StorageGRID 12.1 软件文档

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid/index.html on July 22, 2026.
Always check docs.netapp.com for the latest.

目录

StorageGRID 12.1 软件文档 1
了解 StorageGRID 设备硬件 2
发行说明 3
StorageGRID 12.1 中的新增功能 3
容量 3
控制访问 3
联邦 3
易管理性 3
S3 3
安全性 4
租户 4
升级 5
用户接口 5
StorageGRID 中已删除或弃用的功能和特性 5
定义 5
StorageGRID停止功能支持 6
StorageGRID 中网格管理 API 的更改 7
用于更改 BMC 密码和 LAN IP 设置的新端点 7
StorageGRID 中租户管理 API 的更改 8
用于对象复制的新 API 8
对 StorageGRID S3 REST API 支持的更改 8
开始使用StorageGRID系统 13
了解StorageGRID 13
什么是 StorageGRID？ 13
采用 StorageGRID 的混合云 14
StorageGRID 架构和网络拓扑 15
网格节点和服务 19
StorageGRID 如何管理数据 29
探索StorageGRID 41
网络连接准则 48
StorageGRID 网络准则 48
StorageGRID 网络类型 49
网络拓扑示例 53
StorageGRID 的网络要求 59
StorageGRID 的网络特定要求 61
部署特定的网络注意事项 62
StorageGRID 的网络安装和配置 65
StorageGRID 安装后指南 66
网络端口参考 66

StorageGRID 快速入门 73
安装、升级和修复StorageGRID 76
安装 StorageGRID 节点 76
了解 StorageGRID 设备硬件 76
安装基于软件的节点 76
配置网格并完成安装 164
了解安装 StorageGRID 后所需的和可选的步骤 176
升级 StorageGRID 软件 177
升级 StorageGRID 软件 177
规划和准备升级 178
升级软件 183
对 StorageGRID 升级问题进行故障排除 198
应用StorageGRID修补程序 200
StorageGRID 热修补程序操作步骤 200
应用修补程序时如何影响 StorageGRID 201
获取 StorageGRID 修补程序所需的材料 202
下载 StorageGRID 修补程序文件 202
在应用 StorageGRID 修补程序之前检查系统状况 203
在 StorageGRID 中应用热修复 203
配置和管理StorageGRID系统 208
管理 StorageGRID 208
StorageGRID 管理快速入门 208
开始使用Grid Manager 209
控制对 StorageGRID 的访问 234
使用网格联盟 301
管理安全性 345
管理租户 406
配置客户端连接 424
管理网络和连接 461
管理存储节点 479
管理管理节点 491
使用 ILM 管理对象 493
使用 ILM 在 StorageGRID 中管理对象 493
ILM 和对象生命周期 493
在 StorageGRID 中创建和分配存储等级 513
使用存储池 515
使用云存储池 523
在 StorageGRID 中管理纠删编码配置文件 540
为StorageGRID配置 S3 区域 543
创建 ILM 规则 544
管理ILM策略 559

在 StorageGRID 中使用 ILM 策略和 ILM 规则 574
使用 S3 对象锁定 578
ILM 规则和策略示例 585
StorageGRID 系统加固 605
了解 StorageGRID 的系统加固 605
StorageGRID 软件升级的强化准则 605
StorageGRID 网络强化准则 606
StorageGRID 节点的强化准则 607
StorageGRID 中 TLS 和 SSH 的强化准则 610
StorageGRID 中日志、密码和审核消息的加固准则 611
StorageGRID 与 FabricPool 613
使用 StorageGRID 与 FabricPool 的配置工作流程 613
将 StorageGRID 作为 FabricPool 云层连接所需的信息 614
使用FabricPool 设置向导 615
手动配置StorageGRID 628
配置 ONTAP System Manager 以将 StorageGRID 添加为 FabricPool 云层 637
使用 FabricPool 为 StorageGRID 配置 DNS 服务器条目 638
适用于FabricPool 的StorageGRID 最佳实践 639
从StorageGRID中删除FabricPool数据 642
使用StorageGRID租户和客户端 644
使用租户帐户 644
使用 StorageGRID 租户帐户 644
如何登录和注销 645
StorageGRID 中的租户管理器信息板 647
租户管理 API 649
使用网格联合连接 654
管理组和用户 663
管理 S3 访问密钥 678
管理 S3 存储分段 683
管理 S3 平台服务 709
使用S3 REST API 739
StorageGRID S3 REST API 支持的版本和更新 739
StorageGRID 中支持的 S3 API 请求 743
测试 StorageGRID S3 REST API 配置 762
StorageGRID 如何实施 S3 REST API 764
支持Amazon S3 REST API 778
StorageGRID自定义操作 826
管理访问策略 844
StorageGRID 审核日志中跟踪的 S3 操作 869
使用Swift REST API (使用寿命结束) 870
StorageGRID 中的 Swift REST API 支持 870

监控StorageGRID系统并对其进行故障排除 871
监控StorageGRID 系统 871
使用 AutoSupport 871
监控StorageGRID 系统 883
在 StorageGRID 中查看和管理信息板 883
查看节点页面 886
要定期监控的信息 913
管理警报 938
日志文件参考 969
配置日志管理和外部系统日志服务器 988
配置电子邮件服务器 1002
使用 SNMP 监控 1004
收集其他 StorageGRID 数据 1015
排除StorageGRID 系统故障 1028
对 StorageGRID 系统进行故障排除 1028
对对象和存储问题进行故障排除 1034
对 StorageGRID 中的元数据问题进行故障排除 1049
对 StorageGRID 中的证书错误进行故障排除 1051
对 StorageGRID 中的管理节点和用户界面问题进行故障排除 1053
对 StorageGRID 中的网络、硬件和平台问题进行故障排除 1056
对 StorageGRID 外部系统日志服务器错误消息进行故障排除 1064
了解 StorageGRID 中的负载均衡器缓存问题 1066
查看审核日志 1067
审核消息和日志 1067
审核消息如何通过 StorageGRID 系统移动到 audit.log 文件以进行保留 1067
从 StorageGRID 管理节点命令行访问审核日志文件 1070
了解 StorageGRID 中的审核日志文件轮换 1071
审核日志文件格式 1071
审核消息格式 1083
审核消息和对象生命周期 1087
审核消息 1094
扩展StorageGRID系统的容量或功能 1133
了解如何扩展您的StorageGRID系统 1133
扩张计划 1134
StorageGRID中复制数据的扩展规划 1134
StorageGRID中纠删码（EC）数据的扩展规划 1135
了解StorageGRID扩展后的 EC 重新平衡 1135
扩展指南 1139
StorageGRID中添加对象容量的指南 1139
StorageGRID元数据容量添加指南 1141
StorageGRID中添加网格节点的指南 1142

StorageGRID添加新站点的指南 1143
准备扩展您的StorageGRID系统 1144
下载并提取 StorageGRID 安装文件 1145
验证硬件和网络连接 1149
添加网格节点或站点 1150
向StorageGRID添加网格节点或新站点的工作流程概述 1150
在StorageGRID中添加或更新网格网络子网以进行扩展 1150
在StorageGRID中部署新的网格节点 1152
执行StorageGRID扩展 1155
添加存储卷 1159
向StorageGRID系统添加存储卷 1159
在StorageGRID中向 VMware 存储节点添加存储卷 1162
在StorageGRID中向 Linux 存储节点添加直连卷或 SAN 卷 1163
配置扩展系统 1167
在StorageGRID中配置新添加的节点和站点 1167
在StorageGRID扩展后，验证存储节点是否处于活动状态。 1168
将 Prometheus 指标复制到StorageGRID中的新管理节点 1168
将审计日志复制到StorageGRID中的新管理节点 1169
在向StorageGRID系统添加节点后，重新平衡纠删码数据。 1171
排查StorageGRID中的扩展错误 1174
维护StorageGRID系统 1175
StorageGRID 网格维护 1175
开始之前 1175
设备的维护过程 1175
下载 StorageGRID 恢复包 1175
停用节点或站点 1176
停用 StorageGRID 节点或站点 1176
停用节点 1176
停用站点 1190
重命名网格、站点或节点 1211
使用 StorageGRID 重命名过程 1211
添加或更新 StorageGRID 显示名称 1214
节点过程 1220
StorageGRID 节点维护程序 1221
在 StorageGRID 中移动 ADC 服务 1221
将 StorageGRID 存储节点转换为仅数据节点 1222
重新启动、关闭和电源过程 1223
端口重新映射过程 1235
服务器管理器过程 1238
网络过程 1247
更新 StorageGRID 网格网络的子网 1247

配置 IP 地址 1249
向现有节点添加接口 1266
在 StorageGRID 中配置 DNS 服务器 1270
修改单个 StorageGRID 节点的 DNS 配置 1271
管理 StorageGRID 中的 NTP 服务器 1273
为隔离的 StorageGRID 节点恢复网络连接 1274
主机和中间件过程 1275
将 StorageGRID 节点迁移到新的 Linux 主机 1275
在 StorageGRID 中配置 VMware 虚拟机自动重启 1278
恢复或更换节点 1279
StorageGRID 节点恢复的警告和注意事项 1279
恢复网格节点的前提条件 1279
托管多个网格节点的服务器发生故障时的节点恢复顺序 1279
已恢复节点的 IP 地址 1280
收集 StorageGRID 网格节点恢复所需的材料 1280
下载并提取 StorageGRID 安装文件 1281
选择 StorageGRID 节点恢复过程 1286
从存储节点故障中恢复 1286
从 StorageGRID 存储节点故障中恢复 1286
恢复设备存储节点 1287
从系统驱动器完好无损的存储卷故障中恢复 1300
从系统驱动器故障中恢复 1307
从管理节点故障中恢复 1318
StorageGRID 中的主管理节点或非主管理节点恢复 1318
使用相同的主管理节点从主管理节点故障中恢复 1318
使用非主管理节点从主管理节点故障中恢复 1326
从非主管理节点故障中恢复 1332
从网关节点故障中恢复 1339
替换 StorageGRID 网关节点 1339
选择 Start Recovery 以配置 StorageGRID 网关节点 1340
从归档节点故障中恢复 1341
从 StorageGRID 归档节点故障中恢复 1341
替换Linux节点 1341
替换 StorageGRID 中的 Linux 节点 1341
为 StorageGRID 部署新的 Linux 主机 1341
将 StorageGRID 节点还原到主机 1342
执行其他 StorageGRID 节点恢复步骤 1346
将 StorageGRID 中的 VMware 节点替换为恢复节点 1347
将 StorageGRID 中的 VMware 节点替换为 SG1000 或 SG100 1348
步骤 1：更换 VMware 节点 1349
步骤2：完成节点恢复 1353

将故障节点更换为服务设备 1354
将失败的 StorageGRID 节点替换为服务设备 1354
安装 StorageGRID 服务设备（仅限平台更改） 1354
准备 StorageGRID 设备以重新安装（仅更换平台） 1355
在服务设备上启动 StorageGRID 软件安装 1355
监控 StorageGRID 服务设备安装 1358
技术支持如何恢复 StorageGRID 站点 1359
StorageGRID解决方案和资源 1361
如何使用NetApp控制台管理StorageGRID 1362
法律声明 1363
版权 1363
商标 1363
专利 1363
隐私政策 1363
API 许可证 1363
开放源代码 1363

StorageGRID 12.1 软件文档

了解 StorageGRID 设备硬件

请转至 "StorageGRID 设备文档"以了解如何安装、配置和维护 StorageGRID 存储和服务设备。

发行说明

StorageGRID 12.1 中的新增功能

StorageGRID 12.1 引入了以下功能和功能更改。

有关最新 StorageGRID 12.1 版本中的修复问题和已知问题的详细信息，请参见 "StorageGRID 12.1 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。

容量

EC 再平衡现在使用可用空间

EC再平衡现在使用可用空间而不是已用空间。请参阅 "了解StorageGRID扩展后的 EC 重新平衡"。

元数据允许的空间

现在可以将允许的最大元数据值从 3.96 TB 增加到 7.92 TB。请参阅"允许的元数据空间"。

控制访问

使用 OIDC 的 SSO

您现在可以 "使用 OpenID Connect (OIDC) 在 StorageGRID 中设置单点登录 (SSO)"。

联邦

全局命名空间

您可以设置全局命名空间以允许租户跨多个 StorageGRID 系统访问存储桶。请参阅"了解全局命名空间"。

易管理性

自动移动 ADC 服务

"当需要满足 ADC 仲裁要求时"，当您"将存储节点转换为仅数据节点"或"停用存储节点"时，ADC 服务将自动移动。

主管理节点恢复

您可以从非主管理节点恢复任何节点。请参阅"从主管理节点故障中恢复"。

S3

在现有存储桶上启用 S3 对象锁定

启用现有存储桶的允许 S3 对象锁定设置后，S3 租户帐户现在可以为现有存储桶启用 S3 对象锁定。S3 租户帐户为现有存储桶启用 S3 对象锁定后，无法禁用它。

允许为启用了 **S3** 对象锁的存储桶进行复制

现在，您可以使用 CloudMirror 在启用了 S3 对象锁定的存储桶中复制对象。请参阅 "了解平台服务"。

为非空存储桶启用跨网格复制

现在，您可以为不为空的存储桶启用跨网格复制。请参见"跨网格复制的要求"。

S3 批量操作（仅限 **FPVR**）

您可以使用 S3 批处理操作来复制您计划为跨网格复制配置的启用版本控制的存储桶中的现有对象。

此功能需要 StorageGRID 12.1 的 FPVR 批准。要使用此功能，请联系您的客户代表。

非功能性 **S3 REST API** 标头

`If-Match` 和 `If-None-Match` 标头已被接受，但对于 S3 REST API xref:{relative_path}../s3/put-object.html["PutObject"] 、link:../s3/complete-multipart-upload.html["CompleteMultipartUpload"] 、link:../s3/put-object-copy.html["CopyObject"] 和 xref:{relative_path}../s3/operations-on-objects.html["DeleteObject"] 无效。

有关详细信息，请参阅 "对 StorageGRID S3 REST API 支持的更改"。

支持预先计算的校验和值

S3 REST SPI 现在支持预先计算的校验和值和 `x-amz-checksum-type`请求标头。请参阅"REST API 支持更新"。

安全性

多管理员验证

多管理员验证(MAV)有助于防止对 StorageGRID 系统进行意外或未经授权的更改。请参阅 "了解 StorageGRID 多管理员验证"。

FIPS 的安全策略更新

已更新 FIPS 严格策略条件。请参阅 "在管理 TLS 和 SSH 策略中选择安全策略"。

租户

帐户同步

account clone 功能现在是指特定租户帐户信息的一次性克隆。

Account sync 是一项新功能，允许您在一个或多个网格联合连接中在 StorageGRID 系统之间自动且连续地复制租户帐户、租户组、租户用户和 S3 访问密钥。请参阅 "了解 StorageGRID 中的帐户同步"。

Kafka 端点和 mTLS 身份验证

Kafka 端点现在支持相互传输层安全性 (mTLS)。请参阅"配置平台服务端点"。

最大桶数

StorageGRID 系统现在支持每个 S3 租户帐户最多 20,000 个存储桶。

升级

启用功能的时间增加了

在 StorageGRID 升级到版本 12.1 期间，启用功能的时间从不到五分钟增加到一小时。请参阅 "估计完成 StorageGRID 升级的时间"。

用户接口

BMC 设置页面

新的 BMC 设置选项卡已添加到 Grid Manager 中的节点页面，以允许重置 BMC 密码并更改 BMC LAN IP 设置。请参阅 "更改设备 BMC 密码" 和 "更改设备节点 BMC LAN IP 设置"。还添加了新的 API 端点以支持这些功能。请参阅 "用于更改 BMC 密码和 LAN IP 设置的新端点"。

电子邮件通知

网格管理器现在有一个通用电子邮件页面，用于配置和管理警报、AutoSupport 和多管理员验证 (MAV) 的电子邮件通知。请参阅 "配置电子邮件服务器"。

链路成本页面更新

StorageGRID 12.1 提供了更详细的链路成本信息和设置。请参阅 "管理链路成本"。

USB 端口控制

您可以通过 Grid Manager 启用或禁用 USB 端口。请参阅"通过 USB 端口控制远程访问"。

StorageGRID 中已删除或弃用的功能和特性

了解 StorageGRID 12.1.0 中已删除或弃用的特性和功能。在升级之前，请检查任何已删除或已弃用的功能是否会影响客户端应用程序或网格配置。

定义

已弃用
: 您*不应*在新的生产环境中使用此功能。现有生产环境可以继续使用此功能。

生命周期结束
: 支持此功能的上次发售版本。在某些情况下、此阶段可能会删除此功能的文档。

已删除

第一个*不*支持此功能的版本。

StorageGRID停止功能支持

在N+2主要版本中将删除已弃用的功能。例如、如果某个功能在版本N中已弃用(例如6.3)、则该功能的最后一个版本为N+1 (例如6.4)。当产品中不存在此功能时、版本N+2 (例如6.5)是第一个版本。

有关更多信息、请参见 "软件版本支持页面"。

在某些情况下、NetApp可能会比指示的时间更早地终止对特定功能的支持。

功能	已弃用	生命周期结束	已删除	早期文档的链接
AES-128 加密的全局 SSE 设置	12.1	12.2	12.3	从 StorageGRID 12.1.0 开始，已弃用对新存储的静态对象数据的 AES-128 加密支持。继续支持检索最初使用 AES-128 加密的存储对象。
报警，旧版（非 *Alerts*）	11.7	11.8	11.9	"报警参考(StorageGRID 11.8)"
归档节点支持	11.7	11.8	11.9	"停用归档节点的注意事项(StorageGRID 11.8)" 注意：开始升级之前，您必须： 1. 停用所有存档节点。请参阅 "网格节点停用(StorageGRID 11.8文档站点)"。 2. 从存储池和 ILM 策略中删除所有归档节点引用。请参阅 "NetApp知识库：《StorageGRID软件升级解决方案指南》"。
通过CIFS或Samba审核导出	11.1	11.6	11.7	
CLB服务	11.4	11.6	11.7	
Docker容器引擎	11.8	11.9	待定	不再支持将 Docker 作为纯软件部署的容器引擎。 Docker 将在未来的版本中被另一个容器引擎取代。请参阅"基于软件的节点的软件要求"了解当前支持的 Docker 版本列表。
电子邮件设置（旧版）	11.9	12.0	12.1	"为警报配置通知（旧系统）（StorageGRID 11.8）"

功能	已弃用	生命周期结束	已删除	早期文档的链接
NFS审核导出	11.8	11.9	12.0	"为NFS配置审核客户端访问(StorageGRID 11.8)"
端口重映射	12.0	12.1	12.2	
Swift API支持	11.7	11.9	12.0	"使用Swift REST API (StorageGRID 11.8)"
RHEL 8.8	11.9	11.9	12.0	
RHEL 9.0	11.9	11.9	12.0	
RHEL 9.2	11.9	11.9	12.0	
Ubuntu 18.04	11.9	11.9	12.0	
Ubuntu 20.04	11.9	11.9	12.0	
Debian 11	11.9	11.9	12.0	

另请参见：

- "对网格管理 API 进行的更改"
- "对租户管理 API 进行的更改"

StorageGRID 中网格管理 API 的更改

StorageGRID 12.1 使用网格管理 API 第 4 版。版本 4 弃用版本 3；但是，仍支持版本 1 、2 和 3。

> 您可以继续在 StorageGRID 中使用已弃用的管理 API 版本；但是，在未来的 StorageGRID 版本中，将移除对这些 API 版本的支持。升级到 StorageGRID 12.0 或更高版本后，您可以使用 `PUT /grid/config/management` API 停用已弃用的 API。

要了解更多信息，请访问"使用网格管理 API"。

用于更改 BMC 密码和 LAN IP 设置的新端点

已添加以下端点，以允许您"更改设备 BMC 密码"。

```
PUT /bmc-configuration/root-password
```

已添加以下端点，以允许您"更改或查看 BMC LAN IP 设置"。

`PUT /grid/bmc/{node-id}/lan-ip-config`

`GET /grid/bmc/{node-id}/lan-ip-config`

StorageGRID 中租户管理 API 的更改

StorageGRID 12.1 使用租户管理 API 的版本 4。版本 4 弃用版本 3；但是，仍支持版本 1、2 和 3。

> 您可以继续在 StorageGRID 中使用已弃用的租户管理 API 版本；但是，在未来的 StorageGRID 版本中，将移除对这些 API 版本的支持。升级到 StorageGRID 12.0 或更高版本后，您可以使用 `PUT /grid/config/management` API 停用已弃用的 API。

要了解更多信息，请访问"了解租户管理 API"。

用于对象复制的新 API

您可以使用 `/org/cross-grid-replication/{versionId}/replicate`用于在新配置了跨网格复制的现有存储桶上手动复制对象的 API。

对 StorageGRID S3 REST API 支持的更改

StorageGRID 使用的 S3 REST API 会定期更新。

版本	注释
12.1.0	• `If-Match` 根据您的 StorageGRID 配置， `If-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。 • `If-None-Match` 根据您的 StorageGRID 配置， `If-None-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-None-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。 • 为以下请求和支持的标头添加了对预先计算的校验和值的支持： ◦ CompleteMultipartUpload: `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` ◦ CreateMultipartUpload: `CRC32`, `CRC32C`,以及 `CRC64NVME`用于 `x-amz-checksum-algorithm` ◦ CopyObject: `CRC32`, `CRC32C`, `CRC64NVME`,以及 `SHA256`用于 `x-amz-checksum-algorithm` ◦ PutObject: `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` ◦ UploadPart: `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` • 添加了对 `x-amz-checksum-type`的支持，适用于 CreateMultipartUpload 和 CompleteMultipartUpload。 • 增加了对 `s3:x-amz-copy-source`策略条件键的支持。 • 允许在现有存储桶上启用 S3 对象锁定。
12.0	• 增加了对管理接口的跨域资源共享 (CORS) 支持，允许另一个域使用管理 API 访问StorageGRID中的数据。"了解更多信息。"。 • 添加了对 STS AssumeRole 和会话策略的支持。请参阅"会话策略示例"。您可以在租户组下设置 AssumeRole。

