入门
StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-115/primer/hybrid-clouds-with-storagegrid.html on October 03, 2025. Always check docs.netapp.com for the latest.

目录

入门 1
网格入门 1
关于StorageGRID 1
StorageGRID 架构和网络拓扑 4
StorageGRID 如何管理数据 13
了解网格管理器 24
了解租户管理器 31
使用StorageGRID 33
网络连接准则 64
StorageGRID 网络概述 64
网络要求 73
网络特定要求 75
部署特定的网络注意事项 76
网络安装和配置 79
安装后准则 80
网络端口参考 80

入门

网格入门

了解NetApp StorageGRID 系统的基础知识。

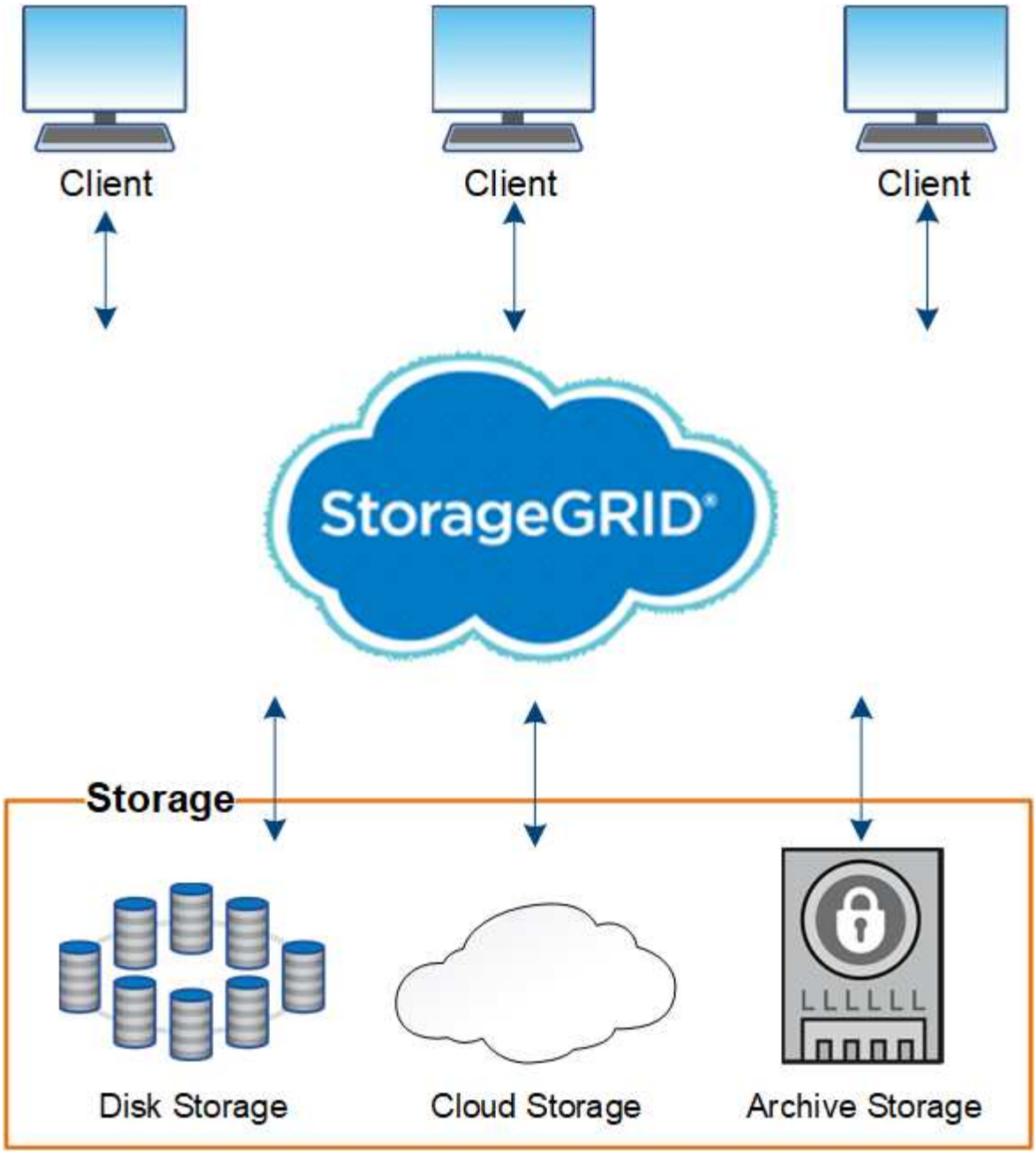
- "关于StorageGRID"
- "StorageGRID 架构和网络拓扑"
- "StorageGRID 如何管理数据"
- "了解网格管理器"
- "了解租户管理器"
- "使用StorageGRID"

关于**StorageGRID**

NetApp StorageGRID 是一款基于对象的软件定义存储解决方案，支持行业标准对象 API，包括 Amazon Simple Storage Service （S3） API 和 OpenStack Swift API 。

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 平台服务支持在公有 云上进行内容复制、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Docker容器。
  - 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。

相关信息

"采用 StorageGRID 的混合云"

"StorageGRID 架构和网络拓扑"

"控制StorageGRID 访问"

"管理租户和客户端连接"

"使用信息生命周期管理"

"监控StorageGRID 操作"

"配置网络设置"

"执行维护过程"

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 的StorageGRID 网络拓扑、要求和网格通信、请参见网络连接准则。

相关信息

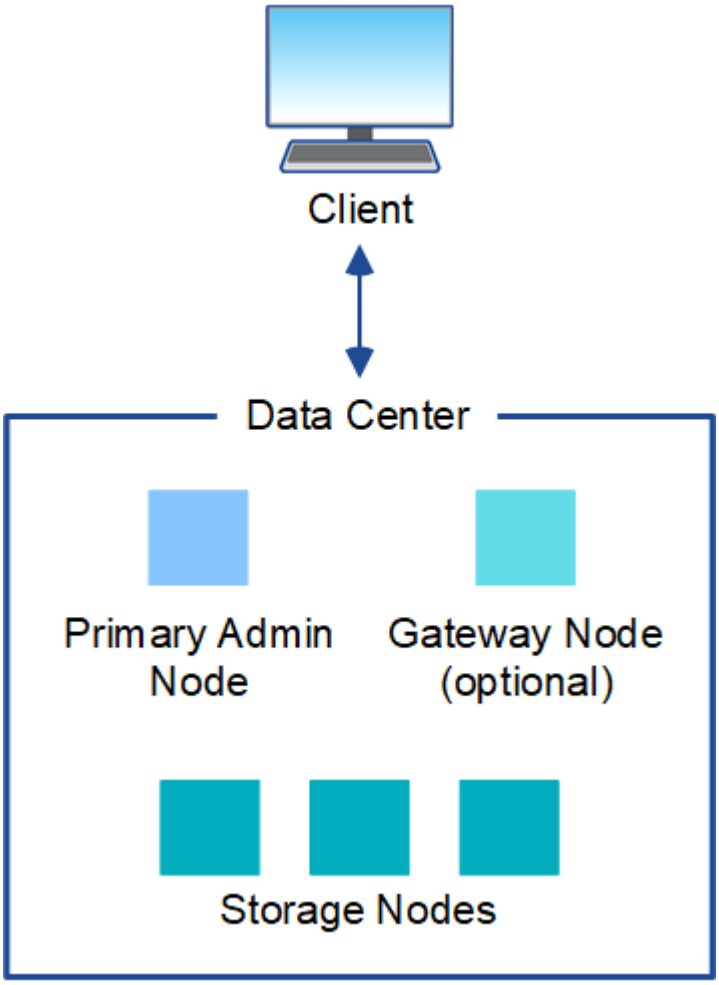
"网络准则"

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

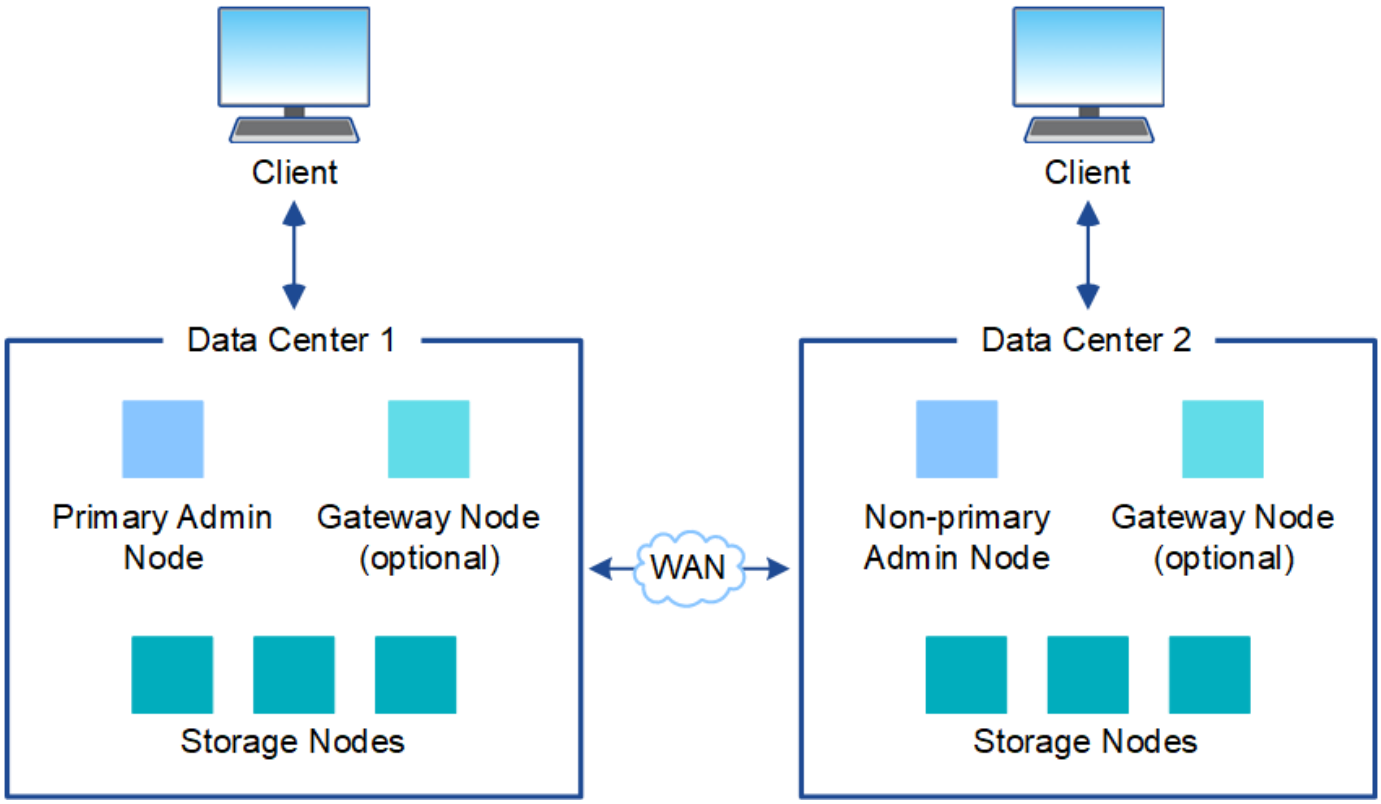
在使用单个站点的部署中， StorageGRID 系统的基础架构和操作会集中进行。



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。



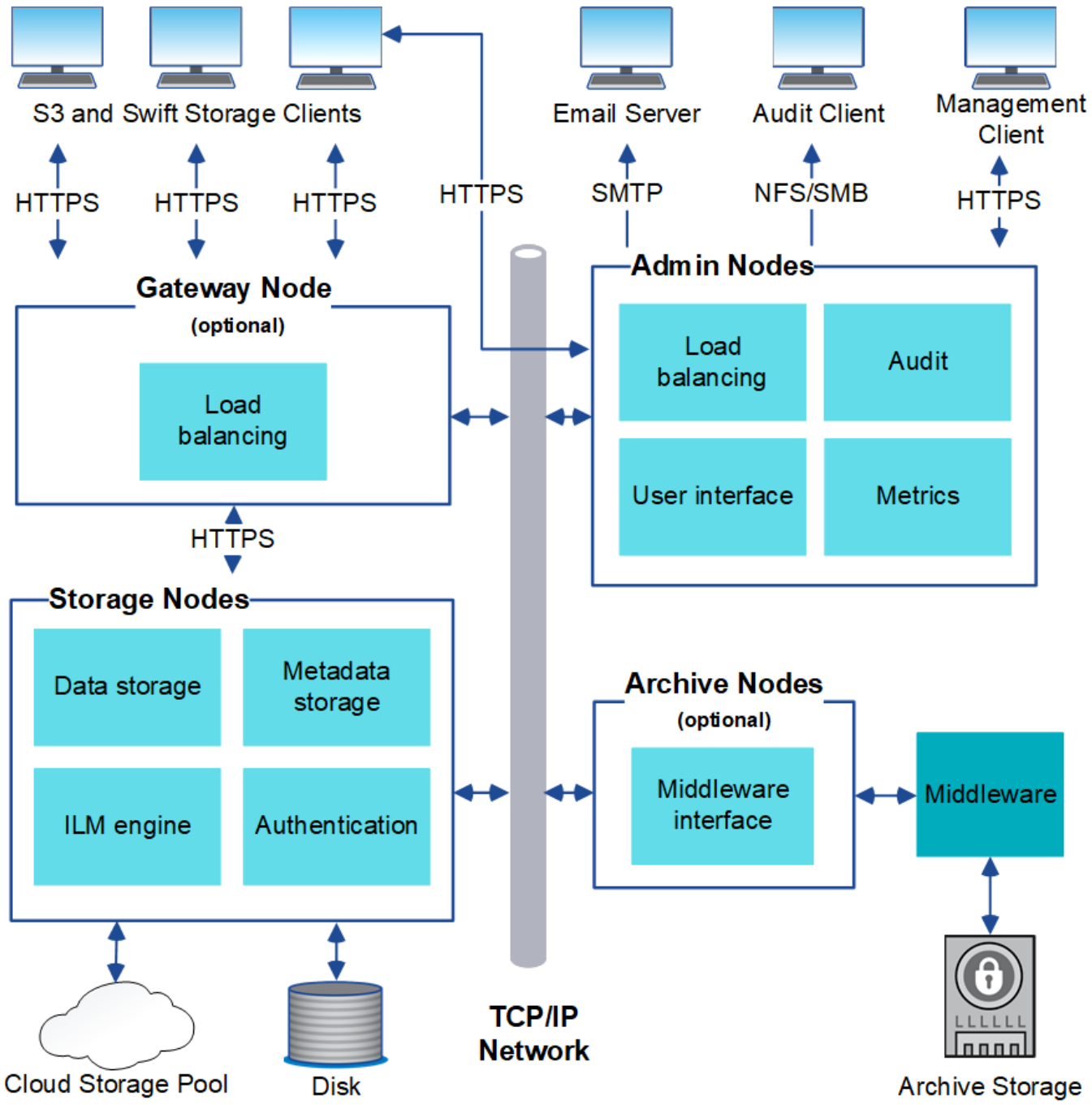
一个数据中心中也可以存在多个逻辑站点，以便使用分布式复制和纠删编码来提高可用性和故障恢复能力。

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）。

相关信息

"管理 StorageGRID"

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。

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 Web Client中的虚拟机(VM)
- 在Linux主机上的Docker容器中。支持以下操作系统：
  - Red Hat Enterprise Linux
  - CentOS
  - Ubuntu
  - Debian

使用 NetApp 互操作性表工具可获取受支持版本的列表。

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 有两种型号：
  - * 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。
  - * SG606060* ： 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。每个 SG6060 设备支持一个或两个 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 有两种型号：
  - * SG5712* ：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。
  - * SG5760* ：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。
- * 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。

有关完整的规格、请参见NetApp Hardware Universe。

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。
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。

- * 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。

相关信息

"NetApp 互操作性表工具"

"NetApp Hardware Universe"

"安装 VMware"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

"管理 StorageGRID"

StorageGRID 如何管理数据

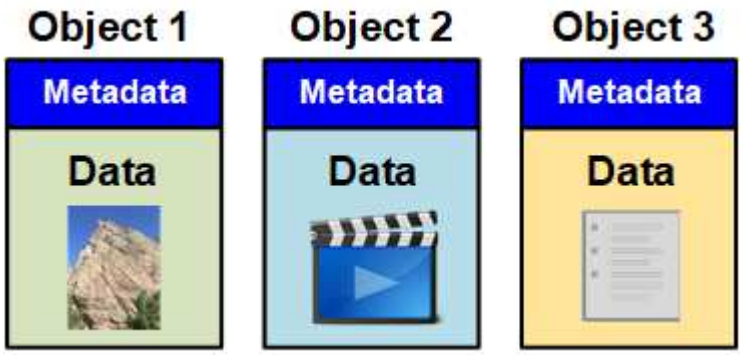
在开始使用 StorageGRID 系统时，了解 StorageGRID 系统如何管理数据非常有用。

- "什么是对象"
- "如何保护对象数据"
- "对象的生命周期"

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"。

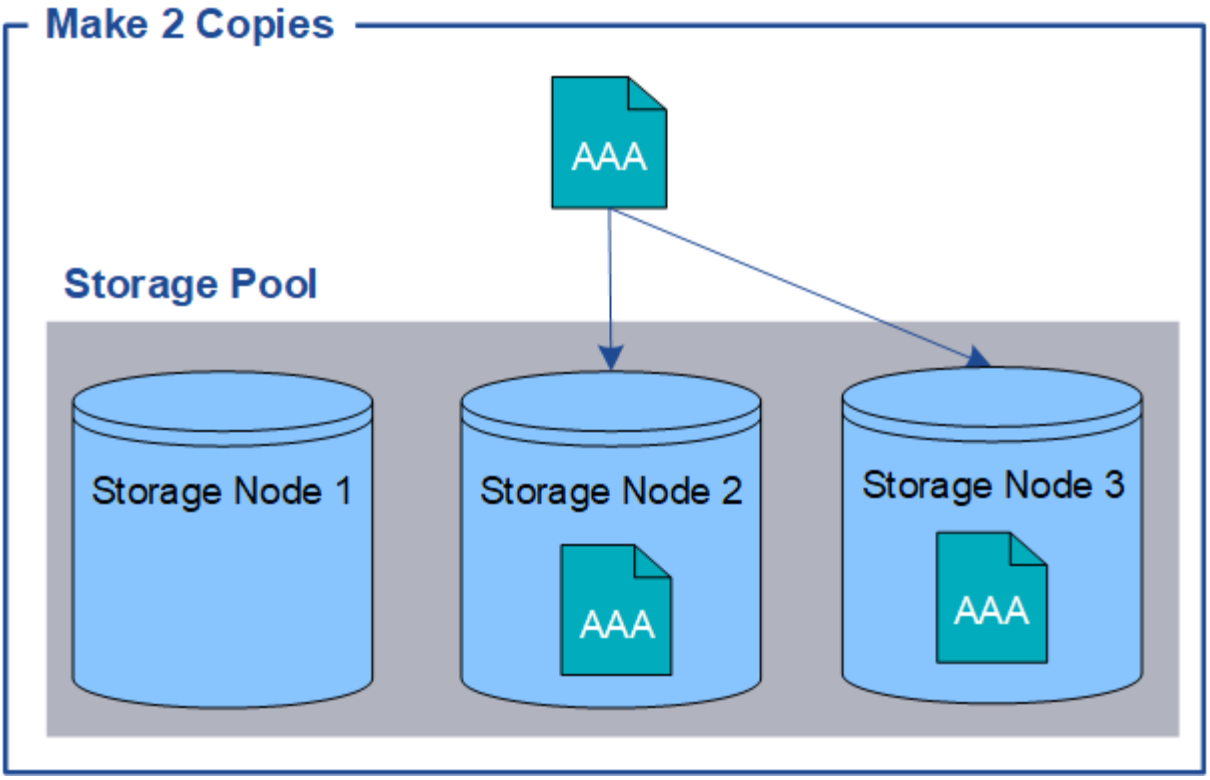
如何保护对象数据

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。

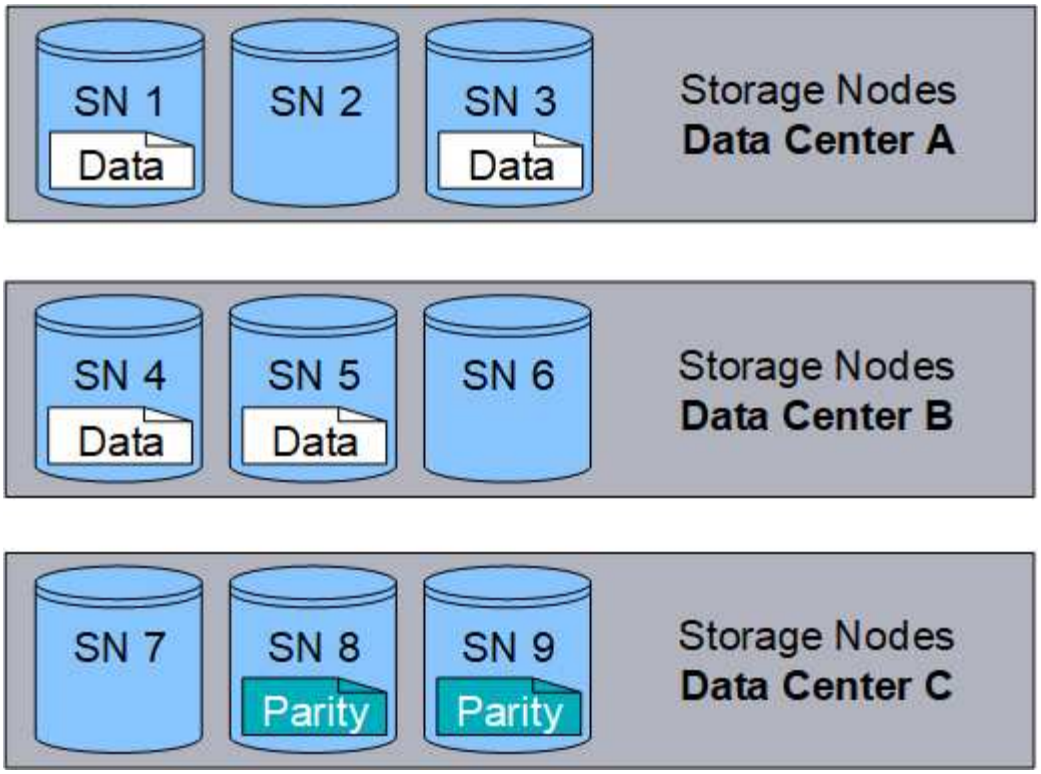
在以下示例中， make 2 copies 规则指定将每个对象的两个复制副本放置在包含三个存储节点的存储池中。



