EC 重新平衡操作步骤 ：

- 仅移动经过纠删编码的对象数据。它不会移动复制的对象数据。
- 在站点内重新分布数据。它不会在站点之间移动数据。
- 在站点的所有存储节点之间重新分布数据。它不会在存储卷中重新分配数据。
- 在确定从何处移动经过纠删编码的数据时，不会考虑每个存储节点上的复制数据使用情况

完成 EC 重新平衡操作步骤 后：

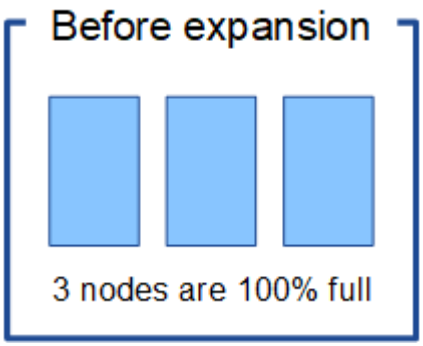
- 经过纠删编码的数据会从可用空间较少的存储节点移至可用空间较多的存储节点。
- 由于 EC 重新平衡操作步骤 不会移动复制的对象副本，因此存储节点之间的已用（ % ）值可能会保持不同。
- 擦除编码对象的数据保护将保持不变。

当 EC 重新平衡操作步骤 运行时， ILM 操作以及 S3 和 Swift 客户端操作的性能可能会受到影响。因此，您只能在有限情况下执行此操作步骤 。

何时不执行 **EC** 重新平衡

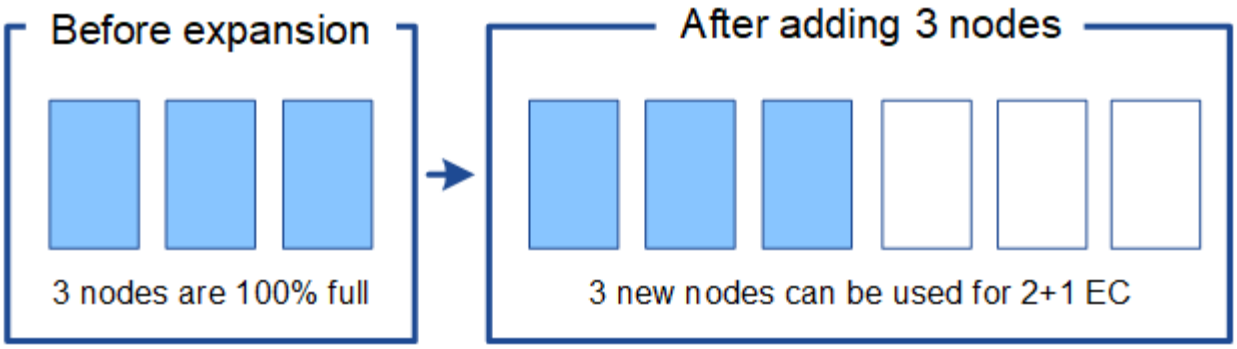
例如，当您不需要执行 EC 重新平衡时，请考虑以下几点：

- StorageGRID 正在一个站点上运行，该站点包含三个存储节点。
- ILM 策略对大于 1.0 MB 的所有对象使用 2+1 擦除编码规则，对较小的对象使用双副本复制规则。
- 所有存储节点均已完全满，并且已在主要严重性级别触发 * 对象存储空间不足 * 警报。建议执行扩展操作步骤 以添加存储节点。



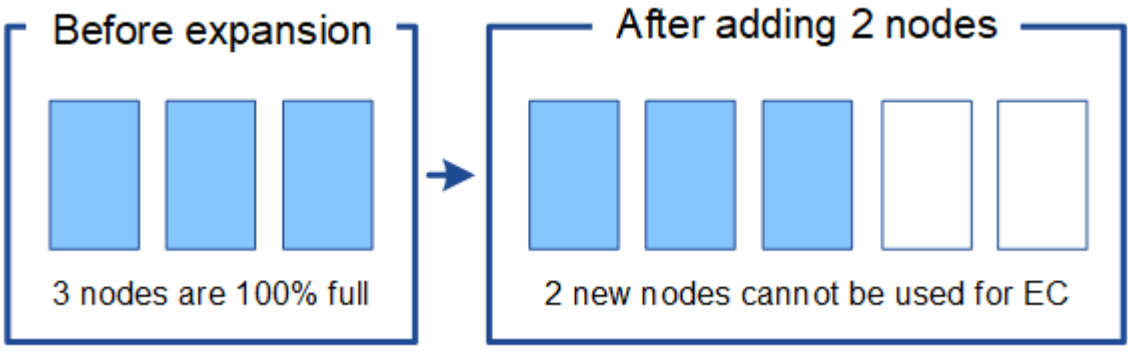
要在此示例中扩展站点，建议您添加三个或更多新的存储节点。StorageGRID 需要三个存储节点来执行 2+1 纠删编码，以便可以将两个数据片段和一个奇偶校验片段放置在不同的节点上。

添加三个存储节点后，原始存储节点将保持全满状态，但可以继续将对象载入新节点上的 2+1 纠删编码方案中。在这种情况下，不建议运行 EC 重新平衡操作步骤 ： 运行操作步骤 将暂时降低性能，这可能会影响客户端操作。

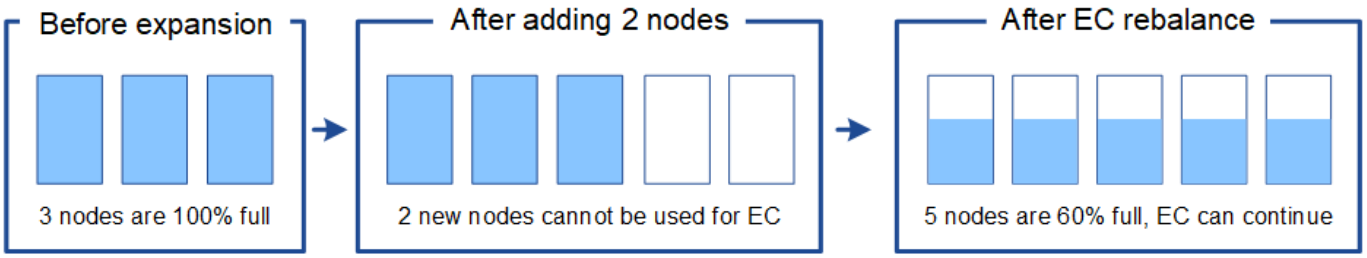


何时执行 **EC** 重新平衡

例如，您应在何时执行 EC 重新平衡操作步骤 ，请考虑相同的示例，但假定您只能添加两个存储节点。由于 2+1 纠删编码至少需要三个存储节点，因此新节点不能用于纠删编码的数据。



要解析此问题描述 并使用新的存储节点，您可以运行 EC 重新平衡操作步骤 。运行此操作步骤 时，StorageGRID 会在站点的所有存储节点之间重新分发经过纠删编码的数据和奇偶校验片段。在此示例中，当 EC 重新平衡操作步骤 完成后，所有五个节点的容量现在仅为 60% ，并且可以继续将对象载入所有存储节点上的 2+1 纠删编码方案。



EC 重新平衡的要求

通常，您只能在有限情况下运行 EC 重新平衡操作步骤 。具体而言，只有在以下所有陈述均正确的情况下，才应执行 EC 重新平衡：

- 您可以对对象数据使用纠删编码。
- 已针对站点上的一个或多个存储节点触发 * 对象存储空间不足 * 警报，表示这些节点已满 80% 或以上。
- 您无法为正在使用的纠删编码方案添加建议数量的新存储节点。请参见 为经过纠删编码的对象添加存储容量。
- 当 EC 重新平衡操作步骤 正在运行时， S3 和 Swift 客户端的写入和读取操作可以容忍较低的性能。

EC 重新平衡操作步骤 如何与其他维护任务进行交互

您不能在运行 EC 重新平衡操作步骤 的同时执行某些维护过程。

操作步骤	在 **EC** 重新平衡操作步骤 期间是否允许?
其他 EC 重新平衡过程	否 一次只能运行一个 EC 重新平衡操作步骤 。
停用操作步骤 EC 数据修复作业	否 • 在 EC 重新平衡操作步骤 运行期间，系统会阻止您启动停用操作步骤或 EC 数据修复。 • 在存储节点停用操作步骤 操作步骤 或 EC 数据修复正在运行时，系统会阻止您启动 EC 重新平衡。
扩展操作步骤	否 如果需要在扩展中添加新的存储节点，应等待运行 EC 重新平衡操作步骤，直到添加完所有新节点为止。如果在添加新存储节点时正在进行 EC 重新平衡操作步骤 ，则不会将数据移动到这些节点。
升级操作步骤	否 如果需要升级 StorageGRID 软件，应在运行 EC 重新平衡操作步骤 之前或之后执行升级操作步骤 。您可以根据需要终止 EC 重新平衡操作步骤以执行软件升级。
设备节点克隆操作步骤	否 如果需要克隆设备存储节点，应等待运行 EC 重新平衡操作步骤 ，直到添加新节点为止。如果在添加新存储节点时正在进行 EC 重新平衡操作步骤 ，则不会将数据移动到这些节点。
修补程序操作步骤	是的。 您可以在 EC 重新平衡操作步骤 运行期间应用 StorageGRID 修补程序。
其他维护过程	否 在运行其他维护过程之前，您必须终止 EC 重新平衡操作步骤 。

EC 重新平衡操作步骤 如何与 ILM 交互

在运行 EC 重新平衡操作步骤 时，请避免进行可能会更改现有纠删编码对象位置的 ILM 更改。例如，请勿开始使用具有不同擦除编码配置文件的 ILM 规则。如果需要进行此类 ILM 更改，应中止 EC 重新平衡操作步骤 。

添加元数据容量

要确保为对象元数据提供足够的可用空间，您可能需要执行扩展操作步骤 以在每个站点添加新的存储节点。

StorageGRID 会为每个存储节点的卷 0 上的对象元数据预留空间。每个站点维护三个所有对象元数据副本，这些副本均匀分布在所有存储节点上。

您可以使用网格管理器监控存储节点的元数据容量，并估计元数据容量的使用速度。此外，当已用元数据空间达到特定阈值时，系统会为存储节点触发 * 低元数据存储 * 警报。

请注意，根据网格的使用方式，网格的对象元数据容量消耗速度可能比其对象存储容量更快。例如，如果您通常要载入大量小对象或向对象添加大量用户元数据或标记，则即使仍有足够的对象存储容量，您可能需要添加存储节点以增加元数据容量。

有关详细信息，请参见以下内容：

- 管理对象元数据存储
- 监控每个存储节点的对象元数据容量

增加元数据容量的准则

在添加存储节点以增加元数据容量之前，请查看以下准则和限制：

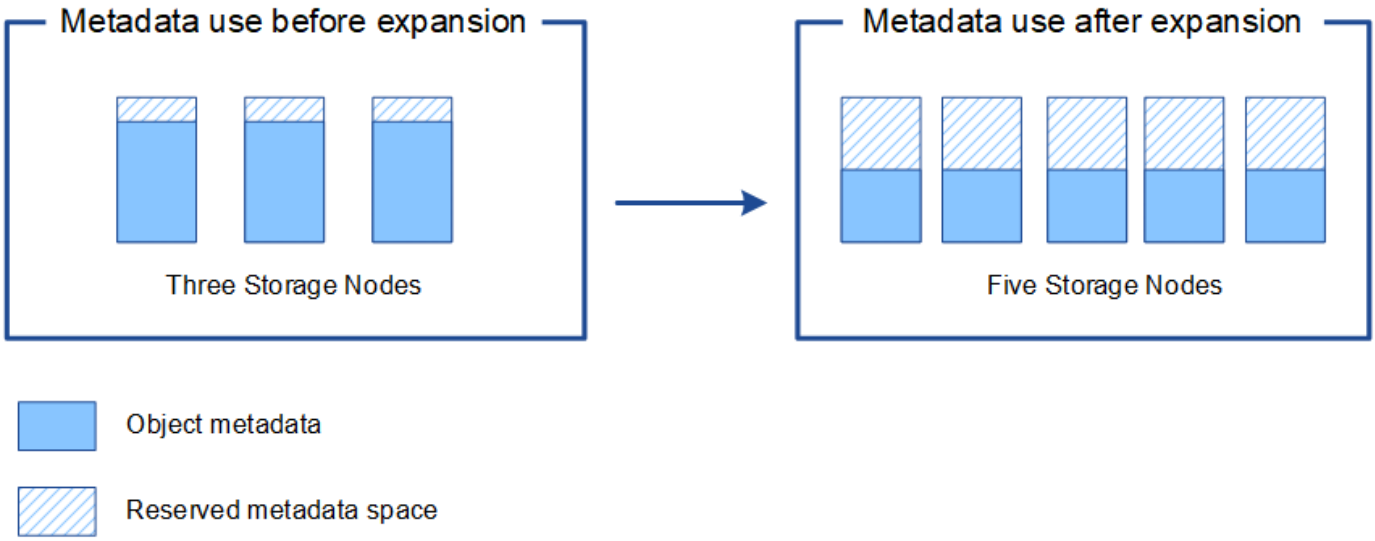
- 假设有足够的对象存储容量可用，则为对象元数据提供更多的可用空间将增加可存储在 StorageGRID 系统中的对象数量。
- 您可以通过向每个站点添加一个或多个存储节点来增加网格的元数据容量。
- 在任何给定存储节点上为对象元数据预留的实际空间取决于元数据预留空间存储选项（系统范围设置），分配给节点的 RAM 量以及节点卷 0 的大小。请参见的说明 管理 StorageGRID。
- 您不能通过向现有存储节点添加存储卷来增加元数据容量，因为元数据仅存储在卷 0 上。
- 您不能通过添加新站点来增加元数据容量。
- StorageGRID 会为每个站点上的所有对象元数据保留三个副本。因此，系统的元数据容量受最小站点的元数据容量限制。
- 在添加元数据容量时，应向每个站点添加相同数量的存储节点。

添加存储节点时如何重新分配元数据

在扩展中添加存储节点时， StorageGRID 会将现有对象元数据重新分发到每个站点的新节点，从而增加网格的整体元数据容量。无需用户操作。

下图显示了在扩展中添加存储节点时 StorageGRID 如何重新分发对象元数据。图的左侧表示扩展之前三个存储节点的卷 0 。元数据占用了每个节点可用元数据空间的相对较大部分，并且已触发 "* 低元数据存储 * " 警报。

图的右侧显示了在向站点添加两个存储节点后如何重新分配现有元数据。每个节点上的元数据数量已减少，不再触发 * 元数据存储不足 * 警报，并且可用于元数据的空间已增加。



添加网格节点以向系统添加功能

您可以通过向现有站点添加新的网格节点来为 StorageGRID 系统添加冗余或其他功能。

例如，您可以选择添加其他网关节点以支持创建网关节点的高可用性组，也可以在远程站点添加管理节点以允许使用本地节点进行监控。

您可以通过单个扩展操作向一个或多个现有站点添加以下一种或多种类型的节点：

- 非主管理节点
- 存储节点
- 网关节点
- 归档节点

准备添加网格节点时，请注意以下限制：

- 主管理节点会在初始安装期间部署。在扩展期间，不能添加主管理节点。
- 您可以在同一扩展中添加存储节点和其他类型的节点。
- 添加存储节点时，必须仔细规划新节点的数量和位置。请参见 添加对象容量的准则。
- 如果要添加归档节点，请注意，每个归档节点仅通过 Tivoli Storage Manager （ TSM ）中间件支持磁带。
- 如果在不可信客户端网络页面上将 * 新节点客户端网络默认 * 选项设置为 * 不可信 * ，则使用客户端网络连接到扩展节点的客户端应用程序必须使用负载平衡器端点端口（ * 配置 * > * 网络 * > * 不可信客户端网络 * ）进行连接。请参见的说明 管理 StorageGRID 更改新节点的设置并配置负载平衡器端点。

添加新站点

您可以通过添加新站点来扩展 StorageGRID 系统。

添加站点的准则

在添加站点之前，请查看以下要求和限制：

- 每个扩展操作只能添加一个站点。
- 不能在同一扩展中向现有站点添加网格节点。
- 所有站点必须至少包含三个存储节点。
- 添加新站点不会自动增加可存储的对象数量。网格的总对象容量取决于每个站点的可用存储容量， ILM 策略和元数据容量。
- 在估算新站点的规模时，您必须确保其包含足够的元数据容量。

  StorageGRID 会为每个站点上的所有对象元数据保留一份副本。添加新站点时，您必须确保它包含足够的元数据容量来容纳现有对象元数据，以及足够的元数据容量来支持增长。

  有关详细信息，请参见以下内容：

  - 管理对象元数据存储
  - 监控每个存储节点的对象元数据容量
- 您必须考虑站点之间的可用网络带宽以及网络延迟级别。元数据更新会在站点之间持续复制，即使所有对象都仅存储在要载入的站点上也是如此。
- 由于 StorageGRID 系统在扩展期间仍可正常运行，因此您必须在启动扩展操作步骤 之前查看 ILM 规则。您必须确保在扩展操作步骤 完成之前不会将对象副本存储到新站点。

  例如，在开始扩展之前，请确定是否有任何规则使用默认存储池（所有存储节点）。如果有，则必须创建一个包含现有存储节点的新存储池，并更新 ILM 规则以使用新存储池。否则，一旦新站点上的第一个节点变为活动状态，对象就会复制到该站点。

  有关在添加新站点时更改 ILM 的详细信息，请参见说明中的更改 ILM 策略示例 使用 ILM 管理对象。

收集所需材料

在执行扩展操作之前，请收集相关材料并安装和配置任何新的硬件和网络。

项目	注释：
StorageGRID 安装归档	如果要添加新的网格节点或新站点，则必须下载并提取 StorageGRID 安装归档。您必须使用网格上当前运行的相同版本。 有关详细信息，请参见的说明 下载并提取 StorageGRID 安装文件。 • 注意： * 如果要向现有存储节点添加新存储卷或安装新的 StorageGRID 设备，则不需要下载文件。
服务笔记本电脑	服务笔记本电脑具有以下功能： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器

项目	注释：
`passwords.txt` file	包含访问命令行上的网格节点所需的密码。包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
StorageGRID 文档	• 管理 StorageGRID • 发行说明 • 适用于您的平台的安装说明 ◦ 安装 Red Hat Enterprise Linux 或 CentOS ◦ 安装 Ubuntu 或 Debian ◦ 安装 VMware
适用于您的平台的最新文档	有关支持的版本，请参见 "互操作性表"。

下载并提取 **StorageGRID** 安装文件

【下载并提取安装文件】

在添加新网格节点或新站点之前，必须下载相应的 StorageGRID 安装归档并提取文件。

关于此任务

您必须使用网格上当前运行的 StorageGRID 版本执行扩展操作。

步骤

1. 转到 StorageGRID 的 "NetApp 下载 " 页面。

   "NetApp 下载： StorageGRID"

2. 选择网格上当前运行的 StorageGRID 版本。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。
5. 在下载页面的 * 安装 StorageGRID * 列中，为您的平台选择 ` .tgz` 或 ` .zip` 文件。

   安装归档文件中显示的版本必须与当前安装的软件版本匹配。

   如果您在服务笔记本电脑上运行 Windows ，请使用 ` .zip` 文件。

平台	安装归档
Red Hat Enterprise Linux 或 CentOS	`storageGRID-Webscale -version-RPM-uniqueID.zip` `StorageGRID-Webscale -version-RPM-uniqueID.tgz`

平台	安装归档
Ubuntu ， Debian 或设备	`storageGRID-Webscale -version-Deb-uniqueID_.zip` `StorageGRID-Webscale -version-Deb-uniqueID_.tgz`
VMware	`storageGRID-Webscale -version-vmware-uniqueID.zip` `StorageGRID-Webscale -version-vmware-uniqueID.tgz`
OpenStack/ 其他虚拟机管理程序	要在 OpenStack 上扩展现有部署，您必须部署一个运行上述受支持 Linux 分发版本之一的虚拟机，并按照适用于 Linux 的相应说明进行操作。

6. 下载并提取归档文件。
7. 按照适用于您的平台的步骤，根据您的平台，计划的网格拓扑以及您将如何扩展 StorageGRID 系统来选择所需的文件。

   步骤中为每个平台列出的路径与归档文件安装的顶级目录相对。

8. 如果要扩展 Red Hat Enterprise Linux 或 CentOS 系统，请选择相应的文件。

路径和文件名	**Description**
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 节点映像。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 主机服务。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。

路径和文件名	Description
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 RHEL 或 CentOS 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要扩展 Ubuntu 或 Debian 系统，请选择相应的文件。

路径和文件名	Description
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。
	文件 ` /debs/storagegrid-webscale-images-version-SHA.deb` 的 MD5 校验和。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。

路径和文件名	Description
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要扩展 VMware 系统，请选择相应的文件。

路径和文件名	Description
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。
	用于部署主管理节点的开放式虚拟化格式模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署非主管理节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署归档节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署网关节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署基于虚拟机的存储节点的模板文件（`.OVF`）和清单文件（`.MF`）。
部署脚本工具	Description

路径和文件名	Description
	Bash shell 脚本，用于自动部署虚拟网格节点。
	与 `deept-vsphere-ovftool.sh` 脚本结合使用的示例配置文件。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	StorageGRID 的 API 架构。 • 注意 * ：在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要扩展基于 StorageGRID 设备的系统，请选择相应的文件。

路径和文件名	Description
	用于在设备上安装 StorageGRID 节点映像的 Deb 软件包。
	StorageGRID 设备安装程序使用的 Deb 安装包的校验和，用于验证该软件包在上传后是否完好无损。

> 对于设备安装，只有在需要避免网络流量时，才需要这些文件。设备可以从主管理节点下载所需文件。

验证硬件和网络连接

开始扩展 StorageGRID 系统之前，请确保满足以下要求：

- 已安装并配置支持新网格节点或新站点所需的硬件。

- 所有新节点都具有指向所有现有节点和新节点的双向通信路径（网格网络的一项要求）。
- 主管理节点可以与用于托管 StorageGRID 系统的所有扩展服务器进行通信。
- 如果任何新节点的子网上有一个网格网络 IP 地址，而此地址以前未使用过，则表示您已使用 已添加新子网 到网格网络子网列表。否则，您必须取消扩展，添加新子网并重新启动操作步骤 。
- 您未在网格节点之间或 StorageGRID 站点之间的网格网络上使用网络地址转换（ Network Address Translation ， NAT ）。如果您对网格网络使用专用 IPv4 地址，则这些地址必须可从每个站点的每个网格节点直接路由。只有在使用对网格中的所有节点都透明的通道应用程序时，才支持使用 NAT 在公有 网段中桥接网格网络，这意味着网格节点不需要了解公有 IP 地址。

  此 NAT 限制特定于网格节点和网格网络。您可以根据需要在外部客户端和网格节点之间使用 NAT ，例如为网关节点提供公有 IP 地址。

添加存储卷

将存储卷添加到存储节点

您可以通过添加其他存储卷来扩展存储卷数量不超过 16 个的存储节点的存储容量。您可能需要将存储卷添加到多个存储节点，以满足对复制的或经过纠删编码的副本的 ILM 要求。

您需要的内容

在添加存储卷之前，请查看 添加对象容量的准则 确保您知道在何处添加卷以满足 ILM 策略的要求。

> 这些说明仅适用于基于软件的存储节点。请参见 将扩展架添加到已部署的SG6060或SG60X 了解如何通过安装扩展架将存储卷添加到SG6060或SG60X。无法扩展其他设备存储节点。

关于此任务

存储节点的底层存储分为多个存储卷。存储卷是基于块的存储设备，由 StorageGRID 系统格式化并挂载以存储对象。每个存储节点最多可支持 16 个存储卷，在网格管理器中称为 *object stores* 。

> 对象元数据始终存储在对象存储 0 中。

每个对象存储都挂载在与其 ID 对应的卷上。例如， ID 为 0000 的对象存储对应于 ` /var/local/rangedb/0` 挂载点。

在添加新存储卷之前，请使用网格管理器查看每个存储节点的当前对象存储以及相应的挂载点。您可以在添加存储卷时使用此信息。

步骤

1. 选择 * 节点 * > * 站点 _* > * 存储节点 _* > * 存储 * 。
2. 向下滚动以查看每个卷和对象存储的可用存储容量。

   对于设备存储节点，每个磁盘的全球通用名称与在 SANtricity 软件（连接到设备存储控制器的管理软件）中查看标准卷属性时显示的卷全球通用标识符（ WWID ）匹配。

   为了帮助您解释与卷挂载点相关的磁盘读取和写入统计信息，磁盘设备表的 * 名称 * 列（即 *sdc* ， *sdd* ， *sde* 等）中显示的名称的第一部分与卷表的 * 设备 * 列中显示的值匹配。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. 按照适用于您的平台的说明向存储节点添加新存储卷。
   - VMware： 将存储卷添加到存储节点
   - Linux： 将直连卷或 SAN 卷添加到存储节点

VMware： 将存储卷添加到存储节点

如果某个存储节点包含的存储卷少于 16 个，则可以使用 VMware vSphere 添加卷来增加其容量。

您需要的内容

- 您可以访问有关安装适用于 VMware 的 StorageGRID 部署的说明。
  - 安装 VMware
- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

> 在软件升级，恢复操作步骤 或其他扩展操作步骤 处于活动状态时，请勿尝试向存储节点添加存储卷。

关于此任务

添加存储卷时，此存储节点将暂时不可用。您应一次在一个存储节点上执行此操作步骤 ，以避免影响面向客户端的网格服务。

步骤

1. 如有必要，请安装新的存储硬件并创建新的 VMware 数据存储库。
2. 向虚拟机添加一个或多个硬盘以用作存储（对象存储）。
   a. 打开 VMware vSphere Client 。
   b. 编辑虚拟机设置以添加一个或多个附加硬盘。

   硬盘通常配置为虚拟机磁盘（ Virtual Machine Disk ， VMDK ）。VMDK 的使用更广泛，管理更方便，而 RDM 则可以为使用较大对象大小（例如大于 100 MB ）的工作负载提供更好的性能。有关向虚拟机添加硬盘的详细信息，请参见 VMware vSphere 文档。
3. 使用 VMware vSphere Client 中的 * 重新启动子操作系统 * 选项或在与虚拟机的 ssh 会话中输入以下命令来重新启动虚拟机：`sudo reboot`

   > 请勿使用 * 关闭电源 * 或 * 重置 * 重新启动虚拟机。
4. 配置新存储以供存储节点使用：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

b. 配置新存储卷：

```
sudo add_rangedbs.rb
```

此脚本将查找任何新存储卷并提示您对其进行格式化。

a. 输入 * 。 * 接受格式化。

b. 如果先前已对任何卷进行格式化，请确定是否要重新格式化这些卷。

- 输入 * y * 重新格式化。
- 输入 * 。 n* 可跳过重新格式化。

c. 当系统询问时，输入 * 。 * 以停止存储服务。

存储服务将停止， `setup_rangedbs.sh` 脚本将自动运行。在卷准备好用作卷集之后，服务将重新启动。

5. 检查服务是否正确启动：

a. 查看服务器上所有服务的状态列表：

```
sUdo storagegRid-status
```

状态将自动更新。

a. 请等待所有服务均已运行或已验证。

b. 退出状态屏幕：

```
Ctrl+C
```

6. 验证存储节点是否联机：

a. 使用登录到网格管理器 支持的 Web 浏览器。

b. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

c. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 存储 * 。

d. 选择 * 配置 * 选项卡，然后选择 * 主 * 选项卡。

e. 如果 * 存储状态 - 所需 * 下拉列表设置为只读或脱机，请选择 * 联机 * 。

f. 选择 * 应用更改 * 。

7. 要查看新对象存储，请执行以下操作：

a. 选择 * 节点 * > * 站点 _* > * 存储节点 _* > * 存储 * 。

b. 在 * 对象存储 * 表中查看详细信息。

结果

您可以使用存储节点的扩展容量来保存对象数据。

Linux：将直连卷或 SAN 卷添加到存储节点

如果某个存储节点包含的存储卷少于 16 个，则可以通过添加新的块存储设备，使其对 Linux 主机可见，并将新的块设备映射添加到用于该存储节点的 StorageGRID 配置文件来增加其容量。

您需要的内容

- 您可以访问有关为 Linux 平台安装 StorageGRID 的说明。
  - 安装 Red Hat Enterprise Linux 或 CentOS
  - 安装 Ubuntu 或 Debian
- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

> 在软件升级，恢复操作步骤 或其他扩展操作步骤 处于活动状态时，请勿尝试向存储节点添加存储卷。

关于此任务

添加存储卷时，此存储节点将暂时不可用。您应一次在一个存储节点上执行此操作步骤 ，以避免影响面向客户端的网格服务。

步骤

1. 安装新的存储硬件。

   有关详细信息，请参见硬件供应商提供的文档。

2. 创建所需大小的新块存储卷。
   - 连接新磁盘驱动器并根据需要更新 RAID 控制器配置，或者在共享存储阵列上分配新的 SAN LUN 并允许 Linux 主机访问这些 LUN 。
   - 请使用与现有存储节点上的存储卷相同的永久性命名方案。
   - 如果使用 StorageGRID 节点迁移功能，请使作为此存储节点迁移目标的其他 Linux 主机可以看到新卷。有关详细信息，请参见有关为 Linux 平台安装 StorageGRID 的说明。
3. 以 root 身份或使用具有 sudo 权限的帐户登录到支持存储节点的 Linux 主机。
4. 确认新存储卷在 Linux 主机上可见。

   您可能需要重新扫描设备。

5. 运行以下命令以临时禁用存储节点：

   ```
   sUdo StorageGRID node stop <node-name>
   ```

6. 使用 vim 或 pico 等文本编辑器编辑存储节点的节点配置文件，该文件位于 ` /etc/storaggrid/nodes/<node-name>.conf` 中。
7. 找到节点配置文件中包含现有对象存储块设备映射的部分。

   在此示例中， `block_device_RANGEDB_00` 到 `block_device_RANGEDB_03` 是现有的对象存储块设备

映射。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. 添加与为此存储节点添加的块存储卷对应的新对象存储块设备映射。

   请务必从下一个 `block_device_RANGEDB_nn` 开始。请勿留下空隙。

   - 基于以上示例，从 `block_device_RANGEDB_04` 开始。
   - 在以下示例中，向节点添加了四个新的块存储卷： `block_device_RANGEDB_04` to `block_device_RANGEDB_07` 。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. 运行以下命令以验证对存储节点的节点配置文件所做的更改：

```
sUdo StorageGRID node validate <node-name>
```

解决所有错误或警告，然后再继续下一步。

如果您发现类似以下内容的错误，则表示节点配置文件正在尝试将 ` <node-name>` for ` <utility>` 使用的块设备映射到 Linux 文件系统中的给定 ` <path-name>` 。 但该位置没有有效的块设备专用文件（或指向块设备专用文件的软链接）。

```
Checking configuration file for node <node-name>…
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device
```

验证您输入的 ` <path-name>` 是否正确。

10. 运行以下命令以重新启动具有新块设备映射的节点：

```
sUdo StorageGRID node start <node-name>
```

11. 使用 `passwords.txt` 文件中列出的密码以管理员身份登录到存储节点。
12. 检查服务是否正确启动：
    a. 查看服务器上所有服务的状态列表： + `sUdo storagegRid-status`

       状态将自动更新。

    b. 请等待所有服务均已运行或已验证。
    c. 退出状态屏幕：

       ```
       Ctrl+C
       ```

13. 配置新存储以供存储节点使用：
    a. 配置新存储卷：

       ```
       sudo add_rangedbs.rb
       ```

    此脚本将查找任何新存储卷并提示您对其进行格式化。

    a. 输入 * 。 * 格式化存储卷。
    b. 如果先前已对任何卷进行格式化，请确定是否要重新格式化这些卷。
       - 输入 * y * 重新格式化。
       - 输入 * 。 n* 可跳过重新格式化。
    c. 当系统询问时，输入 * 。 * 以停止存储服务。

       存储服务将停止， `setup_rangedbs.sh` 脚本将自动运行。在卷准备好用作卷集之后，服务将重新启动。

14. 检查服务是否正确启动：

a. 查看服务器上所有服务的状态列表：

```
sUdo storagegRid-status
```

状态将自动更新。

a. 请等待所有服务均已运行或已验证。

b. 退出状态屏幕：

```
Ctrl+C
```

15. 验证存储节点是否联机：

a. 使用登录到网格管理器 支持的 Web 浏览器。

b. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

c. 选择 * 站点 _* > * 存储节点 _* > * LDR* > * 存储 * 。

d. 选择 * 配置 * 选项卡，然后选择 * 主 * 选项卡。

e. 如果 * 存储状态 - 所需 * 下拉列表设置为只读或脱机，请选择 * 联机 * 。

f. 单击 * 应用更改 * 。

16. 要查看新对象存储，请执行以下操作：

a. 选择 * 节点 * > * 站点 _* > * 存储节点 _* > * 存储 * 。

b. 在 * 对象存储 * 表中查看详细信息。

结果

现在，您可以使用存储节点的扩展容量来保存对象数据。

添加网格节点或站点

向现有站点添加网格节点或添加新站点

您可以按照此操作步骤 向现有站点添加网格节点或添加新站点，但不能同时执行这两种类型的扩展。

您需要的内容

- 您具有 root 访问权限或维护权限。
- 网格中的所有现有节点在所有站点上均已启动且正在运行。
- 先前的任何扩展，升级，停用或恢复过程均已完成。

> 如果正在进行另一个扩展，升级，恢复或活动的停用操作步骤 ，则系统将阻止您启动扩展。但是，如有必要，您可以暂停已停用的操作步骤 以启动扩展。

步骤

1. 更新网格网络的子网。

2. 部署新的网格节点。
3. 执行扩展。

更新网格网络的子网

在扩展中添加网格节点或新站点时，您可能需要更新子网或向网格网络添加子网。

StorageGRID 会维护一个网络子网列表，用于在网格网络（ eth0 ）上的网格节点之间进行通信。这些条目包括 StorageGRID 系统中每个站点用于网格网络的子网，以及通过网格网络网关访问的 NTP ， DNS ， LDAP 或其他外部服务器所使用的任何子网。

您需要的内容

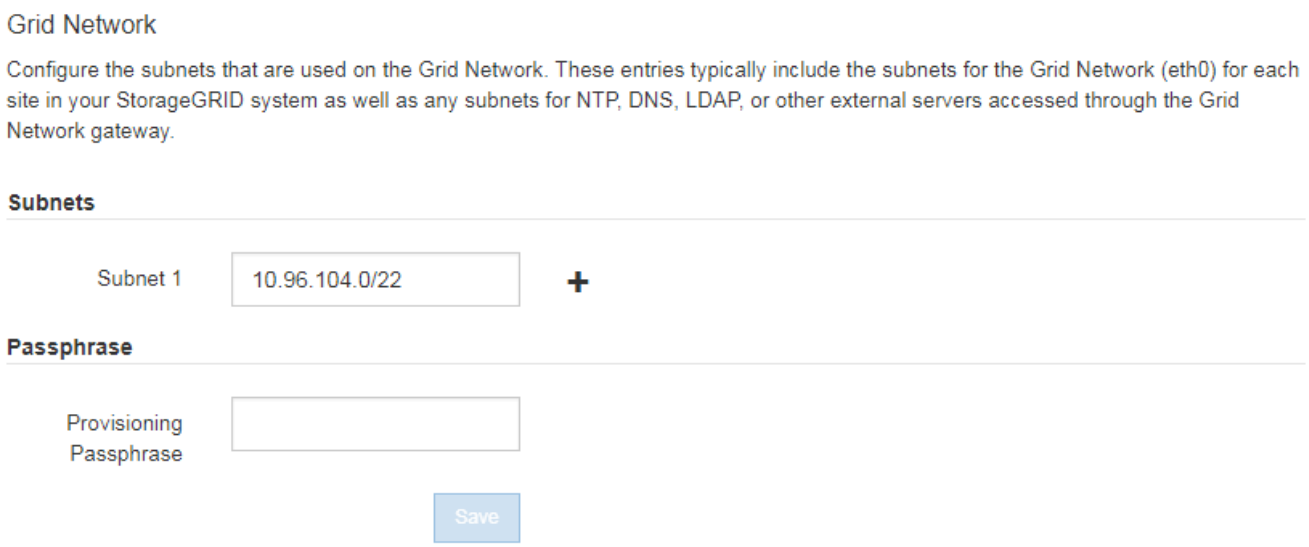
- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有配置密码短语。
- 您已获得要配置的子网的网络地址，以 CIDR 表示法表示。

关于此任务

如果任何新节点的子网上有一个以前未使用的网格网络 IP 地址，则必须在开始扩展之前将此新子网添加到网格网络子网列表中。否则，您必须取消扩展，添加新子网并重新启动操作步骤 。

步骤

1. 选择 * 维护 * > * 网络 * > * 网格网络 * 。



2. 在子网列表中，选择加号以 CIDR 表示法添加新子网。

   例如，输入 10.96.104.0/22 。

3. 输入配置密码短语，然后选择 * 保存 * 。

   您指定的子网将自动为 StorageGRID 系统配置。

在扩展中部署新网格节点的步骤与首次安装网格时使用的步骤相同。您必须先部署所有新的网格节点，然后才能执行扩展。

扩展网格时，您添加的节点不必与现有节点类型匹配。您可以添加 VMware 节点，基于 Linux 容器的节点或设备节点。

VMware： 部署网格节点

您必须在 VMware vSphere 中为要添加到扩展中的每个 VMware 节点部署一个虚拟机。

步骤

1. 将新节点部署为虚拟机 并将其连接到一个或多个 StorageGRID 网络。

   部署节点时，您可以选择重新映射节点端口或增加 CPU 或内存设置。

2. 部署所有新的 VMware 节点后， 执行扩展操作步骤。

Linux： 部署网格节点

您可以在新的 Linux 主机或现有的 Linux 主机上部署网格节点。如果您需要更多的 Linux 主机来满足要添加到网格中的 StorageGRID 节点的 CPU ， RAM 和存储要求，请按照首次安装主机时准备主机的方式对其进行准备。然后，按照安装期间部署网格节点的方式部署扩展节点。

您需要的内容

- 您已获得有关为您的 Linux 版本安装 StorageGRID 的说明，并已查看硬件和存储要求。
  - 安装 Red Hat Enterprise Linux 或 CentOS
  - 安装 Ubuntu 或 Debian
- 如果您计划在现有主机上部署新的网格节点，则已确认现有主机具有足够的 CPU ， RAM 和存储容量来容纳其他节点。
- 您计划最大限度地减少故障域。例如，不应将所有网关节点部署在一个物理主机上。

  在生产部署中，请勿在一个物理或虚拟主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

- 如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

步骤

1. 如果要添加新主机，请访问有关部署 StorageGRID 节点的安装说明。
2. 要部署新主机，请按照说明准备主机。
3. 要创建节点配置文件并验证 StorageGRID 配置，请按照有关部署网格节点的说明进行操作。
4. 如果要向新的 Linux 主机添加节点，请启动 StorageGRID 主机服务。
5. 如果要向现有 Linux 主机添加节点，请使用 StorageGRID 主机服务命令行界面启动新节点：`sUdo StorageGRID node start <<` 节点名称 `\>>`

完成后

部署所有新网格节点后，您可以 执行扩展。

设备：部署存储，网关或非主管理节点

要在设备节点上安装 StorageGRID 软件，请使用设备中提供的 StorageGRID 设备安装程序。在扩展中，每个存储设备都充当一个存储节点，而每个服务设备则充当一个网关节点或非主管理节点。任何设备都可以连接到网格网络，管理网络和客户端网络。

您需要的内容

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 您已使用 StorageGRID 设备安装程序完成设备安装和维护说明中的所有 "`configure hardware` " 步骤。
  - SG100 和 SG1000 服务设备
  - 配置硬件（ SG5600 ）
  - 配置硬件（ SG5700 ）
  - 配置硬件（ SG6000 ）

  配置设备硬件包括配置 StorageGRID 连接（网络链路和 IP 地址）所需的步骤，以及启用节点加密，更改 RAID 模式和重新映射网络端口的可选步骤。
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 替代设备上的 StorageGRID 设备安装程序固件与网格上当前运行的 StorageGRID 软件版本兼容。例如，StorageGRID 设备安装程序 3.6 版与 StorageGRID 11.6 版兼容。（如果版本不兼容，则必须升级 StorageGRID 设备安装程序固件。）
- 您的服务笔记本电脑具有 支持的 Web 浏览器。
- 您知道分配给设备计算控制器的一个 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。

关于此任务

在设备节点上安装 StorageGRID 的过程分为以下阶段：

- 您可以指定或确认主管理节点的 IP 地址以及设备节点的名称。
- 您开始安装，并等待卷配置完毕并安装软件。

  在执行设备安装任务时，安装将暂停。要恢复安装，请登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装过程。

> 如果您需要一次部署多个设备节点，则可以使用 `configure-sGa.py` 设备安装脚本自动执行安装过程。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

   `https://Controller_IP:8443`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在 * 主管理节点 * 连接部分中，确定是否需要指定主管理节点的 IP 地址。

   如果先前已在此数据中心中安装了其他节点，则 StorageGRID 设备安装程序可以自动发现此 IP 地址，前提是主管理节点或至少一个配置了 admin_IP 的其他网格节点位于同一子网上。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 等待连接状态，使新 IP 地址准备就绪。
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 等待显示发现的 IP 地址列表。 c. 为要部署此设备存储节点的网格选择主管理节点。 d. 单击 * 保存 * 。 e. 等待连接状态，使新 IP 地址准备就绪。

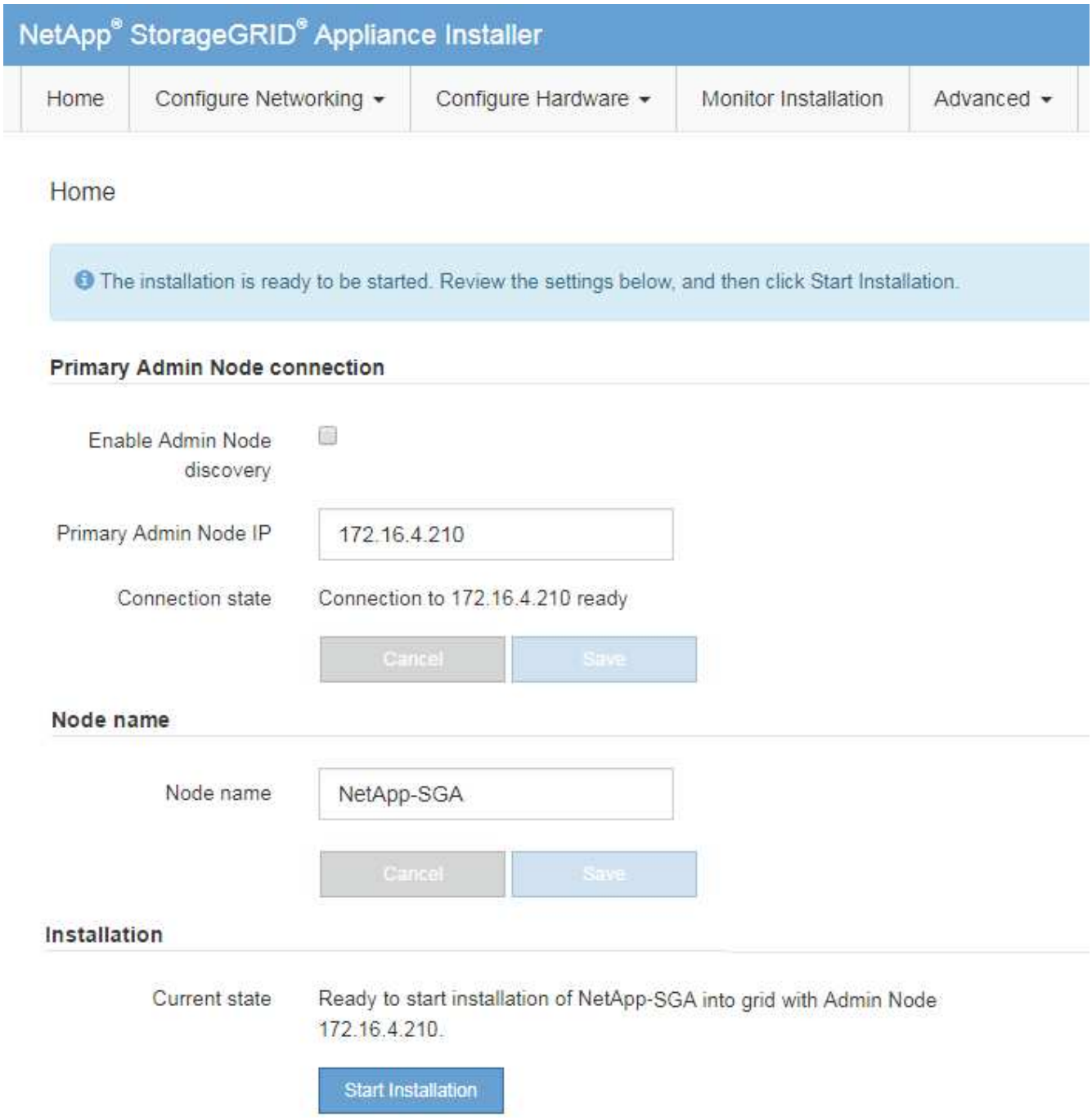
4. 在 * 节点名称 * 字段中，输入要用于此设备节点的名称，然后选择 * 保存 * 。

   节点名称将分配给 StorageGRID 系统中的此设备节点。它显示在网格管理器的节点页面（概述选项卡）上。如果需要，您可以在批准节点时更改名称。

5. 在 * 安装 * 部分中，确认当前状态为 "`Ready to start installation of *node name* into grid with primary Admin Node *admin_ip*` " ，并且 * 开始安装 * 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

6. 从 StorageGRID 设备安装程序主页中，选择 * 开始安装 * 。



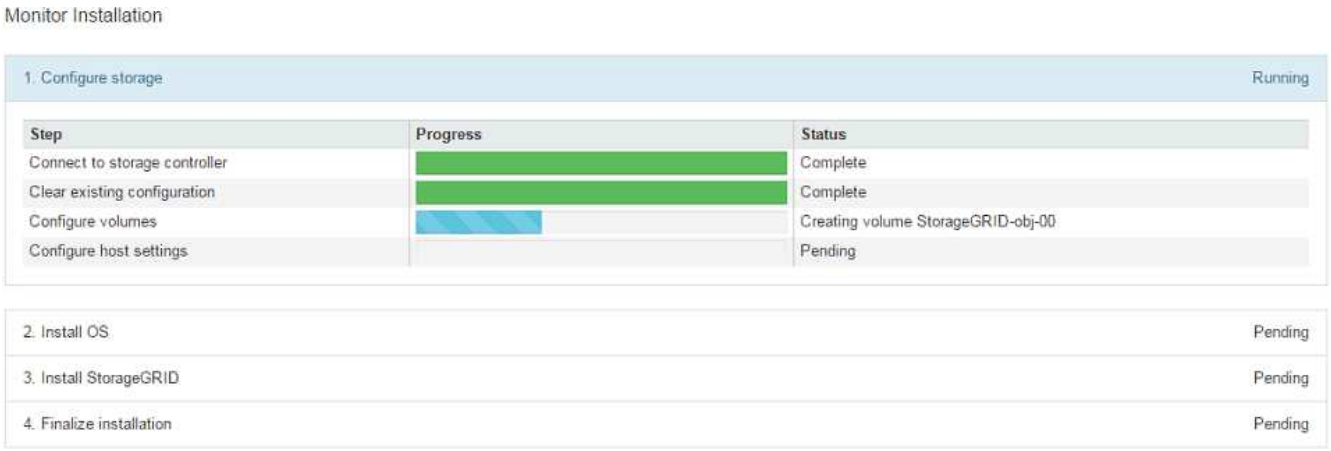
当前状态将更改为 "`Installation is in progress，`"，此时将显示监控器安装页面。

7. 如果扩展包含多个设备节点，请对每个设备重复上述步骤。

   如果您需要一次部署多个设备存储节点，则可以使用 configure-sga.py 设备安装脚本自动执行安装过程。

8. 如果需要手动访问监控器安装页面，请从菜单栏中选择 * 监控器安装 * 。

   "Monitor Installation" 页面将显示安装进度。



蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

> 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

9. 查看前两个安装阶段的进度。

   ◦ 。配置设备 *

   在此阶段，将执行以下过程之一：

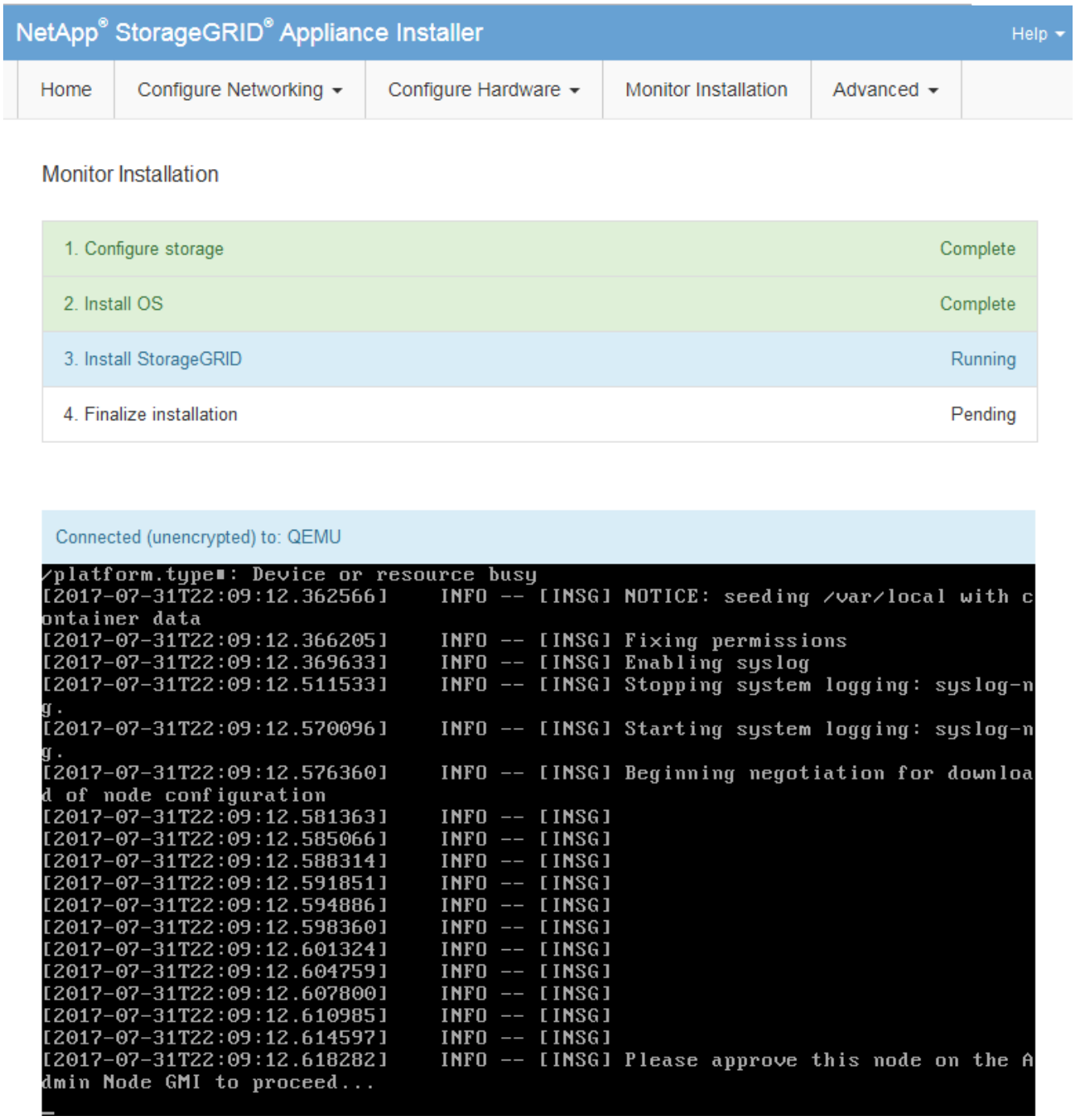
   - 对于存储设备，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。
   - 对于服务设备，安装程序将从计算控制器中的驱动器中清除任何现有配置，并配置主机设置。

   ◦ 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

10. 继续监控安装进度，直到控制台窗口显示一条消息，提示您使用网格管理器批准节点。

> 等待您在此扩展中添加的所有节点都准备好进行批准，然后再转到网格管理器来批准这些节点。



执行扩展

执行扩展时，新的网格节点将添加到现有 StorageGRID 部署中。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有配置密码短语。
- 您已部署要在此扩展中添加的所有网格节点。

- 如果您要添加存储节点，则已确认在恢复过程中执行的所有数据修复操作均已完成。请参见 检查数据修复作业。
- 如果要添加新站点，则必须在启动扩展操作步骤 之前查看和更新 ILM 规则，以确保在扩展完成之前不会将对象副本存储到新站点。例如，如果某个规则使用默认存储池（所有存储节点），则必须创建一个仅包含现有存储节点的新存储池，并更新 ILM 规则以使用新存储池。否则，一旦新站点上的第一个节点变为活动状态，对象就会复制到该站点。请参见的说明 使用 ILM 管理对象。

关于此任务

执行扩展包括以下阶段：

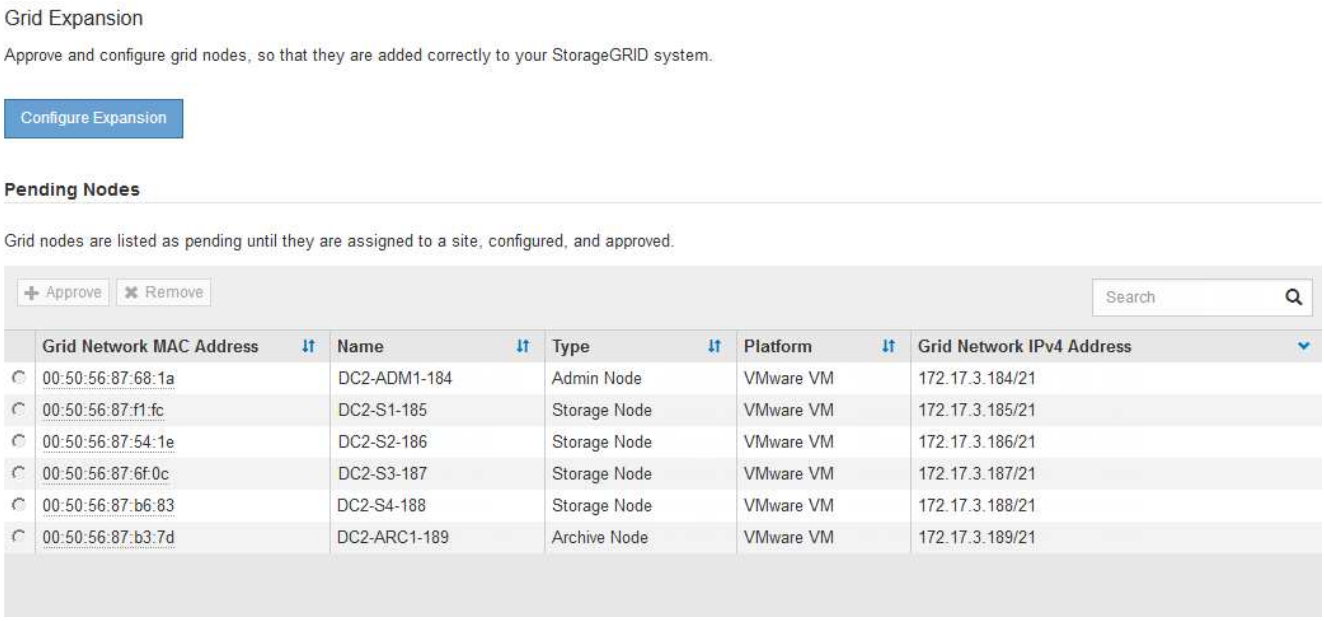
1. 您可以通过指定是添加新网格节点还是添加新站点并批准要添加的网格节点来配置扩展。
2. 开始扩展。
3. 在扩展过程运行期间，您会下载一个新的恢复软件包文件。
4. 您可以监控网格配置阶段的状态，这些配置阶段会自动运行。阶段集取决于要添加的网格节点类型以及是否要添加新站点。

> 在大型网格上运行某些阶段可能需要大量时间。例如，如果 Cassandra 数据库为空，则将 Cassandra 流式传输到新存储节点可能只需要几分钟的时间。但是，如果 Cassandra 数据库包含大量对象元数据，则此阶段可能需要数小时或更长时间。请勿在 " 扩展 Cassandra 集群 " 或 " 启动 Cassandra 和流式数据 " 阶段重新启动任何存储节点。

步骤

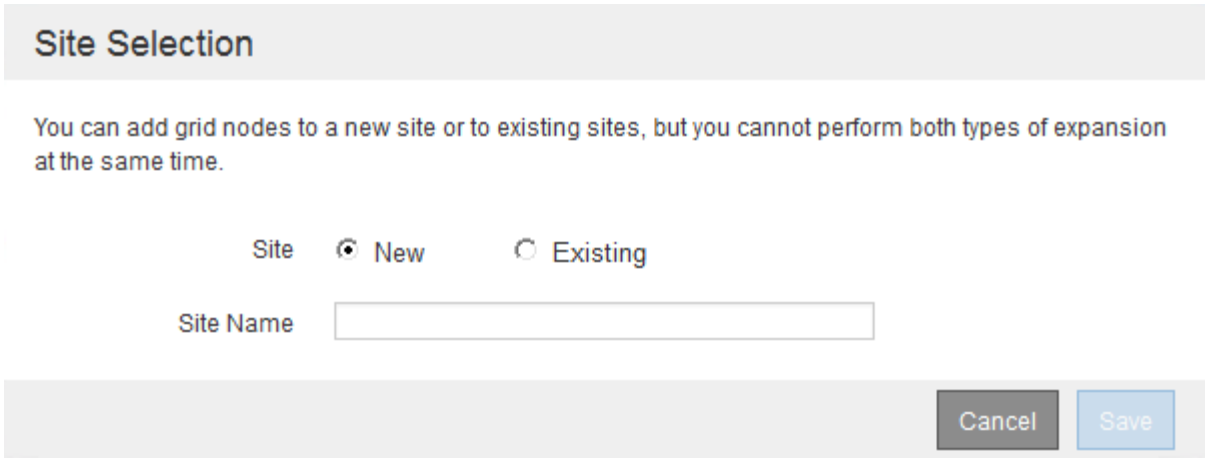
1. 选择 * 维护 * > * 任务 * > * 扩展 * 。

   此时将显示网格扩展页面。"Pending Nodes" 部分列出了准备添加的所有节点。



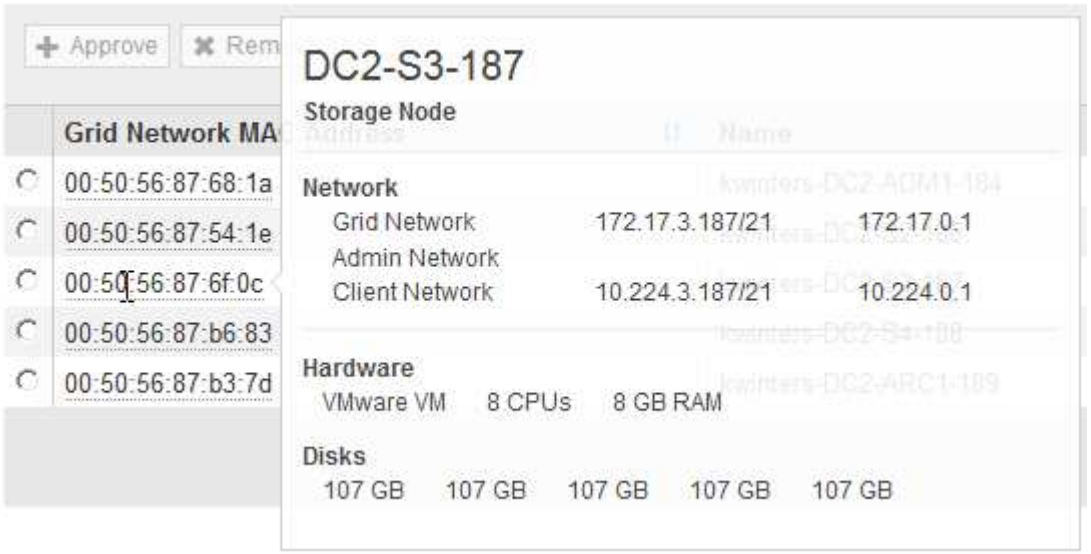
2. 选择 * 配置扩展 * 。

   此时将显示站点选择对话框。



3. 选择要启动的扩展类型：
   - 如果要添加新站点，请选择 * 新建 * ，然后输入新站点的名称。
   - 如果要向现有站点添加网格节点，请选择 * 现有 * 。
4. 选择 * 保存 * 。
5. 查看 * 待定节点 * 列表，并确认它显示了您部署的所有网格节点。

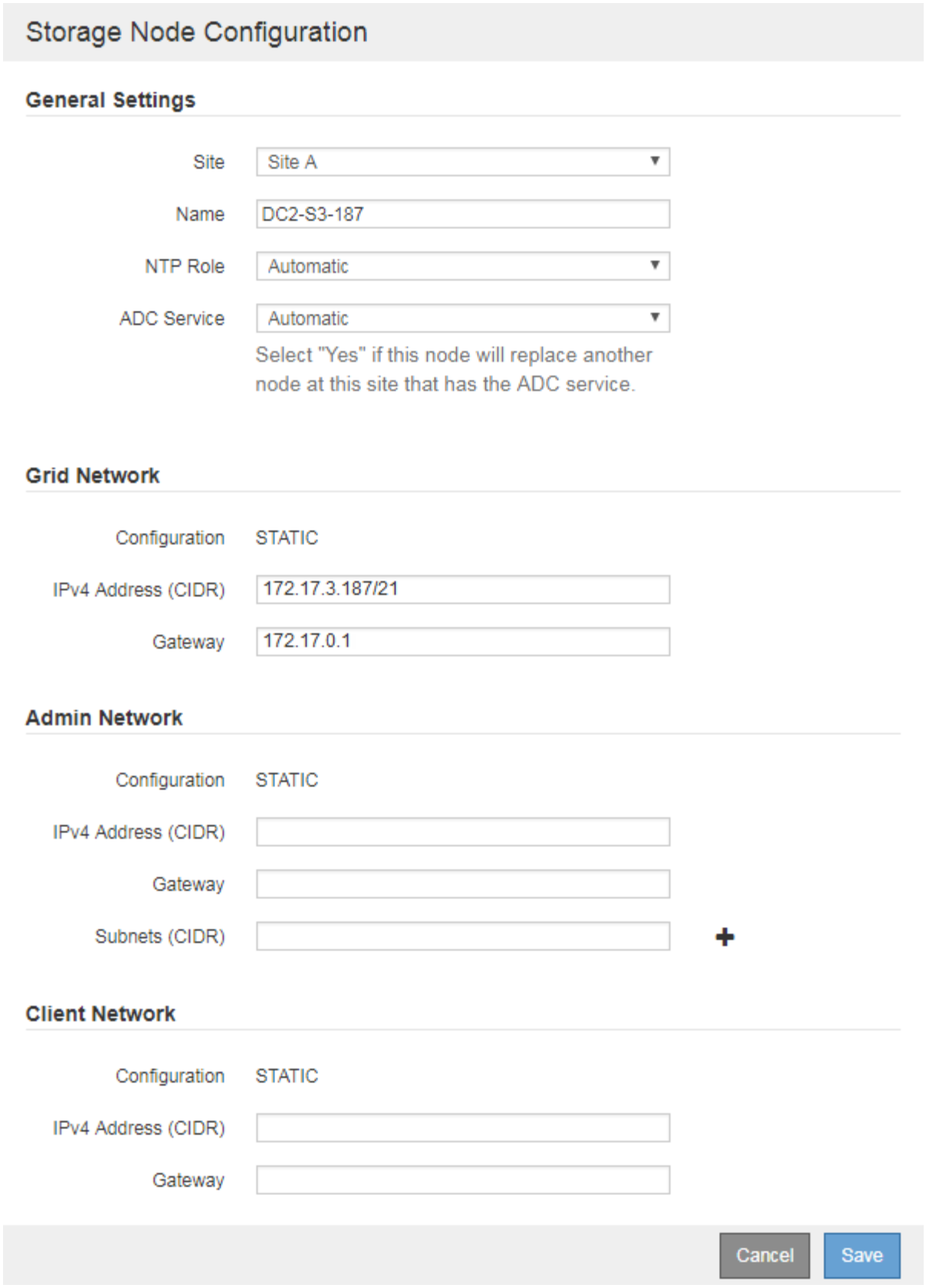
   根据需要，您可以将光标悬停在节点的 * 网格网络 MAC 地址 * 上以查看有关该节点的详细信息。



> 如果缺少网格节点，请确认已成功部署该节点。

6. 从待定节点列表中，批准此扩展的网格节点。
   a. 选择要批准的第一个待定网格节点旁边的单选按钮。
   b. 选择 * 批准 * 。

      此时将显示网格节点配置表单。



c. 根据需要修改常规设置：

- * 站点 * ：要与网格节点关联的站点的名称。如果要添加多个节点，请确保为每个节点选择正确的站点。如果要添加新站点，则所有节点都将添加到新站点。

- * 名称 * ：将分配给节点的主机名以及将在网格管理器中显示的名称。
- * NTP 角色 * ：网格节点的网络时间协议（ NTP ）角色。选项包括 * 自动 * ， * 主 * 和 * 客户端 * 。选择 * 自动 * 会将主角色分配给管理节点，具有模板转换服务的存储节点，网关节点以及具有非静态 IP 地址的任何网格节点。所有其他网格节点都分配有客户端角色。

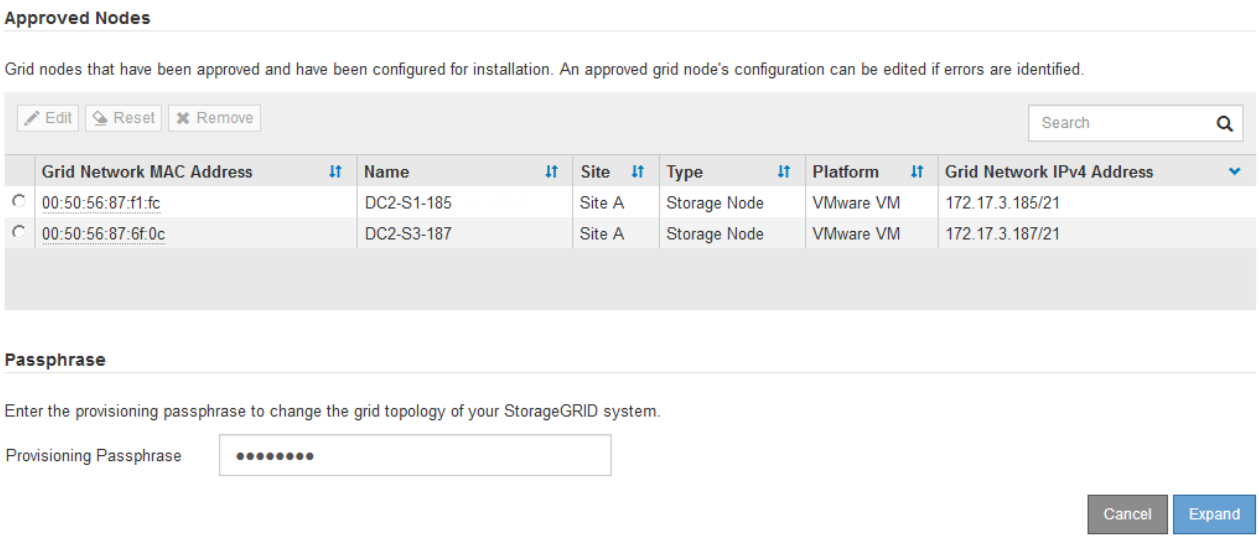
  > 将主 NTP 角色分配给每个站点上至少两个节点。这样，系统便可对外部计时源进行冗余访问。

- * ADC* 服务 * （仅限存储节点）：此存储节点是否将运行管理域控制器（ ADC-A ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。每个站点至少有三个存储节点必须包含此 ADC-Service 。在部署此节点后，您不能将此 ADC 服务添加到该节点中。
  - 如果要添加此节点以替换存储节点，请选择 * 是 * ，前提是要替换的节点包含此 ADA 服务。由于如果仍会保留的 ADD 服务太少，则无法停用存储节点，因此，这样可以确保在删除旧服务之前新的 ADD 服务可用。
  - 否则，请选择 * 自动 * 以让系统确定此节点是否需要使用此 ADC-Service 。了解有关模数转换器仲裁的信息 此处。

d. 根据需要修改网格网络，管理网络和客户端网络的设置。
   - * IPv4 地址（ CIDR ） * ：网络接口的 CIDR 网络地址。例如： 172.16.10.100/24
   - * 网关 * ：网格节点的默认网关。例如： 172.16.10.1
   - * 子网（ CIDR ） * ：管理网络的一个或多个子网。

e. 选择 * 保存 * 。

   批准的网格节点将移至批准的节点列表。



   - 要修改已批准的网格节点的属性，请选择其单选按钮，然后选择 * 编辑 * 。
   - 要将已批准的网格节点移回 "Pending Nodes" 列表，请选择其单选按钮，然后选择 * 重置 * 。
   - 要永久删除已批准的网格节点，请关闭此节点。然后，选择其单选按钮并选择 * 删除 * 。

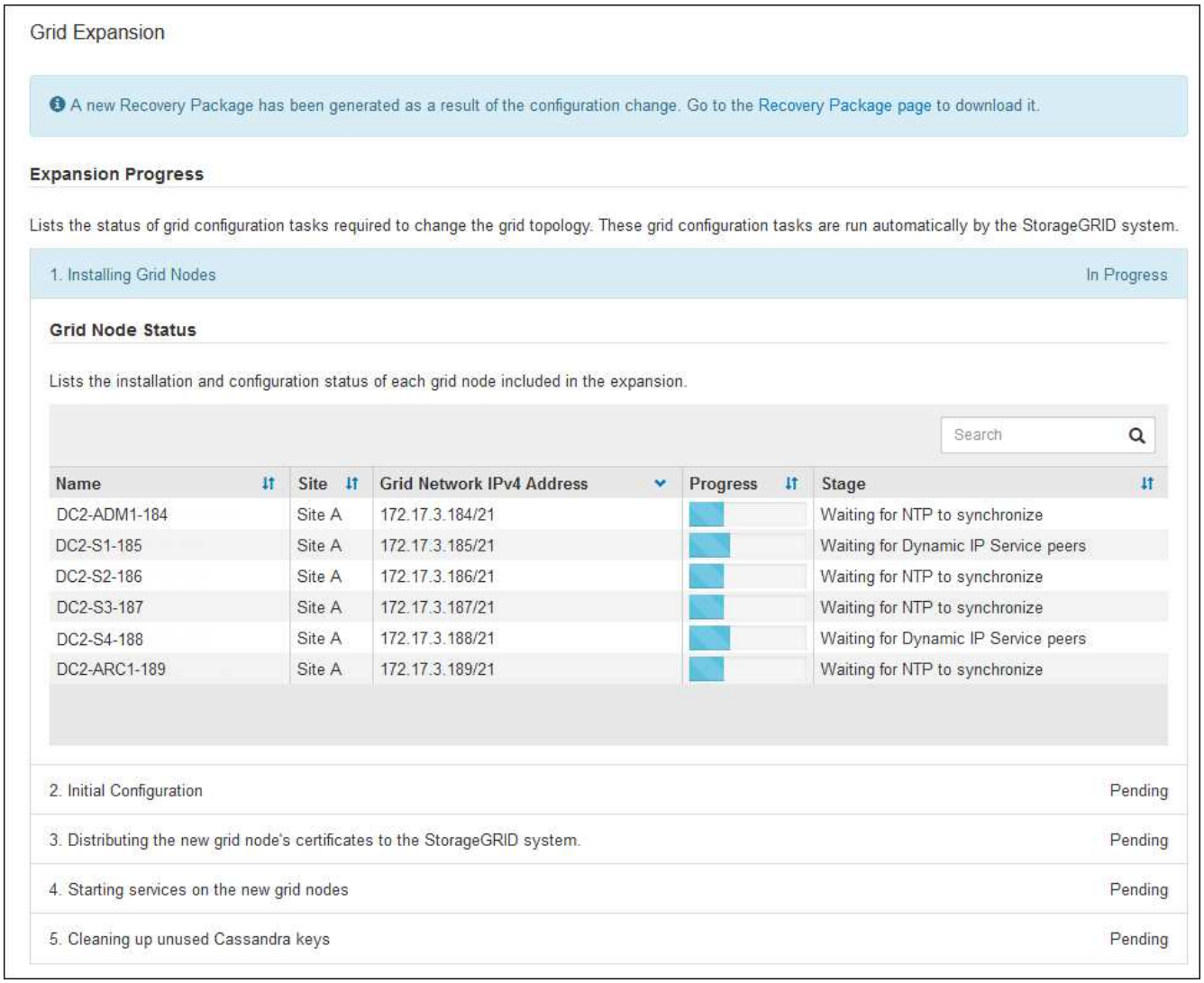
f. 对要批准的每个待定网格节点重复上述步骤。

如果可能，您应批准所有待定网格注释并执行一次扩展。如果执行多个小型扩展，则需要更多时间。

7. 批准所有网格节点后，输入 * 配置密码短语 * ，然后选择 * 扩展 * 。

   几分钟后，此页面将更新以显示扩展操作步骤 的状态。如果正在执行影响单个网格节点的任务，则网格节点状态部分将列出每个网格节点的当前状态。

   在此过程中，对于设备， StorageGRID 设备安装程序会显示安装从第 3 阶段移至第 4 阶段 " 完成安装 " 。阶段 4 完成后，控制器将重新启动。



站点扩展包括一项额外任务，用于为新站点配置 Cassandra 。

8. 显示 * 下载恢复包 * 链接后，立即下载恢复包文件。

   在对 StorageGRID 系统进行网格拓扑更改后，您必须尽快下载恢复包文件的更新副本。通过恢复包文件，您可以在发生故障时还原系统。

   a. 选择下载链接。

b. 输入配置密码短语，然后选择 * 开始下载 * 。

c. 下载完成后，打开 ` .zip` 文件并确认其中包含 `gpt 备份` 目录和 ` sed_said.zip` 文件。然后，提取 ` sa_sid.zip` 文件，转到 ` /GID* _REV*` 目录，确认您可以打开 `passwords.txt` 文件。

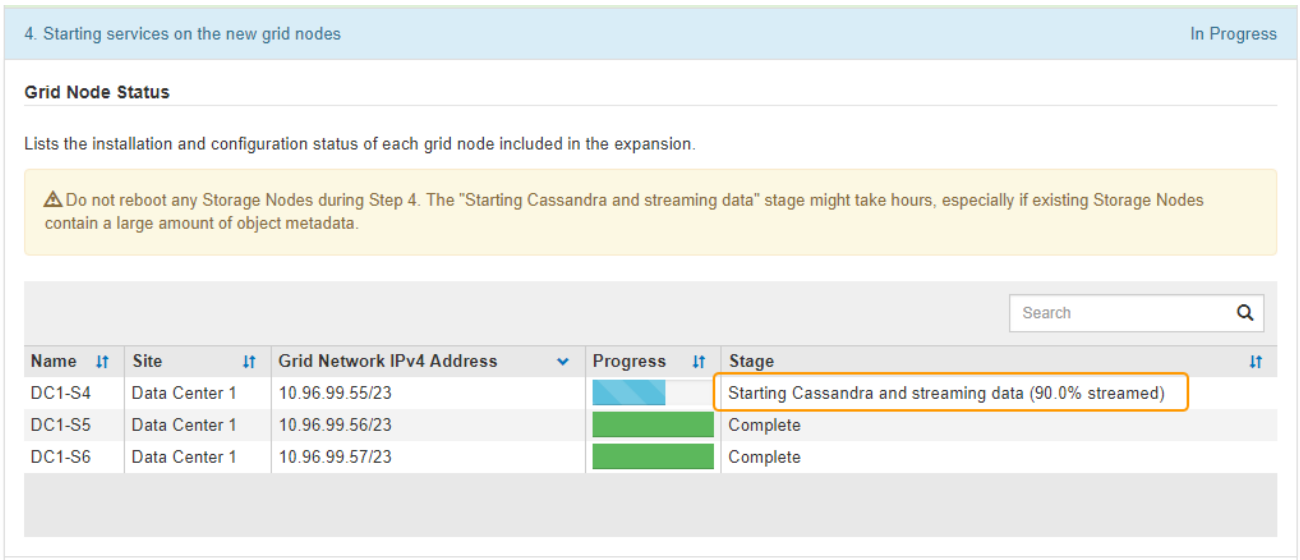
d. 将下载的恢复软件包文件（ .zip ）复制到两个安全的单独位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

9. 按照说明向现有站点添加存储节点或添加新站点。

将存储节点添加到现有站点

如果要向现有站点添加一个或多个存储节点，请查看状态消息中显示的百分比，以监控 " 启动 Cassandra 和流式传输数据 " 阶段的进度。



此百分比根据可用的 Cassandra 数据总量以及已写入新节点的数据量估计 Cassandra 流操作的完成程度。

> 请勿在 " 扩展 Cassandra 集群 " 或 " 启动 Cassandra 和流式数据 " 阶段重新启动任何存储节点。对于每个新存储节点，这些阶段可能需要花费数小时才能完成，尤其是在现有存储节点包含大量对象元数据的情况下。

添加新站点

如果要添加新站点，请使用 `nodetool status` 监控 Cassandra 流式传输的进度，并查看在 " 扩展 Cassandra 集群 " 阶段已向新站点复制多少元数据。新站点上的总数据负载应介于当前站点总负载的 20% 左右。

> 请勿在 " 扩展 Cassandra 集群 " 或 " 启动 Cassandra 和流式数据 " 阶段重新启动任何存储节点。对于每个新存储节点，这些阶段可能需要花费数小时才能完成，尤其是在现有存储节点包含大量对象元数据的情况下。

1. 继续监控扩展，直到所有任务均完成，并且 * 配置扩展 * 按钮再次出现。

完成后

根据您添加的网格节点类型，您必须执行其他集成和配置步骤。请参见 扩展后的配置步骤。

配置扩展系统

扩展后的配置步骤

完成扩展后，您必须执行其他集成和配置步骤。

关于此任务

您必须为要在扩展中添加的网格节点完成以下列出的配置任务。根据在安装和管理系统时选择的选项以及您希望如何配置在扩展期间添加的网格节点，某些任务可能是可选的。

步骤

1. 如果添加了存储节点，请完成以下配置任务：
   a. 查看 ILM 规则中使用的存储池，以确保使用新存储。请参见 使用 ILM 管理对象。
      - 如果您添加了站点，请为此站点创建一个存储池，并更新 ILM 规则以使用新的存储池。
      - 如果已将存储节点添加到现有站点，请确认新节点使用的存储级别正确。

      默认情况下，系统会将新的存储节点分配给所有存储节点存储级别，并将其添加到对站点使用该级别的存储池中。如果您希望新节点使用自定义存储级别，则必须手动将其分配给自定义级别（ * ILM * > * 存储级别 * ）。

   b. 验证存储节点是否正在载入对象。请参见 验证存储节点是否处于活动状态。
   c. 重新平衡擦除编码的数据（仅当无法添加建议数量的存储节点时）。请参见添加存储节点后重新平衡经过纠删编码的数据。
2. 如果添加了网关节点，请完成以下配置任务：
   - 如果将高可用性（ HA ）组用于客户端连接，则可以选择将网关节点添加到 HA 组。选择 * 配置 * > * 网络 * > * 高可用性组 * 以查看现有 HA 组列表并添加新节点。请参见 管理 StorageGRID。
3. 如果添加了管理节点，请完成以下配置任务：
   a. 如果为 StorageGRID 系统启用了单点登录（ Single Sign-On ， SSO ），请为新管理节点创建依赖方信任。创建此依赖方信任之前，您无法登录到此节点。请参见配置单点登录。
   b. 如果您计划在管理节点上使用负载平衡器服务、则可以选择将新的管理节点添加到HA组。选择*配置*网络高可用性组*以查看现有HA组列表并添加新节点。请参见 管理 StorageGRID。
   c. 如果要使每个管理节点上的属性和审核信息保持一致，也可以将管理节点数据库从主管理节点复制到扩展管理节点。请参见 复制管理节点数据库。
   d. 如果要使每个管理节点上的历史指标保持一致，也可以将 Prometheus 数据库从主管理节点复制到扩展管理节点。请参见 复制 Prometheus 指标。
   e. 如果要使每个管理节点上的历史日志信息保持一致，也可以将现有审核日志从主管理节点复制到扩展管理节点。请参见 复制审核日志。
   f. 或者，也可以通过 NFS 或 CIFS 文件共享配置对系统的访问以供审核。请参见 管理 StorageGRID。

      已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

g. 或者，也可以更改通知的首选发件人。您可以将扩展管理节点设置为首选发送器。否则，配置为首选发件人的现有管理节点将继续发送通知，包括 AutoSupport 消息， SNMP 通知，警报电子邮件和警报电子邮件（旧系统）。请参见 管理 StorageGRID。

4. 如果添加了归档节点，请完成以下配置任务。

   a. 配置归档节点与目标外部归档存储系统的连接。完成扩展后，归档节点将处于警报状态，直到您通过 * ARC/ * 目标 * 组件配置连接信息为止。请参见 管理 StorageGRID。

   b. 更新 ILM 策略以通过新的归档节点归档对象数据。请参见 使用 ILM 管理对象。

   c. 为用于监控从归档节点检索对象数据的速度和效率的属性配置自定义警报。请参见 管理 StorageGRID。

5. 要检查扩展节点是否是使用不可信客户端网络添加的，或者更改节点的客户端网络是不可信还是可信，请转到 * 配置 * > * 网络 * > * 不可信客户端网络 * 。

   如果扩展节点上的客户端网络不可信，则必须使用负载平衡器端点与客户端网络上的节点建立连接。请参见 管理 StorageGRID。

6. 配置域名系统（ DNS ）。

   如果您一直在为每个网格节点单独指定 DNS 设置，则必须为新节点添加自定义的每节点 DNS 设置。请参见 修改单网格节点的 DNS 配置。

   最佳做法是，网格范围的 DNS 服务器列表应包含一些可从每个站点本地访问的 DNS 服务器。如果您刚刚添加了一个新站点，请将该站点的新 DNS 服务器添加到网格范围的 DNS 配置中。

   > 为 DNS 服务器提供两到六个 IPv4 地址。您应选择 DNS 服务器，以便在网络隔离时每个站点都可以在本地访问这些服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以进一步自定义每个节点的 DNS 服务器列表。有关详细信息，请参见 修改单网格节点的 DNS 配置…

7. 如果添加了新站点，请确认网络时间协议（ NTP ）服务器可从该站点访问。请参见 配置 NTP 服务器。

   > 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

验证存储节点是否处于活动状态

添加新存储节点的扩展操作完成后， StorageGRID 系统应自动开始使用新存储节点。您必须使用 StorageGRID 系统验证新存储节点是否处于活动状态。

步骤

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 节点 * > * 扩展存储节点 _* > * 存储 * 。
3. 将光标悬停在 * 已用存储 - 对象数据 * 图上可查看 * 已用 * 的值，即已用于对象数据的总可用空间量。
4. 将光标移至图形右侧时，请验证 * 已用 * 的值是否正在增加。