版本	注释
11.9	• 增加了对以下请求和支持的标头预先计算的SHA-256校验和值的支持。您可以使用此功能验证已上传对象的完整性： ◦ CompleteMultipartUpload： `x-amz-checksum-sha256` ◦ CreateMultipartUpload： `x-amz-checksum-algorithm` ◦ GetObject： `x-amz-checksum-mode` ◦ 标题对象： `x-amz-checksum-mode` ◦ ListParts ◦ PutObject： `x-amz-checksum-sha256` ◦ 上传部件： `x-amz-checksum-sha256` • 增加了网格管理员控制租户级别保留和合规性设置的功能。这些设置会影响S3对象锁定设置。 ◦ 分段默认保留模式和对象保留模式：监管或合规(如果网格管理员允许)。 ◦ 存储分段默认保留期限和对象保留截止日期：必须小于或等于网格管理员设置的最长保留期限所允许的值。 • 改进了对内容编码和流 `x-amz-content-sha256`值的支持 `aws-chunked`。限制： ◦ 如果存在、 `chunk-signature`则为可选且不经过验证 ◦ 如果存在、 `x-amz-trailer`则忽略内容
11.8	更新了S3操作的名称，使其与中使用的名称一致 "Amazon Web Services （AWS）文档： Amazon Simple Storage Service API 参考"。
11.7	• 已添加 "快速参考：支持的S3 API请求"。 • 增加了对将监管模式与S3对象锁定结合使用的支持。 • 增加了对GET对象和HEAD对象请求的StorageGRID专用响应标头的支持 `x-ntap-sg-cgr-replication-status`。此标头可提供跨网格复制的对象复制状态。 • 现在，选择对象内容请求支持镶木图对象。
11.6	• 增加了对在GET对象和HEAD对象请求中使用Request参数的支持 `partNumber`。 • 增加了对 S3 对象锁定的默认保留模式和存储分段级别的默认保留期限的支持。 • 增加了对策略条件密钥的支持 `s3:object-lock-remaining-retention-days`、用于设置对象允许的保留期限。 • 已将单个Put对象操作的最大_Recommended_大小更改为5 GiB (5、368、709、120字节)。如果对象大于 5 GiB ，请改用多部分上传。

版本	注释
11.5	• 增加了对管理存储分段加密的支持。 • 增加了对 S3 对象锁定和已弃用旧合规性请求的支持。 • 增加了对在版本控制的存储分段上使用删除多个对象的支持。 • 现在已正确支持此 `Content-MD5`请求标头。
11.4	• 增加了对删除存储分段标记，获取存储分段标记和放置存储分段标记的支持。不支持成本分配标记。 • 对于在 StorageGRID 11.4 中创建的分段，不再需要限制对象密钥名称以满足性能最佳实践。 • 增加了对事件类型分段通知的支持 `s3:ObjectRestore:Post`。 • 现在，多部件的 AWS 大小限制已强制实施。多部分上传中的每个部件必须介于 5 MiB 和 5 GiB 之间。最后一个部件可以小于 5 MiB 。 • 增加了对TLS 1.3的支持
11.3	• 增加了对使用客户提供的密钥（ SSI-C ）对对象数据进行服务器端加密的支持。 • 增加了对删除、获取和放置存储分段生命周期操作(仅限到期操作)以及响应标头的支持 `x-amz-expiration`。 • 更新了 PUT 对象， PUT 对象 - 复制和多部件上传，以说明在载入时使用同步放置的 ILM 规则的影响。 • 不再支持 TLS 1.1 密码。
11.2	增加了对用于云存储池的后对象还原的支持。增加了对在组和存储分段策略中使用 AWS 语法来处理 ARN ，策略条件密钥和策略变量的支持。仍支持使用 StorageGRID 语法的现有组和存储分段策略。 • 注意： * 在其他配置 JSON/XML 中使用 ARN/URN 的情况没有改变，包括在自定义 StorageGRID 功能中使用的情况。
11.1	增加了对跨源站资源共享(CORS)、用于S3客户端连接到网格节点的HTTP以及分段合规性设置的支持。
11.0	增加了对为存储分段配置平台服务（ CloudMirror 复制，通知和 Elasticsearch 搜索集成）的支持。此外、还增加了对存储分段的对象标记位置限制以及可用一致性的支持。
10.4	增加了对版本控制，端点域名页面更新，策略中的条件和变量，策略示例以及 PutOverwriteObject 权限的 ILM 扫描更改的支持。
10.3	增加了对版本控制的支持。
10.2	增加了对组和存储分段访问策略以及多部件副本（上传部件 - 复制）的支持。

版本	注释
10.1	增加了对多部分上传、虚拟托管式请求和 v4 身份验证的支持。
10.0	StorageGRID系统初步支持 S3 REST API。 _简单存储服务 API 参考_当前支持的版本是 2006-03-01。

有关详细信息，请参见 "S3 REST API 支持的版本和更新"。

开始使用StorageGRID系统

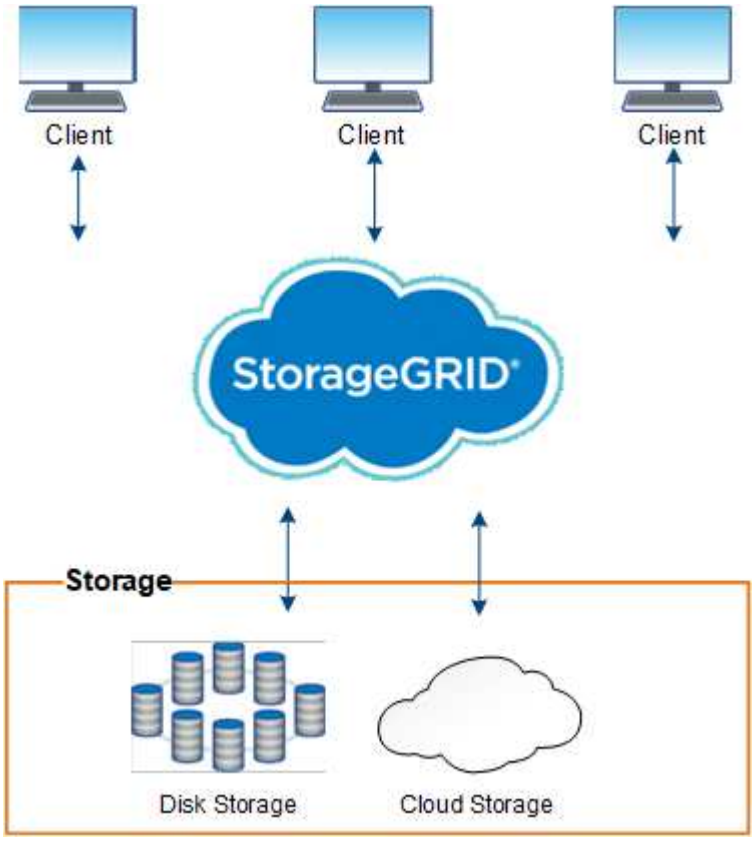
了解StorageGRID

什么是 StorageGRID ？

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

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

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



已删除对归档节点的支持。通过S3 API将对象从归档节点移动到外部归档存储系统已被取代"ILM云存储池"，后者提供了更多功能。

StorageGRID 的优势

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。

- Amazon Web Services 简单存储服务 (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 ）可将对象存储到公有 云，包括 Amazon Web Services （ AWS ）和 Microsoft Azure 。StorageGRID 平台服务支持对存储到公有 云的对象进行内容复制，事件通知和元数据搜索。
- 灵活的数据保护，可确保持久性和可用性。可以使用复制和分层纠删编码来保护数据。空闲和正在运行的数据验证可确保完整性，确保长期保留。
- 动态数据生命周期管理，有助于管理存储成本。您可以创建ILM规则、以便在对象级别管理数据生命周期、自定义数据位置、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，以及集成的负载平衡功能，可优化 StorageGRID 资源中的数据负载。
- 支持多个存储租户帐户，以便按不同实体隔离系统上存储的对象。
- 用于监控 StorageGRID 系统运行状况的众多工具，包括全面的警报系统，图形信息板以及所有节点和站点的详细状态。
- 支持基于软件或硬件的部署。您可以在以下任意位置部署 StorageGRID：
  - 在 VMware 中运行的虚拟机。
  - Linux 主机上的容器引擎。
  - StorageGRID工程设备。
    - 存储设备提供对象存储。
    - 服务设备可提供网格管理和负载平衡服务。
- 符合以下法规的相关存储要求：
  - 《证券和交易委员会（ SEC ）》，采用 17 § 240.17a-4 （ f ），用于监管交易所成员，代理或交易商。
  - 金融行业监管局（ FINRA ）规则 4511 （ c ），该规则符合 SEC 规则 17a-4 （ f ）的格式和介质要求。
  - 商品期货交易委员会（ CFTC ）在监管商品期货交易的第 17 条 CFR § 1.31 （ c ） - （ d ）条中进行了规定。
- 无中断升级和维护操作。在升级，扩展，停用和维护过程中保持对内容的访问。
- 联合身份管理。与 Active Directory、OpenLDAP 或 Oracle Directory Service 集成以进行用户身份验证。支持使用安全断言标记语言 2.0 (SAML 2.0) 或 OpenID Connect (OIDC) 的单点登录 (SSO)，以在 StorageGRID 与外部身份提供程序（例如 Active Directory Federation Services (AD FS)）之间交换身份验证和授权数据。

采用 **StorageGRID** 的混合云

在混合云配置中使用StorageGRID 、方法是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、并使用NetApp FabricPool 将数据从ONTAP 分层到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 Storage 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。

此外、还支持第三方配对存储、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

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。
- 事件通知服务将有关指定操作的消息发送到支持接收简单通知服务 (Amazon SNS) 事件的外部端点。
- 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 服务对数据执行分析。

使用**FabricPool** 进行**ONTAP** 数据层

您可以使用 FabricPool 将数据分层到 StorageGRID ，从而降低 ONTAP 存储的成本。FabricPool 支持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通过自动化数据分层来降低存储成本，从而降低总体拥有成本。它通过分层到公共云和私有云（包括StorageGRID）来提供云经济的优势。

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上的多种类型的网格节点组成。

了解"网格节点类型"。

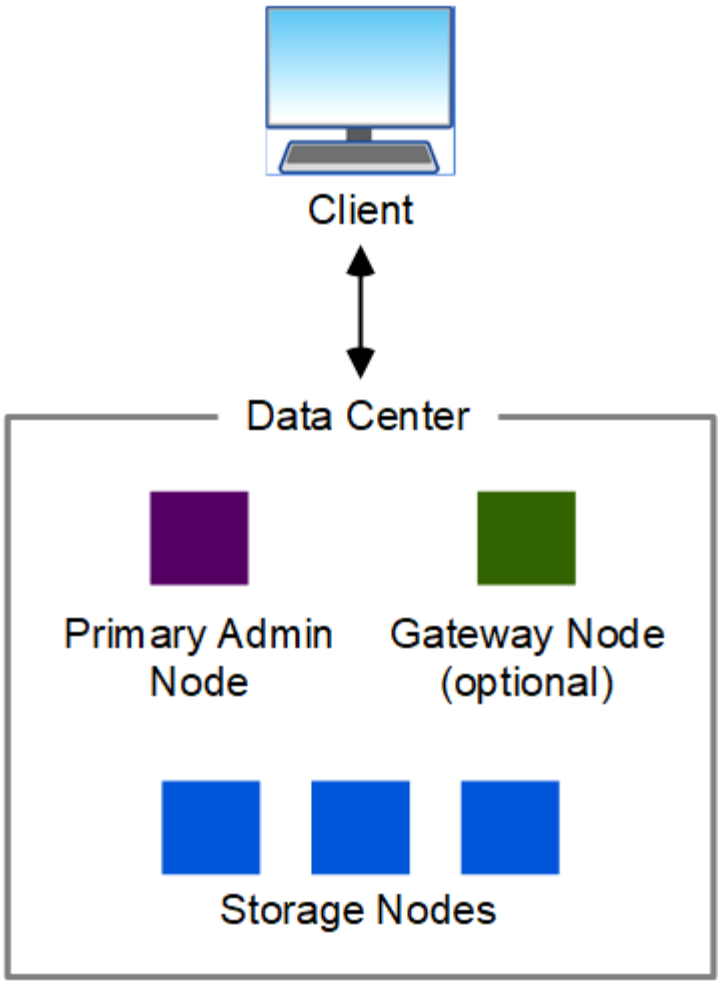
有关 StorageGRID 网络拓扑、要求和网格通信的其他信息，请参阅 "网络连接准则"。

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。每个部署的最大站点数为 16 个。

单个站点

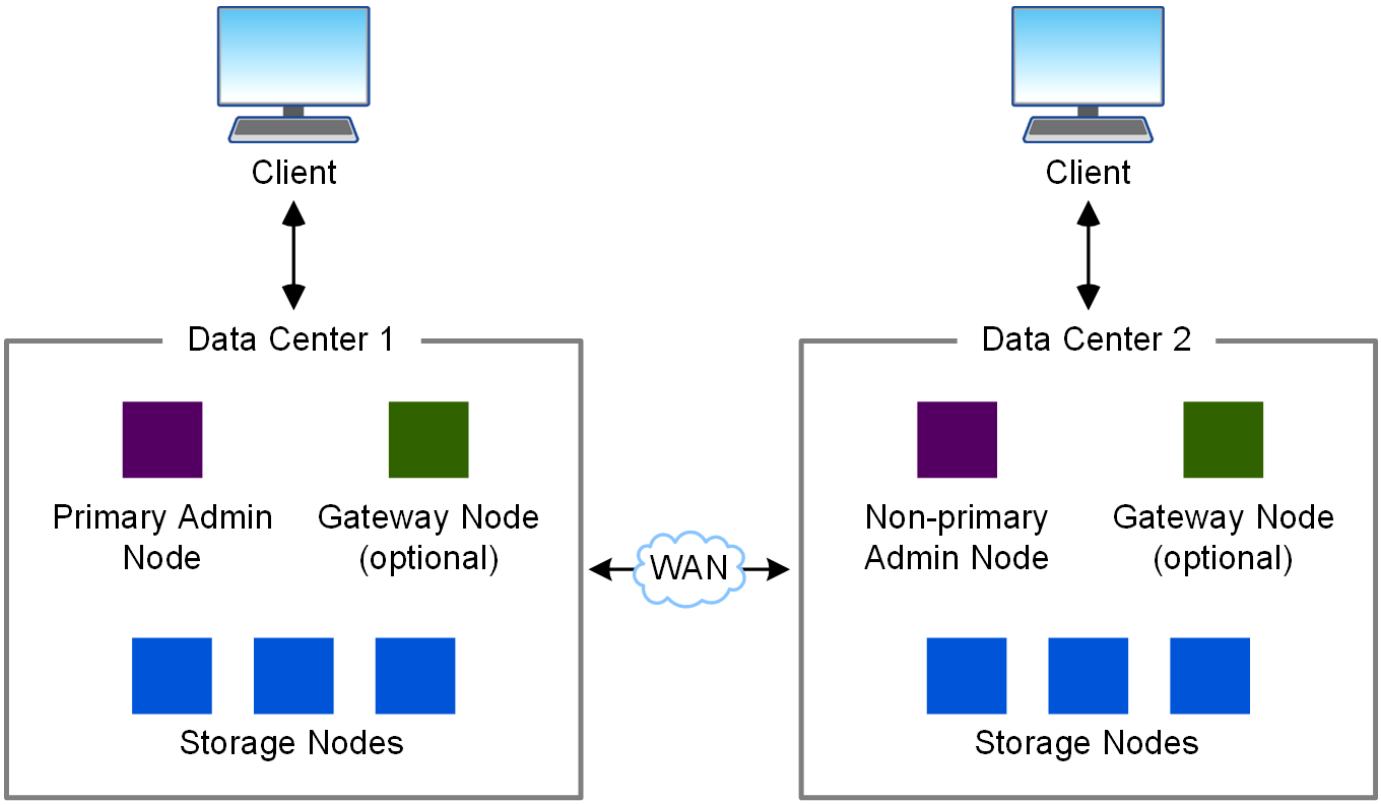
在使用单个站点的部署中， StorageGRID 系统的基础架构和操作会集中进行。



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。

站点通常位于不同故障域的地理位置，例如地震断层线或洪泛区。通过将数据自动分发到其他站点，实现数据共享和灾难恢复。



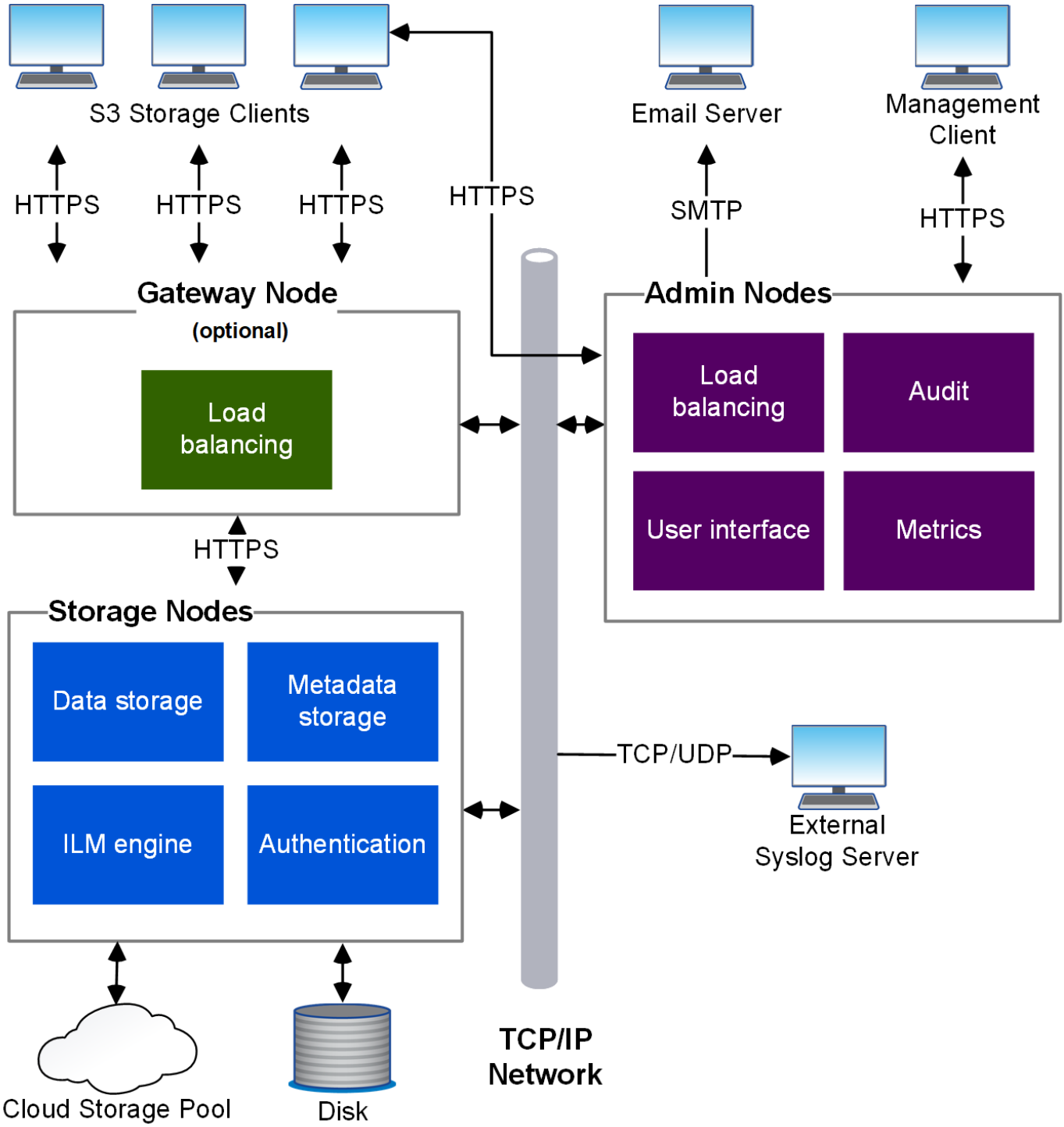
单个数据中心内还可以存在多个逻辑站点，以允许使用分布式复制和擦除编码来提高可用性和弹性。

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 客户端在 StorageGRID 中存储和检索对象。其他客户端用于访问 StorageGRID 管理界面，也可用于访问审计共享。此外，StorageGRID 可以选择通过外部 SMTP 服务器发送电子邮件警报。

S3客户端可以连接到网关节点或管理节点、以便对存储节点使用负载平衡接口。或者、S3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 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 Storage 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。

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、日志等管理服务。当您登录到 Grid Manager 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，您必须使用主管理节点执行大多数维护过程。

  管理节点还可用于对S3客户端流量进行负载平衡。

  请参见 "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具有三个存储节点。

  在新存储节点的初始安装过程中，您可以指定它仅用于 "存储元数据或数据"。

  请参见 "什么是存储节点？"

网关节点(可选)
: 提供一个负载平衡接口、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。

  请参见 "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。

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。

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 主机上的容器引擎内。看"在基于软件的节点上安装StorageGRID" 。

使用 "NetApp 互操作性表工具（ IMT ）"确定支持的版本。

StorageGRID 服务

以下是 StorageGRID 服务的完整列表。

服务	说明	位置
帐户服务提供商	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的负载平衡器服务
ADC (管理域控制器)	维护拓扑信息，提供身份验证服务，并响应 LDR 和 CMN 服务的查询。	每个站点至少有三个存储节点、其中包含ADC服务
AMS (审计管理系统)	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
Avahi 守护进程	处理 mDNS，用于本地网络内的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（仅数据除外）
Cassandra Reaper	自动修复对象元数据。	存储节点
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
CMN (配置管理节点)	管理系统范围的配置和网格任务。每个网格都有一个CMN服务。	主管理节点
DDS (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
DMV (数据移动器)	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	说明	位置
gdu-server	用于网格维护和配置操作的后端任务运行程序。接受来自 `mgmt-api`和其他实用程序脚本的请求，对其进行验证，并将每个操作发送到相应的 GDU 任务处理程序，例如设置、扩展、停用和升级。	管理节点
Grafana	用于在网格管理器中可视化指标。	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。	管理节点和网关节点
身份（ idnt ）	管理本地用户和组、身份验证并联合来自 LDAP 和 Active Directory 的用户身份。	使用ADC服务的存储节点
兰德仲裁员	管理 S3 Select SelectObjectContent 请求。	所有节点
负载平衡器(NGINS-GW)	提供从客户端到存储节点的S3流量的负载平衡。	管理节点和网关节点
LDR (本地分发路由器)	管理网格中内容的存储和传输。	存储节点
mgmt-api	网格管理器后端 API。公开用于管理网格（配置、监控和维护工作流程）的经过身份验证的 REST 端点，强制执行验证和权限，并协调长期运行的操作。网格管理器界面和自动化客户端使用的主控制平面 API。	管理节点
MISCd信息服务控制守护进程	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
nginx	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
nginx-gw 负载均衡器	提供从客户端到存储节点的S3流量的负载平衡。	管理节点和网关节点
NMS (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
节点导出器（Prometheus 数据收集）	发布 Prometheus 时间序列指标收集的系统级统计数据。	所有节点

服务	说明	位置
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新启动后持续存在的文件。	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)	确保平台服务请求发送到其各自的端点。	使用ADC服务的存储节点
SSM (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
追踪代理（jaeger-agent）	接收并处理跟踪收集器（jaeger-collector）提交的跟踪信息。	所有节点
跟踪收集器（jaeger-collector）	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。	管理节点

什么是 **StorageGRID** 管理节点?

