



开始使用 StorageGRID software

NetApp
July 23, 2026

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

目录

开始使用 StorageGRID 系统	1
了解 StorageGRID	1
什么是 StorageGRID?	1
使用 StorageGRID 的混合云	2
StorageGRID 架构和网络拓扑	3
网络节点和服务	7
StorageGRID 管理数据的方式	17
浏览 StorageGRID	29
网络连接准则	36
StorageGRID 网络准则	36
StorageGRID 网络类型	37
网络拓扑示例	41
StorageGRID 的网络要求	47
StorageGRID 的网络特定要求	49
特定于部署的网络注意事项	50
StorageGRID 的网络安装和配置	53
StorageGRID 安装后指南	54
网络端口参考	54
StorageGRID 快速入门	61

开始使用 StorageGRID 系统

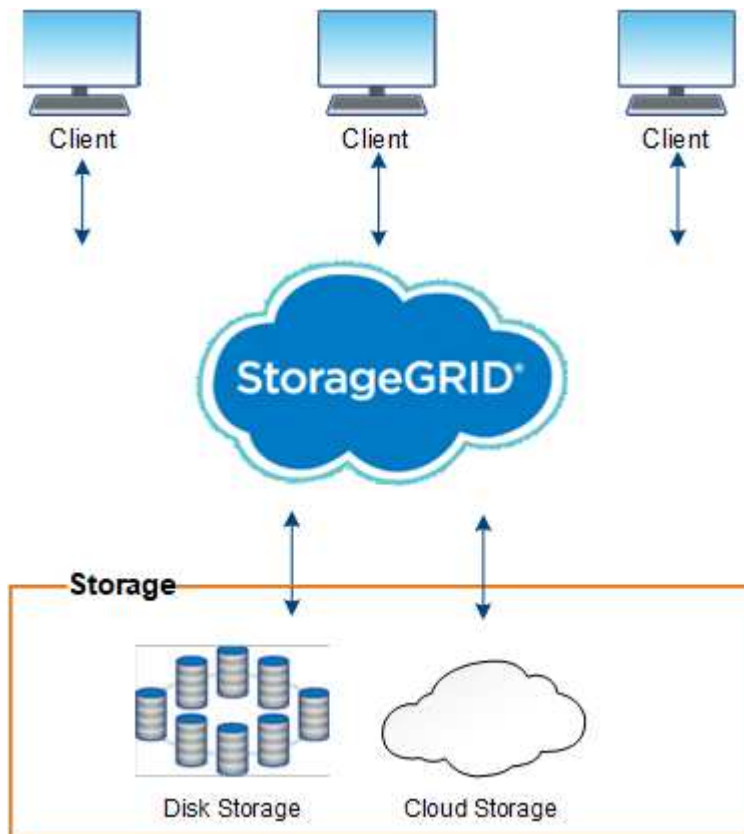
了解 StorageGRID

什么是 StorageGRID?

NetApp® StorageGRID® 是一个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，例如自动化生命周期管理，以经济高效地长期存储、保护和保存非结构化数据。

StorageGRID 为大规模非结构化数据提供安全、持久的存储。集成的元数据驱动生命周期管理策略可优化数据在其整个生命周期中的位置。内容在适当的时间放置在适当的位置和适当的存储层，以降低成本。

StorageGRID 由地理位置分散的冗余异构节点组成，可与现有和下一代客户端应用程序集成。



已删除对存档节点的支持。通过 S3 API 将对象从存档节点移动到外部存档存储系统的功能已被 "ILM Cloud Storage Pools" 取代，后者提供了更多功能。

StorageGRID 的优势

StorageGRID 系统的优点包括以下几点：

- 可大规模扩展且易于使用的地理分布式非结构化数据存储库。
- Amazon Web Services Simple Storage Service (S3) 标准对象存储协议。

- 已启用混合云。基于策略的信息生命周期管理 (ILM) 将对象存储到公共云，包括 Amazon Web Services (AWS) 和 Microsoft Azure。StorageGRID 平台服务支持存储到公共云的对象的内容复制、事件通知和元数据搜索。
- 灵活的数据保护，确保持久性和可用性。可以使用复制和分层纠删码来保护数据。静态和传输中数据验证可确保长期保留的完整性。
- 动态数据生命周期管理，帮助管理存储成本。您可以创建 ILM 规则，在对象级别管理数据生命周期，自定义数据本地性、持久性、性能、成本和保留时间。
- 数据存储和某些管理功能的高可用性，集成负载均衡，以优化 StorageGRID 资源的数据负载。
- 支持多个存储租户帐户，以按不同实体隔离存储在系统上的对象。
- 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、图形仪表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 工程设计的设备。
 - 存储设备提供对象存储。
 - 服务设备提供网络管理和负载均衡服务。
- 符合本规定的相关存储要求：
 - 美国证券交易委员会 (SEC) 在 17 CFR § 240.17a-4(f) 中，监管交易所成员、经纪人或交易商。
 - 金融业监管局 (FINRA) 规则 4511(c)，该规则遵循 SEC 规则 17a-4(f) 的格式和媒体要求。
 - 商品期货交易委员会 (CFTC) 在条例 17 CFR § 1.31(c)-(d) 中，规范商品期货交易。
- 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)，以在 StorageGRID 和 Active Directory Federation Services (AD FS) 之间交换身份验证和授权数据。

使用 StorageGRID 的混合云

通过实施策略驱动的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 将数据从 ONTAP 分层到 StorageGRID，从而在混合云配置中使用 StorageGRID。

云存储池

云存储池允许您将对象存储在 StorageGRID 系统之外。例如，您可能希望将不经常访问的对象移动到成本较低的云存储，例如 Amazon S3 Glacier、S3 Glacier Deep Archive、Google Cloud 或 Microsoft Azure Blob 存储中的存档访问层。或者，您可能需要维护 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。

还支持第三方合作伙伴存储，包括磁盘和磁带存储。



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。

S3 平台服务

S3 平台服务使您能够将远程服务用作对象复制、事件通知或搜索集成的端点。平台服务独立于网络的 ILM 规则运行，并针对单个 S3 存储桶启用。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 存储桶，该存储桶可以位于 Amazon S3 或第二个 StorageGRID 系统上。
- 事件通知服务向支持接收 Simple Notification Service (Amazon SNS) 事件的外部终结点发送有关指定操作的消息。
- 搜索集成服务将对象元数据发送到外部 Elasticsearch 服务，允许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 服务对您的数据执行分析。

ONTAP 数据分层使用 FabricPool

您可以使用 FabricPool 将数据分层到 StorageGRID，从而降低 ONTAP 存储的成本。FabricPool 可将数据自动分层到低成本对象存储层，无论是在内部还是外部。

与手动分层解决方案不同，FabricPool 通过自动执行数据分层来降低总拥有成本，从而降低存储成本。它通过分层到公共云和私有云（包括 StorageGRID）来实现云经济效益。

相关信息

- ["什么是云存储池？"](#)
- ["管理平台服务"](#)
- ["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的多种类型的网格节点组成。

了解 ["网格节点类型"](#)。

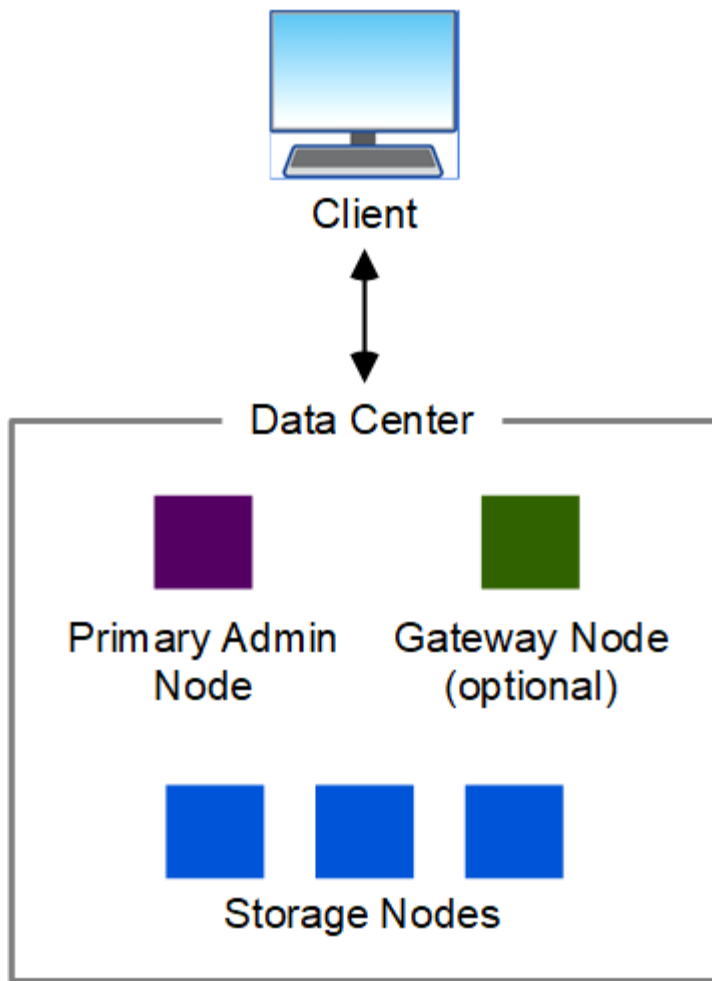
有关 StorageGRID 网络拓扑、要求和网格通信的其他信息，请参见 ["网络连接准则"](#)。

部署拓扑

StorageGRID 系统可以部署到单个数据中心站点或多个数据中心站点。每个部署的站点数上限为 16 个。

单个站点

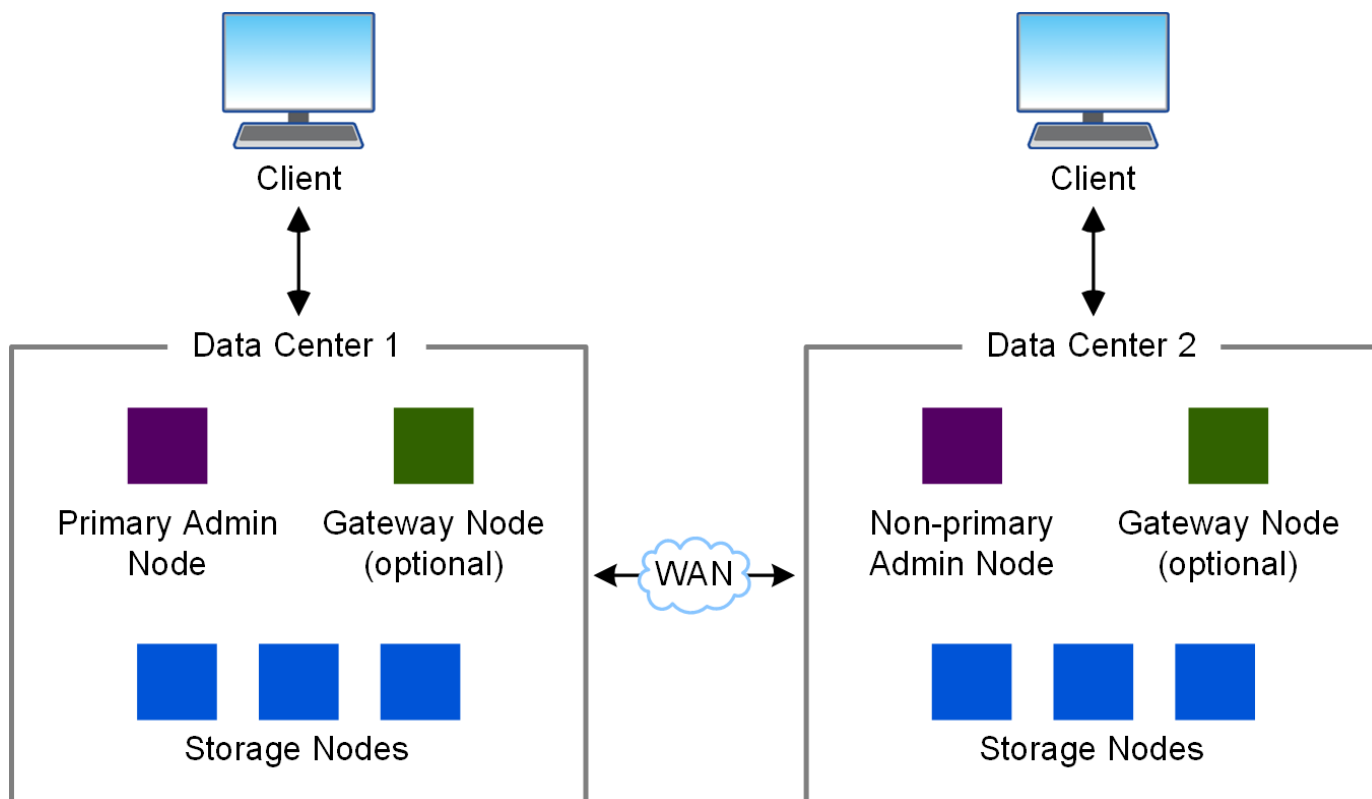
在具有单个站点的部署中，StorageGRID 系统的基础设施和操作是集中管理的。



多个站点

在具有多个站点的部署中，每个站点可以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空间。

站点通常位于不同故障区域的不同地理位置，例如地震断层线或泛滥平原。通过自动将数据分发到其他站点来实现数据共享和灾难恢复。



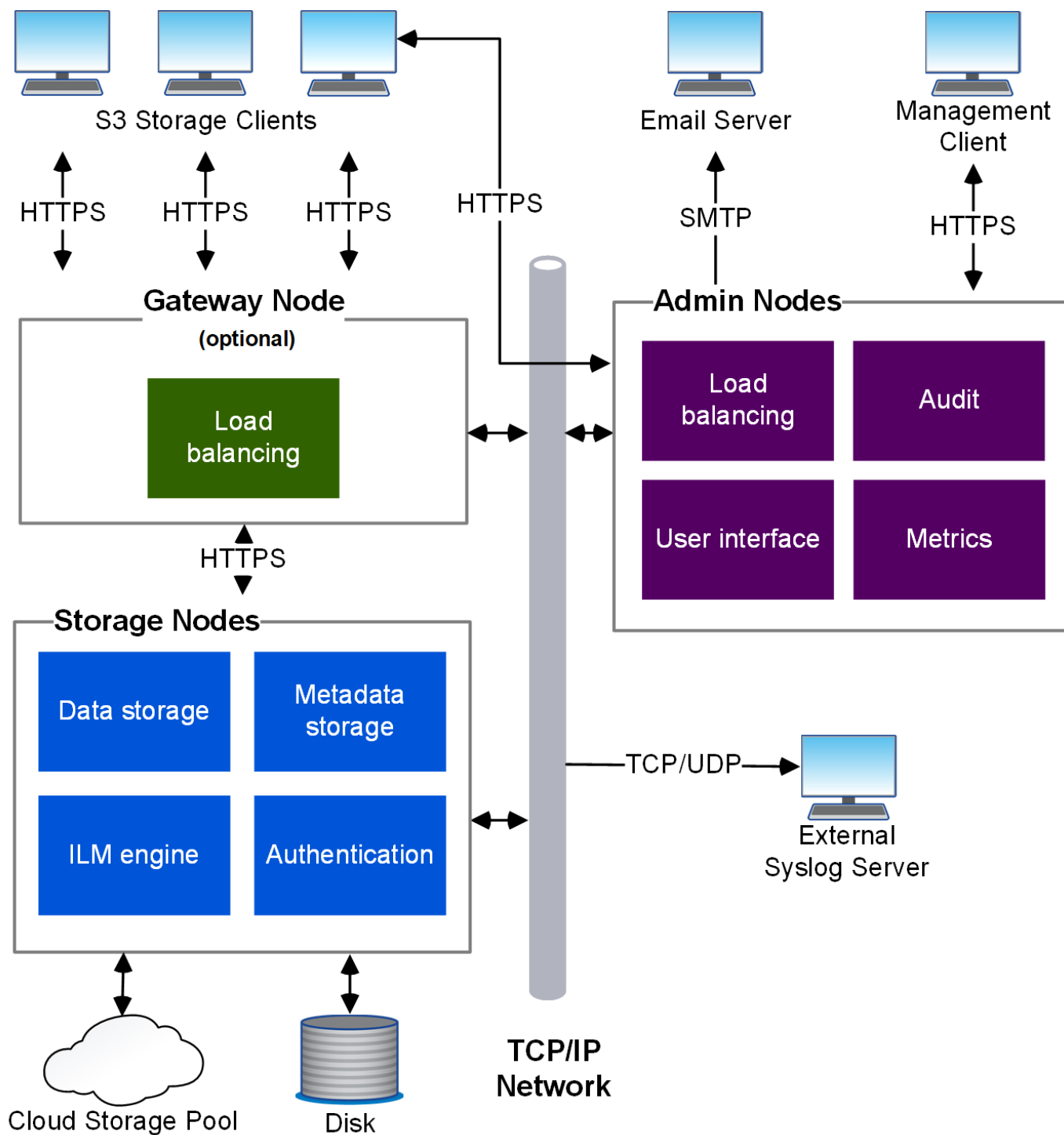
单个数据中心内还可以存在多个逻辑站点，以便使用分布式复制和纠删码来提高可用性和弹性。