复制管理节点数据库

通过扩展操作步骤 添加管理节点时，您可以选择将数据库从主管理节点复制到新的管理节点。通过复制数据库，您可以保留有关属性，警报和警报的历史信息。

您需要的内容

- 您已完成添加管理节点所需的扩展步骤。
- 您已有 `passwords.txt` 文件。
- 您具有配置密码短语。

关于此任务

StorageGRID 软件激活过程会在扩展管理节点上为 NMS 服务创建一个空数据库。当 NMS 服务在扩展管理节点上启动时，它会记录当前属于系统的服务器和服务的信息或稍后添加的服务器和服务的信息。此管理节点数据库包含以下信息：

- 警报历史记录
- 警报历史记录
- 历史属性数据，用于 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的图表和文本报告

为了确保管理节点数据库在节点之间保持一致，您可以将数据库从主管理节点复制到扩展管理节点。

> 将数据库从主管理节点（ _source 管理节点 _ ）复制到扩展管理节点可能需要数小时才能完成。在此期间，无法访问网格管理器。

在复制数据库之前，请按照以下步骤停止主管理节点和扩展管理节点上的 MI 服务和管理 API 服务。

步骤

1. 在主管理节点上完成以下步骤：
   a. 登录到管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 运行以下命令： `re封面访问点`
   c. 输入配置密码短语。
   d. 停止 MI 服务： `service mi stop`
   e. 停止管理应用程序接口（ mgmt-api ）服务： `service mgmt-api stop`
2. 在扩展管理节点上完成以下步骤：
   a. 登录到扩展管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。

b. 停止 MI 服务： `service mi stop`

c. 停止 mgmt-api 服务： `service mgmt-api stop`

d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

e. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

f. 将数据库从源管理节点复制到扩展管理节点： ` /usr/local/mi/bin/mi-clone-db.sh *Source_Admin_Node_IP*`

g. 出现提示时，确认要覆盖扩展管理节点上的 MI 数据库。

数据库及其历史数据将复制到扩展管理节点。完成复制操作后，此脚本将启动扩展管理节点。

h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

3. 在主管理节点上重新启动服务： `service servermanager start`

复制 **Prometheus** 指标

添加新的管理节点后，您可以选择将 Prometheus 维护的历史指标从主管理节点复制到新的管理节点。复制指标可确保管理节点之间的历史指标一致。

您需要的内容

- 新管理节点已安装并正在运行。
- 您已有 `passwords.txt` 文件。
- 您具有配置密码短语。

关于此任务

添加管理节点时，软件安装过程会创建一个新的 Prometheus 数据库。您可以通过将 Prometheus 数据库从主管理节点（ _source 管理节点 _ ）复制到新管理节点来保持节点之间的历史指标一致。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：

a. 输入以下命令： `ssh admin@ grid_node_ip_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

2. 从源管理节点中，停止 Prometheus 服务： `sservice Prometheus stop`

3. 在新管理节点上完成以下步骤：

a. 登录到新的管理节点：

   i. 输入以下命令： `ssh admin@ grid_node_ip_`

   ii. 输入 `passwords.txt` 文件中列出的密码。

   iii. 输入以下命令切换到 root： `su -`

   iv. 输入 `passwords.txt` 文件中列出的密码。

b. 停止 Prometheus 服务： `sservice Prometheus stop`

c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

d. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

e. 将 Prometheus 数据库从源管理节点复制到新的管理节点： ` /usr/local/Prometheus/bin/prometheus-clone-db.sh *Source_Admin_Node_IP*`

f. 出现提示时，按 * 输入 * 确认要销毁新管理节点上的新 Prometheus 数据库。

   原始 Prometheus 数据库及其历史数据将复制到新的管理节点。完成复制操作后，此脚本将启动新的管理节点。此时将显示以下状态：

`d`**已克隆数据库，正在启动服务**

a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入 …

   ```
   ssh-add -D
   ```

4. 在源管理节点上重新启动 Prometheus 服务。

   ```
   sService Prometheus start
   ```

复制审核日志

通过扩展操作步骤 添加新管理节点时，其 AMS 服务仅会记录在加入系统后发生的事件和操作。根据需要，您可以将审核日志从先前安装的管理节点复制到新的扩展管理节点，使其与 StorageGRID 系统的其余部分保持同步。

您需要的内容

- 您已完成添加管理节点所需的扩展步骤。
- 您已有 `passwords.txt` 文件。

关于此任务

要使历史审核消息在新管理节点上可用，必须手动将审核日志文件从现有管理节点复制到扩展管理节点。

默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：

- 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
- 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。

请参见 配置审核消息和日志目标 了解详细信息。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 停止 AMS 服务以防止其创建新文件： `sservice AMS stop`
3. 重命名 `audit.log` 文件，以确保它不会覆盖要将其复制到的扩展管理节点上的文件：

   `cd /var/local/audit/export + ls -l + mv audit.log new_name.txt`
4. 将所有审核日志文件复制到扩展管理节点：

   `scp -p * ip_address ： /var/local/audit/export`
5. 如果系统提示您输入 ` /root/.ssh/id_rsa` 的密码短语，请输入 `passwords.txt` 文件中列出的主管理节点的 SSH 访问密码。
6. 还原原始的 `audit.log` 文件：

   `mv new_name.txt audit.log`
7. 启动 AMS 服务：

   s服务 AMS 开始
8. 从服务器注销：

   退出
9. 登录到扩展管理节点：
   a. 输入以下命令： `ssh admin@ expansion Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

10. 更新审核日志文件的用户和组设置：

```
cd /var/local/audit/export + chown AMS-user ： byncast *
```

11. 从服务器注销：

退出

添加存储节点后重新平衡经过纠删编码的数据

在某些情况下，您可能需要在添加新存储节点后重新平衡经过纠删编码的数据。

您需要的内容

- 您已完成添加新存储节点的扩展步骤。
- 您已查看 重新平衡经过纠删编码的数据的注意事项。

> 只有在为站点上的一个或多个存储节点触发了 * 对象存储空间不足 * 警报且您无法添加建议数量的新存储节点时，才能执行此操作步骤 。

- 您了解此操作步骤 不会移动复制的对象数据，并且在确定将纠删编码的数据移动到何处时， EC 重新平衡操作步骤 不会考虑每个存储节点上的复制数据使用情况。
- 您已有 `passwords.txt` 文件。

关于此任务

当 EC 重新平衡操作步骤 运行时， ILM 操作以及 S3 和 Swift 客户端操作的性能可能会受到影响。因此，您只能在有限情况下执行此操作步骤 。

> EC 重新平衡操作步骤 会临时预留大量存储。可能会触发存储警报，但会在重新平衡完成后解决。如果没有足够的存储空间用于预留， EC 重新平衡操作步骤 将失败。无论操作步骤 出现故障还是成功， EC 重新平衡操作步骤 完成后都会释放存储预留。

> 如果需要超过 24 小时才能完成 EC 重新平衡操作步骤 期间用于上传对象（或对象部件）的 S3 和 Swift API 操作可能会失败。如果适用的 ILM 规则在载入时使用严格或平衡的放置方式，则长时间的 PUT 操作将失败。此时将报告以下错误：
>
> `500` 内部服务器错误

步骤

1. 【 Review object_storage]] 查看计划重新平衡的站点的当前对象存储详细信息。
   a. 选择 * 节点 * 。
   b. 选择站点上的第一个存储节点。
   c. 选择 * 存储 * 选项卡。
   d. 将光标悬停在 " 已用存储 - 对象数据 " 图表上，可查看存储节点上当前复制的数据量以及经过纠删编码的数据。

e. 重复上述步骤以查看站点上的其他存储节点。

2. 登录到主管理节点：

   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

3. 输入以下命令：

   `rebalance-data start -site "site-name"`

   对于 ` "site-name"` ，请指定添加新存储节点的第一个站点。请用引号将 `site-name` 括起来。

   此时将启动 EC 重新平衡操作步骤 ，并返回作业 ID 。

4. 复制作业 ID 。

5. 监控 EC 重新平衡操作步骤 的状态。

   - 要查看单个 EC 重新平衡操作步骤 的状态，请执行以下操作：

     `rebalance-data status -job-id job-id`

     对于 ` 作业 ID` ，指定启动操作步骤 时返回的 ID 。

   - 要查看当前 EC 重新平衡操作步骤 的状态以及先前完成的任何过程：

     `rebalance-data status`

     > 要获取有关 rebalance-data 命令的帮助，请执行以下操作：
     >
     > `rebalance-data — help`

   - 要查看当前作业的估计完成时间和完成百分比，请选择 * 支持 * > * 工具 * > * 指标 * 。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。

6. 根据返回的状态执行其他步骤：

   - 如果状态为 `In progress` ，则 EC 重新平衡操作仍在运行。您应定期监控操作步骤 ，直到其完成。
   - 如果状态为 `failure` ，请执行 失败步骤。
   - 如果状态为 `Success` ，请执行 成功步骤。

7. 如果 EC 重新平衡操作步骤 生成的负载过多（例如，载入操作受到影响），请暂停操作步骤 。

   `rebalance-data pause -job-id job-id`

8. 如果您需要终止 EC 重新平衡操作步骤 （例如，以便执行 StorageGRID 软件升级），请输入以下内容：

   `rebalance-data terminate -job-id job-id`

   > 终止 EC 重新平衡操作步骤 后，已移动的所有数据片段都将保留在新位置。数据不会移回原始位置。

9. 【 rebalance_fail 】如果 EC 重新平衡操作步骤 的状态为 `failure` ，请执行以下步骤：
   a. 确认站点上的所有存储节点均已连接到网格。
   b. 检查并解决可能影响这些存储节点的任何警报。

      有关特定警报的信息，请参见监控和故障排除说明。

   c. 重新启动 EC 重新平衡操作步骤： + `rebalance-data start – -job-id job-id`
   d. 如果 EC 重新平衡操作步骤 的状态仍为 `Failure` ，请联系技术支持。
10. `SEC` 重新平衡操作步骤 的状态为 " 无 `ccess` "（可选） 查看对象存储 以查看此站点的更新详细信息。

    现在，经过纠删编码的数据应在站点的存储节点之间更加平衡。

11. 如果要在多个站点上使用纠删编码，请对所有其他受影响站点运行此操作步骤 。

请联系技术支持

如果您在网格扩展过程中遇到无法解决的错误，或者网格任务失败，请联系技术支持。

关于此任务

联系技术支持时，您必须提供所需的日志文件，以帮助您解决遇到的错误。

步骤

1. 连接到发生故障的扩展节点：
   a. 输入以下命令：`ssh -p 8022 admin@ grid_node_ip_`

      > 端口 8022 是基础操作系统的 SSH 端口，而端口 22 是运行 StorageGRID 的容器引擎的 SSH 端口。

   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录后，提示符将从 ` $` 更改为 ` #` 。

2. 根据安装达到的阶段，检索网格节点上提供的以下任何日志：

平台	日志
VMware	• ` /var/log/daemon 。 log` • ` /var/log/storaggrid/daema.log` • ` /var/log/storaggrid/nodes/<node-name>.log`
Linux	• ` /var/log/storaggrid/daema.log` • ` /etc/storaggrid/nodes/<node-name>.conf` （对于每个故障节点） • ` /var/log/storaggrid/nodes/<node-name>.log` （对于每个故障节点，可能不存在）

恢复和维护

恢复和维护：概述

按照以下说明维护 StorageGRID 系统并从故障中恢复。

关于这些说明

这些说明介绍如何应用软件修补程序，恢复网格节点，恢复故障站点，停用网格节点或整个站点，执行网络维护，执行主机级别和中间件维护过程以及执行网格节点过程。

> 在这些说明中， "`Linux` " 是指 Red Hat ® Enterprise Linux ® ， Ubuntu ® ， CentOS 或 Debian ® 部署。使用 "NetApp 互操作性表工具" 以获取支持的版本列表。

开始之前

- 您对 StorageGRID 系统有着广泛的了解。
- 您已查看 StorageGRID 系统的拓扑并了解网格配置。
- 您知道必须严格按照所有说明进行操作，并注意所有警告。
- 您了解，不支持未介绍的维护过程或需要服务参与。

设备的维护过程

有关硬件过程，请参见 StorageGRID 设备的安装和维护说明。

- SG100 和 SG1000 服务设备
- SG6000 存储设备
- SG5700 存储设备
- SG5600 存储设备

下载恢复包

通过恢复包文件，您可以在发生故障时还原 StorageGRID 系统。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有配置密码短语。
- 您必须具有特定的访问权限。

在对 StorageGRID 系统进行网格拓扑更改之前或升级软件之前，请下载当前的恢复软件包文件。然后，在更改网格拓扑或升级软件后下载恢复包的新副本。

步骤

1. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
2. 输入配置密码短语，然后选择 * 开始下载 * 。

   下载将立即开始。

3. 下载完成后：
   a. 打开 ` .zip` 文件。
   b. 确认它包含 GPT-backup 目录和内部 ` .zip` 文件。
   c. 提取内部 ` .zip` 文件。
   d. 确认您可以打开 `passwords.txt` 文件。
4. 将下载的恢复软件包文件（` .zip` ）复制到两个安全的单独位置。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

相关信息

管理 StorageGRID

StorageGRID 热修补程序操作步骤

如果检测到软件问题并在功能版本之间得到解决，则可能需要将修补程序应用于 StorageGRID 系统。

StorageGRID 修补程序包含在功能或修补程序版本之外进行的软件更改。未来版本也会进行同样的更改。此外，每个热修补程序版本都包含此功能或修补程序版本中所有以前的修补程序的汇总。

应用修补程序的注意事项

应用修补程序时，系统会对 StorageGRID 系统中的节点应用累积系列软件更新。

当另一个维护操作步骤 正在运行时，您无法应用 StorageGRID 修补程序。例如，在停用，扩展或恢复操作步骤正在运行时，您无法应用修补程序。

如果节点或站点停用操作步骤 已暂停，您可以安全地应用修补程序。此外，您还可以在 StorageGRID 升级操作步骤 的最后阶段应用修补程序。有关详细信息，请参见有关升级 StorageGRID 软件的说明。

在网格管理器中上传此修补程序后，此修补程序将自动应用于主管理节点。然后，您可以批准将此修补程序应用于 StorageGRID 系统中的其余节点。

如果某个修补程序无法应用到一个或多个节点，则失败的原因将显示在该修补程序进度表的详细信息列中。您必须解决导致失败的任何问题，然后重试整个过程。先前已成功应用此修补程序的节点将在后续应用程序中跳过。您可以根据需要安全地重试此修复程序多次，直到所有节点均已更新为止。要使应用程序完成，必须在所有网格节点上成功安装此修补程序。

虽然网格节点会使用新的修补程序版本进行更新，但修补程序中的实际更改可能仅影响特定类型节点上的特定服务。例如，某个修补程序可能只会影响存储节点上的 LDR 服务。

如何应用修补程序进行恢复和扩展

在将修补程序应用到网格后，主管理节点会自动为通过恢复操作还原或添加到扩展中的任何节点安装相同的修补程序版本。

但是，如果需要恢复主管理节点，则必须手动安装正确的 StorageGRID 版本，然后应用此修补程序。主管理节点的最终 StorageGRID 版本必须与网格中其他节点的版本匹配。

以下示例说明了如何在恢复主管理节点时应用修补程序：

1. 假设网格运行的是具有最新修补程序的 StorageGRID 11.*A.B* 版本。"`网格版本` " 为 11.*A.B.y* 。
2. 主管理节点出现故障。
3. 您可以使用 StorageGRID 11.*A.B* 重新部署主管理节点，并执行恢复操作步骤 。

   根据需要，要与网格版本匹配，您可以在部署节点时使用次要版本；您无需先部署主要版本。

4. 然后，将修补程序 11.*A.B.y* 应用于主管理节点。

相关信息

配置替代主管理节点

规划并准备修补程序

您必须在应用修补程序之前进行规划，以确保 StorageGRID 系统的中断降至最低。

步骤

- 应用修补程序时对系统的影响
- 获取修补程序所需的材料
- 正在下载修补程序文件
- 在应用修补程序之前检查系统状况

应用修补程序时对系统的影响

您必须了解应用修补程序时 StorageGRID 系统将受到什么影响。

客户端应用程序可能会发生短期中断

StorageGRID 系统可以在整个修补程序过程中从客户端应用程序载入和检索数据；但是，如果修补程序需要在各个网关节点或存储节点上重新启动服务，则客户端与这些节点的连接可能会暂时中断。修复程序过程完成并在各个节点上恢复服务后，连接将恢复。

如果无法接受短时间内断开连接，您可能需要计划停机时间以应用修补程序。您可以使用选择性批准来计划某些节点的更新时间。

> 您可以使用多个网关和高可用性（ High Availability ， HA ）组在修复程序过程中提供自动故障转移。请参见的说明 配置高可用性组。

可能会触发警报和 **SNMP** 通知

当服务重新启动以及 StorageGRID 系统作为混合版本环境运行时（某些网格节点运行早期版本，而另一些网格节点已升级到更高版本），可能会触发警报和 SNMP 通知。通常，这些警报和通知将在修复程序完成时清除。

配置更改受限

将修补程序应用于 StorageGRID 时：

- 在对所有节点应用此修补程序之前，请勿进行任何网格配置更改（例如，指定网格网络子网或批准待定网格节点）。
- 在将此修补程序应用于所有节点之前，请勿更新 ILM 配置。

获取修复所需的材料

在应用修补程序之前，您必须获取所有必需的材料。

项目	注释：
StorageGRID 修补程序文件	您必须下载 StorageGRID 修补程序文件。
• 网络端口 • 支持的 Web 浏览器 • SSH 客户端（例如 PuTTY ）	
恢复软件包（` .zip` ）文件	应用修补程序之前， 下载最新的恢复软件包文件 如果在修复期间发生任何问题，请在应用此修复程序后下载恢复包文件的新副本并将其保存在安全位置。更新后的恢复包文件可用于在发生故障时还原系统。
Passwords.txt 文件	可选，只有在使用 SSH 客户端手动应用修补程序时才使用。`passwords.txt` 文件包含在该软件包中，该软件包是恢复软件包 ` .zip` 文件的一部分。

项目	注释：
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语未列在 `passwords.txt` 文件中。
相关文档	`reADME.txt` 此修补程序的文件。此文件包含在热修补程序下载页面中。在应用此修补程序之前，请务必仔细查看 `reADME` 文件。

相关信息

下载修补程序文件

下载修补程序文件

您必须先下载此修补程序文件，然后才能应用此修补程序。

步骤

1. 转到 StorageGRID 的 "NetApp 下载 " 页面。

   "NetApp 下载： StorageGRID"

2. 选择 * 可用软件 * 下的向下箭头可查看可供下载的修补程序列表。

   修补程序文件版本的格式为： 11.4_.x.y_ 。

3. 查看更新中包含的更改。

   如果您刚刚恢复了主管理节点，并且需要应用修补程序，请选择安装在其他网格节点上的相同修补程序版本。

   a. 选择要下载的热修补程序版本，然后选择 * 执行 * 。
   b. 使用您的 NetApp 帐户的用户名和密码登录。
   c. 阅读并接受最终用户许可协议。

      此时将显示选定版本的下载页面。

   d. 下载热修补程序 `reADME.txt` 文件以查看热修补程序中所含更改的摘要。

4. 选择此修补程序的下载按钮，然后保存此文件。

   请勿更改此文件的名称。

   如果您使用的是 macOS 设备，则此修补程序文件可能会自动保存为 ` .txt` 文件。如果是，则必须重命名此文件，而不使用 ` .txt` 扩展名。

5. 选择下载位置，然后选择 * 保存 * 。

相关信息

配置替代主管理节点

在应用修补程序之前，请检查系统的状况

您必须验证系统是否已准备好容纳此修补程序。

1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 如果可能，请确保系统运行正常，并且所有网格节点均已连接到网格。

   已连接节点具有绿色复选标记 在节点页面上。

3. 如果可能，请检查并解决任何当前警报。

   有关特定警报的信息，请参见 StorageGRID 监控和故障排除说明。

4. 确保未执行任何其他维护过程，例如升级，恢复，扩展或停用操作步骤 。

   应用修补程序之前，您应等待所有活动的维护过程完成。

   当另一个维护操作步骤 正在运行时，您无法应用 StorageGRID 修补程序。例如，在停用，扩展或恢复操作步骤 正在运行时，您无法应用修补程序。

   如果节点或站点停用操作步骤 已暂停，您可以安全地应用修补程序。此外，您还可以在 StorageGRID 升级操作步骤 的最后阶段应用修补程序。有关详细信息，请参见有关升级 StorageGRID 软件的说明。

相关信息

监控和故障排除

暂停和恢复存储节点的停用过程

应用修补程序

此修补程序会首先自动应用于主管理节点。然后，您必须批准将此修补程序应用于其他网格节点，直到所有节点运行相同的软件版本为止。您可以通过选择批准单个网格节点，网格节点组或所有网格节点来自定义批准顺序。

您需要的内容

- 您已查看注意事项并完成中的步骤 规划并准备修补程序。
- 您具有配置密码短语。
- 您具有 root 访问权限或维护权限。

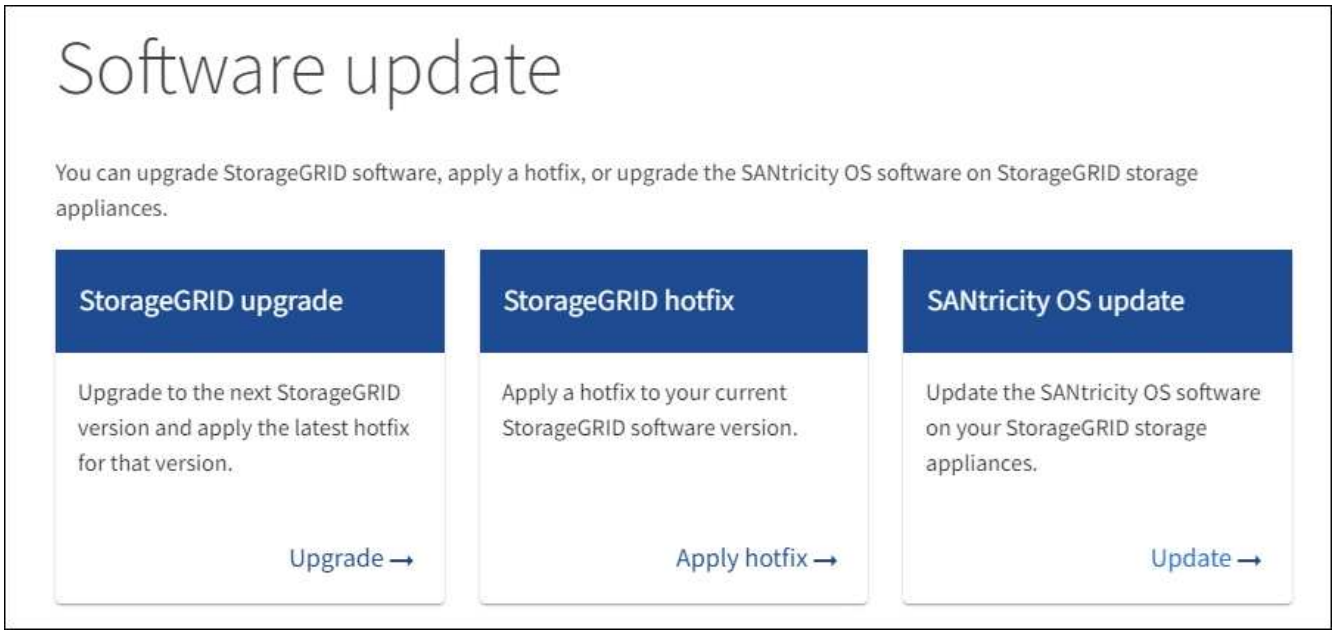
关于此任务

- 您可以延迟向节点应用修补程序，但只有在将修补程序应用到所有节点之后，此修补程序过程才会完成。
- 在完成修复程序过程之前，您无法执行 StorageGRID 软件升级或 SANtricity 操作系统升级。

步骤

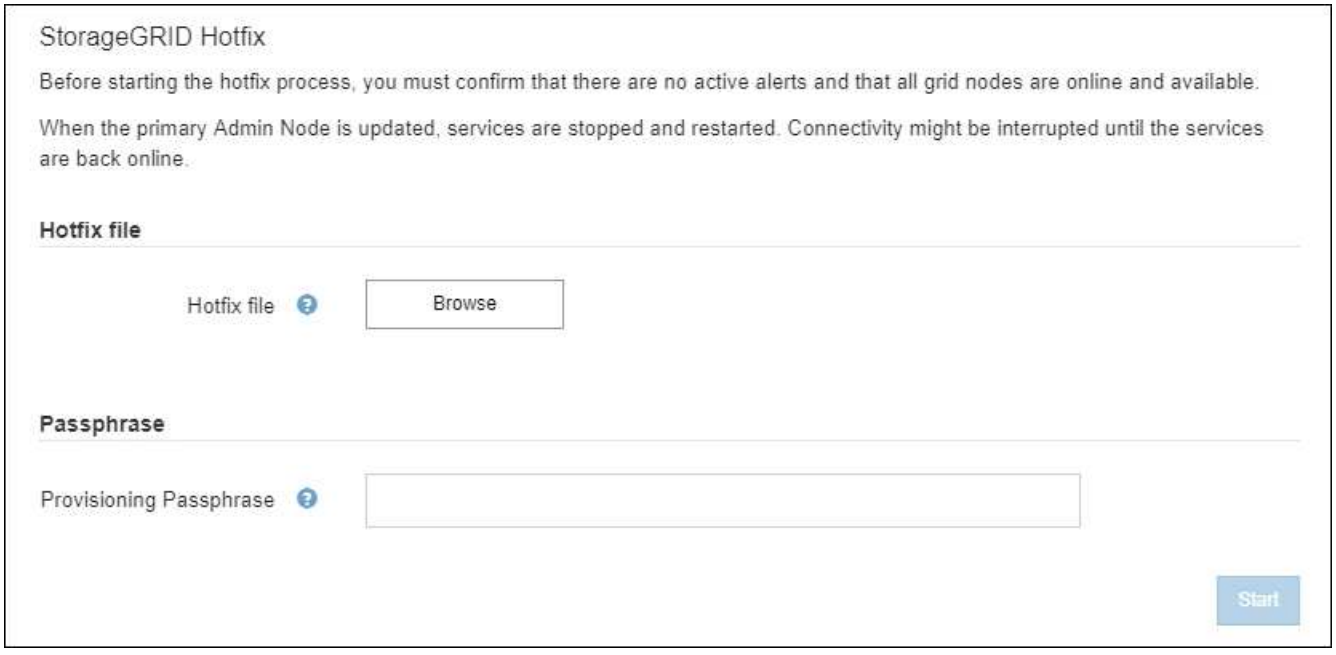
1. 使用登录到网格管理器 支持的 Web 浏览器。
2. 选择 * 维护 * > * 系统 * > * 软件更新 * 。

   此时将显示软件更新页面。



3. 选择 * 应用修补程序 * 。

   此时将显示 StorageGRID 热修补程序页面。



4. 选择从 NetApp 支持站点下载的修补程序文件。
   a. 选择 * 浏览 * 。
   b. 找到并选择文件。

`hotfix-install-version`

c. 选择 * 打开 * 。

已上传此文件。上传完成后，文件名将显示在详细信息字段中。

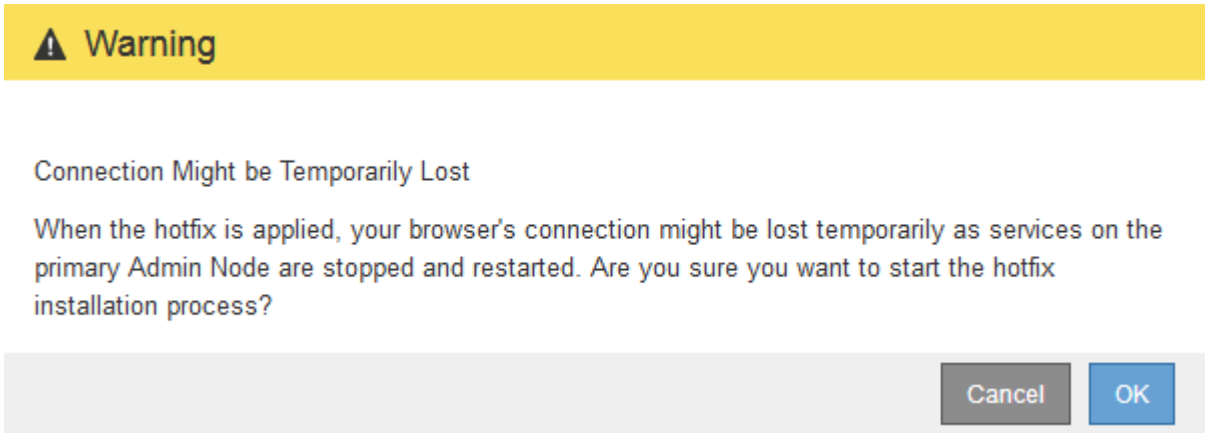
请勿更改文件名，因为它是验证过程的一部分。

5. 在文本框中输入配置密码短语。

此时将启用 * 开始 * 按钮。

6. 选择 * 开始 * 。

此时将显示一条警告，指出当主管理节点上的服务重新启动时，您的浏览器连接可能会暂时断开。



7. 选择 * 确定 * 开始将此修补程序应用于主管理节点。

当修复程序启动时：

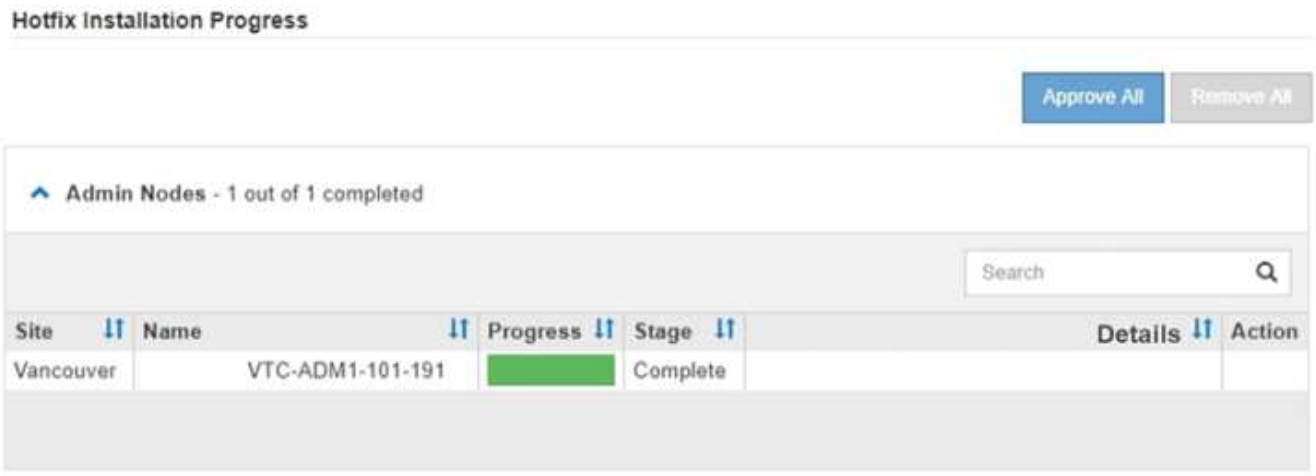
a. 此时将运行修补程序验证。

如果报告了任何错误，请予以解决，重新上传此修复程序文件，然后再次选择 * 启动 * 。

b. 此时将显示热修补程序安装进度表。此表显示了网格中的所有节点以及每个节点的修补程序安装的当前阶段。表中的节点按类型分组：

- 管理节点
- 网关节点
- 存储节点
- 归档节点

进度条将达到完成状态，然后会首先显示主管理节点，并显示阶段 "`complete" 。`



8. 或者，也可以按 * 站点 * ， * 名称 * ， * 进度 * ， * 阶段 * 或 * 详细信息 * 按升序或降序对每个分组中的节点列表进行排序。或者，在 * 搜索 * 框中输入一个术语以搜索特定节点。
9. 批准已准备好更新的网格节点。相同类型的已批准节点将一次升级一个。

   除非您确定节点已准备好进行更新，否则请勿批准节点的修补程序。将此修补程序应用于网格节点时，该节点上的某些服务可能会重新启动。对于与节点通信的客户端，这些操作可能会导致发生原因 服务中断。

   - 选择一个或多个 * 批准 * 按钮将一个或多个单独的节点添加到修补程序队列。
   - 在每个分组中选择 * 全部批准 * 按钮，将所有类型相同的节点添加到修补程序队列。如果您在 * 搜索 * 框中输入了搜索条件，则 * 全部批准 * 按钮将适用场景 所有搜索条件选择的节点。

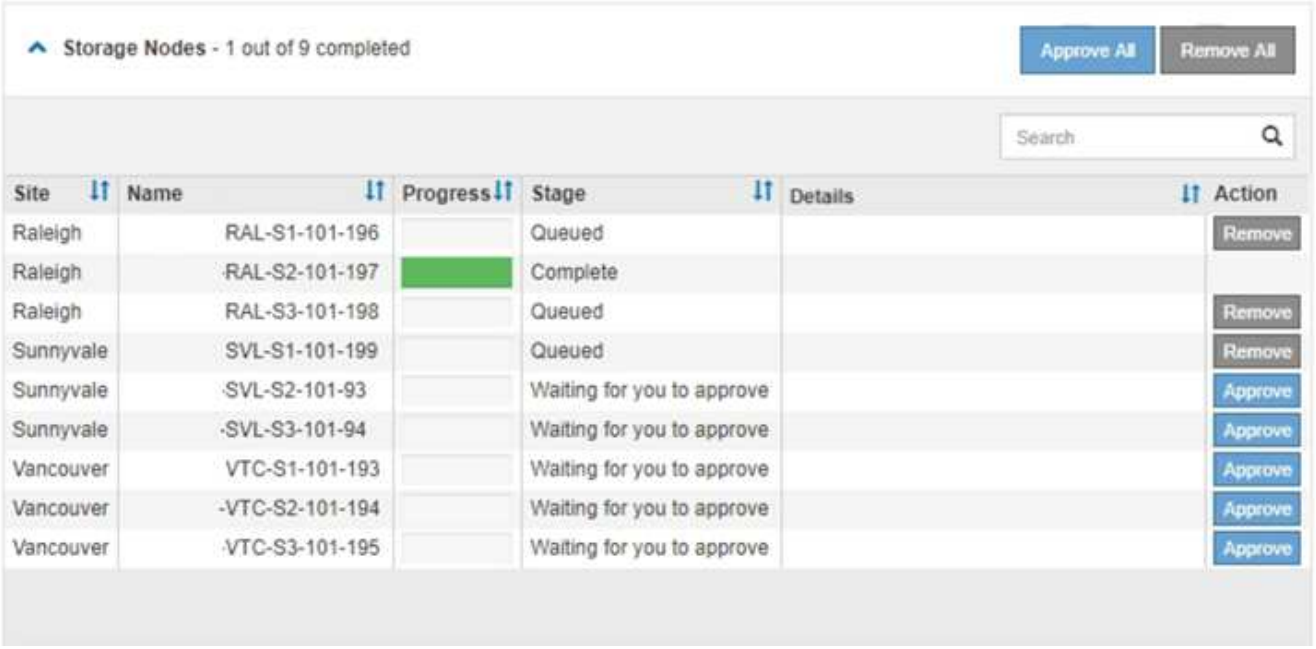
     页面顶部的 * 全部批准 * 按钮批准页面上列出的所有节点，而分组表顶部的 * 全部批准 * 按钮仅批准该组中的所有节点。如果节点升级顺序非常重要，请一次批准一个节点或一组节点，并等待每个节点完成升级，然后再批准下一个节点。

   - 选择页面顶部的顶级 * 全部批准 * 按钮，将网格中的所有节点添加到热修补程序队列。

     您必须先完成 StorageGRID 热修补程序，然后才能启动其他软件更新。如果无法完成此修补程序，请联系技术支持。

   - 选择 * 删除 * 或 * 全部删除 * 可从修补程序队列中删除一个节点或所有节点。

     当此阶段超过 "`Queued ，` " 时， * 删除 * 按钮将处于隐藏状态，您无法再从修补程序进程中删除此节点。



10. 请稍候，此修补程序将应用于每个已批准的网格节点。

    在所有节点上成功安装此修复程序后，热修复程序安装进度表将关闭。绿色横幅显示了完成修补程序的日期和时间。

11. 如果无法将此修补程序应用于任何节点，请查看每个节点的错误，解决问题描述 ，然后重复上述步骤。

    只有在将此修补程序成功应用于所有节点之后，操作步骤 才会完成。您可以根据需要安全地重试此修复程序多次，直到其完成为止。

相关信息

管理 StorageGRID

监控和故障排除

网格节点恢复过程

如果网格节点发生故障，您可以通过更换发生故障的物理或虚拟服务器，重新安装 StorageGRID 软件以及还原可恢复的数据来恢复该节点。

如果硬件，虚拟化，操作系统或软件故障导致节点无法运行或不可靠，则网格节点可能会发生故障。可能会发生多种类型的故障，从而需要恢复网格节点。

恢复网格节点的步骤因托管网格节点的平台和网格节点类型而异。每种类型的网格节点都有一个特定的恢复操作步骤 ，您必须严格遵循该恢复。

通常，您会尝试尽可能保留故障网格节点中的数据，修复或更换故障节点，使用网格管理器配置替代节点并还原节点的数据。

> 如果整个 StorageGRID 站点出现故障，请联系技术支持。技术支持将与您合作，制定和执行站点恢复计划，最大限度地提高已恢复的数据量，并满足您的业务目标。

相关信息

技术支持如何执行站点恢复

有关网格节点恢复的警告和注意事项

如果网格节点发生故障，您必须尽快恢复。开始之前，您必须查看节点恢复的所有警告和注意事项。

StorageGRID 是一个分布式系统，由多个节点组成，这些节点彼此协同工作。请勿使用磁盘快照还原网格节点。请参阅每种类型节点的恢复和维护过程。

尽快恢复出现故障的网格节点的一些原因包括：

- 出现故障的网格节点可以减少系统和对象数据的冗余，因此，如果另一个节点发生故障，您容易受到永久数据丢失的风险。
- 网格节点发生故障可能会影响 Day - 到 - Day 操作的效率。
- 出现故障的网格节点可能会降低您监控系统操作的能力。
- 如果存在严格的 ILM 规则，则出现故障的网格节点可能会发生原因 a 500 internal server error 。
- 如果未及时恢复网格节点，则恢复时间可能会增加。例如，可能会出现需要在恢复完成之前清除的队列。

对于要恢复的特定网格节点类型，请始终遵循恢复操作步骤 。恢复过程因主管理节点或非主管理节点，网关节点，归档节点，设备节点和存储节点而异。

恢复网格节点的前提条件

恢复网格节点时，系统会假设以下所有条件：

- 已更换并配置发生故障的物理或虚拟硬件。
- 替代设备上的 StorageGRID 设备安装程序版本与 StorageGRID 系统的软件版本匹配，如用于验证和升级 StorageGRID 设备安装程序版本的硬件安装和维护中所述。
  - SG100 和 SG1000 服务设备
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备
- 如果要恢复的网格节点不是主管理节点，则要恢复的网格节点与主管理节点之间会建立连接。

托管多个网格节点的服务器发生故障时的节点恢复顺序

如果托管多个网格节点的服务器发生故障，您可以按任意顺序恢复节点。但是，如果发生故障的服务器托管主管理节点，则必须先恢复该节点。首先恢复主管理节点可防止其他节点在等待与主管理节点联系时暂停恢复。

已恢复节点的 **IP** 地址

请勿尝试使用当前已分配给任何其他节点的 IP 地址恢复节点。部署新节点时，请使用故障节点的当前 IP 地址或未使用的 IP 地址。

如果您使用新 IP 地址部署新节点，然后恢复该节点，则新 IP 地址将继续用于已恢复的节点。如果要还原到原始 IP 地址，请在恢复完成后使用更改 IP 工具。

收集网格节点恢复所需的材料

在执行维护过程之前，您必须确保具有必要的材料来恢复出现故障的网格节点。

项目	注释：
StorageGRID 安装归档	如果需要恢复网格节点，则需要 下载 StorageGRID 安装文件 适用于您的平台。 • 注意： * 如果要恢复存储节点上的故障存储卷，则不需要下载文件。
服务笔记本电脑	服务笔记本电脑必须具有以下组件： • 网络端口 • SSH 客户端（例如 PuTTY ） • 支持的 Web 浏览器
恢复软件包 ` .zip` 文件	获取最新恢复软件包 ` .zip` 文件的副本： `sGWS-recovery-package-id-revision.zip` 每次修改系统时，都会更新 ` .zip` 文件的内容。在进行此类更改后，系统会指示您将最新版本的恢复软件包存储在安全位置。使用最新副本从网格故障中恢复。 如果主管理节点运行正常，您可以从网格管理器下载恢复软件包。选择 * 维护 * > * 系统 * > * 恢复软件包 * 。 如果您无法访问网格管理器，则可以在包含此 ADC 服务的某些存储节点上找到恢复软件包的加密副本。在每个存储节点上，检查恢复软件包的位置： ` /var/local/install/sgws-recovery-package-*grid-revision*.zip 。 gpg` 使用修订版号最高的恢复软件包。
`passwords.txt` file	包含访问命令行上的网格节点所需的密码。包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
适用于您的平台的最新文档	请访问平台供应商的网站以获取相关文档。 有关您的平台当前支持的版本，请参见 "NetApp 互操作性表工具"。

下载并提取 **StorageGRID** 安装文件

下载软件并提取文件，除非您这样做 恢复存储节点上的故障存储卷。

您必须使用网格上当前运行的 StorageGRID 版本。

步骤

1. 确定当前安装的软件版本。从网格管理器顶部，选择帮助图标并选择 * 关于 * 。
2. 转至 "StorageGRID 的 "NetApp 下载 " 页面"。
3. 选择网格上当前运行的 StorageGRID 版本。

   StorageGRID 软件版本采用以下格式： `11.x.y` 。
4. 使用您的 NetApp 帐户的用户名和密码登录。
5. 阅读最终用户许可协议，选中复选框，然后选择 * 接受并继续 * 。
6. 在下载页面的 * 安装 StorageGRID * 列中，为您的平台选择 ` .tgz` 或 ` .zip` 文件。

   安装归档文件中显示的版本必须与当前安装的软件版本匹配。

   如果您运行的是 Windows ，请使用 ` .zip` 文件。

平台	安装归档
Red Hat Enterprise Linux 或 CentOS	`storageGRID-Webscale -version-RPM-uniqueID.zip` `StorageGRID-Webscale -version-RPM-uniqueID.tgz`
Ubuntu ， Debian 或设备	`storageGRID-Webscale -version-Deb-uniqueID_.zip` `StorageGRID-Webscale -version-Deb-uniqueID_.tgz`
VMware	`storageGRID-Webscale -version-vmware-uniqueID.zip` `StorageGRID-Webscale -version-vmware-uniqueID.tgz`

7. 下载并提取归档文件。
8. 根据您的平台以及需要恢复的网格节点，按照适用于您的平台的步骤选择所需的文件。

   步骤中为每个平台列出的路径与归档文件安装的顶级目录相对。
9. 如果要恢复 Red Hat Enterprise Linux 或 CentOS 系统下，选择相应的文件。

路径和文件名	Description
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 节点映像。

路径和文件名	Description
	RPM 软件包，用于在 RHEL 或 CentOS 主机上安装 StorageGRID 主机服务。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 RHEL 或 CentOS 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 *： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要恢复 Ubuntu 或 Debian 系统下，选择相应的文件。

路径和文件名	Description
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。

路径和文件名	Description
	文件 ` /debs/storagegrid-webscale-images-version-SHA.deb` 的 MD5 校验和。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	Description
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
	StorageGRID 的 API 架构。 • 注意 * ： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要恢复 VMware 系统下，选择相应的文件。

路径和文件名	Description
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。

路径和文件名	Description
	用于部署主管理节点的开放式虚拟化格式模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署非主管理节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署归档节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署网关节点的模板文件（`.OVF`）和清单文件（`.MF`）。
	用于部署基于虚拟机的存储节点的模板文件（`.OVF`）和清单文件（`.MF`）。
部署脚本工具	Description
	Bash shell 脚本，用于自动部署虚拟网格节点。
	与 `deept-vsphere-ovftool.sh` 脚本结合使用的示例配置文件。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。
	与 `configure-storaggrid.py` 脚本结合使用的示例配置文件。
	用于 `configure-storaggrid.py` 脚本的空配置文件。
	StorageGRID 的 API 架构。 • 注意 *： 在执行升级之前，如果您没有用于升级兼容性测试的非生产 StorageGRID 环境，则可以使用这些架构确认为使用 StorageGRID 管理 API 编写的任何代码都与新的 StorageGRID 版本兼容。

1. 如果要恢复基于 StorageGRID 设备的系统，请选择相应的文件。

路径和文件名	Description
	用于在设备上安装 StorageGRID 节点映像的 Deb 软件包。
	StorageGRID 设备安装程序使用的 Deb 安装包的校验和，用于验证该软件包在上传后是否完好无损。

对于设备安装，只有在需要避免网络流量时，才需要这些文件。设备可以从主管理节点下载所需文件。

选择节点恢复操作步骤

您必须为出现故障的节点类型选择正确的恢复操作步骤 。

网格节点	恢复操作步骤
多个存储节点	请联系技术支持。如果多个存储节点出现故障，技术支持必须协助恢复，以防止数据库不一致导致数据丢失。可能需要站点恢复操作步骤 。 技术支持如何执行站点恢复
一个存储节点	存储节点恢复操作步骤 取决于故障的类型和持续时间。 从存储节点故障中恢复
管理节点	管理节点操作步骤 取决于您是需要恢复主管理节点还是非主管理节点。 从管理节点故障中恢复
网关节点	从网关节点故障中恢复。
归档节点	从归档节点故障中恢复。

如果托管多个网格节点的服务器发生故障，您可以按任意顺序恢复节点。但是，如果发生故障的服务器托管主管理节点，则必须先恢复该节点。首先恢复主管理节点可防止其他节点在等待与主管理节点联系时暂停恢复。

从存储节点故障中恢复

用于恢复故障存储节点的操作步骤 取决于故障类型和故障存储节点的类型。

使用此表为出现故障的存储节点选择恢复操作步骤 。

问题描述	Action	注释：
• 多个存储节点出现故障。 • 第二个存储节点在存储节点发生故障或恢复后不到 15 天出现故障。 这包括在恢复另一个存储节点期间存储节点出现故障的情况。	您必须联系技术支持。	如果所有故障存储节点都位于同一站点，则可能需要执行站点恢复操作步骤 。 技术支持将评估您的情况并制定恢复计划。 技术支持如何执行站点恢复 在 15 天内恢复多个存储节点（或多个存储节点）可能会影响 Cassandra 数据库的完整性，从而可能导致发生原因 数据丢失。 技术支持可以确定何时可以安全地开始恢复第二个存储节点。 • 注意 * ：如果某个站点上有多个包含此 ADA 服务的存储节点发生故障，则该站点的任何待定平台服务请求都将丢失。
存储节点已脱机超过 15 天。	将存储节点恢复到关闭状态超过 15 天	要确保 Cassandra 数据库的完整性，需要使用此操作步骤 。
设备存储节点出现故障。	恢复设备存储节点	对于所有故障，设备存储节点的恢复操作步骤 均相同。
一个或多个存储卷发生故障，但系统驱动器完好无损	从系统驱动器完好无损的存储卷故障中恢复	此操作步骤 用于基于软件的存储节点。
系统驱动器出现故障。	从系统驱动器故障中恢复	节点更换操作步骤 取决于部署平台以及是否有任何存储卷也出现故障。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

将存储节点恢复到关闭状态超过 **15** 天

如果一个存储节点脱机且未连接到其他存储节点超过 15 天，则必须在此节点上重建 Cassandra 。

您需要的内容

- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）

- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）

关于此任务

存储节点具有包含对象元数据的 Cassandra 数据库。如果某个存储节点无法与其他存储节点通信超过 15 天，则 StorageGRID 会假定该节点的 Cassandra 数据库已过时。在使用其他存储节点中的信息重建 Cassandra 之前，存储节点无法重新加入网格。

只有当一个存储节点关闭时，才可以使用此操作步骤 来重建 Cassandra 。如果其他存储节点已脱机或在过去 15 天内已在另一个存储节点上重建 Cassandra ，请联系技术支持；例如，在恢复故障存储卷或恢复故障存储节点的过程中， Cassandra 可能已重建。

如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

步骤

1. 如有必要，打开需要恢复的存储节点的电源。
2. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。 +

如果无法登录到网格节点，则系统磁盘可能不会损坏。转至的操作步骤 从系统驱动器故障中恢复。

1. 对存储节点执行以下检查：
   a. 问题描述 此命令： `nodetool status`

      输出应为 `Connection refused.`

   b. 在网格管理器中，选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   c. 选择 * 站点 _* > * 存储节点 * > * SSM* > * 服务 * 。验证 Cassandra 服务是否显示 `not running` 。
   d. 选择 * 存储节点 * > * SSM* > * 资源 * 。验证卷部分中是否没有错误状态。
   e. 问题描述 此命令： `grep -i Cassandra /var/local/log/servermanager.log`

您应在输出中看到以下消息：

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. 问题描述 此命令并监控脚本输出： `check-Cassandra-rebuild`
   - 如果存储服务正在运行，系统将提示您停止这些服务。输入： *
   - 查看脚本中的警告。如果不适用，请确认您要重建 Cassandra 。输入： *

> 某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

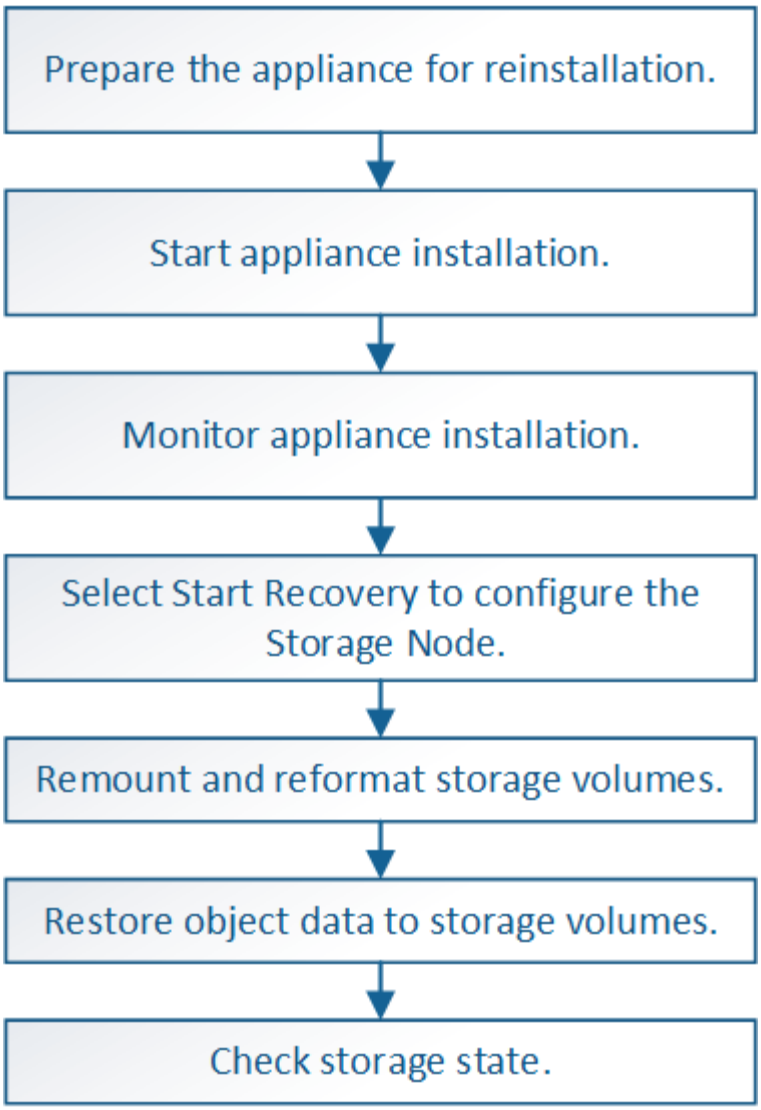
3. 重建完成后，请执行以下检查：
   a. 在网格管理器中，选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
   b. 选择 * 站点 _* > * 已恢复存储节点 * > * SSM* > * 服务 * 。
   c. 确认所有服务均已运行。
   d. 选择 * DDS* > * 数据存储 * 。
   e. 确认 * 数据存储状态 * 为 "`up` " ， * 数据存储状态 * 为 "`Normal" 。`

恢复设备存储节点

无论您是从系统驱动器丢失还是仅从存储卷丢失中恢复，用于恢复出现故障的 StorageGRID 设备存储节点的操作步骤 都是相同的。

关于此任务

您必须准备设备并重新安装软件，配置节点以重新加入网格，重新格式化存储以及还原对象数据。



如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。在 15 天内在两个或多个存储节点上重建 Cassandra 可能会导致数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

如果在恢复期间遇到服务：状态 - Cassandra （ SVST ）警报，请参见有关通过重建 Cassandra 从警报中恢复的监控和故障排除说明。重建 Cassandra 后，应清除警报。如果未清除警报，请联系技术支持。

有关硬件维护过程，例如更换控制器或重新安装 SANtricity OS 的说明，请参见存储设备的安装和维护说明。

相关信息

监控和故障排除

SG6000 存储设备

SG5700 存储设备

SG5600 存储设备

准备要重新安装的设备存储节点

恢复设备存储节点时，必须先准备设备以重新安装 StorageGRID 软件。

1. 登录到发生故障的存储节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 准备设备存储节点以安装 StorageGRID 软件。`sgareinstall`
3. 当系统提示您继续时，输入： `y`

   设备将重新启动， SSH 会话将结束。StorageGRID 设备安装程序通常需要大约 5 分钟才能投入使用，但在某些情况下，您可能需要等待长达 30 分钟。

   StorageGRID 设备存储节点已重置，并且无法再访问存储节点上的数据。在初始安装过程中配置的 IP 地址应保持不变；但是，建议您在操作步骤 完成后进行确认。

   执行 `sgareinstall` 命令后，将删除所有 StorageGRID 配置的帐户，密码和 SSH 密钥，并生成新的主机密钥。

开始安装 **StorageGRID** 设备

要在设备存储节点上安装 StorageGRID ，请使用设备中提供的 StorageGRID 设备安装程序。

您需要的内容

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路和 IP 地址。
- 您知道 StorageGRID 网格的主管理节点的 IP 地址。

- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 您已按照存储设备的安装和维护说明完成以下前提条件任务：
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备
- 您正在使用 支持的 Web 浏览器。
- 您知道分配给设备中计算控制器的一个 IP 地址。您可以使用管理网络（控制器上的管理端口 1 ），网格网络或客户端网络的 IP 地址。

关于此任务

要在设备存储节点上安装 StorageGRID ，请执行以下操作：

- 您可以指定或确认主管理节点的 IP 地址和节点名称。
- 您开始安装，并等待卷配置完毕并安装软件。
- 在整个过程中，安装将暂停。要恢复安装，您必须登录到网格管理器，并将待定存储节点配置为故障节点的替代节点。
- 配置节点后，设备安装过程将完成，设备将重新启动。

步骤

1. 打开浏览器并输入设备中计算控制器的 IP 地址之一。

   ` + https://Controller_IP:8443+`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

   假设主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上， StorageGRID 设备安装程序可以自动发现此 IP 地址。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

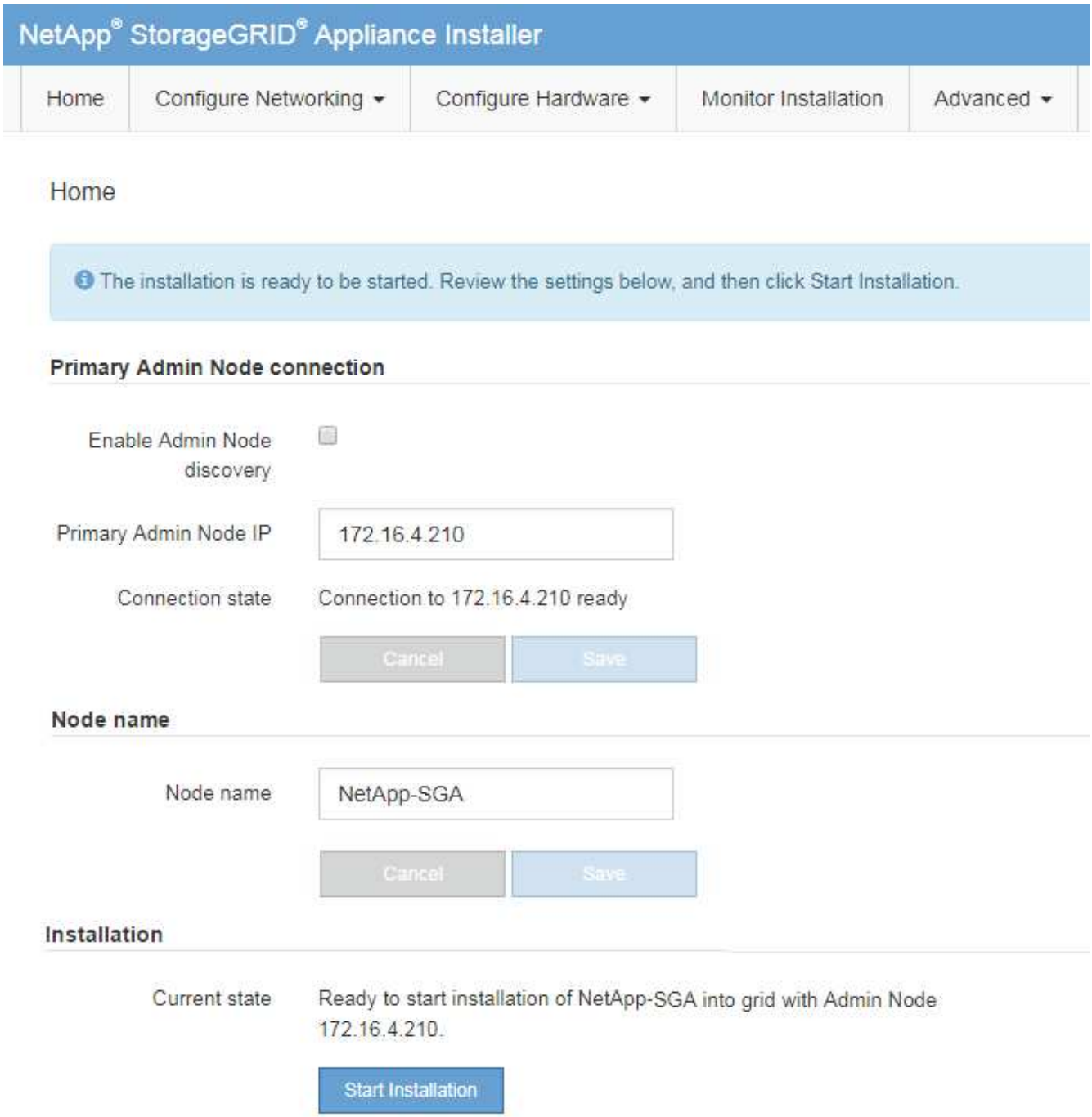
选项	步骤
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

选项	步骤
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 从已发现的 IP 地址列表中，选择要部署此设备存储节点的网格的主管理节点。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

4. 在 * 节点名称 * 字段中，输入与要恢复的节点相同的名称，然后单击 * 保存 * 。
5. 在安装部分中，确认当前状态为 "`Ready to start installation of node name into grid with Primary Admin Node admin_IP` " ，并且已启用 * 开始安装 * 按钮。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

6. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。



当前状态将更改为 "`Installation is in progress，`"，此时将显示监控器安装页面。

如果需要手动访问监控器安装页面，请单击菜单栏中的 * 监控器安装 * 。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

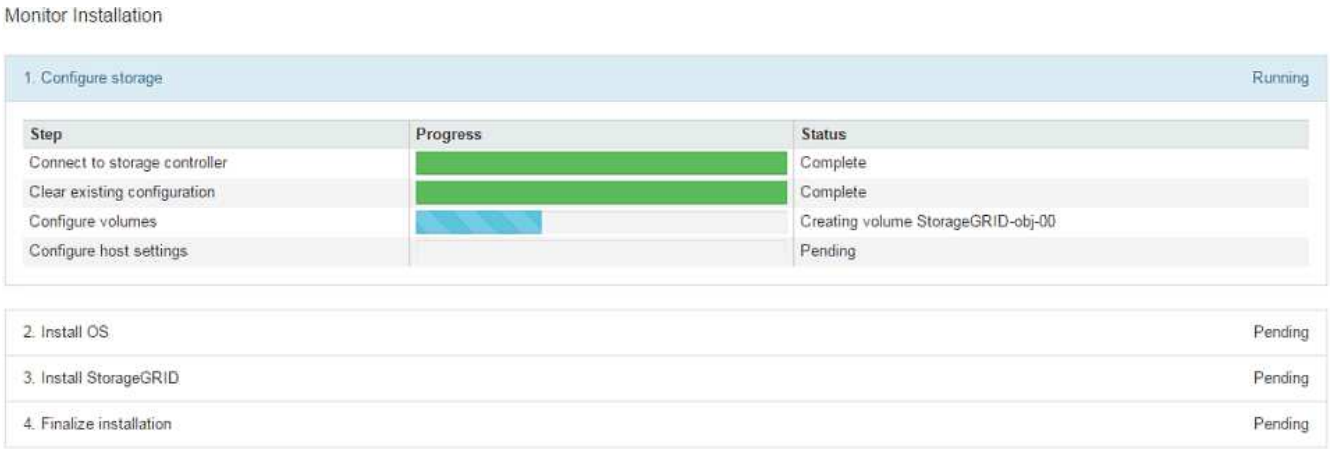
SG5700 存储设备

SG5600 存储设备

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

1. 要监控安装进度，请单击菜单栏中的 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

2. 查看前两个安装阶段的进度。

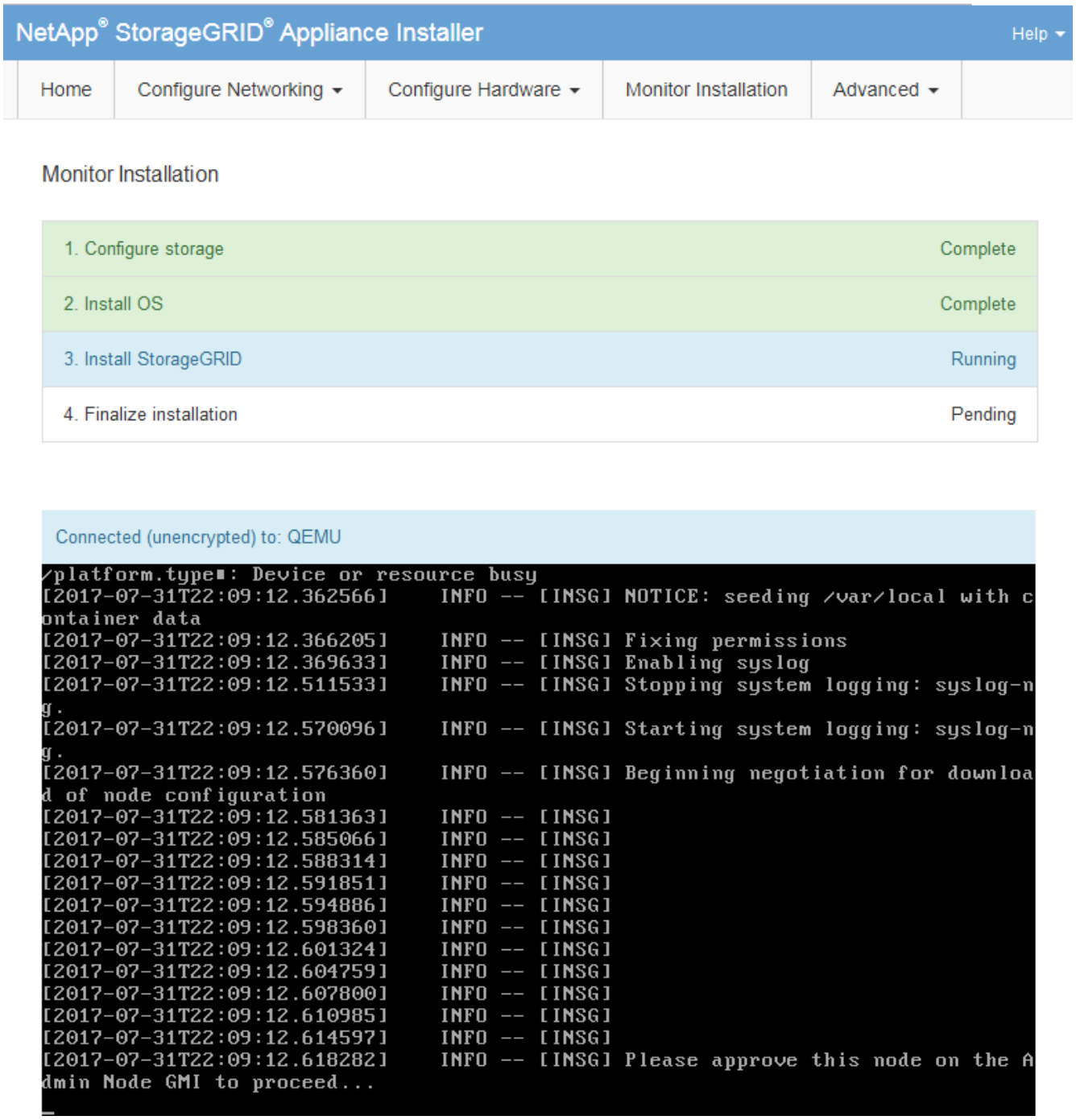
   ◦ * 。配置存储 *

   在此阶段，安装程序将连接到存储控制器，清除任何现有配置，与 SANtricity 软件通信以配置卷以及配置主机设置。

   ◦ * 。安装 OS*

   在此阶段，安装程序会将 StorageGRID 的基本操作系统映像复制到设备。

3. 继续监控安装进度，直到 * 安装 StorageGRID 网格管理器 * 阶段暂停，并且嵌入式控制台上显示一条消息，提示您使用网格管理器在管理节点上批准此节点。



4. 转至操作步骤 以配置设备存储节点。

选择 **Start Recovery** 以配置设备存储节点

您必须在网格管理器中选择启动恢复，才能将设备存储节点配置为故障节点的替代节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。

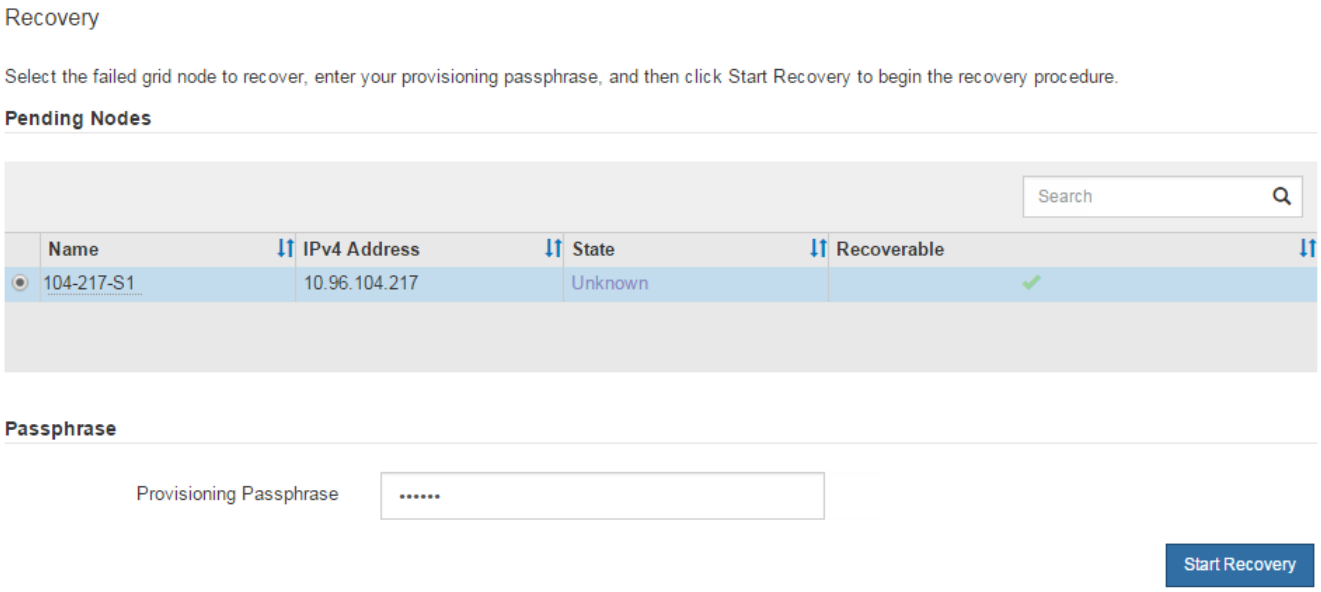
- 您必须已部署恢复设备存储节点。
- 您必须知道擦除编码数据的任何修复作业的开始日期。
- 您必须已确认过去 15 天内未重建此存储节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

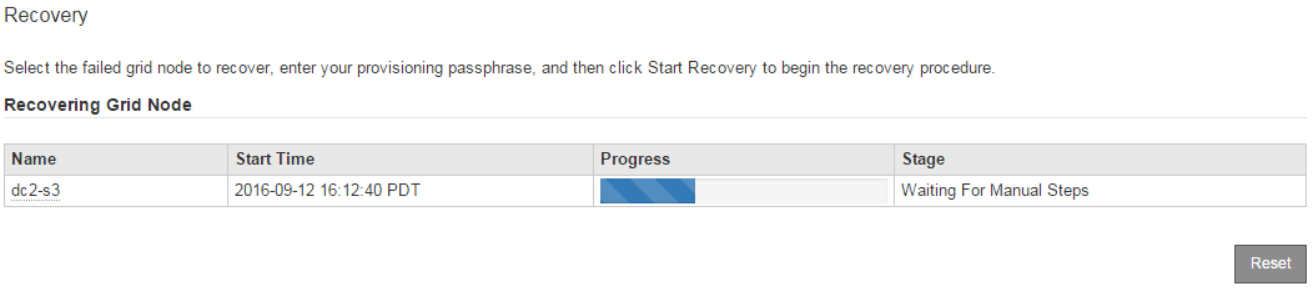
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。

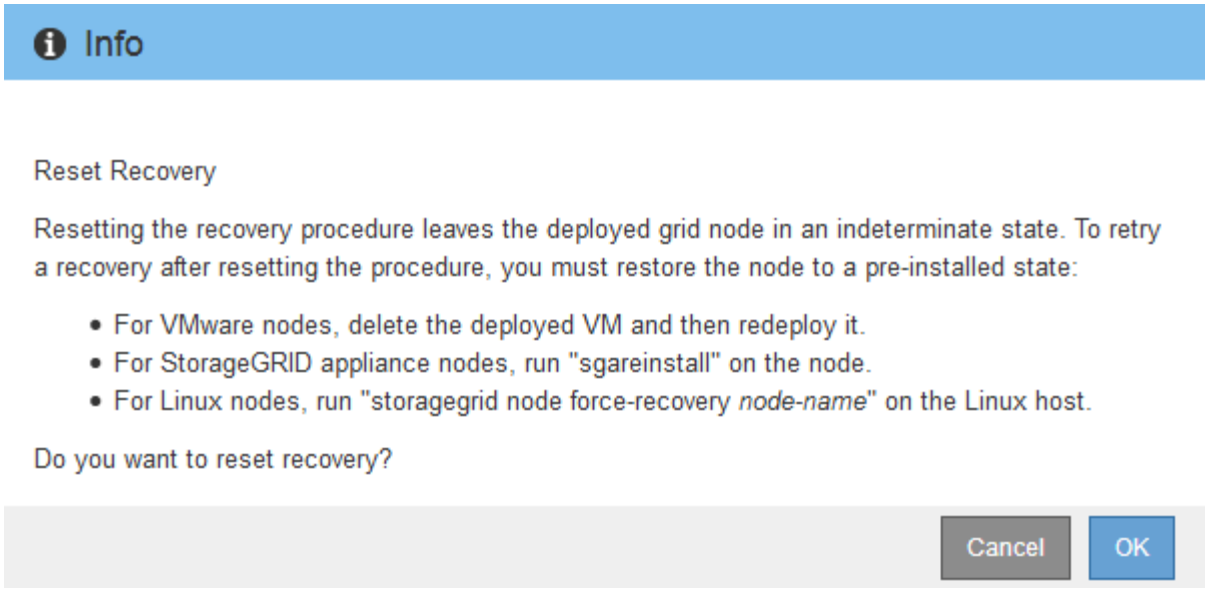


5. 在恢复网格节点表中监控恢复进度。

   当网格节点达到 "`Waiting for Manual steps` " 阶段时，转到下一主题并执行手动步骤以重新挂载和重新格式化设备存储卷。



在恢复期间的任何时刻，您都可以单击 * 重置 * 来启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，则必须通过在该节点上运行 `sgareinstall` 将设备节点还原到预安装状态。

重新挂载并重新格式化设备存储卷（ " 手动步骤 " ）

您必须手动运行两个脚本，才能重新挂载保留的存储卷并重新格式化任何发生故障的存储卷。第一个脚本将重新挂载格式正确的卷，使其格式化为 StorageGRID 存储卷。第二个脚本将重新格式化所有已卸载的卷，根据需要重新构建 Cassandra 数据库并启动服务。

您需要的内容

- 您已更换已知需要更换的任何故障存储卷的硬件。

  运行 `sn-remount-volumes` 脚本可能有助于您确定其他故障存储卷。

- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）
- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）

> 如果多个存储节点脱机或此网格中的存储节点在过去 15 天内已重建，请联系技术支持。请勿运行 `sn-recovery-postinstall.sh` 脚本。在两个或多个存储节点上相互重建 Cassandra 的 15 天内可能会导致数据丢失。

关于此任务

要完成此操作步骤 ，请执行以下高级任务：

- 登录到已恢复的存储节点。
- 运行 `sn-remount-volumes` 脚本重新挂载格式正确的存储卷。运行此脚本时，它将执行以下操作：
  - 挂载和卸载每个存储卷以重放 XFS 日志。
  - 执行 XFS 文件一致性检查。
  - 如果文件系统一致，则确定存储卷是否为格式正确的 StorageGRID 存储卷。

- 如果存储卷格式正确，请重新挂载该存储卷。卷上的所有现有数据保持不变。

- 查看脚本输出并解决任何问题。
- 运行 `sn-recovery-postinstall.sh` 脚本。运行此脚本时，它将执行以下操作。

> 在运行 `sn-recovery-postinstall.sh` （步骤 4 ）重新格式化故障存储卷并还原对象元数据之前，请勿在恢复期间重新启动存储节点。在 `sn-recovery-postinstall.sh` 完成之前重新启动存储节点会导致尝试启动的服务出错，并导致 StorageGRID 设备节点退出维护模式。

  - 重新格式化 `sn-remount-volumes` 脚本无法挂载或发现格式不正确的任何存储卷。

> 如果重新格式化某个存储卷，则该卷上的所有数据都将丢失。假设已将 ILM 规则配置为存储多个对象副本，则必须执行额外的操作步骤 以从网格中的其他位置还原对象数据。

  - 如果需要，在节点上重建 Cassandra 数据库。
  - 启动存储节点上的服务。

步骤

1. 登录到已恢复的存储节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 运行第一个脚本重新挂载任何格式正确的存储卷。

> 如果所有存储卷都是新的，需要进行格式化，或者所有存储卷都出现故障，您可以跳过此步骤并运行第二个脚本，重新格式化所有已卸载的存储卷。

   a. 运行以下脚本： `sn-remount-volumes`

   此脚本可能需要数小时才能在包含数据的存储卷上运行。

   b. 在脚本运行期间，查看输出并问题解答 任何提示。

> 根据需要，您可以使用 `tail -f` 命令监控脚本日志文件的内容（` /var/local/log/SN-remount-volumes.log` ）。日志文件包含比命令行输出更详细的信息。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
```

```
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
```

```
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

在示例输出中，一个存储卷已成功重新挂载，三个存储卷出现错误。

- ` /dev/sdb` 通过了 XFS 文件系统一致性检查，并具有有效的卷结构，因此已成功重新挂载。此脚本重新挂载的设备上的数据将保留下来。
- 由于存储卷是新的或已损坏， ` /dev/sdc` 未通过 XFS 文件系统一致性检查。
- 无法挂载 ` /dev/sdd` ，因为磁盘已取消初始化或磁盘的超级块已损坏。当脚本无法挂载存储卷时，它会询问您是否要运行文件系统一致性检查。
  - 如果存储卷已连接到新磁盘，请将 * N * 问题解答 到提示符处。您无需检查新磁盘上的文件系统。
  - 如果存储卷已连接到现有磁盘，问题解答 请将 * 。 *您可以使用文件系统检查的结果来确定损坏的来源。结果将保存在 ` /var/local/log/sn-remount-volumes.log` 日志文件中。
- ` dev/sde` 通过了 XFS 文件系统一致性检查，并且具有有效的卷结构；但是， `volID` 文件中的 LDR 节点 ID 与此存储节点的 ID 不匹配（顶部显示的 `configured LDR noid` ）。此消息表示此卷属于另一个存储节点。

3. 查看脚本输出并解决任何问题。

> 如果存储卷未通过 XFS 文件系统一致性检查或无法挂载，请仔细查看输出中的错误消息。您必须了解在这些卷上运行 `sn-recovery-postinstall.sh` 脚本的含义。

a. 检查以确保结果中包含所需所有卷的条目。如果未列出任何卷，请重新运行此脚本。

b. 查看所有已挂载设备的消息。确保没有指示存储卷不属于此存储节点的错误。

在此示例中， /dev/sde 的输出包含以下错误消息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 如果报告某个存储卷属于另一个存储节点，请联系技术支持。如果运行 `sn-recovery-postinstall.sh` 脚本，则存储卷将重新格式化，从而可能会丢失发生原因 数据。

c. 如果无法挂载任何存储设备，请记下此设备的名称，然后修复或更换此设备。

> 您必须修复或更换任何无法挂载的存储设备。

您将使用设备名称查找卷 ID ，在运行 `repair-data` 脚本将对象数据还原到卷（下一个操作步骤 ）时，需要输入此 ID 。

d. 修复或更换所有无法挂载的设备后，再次运行 `sn-remount-volumes` 脚本，以确认可以重新挂载的所有存储卷均已重新挂载。

> 如果无法挂载存储卷或存储卷格式不正确，而您继续执行下一步，则此卷以及此卷上的任何数据将被删除。如果对象数据有两个副本，则只有一个副本，直到完成下一个操作步骤（还原对象数据）为止。

> 如果您认为无法从网格中的其他位置重建故障存储卷上的剩余数据，请勿运行 `sn-recovery-postinstall.sh` 脚本（例如， ILM 策略使用的规则仅创建一个副本或卷在多个节点上发生故障）。请联系技术支持以确定如何恢复数据。

4. 运行 `sn-recovery-postinstall.sh` 脚本： `sn-recovery-postinstall.sh`

此脚本将重新格式化无法挂载或格式不正确的任何存储卷；根据需要在节点上重建 Cassandra 数据库；并启动存储节点上的服务。

请注意以下事项：

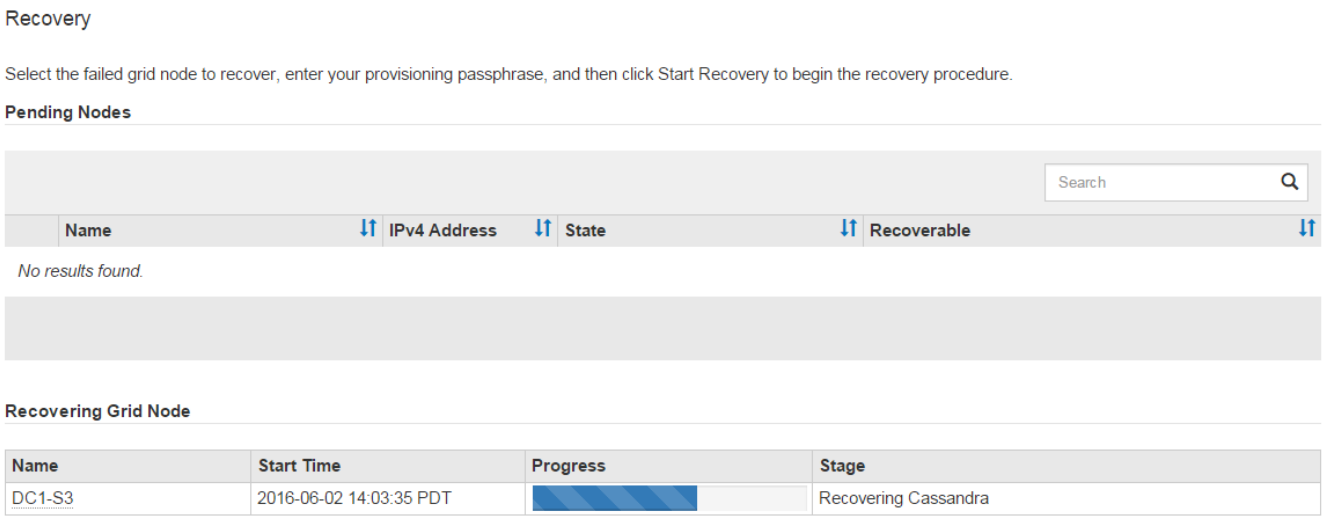
- 此脚本可能需要数小时才能运行。
- 通常，在脚本运行期间，您应单独保留 SSH 会话。
- SSH 会话处于活动状态时，请勿按 * 。 Ctrl+C* 。
- 如果发生网络中断并终止 SSH 会话，则此脚本将在后台运行，但您可以从 " 恢复 " 页面查看进度。
- 如果存储节点使用 RSM 服务，则随着节点服务重新启动，脚本可能会暂停 5 分钟。每当 RSM 服务首次启动时，预计会有 5 分钟的延迟。

> RSM 服务位于包含此 ADC 服务的存储节点上。

> 某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

5. 在 `sn-recovery-postinstall.sh` 脚本运行时，监控网格管理器中的恢复页面。

" 恢复 " 页面上的进度条和阶段列可提供 `sn-recovery-postinstall.sh` 脚本的高级状态。



在 `sn-recovery-postinstall.sh` 脚本启动节点上的服务后，您可以将对象数据还原到由该脚本格式化的任何存储卷，如下一个操作步骤 中所述。

相关信息

查看有关存储节点系统驱动器恢复的警告

将对象数据还原到设备的存储卷

将对象数据还原到设备的存储卷

恢复设备存储节点的存储卷后，您可以还原存储节点发生故障时丢失的对象数据。

您需要的内容

- 您必须确认已恢复的存储节点的连接状态为 * 已连接 * 在网格管理器的 * 节点 * > * 概述 * 选项卡上。

关于此任务

可以从其他存储节点，归档节点或云存储池还原对象数据，前提是已配置网格的 ILM 规则，以便可以使用对象副本。

请注意以下事项：

- 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于出现故障的存储卷上，则您将无法恢复对象。
- 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。在执行此操作步骤 之前，请联系技术支持以帮助估算恢复时间范围和相关成本。
- 如果对象的唯一剩余副本位于归档节点上，则会从归档节点检索对象数据。从归档节点将对象数据还原到存储节点比从其他存储节点还原副本所需时间更长，因为从外部归档存储系统检索数据会产生延迟。