管理节点可提供系统配置，监控和日志记录等管理服务。管理节点还可用于对S3客户端流量进行负载平衡。每个网格都必须有一个主管理节点，并且可能有任意数量的非主管理节点，以实现冗余。

主管理节点与非主管理节点之间的差异

当您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。

下表汇总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
包括SSM服务	是	是
包括负载平衡器和高可用性服务	是	是
支持管理应用程序程序接口(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NTP服务器更新	是	否
可以下载恢复包	是	是
可以在存储节点扩展后执行EC重新平衡	是	否
可用于卷还原操作步骤	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	是
发送警报通知、AutoSupport软件包和SNMP陷阱和通知	是。充当首选发件人。	是。用作备用发送器。

首选发件人管理节点

如果您的StorageGRID部署包含多个管理节点、则主管理节点是警报通知、AutoSupport软件包以及SNMP陷阱和通知的首选发送方。

在正常系统操作下，只有首选发送者发送通知。但是，所有其他管理节点都会监控首选发送者。如果检测到问题，其他管理节点将充当备用发送者。

在以下情况下可能会发送多条通知：

- 如果管理节点彼此"被拒"、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。

- 如果备用发送器检测到首选发送器出现问题并开始发送通知，则首选发送器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。当备用发送器不再检测到首选发送器上的错误时，它将停止发送通知。

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

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
[AMS]审计管理系统(AMS)	跟踪系统活动和事件。
配置管理节点(CMN)	管理系统范围的配置。
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。
负载平衡器	提供从客户端到存储节点的S3流量的负载平衡。 • 注： * 此服务也可在网关节点上找到。
管理应用程序接口(mgmt-api)	处理来自网格管理 API 和租户管理 API 的请求。
网络管理系统(NMS)	提供网格管理器的功能。
普罗米修斯	从所有节点上的服务收集和存储时间序列指标。
服务器状态监控器(SMS)	监控操作系统和底层硬件。

什么是 **StorageGRID** 存储节点？

存储节点可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具有三个存储节点。

存储节点的类型

在安装期间、您可以选择要安装的存储节点类型。以下类型可用于基于软件的存储节点和支持此功能的基于设备的存储节点：

- 数据和元数据组合存储节点
- 纯元数据存储节点

- 纯数据存储节点

在以下情况下、您可以选择存储节点类型：

- 首次安装存储节点时
- 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，所有新的存储节点都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。

纯元数据存储节点

如果网格存储大量小型对象、则将存储节点专用于元数据可能会很有意义。安装专用元数据容量可以在大量小型对象所需的空间与这些对象的元数据所需的空间之间实现更好的平衡。此外、高性能设备上托管的纯元数据存储节点可以提高性能。

纯元数据存储节点具有特定的硬件要求：

- 使用 StorageGRID 设备时，您只能在具有 12 个 1.9 TB 或 12 个 3.8 TB 驱动器的 SGF6112 设备上配置仅元数据节点。
- 使用基于软件的节点时，必须确保纯元数据节点资源与现有存储节点的资源匹配。例如：
  - 如果现有StorageGRID站点使用SG6000或SG6100设备、则基于软件的纯元数据节点必须满足以下最低要求：
    - 128 GB RAM
    - 8核CPU
    - 用于cassandr数据库的8 TB SSD或等效存储(rangedb/0)
  - 如果现有的StorageGRID站点使用具有 24 GB RAM、8 核 CPU 和 3 TB 或 4TB 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 4TB 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至少应与现有站点相匹配。新站点的资源应与现有站点的存储节点相匹配。

> 虽然纯元数据存储节点包含LDR服务、并可处理S3客户端请求、但StorageGRID性能可能不会提高。

纯数据存储节点

如果存储节点具有不同的性能特征、则将存储节点专用于数据可能会很有意义。例如、为了可能提高性能、您可以将纯数据、大容量旋转磁盘存储节点与纯元数据高性能存储节点结合使用。

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" 。

您可以将组合的存储节点转换为仅数据存储节点。如果存储节点包含ADC 服务，并且满足转换的先决条件，则在转换过程中，服务将自动移动到同一站点上的另一个存储节点。有关先决条件和详细步骤，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）：三个模数转换器存储节点（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（可以是任意组合或仅数据）
- 多站点网格：每个站点至少一个对象存储节点（可以是组合的，也可以是仅数据）

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。 仅数据存储节点不提供此服务。
管理域控制器 (ADC)	维护拓扑和网格范围的配置。 仅数据存储节点不提供此服务。 详细信息 管理域控制器（ADC-A）服务对网格节点及其彼此连接进行身份验证。ADC 服务至少托管在一个站点的三个存储节点上。 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。 为了便于分布式和孤岛式操作，每个 StorageGRID 服务会将证书，配置包以及有关服务和拓扑的信息与系统中的其他 ADE 服务进行同步。 通常，所有网格节点都会至少与一个 ADC 服务保持连接。这样可以确保网格节点始终访问最新信息。当网格节点连接时、它们会缓存其他网格节点的证书、从而使系统即使在ADC服务不可用的情况下也能继续使用已知的网格节点。新的网格节点只能通过使用模数转换器服务建立连接。 通过每个网格节点的连接，可以使此 ADA 服务收集拓扑信息。此网格节点信息包括 CPU 负载，可用磁盘空间（如果有存储），支持的服务以及网格节点的站点 ID 。其他服务则通过拓扑查询向此类服务请求拓扑信息。对于从 StorageGRID 系统收到的最新信息，此 ADA 服务会对每个查询做出响应。

服务	关键功能
Cassandra	存储和保护对象元数据。 仅数据存储节点不提供此服务。
Cassandra Reaper	自动修复对象元数据。 仅数据存储节点不提供此服务。
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。 详细信息 每个存储节点都包含分布式数据存储(DDS)服务。此服务与cassanda数据库连接、对存储在StorageGRID系统中的对象元数据执行后台任务。 DDS服务会跟踪StorageGRID系统中已插入的对象总数、以及通过每个系统支持的接口(S3)插入的对象总数。
身份（ idnt ）	从 LDAP 和 Active Directory 联合用户身份。 仅数据存储节点不提供此服务。

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_Comband_、_data-only _和_metadata-only _存储节点都包含本地分发路由器(LDR)服务。此服务负责处理内容传输功能、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 系统的大部分艰苦工作。 LDR 服务可处理以下任务： • 查询 • 信息生命周期管理（ ILM ）活动 • 对象删除 • 对象数据存储 • 从其他 LDR 服务（存储节点）传输对象数据 • 数据存储管理 • S3协议接口 LDR服务还会将每个S3对象映射到其唯一UUID。 对象存储 LDR 服务的底层数据存储分为固定数量的对象存储（也称为存储卷）。每个对象存储都是一个单独的挂载点。 存储在存储节点中的对象使用从 0000 到 002F 的十六进制数字进行标识，该数字称为卷 ID 。在第一个对象存储（卷 0 ）中预留空间用于 Cassandra 数据库中的对象元数据；该卷上的任何剩余空间用于对象数据。所有其他对象存储仅用于对象数据，其中包括复制的副本和经过纠删编码的片段。 为了确保复制的副本的空间使用量均匀，给定对象的对象数据会根据可用存储空间存储到一个对象存储中。当对象存储填满容量时、其余对象存储将继续存储对象、直到存储节点上没有更多空间为止。 元数据保护 StorageGRID 将对象元数据存储在与 LDR 服务连接的 Cassandra 数据库中。 为了确保冗余并防止丢失，每个站点维护三个对象元数据副本。此复制不可配置，并且会自动执行。有关详细信息，请参见 "管理对象元数据存储"。

服务	关键功能
复制状态机（ RSM ）	确保S3平台服务请求发送到其各自的端点。 仅数据存储节点不提供此服务。
服务器状态监控器（ SSM ）	监控操作系统和底层硬件。

什么是 **StorageGRID** 网关节点?

网关节点提供一个专用负载平衡接口、S3客户端应用程序可以使用此接口连接到StorageGRID。负载平衡通过在多个存储节点之间分布工作负载、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。它会终止客户端请求，检查请求并与存储节点建立新的安全连接。负载平衡器服务可以无缝地将客户端定向到最佳存储节点、这样、节点故障甚至整个站点的故障都是透明的。

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访问网关和管理节点上的负载平衡器服务所使用的端口和网络协议(HTTPS或HTTP)。负载平衡器端点还可以定义客户端类型(S3)、绑定模式以及允许或阻止的租户列表(可选)。请参阅。 "负载平衡注意事项"

您可以根据需要将多个网关节点和管理节点的网络接口分组为一个高可用性(HA)组。如果HA组中的活动接口发生故障、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服务；但是，此表并未列出所有节点服务。

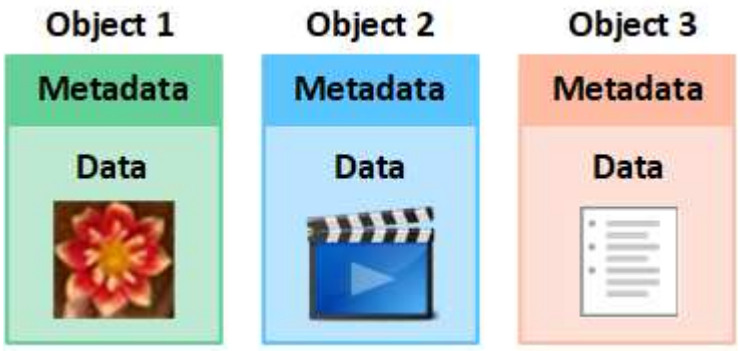
服务	关键功能
缓存服务	管理对象内容的本地缓存。
高可用性	管理管理节点和网关节点组的高可用性虚拟 IP 地址。 • 注： * 此服务也可在管理节点上找到。
负载平衡器	提供从客户端到存储节点的S3流量的第7层负载平衡。这是建议的负载平衡机制。 • 注： * 此服务也可在管理节点上找到。
服务器状态监控器（ SSM ）	监控操作系统和底层硬件。

StorageGRID 如何管理数据

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。



什么是对象数据?

对象数据可以是任何内容；例如，照片，电影或病历。

什么是对象元数据?

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

对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存储对象元数据的方式和位置的详细信息，请访问"管理对象元数据存储"。

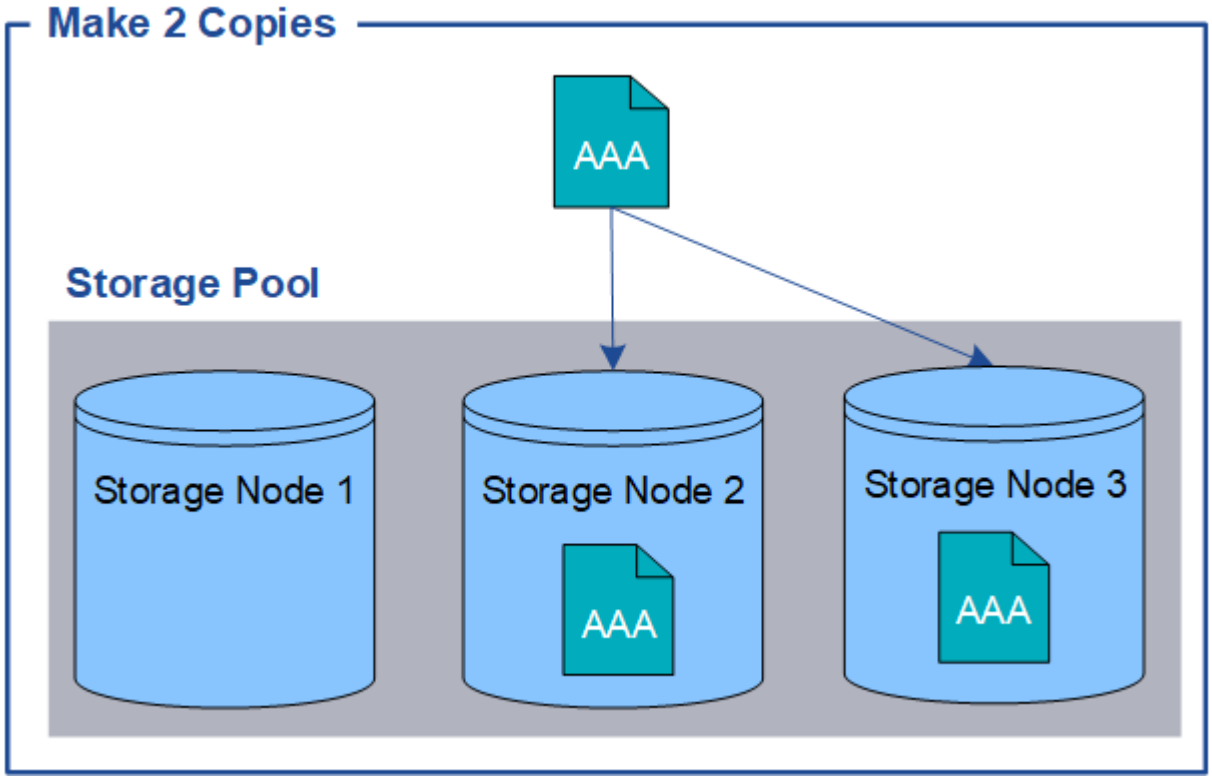
如何保护对象数据?

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。

复制

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)规则进行匹配、则系统会为对象数据创建准确的副本、并将其存储在存储节点或云存储池中。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。

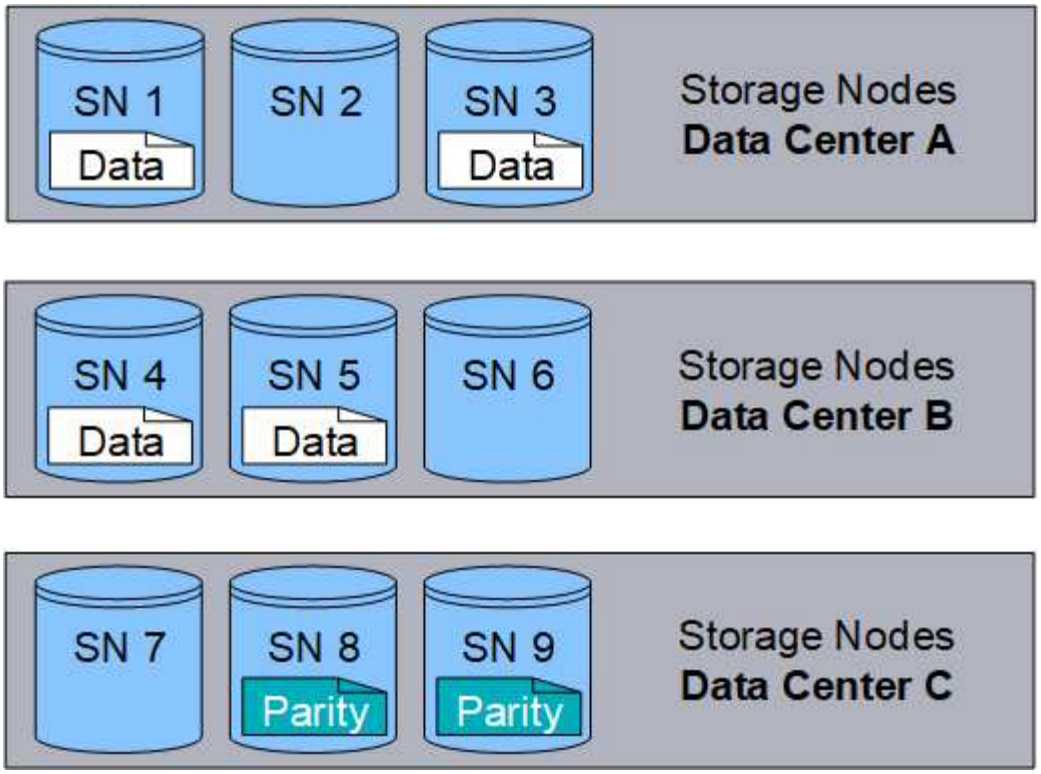
在以下示例中， make 2 copies 规则指定将每个对象的两个复制副本放置在包含三个存储节点的存储池中。



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"

StorageGRID 中的对象生命周期

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。

- **Ingesg**：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系统将开始管理此对象。
- 副本管理：按照活动ILM策略中的ILM规则所述、在StorageGRID中管理已复制和已删除编码副本的过程。在副本管理阶段、StorageGRID通过在存储节点或云存储池中创建和维护指定数量和类型的对象副本、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或云存储池中检索到的对象。
- * 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

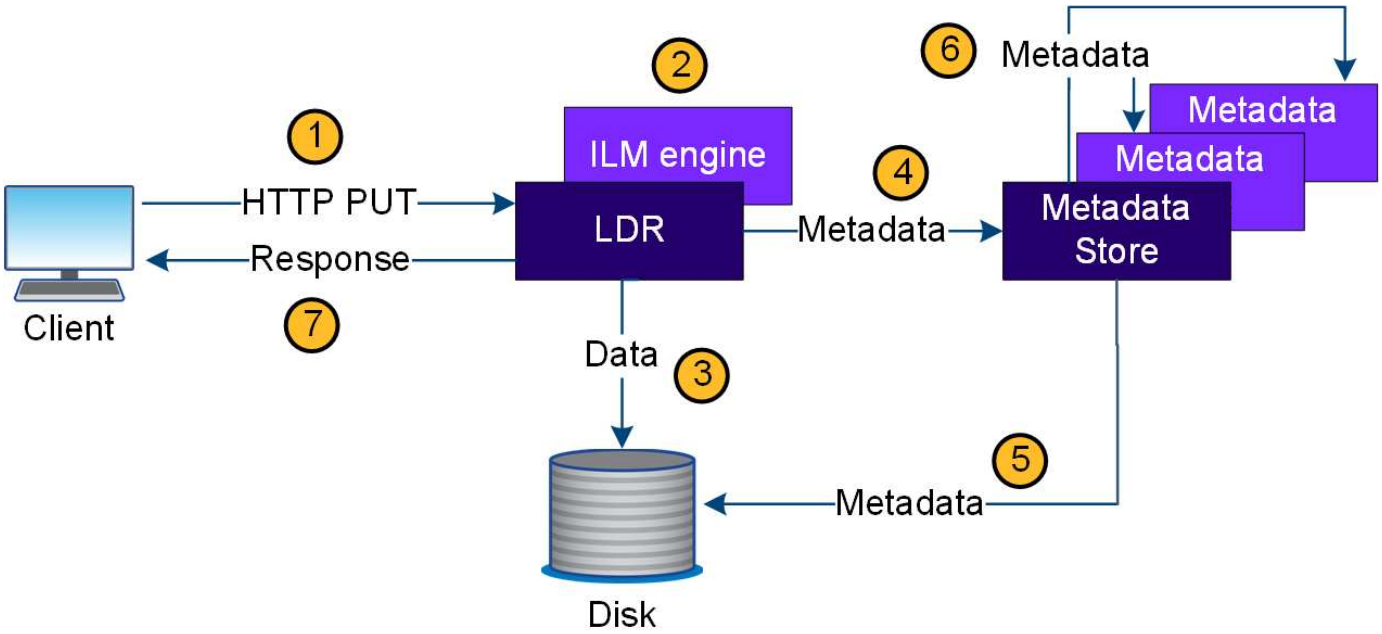
- "使用 ILM 管理对象"
- "使用信息生命周期管理"

StorageGRID 如何处理对象摄取

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

数据流

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



1. 客户端应用程序将创建此对象，并通过 HTTP PUT 请求将其发送到 StorageGRID 系统。
2. 将根据系统的 ILM 策略评估对象。
3. LDR服务将对象数据保存为复制副本或经过删除的副本。（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。