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"

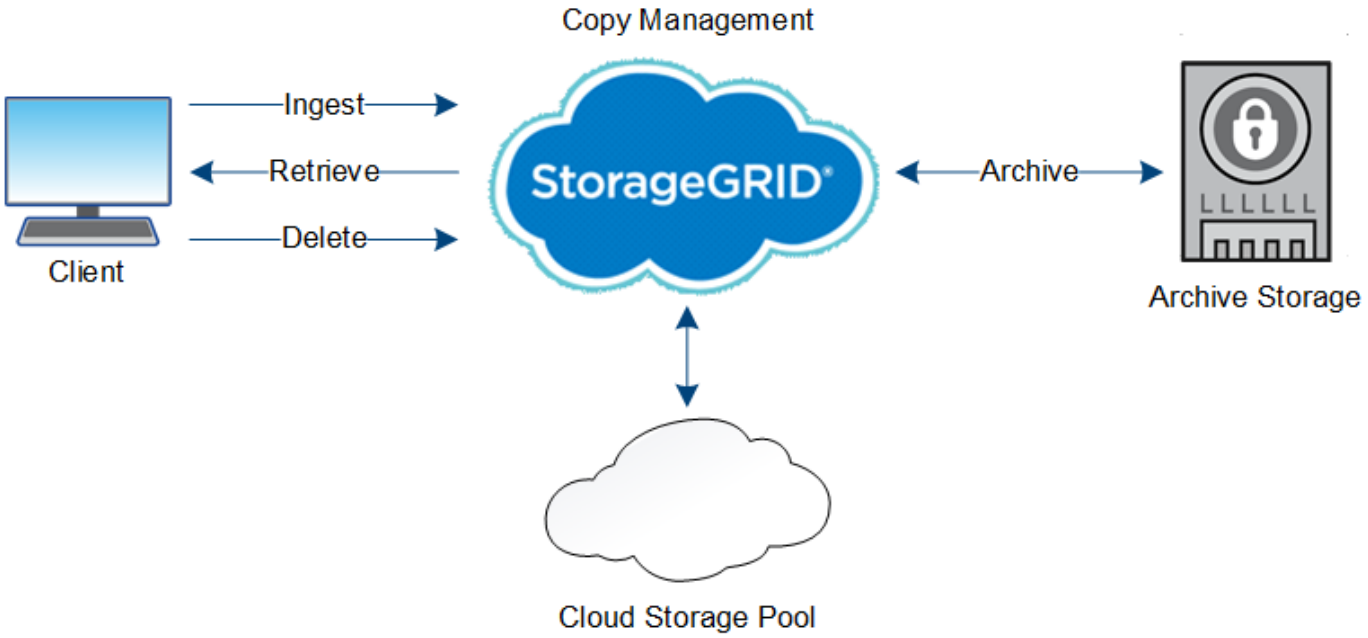
"使用信息生命周期管理"

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"

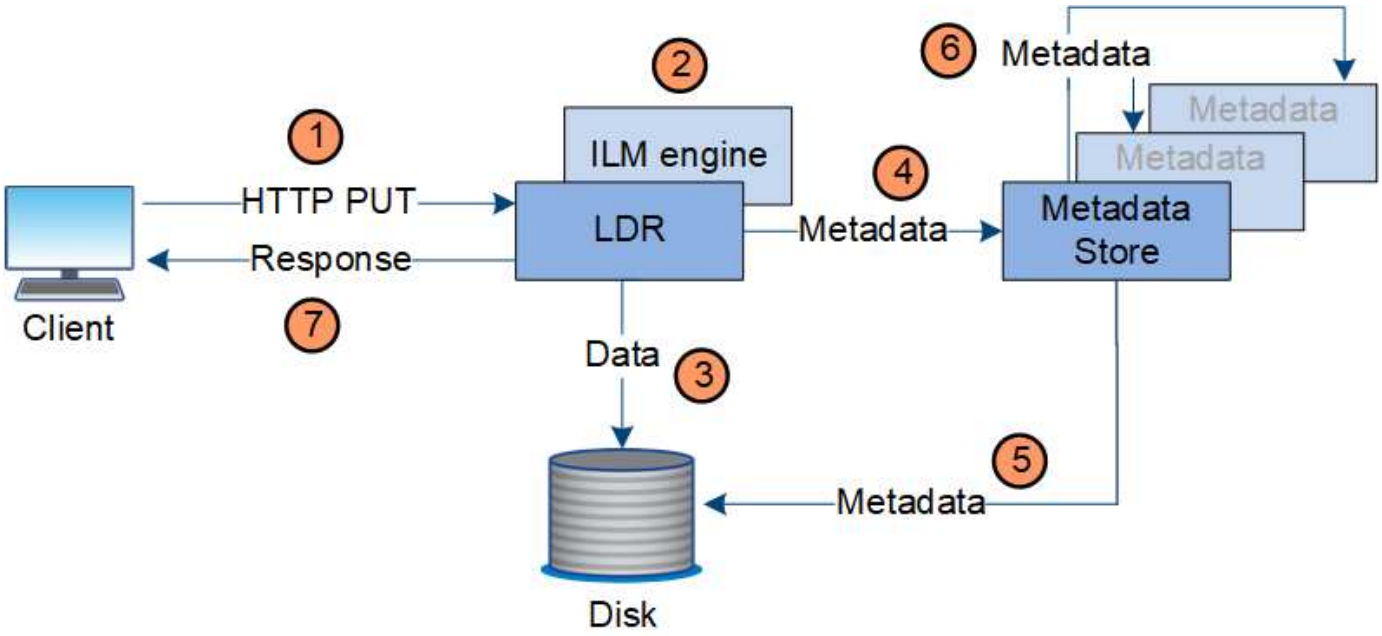
"使用信息生命周期管理"

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

当客户端将对象保存到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。

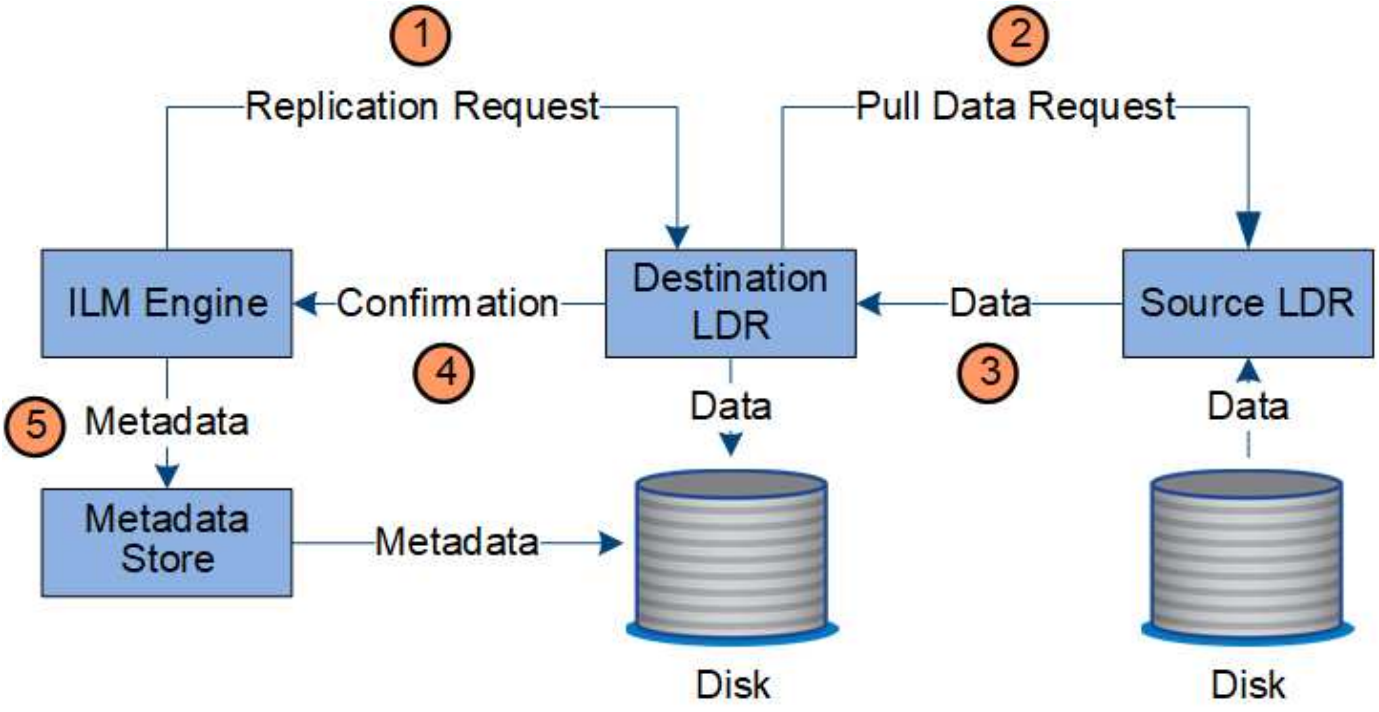
对象数据由 LDR 服务管理。

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。



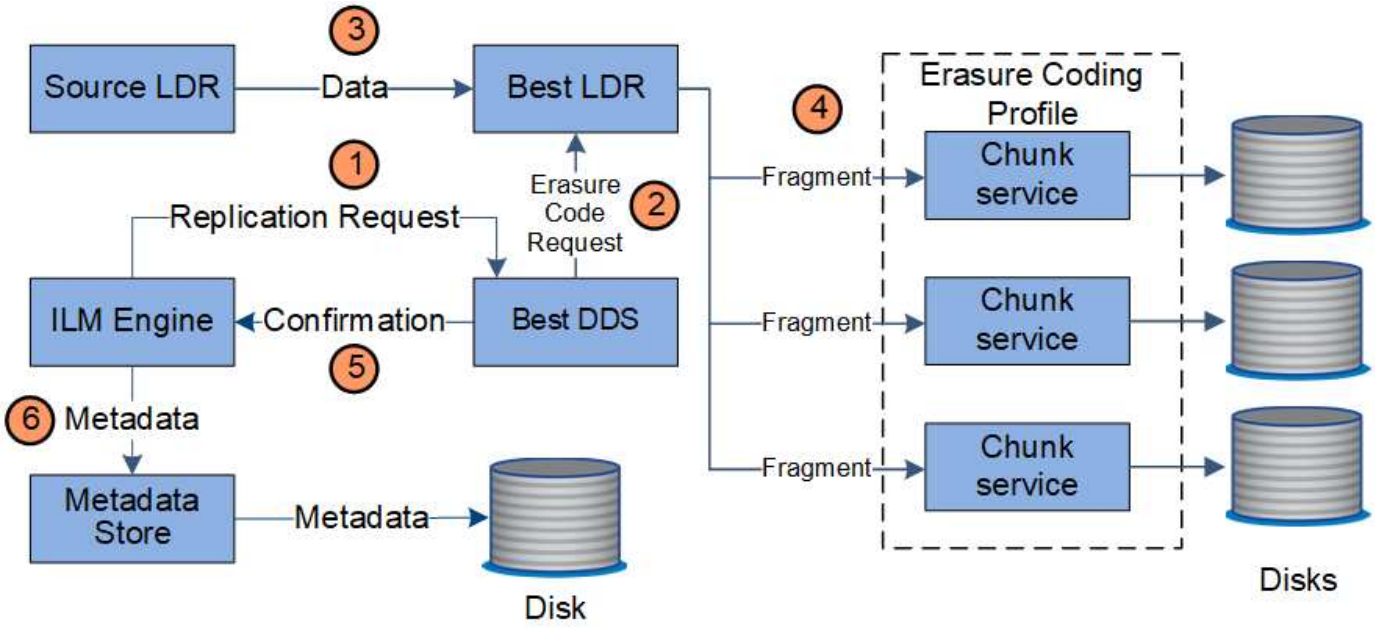
1. ILM 引擎会查询此 ADC-LDR 服务，以确定 ILM 规则指定的存储池中的最佳目标 LDR 服务。然后，它会向该 LDR 服务发送一个命令以启动复制。
2. 目标 LDR 服务会向此 ADC-Service 查询最佳源位置。然后，它会向源 LDR 服务发送复制请求。
3. 源 LDR 服务会向目标 LDR 服务发送一份副本。
4. 目标 LDR 服务通知 ILM 引擎已存储对象数据。
5. ILM 引擎使用对象位置元数据更新元数据存储。

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。



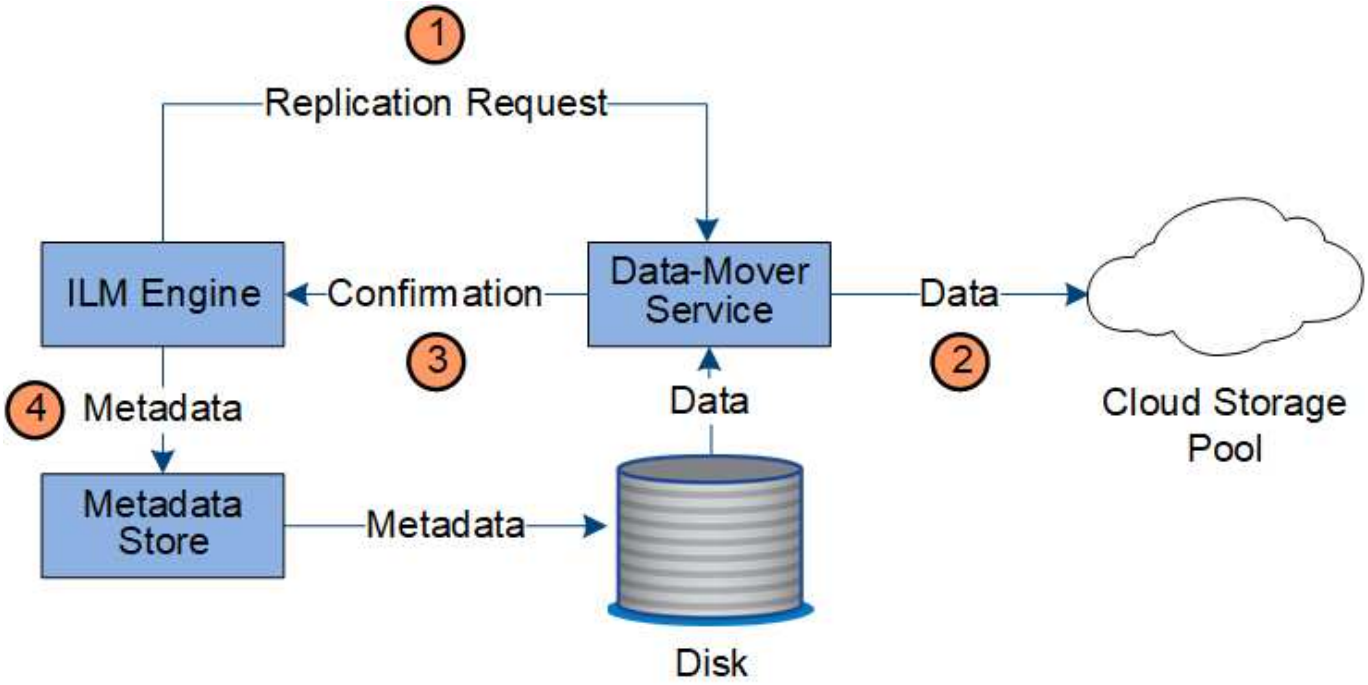
1. ILM 引擎会查询此 ADC-Service ，以确定哪种 DDS 服务能够以最佳方式执行纠删编码操作。一旦确定，ILM 引擎就会向该服务发送 " 启动 " 请求。
2. DDS 服务指示 LDR 对对象数据进行纠删编码。
3. 源 LDR 服务会向选定用于纠删编码的 LDR 服务发送一份副本。
4. 一旦细分为适当数量的奇偶校验和数据片段， LDR 服务会将这些片段分布在构成 Erasure 编码配置文件存储池的存储节点（区块服务）中。
5. LDR 服务通知 ILM 引擎，确认对象数据已成功分发。
6. ILM 引擎使用对象位置元数据更新元数据存储。

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、则对象数据将移动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。