网格节点冗余

在单站点或多站点部署中，您可以选择包括多个管理节点或网关节点以实现冗余。例如，您可以在单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 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 管理界面以及可选地访问审核共享。

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

对象可以存储在 StorageGRID 基于软件或硬件的存储节点上，也可以存储在云存储池中，云存储池由外部 S3 存储桶或 Azure Blob 存储容器组成。

网格节点和服务

StorageGRID 网格节点和服务

StorageGRID 系统的基本构建块是网格节点。节点包含服务，这些服务是向网格节点提供一组功能的软件模块。

网格节点的类型

StorageGRID 系统使用三种类型的网格节点：

管理节点

提供系统配置、监控、日志记录等管理服务。登录到网格管理器时，您正在连接到管理节点。每个网格必须有一个主管理节点，并且可能有其他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 StorageGRID 系统的类似视图。但是，维护程序必须使用主管理节点执行。

管理节点也可用于负载均衡 S3 客户端流量。

请参阅 ["什么是管理节点？"](#)

存储节点

管理和存储对象数据和元数据。StorageGRID 系统中的每个站点必须至少有三个存储节点。

在新存储节点的初始安装过程中，您可以指定它仅用于 ["存储元数据"](#)。

请参阅 ["什么是存储节点？"](#)

网关节点（可选）

提供客户端应用程序可用于连接到 StorageGRID 的负载均衡接口。负载均衡器可将客户端无缝定向到最佳存储节点，因此节点甚至整个站点的故障对客户端而言都是透明的。

请参阅 ["什么是网关节点？"](#)

硬件和软件节点

StorageGRID 节点可以部署为 StorageGRID 设备节点或基于软件的节点。每个系统的最大节点数（包括所有节点类型）为 220 个。

StorageGRID 设备节点

StorageGRID 硬件设备专为用于 StorageGRID 系统而设计。有些设备可以用作存储节点。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相结合，或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。

请参见以下内容，了解可用设备：

- ["StorageGRID 设备文档"](#)
- ["NetApp Hardware Universe"](#)

基于软件的节点

基于软件的网格节点可以部署为 VMware 虚拟机或 Linux 主机上容器引擎内的节点。请参阅 ["在基于软件的节点上安装 StorageGRID"](#)。

使用 ["NetApp 互操作性矩阵工具 \(IMT\)"](#) 确定支持的版本。

StorageGRID 服务

以下是 StorageGRID 服务的完整列表。

服务	问题描述	位置
帐户服务转发器	为负载均衡器服务提供接口，以查询远程主机上的帐户服务，并向负载均衡器服务提供负载均衡器端点配置更改的通知。	管理节点和网关节点上的负载均衡器服务
ADC（管理域控制器）	维护拓扑信息，提供身份验证服务，并响应来自 LDR 和 CMN 服务的查询。	每个站点至少有三个包含 ADC 服务的存储节点
AMS（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
Apache Tomcat	用于基于 Java 的应用程序的 Web 服务器。	管理节点
Avahi Daemon	处理 mDNS，用于在本地网络中进行名称解析和服务发现。	所有节点
缓存服务	在负载均衡器（网关）节点上运行，并管理对象内容的本地缓存。	网关节点
Cassandra	管理对象元数据的分布式数据库。	存储节点（仅数据节点除外）
Cassandra Reaper	执行对象元数据的自动修复。	存储节点
区块服务	管理擦除编码数据和奇偶校验片段。	存储节点
CMN（配置管理节点）	管理系统范围的配置和网格任务。每个网格有一个 CMN 服务。	主管理节点
DDS（分布式数据存储）	与 Cassandra 数据库交互，以管理对象元数据。	存储节点
DMV (Data Mover)	将数据移动到云端点。	存储节点
动态IP (dynip)	监控网格中的动态 IP 更改并更新本地配置。	所有节点

服务	问题描述	位置
Grafana	用于网格管理器中的指标可视化。	管理节点
高可用性	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。此服务也称为 keepalived 服务。	管理和网关节点
身份 (idnt)	管理本地用户和组、身份验证，并从 LDAP 和 Active Directory 联合用户标识。	使用 ADC 服务的存储节点
Lambda Arbitrator	管理 S3 Select SelectObjectContent 请求。	所有节点
负载均衡器(nginx-gw)	提供从客户端到 Storage Nodes 的 S3 流量的负载均衡。可以通过负载均衡器端点配置页面配置负载均衡器服务。此服务也称为 nginx-gw 服务。	管理和网关节点
LDR (本地分发路由器)	管理网格内内容的存储和传输。	存储节点
MISCd 信息服务控制守护进程	提供了一个接口，用于查询和管理其他节点上的服务，以及管理节点上的环境配置，例如查询其他节点上运行的服务的状态。	所有节点
nginx	充当各种网格服务（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
nginx-gw 负载均衡器	提供从客户端到 Storage Nodes 的 S3 流量的负载均衡。可以通过负载均衡器端点配置页面配置负载均衡器服务。此服务也称为 nginx-gw 服务。	管理和网关节点
NMS (网络管理系统)	为通过 Grid Manager 显示的监控、报告和配置选项提供支持。	管理节点
Node Exporter (Prometheus 数据收集)	发布 Prometheus 时间序列指标收集的系統级统计信息。	所有节点
NTP	网络时间协议(NTP)服务。	所有节点
持久性	管理根磁盘上需要在重启后持久保存的文件。	所有节点
Prometheus	从所有节点上的服务收集时间序列指标。	管理节点
RSM (复制状态机)	确保将平台服务请求发送到各自的端点。	使用 ADC 服务的存储节点

服务	问题描述	位置
SSM (Server Status Monitor)	监控硬件状况并向 NMS 服务报告。	每个网格节点上都有一个实例
服务器管理器	管理 StorageGRID 服务。	所有节点
SNMP代理	响应 SNMP 请求。	管理节点
SNMP 端口管理服务	处理 SNMP 端口的动态管理。	所有节点
SSH (安全外壳)	处理安全访问和远程系统管理。	所有节点
SSM (系统状态监视器)	监控硬件状况并向 NMS 服务报告。	所有节点
统计	记录与 S3 存储桶相关的其他指标。	存储节点
Trace Agent (jaeger-agent)	接收并处理由跟踪收集器 (jaeger-collector) 提交的跟踪信息。	所有节点
Trace Collector (jaeger-collector)	执行跟踪收集以收集供技术支持使用的信息。跟踪收集器服务使用开源 Jaeger 软件。	管理节点

什么是 **StorageGRID** 管理节点？

管理节点提供系统配置、监控和日志记录等管理服务。管理节点也可用于负载平衡 S3 客户端流量。每个网格必须有一个主管理节点，并且可以具有任意数量的非主管理节点以实现冗余。

主管理节点和非主管理节点之间的差异

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 StorageGRID 系统的类似视图。但是，主管理节点比非主管理节点提供更多功能。例如，大多数维护程序必须从主管理节点执行。

下表总结了主管理节点和非主管理节点的功能。

功能	主管理节点	非主管理节点
包括 AMS 服务	是	是
包括 CMN 服务	是	否
包括 NMS 服务	是	是
包括 Prometheus 服务	是	是

功能	主管理节点	非主管理节点
包括 SSM 服务	是	是
包括 负载均衡器 和 高可用性 服务	是	是
支持 管理应用程序接口 (mgmt-api)	是	是
可用于所有与网络相关的维护任务，例如 IP 地址更改和更新 NTP 服务器	是	否
可以下载恢复包	是	是
可以在存储节点扩展后执行EC再平衡	是	否
可用于卷恢复程序	是	是
可以从一个或多个节点收集日志文件和系统数据	是	是
可以恢复存储、网关和非主管理节点	是	是
可以恢复主管理节点	是	否
发送警报通知、AutoSupport 包和 SNMP 陷阱并通知	是的。充当 首选发件人 。	是。充当备用发送方。

首选发件人管理节点

如果您的 StorageGRID 部署包括多个管理节点，则主管理节点是警报通知、AutoSupport 包和 SNMP 陷阱和通知的首选发件人。

在正常系统操作下，只有首选发件人才会发送通知。但是，所有其他管理节点都会监视首选发件人。如果检测到问题，其他管理节点将充当备用发件人。

在以下情况下，系统可能会发送多条通知：

- 如果管理节点彼此"孤立"，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。
- 如果备用发件人检测到首选发件人的问题并开始发送通知，则首选发件人可能会重新获得发送通知的能力。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。



当您测试 AutoSupport 包时，所有管理节点都会发送测试。当您测试警报通知时，您必须登录到每个管理节点以验证连接。

管理节点的主要服务

下表显示了管理节点的主要服务；但是，此表未列出所有节点服务。

服务	关键功能
审核管理系统(AMS)	跟踪系统活动和事件。
配置管理节点(CMN)	管理全系统配置。
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。
负载均衡器	提供从客户端到存储节点的 S3 流量的负载均衡。 注： 此服务也可在网关节点上找到。
管理应用程序接口（mgmt-api）	处理来自 Grid Management API 和 Tenant Management API 的请求。
网络管理系统(NMS)	为 Grid Manager 提供功能。
Prometheus	从所有节点上的服务收集和存储时间序列指标。
服务器状态监视器 (SSM)	监控操作系统和底层硬件。

什么是 **StorageGRID** 存储节点？

存储节点管理和存储对象数据和元数据。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流程。

StorageGRID 系统中的每个站点必须至少有三个存储节点。

存储节点类型

安装过程中，可以选择要安装的存储节点类型。这些类型适用于基于软件的存储节点和支持该功能的基于设备的存储节点：

- 组合数据和元数据存储节点
- 仅元数据存储节点
- 仅数据存储节点

您可以在以下情况下选择存储节点类型：

- 初次安装存储节点时
- 在 StorageGRID 系统扩展期间添加存储节点时

数据和元数据存储节点（组合）

默认情况下，所有新的存储节点将同时存储对象数据和元数据。这种类型的存储节点称为 `_combined_` 存储节点。

仅元数据存储节点

如果您的网格存储了大量小型对象，则仅将存储节点用于元数据是有意义的。安装专用元数据容量可以更好地平衡大量小型对象所需的空间和这些对象的元数据所需的空间。此外，托管在高性能设备上的仅元数据存储节点可以提高性能。

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- 使用基于软件的节点时，仅元数据的节点资源必须与现有的存储节点资源匹配。例如：
 - `${post_edited_translations.segment}`
 - 128 GB 内存
 - `${post_edited_translations.segment}`
 - `${post_edited_translations.segment}`
 - 如果现有的 StorageGRID 站点使用具有 24 GB RAM、8 核 CPU 和 3 TB 或 4 TB 元数据存储的虚拟存储节点，则基于软件的仅元数据节点应使用类似的资源（24 GB RAM、8 核 CPU 和 4 TB 元数据存储（`rangedb/0`））。
- 添加新的 StorageGRID 站点时，新站点的总元数据容量应至少与现有站点匹配。新站点的资源应与现有站点的存储节点匹配。



虽然仅元数据存储节点包含 [LDR 服务](#) 并且可以处理 S3 客户端请求，但 StorageGRID 性能可能不会提高。

仅数据存储节点

如果您的存储节点具有不同的性能特征，则将存储节点专用于数据是合理的。例如，为了提高性能，您可以配置仅用于数据的高容量旋转磁盘存储节点，以及仅用于元数据的高性能存储节点。

此外，您可以通过从 Cassandra 中删除低 RAM 节点来获得更多元数据容量，这会增加每个节点的元数据容量限制。请参阅 ["管理对象元数据存储"](#)。

您可以将不包含 [ADC 服务](#) 的存储节点转换为仅数据存储节点。请参阅 ["将存储节点转换为仅数据节点"](#)。

每个网格和每个站点所需的存储节点

在选择要在拓扑中使用的存储节点时，请记住，网格或网格中的每个站点必须包含以下内容：

- 每个站点（在单站点或多站点网格中）：三个 [ADC](#) 存储节点（可以是组合存储节点和仅元数据存储节点的任意组合）
- 单站点网格：至少两个对象存储节点（可以是组合节点和纯数据节点的任意组合）
- 多站点网格：每个站点至少有一个对象存储节点（可以是组合节点或仅数据节点）

存储节点的主要服务

下表显示了存储节点的主要服务；但是，此表未列出所有节点服务。



某些服务，例如 [ADC 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 (acct)	管理租户帐户。 仅数据存储节点不托管此服务。
管理域控制器 (ADC)	维护拓扑和网格范围配置。 仅数据存储节点不托管此服务。 详细信息 管理域控制器 (ADC) 服务对网格节点及其彼此连接进行身份验证。ADC 服务托管在站点上至少三个存储节点上。 ADC 服务维护拓扑信息，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需要由另一个网格节点执行某项操作时，它会联系 ADC 服务，以找到处理其请求的最佳网格节点。此外，ADC 服务保留 StorageGRID 部署的配置捆绑包的副本，允许任何网格节点检索当前配置信息。 为了促进分布式和孤岛操作，每个 ADC 服务将证书、配置捆绑包以及有关服务和拓扑的信息与 StorageGRID 系统中的其他 ADC 服务同步。 一般来说，所有网格节点都保持与至少一个 ADC 服务的连接。这可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，使系统即使在 ADC 服务不可用时也能继续使用已知的网格节点。新网格节点只能通过使用 ADC 服务建立连接。 每个网格节点的连接允许 ADC 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。其他服务通过拓扑查询向 ADC 服务请求拓扑信息。ADC 服务使用从 StorageGRID 系统接收的最新信息响应每个查询。
Cassandra	存储和保护对象元数据。 仅数据存储节点不托管此服务。
Cassandra Reaper	执行对象元数据的自动修复。 仅数据存储节点不托管此服务。
区块	管理擦除编码数据和奇偶校验片段。
数据迁移器 (dmv)	将数据移动到云存储池。

服务	关键功能
分布式数据存储 (DDS)	监控对象元数据存储。 详细信息 每个存储节点都包括分布式数据存储 (DDS) 服务。此服务与 Cassandra 数据库交互，对存储在 StorageGRID 系统中的对象元数据执行后台任务。 DDS 服务跟踪已载入 StorageGRID 系统的对象总数，以及通过系统每个受支持接口 (S3) 载入的对象总数。
身份 (idnt)	从 LDAP 和 Active Directory 联合用户身份。 仅数据存储节点不托管此服务。

服务	关键功能
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。 详细信息 每个 <i>combined</i>、<i>data-only</i> 和 <i>metadata-only</i> 存储节点都包括本地分发路由器 (LDR) 服务。本服务处理内容传输功能，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 系统的大部分工作。 LDR 服务处理以下任务： • 查询 • 信息生命周期管理(ILM)活动 • 对象删除 • 对象数据存储 • 从另一个 LDR 服务（存储节点）传输的对象数据 • 数据存储管理 • S3 协议接口 LDR 服务还会将每个 S3 对象映射到其唯一的 UUID。 对象存储 LDR 服务的底层数据存储被划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。 存储节点中的对象存储由从 0000 到 002F 的十六进制数字标识，称为卷 ID。第一个对象存储（卷 0）中的空间为 Cassandra 数据库中的对象元数据预留；该卷上的任何剩余空间都用于对象数据。所有其他对象存储仅用于对象数据，包括复制副本和纠删码片段。 为了确保复制副本的均匀空间使用，根据可用存储空间，将给定对象的对象数据存储到一个对象存储中。当对象存储达到容量上限时，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 StorageGRID 将对象元数据存储于 Cassandra 数据库中，该数据库与 LDR 服务交互。 为了确保冗余，从而防止丢失，每个站点维护三个对象元数据副本。此复制不可配置并自动执行。有关详细信息，请参见 "管理对象元数据存储"。
复制状态机(RSM)	确保 S3 平台服务请求发送到各自的端点。 仅数据存储节点不托管此服务。

服务	关键功能
服务器状态监视器(SSM)	监控操作系统和底层硬件。

什么是 **StorageGRID** 网关节点？

网关节点提供专用的负载平衡接口，S3 客户端应用程序可以使用该接口连接至 StorageGRID。负载均衡通过在多个存储节点之间分配工作负载来最大限度地提高速度和连接容量。网关节点是可选的。

StorageGRID 负载平衡器服务在所有管理节点和所有网关节点上提供。它执行客户端请求的传输层安全（TLS）终止，检查请求，并建立与存储节点的新安全连接。负载平衡器服务可将客户端无缝定向到最佳存储节点，因此节点甚至整个站点的故障对客户端而言都是透明的。

您可以配置一个或多个负载平衡器端点，以定义传入和传出客户端请求将用于访问网关和管理节点上的负载平衡器服务的端口和网络协议（HTTPS 或 HTTP）。负载平衡器端点还定义了客户端类型 (S3)、绑定模式以及可选的允许或阻止的租户列表。请参阅 ["负载均衡注意事项"](#)。

根据需要，您可以将多个网关节点和管理节点的网络接口分组到高可用性 (HA) 组中。如果 HA 组中的活动接口出现故障，备份接口可以管理客户端应用程序工作负载。请参阅 ["管理高可用性\(HA\)组"](#)。