StorageGRID 如何管理对象副本

对象数据由活动ILM策略和关联ILM规则管理。ILM规则会创建复制或删除编码的副本、以防止对象数据丢失。

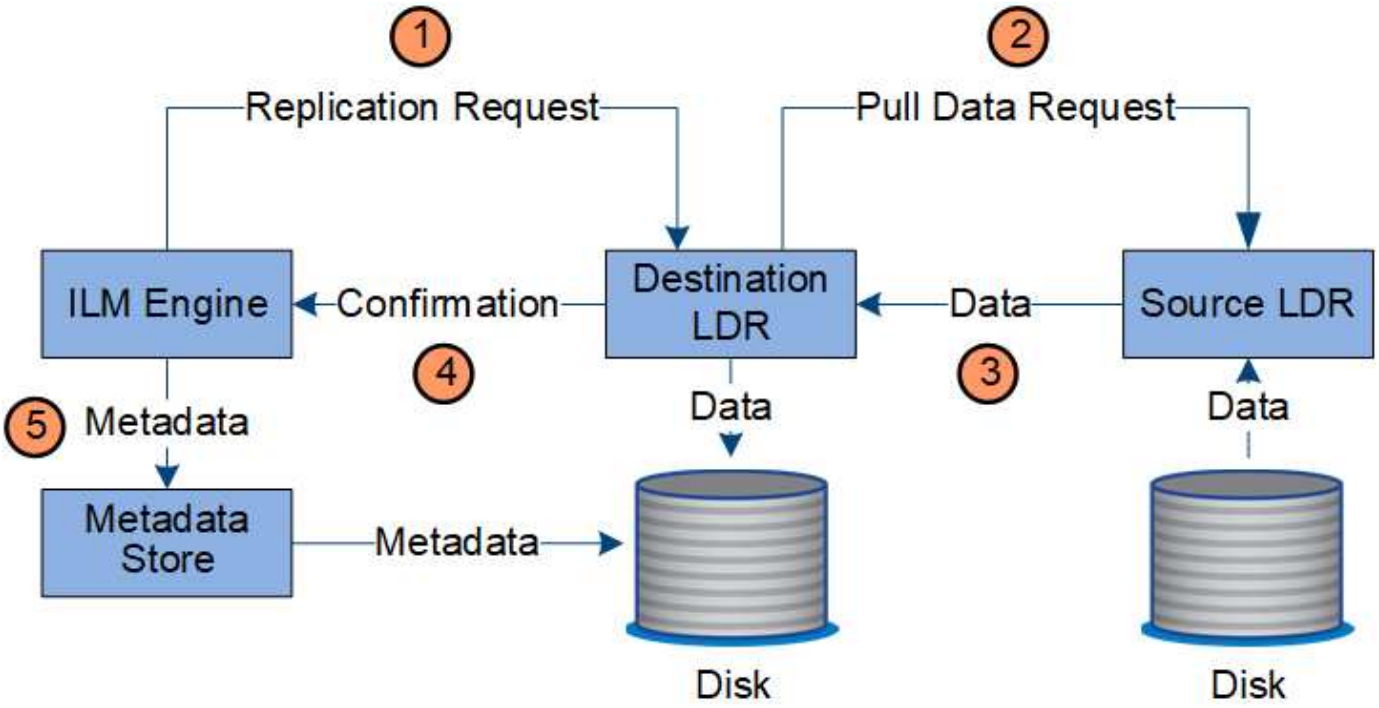
在对象生命周期的不同时间，可能需要不同类型或位置的对象副本。系统会定期评估 ILM 规则，以确保根据需要放置对象。

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。

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。

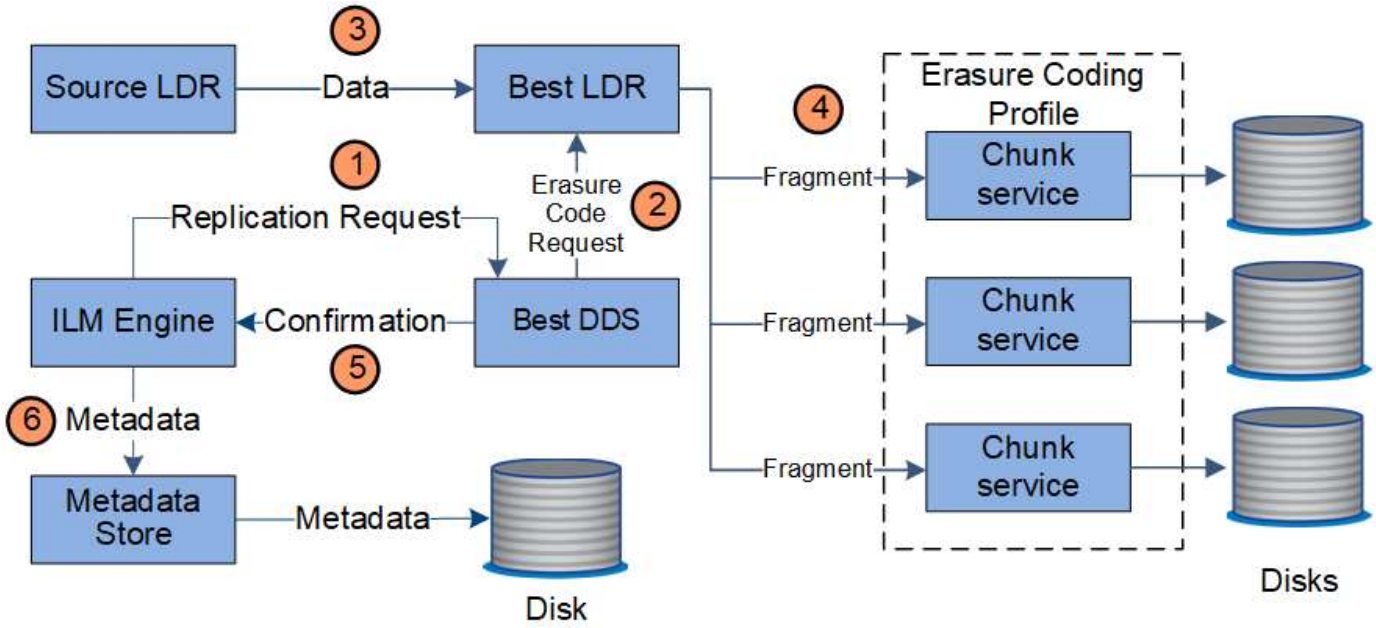


1. ILM 引擎会查询此 ADC-LDR 服务，以确定 ILM 规则指定的存储池中的最佳目标 LDR 服务。然后，它会向该 LDR 服务发送一个命令以启动复制。
2. 目标 LDR 服务会向此 ADC-Service 查询最佳源位置。然后，它会向源 LDR 服务发送复制请求。
3. 源 LDR 服务会向目标 LDR 服务发送一份副本。
4. 目标 LDR 服务通知 ILM 引擎已存储对象数据。
5. ILM 引擎使用对象位置元数据更新元数据存储。

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纠删编码配置文件中配置的存储节点上。

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。

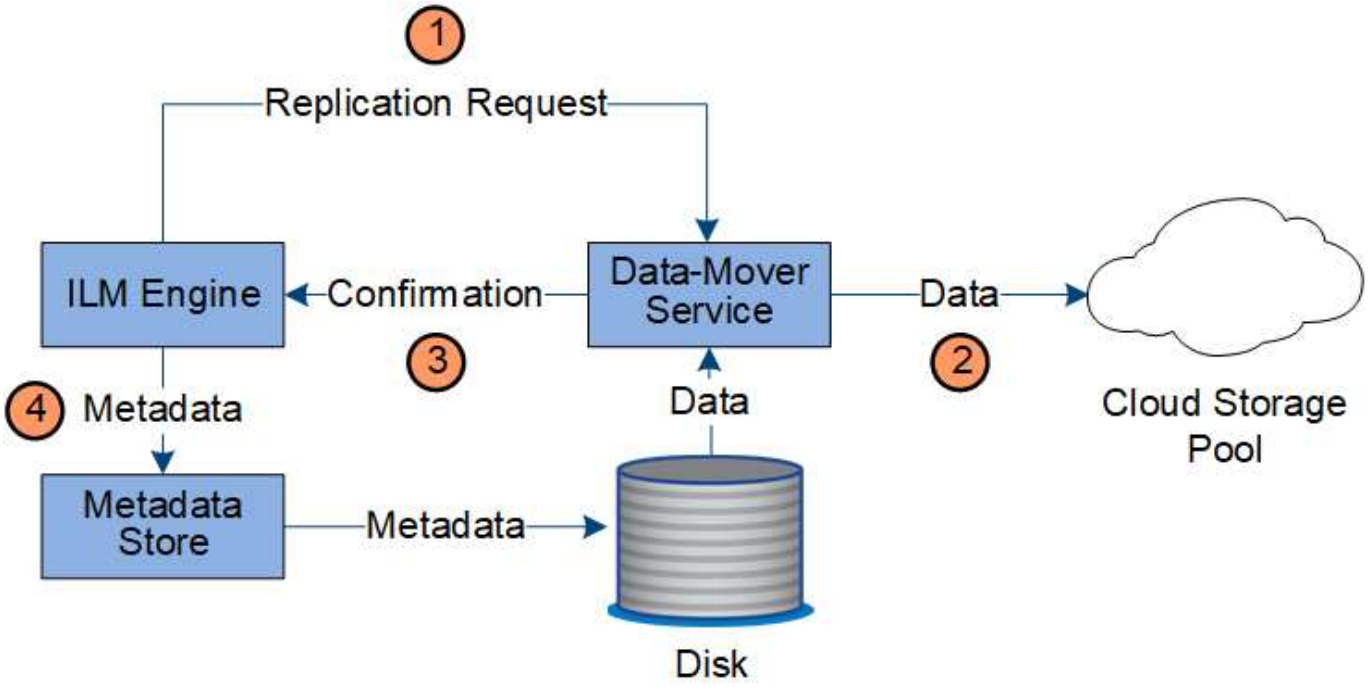


1. ILM 引擎会查询此 ADC-Service ，以确定哪种 DDS 服务能够以最佳方式执行纠删编码操作。确定后、ILM 引擎会向该服务发送"启动"请求。
2. DDS 服务指示 LDR 对对象数据进行纠删编码。
3. 源 LDR 服务会向选定用于纠删编码的 LDR 服务发送一份副本。
4. 创建适当数量的奇偶校验和数据片段后、LDR服务会将这些片段分布在构成纠删编码配置文件存储池的存储节点(区块服务)之间。
5. LDR 服务通知 ILM 引擎，确认对象数据已成功分发。
6. ILM 引擎使用对象位置元数据更新元数据存储。

内容保护：云存储池

如果 ILM 规则的内容放置说明要求对象数据的复制副本存储在云存储池中，则对象数据会复制到为云存储池指定的外部 S3 存储桶或 Azure Blob 存储容器。

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。



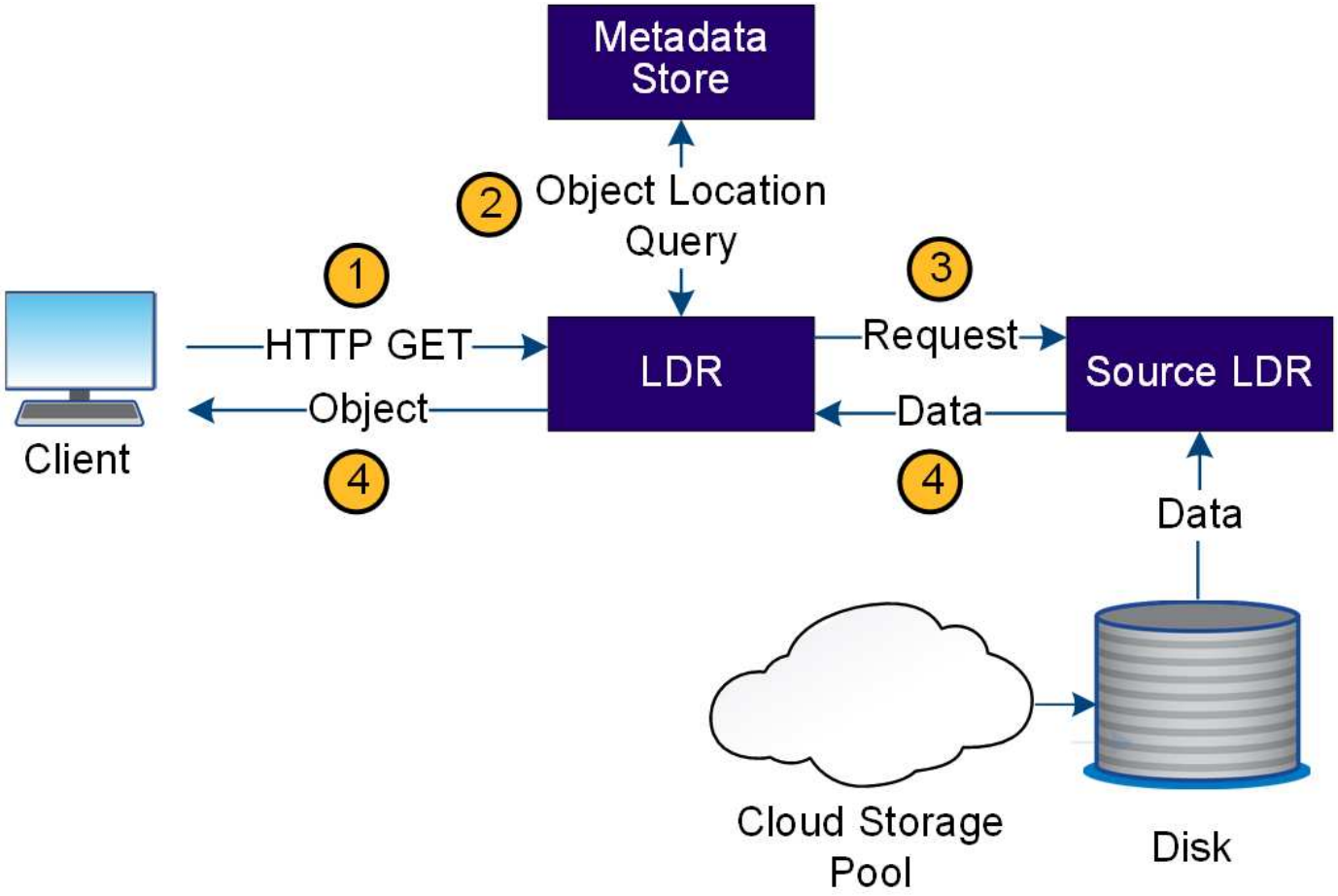
1. ILM 引擎选择要复制到云存储池的数据转换服务。
2. Data Mover 服务会将对象数据发送到云存储池。
3. Data Mover 服务会通知 ILM 引擎已存储对象数据。
4. ILM 引擎使用对象位置元数据更新元数据存储。

StorageGRID 如何处理对象检索

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(如有必要)检索对象的情况。

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、检索请求将定向到云存储池。

如果唯一的对象副本位于AWS GlacierStorage或Azure归档层上、则客户端应用程序必须发出问题描述a S3 Restore-Object请求、才能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服务将检索到的对象数据返回到查询的LDR服务，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。
  - 无法通过任何方法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、任何方法都无法删除该版本。

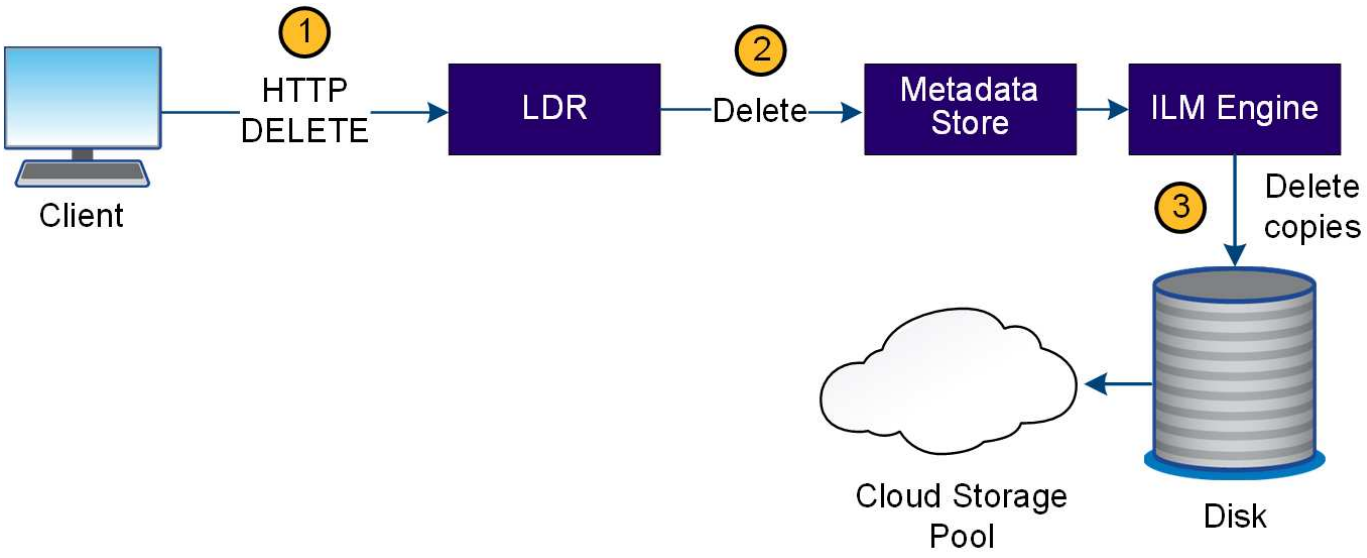
- 启用了S3对象锁定的分段中的对象将由ILM "永久"保留。但是，在达到保留截止日期后，可以通过客户端请求或存储分段生命周期到期来删除对象版本。
- 如果S3客户端对存储分段应用默认的保留截止日期、则无需为每个对象指定保留截止日期。

- 客户端删除请求：S3客户端可以发出删除对象请求。当客户端删除某个对象时，该对象的所有副本都会从 StorageGRID 系统中删除。
- 删除存储分段中的对象：租户管理器用户可以使用此选项从StorageGRID 系统中永久删除选定存储分段中的对象和对象版本的所有副本。
- * 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。

> 配置S3存储分段生命周期后、对于与生命周期筛选器匹配的对象、生命周期到期操作将覆盖ILM策略。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。

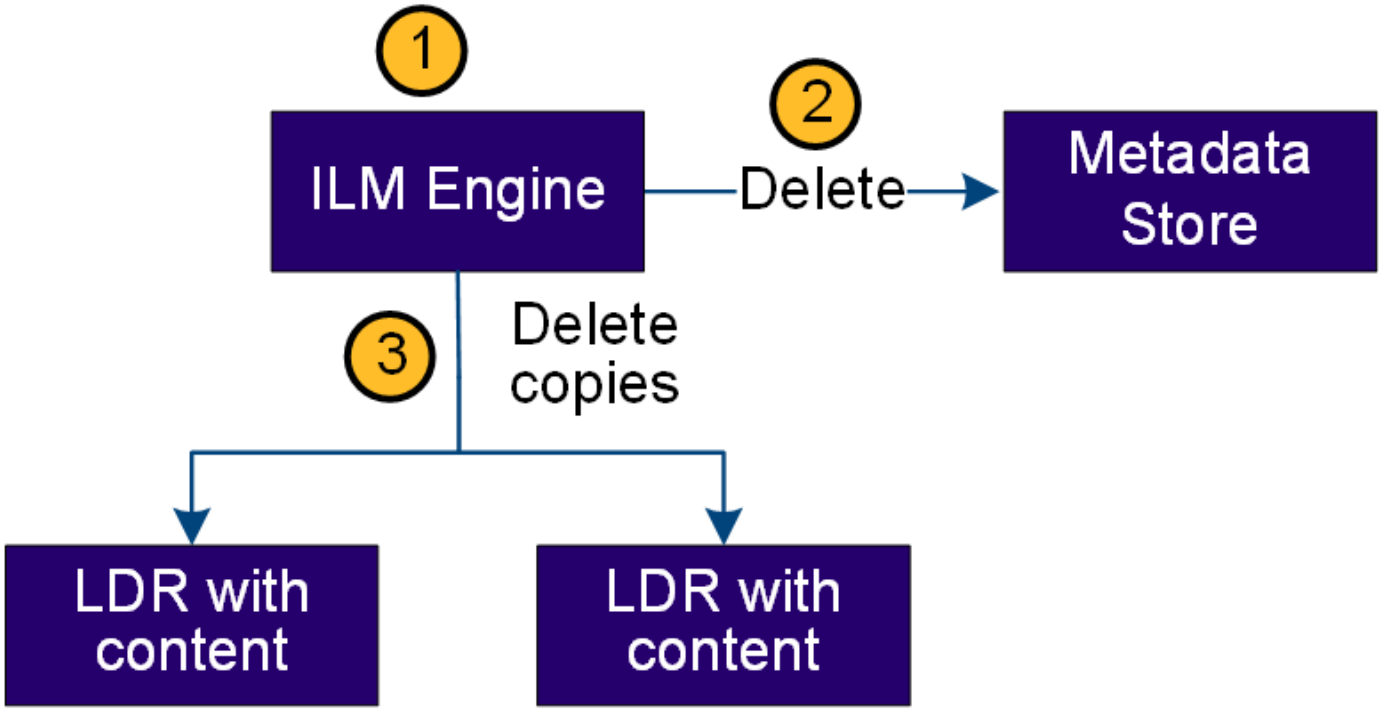
有关详细信息、请参见 "如何删除对象" 。

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。

StorageGRID 中的信息生命周期管理

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、持续时间和摄取行为。 ILM 规则决定了StorageGRID如何随时间存储对象。您可以配置一个或多个 ILM 规则，然后将它们添加到 ILM 策略。一个网格可以同时具有多个活动策略。

ILM 规则定义：

- 应该存储哪些对象。规则可以应用于所有对象，或者您可以指定过滤器来确定规则适用于哪些对象。例如，规则只能应用于与特定租户帐户、特定 S3 存储桶或特定元数据值相关联的对象。
- 存储类型和位置。对象可以存储在存储节点或云存储池中。
- 创建的对象副本的类型。可以复制副本或对副本进行删除编码。
- 对于复制的副本，为创建的副本数。
- 对于纠删编码的副本、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。

ILM 规则示例

例如、ILM规则可以指定以下内容：

- 仅应用于属于租户A的对象
- 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。
- 将这两个副本保留为"永久"、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。
- 使用均衡选项进行加载行为：租户A将对象保存到StorageGRID 后立即应用双站点放置指令、除非无法立即创建两个所需的副本。