关于 repair-data 脚本

要还原对象数据，请运行 repair-data 脚本。此脚本将开始还原对象数据的过程，并与 ILM 扫描配合使用以确保满足 ILM 规则。

选择下面的 * 复制数据 * 或 * 擦除编码（ Erasure-Coded ， EC ）数据 * ，根据您要还原的是复制的数据还是擦除编码的数据，了解 repair-data 脚本的不同选项。如果需要还原这两种类型的数据，则必须同时运行这两组命令。

有关 repair-data 脚本的详细信息，请在主管理节点的命令行中输入 repair-data -help 。

复制的数据

根据您是需要修复整个节点还是仅需要修复节点上的特定卷，可以使用两个命令还原复制的数据：

```
repair-data start-replicated -node-repair

repair-data start-replicated -volume-repair
```

您可以使用以下命令跟踪已复制数据的修复：

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 show -replicate-repair-status 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ Erasure Coded ， EC ）数据

根据您是需要修复整个节点还是仅修复节点上的特定卷，可以使用两个命令来还原经过擦除编码的数据：

```
repair-data start-EC-node-repair

repair-data start-EC-volume-repair
```

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

您可以使用以下命令跟踪纠删编码数据的修复情况：

```
repair-data show-EC-repair-status
```

EC 修复作业会临时预留大量存储。可能会触发存储警报，但会在修复完成后解决。如果没有足够的存储空间用于预留， EC 修复作业将失败。无论作业失败还是成功， EC 修复作业完成后都会释放存储预留。

查找存储节点的主机名

1. 登录到主管理节点：

a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 使用 ` /etc/hosts` 文件查找已还原存储卷的存储节点的主机名。要查看网格中所有节点的列表，请输入以下内容： `cat /etc/hosts` 。

如果所有卷都发生故障，请修复数据

如果所有存储卷都发生故障，请修复整个节点。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果只有部分卷发生故障，请转至 [如果只有部分卷出现故障，请修复数据]。

您不能同时对多个节点运行 `repair-data` 操作。要恢复多个节点，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `repair-data start-replicated -node-repair` 命令和 ` -nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上复制的数据：

```
repair-data start-replicated -node-repair -nodes sg-DC-SN3
```

还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见 监控和故障排除。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `repair-data start-EC-node-repair` 命令和 ` -nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上的擦除编码数据：

```
repair-data start-EC-node-repair -nodes sg-DC-SN3
```

此操作将返回唯一的 `repair ID` ，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

如果只有部分卷出现故障，请修复数据

如果只有部分卷出现故障，请修复受影响的卷。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果所有卷都发生故障，请转至 [如果所有卷都发生故障，请修复数据]。

以十六进制格式输入卷 ID 。例如， `0000` 是第一个卷， `000f` 是第 16 个卷。您可以指定一个卷，一个卷范围或多个不属于一个序列的卷。

所有卷必须位于同一个存储节点上。如果需要还原多个存储节点的卷，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `sSTART-replicated -volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0002`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0002
```

- 卷范围 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0003` 到 `0009` 范围内的所有卷：

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 不在序列中的多个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0001`，`0005` 和 `0008`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0001 ,
0005 ,  0008
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见有关 StorageGRID 监控和故障排除的说明。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `sSTART-EC-volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0007`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 0007
```

- 卷范围 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0004` 到 `0006` 范围内的所有卷：

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- 不在序列中的多个卷 *： 此命令会将经过纠删编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `000a`， `000c` 和 `000E`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 000a ,  000c ,
000E
```

`repair-data` 操作将返回唯一的 `repair ID`，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

监控修复情况

根据您是使用 * 复制数据 * ， * 纠删编码（ EC ）数据 * 还是同时使用这两者来监控修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

恢复设备存储节点后检查存储状态

恢复设备存储节点后，您必须验证设备存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 检查 * 已恢复存储节点 * > * LDR* > * 存储 * > * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值。

   这两个属性的值均应为联机。

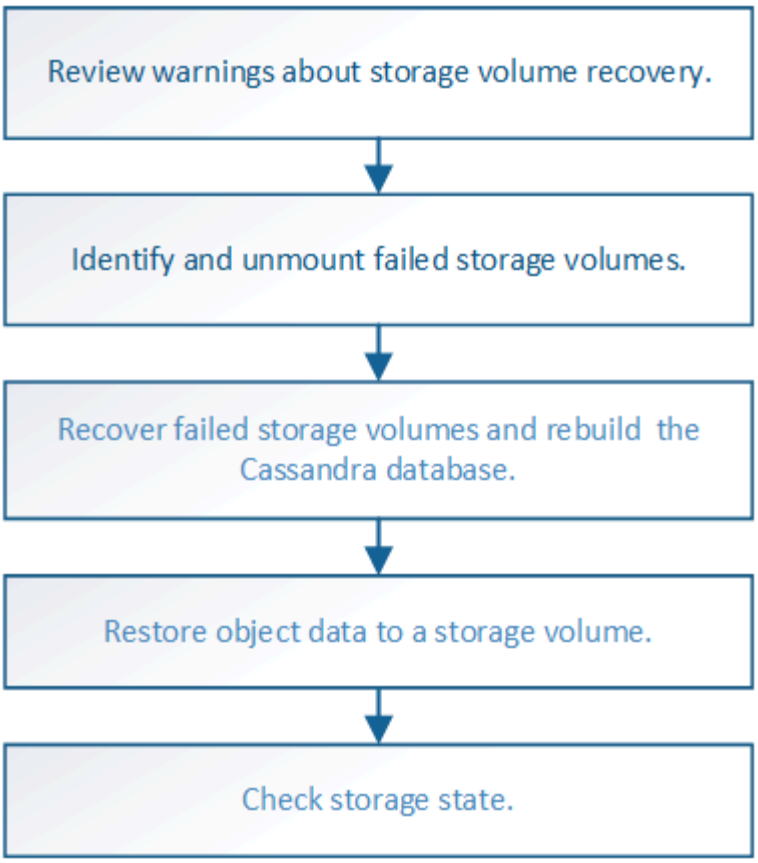
3. 如果 "Storage State" （存储状态）— "Desired " （所需）设置为只读，请完成以下步骤：
   a. 单击 * 配置 * 选项卡。
   b. 从 * 存储状态 - 所需 * 下拉列表中，选择 * 联机 * 。
   c. 单击 * 应用更改 * 。
   d. 单击 * 概述 * 选项卡并确认 * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值已更新为联机。

从系统驱动器完好无损的存储卷故障中恢复

您必须完成一系列任务，才能恢复基于软件的存储节点，如果此存储节点上的一个或多个存储卷发生故障，但系统驱动器完好无损。如果只有存储卷发生故障，则存储节点仍可供 StorageGRID 系统使用。

关于此任务

此恢复仅限基于 操作步骤 适用场景 软件的存储节点。如果设备存储节点上的存储卷发生故障，请使用操作步骤执行 "`Recover appliance Storage Node" 。`



相关信息

恢复设备存储节点

查看有关存储卷恢复的警告

在恢复存储节点的故障存储卷之前，您必须查看以下警告。

存储节点中的存储卷（或卷组）由十六进制数标识，该十六进制数称为卷 ID 。例如， 0000 是第一个卷， 000f 是第 16 个卷。每个存储节点上的第一个对象存储（卷 0 ）最多使用 4 TB 的空间来执行对象元数据和 Cassandra 数据库操作；该卷上的任何剩余空间都用于对象数据。所有其他存储卷专用于对象数据。

如果卷 0 发生故障并需要恢复，则 Cassandra 数据库可能会作为卷恢复操作步骤 的一部分进行重建。在以下情况下，还可以重建 Cassandra ：

- 存储节点脱机超过 15 天后将恢复联机。
- 系统驱动器和一个或多个存储卷发生故障并已恢复。

重建 Cassandra 后，系统将使用其他存储节点中的信息。如果脱机的存储节点过多，则某些 Cassandra 数据可能不可用。如果 Cassandra 最近已重建，则 Cassandra 数据可能尚未在网格中保持一致。如果在存储节点过多脱机时重建 Cassandra ，或者在彼此 15 天内重建两个或多个存储节点，则可能会发生数据丢失。

如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。在 15 天内在两个或多个存储节点上重建 Cassandra 可能会导致数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

如果在恢复期间遇到服务：状态 - Cassandra （ SVST ）警报，请参见有关通过重建 Cassandra 从警报中恢复的监控和故障排除说明。重建 Cassandra 后，应清除警报。如果未清除警报，请联系技术支持。

相关信息

监控和故障排除

有关网格节点恢复的警告和注意事项

确定并卸载故障存储卷

在恢复包含故障存储卷的存储节点时，您必须确定并卸载故障卷。您必须验证在恢复操作步骤 中仅重新格式化故障存储卷。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

您应尽快恢复发生故障的存储卷。

恢复过程的第一步是检测已断开连接，需要卸载或存在 I/O 错误的卷。如果故障卷仍然连接，但文件系统随机损坏，则系统可能无法检测到磁盘中未使用或未分配的部分有任何损坏。

您必须先完成此操作步骤 ，然后再执行手动步骤来恢复卷，例如添加或重新连接磁盘，停止节点，启动节点或重新启动。否则，在运行 `reformat_storage_block_devices.rb` 脚本时，可能会遇到文件系统错误，从而导致脚本挂起或失败。

在运行 `reboot` 命令之前，请修复硬件并正确连接磁盘。

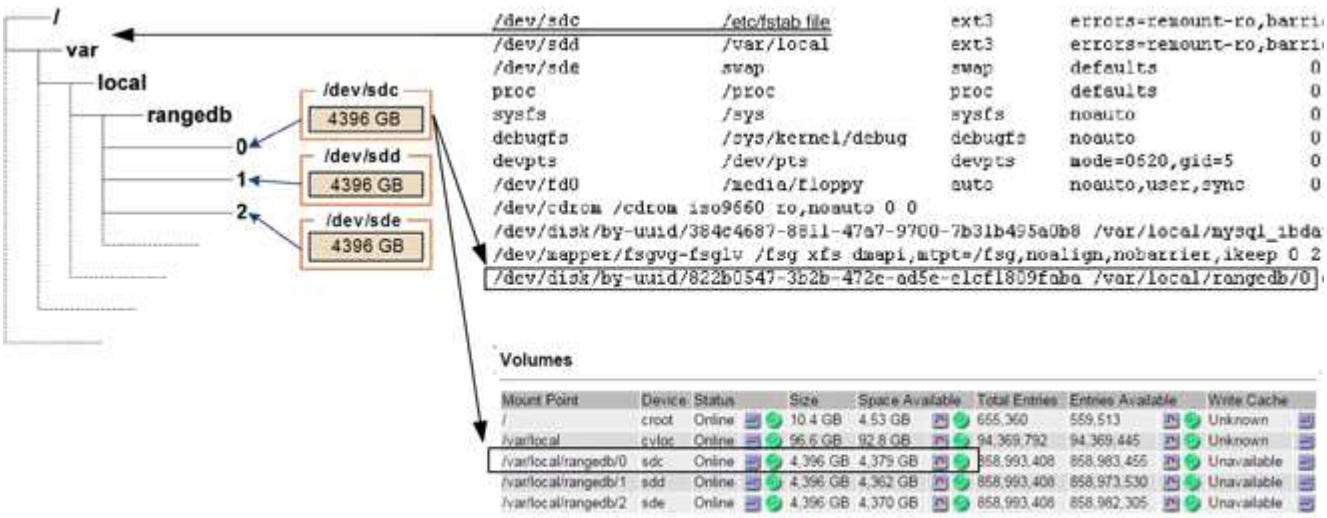
请仔细识别故障存储卷。您将使用此信息验证哪些卷必须重新格式化。重新格式化卷后，卷上的数据将无法恢复。

要正确恢复故障存储卷，您需要知道故障存储卷的设备名称及其卷 ID 。

在安装时，系统会为每个存储设备分配一个文件系统通用唯一标识符（ UUID ），并使用分配的文件系统 UUID 挂载到存储节点上的一个 rangedb 目录。文件系统 UUID 和 rangedb 目录将在 ` /etc/fstab` 文件中列出。网格管

理器中将显示设备名称，范围 b 目录以及已挂载卷的大小。

在以下示例中，设备 ` /dev/sdc` 的卷大小为 4 TB ，使用 `/etc/` 文件中的设备名称 ` /dev/disk/by-uid/822b0547-3b2E-472b-ad5e-e1cf1809faba` 挂载到 ` /var/local/rangedb/0` ：



步骤

1. 完成以下步骤以记录故障存储卷及其设备名称：

   a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

   b. 选择 * 站点 * > * 故障存储节点 * > * LDR* > * 存储 * > * 概述 * > * 主 * ，然后查找包含警报的对象存储。

Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

   c. 选择 * 站点 * > * 故障存储节点 * > * SSM* > * 资源 * > * 概述 * > * 主 * 。确定上一步中确定的每个故障存储卷的挂载点和卷大小。

   对象存储以十六进制表示法进行编号。例如， 0000 是第一个卷， 000f 是第 16 个卷。在此示例中， ID 为 0000 的对象存储对应于设备名称为 sdc 且大小为 107 GB 的 ` /var/local/rangedb/0` 。

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. 登录到发生故障的存储节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

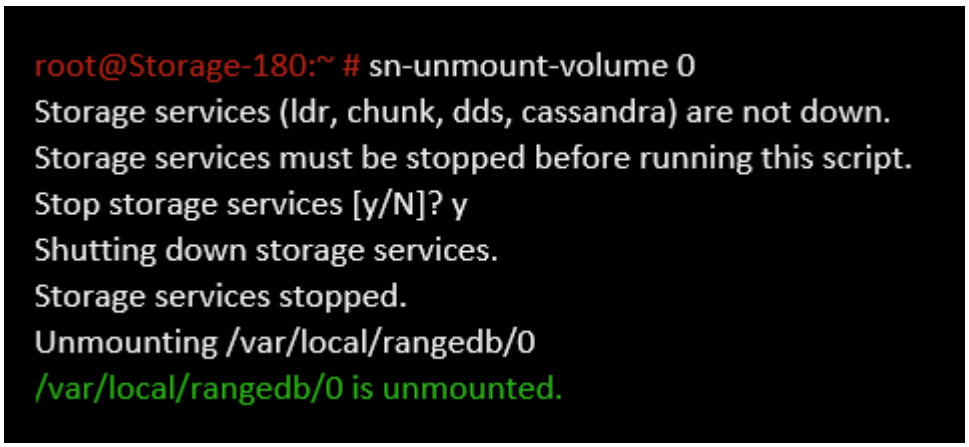
3. 运行以下脚本以停止存储服务并卸载故障存储卷：

   `sn-ununmount 卷 object_store_ID`

   `object_store_ID` 是故障存储卷的 ID 。例如，在命令中为 ID 为 0000 的对象存储指定 `0` 。

4. 如果出现提示，请按 * 。 * 停止存储节点上的存储服务。

   如果存储服务已停止，则不会提示您。仅对卷 0 停止 Cassandra 服务。

   几秒钟后，存储服务将停止，卷将卸载。此时将显示消息，指示此过程的每个步骤。最后一条消息指示卷已卸载。

恢复发生故障的存储卷并重建 **Cassandra** 数据库

您必须运行一个脚本来重新格式化和重新挂载故障存储卷上的存储，并在系统确定有必要时在存储节点上重建 Cassandra 数据库。

- 您必须具有 `passwords.txt` 文件。
- 服务器上的系统驱动器必须完好无损。
- 必须已确定故障的发生原因 ，必要时，必须已购买更换存储硬件。
- 替换存储的总大小必须与原始存储相同。
- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）

- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）
- 您已拥有 已查看有关存储卷恢复的警告。

a. 根据需要，更换与先前已确定并卸载的故障存储卷关联的故障物理或虚拟存储。

   更换存储后，请确保重新扫描或重新启动以确保操作系统能够识别该存储，但不要重新挂载卷。存储将重新挂载并在稍后的步骤中添加到 ` /etc/fstab` 中。

b. 登录到发生故障的存储节点：

   i. 输入以下命令： `ssh admin@ grid_node_ip_`

   ii. 输入 `passwords.txt` 文件中列出的密码。

   iii. 输入以下命令切换到 root： `su -`

   iv. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

c. 使用文本编辑器（ vi 或 vim ）从 ` /etc/fstab` 文件中删除故障卷，然后保存该文件。

   > 在 ` /etc/fstab` 文件中注释掉故障卷不足。必须从 `fstab` 中删除卷，因为恢复过程会验证 `fstab` 文件中的所有行是否与挂载的文件系统匹配。

d. 重新格式化任何发生故障的存储卷，并根据需要重建 Cassandra 数据库。输入： `reformat_storage_block_devices.rb`

   - 如果存储服务正在运行，系统将提示您停止这些服务。输入： *
   - 如果需要，系统将提示您重建 Cassandra 数据库。
     - 查看警告。如果其中任何一项都不适用，请重建 Cassandra 数据库。输入： *
     - 如果多个存储节点脱机或在过去 15 天内重建了另一个存储节点。输入： *

       该脚本将退出而不重建 Cassandra 。请联系技术支持。

   - 对于存储节点上的每个 rangedb 驱动器，当系统询问您以下问题时： **是否重新格式化 `rangedb` 驱动器 `<name>` （ `device` < 主要号码 >： < 次要号码 > ）？** `[Y/n]` **？** ，输入以下回答之一：

     - * y * 重新格式化出现错误的驱动器。这会重新格式化存储卷，并将重新格式化的存储卷添加到 ` /etc/fstab` 文件中。
     - 如果驱动器不包含任何错误，并且您不想重新格式化它，则为 * 否 * 。

       > 选择 * n * 将退出此脚本。挂载驱动器（如果您认为应保留驱动器上的数据且错误地卸载了驱动器）或删除驱动器。然后，再次运行 `reformat_storage_block_devices.rb` 命令。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

在以下示例输出中，必须重新格式化驱动器 ` /dev/sdf` ，而不需要重建 Cassandra ：

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

将对象数据还原到系统驱动器完好无损的存储卷

在系统驱动器完好无损的存储节点上恢复存储卷后，您可以还原存储卷发生故障时丢失的对象数据。

您需要的内容

- 您必须确认已恢复的存储节点的连接状态为 * 已连接 * 在网格管理器的 * 节点 * > * 概述 * 选项卡上。

关于此任务

可以从其他存储节点，归档节点或云存储池还原对象数据，前提是已配置网格的 ILM 规则，以便可以使用对象副本。

请注意以下事项：

- 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于出现故障的存储卷上，则您将无法恢复对象。
- 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。在执行此操作步骤 之前，请联系技术支持以帮助估算恢复时间范围和相关成本。

- 如果对象的唯一剩余副本位于归档节点上，则会从归档节点检索对象数据。从归档节点将对象数据还原到存储节点比从其他存储节点还原副本所需时间更长，因为从外部归档存储系统检索数据会产生延迟。

关于 `repair-data` 脚本

要还原对象数据，请运行 `repair-data` 脚本。此脚本将开始还原对象数据的过程，并与 ILM 扫描配合使用以确保满足 ILM 规则。

选择下面的 * 复制数据 * 或 * 擦除编码（ Erasure-Coded ， EC ）数据 * ，根据您要还原的是复制的数据还是擦除编码的数据，了解 `repair-data` 脚本的不同选项。如果需要还原这两种类型的数据，则必须同时运行这两组命令。

有关 `repair-data` 脚本的详细信息，请在主管理节点的命令行中输入 `repair-data -help` 。

复制的数据

根据您是需要修复整个节点还是仅需要修复节点上的特定卷，可以使用两个命令还原复制的数据：

```
repair-data start-replicated -node-repair
```

```
repair-data start-replicated -volume-repair
```

您可以使用以下命令跟踪已复制数据的修复：

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

根据您是需要修复整个节点还是仅修复节点上的特定卷，可以使用两个命令来还原经过擦除编码的数据：

```
repair-data start-EC-node-repair
```

```
repair-data start-EC-volume-repair
```

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

您可以使用以下命令跟踪纠删编码数据的修复情况：

```
repair-data show-EC-repair-status
```

EC 修复作业会临时预留大量存储。可能会触发存储警报，但会在修复完成后解决。如果没有足够的存储空间用于预留， EC 修复作业将失败。无论作业失败还是成功， EC 修复作业完成后都会释放存储预留。

查找存储节点的主机名

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 使用 ` /etc/hosts` 文件查找已还原存储卷的存储节点的主机名。要查看网格中所有节点的列表，请输入以下内容： `cat /etc/hosts` 。

如果所有卷都发生故障，请修复数据

如果所有存储卷都发生故障，请修复整个节点。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果只有部分卷发生故障，请转至 [如果只有部分卷出现故障，请修复数据]。

> 您不能同时对多个节点运行 `repair-data` 操作。要恢复多个节点，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `repair-data start-replicated -node-repair` 命令和 `-nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上复制的数据：

```
repair-data start-replicated -node-repair -nodes sg-DC-SN3
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见 监控和故障排除。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `repair-data start-EC-node-repair` 命令和 `-nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上的擦除编码数据：

```
repair-data start-EC-node-repair -nodes sg-DC-SN3
```

此操作将返回唯一的 `repair ID` ，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

如果只有部分卷出现故障，请修复数据

如果只有部分卷出现故障，请修复受影响的卷。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果所有卷都发生故障，请转至 [如果所有卷都发生故障，请修复数据]。

以十六进制格式输入卷 ID 。例如， `0000` 是第一个卷， `000f` 是第 16 个卷。您可以指定一个卷，一个卷范围或多个不属于一个序列的卷。

所有卷必须位于同一个存储节点上。如果需要还原多个存储节点的卷，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `sSTART-replicated -volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0002`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0002
```

- 卷范围 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0003` 到 `0009` 范围内的所有卷：

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 不在序列中的多个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0001`，`0005` 和 `0008`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0001 ,
0005 ,  0008
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见有关 StorageGRID 监控和故障排除的说明。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `sSTART-EC-volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0007`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 0007
```

- 卷范围 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0004` 到 `0006` 范围内的所有卷：

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- 不在序列中的多个卷 *： 此命令会将经过纠删编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `000a`， `000c` 和 `000E`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 000a ,  000c ,
000E
```

`repair-data` 操作将返回唯一的 `repair ID`，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

监控修复情况

根据您是使用 * 复制数据 * ， * 纠删编码（ EC ）数据 * 还是同时使用这两者来监控修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

恢复存储卷后检查存储状态

恢复存储卷后，您必须验证存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 检查 * 已恢复存储节点 * > * LDR* > * 存储 * > * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值。

   这两个属性的值均应为联机。

3. 如果 "Storage State" （存储状态）— "Desired " （所需）设置为只读，请完成以下步骤：
   a. 单击 * 配置 * 选项卡。
   b. 从 * 存储状态 - 所需 * 下拉列表中，选择 * 联机 * 。
   c. 单击 * 应用更改 * 。
   d. 单击 * 概述 * 选项卡并确认 * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值已更新为联机。

从系统驱动器故障中恢复

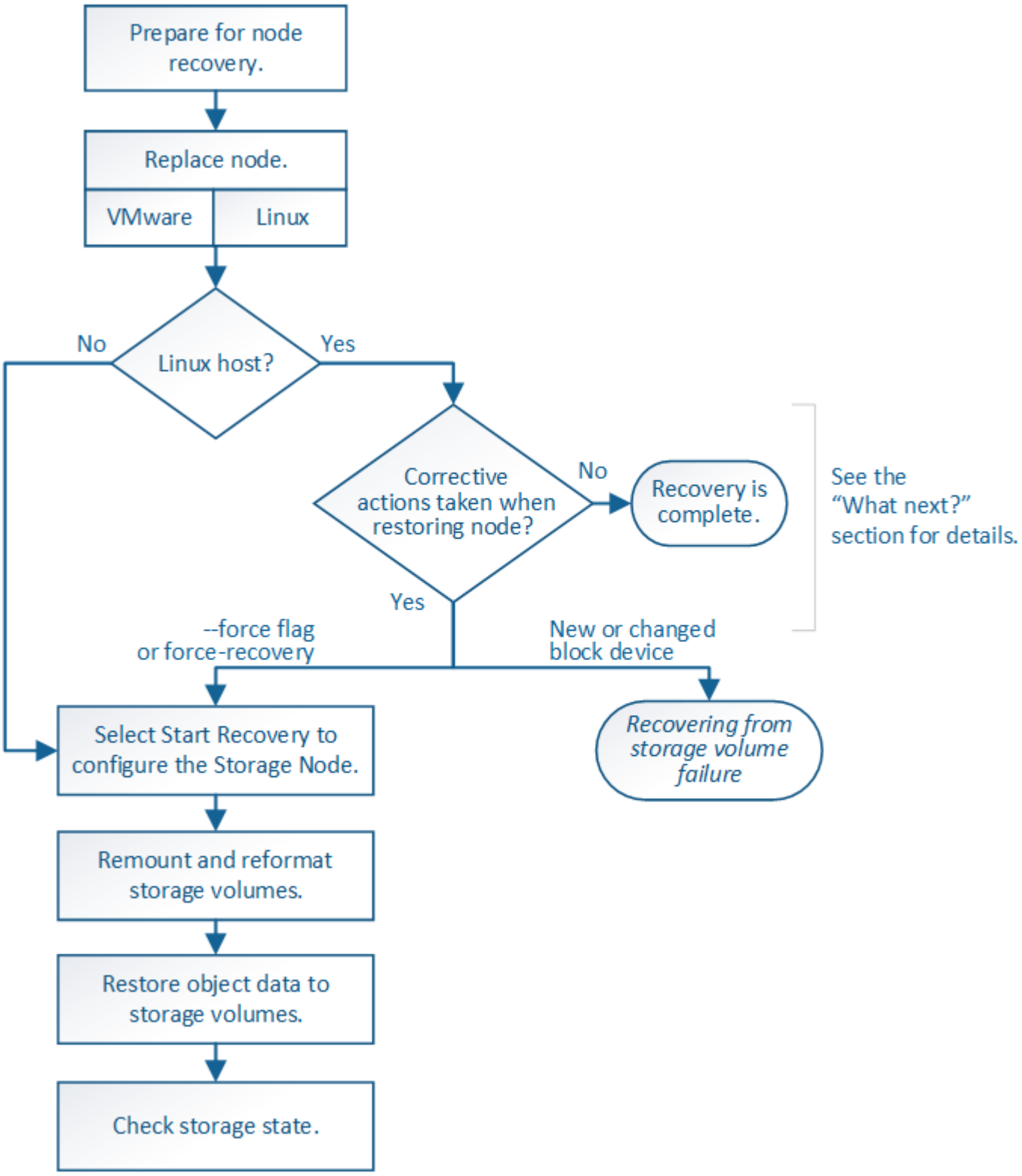
如果基于软件的存储节点上的系统驱动器发生故障，则此存储节点不可用于 StorageGRID 系统。您必须完成一组特定任务才能从系统驱动器故障中恢复。

关于此任务

使用此操作步骤 从基于软件的存储节点上的系统驱动器故障中恢复。此操作步骤 包括在任何存储卷同样出现故障或无法重新挂载时应遵循的步骤。

仅限此基于 操作步骤 适用场景 软件的存储节点。要恢复设备存储节点，您必须遵循其他操作步骤 。

恢复设备存储节点



查看有关存储节点系统驱动器恢复的警告

在恢复存储节点的故障系统驱动器之前，您必须查看以下警告。

存储节点具有包含对象元数据的 Cassandra 数据库。在以下情况下，可能会重建 Cassandra 数据库：

- 存储节点脱机超过 15 天后将恢复联机。
- 存储卷出现故障并已恢复。
- 系统驱动器和一个或多个存储卷发生故障并已恢复。

重建 Cassandra 后，系统将使用其他存储节点中的信息。如果脱机的存储节点过多，则某些 Cassandra 数据可能不可用。如果 Cassandra 最近已重建，则 Cassandra 数据可能尚未在网格中保持一致。如果在存储节点过多脱机时重建 Cassandra ，或者在彼此 15 天内重建两个或多个存储节点，则可能会发生数据丢失。

如果多个存储节点出现故障（或脱机），请联系技术支持。请勿执行以下恢复操作步骤 。可能发生数据丢失。

如果这是在存储节点发生故障或恢复后不到 15 天内第二个存储节点发生故障，请联系技术支持。在 15 天内在两个或多个存储节点上重建 Cassandra 可能会导致数据丢失。

如果一个站点上的多个存储节点出现故障，则可能需要一个站点恢复操作步骤 。请联系技术支持。

技术支持如何执行站点恢复

如果此存储节点处于只读维护模式，以便允许存储卷出现故障的另一个存储节点检索对象，请先在存储卷出现故障的存储节点上恢复卷，然后再恢复此故障存储节点。请参见有关从系统驱动器完好无损的存储卷丢失中恢复的说明。

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

如果在恢复期间遇到服务：状态 - Cassandra （ SVST ）警报，请参见有关通过重建 Cassandra 从警报中恢复的监控和故障排除说明。重建 Cassandra 后，应清除警报。如果未清除警报，请联系技术支持。

相关信息

监控和故障排除

有关网格节点恢复的警告和注意事项

从系统驱动器完好无损的存储卷故障中恢复

更换存储节点

如果系统驱动器发生故障，您必须先更换存储节点。

您必须为您的平台选择节点替代操作步骤 。对于所有类型的网格节点，更换节点的步骤都相同。

仅限此基于 操作步骤 适用场景 软件的存储节点。要恢复设备存储节点，您必须遵循其他操作步骤 。

恢复设备存储节点

- Linux： * 如果您不确定系统驱动器是否出现故障，请按照说明更换节点以确定需要执行哪些恢复步骤。

平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

选择启动恢复以配置存储节点

更换存储节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。
- 您必须知道擦除编码数据的任何修复作业的开始日期。
- 您必须已确认过去 15 天内未重建此存储节点。

关于此任务

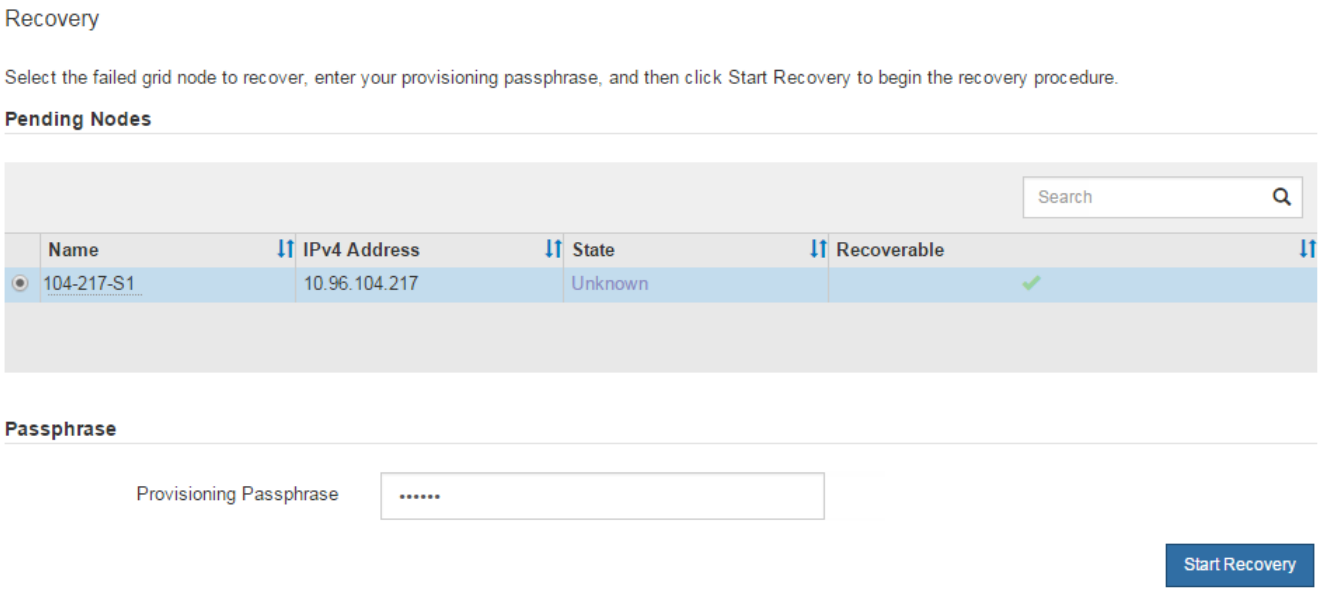
如果存储节点作为容器安装在 Linux 主机上，则只有在满足以下条件之一时，才必须执行此步骤：

- 您必须使用 ` -force` 标志导入节点，或者发出 `StorageGRID node force-recovery node-name`
- 您必须执行完整节点重新安装，或者需要还原 /var/local 。

步骤

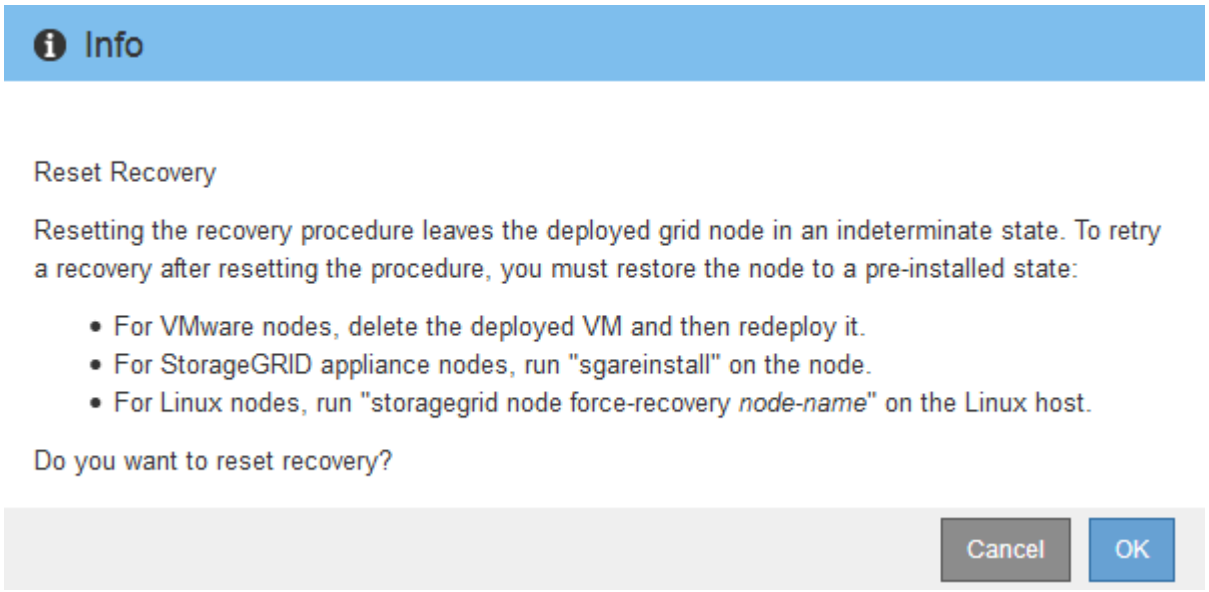
1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。
3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

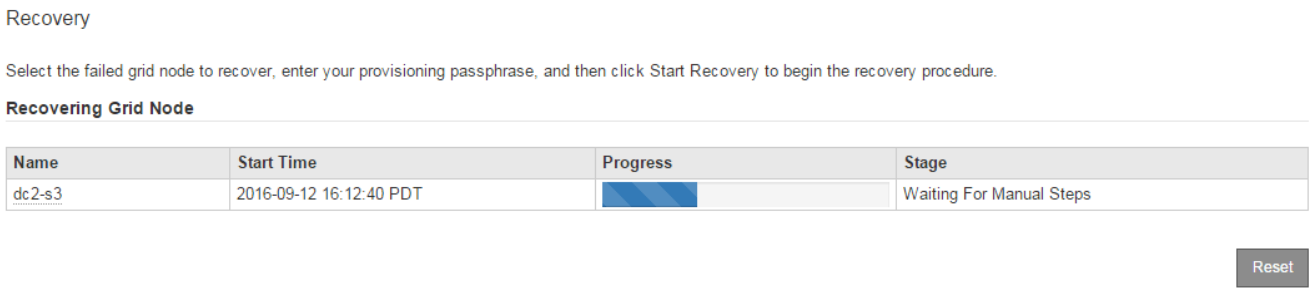
> 在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`

6. 当存储节点达到 "`Waiting for Manual steps` " 阶段时，请转至恢复操作步骤 中的下一个任务以重新挂载和重新格式化存储卷。



相关信息

准备要重新安装的设备（仅限平台更换）

重新挂载并重新格式化存储卷（ " 手动步骤 " ）

要重新挂载保留的存储卷并重新格式化任何故障存储卷，您必须手动运行两个脚本。第一个脚本将重新挂载格式正确的卷，使其格式化为 StorageGRID 存储卷。第二个脚本将重新格式化所有已卸载的卷，根据需要重新构建 Cassandra 并启动服务。

您需要的内容

- 您已更换已知需要更换的任何故障存储卷的硬件。

  运行 `sn-remount-volumes` 脚本可能有助于您确定其他故障存储卷。

- 您已检查是否未在执行存储节点停用，或者已暂停节点停用操作步骤 。（在网格管理器中，选择 * 维护 * > * 任务 * > * 取消配置 * 。）
- 您已检查扩展是否未在进行中。（在网格管理器中，选择 * 维护 * > * 任务 * > * 扩展 * 。）
- 您已拥有 已查看有关存储节点系统驱动器恢复的警告。

> 如果多个存储节点脱机或此网格中的存储节点在过去 15 天内已重建，请联系技术支持。请勿运行 `sn-recovery-postinstall.sh` 脚本。在两个或多个存储节点上相互重建 Cassandra 的 15 天内可能会导致数据丢失。

关于此任务

要完成此操作步骤 ，请执行以下高级任务：

- 登录到已恢复的存储节点。
- 运行 `sn-remount-volumes` 脚本重新挂载格式正确的存储卷。运行此脚本时，它将执行以下操作：
  - 挂载和卸载每个存储卷以重放 XFS 日志。
  - 执行 XFS 文件一致性检查。
  - 如果文件系统一致，则确定存储卷是否为格式正确的 StorageGRID 存储卷。
  - 如果存储卷格式正确，请重新挂载该存储卷。卷上的所有现有数据保持不变。
- 查看脚本输出并解决任何问题。
- 运行 `sn-recovery-postinstall.sh` 脚本。运行此脚本时，它将执行以下操作。

运行之前、请勿在恢复期间重新启动存储节点 `sn-recovery-postinstall.sh` 重新格式化故障存储卷并还原对象元数据。之前重新启动存储节点 `sn-recovery-postinstall.sh` 完成会导致尝试启动的服务出错、并导致StorageGRID 设备节点退出维护模式。请参见的步骤 安装后脚本。

- 重新格式化 `sn-remount-volumes` 脚本无法挂载或发现格式不正确的任何存储卷。

  如果重新格式化某个存储卷，则该卷上的所有数据都将丢失。假设已将 ILM 规则配置为存储多个对象副本，则必须执行额外的操作步骤 以从网格中的其他位置还原对象数据。

- 如果需要，在节点上重建 Cassandra 数据库。
- 启动存储节点上的服务。

步骤

1. 登录到已恢复的存储节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 运行第一个脚本重新挂载任何格式正确的存储卷。

   如果所有存储卷都是新的，需要进行格式化，或者所有存储卷都出现故障，您可以跳过此步骤并运行第二个脚本，重新格式化所有已卸载的存储卷。

   a. 运行以下脚本： `sn-remount-volumes`

      此脚本可能需要数小时才能在包含数据的存储卷上运行。

   b. 在脚本运行期间，查看输出并问题解答 任何提示。

      根据需要，您可以使用 `tail -f` 命令监控脚本日志文件的内容（` /var/local/log/SN-remount-volumes.log` ）。日志文件包含比命令行输出更详细的信息。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
```

```
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.
```

```
This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

在示例输出中，一个存储卷已成功重新挂载，三个存储卷出现错误。

- ` /dev/sdb` 通过了 XFS 文件系统一致性检查，并具有有效的卷结构，因此已成功重新挂载。此脚本重新挂载的设备上的数据将保留下来。
- 由于存储卷是新的或已损坏， ` /dev/sdc` 未通过 XFS 文件系统一致性检查。
- 无法挂载 ` /dev/sdd` ，因为磁盘已取消初始化或磁盘的超级块已损坏。当脚本无法挂载存储卷时，它会询问您是否要运行文件系统一致性检查。
  - 如果存储卷已连接到新磁盘，请将 * N * 问题解答 到提示符处。您无需检查新磁盘上的文件系统。
  - 如果存储卷已连接到现有磁盘，问题解答 请将 * 。 *您可以使用文件系统检查的结果来确定损坏的来源。结果将保存在 ` /var/local/log/sn-remount-volumes.log` 日志文件中。
- ` dev/sde` 已通过 XFS 文件系统一致性检查，并且卷结构有效；但是， volID 文件中的 LDR 节点 ID 与此存储节点的 ID 不匹配（顶部显示的 `configured LDR noid` ）。此消息表示此卷属于另一个

存储节点。

3. 查看脚本输出并解决任何问题。

> 如果存储卷未通过 XFS 文件系统一致性检查或无法挂载，请仔细查看输出中的错误消息。您必须了解在这些卷上运行 `sn-recovery-postinstall.sh` 脚本的含义。

a. 检查以确保结果中包含所需所有卷的条目。如果未列出任何卷，请重新运行此脚本。

b. 查看所有已挂载设备的消息。确保没有指示存储卷不属于此存储节点的错误。

在此示例中，` /dev/sde` 的输出包含以下错误消息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 如果报告某个存储卷属于另一个存储节点，请联系技术支持。如果运行 `sn-recovery-postinstall.sh` 脚本，则存储卷将重新格式化，从而可能会丢失发生原因 数据。

c. 如果无法挂载任何存储设备，请记下此设备的名称，然后修复或更换此设备。

> 您必须修复或更换任何无法挂载的存储设备。

您将使用设备名称查找卷 ID ，在运行 `repair-data` 脚本将对象数据还原到卷（下一个操作步骤 ）时，需要输入此 ID 。

d. 修复或更换所有无法挂载的设备后，再次运行 `sn-remount-volumes` 脚本，以确认可以重新挂载的所有存储卷均已重新挂载。

> 如果无法挂载存储卷或存储卷格式不正确，而您继续执行下一步，则此卷以及此卷上的任何数据将被删除。如果对象数据有两个副本，则只有一个副本，直到完成下一个操作步骤（还原对象数据）为止。

> 如果您认为无法从网格中的其他位置重建故障存储卷上的剩余数据，请勿运行 `sn-recovery-postinstall.sh` 脚本（例如， ILM 策略使用的规则仅创建一个副本或卷在多个节点上发生故障）。请联系技术支持以确定如何恢复数据。

4. 运行 `sn-recovery-postinstall.sh` 脚本： `sn-recovery-postinstall.sh`

此脚本将重新格式化无法挂载或格式不正确的任何存储卷；根据需要在节点上重建 Cassandra 数据库；并启动存储节点上的服务。

请注意以下事项：

- 此脚本可能需要数小时才能运行。
- 通常，在脚本运行期间，您应单独保留 SSH 会话。
- SSH 会话处于活动状态时，请勿按 * 。 Ctrl+C* 。

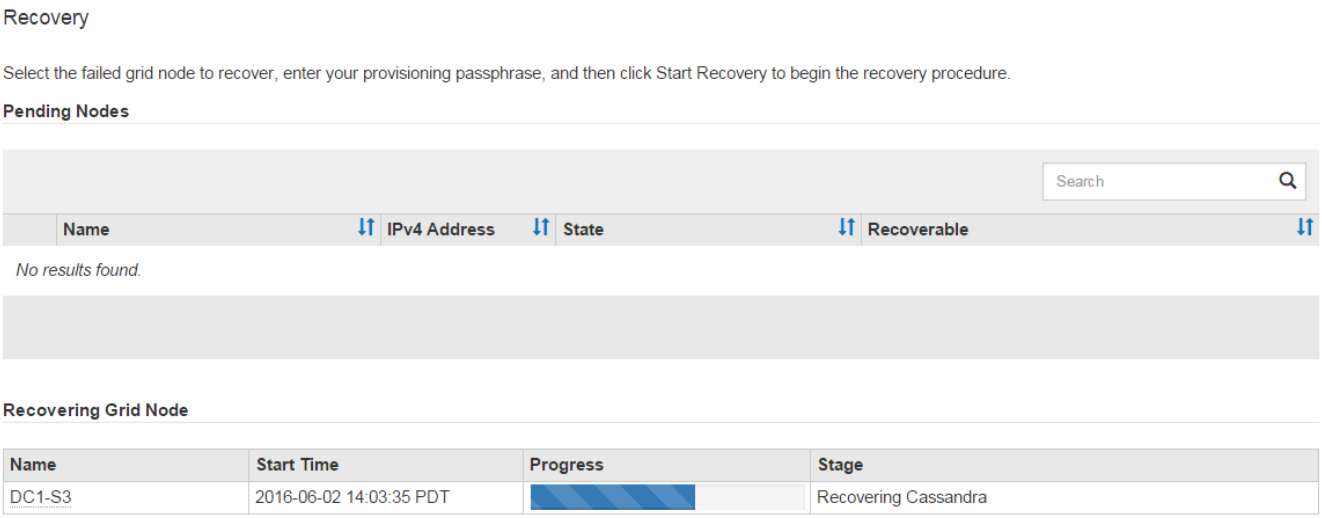
- 如果发生网络中断并终止 SSH 会话，则此脚本将在后台运行，但您可以从 " 恢复 " 页面查看进度。
- 如果存储节点使用 RSM 服务，则随着节点服务重新启动，脚本可能会暂停 5 分钟。每当 RSM 服务首次启动时，预计会有 5 分钟的延迟。

RSM 服务位于包含此 ADC 服务的存储节点上。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到 " `reaper` " 或 "`Cassandra repair.` " 。 如果您看到指示修复失败的错误消息，请运行错误消息中指示的命令。

5. [[post-install-script-step]]作为 `sn-recovery-postinstall.sh` 脚本运行时、监控网格管理器中的恢复页面。

" 恢复 " 页面上的进度条和阶段列可提供 `sn-recovery-postinstall.sh` 脚本的高级状态。



在 `sn-recovery-postinstall.sh` 脚本启动节点上的服务后，您可以将对象数据还原到该脚本格式化的任何存储卷，如该操作步骤 中所述。

相关信息

查看有关存储节点系统驱动器恢复的警告

根据需要将对象数据还原到存储卷

根据需要将对象数据还原到存储卷

如果需要使用 `sn-recovery-postinstall.sh` 脚本重新格式化一个或多个故障存储卷，则必须将对象数据从其他存储节点和归档节点还原到重新格式化的存储卷。除非重新格式化了一个或多个存储卷，否则不需要执行这些步骤。

您需要的内容

- 您必须确认已恢复的存储节点的连接状态为 * 已连接 * 在网格管理器的 * 节点 * > * 概述 * 选项卡上。

关于此任务

可以从其他存储节点，归档节点或云存储池还原对象数据，前提是已配置网格的 ILM 规则，以便可以使用对象副本。

请注意以下事项：

- 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于出现故障的存储卷上，则您将无法恢复对象。
- 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。在执行此操作步骤 之前，请联系技术支持以帮助估算恢复时间范围和相关成本。
- 如果对象的唯一剩余副本位于归档节点上，则会从归档节点检索对象数据。从归档节点将对象数据还原到存储节点比从其他存储节点还原副本所需时间更长，因为从外部归档存储系统检索数据会产生延迟。

关于 `repair-data` 脚本

要还原对象数据，请运行 `repair-data` 脚本。此脚本将开始还原对象数据的过程，并与 ILM 扫描配合使用以确保满足 ILM 规则。

选择下面的 * 复制数据 * 或 * 擦除编码（ Erasure-Coded ， EC ）数据 * ，根据您要还原的是复制的数据还是擦除编码的数据，了解 `repair-data` 脚本的不同选项。如果需要还原这两种类型的数据，则必须同时运行这两组命令。

> 有关 `repair-data` 脚本的详细信息，请在主管理节点的命令行中输入 `repair-data -help` 。

复制的数据

根据您是需要修复整个节点还是仅需要修复节点上的特定卷，可以使用两个命令还原复制的数据：

```
repair-data start-replicated -node-repair

repair-data start-replicated -volume-repair
```

您可以使用以下命令跟踪已复制数据的修复：

```
repair-data show-repliced-repair-status
```

> 在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

根据您是需要修复整个节点还是仅修复节点上的特定卷，可以使用两个命令来还原经过擦除编码的数据：

```
repair-data start-EC-node-repair

repair-data start-EC-volume-repair
```

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

您可以使用以下命令跟踪纠删编码数据的修复情况：

```
repair-data show-EC-repair-status
```

> EC 修复作业会临时预留大量存储。可能会触发存储警报，但会在修复完成后解决。如果没有足够的存储空间用于预留， EC 修复作业将失败。无论作业失败还是成功， EC 修复作业完成后都会释放存储预留。

查找存储节点的主机名

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 使用 ` /etc/hosts` 文件查找已还原存储卷的存储节点的主机名。要查看网格中所有节点的列表，请输入以下内容： `cat /etc/hosts` 。

如果所有卷都发生故障，请修复数据

如果所有存储卷都发生故障，请修复整个节点。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果只有部分卷发生故障，请转至 [如果只有部分卷出现故障，请修复数据]。

您不能同时对多个节点运行 `repair-data` 操作。要恢复多个节点，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `repair-data start-replicated -node-repair` 命令和 ` -nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上复制的数据：

```
repair-data start-replicated -node-repair -nodes sg-DC-SN3
```

还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见 监控和故障排除。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `repair-data start-EC-node-repair` 命令和 ` -nodes` 选项修复整个存储节点。

此命令将修复名为 SG-DC-SN3 的存储节点上的擦除编码数据：

```
repair-data start-EC-node-repair -nodes sg-DC-SN3
```

此操作将返回唯一的 `repair ID` ，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

如果只有部分卷出现故障，请修复数据

如果只有部分卷出现故障，请修复受影响的卷。根据您是使用复制的数据，还是使用纠删编码（ Erasure-coded ， EC ）数据，或者同时使用这两者，按照有关 * 复制的数据 * ， * 纠删编码（ Erasure-Coded ， EC ）数据 * 或这两者的说明进行操作。

如果所有卷都发生故障，请转至 [如果所有卷都发生故障，请修复数据]。

以十六进制格式输入卷 ID 。例如， `0000` 是第一个卷， `000f` 是第 16 个卷。您可以指定一个卷，一个卷范围或多个不属于一个序列的卷。

所有卷必须位于同一个存储节点上。如果需要还原多个存储节点的卷，请联系技术支持。

复制的数据

如果网格包含复制的数据，请使用 `sSTART-replicated -volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0002`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0002
```

- 卷范围 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0003` 到 `0009` 范围内的所有卷：

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

- 不在序列中的多个卷 *： 此命令会将复制的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0001`，`0005` 和 `0008`：

```
repair-data start-replicated -volume-repair -nodes sg-DC-SN3 -volumes 0001 ,
0005 ,  0008
```

> 还原对象数据后，如果 StorageGRID 系统找不到复制的对象数据，则会触发 * 对象丢失 * 警报。可能会在整个系统的存储节点上触发警报。您应确定丢失的发生原因 以及是否可以恢复。请参见有关 StorageGRID 监控和故障排除的说明。

纠删编码（ **Erasure Coded** ， **EC** ）数据

如果网格包含擦除编码的数据，请使用 `sSTART-EC-volume-repair` 命令和 ` -nodes` 选项来标识节点。然后添加 ` -volumes` 或 ` -volume-range` 选项，如以下示例所示。

- 单个卷 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `0007`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 0007
```

- 卷范围 *： 此命令会将经过擦除编码的数据还原到名为 SG-DC-SN3 的存储节点上介于 `0004` 到 `0006` 范围内的所有卷：

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

- 不在序列中的多个卷 *： 此命令会将经过纠删编码的数据还原到名为 SG-DC-SN3 的存储节点上的卷 `000a`， `000c` 和 `000E`：

```
repair-data start-EC-volume-repair -nodes sg-DC-SN3 -volumes 000a ,  000c ,
000E
```

`repair-data` 操作将返回唯一的 `repair ID`，用于标识此 `repair_data` 操作。使用此 `repair ID` 跟踪 `repair_data` 操作的进度和结果。恢复过程完成后，不会返回任何其他反馈。

> 在某些存储节点脱机时，可以开始修复经过擦除编码的数据。修复将在所有节点均可用后完成。

监控修复情况

根据您是使用 * 复制数据 * ， * 纠删编码（ EC ）数据 * 还是同时使用这两者来监控修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

恢复存储节点系统驱动器后检查存储状态

恢复存储节点的系统驱动器后，您必须验证存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 检查 * 已恢复存储节点 * > * LDR* > * 存储 * > * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值。

   这两个属性的值均应为联机。

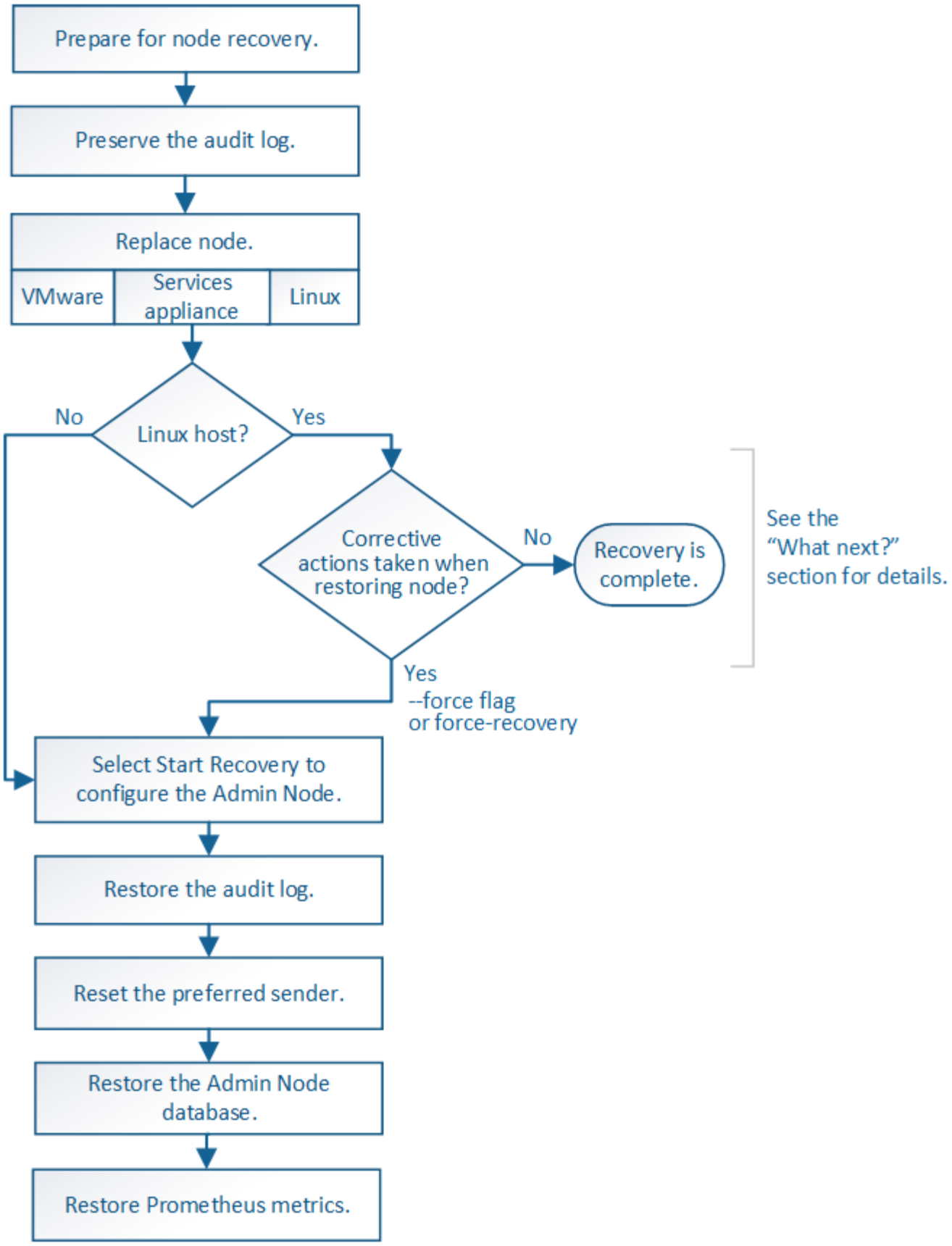
3. 如果 "Storage State" （存储状态） — "Desired " （所需）设置为只读，请完成以下步骤：
   a. 单击 * 配置 * 选项卡。
   b. 从 * 存储状态 - 所需 * 下拉列表中，选择 * 联机 * 。
   c. 单击 * 应用更改 * 。
   d. 单击 * 概述 * 选项卡并确认 * 存储状态 - 所需 * 和 * 存储状态 - 当前 * 的值已更新为联机。

从管理节点故障中恢复

管理节点的恢复过程取决于它是主管理节点还是非主管理节点。

关于此任务

恢复主管理节点或非主管理节点的高级步骤相同，但具体步骤有所不同。



对于要恢复的管理节点，请始终遵循正确的恢复操作步骤 。这些过程从较高的层面来看是相同的，但细节却有所不同。

相关信息

SG100 和 SG1000 服务设备

选项

- 从主管理节点故障中恢复
- 从非主管理节点故障中恢复

从主管理节点故障中恢复

要从主管理节点故障中恢复，您必须完成一组特定的任务。主管理节点托管网格的配置管理节点（ CMN ）服务。

关于此任务

应立即更换发生故障的主管理节点。主管理节点上的配置管理节点（ CMN ）服务负责为网格发出对象标识符块。这些标识符将在载入对象时分配给对象。除非具有可用标识符，否则无法载入新对象。由于网格中缓存了大约一个月的标识符，因此在 CMN 不可用时，对象载入可以继续。但是，在缓存的标识符用尽后，无法添加任何新对象。

> 您必须在大约一个月内修复或更换发生故障的主管理节点，否则网格可能无法载入新对象。确切的时间段取决于对象载入率：如果您需要更准确地评估网格的时间范围，请联系技术支持。

从发生故障的主管理节点复制审核日志

如果您能够从出现故障的主管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的主管理节点启动并运行后将保留的审核日志还原到该节点。

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

> 如果现在无法在出现故障的管理节点上访问审核日志，您可以稍后访问这些日志，例如在主机恢复之后。

1. 如果可能，请登录到出现故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果有）。
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 停止 AMS 服务以防止其创建新的日志文件：`sservice AMS stop`
3. 重命名 audit.log 文件，使其在复制到已恢复的管理节点时不会覆盖现有文件。

将 audit.log 重命名为唯一编号的文件名，例如 yyyy-mm-dd.txt.1 。例如，您可以将 audit.log 文件重命名为 2015-10-25.txt 。 1cd /var/local/audit/exportls -l``mv audit.log 2015-10-25.1

4. 重新启动 AMS 服务： `sservice AMS start`
5. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@ grid_node_ip_ mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

6. 复制所有审核日志文件： `scp -p * admin@ grid_node_ip_ ： /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

7. 以 root 用户身份注销： `exit`

更换主管理节点

要恢复主管理节点，必须先更换物理或虚拟硬件。

您可以将出现故障的主管理节点替换为在同一平台上运行的主管理节点，也可以将在 VMware 或 Linux 主机上运行的主管理节点替换为服务设备上托管的主管理节点。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将引导您进入主管理节点恢复的下一步。

更换平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
SG100 和 SG1000 服务设备	更换服务设备
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

配置替代主管理节点

必须将替代节点配置为 StorageGRID 系统的主管理节点。

您需要的内容

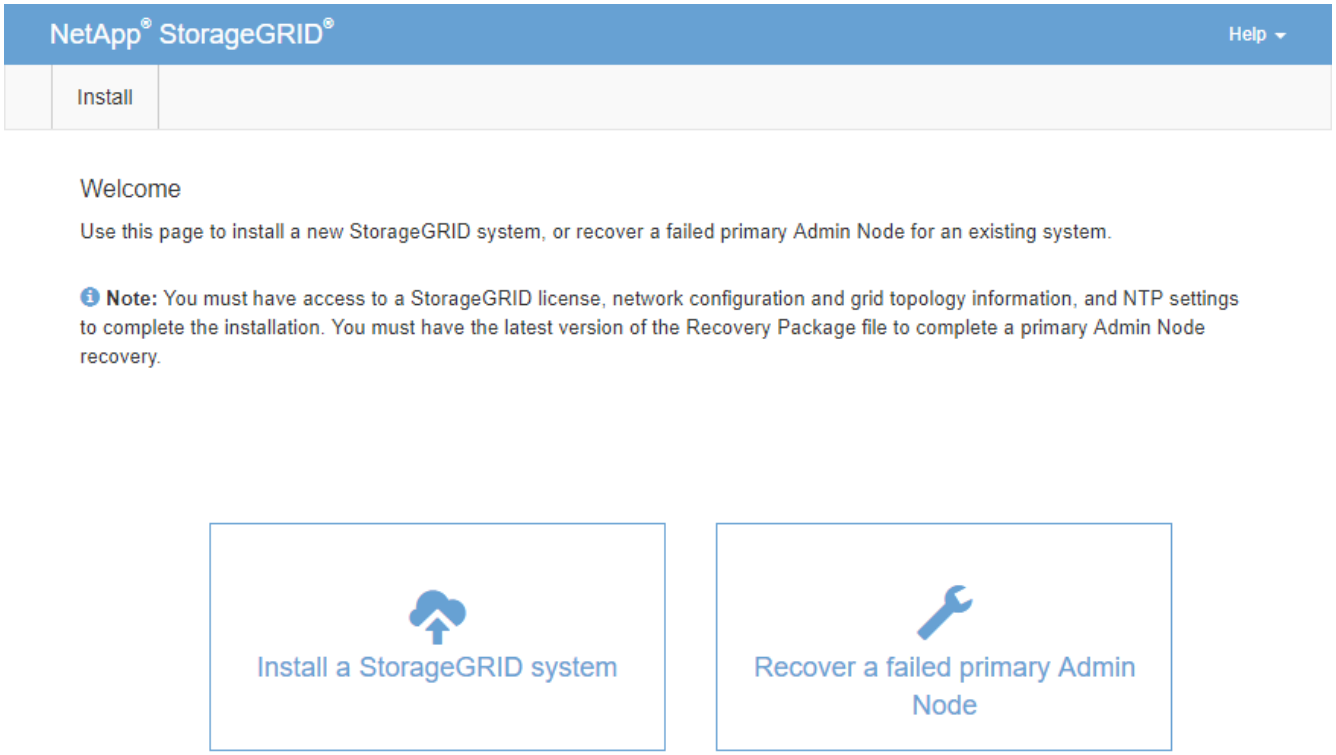
- 对于虚拟机上托管的主管理节点，必须部署，启动和初始化虚拟机。
- 对于服务设备上托管的主管理节点，您已更换此设备并安装了软件。请参见适用于您的设备的安装指南。

  SG100 和 SG1000 服务设备

- 您必须拥有恢复软件包文件的最新备份（ `sGWS-recovery-package-id-revision.zip` ）。
- 您必须具有配置密码短语。

步骤

1. 打开 Web 浏览器并导航到 `https://primary_admin_node_ip` 。



2. 单击 * 恢复发生故障的主管理节点 * 。
3. 上传恢复包的最新备份：
   a. 单击 * 浏览 * 。
   b. 找到 StorageGRID 系统的最新恢复软件包文件，然后单击 * 打开 * 。
4. 输入配置密码短语。
5. 单击 * 启动恢复 * 。

   恢复过程开始。随着所需服务的启动，网格管理器可能会在几分钟内不可用。恢复完成后，将显示登录页面。

6. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

   要配置依赖方信任，请参见有关管理 StorageGRID 的说明。要访问默认服务器证书，请登录到管理节点的命令 Shell 。转至 ` /var/local/mgmt-api` 目录，然后选择 `server.crt` 文件。

7. 确定是否需要应用修补程序。

a. 使用登录到网格管理器 支持的 Web 浏览器。

b. 选择 * 节点 * 。

c. 从左侧列表中，选择主管理节点。

d. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。

e. 选择任何其他网格节点。

f. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。

- 如果 * 软件版本 * 字段中显示的版本相同，则无需应用修补程序。
- 如果 * 软件版本 * 字段中显示的版本不同，则必须应用修补程序将恢复的主管理节点更新到相同版本。

相关信息

管理 StorageGRID

StorageGRID 热修补程序操作步骤

在已恢复的主管理节点上还原审核日志

如果能够保留故障主管理节点中的审核日志，则可以将其复制到要恢复的主管理节点。

- 必须安装并运行已恢复的管理节点。
- 在原始管理节点出现故障后，您必须已将审核日志复制到其他位置。

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点，并且无法从故障节点复制审核日志，则恢复的管理节点会开始将事件记录到审核日志中，就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

> 默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：
>
> - 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
> - 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。
>
> 请参见 配置审核消息和日志目标 了解详细信息。

步骤

1. 登录到已恢复的管理节点：

a. 输入以下命令： `ssh admin@recovery_Admin_Node_IP`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录后，提示符将从 ` $` 更改为 ` #` 。

2. 检查已保留哪些审核文件： `cd /var/local/audit/export`
3. 将保留的审核日志文件复制到已恢复的管理节点： `scp admin@ grid_node_ip_ : /var/local/tmp/saved-audit-logs/yyy*` 。

   出现提示时，输入 admin 的密码。

4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复管理节点上审核日志文件的用户和组设置： `chown AMS-user : bycast *`
6. 以 root 用户身份注销： `exit`

您还必须还原对审核共享的任何已有客户端访问。有关详细信息，请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

重置已恢复的主管理节点上的首选发送器

如果您要恢复的主管理节点当前设置为警报通知，警报通知和 AutoSupport 消息的首选发送方，则必须重新配置此设置。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 必须安装并运行已恢复的管理节点。

步骤

1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。
2. 从 * 首选发件人 * 下拉列表中选择已恢复的管理节点。
3. 单击 * 应用更改 * 。

相关信息

管理 StorageGRID

恢复主管理节点时还原管理节点数据库

如果要在出现故障的主管理节点上保留有关属性，警报和警报的历史信息，则可以还原管理节点数据库。只有当 StorageGRID 系统包含另一个管理节点时，才能还原此数据库。

- 必须安装并运行已恢复的管理节点。

- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 警报历史记录
- 历史属性数据，用于 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的图表和文本报告。

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统一部分或稍后添加的服务器和服务的信息。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将管理节点数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史信息。如果您的系统只有主管理节点，则无法还原管理节点数据库。

> 复制管理节点数据库可能需要几小时的时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 从源管理节点中，停止 MI 服务： `service mi stop`
3. 从源管理节点中，停止管理应用程序接口（ Management Application Program Interface ， mgmt-API ）服务： `service mgmt-api stop`
4. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 停止 MI 服务： `service mi stop`
   c. 停止 mgmt-api 服务： `service mgmt-api stop`
   d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   e. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。
   f. 将数据库从源管理节点复制到已恢复的管理节点： ` /usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. 出现提示时，确认要覆盖已恢复的管理节点上的 MI 数据库。

数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。

h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

5. 在源管理节点上重新启动服务： `service servermanager start`

恢复主管理节点时还原 **Prometheus** 指标

或者，您也可以在出现故障的主管理节点上保留 Prometheus 维护的历史指标。只有当您的 StorageGRID 系统包含另一个管理节点时，才能还原 Prometheus 指标。

- 必须安装并运行已恢复的管理节点。
- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将 Prometheus 数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史指标。如果您的系统只有主管理节点，则无法还原 Prometheus 数据库。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 从源管理节点中，停止 Prometheus 服务： `sservice Prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 停止 Prometheus 服务： `sservice Prometheus stop`

c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

d. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

e. 将 Prometheus 数据库从源管理节点复制到已恢复的管理节点：` /usr/local/Prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

已克隆数据库，正在启动服务

a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

4. 在源管理节点上重新启动 Prometheus 服务。 `sservice Prometheus start`

从非主管理节点故障中恢复

要从非主管理节点故障中恢复，您必须完成以下任务。一个管理节点托管配置管理节点（ CMN ）服务，称为主管理节点。尽管可以有多个管理节点，但每个 StorageGRID 系统仅包含一个主管理节点。所有其他管理节点均为非主管理节点。

相关信息

SG100 和 SG1000 服务设备

从出现故障的非主管理节点复制审核日志

如果您能够从出现故障的管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的非主管理节点启动并运行后将保留的审核日志还原到该节点。

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

如果现在无法在出现故障的管理节点上访问审核日志，您可以稍后访问这些日志，例如在主机恢复之后。

1. 如果可能，请登录到出现故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果有）。

a. 输入以下命令： `ssh admin@grid_node_ip`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止 AMS 服务以防止其创建新的日志文件：`sservice AMS stop`
3. 重命名 audit.log 文件，使其在复制到已恢复的管理节点时不会覆盖现有文件。

   将 audit.log 重命名为唯一编号的文件名，例如 yyyy-mm-dd.txt.1 。例如，您可以将 audit.log 文件重命名为 2015-10-25.txt 。 `1cd /var/local/audit/exportls -l``mv audit.log 2015-10-25.1`
4. 重新启动 AMS 服务： `sservice AMS start`
5. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@grid_node_ip mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。
6. 复制所有审核日志文件： `scp -p * admin@grid_node_ip ： /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。
7. 以 root 用户身份注销： `exit`

更换非主管理节点

要恢复非主管理节点，必须首先更换物理或虚拟硬件。

您可以将出现故障的非主管理节点替换为在同一平台上运行的非主管理节点，也可以将 VMware 上运行的非主管理节点或 Linux 主机替换为服务设备上托管的非主管理节点。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将指导您执行非主管理节点恢复的下一步。

更换平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
SG100 和 SG1000 服务设备	更换服务设备
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

选择 **Start Recovery** 以配置非主管理节点

更换非主管理节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。

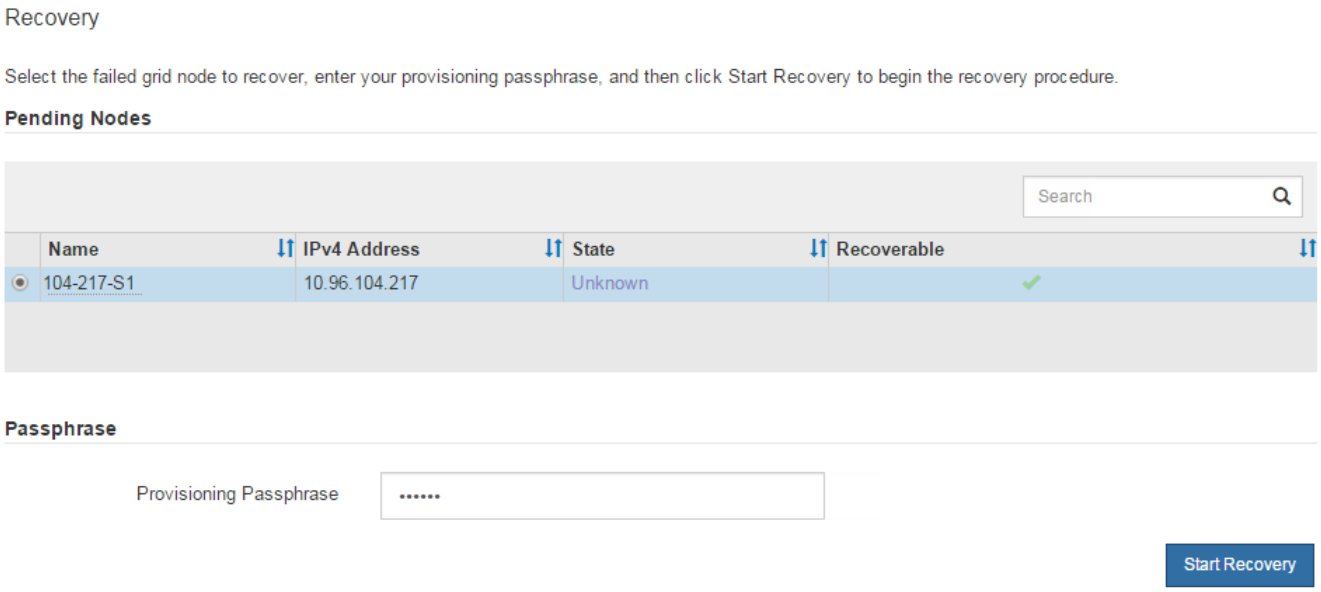
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

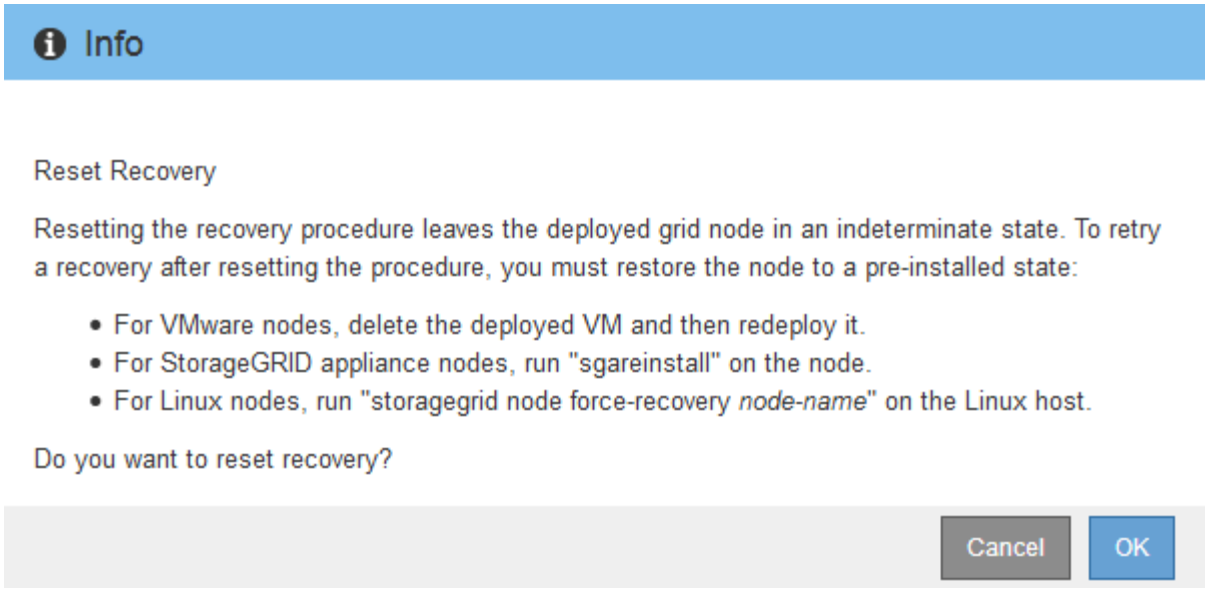
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

> 在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`
- * 设备 * ：如果要在重置操作步骤 后重试恢复，则必须通过在节点上运行 `sgareinstall` 将设备节点还原到预安装状态。

6. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

> 要配置依赖方信任，请参见有关管理 StorageGRID 的说明。要访问默认服务器证书，请登录到管理节点的命令 Shell 。转至 ` /var/local/mgmt-api` 目录，然后选择 `server.crt` 文件。

相关信息

管理 StorageGRID

准备要重新安装的设备（仅限平台更换）

在已恢复的非主管理节点上还原审核日志

如果您能够保留故障非主管理节点中的审核日志，以便保留历史审核日志信息，则可以将其复制到要恢复的非主管理节点。

- 必须安装并运行已恢复的管理节点。
- 在原始管理节点出现故障后，您必须已将审核日志复制到其他位置。

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点，并且无法从故障节点复制审核日志，则恢复的管理节点会开始将事件记录到审核日志中，就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

> 默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：
>
> - 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
> - 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。
>
> 请参见 配置审核消息和日志目标 了解详细信息。

步骤

1. 登录到已恢复的管理节点：
   a. 输入以下命令： + `ssh admin@recovery_Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录后，提示符将从 ` $` 更改为 ` #` 。
2. 检查已保留哪些审核文件：

   ```
   cd /var/local/audit/export
   ```
3. 将保留的审核日志文件复制到已恢复的管理节点：

   ```
   scp admin@grid_node_ip ： /var/local/tmp/saved-audit-logs/yyy*
   ```

   出现提示时，输入 admin 的密码。
4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复管理节点上审核日志文件的用户和组设置：

   ```
   chown AMS-user ： byncast *
   ```
6. 以 root 用户身份注销： `exit`

您还必须还原对审核共享的任何已有客户端访问。有关详细信息，请参见有关管理 StorageGRID 的说明。

相关信息

管理 StorageGRID

在已恢复的非主管理节点上重置首选发送器

如果您要恢复的非主管理节点当前设置为警报通知，警报通知和 AutoSupport 消息的首选发送方，则必须在 StorageGRID 系统中重新配置此设置。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有特定的访问权限。
- 必须安装并运行已恢复的管理节点。

步骤

1. 选择 * 配置 * > * 系统 * > * 显示选项 * 。
2. 从 * 首选发件人 * 下拉列表中选择已恢复的管理节点。
3. 单击 * 应用更改 * 。

相关信息

管理 StorageGRID

恢复非主管理节点时还原管理节点数据库

如果要在出现故障的非主管理节点上保留有关属性，警报和警报的历史信息，则可以从主管理节点还原管理节点数据库。

- 必须安装并运行已恢复的管理节点。
- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 警报历史记录
- 历史属性数据，用于 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的图表和文本报告。

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统一部分或稍后添加的服务器和服务的信息。

如果还原了非主管理节点，则可以通过将管理节点数据库从主管理节点（ *source Admin Node* ）复制到恢复的节点来还原历史信息。

> 复制管理节点数据库可能需要几小时的时间。在源节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

2. 从源管理节点运行以下命令。然后，根据提示输入配置密码短语。`re`覆盖访问点

3. 从源管理节点中，停止 MI 服务： `service mi stop`

4. 从源管理节点中，停止管理应用程序接口（ Management Application Program Interface ， mgmt-API ）服务： `service mgmt-api stop`

5. 在已恢复的管理节点上完成以下步骤：

a. 登录到已恢复的管理节点：

i. 输入以下命令： `ssh admin@ grid_node_ip_`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。

b. 停止 MI 服务： `service mi stop`

c. 停止 mgmt-api 服务： `service mgmt-api stop`

d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

e. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

f. 将数据库从源管理节点复制到已恢复的管理节点： ` /usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. 出现提示时，确认要覆盖已恢复的管理节点上的 MI 数据库。

数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。

h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

6. 在源管理节点上重新启动服务： `service servermanager start`

恢复非主管理节点时还原 **Prometheus** 指标

您也可以在出现故障的非主管理节点上保留 Prometheus 维护的历史指标。

- 必须安装并运行已恢复的管理节点。
- StorageGRID 系统必须至少包含两个管理节点。
- 您必须具有 `passwords.txt` 文件。
- 您必须具有配置密码短语。

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果还原了非主管理节点，则可以通过将 Prometheus 数据库从主管理节点（ *source Admin Node* ）复制到恢

复的管理节点来还原历史指标。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 从源管理节点中，停止 Prometheus 服务： `sservice Prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@ grid_node_ip_`
      ii. 输入 `passwords.txt` 文件中列出的密码。
      iii. 输入以下命令切换到 root： `su -`
      iv. 输入 `passwords.txt` 文件中列出的密码。
   b. 停止 Prometheus 服务： `sservice Prometheus stop`
   c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   d. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。
   e. 将 Prometheus 数据库从源管理节点复制到已恢复的管理节点： ` /usr/local/Prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

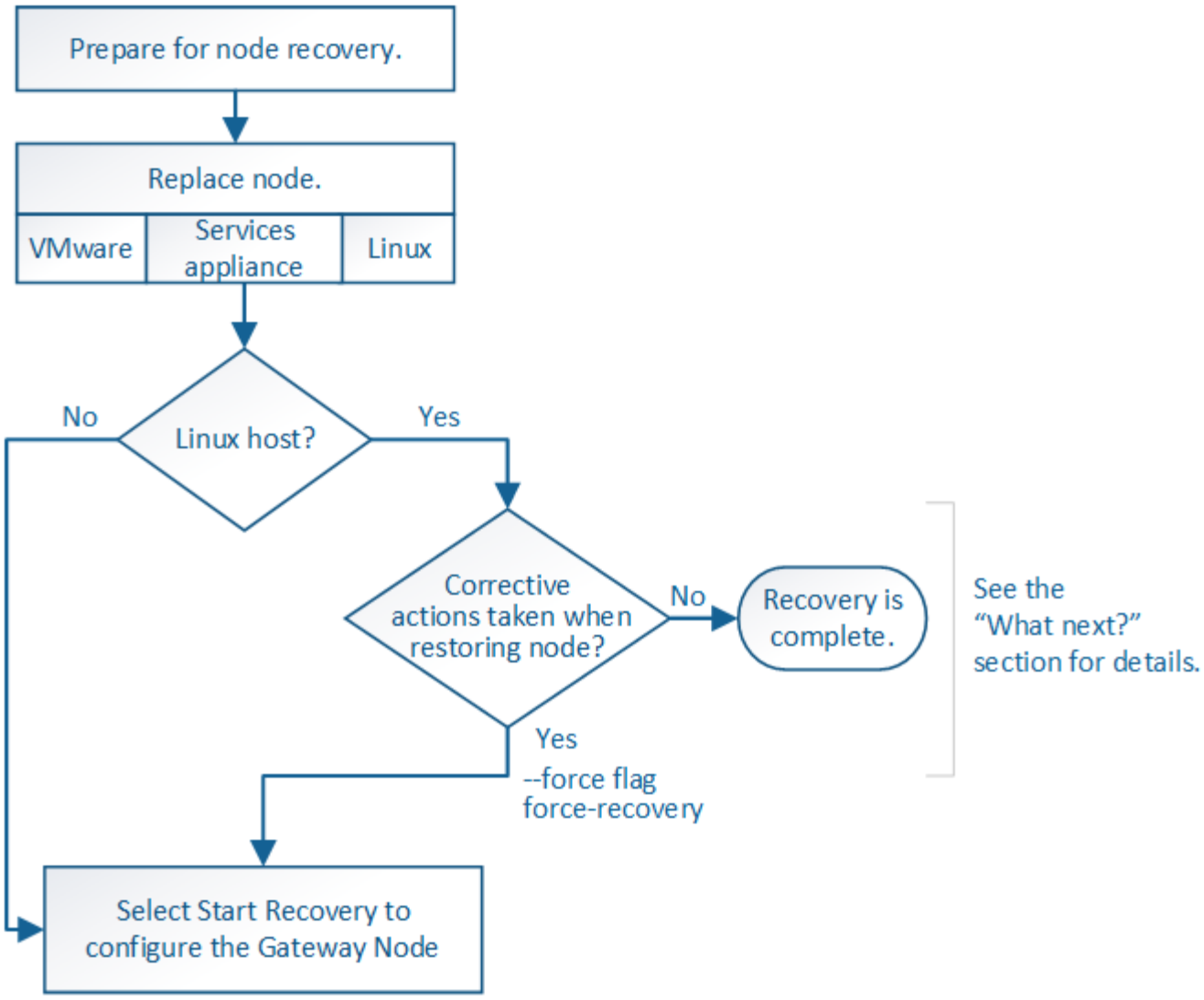
      原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

   已克隆数据库，正在启动服务

   a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`
4. 在源管理节点上重新启动 Prometheus 服务。 `sservice Prometheus start`

从网关节点故障中恢复

要从网关节点故障中恢复，您必须按确切顺序完成一系列任务。



相关信息

SG100 和 SG1000 服务设备

更换网关节点

您可以将出现故障的网关节点更换为运行在同一物理或虚拟硬件上的网关节点，也可以将运行在 VMware 或 Linux 主机上的网关节点更换为托管在服务设备上的网关节点。

您必须遵循的节点更换操作步骤 取决于更换节点将使用的平台。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将指导您执行网关节点恢复的下一步。

更换平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
SG100 和 SG1000 服务设备	更换服务设备

更换平台	操作步骤
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

选择 **Start Recovery** 以配置网关节点

更换网关节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

您需要的内容

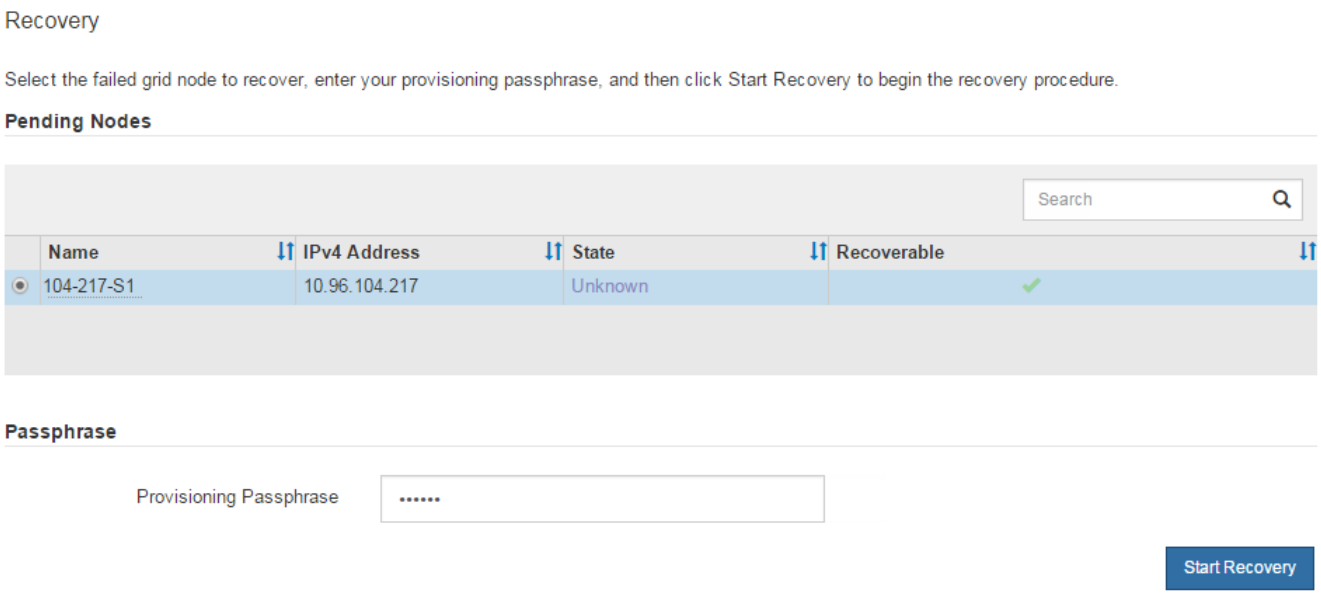
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。

步骤

1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

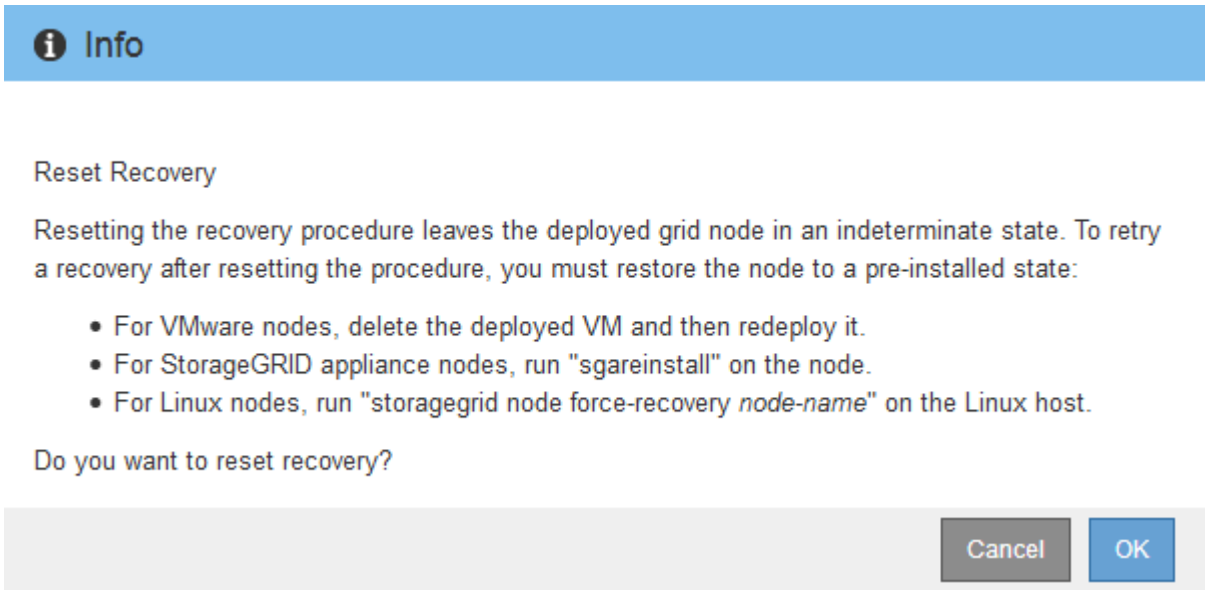
   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。

3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

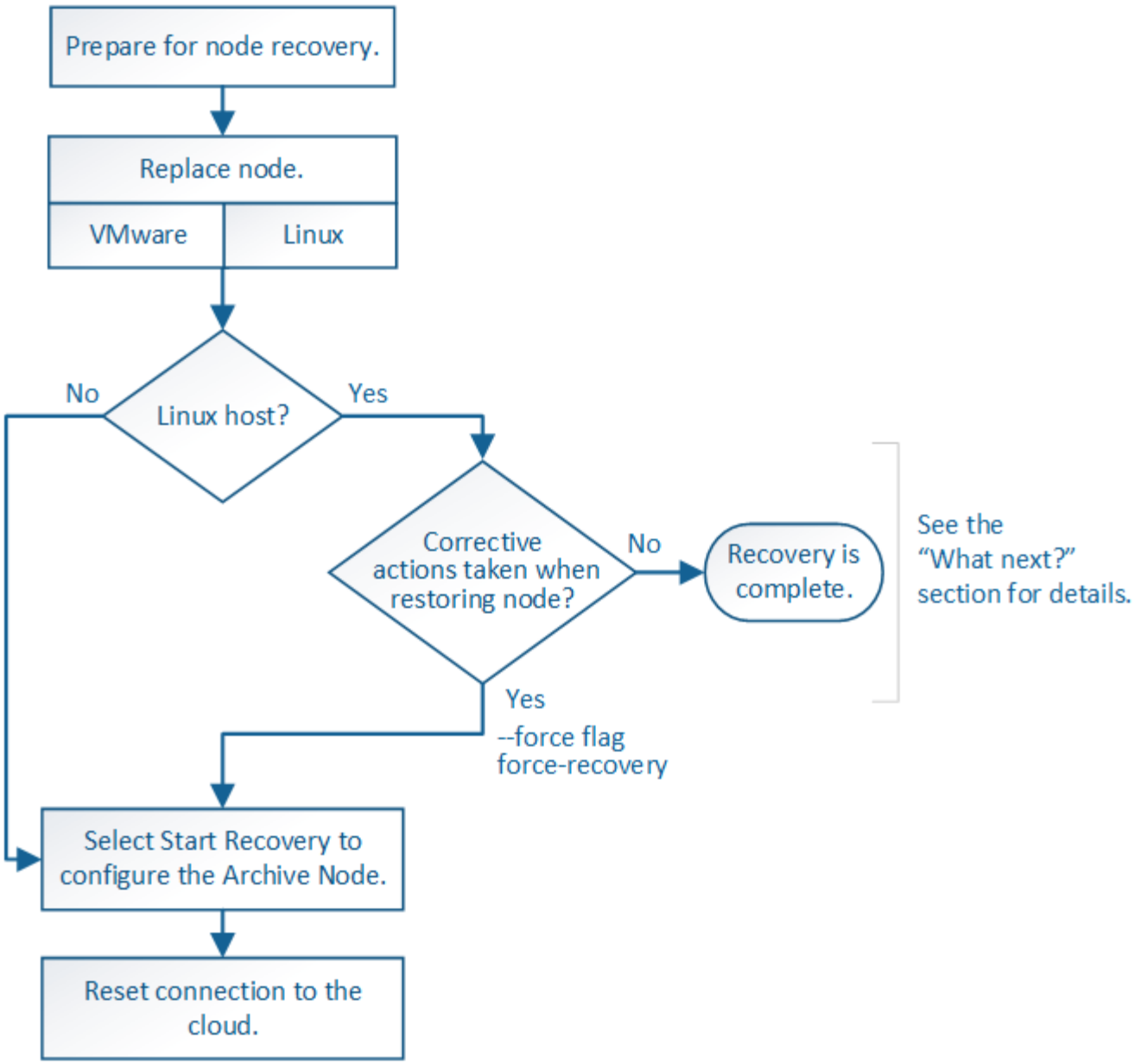
- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`
- * 设备 * ：如果要在重置操作步骤 后重试恢复，则必须通过在节点上运行 `sgareinstall` 将设备节点还原到预安装状态。

相关信息

准备要重新安装的设备（仅限平台更换）

从归档节点故障中恢复

要从归档节点故障中恢复，您必须按确切顺序完成一系列任务。



关于此任务

归档节点恢复受以下问题影响：

- 如果 ILM 策略配置为复制单个副本。

  在配置为创建一个对象副本的 StorageGRID 系统中，归档节点故障可能会导致无法恢复的数据丢失。如果发生故障，所有此类对象都将丢失；但是，您仍必须执行恢复过程 "`清理` " StorageGRID 系统并清除数据库中丢失的对象信息。

- 如果在存储节点恢复期间发生归档节点故障。

  如果在存储节点恢复过程中处理批量检索时归档节点出现故障， 您必须重复操作步骤 以从头开始将对象数据的副本恢复到存储节点，以确保从归档节点检索到的所有对象数据都还原到存储节点。

要恢复归档节点，必须先更换该节点。

您必须为您的平台选择节点替代操作步骤 。对于所有类型的网格节点，更换节点的步骤都相同。

平台	操作步骤
VMware	更换 VMware 节点
Linux	更换 Linux 节点
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照操作步骤 更换 Linux 节点。

更换归档节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

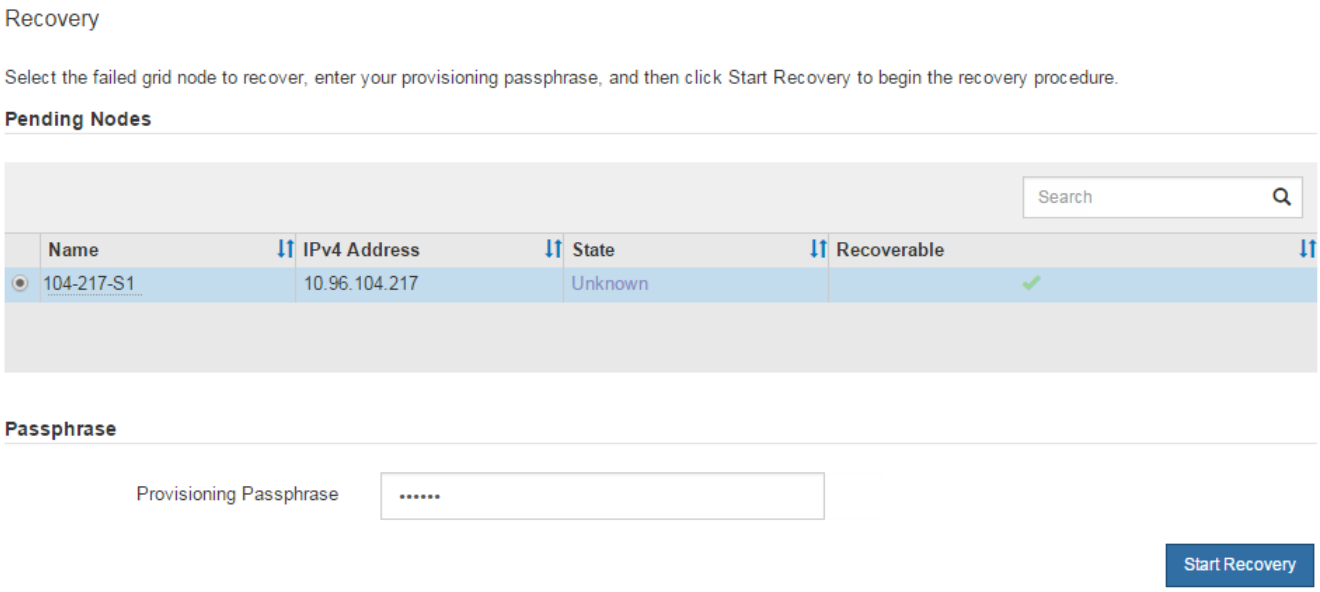
您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须已部署并配置替代节点。

步骤

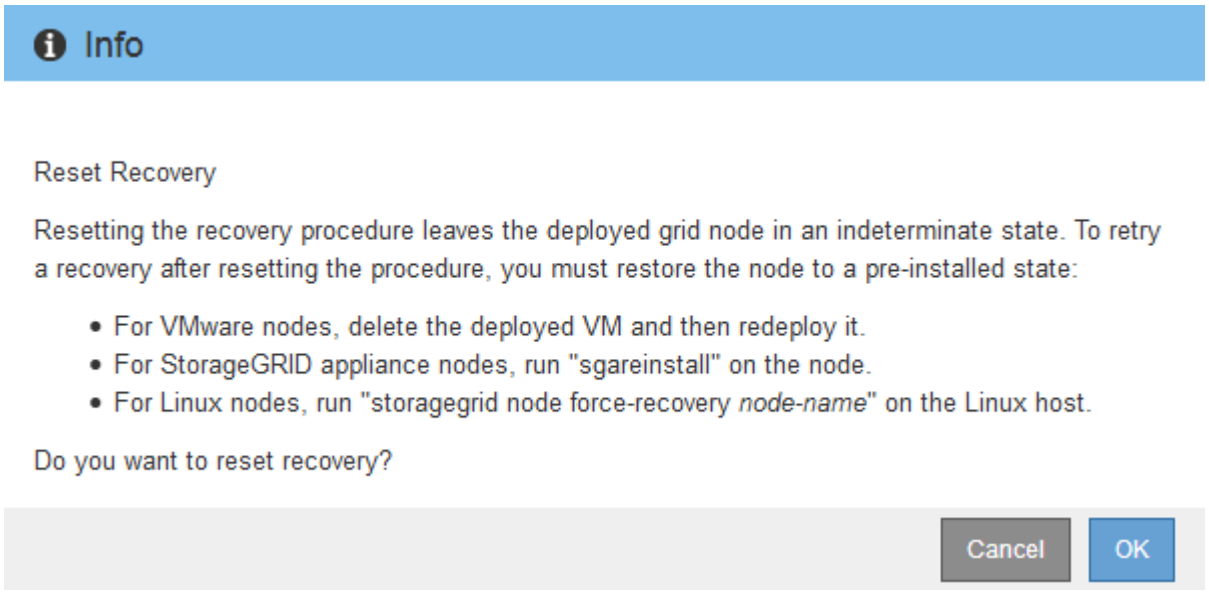
1. 在网格管理器中，选择 * 维护 * > * 任务 * > * 恢复 * 。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点出现故障后，它们将显示在列表中，但您无法选择节点，除非节点已重新安装并准备好进行恢复。
3. 输入 * 配置密码短语 * 。
4. 单击 * 启动恢复 * 。



5. 在恢复网格节点表中监控恢复进度。

> 在恢复操作步骤 运行期间，您可以单击 * 重置 * 以启动新的恢复。此时将显示一个信息对话框，指示在重置操作步骤 时节点将处于不确定状态。



如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- * Linux * ：在 Linux 主机上运行此命令以重新启动节点： `StorageGRID node force-recovery node-name`

将归档节点连接重置为云

通过 S3 API 恢复以云为目标的归档节点后，您需要修改配置设置以重置连接。如果归档节点无法检索对象数据，则会触发出站复制状态（ ORSU ）警报。

如果归档节点通过 TSM 中间件连接到外部存储，则该节点将自动重置，您无需重新配置。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARE* > * 目标 * 。
3. 输入不正确的值以编辑 * 访问密钥 * 字段，然后单击 * 应用更改 * 。
4. 输入正确的值以编辑 * 访问密钥 * 字段，然后单击 * 应用更改 * 。

所有网格节点类型：更换 **VMware** 节点

在恢复 VMware 上托管的故障 StorageGRID 节点时，必须删除故障节点并部署恢复节点。

您需要的内容

您必须已确定虚拟机无法还原，并且必须更换。

关于此任务

您可以使用 VMware vSphere Web Client 首先删除与故障网格节点关联的虚拟机。然后，您可以部署新的虚拟机。

此操作步骤 只是网格节点恢复过程中的一个步骤。所有 VMware 节点的节点删除和部署操作步骤 均相同，包括管理节点，存储节点，网关节点和归档节点。

步骤

1. 登录到 VMware vSphere Web Client 。
2. 导航到出现故障的网格节点虚拟机。
3. 记下部署恢复节点所需的所有信息。
   a. 右键单击虚拟机，选择 * 编辑设置 * 选项卡，并记下正在使用的设置。
   b. 选择 * vApp 选项 * 选项卡以查看和记录网格节点网络设置。
4. 如果发生故障的网格节点是存储节点，请确定用于数据存储的任何虚拟硬盘是否完好无损，并保留这些虚拟硬盘以重新连接到已恢复的网格节点。
5. 关闭虚拟机。
6. 选择 * 操作 * > * 所有 vCenter 操作 * > * 从磁盘中删除 * 以删除虚拟机。
7. 将新虚拟机部署为替代节点，并将其连接到一个或多个 StorageGRID 网络。

   部署节点时，您可以选择重新映射节点端口或增加 CPU 或内存设置。

   部署新节点后，您可以根据存储要求添加新的虚拟磁盘，重新连接从先前删除的故障网格节点中保留的任何虚拟硬盘，或者同时添加这两者。

   有关说明：

安装 VMware > 将 StorageGRID 节点部署为虚拟机

8. 根据要恢复的节点类型完成节点恢复操作步骤 。

节点类型	转至
主管理节点	配置替代主管理节点
非主管理节点	选择 Start Recovery 以配置非主管理节点
网关节点	选择 Start Recovery 以配置网关节点
存储节点	选择启动恢复以配置存储节点
归档节点	选择启动恢复以配置归档节点

所有网格节点类型：替换 **Linux** 节点

如果发生故障时需要部署一个或多个新的物理或虚拟主机或在现有主机上重新安装 Linux ，则必须先部署和配置替代主机，然后才能恢复网格节点。对于所有类型的网格节点，此操作步骤 是网格节点恢复过程的一个步骤。

"`Linux` " 是指 Red Hat ® Enterprise Linux ® ， Ubuntu ® ， CentOS 或 Debian ® 部署。使用 NetApp 互操作性表工具可获取受支持版本的列表。

此操作步骤 仅在恢复基于软件的存储节点，主管理节点或非主管理节点，网关节点或归档节点的过程中执行一步。无论您要恢复的网格节点类型如何，这些步骤都是相同的。

如果物理或虚拟 Linux 主机上托管了多个网格节点，则可以按任意顺序恢复网格节点。但是，如果存在主管理节点，则首先恢复主管理节点会阻止其他网格节点在尝试联系主管理节点进行注册以进行恢复时停止恢复。

相关信息

"NetApp 互操作性表工具"

部署新的 **Linux** 主机

除了一些例外情况，您可以像在初始安装过程中一样准备新主机。

要部署新的或重新安装的物理或虚拟 Linux 主机，请按照适用于 Linux 操作系统的 StorageGRID 安装说明中的操作步骤 准备主机。

此操作步骤 包含用于完成以下任务的步骤：

1. 安装 Linux 。
2. 配置主机网络。
3. 配置主机存储。
4. 安装容器引擎。

5. 安装 StorageGRID 主机服务。

> 完成安装说明中的 "`安装 StorageGRID 主机服务` " 任务后停止。请勿启动 " D部署网格节点 " 任务。

执行这些步骤时，请注意以下重要准则：

- 请确保使用与原始主机上使用的主机接口名称相同的主机接口名称。
- 如果您使用共享存储来支持 StorageGRID 节点，或者已将部分或全部磁盘驱动器或 SSD 从故障节点移至替代节点，则必须重新建立原始主机上的相同存储映射。例如，如果按照安装说明中的建议在 ` /etc/multipath.conf` 中使用了 WWID 和别名，请务必在替代主机上的 ` /etc/multipath.conf` 中使用相同的别名 /WWID 对。
- 如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

将网格节点还原到主机

要将出现故障的网格节点还原到新的 Linux 主机，请使用相应的命令还原节点配置文件。

执行全新安装时，您需要为要安装在主机上的每个网格节点创建一个节点配置文件。将网格节点还原到替代主机时，您需要还原或替换任何出现故障的网格节点的节点配置文件。

如果从上一主机保留了任何块存储卷，则可能需要执行其他恢复过程。本节中的命令可帮助您确定需要执行的其他过程。

步骤

- 还原和验证网格节点
- 启动 StorageGRID 主机服务
- 恢复无法正常启动的节点

还原和验证网格节点

您必须还原任何出现故障的网格节点的网格配置文件，然后验证网格配置文件并解决任何错误。

关于此任务

您可以导入主机上应存在的任何网格节点，前提是其 ` 或 var/local` 卷未因上一主机故障而丢失。例如，如果您为 StorageGRID 系统数据卷使用共享存储，则 ` /var/local` 卷可能仍存在，如适用于 Linux 操作系统的 StorageGRID 安装说明中所述。导入节点会将其节点配置文件还原到主机。

如果无法导入缺少的节点，则必须重新创建其网格配置文件。

然后，您必须验证网格配置文件，并解决可能发生的任何网络或存储问题，然后再继续重新启动 StorageGRID 。重新创建节点的配置文件时，必须为要恢复的节点所使用的替代节点使用相同的名称。

有关节点的 ` /var/local` 卷位置的详细信息，请参见安装说明。

步骤

1. 在已恢复主机的命令行中，列出当前已配置的所有 StorageGRID 网格节点：`sUdo StorageGRID node list`

   如果未配置网格节点，则不会显示任何输出。如果配置了某些网格节点，则输出格式应为：