网关节点的主要服务

下表显示了网关节点的主要服务；但是，此表未列出所有节点服务。

服务	关键功能
缓存服务	管理对象内容的本地缓存。
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。 注意： 此服务也可以在管理节点上找到。
负载平衡器	提供从客户端到存储节点的 S3 流量的第 7 层负载均衡。这是建议的负载均衡机制。 注意： 此服务也可以在管理节点上找到。
服务器状态监视器(SSM)	监控操作系统和底层硬件。

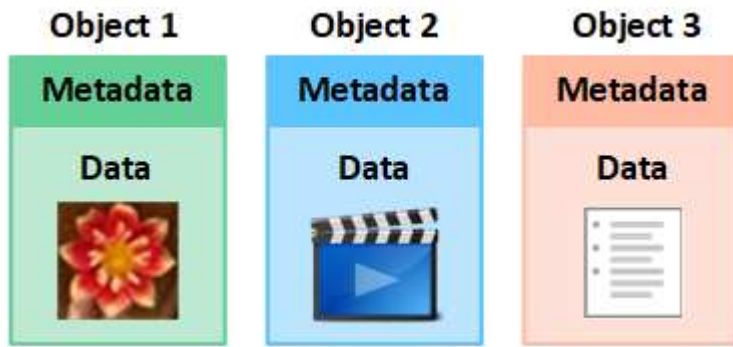
StorageGRID 管理数据的方式

什么是 **StorageGRID** 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，对象存储以平坦的非结构化布局组织数据。

对象存储将数据的物理位置与用于存储和检索该数据的方法分离。

基于对象的存储系统中的每个对象都有两个部分：对象数据和对象元数据。



什么是对象数据？

对象数据可以是任何东西，例如照片、电影或医疗记录。

什么是对象元数据？

对象元数据是描述对象的任何信息。StorageGRID 使用对象元数据来跟踪网格中所有对象的位置，并随时间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 存储桶的名称、租户帐户名称或 ID、对象的逻辑大小、对象首次创建的日期和时间以及对象上次修改的日期和时间。
- 每个对象副本或擦除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且可扩展，使应用程序能够灵活使用。

要了解 StorageGRID 存储对象元数据的方式和位置的详细信息，请转到 ["管理对象元数据存储"](#)。

如何保护对象数据？

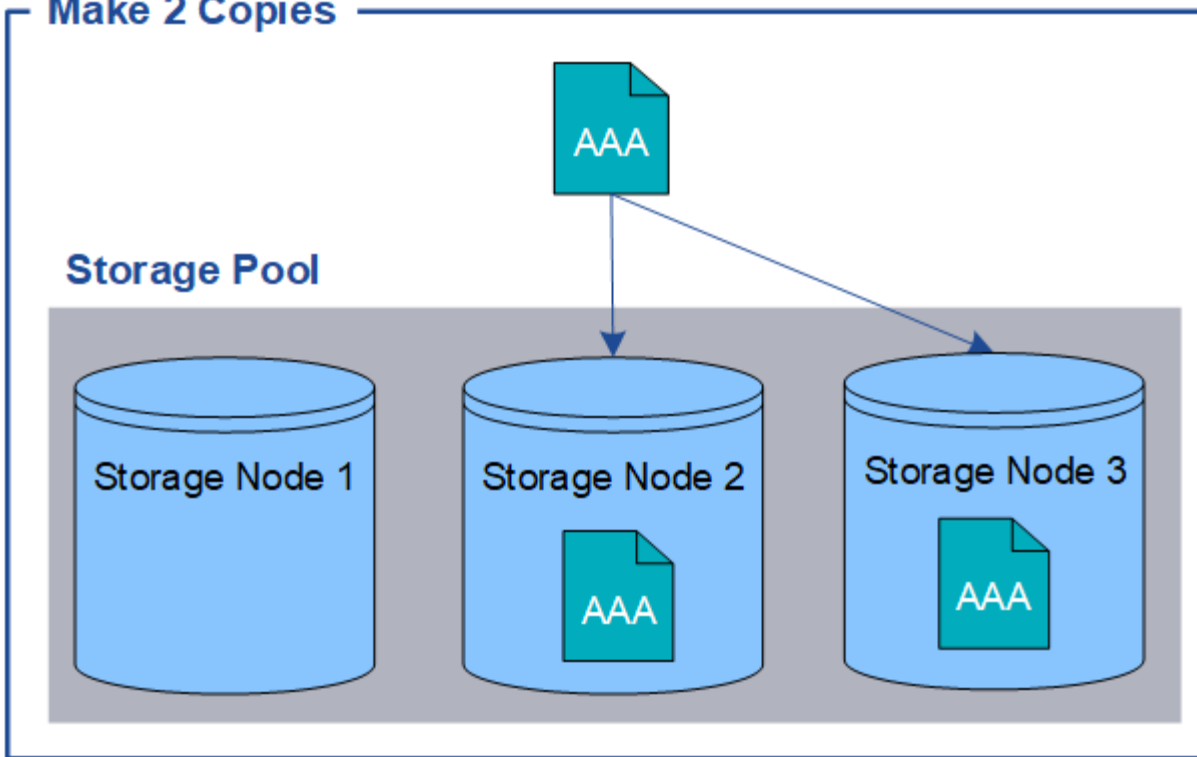
StorageGRID 系统为您提供了两种保护对象数据免受丢失的机制：复制和纠删编码。

复制

当 StorageGRID 将对象与配置为创建复制副本的信息生命周期管理 (ILM) 规则匹配时，系统会创建对象数据的精确副本，并将其存储在存储节点或云存储池中。ILM 规则规定了制作的副本数、存储这些副本的位置以及系统保留这些副本的时长。如果副本丢失（例如，由于存储节点丢失），只要该对象的副本存在于 StorageGRID 系统中的其他位置，该对象仍然可用。

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。

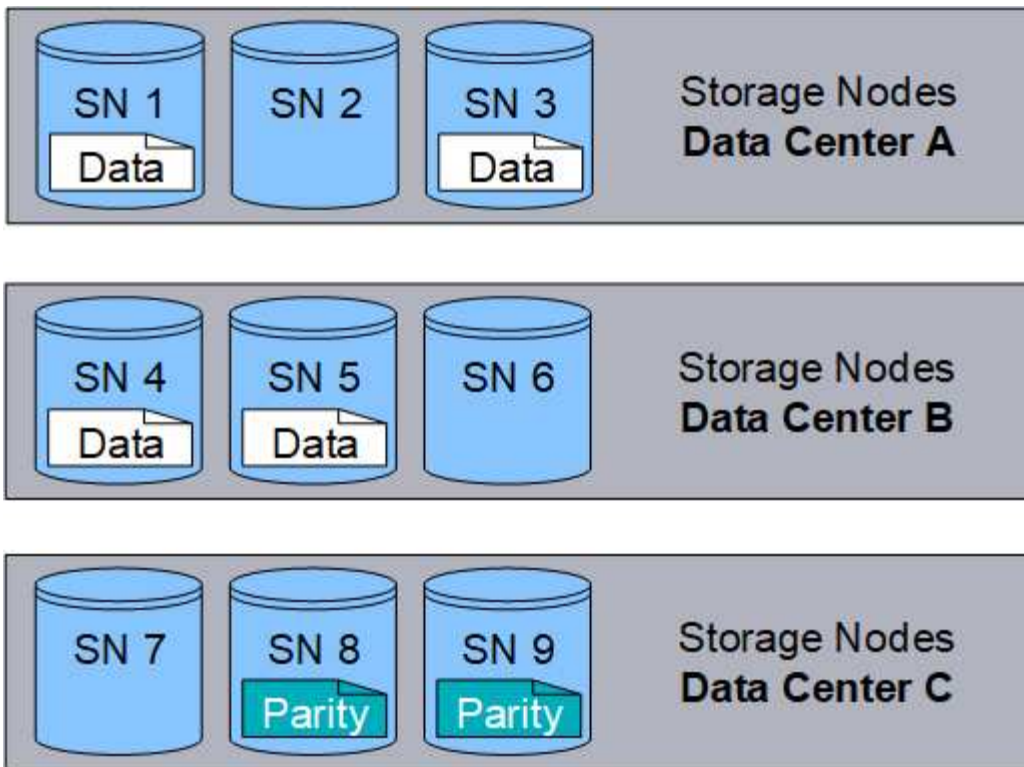
Make 2 Copies



纠删编码

当 StorageGRID 将对象与配置为创建纠删码副本的 ILM 规则匹配时，它会将对象数据切片为数据片段，计算其他奇偶校验片段，并将每个片段存储在不同的存储节点上。访问对象时，使用存储的片段重新组装对象。如果数据或奇偶校验片段损坏或丢失，纠删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 规则和纠删码配置文件决定了所使用的纠删码方案。

以下示例说明了对对象数据的纠删编码的使用。在此示例中，ILM 规则使用 4+2 纠删编码方案。每个对象被切割成四个相等的数据片段，并从对象数据中计算出两个奇偶校验片段。六个片段中的每一个都存储在三个数据中心的不同存储节点上，以提供针对节点故障或站点丢失的数据保护。



相关信息

- ["使用 ILM 管理对象"](#)
- ["使用信息生命周期管理"](#)

StorageGRID 中的对象生命周期

对象的生命周期由不同的阶段组成。每个阶段表示对象所发生的操作。

对象的生命周期包括接收、复制管理、检索和删除操作。

- **导入：** S3 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 系统开始管理对象。
- **副本管理：** 在 StorageGRID 中管理复制副本和纠删编码副本的过程，如活动 ILM 策略中的 ILM 规则所述。在副本管理阶段，StorageGRID 通过在存储节点或云存储池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免遭丢失。
- **检索：** 客户端应用程序访问 StorageGRID 系统存储的对象的过程。客户端读取对象，该对象从存储节点或 Cloud Storage Pool 中检索。
- **删除：** 从网格中删除所有对象副本的过程。对象可以因客户端应用程序向 StorageGRID 系统发送删除请求而被删除，也可以因 StorageGRID 在对象生命周期到期时执行的自动过程而被删除。



相关信息

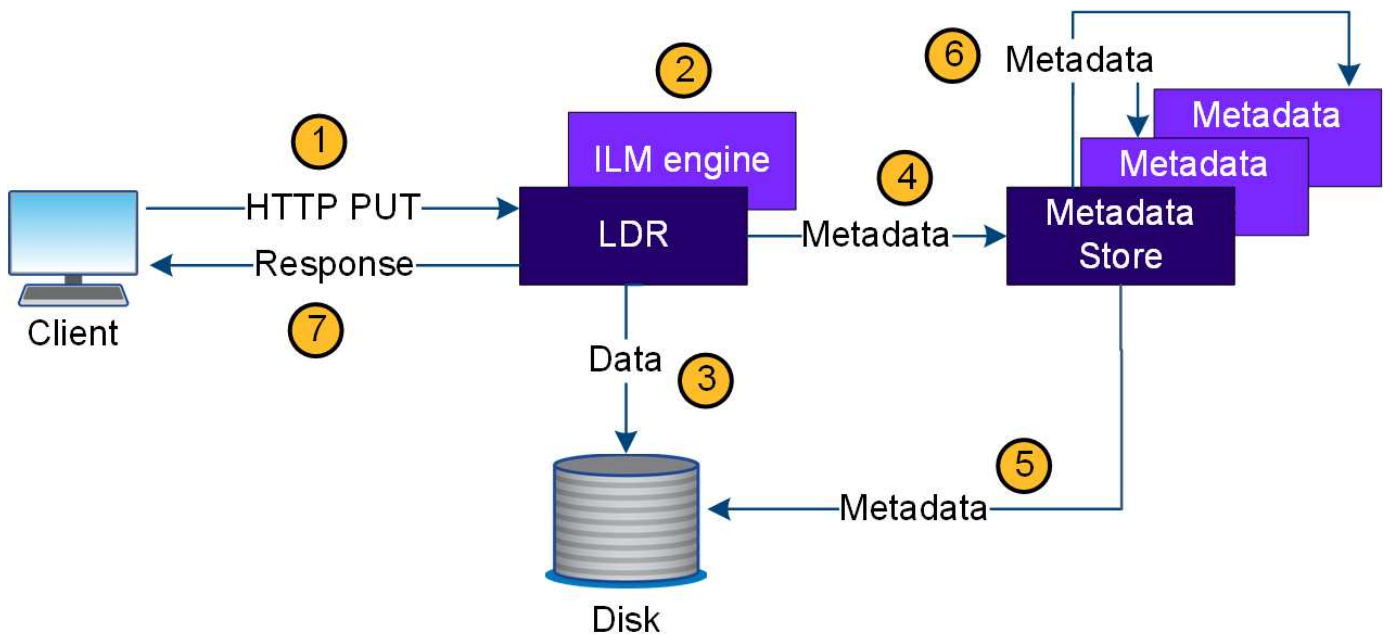
- "使用 ILM 管理对象"
- "使用信息生命周期管理"

StorageGRID 如何处理对象摄取

摄取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 服务将处理该请求并将元数据和数据存储到磁盘。



1. 客户端应用程序创建对象，并通过 HTTP PUT 请求将其发送到 StorageGRID 系统。
2. 根据系统的 ILM 策略评估该对象。
3. LDR 服务将对象数据保存为复制副本或纠删编码副本。（图表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。
7. LDR 服务向客户端返回 HTTP 200 OK 响应，确认对象已被接收。

StorageGRID 如何管理对象副本

对象数据由活动 ILM 策略和相关 ILM 规则管理。ILM 规则生成复制或纠删编码的副本，以防止对象数据丢失。

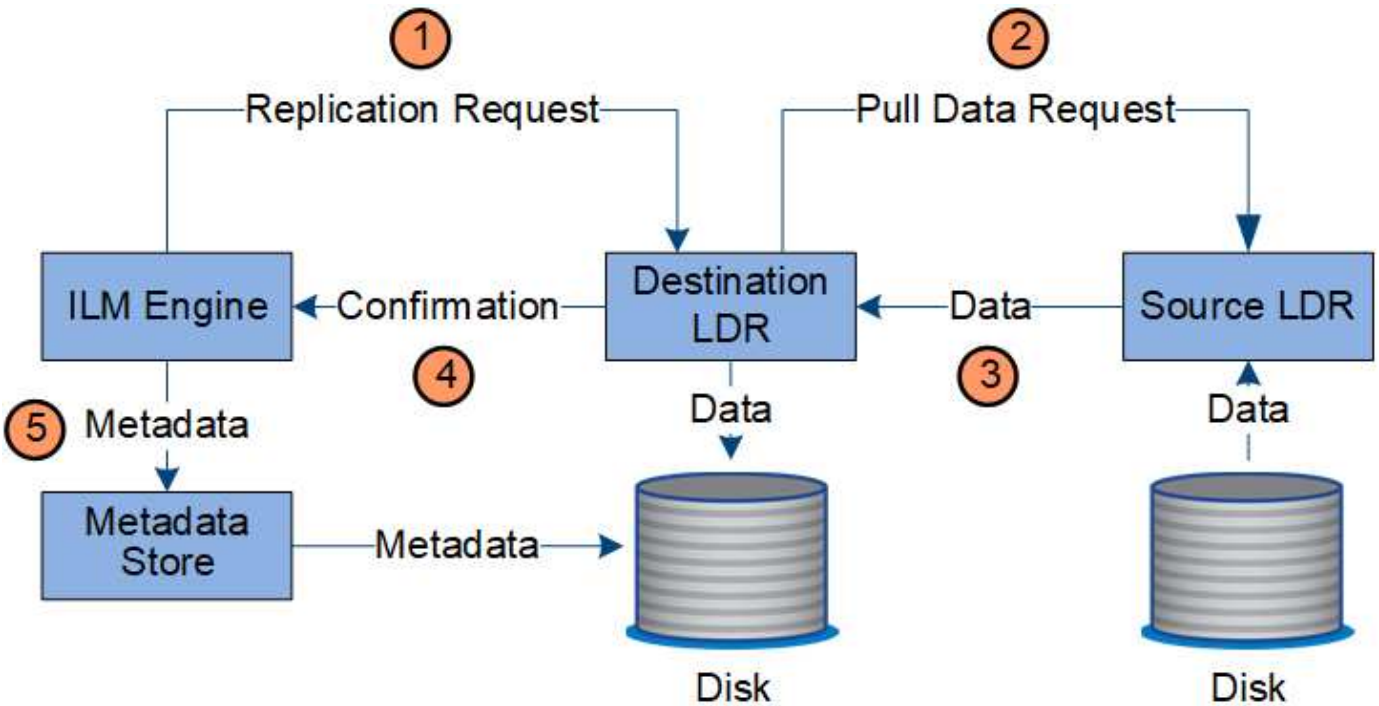
在对象生命周期的不同时间，可能需要不同类型或位置的对象副本。系统会定期评估 ILM 规则，以确保按要求放置对象。