  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策略可控制所有对象的放置、持续时间和入射行为。

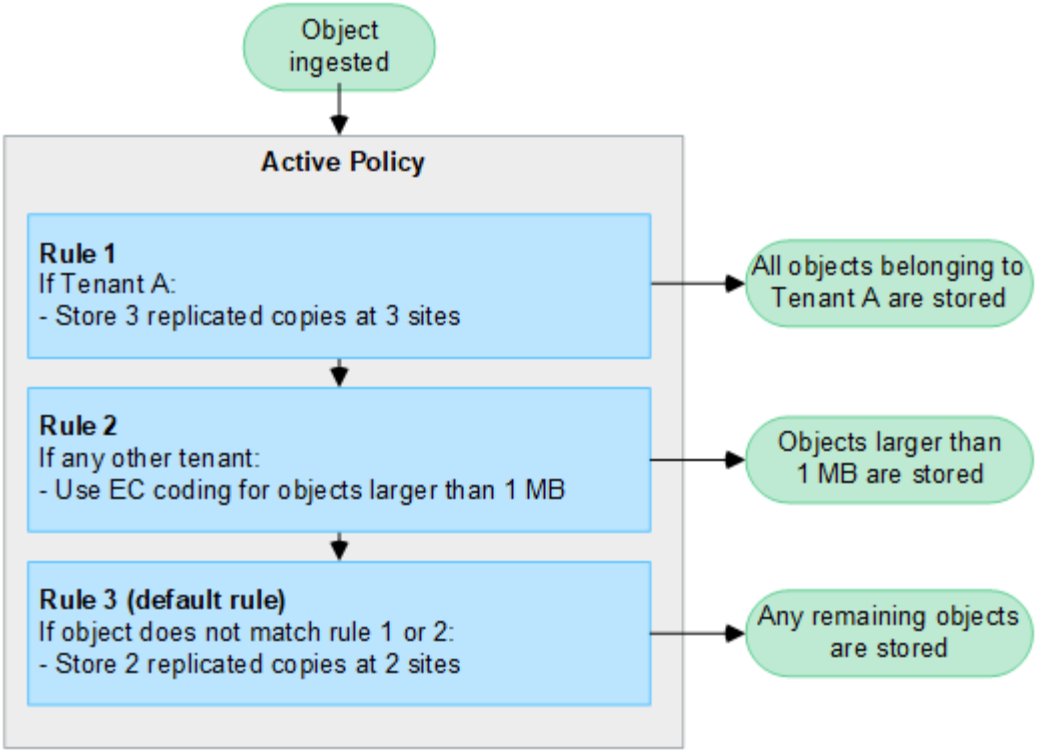
当客户端将对象保存到 StorageGRID 时，系统会根据活动策略中按顺序排列的一组 ILM 规则对这些对象进行评估，如下所示：

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、则系统将根据策略中的每个后续规则评估对象、直到进行匹配为止。
3. 如果没有与对象匹配的规则，则会应用策略中默认规则的载入行为和放置说明。默认规则是策略中的最后一个规则、不能使用任何筛选器。它必须应用于所有租户，所有分段和所有对象版本。

ILM 策略示例

例如、一个ILM策略可以包含三个ILM规则、这些规则可指定以下内容：

- *规则1：为租户A*复制的副本
  - 匹配属于租户A的所有对象
  - 将这些对象作为三个复制副本存储在三个站点上。
  - 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：对大于1 MB*的对象进行纠删编码
  - 匹配其他租户的所有对象、但前提是这些对象大于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。
  - 与小于或等于1 MB的对象不匹配、因此将根据规则3评估这些对象。
- 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。不使用筛选器。
  - 为规则1或规则2不匹配的所有对象创建两个复制副本(不属于租户A且小于或等于1 MB的对象)。



相关信息

- "使用 ILM 管理对象"

探索StorageGRID

浏览 **StorageGRID** 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。

Grid Manager随每个版本更新、可能与此页面上的示例屏幕截图不匹配。

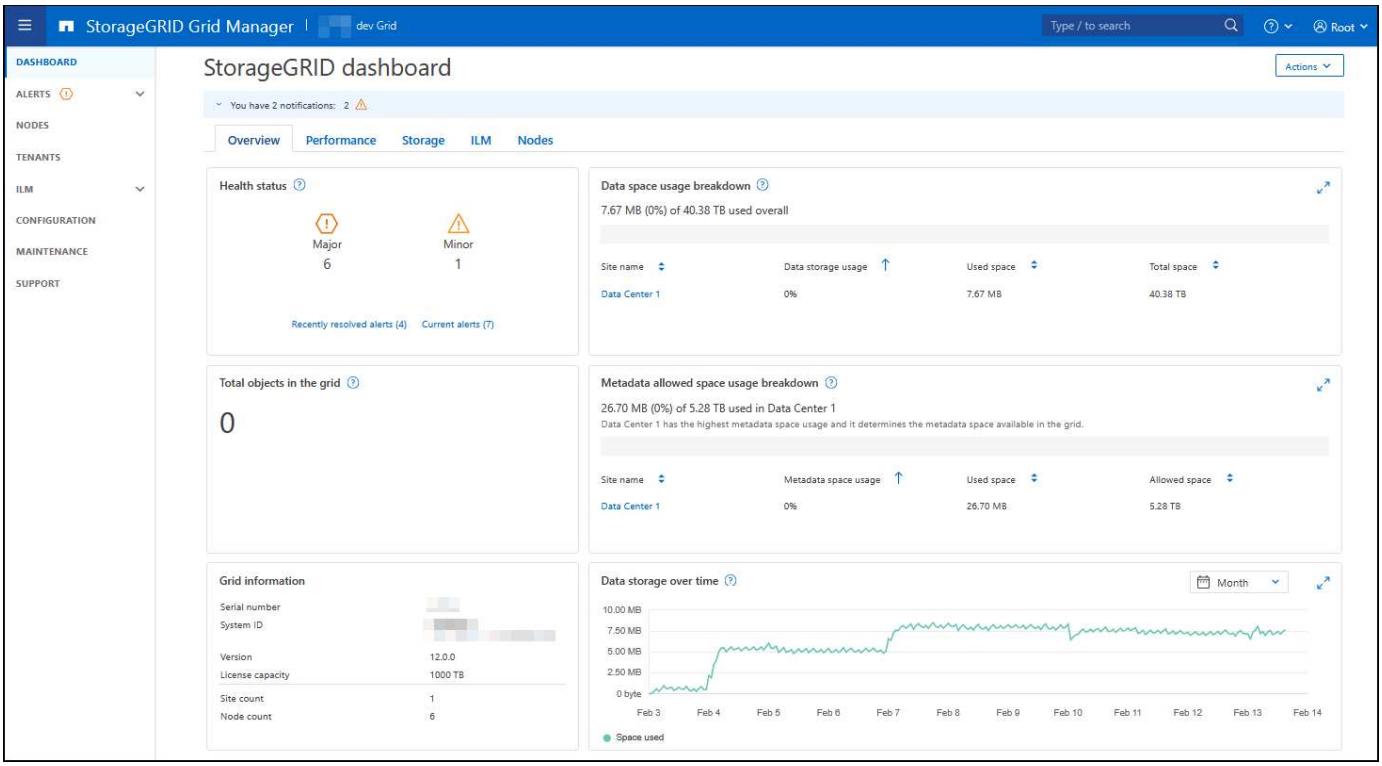
登录到网格管理器后，您将连接到管理节点。每个 StorageGRID 系统都包括一个主管理节点和任意数量的非主管理节点。您可以连接到任何管理节点，每个管理节点都会显示一个类似的 StorageGRID 系统视图。

您可以使用访问网格管理器"支持的 Web 浏览器"。

网格管理器信息板

首次登录网格管理器时、您可以使用信息板"监控系统活动"一目了然。

信息板包含有关系统运行状况和性能、存储使用情况、ILM进程、S3操作以及网格中节点的信息。您可以"配置信息板"从一组包含有效监控系统所需信息的卡中进行选择。



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 * 字段可用于快速导航到网格管理器中的特定页面。例如，您可以输入*KM*来访问密钥管理服务器(KMS)页面。

您可以使用 * 搜索 * 在网格管理器的边栏以及配置，维护和支持菜单中查找条目。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：

- 这"FabricPool"和"S3设置"巫师
- 当前版本的StorageGRID文档站点
- "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。

在“警报”菜单中，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
- 配置静音以禁止警报通知

- 为触发警报的条件定义警报规则
- 为 StorageGRID 警报配置电子邮件通知

节点页面

这"节点页面"显示有关整个网格、网格中每个站点以及站点上每个节点的信息。要查看特定站点或节点的信息，请选择该站点或节点。

租户页面

"租户页面"允许您"创建并监控存储租户帐户"为StorageGRID系统设置。您必须至少创建一个租户帐户，以指定谁可以存储和检索对象以及这些对象可以使用哪些功能。

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

ILM 菜单

"ILM 菜单"通过、您可以"配置信息生命周期管理(ILM)规则和策略"管理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。

从ILM菜单中、您可以查看和管理ILM：

- 规则
- 策略
- 策略标记
- 存储池
- 存储等级
- regions
- 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"
- "管理流量分类策略"
- "配置 VLAN 接口"
- "为管理接口启用StorageGRID CORS"

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"
- "配置密钥管理服务器"
- 配置安全设置，包括"TLS和SSH策略"，"网络和对象安全选项"，"接口安全设置"， 和"SSH 访问选项"
- 配置设置"存储代理"或"管理员代理"

系统任务

系统任务包括：

- 使用 "网格联盟" 在两个 StorageGRID 系统之间同步租户帐户信息和复制对象数据
- （可选）启用"压缩存储的对象"选项
- 或者，配置"默认桶一致性设置"
- "管理 S3 对象锁定"
- 了解存储设置，例如"存储卷水印"
- "管理纠删编码配置文件"

监控任务

监控任务包括：

- "配置电子邮件服务器"
- "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：

- "管理管理组"
- "管理管理员用户"
- 更改"配置密码短语"或者"节点控制台密码"
- "使用身份联合"
- "配置 SSO"
- "配置多管理员验证"

维护菜单

通过维护菜单，您可以执行维护任务，系统维护和网络维护。

任务

维护任务包括：

- "取消配置操作"删除未使用的网格节点和站点
- "扩展操作"添加新的网格节点和站点
- "网格节点恢复过程"以更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(尽管不是正确的)
- 执行"滚动重新启动"重新启动多个网格节点
- 还原对象数据
  - "将对象数据还原到设备的存储卷"
  - "将对象数据还原到系统驱动器完好无损的存储卷"
  - "将对象数据还原到存储卷(系统驱动器故障)"

系统

您可以执行的系统维护任务包括：

- "查看 StorageGRID 许可证信息"或者"更新许可证信息"
- 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、修补程序以及SANtricity OS软件更新
  - "升级操作步骤"
  - "修补程序操作步骤"
  - "使用网格管理器升级SG6000存储控制器上的SANtricity操作系统"
  - "使用网格管理器升级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。

工具

从支持菜单的工具部分，您可以：

- "配置 AutoSupport"
- "Run diagnostics" 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。

其他

从支持菜单的其他部分、您可以：

- 配置"I/O 优先级"
- 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"是一个基于浏览器的图形界面、租户用户可通过此界面来配置、管理和监控其存储帐户。

租户管理器会随每个版本更新、并且可能与此页面上的示例屏幕截图不匹配。

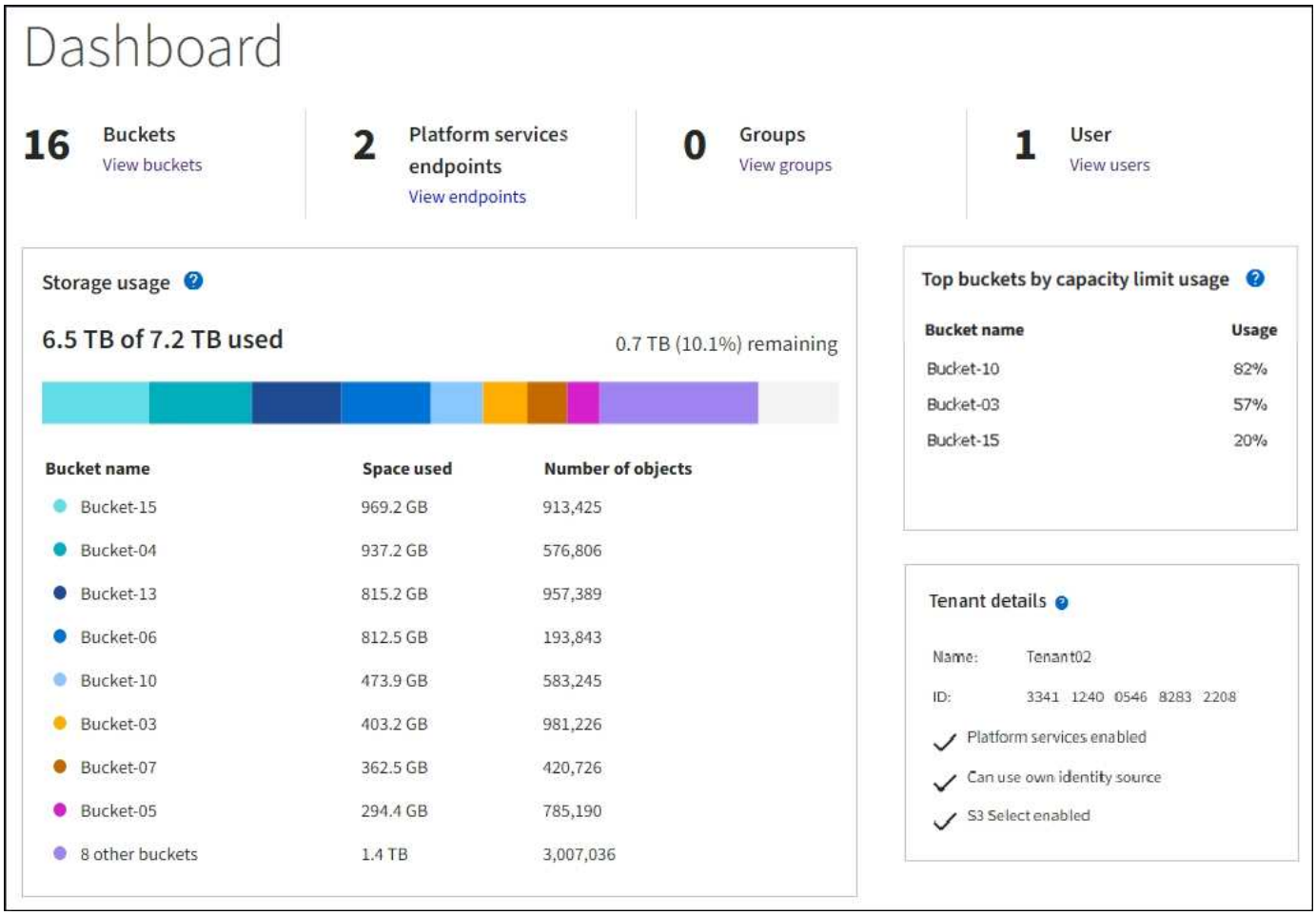
当租户用户登录到租户管理器时，他们将连接到管理节点。

租户管理器信息板

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

租户管理器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的 S3 存储桶列表。已用空间值是存储桶或容器中的对象数据总量。条形图表示这些桶或容器的相对大小。

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**(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
- 查看他们被允许使用的任何电网联合连接

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。

通过访问管理菜单可以管理其他用户的访问密钥。

存储分段

具有适当权限的S3租户用户可以对其分段执行以下任务：

- 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）
- 更新一致性值
- 启用和禁用上次访问时间更新
- 启用或暂停对象版本控制
- 更新S3对象锁定默认保留
- 配置跨源资源共享（ CORS ）
- 删除存储分段中的所有对象
- 删除空分段
- 使用"S3控制台"管理存储分段对象

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、此通知可发送到支持Amazon Simple Notification Service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。

网格联合连接

如果网格管理员为租户帐户启用了网格联合连接、则具有root访问权限的S3租户用户可以查看连接名称、并访问已启用跨网格复制的每个存储分段的存储分段详细信息页面、 并查看在将存储分段数据复制到连接中的另一个网格时发生的最新错误。请参阅。 "查看网格联合连接"

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 ）。

网络连接准则

StorageGRID 网络准则

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

关于这些说明

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

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

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

必须正确配置 StorageGRID 网络，才能处理这些功能等的流量。

开始之前

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

在配置网络连接之前，请熟悉中所述的StorageGRID架构"了解StorageGRID"。

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"

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

您可以通过以下方式配置网络：

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

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

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

网络接口

StorageGRID 节点使用以下特定接口连接到每个网络：

网络	接口名称
网格网络（必需）	eth0
管理网络（可选）	eth1
客户端网络（可选）	eth2

有关将虚拟或物理端口映射到节点网络接口的详细信息，请参阅"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"
- "SG8600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

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、则应使用IP地址作为网关地址。

高可用性组

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

网格网络

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

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

网格网络可用于所有管理流量和所有客户端流量，即使已配置管理网络和客户端网络也是如此。除非节点配置了客户端网络，否则网格网络网关是节点的默认网关。

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

请注意网格网络网关的以下要求和详细信息：

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

管理网络

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

您可以选择应在哪些网格节点上启用管理网络。

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

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

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

请注意管理网络网关的以下要求和详细信息：

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

客户端网络

客户端网络是可选的。配置后、它可用于为S3等客户端应用程序提供网格服务访问权限。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、节点将永远不会通过客户端网络彼此进行通信。网格安装完成后，客户端网络才会运行。

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

使用客户端网络时，客户端流量不需要通过网格网络传输。网格网络流量可以分隔到安全的不可路由网络上。以下节点类型通常配置有客户端网络：

- 网关节点、因为这些节点提供对StorageGRID负载平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、云存储池和CloudMirror复制服务的访问。
- 管理节点、以确保租户用户无需使用管理网络即可连接到租户管理器。

对于客户端网络网关，请注意以下事项：

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

可选 **VLAN** 网络

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

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

如果将 eth0 配置为中继，网格网络流量将按交换机上的配置流经中继原生 接口。同样，如果 eth2 配置为中继

，并且客户端网络也配置在同一节点上，则客户端网络将使用交换机上配置的中继端口的原生 VLAN 。

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

> 只能将 VLAN 接口添加到管理节点和网关节点。您不能使用VLAN接口进行客户端或管理员对存储节点的访问。

有关说明和准则、请参见"配置 VLAN 接口"。

VLAN 接口仅用于 HA 组，并在活动节点上分配 VIP 地址。有关说明和准则、请参见"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。

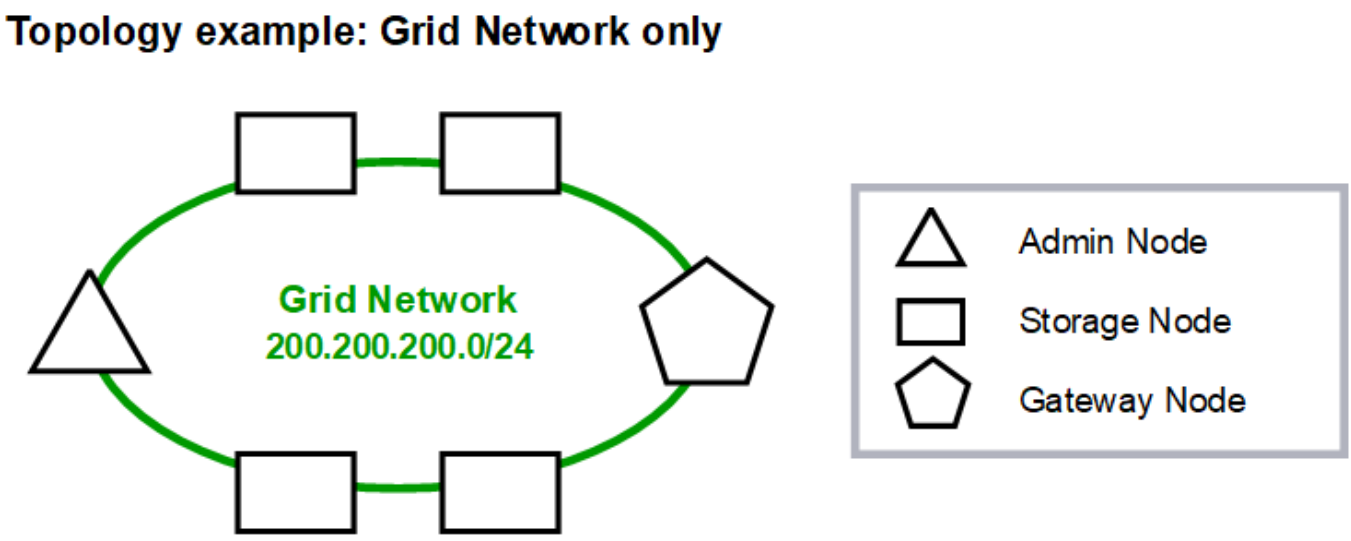
配置网格网络时，您需要为每个网格节点的 eth0 接口建立主机 IP 地址，子网掩码和网关 IP 地址。

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、或者第三方负载平衡器充当客户端访问边界的情况。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。