```
Name                Metadata-Volume
=============================================================
dc1-adm1            /dev/mapper/sgws-adm1-var-local
dc1-gw1             /dev/mapper/sgws-gw1-var-local
dc1-sn1             /dev/mapper/sgws-sn1-var-local
dc1-arc1            /dev/mapper/sgws-arc1-var-local
```

   如果未列出应在主机上配置的部分或全部网格节点，则需要还原缺少的网格节点。

2. 要导入具有 ` /var/local` 卷的网格节点，请执行以下操作：

   a. 对要导入的每个节点运行以下命令：`sUdo StorageGRID node import node-var-local-volume-path`

      只有当目标节点在上次运行的主机上完全关闭时， `StorageGRID node import` 命令才会成功。否则，您将看到类似以下内容的错误：

      此节点（ *node-name* ）似乎归另一主机所有（ `UUID host-uuid` ）。

   如果您确定导入安全，请使用 `-force` 标志。

   a. 如果您看到有关节点归另一主机所有的错误，请使用 ` -force` 标志再次运行命令以完成导入：`sUdo StorageGRID --force node import node-var-local-volume-path`

      使用 ` -force` 标志导入的任何节点都需要执行额外的恢复步骤，才能重新加入网格，如中所述 下一步操作：如果需要，执行其他恢复步骤。

3. 对于没有 ` /var/local` 卷的网格节点，请重新创建节点的配置文件以将其还原到主机。

   请按照安装说明中 "`Create node configuration files` " 中的准则进行操作。

   重新创建节点的配置文件时，必须为要恢复的节点所使用的替代节点使用相同的名称。对于 Linux 部署，请确保配置文件名称包含节点名称。应尽可能使用相同的网络接口，块设备映射和 IP 地址。这种做法可以最大限度地减少恢复期间需要复制到节点的数据量，从而可以显著加快恢复速度（在某些情况下，只需几分钟而不是几周）。

如果在为节点重新创建配置文件时使用任何新的块设备（ StorageGRID 节点先前未使用的设备）作为以 `block_device_` 开头的任何配置变量的值，请务必遵循中的所有准则 修复缺少的块设备错误。

4. 在已恢复的主机上运行以下命令以列出所有 StorageGRID 节点。

   `sUdo StorageGRID 节点列表`

5. 验证名称显示在 StorageGRID 节点列表输出中的每个网格节点的节点配置文件：

   `sUdo StorageGRID node validate node-name`

   在启动 StorageGRID 主机服务之前，您必须解决任何错误或警告。以下各节详细介绍了在恢复期间可能具有特殊意义的错误。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

修复缺少的网络接口错误

修复缺少的网络接口错误

如果主机网络配置不正确或名称拼写错误，则在 StorageGRID 检查 ` /etc/storaggrid/nodes/*node-name*.conf` 文件中指定的映射时会发生错误。

您可能会看到与此模式匹配的错误或警告：

正在检查节点 *node-name* **的配置文件** ` /etc/storaggrid/nodes/*node-name*.conf 。` **错误：** *node-name* ： `grid_network_target = *host-interface-name*` *node-name* ： interface '*host-interface-name*' does not exist`

可能会报告网格网络，管理网络或客户端网络的错误。此错误表示 ` /etc/storaggrid/nodes/*node-name*.conf` 文件会将指示的 StorageGRID 网络映射到名为 ` 主机接口名称 _` 的主机接口，但当前主机上没有具有此名称的接口。

如果收到此错误，请确认您已完成中的步骤 部署新的 Linux 主机。对所有主机接口使用与原始主机相同的名称。

如果您无法为主机接口命名以匹配节点配置文件，则可以编辑节点配置文件，并更改 grid_network_target ，admin_network_target 或 client_network_target 的值以匹配现有主机接口。

确保主机接口提供对相应物理网络端口或 VLAN 的访问，并且该接口不直接引用绑定或网桥设备。您必须在主机上的绑定设备上配置 VLAN （或其他虚拟接口），或者使用网桥和虚拟以太网（ veth ）对。

修复缺少的块设备错误

系统会检查每个已恢复的节点是否映射到有效的块设备专用文件或块设备专用文件的有效软链接。如果 StorageGRID 在 ` /etc/storaggrid/nodes/*node-name*.conf` 文件中发现映射

无效，则会显示缺少块设备错误。

如果您发现与此模式匹配的错误：

正在检查节点 *node-name* 的配置文件 `/etc/storaggrid/nodes/node-name.conf` … 错误： *node-name* ： `block_device_purpose = path-name` *node-name* ： *path-name* 不存在`

这意味着， `/etc/storagegRid/nodes/*node-name*.conf` 会将 *node-name* 用于目的的块设备映射到 Linux 文件系统中的给定路径名，但该位置没有有效的块设备专用文件或指向块设备专用文件的软链接。

确认您已完成中的步骤 部署新的 Linux 主机。对所有块设备使用与原始主机相同的永久性设备名称。

如果无法还原或重新创建缺少的块设备专用文件，您可以分配一个具有适当大小和存储类别的新块设备，并编辑节点配置文件以更改 block_device_purpose 的值以指向新的块设备专用文件。

从适用于您的 Linux 操作系统的安装说明的 s存储要求 一节中的表中确定适当的大小和存储类别。在继续更换块设备之前，请查看 "`配置主机存储` " 中的建议。

> 如果您必须为以 `block_device_` 开头的任何配置文件变量提供一个新的块存储设备，因为故障主机丢失了原始块设备，请在尝试执行进一步的恢复过程之前确保新块设备未格式化。如果您使用的是共享存储并已创建新卷，则新块设备将取消格式化。如果不确定，请对任何新的块存储设备特殊文件运行以下命令。

小心

仅对新块存储设备运行以下命令。如果您认为块存储仍包含要恢复的节点的有效数据，请勿运行此命令，因为设备上的任何数据都将丢失。

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

启动 **StorageGRID** 主机服务

要启动 StorageGRID 节点并确保它们在主机重新启动后重新启动，您必须启用并启动 StorageGRID 主机服务。

1. 在每个主机上运行以下命令：

   ```
   sudo systemctl enable storagegrid
   sudo systemctl start storagegrid
   ```

2. 运行以下命令以确保部署正在进行：

   `sUdo StorageGRID node status *node-name*`

对于返回未运行或已停止状态的任何节点，请运行以下命令：

`sUdo StorageGRID node start node-name`

3. 如果您先前已启用并启动 StorageGRID 主机服务（或者不确定此服务是否已启用和启动），请同时运行以下命令：

```
sudo systemctl reload-or-restart storagegrid
```

恢复无法正常启动的节点

如果 StorageGRID 节点未正常重新加入网格，并且无法显示为可恢复，则可能已损坏。您可以强制节点进入恢复模式。

要强制节点进入恢复模式，请执行以下操作：

`sUdo StorageGRID node force-recovery node-name`

发出此命令之前，请确认节点的网络配置正确无误；节点可能由于网络接口映射不正确或网格网络 IP 地址或网关不正确而无法重新加入网格。

发出 `StorageGRID node force-recovery node-name` 命令后，您必须对 *node-name* 执行其他恢复步骤。

相关信息

下一步操作：如果需要，执行其他恢复步骤

下一步操作：如果需要，执行其他恢复步骤

根据您为使 StorageGRID 节点在替代主机上运行而采取的特定操作，您可能需要对每个节点执行其他恢复步骤。

如果在更换 Linux 主机或将故障网格节点还原到新主机时不需要采取任何更正操作，则节点恢复已完成。

更正操作和后续步骤

在更换节点期间，您可能需要执行以下更正操作之一：

- 您必须使用 ` -force` 标志来导入节点。
- 对于任何 ` ， `block_device_<utility> 配置文件变量的值是指块设备，该块设备包含的数据与主机发生故障之前的数据不同。
- 您已为此节点发出 `StorageGRID node force-recovery node-name` 命令。
- 您添加了一个新的块设备。

如果您采取了上述 * 任何 * 更正操作，则必须执行其他恢复步骤。

恢复类型	下一步
主管理节点	配置替代主管理节点
非主管理节点	选择 Start Recovery 以配置非主管理节点
网关节点	选择 Start Recovery 以配置网关节点
归档节点	选择启动恢复以配置归档节点
存储节点（基于软件）： • 如果您必须使用 ` -force` 标志导入节点，或者发出了 `StorageGRID node force-recovery node-name` • 如果您必须执行完整节点重新安装，或者需要还原 /var/local	选择启动恢复以配置存储节点
存储节点（基于软件）： • 添加新块设备时。 • 如果对于任何 ` < 目的 >` ， `block_device_<目的>` 配置文件变量的值是指块设备，而该块设备所包含的数据与主机发生故障之前的数据不同。	从系统驱动器完好无损的存储卷故障中恢复

将故障节点更换为服务设备

您可以使用 SG100 或 SG1000 服务设备恢复出现故障的网关节点，出现故障的非主管理节点或 VMware 上托管的主管理节点， Linux 主机或服务设备发生故障。此操作步骤 是网格节点恢复操作步骤 的一个步骤。

您需要的内容

- 您必须已确定以下情况之一是正确的：
  - 无法还原托管此节点的虚拟机。
  - 网格节点的物理或虚拟 Linux 主机出现故障，必须更换。
  - 必须更换托管网格节点的服务设备。
- 您必须确保服务设备上的 StorageGRID 设备安装程序版本与 StorageGRID 系统的软件版本匹配，如用于验证和升级 StorageGRID 设备安装程序版本的硬件安装和维护中所述。

  SG100 和 SG1000 服务设备

> 不要在同一站点同时部署 SG100 和 SG1000 服务设备。可能会导致性能不可预测。

关于此任务

在以下情况下，您可以使用 SG100 或 SG1000 服务设备恢复出现故障的网格节点：

- 故障节点托管在 VMware 或 Linux 上（平台更改）
- 故障节点托管在服务设备上（平台更换）

安装服务设备（仅限平台更改）

如果要恢复 VMware 或 Linux 主机上托管的故障网格节点，并且要使用 SG100 或 SG1000 服务设备作为替代节点，则必须先使用与故障节点相同的节点名称安装新设备硬件。

您必须具有有关故障节点的以下信息：

- * 节点名称 *：必须使用与故障节点相同的节点名称安装服务设备。
- * IP 地址 *：您可以为服务设备分配与故障节点相同的 IP 地址，这是首选选项，也可以在每个网络上选择新的未使用的 IP 地址。

只有在恢复 VMware 或 Linux 上托管的故障节点并将其替换为服务设备上托管的节点时，才执行此操作步骤 。

1. 按照说明安装新的 SG100 或 SG1000 服务设备。
2. 当系统提示您输入节点名称时，请使用故障节点的节点名称。

相关信息

SG100 和 SG1000 服务设备

准备要重新安装的设备（仅限平台更换）

在恢复服务设备上托管的网格节点时，您必须先准备该设备以重新安装 StorageGRID 软件。

只有在更换服务设备上托管的故障节点时，才执行此操作步骤 。如果故障节点最初托管在 VMware 或 Linux 主机上，请勿执行以下步骤。

1. 登录到出现故障的网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 准备用于安装 StorageGRID 软件的设备。输入： `sgareinstall`
3. 当系统提示您继续时，输入： `y`

   设备将重新启动， SSH 会话将结束。StorageGRID 设备安装程序通常需要大约 5 分钟才能投入使用，但在某些情况下，您可能需要等待长达 30 分钟。

服务设备将重置，并且网格节点上的数据将无法再访问。在初始安装过程中配置的 IP 地址应保持不变；但是，建议您在操作步骤 完成后进行确认。

执行 `sgareinstall` 命令后，将删除所有 StorageGRID 配置的帐户，密码和 SSH 密钥，并生成新的主机密钥。

开始在服务设备上安装软件

要在 SG100 或 SG1000 服务设备上安装网关节点或管理节点，请使用此设备上随附的 StorageGRID 设备安装程序。

您需要的内容

- 此设备必须安装在机架中，并连接到您的网络并已启动。
- 必须使用 StorageGRID 设备安装程序为此设备配置网络链路和 IP 地址。
- 如果要安装网关节点或非主管理节点，则您知道 StorageGRID 网格的主管理节点的 IP 地址。
- 必须在主管理节点上的网格网络子网列表中定义 StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网。

有关完成这些前提条件任务的说明，请参见 SG100 或 SG1000 服务设备的安装和维护说明。

- 您必须使用 支持的 Web 浏览器。
- 您必须知道分配给设备的 IP 地址之一。您可以使用管理网络，网格网络或客户端网络的 IP 地址。
- 如果您要安装主管理节点，则可以使用此版本 StorageGRID 的 Ubuntu 或 Debian 安装文件。

> 在制造过程中，服务设备会预加载最新版本的 StorageGRID 软件。如果预加载的软件版本与 StorageGRID 部署中使用的版本匹配，则不需要安装文件。

关于此任务

要在 SG100 或 SG1000 服务设备上安装 StorageGRID 软件，请执行以下操作：

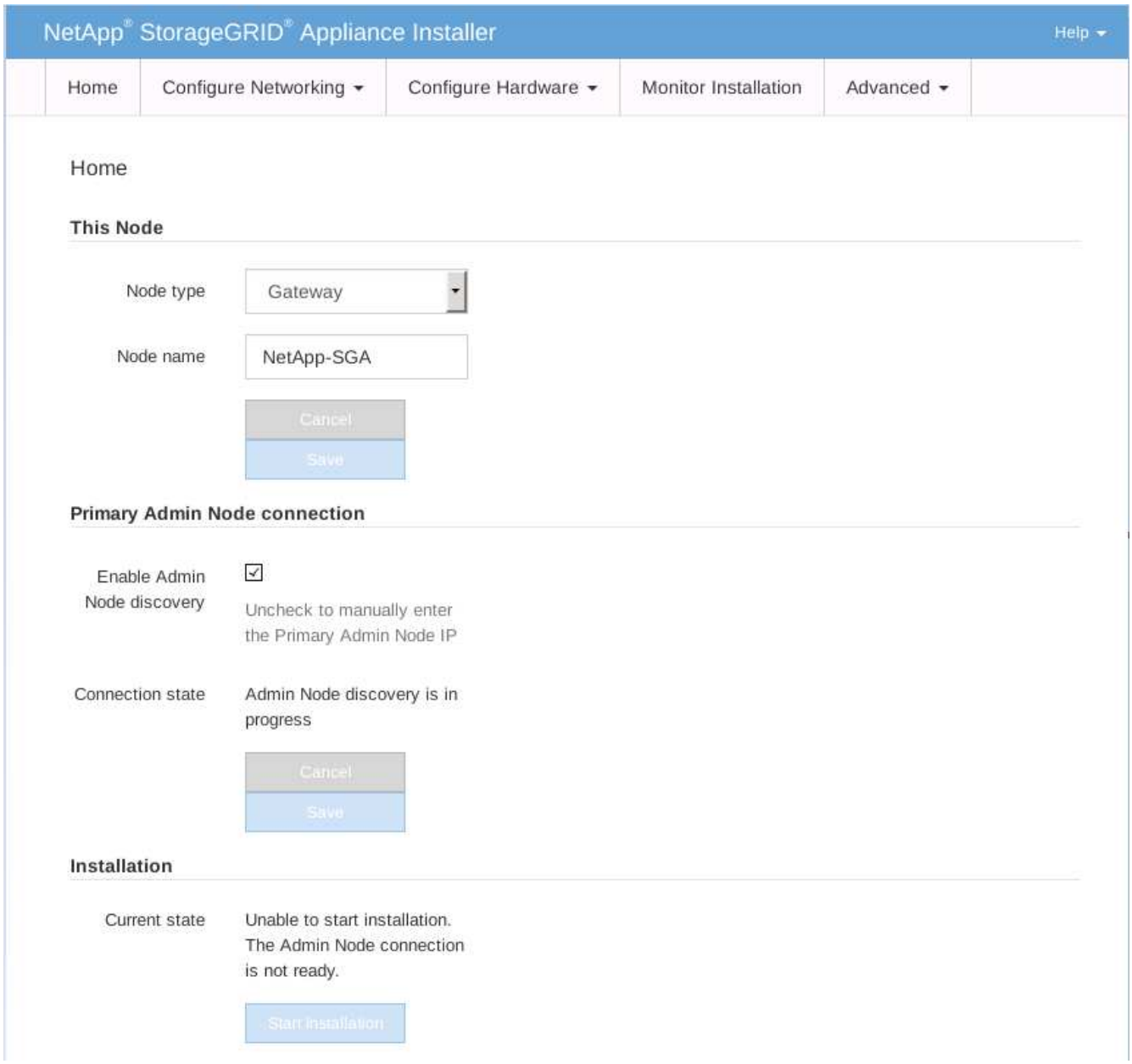
- 对于主管理节点，您可以指定节点的名称，然后上传相应的软件包（如果需要）。
- 对于非主管理节点或网关节点，您可以指定或确认主管理节点的 IP 地址以及节点的名称。
- 您开始安装，并等待卷配置完毕并安装软件。
- 在整个过程中，安装将暂停。要恢复安装，您必须登录到网格管理器并将待定节点配置为故障节点的替代节点。
- 配置节点后，设备安装过程将完成，设备将重新启动。

步骤

1. 打开浏览器并输入 SG100 或 SG1000 服务设备的 IP 地址之一。

   ` + https://Controller_IP:8443+`

   此时将显示 StorageGRID 设备安装程序主页页面。



2. 安装主管理节点：

   a. 在 "This Node" 部分中，对于 "* 节点类型 " ，选择 "* 主管理 * " 。

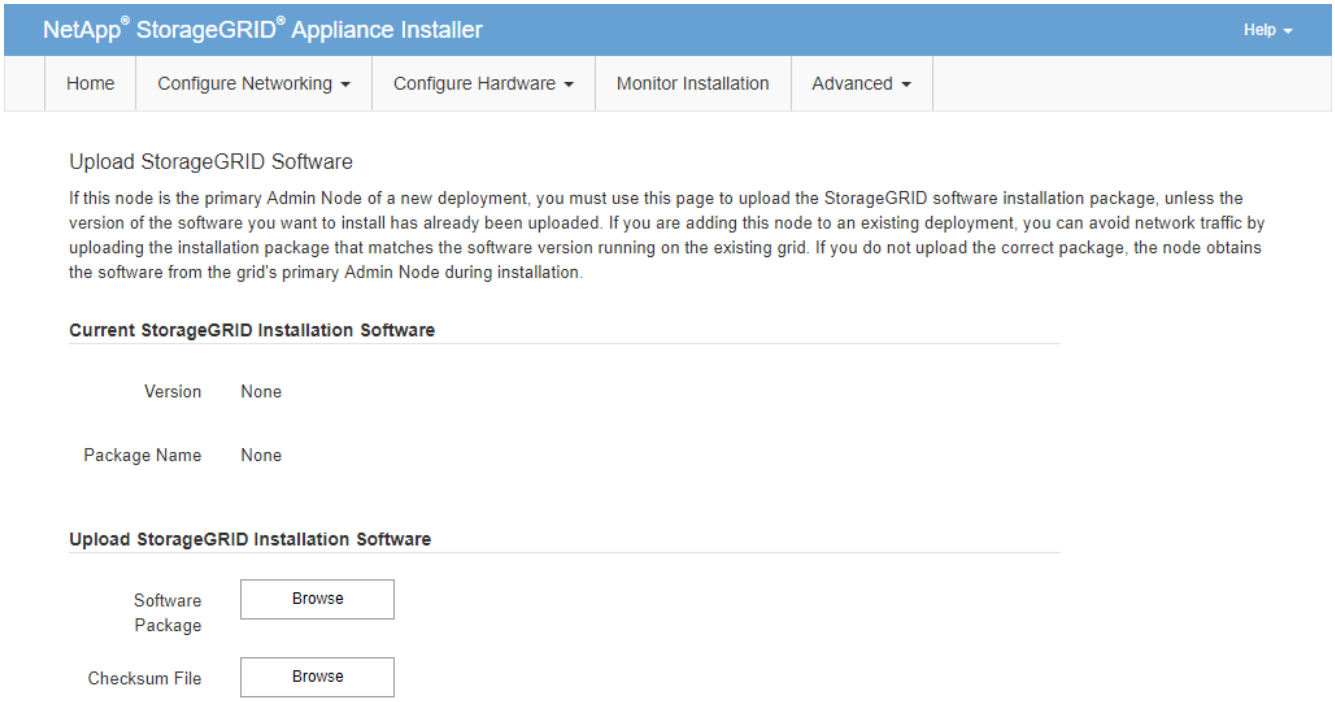
   b. 在 * 节点名称 * 字段中，输入与要恢复的节点相同的名称，然后单击 * 保存 * 。

   c. 在安装部分中，检查当前状态下列出的软件版本

      如果准备安装的软件版本正确，请跳至 安装步骤。

   d. 如果需要上传其他版本的软件，请在 * 高级 * 菜单下选择 * 上传 StorageGRID 软件 * 。

      此时将显示上传 StorageGRID 软件页面。



a. 单击 * 浏览 * 上传适用于 StorageGRID 软件的 * 软件包 * 和 * 校验和文件 * 。

选择这些文件后，这些文件将自动上传。

b. 单击 * 主页 * 返回到 StorageGRID 设备安装程序主页页面。

3. 安装网关节点或非主管理节点：

a. 在 "This Node" 部分中，对于 "* 节点类型 " ，根据要还原的节点类型选择 "* 网关 * " 或 "* 非主管理 * " 。

b. 在 * 节点名称 * 字段中，输入与要恢复的节点相同的名称，然后单击 * 保存 * 。

c. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

假设主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上， StorageGRID 设备安装程序可以自动发现此 IP 地址。

d. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	Description
手动输入 IP	a. 取消选中 * 启用管理节点发现 * 复选框。 b. 手动输入 IP 地址。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

选项	Description
自动发现所有已连接的主管理节点	a. 选中 * 启用管理节点发现 * 复选框。 b. 从已发现的 IP 地址列表中，选择要部署此服务设备的网格的主管理节点。 c. 单击 * 保存 * 。 d. 请稍候，此时新 IP 地址的连接状态将变为 `ready` 。

4. 在 "Installation_section_steP]] 中，确认当前状态为 Ready to start installation of node name 且 * Start Installation* 按钮已启用。

   如果未启用 * 开始安装 * 按钮，则可能需要更改网络配置或端口设置。有关说明，请参见设备的安装和维护说明。

5. 在 StorageGRID 设备安装程序主页中，单击 * 开始安装 * 。

   当前状态将更改为 "`Installation is in progress ，` " ，此时将显示监控器安装页面。

   如果需要手动访问监控器安装页面，请单击菜单栏中的 * 监控器安装 * 。

相关信息

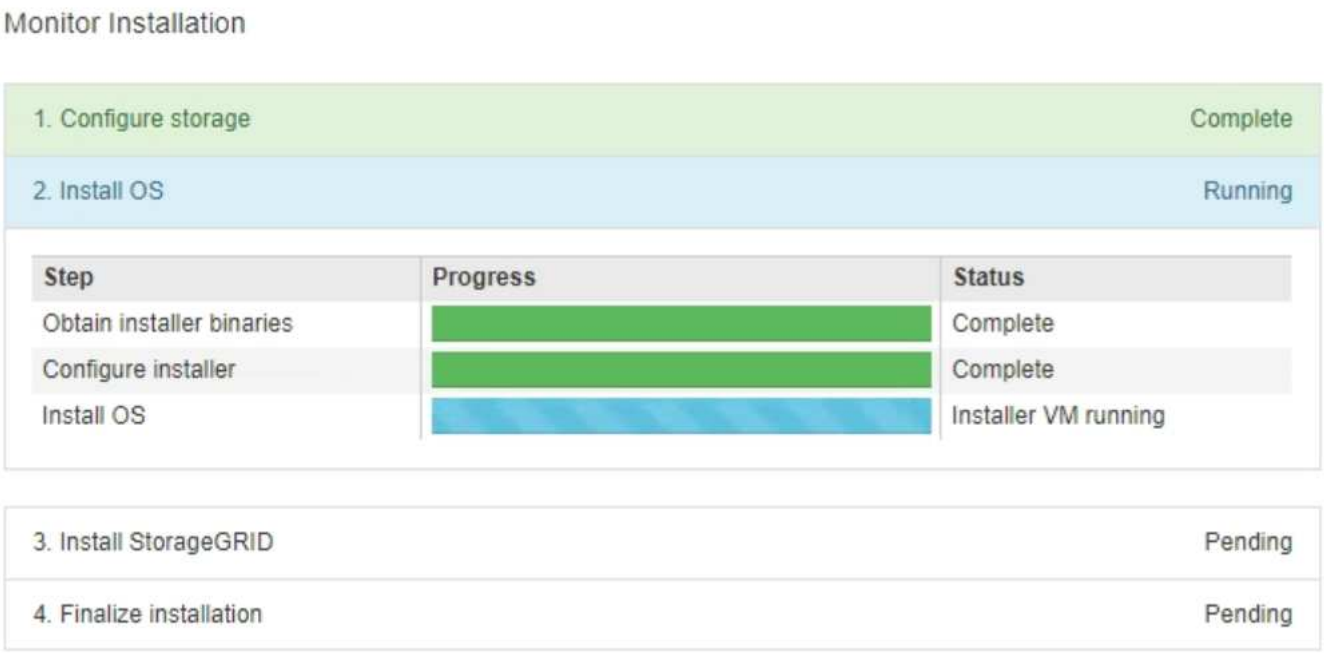
SG100 和 SG1000 服务设备

监控服务设备安装

在安装完成之前， StorageGRID 设备安装程序会提供状态。软件安装完成后，设备将重新启动。

1. 要监控安装进度，请单击菜单栏中的 * 监控安装 * 。

   "Monitor Installation" 页面将显示安装进度。



蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

> 安装程序可确保在先前安装中完成的任务不会重新运行。如果您要重新运行安装，则不需要重新运行的任何任务都会显示绿色状态条和状态 `Skipped` 。

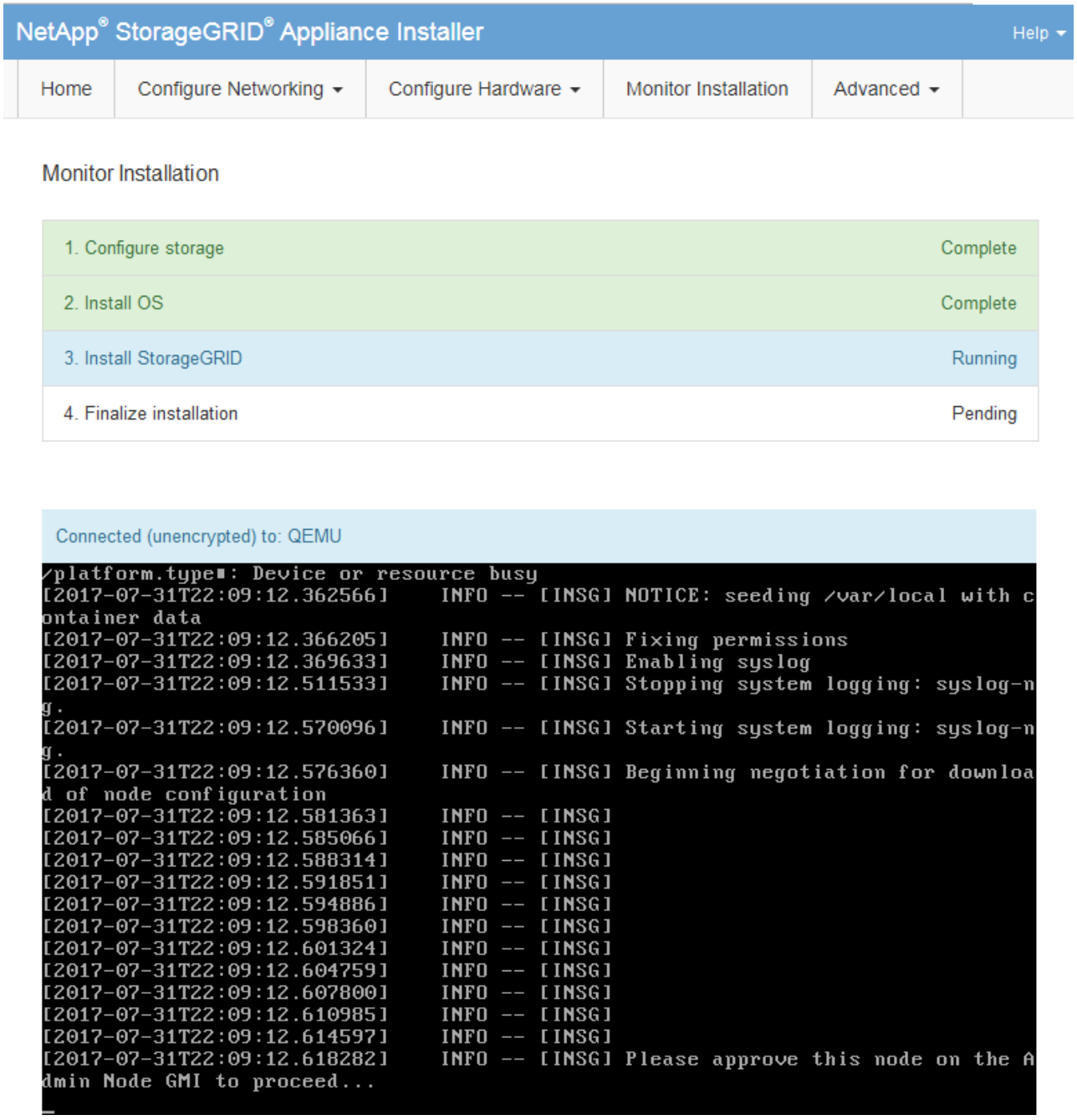
2. 查看前两个安装阶段的进度。
   - * 。配置存储 *

     在此阶段，安装程序将从驱动器中清除任何现有配置，并配置主机设置。

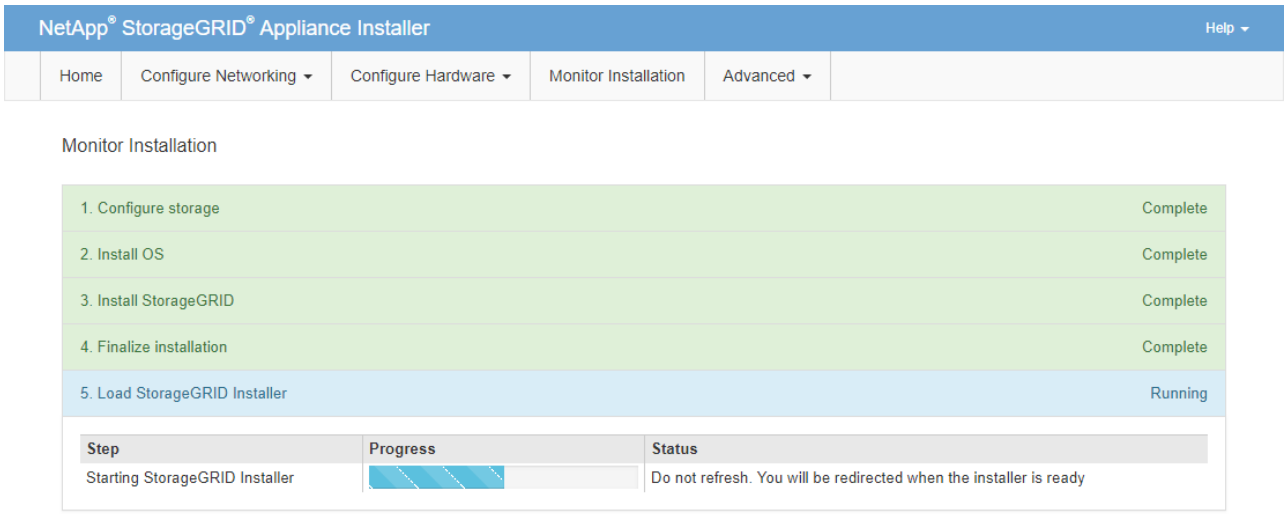
   - * 。安装 OS*

     在此阶段，安装程序会将 StorageGRID 的基本操作系统映像从主管理节点复制到设备，或者从主管理节点的安装包安装基本操作系统。

3. 继续监控安装进度，直到出现以下情况之一：
   - 对于设备网关节点或非主设备管理节点， * 安装 StorageGRID * 阶段将暂停，嵌入式控制台上会显示一条消息，提示您使用网格管理器在管理节点上批准此节点。



- 对于设备主管理节点，将显示第五阶段（ Load StorageGRID 安装程序）。如果第五阶段的进度超过 10 分钟，请手动刷新页面。



4. 对于要恢复的设备网格节点类型，请继续执行恢复过程的下一步。

恢复类型	参考
网关节点	选择 Start Recovery 以配置网关节点
非主管理节点	选择 Start Recovery 以配置非主管理节点
主管理节点	配置替代主管理节点

技术支持如何执行站点恢复

如果整个 StorageGRID 站点出现故障或多个存储节点出现故障，您必须联系技术支持。技术支持将评估您的情况，制定恢复计划，然后按照符合您业务目标的方式恢复故障节点或站点，优化恢复时间并防止不必要的数据丢失。

站点恢复只能由技术支持执行。

StorageGRID 系统可以对各种故障进行故障恢复，您可以自行成功执行许多恢复和维护过程。但是，创建一个简单的通用站点恢复操作步骤 很困难，因为详细步骤取决于您的具体情况。例如：

- * 您的业务目标 * ： 在完全丢失 StorageGRID 站点后，您应评估如何以最佳方式实现您的业务目标。例如，是否要原位重建丢失的站点？是否要在新位置更换丢失的 StorageGRID 站点？每个客户的情况都不同，您的恢复计划必须针对您的优先事项进行设计。
- * 故障的确切性质 * ： 在开始站点恢复之前，请务必确定故障站点上的任何节点是否完好无损，或者任何存储节点是否包含可恢复的对象。如果重建包含有效数据的节点或存储卷，可能会发生不必要的数据丢失。
- * 活动 ILM 策略 * ： 网格中对象副本的数量，类型和位置由活动 ILM 策略控制。ILM 策略的具体内容可能会影响可恢复的数据量以及恢复所需的特定技术。

  如果某个站点包含某个对象的唯一副本，而该站点丢失，则该对象将丢失。

- * 分段（或容器）一致性 * ： 应用于分段（或容器）的一致性级别会影响 StorageGRID 在通知客户端对象载

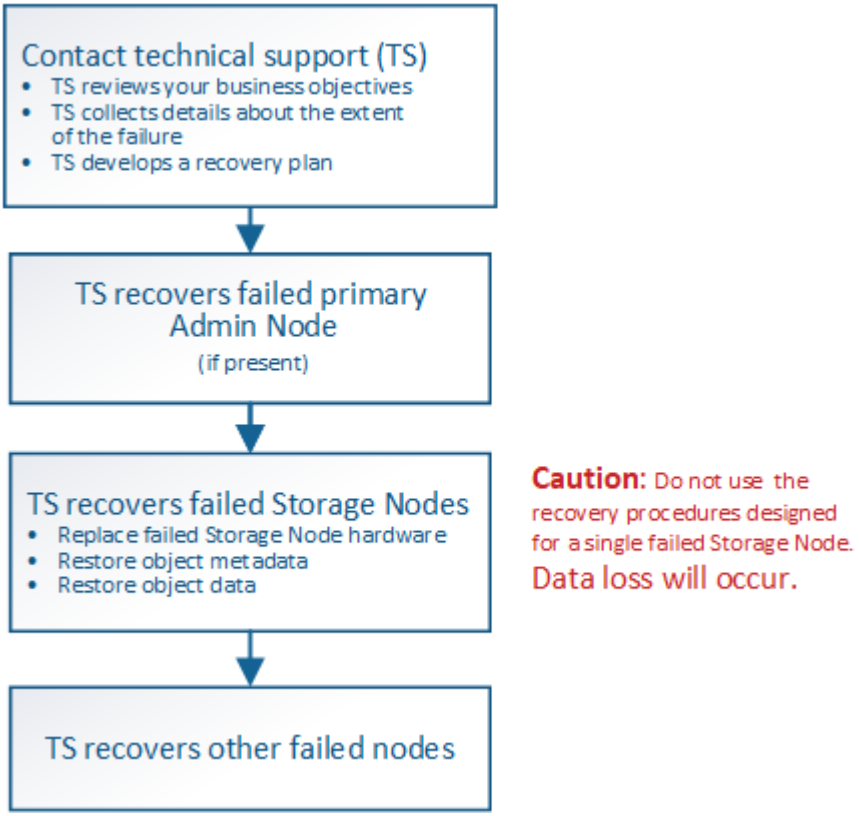
入成功之前是否将对象元数据完全复制到所有节点和站点。如果您的一致性级别允许最终保持一致性，则站点故障可能会丢失某些对象元数据。这可能会影响可恢复的数据量以及恢复操作步骤 的详细信息。

- * 近期更改历史记录 * ： 恢复操作步骤 的详细信息可能会受到故障发生时是否正在执行任何维护过程或是否最近对 ILM 策略进行了任何更改的影响。在开始站点恢复之前，技术支持必须评估网格的最新历史记录及其当前状况。

站点恢复概述

本文档概括介绍了技术支持用于恢复故障站点的过程。

站点恢复只能由技术支持执行。



1. 请联系技术支持。

   技术支持会对故障进行详细评估，并与您一起审核您的业务目标。根据这些信息，技术支持会根据您的具体情况制定一个恢复计划。

2. 如果主管理节点出现故障，技术支持将恢复该节点。
3. 技术支持将按照以下概述恢复所有存储节点：

   a. 根据需要更换 Storage Node 硬件或虚拟机。
   b. 将对象元数据还原到故障站点。
   c. 将对象数据还原到已恢复的存储节点。

   如果对单个故障存储节点执行恢复过程，则会发生数据丢失。

当整个站点出现故障时，需要使用专用命令来成功还原对象和对象元数据。

4. 技术支持可恢复其他故障节点。

恢复对象元数据和数据后，可以使用标准过程恢复出现故障的网关节点，非主管理节点或归档节点。

相关信息

站点停用

停用操作步骤

您可以执行停用操作步骤 ，以便从 StorageGRID 系统中永久删除网格节点或整个站点。

要删除网格节点或站点，请执行以下停用过程之一：

- 执行 * 节点停用 * 以删除一个或多个节点，这些节点可以位于一个或多个站点上。您删除的节点可以联机并连接到 StorageGRID 系统，也可以脱机并断开连接。
- 执行 * 已连接站点停用 * 以删除所有节点均已连接到 StorageGRID 的站点。
- 执行 * 已断开连接的站点停用 * 以删除所有节点均已从 StorageGRID 断开的站点。

在执行已断开连接的站点停用之前，您必须联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。如果您认为可以恢复站点或从站点恢复对象数据，则不应尝试执行已断开连接的站点停用。

如果站点包含混合的 Connected （ ）和已断开连接的节点（ 或 ），您必须使所有脱机节点重新联机。

如果需要执行第二个维护操作步骤 ，可以 在删除存储节点时暂停停用操作步骤。只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。第二个维护操作步骤 完成后，您可以恢复停用。

相关信息

网格节点停用

站点停用

网格节点停用

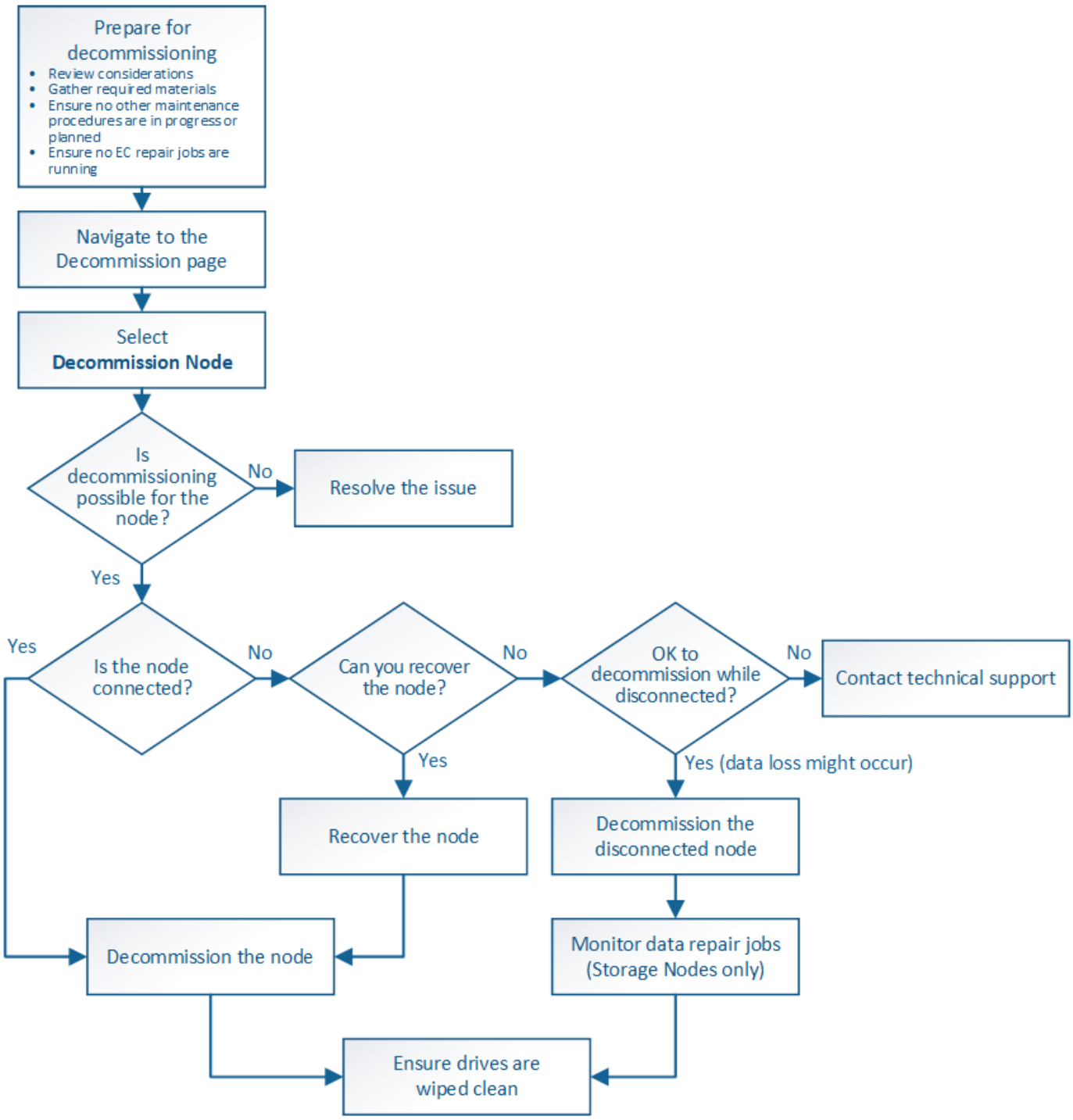
您可以使用节点停用操作步骤 删除一个或多个站点上的一个或多个存储节点，网关节点或非主管理节点。您不能停用主管理节点或归档节点。

通常，只有当网格节点已连接到 StorageGRID 系统且所有节点均处于正常运行状况时（在 * 节点 * 页面和 * 停用节点 * 页面上有绿色图标），才应停用这些节点。但是，如果需要，您可以停用已断开连接的网格节点。在删除已断开连接的节点之前，请确保您了解此过程的含义和限制。

如果满足以下任一条件，请使用节点停用操作步骤 ：

- 您已向系统中添加较大的存储节点，并希望删除一个或多个较小的存储节点，同时保留对象。
- 您所需的总存储较少。
- 您不再需要网关节点。
- 您不再需要非主管理节点。
- 您的网格包含一个断开连接的节点，您无法恢复此节点或使其恢复联机。

此流程图显示了停用网格节点的高级步骤。



您必须查看删除网格节点的注意事项，并确认擦除编码的数据没有处于活动状态的修复作业。

网格节点停用注意事项

在启动此操作步骤 以停用一个或多个节点之前，您必须了解删除每种类型的节点的含义。成功停用节点后，其服务将被禁用，并且节点将自动关闭。

如果停用某个节点会使 StorageGRID 处于无效状态，则无法停用此节点。将强制实施以下规则：

- 您不能停用主管理节点。
- 您不能停用归档节点。
- 如果管理节点或网关节点的某个网络接口属于高可用性（ HA ）组，则无法停用此节点。
- 如果删除存储节点会影响到模数转换器仲裁，则无法停用该存储节点。
- 如果活动 ILM 策略需要存储节点，则无法停用它。
- 在一个 " 停用节点 " 操作步骤 中停用的存储节点不应超过 10 个。
- 如果网格包含任何已断开连接的节点（运行状况为未知或管理员关闭的节点），则无法停用已连接节点。您必须先停用或恢复已断开连接的节点。
- 如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。
- 如果无法删除已断开连接的节点（例如，为实现模数转换器仲裁所需的存储节点），则不能删除任何其他已断开连接的节点。
- 如果要将旧设备更换为新设备，请考虑 正在克隆设备节点 而不是停用旧节点并在扩展中添加新节点。

> 在停用过程中指示删除网格节点的虚拟机或其他资源之前，请勿删除。

管理节点或网关节点停用的注意事项

停用管理节点或网关节点之前，请查看以下注意事项。

- 停用操作步骤 要求对某些系统资源具有独占访问权限，因此您必须确认未运行任何其他维护过程。
- 您不能停用主管理节点。
- 如果管理节点或网关节点的某个网络接口属于高可用性（ HA ）组，则无法停用此节点。您必须先从 HA 组中删除网络接口。请参见有关管理 StorageGRID 的说明。
- 您可以根据需要在停用网关节点或管理节点时安全地更改 ILM 策略。
- 如果停用管理节点并为 StorageGRID 系统启用了单点登录（ SSO ），则必须记住从 Active Directory 联合身份验证服务（ AD FS ）中删除该节点的依赖方信任。

相关信息

管理 StorageGRID

存储节点停用注意事项

如果您计划停用存储节点，则必须了解 StorageGRID 如何管理该节点上的对象数据和元数据。

停用存储节点时，应遵循以下注意事项和限制：

- 系统必须始终包含足够的存储节点以满足操作要求，包括模块数转换仲裁和活动 ILM 策略。要满足此限制，您可能需要在扩展操作中添加新的存储节点，然后才能停用现有存储节点。
- 如果在停用存储节点时断开了该存储节点的连接，则系统必须使用已连接存储节点中的数据重建数据，这可能会导致数据丢失。
- 删除存储节点时，必须通过网络传输大量对象数据。尽管这些传输不应影响正常系统操作，但它们可能会影响 StorageGRID 系统占用的网络带宽总量。
- 与正常系统操作相关的任务相比，与存储节点停用相关的任务的优先级更低。这意味着停用不会干扰 StorageGRID 系统的正常运行，也不需要计划系统在一段时间内处于非活动状态。由于停用是在后台执行的，因此很难估计完成此过程需要多长时间。通常，在系统处于静默状态或一次仅删除一个存储节点时，停用速度会更快。
- 停用存储节点可能需要数天或数周时间。相应地规划此操作步骤 。尽管停用过程不会影响系统运行，但它会限制其他过程。通常，在删除网格节点之前，您应执行任何计划内的系统升级或扩展。
- 涉及存储节点的停用过程可以在某些阶段暂停，以便在需要时运行其他维护过程，并在完成后继续执行。
- 当停用任务正在运行时，您不能在任何网格节点上运行数据修复操作。
- 在停用存储节点期间，不应对 ILM 策略进行任何更改。
- 删除存储节点时，节点上的数据将迁移到其他网格节点；但是，此数据不会从已停用的网格节点中完全删除。要永久安全地删除数据，必须在停用操作步骤 完成后擦除已停用网格节点的驱动器。
- 停用存储节点时，可能会发出以下警报，您可能会收到相关电子邮件和 SNMP 通知：
  - * 无法与节点 * 警报通信。停用包含此 ADC-Service 的存储节点时会触发此警报。停用操作完成后，此警报将得到解决。
  - VSTU （对象验证状态）警报。此通知级别的警报表示存储节点在停用过程中将进入维护模式。
  - CASA （数据存储状态）警报。此主要级别的警报表示 Cassandra 数据库正在关闭，因为服务已停止。

相关信息

根据需要将对象数据还原到存储卷

了解模数转换器仲裁

如果在停用后管理域控制器（ ADA ）服务仍会过多，您可能无法停用数据中心站点上的某些存储节点。此服务位于某些存储节点上，用于维护网格拓扑信息并为网格提供配置服务。StorageGRID 系统要求每个站点始终提供一定的数字转换服务仲裁。

如果删除某个存储节点将无法再满足发生原因 的仲裁，则无法停用此存储节点。要在停用期间满足模块转换仲裁要求，每个数据中心站点至少有三个存储节点必须具有模块转换服务。如果数据中心站点具有三个以上使用了 ADC 服务的存储节点，则在停用后，这些节点中的大多数节点必须保持可用（（ 0.5 * ` *Storage Nodes with ADC*` ） + 1 ）。

例如，假设一个数据中心站点当前包含六个具有模块化转换服务的存储节点，而您希望停用三个存储节点。由于

需要使用 ADC 仲裁，您必须完成两个停用过程，如下所示：

- 在第一个停用操作步骤 中，您必须确保具有 ADA 服务的四个存储节点仍然可用（（（ 0.5 * 6 ） +1 ）。这意味着最初只能停用两个存储节点。
- 在第二个停用操作步骤 中，您可以删除第三个存储节点，因为现在，由于仲裁只需要三个可用的 ADC 服务（（ 0.5 * 4 ） + 1 ）。

如果您需要停用某个存储节点，但由于要求使用的是 ADA 仲裁而无法停用，则必须在扩展中添加一个新的存储节点，并指定该存储节点应具有一个 ADA 服务。然后，您可以停用现有存储节点。

相关信息

扩展网格

查看 **ILM** 策略和存储配置

如果您计划停用存储节点，则应在开始停用过程之前查看 StorageGRID 系统的 ILM 策略。

在停用期间，所有对象数据都会从停用的存储节点迁移到其他存储节点。

停用期间使用的 ILM 策略将是停用后使用的策略。在开始停用之前和停用完成后，您必须确保此策略满足您的数据要求。

您应查看活动 ILM 策略中的规则，以确保 StorageGRID 系统将继续具有正确类型和位置的足够容量，以支持存储节点的停用。

请考虑以下几点：

- ILM 评估服务是否可以复制对象数据以满足 ILM 规则？
- 如果在停用过程中某个站点暂时不可用，会发生什么情况？是否可以在备用位置创建其他副本？
- 停用过程将如何影响内容的最终分发？如中所述 整合存储节点，您应先添加新的存储节点，然后再停用旧的存储节点。如果在停用较小的存储节点后添加较大的替代存储节点，则旧存储节点可能接近容量，新存储节点可能几乎没有任何内容。然后，新对象数据的大多数写入操作将定向到新存储节点，从而降低系统操作的整体效率。
- 系统是否会始终包含足够的存储节点来满足活动 ILM 策略？

无法满足的 ILM 策略将导致回退日志和警报，并可能会暂停 StorageGRID 系统的运行。

通过评估表中列出的因素，验证停用过程所产生的建议拓扑是否符合 ILM 策略。

要评估的区域	注释：
Available capacity	是否有足够的存储容量来容纳存储在 StorageGRID 系统中的所有对象数据？ 包括当前存储在要停用的存储节点上的对象数据的永久副本？在停用完成后，是否有足够的容量在合理的时间间隔内处理预期的存储对象数据增长？

要评估的区域	注释：
存储位置	如果整个 StorageGRID 系统中仍有足够的容量，则容量是否位于合适的位置以满足 StorageGRID 系统的业务规则？
Storage type	停用完成后，是否有足够的相应类型存储？例如， ILM 规则可能会规定在内容老化时将内容从一种存储类型移动到另一种存储类型。如果是，您必须确保在 StorageGRID 系统的最终配置中具有足够的相应类型的存储。

相关信息

使用 ILM 管理对象

扩展网格

停用已断开连接的存储节点

您必须了解在存储节点断开连接（运行状况为未知或管理员关闭）时停用存储节点可能会发生什么情况。

停用与网格断开的存储节点时， StorageGRID 会使用其他存储节点中的数据重建已断开连接的节点上的对象数据和元数据。为此，它会在停用过程结束时自动启动数据修复作业。

停用已断开连接的存储节点之前，请注意以下事项：

- 除非您确定已断开连接的节点无法联机或恢复，否则切勿停用此节点。

> 如果您认为可以从节点恢复对象数据，请勿执行此操作步骤 。请联系技术支持以确定是否可以进行节点恢复。

- 如果断开连接的存储节点包含某个对象的唯一副本，则在停用此节点时，此对象将丢失。只有当当前连接的存储节点上至少存在一个复制副本或足够多的纠删编码片段时，数据修复作业才能重建和恢复对象。
- 停用已断开连接的存储节点时，停用操作步骤 的完成速度相对较快。但是，数据修复作业可能需要数天或数周才能运行，并且不受停用操作步骤 的监控。您必须手动监控这些作业并根据需要重新启动它们。请参见检查数据修复作业。
- 如果一次停用多个已断开连接的存储节点，则可能会发生数据丢失。如果对象数据，元数据或纠删编码片段的副本太少，则系统可能无法重建数据。

> 如果有多个已断开连接的存储节点无法恢复，请联系技术支持以确定最佳操作方案。

整合存储节点

您可以整合存储节点以减少站点或部署的存储节点数，同时增加存储容量。

整合存储节点时，您可以扩展 StorageGRID 系统以添加容量更大的新存储节点，然后停用容量较小的旧存储节点。在停用操作步骤 期间，对象会从旧存储节点迁移到新存储节点。

如果您要将较旧的和较小的设备与新型号或容量较大的设备进行整合，则许多用户都使用节点克隆功能，或者如果不执行一对一更换，则使用节点克隆操作步骤 和停用操作步骤 。

例如，您可以添加两个容量更大的新存储节点来替换三个旧存储节点。您应首先使用扩展操作步骤 添加两个更大的新存储节点，然后使用停用操作步骤 删除三个容量较小的旧存储节点。

通过在删除现有存储节点之前添加新容量，您可以确保在 StorageGRID 系统中更平衡地分布数据。此外，还可以减少现有存储节点可能被推送到存储水印级别以外的可能性。

相关信息

扩展网格

停用多个存储节点

如果需要删除多个存储节点，可以按顺序或并行停用它们。

- 如果您按顺序停用存储节点，则必须等待第一个存储节点完成停用，然后再开始停用下一个存储节点。
- 如果您并行停用存储节点，则存储节点会同时处理要停用的所有存储节点的停用任务。这可能会导致文件的所有永久副本被标记为 `read-only` ， 在启用了此功能的网格中暂时禁用删除。

检查数据修复作业

停用网格节点之前，您必须确认没有处于活动状态的数据修复作业。如果任何修复失败，您必须重新启动修复并让其完成，然后再执行停用操作步骤 。

如果您需要停用已断开连接的存储节点，则还需要在停用操作步骤 完成后完成这些步骤，以确保数据修复作业已成功完成。您必须确保已成功还原已删除节点上的任何经过擦除编码的片段。

这些步骤仅适用于具有纠删编码对象的系统。

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。
2. 检查正在运行的修复： `repair-data show-EC-repair-status`
   - 如果您从未运行过数据修复作业，则输出为 `No job found` 。您无需重新启动任何修复作业。
   - 如果数据修复作业先前已运行或当前正在运行，则输出将列出要修复的信息。每个修复都有一个唯一的修复 ID 。继续执行下一步。

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
================================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. S所有修复的状态为 " 无 "，则无需重新启动任何修复作业。
4. 如果要进行任何修复的状态为 `failure` ，则必须重新启动此修复。
   a. 从输出中获取失败修复的修复 ID 。
   b. 运行 `repair-data start-EC-node-repair` 命令。

      使用 ` -repair-id` 选项指定修复 ID 。例如，如果要重试修复 ID 为 949292 的修复，请运行以下命令：
      `repair-data start-EC-node-repair -repair-id 949292`

   c. S跟踪 `EC` 数据修复的状态，直到所有修复的状态为 " 无 " 。

收集所需材料

在执行网格节点停用之前，您必须获取以下信息。

项目	注释：
恢复软件包 ` .zip` 文件	您必须 下载最新的恢复软件包 ` .zip` file （ `sGWS-recovery-package-id-revision.zip` ）。如果发生故障，您可以使用恢复包文件还原系统。
`passwords.txt` file	此文件包含在命令行上访问网格节点所需的密码，并包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
停用前 StorageGRID 系统拓扑的问题描述	如果有，请获取描述系统当前拓扑的任何文档。

相关信息

访问 " 取消配置节点 " 页面

访问网格管理器中的 " 停用节点 " 页面时，您可以一目了然地看到哪些节点可以停用。

您需要的内容

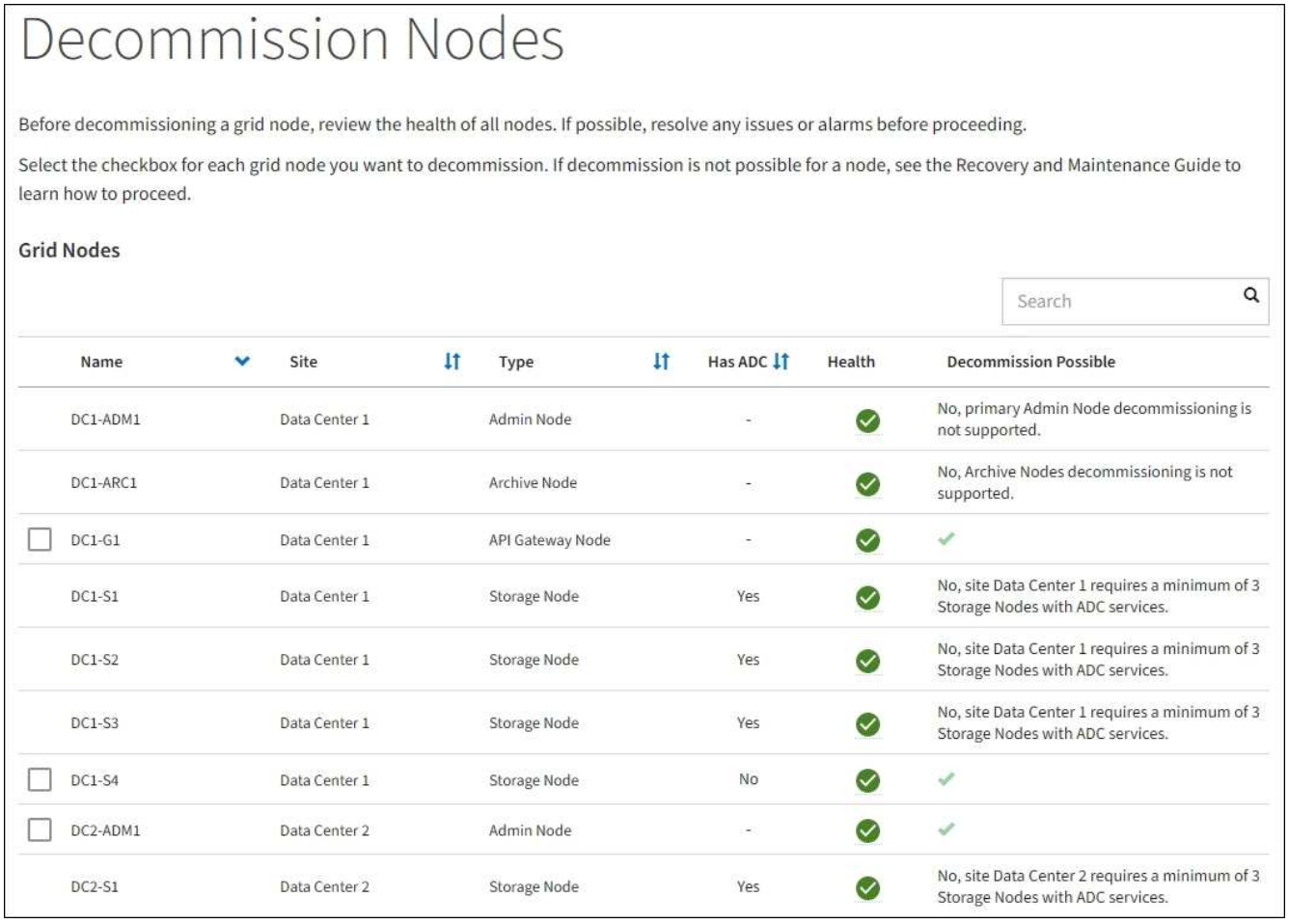
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。

步骤

1. 选择 * 维护 * > * 任务 * > * 取消配置 * 。
2. 选择 * 取消配置节点 * 。

   此时将显示 Decommission Nodes 页面。在此页面中，您可以：

   - 确定当前可以停用的网格节点。
   - 查看所有网格节点的运行状况
   - 按 * 名称 * ， * 站点 * ， * 类型 * 或 * 具有 ADC* 按升序或降序对列表进行排序。
   - 输入搜索词可快速查找特定节点。例如，此页面显示两个数据中心中的网格节点。Decommission possible 列指示您可以停用网关节点，五个存储节点之一和非主管理节点。



3. 查看要停用的每个节点的 * 可能停用 * 列。

   如果可以停用网格节点，则此列会显示一个绿色复选标记，最左侧的列会显示一个复选框。如果无法停用某个节点，此列将介绍问题描述 。如果无法停用某个节点的原因不止一个，则会显示最关键的原因。

停用可能的原因	Description	解决步骤
不支持，不支持节点类型停用。	您不能停用主管理节点或归档节点。	无
否，至少有一个网格节点已断开连接。 • 注： * 此消息仅针对已连接的网格节点显示。	如果任何网格节点已断开连接，则无法停用已连接的网格节点。 对于已断开连接的网格节点， * 运行状况 * 列包含以下图标之一： • （灰色）：已管理员关闭 • （蓝色）：未知	转至 列出停用操作步骤 选项的步骤。
否，一个或多个所需节点当前已断开连接，必须进行恢复。 • 注： * 此消息仅针对已断开连接的网格节点显示。	如果一个或多个所需节点也已断开连接，则您无法停用已断开连接的网格节点（例如，为实现 ADC 仲裁所需的存储节点）。	a. 查看所有已断开连接的节点的 " 取消配置 " 可能消息。 b. 确定哪些节点因需要而无法停用。 ◦ 如果所需节点的运行状况已被管理员关闭，请使此节点重新联机。 ◦ 如果所需节点的运行状况未知，请执行节点恢复操作步骤 以恢复所需节点。
否， HA 组的成员： *x* 。要停用此节点，必须先将其从所有 HA 组中删除。	如果某个节点接口属于高可用性（ HA ）组，则无法停用管理节点或网关节点。	编辑 HA 组以删除节点的接口或删除整个 HA 组。请参见有关管理 StorageGRID 的说明。
不可以，站点 *x* 至少需要具有模块化转换服务的 *n* 存储节点。	• 仅限存储节点。 * 如果站点上保留的节点不足以满足模块化转换仲裁要求，则无法停用存储节点。	执行扩展。向站点添加新的存储节点，并指定其应具有一个模块转换服务。请参见有关模数转换器仲裁的信息。

停用可能的原因	Description	解决步骤
不需要，一个或多个擦除编码配置文件至少需要 *n* 存储节点。如果在 ILM 规则中未使用此配置文件，您可以将其停用。	• 仅限存储节点。 * 除非为现有擦除编码配置文件保留足够的节点，否则无法停用存储节点。 例如，如果 4+2 纠删编码存在擦除编码配置文件，则必须至少保留 6 个存储节点。	对于每个受影响的擦除编码配置文件，根据配置文件的使用方式执行以下步骤之一： • * 用于活动 ILM 策略 * ：执行扩展。添加足够多的新存储节点，以便继续进行纠删编码。请参见有关扩展 StorageGRID 的说明。 • * 用于 ILM 规则，但不用于活动 ILM 策略 * ：编辑或删除规则，然后停用擦除编码配置文件。 • * 未在任何 ILM 规则中使用 * ：停用擦除编码配置文件。 ◦ 注： * 如果您尝试停用擦除编码配置文件，但对象数据仍与该配置文件关联，则会显示一条错误消息。您可能需要等待几周才能再次尝试停用过程。 有关通过信息生命周期管理管理对象的说明，请了解如何停用擦除编码配置文件。

4. 【解压缩程序选择】如果节点可以停用，请确定需要执行的操作步骤：

网格是否包括 ...	转至 ...
任何已断开连接的网格节点	停用已断开连接的网格节点
仅连接网格节点	停用已连接的网格节点

相关信息

检查数据修复作业

了解模数转换器仲裁

使用 ILM 管理对象

扩展网格

管理 StorageGRID

停用已断开连接的网格节点

您可能需要停用当前未连接到网格的节点（运行状况为未知或管理员关闭的节点）。

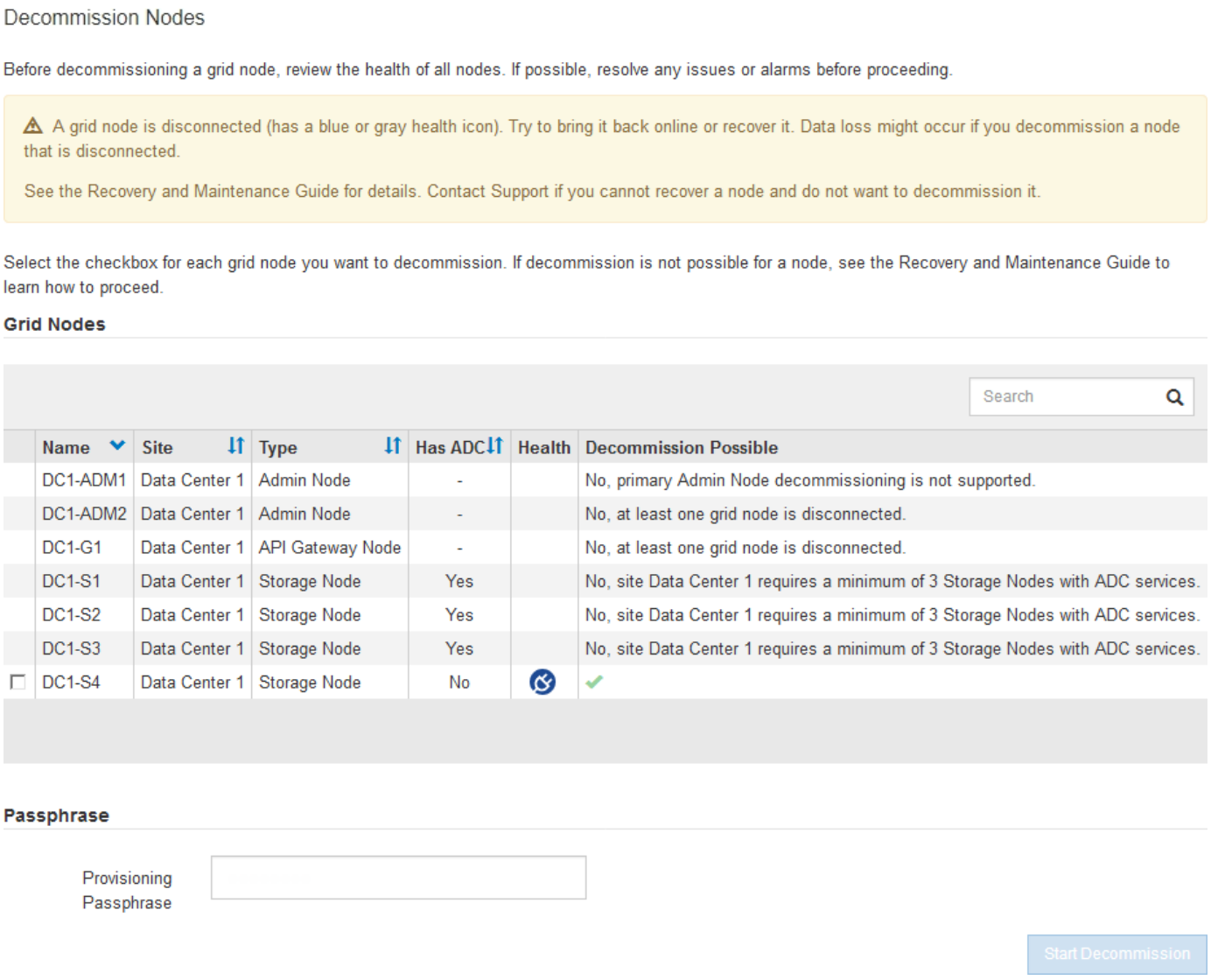
您需要的内容

- 您了解要求和 停用网格节点的注意事项。
- 您已获取所有前提条件项。
- 您已确保没有处于活动状态的数据修复作业。请参见 检查数据修复作业。

- 您已确认网格中的任何位置均未进行存储节点恢复。如果是，则必须等待在恢复过程中执行的任何 Cassandra 重建完成。然后，您可以继续停用。
- 您已确保在节点停用操作步骤 运行期间不会运行其他维护过程，除非节点停用操作步骤 已暂停。
- 要停用的已断开连接节点的 * 可停用 * 列包含一个绿色复选标记。
- 您必须具有配置密码短语。

关于此任务

您可以通过在 * 运行状况 * 列中查找未知（蓝色）或管理员关闭（灰色）图标来识别已断开连接的节点。在此示例中，名为 DC1-S4 的存储节点已断开连接；所有其他节点均已连接。



停用任何已断开连接的节点之前，请注意以下事项：

- 此操作步骤 主要用于删除一个断开连接的节点。如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。

> 一次停用多个断开连接的网格节点时，请务必小心，尤其是在选择多个断开连接的存储节点时。

- 如果无法删除已断开连接的节点（例如，为实现模数转换器仲裁所需的存储节点），则不能删除任何其他已断开连接的节点。

停用已断开连接的 * 存储节点 * 之前，请注意以下事项

- 您不应停用已断开连接的存储节点，除非您确定它无法联机或恢复。

  如果您认为仍可从节点恢复对象数据，请勿执行此操作步骤 。请联系技术支持以确定是否可以进行节点恢复。

- 如果停用多个已断开连接的存储节点，则可能会发生数据丢失。如果没有足够的对象副本，纠删编码片段或对象元数据保持可用，则系统可能无法重建数据。

  如果有多个已断开连接的存储节点无法恢复，请联系技术支持以确定最佳操作方案。

- 停用已断开连接的存储节点时， StorageGRID 会在停用过程结束时启动数据修复作业。这些作业会尝试重建已断开连接的节点上存储的对象数据和元数据。
- 停用已断开连接的存储节点时，停用操作步骤 的完成速度相对较快。但是，数据修复作业可能需要数天或数周才能运行，并且不受停用操作步骤 的监控。您必须手动监控这些作业并根据需要重新启动它们。请参见检查数据修复作业。
- 如果停用的存储节点已断开连接，而该存储节点包含某个对象的唯一副本，则该对象将丢失。只有当当前连接的存储节点上至少存在一个复制副本或足够多的纠删编码片段时，数据修复作业才能重建和恢复对象。

停用已断开连接的 * 管理节点 * 或 * 网关节点 * 之前，请注意以下事项：

- 停用已断开连接的管理节点时，该节点上的审核日志将丢失；但是，这些日志也应存在于主管理节点上。
- 您可以在网关节点断开连接时安全地停用它。

步骤

1. 尝试将任何已断开连接的网格节点恢复联机或进行恢复。

   有关说明，请参见恢复过程。

2. 如果无法恢复已断开连接的网格节点，并且您希望在该节点断开连接后将其停用，请选中该节点的复选框。

   如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。

   如果选择一次停用多个断开连接的网格节点，请务必格外小心，尤其是在选择多个断开连接的存储节点时。如果有多个已断开连接的存储节点无法恢复，请联系技术支持以确定最佳操作方案。

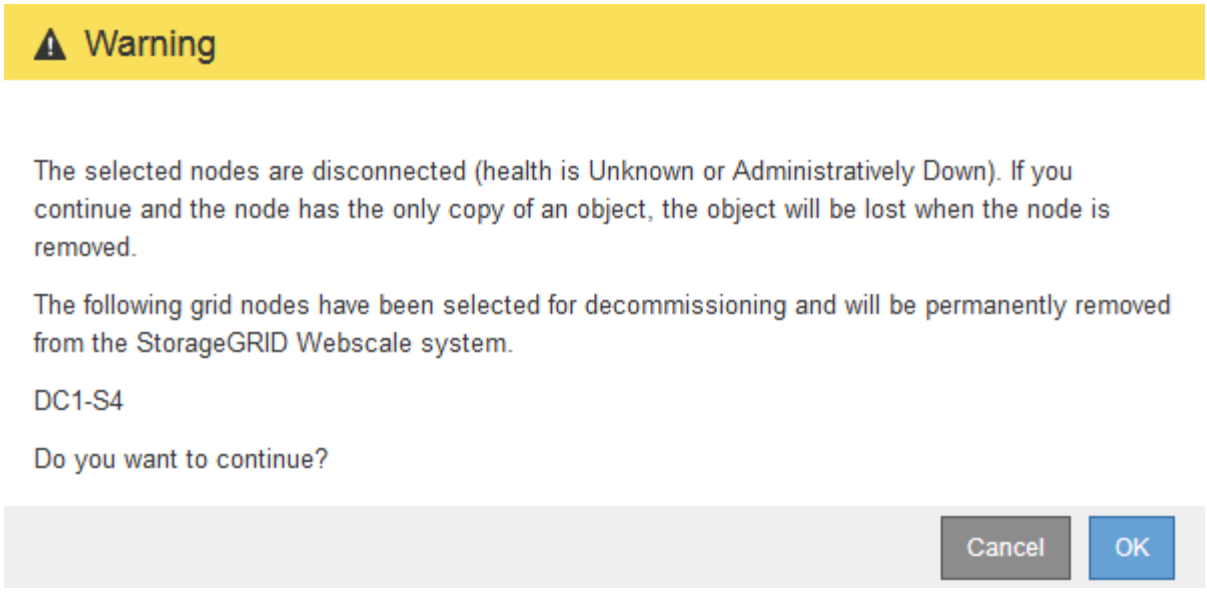
3. 输入配置密码短语。

   已启用 * 开始取消配置 * 按钮。

4. 单击 * 开始取消配置 * 。

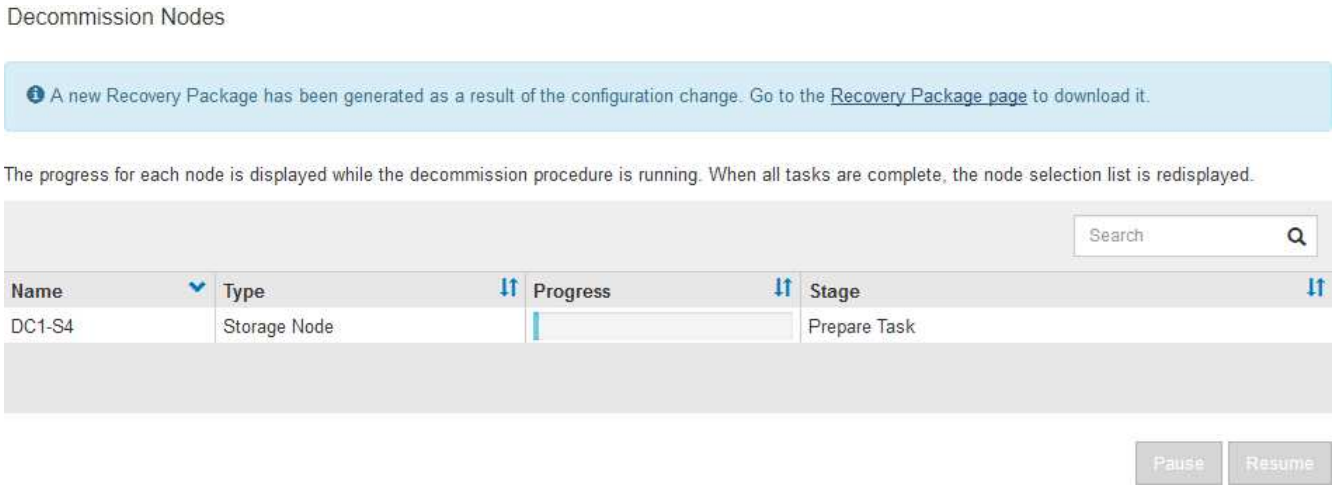
   此时将显示一条警告，指示您已选择断开连接的节点，如果此节点具有唯一的对象副本，则此对象数据将丢

失。



5. 查看节点列表，然后单击 * 确定 * 。

   停用操作步骤 将启动，并显示每个节点的进度。在操作步骤 期间，将生成一个新的恢复软件包，其中包含网格配置更改。



6. 新的恢复软件包一旦可用，请单击链接或选择 * 维护 * > * 系统 * > * 恢复软件包 * 以访问 " 恢复软件包 " 页面。然后，下载 ` .zip` 文件。

   请参见的说明 正在下载恢复包。

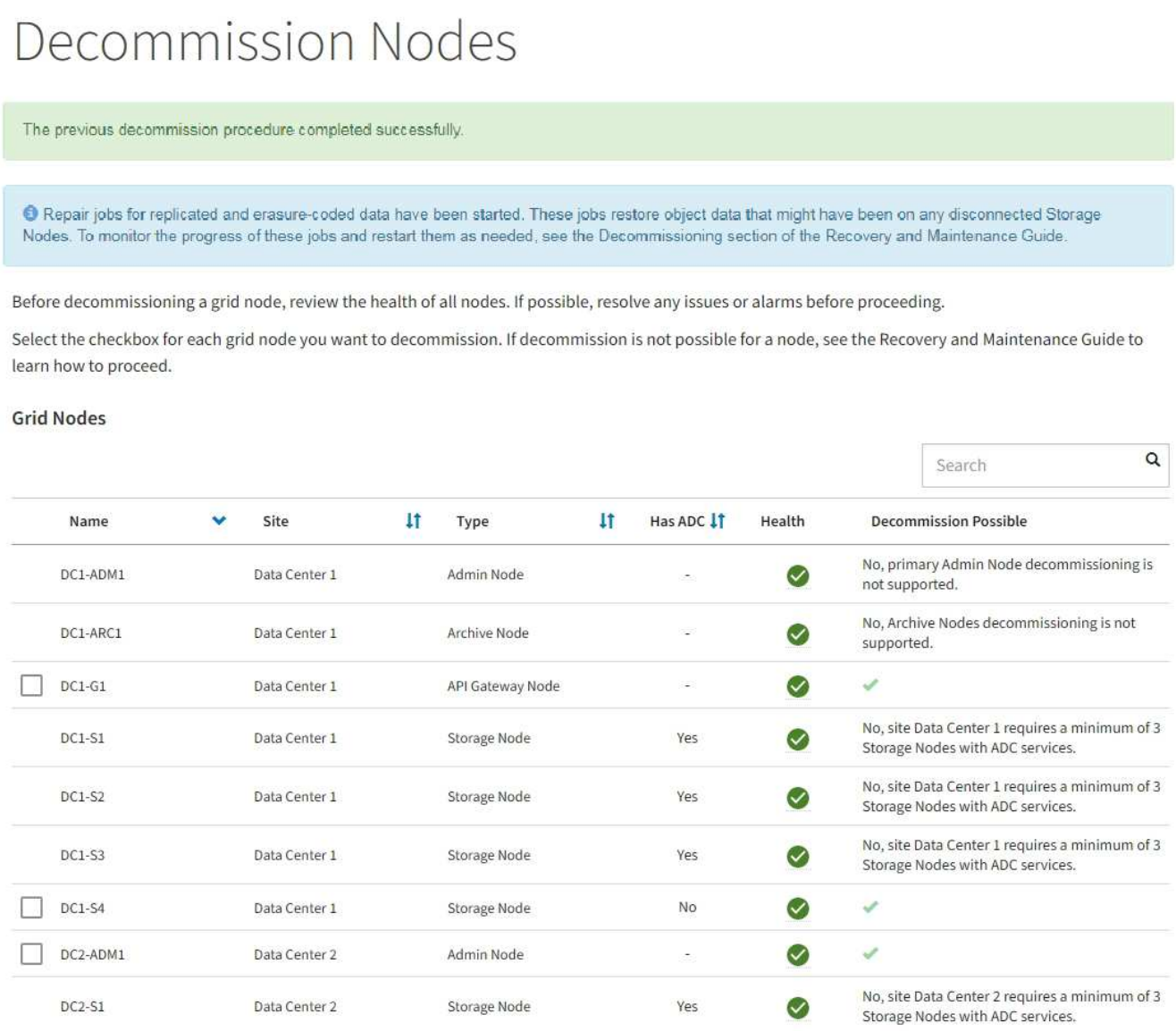
   请尽快下载恢复包，以确保在停用操作步骤 期间出现问题时可以恢复网格。

   恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

7. 定期监控 " 停用 " 页面，以确保所有选定节点均已成功停用。

   存储节点停用可能需要数天或数周时间。完成所有任务后，系统将重新显示节点选择列表，并显示成功消

息。如果停用了已断开连接的存储节点，则会显示一条信息消息，指出修复作业已启动。



8. 在停用操作步骤 期间自动关闭节点后，请删除与已停用节点关联的任何剩余虚拟机或其他资源。

   在节点自动关闭之前，请勿执行此步骤。

9. 如果要停用存储节点，请监控在停用过程中自动启动的 * 复制数据 * 和 * 纠删编码（ EC ）数据 * 修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  a. 选择 * 节点 * > * 正在修复的存储节点 _* > * ILM * 。
  b. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  a. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
  b. 选择 ***grid*** > * 正在修复的存储节点 _* > * LDR* > * 数据存储 * 。
  c. 结合使用以下属性，尽可能确定复制的修复是否已完成。

  可能存在 Cassandra 不一致，并且无法跟踪失败的修复。

  - * 尝试修复（ XRPA ） * ：使用此属性跟踪复制修复的进度。每当存储节点尝试修复高风险对象时，此属性都会增加。如果此属性的增加时间不超过当前扫描期间（由 * 扫描期间 - 估计 * 属性提供），则表示 ILM 扫描未在任何节点上发现任何需要修复的高风险对象。

    高风险对象是指可能完全丢失的对象。这不包括不满足其 ILM 配置的对象。

  - * 扫描期间 - 估计值（ XSCM ） * ：使用此属性可估计何时对先前载入的对象应用策略更改。如果 * 已尝试修复 * 属性的增加时间未超过当前扫描期间，则复制的修复很可能已完成。请注意，扫描期限可能会更改。* 扫描期限 - 估计（ XSCM ） * 属性适用场景 整个网格，是所有节点扫描期限的最大值。您可以查询网格的 * 扫描时间段 - 估计 * 属性历史记录以确定适当的时间范围。
- 或者，要获得复制修复的估计完成百分比，请在 repair-data 命令中添加 `sHow-replicate-repair-status` 选项。