对象数据由 LDR 服务管理。

内容保护：复制

如果 ILM 规则的内容放置指令需要对象数据的复制副本，则由构成已配置存储池的存储节点制作副本并将其存储到磁盘。

LDR服务中的ILM引擎控制复制，并确保在正确的位置和正确的时间内存储正确数量的副本。

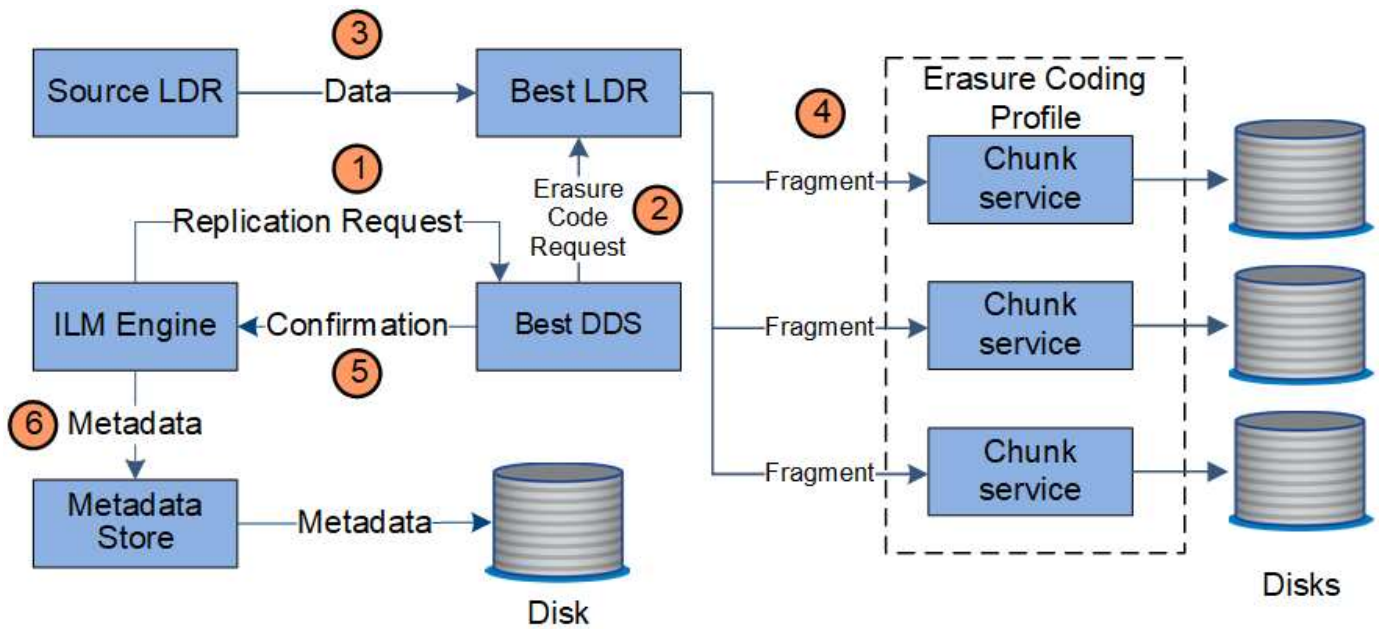


1. ILM 引擎查询 ADC 服务，以确定 ILM 规则指定的存储池中的最佳目标 LDR 服务。然后，它向该 LDR 服务发送命令以启动复制。
2. 目标 LDR 服务向 ADC 服务查询最佳源位置。然后，它向源 LDR 服务发送复制请求。
3. 源 LDR 服务将副本发送到目标 LDR 服务。
4. 目标 LDR 服务通知 ILM 引擎已存储对象数据。
5. ILM 引擎使用对象位置元数据更新元数据存储。

内容保护：纠删码

如果 ILM 规则包括制作对象数据的纠删编码副本的指令，则适用的纠删编码方案将对象数据分解为数据和奇偶校验片段，并将这些片段分布在纠删编码配置文件中配置的 Storage Nodes 上。

ILM 引擎是 LDR 服务的组成部分，它控制纠删码并确保将纠删码配置文件应用于对象数据。

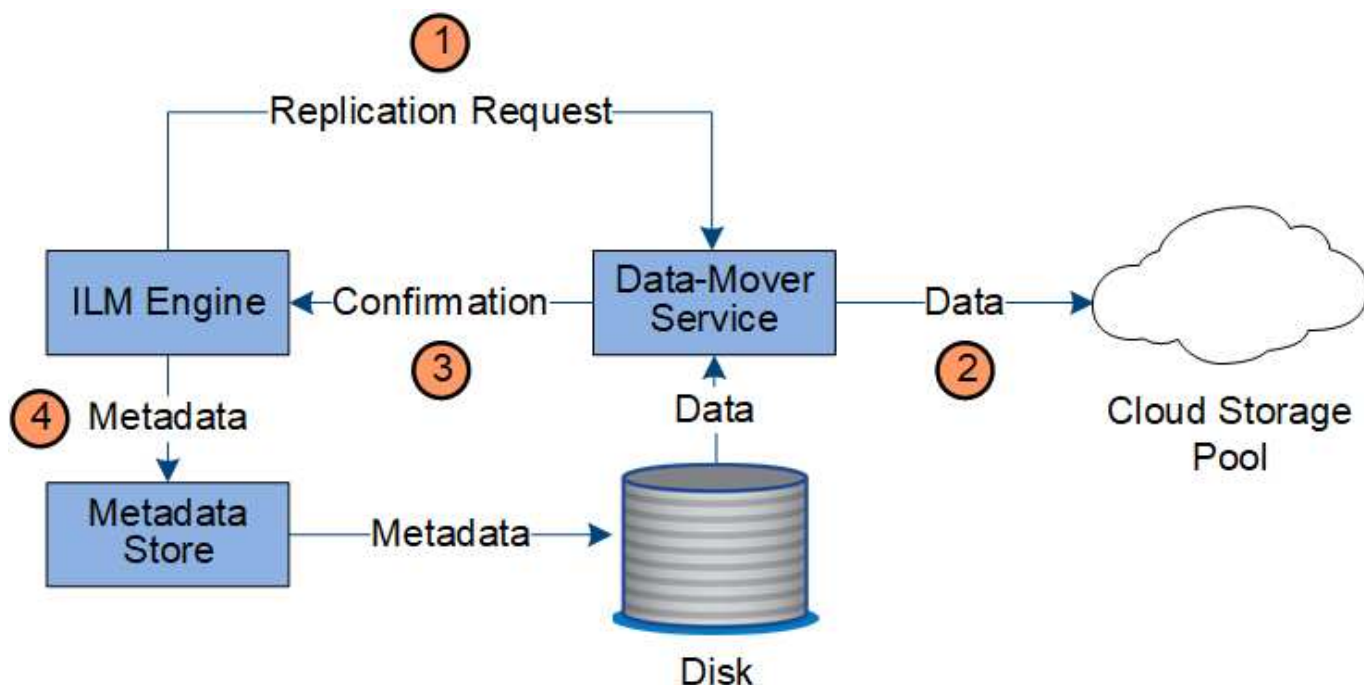


1. ILM 引擎查询 ADC 服务以确定哪个 DDS 服务可以最好地执行纠删码操作。确定后，ILM 引擎向该服务发送"启动"请求。
2. DDS 服务指示 LDR 对对象数据进行纠删码编码。
3. 源 LDR 服务将副本发送到选择用于纠删码的 LDR 服务。
4. 在创建适当数量的奇偶校验和数据片段后，LDR 服务将这些片段分布在构成纠删码配置文件存储池的存储节点（块服务）上。
5. LDR 服务通知 ILM 引擎，确认已成功分发对象数据。
6. ILM 引擎使用对象位置元数据更新元数据存储。

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云存储池指定的外部 S3 存储桶或 Azure Blob 存储容器。

作为 LDR 服务组件的 ILM 引擎和 Data Mover 服务控制对象向云存储池的移动。



1. ILM 引擎选择一个数据移动器服务以复制到云存储池。
2. Data Mover 服务将对象数据发送至云存储池。
3. Data Mover 服务通知 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。

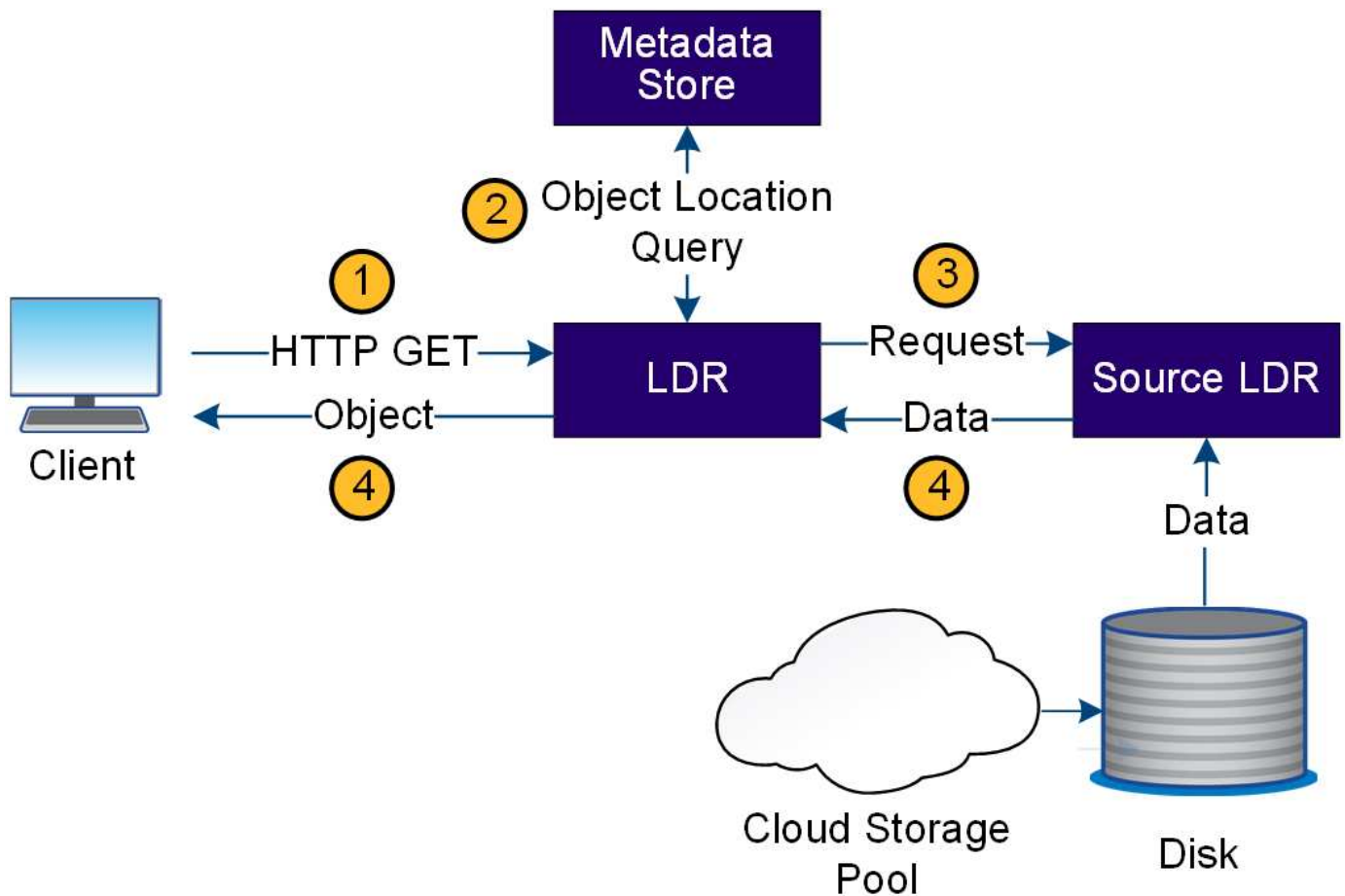
StorageGRID 如何处理对象检索

检索操作由 StorageGRID 系统和客户端之间定义的数据流组成。系统使用属性来跟踪从存储节点或必要时从云存储池检索对象的过程。

存储节点的 LDR 服务向元数据存储查询对象数据的位置，并从源 LDR 服务中检索该数据。优先从存储节点检索。如果对象在存储节点上不可用，则检索请求将定向到 Cloud Storage Pool。



如果唯一的对象副本位于 AWS Glacier 存储或 Azure 存档层，则客户端应用程序必须发出 S3 RestoreObject 请求，以将可检索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 服务向元数据存储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，系统将该对象返回到客户端应用程序。

StorageGRID 如何处理对象删除

当客户端执行删除操作或对象的生命周期到期时，所有对象副本将从 StorageGRID 系统中删除，从而触发其自动删除。对象删除有一个已定义的数据流。

删除层次结构

StorageGRID 提供了几种方法来控制何时保留或删除对象。对象可以通过客户端请求删除，也可以自动删除。StorageGRID 始终将任何 S3 对象锁定设置优先于客户端删除请求，而客户端删除请求又优先于 S3 存储桶生命周期和 ILM 放置指令。

- **S3 Object Lock:** 如果为网格启用了全局 S3 Object Lock 设置，则 S3 客户端可以创建启用了 S3 Object Lock 的存储桶，然后使用 S3 REST API 为添加到该存储桶的每个对象版本指定保留截止日期和法定保留设置。
 - 无法通过任何方法删除合法冻结的对象版本。
 - 在达到对象版本的 retain-until-date 之前，无法通过任何方法删除该版本。

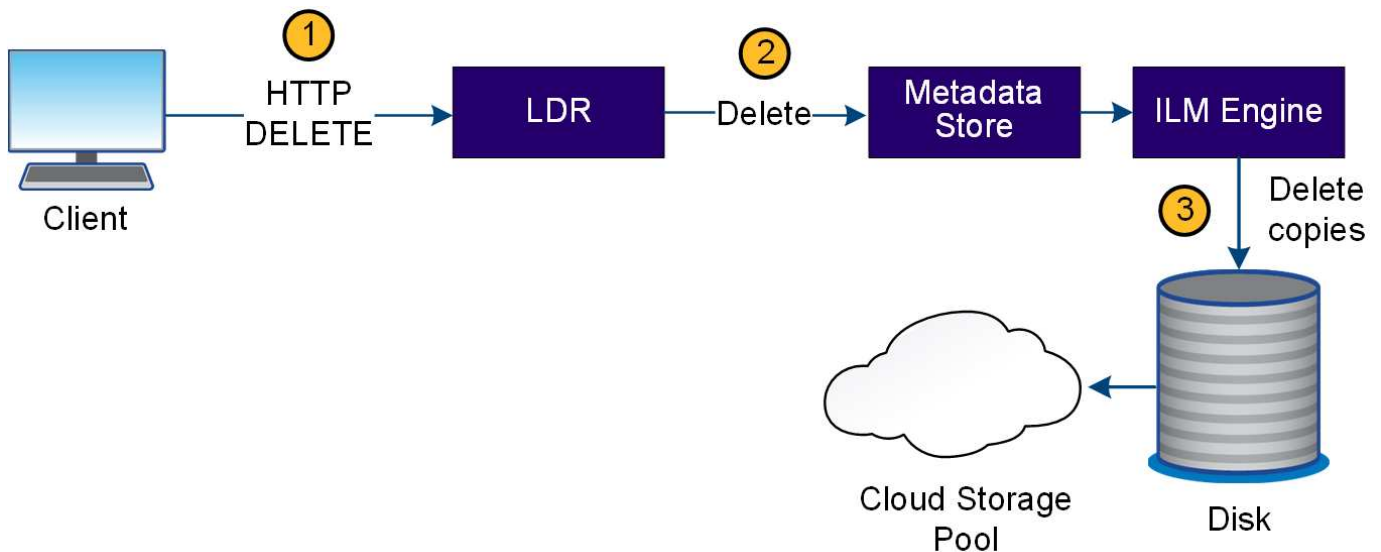
- 启用了 S3 Object Lock 的存储桶中的对象由 ILM "永久"保留。但是，在达到其 retain-until-date 后，可以通过客户端请求或存储桶生命周期到期来删除对象版本。
- 如果 S3 客户端将默认的 retain-until-date 应用于存储桶，则无需为每个对象指定 retain-until-date。
- 客户端删除请求：S3 客户端可以发出删除对象请求。当客户端删除对象时，该对象的所有副本都将从 StorageGRID 系统中删除。
- 删除存储桶中的对象：租户管理器用户可以使用此选项从 StorageGRID 系统中永久删除所选存储桶中对象和对象版本的所有副本。
- **S3 存储桶生命周期**：S3 客户端可以向其存储桶添加指定过期操作的生命周期配置。如果存在存储桶生命周期，则当满足过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**：假设存储桶未启用 S3 Object Lock，且没有存储桶生命周期，当 ILM 规则中的最后一个时间段结束且未为该对象指定进一步的放置时，StorageGRID 会自动删除该对象。



配置 S3 存储桶生命周期后，生命周期到期操作将覆盖与生命周期筛选器匹配的对象 ILM 策略。因此，即使放置对象的所有 ILM 指令均已失效，对象仍可能保留在网格中。