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

StorageGRID 的管理网络拓扑

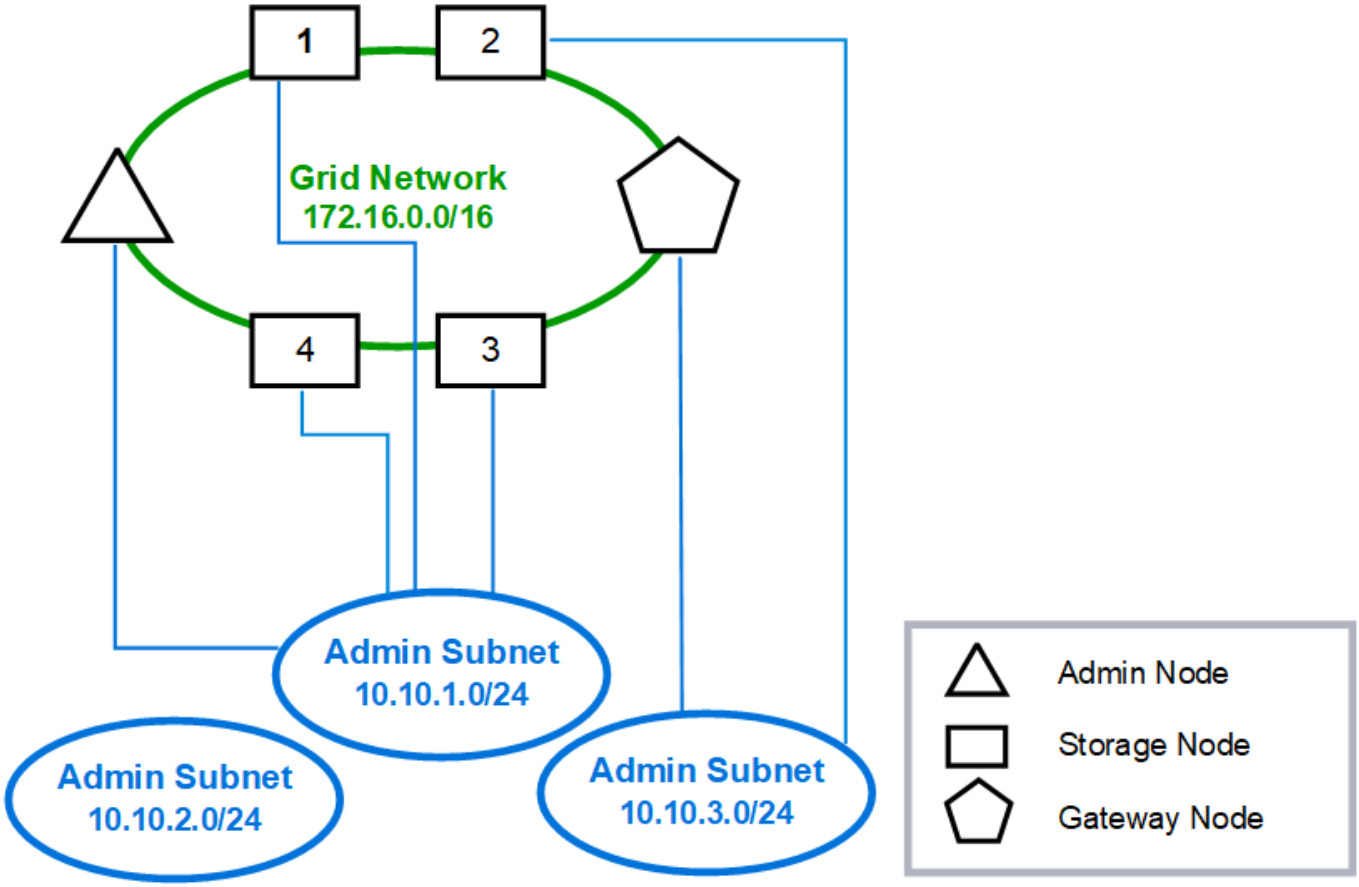
可以选择使用管理网络。使用管理网络和网格网络的一种方法是，为每个节点配置可路由的网格网络和有限制的管理网络。

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



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

StorageGRID 的客户端网络拓扑

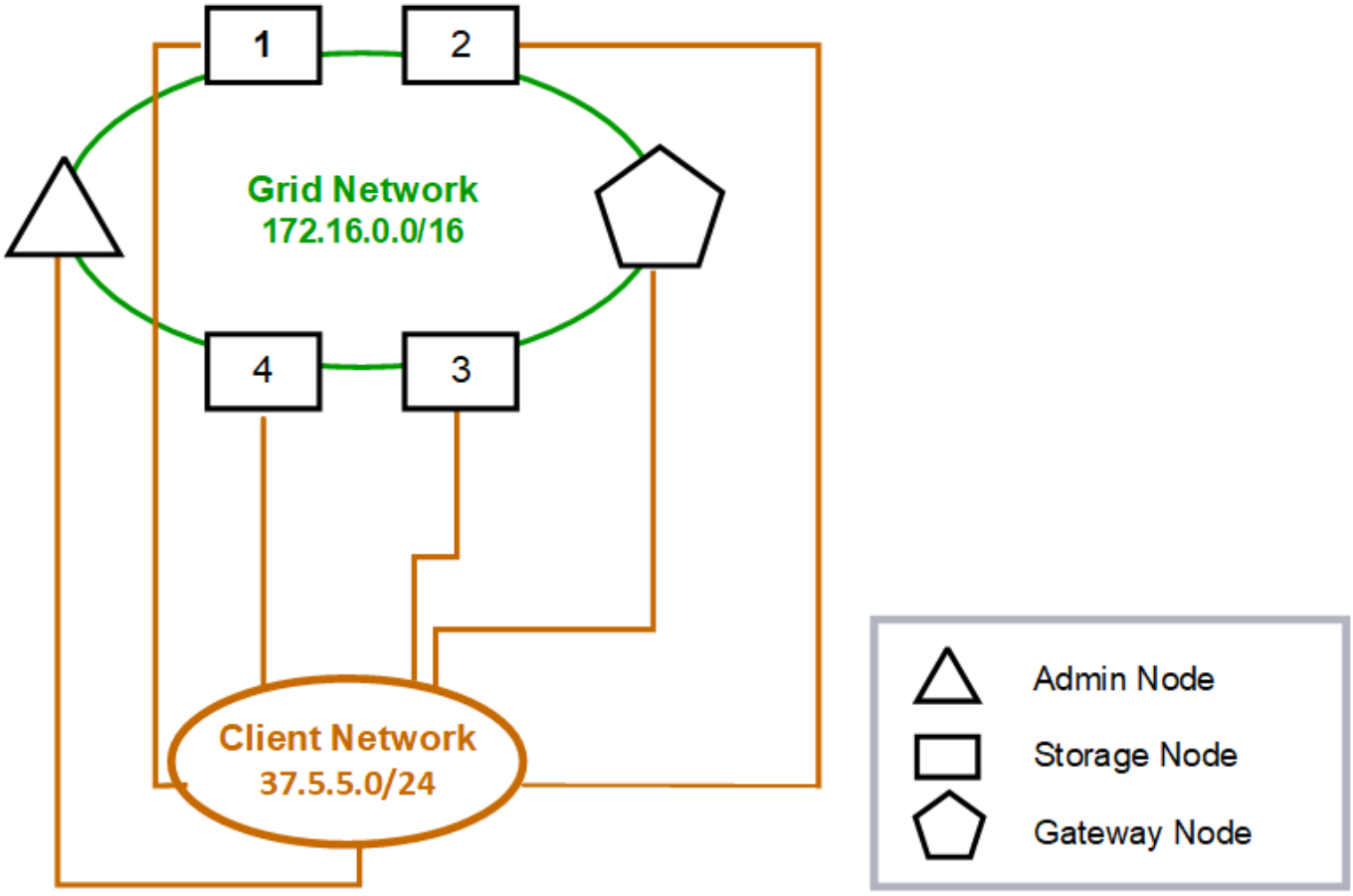
可以选择使用客户端网络。使用客户端网络可以将客户端网络流量(例如S3)与网格内部流量分隔开、从而提高网格网络的安全性。如果未配置管理网络，则可通过客户端网络或网格网络处理管理流量。

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



Provisioned

GNSL → 172.16.0.0/16

Nodes	Grid Network IP/mask	Client Network IP/mask	Client Network 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"

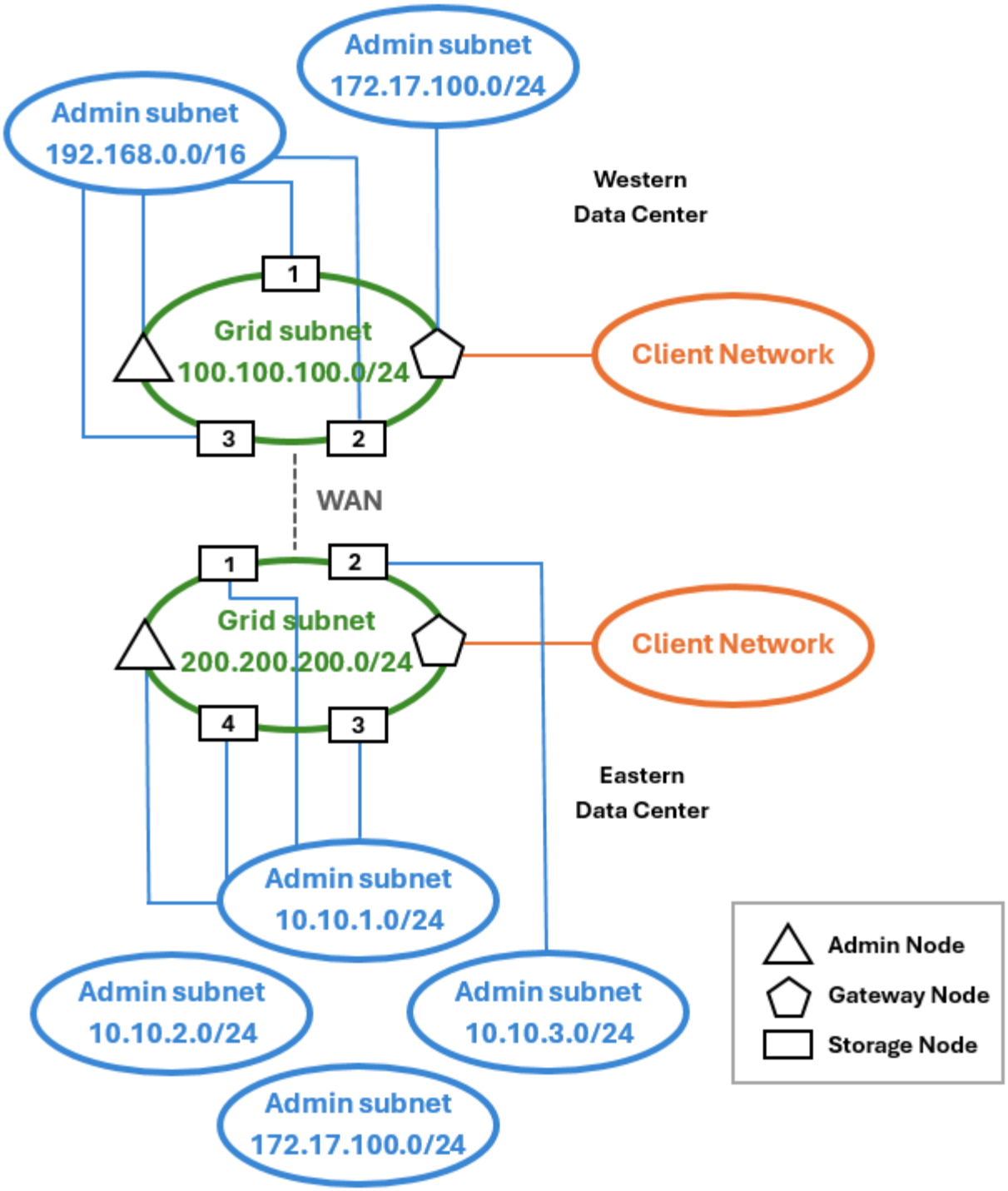
所有三个 **StorageGRID** 网络的网络拓扑

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。
- 客户端网络用于传输与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。
- **tcp**：从管理节点到或客户配置的代理的出站AutoSupport连接 `support.netapp.com`。
- * 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客户端的入站TCP连接。
- 来自 StorageGRID 平台服务（例如 CloudMirror 复制）或云存储池的出站请求。

如果StorageGRID 无法使用默认路由规则联系任何已配置的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。

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

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

适用于多个站点的广域网（ **WAN** ）

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

实际的最小WAN带宽要求取决于客户端活动和ILM保护方案。要在估算最低WAN带宽要求时获得帮助、请联系您的NetApp专业服务顾问。

管理节点和网关节点的连接

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

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

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

请勿在网格网络中的网格节点之间或StorageGRID 站点之间使用网络地址转换(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。

StorageGRID 的网络特定要求

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地址的子网掩码都不能为255.254或255.255 (CIDR表示法中的/31或/32)。
- 由网络接口IP地址和子网掩码(CIDR)定义的子网不能与在同一节点上配置的任何其他接口的子网重叠。
- 请勿对任何节点的网格网络、管理网络或客户端网络使用包含以下 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，不要对任何节点的网格网络、管理网络或客户端网络使用以下子网范围：

  - 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
  - 198.51.100.0/24，因为此子网范围包含 IP 地址 198.51.100.2 和 198.51.100.4
- 每个节点的网格网络子网必须包含在 GNSL 中。
- 管理网络子网不能与网格网络子网、客户端网络子网或GNSL中的任何子网重叠。

- AESL中的子网不能与GNSL中的任何子网重叠。
- 客户端网络子网不能与网格网络子网、管理网络子网、GNSL中的任何子网或AESL中的任何子网重叠。

网格网络

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

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

- 如果网格网络包含多个子网，请将其添加到网格网络子网列表（ GSLL ）中。在 GNSL 中的每个子网的所有节点上创建静态路由。
- 如果将网格网络接口配置为支持 VLAN 接口的中继，则中继原生 VLAN 必须是用于网格网络流量的 VLAN 。所有网格节点都必须可通过中继原生 VLAN 进行访问。

管理网络

管理网络是可选的。如果您计划配置管理网络，请遵循以下要求和准则。

管理网络的典型用途包括管理连接、AutoSupport 、KMS以及与关键服务器(如NTP、DNS和LDAP)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。

- 客户端网络旨在支持来自S3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。请参阅。 "配置负载平衡器端点"
- 如果客户端网络接口配置为中继以支持 VLAN 接口，请考虑是否需要配置客户端网络接口（ eth2 ）。如果已配置，则客户端网络流量将按交换机中的配置流经中继原生 VLAN 。

相关信息

"更改节点网络配置"

部署特定的网络注意事项

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 上作为一组容器引擎运

行。StorageGRID 系统不需要与容器引擎相关的网络配置。

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

> 不要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。

查看"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。主机和节点无法共享IP地址。

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

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ 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
	最小**LAN**带宽	管理员	10 Gbps
1 Gbps	1 Gbps	网关	10 Gbps

节点类型	网络类型		
1 Gbps	10 Gbps	存储	10 Gbps
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部署的一些推荐方法，请参阅"配置主机网络"。

用于平台服务和云存储池的网络和端口

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

平台服务的网络连接

如和中所述"管理租户的平台服务""管理平台服务"，平台服务包括提供搜索集成、事件通知和CloudMirror复制的外部服务。

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

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

云存储池网络连接

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

用于平台服务和云存储池的端口

默认情况下，平台服务和云存储池通信使用以下端口：

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

创建或编辑端点时，可以指定其他端口。请参阅。 "网络端口参考"

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

VLAN 和平台服务以及云存储池

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

StorageGRID 设备节点的网络配置

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(SG波特 性控制器)"
- "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。如果网格网络已隔离，则可以在主管理节点上配置管理网络，以便从网格网络外部进行配置和安装访问。

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

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

自动向主管理节点注册节点

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

禁用管理网络或客户端网络

如果要禁用管理网络或客户端网络，则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 。配置期间无法设置DHCP。

  通过DHCP更改网格网络配置后、节点会重新启动、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，必须使用更改 IP 过程。请参阅。 "配置 IP 地址"
- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改、您可能需要重新建立这些连接。

网络端口参考

StorageGRID 的内部网格节点通信

StorageGRID 内部防火墙允许与网格网络上的特定端口建立传入连接。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 。只有在配置了时、才需要VRRP"高可用性组"。

基于 **Linux** 的节点的准则

如果企业网络策略限制对任何这些端口的访问，您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更多信息，请参阅"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，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除裸机主机上的端口重新映射"。

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任何这些端口的访问，您可以在使用 VMware vSphere Web Client 部署节点时重新映射端口，或者在自动化网格节点部署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更多信息，请参阅"在 VMware 上安装StorageGRID"。

> 对端口重新映射的支持已弃用，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除裸机主机上的端口重新映射"。

设备节点准则

如果企业网络策略限制对其中任何端口的访问，则可以使用 StorageGRID 设备安装程序重新映射端口。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，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除StorageGRID设备上的端口重新映射"。

StorageGRID 内部端口

端口	**TCP** 或 **UDP**	发件人	至	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	主管理节点和非主管理节点	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	主管理节点和非主管理节点	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。
1055	TCP	所有节点	主管理节点和非主管理节点	用于安装、扩展、恢复和其他维护过程的内部流量。
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	具有模块转换器的存储节点	报告，审核和配置内部流量。

端口	**TCP** 或 **UDP**	发件人	至	详细信息
1502	TCP	所有节点	存储节点	与 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。
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。
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	提供用于全网格 IP 更改以及安装、扩展和恢复期间的主要管理节点发现的多播 DNS (mDNS) 服务。 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	主管理节点和非主管理节点	用于安装、扩展、恢复、其他维护过程和错误报告的内部流量。
8011	TCP	所有节点	主管理节点和非主管理节点	用于安装、扩展、恢复和其他维护过程的内部流量。
8443	TCP	主管理节点	设备节点	与维护模式操作步骤 相关的内部流量。
9042	TCP	存储节点	存储节点	Cassandra 客户端端口。
9999	TCP	所有节点	所有节点	多个服务的内部流量。包括维护过程，指标和网络更新。
10226	TCP	存储节点	主管理节点	由StorageGRID设备使用、用于将AutoSupport软件包从E系列SANtricity系统管理器转发到主管理节点。
10342	TCP	所有节点	主管理节点和非主管理节点	用于安装、扩展、恢复和其他维护过程的内部流量。

端口	TCP 或 UDP	发件人	至	详细信息
18000	TCP	所有节点	具有模块转换器的存储节点	帐户服务内部流量。
18001	TCP	所有节点	具有模块转换器的存储节点	身份联合内部流量。
18002	TCP	所有节点	存储节点	与对象协议相关的内部 API 流量。
18003	TCP	所有节点	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	所有节点	所有节点	用于擦除编码和复制的块服务内部流量
18082	TCP	管理 / 存储节点	存储节点	与 S3 相关的内部流量。
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	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"

StorageGRID 的外部通信

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

对端口的访问受限

如果企业网络策略限制对任何端口的访问、您可以执行以下操作之一：

- "负载平衡器端点"用于允许对用户定义的端口进行访问。

- 部署节点时重新映射端口。但是，您不应重新映射负载平衡器端点。请参见有关StorageGRID节点的端口重新映射的信息：

> 对端口重新映射的支持已弃用，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除StorageGRID设备上的端口重新映射"或者"删除裸机主机上的端口重新映射"。

- "在Red Hat Enterprise Linux上为StorageGRID重新映射端口密钥"
- "重新映射VMware上StorageGRID的端口"
- "可选：重新映射设备的网络端口"

用于外部通信的端口

下表显示了用于向节点进行流量的端口。

> 此列表不包括可能配置为"负载平衡器端点"的端口。

端口	**TCP** 或 **UDP**	协议	发件人	至	详细信息
22	TCP	SSH	服务笔记本电脑	所有节点	包含控制台步骤的过程需要 SSH 或控制台访问。或者，您可以使用端口 2022 而不是 22。 注意：仅当需要启用 SSH 访问以进行某些维护操作时才需要此端口。
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	也可用于支持基于 DHCP 的网络配置。dhclient 服务不会对静态配置的网格运行。
68	UDP	DHCP	DHCP服务	所有节点	也可用于支持基于 DHCP 的网络配置。对于使用静态 IP 地址的网格，不会运行 dhclient 服务。
80	TCP	HTTP	浏览器	管理节点	端口 80 重定向到管理节点用户界面的端口 443 。
80	TCP	HTTP	浏览器	设备	端口 80 重定向到 StorageGRID 设备安装程序的端口 8443 。

端口	**TCP** 或 **UDP**	协议	发件人	至	详细信息
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 HTTP 端口设置 80 。
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。
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	由 Web 浏览器和管理 API 客户端用来访问网格管理器和租户管理器。 注意：如果您关闭网格管理器端口 443 或 8443 ，则当前连接到被阻止端口的任何用户（包括您）都将失去对网格管理器的访问权限，除非他们的 IP 地址已添加到特权地址列表中。参考"配置防火墙控件"配置特权IP地址。

端口	**TCP** 或 **UDP**	协议	发件人	至	详细信息
443	TCP	HTTPS	管理节点	Active Directory	如果启用了单点登录（ SSO ），则由连接到 Active Directory 的管理节点使用。
443	TCP	HTTPS	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 。
636	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。
5353	UDP	mDNS	所有节点	所有节点	提供用于全网格 IP 更改以及安装、扩展和恢复期间的主要管理节点发现的多播 DNS (mDNS) 服务。 注意：配置此端口是可选的。
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。
8443	TCP	HTTPS	浏览器	管理节点	可选。由 Web 浏览器和管理 API 客户端用来访问网格管理器。可用于分离网格管理器和租户管理器通信。 注意：如果您关闭网格管理器端口 443 或 8443 ，则当前连接到被阻止端口的任何用户（包括您）都将失去对网格管理器的访问权限，除非他们的 IP 地址已添加到特权地址列表中。参考"配置防火墙控件"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 Appliance Installer。 注意：端口 443 重定向到StorageGRID设备安装程序的端口 8443。
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。

端口	**TCP** 或 **UDP**	协议	发件人	至	详细信息
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。
9092	TCP	Kafka	具有模块转换器的存储节点	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Kafka端口设置9092。
9443	TCP	HTTPS	浏览器	管理节点	可选。由 Web 浏览器和管理 API 客户端用来访问租户管理器。可用于分离网格管理器和租户管理器通信。
18082	TCP	HTTPS	S3 客户端	存储节点	直接发送到存储节点（ HTTPS ）的 S3 客户端流量。
18084	TCP	HTTP	S3 客户端	存储节点	直接发送到存储节点（ HTTP ）的 S3 客户端流量。
23000-23999	TCP	HTTPS	源网格上用于跨网格复制的所有节点	目标网格上用于跨网格复制的管理节点和网关节点	此端口范围是为网格联合连接预留的。给定连接中的两个网格使用相同的端口。

StorageGRID 快速入门

请按照以下简要步骤配置和使用任何StorageGRID 系统。

1 了解、规划和收集数据

请与您的NetApp客户代表联系、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：

- 您希望在初始阶段和一段时间内存储多少对象数据？
- 您需要多少站点？
- 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性或存储要求？
- 您是否需要遵守任何法律或法规要求？