```
repair-data show-repliced-repair-status
```

在 StorageGRID 11.6 中，可以使用 `show -replicate-repair-status` 选项进行技术预览。此功能正在开发中，返回的值可能不正确或延迟。要确定修复是否已完成，请使用 * 等待–全部 * ， * 尝试修复（ XRPA ） * 和 * 扫描期限 - 估计（ XSCM ） * ，如中所述 监控修复情况。

纠删编码（ **Erasure Coded** ， **EC** ）数据

要监控纠删编码数据的修复情况，并重试任何可能失败的请求：

1. 确定经过纠删编码的数据修复的状态：
   - 选择 * 支持 * > * 工具 * > * 指标 * 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分中选择 * EC Overview* 。查看 * 网格 EC 作业预计完成时间 * 和 * 网格 EC 作业已完成百分比 * 信息板。
   - 使用此命令可查看特定 `repair-data` 操作的状态：

     ```
     repair-data show-EC-repair-status -repair-id repair ID
     ```

   - 使用此命令可列出所有修复：

```
repair-data show-EC-repair-status
```

输出列出了所有先前和当前正在运行的修复的信息，包括 `repair ID`。

2. 如果输出显示修复操作失败，请使用 ` -repair-id` 选项重试修复。

   此命令使用修复 ID 6949309319275667690 重试失败的节点修复：

   ```
   repair-data start-EC-node-repair -repair-id 6949309319275667690
   ```

   此命令使用修复 ID 6949309319275667690 重试失败的卷修复：

   ```
   repair-data start-EC-volume-repair -repair-id 6949309319275667690
   ```

完成后

一旦断开连接的节点停用并完成所有数据修复作业，您就可以根据需要停用任何已连接的网格节点。

然后，在完成停用操作步骤 后完成以下步骤：

- 确保已停用网格节点的驱动器已擦除干净。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果您停用了某个设备节点，并且该设备上的数据已使用节点加密进行保护，请使用 StorageGRID 设备安装程序清除密钥管理服务器配置（清除 KMS ）。如果要将设备添加到另一个网格，则必须清除 KMS 配置。
  - SG100 和 SG1000 服务设备
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备

相关信息

网格节点恢复过程

停用已连接的网格节点

您可以停用并永久删除连接到网格的节点。

- 您必须了解要求和 停用网格节点的注意事项。
- 您必须已收集所有必需的材料。
- 您必须确保没有处于活动状态的数据修复作业。
- 您必须已确认网格中任何位置均未进行存储节点恢复。如果是，则必须等待在恢复过程中执行的任何 Cassandra 重建完成。然后，您可以继续停用。
- 您必须确保在节点停用操作步骤 运行期间不会运行其他维护过程，除非节点停用操作步骤 已暂停。
- 您必须具有配置密码短语。
- 已连接网格节点。
- 要停用的一个或多个节点的 * 可能停用 * 列必须包含一个绿色复选标记。

- 所有网格节点都必须运行状况正常（绿色） 。如果您在 * 运行状况 * 列中看到以下图标之一，则必须尝试解析问题描述：

图标。	颜色	severity
	黄色	通知
	浅橙色	次要
	深橙色	major
	红色	严重

- 如果您先前停用了已断开连接的存储节点，则数据修复作业均已成功完成。请参见 检查数据修复作业。

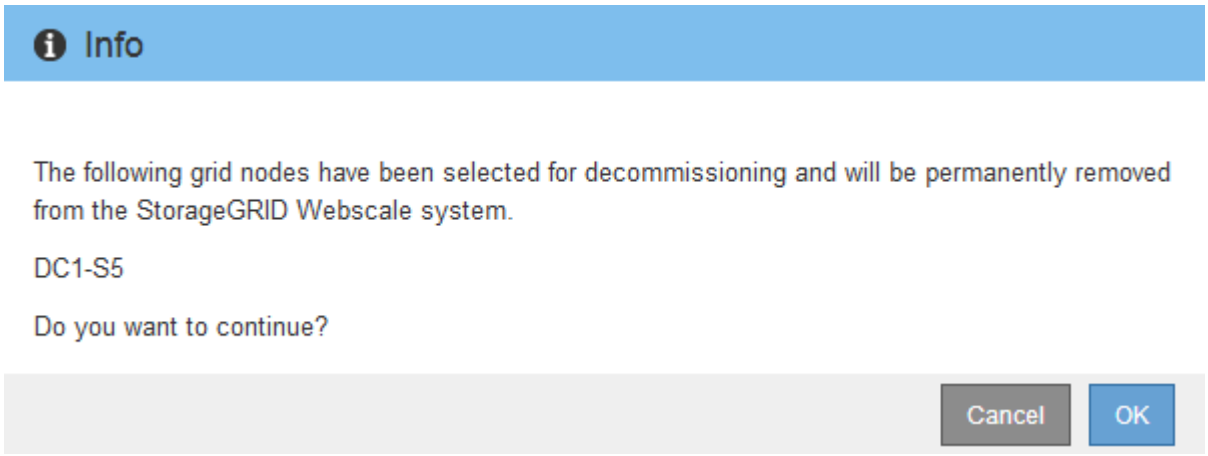
> 除非在此操作步骤 中指示删除网格节点的虚拟机或其他资源，否则请勿删除此虚拟机或其他资源。

1. 从 " 停用节点 " 页面中，选中要停用的每个网格节点对应的复选框。
2. 输入配置密码短语。

   已启用 * 开始取消配置 * 按钮。

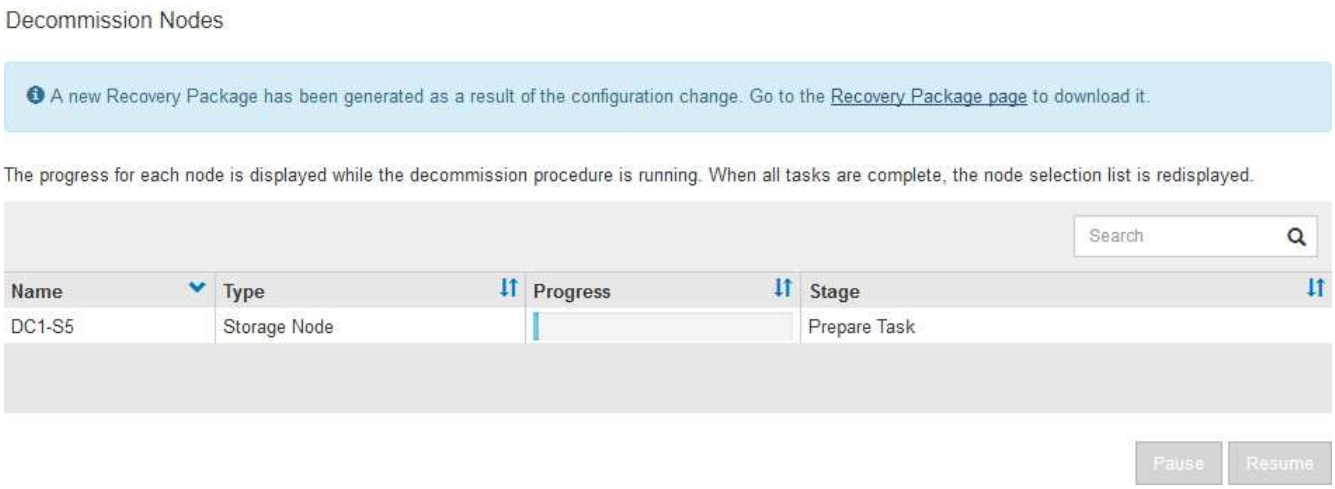
3. 单击 * 开始取消配置 * 。

   此时将显示确认对话框。



4. 查看选定节点的列表，然后单击 * 确定 * 。

   此时将启动节点停用操作步骤 ，并显示每个节点的进度。在操作步骤 期间，系统会生成一个新的恢复软件包以显示网格配置更改。



停用操作步骤 启动后，请勿使存储节点脱机。更改状态可能会导致某些内容未复制到其他位置。

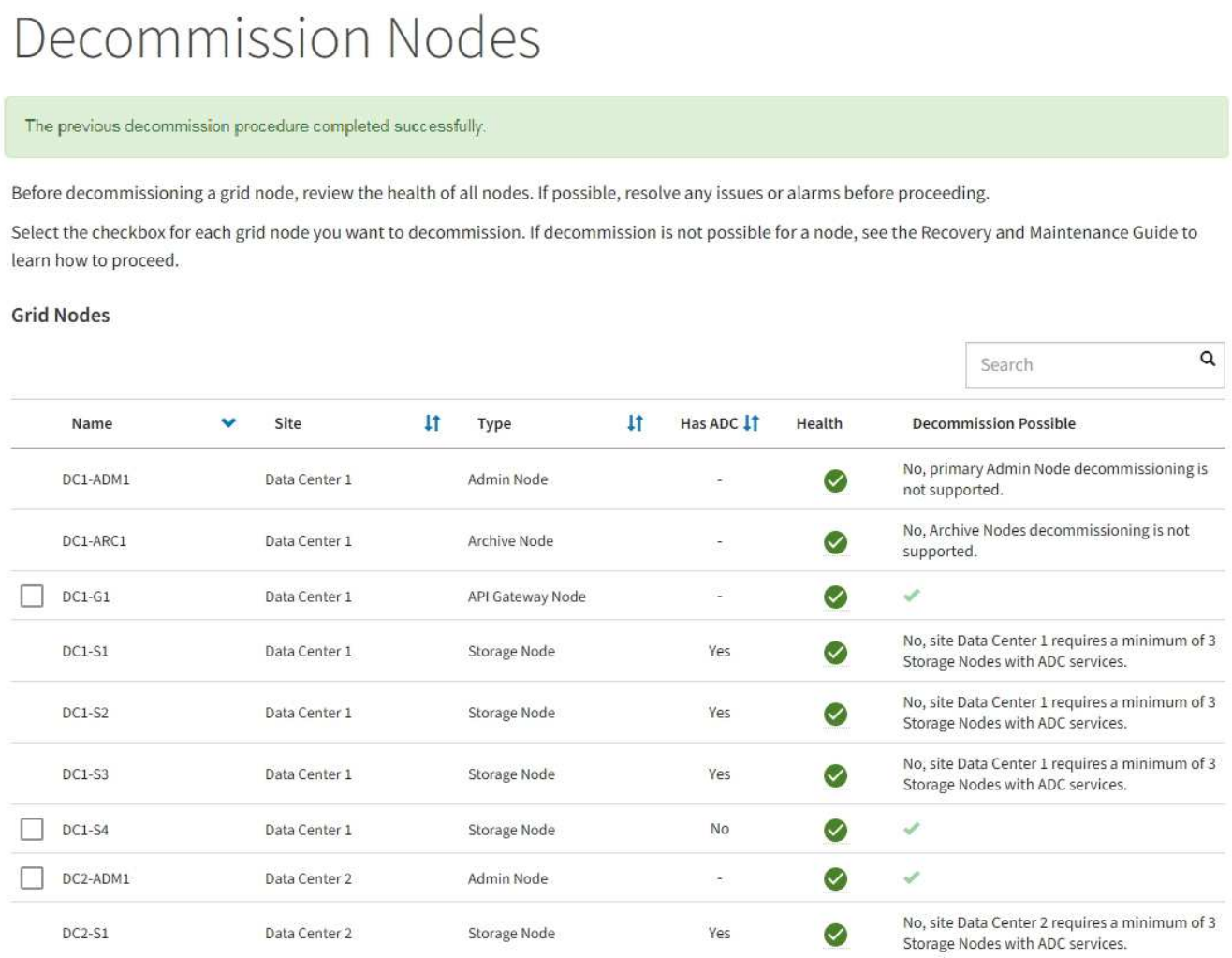
5. 新的恢复软件包一旦可用，请单击链接或选择 * 维护 * > * 系统 * > * 恢复软件包 * 以访问 " 恢复软件包 " 页面。然后，下载 ` .zip` 文件。

   请参见的说明 正在下载恢复包。

   请尽快下载恢复包，以确保在停用操作步骤 期间出现问题时可以恢复网格。

6. 定期监控 " 停用节点 " 页面，以确保所有选定节点均已成功停用。

   存储节点停用可能需要数天或数周时间。完成所有任务后，系统将重新显示节点选择列表，并显示成功消息。



7. 按照适用于您的平台的步骤进行操作。例如：
   - * Linux * ： 您可能需要断开卷的连接并删除在安装期间创建的节点配置文件。
   - * D * ： 您可能需要使用 vCenter 的 " 从磁盘删除 " 选项来删除虚拟机。您可能还需要删除独立于虚拟机的任何数据磁盘。
   - * StorageGRID 设备 * ： 设备节点会自动恢复为未部署状态，您可以在此状态下访问 StorageGRID 设备安装程序。您可以关闭设备电源或将其添加到另一个 StorageGRID 系统。

完成节点停用操作步骤 后，请完成以下步骤：

- 确保已停用网格节点的驱动器已擦除干净。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果您停用了某个设备节点，并且该设备上的数据已使用节点加密进行保护，请使用 StorageGRID 设备安装程序清除密钥管理服务器配置（清除 KMS ）。如果要在另一网格中使用此设备，则必须清除 KMS 配置。

SG100 和 SG1000 服务设备

SG5600 存储设备

SG5700 存储设备

SG6000 存储设备

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

暂停和恢复存储节点的停用过程

如果需要执行第二个维护操作步骤 ，可以在某些阶段暂停存储节点的停用操作步骤 。另一个操作步骤 完成后，您可以恢复停用。

只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。

步骤

1. 选择 * 维护 * > * 任务 * > * 取消配置 * 。

   此时将显示 Decommission 页面。

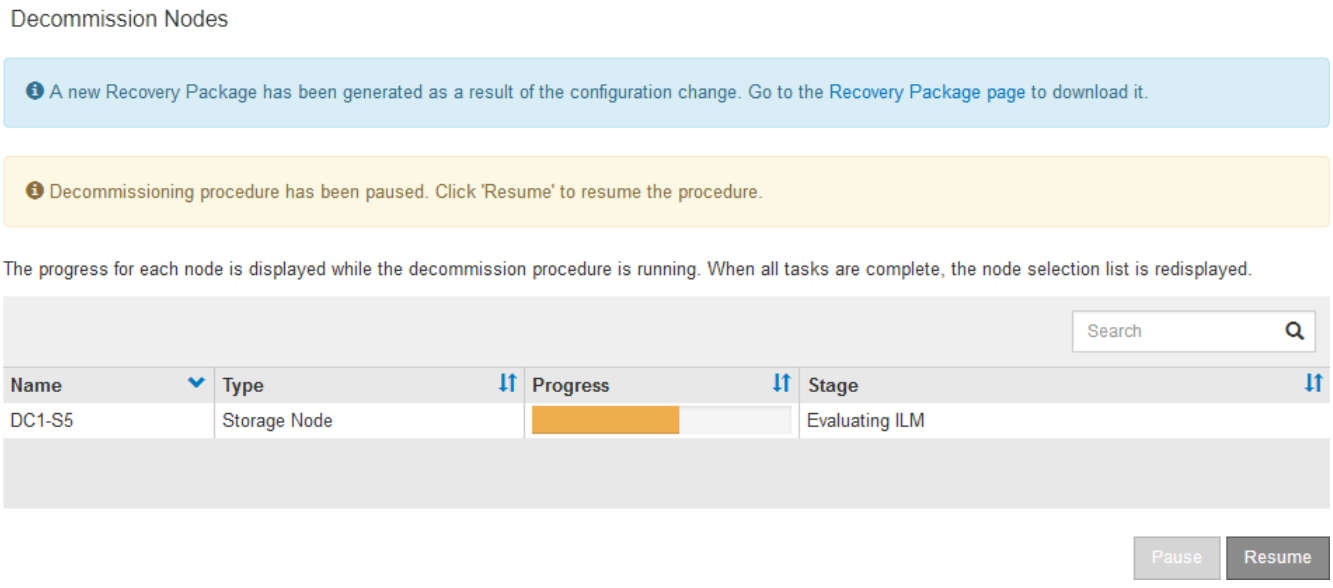
2. 选择 * 取消配置节点 * 。

   此时将显示 Decommission Nodes 页面。当停用操作步骤 达到以下任一阶段时， * 暂停 * 按钮将处于启用状态。

   - 评估 ILM
   - 停用纠删编码数据

3. 选择 * 暂停 * 以暂停操作步骤 。

   当前阶段已暂停，并且 * 恢复 * 按钮已启用。



4. 另一个维护操作步骤 完成后，选择 * 恢复 * 继续执行停用。

如果节点停用操作步骤 因错误而停止，您可以采取特定步骤对问题进行故障排除。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

关于此任务

如果关闭要停用的网格节点，则此任务将停止，直到网格节点重新启动为止。网格节点必须处于联机状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 在网格拓扑树中，展开每个存储节点条目，并验证 DDS 和 LDR 服务是否均联机。

   要执行存储节点停用，在联机节点 / 站点停用开始时，所有节点和所有服务都必须运行正常。

3. 要查看活动的网格任务，请选择 * 主管理节点 * > * 。 CMN* > * 网格任务 * > * 概述 * 。
4. 检查停用网格任务的状态。

   a. 如果停用网格任务的状态指示保存网格任务包时出现问题，请选择 * 主管理节点 * > * 。 CMN* > * 事件 * > * 。概述 *

   b. 检查可用审核中继的数量。

      如果可用审核中继属性为一个或多个，则 CMN 服务至少会连接到一个 ADE 服务。ADC" 服务 " 充当审核中继。

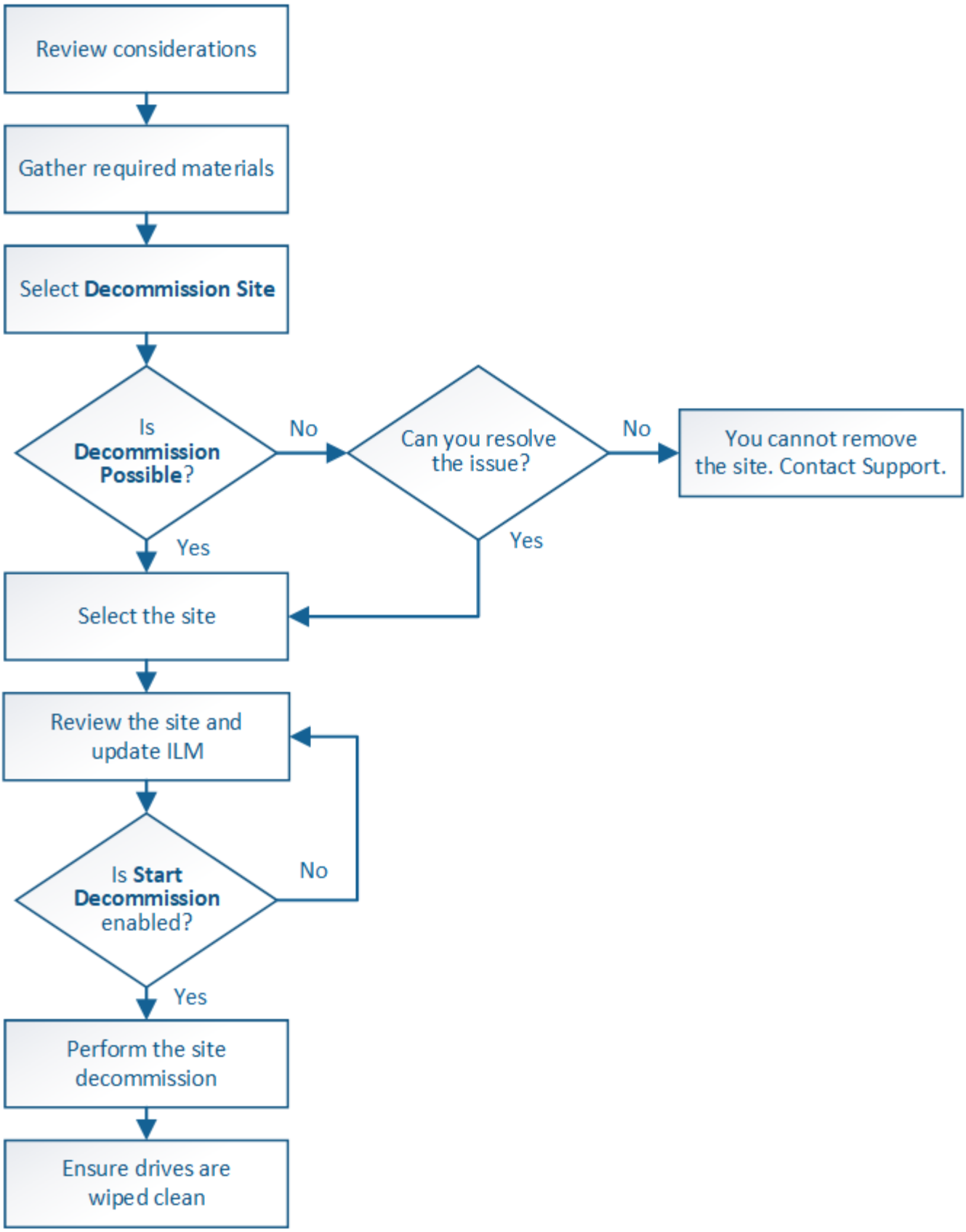
   CMN 服务必须至少连接到一个 StorageGRID 服务，并且必须有大部分（ 50% 加上一个）的系统的 ADC 服务可用，才能使网格任务从停用的一个阶段转移到另一个阶段并完成。

   a. 如果 CMN 服务未连接到足够的模块转换服务，请确保存储节点处于联机状态，并检查主管理节点与存储节点之间的网络连接。

站点停用

您可能需要从 StorageGRID 系统中删除数据中心站点。要删除站点，必须停用它。

流程图显示了停用站点的高级步骤。



删除站点的注意事项

在使用站点停用操作步骤 删除站点之前，您必须查看注意事项。

停用站点时会发生什么情况

停用站点时， StorageGRID 会从 StorageGRID 系统中永久删除站点上的所有节点以及站点本身。

站点停用操作步骤 完成后：

- 您不能再使用 StorageGRID 查看或访问站点或站点上的任何节点。
- 您不能再使用引用此站点的任何存储池或擦除编码配置文件。当 StorageGRID 停用站点时，它会自动删除这些存储池并停用这些擦除编码配置文件。

已连接站点与已断开站点停用过程之间的差异

您可以使用站点停用操作步骤 删除所有节点均已连接到 StorageGRID 的站点（称为已连接站点停用），或者删除所有节点均已与 StorageGRID 断开连接的站点（称为已断开连接的站点停用）。开始之前，您必须了解这些过程之间的差异。

> 如果站点包含混合的 Connected （）和已断开连接的节点（ 或 ），您必须使所有脱机节点重新联机。

- 通过已连接站点停用，您可以从 StorageGRID 系统中删除操作站点。例如，您可以执行已连接站点停用以删除正常运行但不再需要的站点。
- 当 StorageGRID 删除已连接站点时，它会使用 ILM 管理该站点上的对象数据。在开始停用已连接站点之前，必须先从所有 ILM 规则中删除此站点并激活新的 ILM 策略。迁移对象数据的 ILM 过程和删除站点的内部过程可以同时进行，但最佳实践是，在开始实际停用操作步骤 之前，允许完成 ILM 步骤。
- 断开连接的站点停用允许您从 StorageGRID 系统中删除故障站点。例如，您可以执行已断开连接的站点停用，以删除已被火灾或洪水破坏的站点。

  当 StorageGRID 删除已断开连接的站点时，它会将所有节点视为不可恢复的，并且不会尝试保留数据。但是，在开始执行已断开连接的站点停用之前，必须先从所有 ILM 规则中删除此站点并激活新的 ILM 策略。

> 在执行已断开连接的站点停用操作步骤 之前，您必须联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。如果您认为可以恢复站点或从站点恢复对象数据，则不应尝试执行已断开连接的站点停用。

删除已连接或已断开连接的站点的一般要求

在删除已连接或已断开连接的站点之前，您必须了解以下要求：

- 您不能停用包含主管理节点的站点。
- 您不能停用包含归档节点的站点。
- 如果任何节点的接口属于高可用性（ HA ）组，则无法停用站点。您必须编辑 HA 组以删除节点的接口或删除整个 HA 组。
- 如果站点包含已连接（）并断开连接（ 或 ）节点。
- 如果任何其他站点上的任何节点已断开连接（ 或 ）。
- 如果正在执行 EC-node-repair 操作，则无法启动站点停用操作步骤 。请参见 检查数据修复作业 跟踪纠删编码数据的修复情况。

- 站点停用操作步骤 运行时：
  - 您不能创建引用要停用的站点的 ILM 规则。您也不能编辑现有 ILM 规则来引用站点。
  - 您不能执行其他维护过程，例如扩展或升级。

> 如果您需要在已连接站点停用期间执行另一个维护操作步骤 ，则可以 在删除存储节点时暂停操作步骤。只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。第二个维护操作步骤 完成后，您可以恢复停用。

  - 如果您需要在启动站点停用操作步骤 后恢复任何节点，必须联系支持部门。
- 您不能一次停用多个站点。
- 如果站点包含一个或多个管理节点，并且为 StorageGRID 系统启用了单点登录（ Single Sign-On ， SSO ），则必须从 Active Directory 联合身份验证服务（ Active Directory Federation Services ， AD FS ）中删除此站点的所有依赖方信任。

信息生命周期管理（ **ILM** ）的要求

在删除站点时，您必须更新 ILM 配置。" 取消配置站点 " 向导将指导您完成许多前提条件步骤，以确保满足以下要求：

- 此站点不是由活动 ILM 策略引用的。如果是，则必须使用新的 ILM 规则创建并激活新的 ILM 策略。
- 不存在建议的 ILM 策略。如果您有建议的策略，则必须将其删除。
- 任何 ILM 规则都不引用站点，即使活动策略或建议策略中未使用这些规则也是如此。您必须删除或编辑引用此站点的所有规则。

当 StorageGRID 停用站点时，它将自动停用引用该站点的任何未使用的擦除编码配置文件，并自动删除引用该站点的任何未使用的存储池。系统默认的所有存储节点存储池将被删除，因为它会使用所有站点。

> 在删除站点之前，您可能需要创建新的 ILM 规则并激活新的 ILM 策略。这些说明假定您已充分了解 ILM 的工作原理，并且熟悉创建存储池，擦除编码配置文件， ILM 规则以及模拟和激活 ILM 策略。请参见有关通过信息生命周期管理来管理对象的说明。

使用 ILM 管理对象

已连接站点上的对象数据注意事项

如果要执行已连接站点停用，则必须在创建新的 ILM 规则和新的 ILM 策略时确定如何处理站点上的现有对象数据。您可以执行以下任一操作，也可以同时执行这两项操作：

- 将对象数据从选定站点移动到网格中的一个或多个其他站点。
- 移动数据的示例 * ：假设您要停用罗利的某个站点，因为您在森尼韦尔添加了一个新站点。在此示例中，您希望将所有对象数据从旧站点移动到新站点。在更新 ILM 规则和 ILM 策略之前，您必须查看两个站点的容量。您必须确保森尼韦尔站点具有足够的容量来容纳来自罗利站点的对象数据，并且森尼韦尔将保留足够的容量以满足未来增长的需要。

> 要确保有足够的可用容量，您可能需要先向现有站点添加存储卷或存储节点，或者添加新站点，然后再执行此操作步骤 。请参见有关扩展 StorageGRID 系统的说明。

- 从选定站点删除对象副本。
- 删除数据的示例 * ：假设您当前使用 3 个副本 ILM 规则在三个站点之间复制对象数据。在停用站点之前，您可以创建等效的双副本 ILM 规则，以便仅将数据存储在两个站点上。激活使用双副本规则的新 ILM 策略时， StorageGRID 会从第三个站点删除这些副本，因为它们不再满足 ILM 要求。但是，对象数据仍会受到保护，其余两个站点的容量将保持不变。

> 切勿创建单个副本 ILM 规则来容纳站点的删除。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

已连接站点停用的其他要求

在 StorageGRID 删除已连接站点之前，您必须确保满足以下条件：

- StorageGRID 系统中的所有节点的连接状态都必须为 * 已连接 * （）；但是，节点可以具有活动警报。

> 如果一个或多个节点断开连接，您可以完成 " 取消配置站点 " 向导的步骤 1-4 。但是，除非所有节点均已连接，否则无法完成向导的第 5 步，该步骤将启动停用过程。

- 如果要删除的站点包含用于负载平衡的网关节点或管理节点，则可能需要执行扩展操作步骤 ，以便在另一个站点添加等效的新节点。在启动站点停用操作步骤 之前，请确保客户端可以连接到替代节点。
- 如果要删除的站点包含高可用性（ HA ）组中的任何网关节点或管理节点，则可以完成 " 取消配置站点 " 向导的步骤 1-4 。但是，在从所有 HA 组中删除这些节点之前，您无法完成向导的第 5 步，该步骤将启动停用过程。如果现有客户端连接到包含站点中节点的 HA 组，则必须确保它们可以在删除站点后继续连接到 StorageGRID 。
- 如果客户端直接连接到您要删除的站点上的存储节点，则必须确保它们可以连接到其他站点上的存储节点，然后再启动站点停用操作步骤 。
- 您必须在其余站点上提供足够的空间，以容纳因活动 ILM 策略更改而要移动的任何对象数据。在某些情况下，您可能需要先通过添加存储节点，存储卷或新站点来扩展 StorageGRID 系统，然后才能完成已连接站点的停用。
- 您必须留出足够的时间来完成停用操作步骤 。StorageGRID ILM 过程可能需要数天，数周甚至数月才能从站点中移动或删除对象数据，然后才能停用此站点。

> 从站点移动或删除对象数据可能需要数天，数周甚至数月的时间，具体取决于站点上的数据量，系统上的负载，网络延迟以及所需 ILM 更改的性质。

- 您应尽可能早地完成 " 弃用站点 " 向导的步骤 1-4 。如果您允许在启动实际停用操作步骤 之前从站点移动数据，则停用操作步骤 将更快地完成，并且中断和性能影响更少（方法是在向导的步骤 5 中选择 * 启动停用 * ）。

断开连接的站点停用的其他要求

在 StorageGRID 删除已断开连接的站点之前，您必须确保满足以下条件：

- 您已联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。

如果您认为可以恢复站点或从站点恢复任何对象数据，则不应尝试执行已断开连接的站点停用。

- 站点上的所有节点的连接状态必须为以下之一：
  - * 未知 * （）：节点未连接到网格，原因未知。例如，节点之间的网络连接已断开或电源已关闭。
  - * 管理员关闭 * （）：由于预期原因，节点未连接到网格。例如，节点上的一个或多个节点已正常关闭。
- 所有其他站点上的所有节点的连接状态都必须为 * 已连接 * （）；但是，这些其他节点可能具有活动警报。
- 您必须了解，您将无法再使用 StorageGRID 查看或检索站点上存储的任何对象数据。当 StorageGRID 执行此操作步骤 时，它不会尝试保留已断开连接的站点中的任何数据。

如果您的 ILM 规则和策略旨在防止单个站点丢失，则其余站点上仍存在对象的副本。

- 您必须了解，如果站点包含对象的唯一副本，则该对象将丢失，无法检索。

删除站点时的一致性控制注意事项

S3 存储分段或 Swift 容器的一致性级别可确定 StorageGRID 是否在通知客户端对象载入成功之前将对象元数据完全复制到所有节点和站点。一致性控制可以在对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。

StorageGRID 删除站点时，需要确保不会向要删除的站点写入任何数据。因此，它会临时覆盖每个分段或容器的一致性级别。启动站点停用过程后， StorageGRID 会暂时使用强站点一致性来防止将对象元数据写入要删除的站点。

由于这种临时覆盖，请注意，如果其他站点上的多个节点不可用，则站点停用期间发生的任何客户端写入，更新和删除操作都可能失败。

相关信息

技术支持如何执行站点恢复

使用 ILM 管理对象

扩展网格

收集所需材料

停用站点之前，您必须获取以下材料。

项目	注释：
恢复软件包 ` .zip` 文件	您必须下载最新的恢复软件包 ` .zip` 文件（ `sGWS-recovery-package-id-revision.zip` ）。如果发生故障，您可以使用恢复包文件还原系统。

`passwords.txt` file	此文件包含在命令行上访问网格节点所需的密码，并包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在 `passwords.txt` 文件中。
停用前 StorageGRID 系统拓扑的问题描述	如果有，请获取描述系统当前拓扑的任何文档。

相关信息

Web 浏览器要求

下载恢复包

第 **1** 步：选择站点

要确定是否可以停用某个站点，请首先访问 " 停用站点 " 向导。

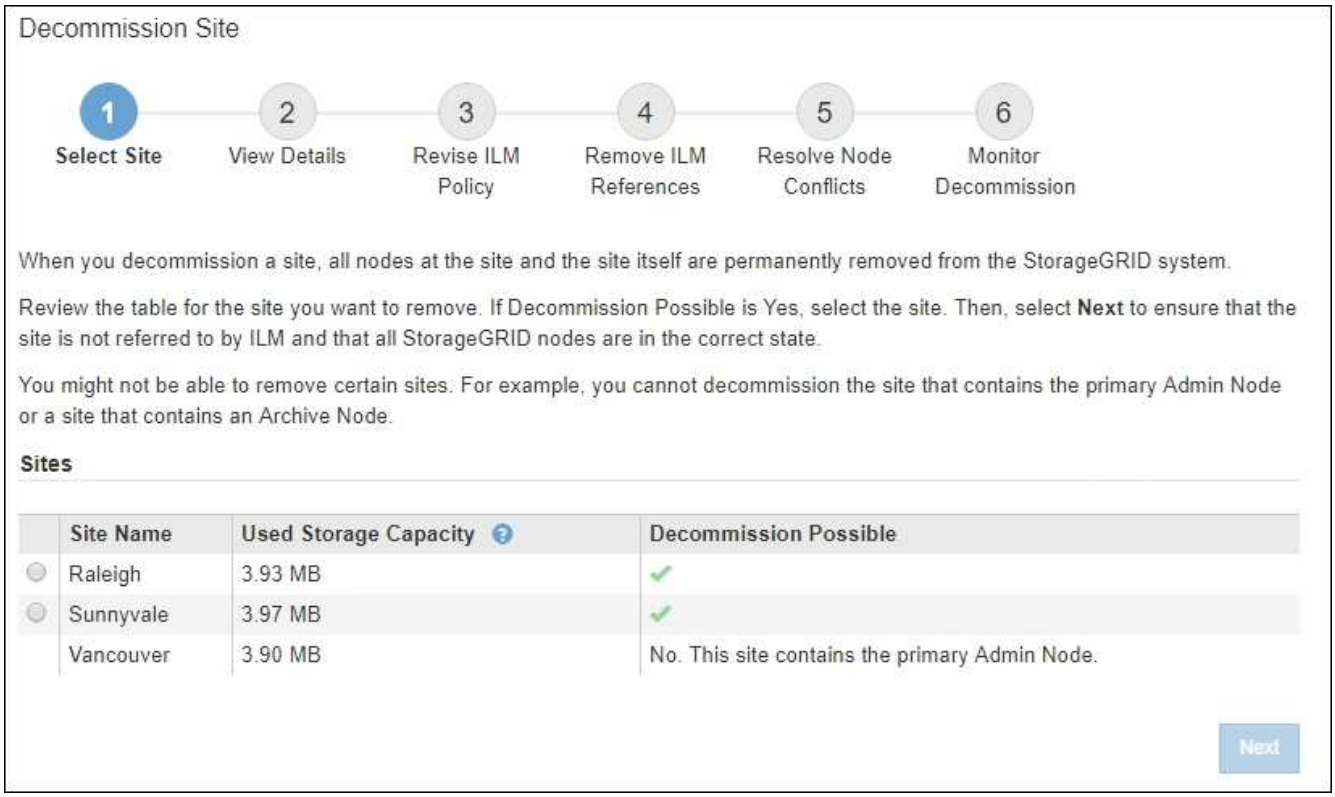
您需要的内容

- 您必须已获取所有必需的材料。
- 您必须已查看删除站点的注意事项。
- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有 " 根访问 " 权限或 " 维护 " 和 "ILM " 权限。

步骤

1. 选择 * 维护 * > * 任务 * > * 取消配置 * 。
2. 选择 * 取消配置站点 * 。

   此时将显示取消配置站点向导的第 1 步（选择站点）。此步骤包含 StorageGRID 系统中站点的字母列表。



3. 查看 * 已用存储容量 * 列中的值，确定每个站点上的对象数据当前使用的存储容量。

   已用存储容量是一个估计值。如果节点处于脱机状态，则已用存储容量是站点的最后一个已知值。

   - 对于已连接站点停用，此值表示在安全停用此站点之前需要将多少对象数据移动到其他站点或由 ILM 删除。
   - 对于已断开连接的站点停用，此值表示停用此站点后系统的数据存储容量将变得不可访问。

   如果您的 ILM 策略旨在防止单个站点丢失，则其余站点上仍应存在对象数据的副本。

4. 查看 * 可能停用 * 列中的原因，确定哪些站点当前可以停用。

   如果无法停用某个站点的原因不止一个，则会显示最关键的原因。

停用可能的原因	Description	下一步
绿色复选标记（✔）	您可以停用此站点。	转至 下一步。
否此站点包含主管理节点。	您不能停用包含主管理节点的站点。	无您无法执行此操作步骤 。
否此站点包含一个或多个归档节点。	您不能停用包含归档节点的站点。	无您无法执行此操作步骤 。

停用可能的原因	**Description**	下一步
否此站点上的所有节点均已断开连接。请联系您的 NetApp 客户代表。	除非站点中的每个节点都已连接（）。	如果您要执行已断开连接的站点停用，必须联系您的 NetApp 客户代表，客户代表将查看您的要求并启用停用站点向导的其余部分。 • 重要信息 *：切勿使联机节点脱机，以便可以删除站点。您将丢失数据。

此示例显示了一个包含三个站点的 StorageGRID 系统。绿色复选标记（）对于罗利和森尼韦尔站点，表示您可以停用这些站点。但是，您无法停用温哥华站点，因为它包含主管理节点。

1. 如果可以停用，请选择站点的单选按钮。

   此时将启用 * 下一步 * 按钮。

2. 选择 * 下一步 * 。

   此时将显示第 2 步（查看详细信息）。

第 **2** 步：查看详细信息

从 " 弃用站点 " 向导的第 2 步（查看详细信息）中，您可以查看站点中包含的节点，查看每个存储节点上已使用的空间量，并评估网格中其他站点上的可用空间量。

您需要的内容

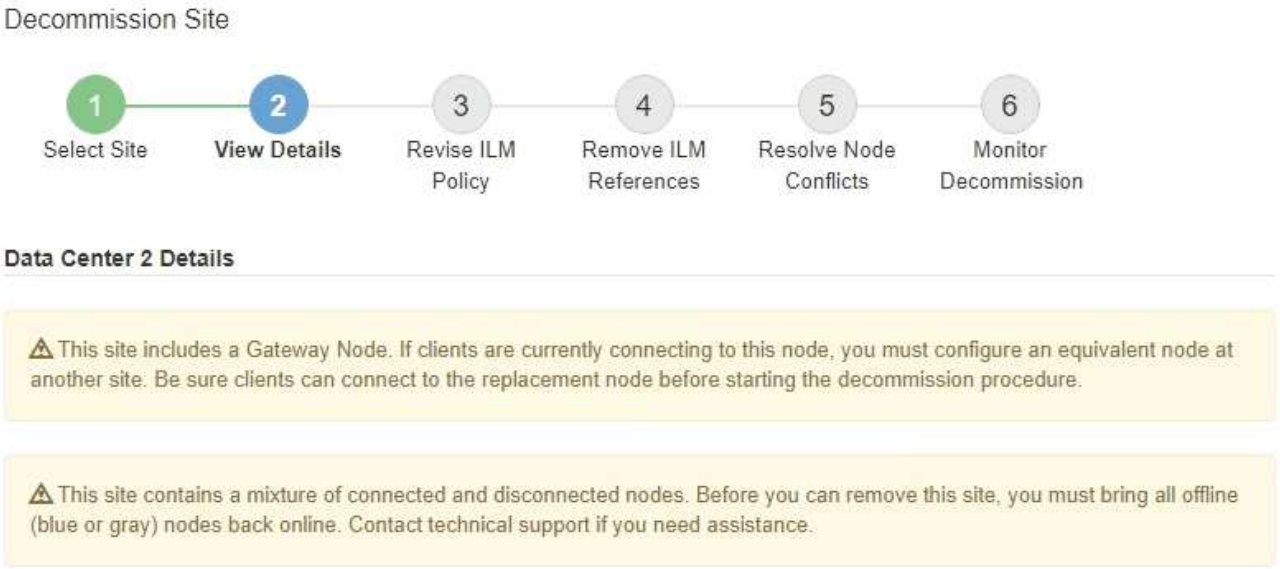
停用站点之前，您必须查看站点上存在的对象数据量。

- 如果您要执行已连接站点停用，则必须先了解站点上当前存在的对象数据量，然后再更新 ILM 。根据站点容量和数据保护需求，您可以创建新的 ILM 规则，将数据移动到其他站点或从站点中删除对象数据。
- 如果可能，请在启动停用操作步骤 之前执行任何所需的存储节点扩展。
- 如果您要执行断开连接的站点停用，则必须了解删除此站点后将永久无法访问多少对象数据。

> 如果您正在执行断开连接的站点停用， ILM 将无法移动或删除对象数据。站点上保留的所有数据都将丢失。但是，如果您的 ILM 策略旨在防止单个站点丢失，则其余站点上仍存在对象数据的副本。

步骤

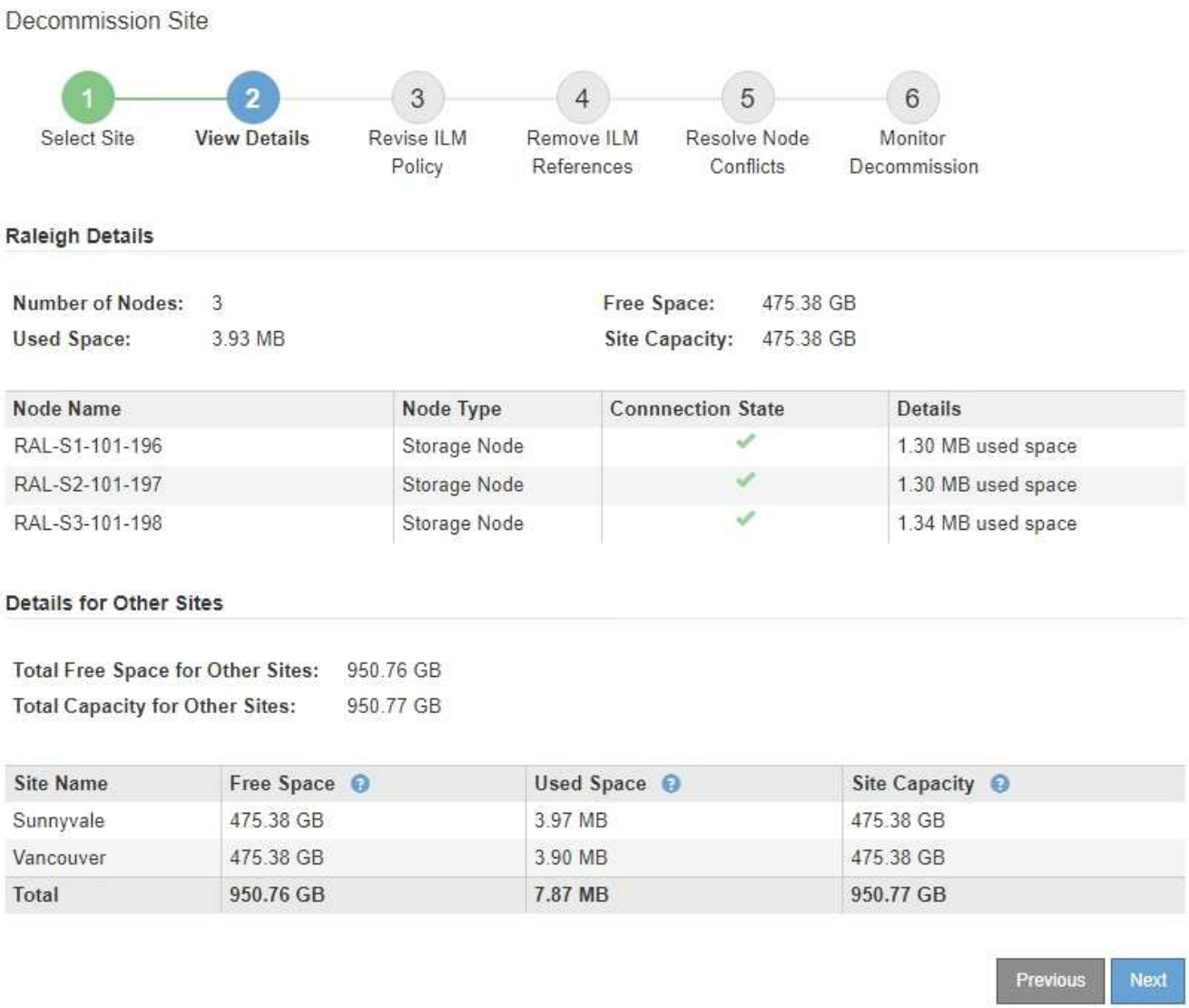
1. 从第 2 步（查看详细信息）中，查看与您选择删除的站点相关的任何警告。



在以下情况下会显示警告：

- 此站点包含一个网关节点。如果 S3 和 Swift 客户端当前正在连接到此节点，则必须在另一站点配置等效节点。在继续执行停用操作步骤 之前，请确保客户端可以连接到替代节点。
- 此站点包含一个混合的 Connected （ ）和已断开连接的节点（ 或 ）。在删除此站点之前，您必须使所有脱机节点重新联机。

2. 查看有关选定要删除的站点的详细信息。



选定站点包含以下信息：

- 节点数
- 站点中所有存储节点的已用总空间，可用空间和容量。
  - 对于已连接站点停用， * 已用空间 * 值表示必须将多少对象数据移动到其他站点或使用 ILM 删除。
  - 对于已断开连接的站点停用， * 已用空间 * 值表示删除此站点后将无法访问多少对象数据。
- 节点名称，类型和连接状态：
  - （已连接）
  - （管理员关闭）
  - （未知）
- 有关每个节点的详细信息：
  - 对于每个存储节点，为对象数据使用的空间量。
  - 对于管理节点和网关节点，表示此节点当前是否在高可用性（ HA ）组中使用。您不能停用HA组中

使用的管理节点或网关节点。开始停用之前，必须编辑 HA 组以删除站点上的所有节点。或者，如果 HA 组仅包含此站点中的节点，则可以将其删除。

管理 StorageGRID

3. 在页面的其他站点的详细信息部分中，评估网格中其他站点的可用空间量。

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

如果您正在执行已连接站点停用，并且计划使用 ILM 从选定站点移动对象数据（而不是仅删除该数据），则必须确保其他站点具有足够的容量来容纳移动的数据，并且为未来的增长保留足够的容量。

如果要删除的站点的 * 已用空间 * 大于 * 其他站点的总可用空间 * ，则会显示警告。要确保删除站点后有足够的存储容量可用，您可能需要在执行此操作步骤 之前执行扩展。

4. 选择 * 下一步 * 。

此时将显示第 3 步（修订 ILM 策略）。

相关信息

使用 ILM 管理对象

第 3 步：修订 ILM 策略

从 " 弃用站点 " 向导的第 3 步（修订 ILM 策略）中，您可以确定活动的 ILM 策略是否引用此站点。

您需要的内容

您很好地了解 ILM 的工作原理，并且熟悉创建存储池，擦除编码配置文件， ILM 规则以及模拟和激活 ILM 策略。

使用 ILM 管理对象

关于此任务

如果某个站点是由活动 ILM 策略中的任何 ILM 规则引用的，则 StorageGRID 无法停用该站点。

如果您当前的 ILM 策略是指要删除的站点，则必须激活满足特定要求的新 ILM 策略。具体而言，新的 ILM 策略：

- 无法使用引用站点的存储池。

- 无法使用引用站点的擦除编码配置文件。
- 无法使用默认的 * 所有存储节点 * 存储池或默认的 * 所有站点 * 站点。
- 无法使用常用 * 创建 2 个副本 * 规则。
- 必须设计为完全保护所有对象数据。

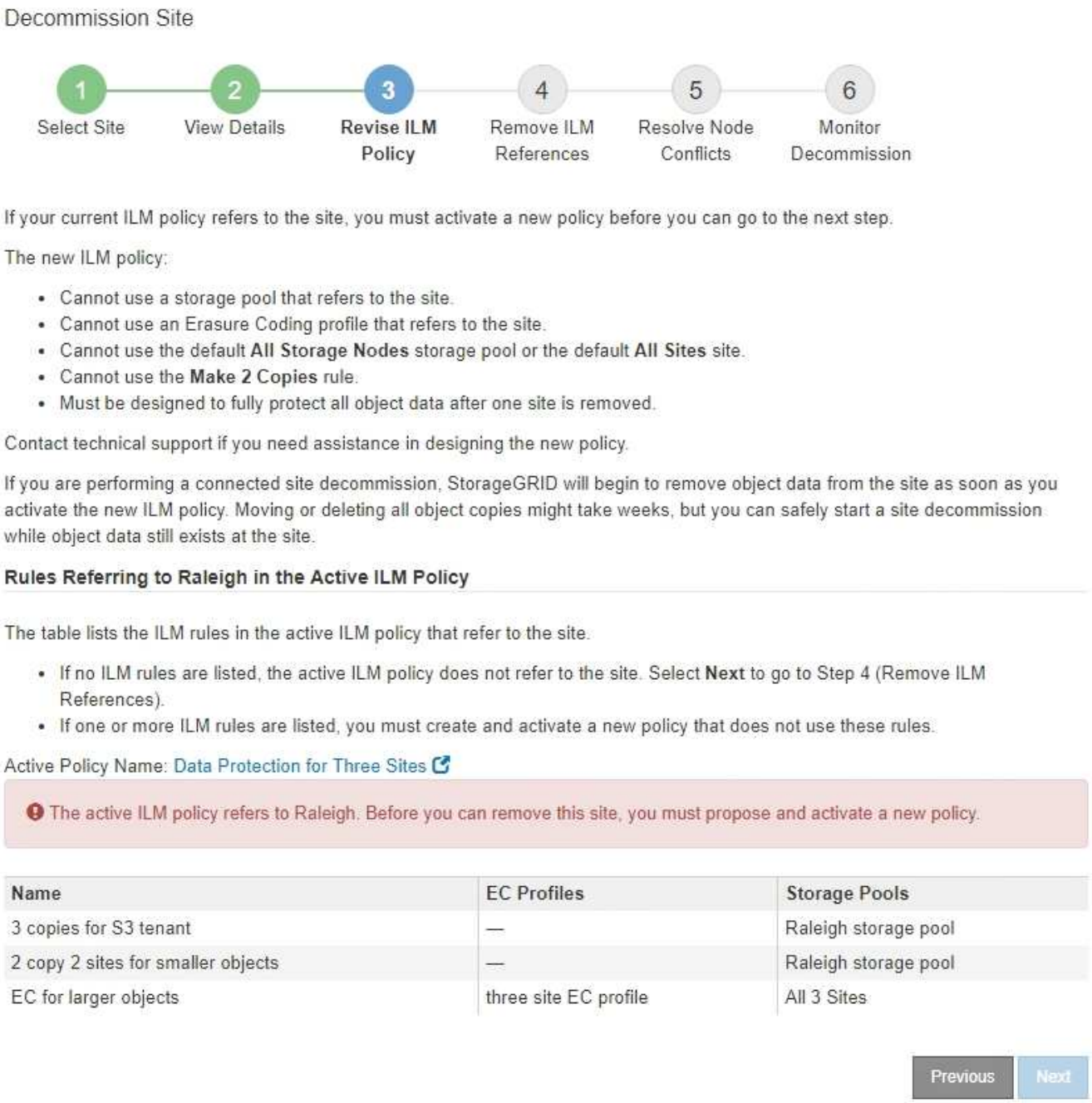
> 切勿创建单个副本 ILM 规则来容纳站点的删除。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

如果您要执行 *connected site decommission* ，则必须考虑 StorageGRID 应如何管理您要删除的站点上当前的对象数据。根据您的数据保护要求，新规则可以将现有对象数据移动到不同的站点，也可以删除不再需要的任何额外对象副本。

如果您在设计新策略时需要帮助，请联系技术支持。

步骤

1. 从第 3 步（修订 ILM 策略）中，确定活动 ILM 策略中的任何 ILM 规则是否引用您选择删除的站点。



2. 如果未列出任何规则，请选择 * 下一步 * 以转到步骤 4 （删除 ILM 引用）

   第 4 步：删除 ILM 引用

3. 如果表中列出了一个或多个 ILM 规则，请选择 * 活动策略名称 * 旁边的链接。

   此时， ILM 策略页面将显示在新的浏览器选项卡中。使用此选项卡更新 ILM 。" 取消配置站点 " 页面将在 " 其他 " 选项卡上保持打开状态。

   a. 如有必要，请选择 * ILM * > * 存储池 * 以创建一个或多个不引用站点的存储池。

      有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

b. 如果您计划使用纠删编码，请选择 * 。 IL* > * 纠删编码 * 以创建一个或多个纠删编码配置文件。

您必须选择不引用站点的存储池。

请勿在擦除编码配置文件中使用 * 所有存储节点 * 存储池。

4. 选择 * ILM * > * 规则 * ，然后克隆步骤 3 （修订 ILM 策略）表中列出的每个规则。

有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

a. 使用名称可以轻松地在新策略中选择这些规则。

b. 更新放置说明。

删除引用站点的任何存储池或擦除编码配置文件，并将其替换为新的存储池或擦除编码配置文件。

请勿在新规则中使用 * 所有存储节点 * 存储池。

5. 选择 * ILM * > * 策略 * ，然后创建一个使用新规则的新策略。

有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

a. 选择活动策略，然后选择 * 克隆 * 。

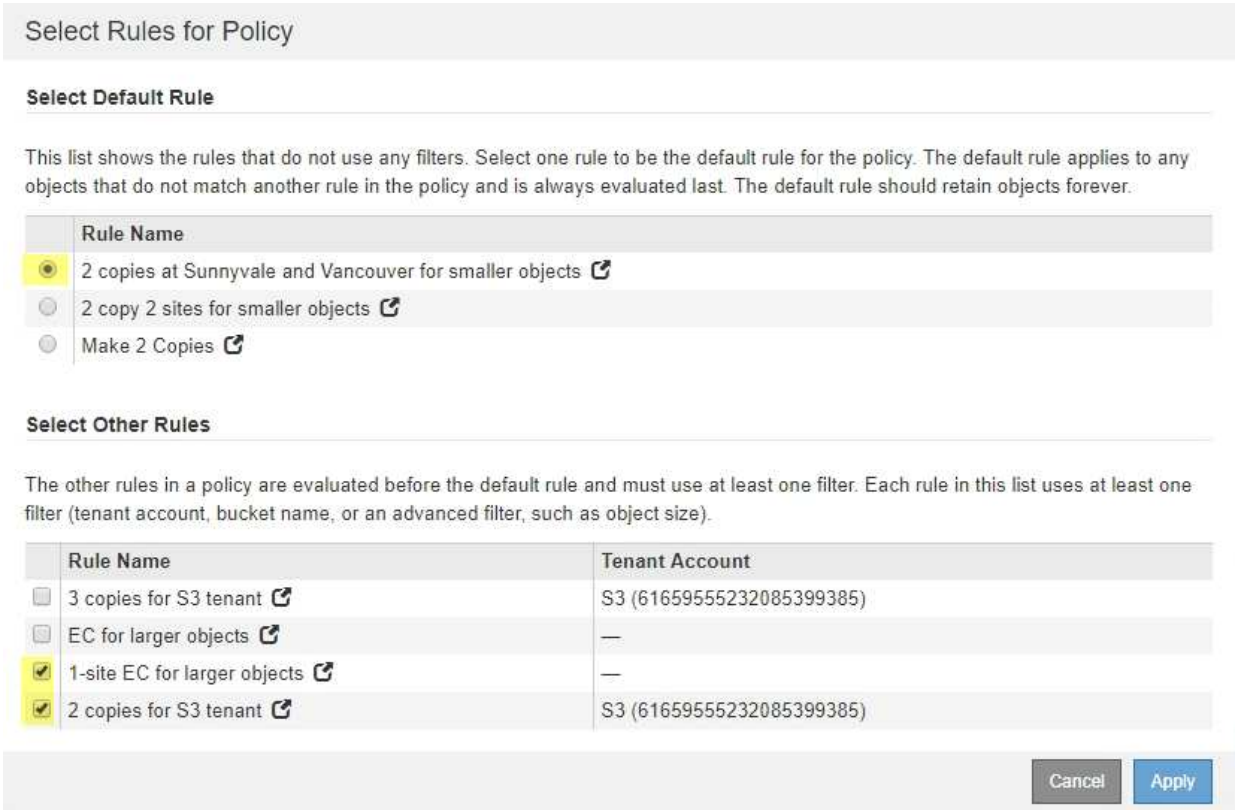
b. 指定策略名称和更改原因。

c. 为克隆的策略选择规则。

- 取消选择 " 弃用站点 " 页面的第 3 步（修订 ILM 策略）中列出的所有规则。
- 选择不引用站点的默认规则。

请勿选择 * 创建 2 个副本 * 规则，因为该规则使用 * 所有存储节点 * 存储池，这是不允许的。

- 选择您创建的其他替换规则。这些规则不应引用站点。



d. 选择 * 应用 * 。

e. 拖放这些行以重新排列策略中的规则。

您不能移动默认规则。

> 您必须确认 ILM 规则的顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。

a. 保存建议的策略。

6. 载入测试对象并模拟建议的策略，以确保应用正确的规则。

> ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。在激活策略之前，请仔细查看并模拟策略，以确认策略将按预期运行。

> 激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

7. 激活新策略。

如果您要执行已连接站点停用，则一旦激活新的 ILM 策略， StorageGRID 就会开始从选定站点删除对象数据。移动或删除所有对象副本可能需要数周时间。尽管在站点上仍存在对象数据的情况下，您可以安全地开始站点停用，但如果您允许在实际停用操作步骤 之前从站点移动数据，则停用操作步骤 将更快地完成，并减少中断和性能影响 （通过在向导的步骤 5 中选择 * 启动取消配置 * ）。

8. 返回到 * 步骤 3 （修订 ILM 策略） * ，以确保新活动策略中没有引用站点的 ILM 规则，并且已启用 * 下一步

* 按钮。

如果列出了任何规则，则必须先创建并激活新的 ILM 策略，然后才能继续。

9. 如果未列出任何规则，请选择 * 下一步 * 。

   此时将显示第 4 步（删除 ILM 参考）。

第 **4** 步：删除 **ILM** 引用

从 " 弃用站点 " 向导的第 4 步（删除 ILM 引用）中，您可以删除建议的策略（如果存在），并删除或编辑仍引用此站点的任何未使用的 ILM 规则。

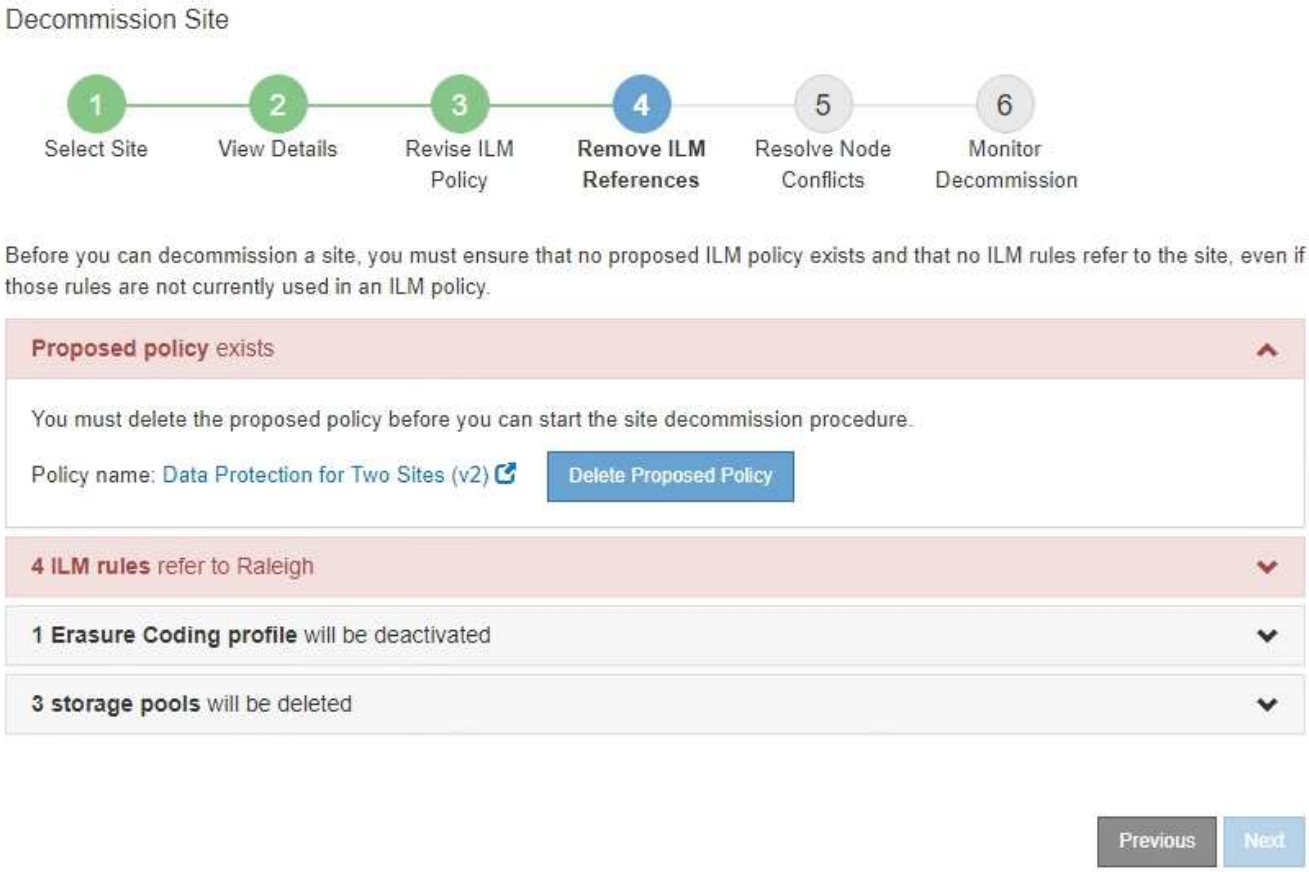
关于此任务

在以下情况下，您将无法启动站点停用操作步骤：

- 已存在建议的 ILM 策略。如果您有建议的策略，则必须将其删除。
- 任何 ILM 规则均指站点，即使此规则未在任何 ILM 策略中使用也是如此。您必须删除或编辑引用此站点的所有规则。

步骤

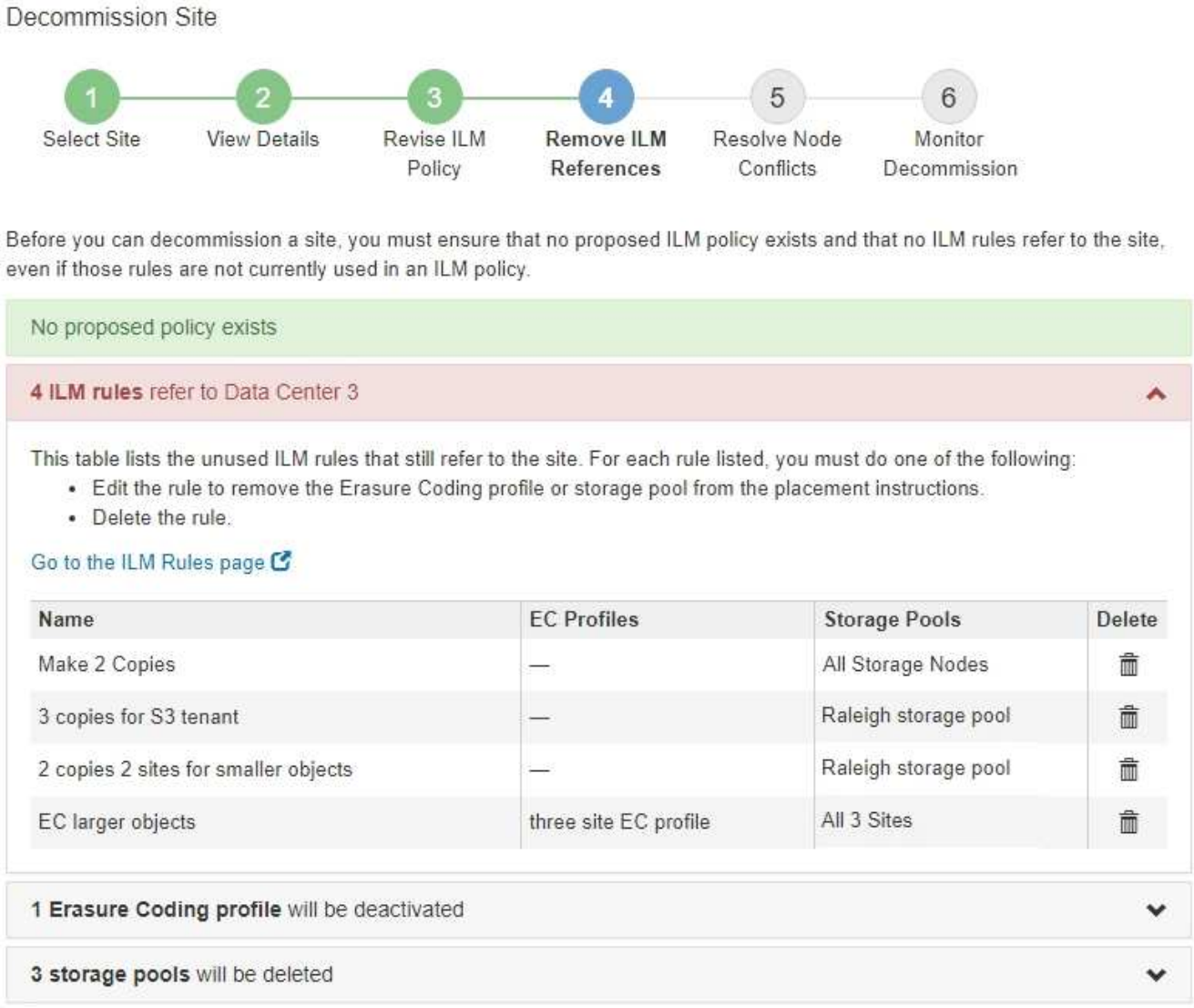
1. 如果列出了建议的策略，请将其删除。



a. 选择 * 删除建议的策略 * 。

b. 在确认对话框中选择 * 确定 * 。

2. 确定任何未使用的 ILM 规则是否引用站点。



列出的任何 ILM 规则仍引用站点，但不会在任何策略中使用。在示例中：

- 常用 * 创建 2 个副本 * 规则使用系统默认的 * 所有存储节点 * 存储池，该存储池使用所有站点站点站点。
- S3 租户 * 未使用的 * 3 个副本规则是指 * 罗利 * 存储池。
- 对于较小对象 * ，未使用的 * 2 个副本 2 个站点是指 * 罗利 * 存储池。
- 未使用的 * 较大对象 * 规则使用 * 所有 3 个站点 * 纠删编码配置文件中的罗利站点。
- 如果未列出 ILM 规则，请选择 * 下一步 * 以转到 * 步骤 5 （解决节点冲突） * 。

  第 5 步：解决节点冲突（并开始停用）

  > 当 StorageGRID 停用站点时，它将自动停用引用该站点的任何未使用的擦除编码配置文件，并自动删除引用该站点的任何未使用的存储池。系统默认的所有存储节点存储池将被删除，因为它使用的是所有站点站点站点。

- 如果列出了一个或多个 ILM 规则，请转至下一步。

3. 编辑或删除每个未使用的规则：

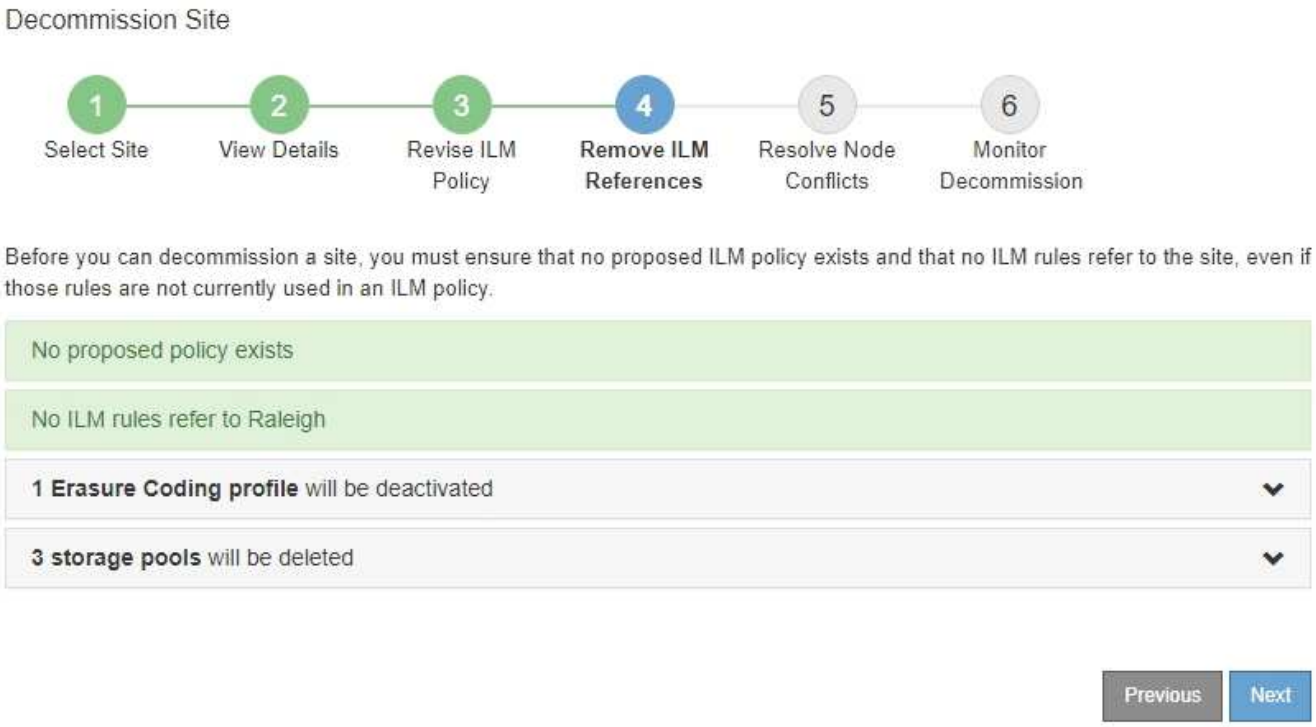
- 要编辑规则，请转到 "ILM 规则 " 页面，并更新使用擦除编码配置文件或引用站点的存储池的所有放置位置。然后，返回到 * 步骤 4 （删除 ILM 参考） * 。

  有关详细信息，请参见有关通过信息生命周期管理来管理对象的说明。

- 要删除规则，请选择垃圾桶图标 并选择 * 确定 * 。

  您必须先删除常用的 * 创建 2 个副本 * 规则，然后才能停用站点。

4. 确认不存在建议的 ILM 策略，未使用的 ILM 规则均未引用此站点，并且已启用 * 下一步 * 按钮。



5. 选择 * 下一步 * 。

   删除此站点后，引用此站点的任何剩余存储池和擦除编码配置文件将无效。当 StorageGRID 停用站点时，它将自动停用引用该站点的任何未使用的擦除编码配置文件，并自动删除引用该站点的任何未使用的存储池。系统默认的所有存储节点存储池将被删除，因为它使用的是所有站点站点站点。

此时将显示第 5 步（解决节点冲突）。

第 **5** 步：解决节点冲突（并开始停用）

从 " 弃用站点 " 向导的第 5 步（解决节点冲突）中，您可以确定 StorageGRID 系统中的任何节点是否已断开连接，或者选定站点中的任何节点是否属于高可用性（ HA ）组。解决任何节点冲突后，您可以从此页面启动停用操作步骤 。

您必须确保 StorageGRID 系统中的所有节点均处于正确状态，如下所示：

- StorageGRID 系统中的所有节点都必须已连接（）。

> 如果要执行已断开连接的站点停用，则必须断开要删除站点上的所有节点，并且必须连接所有其他站点上的所有节点。

- 要删除的站点上的任何节点都不能具有属于高可用性（ HA ）组的接口。

如果步骤 5 （解决节点冲突）中列出了任何节点，则必须更正问题描述 ，然后才能开始停用。

在此页面中启动站点停用操作步骤 之前，请查看以下注意事项：

- 您必须留出足够的时间来完成停用操作步骤 。

> 从站点移动或删除对象数据可能需要数天，数周甚至数月的时间，具体取决于站点上的数据量，系统上的负载，网络延迟以及所需 ILM 更改的性质。

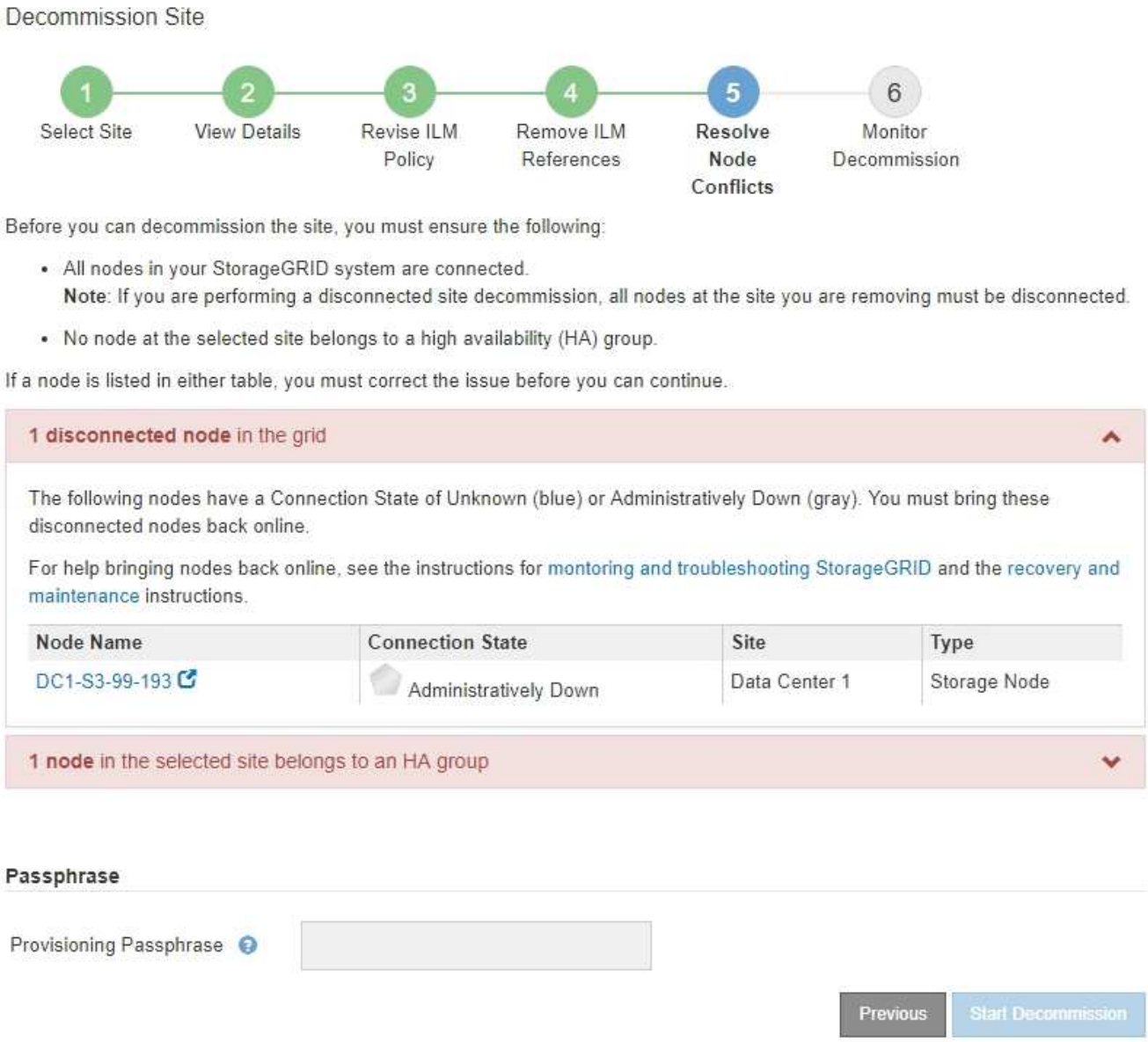
- 站点停用操作步骤 运行时：
  - 您不能创建引用要停用的站点的 ILM 规则。您也不能编辑现有 ILM 规则来引用站点。
  - 您不能执行其他维护过程，例如扩展或升级。

> 如果在已连接站点停用期间需要执行另一个维护操作步骤 ，则可以在删除存储节点时暂停操作步骤 。在 " D复制和擦除编码数据 " 阶段， * 暂停 * 按钮将启用。

  - 如果您需要在启动站点停用操作步骤 后恢复任何节点，必须联系支持部门。

步骤

1. 查看步骤 5 （解决节点冲突）中的已断开节点部分，确定 StorageGRID 系统中的任何节点的连接状态是否为未知（）或管理员关闭（）。

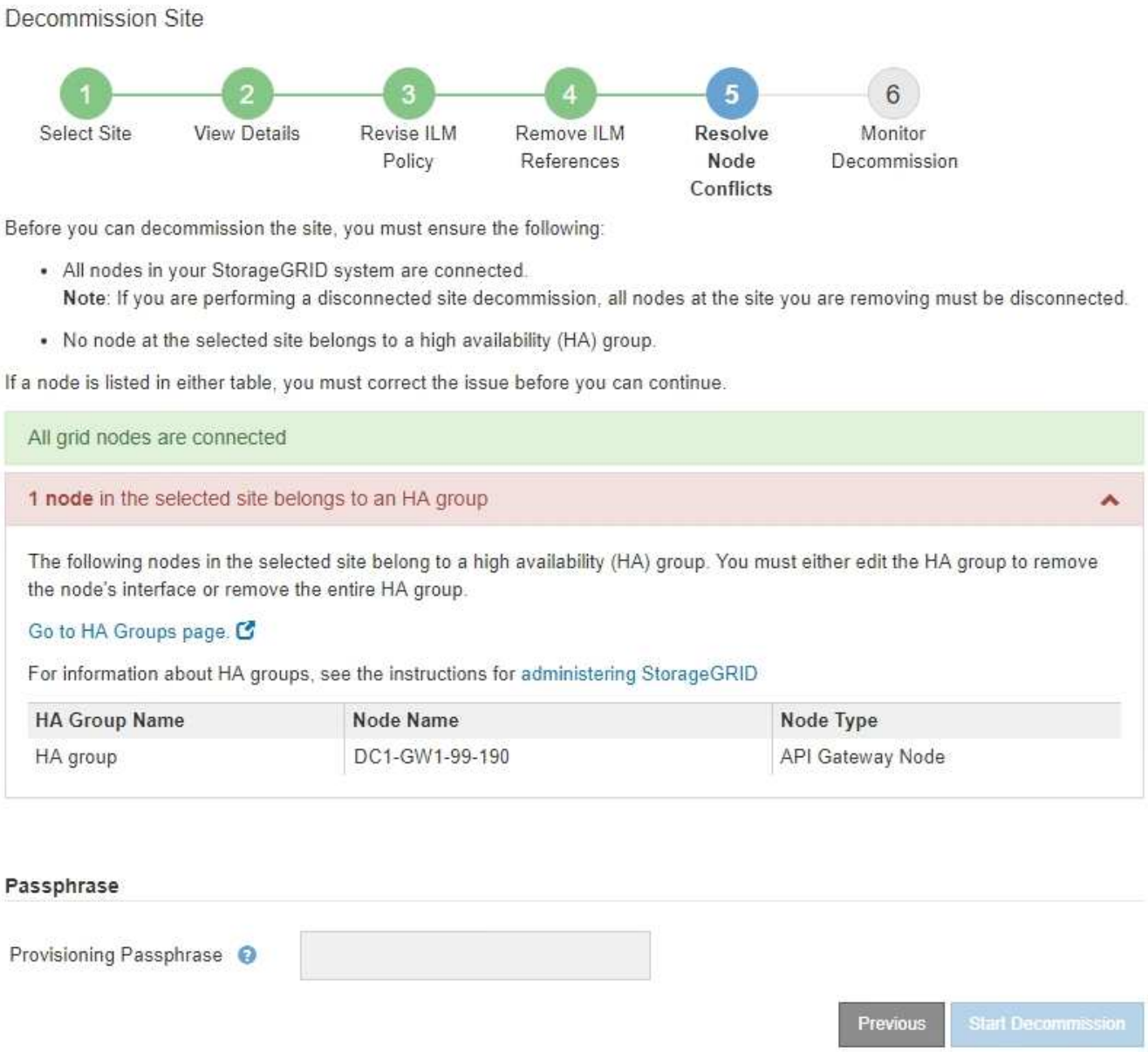


2. 如果任何节点已断开连接，请将其恢复联机。

   请参见有关监控 StorageGRID 和网格节点过程并对其进行故障排除的说明。如需帮助，请联系技术支持。

3. 当所有已断开连接的节点恢复联机后，请查看步骤 5 （解决节点冲突）中的 HA 组部分。

   此表列出了选定站点中属于高可用性（ HA ）组的任何节点。



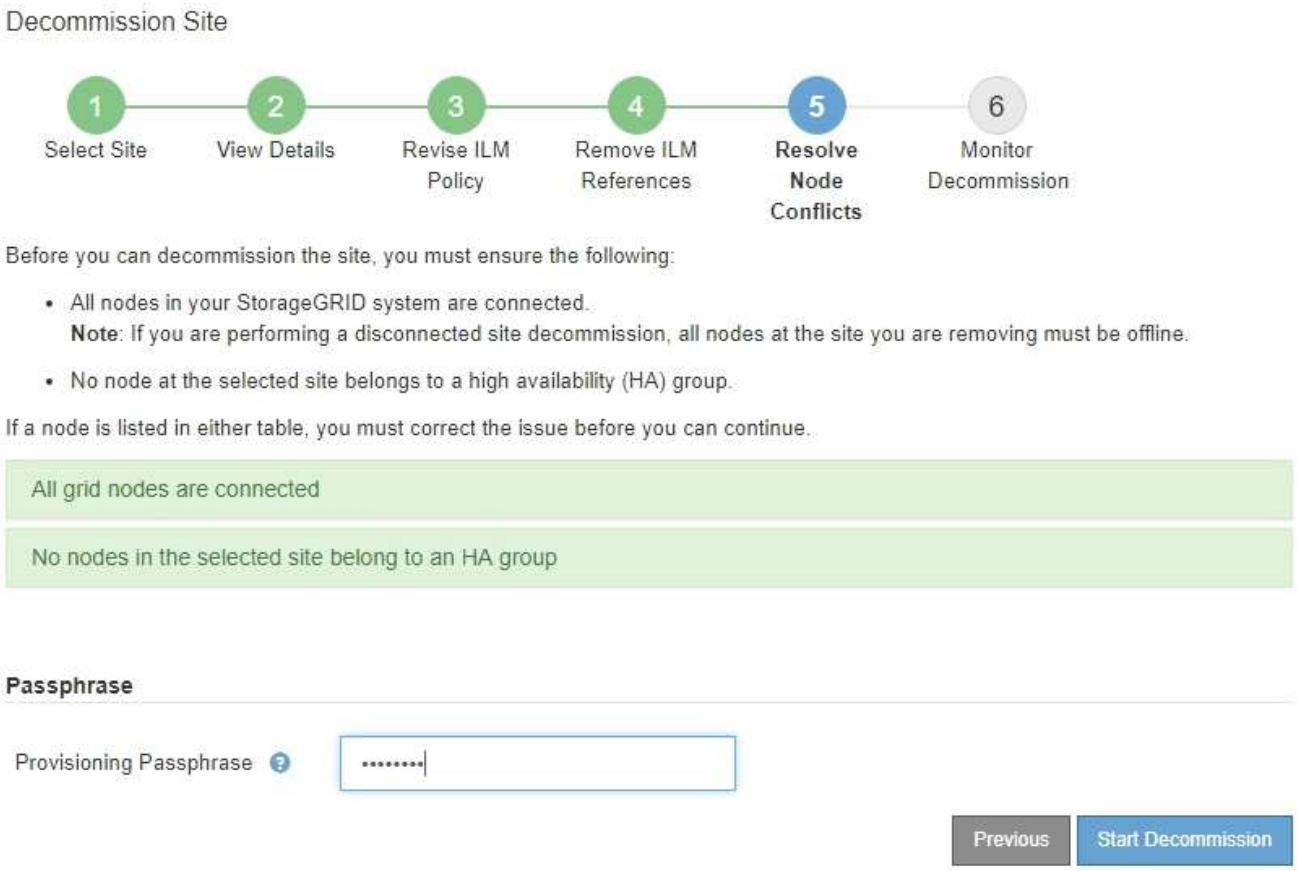
4. 如果列出了任何节点，请执行以下操作之一：

   - 编辑每个受影响的 HA 组以删除节点接口。
   - 从此站点中删除仅包含节点的 HA 组。请参见有关管理 StorageGRID 的说明。

   如果连接了所有节点，并且在 HA 组中未使用选定站点中的任何节点，则会启用 * 配置密码短语 * 字段。

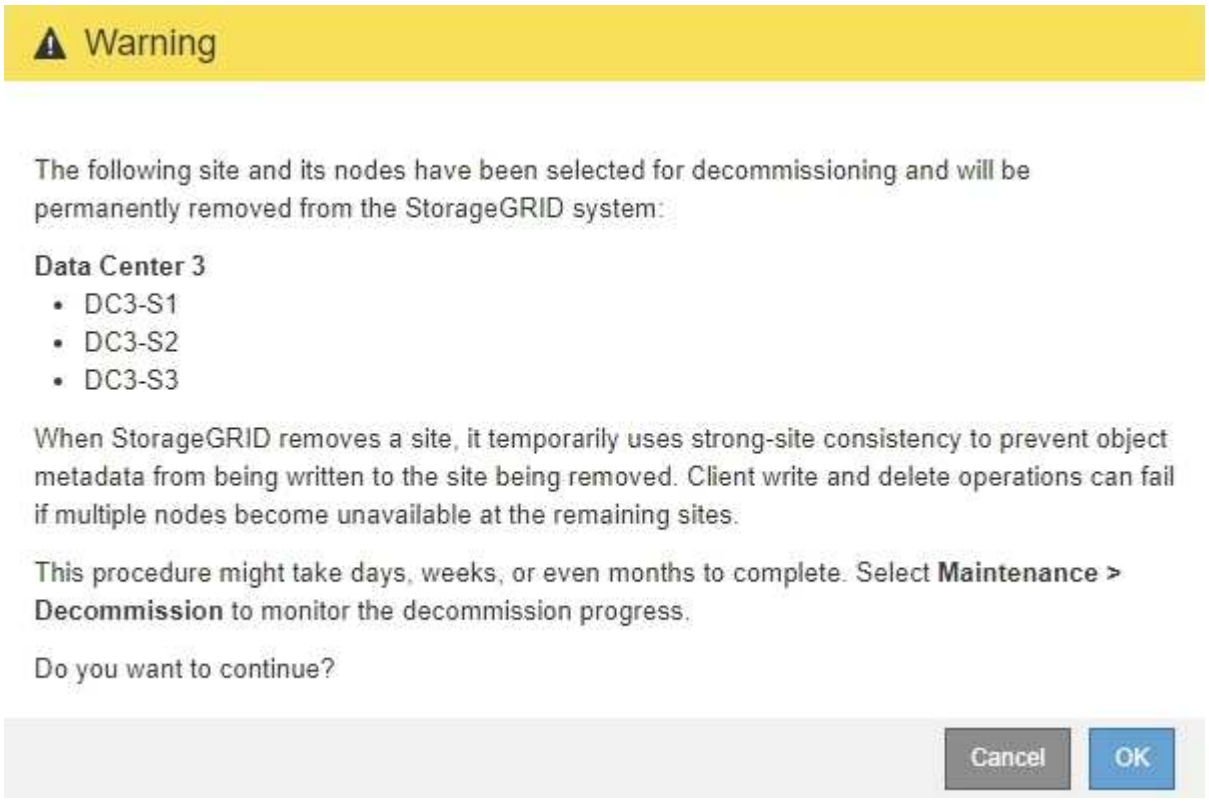
5. 输入配置密码短语。

   此时， * 开始取消配置 * 按钮将变为启用状态。



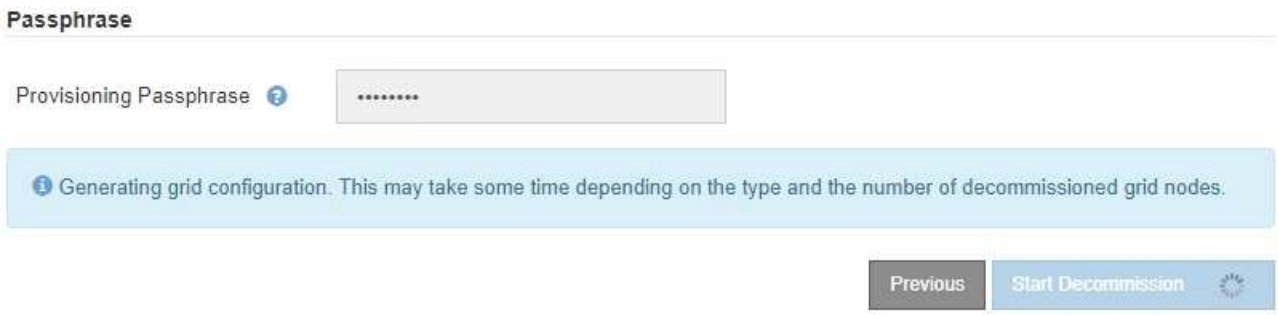
6. 如果您已准备好启动站点停用操作步骤，请选择 * 启动停用 * 。

警告将列出要删除的站点和节点。系统会提醒您，完全删除此站点可能需要数天，数周甚至数月的时间。



7. 查看警告。如果您已准备好开始，请选择 * 确定 * 。

   生成新网格配置时，将显示一条消息。此过程可能需要一些时间，具体取决于停用的网格节点的类型和数量。



   生成新网格配置后，将显示步骤 6 （监控取消配置）。

   在停用完成之前， * 上一步 * 按钮将保持禁用状态。

相关信息

监控和故障排除

网格节点过程

管理 StorageGRID

第 6 步：监控取消配置

从 " 取消配置站点 " 页面向导的第 6 步（监控取消配置）中，您可以在删除站点时监控进度。

关于此任务

当 StorageGRID 删除已连接站点时，它将按以下顺序删除节点：

1. 网关节点
2. 管理节点
3. 存储节点

当 StorageGRID 删除已断开连接的站点时，它会按以下顺序删除节点：

1. 网关节点
2. 存储节点
3. 管理节点

每个网关节点或管理节点可能只需要几分钟或一小时即可删除；但是，存储节点可能需要数天或数周的时间。

步骤

1. 生成新的恢复软件包后，立即下载该文件。

请尽快下载恢复包，以确保在停用操作步骤 期间出现问题时可以恢复网格。

a. 选择消息中的链接，或选择 * 维护 * > * 系统 * > * 恢复软件包 * 。

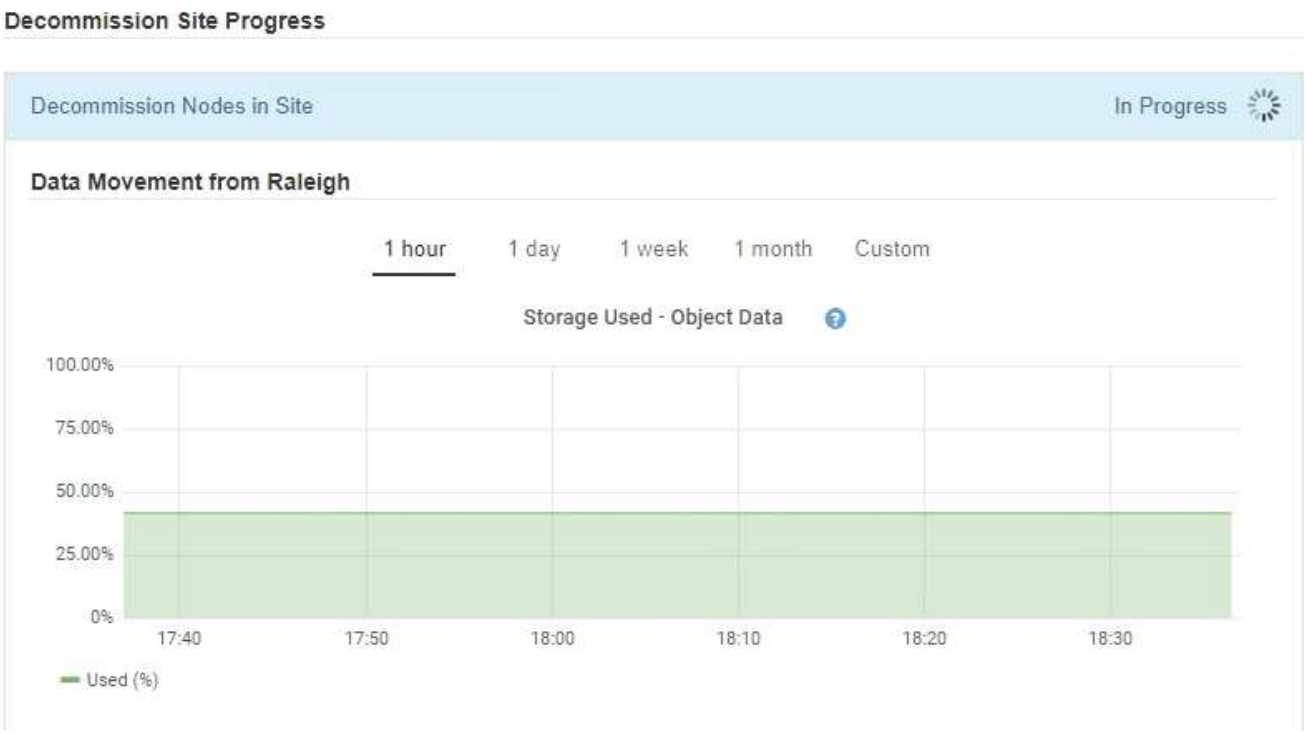
b. 下载 ` .zip` 文件。

请参见的说明 正在下载恢复包。

恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

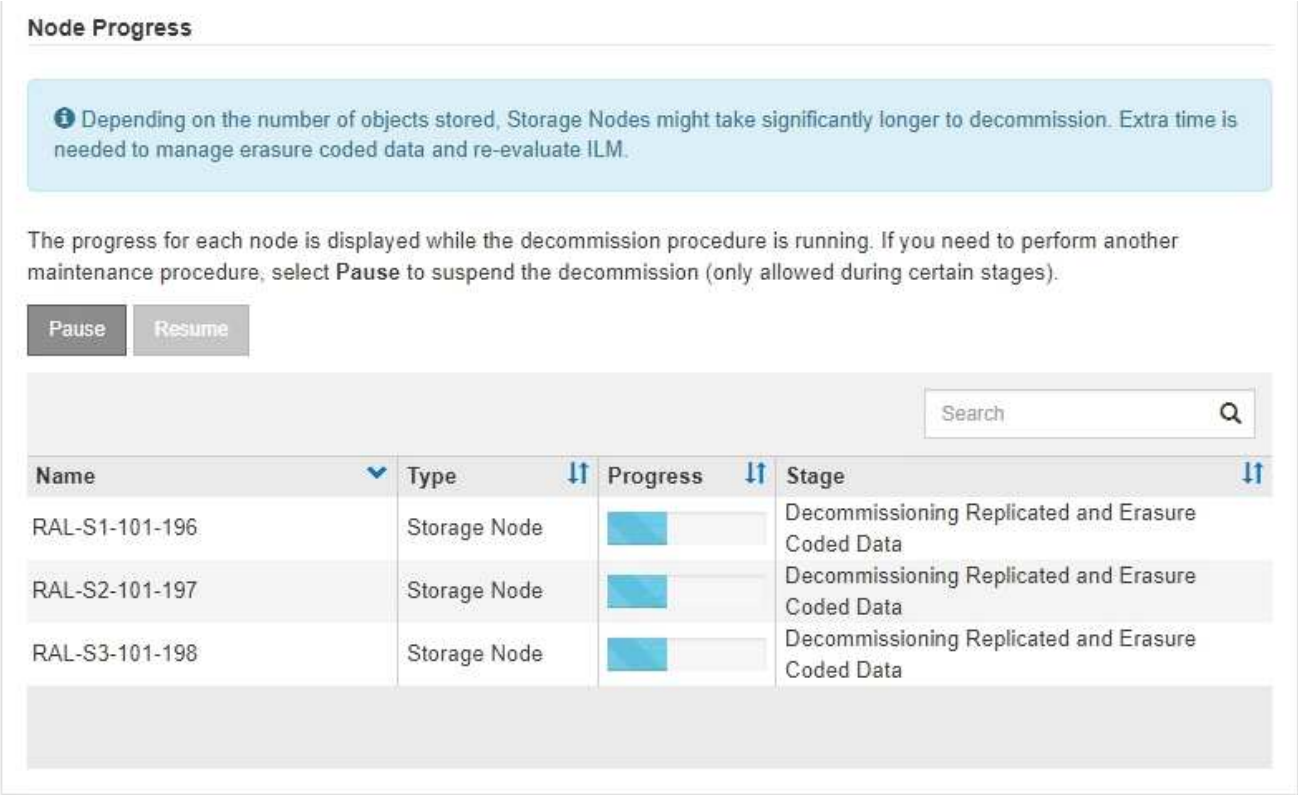
2. 使用 " 数据移动 " 图表监控对象数据从该站点到其他站点的移动情况。

在步骤 3 （修订 ILM 策略）中激活新的 ILM 策略后，数据移动开始。数据移动将在整个停用操作步骤 中进行。



3. 在页面的节点进度部分中，在删除节点时监控停用操作步骤 的进度。

删除存储节点后，每个节点将经历一系列阶段。尽管其中大多数阶段发生得很快甚至不可能发生，但根据需要移动的数据量，您可能需要等待几天甚至几周才能完成其他阶段。需要更多时间来管理经过纠删编码的数据并重新评估 ILM 。



如果您正在监控已连接站点停用的进度，请参阅此表以了解存储节点的停用阶段：

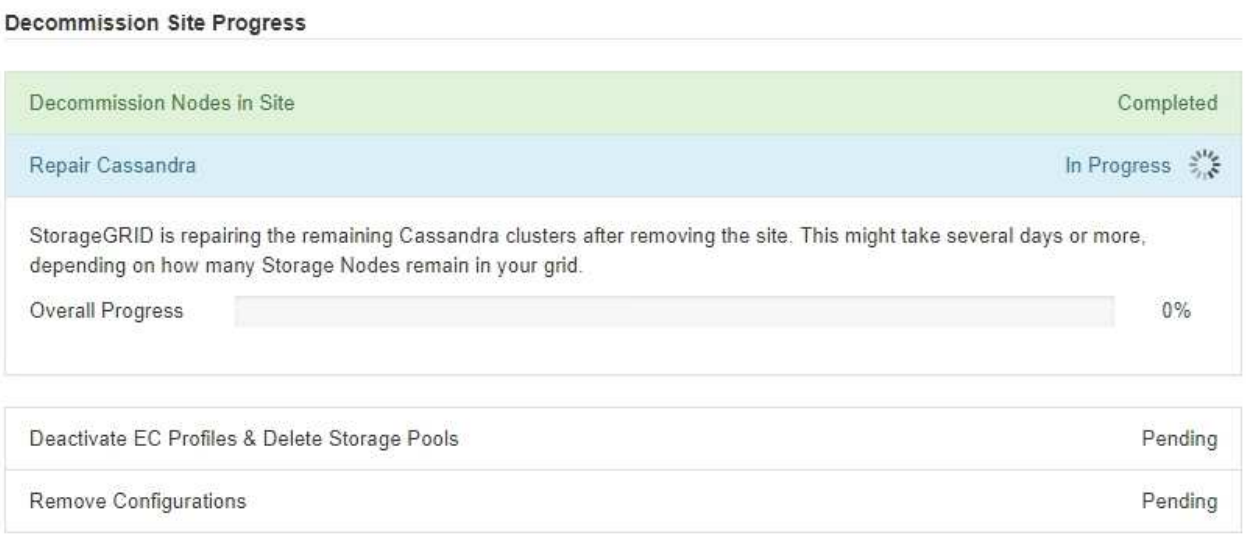
阶段	估计持续时间
待定	分钟或更短
等待锁定	minutes
准备任务	分钟或更短
将 LDR 标记为已停用	minutes
停用复制的数据和擦除编码的数据	小时，天或周，具体取决于数据量 • 注意 *： 如果您需要执行其他维护活动，可以在此阶段暂停站点停用。
LDR 设置状态	minutes
刷新审核队列	分钟到小时，具体取决于消息数量和网络延迟。

阶段	估计持续时间
完成	minutes

如果您要监控已断开连接的站点停用的进度，请参见下表以了解存储节点的停用阶段：

阶段	估计持续时间
待定	分钟或更短
等待锁定	minutes
准备任务	分钟或更短
禁用外部服务	minutes
证书撤消	minutes
节点取消注册	minutes
存储级别取消注册	minutes
删除存储组	minutes
实体删除	minutes
完成	minutes

4. 在所有节点均已达到完成阶段后，请等待其余站点停用操作完成。
   - 在 * 修复 Cassandra* 步骤中， StorageGRID 会对网格中保留的 Cassandra 集群进行任何必要的修复。这些修复可能需要几天或更长时间，具体取决于网格中剩余的存储节点数。

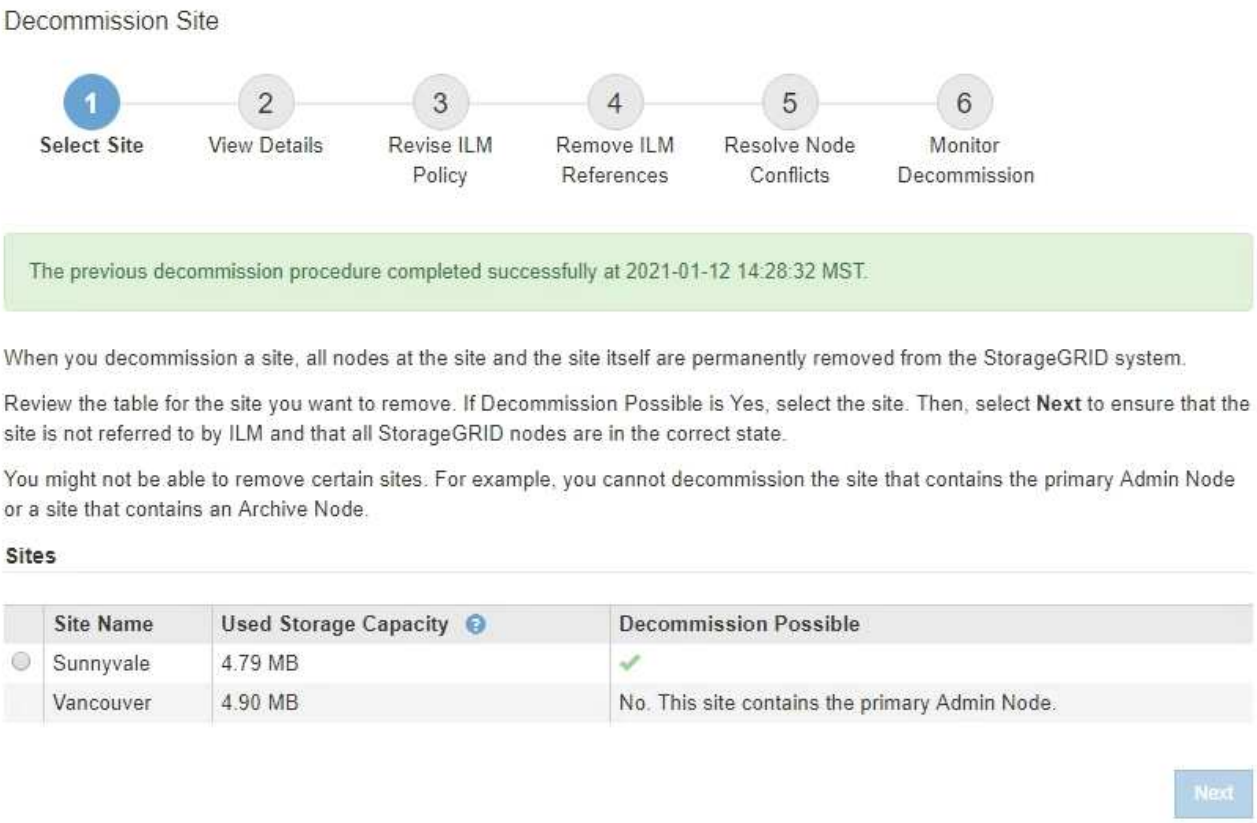


- 在 * 停用 EC 配置文件并删除存储池 * 步骤中，将进行以下 ILM 更改：
  - 引用此站点的任何擦除编码配置文件均会被停用。
  - 系统将删除引用此站点的任何存储池。

  系统默认的所有存储节点存储池也会被删除，因为它使用的是所有站点站点站点。

- 最后，在 * 删除配置 * 步骤中，对站点及其节点的任何剩余引用都将从网格的其余部分中删除。

5. 停用操作步骤 完成后， " 停用站点 " 页面将显示一条成功消息，并且不再显示已删除的站点。



完成后

完成站点停用操作步骤 后，完成以下任务：

- 确保已擦除已停用站点中所有存储节点的驱动器。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果此站点包含一个或多个管理节点，并且已为您的 StorageGRID 系统启用单点登录（ SSO ），请从 Active Directory 联合身份验证服务（ AD FS ）中删除此站点的所有依赖方信任。
- 在已连接站点停用操作步骤 期间正常关闭节点后，请删除关联的虚拟机。

网络维护过程

更新网格网络的子网

StorageGRID 会维护一个网络子网列表，用于在网格网络（ eth0 ）上的网格节点之间进行通信。这些条目包括 StorageGRID 系统中每个站点用于网格网络的子网，以及通过网格网络网关访问的 NTP ， DNS ， LDAP 或其他外部服务器所使用的任何子网。在扩展中添加网格节点或新站点时，您可能需要更新子网或向网格网络添加子网。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。

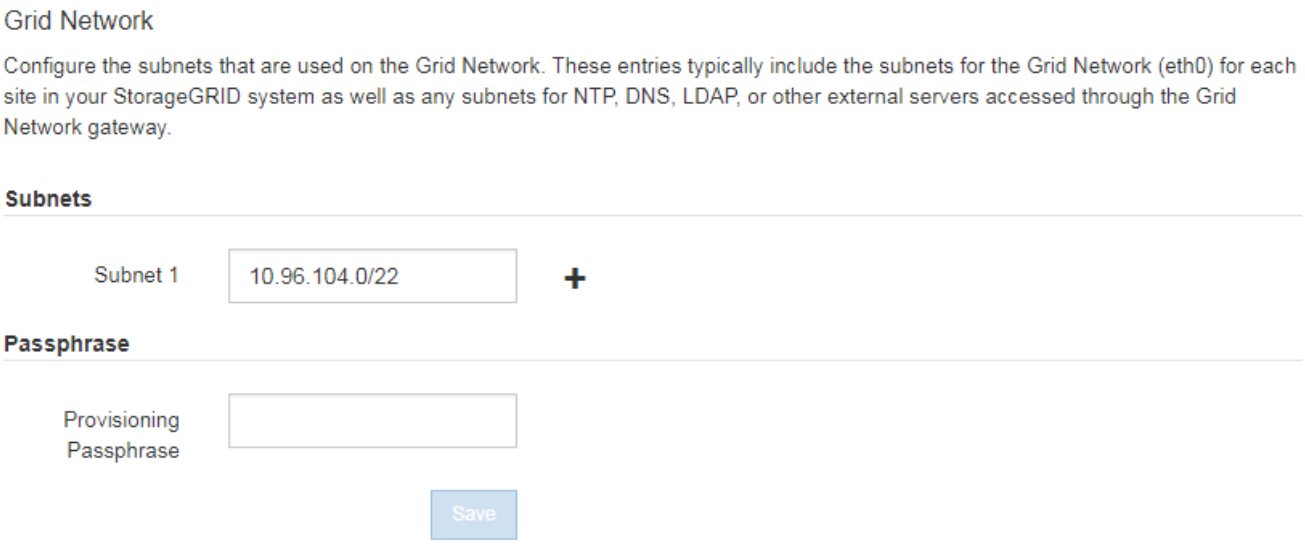
- 您必须具有要配置的子网的网络地址，以 CIDR 表示法表示。

关于此任务

如果要执行的扩展活动包括添加新子网，则必须先添加新的网格子网，然后再启动扩展操作步骤 。

步骤

1. 选择 * 维护 * > * 网络 * > * 网格网络 * 。



2. 在子网列表中，单击加号以 CIDR 表示法添加新子网。

   例如，输入 `10.96.104.0/22` 。

3. 输入配置密码短语，然后单击 * 保存 * 。

   您指定的子网将自动为 StorageGRID 系统配置。

4. 从网格管理器下载新的恢复软件包。
   a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
   b. 输入配置密码短语。

配置 **IP** 地址

您可以使用更改 IP 工具为网格节点配置 IP 地址来执行网络配置。

您必须使用更改 IP 工具对网格部署期间最初设置的网络配置进行大部分更改。使用标准 Linux 网络命令和文件进行的手动更改可能不会传播到所有 StorageGRID 服务，并且可能不会在升级，重新启动或节点恢复过程中持续存在。

如果要更改网格中所有节点的网格网络 IP 地址，请使用 适用于网格范围更改的特殊操作步骤。

如果仅更改网格网络子网列表，请使用网格管理器添加或更改网络配置。否则，如果网格管理器因网络配置问题描述 而无法访问，或者您同时执行网格网络路由更改和其他网络更改，请使用更改 IP 工具。

IP 更改操作步骤 可以是中断操作步骤 。在应用新配置之前，网格的某些部分可能不可用。

- 以太网接口 *

分配给 eth0 的 IP 地址始终是网格节点的网格网络 IP 地址。分配给 eth1 的 IP 地址始终是网格节点的管理网络 IP 地址。分配给 eth2 的 IP 地址始终是网格节点的客户端网络 IP 地址。

请注意，在某些平台上，例如 StorageGRID 设备， eth0 ， eth1 和 eth2 可能是由物理或 VLAN 接口的从属网桥或绑定组成的聚合接口。在这些平台上， * SSM* > * 资源 * 选项卡可能会显示除 eth0 ， eth1 或 eth2 之外分配给其他接口的网格，管理员和客户端网络 IP 地址。

- DHCP *

您只能在部署阶段设置 DHCP 。您不能在配置期间设置 DHCP 。如果要更改网格节点的 IP 地址，子网掩码和默认网关，则必须使用 IP 地址更改过程。使用更改 IP 工具将使发生原因 DHCP 地址变为静态地址。

- 高可用性（ HA ）组 *
- 如果客户端网络接口包含在 HA 组中，则不能将该接口的客户端网络 IP 地址更改为为 HA 组配置的子网之外的地址。
- 您不能将客户端网络 IP 地址更改为分配给客户端网络接口上配置的 HA 组的现有虚拟 IP 地址的值。
- 如果网格网络接口包含在 HA 组中，则不能将该接口的网格网络 IP 地址更改为为 HA 组配置的子网之外的地址。
- 您不能将网格网络 IP 地址更改为分配给在网格网络接口上配置的 HA 组的现有虚拟 IP 地址的值。

更改节点网络配置