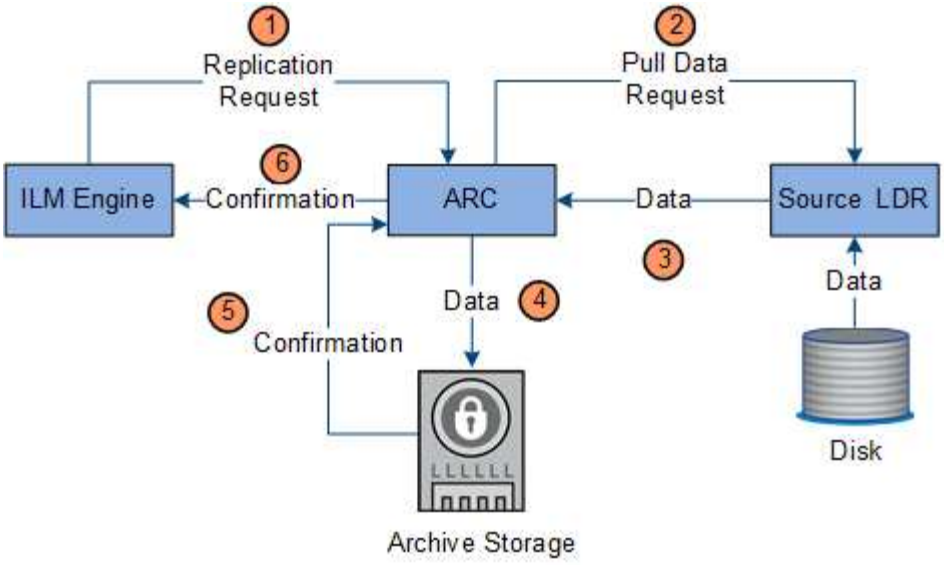


1. ILM 引擎选择要复制到云存储池的数据转换服务。
2. Data Mover 服务会将对象数据发送到云存储池。
3. Data Mover 服务会通知 ILM 引擎已存储对象数据。
4. ILM 引擎使用对象位置元数据更新元数据存储。

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。



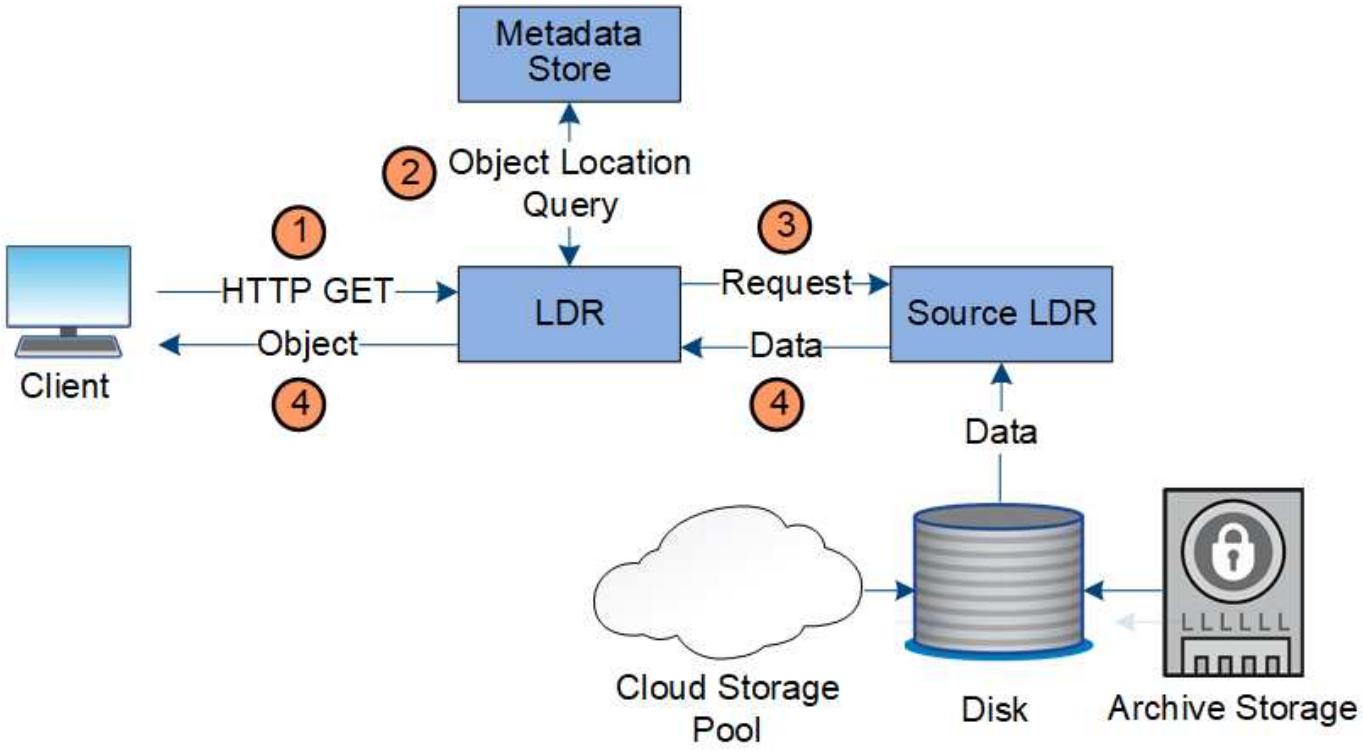
1. ILM 引擎会向 ARC-Service 发送一个请求，要求将副本存储在归档介质上。
2. 此 ARR 服务会向此 ADC/ 服务查询最佳源位置，并向源 LDR 服务发送请求。
3. ARR 服务从 LDR 服务检索对象数据。
4. 此应用程序服务会将对象数据发送到归档介质目标。
5. 归档介质会通知 ARC-Service 对象数据已存储。
6. ARC-Service 会通知 ILM 引擎已存储对象数据。

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

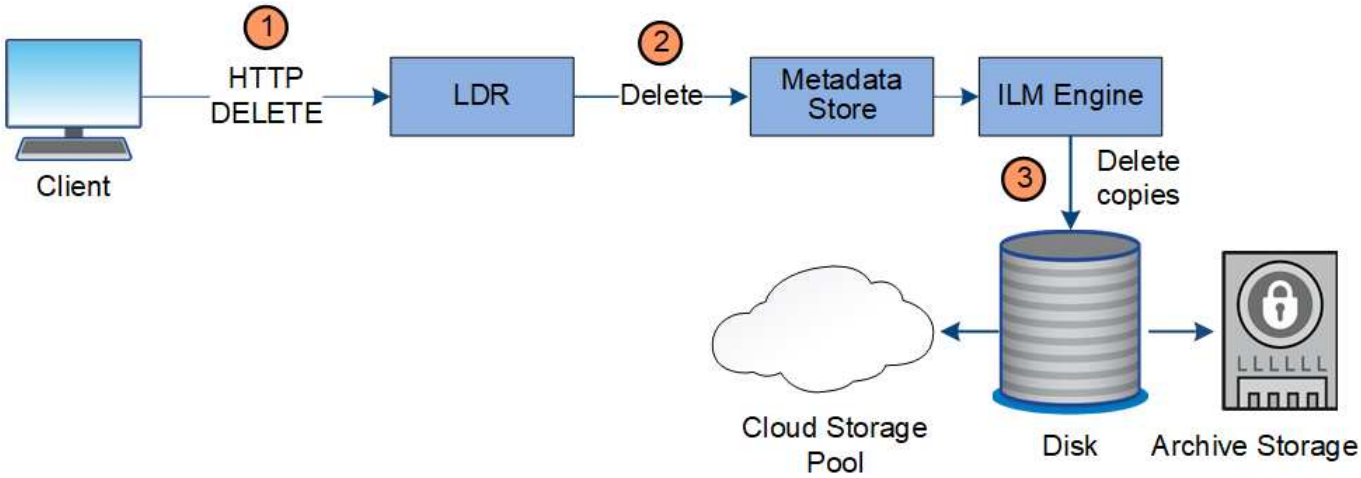
StorageGRID 提供了多种方法来控制何时保留或删除对象。可以根据客户端请求删除对象、也可以自动删除对象。StorageGRID 始终将任何 S3 对象锁定设置优先于客户端删除请求，而客户端删除请求优先于 S3 存储分段生命周期和 ILM 放置说明。

- * 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。
- * 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。

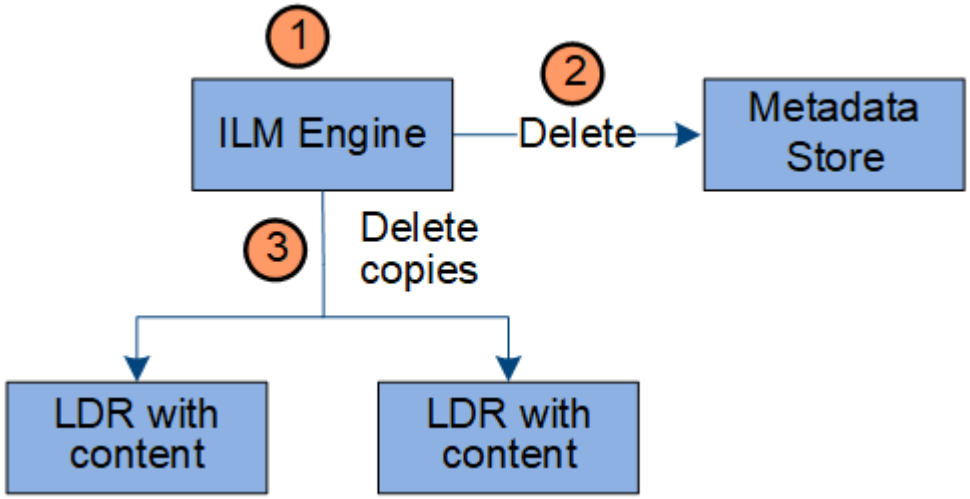
> S3 存储分段生命周期中的到期操作始终会覆盖 ILM 设置。因此，即使有关放置对象的任何 ILM 指令已失效，该对象也可能会保留在网格中。

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。

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。

您可以使用支持的Web浏览器访问网格管理器。

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	87
Microsoft Edge	87
Mozilla Firefox	84.

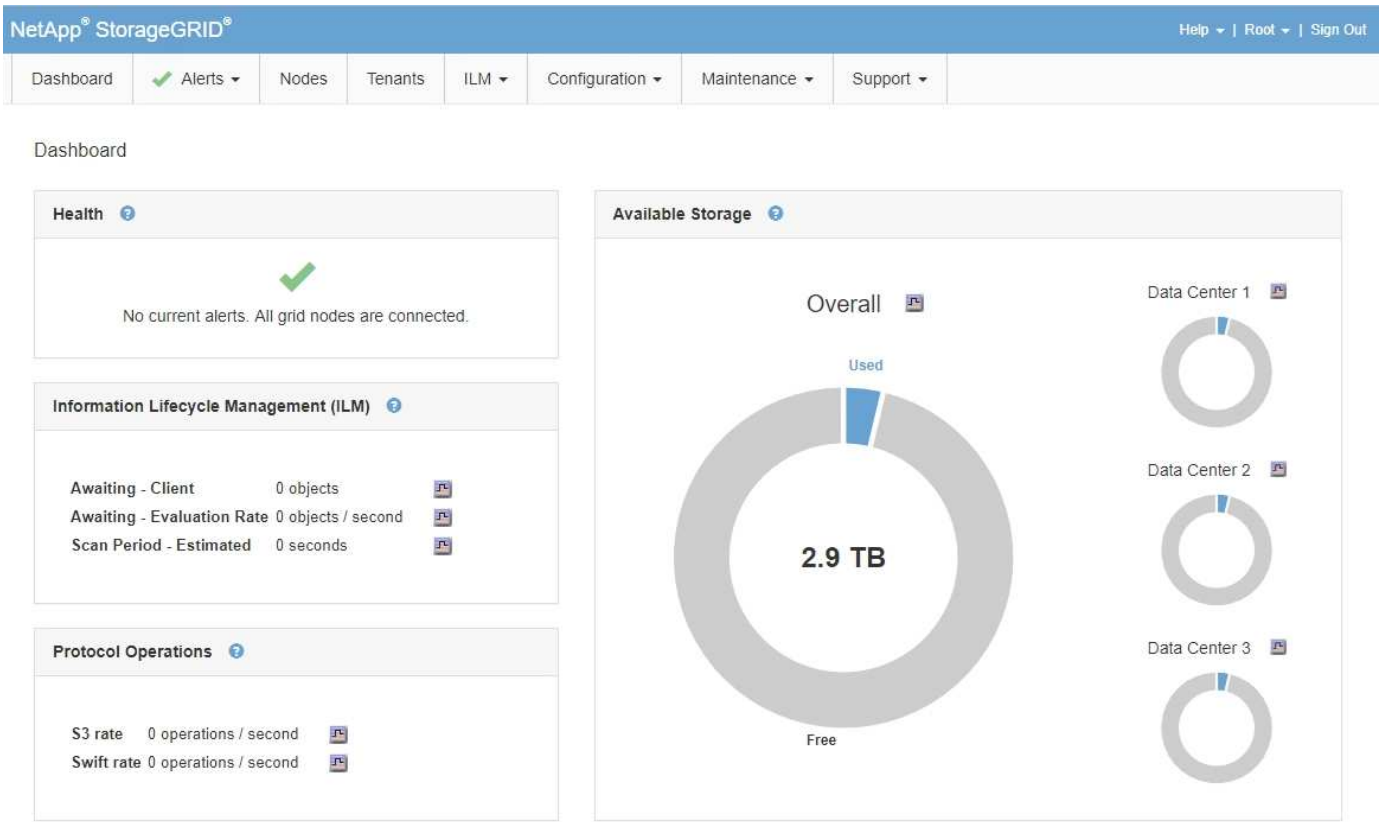
您应将浏览器窗口设置为建议的宽度。

浏览器宽度	像素
最小值	1024
最佳	1280

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。



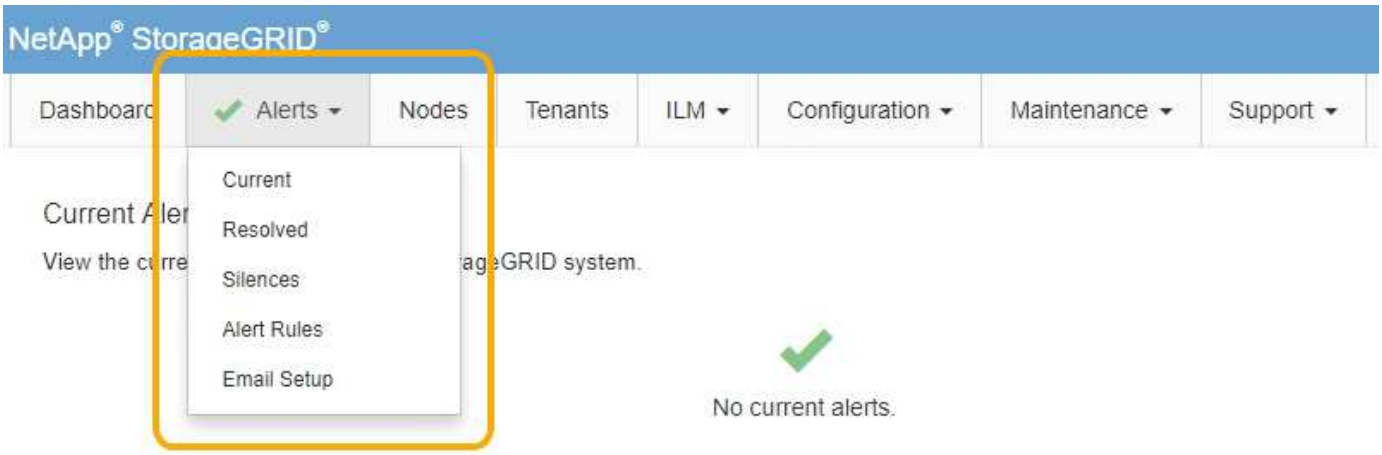
有关每个面板上信息的说明，请单击帮助图标 ? 。

相关信息

"监控和放大；故障排除"

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
- 为警报通知配置电子邮件服务器
- 为触发警报的条件定义警报规则

相关信息

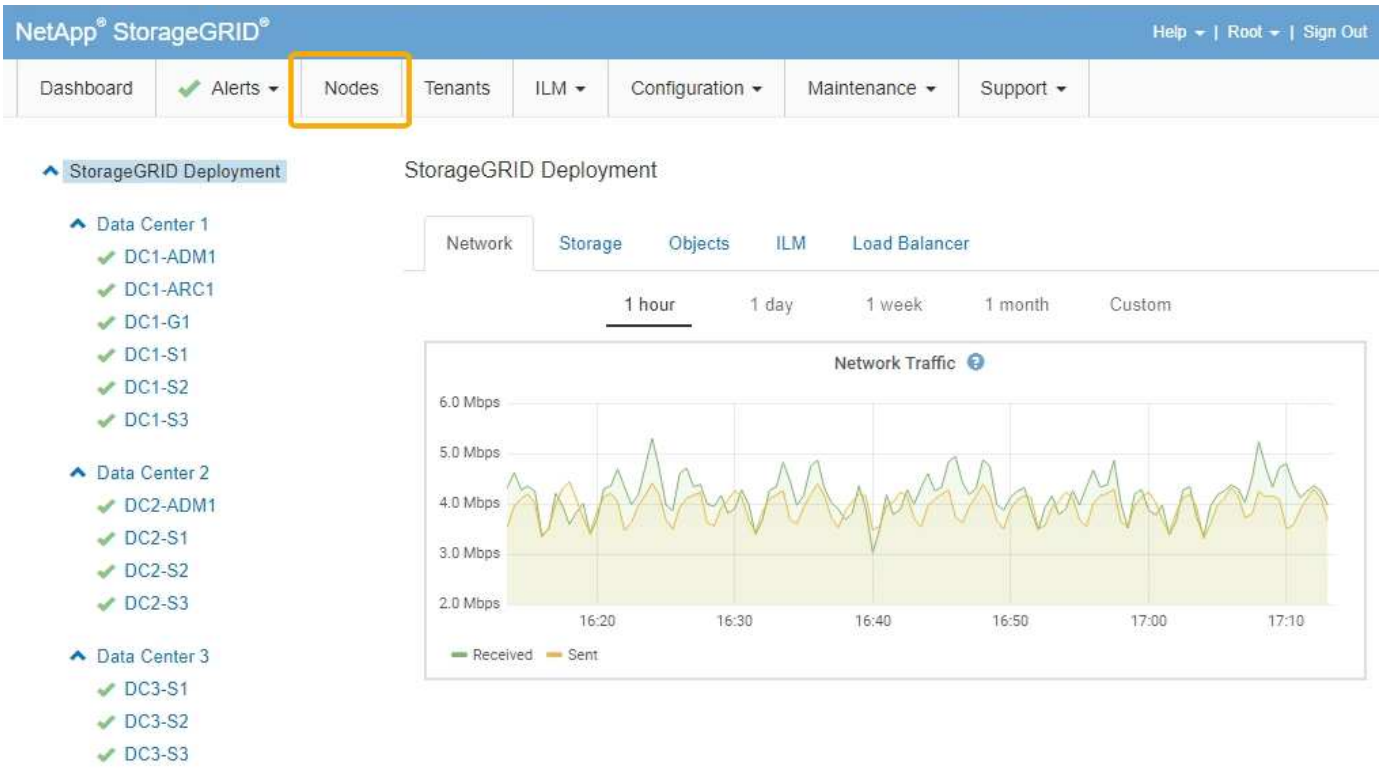
"监控和管理警报"

"监控和放大；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、请单击左侧的相应链接。



相关信息

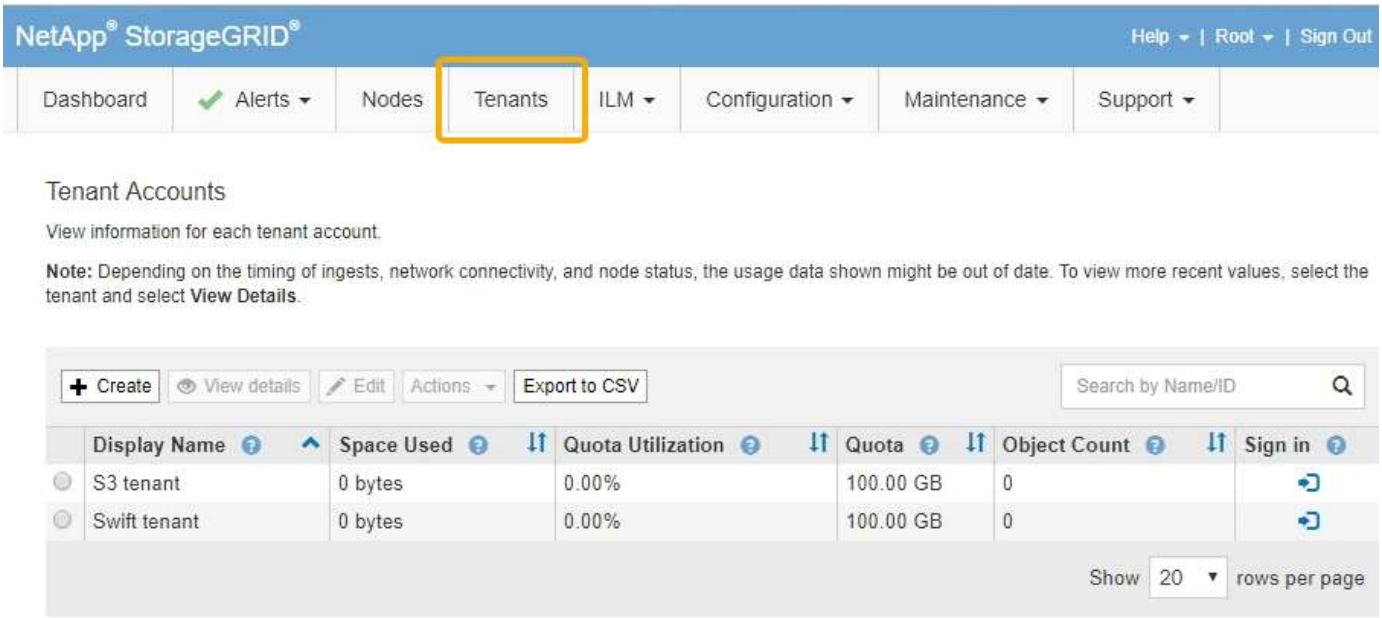
"查看节点页面"