(可选)与NetApp专业服务顾问一起访问NetApp ConfigBuilder工具、以完成配置工作簿、以便在安装和部署新系统时使用。您还可以使用此工具帮助自动配置任何StorageGRID 设备。请参阅。 "自动安装和配置设备"

查看 "了解StorageGRID" 和 "网络连接准则"。



安装节点

StorageGRID 系统由单个基于硬件和基于软件的节点组成。首先、请为每个设备节点安装硬件并配置每个Linux或VMware主机。

要完成安装、您需要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、您需要提供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。

了解如何：

- "安装设备硬件"
- "在基于软件的节点上安装StorageGRID"



登录并检查系统运行状况

网格安装完成后，您可以登录网格管理器。从那里，您可以查看新系统的总体健康状况，启用AutoSupport和警报电子邮件，并设置 S3 端点域名。

了解如何：

- "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"



配置和管理

您需要对新StorageGRID 系统执行的配置任务取决于您使用网格的方式。您至少需要设置系统访问、使用FabricPool 和S3向导以及管理各种存储和安全设置。

了解如何：

- "控制 StorageGRID 访问"
- "使用S3设置向导"
- "使用FabricPool 设置向导"
- "管理安全性"
- "系统强化"

5 设置ILM

您可以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)策略来控制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、以及如何随着时间的推移管理这些副本。

了解如何："使用 ILM 管理对象"

6 使用StorageGRID

完成初始配置后、StorageGRID租户帐户可以使用S3客户端应用程序来加载、检索和删除对象。

了解如何：

- "使用租户帐户"
- "使用S3 REST API"

7 监控和故障排除

系统启动并运行后、您应定期监控其活动、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系统日志服务器、使用SNMP监控或收集其他数据。

了解如何：

- "监控StorageGRID"
- "对StorageGRID 进行故障排除"

8 扩展、维护和恢复

您可以添加节点或站点来扩展系统的容量或功能。您还可以执行各种维护过程、以便从故障中恢复、或者使StorageGRID 系统保持最新并高效运行。

了解如何：

- "扩展网格"
- "维护您的网格"
- "恢复节点"

安装、升级和修复StorageGRID

安装 StorageGRID 节点

了解 StorageGRID 设备硬件

请转至 "StorageGRID 设备文档"以了解如何安装、配置和维护 StorageGRID 存储和服务设备。

安装基于软件的节点

在基于软件的节点上安装StorageGRID 的快速入门

按照这些高级步骤安装 Linux 或 VMware StorageGRID节点。

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

1 准备

- 了解 "StorageGRID 架构和网络拓扑"。
- 了解的具体信息"StorageGRID 网络连接"。
- 收集并准备"所需信息和材料"。
- （仅限 VMware）安装和配置"VMware vSphere虚拟机管理程序、vCenter和ESX主机"。
- 准备所需的"CPU和RAM"。
- 为提供"存储和性能要求"。
- （仅限 Linux）"准备Linux服务器"将托管您的StorageGRID节点。

2 部署

部署网格节点。部署网格节点时，它们会作为 StorageGRID 系统的一部分创建并连接到一个或多个网络。

- （仅限 Linux）要在步骤 1 中准备的主机上部署基于软件的网格节点，请使用 Linux 命令行和"节点配置文件"。
- （仅限 VMware）使用 VMware vSphere Web Client、.vmdk 文件和一组 .ovf 文件模板来"将基于软件的节点部署为虚拟机(VM)"在步骤 1 中准备的服务器上。
- 要部署StorageGRID设备节点，请执行 "硬件安装快速入门"。

3 配置

部署完所有节点后，使用网格管理器"配置网格并完成安装"。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

Linux

为了节省时间并保持一致性、您可以自动安装StorageGRID主机服务和配置网格节点。

- 使用标准流程编排框架(例如、Ands还是Puppet或Chef)实现自动化：
  - Linux 的安装
  - 配置网络和存储
  - 安装容器引擎和StorageGRID主机服务
  - 部署虚拟网格节点

  看"自动安装和配置 StorageGRID 主机服务" 。
- 部署网格节点后，"自动配置StorageGRID系统"使用安装档案中提供的 Python 配置脚本。
- "自动安装和配置设备网格节点"
- 如果您是StorageGRID部署的高级开发人员，请使用自动安装网格节点"安装REST API"。

VMware

为了节省时间并保持一致性、您可以自动部署和配置网格节点以及配置StorageGRID系统。

- "使用VMware vSphere自动部署网格节点"(英文)
- 在部署网格节点后、"自动配置StorageGRID系统"使用安装归档文件中提供的Python配置脚本。
- "自动安装和配置设备网格节点"
- 如果您是StorageGRID部署的高级开发人员，请使用自动安装网格节点"安装REST API"。

规划和准备在基于软件的节点上进行安装

StorageGRID 所需的信息和材料

安装StorageGRID之前、请收集并准备所需的信息和材料。

所需信息

网络计划

要连接到每个StorageGRID节点的网络。StorageGRID支持多个网络、以实现流量隔离、安全性和管理便利性。

请参阅 "网络连接准则"。

网络信息

要分配给每个网格节点的IP地址以及DNS和NTP服务器的IP地址。

网格节点的服务器

确定一组服务器（物理服务器，虚拟服务器或两者），这些服务器可在聚合中提供足够的资源来支持您计划部署的 StorageGRID 节点的数量和类型。

> 如果您的StorageGRID 安装不会使用StorageGRID 设备(硬件)存储节点、则必须使用具有备用电池的写入缓存(BBWC)的硬件RAID存储。StorageGRID 不支持使用虚拟存储区域网络(VSAN)、软件RAID或不支持RAID保护。

节点迁移（如果需要，仅限 **Ubuntu** 和 **Debian**）

"节点迁移的要求"如果要在不中断服务的情况下对物理主机执行计划内维护，请了解。

相关信息

"NetApp 互操作性表工具"

所需材料

NetApp StorageGRID 许可证

您必须具有有效的数字签名 NetApp 许可证。

> StorageGRID安装归档文件中包含一个非生产许可证、可用于测试和概念验证网格。

StorageGRID 安装归档

"下载StorageGRID安装归档文件并解压缩文件"(英文)

服务笔记本电脑

StorageGRID 系统通过服务笔记本电脑进行安装。

服务笔记本电脑必须具有：

- 网络端口
- SSH 客户端（例如 PuTTY ）
- "支持的 Web 浏览器"

StorageGRID 文档

- "发行说明"。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。
- "有关管理 StorageGRID 的说明"

下载并提取 **StorageGRID** 安装文件

您必须下载 StorageGRID 安装归档并提取所需文件。您也可以手动验证安装包中的文件。

步骤

1. 转到。 "StorageGRID 的 "NetApp 下载 " 页面"
2. 选择用于下载最新版本的按钮，或者从下拉菜单中选择其他版本并选择 * 执行 * 。
3. 使用您的 NetApp 帐户的用户名和密码登录。

4. 如果显示Cauy/MustRead语句，请阅读该语句并选中该复选框。

   安装 StorageGRID 版本后，您必须应用任何所需的修补程序。有关详细信息、请参见"恢复和维护说明中的热修补程序操作步骤"

5. 阅读最终用户许可协议，选中复选框，然后选择*接受并继续*。
6. 在 安装**StorageGRID** 列中，选择适合您基于软件的节点类型的 .tgz 或 .zip 安装存档：RHEL、Ubuntu 或 Debian 或 VMware。

   如果您在服务笔记本电脑上运行Windows、请使用此 `.zip`文件。

7. 保存安装归档文件。
8. 代码签名验证在 Linux 节点上是手动的。或者，如果您需要验证安装档案：

   a. 下载StorageGRID代码签名验证包。此软件包的文件名使用格式 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`，其中 `<version-number>` 是StorageGRID软件版本。

   b. 按照步骤"手动验证安装文件"。

9. 从安装归档文件中提取文件。
10. 选择所需的文件。

    所需文件取决于规划的网格拓扑以及StorageGRID系统的部署方式。

    表中列出的路径与提取的安装归档所安装的顶级目录相对。

RHEL

路径和文件名	说明
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM软件包、用于在RHEL主机上安装StorageGRID节点映像。
	RPM软件包、用于在RHEL主机上安装StorageGRID主机服务。
部署脚本工具	说明
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	用于为StorageGRID容器部署配置RHEL主机的AndsableRole和操作手册示例。您可以根据需要自定义角色或攻略手册。
	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。

路径和文件名	说明
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

Ubuntu 或 Debian

路径和文件名	说明
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。
	文件的MD5校验和 `/debs/storagegrid-webscale-images-version-SHA.deb`。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	说明
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	用于脚本的空配置文件 `configure-storagegrid.py`。

路径和文件名	说明
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
storagegrid-ssoauth-azure.py	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

VMware

路径和文件名	说明
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。
	(`.mf`用于部署主管理节点(`.ovf`的开放式虚拟化格式模板文件()和清单文件()。
	(`.mf`用于部署非主管理节点(`.ovf`的模板文件()和清单文件()。
	(`.mf`用于部署网关节点(`.ovf`的模板文件()和清单文件()。
	(`.mf`用于部署基于虚拟机的存储节点的模板(`.ovf`文件()和清单文件()。
部署脚本工具	说明

路径和文件名	说明
	Bash shell 脚本，用于自动部署虚拟网格节点。
	用于脚本的示例配置文件 `deploy-vsphere-ovftool.sh`。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个Python脚本示例、在启用单点登录(Single Sign On、SSO)后、您可以使用该脚本登录到网格管理API。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

验证 **StorageGRID** 安装文件

如有必要、您可以手动验证StorageGRID安装归档文件中的文件。

开始之前

你有"已下载验证软件包"从 "StorageGRID 的 "NetApp 下载 " 页面"。

步骤

1. 从验证软件包中提取项目：

   ```
   tar -xf StorageGRID_12.1.0_Code_Signature_Verification_Package.tar.gz
   ```

2. 确保已提取这些项目：

   - 叶证书： `Leaf-Cert.pem`
   - 证书链： `CA-Int-Cert.pem`
   - 时间戳响应链： `TS-Cert.pem`
   - 校验和文件： `sha256sum`
   - 校验和签名： `sha256sum.sig`
   - 时间戳响应文件： `sha256sum.sig.tsr`

3. 使用链验证叶证书是否有效。

   示例： `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

   预期输出： `Leaf-Cert.pem: OK`

4. 如果步骤_2_因叶证书过期而失败、请使用 `tsr`文件进行验证。

   示例： `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   预期输出包括： `Verification: OK`

5. 从叶证书创建公共密钥文件。

   示例： `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

   预期输出：*none*

6. 使用公共密钥根据验证 `sha256sum`文件 `sha256sum.sig`。

   示例： `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   预期输出： `Verified OK`

7. 根据新创建的校验和验证 `sha256sum`文件内容。

   示例： `sha256sum -c sha256sum`

   预期输出： *`<filename>`*`: OK`+
   `*<filename>*`是您下载的归档文件的名称。

8. "完成其余步骤"从安装档案中提取并选择适当的文件。

您可以使用虚拟机托管任何类型的StorageGRID节点。每个网格节点需要一个虚拟机。

RHEL

要在 RHEL 上安装StorageGRID ，您必须安装一些第三方软件包。某些受支持的 Linux 发行版默认不包含这些软件包。 StorageGRID安装所测试的软件包版本包括本页列出的版本。

如果您选择的Linux分发版和容器运行时安装选项需要这些软件包中的任何一个，并且Linux分发版不会自动安装这些软件包，请安装此处列出的其中一个版本(如果您的供应商或Linux分发版的支持供应商提供了这些版本)。否则、请使用供应商提供的默认软件包版本。

所有安装选项都需要使用Podman或Docker。请勿同时安装这两个软件包。仅安装安装选项所需的软件包。

> 不再支持将Docker用作纯软件部署的容器引擎。在未来版本中、Docker将被另一个容器引擎取代。

测试的 **Python** 版本

- 3.5.2.2.
- 3.6.8-2.
- 3.6.8-38.
- 3.6.9-1.
- 3.7.3-1.
- 3.8.10-0
- 3.9.2-1.
- 3.9.10-2.
- 3.9.16-1.
- 3.10.6-1.
- 3.11.2-6.

已测试的 **Podman** 版本

- 3.2.3-0
- 3.4.4+DS1.
- 4.1.1-7.
- 4.2.0-11.
- 4.3.1+DS1-8+B1
- 4.4.1-8.
- 4.4.1-12.

测试的 **Docker** 版本

> Docker支持已弃用、将在未来版本中删除。

- Docker CE 20.10.7.
- Docker CE 20.10.20-3

- Docker -CE 23.0.6-1
- Docker -CE 24.0.2-1
- Docker -CE 24.0.4-1
- Docker -CE 24.0.5-1
- Docker -CE 24.0.7-1
- 1.5-2

Ubuntu 和 Debian

要在Ubuntu或Debian上安装StorageGRID、您必须安装某些第三方软件包。默认情况下、某些受支持的Linux分发版不包含这些软件包。测试StorageGRID安装的软件包版本包括此页面上列出的软件包版本。

如果您选择的Linux分发版和容器运行时安装选项需要这些软件包中的任何一个，并且Linux分发版不会自动安装这些软件包，请安装此处列出的其中一个版本(如果您的供应商或Linux分发版的支持供应商提供了这些版本)。否则、请使用供应商提供的默认软件包版本。

所有安装选项都需要使用Podman或Docker。请勿同时安装这两个软件包。仅安装安装选项所需的软件包。

> 不再支持将Docker用作纯软件部署的容器引擎。在未来版本中、Docker将被另一个容器引擎取代。

测试的 **Python** 版本

- 3.5.2.2.
- 3.6.8-2.
- 3.6.8-38.
- 3.6.9-1.
- 3.7.3-1.
- 3.8.10-0
- 3.9.2-1.
- 3.9.10-2.
- 3.9.16-1.
- 3.10.6-1.
- 3.11.2-6.

已测试的 **Podman** 版本

- 3.2.3-0
- 3.4.4+DS1.
- 4.1.1-7.
- 4.2.0-11.
- 4.3.1+DS1-8+B1
- 4.4.1-8.

- 4.4.1-12.

测试的 **Docker** 版本

Docker支持已弃用、将在未来版本中删除。

- Docker CE 20.10.7.
- Docker CE 20.10.20-3
- Docker -CE 23.0.6-1
- Docker -CE 24.0.2-1
- Docker -CE 24.0.4-1
- Docker -CE 24.0.5-1
- Docker -CE 24.0.7-1
- 1.5-2

VMware

VMware vSphere 虚拟机管理程序

您必须在已准备好的物理服务器上安装 VMware vSphere 虚拟机管理程序。在安装 VMware 软件之前，必须正确配置硬件（包括固件版本和 BIOS 设置）。

- 根据需要在虚拟机管理程序中配置网络，以支持要安装的 StorageGRID 系统的网络连接。

  "网络连接准则"

- 确保数据存储库足够大，足以容纳托管网格节点所需的虚拟机和虚拟磁盘。
- 如果创建多个数据存储库，请为每个数据存储库命名，以便在创建虚拟机时轻松确定要用于每个网格节点的数据存储库。

ESX 主机配置要求

您必须在每个 ESX 主机上正确配置网络时间协议（ NTP ）。如果主机时间不正确，可能会产生负面影响，包括数据丢失。

VMware 配置要求

在部署StorageGRID节点之前、您必须安装和配置VMware vSphere和vCenter。

有关受支持的VMware vSphere Hypervisor(虚拟机管理程序)和VMware vCenter Server软件版本，请参见"NetApp 互操作性表工具"。

有关安装这些 VMware 产品所需的步骤，请参见 VMware 文档。

StorageGRID 的 CPU 和 RAM 要求

在安装 StorageGRID 软件之前，请验证并配置硬件，使其可以支持 StorageGRID 系统。

每个 StorageGRID 节点需要以下最低资源：

- CPU 核心：每个节点 8 个
- RAM：取决于可用的总RAM以及系统上运行的非StorageGRID软件的数量
  - 通常、每个节点至少24 GB、比系统总RAM少2到16 GB
  - 如果多个租户每个都有多达 5,000 个存储桶，则每个节点至少 64 GB

> StorageGRID 系统为每个 S3 租户帐户最多支持 20,000 个存储桶。

基于软件的纯元数据节点资源必须与现有存储节点资源匹配。例如：

- 如果现有StorageGRID站点使用SG6000或SG6100设备、则基于软件的纯元数据节点必须满足以下最低要求：
  - 128 GB RAM
  - 8核CPU
  - 用于cassandr数据库的8 TB SSD或等效存储(rangedb/0)
- 如果现有的StorageGRID站点使用具有 24 GB RAM、8 核 CPU 和 3 TB 或 4TB 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 4TB 元数据存储（rangedb/0））。

添加新StorageGRID站点时、新站点的元数据总容量至少应与现有StorageGRID站点匹配、新站点资源应与现有StorageGRID站点的存储节点匹配。

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

Linux

确保计划在每个物理或虚拟主机上运行的 StorageGRID 节点数不超过可用的 CPU 核心数或物理 RAM 数。如果主机不是专用于运行StorageGRID (不建议这样做)、请务必考虑其他应用程序的资源要求。

VMware

VMware支持每个虚拟机使用一个节点。确保StorageGRID节点不超过可用物理RAM。每个虚拟机都必须专用于运行StorageGRID。

> 定期监控您的 CPU 和内存使用情况，以确保这些资源能够持续满足您的工作负载需求。例如，将虚拟存储节点的 RAM 和 CPU 分配加倍，将提供与 StorageGRID 设备节点相似的资源。此外，如果每个节点的元数据量超过 500 GB，请考虑将每个节点的 RAM 增加到 48 GB 或更多。有关管理对象元数据存储、增加元数据保留空间设置以及监控 CPU 和内存使用情况的信息，请参阅 "管理"、"监控" 和 "正在升级" StorageGRID 的相关说明。

如果在底层物理主机上启用了超线程功能，则可以为每个节点提供 8 个虚拟核心（ 4 个物理核心）。如果底层物理主机上未启用超线程，则必须为每个节点提供 8 个物理核心。

如果要使用虚拟机作为主机并控制 VM 的大小和数量，则应为每个 StorageGRID 节点使用一个 VM 并相应地调整 VM 的大小。

（仅限 RHEL、Debian 和 Ubuntu）对于生产部署，您不应在同一物理存储硬件或虚拟主机上运行多个存储节点。单个StorageGRID部署中的每个存储节点都应位于其自己的隔离故障域中。如果确保单个硬件故障仅影响单个存储节点，则可以最大限度地提高对象数据的持久性和可用性。

请参阅 "存储和性能要求"。

StorageGRID 的存储和性能要求

您必须了解 StorageGRID 节点的存储要求，以确保您有足够的空间来支持初始配置和未来的存储扩展。

存储和性能要求根据基于软件的节点实现而有所不同。

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

存储类别

StorageGRID 节点需要三种逻辑存储类别：

- 容器池 — 节点容器的性能层（10K SAS 或 SSD）存储，当您在支持 StorageGRID 节点的主机上安装和配置容器引擎时，该存储将分配给容器引擎存储驱动程序。
- 系统数据 — 性能层（10K SAS 或 SSD）存储，用于按节点持久存储系统数据和事务日志，StorageGRID 主机服务使用并映射到单个节点。
- * 对象数据 * —性能层（ 10K SAS 或 SSD ）存储和容量层（ NL-SAS/SATA ）批量存储，用于永久存储对象数据和对象元数据。

您必须为所有存储类别使用 RAID 支持的块设备。不支持非冗余磁盘、SSD 或 JBOD。您可以为任何存储类别使用共享或本地 RAID 存储。要迁移 StorageGRID 中的节点，必须在共享存储上存储系统数据和对象数据。有关详细信息，请参见 "节点容器迁移要求"。

性能要求

用于容器池，系统数据和对象元数据的卷的性能会显著影响系统的整体性能。您应对这些卷使用性能层（ 10K SAS 或 SSD ）存储，以确保在延迟，每秒输入 / 输出操作数（ IOPS ）和吞吐量方面具有足够的磁盘性能。您可以使用容量层（ NL-SAS/SATA ）存储来永久存储对象数据。

用于容器池，系统数据和对象数据的卷必须启用回写缓存。缓存必须位于受保护或永久性介质上。

使用**NetApp ONTAP** 存储的主机的要求

如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

所需的主机数

每个 StorageGRID 站点至少需要三个存储节点。

> 在生产部署中，不要在单个物理或虚拟主机上运行多个存储节点。每个存储节点的专用主机提供隔离的故障域。

您可以在同一主机上部署其他类型的节点，例如管理节点或网关节点，也可以根据需要在其自己的专用主机上部署它们。

> 您不能使用磁盘快照来恢复网格节点。请参见每种类型节点的"网格节点恢复"过程。

每个节点的存储卷数量

下表显示了每个主机所需的存储卷（LUN）数量以及每个 LUN 所需的最小大小（基于在该主机上部署的节点）。

测试的最大 LUN 大小为 100 TiB。

> 这些数字适用于每个主机，而不适用于整个网格。

LUN 用途	存储类别	**LUN** 数量	最小大小 **/LUN**
容器引擎存储池	容器池	1	节点总数 × 100 GB
`/var/local`卷	系统数据	此主机上的每个节点 1 个	100 GB
存储节点	对象数据	此主机上的每个存储节点 3 个 注意： 基于 Linux 软件的存储节点和基于 VMware 软件的存储节点可以具有 1 至 48 个存储卷。建议至少有 3 个存储卷。	12 TB（最低 4 TB/LUN） 测试的最大 LUN 大小：100 TiB。 有关详细信息，请参见 存储节点的存储要求。
存储节点(仅限元数据)	对象元数据	1	最低 4 TB/LUN 测试的最大 LUN 大小：100 TiB。 有关详细信息，请参见 存储节点的存储要求。 注意：对于纯元数据存储节点、只需要一个 rangedb。

LUN 用途	存储类别	LUN 数量	最小大小 /LUN
管理节点审核日志	系统数据	此主机上的每个管理节点 1 个	200 GB
管理节点表	系统数据	此主机上的每个管理节点 1 个	200 GB