您可以使用更改 IP 工具更改一个或多个节点的网络配置。您可以更改网格网络的配置，或者添加，更改或删除管理员网络或客户端网络。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

- Linux： * 如果您是首次将网格节点添加到管理网络或客户端网络，并且先前未在节点配置文件中配置 admin_network_target 或 client_network_target ，则必须立即执行此操作。

请参见适用于您的 Linux 操作系统的 StorageGRID 安装说明。

- 设备： * 在 StorageGRID 设备上，如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络，则无法仅使用更改 IP 工具添加网络。首先，您必须 将设备置于维护模式，配置链路，将设备恢复为正常运行模式，然后使用更改 IP 工具修改网络配置。有关如何配置网络链路的信息，请参见适用于您的设备的安装和维护说明中的操作步骤 。

您可以更改任何网络上一个或多个节点的 IP 地址，子网掩码，网关或 MTU 值。

您还可以从客户端网络或管理网络添加或删除节点：

- 您可以通过向客户端网络或管理网络添加节点上的 IP 地址 / 子网掩码来将该节点添加到该节点。
- 您可以通过删除客户端网络或管理网络中某个节点的 IP 地址 / 子网掩码来从该网络中删除该节点。

  无法从网格网络中删除节点。

> 不允许使用 IP 地址交换。如果必须在网格节点之间交换 IP 地址，则必须使用临时中间 IP 地址。

> 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且您要更改管理节点的 IP 地址，请注意，使用管理节点的 IP 地址（而不是建议的完全限定域名）配置的任何依赖方信任都将无效。您将无法再登录到此节点。更改 IP 地址后，您必须立即使用新的 IP 地址更新或重新配置 Active Directory 联合身份验证服务（ AD FS ）中节点的依赖方信任。请参见有关管理 StorageGRID 的说明。

> 使用更改 IP 工具对网络所做的任何更改都会传播到 StorageGRID 设备的安装程序固件。这样，如果在设备上重新安装 StorageGRID 软件，或者将设备置于维护模式，则网络配置将正确无误。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 输入以下命令以启动更改 IP 工具： `change-ip`
3. 在提示符处输入配置密码短语。

   此时将显示主菜单。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. 也可以选择 * 1 * 来选择要更新的节点。然后选择以下选项之一：

- * 1 *： 单节点—按名称选择
- * 2 *： 单节点—按站点选择，然后按名称选择
- **3**： 单节点—按当前 IP 选择
- **4**： 站点上的所有节点
- **5**： 网格中的所有节点
  - 注： * 如果要更新所有节点，请允许 " 全部 " 保持选中状态。

选择后，将显示主菜单，并更新 * 选定节点 * 字段以反映您的选择。所有后续操作仅在显示的节点上执行。

5. 在主菜单上，选择选项 * 2 * 以编辑选定节点的 IP/ 掩码，网关和 MTU 信息。
   a. 选择要更改的网络：
      - * 1 *： 网格网络
      - * 2 *： 管理网络
      - * 3 *： 客户端网络
      - **4**： 选择所有网络后，提示符将显示节点名称，网络名称（网格，管理员或客户端），数据类型（ IP/ 掩码， 网关或 MTU ）和当前值。

        编辑 DHCP 配置接口的 IP 地址，前缀长度，网关或 MTU 将使接口更改为静态。如果选择更改由 DHCP 配置的接口，则会显示一条警告，通知您该接口将更改为静态。

      无法编辑配置为 `FIXED` 的接口。

   b. 要设置新值，请按当前值所示格式输入该值。
   c. 要保持当前值不变，请按 * 输入 * 。
   d. 如果数据类型为 `IP/ 掩码` ，则可以输入 * d* 或 * 。 0.0.0.0/0* 从节点中删除管理员网络或客户端网络。
   e. 编辑要更改的所有节点后，输入 * 。 q* 返回主菜单。

      您所做的更改将一直保留，直到清除或应用为止。

6. 选择以下选项之一，查看您所做的更改：
   - * 5*： 显示输出中的编辑内容，这些编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如示例输出所示：

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

- * 6 *： 显示输出中显示的编辑内容，其中显示了完整配置。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。正确显示取决于您的终端客户端是否支持必要的 VT100 转义序列。

7. 选择选项 * 7* 以验证所有更改。

   此验证可确保不会违反网格，管理和客户端网络的规则，例如不使用重叠的子网。

   在此示例中，验证返回错误。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   在此示例中，验证已通过。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. 验证通过后，请选择以下选项之一：

- **8**：保存未应用的更改。

  使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

- * 。 10*：应用新网络配置。

9. 如果选择了选项 * 。 10* ，请选择以下选项之一：

   - * 应用 *：立即应用更改，并在必要时自动重新启动每个节点。

     如果新网络配置不需要更改任何物理网络连接，您可以选择 * 应用 * 以立即应用更改。如果需要，节点将自动重新启动。此时将显示需要重新启动的节点。

   - * 阶段 *：下次手动重新启动节点时应用更改。

     如果要使新网络配置正常运行，需要更改物理或虚拟网络配置，则必须使用 * 阶段 * 选项，关闭受影响的节点，进行必要的物理网络更改并重新启动受影响的节点。如果选择 * 应用 * 而未先进行这些网络更改，则更改通常会失败。

     如果使用 * 阶段 * 选项，则必须在暂存后尽快重新启动节点，以最大程度地减少中断。

   - * 取消 *：此时不要更改任何网络。

     如果您不知道建议的更改需要重新启动节点，则可以推迟更改以最大限度地减少对用户的影响。选择 * 取消 * 将返回到主菜单并保留所做的更改，以便稍后应用。

     如果选择 * 应用 * 或 * 阶段 * ，则会生成一个新的网络配置文件，并执行配置，同时会使用新的工作信息更新节点。

     在配置期间，输出将在应用更新时显示状态。

     ```
     Generating new grid networking description file...

     Running provisioning...

     Updating grid network configuration on Name
     ```

   应用或暂存更改后，由于网格配置更改，系统将生成新的恢复软件包。

10. 如果选择了 * 阶段 * ，请在配置完成后按照以下步骤进行操作：

    a. 根据需要进行物理或虚拟网络更改。

       - 物理网络更改 *：进行必要的物理网络更改，必要时安全关闭节点。
       - Linux *：如果您是首次将节点添加到管理网络或客户端网络，请确保已按照 "`将接口添加到现有节点 " 中所述添加接口。`

    b. 重新启动受影响的节点。

11. 完成更改后，选择 * 。 0* 退出更改 IP 工具。

12. 从网格管理器下载新的恢复软件包。

a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
b. 输入配置密码短语。

相关信息

Linux ：向现有节点添加接口

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

管理 StorageGRID

配置 IP 地址

在管理网络上添加或更改子网列表

您可以在管理网络子网列表中添加，删除或更改一个或多个节点的子网。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

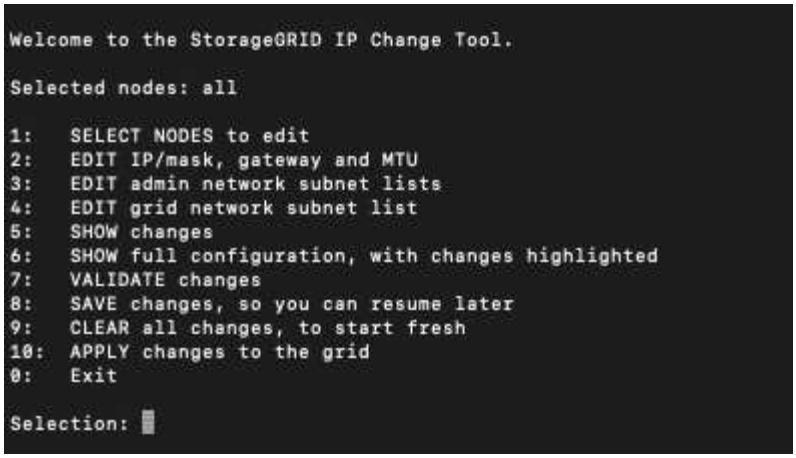
您可以为管理网络子网列表中的所有节点添加，删除或更改子网。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root ： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 输入以下命令以启动更改 IP 工具： `change-ip`
3. 在提示符处输入配置密码短语。

   此时将显示主菜单。



4. 或者，也可以限制执行操作的网络 / 节点。选择以下选项之一：
   - 如果要筛选要执行操作的特定节点，请选择 * 1 * 以选择要编辑的节点。选择以下选项之一：
     - * 1 * ：单个节点（按名称选择）
     - * 2 * ：单个节点（按站点选择，然后按名称选择）
     - * 3 * ：单个节点（由当前 IP 选择）
     - **4** ：站点上的所有节点
     - **5** ：网格中的所有节点
     - **0** ：返回
   - 允许 "`所有` " 保持选中状态。进行选择后，将显示主菜单屏幕。选定节点字段反映了您的新选择，现在，选定的所有操作将仅对此项执行。
5. 在主菜单上，选择用于编辑管理网络子网的选项（选项 * 3 * ）。
6. 选择以下选项之一：
   - 输入以下命令添加子网： `add CIDR`
   - 输入以下命令删除子网： `del CIDR`
   - 输入以下命令设置子网列表： `set CIDR`

   对于所有命令，您可以使用以下格式输入多个地址： `add CIDR , CIDR`

   示例： `add 172.14.0.0/16 , 172.15.0.0/16 , 172.16.0.0/16`

   您可以使用 "`向上箭头` " 将先前键入的值调用到当前输入提示符，然后根据需要对其进行编辑，从而减少所需的键入量。

   以下示例输入显示了如何向管理网络子网列表添加子网：

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. 准备好后，输入 * 。 q* 可返回主菜单屏幕。您所做的更改将一直保留，直到清除或应用为止。

> 如果您在步骤 2 中选择了任何 " 全部 " 节点选择模式，则必须按 * 输入 * （不带 * q* ）才能访问列表中的下一个节点。

8. 选择以下选项之一：

   - 选择选项 * 5* 可显示输出中的编辑内容，而输出中的编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如以下示例输出所示：

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - 选择选项 **6** 可在显示完整配置的输出中显示编辑内容。更改将以绿色（添加项）或红色（删除项）突出显示。* 注： * 某些终端模拟器可能会使用删除线格式显示添加和删除内容。

     尝试更改子网列表时，将显示以下消息：

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

如果您未明确将 NTP 和 DNS 服务器子网分配给网络，则 StorageGRID 会自动为此连接创建一个主机路由（ /32 ）。例如，如果您希望使用 /16 或 /24 路由与 DNS 或 NTP 服务器建立出站连接，则应删除自动创建的 /32 路由并添加所需的路由。如果不删除自动创建的主机路由，则在对子网列表进行任何更改后，此路由将保留。

> 虽然您可以使用这些自动发现的主机路由，但通常应手动配置 DNS 和 NTP 路由以确保连接。

9. 选择选项 * 7* 以验证所有暂存更改。

   此验证可确保遵循网格网络，管理网络和客户端网络的规则，例如使用重叠的子网。

10. （可选）选择选项 * 8* 保存所有分阶段更改，稍后返回以继续进行更改。

    使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

11. 执行以下操作之一：
    - 如果要在不保存或应用新网络配置的情况下清除所有更改，请选择选项 * 。
    - 如果您已准备好应用更改并配置新的网络配置，请选择选项 * 。在配置期间，输出将在应用更新时显示状态，如以下示例输出所示：

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

12. 从网格管理器下载新的恢复软件包。
    a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
    b. 输入配置密码短语。

相关信息

配置 IP 地址

您可以使用更改 IP 工具在网格网络上添加或更改子网。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

您可以在网格网络子网列表中添加，删除或更改子网。更改将影响网格中所有节点上的路由。

> 如果仅更改网格网络子网列表，请使用网格管理器添加或更改网络配置。否则，如果网格管理器因网络配置问题描述 而无法访问，或者您同时执行网格网络路由更改和其他网络更改，请使用更改 IP 工具。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 输入以下命令以启动更改 IP 工具： `change-ip`
3. 在提示符处输入配置密码短语。

   此时将显示主菜单。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. 在主菜单上，选择用于编辑网格网络子网的选项（选项 * 4* ）。

   > 对网格网络子网列表所做的更改在网格范围内进行。

5. 选择以下选项之一：
   - 输入以下命令添加子网： `add CIDR`

- 输入以下命令删除子网： `del CIDR`
- 输入以下命令设置子网列表： `set CIDR`

> 对于所有命令，您可以使用以下格式输入多个地址： `add CIDR ， CIDR`

示例： `add 172.14.0.0/16 ， 172.15.0.0/16 ， 172.16.0.0/16`

> 您可以使用 "`向上箭头` " 将先前键入的值调用到当前输入提示符，然后根据需要对其进行编辑，从而减少所需的键入量。

以下示例输入显示了为网格网络子网列表设置子网：

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. 准备好后，输入 * 。 q* 可返回主菜单屏幕。您所做的更改将一直保留，直到清除或应用为止。
7. 选择以下选项之一：
   - 选择选项 * 5* 可显示输出中的编辑内容，而输出中的编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如以下示例输出所示：

```
================================================================================
Grid Network Subnet List (GNSL)
================================================================================
                                                    add 172.30.0.0/21
                                                    add 172.31.0.0/21
                                                    del 172.16.0.0/21
                                                    del 172.17.0.0/21
                                                    del 172.18.0.0/21
                              [      172.30.0.0/21 ]
                              [      172.31.0.0/21 ]
                              [     192.168.0.0/21 ]
Press Enter to continue
```

   - 选择选项 **6** 可在显示完整配置的输出中显示编辑内容。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。

8. 选择选项 * 7* 以验证所有暂存更改。

   此验证可确保遵循网格网络，管理网络和客户端网络的规则，例如使用重叠的子网。

9. （可选）选择选项 * 8* 保存所有分阶段更改，稍后返回以继续进行更改。

   使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

10. 执行以下操作之一：

    - 如果要在不保存或应用新网络配置的情况下清除所有更改，请选择选项 * 。
    - 如果您已准备好应用更改并配置新的网络配置，请选择选项 * 。在配置期间，输出将在应用更新时显示状态，如以下示例输出所示：

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

11. 如果在更改网格网络时选择了选项 * 。 10 ，请选择以下选项之一：

    - * 应用 * ： 立即应用更改，并在必要时自动重新启动每个节点。

      如果新网络配置将与旧网络配置同时运行而不进行任何外部更改，则可以使用 * 应用 * 选项进行完全自动化的配置更改。

    - * 阶段 * ： 下次重新启动节点时应用更改。

      如果要使新网络配置正常运行，需要更改物理或虚拟网络配置，则必须使用 * 阶段 * 选项，关闭受影响的节点，进行必要的物理网络更改并重新启动受影响的节点。

      > 如果使用 * 阶段 * 选项，则必须在暂存后尽快重新启动节点，以最大程度地减少中断。

    - * 取消 * ： 此时不要更改任何网络。

      如果您不知道建议的更改需要重新启动节点，则可以推迟更改以最大限度地减少对用户的影响。选择 * 取消 * 将返回到主菜单并保留所做的更改，以便稍后应用。

    应用或暂存更改后，由于网格配置更改，系统将生成新的恢复软件包。

12. 如果配置因错误而停止，则可以使用以下选项：

    - 要中止 IP 更改操作步骤 并返回主菜单，请输入 * A* 。
    - 要重试失败的操作，请输入 * 。
    - 要继续执行下一个操作，请输入 * c* 。

      稍后可以从主菜单中选择选项 * 10 * （应用更改）重试失败的操作。只有成功完成所有操作后， IP 更改操作步骤 才会完成。

- 如果您必须手动干预（例如重新启动节点），并确信工具认为失败的操作已实际成功完成，请输入 * f* 将其标记为成功并移至下一操作。

13. 从网格管理器下载新的恢复软件包。

    a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。

    b. 输入配置密码短语。

> 恢复包文件必须受到保护，因为它包含可用于从 StorageGRID 系统获取数据的加密密钥和密码。

相关信息

配置 IP 地址

更改网格中所有节点的 **IP** 地址

如果需要更改网格中所有节点的网格网络 IP 地址，则必须遵循此专用操作步骤 。您不能使用操作步骤 更改单个节点来更改网格范围的网格网络 IP 。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

要确保网格成功启动，您必须一次性完成所有更改。

> 此 操作步骤 适用场景 仅适用于网格网络。您不能使用此操作步骤 更改管理员网络或客户端网络上的 IP 地址。

如果要仅更改一个站点上节点的 IP 地址和 MTU ，请按照执行操作 更改节点网络配置 说明。

步骤

1. 提前规划需要在更改 IP 工具之外进行的更改，例如更改 DNS 或 NTP 以及更改单点登录（ Single Sign-On ， SSO ）配置（如果使用）。

> 如果现有 NTP 服务器无法通过新 IP 地址访问网格，请在执行 change-IP 操作步骤 之前添加新的 NTP 服务器。

> 如果现有 DNS 服务器无法通过新 IP 地址访问网格，请在执行 change-IP 操作步骤 之前添加新的 DNS 服务器。

> 如果为 StorageGRID 系统启用了 SSO ，并且任何依赖方信任均使用管理节点 IP 地址（而不是建议的完全限定域名）进行配置，请准备在 Active Directory 联合身份验证服务（ AD FS ）中更新或重新配置这些依赖方信任 更改 IP 地址后立即执行。请参见有关管理 StorageGRID 的说明。

> 如有必要，请为新 IP 地址添加新子网。

2. 登录到主管理节点：

a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

3. 输入以下命令以启动更改 IP 工具： `change-ip`

4. 在提示符处输入配置密码短语。

此时将显示主菜单。默认情况下， `SElected nodes` 字段设置为 `All` 。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. 在主菜单上，选择 * 。 2* 以编辑所有节点的 IP/ 子网掩码，网关和 MTU 信息。

a. 选择 * 1 * 以更改网格网络。

选择后，提示符将显示节点名称，网格网络名称，数据类型（ IP/ 掩码，网关或 MTU ）， 和当前值。

编辑 DHCP 配置接口的 IP 地址，前缀长度，网关或 MTU 将使接口更改为静态。在 DHCP 配置每个接口之前，系统会显示一条警告。

无法编辑配置为 `FIXED` 的接口。

a. 要设置新值，请按当前值所示格式输入该值。

b. 编辑要更改的所有节点后，输入 * 。 q* 返回主菜单。

您所做的更改将一直保留，直到清除或应用为止。

6. 选择以下选项之一，查看您所做的更改：

◦ * 5* ：显示输出中的编辑内容，这些编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如示例输出所示：

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [        10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

- * 6 *： 显示输出中显示的编辑内容，其中显示了完整配置。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。正确显示取决于您的终端客户端是否支持必要的 VT100 转义序列。

7. 选择选项 * 7* 以验证所有更改。

   此验证可确保不会违反网格网络的规则，例如不使用重叠的子网。

   在此示例中，验证返回错误。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   在此示例中，验证已通过。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. 验证通过后，选择 * 。 10* 以应用新的网络配置。

9. 选择 * 阶段 * ，以便在下次重新启动节点时应用更改。

> 必须选择 * 阶段 * 。请勿手动或通过选择 * 应用 * 而不是 * 阶段 * 来执行滚动重新启动；网格将无法成功启动。

10. 完成更改后，选择 * 。 0* 退出更改 IP 工具。
11. 同时关闭所有节点。

> 必须一次性关闭整个网格，以便所有节点同时关闭。

12. 根据需要进行物理或虚拟网络更改。
13. 验证所有网格节点是否均已关闭。
14. 打开所有节点的电源。
15. 成功启动网格后：
    a. 如果添加了新的 NTP 服务器，请删除旧的 NTP 服务器值。
    b. 如果添加了新的 DNS 服务器，请删除旧的 DNS 服务器值。
16. 从网格管理器下载新的恢复软件包。
    a. 选择 * 维护 * > * 系统 * > * 恢复软件包 * 。
    b. 输入配置密码短语。

相关信息

管理 StorageGRID

在网格网络上添加或更改子网列表

关闭网格节点

向现有节点添加接口

Linux： 将管理员或客户端接口添加到现有节点

按照以下步骤将管理网络或客户端网络上的接口添加到安装后的 Linux 节点中。

如果在安装期间未在 Linux 主机上的节点配置文件中配置 admin_network_target 或 client_network_target ，请使用此操作步骤 添加接口。有关节点配置文件的详细信息，请参见适用于 Linux 操作系统的说明：

- 安装 Red Hat Enterprise Linux 或 CentOS
- 安装 Ubuntu 或 Debian

您可以在托管需要新网络分配的节点的 Linux 服务器上执行此操作步骤 ，而不是在节点内部执行。此操作步骤仅会将接口添加到节点；如果您尝试指定任何其他网络参数，则会发生验证错误。

要提供地址信息，必须使用更改 IP 工具。请参见 更改节点网络配置。

步骤

1. 登录到托管此节点的 Linux 服务器。
2. 编辑节点配置文件： ` /etc/storagegRid/nodes/*node-name*.conf` 。

   请勿指定任何其他网络参数，否则将导致验证错误。

   a. 为新网络目标添加一个条目。例如：

      ```
      client_network_target = bond0.3206
      ```

   b. 可选：为 MAC 地址添加一个条目。例如：

      ```
      client_network_MAC = aa ： 57 ： 61 ： 07 ： ea ： 5c
      ```

3. 运行 node validate 命令：

   ```
   sUdo StorageGRID node validate node-name
   ```

4. 解决所有验证错误。
5. 运行 node reload 命令：

   ```
   sUdo StorageGRID node reload node-name
   ```

Linux： 向节点添加中继或访问接口

安装 Linux 节点后，您可以向该节点添加额外的中继或访问接口。添加的接口将显示在 VLAN 接口页面和 HA 组页面上。

您需要的内容

- 您可以访问有关在 Linux 平台上安装 StorageGRID 的说明。
  - 安装 Red Hat Enterprise Linux 或 CentOS
  - 安装 Ubuntu 或 Debian
- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

在软件升级，恢复操作步骤 或扩展操作步骤 处于活动状态时，请勿尝试向节点添加接口。

关于此任务

安装完 Linux 节点后，请按照以下步骤向该节点添加一个或多个额外的接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。

添加接口时，节点暂时不可用。您应一次在一个节点上执行此操作步骤 。

步骤

1. 登录到托管此节点的 Linux 服务器。
2. 使用 vim 或 pico 等文本编辑器编辑节点配置文件：

   ` /etc/storaggrid/nodes/*node-name*.conf`

3. 向文件中添加一个条目，以指定要添加到节点的每个额外接口的名称以及问题描述 （可选）。请使用此格式。

   ```
   interfaces_target_nnn=value
   ```

   对于 *nnnn* ，请为要添加的每个 `interfaces_target` 条目指定一个唯一编号。

   对于 *value* ，指定裸机主机上物理接口的名称。然后，也可以添加一个逗号并提供接口的问题描述 ，该接口将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。

   例如：

   ```
   interfaces_target_01=ens256 ，中继
   ```

   请勿指定任何其他网络参数，否则将导致验证错误。

4. 运行以下命令以验证对节点配置文件所做的更改：

   ```
   sUdo StorageGRID node validate node-name
   ```

   解决所有错误或警告，然后再继续下一步。

5. 运行以下命令以更新节点的配置：

   ```
   sUdo StorageGRID node reload node-name
   ```

完成后

- 如果添加了一个或多个中继接口，请转到 配置 VLAN 接口 为每个新的父接口配置一个或多个 VLAN 接口。
- 如果添加了一个或多个访问接口，请转到 配置高可用性组 将新接口直接添加到 HA 组。

VMware： 向节点添加中继或访问接口

您可以在安装 VM 节点后向该节点添加中继或访问接口。添加的接口将显示在 VLAN 接口页面和 HA 组页面上。

您需要的内容

- 您可以访问有关在 VMware 平台上安装 StorageGRID 的说明。

安装 VMware

- 您已配置 StorageGRID 11.6.
- 您拥有管理节点和网关节点 VMware 虚拟机。
- 您的网络子网未用作网格，管理员或客户端网络。

- 您已有 `passwords.txt` 文件。
- 您具有特定的访问权限。

> 在软件升级，恢复操作步骤 或扩展操作步骤 处于活动状态时，请勿尝试向节点添加接口。

关于此任务

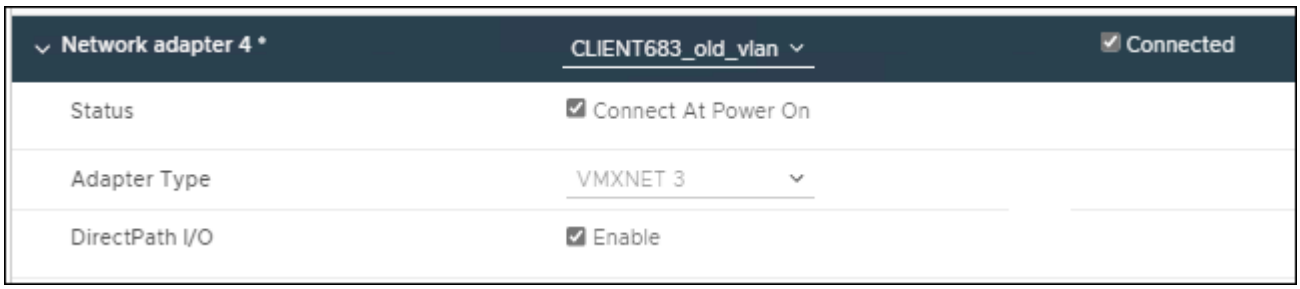
安装 VMware 节点后，请按照以下步骤向该节点添加一个或多个额外接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口，则可以将该接口直接添加到 HA 组；而无需配置 VLAN 接口。

添加接口时，节点可能会暂时不可用。

步骤

1. 在 vCenter 中，向管理节点和网关节点虚拟机添加新的网络适配器（类型为 VMXNET3 ）。选中 * 已连接 * 和 * 在启动时连接 * 复选框。



2. 使用 SSH 登录到管理节点或网关节点。
3. 使用 `ip link show` 确认检测到新的网络接口 ens256 。

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

完成后

- 如果添加了一个或多个中继接口，请转到 配置 VLAN 接口 为每个新的父接口配置一个或多个 VLAN 接口。
- 如果添加了一个或多个访问接口，请转到 配置高可用性组 将新接口直接添加到 HA 组。

配置 **DNS** 服务器

您可以添加，删除和更新域名系统（ DNS ）服务器，以便使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有要配置的 DNS 服务器的 IP 地址。

通过指定 DNS 服务器信息，您可以对电子邮件或 SNMP 通知和 AutoSupport 使用完全限定域名（ FQDN ）主机名，而不是 IP 地址。建议至少指定两个 DNS 服务器。

> 为 DNS 服务器提供 2 到 6 个 IP 地址。通常，选择每个站点在发生网络隔离时可在本地访问的 DNS 服务器。这是为了确保已隔离的站点可以继续访问 DNS 服务。配置网格范围的 DNS 服务器列表后，您可以 进一步自定义每个节点的 DNS 服务器列表。

如果省略 DNS 服务器信息或 DNS 服务器信息配置不正确，则会在每个网格节点的 SSM 服务上触发 DNST 警报。如果 DNS 配置正确且新服务器信息已到达所有网格节点，则警报将清除。

步骤

1. 选择 * 维护 * > * 网络 * > * DNS 服务器 * 。
2. 在服务器部分中，根据需要添加更新或删除 DNS 服务器条目。

   最佳做法是，每个站点至少指定两个 DNS 服务器。最多可以指定六个 DNS 服务器。

3. 单击 * 保存 * 。

修改单网格节点的 **DNS** 配置

您可以运行一个脚本，为每个网格节点配置不同的 DNS ，而不是在整个部署中全局配置域名系统（ Domain Name System ， DNS ）。

通常，您应使用网格管理器上的 * 维护 * > * 网络 * > * DNS 服务器 * 选项来配置 DNS 服务器。只有在需要为不同网格节点使用不同 DNS 服务器时，才可使用以下脚本。

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root ： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 `$` 更改为 `#` 。

e. 将 SSH 专用密钥添加到 SSH 代理。输入： `ssh-add`

f. 输入 `passwords.txt` 文件中列出的 SSH 访问密码。

2. 【登录到要使用自定义 DNS 配置更新的节点： `ssh node_ip_address`

3. 运行 DNS 设置脚本： `setup_resolv.rb` 。

此脚本将以支持的命令列表进行响应。

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. 添加为网络提供域名服务的服务器的 IPv4 地址： `add <nameserver IP_address>`

5. 重复 `add nameserver` 命令以添加名称服务器。
6. 按照提示输入其他命令时的说明进行操作。
7. 保存所做的更改并退出应用程序： `save`
8. 关闭服务器上的命令 Shell： `exit`
9. 对于每个网格节点，重复中的步骤 登录到节点 到 关闭命令 Shell。
10. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入： `ssh-add -D`

配置 **NTP** 服务器

您可以添加，更新或删除网络时间协议（ Network Time Protocol ， NTP ）服务器，以确保 StorageGRID 系统中的网格节点之间准确同步数据。

您需要的内容

- 您必须使用登录到网格管理器 支持的 Web 浏览器。
- 您必须具有维护或根访问权限。
- 您必须具有配置密码短语。
- 您必须具有要配置的 NTP 服务器的 IPv4 地址。

关于此任务

StorageGRID 系统使用网络时间协议（ NTP ）来同步网格中所有网格节点之间的时间。

在每个站点上，至少会为 StorageGRID 系统中的两个节点分配主 NTP 角色。它们会同步到建议的至少四个外部时间源，最多六个外部时间源以及彼此之间。StorageGRID 系统中不是主 NTP 节点的每个节点都充当 NTP 客户端，并与这些主 NTP 节点同步。

外部 NTP 服务器连接到先前已为其分配主 NTP 角色的节点。因此，建议至少指定两个具有主 NTP 角色的节点。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

指定的外部 NTP 服务器必须使用 NTP 协议。您必须指定 Stratum 3 或更高的 NTP 服务器引用，以防止出现时间偏差问题。

> 在为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows 时间（ W32Time ）服务。早期版本的 Windows 上的时间服务不够准确， Microsoft 不支持在 StorageGRID 等高精度环境中使用。

"支持边界，用于为高精度环境配置 Windows 时间服务"

如果您遇到安装期间最初指定的 NTP 服务器的稳定性或可用性问题，可以通过添加其他服务器或更新或删除现有服务器来更新 StorageGRID 系统使用的外部 NTP 源列表。

步骤

1. 选择 * 维护 * > * 网络 * > * NTP 服务器 * 。

2. 在服务器部分中，根据需要添加更新或删除 NTP 服务器条目。

   您应至少包含 4 个 NTP 服务器，并且最多可以指定 6 个服务器。

3. 在 * 配置密码短语 * 文本框中，输入 StorageGRID 系统的配置密码短语，然后单击 * 保存 * 。

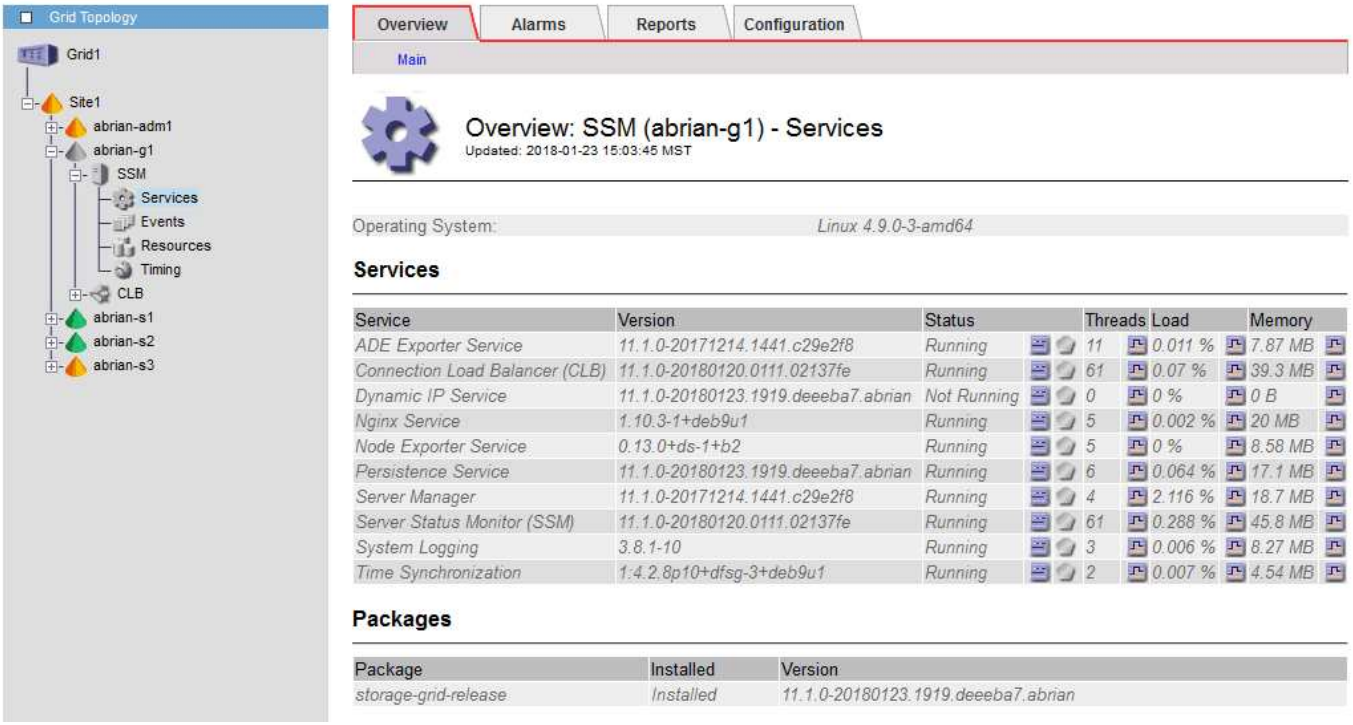
   操作步骤 的状态显示在页面顶部。在配置更新完成之前，此页面将处于禁用状态。

   如果在保存新 NTP 服务器后所有 NTP 服务器均未通过连接测试，请勿继续。请联系技术支持。

恢复隔离节点的网络连接

在某些情况下，例如站点范围或网格范围的 IP 地址更改，一组或多组节点可能无法与网格的其余部分联系。

在网格管理器（ * 支持 * > * 工具 * > * 网格拓扑 * ）中，如果某个节点为灰色，或者某个节点为蓝色，其许多服务显示的状态不是 " 正在运行 " ，则应检查节点隔离情况。



隔离节点会产生以下后果：

- 如果隔离了多个节点，您可能无法登录或访问网格管理器。
- 如果隔离了多个节点，则租户管理器的信息板上显示的存储使用量和配额值可能已过时。恢复网络连接后，总数将更新。

要解决隔离问题描述 ，您可以在与网格隔离的每个隔离节点或组中的一个节点（子网中不包含主管理节点的所有节点）上运行命令行实用程序。该实用程序可为节点提供网格中非隔离节点的 IP 地址，从而使隔离的节点或节点组能够再次访问整个网格。

如果在网络中禁用了多播域名系统（ mDNS ），则可能需要在每个隔离节点上运行命令行实用程序。

1. 访问此节点并检查 ` /var/local/log/dynip.log` 中是否存在隔离消息。

   例如：

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action may be required.
   ```

   如果您使用的是 VMware 控制台，则它将包含一条消息，指出此节点可能已隔离。

   在 Linux 部署中，隔离消息将显示在 ` /var/log/storagegrid/node/<nodename>.log` 文件中。

2. 如果隔离消息重复出现且持久，请运行以下命令：

   `add_node_ip.py < 地址 >`

   其中 ` < 地址 >` 是连接到网格的远程节点的 IP 地址。

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. 验证先前隔离的每个节点的以下情况：
   - 节点的服务已启动。
   - 运行 `storagegRid-status` 命令后，动态 IP 服务的状态为 "`running` " 。
   - 在网格拓扑树中，节点不再显示为与网格其余部分断开连接。

如果运行 `add_node_ip.py` 命令无法解决此问题，则可能还有其他网络问题需要解决。

主机级别和中间件过程

某些维护过程专用于 StorageGRID 的 Linux 或 VMware 部署，或者专用于 StorageGRID 解决方案 的其他组件。

Linux： 将网格节点迁移到新主机

您可以将 StorageGRID 节点从一台 Linux 主机迁移到另一台 Linux 主机以执行主机维护（例如操作系统修补和重新启动），而不会影响网格的功能或可用性。

您将一个或多个节点从一个 Linux 主机（" s源主机 "）迁移到另一个 Linux 主机（"`目标主机` "）。目标主机必须事先已准备好供 StorageGRID 使用。

只有在您计划的 StorageGRID 部署包含迁移支持时，才能使用此操作步骤 。

要将网格节点迁移到新主机，必须满足以下两个条件：

- 共享存储用于所有每个节点的存储卷
- 网络接口在主机之间的名称一致

在生产部署中，请勿在一台主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

可以在同一主机上部署其他类型的节点，例如管理节点或网关节点。但是，如果您有多个相同类型的节点（例如两个网关节点），请勿将所有实例安装在同一主机上。

有关详细信息，请参见适用于 Linux 操作系统的 StorageGRID 安装说明中的 "`节点迁移要求` " 。

相关信息

部署新的 Linux 主机

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

Linux： 从源主机导出节点

关闭网格节点并将其从源 Linux 主机导出。

在源 Linux 主机上运行以下命令。

1. 获取源主机上当前正在运行的所有节点的状态。

```
sudo storagegrid node status all
```

名称 `Config-State Run-State`

`dC1-ADM1` 配置为运行

`dC1-ARC1` 已配置为运行

`dC1-GW1` 已配置为运行

`dC1-S1` 已配置为运行

`dC1-S2` 配置为运行

`dC1-S3` 已配置为运行

2. 确定要迁移的节点的名称，如果其运行状态为 `running` ，则将其停止。

```
sudo storagegrid node stop DC1-S3
```

s顶部节点 `DC1-S3`

等待长达 `630` 秒以关闭节点

3. 从源主机导出节点。

```
sudo storagegrid node export DC1-S3
```

已将节点 `DC1-S3` 导出到 `/dev/mapper/sgws-DC1-s3-var-local` 。

如果您，请使用 StorageGRID 节点导入 /dev/mapper/sgws-DC1-s3-var-local

希望重新导入。

4. 记下 `export` 命令输出中建议的 `import 命令。

您将在下一步的目标主机上运行此命令。

Linux：目标主机上的导入节点

从源主机导出节点后，您可以在目标 Linux 主机上导入并验证此节点。验证可确认节点可以访问与源主机上相同的块存储和网络接口设备。

在目标 Linux 主机上运行以下命令。

1. 在目标主机上导入节点。

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

已从 `/dev/mapper/sgws-DC1-s3-var-local` 导入节点 `DC1-S3` 。

您应运行 `StorageGRID node validate DC1-s3"`

2. 验证新主机上的节点配置。

```
sudo storagegrid node validate DC1-S3
```

` + 确认节点 DC1-S3 存在 … 已通过 +`

` + 检查节点 DC1-S3 的配置文件 /etc/storaggrid/nodes/DC1-s3.conf … 已通过 +`

` + 检查唯一值是否重复 … 已通过 +`

3. 如果发生任何验证错误，请在启动迁移的节点之前解决这些错误。

   有关故障排除信息，请参见适用于 Linux 操作系统的 StorageGRID 安装说明。

相关信息

安装 Red Hat Enterprise Linux 或 CentOS

安装 Ubuntu 或 Debian

Linux：启动已迁移的节点

验证迁移的节点后，您可以在目标 Linux 主机上运行命令来启动该节点。

步骤

1. 在新主机上启动节点。

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. 在网格管理器中，验证节点的状态是否为绿色，并且未针对该节点发出任何警报。

   验证节点的状态是否为绿色可确保已迁移的节点已完全重新启动并重新加入网格。如果状态不是绿色，请勿迁移任何其他节点，以免多个节点停止服务。

   如果无法访问网格管理器，请等待 10 分钟，然后运行以下命令：

   `sUdo StorageGRID 节点状态 * ； node-name_*`

   确认迁移的节点的运行状态为 `running` 。

TSM 中间件的归档节点维护

可以将归档节点配置为通过 TSM 中间件服务器锁定磁带或通过 S3 API 将云锁定。配置后，无法更改归档节点的目标。

如果托管归档节点的服务器发生故障，请更换该服务器并按照相应的恢复操作步骤 进行操作。

归档存储设备出现故障

如果您确定归档节点通过 Tivoli Storage Manager （ TSM ）访问的归档存储设备存在故障，请使归档节点脱机，以限制 StorageGRID 系统中显示的警报数量。然后，您可以使用 TSM 服务器或存储设备的管理工具或这两者来进一步诊断和解决问题。

使目标组件脱机

在对 TSM 中间件服务器进行任何可能导致其不可供归档节点使用的维护之前，请使目标组件脱机，以限制在

TSM 中间件服务器不可用时触发的警报数量。

您需要的内容

您必须使用登录到网格管理器 支持的 Web 浏览器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARC* > * 目标 * > * 配置 * > * 主 * 。
3. 将 Tivoli Storage Manager State 的值更改为 * 脱机 * ，然后单击 * 应用更改 * 。
4. 维护完成后，将 Tivoli Storage Manager State 的值更改为 * 联机 * ，然后单击 * 应用更改 * 。

Tivoli Storage Manager 管理工具

dsmadc 工具是安装在归档节点上的 TSM 中间件服务器的管理控制台。您可以通过在服务器的命令行中键入 `dsmadc` 来访问此工具。使用与为 ARC-Service 配置的管理用户名和密码相同的管理用户名和密码登录到管理控制台。

创建 `tsmquery.rb` 脚本是为了以更易读的形式从 dsmadc 生成状态信息。您可以在归档节点的命令行中输入以下命令来运行此脚本： ` /usr/local/arc/tsmquery.rb status`

有关 TSM 管理控制台 dsmadc 的详细信息，请参见 *Tivoli Storage Manager for Linux： Administrator's Referation*.