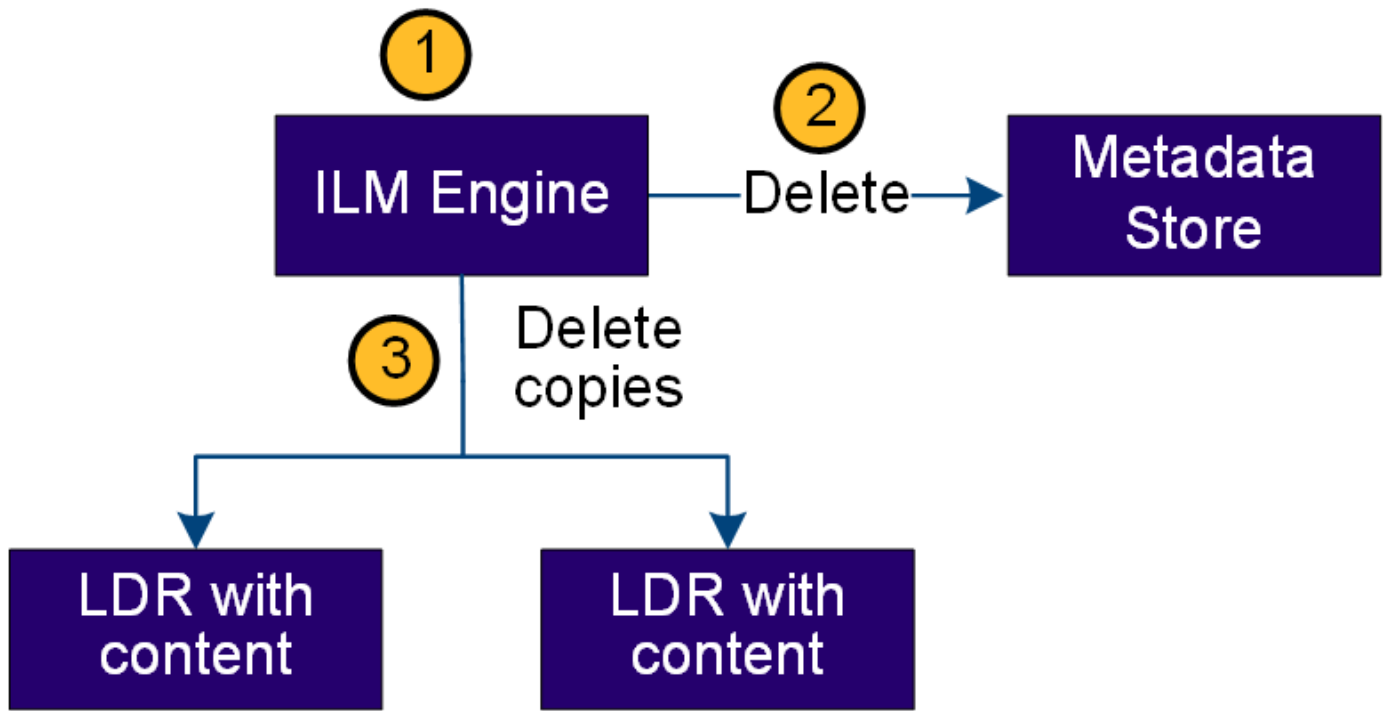
有关详细信息，请参见 ["如何删除对象"](#)。

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 服务更新元数据存储，使对象在客户端请求中显示为已删除，并指示 ILM 引擎删除对象数据的所有副本。
3. 对象已从系统中删除。已更新元数据存储以删除对象元数据。

ILM 删除的数据流



1. ILM 引擎确定需要删除该对象。
2. ILM 引擎通知元数据存储。元数据存储更新对象元数据，使对象在客户端请求中看起来已删除。
3. ILM 引擎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。

StorageGRID 中的信息生命周期管理

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、持续时间和接收行为。ILM 规则确定 StorageGRID 如何随时间推移存储对象。配置一个或多个 ILM 规则，然后将其添加到 ILM 策略中。一个网格一次可以有多个活动策略。

ILM规则定义：

- 应存储哪些对象。规则可以应用于所有对象，也可以指定筛选器以标识规则应用于哪些对象。例如，规则只能应用于与某些租户帐户、特定 S3 存储区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或云存储池中。
- 生成的对象副本的类型。副本可以是复制的，也可以是纠删编码的。
- 对于复制副本，则为已制作的副本数。
- 对于纠删编码副本，所使用的纠删编码方案。
- 随着时间的推移，对象的存储位置和副本类型会发生变化。
- 在对象被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。相反，对象元数据存储于 Cassandra 数据库中，即所谓的元数据存储。每个站点自动维护三个对象元数据副本，以防止数据丢失。

ILM 规则示例

例如，ILM 规则可以指定以下内容：

- 仅适用于属于租户 A 的对象。
- 制作这些对象的两个复制副本，并将每个副本存储在不同的站点。
- 永久保留这两个副本，这意味着 StorageGRID 不会自动删除它们。相反，StorageGRID 将保留这些对象，直到客户端发出删除请求或存储桶生命周期到期时才将其删除。
- 使用 Balanced 选项进行摄取行为：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，除非无法立即生成所需的两个副本。

例如，如果租户 A 保存对象时无法访问站点 2，StorageGRID 将在站点 1 的存储节点上生成两个临时副本。一旦站点 2 可用，StorageGRID 将在该站点制作所需的副本。

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、持续时间和接收行为。

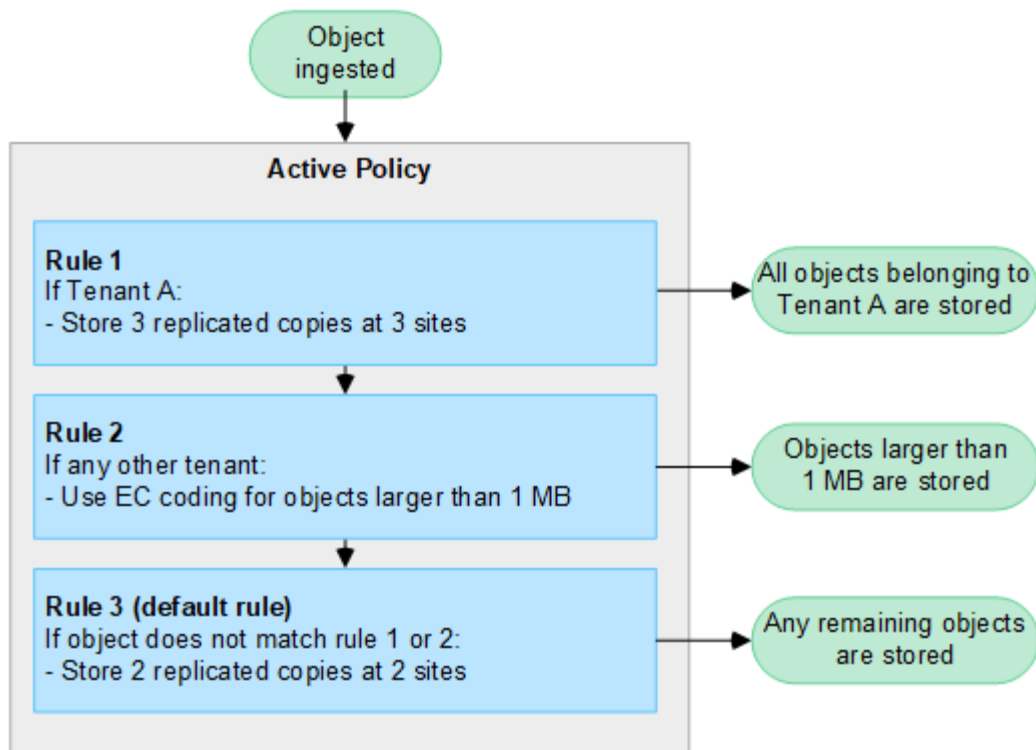
当客户端将对象保存到 StorageGRID 时，将根据活动策略中的有序 ILM 规则集对对象进行评估，如下所示：

1. 如果策略中第一个规则的筛选器与对象匹配，则根据该规则的摄取行为摄取该对象，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，则根据策略中的每个后续规则对对象进行评估，直到找到匹配项为止。
3. 如果没有与对象匹配的规则，则应用策略中默认规则的接收行为和放置说明。默认规则为策略中的最后一个规则，并且不能使用任何筛选器。它必须应用于所有租户、所有存储桶以及所有对象版本。

ILM 策略示例

例如，ILM 策略可以包含三个指定以下内容的 ILM 规则：

- 规则 1：租户 A 的复制副本
 - 匹配属于租户 A 的所有对象。
 - 将这些对象存储为三个站点的三个复制副本。
 - 属于其他租户的对象与规则 1 不匹配，因此将根据规则 2 对其进行评估。
- 规则 2：大于 1 MB 的对象的纠删码
 - 匹配来自其他租户的所有对象，但仅当它们大于 1 MB 时。这些较大的对象使用 6+3 纠删码存储在三个站点。
 - 不匹配 1 MB 或更小的对象，因此这些对象将根据规则 3 进行评估。
- 规则 3：2 个副本 2 个数据中心（默认）
 - 是策略中的最后一个默认规则。不使用过滤器。
 - 制作与规则 1 或规则 2 不匹配的所有对象的两个复制副本（不属于租户 A 且大小为 1 MB 或更小的对象）。



相关信息

- ["使用 ILM 管理对象"](#)

浏览 StorageGRID

浏览 **StorageGRID** 网络管理器

网络管理器是基于浏览器的图形界面，允许您配置、管理和监控 StorageGRID 系统。



网络管理器随每个版本更新，可能与此页面上的示例屏幕截图不匹配。

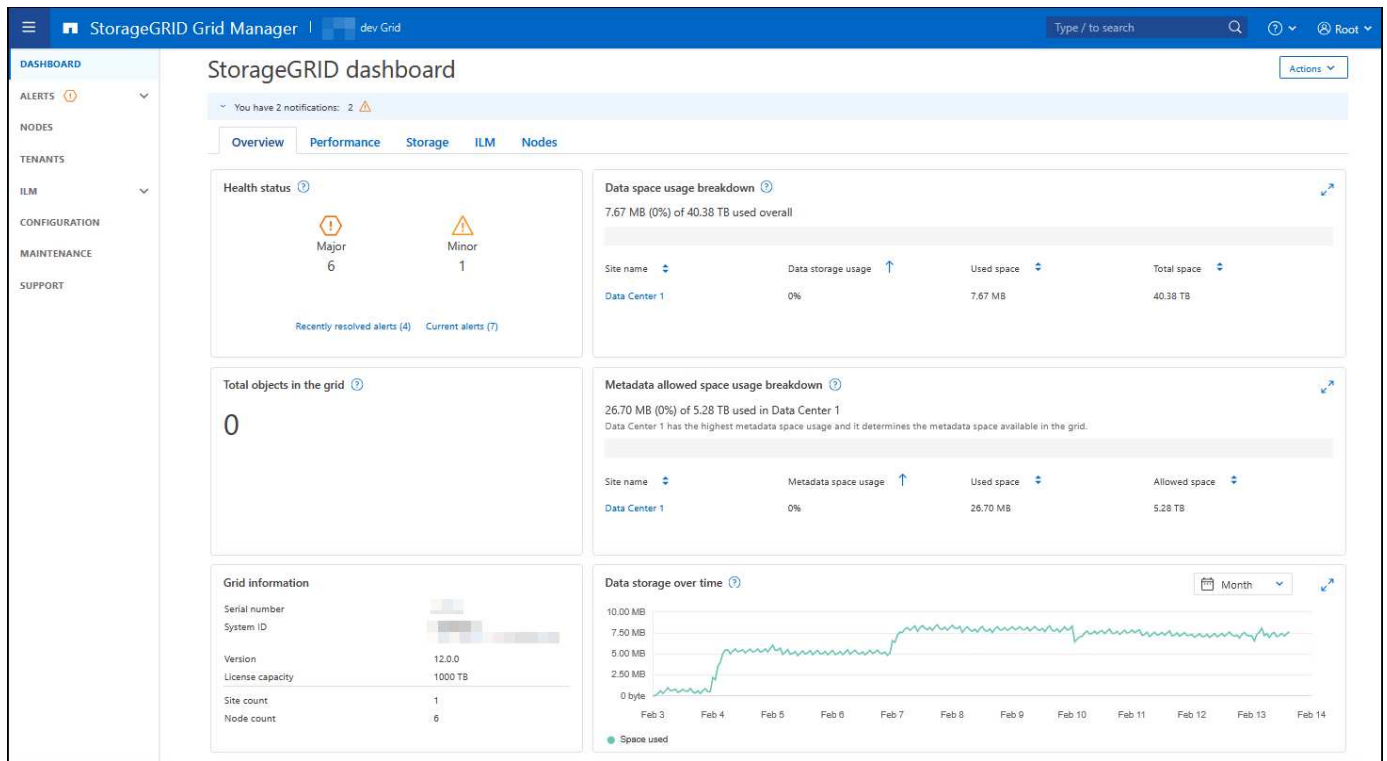
登录到网络管理器时，您正在连接到管理节点。每个 StorageGRID 系统包括一个主管理节点和任意数量的非主管理节点。您可以连接到任何管理节点，每个管理节点都会显示 StorageGRID 系统的类似视图。

您可以使用 ["支持的 Web 浏览器"](#) 访问网络管理器。

Grid Manager 仪表板

首次登录 Grid Manager 时，您可以使用仪表板—["监控系统活动"](#)一目了然。

仪表板包含有关系统运行状况和性能、存储使用、ILM 流程、S3 操作以及网格中节点的信息。您可以 ["配置仪表板"](#) 从包含有效监控系统所需信息的卡片集合中进行选择。



有关每张卡上显示的信息的说明，请选择该卡的帮助图标 .

搜索字段

标题栏中的*搜索*字段允许您快速导航到 Grid Manager 中的特定页面。例如，您可以输入 **km** 来访问密钥管理服务 (KMS) 页面。

您可以使用*搜索*在网格管理器的侧边栏以及配置、维护和支持菜单中查找条目。您还可以按名称搜索网格节点和租户帐户等项目。

帮助菜单

帮助菜单   提供对以下内容的访问：

- "FabricPool" 和 "S3 设置" 向导
- 当前版本的 StorageGRID 文档网站
- "API 文档"
- 有关当前安装的 StorageGRID 版本的信息

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。

通过"提醒"菜单，您可以执行以下操作 "管理警报"：

- 查看当前警报
- 查看已解决的警报
- 配置静默以抑制警报通知

- 为触发警报的条件定义警报规则
- 配置警报通知的电子邮件服务器

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。要查看特定站点或节点的信息，请选择该站点或节点。

``${post_edited_translations.segment}``

The "``${post_edited_translations.segment}``" 允许您为您的 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，以指定可以存储和检索对象的人员及其可用的功能。

租户页面还提供每个租户的使用情况详细信息，包括使用的存储空间量和对象数。如果在创建租户时设置了配额，则可以看到该配额的使用量。

ILM 菜单

"[ILM 菜单](#)" 允许您 "[配置信息生命周期管理\(ILM\)规则和策略](#)" 控制数据持久性和可用性。您还可以输入对象标识符以查看该对象的元数据。

在 ILM 菜单中，您可以查看和管理 ILM：

- 规则
- 策略
- 策略标签
- 存储池
- 存储级别
- 地区
- 对象元数据查找

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。

网络任务

网络任务包括：

- "[管理高可用性组](#)"
- "[管理负载均衡器端点](#)"
- "[配置 S3 端点域名](#)"
- "``${post_edited_translations.segment}``"
- "[配置 VLAN 接口](#)"
- "``${post_edited_translations.segment}``"

安全任务

安全任务包括：

- "管理安全证书"
- "管理内部防火墙控制"
- "配置密钥管理服务"
- 配置安全设置，包括 "TLS和SSH策略"、"网络 and 对象安全选项"、"界面安全设置" 和 "SSH 访问选项"
- 配置 "存储代理" 或 "管理员代理" 的设置

系统任务

系统任务包括：

- 使用 "网格联盟" 在两个 StorageGRID 系统之间克隆租户帐户信息和复制对象数据
- 或者，启用 "压缩存储的对象" 选项
- 或者，配置 "默认存储桶一致性设置"
- "管理 S3 对象锁定"
- 了解存储设置，例如 "存储卷水印"
- "管理擦除编码配置文件"

监控任务

监控任务包括：

- "配置日志管理"
- "使用 SNMP 监控"

访问控制任务

访问控制任务包括：

- "管理管理员组"
- "管理管理员用户"
- 更改 "配置密码短语" 或 "节点控制台密码"
- "\${post_edited_translations.segment}"
- "配置 SSO"

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。

Tasks

维护任务包括：

- "停用操作" 删除未使用的网格节点和站点
- "扩展操作" 添加新网格节点和站点
- "网格节点恢复过程" 替换故障节点并还原数据
- "重命名过程" 更改网格、站点和节点的显示名称
- "对象存在性检查操作" 验证对象数据是否存在（但不验证其正确性）
- 执行"滚动重新启动"以重新启动多个网格节点
- "卷还原操作"

系统

您可以执行的系统维护任务包括：

- "查看 StorageGRID 许可证信息" 或 "更新许可证信息"
- 正在生成并下载 "恢复包"
- 在选定设备上执行 StorageGRID 软件更新，包括软件升级、热修复和 SANtricity 操作系统软件更新
 - "升级过程"
 - "修补程序过程"
 - "使用 Grid Manager 升级 SG6000 存储控制器上的 SANtricity 操作系统"
 - "使用 Grid Manager 升级 SG5700 存储控制器上的 SANtricity 操作系统"

网络

您可以执行的网络维护任务包括：

- "配置 DNS 服务器"
- "更新网格网络子网"
- "管理 NTP 服务器"