"监控和放大；故障排除"

租户帐户页面

您可以通过租户帐户页面为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。

"租户帐户"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。



相关信息

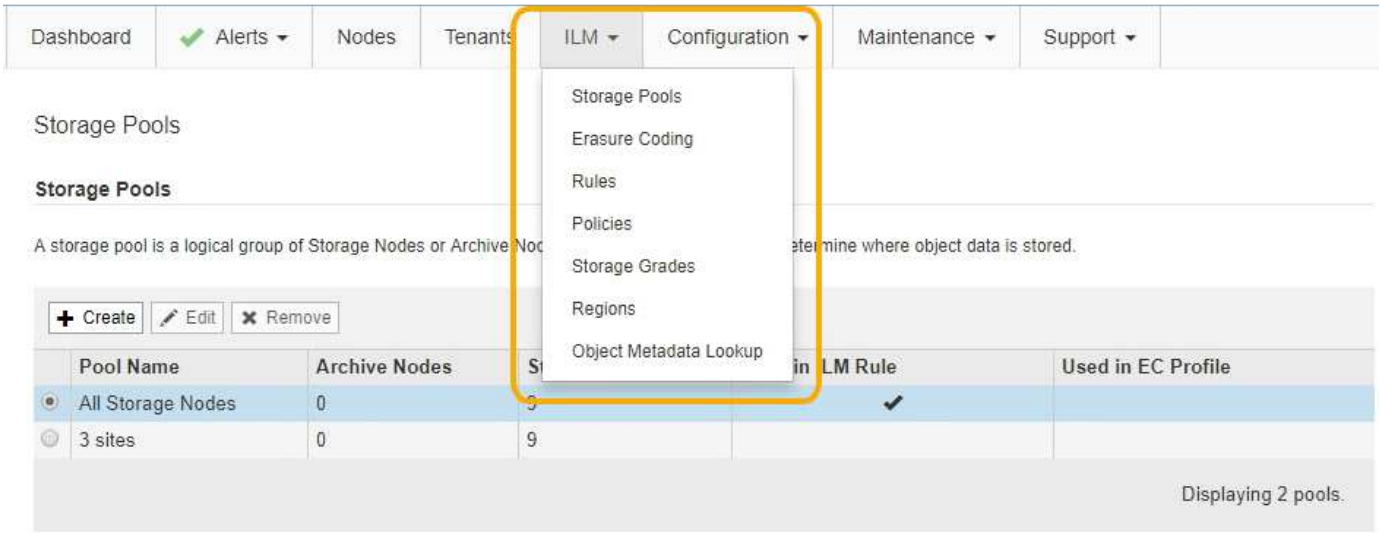
"管理租户和客户端连接"

"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。



相关信息

"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、系统设置、监控选项和访问控制选项。

相关信息

"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"

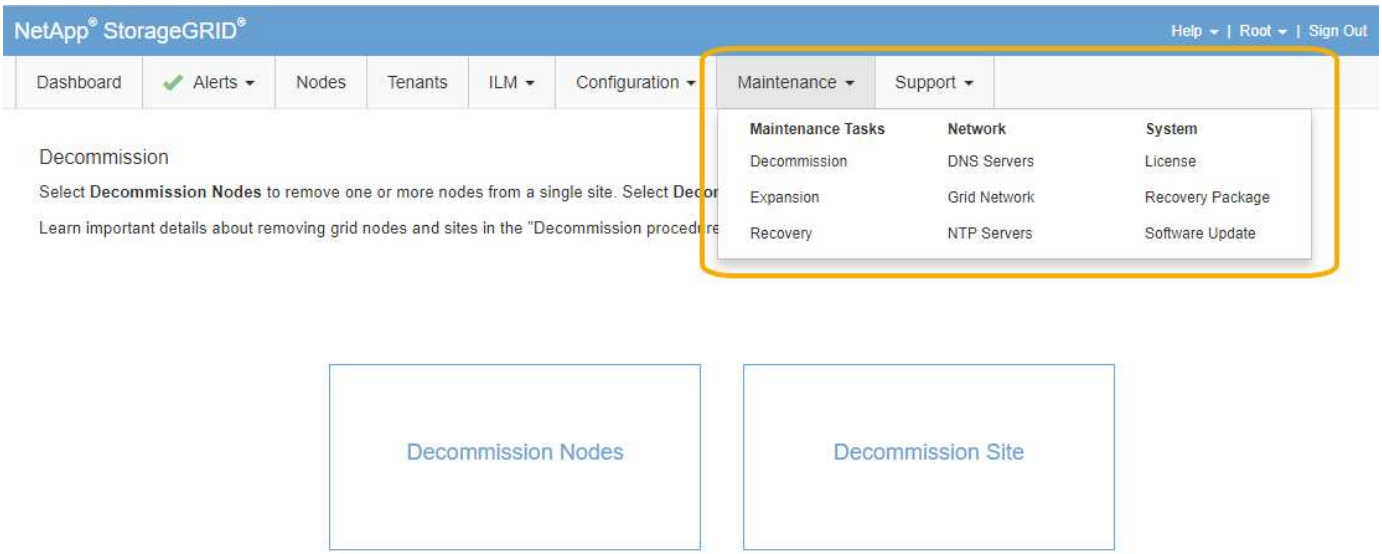
"管理 StorageGRID"

"监控和放大；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、网络任务和系统任务。



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。

网络

您可以从维护菜单执行的网络任务包括：

- 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。

系统

您可以从维护菜单执行的系统任务包括：

- 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。

相关信息

"执行维护过程"

"正在下载恢复包"

"扩展网格"

"升级软件"

"保持并恢复()"

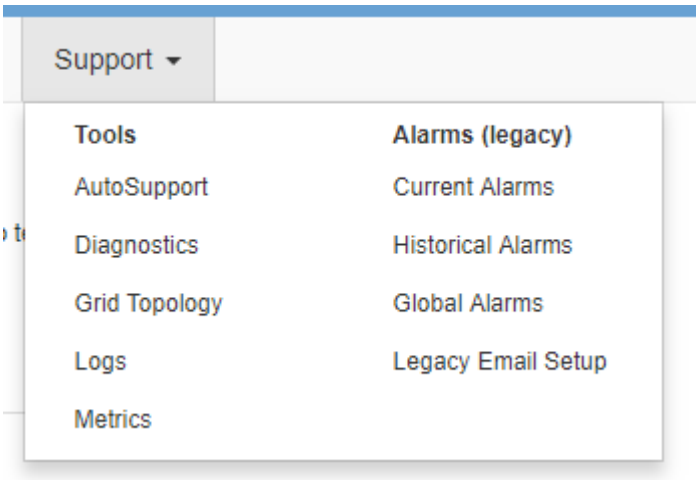
"SG6000 存储设备"

"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、并为旧警报和AutoSupport 设置电子邮件通知。

相关信息

"StorageGRID 架构和网络拓扑"

"StorageGRID 属性"

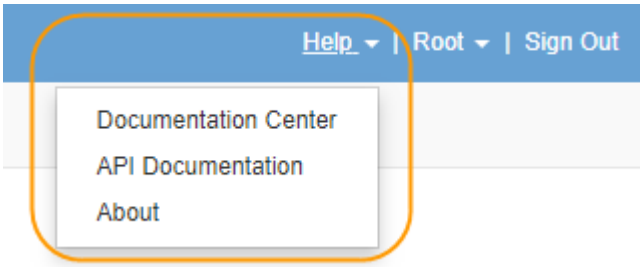
"使用StorageGRID 支持选项"

"管理 StorageGRID"

"监控和放大；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。



相关信息

"管理 StorageGRID"

了解租户管理器

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。

相关信息

"了解网格管理器"

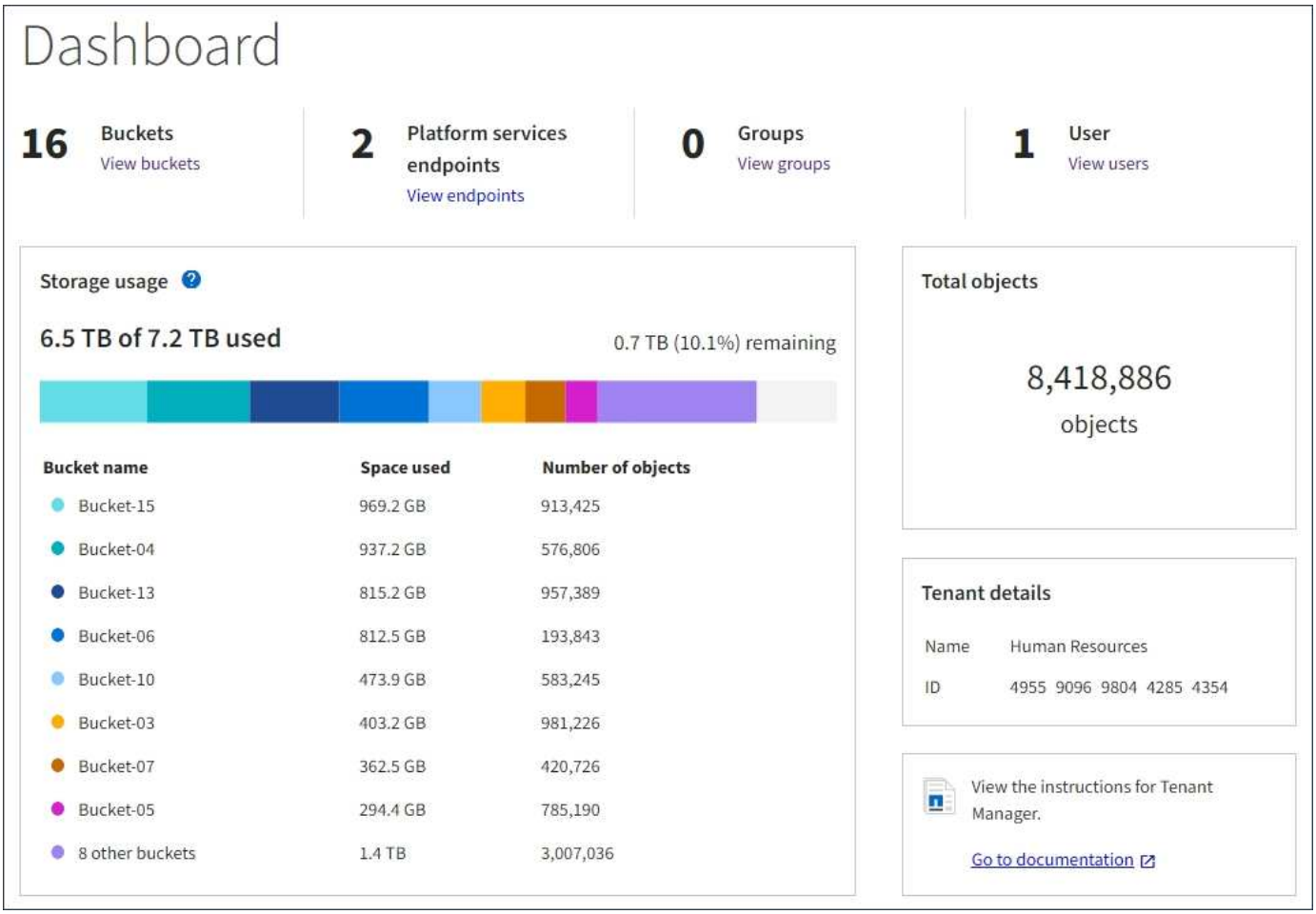
"使用租户帐户"

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
- 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

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：

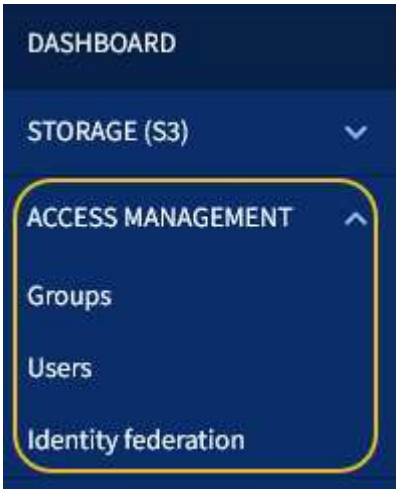
- 配置 S3 事件通知，可将其发送到支持 AWS Simple Notification Service （ SNS ）的目标服务。
- 配置 CloudMirror 复制，从而使租户能够自动将对象复制到外部 S3 存储分段。
- 配置搜索集成，每当创建，删除对象或更新其元数据或标记时，此集成都会将对象元数据发送到目标搜索索引。

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 ）。



使用StorageGRID

安装网格节点和StorageGRID 网络后、您可以开始配置和使用StorageGRID。您要执行的

部分任务包括控制用户对系统管理功能的访问、设置租户帐户、管理客户端连接、设置配置选项、使用ILM管理对象位置、监控StorageGRID 系统的运行状况和日常活动、以及执行例行和非例行维护活动。

- "控制StorageGRID 访问"
- "管理租户和客户端连接"
- "配置网络设置"
- "配置系统设置"
- "使用信息生命周期管理"
- "监控StorageGRID 操作"
- "执行维护过程"
- "使用StorageGRID 支持选项"

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。

使用客户端证书

您可以使用客户端证书允许授权的外部客户端访问StorageGRID Prometheus数据库。客户端证书提供了一种使

用外部工具监控StorageGRID 的安全方式。您可以提供自己的客户端证书、也可以使用网格管理器生成一个客户端证书。

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. 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）。
2. （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。
3. 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。

相关信息

"管理 StorageGRID"

"使用租户帐户"

"使用 S3"

"使用 Swift"

"了解租户管理器"

"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

高可用性组使用虚拟IP地址(VIP)为网关节点或管理节点服务提供主动备份访问。HA组由管理节点和网关节点上的一个或多个网络接口组成。创建HA组时、您可以选择属于网格网络(eth0)或客户端网络(eth2)的网络接口。

> 管理网络不支持HA VIP。

HA组维护一个或多个虚拟IP地址、这些地址会添加到组中的活动接口中。如果活动接口不可用、则虚拟IP地址将移至另一个接口。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。

出于多种原因、您可能希望使用高可用性(HA)组。

- 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。

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。

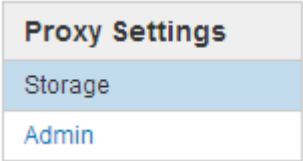
负载平衡器端点

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。

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。



服务器证书

您可以上传两种类型的服务器证书：

- 管理接口服务器证书、用于访问管理接口的证书。
- 对象存储API服务端点服务器证书、用于保护S3和Swift端点的安全、以便直接连接到存储节点或在网关节点上使用CLB服务。

> CLB 服务已弃用。

负载平衡器证书在负载平衡器端点页面上进行配置。密钥管理服务器(Key Management Server、KMS)证书在密钥管理服务器页面上进行配置。

流量分类策略

通过流量分类策略、您可以创建规则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。

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。

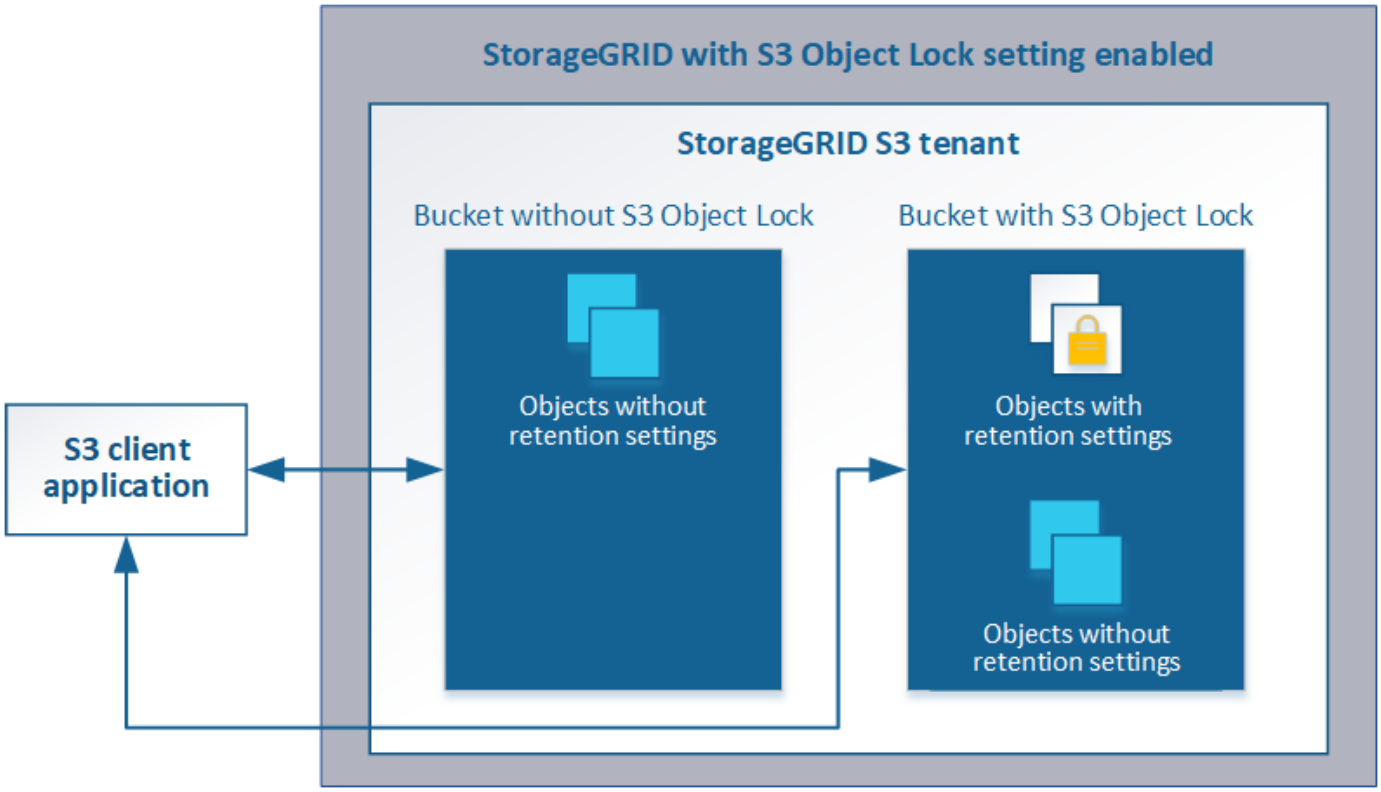
密钥管理服务器

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。

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）。



存储选项

通过存储选项、您可以控制对象分段并定义存储水印、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：

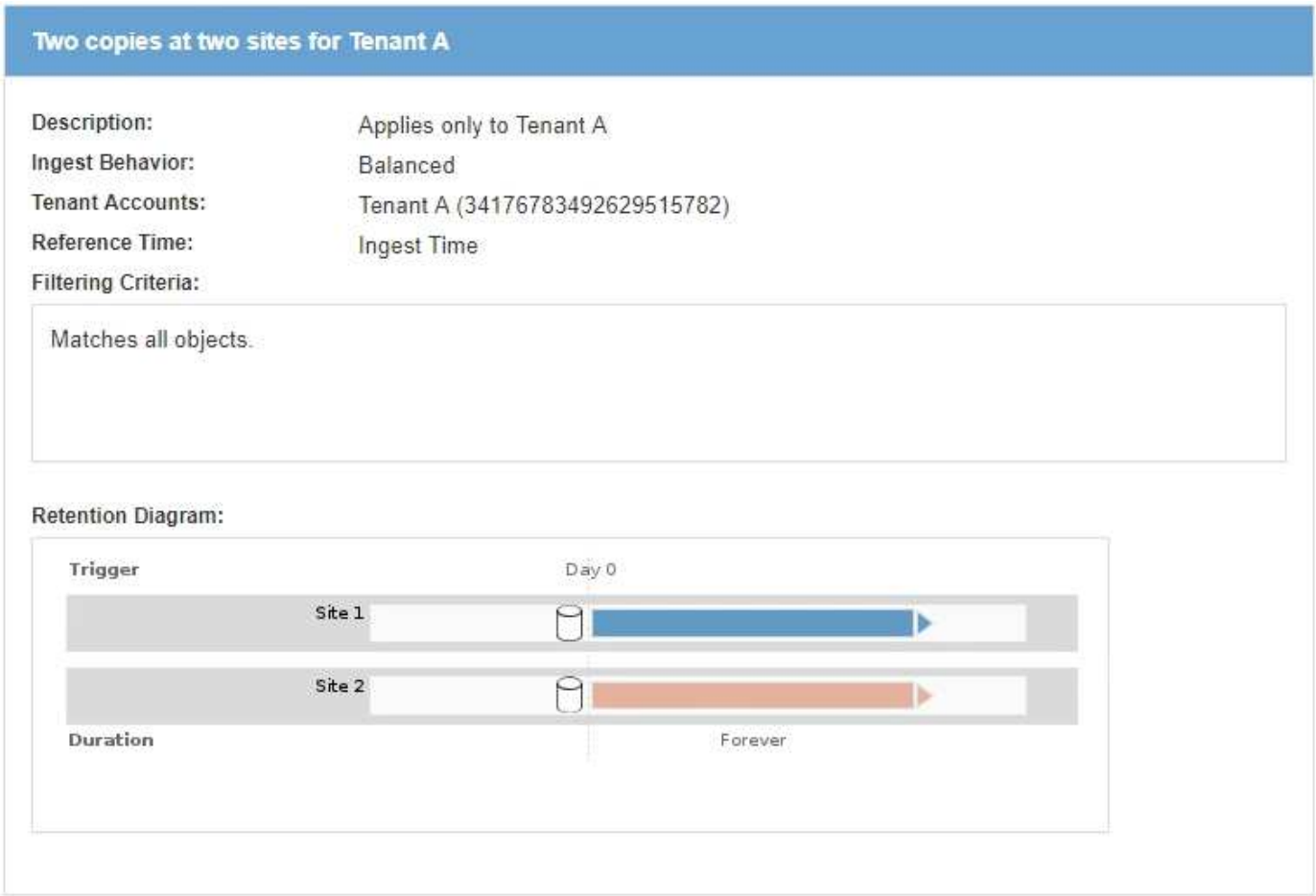
- 应存储哪些对象。规则可以应用于所有对象，也可以指定筛选器来标识规则适用场景 中的对象。例如，规则只能应用于与特定租户帐户，特定 S3 分段或 Swift 容器或特定元数据值关联的对象。
- 存储类型和位置。对象可以存储在存储节点，云存储池或归档节点上。
- 创建的对象副本的类型。可以复制副本或对副本进行纠删编码。
- 对于复制的副本，为创建的副本数。
- 对于纠删编码副本，使用纠删编码方案。
- 对象的存储位置和副本类型会随时间发生变化。
- 在将对象载入网格时如何保护对象数据（同步放置或双提交）。