对象永久不可用

当归档节点从 Tivoli Storage Manager （ TSM ）服务器请求对象而检索失败时，归档节点会在 10 秒间隔后重试此请求。如果对象永久不可用（例如，由于对象在磁带上损坏）， TSM API 无法向归档节点指示此情况，因此归档节点会继续重试此请求。

发生这种情况时，系统会触发警报，并且此值会继续增加。要查看警报，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 归档节点 * > * ARC/ * 检索 * > * 请求故障 * 。

如果对象永久不可用，则必须确定该对象，然后按照操作步骤 中所述手动取消归档节点的请求。 确定对象是否永久不可用。

如果对象暂时不可用，检索也可能失败。在这种情况下，后续检索请求最终应成功。

如果将 StorageGRID 系统配置为使用创建单个对象副本的 ILM 规则，并且无法检索该副本，则该对象将丢失，无法恢复。但是，您仍然必须按照操作步骤 来确定对象是否永久不可用于 "`清理` " StorageGRID 系统，取消归档节点的请求以及清除丢失对象的元数据。

确定对象是否永久不可用

您可以通过使用 TSM 管理控制台发出请求来确定对象是否永久不可用。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。
- 您必须知道管理节点的 IP 地址。

关于此任务

此示例仅供您参考；此操作步骤 无法帮助您确定可能导致对象或磁带卷不可用的所有故障情况。有关 TSM 管理的信息，请参见 TSM 服务器文档。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 确定归档节点无法检索到的一个或多个对象：
   a. 转到包含审核日志文件的目录： `cd /var/local/audit/export`

      活动的审核日志文件名为 audit.log 。每天保存一次活动的 `audit.log` 文件，并启动一个新的 `audit.log` 文件。已保存文件的名称以 `yyyy-mm-dd.txt` 格式指示其保存时间。一天之后，保存的文件将被压缩并重命名，格式为 `yyyy-mm-dd.txt.gz` ，从而保留原始日期。

   b. 在相关审核日志文件中搜索指示无法检索归档对象的消息。例如，输入： `grep Arce audit.log ; less -n`

      如果无法从归档节点检索对象，则 Arce 审核消息（归档对象检索结束）会在结果字段中显示 Arun （归档中间件不可用）或 GERR （一般错误）。审核日志中的以下示例行显示，对于 CBID 498D8A1F681F05B3 ， Arce 消息已终止，结果为 Arun 。

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      有关详细信息，请参见了解审核消息的说明。

   c. 记录请求失败的每个对象的 CBID 。

      您可能还需要记录 TSM 用于标识归档节点保存的对象的以下追加信息：

      - * 文件空间名称 * ： 等效于归档节点 ID 。要查找归档节点 ID ，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 归档节点 * > * ARC/ * 目标 * > * 概述 * 。
      - * 高级名称 * ： 相当于归档节点分配给对象的卷 ID 。卷 ID 采用日期的形式（例如， `2009 1127` ），并在归档审核消息中记录为对象的 VLID 。
      - * 低级别名称 * ： 相当于 StorageGRID 系统分配给对象的 CBID 。

   d. 注销命令 Shell： `exit`
3. 检查 TSM 服务器，查看步骤 2 中标识的对象是否永久不可用：
   a. 登录到 TSM 服务器的管理控制台： `dsmadc`

      请使用为该应用程序中心服务配置的管理用户名和密码。在网格管理器中输入用户名和密码。（要查看

用户名，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。然后，选择 * 归档节点 * > * ARC* > * 目标 * > * 配置 * 。）

b. 确定对象是否永久不可用。

例如，您可以在 TSM 活动日志中搜索该对象的数据完整性错误。以下示例显示了在过去一天的活动日志中搜索 CBID `498D8A1F681F05B3` 的对象。

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

根据错误的性质， CBID 可能不会记录在 TSM 活动日志中。您可能需要在日志中搜索请求失败前后的其他 TSM 错误。

c. 如果整个磁带永久不可用，请确定存储在该卷上的所有对象的 CBID： `query content Tsm_Volume_Name`

其中 `TSM_Volume_Name` 是不可用磁带的 TSM 名称。以下是此命令的输出示例：

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ---------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

文件名` 的 客户端名称与归档节点卷 `ID` （或 `TSM "`high level name`"`）相同，后跟对象的 CBID （或 TSM "`low level name`"）。也就是说， `Client` 的 `Name for File Name` 采用 ` /Archive Node 卷 ID /CBID` 的形式。在示例输出的第一行中，文件名` 的 客户端名称是 ` `/20081201/C1D172940E6C7E12` 。

另请记住， 文件空间 是归档节点的节点 ID 。

要取消检索请求，您需要卷上存储的每个对象的 CBID 以及归档节点的节点 ID 。

4. 对于永久不可用的每个对象，请取消检索请求并执行问题描述 a 命令，以通知 StorageGRID 系统对象副本已丢失：

> 请谨慎使用 ADE 控制台。如果控制台使用不当，则可能会中断系统操作并损坏数据。请认真输入命令，并且只能使用此操作步骤 中记录的命令。

a. 如果尚未登录到归档节点，请按以下方式登录：

i. 输入以下命令： `ssh admin@ grid_node_ip_`

ii. 输入 `passwords.txt` 文件中列出的密码。

iii. 输入以下命令切换到 root： `su -`

iv. 输入 `passwords.txt` 文件中列出的密码。

b. 访问该 ARC 服务的 ADE 控制台： `telnet localhost 1409`

c. 取消对象的请求： ` /proc/BRTR/cancel -c CBID`

其中 `CBID` 是无法从 TSM 检索到的对象的标识符。

如果此对象的唯一副本位于磁带上，则 "`bulk retrretr检 索` " 请求将被取消，并显示消息 "`1 Requests cancelled` " 。如果对象的副本位于系统中的其他位置，则对象检索将由其他模块处理，因此对消息的响应为 "`0 Requests cancelled` " 。

d. 问题描述 一个命令，用于通知 StorageGRID 系统某个对象副本已丢失且必须创建另一个副本： ` /proc/CMSI/Object_Lost CBID node_ID`

其中， `CBID` 是无法从 TSM 服务器检索的对象的标识符， `node_ID` 是检索失败的归档节点的节点 ID 。

您必须为每个丢失的对象副本输入一个单独的命令：不支持输入 CBID 范围。

在大多数情况下， StorageGRID 系统会立即开始为对象数据创建更多副本，以确保系统的 ILM 策略得到遵守。

但是，如果对象的 ILM 规则指定只创建一个副本，而该副本现已丢失，则无法恢复该对象。在这种情况下，运行 `Object_Lost` 命令可从 StorageGRID 系统清除丢失对象的元数据。

当 `Object_Lost` 命令成功完成后，将返回以下消息：

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

ℹ ` /proc/CMSI/Object_Lost` 命令仅适用于归档节点上存储的丢失对象。

a. 退出 ADE 控制台： `exit`

b. 从归档节点中注销： `exit`

5. 重置 StorageGRID 系统中的请求失败值：

a. 转到 * 归档节点 * > * ARC* > * 检索 * > * 配置 * ，然后选择 * 重置请求失败计数 * 。

b. 单击 * 应用更改 * 。

相关信息

管理 StorageGRID

查看审核日志

VMware：配置虚拟机以进行自动重新启动

如果在重新启动 VMware vSphere 虚拟机管理程序后虚拟机未重新启动，则可能需要对虚拟机进行配置，使其自动重新启动。

如果在恢复网格节点或执行其他维护操作步骤 期间发现虚拟机未重新启动，则应执行此操作步骤 。

步骤

1. 在 VMware vSphere Client 树中，选择未启动的虚拟机。
2. 右键单击虚拟机，然后选择 * 启动 * 。
3. 配置 VMware vSphere 虚拟机管理程序，以便将来自动重新启动虚拟机。

网格节点过程

您可能需要在特定网格节点上执行相关过程。虽然您可以从网格管理器执行其中几个过程，但大多数过程都要求您从节点的命令行访问 Server Manager 。

服务器管理器在每个网格节点上运行，用于监控服务的启动和停止，并确保服务正常加入和退出 StorageGRID 系统。Server Manager 还会监控每个网格节点上的服务，并自动尝试重新启动报告故障的任何服务。

只有在技术支持指示您访问 Server Manager 时，才应访问此服务器管理器。

使用完 Server Manager 后，您必须关闭当前命令 Shell 会话并注销。输入： `exit`

查看 **Server Manager** 状态和版本

对于每个网格节点，您可以查看该网格节点上运行的 Server Manager 的当前状态和版本。您还可以获取该网格节点上运行的所有服务的当前状态。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 查看网格节点上运行的 Server Manager 的当前状态： ` * service servermanager status*`

   报告网格节点上运行的 Server Manager 的当前状态（无论是否正在运行）。如果 Server Manager 的状态为 `running` ，则会列出自上次启动以来其一直运行的时间。例如：

```
servermanager running for 1d, 13h, 0m, 30s
```

3. 查看在网格节点上运行的 Server Manager 的当前版本： ` * 服务服务器管理器版本 *`

   此时将列出当前版本。例如：

```
11.1.0-20180425.1905.39c9493
```

4. 从命令 Shell ` * exit *` 中注销

查看所有服务的当前状态

您可以随时查看网格节点上运行的所有服务的当前状态。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

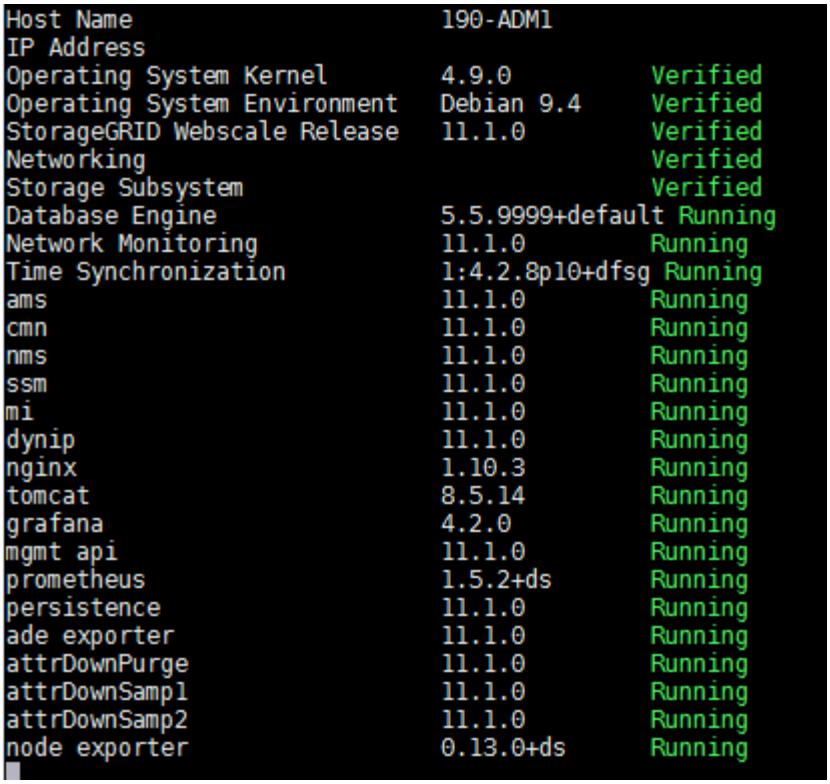
   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 查看网格节点上运行的所有服务的状态： `storagegRid-status`

   例如，主管理节点的输出将 AMS ， CMN 和 NMS 服务的当前状态显示为正在运行。如果服务状态发生变化，此输出将立即更新。



3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 也可以查看网格节点上运行的所有服务的静态报告： ` /usr/local/servermanager/reader.rb`

   此报告包含与持续更新报告相同的信息，但如果服务状态发生变化，则不会更新此报告。

5. 注销命令 Shell： `exit`

启动服务器管理器和所有服务

您可能需要启动 Server Manager ，该操作也会启动网格节点上的所有服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

如果在已运行 Server Manager 的网格节点上启动 Server Manager ，则会重新启动 Server Manager 以及网格节点上的所有服务。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 启动服务器管理器： `service servermanager start`
3. 注销命令 Shell： `exit`

重新启动 **Server Manager** 和所有服务

您可能需要重新启动服务器管理器以及网格节点上运行的所有服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 重新启动服务器管理器以及网格节点上的所有服务： `service servermanager restart`

   Server Manager 以及网格节点上的所有服务将停止并重新启动。

   使用 `restart` 命令与依次使用 `stop` 命令和 `sstart` 命令相同。
3. 注销命令 Shell： `exit`

停止 **Server Manager** 和所有服务

Server Manager 可始终运行，但您可能需要停止 Server Manager 以及网格节点上运行的所有服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止服务器管理器以及网格节点上运行的所有服务： `sservice servermanager stop`

   服务器管理器以及网格节点上运行的所有服务均正常终止。服务可能需要长达 15 分钟才能关闭。

3. 注销命令 Shell： `exit`

查看服务的当前状态

您可以随时查看网格节点上运行的服务的当前状态。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 查看在网格节点上运行的服务的当前状态： ` * service *servicename* status* 报告在网格节点上运行的请求服务的当前状态（无论是否正在运行）。例如：

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. 从命令 Shell ` * exit *` 中注销

停止服务

某些维护过程要求您停止一项服务，同时保持网格节点上的其他服务正常运行。只有在维护操作步骤 指示停止单个服务时，才停止这些服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

使用以下步骤 "`以管理员方式停止` " 服务时， Server Manager 不会自动重新启动该服务。您必须手动启动单个服务或重新启动 Server Manager 。

如果需要停止存储节点上的 LDR 服务，请注意，如果存在活动连接，则停止此服务可能需要一段时间。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止单个服务： `sservice_servicename_ stop`

   例如：

   ```
   service ldr stop
   ```

   > 服务可能需要长达 11 分钟才能停止。

3. 注销命令 Shell： `exit`

相关信息

强制终止服务

将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

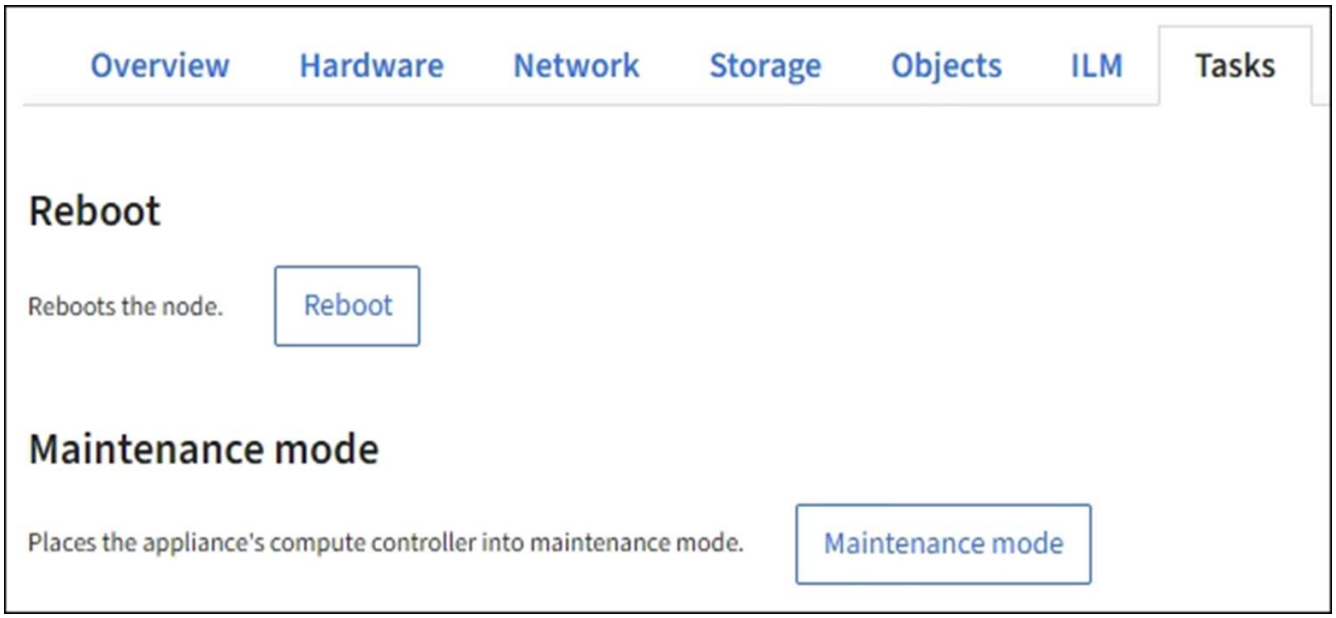
关于此任务

在极少数情况下，将 StorageGRID 设备置于维护模式可能会使该设备无法进行远程访问。

> 处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

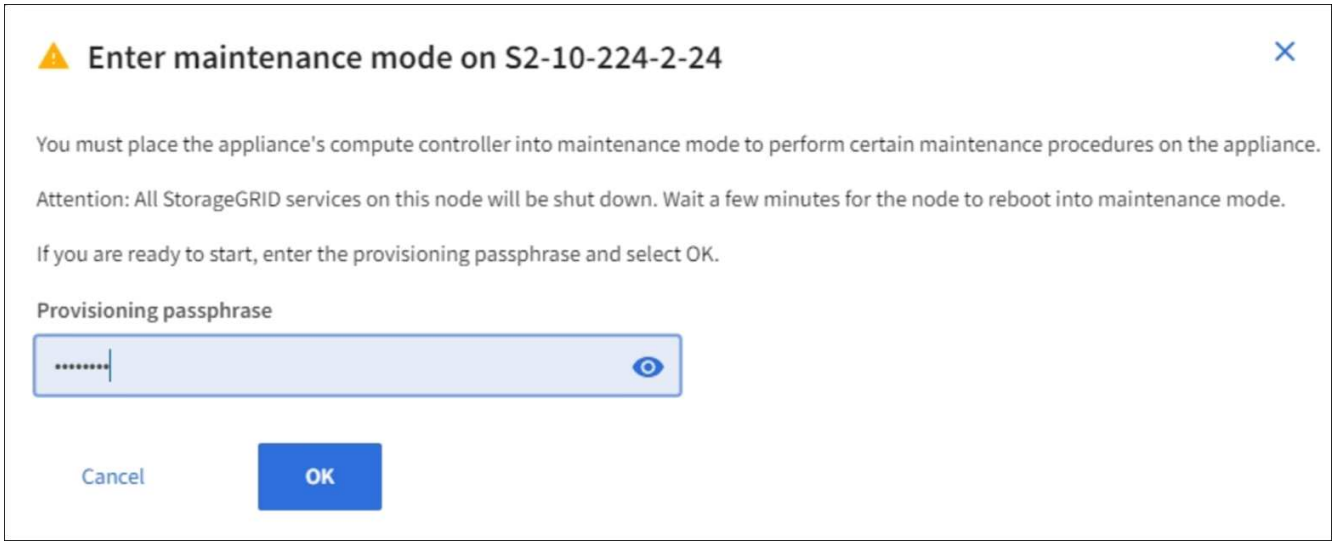
步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 从节点页面的树视图中，选择设备存储节点。
3. 选择 * 任务 * 。



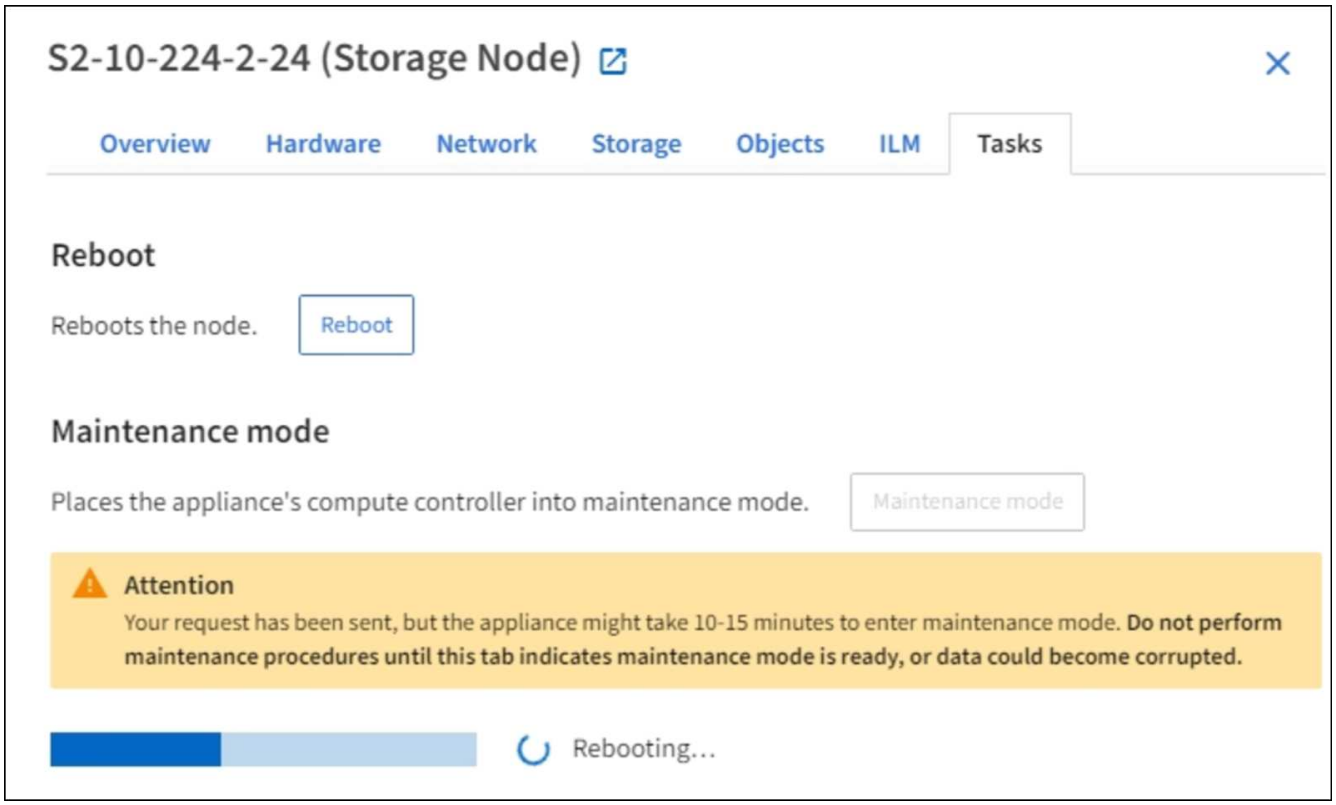
4. 选择 * 维护模式 * 。

   此时将显示确认对话框。

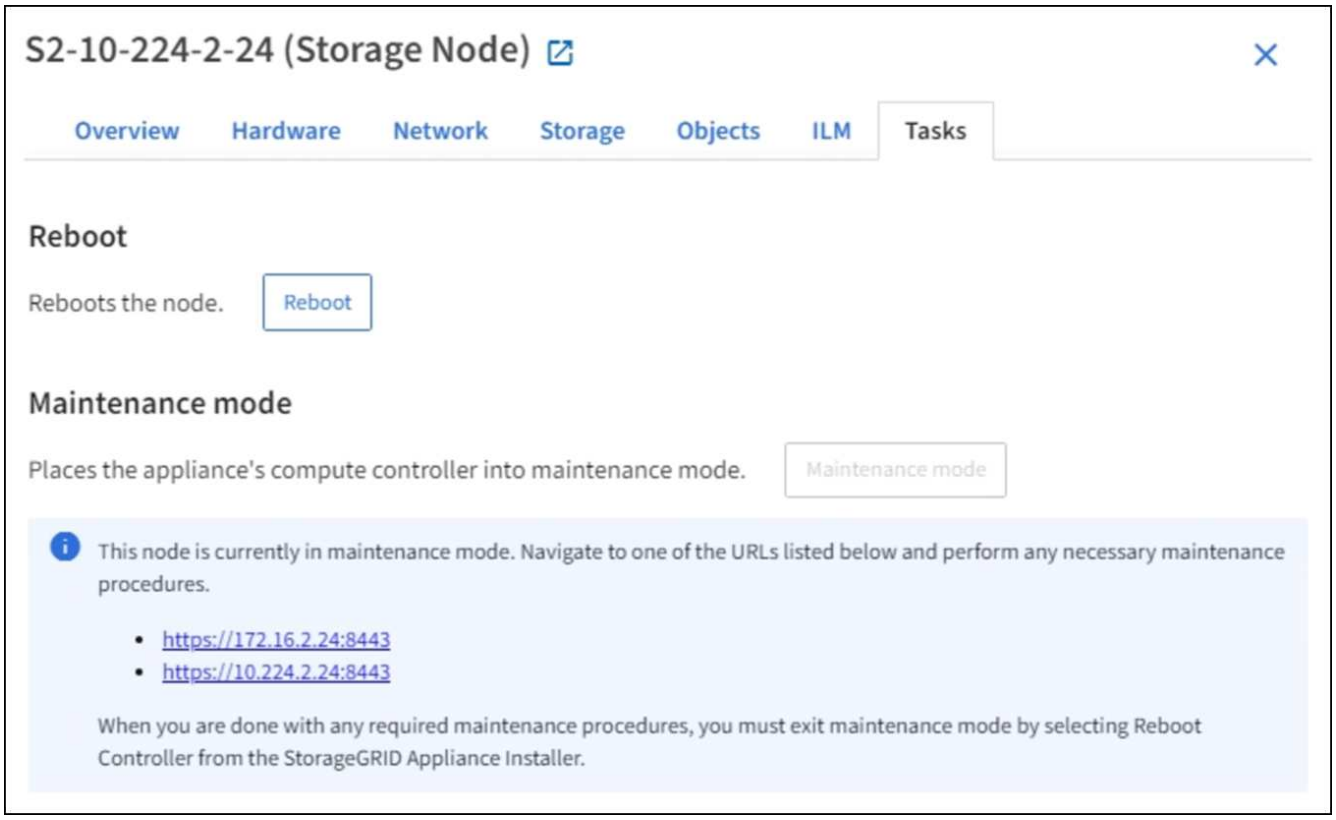


5. 输入配置密码短语，然后选择 * 确定 * 。

   进度条和一系列消息（包括 " 已发送请求 " ， " 正在停止 StorageGRID " 和 " 正在重新启动 " ）表示设备正在完成进入维护模式的步骤。



设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL 。



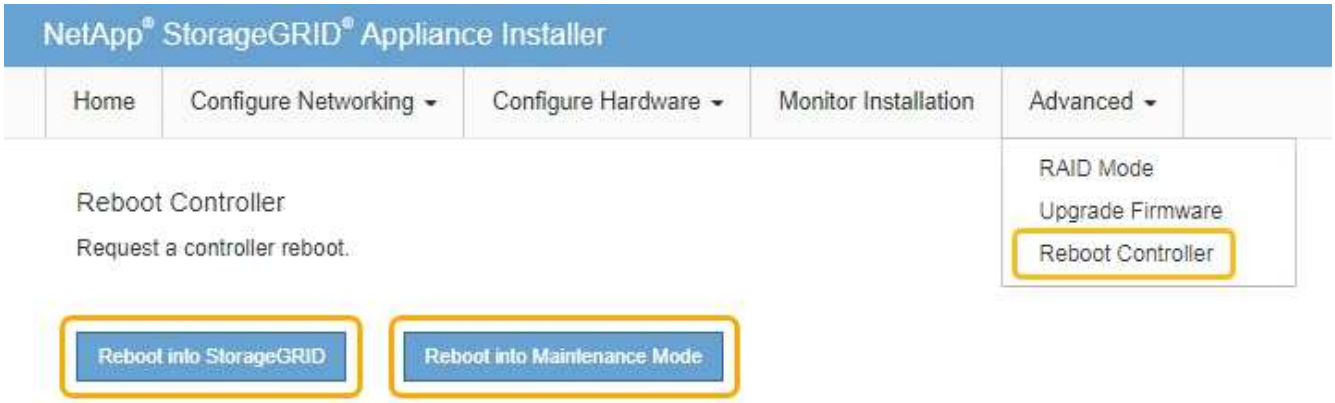
6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL 。

   如果可能，请使用包含设备管理网络端口 IP 地址的 URL 。

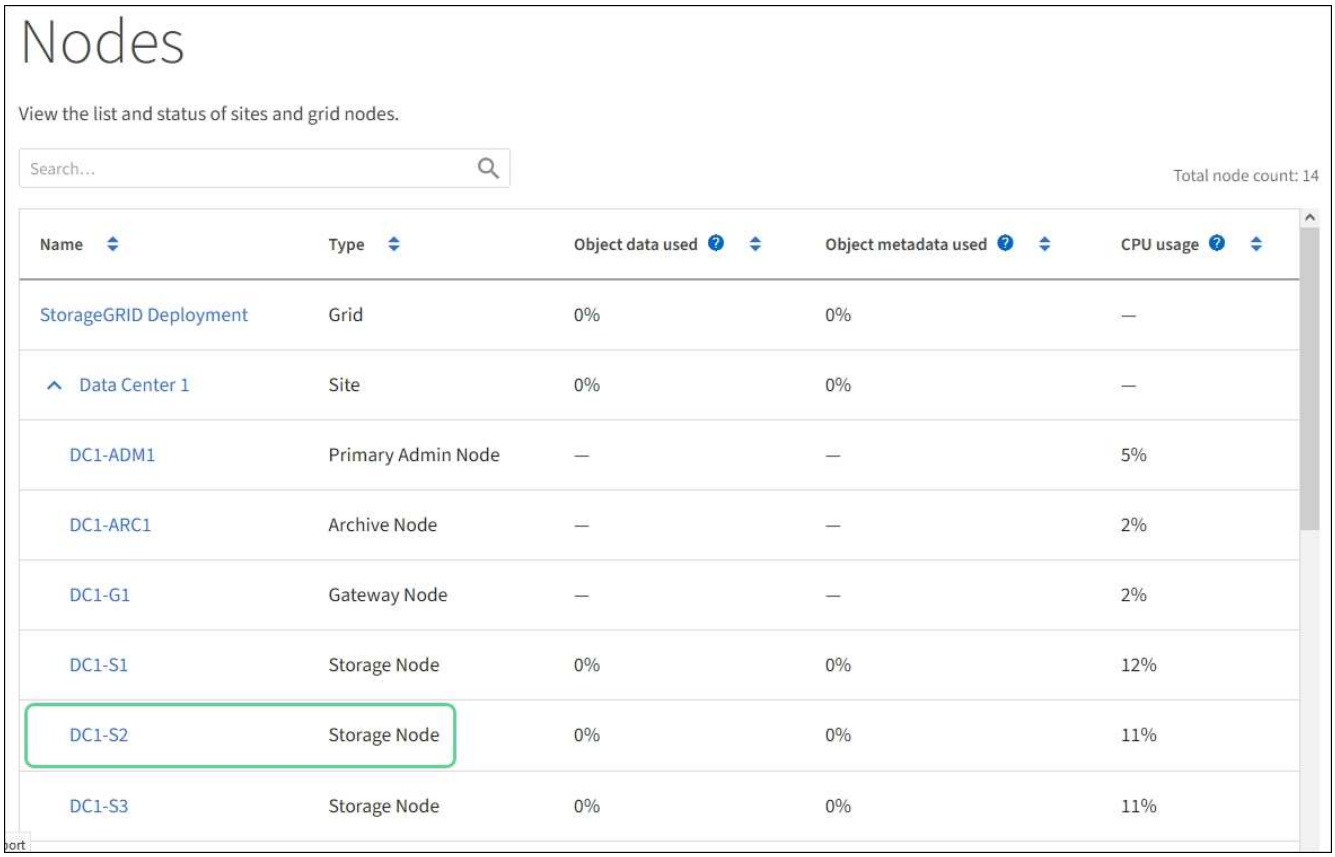
访问 ` + https://169.254.0.1:8443+` 需要直接连接到本地管理端口。

7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。

8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动至 StorageGRID * 。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。"* 节点 * " 页面应显示设备节点的正常状态（节点名称左侧没有图标），表示没有处于活动状态的警报，并且节点已连接到网格。



强制终止服务

如果需要立即停止服务，可以使用 `force-stop` 命令。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 手动强制终止服务： `service servicename force-stop`

   例如：

```
service ldr force-stop
```

系统将等待 30 秒，然后再终止此服务。

3. 注销命令 Shell： `exit`

启动或重新启动服务

您可能需要启动已停止的服务，或者可能需要停止并重新启动服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 根据服务当前是正在运行还是已停止，确定向问题描述 发出的命令。
   - 如果此服务当前已停止，请使用 `sstart` 命令手动启动此服务： `service servicename start`

     例如：

     ```
     service ldr start
     ```

   - 如果此服务当前正在运行，请使用 `restart` 命令停止此服务，然后重新启动它： `service servicename restart`

     例如：

```
service ldr restart
```

+

> 使用 `restart` 命令与依次使用 `stop` 命令和 `sstart` 命令相同。即使服务当前已停止，您也可以使用问题描述 `restart` 。

3. 注销命令 Shell： `exit`

删除端口重新映射

如果要为负载平衡器服务配置端点，并且要使用已配置为端口重新映射的映射到端口的端

口，则必须先删除现有端口重新映射，否则此端点将无效。您必须在每个管理节点和网关节点上运行一个脚本，该节点具有冲突的重新映射端口，以删除该节点的所有端口重新映射。

关于此任务

此操作步骤 将删除所有端口重新映射。如果需要保留部分重新映射，请联系技术支持。

有关配置负载平衡器端点的信息，请参见有关管理 StorageGRID 的说明。

如果端口重新映射提供了客户端访问，则应重新配置客户端，以便尽可能使用配置为负载平衡器端点的其他端口，以避免服务丢失，否则，删除端口映射将导致客户端访问丢失，并应相应地进行计划。

对于在裸机主机上部署为容器的 StorageGRID 系统，此操作步骤 不起作用。请参见的说明 删除裸机主机上的端口重新映射。

步骤

1. 登录到此节点。
   a. 输入以下命令： `ssh -p 8022 admin@node_ip`

      端口 8022 是基础操作系统的 SSH 端口，而端口 22 是运行 StorageGRID 的容器引擎的 SSH 端口。

   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 运行以下脚本： `remove-port-remap.sh`
3. 重新启动节点。

   按照的说明进行操作 重新启动网格节点。

4. 对具有冲突重新映射端口的每个管理节点和网关节点重复上述步骤。

相关信息

管理 StorageGRID

删除裸机主机上的端口重新映射

如果要为负载平衡器服务配置端点，并且要使用已配置为端口重新映射的映射到端口的端口，则必须先删除现有端口重新映射，否则此端点将无效。如果您在裸机主机上运行 StorageGRID ，请按照此操作步骤 而不是常规操作步骤 删除端口重新映射。您必须为每个管理节点和网关节点编辑节点配置文件，该节点的重新映射端口相互冲突，以删除该节点的所有端口重新映射并重新启动该节点。

关于此任务

此操作步骤 将删除所有端口重新映射。如果需要保留部分重新映射，请联系技术支持。

有关配置负载平衡器端点的信息，请参见有关管理 StorageGRID 的说明。

此操作步骤 可能会在节点重新启动时暂时丢失服务。

步骤

1. 登录到支持此节点的主机。以 root 用户身份或使用具有 sudo 权限的帐户登录。
2. 运行以下命令以临时禁用节点： `sUdo StorageGRID node stop node-name`
3. 使用 vim 或 pico 等文本编辑器编辑节点的节点配置文件。

   节点配置文件位于 ` /etc/storaggrid/nodes/*node-name*.conf` 中。

4. 找到节点配置文件中包含端口重新映射的部分。

   请参见以下示例中的最后两行。

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. 编辑 port_remap 和 port_remap_inbound 条目以删除端口重新映射。

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 运行以下命令以验证对节点的节点配置文件所做的更改： `sUdo StorageGRID node validate node-name`

   解决所有错误或警告，然后再继续下一步。

7. 运行以下命令以在不重新映射端口的情况下重新启动节点： `sUdo StorageGRID node start node-name`
8. 使用 `passwords.txt` 文件中列出的密码以管理员身份登录到此节点。
9. 验证服务是否正确启动。
   a. 查看服务器上所有服务的状态列表：`sudo storagegRid-status`

      状态将自动更新。

   b. 请等待，直到所有服务的状态均为 " 正在运行 " 或 " 已验证 " 。
   c. 退出状态屏幕：`Ctrl+C`
10. 对具有冲突重新映射端口的每个管理节点和网关节点重复上述步骤。

重新启动网格节点

您可以从网格管理器或节点的命令 Shell 重新启动网格节点。

关于此任务

重新启动网格节点时，该节点将关闭并重新启动。所有服务都会自动重新启动。

如果您计划重新启动存储节点，请注意以下事项：

- 如果 ILM 规则指定了 " 双提交 " 的载入行为或规则指定了 " 已平衡 " ，并且无法立即创建所有必需的副本，则 StorageGRID 会立即将任何新载入的对象提交到同一站点上的两个存储节点，并在稍后评估 ILM 。如果要重新启动给定站点上的两个或多个存储节点，则在重新启动期间可能无法访问这些对象。
- 为了确保您可以在存储节点重新启动时访问所有对象，请在重新启动节点之前，停止在站点上载入对象大约一小时。

相关信息

管理 StorageGRID

从网格管理器重新启动网格节点

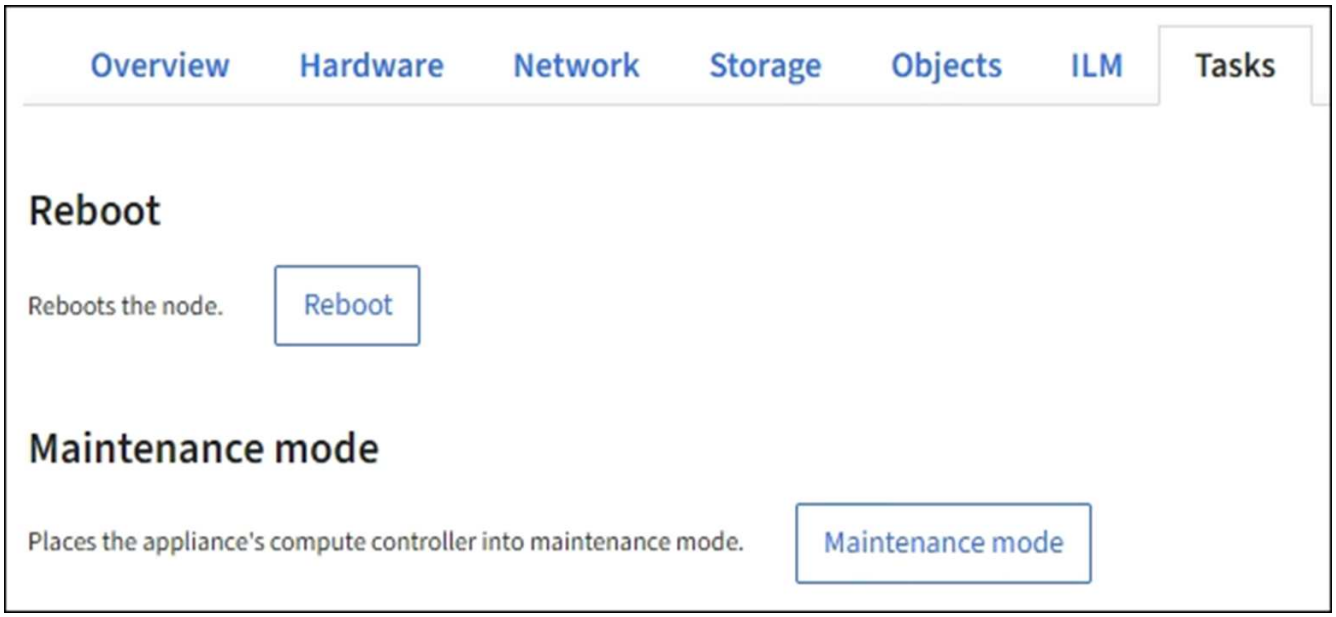
从网格管理器重新启动网格节点会在目标节点上发出 `reboot` 命令。

您需要的内容

- 您将使用登录到网格管理器 支持的 Web 浏览器。
- 您具有维护或 root 访问权限。
- 您具有配置密码短语。

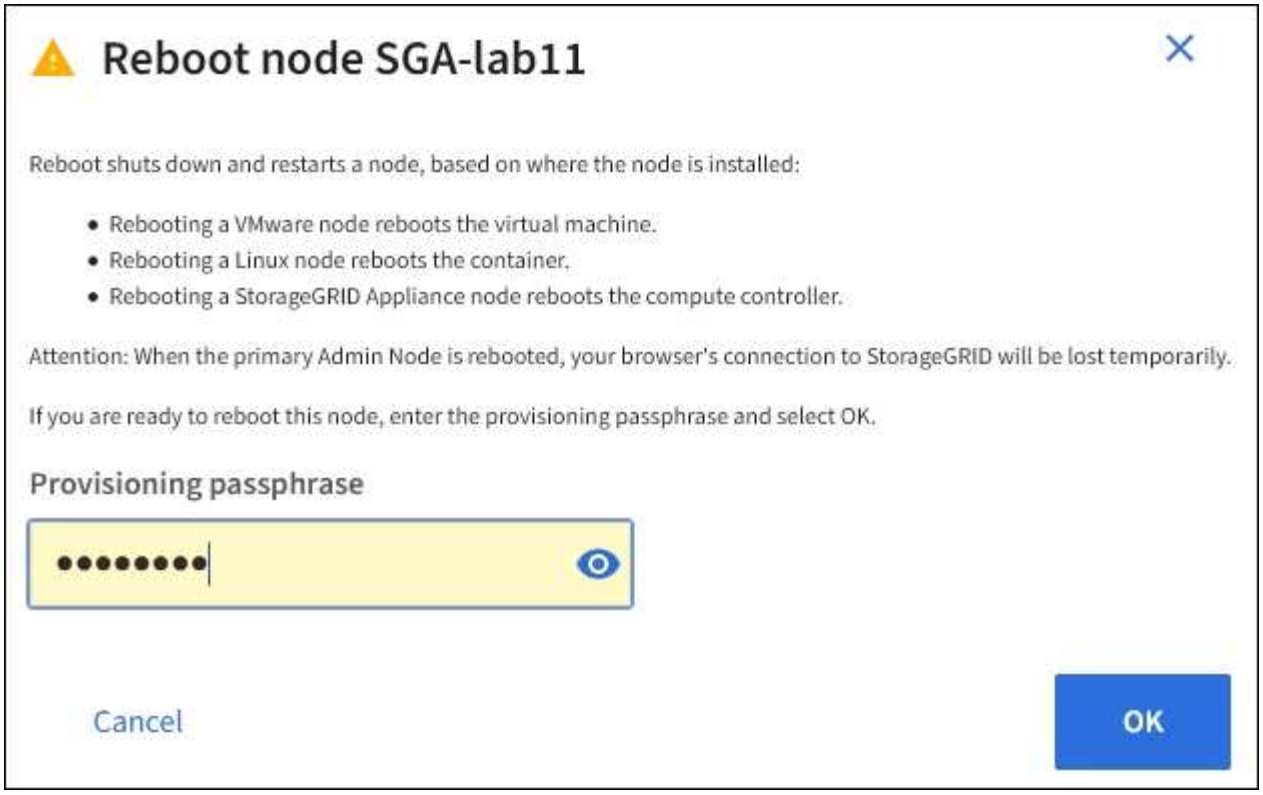
步骤

1. 选择 * 节点 * 。
2. 选择要重新启动的网格节点。
3. 选择 * 任务 * 选项卡。



4. 选择 * 重新启动 * 。

   此时将显示确认对话框。



如果要重新启动主管理节点，则确认对话框会提醒您，服务停止后，浏览器与网格管理器的连接将暂时断开。

5. 输入配置密码短语，然后单击 * 确定 * 。
6. 等待节点重新启动。

   关闭服务可能需要一些时间。

   节点重新启动时， * 节点 * 页面左侧会显示灰色图标（管理员关闭）。当所有服务重新启动且节点已成功连接到网格时， * 节点 * 页面应显示正常状态（节点名称左侧没有图标），表示没有活动警报且节点已连接到网格。

从命令 **Shell** 重新启动网格节点

如果您需要更密切地监控重新启动操作，或者无法访问网格管理器，则可以登录到网格节点并从命令 Shell 运行 Server Manager reboot 命令。

您必须具有 `passwords.txt` 文件。

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 或者，停止服务： `service servermanager stop`

   停止服务是一个可选步骤，但建议执行此步骤。服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程，然后再在下一步中重新启动节点。

3. 重新启动网格节点： `reboot`
4. 注销命令 Shell： `exit`

关闭网格节点

您可以使用节点的命令 Shell 关闭网格节点。

您需要的内容

- 您必须具有 `passwords.txt` 文件。

关于此任务

在执行此操作步骤 之前，请查看以下注意事项：

- 通常，一次关闭的节点不应超过一个，以避免中断。
- 除非文档或技术支持明确指示，否则请勿在维护操作步骤 期间关闭节点。
- 关闭过程取决于节点的安装位置，如下所示：
  - 关闭 VMware 节点将关闭虚拟机。
  - 关闭 Linux 节点将关闭容器。
  - 关闭 StorageGRID 设备节点将关闭计算控制器。
- 如果您计划关闭一个站点上的多个存储节点、请在关闭这些节点之前停止在该站点上载入对象大约一小时。

  如果任何ILM规则使用*双提交*载入选项(或者某个规则使用*平衡*选项、并且无法立即创建所有必需的副本)、则StorageGRID 会立即将任何新载入的对象提交到同一站点上的两个存储节点、并在稍后对ILM进行评估。如果某个站点上的多个存储节点关闭、则在关闭期间、您可能无法访问新载入的对象。如果站点上的可用存储节点太少、写入操作也可能失败。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。

3. 如果此节点正在 VMware 虚拟机上运行或它是设备节点，请使用问题描述 关闭命令： `shutdown -h now`

   执行此步骤，无论 `sservice servermanager stop` 命令的结果如何。

   > 在设备节点上执行问题描述 `shutdown -h now` 命令后，必须重新启动设备以重新启动节点。

   对于设备，此命令将关闭控制器，但设备仍处于打开状态。您必须完成下一步。

4. 如果要关闭设备节点：
   - 对于 SG100 或 SG1000 服务设备
     i. 关闭设备电源。
     ii. 等待蓝色电源 LED 熄灭。
   - 对于 SG6000 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

     当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，然后等待蓝色电源 LED 熄灭。
   - 对于 SG5700 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

     当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，等待所有 LED 和七段显示活动停止。

相关信息

管理 StorageGRID

关闭主机

在关闭主机电源之前，必须停止该主机上所有网格节点上的服务。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 停止节点上运行的所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。

3. 对主机上的每个节点重复步骤 1 和 2 。
4. 如果您使用的是 Linux 主机：
   a. 登录到主机操作系统。
   b. 停止节点： `StorageGRID node stop`
   c. 关闭主机操作系统。
5. 如果此节点正在 VMware 虚拟机上运行或它是设备节点，请使用问题描述 关闭命令： `shutdown -h now`

   执行此步骤，无论 `sservice servermanager stop` 命令的结果如何。

   > 在设备节点上执行问题描述 `shutdown -h now` 命令后，必须重新启动设备以重新启动节点。

   对于设备，此命令将关闭控制器，但设备仍处于打开状态。您必须完成下一步。
6. 如果要关闭设备节点：
   - 对于 SG100 或 SG1000 服务设备
     i. 关闭设备电源。
     ii. 等待蓝色电源 LED 熄灭。
   - 对于 SG6000 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，然后等待蓝色电源 LED 熄灭。
   - 对于 SG5700 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，等待所有 LED 和七段显示活动停止。
7. 注销命令 Shell： `exit`

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

关闭并打开网格中的所有节点

例如，如果要移动数据中心，您可能需要关闭整个 StorageGRID 系统。以下步骤简要概述了执行受控关闭和启动的建议顺序。

关闭站点或网格中的所有节点后，在存储节点脱机时，您将无法访问已载入的对象。

停止服务并关闭网格节点

在关闭 StorageGRID 系统之前，必须先停止每个网格节点上运行的所有服务，然后关闭所有 VMware 虚拟机，容器引擎和 StorageGRID 设备。

关于此任务

首先停止管理节点和 API 网关节点上的服务，然后停止存储节点上的服务。

通过此方法，您可以使用主管理节点尽可能长时间地监控其他网格节点的状态。

> 如果一个主机包含多个网格节点，请勿关闭该主机，直到停止该主机上的所有节点为止。如果主机包含主管理节点，请最后关闭该主机。

> 如果需要，您可以 将节点从一台 Linux 主机迁移到另一台 Linux 主机 在不影响网格功能或可用性的情况下执行主机维护。

步骤

1. 停止所有客户端应用程序访问网格。
2. 【登录到每个网关节点】登录到每个网关节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

      以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
3. 【 stop_all_services]] 停止节点上运行的所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。
4. 重复上述两个步骤，停止所有存储节点，归档节点和非主管理节点上的服务。

   您可以按任何顺序停止这些节点上的服务。

   > 如果问题描述 您使用 `sservice servermanager stop` 命令停止设备存储节点上的服务，则必须重新启动设备以重新启动节点。
5. 对于主管理节点，重复执行的步骤 登录到节点 和 停止节点上的所有服务。
6. 对于在 Linux 主机上运行的节点：
   a. 登录到主机操作系统。
   b. 停止节点： `StorageGRID node stop`
   c. 关闭主机操作系统。

7. 对于在 VMware 虚拟机上运行的节点以及设备存储节点，请使用问题描述 关闭命令： `shutdown -h now`

   执行此步骤，无论 `sservice servermanager stop` 命令的结果如何。

   对于设备，此命令将关闭计算控制器，但设备仍处于打开状态。您必须完成下一步。

8. 如果您有设备节点：
   - 对于 SG100 或 SG1000 服务设备
     i. 关闭设备电源。
     ii. 等待蓝色电源 LED 熄灭。
   - 对于 SG6000 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，然后等待蓝色电源 LED 熄灭。
   - 对于 SG5700 设备
     i. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

        当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

     ii. 关闭设备电源，等待所有 LED 和七段显示活动停止。
9. 如果需要，请注销命令 Shell： `exit`

   此时， StorageGRID 网格已关闭。

相关信息

SG100 和 SG1000 服务设备

SG6000 存储设备

SG5700 存储设备

启动网格节点

按照以下顺序在完全关闭后启动网格节点。

> 您需要什么？ **#8217**；将需要什么
>
> 如果整个网格已关闭超过 15 天，则在启动任何网格节点之前，您必须联系技术支持。请勿尝试执行重建 Cassandra 数据的恢复过程。这样做可能会导致数据丢失。

关于此任务

如果可能，应按以下顺序启动网格节点：

- 首先为管理节点接通电源。

- 请最后为网关节点通电。

如果主机包含多个网格节点，则在启动主机时，这些节点将自动恢复联机。

步骤

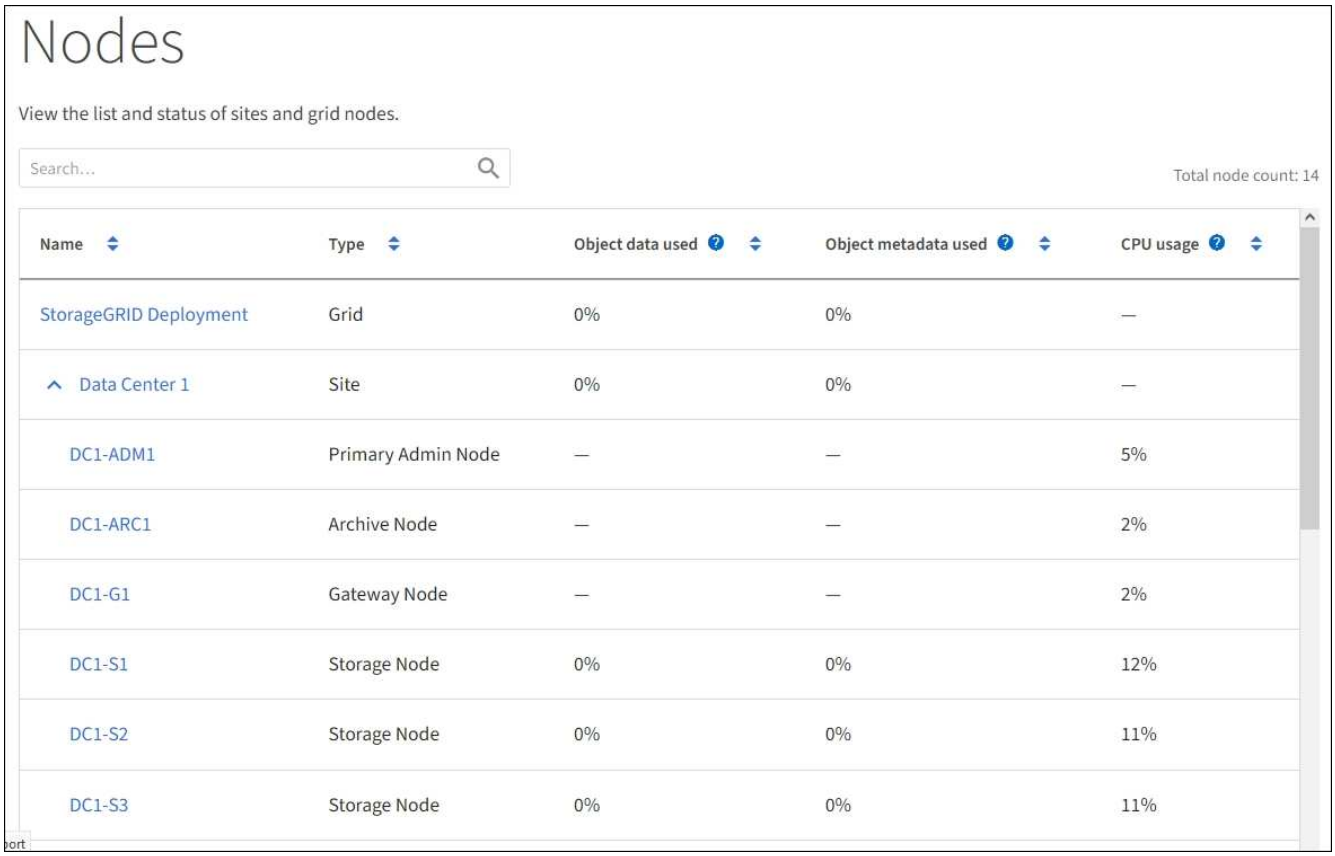
1. 打开主管理节点和任何非主管理节点的主机的电源。

   在重新启动存储节点之前，您将无法登录到管理节点。

2. 启动所有归档节点和存储节点的主机。

   您可以按任意顺序打开这些节点的电源。

3. 启动所有网关节点的主机。
4. 登录到网格管理器。
5. 选择 * 节点 * 并监控网格节点的状态。验证节点名称旁边是否没有警报图标。



使用 **DoNotStart** 文件

如果您在技术支持的指导下执行各种维护或配置过程，则可能会要求您使用 DoNotStart 文件来防止在启动或重新启动 Server Manager 时启动服务。

只有在技术支持要求您添加或删除 DoNotStart 文件时，才应添加或删除此文件。

要阻止服务启动，请将 DoNotStart 文件置于要阻止启动的服务的目录中。启动时， Server Manager 将查找 DoNotStart 文件。如果文件存在，则会阻止服务（以及与之相关的任何服务）启动。删除 DoNotStart 文件后，先前停止的服务将在下次启动或重新启动 Server Manager 时启动。删除 DoNotStart 文件后，服务不会自动启动。

阻止所有服务重新启动的最有效方法是阻止 NTP 服务启动。所有服务都依赖于 NTP 服务，如果 NTP 服务未运行，则无法运行。

为服务添加 **DoNotStart** 文件

通过将 DoNotStart 文件添加到网格节点上某个服务的目录中，您可以阻止单个服务启动。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`
   b. 输入 `passwords.txt` 文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `passwords.txt` 文件中列出的密码。

   以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。
2. 添加 DoNotStart 文件： `touch /etc/sv/service/DoNotStart`

   其中 `sservice` 是要阻止启动的服务的名称。例如：

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   此时将创建 DoNotStart 文件。不需要文件内容。

   重新启动 Server Manager 或网格节点后， Server Manager 将重新启动，但服务不会重新启动。
3. 注销命令 Shell： `exit`

删除 **DoNotStart** 文件以进行维护

删除阻止服务启动的 DoNotStart 文件时，必须启动该服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@ grid_node_ip_`

b. 输入 `passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 从服务目录中删除 DoNotStart 文件： `rm /etc/sv/service/DoNotStart`

   其中 `sservice` 是服务的名称。例如：

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. 启动服务： `sservice_servicename_ start`

4. 注销命令 Shell： `exit`

对 **Server Manager** 进行故障排除

访问 **Server Manager** 日志文件

如果使用 Server Manager 时出现问题，请检查其日志文件。

与 Server Manager 相关的错误消息会记录在 Server Manager 日志文件中，该文件位于 ` /var/local/log/servermanager.log`

检查此文件中有关故障的错误消息。如果需要，请将问题描述 升级到技术支持。系统可能会要求您将日志文件转发给技术支持。

存在错误状态的服务

如果您检测到某个服务已进入错误状态，请尝试重新启动此服务。

您需要的内容

您必须具有 `passwords.txt` 文件。

关于此任务

Server Manager 可监控服务并重新启动任何意外停止的服务。如果服务失败， Server Manager 将尝试重新启动它。如果在五分钟内启动服务的尝试失败三次，则该服务将进入错误状态。Server Manager 不会尝试再次重新启动。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@ grid_node_ip_`

   b. 输入 `passwords.txt` 文件中列出的密码。

   c. 输入以下命令切换到 root： `su -`

   d. 输入 `passwords.txt` 文件中列出的密码。

以 root 用户身份登录时，提示符将从 ` $` 更改为 ` #` 。

2. 确认服务的错误状态： `sservice_servicename_ status`

   例如：

   ```
   service ldr status
   ```

   如果服务处于错误状态，则会返回以下消息： ` *servicename* in error state` 。例如：

   ```
   ldr in error state
   ```

   如果服务状态为 d**已禁用** ，请参见的说明 删除服务的 DoNotStart 文件。

3. 尝试通过重新启动服务来删除错误状态： `sservice_servicename_ restart`

   如果服务无法重新启动，请联系技术支持。

4. 注销命令 Shell： `exit`

设备节点克隆

您可以在 StorageGRID 中克隆设备节点，以使用设计较新或功能增强的设备。克隆会将现有节点上的所有信息传输到新设备，提供易于执行的硬件升级过程，并提供停用和扩展的替代方案来更换设备。

设备节点克隆的工作原理

通过设备节点克隆，您可以轻松地将网格中的现有设备节点（源）替换为同一逻辑 StorageGRID 站点中的兼容设备（目标）。此过程会将所有数据传输到新设备，从而使其投入使用以更换旧设备节点，并使旧设备处于预安装状态。

为何克隆设备节点?

如果需要，您可以克隆设备节点：

- 更换即将达到使用寿命的设备。
- 升级现有节点以利用经过改进的设备技术。
- 增加网格存储容量，而不更改 StorageGRID 系统中的存储节点数。
- 提高存储效率，例如将 RAID 模式从 DDP-8 更改为 DDP-16 或 RAID-6 。
- 高效地实施节点加密，以允许使用外部密钥管理服务器（ KMS ）。

使用的是哪个 **StorageGRID** 网络?

克隆可通过三个 StorageGRID 网络中的任何一个将数据从源节点直接传输到目标设备。通常使用网格网络，但如果源设备连接到这些网络，您也可以使用管理网络或客户端网络。选择用于克隆流量的网络，该网络可在不降低 StorageGRID 网络性能或数据可用性的情况下提供最佳数据传输性能。

安装替代设备时，必须为 StorageGRID 连接和数据传输指定临时 IP 地址。由于替代设备将与它所替代的设备节点属于同一网络，因此您必须为替代设备上的每个网络指定临时 IP 地址。

目标设备兼容性

替代设备的类型必须与要替换的源节点相同，并且这两个设备都必须属于同一逻辑 StorageGRID 站点。

- 替代服务设备可以不同于要替换的管理节点或网关节点。
  - 您可以将 SG100 源节点设备克隆到 SG1000 服务目标设备，以增强管理节点或网关节点的功能。
  - 您可以将 SG1000 源节点设备克隆到 SG100 服务目标设备，以便为要求更苛刻的应用程序重新部署 SG1000 。

    例如，如果将 SG1000 源节点设备用作管理节点，而您希望将其用作专用负载平衡节点。

  - 将 SG1000 源节点设备更换为 SG100 服务目标设备会将网络端口的最大速度从 100-GbE 降低到 25-GbE 。
  - SG100 和 SG1000 设备具有不同的网络连接器。更改设备类型可能需要更换缆线或 SFP 模块。
- 更换用的存储设备的容量必须等于或大于要更换的存储节点的容量。
  - 如果目标存储设备与源节点具有相同数量的驱动器、则目标设备中的驱动器必须具有更大容量(以TB为单位)。
  - 如果您计划在目标节点上使用与源节点上相同的 RAID 模式， 或者，如果 RAID 模式的存储效率较低（例如，从 RAID6 切换到 DDP ），则目标设备中的驱动器必须大于源设备中的驱动器（以 TB 为单位）。
  - 如果由于安装了固态驱动器（ SSD ），目标存储设备中安装的标准驱动器数量小于源节点中的驱动器数量，则目标设备中标准驱动器的整体存储容量（以 TB 为单位） 必须满足或超过源存储节点中所有驱动器的总功能驱动器容量。

    例如、在将包含60个驱动器的SG5660源存储节点设备克隆到包含58个标准驱动器的SG6060或SG60X目标设备时、应在克隆之前在SG6060或SG60X目标设备中安装更大的驱动器、以保持存储容量。（目标设备中包含 SSD 的两个驱动器插槽不包括在设备存储总容量中。）

    但是、如果为60个驱动器的SG5660源节点设备配置了SANtricity 动态磁盘池DDP-8、则使用DDP-16配置58个驱动器大小相同的SG6060或SG6060X目标设备可能会使SG6060或SG6060X设备成为有效的克隆目标、因为它提高了存储效率。

  您可以在网格管理器的 * 节点 * 页面上查看有关源设备节点当前 RAID 模式的信息。选择设备的 * 存储 * 选项卡。

哪些信息不会克隆?

在克隆期间，以下设备配置不会传输到替代设备。您必须在更换设备的初始设置期间对其进行配置。

- BMC 接口

- 网络链路
- 节点加密状态
- SANtricity 系统管理器（适用于存储节点）
- RAID 模式（适用于存储节点）

哪些问题会阻止克隆?

如果在克隆时遇到以下任何问题，则克隆过程将暂停并生成错误消息：

- 网络配置错误
- 源设备与目标设备之间缺乏连接
- 源设备和目标设备不兼容
- 对于存储节点，是指容量不足的替代设备

要继续克隆，必须解析每个问题描述 。

设备节点克隆的注意事项和要求

在克隆设备节点之前，您必须了解注意事项和要求。

更换设备的硬件要求

确保替代设备符合以下标准：

- 源节点（要更换的设备）和目标（新）设备必须为相同类型的设备：
  - 您只能将管理节点设备或网关节点设备克隆到新的服务设备。
  - 您只能将存储节点设备克隆到新的存储设备。
- 对于管理节点或网关节点设备，源节点设备和目标设备不必是相同类型的设备；但是，更改设备类型可能需要更换缆线或 SFP 模块。

  例如，您可以将 SG1000 节点设备更换为 SG100 ，也可以将 SG100 设备更换为 SG1000 设备。

- 对于存储节点设备，源节点设备和目标设备不必是相同类型的设备；但是，目标设备的存储容量必须大于源设备。

  例如，您可以将 SG5600 节点设备更换为 SG5700 或 SG6000 设备。

请联系您的 StorageGRID 销售代表，以帮助您选择兼容的替代设备来克隆 StorageGRID 安装中的特定设备节点。

准备克隆设备节点

克隆设备节点之前，您必须具有以下信息：

- 从网络管理员处获取网格网络的临时 IP 地址，以便在初始安装期间与目标设备配合使用。如果源节点属于管理网络或客户端网络，请获取这些网络的临时 IP 地址。

临时 IP 地址通常与要克隆的源节点设备位于同一子网中，克隆完成后不需要这些地址。源设备和目标设备都必须连接到 StorageGRID 的主管理节点，才能建立克隆连接。

- 确定要使用哪个网络克隆数据传输流量，从而在不降低 StorageGRID 网络性能或数据可用性的情况下提供最佳数据传输性能。

  使用 1-GbE 管理网络进行克隆数据传输会导致克隆速度变慢。

- 确定目标设备是否将使用密钥管理服务器（ KMS ）进行节点加密，以便在克隆之前在初始目标设备安装期间启用节点加密。您可以按照设备安装中所述检查源设备节点上是否启用了节点加密。

  源节点和目标设备可以具有不同的节点加密设置。在数据传输期间以及目标节点重新启动并加入网格时，系统会自动执行数据解密和加密。

  - SG100 和 SG1000 服务设备
  - SG5600 存储设备
  - SG5700 存储设备
  - SG6000 存储设备

- 确定是否应更改目标设备上的 RAID 模式及其默认设置，以便您可以在克隆之前的初始目标设备安装期间指定此信息。您可以在网格管理器的 * 节点 * 页面上查看有关源设备节点当前 RAID 模式的信息。选择设备的 * 存储 * 选项卡。

  源节点和目标设备可以具有不同的 RAID 设置。

- 规划足够的时间以完成节点克隆过程。将数据从运行中的存储节点传输到目标设备可能需要几天时间。计划一次克隆，尽可能地减少对业务的影响。
- 一次只能克隆一个设备节点。克隆可能会阻止您同时执行其他 StorageGRID 维护功能。
- 克隆设备节点后，您可以使用已恢复预安装状态的源设备作为克隆另一个兼容节点设备的目标。

克隆设备节点

克隆过程可能需要几天时间才能在源节点（正在更换的设备）和目标（新）设备之间传输数据。

您需要的内容

- 您已将兼容的目标设备安装到机柜或机架中，并已连接所有缆线并已接通电源。
- 您已验证更换设备上的 StorageGRID 设备安装程序版本是否与 StorageGRID 系统的软件版本匹配，如有必要，可升级 StorageGRID 设备安装程序固件。
- 您已配置目标设备，包括配置 StorageGRID 连接， SANtricity 系统管理器（仅限存储设备）和 BMC 接口。
  - 配置 StorageGRID 连接时，请使用临时 IP 地址。
  - 配置网络链路时，请使用最终的链路配置。

完成初始目标设备配置后，保持 StorageGRID 设备安装程序处于打开状态。启动节点克隆过程后，您将返回到目标设备的安装程序页面。

- 您也可以选择为目标设备启用节点加密。
- 您也可以为目标设备（仅限存储设备）设置 RAID 模式。
- 设备节点克隆的注意事项和要求

  SG100 和 SG1000 服务设备

  SG5600 存储设备

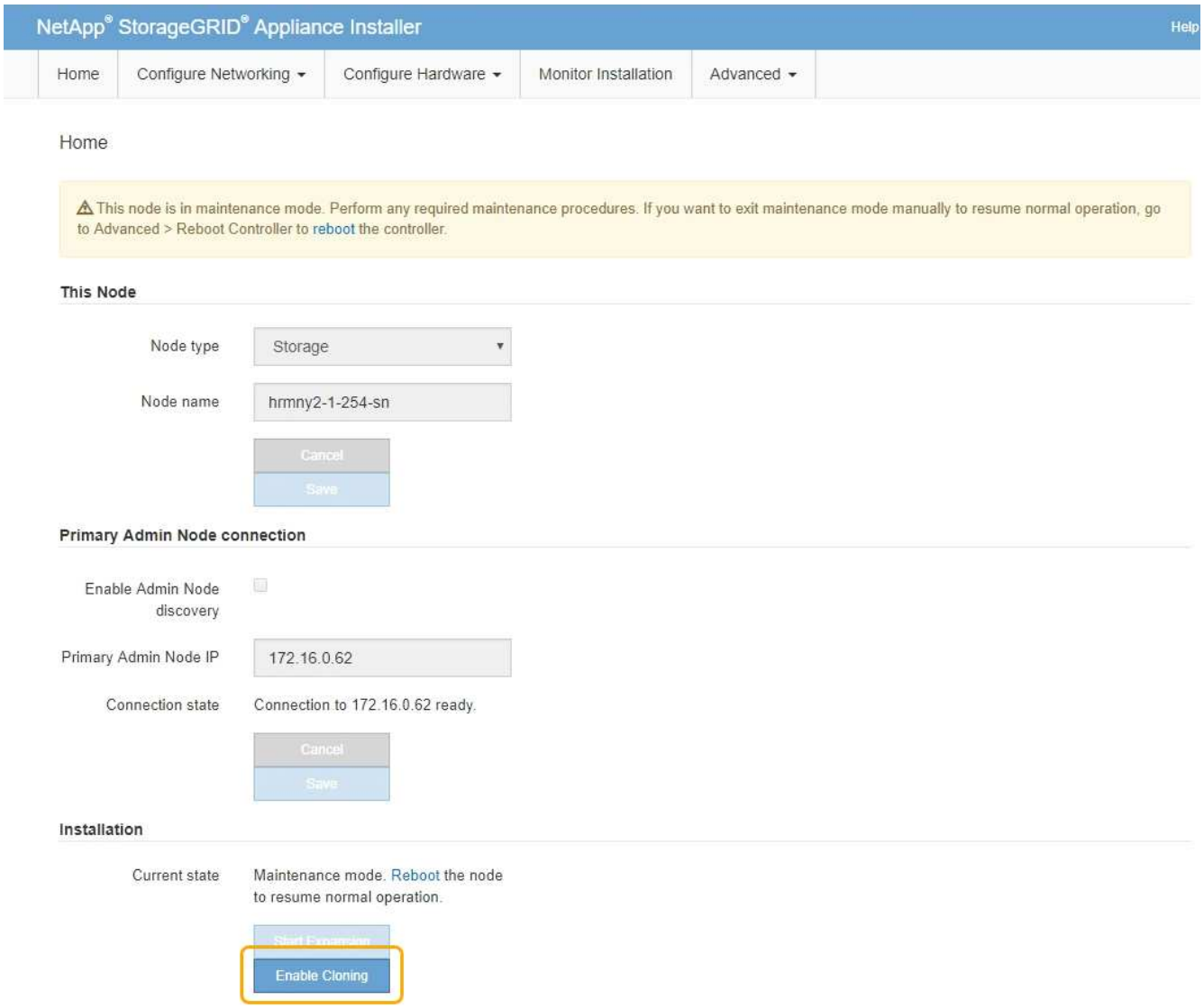
  SG5700 存储设备

  SG6000 存储设备

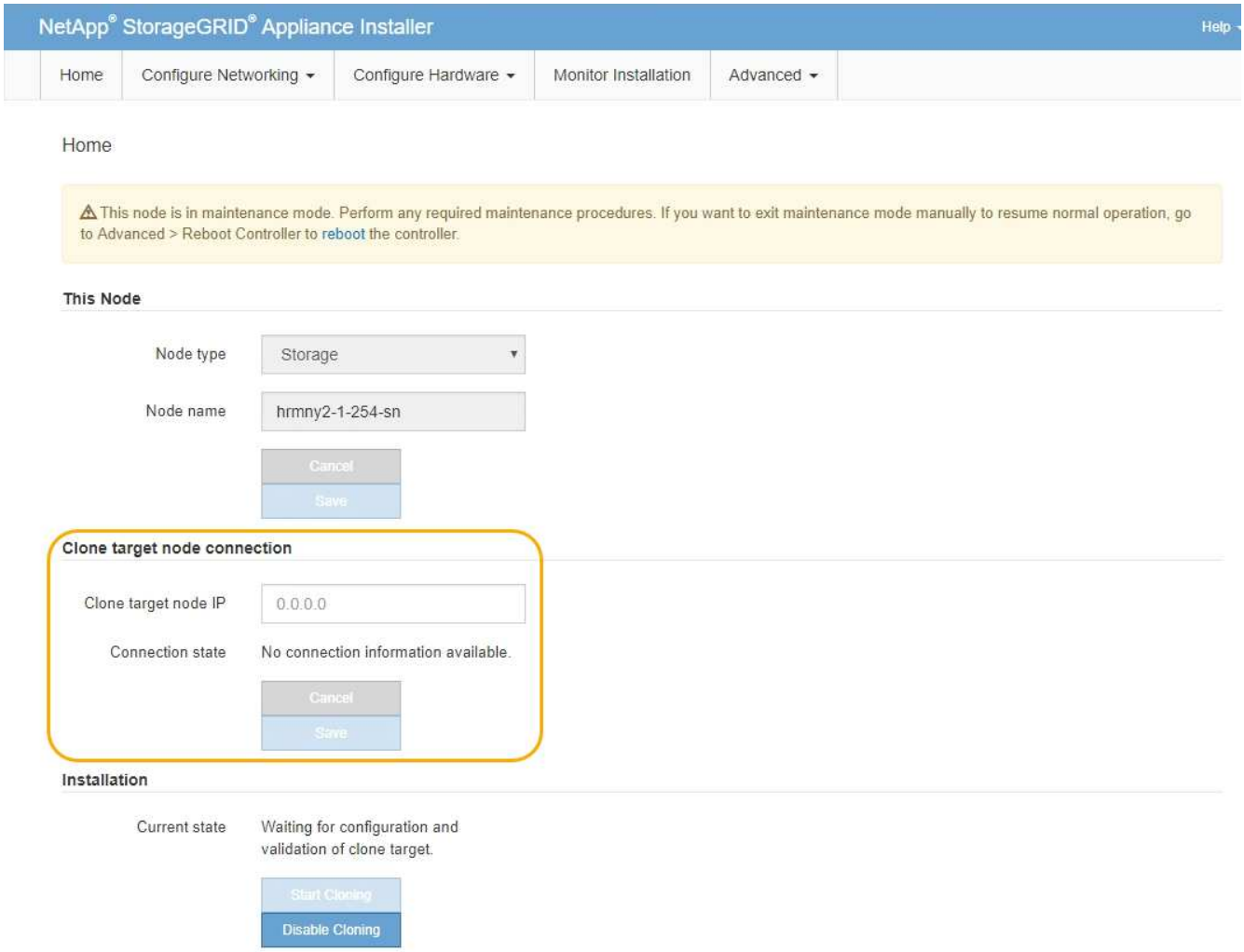
一次只应克隆一个设备节点，以保持 StorageGRID 网络性能和数据可用性。