支持菜单

"支持"菜单提供了帮助技术支持分析和排除系统故障的选项。

工具

在"支持"菜单的"工具"部分，您可以：

- "配置 AutoSupport"
- "运行诊断" 关于网格的当前状态
- "收集日志文件和系统数据"
- "查看支持指标"



*指标*选项中提供的工具旨在供技术支持人员使用。这些工具中的某些功能和菜单项故意设置为不可用。

其他

在"支持"菜单的"其他"部分，您可以：

- 配置 "I/O 优先级"
- 配置 "AutoSupport 电子邮件设置 (旧版) "
- 管理 "链路成本"
- 查看节点服务 ID
- 管理 "存储水印"

浏览 StorageGRID 租户管理器

"**租户管理器**" 是基于浏览器的图形界面，租户用户可以访问该界面来配置、管理和监视其存储帐户。



租户管理器随每个版本更新，可能与此页面上的示例屏幕截图不匹配。

当租户用户登录到 Tenant Manager 时，他们正在连接到管理节点。

租户管理器控制面板

网络管理员使用 Grid Manager 或网络管理 API 创建租户帐户后，租户用户可以登录到 Tenant Manager。

租户管理器仪表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 S3 存储桶的列表。已用空间值是存储桶或容器中对象数据的总量。条形图表示这些存储桶或容器的相对大小。

条形图上方显示的值是用于所有租户存储桶或容器的空间的总和。如果在创建帐户时指定了租户可用的最大千兆字节、太字节或拍字节数，则还会显示已使用和剩余的配额量。

Dashboard

16 Buckets
[View buckets](#)

2 Platform services
endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02
ID: 3341 1240 0546 8283 2208
✓ Platform services enabled
✓ Can use own identity source
✓ S3 Select enabled

存储菜单 (S3)

此菜单允许 S3 用户：

- 管理访问密钥
- 创建、管理和删除存储桶
- 管理平台服务端点
- 查看允许其使用的任何网格联盟连接

我的访问密钥

S3 租户用户可以按以下方式管理访问密钥：

- 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 Root 访问权限的用户可以管理 S3 根帐户、自己的帐户和所有其他用户的访问密钥。根访问密钥还提供对租户存储桶和对象的完全访问权限，除非存储桶策略明确禁用。



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 租户用户可以为存储桶执行以下任务：

- 创建存储桶
- 为新存储桶启用 S3 对象锁定（假设已为 StorageGRID 系统启用 S3 对象锁定）
- 更新一致性值
- 启用和禁用上次访问时间更新
- 启用或挂起对象版本控制
- 更新 S3 对象锁定默认保留
- 配置跨源资源共享（CORS）
- 删除存储桶中的所有对象
- 删除空存储桶
- 使用 ["S3 控制台"](#) 管理存储桶对象

如果网格管理员已为租户帐户启用平台服务，则具有相应权限的 S3 租户用户也可以执行以下任务：

- 配置 S3 事件通知，该通知可发送到支持 Amazon Simple Notification Service 的目标服务。
- 配置 CloudMirror 复制，使租户能够自动将对象复制到外部 S3 存储桶。
- 配置搜索集成，每当创建、删除对象或更新对象的元数据或标记时，它会将对象元数据发送到目标搜索索引。

平台服务端点

如果网格管理员已为租户帐户启用平台服务，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。

网格联盟连接

如果网格管理员为租户帐户启用了网格联合连接的使用，则具有 Root 访问权限的 S3 租户用户可以查看连接名称，访问启用了跨网格复制的每个存储桶的存储桶详细信息页面，并查看将存储桶数据复制到连接中的其他网格时发生的最新错误。请参阅 ["查看网格联盟连接"](#)。

访问管理菜单

Access Management 菜单允许 StorageGRID 租户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 and 用户，除非单点登录 (SSO) 对整个 StorageGRID 系统有效。

网络连接准则

StorageGRID 网络准则

使用这些指南了解 StorageGRID 体系结构和网络拓扑，并了解网络配置和设置的要求。

`${post_edited_translations.segment}`

这些指南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。使用这些指南可帮助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能够进行通信。

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

- 存储和检索对象数据
- 接收电子邮件通知
- 访问 StorageGRID 管理接口（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(KMS)

必须适当配置 StorageGRID 网络，以处理这些功能及更多功能的流量。

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 ["了解 StorageGRID"](#) 中所述。

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。

安装设备节点

- ["安装设备硬件"](#)

安装基于软件的节点

- ["在基于软件的节点上安装 StorageGRID"](#)

配置并管理 StorageGRID 软件

- ["管理 StorageGRID"](#)
- ["发行说明"](#)。您必须使用您的 NetApp 帐户登录或创建帐户才能访问发行说明。

StorageGRID 网络类型

StorageGRID 系统中的网格节点处理_网络流量_、管理流量_和_客户端流量。您必须适当配置网络，以管理这三种类型的流量并提供控制 and 安全性。

流量类型

流量类型	问题描述	网络类型
网络流量	在网格中的所有节点之间传输的内部 StorageGRID 流量。所有网格节点必须能够通过此网络与所有其他网格节点通信。	网格网络（必填）
管理员流量	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 客户端的所有对象存储请求。	客户端网络（可选）， VLAN 网络（可选）

可以通过以下方式配置网络：

- 仅网格网络
- 网格和管理网络
- 网格和客户端网络
- 网格、管理和客户端网络

网格网络是强制性的，可以管理所有网格流量。管理网络和客户端网络可以在安装时加入，也可以稍后添加以适应需求变化。虽然管理网络和客户端网络是可选的，但当您使用这些网络来处理管理和客户端流量时，网格网络可以实现隔离和安全保护。

内部端口只能通过网格网络访问。外部端口可从所有网络类型访问。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 和端口过滤提供了多个选项。请参阅["内部网格节点通信"](#)和["外部通信"](#)。

网络接口

StorageGRID 节点通过以下特定接口连接到每个网络：

网络	接口名称
网格网络（必填）	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 ["在基于软件的节点上安装 StorageGRID"](#)。

设备节点

- ["SG6160 存储设备"](#)
- ["SGF6112 存储设备"](#)
- ["SG6000 存储设备"](#)
- ["SG5800 存储设备"](#)
- ["SG5700 存储设备"](#)

- ["SG110 和 SG1100 服务设备"](#)
- ["SG100 和 SG1000 服务设备"](#)

每个节点的网络信息

必须为在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，则应使用 IP 地址作为网关地址。

高可用性组

高可用性 (HA) 组提供将虚拟 IP (VIP) 地址添加到网格或客户端网络接口的功能。有关详细信息，请参见 ["管理高可用性组"](#)。

网格网络

网格网络是必需的。它用于所有内部 StorageGRID 流量。网格网络提供网格中所有节点之间、所有站点和子网之间的连接。网格网络上的所有节点必须能够与所有其他节点通信。网格网络可以由多个子网组成。包含关键网格服务（如 NTP）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 (NAT)。

即使配置了管理网络和客户端网络，也可以将网格网络用于所有管理流量和所有客户端流量。除非节点配置了客户端网络，否则网格网络网关是节点默认网关。



配置网格网络时，您必须确保网络免受不受信任的客户端（例如开放互联网上的客户端）的侵害。

请注意网格网络网关的以下要求和详细信息：

- 如果有多个网格子网，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。
- 系统会自动为全局网格网络子网列表中配置的所有子网的所有节点生成静态路由。
- 如果添加了客户端网络，则在完成网格配置后，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，可用于系统管理和维护流量。管理网络通常是专用网络，不需要在节点之间进行路由。

您可以选择哪些网格节点应启用管理网络。

使用管理网络时，管理和维护流量不需要跨网格网络传输。管理网络的典型用途包括以下内容：

- 访问 Grid Manager 和 Tenant Manager 用户界面。
- 访问关键服务，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。
- 用于维护和支持的安全外壳协议 (SSH) 访问。

管理网络绝不会用于内部网络流量。提供了管理网络网关，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：

- 如果将从管理网络子网外部进行连接，或者配置了多个管理网络子网，则需要管理网络网关。
- 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，它用于为 S3 等客户端应用程序提供对网格服务的访问。如果您计划使 StorageGRID 数据可供外部资源（例如，云存储池或 StorageGRID CloudMirror 复制服务）访问，则外部资源也可以使用客户端网络。网格节点可以与通过客户端网络网关可访问的任何子网通信。

您可以选择哪些网格节点应启用客户端网络。所有节点不必在同一个客户端网络上，并且节点永远不会通过客户端网络相互通信。在网格安装完成之前，客户端网络不会开始运行。

为了增加安全性，您可以指定节点的客户端网络接口不受信任，以便客户端网络对允许的连接进行更严格的限制。如果节点的客户端网络接口不受信任，则该接口将接受 CloudMirror 复制使用的出站连接，但仅接受已显式配置为负载均衡器端点的端口上的入站连接。请参阅 ["管理防火墙控件"](#) 和 ["配置负载均衡器端点"](#)。

使用客户端网络时，客户端流量不需要跨网格网络传输。网格网络流量可以分离到安全、不可路由的网络上。以下节点类型通常配置有客户端网络：

- 网关节点，因为这些节点提供对 StorageGRID 负载均衡器服务的访问权限以及对网格的 S3 客户端访问权限。
- 存储节点，因为这些节点提供对 S3 协议以及云存储池和 CloudMirror 复制服务的访问。
- 管理节点，以确保租户用户可以连接到 Tenant Manager，而无需使用管理网络。

对于客户端网络网关，请注意以下内容：

- 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，您可以选择将虚拟 LAN (VLAN) 网络用于客户端流量和某些类型的管理员流量。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，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，也可以将中继接口添加到该节点。

如果将 eth0 配置为中继，则网格网络流量将按照交换机上的配置通过中继本机接口。同样，如果将 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本征 VLAN。

仅在 VLAN 网络上支持入站管理流量，例如用于 SSH、Grid Manager 或 Tenant Manager 流量。出站流量（例如用于 NTP、DNS、LDAP、KMS 和 Cloud Storage Pools）不支持通过 VLAN 网络传输。



VLAN 接口只能添加到管理节点和网关节点。您不能将 VLAN 接口用于客户端或管理员对存储节点的访问。

有关说明和指南，请参见 ["配置 VLAN 接口"](#)。

VLAN 接口仅在 HA 组中使用，并在活动节点上分配 VIP 地址。有关说明和指南，请参阅 ["管理高可用性组"](#)。

网络拓扑示例

StorageGRID 的网格网络拓扑

最简单的网络拓扑仅通过配置网格网络来创建。

配置网格网络时，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。

在配置过程中，您必须将所有网格网络子网添加到网格网络子网列表 (GNSL)。此列表包括所有站点的所有子网，还可能包括提供对 NTP、DNS 或 LDAP 等关键服务的访问权限的外部子网。

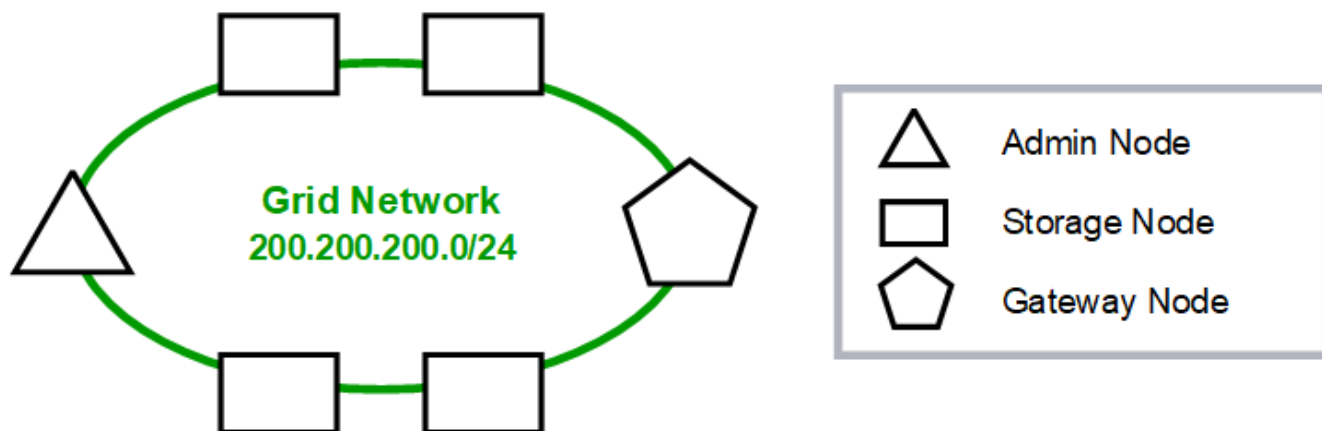
安装时，网格网络接口为 GNSL 中的所有子网应用静态路由，并将节点的默认路由设置为网格网络网关（如果已配置）。如果没有客户端网络，且网格网络网关是节点的默认路由，则不需要 GNSL。此外，还会生成指向网格中所有其他节点的主机路由。

在此示例中，所有流量共享同一个网络，包括与 S3 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，或第三方负载均衡器充当客户端访问边界的情况。在可能的情况下，网格网络应仅用于内部流量。管理网络和客户端网络都有额外的防火墙限制，可以阻止到内部服务的外部流量。支持将网格网络用于外部客户端流量，但这种使用提供的保护层较少。

Topology example: Grid Network only



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

StorageGRID 的管理网络拓扑

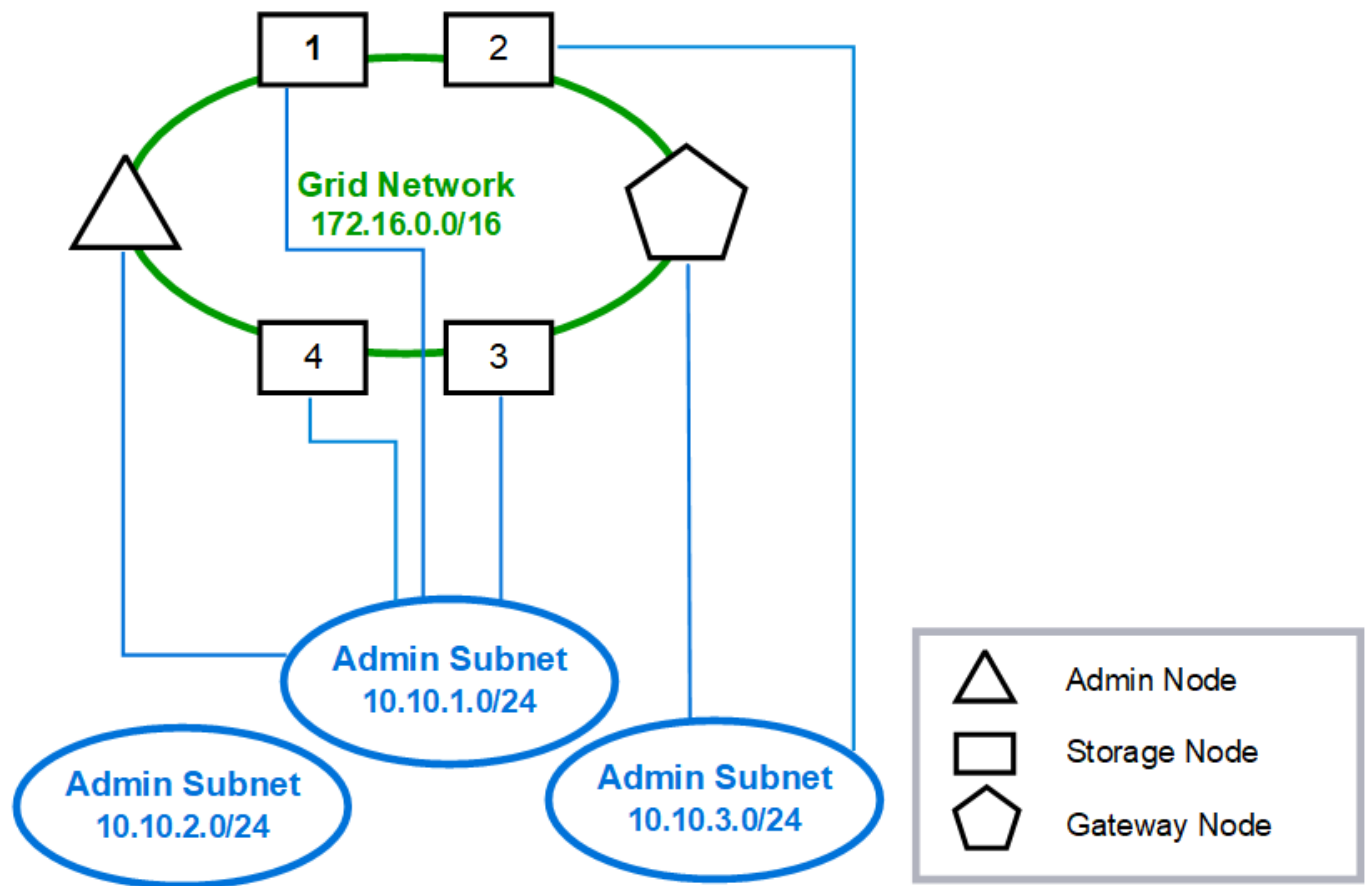
拥有管理网络是可选的。使用管理网络和网格网络的一种方法是为每个节点配置可路由的网格网络和有界管理网络。