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

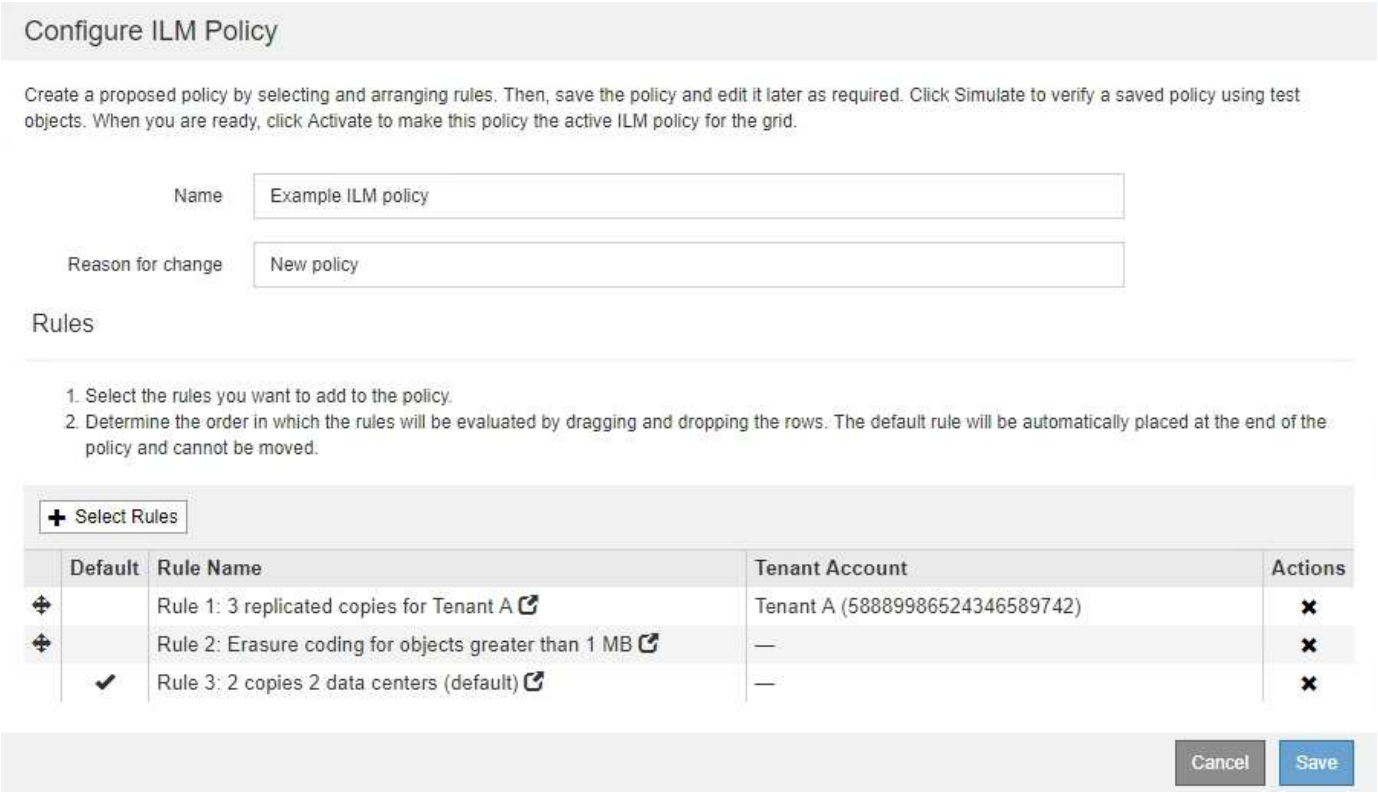
StorageGRID 系统的活动 ILM 策略控制所有对象的放置，持续时间和数据保护。

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。

ILM 策略示例

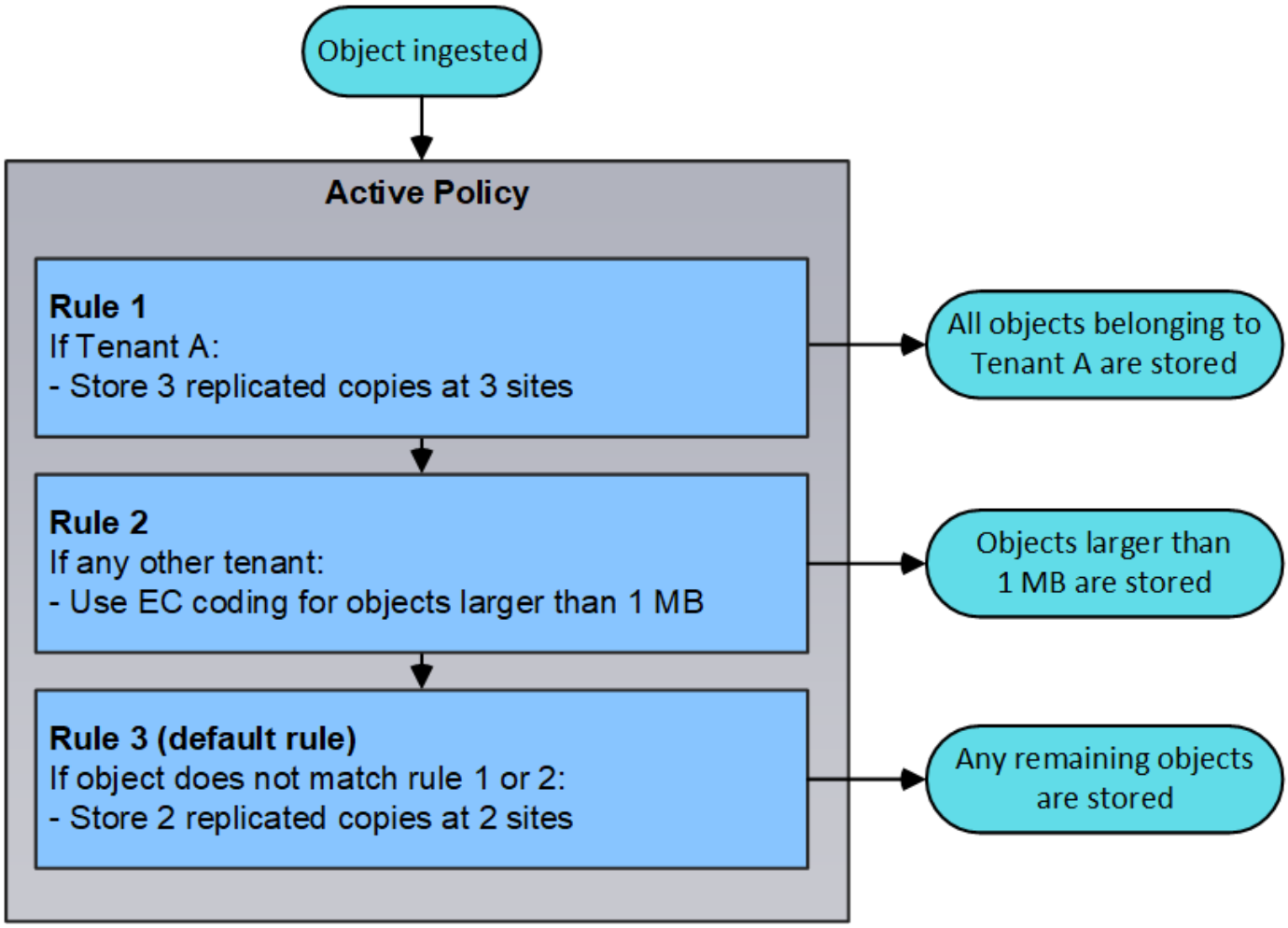
此示例 ILM 策略使用三个 ILM 规则。



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"

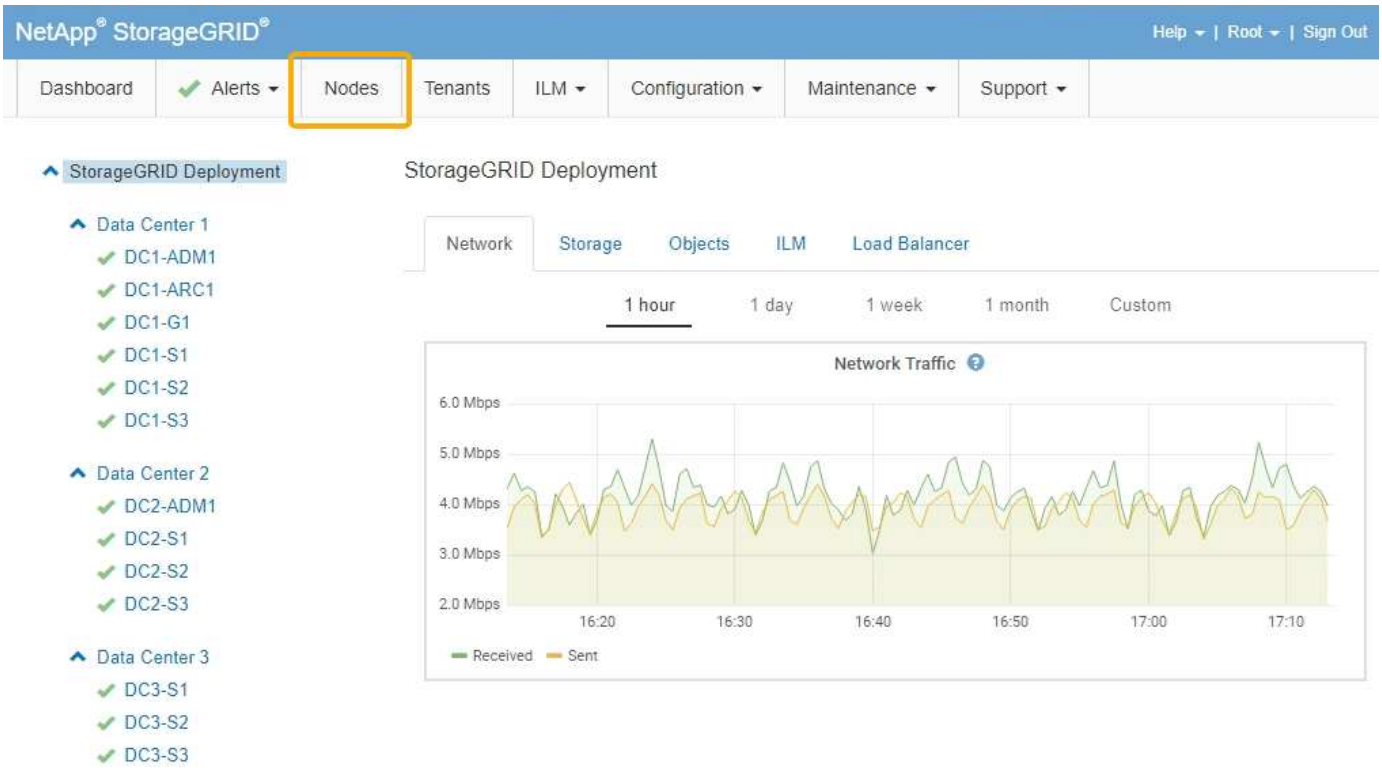
监控**StorageGRID** 操作

网格管理器可提供有关监控StorageGRID 系统日常活动的信息、包括其运行状况。

- "查看节点页面"
- "监控和管理警报"
- "使用SNMP监控"
- "查看审核消息"

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。



从左侧的树视图中、您可以看到StorageGRID 系统中的所有站点和所有节点。每个节点的图标用于指示节点是否已连接或是否存在任何活动警报。

连接状态图标

如果节点与网格断开连接、树视图将显示一个蓝色或灰色连接状态图标、而不是任何底层警报的图标。

- * 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。

警报图标

如果节点连接到网格、则树视图将显示以下图标之一、具体取决于节点当前是否存在任何警报。

- * 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。
- * 正常 * ：没有处于活动状态的警报、并且节点已连接到网格。

查看系统，站点或节点的详细信息

要查看可用信息、请单击左侧相应的链接、如下所示：

- 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。

相关信息

"监控和放大；故障排除"

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当前未确认警报。	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。	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
事件	显示任何系统错误或故障事件的计数、包括网络错误等错误。	所有节点
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

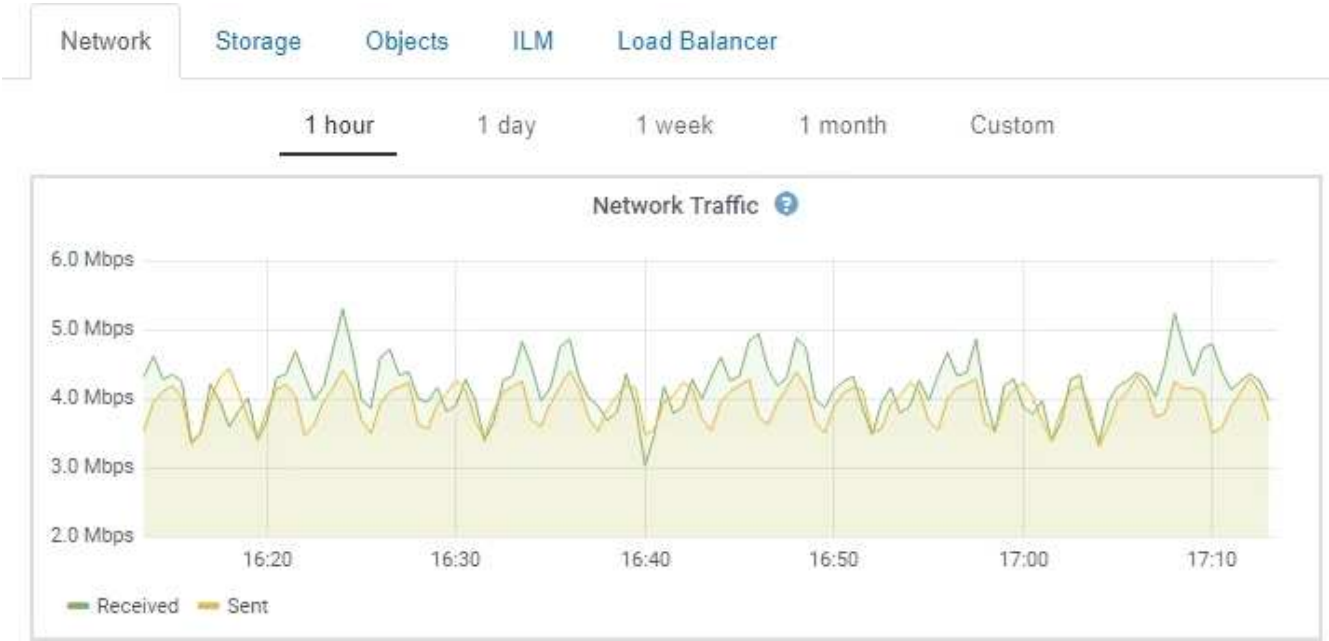
选项卡名称	**Description**	包括的
ILM	提供有关信息生命周期管理（ILM）操作的信息。 • 对于存储节点，提供有关纠删编码对象的 ILM 评估和后台验证的详细信息。 • 对于每个站点和整个网格，显示一个 ILM 队列随时间变化的图形。 • 对于整个网格，提供完成对所有对象的完整 ILM 扫描的估计时间。	存储节点，每个站点和整个网格
负载平衡器	包括与负载平衡器服务相关的性能和诊断图。 • 对于每个站点，提供该站点上所有节点的统计信息的聚合摘要。 • 对于整个网格，提供所有站点的统计信息的聚合摘要。	管理节点和网关节点，每个站点和整个网格
平台服务	提供有关站点上任何 S3 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低于8.70、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、请参见网格管理API (帮助>* API文档*>*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、它们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。

相关信息

"监控和管理警报"

"使用StorageGRID 支持选项"

"监控和放大；故障排除"

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

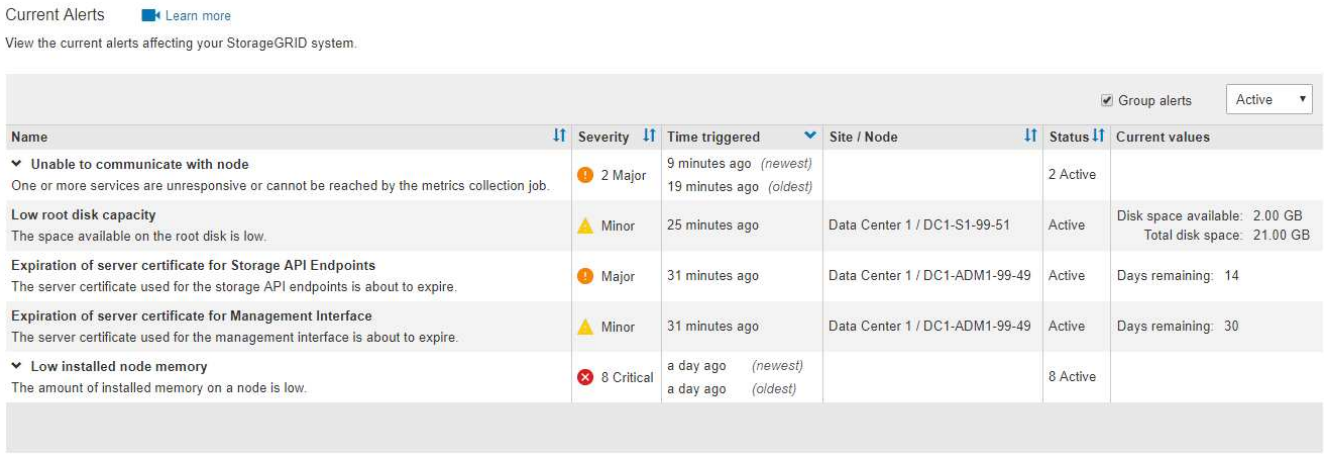
"监控和放大；故障排除"