步骤

1. 将要克隆的源节点置于维护模式。
2. 从源节点上的 StorageGRID 设备安装程序中，在主页的安装部分中，选择 * 启用克隆 * 。



主管理节点连接部分将替换为克隆目标节点连接部分。

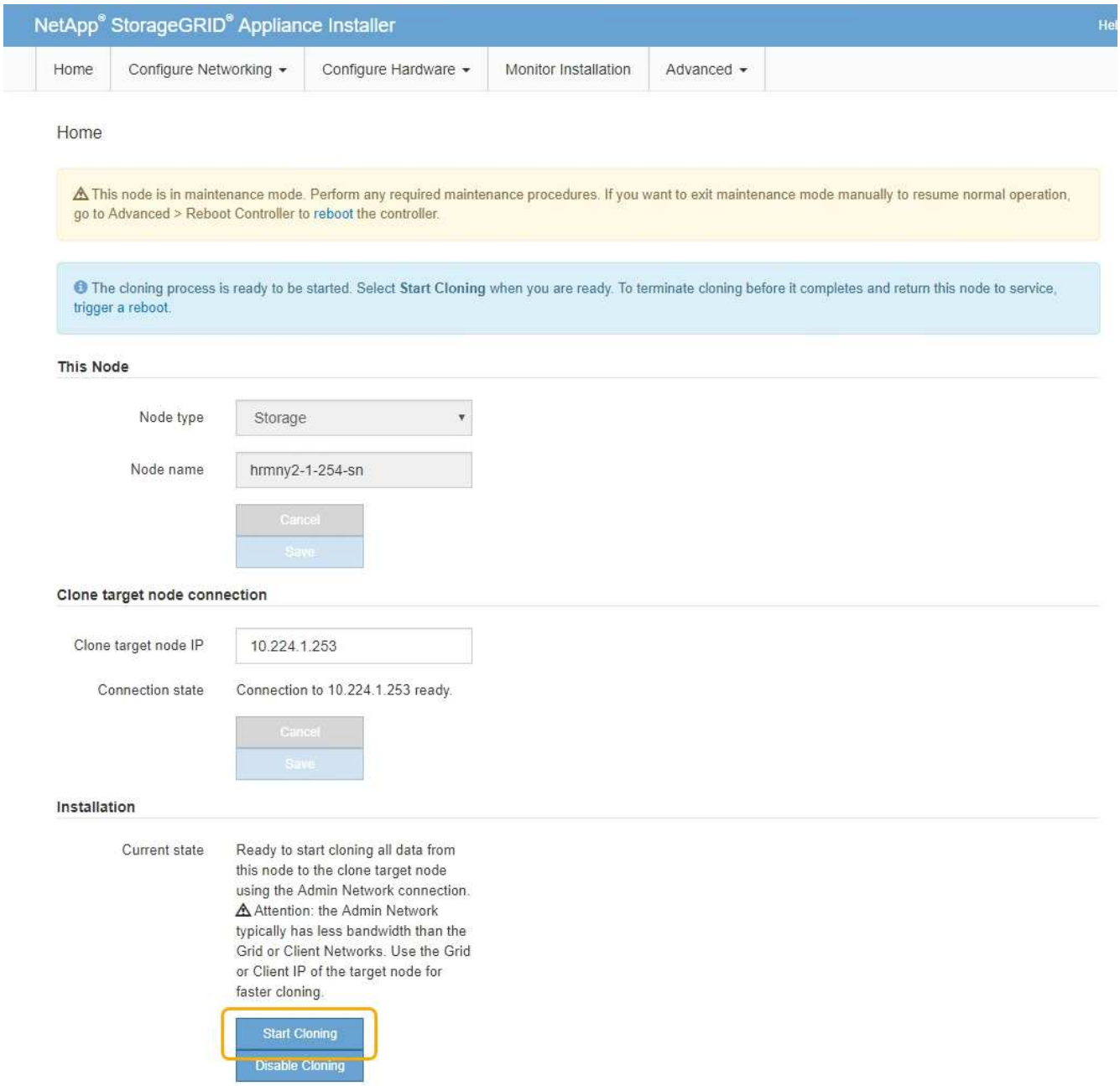


3. 对于 * 克隆目标节点 IP* ，输入分配给目标节点的临时 IP 地址，以便网络用于克隆数据传输流量，然后选择 * 保存 * 。

   通常，您可以输入网格网络的 IP 地址，但如果需要使用其他网络来传输克隆数据传输流量，请输入该网络上目标节点的 IP 地址。

   使用 1-GbE 管理网络进行克隆数据传输会导致克隆速度变慢。

配置并验证目标设备后，在 "Installation" 部分中，源节点上会启用 * 开始克隆 * 。



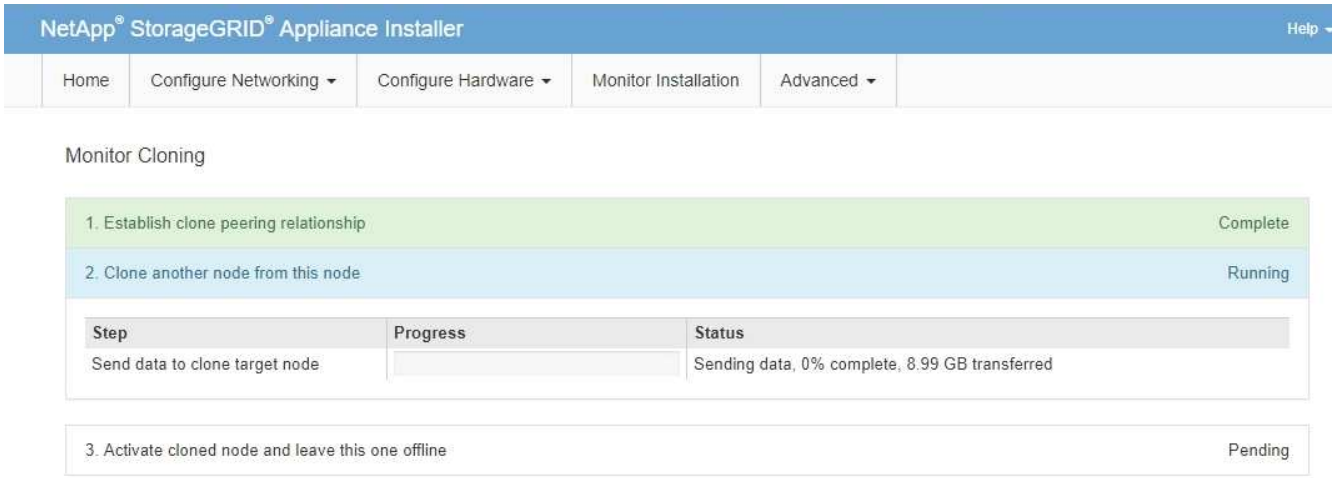
如果存在阻止克隆的问题，则不会启用 * 启动克隆 * ，必须解决的问题将列为 * 连接状态 * 。源节点和目标设备的 StorageGRID 设备安装程序主页均列出了这些问题。一次仅显示一个问题描述，状态会随着条件的变化自动更新。解决所有克隆问题以启用 * 开始克隆 * 。

启用 * 开始克隆 * 后， * 当前状态 * 将指示为克隆流量选择的 StorageGRID 网络以及有关使用该网络连接的信息。

设备节点克隆的注意事项和要求

4. 在源节点上选择 * 开始克隆 * 。
5. 在源节点或目标节点上使用 StorageGRID 设备安装程序监控克隆进度。

   源节点和目标节点上的 StorageGRID 设备安装程序指示相同的状态。



"Monitor Cloning" 页面提供了克隆过程每个阶段的详细进度：

- * 建立克隆对等关系 * 显示克隆设置和配置的进度。
- * 从此节点克隆另一个节点 * 将显示数据传输的进度。（克隆过程的这一部分可能需要几天时间才能完成。）
- * 激活克隆的节点并使其脱机 * 将显示在数据传输完成后将控制权移交给目标节点并将源节点置于预安装状态的进度。

6. 如果需要在克隆完成之前终止克隆过程并将源节点恢复服务，请在源节点上转到 StorageGRID 设备安装程序主页页面，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动到 StorageGRID * 。

   如果克隆过程终止：

   - 源节点将退出维护模式并重新加入 StorageGRID 。
   - 目标节点将保持预安装状态。要重新启动源节点的克隆，请从步骤 1 中重新启动克隆过程。

成功完成克隆后：

- 源节点和目标节点交换 IP 地址：
  - 现在，目标节点将使用最初分配给源节点的网格网络，管理网络和客户端网络 IP 地址。
  - 现在，源节点将使用最初分配给目标节点的临时 IP 地址。
- 目标节点将退出维护模式并加入 StorageGRID ，从而替换源节点。
- 源设备处于预安装状态，就像您已安装一样 已准备好重新安装。

> 如果设备未重新加入网格，请转到源节点的 StorageGRID 设备安装程序主页页面，选择 * 高级 * > * 重新启动控制器 * ，然后选择 * 重新启动到维护模式 * 。在源节点以维护模式重新启动后，重复节点克隆操作步骤 。

如果目标节点发生意外的问题描述 ，则用户数据将作为恢复选项保留在源设备上。目标节点成功重新加入 StorageGRID 后，源设备上的用户数据已过时，不再需要。如果需要，请 StorageGRID 支持部门清除源设备以销毁此数据。

您可以

- 将源设备用作其他克隆操作的目标：不需要其他配置。此设备已分配最初为第一个克隆目标指定的临时 IP 地址。
- 将源设备安装为新设备节点并进行设置。
- 如果源设备不再用于 StorageGRID ，请丢弃该源设备。

查看审核日志

查看审核日志：概述

这些说明包含有关 StorageGRID 审核消息和审核日志的结构和内容的信息。您可以使用此信息读取和分析系统活动的审核跟踪。

这些说明适用于负责生成系统活动和使用情况报告的管理员，这些报告需要分析 StorageGRID 系统的审核消息。

要使用文本日志文件，您必须有权访问管理节点上配置的审核共享。

有关配置审核消息级别和使用外部系统日志服务器的信息，请参见 配置审核消息和日志目标。

相关信息

- 管理 StorageGRID

审核消息流和保留

所有 StorageGRID 服务都会在系统正常运行期间生成审核消息。您应了解这些审核消息如何在 StorageGRID 系统中移动到 `audit.log` 文件。

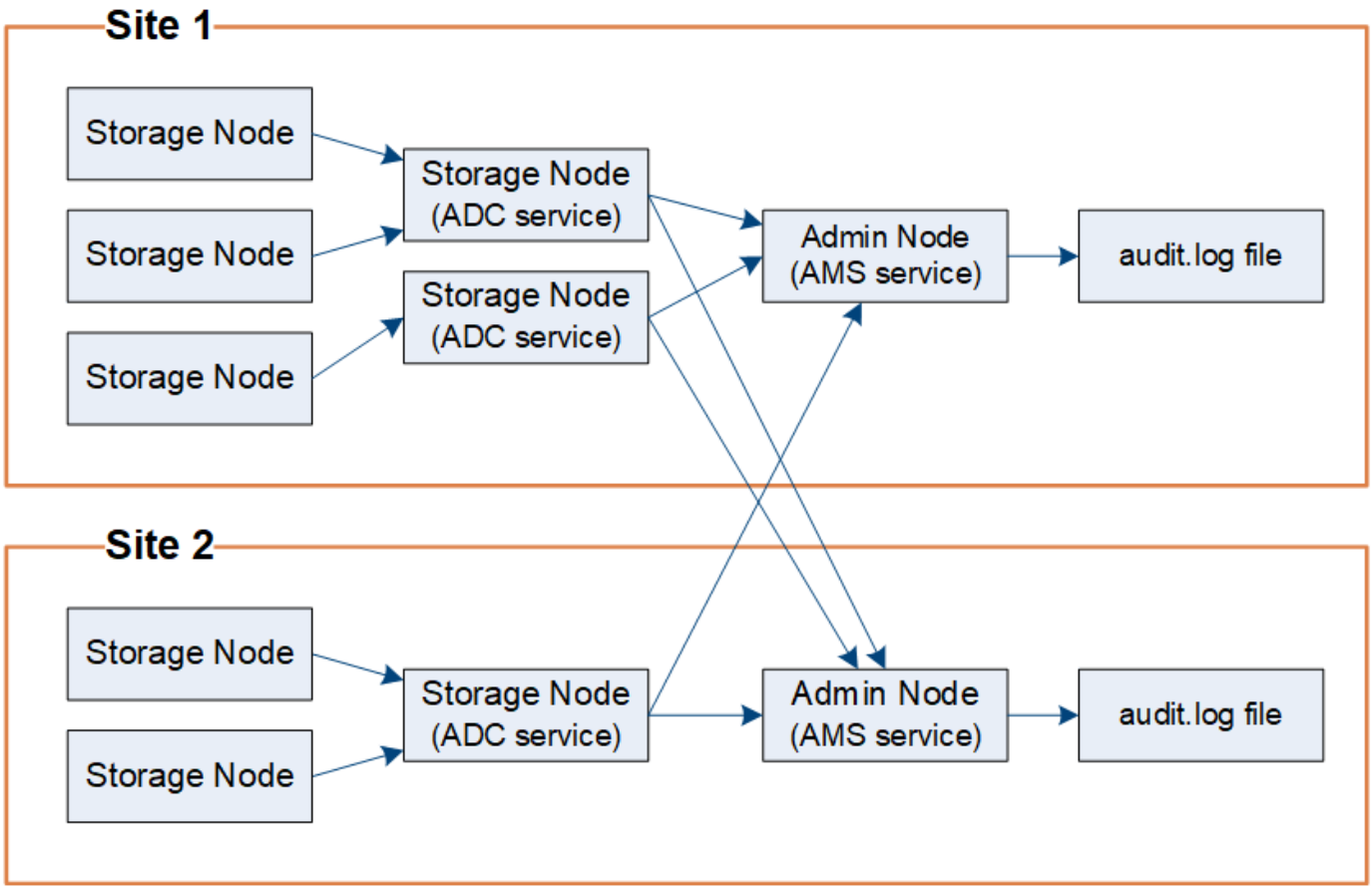
审核消息流

审核消息由管理节点以及具有管理域控制器（ ADO ）服务的存储节点处理。

如审核消息流程图所示，每个 StorageGRID 节点都会将其审核消息发送到数据中心站点的一个模板服务。每个站点上安装的前三个存储节点会自动启用此 ADC-Service 。

反过来，每个 ADC 服务都充当中继，并将其审核消息集合发送到 StorageGRID 系统中的每个管理节点，从而为每个管理节点提供完整的系统活动记录。

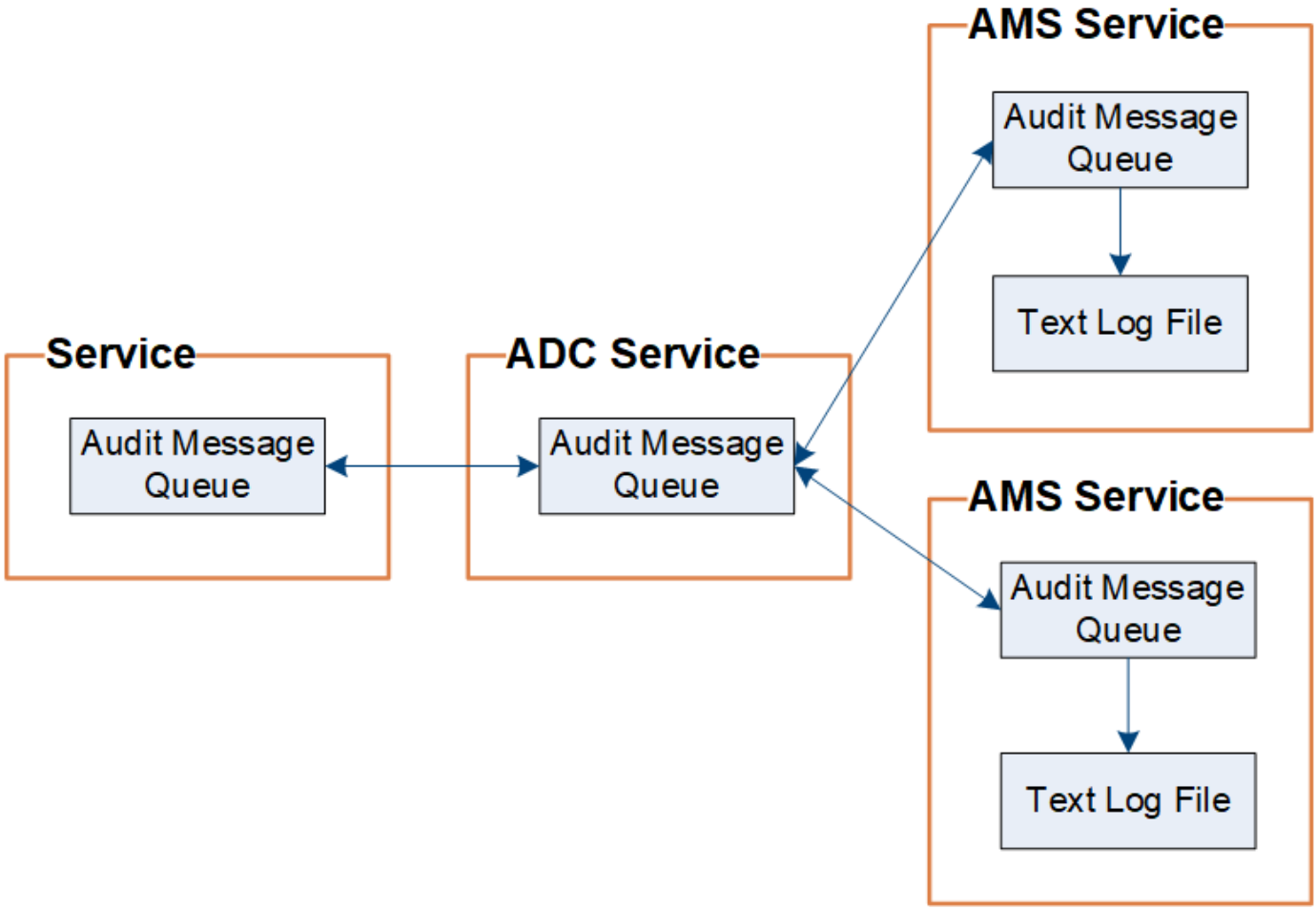
每个管理节点都会将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log` 。



审核消息保留

StorageGRID 使用复制和删除过程来确保在将审核消息写入审核日志之前不会丢失任何审核消息。

当节点生成或转发审核消息时，此消息会存储在网格节点的系统磁盘上的审核消息队列中。此消息的副本始终保留在审核消息队列中，直到将此消息写入管理节点的 ` /var/local/audit/export` 目录中的审核日志文件为止。这有助于防止传输期间丢失审核消息。



由于网络连接问题或审核容量不足，审核消息队列可能会暂时增加。随着队列的增加，它们会占用每个节点的 ` /var/local/` 目录中更多的可用空间。如果问题描述 仍然存在，并且节点的审核消息目录过满，则各个节点将优先处理其积压工作，并暂时不可用于处理新消息。

具体来说，您可能会看到以下行为：

- 如果管理节点使用的 ` /var/local/audit/export` 目录已满，则管理节点将标记为不可用于新的审核消息，直到目录不再全满为止。S3 和 Swift 客户端请求不受影响。如果无法访问审核存储库，则会触发 XAMS （无法访问审核存储库）警报。
- 如果具有` 服务的存储节点使用的 ` /var/local/ 目录已满 92% ，则该节点将标记为不可用于审核消息，直到该目录仅已满 87% 为止。对其他节点的 S3 和 Swift 客户端请求不受影响。如果无法访问审核中继，则会触发 NRLY （可用审核中继）警报。

> 如果没有可用于此` 服务的存储节点，则存储节点会将审核消息本地存储在 ` /var/local/log/localaudit.log 文件中。

- 如果存储节点使用的 ` /var/local/` 目录已满 85% ，则该节点将开始拒绝服务不可用` 为 `503 的 S3 和 Swift 客户端请求。

以下类型的问题可能会使发生原因 审核消息队列变得非常庞大：

- 管理节点或存储节点使用 ADC-Service 中断的情况。如果系统的一个节点已关闭，则其余节点可能会回记录。

- 超过系统审核容量的持续活动率。
- 由于与审核消息无关的原因，` 存储节点上的 ` /var/local/ 空间已满。发生这种情况时，节点将停止接受新的审核消息，并优先处理当前的积压工作，而这可能会使发生原因 回退到其他节点上。

大型审核队列警报和审核消息已排队（ **Audit Messages Queued** ， **AMQS** ）警报

为了帮助您监控一段时间内审核消息队列的大小，当存储节点队列或管理节点队列中的消息数量达到特定阈值时，将触发 * 大型审核队列 * 警报和原有 AMQS 警报。

如果触发了 * 大型审核队列 * 警报或原有 AMQS 警报，请首先检查系统上的负载—如果最近发生了大量事务，则警报和警报应随着时间的推移而解决，并且可以忽略。

如果警报或警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将客户端写入和客户端读取的审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 "配置审核消息和日志目标。 "

重复的消息

如果发生网络或节点故障， StorageGRID 系统会采取保守的方法。因此，审核日志中可能存在重复的消息。

访问审核日志文件

审核共享包含活动的 `audit.log` 文件和任何压缩的审核日志文件。为了便于访问审核日志，您可以配置客户端对 NFS 和 CIFS 的审核共享的访问权限（ CIFS 已弃用）。您也可以直接从管理节点的命令行访问审核日志文件。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。
- 您必须知道管理节点的 IP 地址。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 转到包含审核日志文件的目录：

```
cd /var/local/audit/export
```

3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

相关信息

管理 StorageGRID

审核日志文件轮换

审核日志文件会保存到管理节点的 ` /var/local/audit/export` 目录中。活动的审核日志文件

名为 `audit.log` 。

> 您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。请参见 配置审核消息和日志目标。

每天保存一次活动的 `audit.log` 文件，并启动一个新的 `audit.log` 文件。已保存文件的名称以 ` yyyy-mm-dd.txt_` 的格式指示其保存时间。如果在一天内创建了多个审核日志，则文件名将使用保存文件的日期，并附加一个数字，格式为 ` yyyy-mm-dd.txt.n_` 。例如， `2018-04-15.txt` 和 `2018-04-15.txt.1` 是在 2018 年 4 月 15 日创建并保存的第一个和第二个日志文件。

一天后，保存的文件将按 ` yyyy-mm-dd.txt.gz_` 格式进行压缩和重命名，从而保留原始日期。随着时间的推移，这会导致为管理节点上的审核日志分配的存储被占用。脚本可监控审核日志空间占用情况，并根据需要删除日志文件，以释放 ` /var/local/audit/export` 目录中的空间。审核日志会根据创建日期进行删除，最早的日志会先删除。您可以在以下文件中监控脚本的操作： ` /var/local/log/manage-audit.log` 。

此示例显示了活动的 `audit.log` 文件，前一天的文件（ `2018-04-15.txt` ）和前一天的压缩文件（ `2018-04-14.txt.gz` ）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

审核日志文件和消息格式

您可以使用审核日志收集有关系统的信息并对问题进行故障排除。您应了解审核日志文件的格式以及审核消息使用的常规格式。

审核日志文件格式

审核日志文件位于每个管理节点上，其中包含一组单独的审核消息。

每个审核消息都包含以下内容：

- 触发审核消息（ ATIM ）的事件的协调世界时（ UTC ），格式为 ISO 8601 ，后跟一个空格：

  ` YYYY-MM-DDTHH： MM： SS.UUUUUUU_` ，其中 ` *UUUU*` 为微秒。

- 审核消息本身，括在方括号内，以 `AUDT` 开头。

以下示例显示了一个审核日志文件中的三条审核消息（为便于阅读，添加了换行符）。这些消息是在租户创建 S3 存储分段并向该存储分段添加两个对象时生成的。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

以默认格式，审核日志文件中的审核消息不易阅读或解释。您可以使用 `audit-explain` 工具获取审核日志中审核消息的简化摘要。您可以使用 `audit-sum` 工具总结已记录的写入，读取和删除操作的数量以及这些操作所需的时间。

相关信息

使用审核解释工具

使用 audit-sum 工具

您可以使用 audit-explain 工具将审核日志中的审核消息转换为易于阅读的格式。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 passwords.txt 文件。
- 您必须知道主管理节点的 IP 地址。

关于此任务

主管理节点上提供的 audit-explain 工具可在审核日志中简化审核消息的摘要。

audit-explain 工具主要供技术支持在故障排除操作期间使用。处理 审核 - 解释 查询可能会占用大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 audit-explain 工具的典型输出。当帐户 ID 为 92484777680322627870 的 S3 租户使用 S3 PUT 请求创建名为 "Bucket1" 的存储分段并向该存储分段添加三个对象时，会生成这四条 SPUT 审核消息。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

audit-explain 工具可以处理简单或压缩的审核日志。例如：

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

audit-explain 工具还可以同时处理多个文件。例如：

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

最后， audit-explain 工具可以接受来自管道的输入，这样，您可以使用 grep 命令或其他方法筛选和预处理输入。例如：

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

由于审核日志可能非常大且解析速度较慢，因此您可以通过筛选要查看的部分并在这些部分（而不是整个文件）上运行 `audit-explain` 来节省时间。

> `audit-explain` 工具不接受将压缩文件作为管道输入。要处理压缩的文件，请将其文件名作为命令行参数提供，或者使用 `zcat` 工具先解压缩这些文件。例如：

```
zcat audit.log.gz | audit-explain
```

使用 `help` （ `-h` ） 选项查看可用选项。例如：

```
$ audit-explain -h
```

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 输入以下命令，其中 ` /var/local/audit/export/audit.log` 表示要分析的一个或多个文件的名称和位置：

   ` $ audit-explain /var/local/audit/export/audit.log`

   `audit-explain` 工具可为指定文件中的所有消息输出可供用户读取的解释。

   > 为了缩短行长度并提高可读性，默认情况下不会显示时间戳。如果要查看时间戳，请使用 timestamp （` -t` ）选项。

相关信息

SPUT： S3 PUT

使用 **audit-sum** 工具

您可以使用 `audit-sum` 工具对写入，读取，标头和删除审核消息进行计数，并查看每种操作类型的最小，最大和平均时间（或大小）。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。

- 您必须知道主管理节点的 IP 地址。

关于此任务

主管理节点上提供的 `audit-sum` 工具总结了记录的写入，读取和删除操作数量以及这些操作所需的时间。

> `audit-sum` 工具主要供技术支持在故障排除操作期间使用。处理 `audit-sum` 查询可能会占用大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 `audit-sum` 工具的典型输出。此示例显示了协议操作所需的时间。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

`audit-sum` 工具可在审核日志中提供以下 S3 ， Swift 和 ILM 审核消息的计数和时间：

代码	**Description**	请参见
ARCT	从云层检索归档	ARCT ： 从云层检索归档
上一个月	归档存储云层	SCT ： 归档存储云层
标识	ILM Initiated Delete ： 记录 ILM 开始删除对象的过程。	idel ： ILM 已启动删除
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。	SDEL ： S3 delete
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。	SGET ： S3 GET
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	Shea ： S3 机头

代码	Description	请参见
SPUT	S3 PUT： 记录成功的事务以创建新对象或存储分段。	SPUT： S3 PUT
WDEL	Swift delete： 记录成功的事务以删除对象或容器。	WDEL： Swift delete
wget	Swift get： 记录成功的事务以检索对象或列出容器中的对象。	WGET： Swift GET
WHEA	Swift head： 记录成功的事务以检查是否存在对象或容器。	WHEA： Swift head
WWPUT	Swift PUT： 记录成功的事务以创建新对象或容器。	WWPUT： Swift PUT

`audit-sum` 工具可以处理纯审核日志或压缩的审核日志。例如：

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

`audit-sum` 工具还可以同时处理多个文件。例如：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

最后， `audit-sum` 工具还可以接受来自管道的输入，这样，您可以使用 `grep` 命令或其他方法筛选和预处理输入。例如：

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

此工具不接受将压缩文件作为管道输入。要处理压缩的文件，请将其文件名作为命令行参数提供，或者使用 `zcat` 工具先解压缩这些文件。例如：

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

您可以使用命令行选项将存储分段上的操作与对象上的操作分开进行汇总，或者按存储分段名称，时间段或目标类型对消息摘要进行分组。默认情况下，摘要会显示最小，最大和平均操作时间，但您可以使用 `size` （ `-s` ） 选项查看对象大小。

使用 `help` （ `-h` ） 选项查看可用选项。例如：

```
 $ audit-sum -h
```

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 如果要分析与写入，读取，磁头和删除操作相关的所有消息，请执行以下步骤：
   a. 输入以下命令，其中 ` /var/local/audit/export/audit.log` 表示要分析的一个或多个文件的名称和位置：

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      此示例显示了 `audit-sum` 工具的典型输出。此示例显示了协议操作所需的时间。

      ```
        message group           count     min(sec)        max(sec)
      average(sec)
        =============           =====     ========        ========
      ============
        IDEL                      274
        SDEL                   213371        0.004          20.934
      0.352
        SGET                   201906        0.010        1740.290
      1.132
        SHEA                    22716        0.005           2.349
      0.272
        SPUT                 1771398        0.011        1770.563
      0.487
      ```

在此示例中， SGET （ S3 GET ）操作的平均速度最慢，为 1.13 秒，但 SGET 和 SPUT （ S3 PUT ）操作的最坏情况时间都较长，约为 1 ， 770 秒。

b. 要显示速度最慢的 10 个检索操作，请使用 grep 命令仅选择 SGET 消息，并添加较长的输出选项（` -l` ）以包含对象路径： `grep SGET audit.log ； audit-sum -l`

结果包括类型（对象或分段）和路径，您可以通过此类结果在审核日志中添加与这些特定对象相关的其他消息。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== =============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
在此示例输出中，您可以看到，三个最慢的 S3 GET 请求针对的是大小约为 5 GB 的对象，该大小远远大于其他对象。大容量导致最差情况检索时间较慢。

3. 如果要确定要将哪些大小的对象输入网格并从网格中检索到，请使用 size 选项（` -s` ）：

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

在此示例中， SPUT 的平均对象大小小于 2.5 MB ，但 SGET 的平均大小要大得多。SPUT 消息的数量远远高于 SGET 消息的数量，这表明大多数对象永远不会被检索到。

4. 如果要确定昨天的检索速度是否较慢：
   a. 在相应的审核日志上输入命令并使用 group-by-time 选项（` -gt` ），后跟时间段（例如 15M ， 1H ， 10S ）问题描述：

```
grep SGET audit.log | audit-sum -gt 1H
```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

这些结果显示 S3 GET 流量在 06： 00 到 07： 00 之间达到高峰。这些时间的最大和平均时间也明显较高，并且不会随着数量的增加而逐渐增加。这表明容量已超出某个位置，可能是在网络中，也可能是在网格处理请求的能力中。

b. 要确定昨天每小时检索的对象大小，请在命令中添加 size 选项（` -s` ）：

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

这些结果表明，当整体检索流量达到最大值时，会发生一些非常大的检索。

c. 要查看更多详细信息，请使用 `audit-explain` 工具查看该时段的所有 SGET 操作：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

如果 grep 命令的输出应为多行，请添加 `less` 命令，以便一次显示一页（一个屏幕）的审核日志文件内容。

5. 如果要确定存储分段上的 SPUT 操作是否比对象的 SPUT 操作慢：

a. 首先使用 ` -go` 选项，该选项可分别对对象和存储分段操作的消息进行分组：

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

结果显示，存储分段的 SPUT 操作与对象的 SPUT 操作具有不同的性能特征。

b. 要确定哪些存储分段的 SPUT 操作最慢，请使用 ` -GB` 选项，该选项可按存储分段对消息进行分组：

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. 要确定哪些分段的 SPUT 对象大小最大，请使用 ` -GB` 和 ` -s` 选项：

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

相关信息

使用审核解释工具

审核消息格式

在 StorageGRID 系统中交换的审核消息包括所有消息通用的标准信息以及描述所报告事件或活动的特定内容。

如果 `audit-explain` 和 `audit-sum` 工具提供的摘要信息不足，请参阅本节了解所有审核消息的常规格式。

下面是可能显示在审核日志文件中的审核消息示例：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

每个审核消息都包含一个属性元素字符串。整个字符串用方括号（`[]` ）括起来，字符串中的每个属性元素都具有以下特征：

- 括在方括号中 `` .....
- 由字符串 `AUDT` 引入，表示审核消息
- 前后不带分隔符（无逗号或空格）
- 由换行符 ` n` 终止

每个元素都包含一个属性代码，一个数据类型以及一个以以下格式报告的值：

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

消息中的属性元素数量取决于消息的事件类型。属性元素不按任何特定顺序列出。

以下列表介绍了这些属性元素：

- `attr` 是所报告属性的四字符代码。某些属性对于所有审核消息都是通用的，而其他属性则针对事件。
- `type` 是值的编程数据类型的四字符标识符，例如 UI64 ， FC32 等。此类型用圆括号括起来 ` （） ` 。
- `value` 是属性的内容，通常为数字或文本值。值始终后跟冒号（ ` ： ` ）。数据类型 CStr 的值由双引号 ` " "` 括起来。

相关信息

使用审核解释工具

使用 audit-sum 工具

审核消息

审核消息中的常见元素

数据类型

审核消息示例

数据类型

使用不同的数据类型将信息存储在审核消息中。

Type	Description
UI32	无符号长整数（ 32 位）；它可以存储 0 到 4 ， 294 ， 967 ， 295 之间的数字。
UI64	无符号双长整数（ 64 位）；它可以存储 0 到 18 ， 446 ， 744 ， 073 ， 709 ， 551 ， 615 之间的数字。
FC32	四字符常量；一个 32 - 位无符号整数值，表示为四个 ASCII 字符，如 "ABCD" 。
iPad	用于 IP 地址。

Type	Description
CStr	一个长度可变的数组，由 UTF-8 - 字符组成。可以按照以下约定对字符进行转义： • 反斜杠为 \\ 。 • 回车符为 • 双引号为 " 。 • 换行符（新行）为 • 字符可以替换为其十六进制等效项（格式为 \xHH ，其中 HH 是表示该字符的十六进制值）。

事件专用数据

审核日志中的每个审核消息都会记录特定于系统事件的数据。

在用于标识消息本身的打开 ` [AUDT ： ` 容器之后，下一组属性将提供有关审核消息所述事件或操作的信息。以下示例突出显示了这些属性：

```
2018-12-05T08 ： 24 ： 45.921845 [AUTT ： \[RSLT\ （ FC32\ ） ： SUC\] \[ 时间 \ （ UI64\ ） ：
11454\]\[SAIP\ （ IPAD\ ） ： "10.224.0.100"\]\"S3AI\ （ C3CSST\" ） ： " ： "KST" （ S36599" ） ：
```

`ATYP` 元素（在示例中加下划线）用于标识生成消息的事件。此示例消息包含 Shea 消息代码（ [ATYP （ FC32 ） ： Shea] ），表示此消息是由成功的 S3 head 请求生成的。

相关信息

审核消息中的常见元素

审核消息

审核消息中的常见元素

所有审核消息都包含通用要素。

代码	Type	Description
在中	FC32	模块 ID ： 生成消息的模块 ID 的四个 - 字符标识符。这表示生成审核消息的代码段。
ANID	UI32	Node ID ： 分配给生成消息的服务的网格节点 ID 。在配置和安装 StorageGRID 系统时，系统会为每个服务分配一个唯一的标识符。无法更改此 ID 。

代码	Type	Description
ASE	UI64	审核会话标识符：在先前版本中，此元素表示在服务启动后初始化审核系统的时间。此时间值是自操作系统 Epoch （ 1970 年 1 月 1 日 00： 00： 00 UTC ）以来以微秒为单位测量的。 • 注： * 此元素已废弃，不再显示在审核消息中。
ASQN	UI64	序列计数：在先前版本中，对于网格节点（ ANID ）上生成的每个审核消息，此计数器会递增，并在服务重新启动时重置为零。 • 注： * 此元素已废弃，不再显示在审核消息中。
Atid	UI64	跟踪 ID ： 由单个事件触发的一组消息共享的标识符。
Atim	UI64	timestamp ： 生成触发审核消息的事件的时间，以操作系统 Epoch （ 1970 年 1 月 1 日 00： 00： 00 UTC ）之后的微秒为单位。请注意，用于将时间戳转换为本地日期和时间的大多数可用工具均以毫秒为基础。 可能需要对记录的时间戳进行舍入或截断。`audit.log` 文件中审核消息开头显示的人工 - 可读时间是 ISO 8601 格式的 ATIM 属性。日期和时间以 ` YYYY-MMDDDTHH： MM： SS.UUUUUUU_` 表示，其中 `T` 是一个文字字符串，用于指示日期时间段的开始。` UUUUUUU_` 为微秒。
ATYP	FC32	Event Type ： 所记录事件的四 - 字符标识符。这将控制消息的 " 有效负载 " 内容：包含的属性。
保护程序	UI32	version ： 审核消息的版本。随着 StorageGRID 软件的发展，新版本的服务可能会在审核报告中加入新功能。通过此字段，可以在 AMS 服务中实现向后兼容性，以处理来自旧版本服务的消息。
RSLT	FC32	result ： 事件，进程或事务的结果。如果与消息无关，则不会使用 none 而不是 SUC ，这样就不会意外筛选该消息。

审核消息示例

您可以在每个审核消息中找到详细信息。所有审核消息都使用相同的格式。

以下是可能出现在 `audit.log` 文件中的审核消息示例：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

审核消息包含有关所记录事件的信息以及有关审核消息本身的信息。

要确定审核消息记录的事件，请查找 ATYP 属性（突出显示在下方）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP\(FC32\):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性的值为 SPUT 。SPUT 表示 S3 PUT 事务，用于记录对象载入到存储分段的情况。

以下审核消息还会显示与对象关联的存储分段：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

要发现 PUT 事件发生的时间，请注意审核消息开头的通用协调时间（ UTC ）时间戳。此值为审核消息本身的 ATIM 属性的用户 - 可读版本：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

Atim 会以微秒为单位记录自 UNIX Epoch 开始以来的时间。在此示例中，值 `1405631878959669` 转换为 2014 年 7 月 17 日星期四 21： 17： 59 UTC 。

相关信息

SPUT： S3 PUT

审核消息中的常见元素

审核消息和对象生命周期

每次载入，检索或删除对象时都会生成审核消息。您可以通过查找特定于 API （ S3 或 Swift ）的审核消息在审核日志中标识这些事务。

审核消息通过每个协议专用的标识符进行链接。

协议	代码
链接 S3 操作	S3BK （ S3 分段）和 / 或 S3KY （ S3 密钥）
链接 Swift 操作	WCON （ Swift 容器）和 / 或 WOBJ （ Swift 对象）
链接内部操作	CBID （对象的内部标识符）

审核消息的时间

由于网格节点之间的时间差异，对象大小和网络延迟等因素，不同服务生成的审核消息的顺序可能与本节示例中所示的顺序不同。

信息生命周期管理策略配置

使用默认 ILM 策略（基线 2 副本），对象数据复制一次，总共复制两个副本。如果 ILM 策略需要两个以上的副本，则每个额外的副本还会另外显示一组 CBRE ， CBSE 和 SCMT 消息。有关 ILM 策略的详细信息，请参见有关通过信息生命周期管理管理对象的信息。

归档节点

归档节点向外部归档存储系统发送对象数据时生成的一系列审核消息与存储节点的类似，只是没有 SCMT （存储对象提交）消息。 对于对象数据的每个归档副本，系统会生成 ATCE （ Archive Object Store Begin ）和

ASCE （ Archive Object Store End ）消息。

归档节点从外部归档存储系统检索对象数据时生成的一系列审核消息与存储节点的类似，只是为每个检索到的对象数据副本生成了 ARCB （归档对象检索开始）和 Arce （归档对象检索结束）消息。

归档节点从外部归档存储系统删除对象数据时生成的一系列审核消息与存储节点的类似，只是没有 Srem （对象存储删除）消息，并且每个删除请求都有一条 AREM （归档对象删除）消息。

相关信息

使用 ILM 管理对象

对象载入事务

您可以通过查找特定于 API （ S3 或 Swift ）的审核消息，在审核日志中确定客户端载入事务。

下表列出了在载入事务期间生成的并非所有审核消息。仅包含跟踪载入事务所需的消息。

S3 载入审核消息

代码	**Name**	**Description**	跟踪	请参见
SPUT	S3 PUT 事务	S3 PUT 载入事务已成功完成。	CBID ， S3BK ， S3KY	SPUT ： S3 PUT
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	ORLM ： 符合对象规则

Swift 载入审核消息

代码	**Name**	**Description**	跟踪	请参见
WWPUT	Swift PUT 事务	Swift PUT 载入事务已成功完成。	CBID ， WCON ， WOBJ	WWPUT ： Swift PUT
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	ORLM ： 符合对象规则

示例： **S3** 对象载入

下面的一系列审核消息是在 S3 客户端将对象载入存储节点（ LDR 服务）时生成并保存到审核日志中的审核消息的示例。

在此示例中，活动 ILM 策略包括常用 ILM 规则，创建 2 个副本。

> 在以下示例中并未列出事务期间生成的所有审核消息。仅列出与 S3 载入事务（ SPUT ）相关的那些。

此示例假设先前已创建 S3 存储分段。

SPUT： S3 PUT

此时将生成 SPUT 消息，以指示已发出 S3 PUT 事务，以便在特定存储分段中创建对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM： 符合对象规则

ORLM 消息指示已对此对象满足 ILM 策略要求。此消息包含对象的 CBID 以及应用的 ILM 规则的名称。

对于复制的对象， " LOC" 字段包含对象位置的 LDR 节点 ID 和卷 ID 。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

对于经过纠删编码的对象， LOC 字段包括纠删编码配置文件 ID 和纠删编码组 ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

路径字段包括 S3 存储分段和密钥信息或 Swift 容器和对象信息，具体取决于所使用的 API 。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

对象删除事务

您可以通过查找特定于 API （ S3 和 Swift ）的审核消息来确定审核日志中的对象删除事务。

下表列出了在删除事务期间生成的并非所有审核消息。仅包含跟踪删除事务所需的消息。

S3 删除审核消息

代码	Name	Description	跟踪	请参见
SDEL	S3 删除	请求从存储分段中删除对象。	CBID ， S3KY	SDEL： S3 delete

Swift 删除审核消息

代码	Name	Description	跟踪	请参见
WDEL	Swift 删除	请求从容器或容器中删除对象。	CBID ， WOBJ	WDEL： Swift delete

示例： **S3** 对象删除

当 S3 客户端从存储节点（ LDR 服务）中删除对象时，系统会生成一条审核消息并将其保存到审核日志中。

在删除事务期间生成的审核消息并非都在以下示例中列出。仅列出与 S3 删除事务（ SDEL ）相关的那些。

SDEL： S3 删除

当客户端向 LDR 服务发送删除对象请求时，对象删除即开始。此消息包含用于删除对象的存储分段以及用于标识对象的 S3 密钥。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

对象检索事务

您可以通过查找特定于 API （ S3 和 Swift ）的审核消息来确定审核日志中的对象检索事务。

下表列出了在检索事务期间生成的并非所有审核消息。仅包含跟踪检索事务所需的消息。

S3 检索审核消息

代码	Name	Description	跟踪	请参见
SGET	S3 GET	请求从存储分段中检索对象。	CBID ， S3BK ， S3KY	SGET： S3 GET

Swift 检索审核消息

代码	Name	Description	跟踪	请参见
wget	Swift GET	请求从容器中检索对象。	CBID ， WCON ， WOBJ	WGET： Swift GET

示例： **S3** 对象检索

当 S3 客户端从存储节点（ LDR 服务）检索对象时，系统会生成一条审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 检索事务（ SGET ）相关的那些。

SGET： S3 GET

当客户端向 LDR 服务发送获取对象请求时，对象检索即开始。此消息包含用于检索对象的存储分段以及用于标识对象的 S3 密钥。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

如果存储分段策略允许，客户端可以匿名检索对象，或者从其他租户帐户拥有的存储分段中检索对象。审核消息包含有关存储分段所有者的租户帐户的信息，以便您可以跟踪这些匿名请求和跨帐户请求。

在以下示例消息中，客户端会为存储在非自有存储分段中的对象发送 GET 对象请求。SBAI 和 SBAC 的值会记录存储分段所有者的租户帐户 ID 和名称，这与 S3AI 和 SACC 中记录的租户帐户 ID 和客户端名称不同。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

示例：对象上的 **S3 Select**

当 S3 客户端对某个对象发出 S3 Select 查询时，系统会生成审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 Select 事务（ SelectObjectContent ）相关的那些内容。

每个查询都会生成两条审核消息：一条用于执行 S3 Select 请求的授权（ S3SR 字段设置为 "Select" ），另一条用于在处理期间从存储中检索数据的后续标准 GET 操作。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

元数据更新消息

当 S3 客户端更新对象的元数据时，系统会生成审核消息。

S3 元数据更新审核消息

代码	Name	Description	跟踪	请参见
SUPD	已更新 S3 元数据	当 S3 客户端更新已载入对象的元数据时生成。	CBID ， S3KY ， HTRH	SUPD ： 已更新 S3 元数据

示例： **S3** 元数据更新

此示例显示了更新现有 S3 对象的元数据的成功事务。

SUPD： S3 元数据更新

S3 客户端请求（ SUPD ）更新 S3 对象（ S3KY ）的指定元数据（`x-AMZ-meta-*` ）。在此示例中，请求标头包含在字段 HTRH 中，因为它已配置为审核协议标头（ "* 配置 ">"* 监控 ""><"* 审核和系统日志服务器 "* ）。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

相关信息

配置审核消息和日志目标

审核消息

以下各节列出了系统返回的审核消息的详细说明。每个审核消息首先列在一个表中，该表按相关消息所代表的活动类别对相关消息进行分组。这些分组对于了解要审核的活动类型以及选择所需的审核消息筛选类型都很有用。

审核消息也会按其四个字符的代码的字母顺序列出。此字母列表可用于查找有关特定消息的信息。

本章中使用的四字符代码是审核消息中的 ATYP 值，如以下示例消息所示：

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

有关设置审核消息级别，更改日志目标以及使用外部系统日志服务器获取审核信息的信息，请参见 配置审核消

息和日志目标

审核消息类别

您应熟悉对审核消息进行分组的各个类别。这些组将根据消息表示的活动类别进行组织。

系统审核消息

您应熟悉属于系统审核类别的审核消息。这些事件与审核系统本身，网格节点状态，系统范围的任务活动（网格任务）和服务备份操作相关，可帮助您解决潜在问题。

代码	消息标题和问题描述	请参见
ECMC	缺少纠删编码数据片段：表示检测到缺少纠删编码数据片段。	ECMC ： 缺少擦除编码的数据片段
ECOC	Erasure 编码数据片段损坏：表示检测到擦除编码数据片段损坏。	EcC ： 擦除编码数据片段损坏
ETAF	安全身份验证失败：尝试使用传输层安全（ Transport Layer Security ， TLS ）进行连接失败。	ETAF ： 安全身份验证失败
GNRG	GNDS 注册：服务在 StorageGRID 系统中更新或注册了有关自身的信息。	GNRG ： GNDS 注册
GNUR	GNDS 注销：服务已从 StorageGRID 系统中注销自身。	GN-R ： GNDS 注销
GTED	网格任务已结束： CMN 服务已完成网格任务的处理。	GTed ： 网格任务已结束
GTSt	网格任务已启动： CMN 服务已开始处理网格任务。	GTST ： 已启动网格任务
GTSU	已提交网格任务：已将网格任务提交到 CMN 服务。	GTSU ： 已提交网格任务
标识	ILM Initiated Delete ： 当 ILM 开始删除对象的过程时，会生成此审核消息。	idel ： ILM 已启动删除
LKCU	已覆盖对象清理。自动删除已覆盖的对象以释放存储空间时会生成此审核消息。	LKCU ： 覆盖对象清理

代码	消息标题和问题描述	请参见
LLST	Location Lost ： 当某个位置丢失时，会生成此审核消息。	LLST ： 位置丢失
OLST	对象丢失：无法在 StorageGRID 系统中找到请求的对象。	OLST ： 系统检测到丢失对象
ORLM	满足对象规则：对象数据按照 ILM 规则的指定进行存储。	ORLM ： 符合对象规则
Sadd	禁用安全审核：已关闭审核消息日志记录。	Sadd ： 禁用安全审核
Sade	启用安全审核：审核消息日志记录已还原。	Sade ： 启用安全审核
SVRF	对象存储验证失败：内容块验证检查失败。	SVRF ： 对象存储验证失败
SVRU	对象存储验证未知：在对象存储中检测到意外的对象数据。	SVRU ： 对象存储验证未知
系统	节点停止：已请求关闭。	SYSD ： 节点停止
系统	节点停止：服务已正常停止。	Syst ： 节点正在停止
系统	节点启动：服务已启动；消息中显示了上次关闭的性质。	SYSU ： 节点启动
VLST	User Initiated Volume Lost ： 已运行 ` /proc/CMSI/Volume_Lost` 命令。	VLST ： 用户启动的卷丢失

相关信息

LKCU ： 覆盖对象清理

对象存储审核消息

您应熟悉属于对象存储审核类别的审核消息。这些事件与 StorageGRID 系统中对象的存储和管理相关。其中包括对象存储和检索，网格节点到网格节点的传输以及验证。

代码	Description	请参见
APCT	从云层清除归档：已归档的对象数据将从外部归档存储系统中删除，该系统通过 S3 API 连接到 StorageGRID 。	APCT ： 从云层清除归档
ARCB	归档对象检索开始： ARC-Service 开始从外部归档存储系统检索对象数据。	ARCB ： 开始归档对象检索
Arce	归档对象检索结束：对象数据已从外部归档存储系统中检索，并且 ARC-Service 会报告检索操作的状态。	Arce ： 归档对象检索结束
ARCT	从云层检索归档：归档对象数据从外部归档存储系统中检索，该系统通过 S3 API 连接到 StorageGRID 。	ARCT ： 从云层检索归档
AREM	归档对象删除：已从外部归档存储系统成功或未成功删除内容块。	AREM ： 归档对象删除
ASCE	归档对象存储结束：已将内容块写入外部归档存储系统，并且 ARC-Service 会报告写入操作的状态。	ASCE ： 归档对象存储结束
上一个月	归档存储云层：对象数据存储到外部归档存储系统，该系统通过 S3 API 连接到 StorageGRID 。	SCT ： 归档存储云层
ATCE	归档对象存储开始：已开始向外部归档存储写入内容块。	ATCE ： 开始归档对象存储
AVCC	归档验证云层配置：提供的帐户和存储分段设置已成功验证或未成功验证。	AVCC ： 归档验证云层配置
CBSE	对象发送结束：源实体完成了网格节点到网格节点的数据传输操作。	CBSE ： 对象发送结束
CBRE	对象接收结束：目标实体完成了网格节点到网格节点的数据传输操作。	CBRE ： 对象接收结束
SCMT	对象存储提交：内容块已完全存储和验证，现在可以请求。	SCMT ： 对象存储提交

代码	Description	请参见
Srem	对象存储删除：已从网格节点中删除内容块，无法再直接请求。	Srem ： 对象存储删除

客户端读取审核消息

当 S3 或 Swift 客户端应用程序请求检索对象时，系统会记录客户端读取审核消息。

代码	Description	使用人	请参见
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	SGET ： S3 GET
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	S3 客户端	Shea ： S3 机头
wget	Swift get ： 记录成功的事务以检索对象或列出容器中的对象。	Swift 客户端	WGET ： Swift GET
WHEA	Swift head ： 记录成功的事务以检查是否存在对象或容器。	Swift 客户端	WHEA ： Swift head

客户端写入审核消息

当 S3 或 Swift 客户端应用程序请求创建或修改对象时，系统会记录客户端写入审核消息。

代码	Description	使用人	请参见
OVWR	对象覆盖：记录一个事务，以便使用另一个对象覆盖一个对象。	S3 客户端 Swift 客户端	OVWR ： 对象覆盖

代码	Description	使用人	请参见
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	SDEL ： S3 delete
SPOS	S3 POST ： 记录将对象从 AWS Glacier 存储还原到云存储池的成功事务。	S3 客户端	SPOS ： S3 POST
SPUT	S3 PUT ： 记录成功的事务以创建新对象或存储分段。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	SPUT ： S3 PUT
SUPD	S3 元数据已更新：记录成功的事务以更新现有对象或存储分段的元数据。	S3 客户端	SUPD ： 已更新 S3 元数据
WDEL	Swift delete ： 记录成功的事务以删除对象或容器。	Swift 客户端	WDEL ： Swift delete
WWPUT	Swift PUT ： 记录成功的事务以创建新对象或容器。	Swift 客户端	WWPUT ： Swift PUT

管理审核消息

" 管理 " 类别可将用户请求记录到管理 API 。

代码	消息标题和问题描述	请参见
MGAU	Management API 审核消息：用户请求日志。	MGAU ： 管理审核消息

审核消息参考

APCT ： 从云层清除归档

从通过 S3 API 连接到 StorageGRID 的外部归档存储系统中删除归档对象数据时会生成此

消息。

代码	字段	Description
CBID	内容块 ID	已删除的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。始终返回 0 。
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	从中删除对象的云层的唯一标识符（ UUID ）。

ARCB ： 开始归档对象检索

在请求检索归档的对象数据且检索过程开始时会生成此消息。检索请求会立即处理，但可以重新排序，以提高从磁带等线性介质检索的效率。

代码	字段	Description
CBID	内容块 ID	要从外部归档存储系统检索的内容块的唯一标识符。
RSLT	结果	指示启动归档检索过程的结果。当前定义的值为： suC ： 已收到内容请求并排队等待检索。

此审核消息用于标记归档检索的时间。通过该选项，您可以将该消息与相应的 Arce End 消息进行匹配，以确定归档检索的持续时间以及操作是否成功。

Arce ： 归档对象检索结束

当归档节点尝试从外部归档存储系统检索对象数据时，将生成此消息。如果成功，则此消息指示已从归档位置完全读取请求的对象数据，并已成功验证。检索并验证对象数据后，这些数据将传送到请求服务。

代码	字段	Description
CBID	内容块 ID	要从外部归档存储系统检索的内容块的唯一标识符。
VLID	卷标识符	归档数据的卷的标识符。如果未找到内容的归档位置，则返回卷 ID 0 。

代码	字段	Description
RSLT	检索结果	归档检索过程的完成状态： • SUC ： 成功 • VRFL ： 失败（对象验证失败） • Arun ： 失败（外部归档存储系统不可用） • 取消：失败（已取消检索操作） • GERR ： 失败（一般错误）

将此消息与相应的 ARCB 消息进行匹配可以指示执行归档检索所需的时间。此消息指示检索是否成功，如果失败，则指示检索内容块失败的发生原因 。

ARCT ： 从云层检索归档

从通过 S3 API 连接到 StorageGRID 的外部归档存储系统检索归档对象数据时会生成此消息。

代码	字段	Description
CBID	内容块 ID	已检索到的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。此值仅适用于成功检索。
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	外部归档存储系统的唯一标识符（ UUID ）。
时间	时间	请求的总处理时间，以微秒为单位。

AREM ： 归档对象删除

" 归档对象删除 " 审核消息指示已从归档节点成功删除内容块或未成功删除内容块。如果结果成功，则归档节点已成功通知外部归档存储系统 StorageGRID 已释放对象位置。对象是否从外部归档存储系统中删除取决于系统类型及其配置。

代码	字段	Description
CBID	内容块 ID	要从外部归档介质系统检索的内容块的唯一标识符。

代码	字段	Description
VLID	卷标识符	用于归档对象数据的卷的标识符。
RSLT	结果	归档删除过程的完成状态： • SUC ： 成功 • Arun ： 失败（外部归档存储系统不可用） • GERR ： 失败（一般错误）

ASCE ： 归档对象存储结束

此消息表示向外部归档存储系统写入内容块的操作已结束。

代码	字段	Description
CBID	内容块标识符	存储在外部归档存储系统上的内容块的标识符。
VLID	卷标识符	将对象数据写入到的归档卷的唯一标识符。
VRN	已启用验证	指示是否对内容块执行验证。当前定义的值为： • vena ： 已启用验证 • VDSA ： 已禁用验证
MCLS	管理类	一个字符串，用于标识内容块分配到的 TSM 管理类（如果适用）。
RSLT	结果	指示归档过程的结果。当前定义的值为： • SUC ： 成功（归档过程成功） • OFFL ： 失败（归档已脱机） • VRFL ： 失败（对象验证失败） • Arun ： 失败（外部归档存储系统不可用） • GERR ： 失败（一般错误）

此审核消息表示指定的内容块已写入外部归档存储系统。如果写入失败，则结果将提供有关故障发生位置的基本故障排除信息。有关归档故障的更多详细信息，请参见 StorageGRID 系统中的归档节点属性。

SCT： 归档存储云层

将归档对象数据存储到外部归档存储系统时会生成此消息，该系统通过 S3 API 连接到 StorageGRID 。

代码	字段	Description
CBID	内容块 ID	已检索到的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	存储内容的云层的唯一标识符（ UUID ）。
时间	时间	请求的总处理时间，以微秒为单位。

ATCE： 开始归档对象存储

此消息表示已开始向外部归档存储写入内容块。

代码	字段	Description
CBID	内容块 ID	要归档的内容块的唯一标识符。
VLID	卷标识符	将内容块写入到的卷的唯一标识符。如果操作失败，则返回卷 ID 0 。
RSLT	结果	指示内容块传输的结果。当前定义的值为： • SUC ： 成功（已成功存储内容块） • exis ： 忽略（内容块已存储） • ISFD ： 发生故障（磁盘空间不足） • ster ： 失败（存储 CBID 时出错） • OFFL ： 失败（归档已脱机） • GERR ： 失败（一般错误）

AVCC： 归档验证云层配置

验证 Cloud Tiering - Simple Storage Service （ S3 ）目标类型的配置设置时，会生成此消息。

代码	字段	Description
RSLT	结果代码	返回成功（ SUC ）或后端报告的错误。
SUID	存储唯一标识符	与要验证的外部归档存储系统关联的 UUID 。

CBRB： 对象接收开始

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，目标实体会发出此消息。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push： 发送实体请求传输操作。 Pull： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。
CTES	预期结束序列计数	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。

代码	字段	Description
RSLT	传输开始状态	传输开始时的状态： SUCS ： 已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从 " 开始序列计数 " 到 " 预期结束序列计数 " 请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

CBRE ： 对象接收结束

内容块从一个节点传输到另一个节点完成后，此消息将由目标实体发出。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。

代码	字段	Description
RSLT	传输结果	传输操作的结果（从发送实体的角度来看）： SUC ： 传输成功完成；已发送请求的所有序列计数。 CONL ： 传输期间连接丢失 CTMO： 建立或传输期间连接超时 UNDE ： 无法访问目标节点 ID CRPT ： 由于接收到损坏或无效的数据（可能表示发生篡改），传输已结束

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 " 。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

CBSB ： 对象发送开始

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，源实体会发出此消息。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。

代码	字段	Description
CTES	预期结束序列计数	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS ： 已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从 " 开始序列计数 " 到 " 预期结束序列计数 " 请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

CBSE ： 对象发送结束

在将内容块从一个节点传输到另一个节点后，源实体会发出此消息。

代码	字段	Description
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。

代码	字段	Description
RSLT	传输结果	传输操作的结果（从发送实体的角度来看）： SUC ： 传输成功完成；已发送请求的所有序列计数。 CONL ： 传输期间连接丢失 CTMO： 建立或传输期间连接超时 UNDE ： 无法访问目标节点 ID CRPT ： 由于接收到损坏或无效的数据（可能表示发生篡改），传输已结束

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 " 。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

ECMC ： 缺少擦除编码的数据片段

此审核消息指示系统检测到缺少经过纠删编码的数据片段。

代码	字段	Description
VCMC	VCS ID	包含缺少的块的 VCS 的名称。
MCID	区块 ID	缺少纠删编码片段的标识符。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

EcC ： 擦除编码数据片段损坏

此审核消息指示系统检测到经过纠删编码的数据片段已损坏。

代码	字段	Description
VCCO	VCS ID	包含损坏区块的 VCS 的名称。
VLID	卷 ID	包含损坏的纠删编码片段的 RangeDB 卷。

代码	字段	Description
CCID	区块 ID	已损坏的纠删编码片段的标识符。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

ETAF ： 安全身份验证失败

如果尝试使用传输层安全（ Transport Layer Security ， TLS ）进行连接失败，则会生成此消息。

代码	字段	Description
CNID	连接标识符	身份验证失败的 TCP/IP 连接的唯一系统标识符。
RID	用户身份	表示远程用户身份的服务相关标识符。
RSLT	原因代码	失败的原因： SCNI ： 安全连接建立失败。 CERM ： 证书缺失。 证书：证书无效。 cere ： 证书已过期。 CERR ： 证书已撤销。 CSGN ： 证书签名无效。 CSGU ： 证书签名者未知。 UCRM ： 缺少用户凭据。 UCRI ： 用户凭据无效。 UCRU ： 不允许使用用户凭据。 tout ： 身份验证超时。

在与使用 TLS 的安全服务建立连接后，系统会使用 TLS 配置文件和服务中内置的其他逻辑来验证远程实体的凭据。如果此身份验证因证书或凭据无效，意外或不允许而失败，则会记录审核消息。这样可以查询未经授权的访问尝试以及其他与安全相关的连接问题。

此消息可能是由于远程实体的配置不正确或尝试向系统提供无效或不允许的凭据而导致的。应监控此审核消息，以检测未经授权访问系统的尝试。

GNRG： GNDS 注册

如果某个服务在 StorageGRID 系统中更新或注册了有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	**Description**
RSLT	结果	更新请求的结果： • SUC： 成功 • SUNV： 服务不可用 • GERR： 其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID 。
GNTP	设备类型	网格节点的设备类型（例如 LDR 服务的 BLDR ）。
GNDV	设备型号版本	标识 DMDL 捆绑包中网格节点设备型号版本的字符串。
GNGP	组	网格节点所属的组（在链路成本和服务查询排名环境中）。
GNIA	IP 地址	网格节点的 IP 地址。

每当网格节点更新其在网格节点包中的条目时，都会生成此消息。

GN-R： GNDS 注销

如果某个服务已从 StorageGRID 系统中取消注册有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	**Description**
RSLT	结果	更新请求的结果： • SUC： 成功 • SUNV： 服务不可用 • GERR： 其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID 。

GTed： 网格任务已结束

此审核消息表示 CMN 服务已完成指定网格任务的处理，并已将此任务移至历史表。如果结果为 SUC ， ABRT 或 Rolf ，则会显示相应的 Grid Task Started 审核消息。其他结果表明，此网格任务的处理从未开始。

代码	字段	Description
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在整个生命周期内对网格任务进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	网格任务的最终状态结果： • SUC ： 已成功完成网格任务。 • ABRT ： 已中止网格任务，但未出现回滚错误。 • Rolf ： 网格任务已中止，无法完成回滚过程。 • 取消：用户在启动网格任务之前已取消此任务。 • expr ： 网格任务在启动之前已过期。 • IVLD ： 网格任务无效。 • auth ： 未授权网格任务。 • DUPL ： 网格任务被拒绝为重复项。

GTST： 已启动网格任务

此审核消息指示 CMN 服务已开始处理指定的网格任务。对于由内部网格任务提交服务启动并选择自动激活的网格任务，审核消息会紧跟在网格任务提交消息之后。对于提交到 "Pending" 表中的网格任务，用户启动网格任务时会生成此消息。

代码	字段	Description
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在任务的整个生命周期内对其进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	结果。此字段只有一个值： • SUC ： 已成功启动网格任务。

GTSU ： 已提交网格任务

此审核消息表示已将网格任务提交到 CMN 服务。

代码	字段	Description
SID	任务 ID	唯一标识生成的网格任务，并允许在整个生命周期内对该任务进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
TTYP	任务类型	网格任务的类型。
版本	任务版本	指示网格任务版本的数字。
TDSC	任务问题描述	网格任务的用户可读问题描述 。
VAT	在时间戳之后有效	网格任务最早有效的时间（从 1970 年 1 月 1 日开始的 UINT64 微秒 - UNIX 时间）。
Vbts	在时间戳之前有效	网格任务有效的最新时间（从 1970 年 1 月 1 日开始的 UINT64 微秒 - UNIX 时间）。

代码	字段	Description
TRC	源	任务源： • TXTB ： 网格任务是以签名文本块的形式通过 StorageGRID 系统提交的。 • 网格：网格任务是通过内部网格任务提交服务提交的。
ACTV	激活类型	激活类型： • Auto ： 已提交网格任务以自动激活。 • PEND ： 网格任务已提交到待定表中。这是 TXTB 源的唯一可能性。
RSLT	结果	提交结果： • SUC ： 已成功提交网格任务。 • fail ： 任务已直接移至历史表。

idel ： ILM 已启动删除

ILM 开始删除对象时会生成此消息。

在以下任一情况下都会生成 idel 消息：

- * 对于合规 S3 存储分段中的对象 * ： 当 ILM 开始自动删除对象的过程时，系统会生成此消息，因为该对象的保留期限已过期（假设已启用自动删除设置且已关闭合法保留）。
- * 用于不合规 S3 存储分段或 Swift 容器中的对象 * 。ILM 开始删除对象的过程时会生成此消息，因为活动 ILM 策略中的放置说明当前不适用于此对象。

代码	字段	Description
CBID	内容块标识符	对象的 CBID 。
CMPA	合规性：自动删除	仅适用于合规 S3 存储分段中的对象。0 （ false ）或 1 （ true ），指示合规对象在保留期限结束时是否应自动删除，除非分段处于合法保留状态。
Cmpl	合规性：法律保留	仅适用于合规 S3 存储分段中的对象。0 （ false ）或 1 （ true ），指示存储分段当前是否处于合法保留状态。
CMPR	合规性：保留期限	仅适用于合规 S3 存储分段中的对象。对象保留期限的长度，以分钟为单位。

代码	字段	Description
CTME	合规性：载入时间	仅适用于合规 S3 存储分段中的对象。对象的载入时间。您可以将保留期限（以分钟为单位）添加到此值，以确定何时可以从存储分段中删除对象。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID 。存储分段上的操作不包括此字段。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOC	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 "" 。 CLEC ： 对于经过纠删编码的对象，应用于对象数据的纠删编码配置文件 ID 和纠删编码组 ID 。 CLDI ： 对于复制的对象， LDR 节点 ID 和对象位置的卷 ID 。 CLNL ： 归档对象数据时对象位置的弧节点 ID 。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	ILM 操作的结果。 SUC ： ILM 操作成功。
规则	规则标签	• 如果合规 S3 存储分段中的某个对象因其保留期限已过期而被自动删除，则此字段为空。 • 如果由于当前没有其他应用于对象的放置指令而删除对象，则此字段将显示应用于对象的最后一个 ILM 规则的可读标签。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

LKCU ： 覆盖对象清理

如果 StorageGRID 删除了先前需要清理以释放存储空间的已覆盖对象，则会生成此消息。当 S3 或 Swift 客户端将对象写入已包含对象的路径时，对象将被覆盖。删除过程会自动在后台进行。

代码	字段	Description
CSIZ	内容大小	对象的大小（以字节为单位）。
LTYP	清理类型	_ 仅供内部使用。 _
LUID	已删除对象 UUID	已删除的对象的标识符。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
SEGC	容器 UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
UUID	通用唯一标识符	仍存在的对象的标识符。只有在尚未删除对象时，此值才可用。

LLST： 位置丢失

如果找不到对象副本的位置（复制或擦除编码），则会生成此消息。

代码	字段	Description
CBIL	CBID	受影响的 CBID 。
NOID	源节点 ID	丢失位置的节点 ID 。
UUID	通用唯一 ID	StorageGRID 系统中受影响对象的标识符。
ECPR	纠删编码配置文件	用于经过擦除编码的对象数据。使用的擦除编码配置文件的 ID 。
LTYP	位置类型	CLDI （联机）：用于复制的对象数据 CLEC （联机）：用于经过纠删编码的对象数据 CLNL （近线）：用于归档复制的对象数据

代码	字段	Description
PCLD	复制对象的路径	丢失对象数据的磁盘位置的完整路径。仅当 LTYP 的值为 CLDI （即，对于复制的对象）时才返回。 采用 ` /var/local/rangedb/2/p/13/13/00oJs6X% ｛h ｛U） SeUFxE@` 的形式
RSLT	结果	始终为无。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。
TRC	触发源	User： 用户触发 Syst： 系统已触发

MGAU： 管理审核消息

" 管理 " 类别可将用户请求记录到管理 API 。对于 API ，并非 GET 或 HEAD 请求的每个请求都会记录一个响应，其中包含 API 的用户名， IP 和请求类型。

代码	字段	Description
MDIP	目标 IP 地址	服务器（目标） IP 地址。
MDNA	域名	主机域名。
MPAT	请求路径	请求路径。
MPQP	请求查询参数	请求的查询参数。

代码	字段	Description
MRBD	请求正文	请求正文的内容。虽然默认情况下会记录响应正文，但在某些情况下，如果响应正文为空，则会记录请求正文。由于响应正文中不提供以下信息，因此会从以下 POST 方法的请求正文中获取这些信息： • * POST Authorize * 中的用户名和帐户 ID • * POST /grid/grid-networks/update* 中的新子网配置 • * POST /grid/ntp-servers/update* 中的新 NTP 服务器 • 已停用的服务器 ID 位于 * POST /grid/servers/decommission* 中 • 注： * 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。
MRmd	请求方法	HTTP 请求方法： • 发布 • PUT • 删除 • patch
MRSC	响应代码	响应代码。
MRSP	响应正文	默认情况下，系统会记录响应的内容（响应正文）。 • 注： * 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。
MSIP	源 IP 地址	客户端（源） IP 地址。
MUN	用户 URN	发送请求的用户的 URN （统一资源名称）。
RSLT	结果	返回成功（ SUC ）或后端报告的错误。

OLST： 系统检测到丢失对象

如果 DDS 服务在 StorageGRID 系统中找不到对象的任何副本，则会生成此消息。

代码	字段	Description
CBID	内容块标识符	丢失对象的 CBID 。
NOID	节点 ID	如果可用，则为丢失对象的最后一个已知直接位置或近线位置。如果卷信息不可用，则只能使用节点 ID 而不使用卷 ID 。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	如果可用，则为 S3 存储分段名称和 S3 密钥名称，或者 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。
UUID	通用唯一 ID	StorageGRID 系统中丢失对象的标识符。
卷	卷 ID	如果可用，则为丢失对象的最后一个已知位置的存储节点或归档节点的卷 ID 。

ORLM： 符合对象规则

如果对象已按照 ILM 规则的指定成功存储和复制，则会生成此消息。

如果策略中的另一条规则使用对象大小高级筛选器，则使用默认的 Make 2 Copies 规则成功存储对象时不会生成 ORLM 消息。

代码	字段	Description
BUID	存储分段标题	存储分段 ID 字段。用于内部操作。仅当统计数据为 PRGD 时才显示。
CBID	内容块标识符	对象的 CBID 。
CSIZ	内容大小	对象的大小（以字节为单位）。

代码	字段	Description
LOC	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 "" 。 CLEC ： 对于经过纠删编码的对象，应用于对象数据的纠删编码配置文件 ID 和纠删编码组 ID 。 CLDI ： 对于复制的对象， LDR 节点 ID 和对象位置的卷 ID 。 CLNL ： 归档对象数据时对象位置的弧节点 ID 。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	ILM 操作的结果。 SUC ： ILM 操作成功。
规则	规则标签	为应用于此对象的 ILM 规则提供的可读标签。
SEGC	容器 UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
SGCB	容器 CBID	已分段对象的容器的 CBID 。此值仅适用于已分段和多部分对象。
统计	Status	ILM 操作的状态。 Done ： 已完成对对象的 ILM 操作。 DDER ： 对象已标记为待未来 ILM 重新评估。 PRGD ： 此对象已从 StorageGRID 系统中删除。 NLOC ： 在 StorageGRID 系统中找不到对象数据。此状态可能表示对象数据的所有副本均缺失或已损坏。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

可以对单个对象多次发出 ORLM 审核消息。例如，每当发生以下事件之一时都会发出此消息：

- 对象的 ILM 规则将永久满足。
- 此 Epoch 已满足对象的 ILM 规则。
- ILM 规则已删除此对象。
- 后台验证过程检测到复制的对象数据的副本已损坏。StorageGRID 系统会执行 ILM 评估以替换损坏的对

象。

相关信息

- 对象载入事务
- 对象删除事务

OVWR：对象覆盖

如果外部（客户端请求的）操作导致一个对象被另一个对象覆盖，则会生成此消息。

代码	字段	Description
CBID	内容块标识符（新增）	新对象的 CBID 。
CSIZ	先前对象大小	要覆盖的对象的大小（以字节为单位）。
OCBD	内容块标识符（上一个）	上一个对象的 CBID 。
UUID	通用唯一 ID （新）	StorageGRID 系统中新对象的标识符。
OUID	通用唯一 ID （以前的）	StorageGRID 系统中上一个对象的标识符。
路径	S3 或 Swift 对象路径	用于上一个对象和新对象的 S3 或 Swift 对象路径
RSLT	结果代码	对象覆盖事务的结果。结果始终为： SUC ：成功
SGRP	站点（组）	如果存在此参数，则会在指定的站点上删除此覆盖对象，而不是在其中载入此覆盖对象的站点。

Sadd：禁用安全审核

此消息指示发起服务（节点 ID ）已关闭审核消息日志记录；不再收集或传送审核消息。

代码	字段	Description
AETM	启用方法	用于禁用审核的方法。
AEUN	用户名	执行命令以禁用审核日志记录的用户名。

代码	字段	Description
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。

此消息表示先前已启用日志记录，但现在已禁用。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，将还原审核（ SAade ），并永久阻止禁用审核的功能。

Sade ： 启用安全审核

此消息表示发起服务（节点 ID ）已还原审核消息日志记录；正在再次收集和传送审核消息。

代码	字段	Description
AETM	启用方法	用于启用审核的方法。
AEUN	用户名	执行命令以启用审核日志记录的用户名。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。

此消息表示先前已禁用日志记录（ Sadd ），但现在已还原。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，审核将恢复，而禁用审核的功能将被永久阻止。

SCMT ： 对象存储提交

网格内容在提交之前不可用或无法识别为已存储（这意味着它已持久存储）。持久存储的内容已完全写入磁盘，并已通过相关的完整性检查。将内容块提交到存储时会发出此消息。

代码	字段	Description
CBID	内容块标识符	提交到永久存储的内容块的唯一标识符。
RSLT	结果代码	将对象存储到磁盘时的状态： SUCS ： 对象已成功存储。

此消息表示给定内容块已完全存储和验证，现在可以请求。它可用于跟踪系统内的数据流。

SDEL： S3 delete

当 S3 客户端发出删除事务时，系统会请求删除指定的对象或存储分段。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID 。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	删除事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。

代码	字段	Description
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： : 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SGET： S3 GET

当 S3 客户端发出 GET 事务时，系统会请求检索对象或列出存储分段中的对象。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。

代码	字段	Description
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
已振铃	范围读取	仅适用于范围读取操作。指示此请求读取的字节数范围。斜杠（ / ）后面的值显示整个对象的大小。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

Shea： S3 机头

当 S3 客户端发出 HEAD 事务时，系统会请求检查是否存在对象或存储分段，并检索有关对象的元数据。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检查对象的大小（以字节为单位）。存储分段上的操作不包括此字段。

代码	字段	Description
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。

代码	字段	Description
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SPOS： S3 POST

当 S3 客户端发出 POST 对象请求时，如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	POST 对象还原请求的结果。结果始终为： SUC ： 成功

代码	字段	Description
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。 对于 S3 Select 操作，设置为 `select` 。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SRCF	子资源配置	还原信息。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。

代码	字段	Description
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SPUT： S3 PUT

当 S3 客户端发出 PUT 事务时，系统会请求创建新对象或存储分段。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CMPS	合规性设置	创建存储分段时使用的合规性设置（如果 PUT 存储分段请求中存在）（截断为前 1024 个字符）
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。

代码	字段	Description
LKEN	对象锁定已启用	请求标题 `x-AMZ-bucket-object-lock-enabled` 的值（如果 PUT Bucket 请求中存在）。
LKLH	对象锁定合法保留	请求标题 `x-AMZ-object-lock-legal-hold` 的值（如果 PUT 对象请求中存在）。
LKMD	对象锁定保留模式	请求标题 `x-AMZ-object-lock-mode` 的值（如果 PUT 对象请求中存在）。
LKRU	对象锁定保留至日期	请求标题 `x-AMZ-object-lock-retain-until date` 的值（如果 PUT 对象请求中存在）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3KY	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SRCF	子资源配置	新的子资源配置（截断为前 1024 个字符）。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
ULID	上传 ID	仅包含在用于完成多部件上传操作的 SPUT 消息中。表示所有部件均已上传和组装。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在受版本控制的存储分段中创建的新对象的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。
VSST	版本控制状态	存储分段的新版本控制状态。使用两种状态： "enabled" 或 "suspended" 。 对对象执行的操作不包括此字段。

Srem ： 对象存储删除

从永久性存储中删除内容后会发出此消息，并且无法再通过常规 API 进行访问。

代码	字段	Description
CBID	内容块标识符	从永久存储中删除的内容块的唯一标识符。
RSLT	结果代码	指示内容删除操作的结果。唯一定义的值为： SUC ： 从永久性存储中删除的内容

此审核消息表示已从节点中删除给定内容块，无法再直接请求。此消息可用于跟踪系统中已删除内容的流。

SUPD ： 已更新 **S3** 元数据

当 S3 客户端更新所载入对象的元数据时， S3 API 会生成此消息。如果元数据更新成功，则服务器会发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	更新存储分段的合规性设置时，如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功

代码	字段	Description
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn ： sgws ： identity ： ： 03393893651506583485 ： root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

代码	字段	Description
VSID	版本 ID	已更新其元数据的对象的特定版本的版本 ID 。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SVRF： 对象存储验证失败

每当内容块验证过程失败时，都会发出此消息。每次从磁盘读取或写入复制的对象数据时，都会执行多项验证和完整性检查，以确保发送给请求用户的数据与最初载入系统的数据完全相同。如果其中任何一项检查失败，系统会自动隔离损坏的复制对象数据，以防止再次检索该数据。

代码	字段	Description
CBID	内容块标识符	验证失败的内容块的唯一标识符。
RSLT	结果代码	验证失败类型： CRCF： 循环冗余检查（ CRC ）失败。 HMAC： 基于哈希的消息身份验证代码（ HMAC ）检查失败。 EHSH： 意外的加密内容哈希。 PHSH： 意外的原始内容哈希。 SEQC： 磁盘上的数据顺序不正确。 PERR： 磁盘文件的结构无效。 DERR： 磁盘错误。 fnam： 文件名错误。

- 注： * 应密切监控此消息。内容验证失败可能表示尝试篡改内容或即将发生的硬件故障。

要确定哪个操作触发了消息，请参见 amid （模块 ID ）字段的值。例如， SV财年 值表示消息是由存储验证程序模块生成的，即后台验证， STor 表示消息是通过内容检索触发的。

SVRU： 对象存储验证未知

LDR 服务的存储组件会持续扫描对象存储中复制的对象数据的所有副本。如果在对象存储中检测到复制的对象数据的未知或意外副本并将其移动到隔离目录，则会发出此消息。

代码	字段	Description
FPTH	文件路径	意外对象副本的文件路径。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

- 注： * 应密切监控 SVRU： Object Store Verify Unknown 审核消息。这意味着在对象存储中检测到意外的对象数据副本。应立即调查这种情况，以确定这些副本是如何创建的，因为这可能表示尝试篡改内容或即将发生硬件故障。

SYSD： 节点停止

如果服务正常停止，则会生成此消息以指示已请求关闭。通常，只有在后续重新启动后才会发送此消息，因为在关闭之前未清除审核消息队列。如果服务未重新启动，请查找在关闭序列开始时发送的 SYST 消息。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC： 系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYSD 的 RSLT 不能指示 " 异常 " 关闭，因为只有 " 清理 " 关闭才会生成此消息。

Syst： 节点正在停止

如果服务正常停止，则会生成此消息，以指示已请求关闭，并且此服务已启动其关闭序列。Syst 可用于确定是否在重新启动服务之前请求关闭（与通常在服务重新启动后发送的 SYSD 不同）。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC： 系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYST 消息的 RSLT 代码不能指示 " 异常 " 关闭，因为只有 " 清理 " 关闭才会生成此消息。

SYSU： 节点启动

重新启动服务时，系统会生成此消息，以指示上次关闭是正常关闭（已发出命令）还是无序关闭（意外关闭）。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC ： 系统已完全关闭。 DSDN ： 系统未完全关闭。 VRGN ： 在安装（或重新安装）服务器后首次启动系统。

此消息不会指示是否已启动主机服务器，仅会指示报告服务。此消息可用于：

- 检测审核跟踪中的不连续性。
- 确定服务在运行期间是否出现故障（因为 StorageGRID 系统的分布式特征可能会掩盖这些故障）。Server Manager 会自动重新启动失败的服务。

VLST ： 用户启动的卷丢失

每当运行 ` /proc/CMSI/Volume_Lost` 命令时，都会发出此消息。

代码	字段	Description
VOLL	卷标识符下限	受影响卷范围的下端或单个卷。
VOLU	卷标识符上限	受影响卷范围的上限。如果只有一个卷，则等于 VOLL 。
NOID	源节点 ID	丢失位置的节点 ID 。
LTYP	位置类型	"CLDI" （联机）或 "CLNL" （近线）。如果未指定，则默认为 "CLDI" 。
RSLT	结果	始终为 " 无 " 。RSLT- 是一个必填消息字段，但与此消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

WDEL ： Swift delete

当 Swift 客户端发出删除事务时，系统会请求删除指定的对象或容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对容器执行的操作不包括此字段。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。对容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	删除事务的结果。结果始终为： SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。
WOBJ	Swift 对象	Swift 对象标识符。对容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WGET： Swift GET

当 Swift 客户端发出 GET 事务时，系统会请求检索对象，列出容器中的对象或列出帐户中的容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对帐户和容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对帐户和容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	GET 事务的结果。结果始终为 SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。对帐户执行的操作不包括此字段。
WOBJ	Swift 对象	Swift 对象标识符。对帐户和容器执行的操作不包括此字段。

代码	字段	Description
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WHEA： Swift head

当 Swift 客户端发出 HEAD 事务时，系统会请求检查是否存在帐户，容器或对象，并检索任何相关元数据。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对帐户和容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对帐户和容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
RSLT	结果代码	HEAD 事务的结果。结果始终为： SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

代码	字段	Description
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。对帐户执行的操作不包括此字段。
WOBJ	Swift 对象	Swift 对象标识符。对帐户和容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WWPUT： Swift PUT

当 Swift 客户端发出 PUT 事务时，系统会请求创建新的对象或容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。对容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * 如果请求中存在 `X-Forwarded-for` ，并且 `X-Forwarded-for` 值与请求发送方 IP 地址不同，则系统会自动将其包括在内（ SAIP 审核字段）。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUC ： 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID 。
WCON	Swift 容器	Swift 容器名称。
WOBJ	Swift 对象	Swift 对象标识符。对容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

如何在您的环境中启用StorageGRID

了解如何在StorageGRID 环境中测试和启用应用程序。

转至 "storagegrid-enable" 文档站点、查找可在此站点的产品文档上扩展的示例和指南。* storagegrid enable*站点还介绍了评估和集成StorageGRID 的一些后续步骤。

其中包括以下信息：

- 列出了过去和当前StorageGRID 版本中经过验证的第三方解决方案。
- 产品功能指南。例如、这些指南提供了有关创建云存储池的详细信息。
- 工具和应用程序指南。
- 使用S3加密和S3对象锁定等StorageGRID 功能的API示例。

其他版本的NetApp StorageGRID 文档

您可以在此处找到其他版本的NetApp StorageGRID 软件的文档：

- "StorageGRID 11.9文档"
- "StorageGRID 1.18文档"
- "StorageGRID 11.7文档"
- "StorageGRID 11.5 文档"
- "StorageGRID 11.4 文档中心"
- "StorageGRID 11.3 文档中心"
- "StorageGRID 11.2 文档中心"

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

"https://www.netapp.com/company/legal/trademarks/"

专利

有关 NetApp 拥有的专利的最新列表，请访问：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

https://library.netapp.com/ecm/ecm_download_file/ECMLP2879263

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。