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

管理网络可以对每个节点都是唯一的，并且可以由多个子网组成。可以为每个节点配置管理外部子网列表 (AESL)。AESL 列出每个节点通过管理网络可访问的子网。AESL 还必须包括网格将通过管理网络访问的任何服务的子网，例如 NTP、DNS、KMS 和 LDAP。静态路由应用于 AESL 中的每个子网。

在此示例中，网格网络用于与 S3 客户端请求和对象管理相关的流量，而管理网络用于管理功能。

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	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

StorageGRID 的客户端网络拓扑

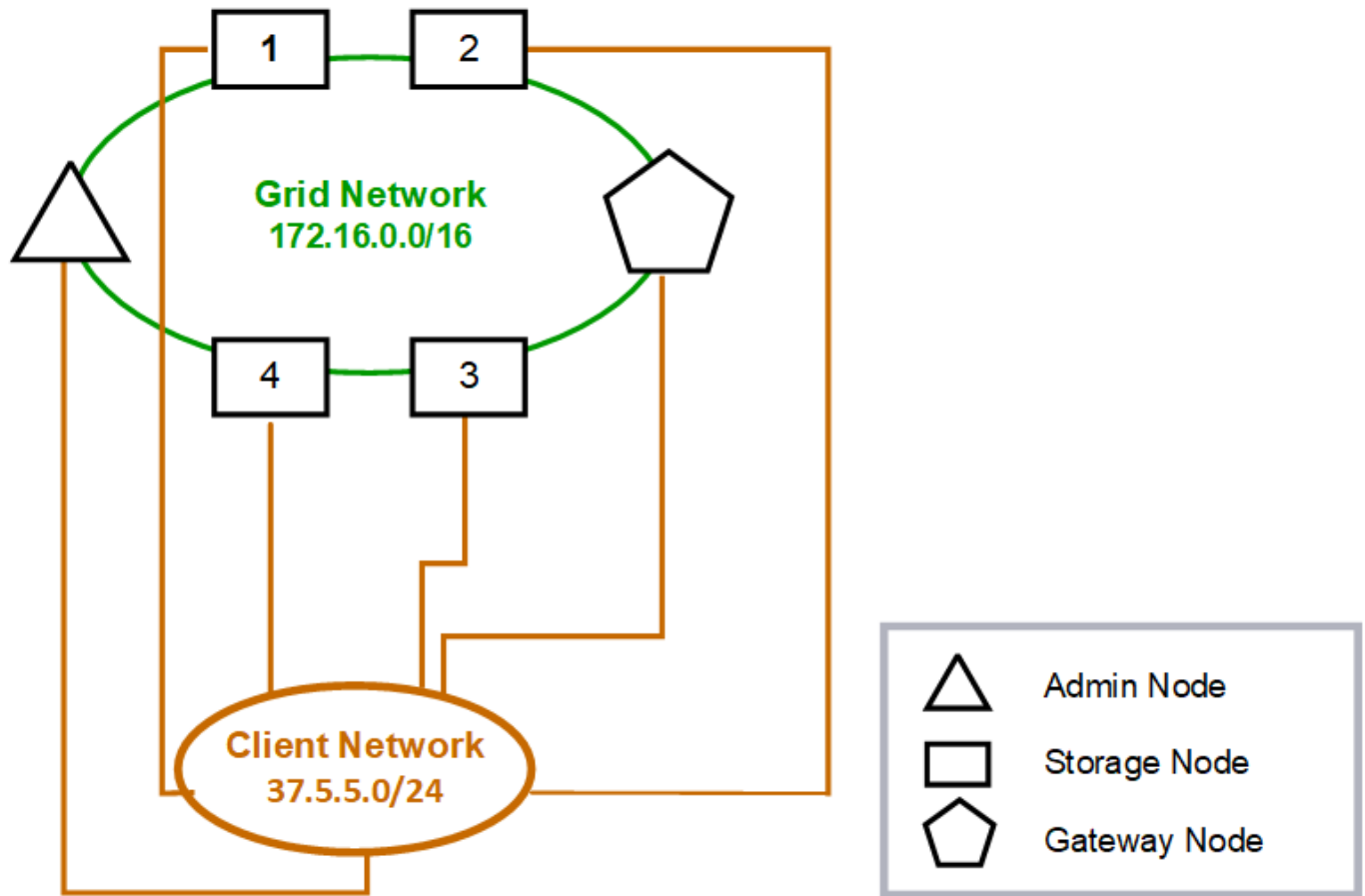
拥有客户端网络是可选的。使用客户端网络允许将客户端网络流量（例如 S3）与网格内部流量分开，从而使网格网络更加安全。未配置管理网络时，可由客户端或网格网络处理管理流量。

配置客户端网络时，需要为配置的节点的 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。

如果在安装过程中为节点配置客户端网络，则在安装完成后，该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。如果稍后添加了客户端网络，则节点的默认网关将以相同的方式切换。

在此示例中，客户端网络用于 S3 客户端请求和管理功能，而网格网络专用于内部对象管理操作。

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	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

相关信息

["更改节点网络配置"](#)

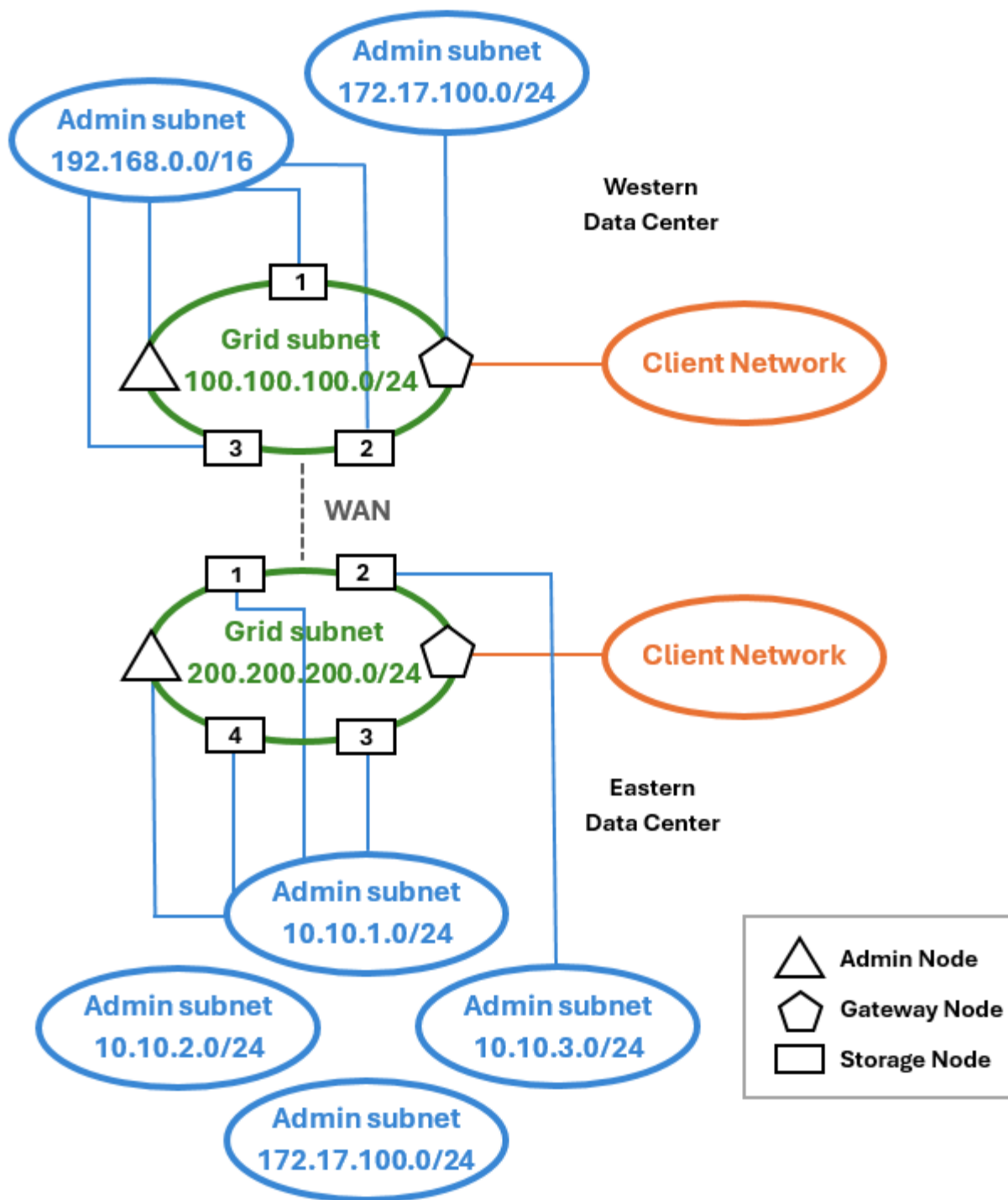
所有三个 **StorageGRID** 网络的网络拓扑

您可以将所有三个网络配置为由专用网格网络、特定于站点的有界管理网络和开放客户端网络组成的网络拓扑。如果需要，使用负载均衡器端点和不受信任的客户端网络可以提供额外的安全性。

在此示例中：

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

拓扑示例：网格、管理和客户端网络



StorageGRID 的网络要求

您必须验证当前的网络基础设施和配置是否能够支持计划的 StorageGRID 网络设计。

一般网络要求

所有 StorageGRID 部署必须能够支持以下连接。

这些连接可以通过网格、管理或客户端网络，或网络拓扑示例中所示的这些网络的组合来实现。

- **管理连接**：从管理员到节点的入站连接，通常通过 SSH。Web 浏览器访问 Grid Manager、Tenant Manager 和 StorageGRID Appliance Installer。
- **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**：来自存储节点上身份服务的出站 TCP 连接。
- **AutoSupport**：从管理节点到 `support.netapp.com` 或客户配置代理的出站 TCP 连接。
- **外部密钥管理服务器**：从每个已启用节点加密的设备节点出站 TCP 连接。
- 来自 S3 客户端的入站 TCP 连接。
- 来自 StorageGRID 平台服务（如 CloudMirror 复制）或来自云存储池的出站请求。

如果 StorageGRID 无法使用默认路由规则联系任何已配置的 NTP 或 DNS 服务器，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，以确保该网络用于将来所有的连接尝试。



虽然您可以使用这些自动发现的主机路由，但一般来说，您应该手动配置 DNS 和 NTP 路由，以确保在自动发现失败时的连接性。

如果您尚未准备好在部署期间配置可选的管理员和客户端网络，则可以在配置步骤中批准网格节点时配置这些网络。此外，您可以在安装后使用 Change IP 工具配置这些网络（请参阅[配置 IP 地址](#)）。

仅支持通过 VLAN 接口进行 S3 客户端连接以及 SSH、Grid Manager 和 Tenant Manager 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。如果将接口配置为中继以支持 VLAN 接口，则此流量将按照交换机的配置在接口的本机 VLAN 上流动。

适用于多个站点的广域网 (WAN)

在配置具有多个站点的 StorageGRID 系统时，站点之间的 WAN 连接在考虑客户端流量之前，每个方向的最小带宽必须为 25 Mbit/秒。站点之间的数据复制或纠删编码、节点或站点扩展、节点恢复以及其他操作或配置将需要额外的带宽。

实际的最小 WAN 带宽要求取决于客户端活动和 ILM 保护方案。如需在估算最小 WAN 带宽要求方面获得帮助，请联系您的 NetApp 专业服务顾问。

管理节点和网关节点的连接

必须始终保护管理节点不受不受信任的客户端（例如开放互联网上的客户端）的攻击。您必须确保任何不受信任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。

计划添加到高可用性组的管理节点和网关节点必须配置静态 IP 地址。有关详细信息，请参见[管理高可用性组](#)。

使用网络地址转换(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 (NAT)。当您为网格网络使用私有 IPv4 地址时，这些地址必须能够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的客户端和网格节点之间使用 NAT，例如为网关节点提供公共 IP 地址。仅当您使用对网格中所有节点透明的隧道应用程序

序时，才支持使用 NAT 来桥接公网段，这意味着网格节点不需要知道公共 IP 地址。

StorageGRID 的网络特定要求

请遵循每个 StorageGRID 网络类型的要求。

网络网关和路由器

- 如果设置，给定网络的网关必须在特定网络的子网内。
- 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。
- 如果没有网关，最佳做法是将网关地址设置为网络接口的 IP 地址。

子网



每个网络必须连接到自己的子网，该子网不与节点上的任何其他网络重叠。

网络管理器在部署期间强制执行以下限制。此处提供这些信息以协助部署前的网络规划。

- 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 表示法中为 /31 或 /32）。
- 由网络接口 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。
- 对于任何节点的网格网络、管理网络或客户端网络，请勿使用包含以下 IPv4 地址的子网：
 - 192.168.130.101
 - 192.168.130.121
 - 192.168.131.101
 - 192.168.131.121
 - 192.168.130.102
 - 192.168.130.122
 - 192.168.131.102
 - 192.168.131.122
 - 198.51.100.2
 - 198.51.100.4

例如，对于任何节点的网格网络、管理网络或客户端网络，请不要使用以下子网范围：

- 192.168.130.0/24，因为此子网范围包含 IP 地址 192.168.130.101 和 192.168.130.102
- 192.168.131.0/24，因为此子网范围包含 IP 地址 192.168.131.101 和 192.168.131.102
- `${post_edited_translations.segment}`
- 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，每个网格节点必须连接到网格网络，并且必须能够使用您在部署节点时指定的网络配置与主管理节点通信。
- 在正常网格操作期间，每个网格节点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路由。不支持节点之间的网络地址转换（NAT）。

- 如果网格网络由多个子网组成，请将其添加到网格网络子网列表 (GNSL)。系统会为 GNSL 中每个子网的所有节点创建静态路由。
- 如果将网格网络接口配置为中继以支持 VLAN 接口，则中继本征 VLAN 必须是用于网格网络流量的 VLAN。必须能够通过中继本征 VLAN 访问所有网格节点。

管理网络

管理网络是可选的。如果您计划配置管理网络，请遵循这些要求和准则。

管理网络的典型用途包括管理连接、AutoSupport、KMS 以及与关键服务器（如 NTP、DNS 和 LDAP）的连接（如果未通过网格网络或客户端网络提供这些连接）。



只要所需的网络服务和客户端可访问，管理网络和 AESL 对于每个节点都可以是唯一的。



要启用来自外部子网的入站连接，必须至少在管理网络上定义一个子网。系统会自动为 AESL 中每个子网的每个节点生成静态路由。

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，请注意以下注意事项。

- 客户端网络旨在支持来自 S3 客户端的流量。如果已配置，则客户端网络网关将成为该节点的默认网关。
- 如果使用客户端网络，则可以通过仅接受显式配置的负载均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。请参阅 ["配置负载均衡器端点"](#)。
- 如果将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，客户端网络流量将按照交换机中的配置通过中继本征 VLAN。

相关信息

["更改节点网络配置"](#)

特定于部署的网络注意事项

StorageGRID Linux 部署的网络配置

为了提高效率、可靠性和安全性，StorageGRID 系统在 Linux 上作为容器引擎的集合运行。StorageGRID 系统中不需要与容器引擎相关的网络配置。

为容器网络接口使用非绑定设备，例如 VLAN 或虚拟以太网 (veth) 对。在节点配置文件中将此设备指定为网络接口。



不要直接使用绑定或桥接设备作为容器网络接口。这样做可能会阻止节点启动，因为在容器命名空间中使用带有绑定和桥接设备的 `macvlan` 存在内核问题。

请参阅["安装说明"](#)。

用于容器引擎部署的主机网络配置

在容器引擎平台上启动 StorageGRID 部署之前，请确定每个节点将使用哪些网络（网络、管理、客户端）。您必须确保每个节点的网络接口配置在正确的虚拟或物理主机接口上，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络节点：

- 确保所有主机对每个节点接口使用相同的主机接口。此策略简化了主机配置，并为未来的节点迁移提供了便利。
- 获取物理主机本身的 IP 地址。



主机上的物理接口可以由主机本身和主机上运行的一个或多个节点使用。使用此接口分配给主机或节点的任何 IP 地址必须是唯一的。主机和节点无法共享 IP 地址。

- 打开到主机的所需端口。
- 如果您打算在 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` 或附加接口传入节点容器。要添加中继或接入接口，请参见以下内容：
 - **Linux**（安装节点之前）：["创建节点配置文件"](#)
 - **Linux**（安装节点后）：["将中继或接入接口添加到节点"](#)



"Linux"是指 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参见 ["NetApp 互操作性矩阵工具 \(IMT\)"](#)。

最小带宽建议

下表提供了每种 StorageGRID 节点类型和每种网络类型的最低 LAN 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，以满足您计划在该主机上运行的 StorageGRID 节点总数和类型的最低带宽要求。

节点类型	网络类型		
	Grid	管理员	客户端
	最小局域网带宽	管理员	10 Gbps
1 Gbps	1 Gbps	网关	10 Gbps
1 Gbps	10 Gbps	存储	10 Gbps