监控和管理警报

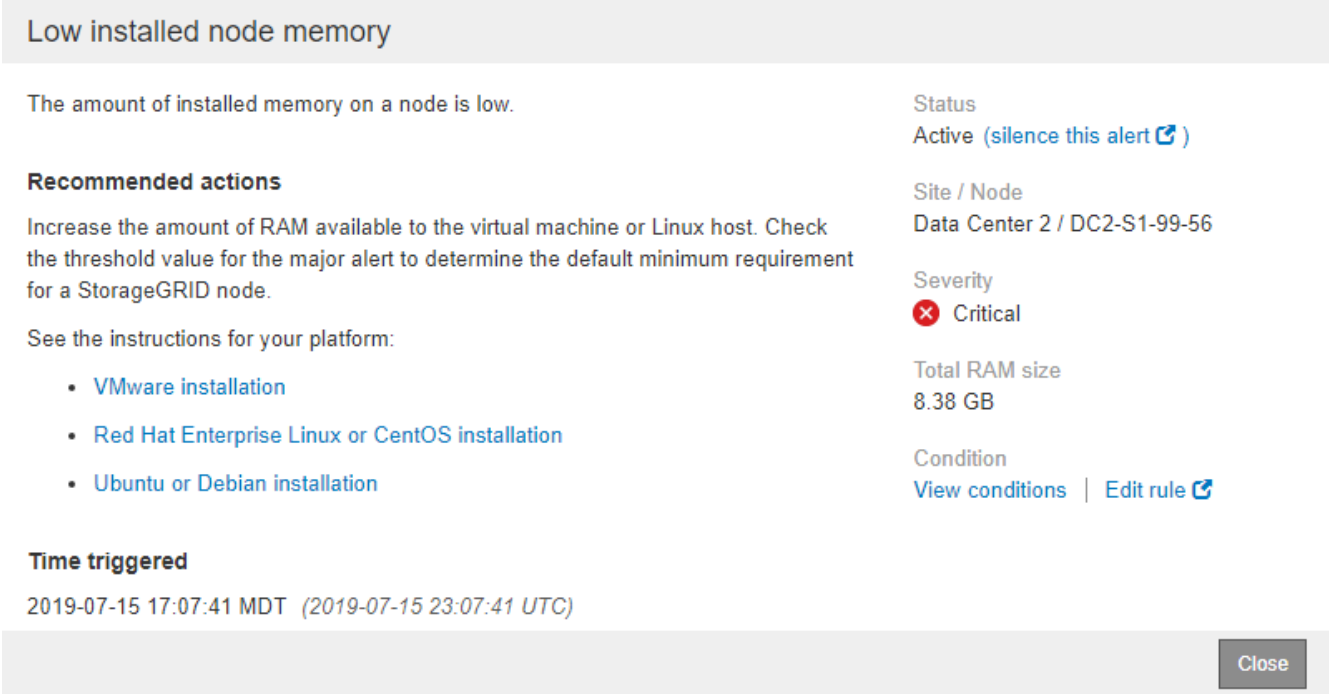
警报系统提供了一个易于使用的界面，用于检测，评估和解决 StorageGRID 运行期间可能发生的问题。

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。



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。

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 *

"监控和放大；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 *

"监控和放大；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。

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

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"

"管理 StorageGRID"

执行维护过程

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。

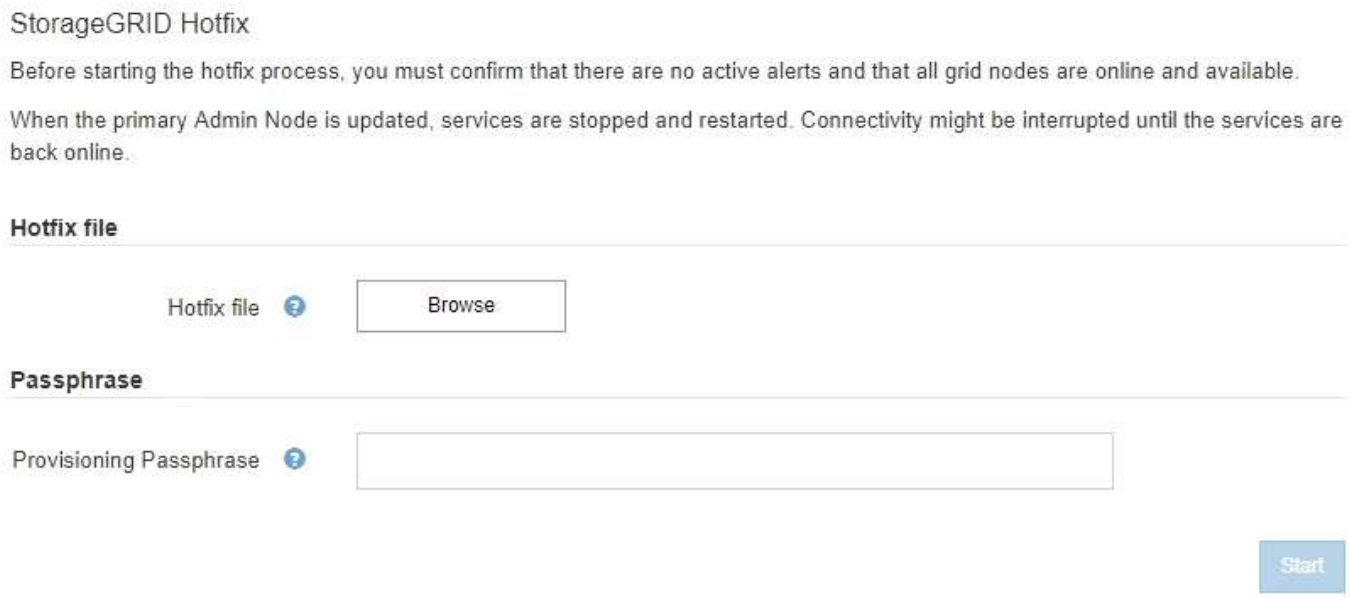
在 StorageGRID 软件升级期间，客户端应用程序可以继续载入和检索对象数据。

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。



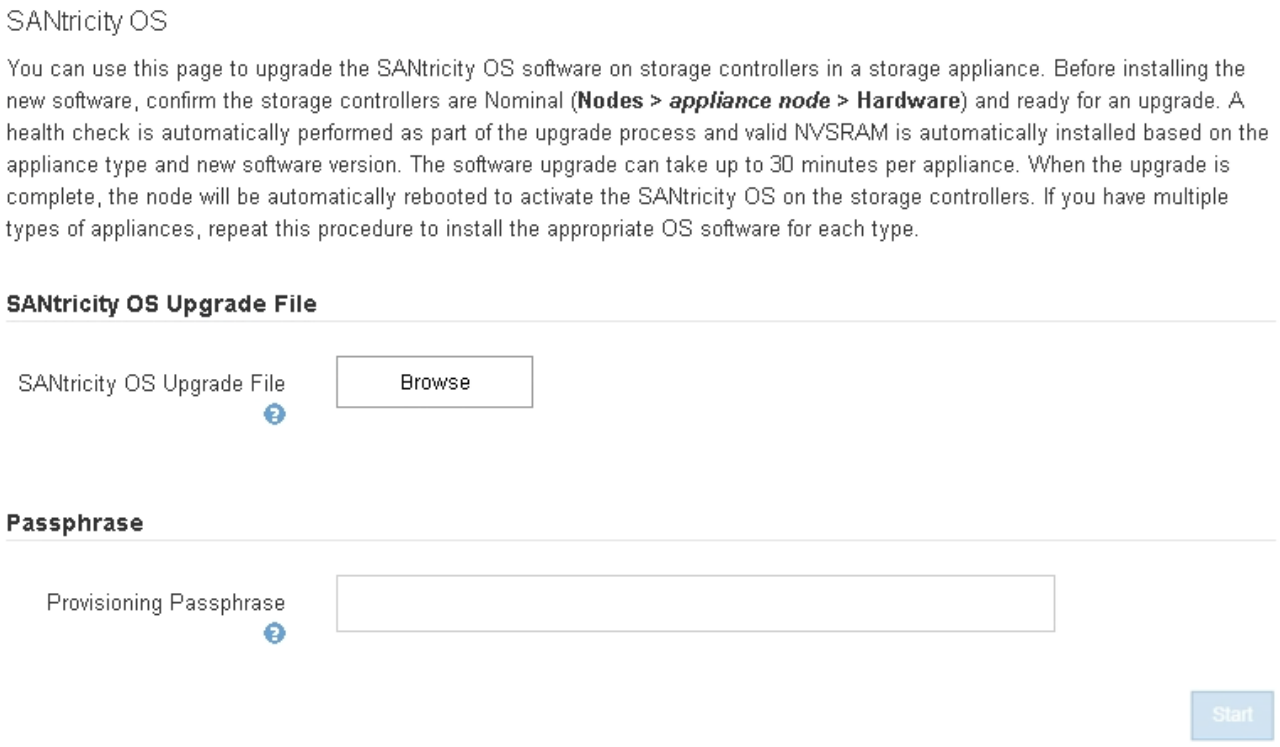
此修补程序会首先应用于主管理节点。然后，您必须批准将此修补程序应用于其他网格节点，直到 StorageGRID 系统中的所有节点运行相同的软件版本为止。您可以通过选择批准单个网格节点，网格节点组或所有网格节点来自定义批准顺序。

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 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 。

Grid Expansion

A new Recovery Package has been generated as a result of the configuration change. Go to the Recovery Package page to download it.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing Grid Nodes — In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Search

Name	Site	Grid Network IPv4 Address	Progress	Stage
DC2-ADM1-184	Site A	172.17.3.184/21		Waiting for NTP to synchronize
DC2-S1-185	Site A	172.17.3.185/21		Waiting for Dynamic IP Service peers
DC2-S2-186	Site A	172.17.3.186/21		Waiting for NTP to synchronize
DC2-S3-187	Site A	172.17.3.187/21		Waiting for NTP to synchronize
DC2-S4-188	Site A	172.17.3.188/21		Waiting for Dynamic IP Service peers
DC2-ARC1-189	Site A	172.17.3.189/21		Waiting for NTP to synchronize

2. Initial Configuration — Pending

3. Distributing the new grid node's certificates to the StorageGRID system. — Pending

4. Starting services on the new grid nodes — Pending

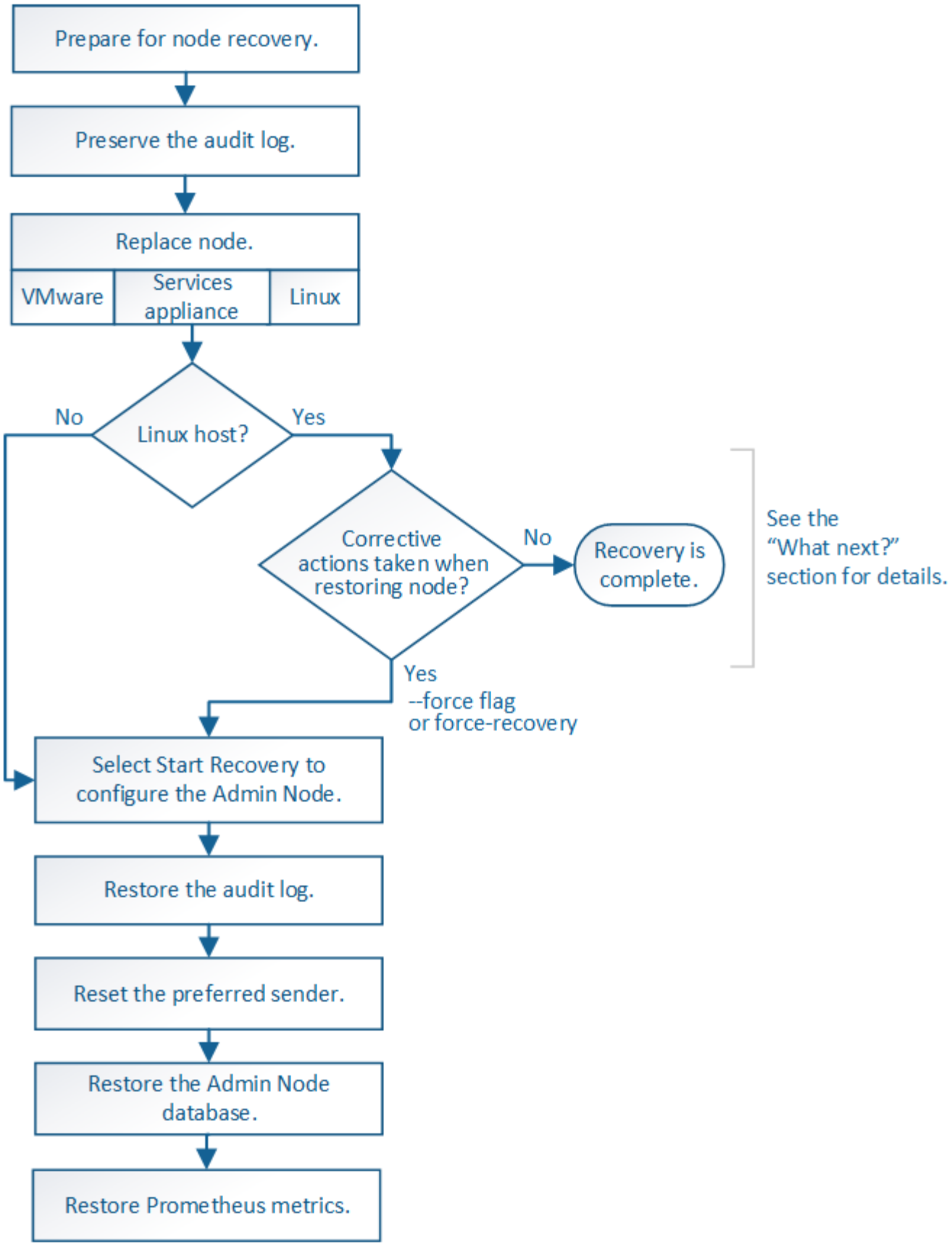
5. Cleaning up unused Cassandra keys — Pending

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

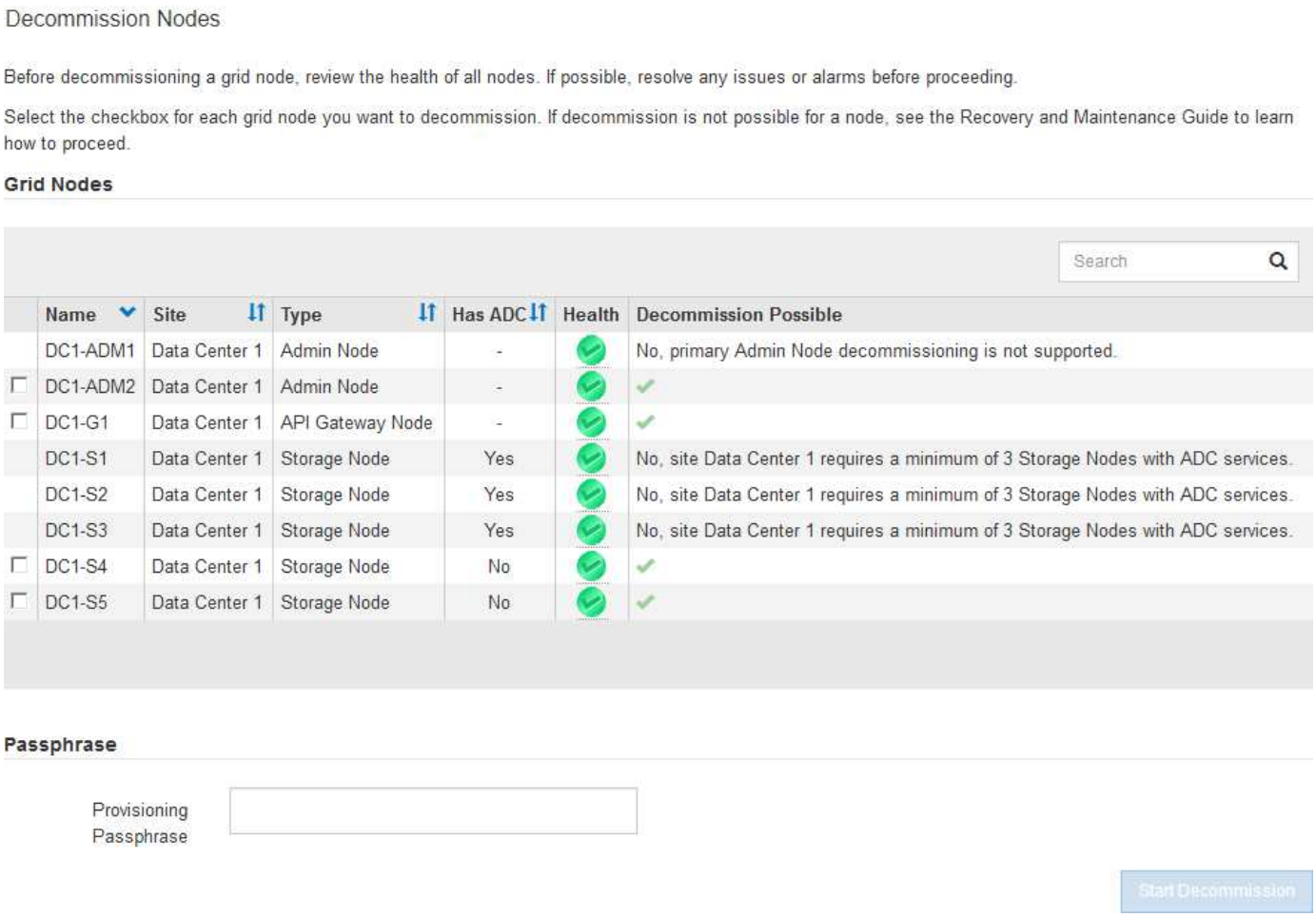
您可能需要从 StorageGRID 系统中永久删除网格节点或整个数据中心站点。

例如，在以下情况下，您可能需要停用一个或多个网格节点：

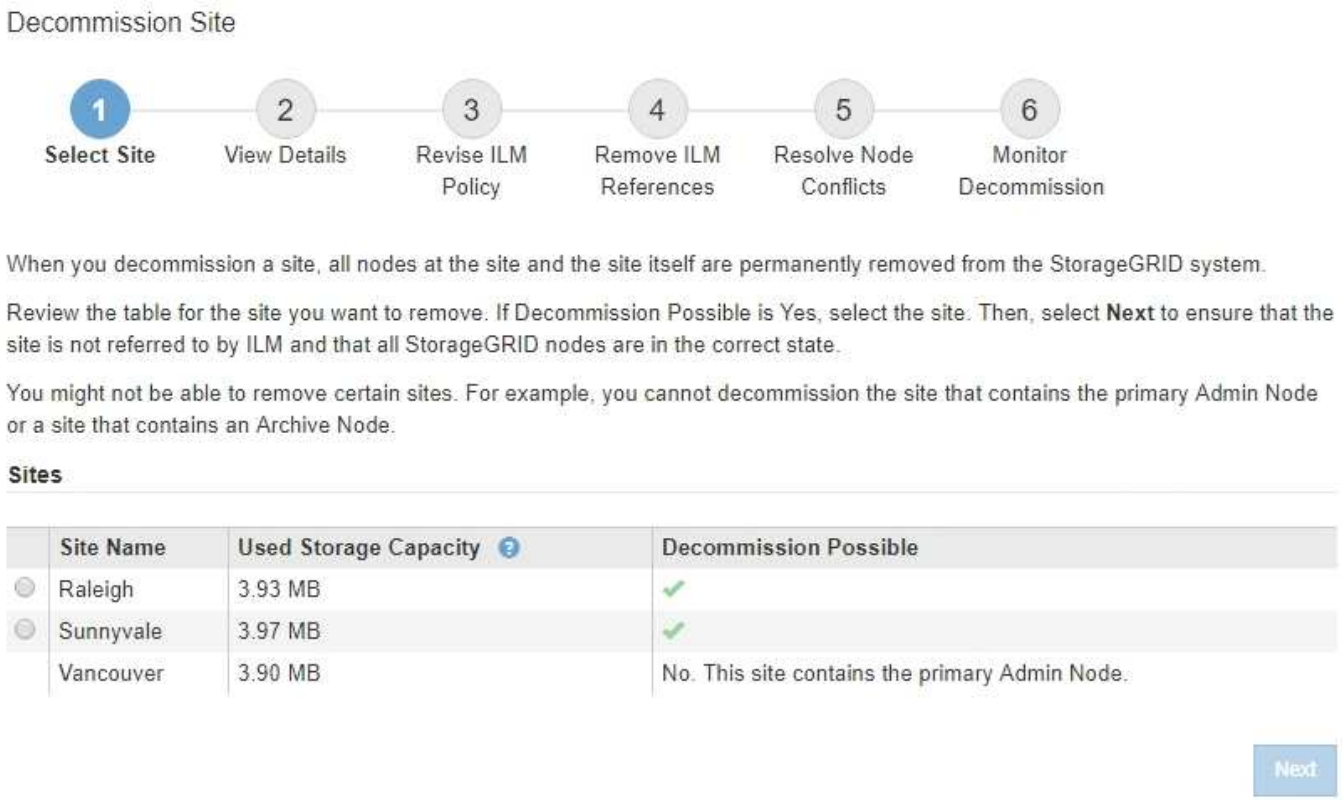
- 您已向系统中添加较大的存储节点，并希望删除一个或多个较小的存储节点，同时保留对象。
- 您所需的总存储较少。
- 您不再需要网关节点或非主管理节点。
- 您的网格包含一个断开连接的节点，您无法恢复此节点或使其恢复联机。

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（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。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"

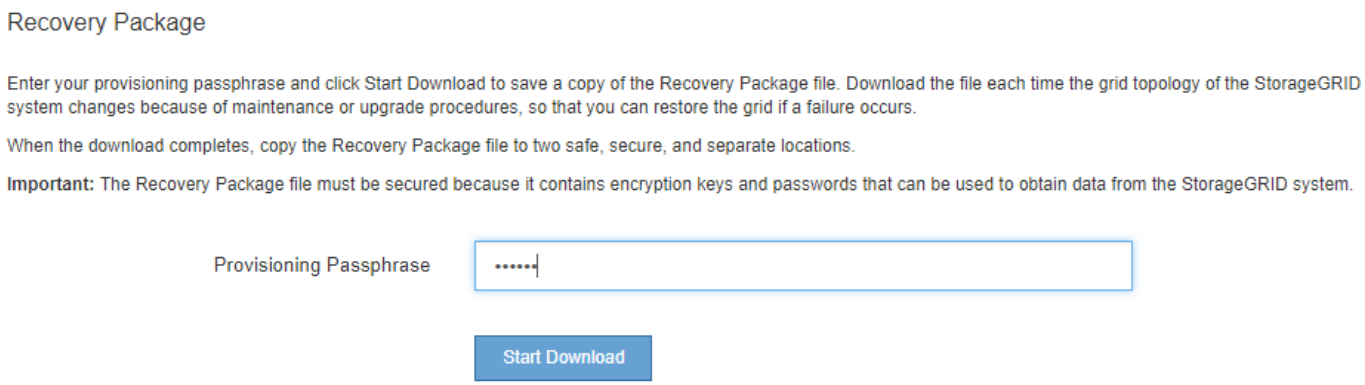
"保持并恢复()"

正在下载恢复包

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"

"保持并恢复()"

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。

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
- 事件信息、如*节点*>*节点_*>*事件*页面中所示
- 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 、则网格管理器信息板上会显示一条消息。此消息包含指向 AutoSupport 配置页面的链接。

您可以选择"`x`"符号 ✕ 以关闭消息。清除浏览器缓存后、即使AutoSupport 仍处于禁用状态、此消息也不会再次显示。

使用**Active IQ**

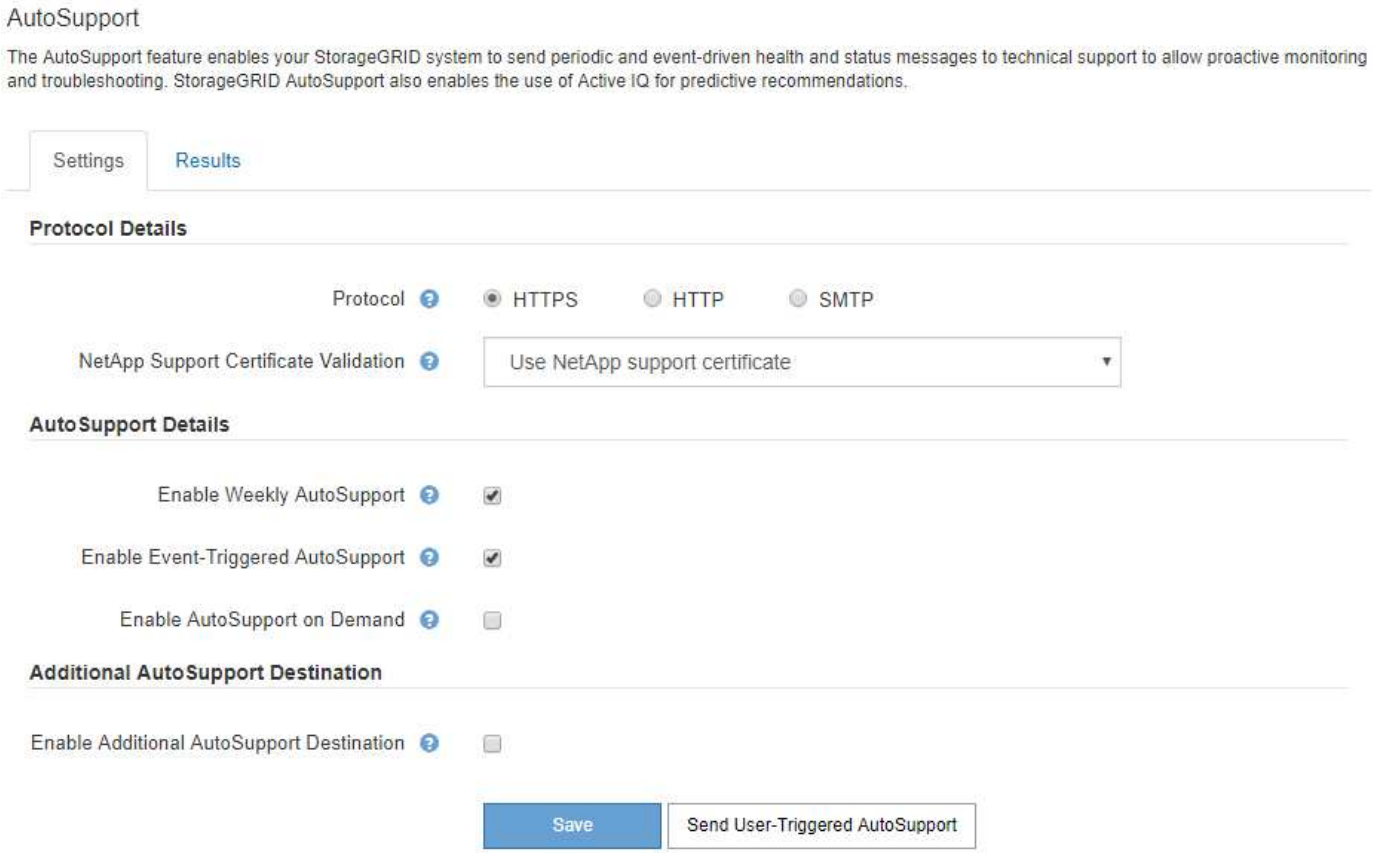
Active IQ 是一名基于云的数字顾问，利用 NetApp 客户群的预测性分析和社区智慧。其持续风险评估，预测性警报，规范化指导和自动化操作可帮助您在问题发生之前防患于未然，从而改善系统运行状况并提高系统可用性。

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 Digital Advisor 文档"

访问**AutoSupport** 设置

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 * 。



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

"管理 StorageGRID"

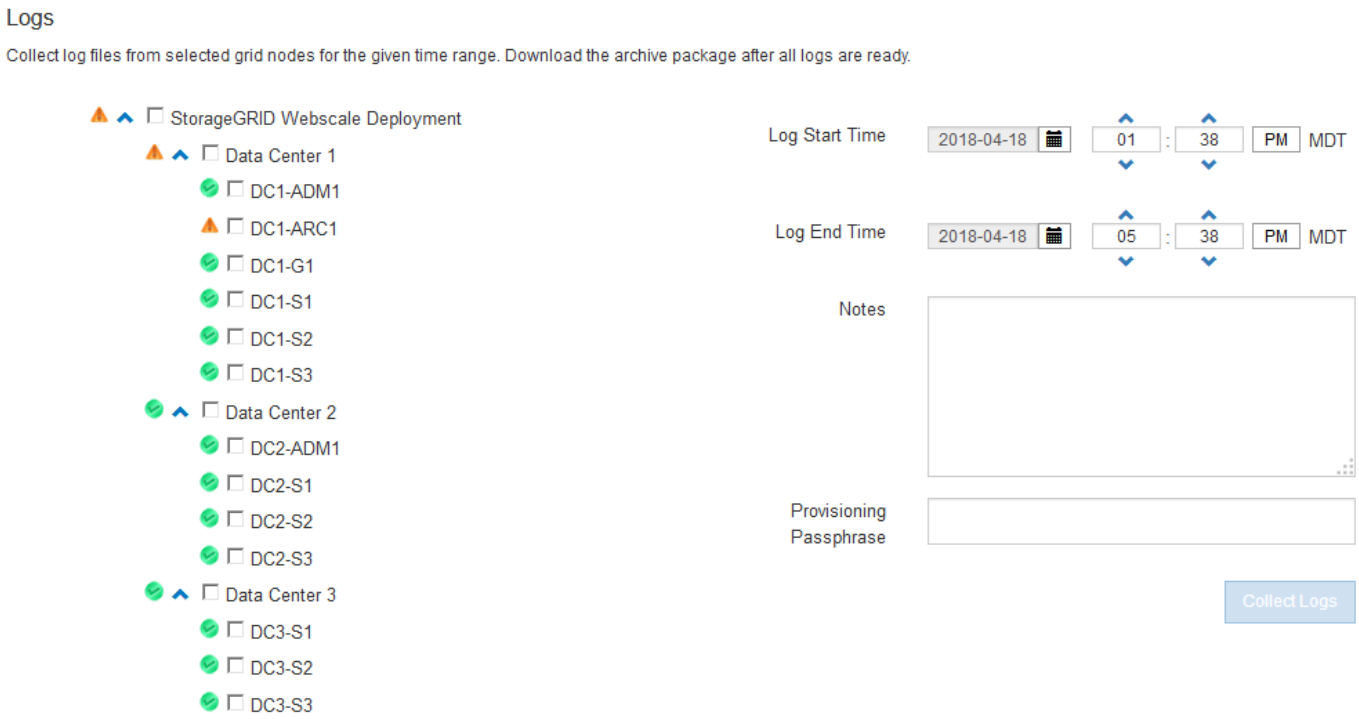
"配置网络设置"

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。数据会在中收集并归档 `.tar.gz` 文件、您可以将其下载到本地计算机。在此文件中，每个网格节点都有一个日志文件归档。



相关信息

"监控和放大；故障排除"

"管理 StorageGRID"

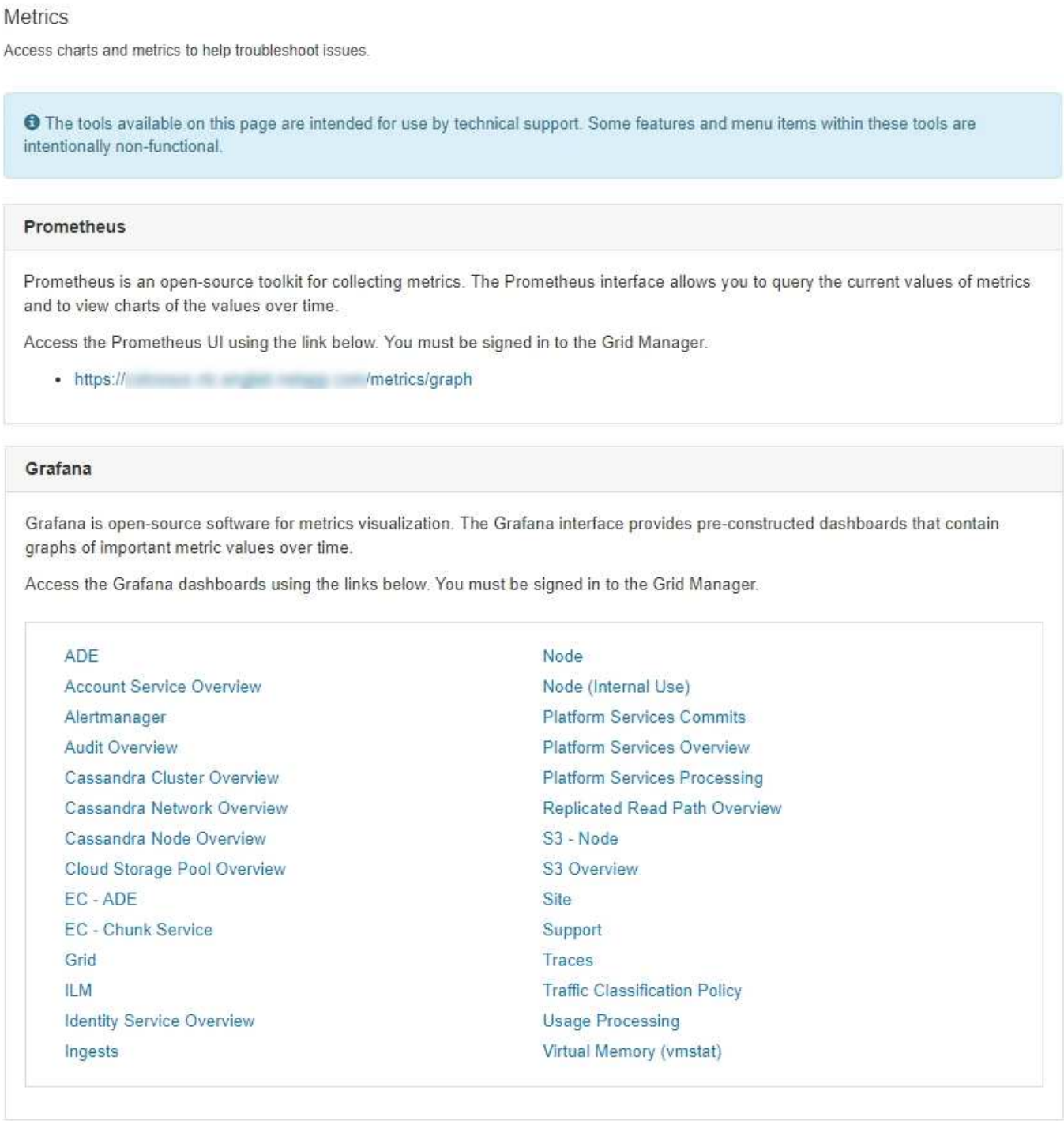
使用指标并运行诊断

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。

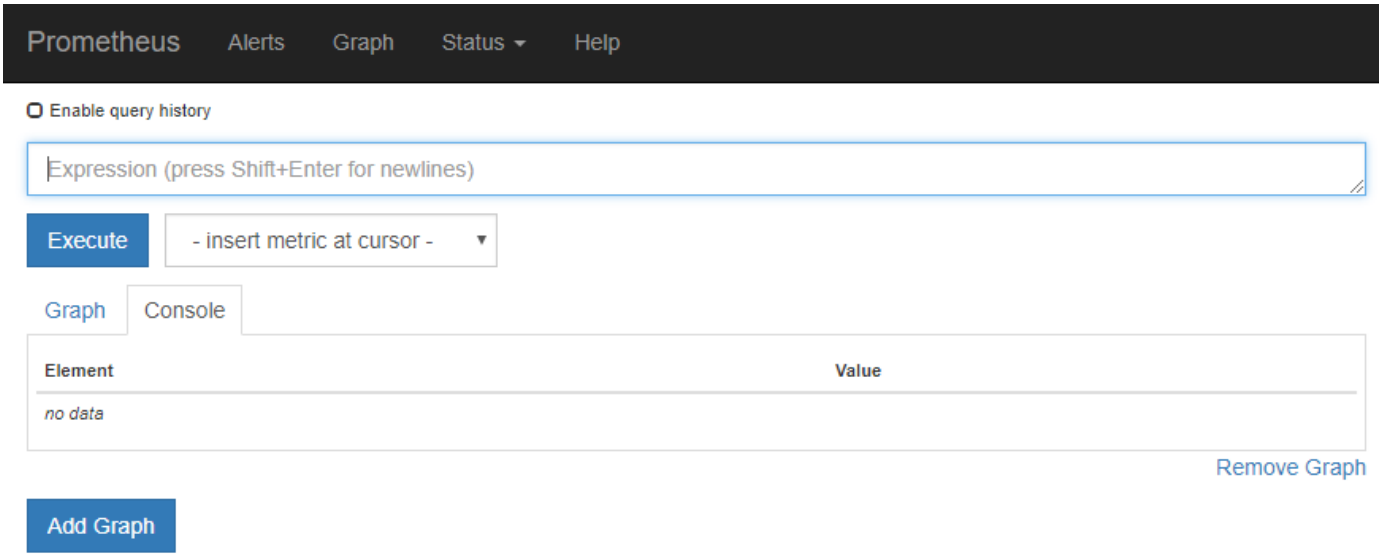
指标页面

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。

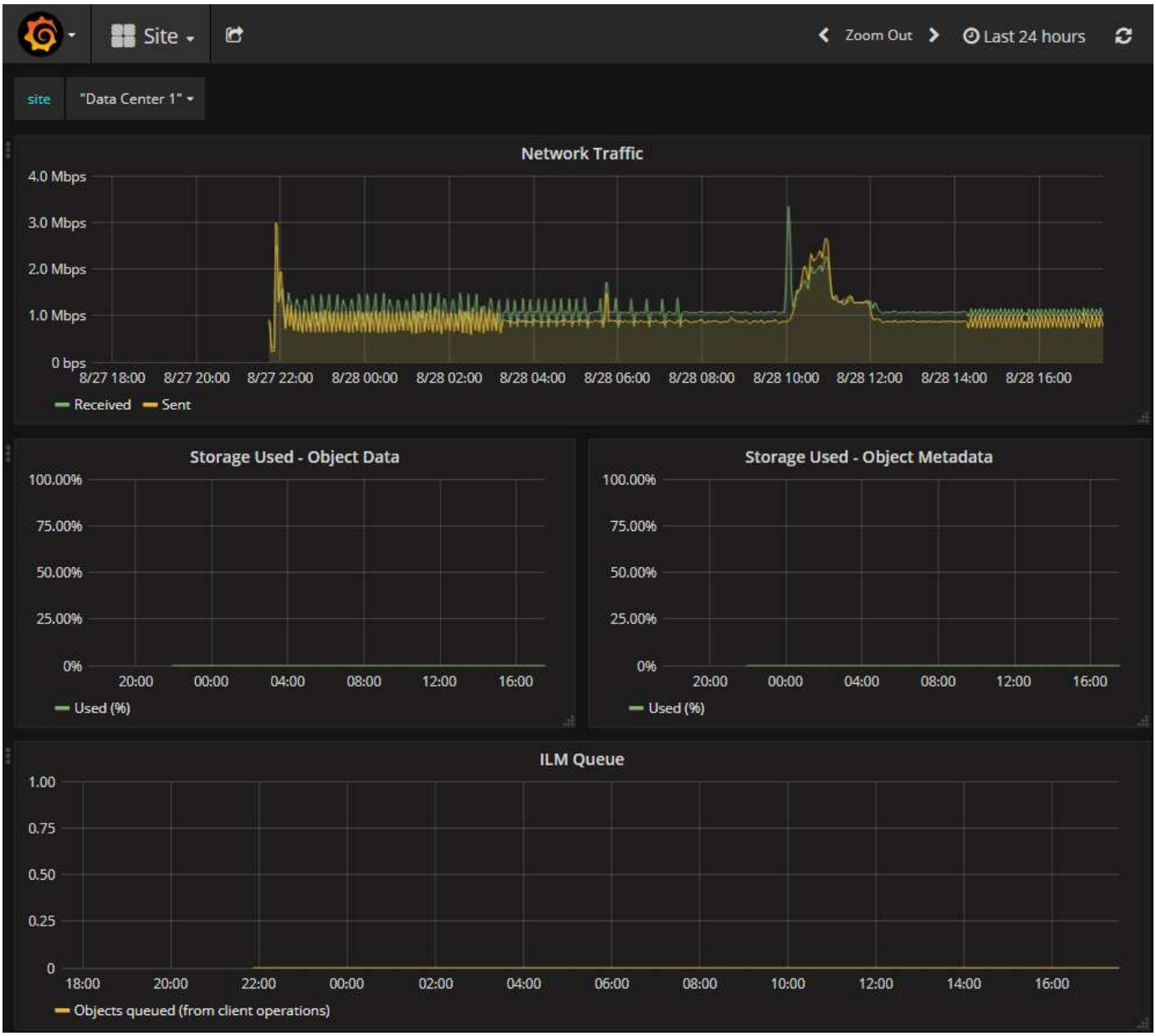


您可以通过指标页面的 Prometheus 部分中的链接查询 StorageGRID 指标的当前值，并查看这些值随时间变化的图形。



> 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。

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- **Normal**: All values are within the normal range.
- **Attention**: One or more of the values are outside of the normal range.
- **Caution**: One or more of the values are significantly outside of the normal range.