节点类型	网络类型		
1 Gbps	10 Gbps	归档	10 Gbps



此表不包括访问共享存储所需的 SAN 带宽。如果使用通过以太网访问的共享存储（iSCSI 或 FCoE），则应在每台主机上配置单独的物理接口，以提供足够的 SAN 带宽。为了避免引入瓶颈，给定主机的 SAN 带宽应与该主机上运行的所有存储节点的总存储节点网络带宽大致匹配。

根据计划在每台主机上运行的 StorageGRID 节点的数量和类型，使用该表确定要在该主机上设置的最小网络接口数量。

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：

- 连接管理节点上的网络和管理网络（需要 $10 + 1 = 11$ Gbps）
- 连接网关节点上的网络和客户端网络（需要 $10 + 10 = 20$ Gbps）
- 连接存储节点上的网络网络（需要 10 Gbps）

在这种情况下，您应提供至少 $11 + 20 + 10 = 41$ Gbps 的网络带宽，这可以通过两个 40 Gbps 接口或五个 10 Gbps 接口来满足，这些接口可能会聚合到中继，然后由三个或更多承载 Grid、Admin 和 Client 子网的 VLAN 共享，这些子网位于包含主机的物理数据中心本地。

有关在 StorageGRID 集群中的主机上配置物理和网络资源以准备 StorageGRID 部署的一些推荐方法，请参见 "[配置主机网络](#)"。

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，则必须配置网络网络和防火墙，以确保可以到达目标端点。

平台服务的网络

如"[为租户管理平台服务](#)"和"[管理平台服务](#)"中所述，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 ADC 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 ADC 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。如果您使用默认路由，则可以使用 "[不受信任的客户端网络功能](#)" 限制入站连接。

云存储池的网络

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](#)"。

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

可以在创建或编辑端点时指定不同的端口。请参阅["网络端口参考"](#)。

如果使用不透明的代理服务器，则还必须["配置存储代理设置"](#)以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

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、管理或客户端网络访问。

StorageGRID 设备节点的网络配置

您可以配置 StorageGRID 设备上的网络端口，以使用满足吞吐量、冗余和故障转移要求的端口绑定模式。

StorageGRID 设备上的 10/25-GbE 端口可以配置为固定或聚合绑定模式，以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，以连接到管理网络。

请参见有关设备的端口绑定模式的信息：

- ["端口绑定模式 \(SG6160\)"](#)
- ["端口绑定模式 \(SGF6112\)"](#)
- ["端口绑定模式 \(SG6000-CN 控制器\)"](#)
- ["端口绑定模式 \(SG5800 控制器\)"](#)
- ["端口绑定模式 \(E5700SG 控制器\)"](#)
- ["端口绑定模式 \(SG110 和 SG1100\)"](#)
- ["端口绑定模式 \(SG100 和 SG1000\)"](#)

StorageGRID 的网络安装和配置

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。如果网格网络是隔离的，您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，包含 NTP 服务器或需要访问 Grid Manager 或 API 的子网也可以配置为网格子网。

使用主管理节点自动注册节点

部署节点后，它们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。在网格配置过程中，您可以配置多个网格子网。完成网格配置后，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删除它们的配置，也可以在安装完成后使用更改 IP 工具（请参阅["配置 IP 地址"](#)）。

StorageGRID 安装后指南

完成网格节点部署和配置后，请按照以下指导原则进行 DHCP 寻址和网络配置更改。

- 如果使用 DHCP 分配 IP 地址，请为正在使用的网络上的每个 IP 地址配置 DHCP 保留。

您只能在部署阶段设置 DHCP。您无法在配置期间设置 DHCP。



当 DHCP 更改网格网络配置时，节点将重新启动，如果 DHCP 更改同时影响多个节点，则可能会导致中断。

- 如果要更改网格节点的 IP 地址、子网掩码和默认网关，则必须使用更改 IP 过程。请参阅["配置 IP 地址"](#)。
- 如果进行网络配置更改，包括路由和网关更改，则客户端与主管理节点和其他网格节点的连接可能会丢失。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

StorageGRID 的内部网格节点通信

StorageGRID 内部防火墙允许传入到网格网络上的特定端口的连接。负载均衡器端点定义的端口也接受连接。



NetApp 建议您启用网格节点之间的互联网控制消息协议 (ICMP) 流量。当无法访问网格节点时，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 使用虚拟路由器冗余协议 (VRRP)。VRRP 是一种使用 IP 协议编号 112 的互联网协议。StorageGRID 仅在单播模式下使用 VRRP。仅当配置了["高可用性组"](#)时才需要 VRRP。

基于 Linux 的节点指南

如果企业网络策略限制对任何这些端口的访问，则可以使用部署配置参数在部署时重新映射端口。有关端口重映射和部署配置参数的详细信息，请参见["在基于软件的节点上安装 StorageGRID"](#)。



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅["删除裸主机上的端口重映射"](#)。

仅当需要定义 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任何这些端口的访问，则可以在使用 VMware vSphere Web Client 部署节点时或在自动化网络节点部署时使用配置文件设置来重新映射端口。有关端口重映射和部署配置参数的详细信息，请参见 "[在 VMware 上安装 StorageGRID](#)" 的说明。



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 "[删除裸机主机上的端口重映射](#)"。

设备节点指南

如果企业网络策略限制对任何这些端口的访问，则可以使用 StorageGRID 设备安装程序重新映射端口。请参阅 "[可选：重新映射设备的网络端口](#)"。



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 "[删除 StorageGRID 设备上的端口重映射](#)"。

StorageGRID 内部端口

端口	TCP 或 UDP	自	至	详细信息
22	TCP	主管理节点	所有节点	对于维护过程，主管理节点必须能够使用端口 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	由 StorageGRID 设备用于与主管理节点通信以开始安装。
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 与其他每个节点同步其时间。
443	TCP	所有节点	主管理节点	用于在安装和其他维护过程中向主管理节点传达状态。
1055	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护程序的内部流量。
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	带 ADC 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	S3 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。

端口	TCP 或 UDP	自	至	详细信息
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	负载均衡器内部流量。
1508	TCP	所有节点	主管理节点	配置管理内部流量。
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	提供组播 DNS (mDNS) 服务，用于在安装、扩展和恢复期间进行全网格 IP 更改和主管理节点发现。 注意：配置此端口是可选的。
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	主管理节点	用于安装、扩展、恢复、其他维护程序和错误报告的内部流量。
8011	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护程序的内部流量。
8443	TCP	主管理节点	设备节点	与维护模式过程相关的内部流量。
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。包括维护程序、指标和网络更新。
10226	TCP	存储节点	主管理节点	由 StorageGRID 设备用于将 AutoSupport 包从 E 系列 SANtricity System Manager 转发到主管理节点。
10342	TCP	所有节点	主管理节点	用于安装、扩展、恢复和其他维护程序的内部流量。
18000	TCP	管理/存储节点	带 ADC 的存储节点	帐户服务内部流量。
18001	TCP	管理/存储节点	带 ADC 的存储节点	Identity Federation 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。

端口	TCP 或 UDP	自	至	详细信息
18003	TCP	管理/存储节点	带 ADC 的存储节点	平台服务内部流量。
18017	TCP	管理/存储节点	存储节点	Data Mover 服务用于云存储池的内部流量。
18019	TCP	所有节点	所有节点	用于擦除编码和复制的区块服务内部流量
18082	TCP	管理/存储节点	存储节点	S3 相关的内部流量。
18086	TCP	所有节点	存储节点	与 LDR 服务相关的内部流量。
18200	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	带 ADC 的存储节点	Keystone 服务内部流量。

相关信息

["外部通信"](#)

StorageGRID 的外部通信

客户端需要与网格节点进行通信，以获取和检索内容。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。

限制访问端口

如果企业网络策略限制对任何端口的访问，则可以执行以下操作之一：

- 使用 ["负载均衡器端点"](#) 允许访问用户定义的端口。
- 部署节点时重新映射端口。但是，不应重新映射负载均衡器端点。请参阅有关 StorageGRID 节点端口重新映射的信息：



对端口重新映射的支持已弃用，将在未来版本中删除。要删除重新映射的端口，请参阅 ["删除 StorageGRID 设备上的端口重映射"](#) 或 ["删除裸机主机上的端口重映射"](#)。

- ["StorageGRID on Red Hat Enterprise Linux 的端口重映射密钥"](#)
- ["在 VMware 上重新映射 StorageGRID 的端口"](#)
- ["可选：重新映射设备的网络端口"](#)

下表显示了流入节点的流量所使用的端口。



此列表不包括可能配置为 "负载均衡器端点" 的端口。

端口	TCP 或 UDP	协议	自	至	详细信息
22	TCP	SSH	维修笔记本电脑	所有节点	具有控制台步骤的操作步骤需要 SSH 或控制台访问权限。您也可以选择使用端口 2022 而非端口 22。 注意：仅当需要为某些维护操作启用 SSH 访问时，才需要此端口。
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 DNS。
67	UDP	DHCP	所有节点	DHCP 服务	可选用于支持基于 DHCP 的网络配置。dhclient 服务不为静态配置的网格运行。
68	UDP	DHCP	DHCP 服务	所有节点	可选用于支持基于 DHCP 的网络配置。dhclient 服务不会为使用静态 IP 地址的网格运行。
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 将重定向到 StorageGRID 设备安装程序的端口 8443。
80	TCP	HTTP	带 ADC 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。租户可以在创建端点时覆盖默认的 HTTP 端口设置 80。
80	TCP	HTTP	存储节点	AWS	云存储池请求发送到使用 HTTP 的 AWS 目标。网格管理员可以在配置云存储池时覆盖默认的 HTTP 端口设置 80。
123	UDP	NTP	主 NTP 节点	外部 NTP	网络时间协议服务。被选为主 NTP 源的节点也与外部 NTP 时间源同步时钟时间。

端口	TCP 或 UDP	协议	自	至	详细信息
161	TCP/UDP	SNMP	SNMP 客户端	所有节点	用于 SNMP 轮询。所有节点都提供基本信息；管理节点还提供警报数据。配置时默认为 UDP 端口 161。 注意：此端口仅为必需端口，并且仅在配置 SNMP 时在节点防火墙上打开。如果您计划使用 SNMP，则可以配置备用端口。 注意：有关在 StorageGRID 中使用 SNMP 的信息，请联系您的 NetApp 客户代表。
162	TCP/UDP	SNMP 通知	所有节点	通知目的地	出站 SNMP 通知和陷阱默认为 UDP 端口 162。 *注意：*仅当启用了 SNMP 并配置了通知目的地时，才需要此端口。如果您计划使用 SNMP，则可以配置备用端口。 注意：有关在 StorageGRID 中使用 SNMP 的信息，请联系您的 NetApp 客户代表。
389	TCP/UDP	LDAP	带 ADC 的存储节点	Active Directory/LDAP	用于连接到 Active Directory 或 LDAP 服务器以进行 Identity Federation。
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 Tenant Manager。 注意：如果您关闭 Grid Manager 端口 443 或 8443，则当前连接到被阻止端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。请参阅配置防火墙控件以配置特权 IP 地址。
443	TCP	HTTPS	管理节点	Active Directory	如果启用单一登录 (SSO)，则由连接到 Active Directory 的管理节点使用。
443	TCP	HTTPS	带 ADC 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。租户可以在创建端点时覆盖默认的 HTTP 端口设置 443。
443	TCP	HTTPS	存储节点	AWS	云存储池请求发送到使用 HTTPS 的 AWS 目标。网格管理员可以在配置云存储池时覆盖默认 HTTPS 端口设置 443。

端口	TCP 或 UDP	协议	自	至	详细信息
5353	UDP	mDNS	所有节点	所有节点	提供组播 DNS (mDNS) 服务，用于在安装、扩展和恢复期间进行全网格 IP 更改和主管理节点发现。 注意：配置此端口是可选的。
5696	TCP	KMIP	设备	KMS	从配置为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 (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。
8443	TCP	HTTPS	浏览器	管理节点	可选。由 Web 浏览器和管理 API 客户端用于访问 Grid Manager。可用于分隔 Grid Manager 和 Tenant Manager 通信。 注意：如果您关闭 Grid Manager 端口 443 或 8443，则当前连接到受阻端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。请参阅"配置防火墙控件"以配置特权 IP 地址。
8443	TCP	HTTPS	浏览器	设备	由 Web 浏览器和管理 API 客户端用于访问 StorageGRID 设备安装程序。 注意：端口 443 重定向到 StorageGRID 设备安装程序的端口 8443。
9022	TCP	SSH	维修笔记本电脑	设备	在预配置模式下授予对 StorageGRID 设备的访问权限，以进行支持和故障排除。此端口无需在网格节点之间或正常操作期间访问。
9091	TCP	HTTPS	外部 Grafana 服务	管理节点	由外部 Grafana 服务用于安全访问 StorageGRID Prometheus 服务。 注意：仅当启用了基于证书的 Prometheus 访问权限时，才需要此端口。
9092	TCP	Kafka	带 ADC 的存储节点	Kafka 集群	用于发送到 Kafka 集群的平台服务消息。租户可以在创建端点时覆盖默认的 Kafka 端口设置 9092。
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。可用于分离 Grid Manager 和租户管理器通信。
18082	TCP	HTTPS	S3 客户端	存储节点	S3 客户端流量直接到达存储节点 (HTTPS)。

端口	TCP 或 UDP	协议	自	至	详细信息
18084	TCP	HTTP	S3 客户端	存储节点	S3 客户端流量直接到达存储节点 (HTTP)。
23000-23999	TCP	HTTPS	跨网格复制的源网格上的所有节点	用于跨网格复制的目标网格上的管理节点和网关节点	此端口范围保留用于网格联合连接。给定连接中的两个网格使用相同的端口。

StorageGRID 快速入门

按照以下高级步骤配置和使用任何 StorageGRID 系统。

1

学习、规划和收集数据

与您的 NetApp 客户代表合作，了解相关选项并规划您的新 StorageGRID 系统。请考虑以下类型的问题：

- 您希望最初和一段时间内存储多少对象数据？
- 您需要多少个站点？
- 每个站点需要多少个节点以及哪些类型的节点？
- 您将使用哪些 StorageGRID 网络？
- 谁将使用您的网格来存储对象？他们将使用哪些应用程序？
- 您是否有任何特殊的安全或存储要求？
- 是否需要遵守任何法律或监管要求？

(可选) 与您的 NetApp 专业服务顾问一起访问 NetApp ConfigBuilder 工具，以完成安装和部署新系统时使用的配置工作簿。您还可以使用此工具帮助自动配置任何 StorageGRID 设备。请参阅 ["自动化设备安装和配置"](#)。

查看 ["了解 StorageGRID"](#) 和 ["网络连接准则"](#)。

2

安装节点

StorageGRID 系统由单独的基于硬件和基于软件的节点组成。首先为每个设备节点安装硬件，然后配置每个 Linux 或 VMware 主机。

要完成安装，请在每个设备或软件主机上安装 StorageGRID 软件，并将节点连接到网格中。在此步骤中，您将提供 NTP 和 DNS 服务器的站点和节点名称、子网详细信息以及 IP 地址。

了解具体操作方法：

- ["安装设备硬件"](#)
- ["在基于软件的节点上安装 StorageGRID"](#)

3

登录并检查系统运行状况

网格安装完成后，您可以登录到 Grid Manager。在那里，您可以查看新系统的整体运行状况，启用 AutoSupport 和警报电子邮件，并设置 S3 端点域名。

了解具体操作方法：

- ["登录到网格管理器"](#)
- ["监控系统运行状况"](#)
- ["配置 AutoSupport"](#)
- ["为警报设置电子邮件通知"](#)
- ["配置 S3 端点域名"](#)

4

配置和管理

您需要为新的 StorageGRID 系统执行的配置任务取决于您将如何使用网格。至少，您需要设置系统访问权限；使用 FabricPool 和 S3 向导；以及管理各种存储和安全设置。

了解具体操作方法：

- ["控制 StorageGRID 访问"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["使用 FabricPool 设置向导"](#)
- ["管理安全"](#)
- ["系统加固"](#)

5

设置 ILM

通过配置由一个或多个 ILM 规则组成的信息生命周期管理 (ILM) 策略，您可以控制 StorageGRID 系统中每个对象的放置位置和持续时间。ILM 规则指示 StorageGRID 如何创建和分发对象数据的副本，以及如何随时间推移管理这些副本。

了解具体操作方法：["使用 ILM 管理对象"](#)

6

使用 StorageGRID

初始配置完成后，StorageGRID 租户帐户可以使用 S3 客户端应用程序来接收、检索和删除对象。

了解具体操作方法：

- ["使用租户帐户"](#)
- ["使用 S3 REST API"](#)

7

监控和故障排除

当您的系统启动并运行时，您应该定期监控其活动，并对任何警报进行故障排除和解决。您可能还需要配置外部 syslog 服务器、使用 SNMP 监控或收集其他数据。

了解具体操作方法：

- ["监控 StorageGRID"](#)
- ["StorageGRID 故障排除"](#)

8

扩展、维护和恢复

您可以添加节点或站点以扩展系统的容量或功能。您还可以执行各种维护程序，以从故障中恢复，或使您的 StorageGRID 系统保持最新状态并高效运行。

了解具体操作方法：

- ["展开网格"](#)
- ["维护您的网格"](#)
- ["恢复节点"](#)

版权信息

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

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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