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

Run Diagnostics

- Cassandra blocked task queue too large
- Cassandra commit log latency
- Cassandra commit log queue depth
- Cassandra compaction queue too large

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。

CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the **Node** Grafana dashboard.

Status Normal

Prometheus query

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))
```

View in Prometheus

Thresholds
Attention >= 75%
Caution >= 95%

Status	Instance	CPU Utilization
	DC1-ADM1	2.598%
	DC1-ARC1	0.937%
	DC1-G1	2.119%
	DC1-S1	8.708%
	DC1-S2	8.142%
	DC1-S3	9.669%
	DC2-ADM1	2.515%
	DC2-ARC1	1.152%
	DC2-S1	8.204%
	DC2-S2	5.000%
	DC2-S3	10.469%

相关信息

"监控和放大；故障排除"

网络连接准则

了解StorageGRID 架构和网络拓扑。熟悉网络配置和配置的要求。

- "StorageGRID 网络概述"
- "网络连接要求和准则"
- "部署特定的网络注意事项"
- "网络安装和配置"
- "安装后准则"
- "网络端口参考"

StorageGRID 网络概述

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_Grid primer_中所述的StorageGRID 架构。

在部署和配置StorageGRID 之前、您必须配置网络基础架构。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都需要进行通信。

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。

在确定要使用的三个StorageGRID 网络中的哪一个以及这些网络的配置方式之后、您可以按照相应的说明安装和配置StorageGRID 节点。

相关信息

"网格入门"

"管理 StorageGRID"

"发行说明"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

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）
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）

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。

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。

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。

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地址。有关详细信息，请参见有关管理 StorageGRID 的说明。

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。

通过使用管理网络、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用户界面；访问NTP、DNS、外部密钥管理(KMS)和轻型目录访问协议(LDAP)等关键服务；访问管理节点上的审核日志；以及访问安全Shell协议(SSH)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。有关不可信客户端网络功能和负载平衡器服务的详细信息、请参见有关管理StorageGRID 的说明。

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、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。

相关信息

"网络连接要求和准则"

"管理 StorageGRID"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

网络拓扑示例

除了所需的网格网络之外、在为单站点或多站点部署设计网络拓扑时、您还可以选择是配置管理网络接口还是客户端网络接口。

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。有关内部和外部端口的详细信息、请参见网络端口参考。

如果您指定节点的客户端网络接口不可信、请配置负载平衡器端点以接受入站流量。有关配置不可信客户端网络和负载平衡器端点的信息、请参见有关管理StorageGRID 的说明。

相关信息

"管理 StorageGRID"

"网络端口参考"

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。

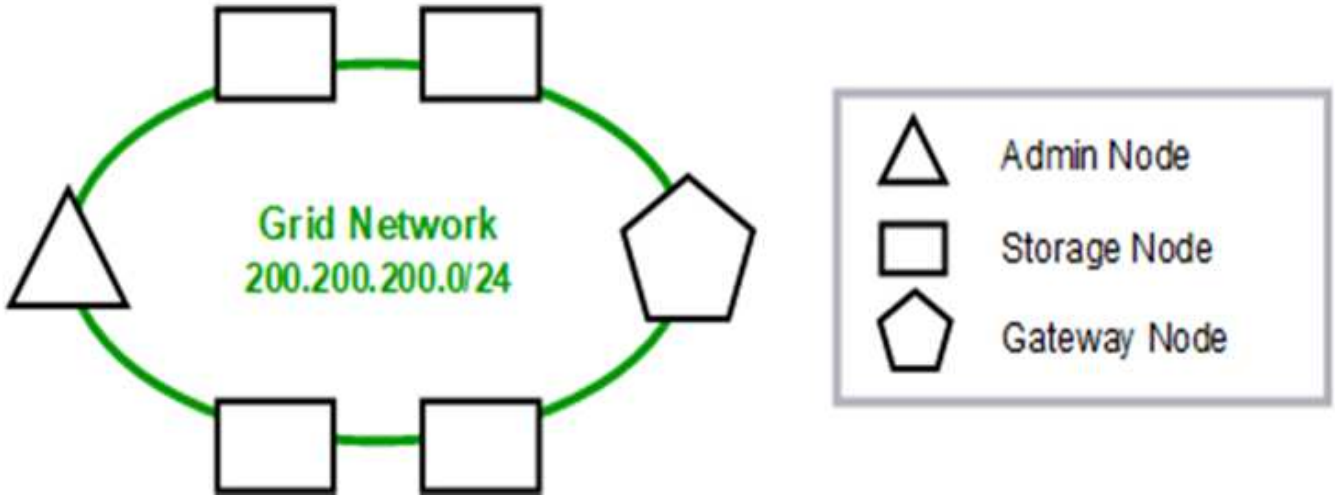
在配置期间，必须将所有网格网络子网添加到网格网络子网列表（ GSLL ）中。此列表包括所有站点的所有子网，并且可能还包括外部子网，这些子网可提供对 NTP ， DNS 或 LDAP 等关键服务的访问权限。

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

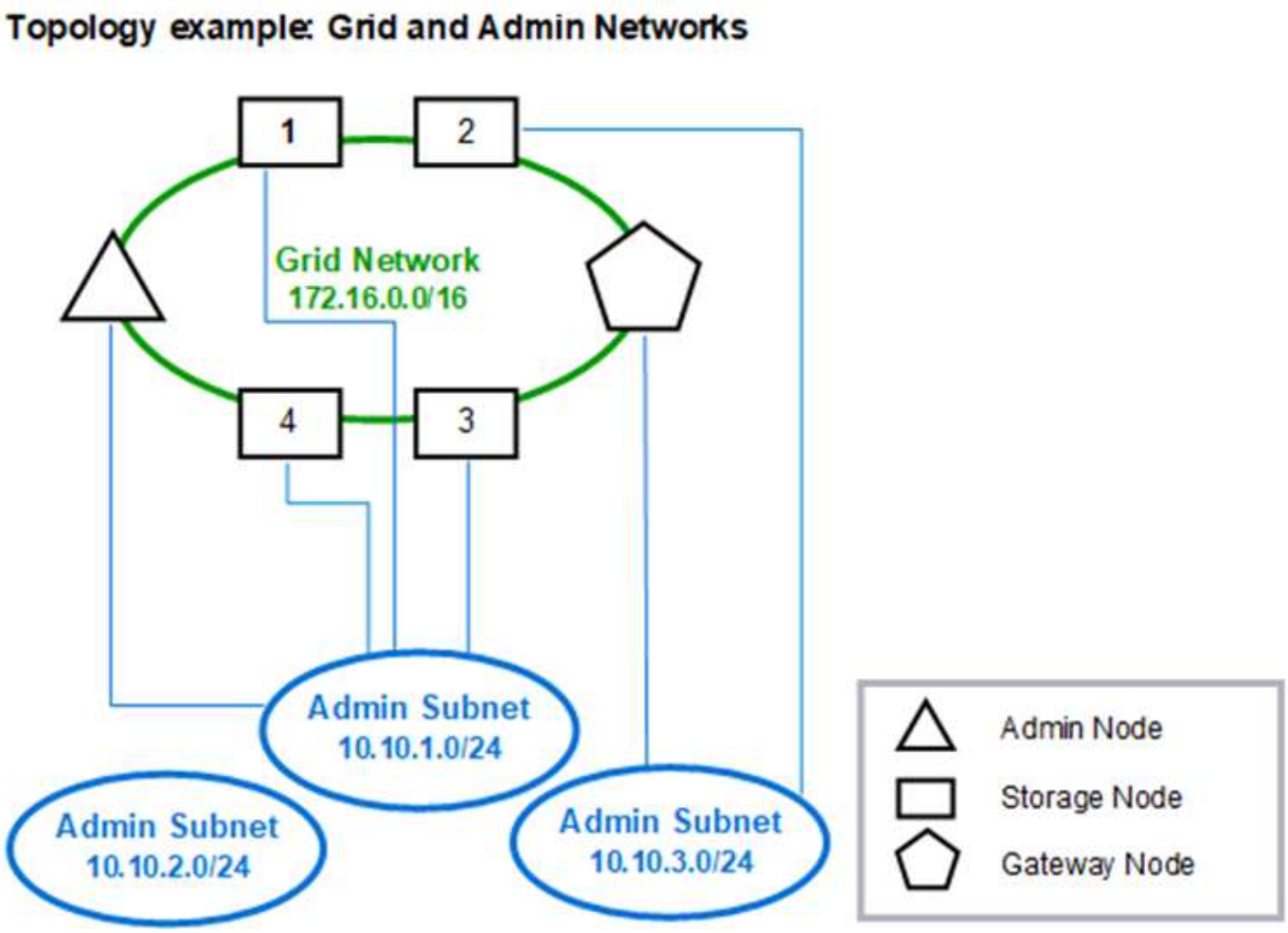
可以选择使用管理网络。使用管理网络和网格网络的一种方法是，为每个节点配置可路由的网格网络和有限制的管理网络。

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。


Topology example: Grid and Admin Networks
1
2
Grid Network
172.16.0.0/16
4
3
Admin Subnet
10.10.1.0/24
Admin Subnet
10.10.2.0/24
Admin Subnet
10.10.3.0/24
Admin Node
Storage Node
Gateway Node

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

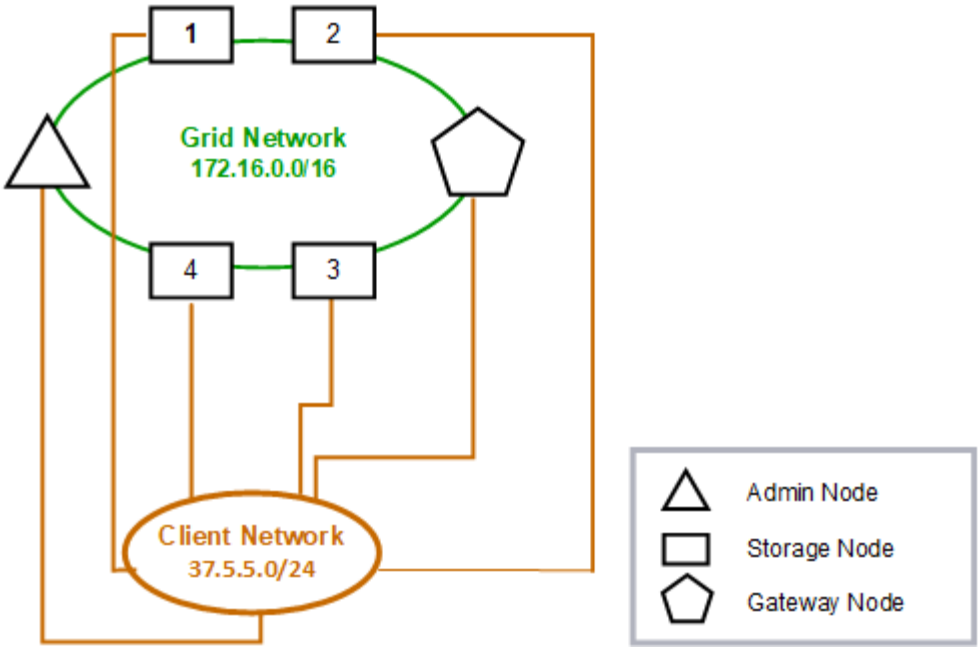
可以选择使用客户端网络。使用客户端网络可以将客户端网络流量（例如 S3 和 Swift ）与网格内部流量分隔开，从而提高网格网络连接的安全性。如果未配置管理网络，则可通过客户端网络或网格网络处理管理流量。

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

Nodes	Grid Network IP/mask	Client Network 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

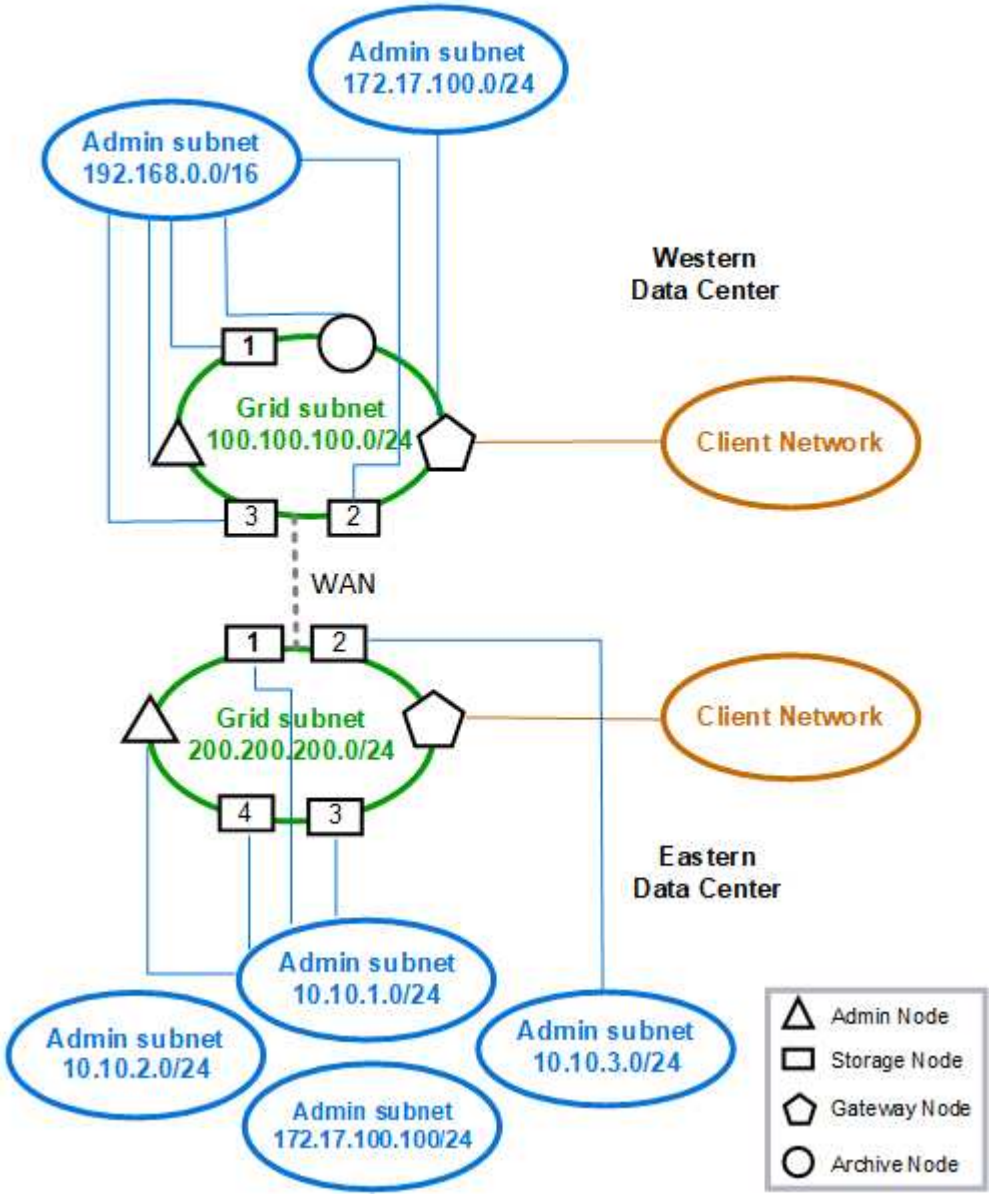
您可以将所有这三个网络配置为一个网络拓扑，其中包括专用网格网络，特定于特定于站点的受限制管理网络和开放式客户端网络。如果需要，使用负载平衡器端点和不可信的客

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eithersupport.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。
- 来自云镜像复制等StorageGRID 平台服务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、您还可以使用恢复和维护说明中所述的更改IP工具在安装完成后配置这些网络。

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。请参见有关管理StorageGRID 的说明中有关高可用性组的信息。

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。

相关信息

"网格入门"

"管理 StorageGRID"

"保持并恢复()"

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。

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。请参见有关管理StorageGRID 的说明中有关管理负载平衡和管理不可信客户端网络的信息。

相关信息

"管理 StorageGRID"

部署特定的网络注意事项

根据您使用的部署平台、您可能还需要考虑StorageGRID 网络设计的其他注意事项。

网格节点可部署为：

- 在VMware vSphere Web Client中部署为虚拟机的基于软件的网格节点
- 基于软件的网格节点、部署在Linux主机上的Docker容器中
- 基于设备的节点

有关网格节点的追加信息 、请参见_Grid primer_。

相关信息

"网格入门"

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Docker容器运行。StorageGRID 系统不需要配置与Docker相关的网络。

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Red Hat Enterprise Linux/CentOS或Ubuntu或Debian部署的安装说明。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

适用于**Docker**部署的主机网络配置

在Docker容器平台上开始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。

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、请参见适用于Linux平台的安装说明中有关配置主机网络的信息。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 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。在此示例中、可以使用不可信客户端网络功能限制入站连接。

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。

默认情况下，平台服务和云存储池通信使用以下端口：

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

创建或编辑端点时，可以指定其他端口。

如果您使用的是非透明代理服务器、则还必须配置代理设置、以允许将消息发送到外部端点、例如Internet上的端点。请参见管理StorageGRID 以了解如何配置代理设置。

有关不可信客户端网络的详细信息、请参见有关管理StorageGRID 的说明。有关平台服务的详细信息、请参见有关使用租户帐户的说明。有关云存储池的详细信息、请参见有关通过信息生命周期管理来管理对象的说明。

相关信息

"网络端口参考"

"网格入门"

"管理 StorageGRID"

"使用租户帐户"

"使用 ILM 管理对象"

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。

相关信息

"SG100和AMP；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、即 `configure-storagegrid.py` Python脚本或安装API、用于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。请参见恢复和维护说明中有关网络维护过程的信息。

相关信息

"保持并恢复()"

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。请参见恢复和维护说明中有关配置IP地址的信息。
- 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。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

"保持并恢复()"

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。

使用为内部网格节点通信和外部通信提供的详细信息来确定如何配置每个所需端口。

- "内部网格节点通信"
- "外部通信"

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 。只有在配置了高可用性(HA)组时、才需要VRRP。

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、请参见适用于Linux平台的安装说明。

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VMware的安装说明。

设备存储节点准则

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、请参见存储设备的安装说明。

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。
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"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

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。

如果企业网络策略限制对任何端口的访问、则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。不可信客户端网络功能只能用于允许对负载平衡器端点端口进行访问。

> 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、不应重新映射平衡器端点。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。

下表显示了用于向节点进行流量的端口。

> 此列表不包含可能配置为负载平衡器端点的端口。有关详细信息、请参见有关配置负载平衡器端点的说明。

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。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
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 。
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。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
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。
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。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
443.	TCP	HTTPS	归档节点	Amazon S3	用于从归档节点访问 Amazon S3 。
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	连接到网关节点(HTTPS)的S3相关外部流量。
8083.	TCP	HTTPS	Swift 客户端	网关节点	与Swift相关的外部流量传输到网关节点(HTTPS)。
8084	TCP	HTTP	S3 客户端	网关节点	连接到网关节点(HTTP)的S3相关外部流量。
8085	TCP	HTTP	Swift 客户端	网关节点	与Swift相关的外部流量传输到网关节点(HTTP)。
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。
18082	TCP	HTTPS	S3 客户端	存储节点	与S3相关的到存储节点的外部流量(HTTPS)。

Port	TCP 或 UDP	协议	from	收件人：	详细信息
18083.	TCP	HTTPS	Swift 客户端	存储节点	与Swift相关的存储节点外部流量(HTTPS)。
18084	TCP	HTTP	S3 客户端	存储节点	与S3相关的存储节点外部流量(HTTP)。
18085	TCP	HTTP	Swift 客户端	存储节点	与Swift相关的存储节点外部流量(HTTP)。

相关信息

"内部网格节点通信"

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

版权信息

版权所有 © 2025 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。