> 您可能需要增加每个管理节点上审核日志 LUN 的大小，具体取决于配置的审核级别、用户输入的大小（如 S3 对象密钥名称）以及需要保留的审核日志数据量。通常，网格每个 S3 操作生成约 1 KB 的审核数据，这意味着 200 GB LUN 将每天支持 7000 万个操作或每秒 800 个操作，持续两到三天。

主机的最小存储空间

下表显示了每种类型的节点所需的最小存储空间。您可以使用此表确定必须为每个存储类别中的主机提供的最小存储量，具体取决于在该主机上部署的节点。

> 您不能使用磁盘快照来恢复网格节点。请参见每种类型节点的"网格节点恢复"过程。

每个节点主机都需要一个 100 GB 的 LUN 用于操作系统。

节点类型	容器池	系统数据	对象数据
存储节点	100 GB	100 GB	4,000 GB
管理节点	100 GB	500 GB（3 个 LUN）	_ 不适用 _
网关节点	100 GB	100 GB	_ 不适用 _

示例：计算主机或虚拟机的存储需求

假设您计划在同一主机或虚拟机上部署三个节点：一个存储节点、一个管理节点和一个网关节点。您应向主机提供至少九个存储卷。您需要至少 300 GB 的性能层存储用于节点容器、700 GB 的性能层存储用于系统数据和事务日志，以及 12 TB 的容量层存储用于对象数据。

Linux 主机示例

节点类型	**LUN** 用途	**LUN** 数量	**LUN**大小
存储节点	容器引擎存储池	1	300 GB （ 100 GB/ 节点 ）
存储节点	`/var/local`卷	1	100 GB
存储节点	对象数据	3	12 TB （ 4 TB/LUN ）
管理节点	`/var/local`卷	1	100 GB
管理节点	管理节点审核日志	1	200 GB
管理节点	管理节点表	1	200 GB
网关节点	`/var/local`卷	1	100 GB
• 总计 *		**9**	• 容器池： * 300 GB 系统数据： 700 GB • 对象数据： * 12 ，000 GB

VMware 虚拟机示例

节点类型	**LUN** 用途	**LUN** 数量	**LUN**大小
存储节点	操作系统卷	1	100 GB
存储节点	对象数据	3	12 TB （ 4 TB/LUN ）
管理节点	操作系统卷	1	100 GB
管理节点	管理节点审核日志	1	200 GB
管理节点	管理节点表	1	200 GB
网关节点	操作系统卷	1	100 GB
• 总计 *		**8**	系统数据： 700 GB • 对象数据： * 12 ，000 GB

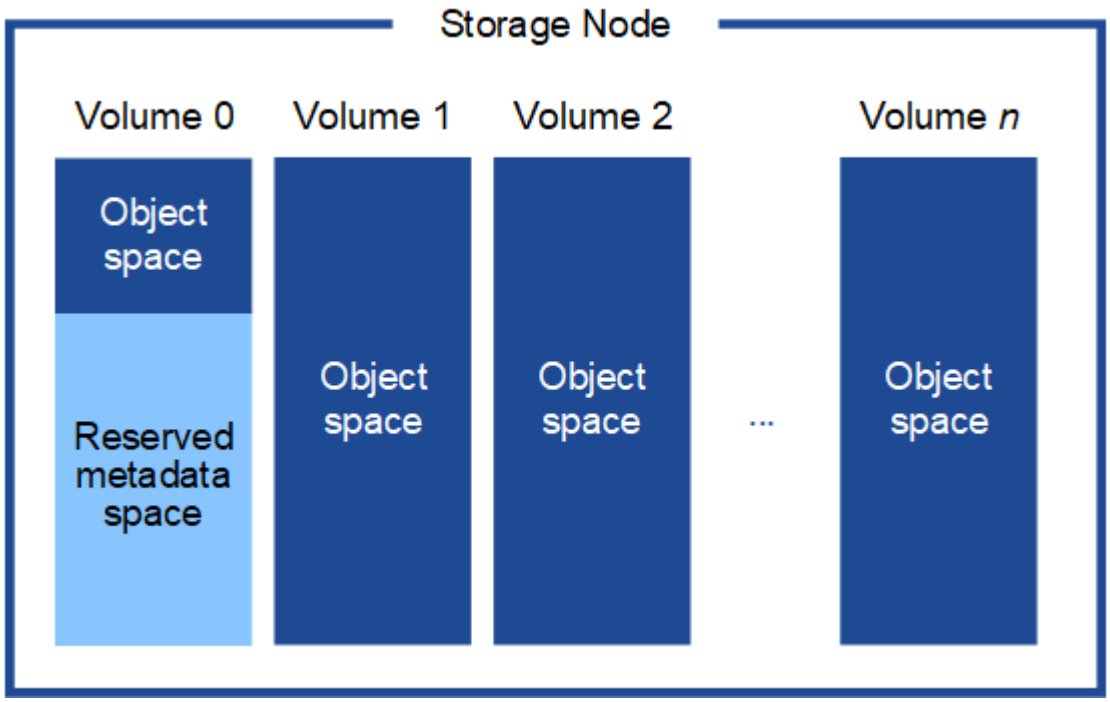
存储节点的特定存储要求

Linux和VMware对存储节点有下列存储要求：

- 基于 Linux 软件的存储节点可具有 1 至 48 个存储卷。
- 基于 VMware 软件的存储节点可具有 1 至 48 个存储卷。
- 建议使用三个或更多个存储卷。
- 每个存储卷应为 4 TB 或更大。

设备存储节点还可以拥有最多 48 个存储卷。

如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。存储卷 0 和存储节点中的任何其他存储卷上的任何剩余空间专用于对象数据。



为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。对象元数据的三个副本均匀分布在每个站点的所有存储节点上。

在安装具有仅元数据存储节点的网格时，网格还必须包含用于对象存储的最小数量的节点。有关仅元数据存储节点的详细信息，请参见 "存储节点的类型"。

- 对于单站点网格、至少为对象和元数据配置了两个存储节点。
- 对于多站点网格、每个站点至少为对象和元数据配置一个存储节点。

在为新存储节点的卷 0 分配空间时，必须确保为该节点在所有对象元数据中的部分分配足够的空间。

- 您必须至少为卷 0 分配 4 TB 。

如果一个存储节点仅使用一个存储卷、而为该卷分配的存储容量不超过4 TB、则该存储节点可能会在启动时进入存储只读状态、并仅存储对象元数据。

如果为卷0分配的空间小于500 GB (仅限非生产环境使用)、则存储卷的容量中有10%将预留用于元数据。

- 基于软件的纯元数据节点资源必须与现有存储节点资源匹配。例如：
  - 如果现有StorageGRID站点使用SG6000或SG6100设备、则基于软件的纯元数据节点必须满足以下最低要求：
    - 128 GB RAM
    - 8核CPU
    - 用于cassandr数据库的8 TB SSD或等效存储(rangedb/0)
  - 如果现有的StorageGRID站点使用具有 24 GB RAM、8 核 CPU 和 3 TB 或 4TB 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 4TB 元数据存储（rangedb/0））。

    添加新StorageGRID站点时、新站点的元数据总容量至少应与现有StorageGRID站点匹配、新站点资源应与现有StorageGRID站点的存储节点匹配。
- 如果要安装新系统(StorageGRID 11.6或更高版本)、并且每个存储节点的RAM大于或等于128 GB、请为卷0分配8 TB或更多。如果对卷 0 使用较大的值，则可以增加每个存储节点上允许的元数据空间。
- 为站点配置不同的存储节点时，如果可能，请对卷 0 使用相同的设置。如果站点包含不同大小的存储节点，则卷 0 最小的存储节点将决定该站点的元数据容量。

有关详细信息，请访问"管理对象元数据存储"。

Linux 的 StorageGRID 节点容器迁移要求

通过节点迁移功能，您可以手动将节点从一台主机移动到另一台主机。通常，两台主机位于同一物理数据中心。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

通过节点迁移，您可以在不中断网格操作的情况下执行物理主机维护。在使物理主机脱机之前、可以将所有StorageGRID 节点逐个移动到另一台主机。迁移节点只需要每个节点短暂停机，不应影响网格服务的运行或可用性。

如果要使用 StorageGRID 节点迁移功能，则部署必须满足其他要求：

- 在一个物理数据中心的主机之间使用一致的网络接口名称
- StorageGRID 元数据和对象存储库卷的共享存储，可由单个物理数据中心中的所有主机访问。例如，您可以使用 NetApp E 系列存储阵列。

如果您使用的是虚拟主机、并且底层虚拟机管理程序层支持VM迁移、则可能需要使用此功能、而不是StorageGRID 中的节点迁移功能。在这种情况下，您可以忽略这些附加要求。

在执行迁移或虚拟机管理程序维护之前，请正常关闭节点。请参阅的说明"关闭网格节点"。

不支持 **VMware** 实时迁移

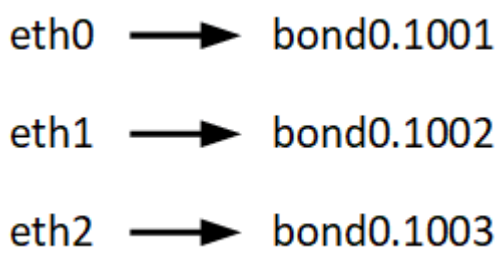
在VMware VM、OpenStack实时迁移和VMware实时vMotion发生原因上执行裸机安装时、虚拟机时钟时间会跳过、任何类型的网格节点均不支持。尽管时钟时间不正确，但极少会导致数据丢失或配置更新。

支持冷迁移。在冷迁移中，您需要先关闭 StorageGRID 节点，然后再在主机之间迁移它们。请参阅的说明"关闭网格节点"。

网络接口名称一致

要将节点从一台主机移动到另一台主机、StorageGRID 主机服务需要具有一定的信心、即该节点当前位置的外部网络连接可以在新位置复制。它可以通过在主机中使用一致的网络接口名称来获得这种信心。

例如，假设主机 1 上运行的 StorageGRID 节点 A 已配置以下接口映射：



箭头的左侧对应于从 StorageGRID 容器中查看的传统接口（即网格接口，管理接口和客户端网络接口）。箭头的右侧对应于提供这些网络的实际主机接口，它们是同一物理接口绑定下的三个 VLAN 接口。

现在，假设您要将节点 A 迁移到 Host2 。如果 Host2 还具有名为 bond0.1001 ， bond0.1002 和 bond0.1003 的接口，则系统将允许移动，前提是同名接口在 Host2 上提供的连接与在 Host1 上提供的连接相同。如果 Host2 的接口名称不相同，则不允许移动。

可通过多种方法在多个主机之间实现一致的网络接口命名；有关一些示例、请参见"配置主机网络"。

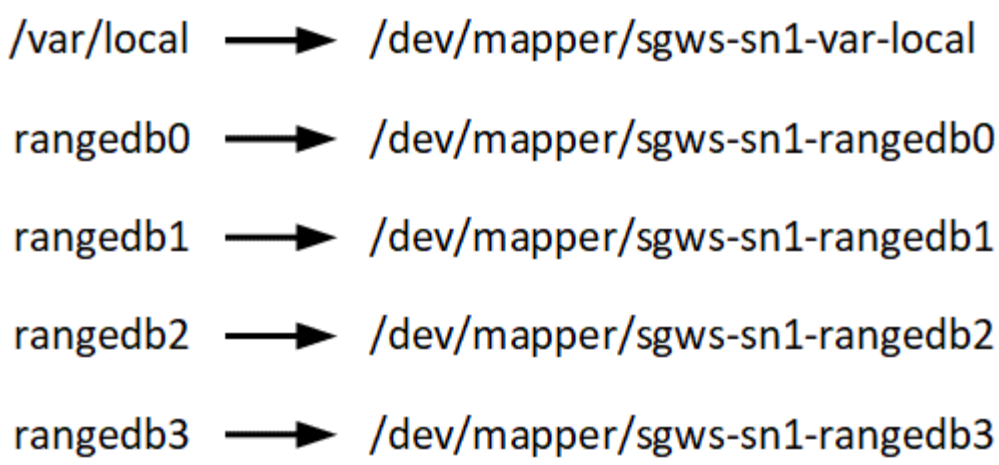
共享存储

为了实现快速、低开销的节点迁移、StorageGRID 节点迁移功能不会以物理方式移动节点数据。而是将节点迁移作为一对导出和导入操作来执行，如下所示：

- 在"节点导出"操作期间、系统会从HostA上运行的节点容器中提取少量永久性状态数据、并将其缓存在该节点的系统数据卷上。然后，将对 HostA 上的节点容器进行实例化。
- 在"节点导入"操作期间、将例化主机B上使用与主机A上有效的相同网络接口和块存储映射的节点容器。然后，缓存的永久性状态数据将插入到新实例中。

在这种操作模式下，节点的所有系统数据和对象存储卷都必须可从主机 A 和主机 B 访问，才能允许迁移并正常运行。此外，它们必须已使用名称映射到节点，这些名称可以保证引用主机 A 和主机 B 上的相同 LUN 。

以下示例显示了StorageGRID存储节点块设备映射的一个解决方案、其中、主机上正在使用DM多路径、而中使用了别名字段 `/etc/multipath.conf`、以便在所有主机上提供一致且友好的块设备名称。



StorageGRID 如何更改主机范围的设置

在裸机系统上、StorageGRID会对主机范围的设置进行一些更改 `sysctl`。

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

将进行以下更改：

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
```

```
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
```

```
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

在 **Linux** 网格主机上安装 **StorageGRID**

您必须在所有 Linux 网格主机上安装StorageGRID 。要获取受支持版本的列表，请使用NetApp互操作性表工具。

开始之前

确保您的操作系统满足StorageGRID的最低内核版本要求、如下所示。使用命令 `uname -r`获取操作系统的内核版本、或者咨询操作系统供应商。

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

RHEL

RHEL 版本	最低内核版本	内核软件包名称
8.8 (已弃用)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8.10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0 (已弃用)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2 (已弃用)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9.4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64
9.6	5.14.0-570.18.1.el9_6.x86_64	内核-5.14.0-570.18.1.el9_6.x86_64

Ubuntu

*注意：*对Ubuntu版本18.04和20.04的支持已弃用、将在未来版本中删除。

Ubuntu版本	最低内核版本	内核软件包名称
22.04.1	5.15.0-47-通用	linux-image-5.15.0-47-generic/jammy-updates 、jammy-security、now 5.15.0-47.51
24.04	6.8.0-31-generic	linux-image-6.8.0-31-generic/Noble、现在为6.8.0-31.31

Debian

注： Debian版本11的支持已弃用，将在未来版本中删除。

Debian版本	最低内核版本	内核软件包名称
11 (已弃用)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable、现在为5.10.150-1
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable、现在为6.1.27-1

步骤

1. 按照分销商的说明或您的标准操作步骤 在所有物理或虚拟网格主机上安装 Linux 。

   不要安装任何图形桌面环境。

   ◦ 如果在安装 RHEL 时使用标准 Linux 安装程序，请选择“计算节点”软件配置（如果可用）或“最小安装”基础环境。

- 安装 Ubuntu 时，您必须选择*标准系统实用程序*。建议选择 **OpenSSH** 服务器 以启用对 Ubuntu 主机的 ssh 访问。所有其他选项可以保持清除状态。

2. 确保所有主机都可以访问软件包存储库，包括 RHEL 的 Extras 频道。
3. 如果已启用交换：
   a. 运行以下命令： `$ sudo swapoff --all`
   b. 从中删除所有交换条目 `/etc/fstab`以保留设置。

   如果未完全禁用交换，则会严重降低性能。

了解 **Ubuntu** 和 **Debian** 上的 **AppArmor** 配置文件用于 **StorageGRID**

如果您在自行部署的 Ubuntu 环境中运行并使用了必需的 AppArmor-Access Control 系统，则与在基础系统上安装的软件包关联的 StorageGRID 配置文件可能会被随一起安装的相应软件包阻止。

默认情况下，系统会为您在基础操作系统上安装的软件包安装 AppArmort 配置文件。从 StorageGRID 系统容器运行这些软件包时，将阻止这些配置文件。DHCP ， MySQL ， NTP 和 TCdump 基本软件包与 AppArp 冲突，而其他基本软件包也可能发生冲突。

您可以选择两种方法来处理 AppArmor 配置文件：

- 为基础系统上安装的与 StorageGRID 系统容器中的软件包重叠的软件包禁用各个配置文件。禁用各个配置文件时， StorageGRID 日志文件中会显示一个条目，指示已启用。

  使用以下命令：

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

- 示例： *

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- 完全禁用 AppArmor。对于 Ubuntu 9.10 或更高版本，请按照 "Ubuntu 在线社区"中的说明操作。在较新的 Ubuntu 版本上可能无法完全禁用 AppArmor。

  禁用AppArmor后、StorageGRID日志文件中不会显示任何指示AppArmor已启用的条目。

为 **Linux** 部署配置 **StorageGRID** 主机网络

在主机上完成 Linux 安装后，您可能需要执行一些额外的配置，以便在每个主机上准备一组适合映射到稍后要部署的 StorageGRID 节点的网络接口。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

开始之前

- 您已查看 "网络连接准则" 中的信息。
- 您已查看有关的信息"节点容器迁移要求"。
- 如果您正在使用虚拟主机，则您已阅读MAC 地址克隆的注意事项和建议在配置主机网络之前。

如果要使用 VM 作为主机，则应选择 VMXNET 3 作为虚拟网络适配器。VMware E1000 网络适配器已导致在某些 Linux 版本上部署 StorageGRID 容器时出现连接问题。

关于此任务

网格节点必须能够访问网格网络，还可以访问管理网络和客户端网络。您可以通过创建映射来提供此访问权限，此映射会将主机的物理接口与每个网格节点的虚拟接口相关联。创建主机接口时，请使用友好名称以方便在所有主机之间进行部署，并启用迁移。

同一接口可以在主机与一个或多个节点之间共享。例如，您可以使用相同的接口进行主机访问和节点管理网络访问，以便于维护主机和节点。尽管主机和各个节点之间可以共享同一接口，但所有接口都必须具有不同的 IP 地址。不能在节点之间或主机与任何节点之间共享IP地址。

您可以使用相同的主机网络接口为主机上的所有 StorageGRID 节点提供网格网络接口；可以为每个节点使用不同的主机网络接口；也可以在这两者之间执行操作。但是，通常不会提供与单个节点的网格和管理网络接口相同的主机网络接口，也不会提供与一个节点的网格网络接口和另一个节点的客户端网络接口相同的主机网络接口。

您可以通过多种方式完成此任务。例如、如果您的主机是虚拟机、而您要为每个主机部署一个或两个StorageGRID 节点、则可以在虚拟机管理程序中创建正确数量的网络接口、并使用一对一映射。如果要在裸机主机上部署多个节点以供生产使用，则可以利用 Linux 网络堆栈对 VLAN 和 LACP 的支持来实现容错和带宽共享。以下各节详细介绍了这两个示例的方法。您无需使用其中任何一个示例；您可以使用任何符合您需求的方法。

不要直接使用绑定或网桥设备作为容器网络接口。这样做可能会阻止内核问题描述 在容器命名空间中对绑定和网桥设备使用 MACVLAN 导致节点启动。请改用非绑定设备，例如 VLAN 或虚拟以太网（ Veth ）对。在节点配置文件中指定此设备作为网络接口。

MAC 地址克隆的注意事项和建议

MAC 地址克隆导致容器使用主机的 MAC 地址，而主机使用您指定的地址或随机生成的地址的 MAC 地址。

启用 **MAC** 克隆

在某些环境中，可以通过 MAC 地址克隆来增强安全性，因为它使您能够为管理网络、网格网络和客户端网络使用专用的虚拟 NIC。

MAC 地址克隆用于安装虚拟服务器，可能无法在所有物理设备配置中正常运行。

如果某个节点由于 MAC 克隆目标接口繁忙而无法启动，则在启动节点之前，您可能需要将链路设置为 " 关闭 " 。此外，在链路启动时，虚拟环境可能会阻止网络接口上的 MAC 克隆。如果某个节点由于接口繁忙而无法设置 MAC 地址并启动，则在启动该节点之前将链路设置为 " 关闭 " 可能会修复问题描述 。

默认情况下， MAC 地址克隆处于禁用状态，必须通过节点配置密钥进行设置。您应在安装 StorageGRID 时启用它。

每个网络有一个密钥：

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

如果将密钥设置为 "true" ，则容器将使用主机 NIC 的 MAC 地址。此外，主机将使用指定容器网络的 MAC 地址。默认情况下、容器地址是随机生成的地址、但如果您使用节点配置密钥设置了一个 `_NETWORK_MAC`地址、则会改用该地址。主机和容器始终具有不同的 MAC 地址。

Mac 克隆使用情形

MAC 克隆需要考虑两种使用情形：

- MAC 克隆未启用：当节点配置文件中的 `_CLONE_MAC`密钥未设置或设置为 "false," 时，主机将使用主机 NIC MAC，除非在 `_NETWORK_MAC`密钥中指定了 MAC，否则容器将具有 StorageGRID 生成的 MAC。如果在 `_NETWORK_MAC`密钥中设置了地址，则容器将具有 `_NETWORK_MAC`密钥中指定的地址。
- MAC 克隆已启用：当节点配置文件中的 `_CLONE_MAC`密钥设置为"true"时，容器使用主机 NIC MAC，主机使用 StorageGRID 生成的 MAC，除非在 `_NETWORK_MAC`密钥中指定了 MAC。如果在 `_NETWORK_MAC`密钥中设置了地址，则主机使用指定的地址而不是生成的地址。

如果您不想使用 MAC 地址克隆，而是希望允许所有接口接收和传输除虚拟机管理程序分配的 MAC 地址之外的数据，请确保虚拟交换机和端口组级别的安全属性对于 MAC Address Changes 和 Forged Transmits 均设置为 **Accept**。虚拟交换机上设置的值可以被端口组级别的值覆盖，因此请确保两处的设置相同。

要启用MAC克隆，请参见"有关创建节点配置文件的说明"。

Mac 克隆示例

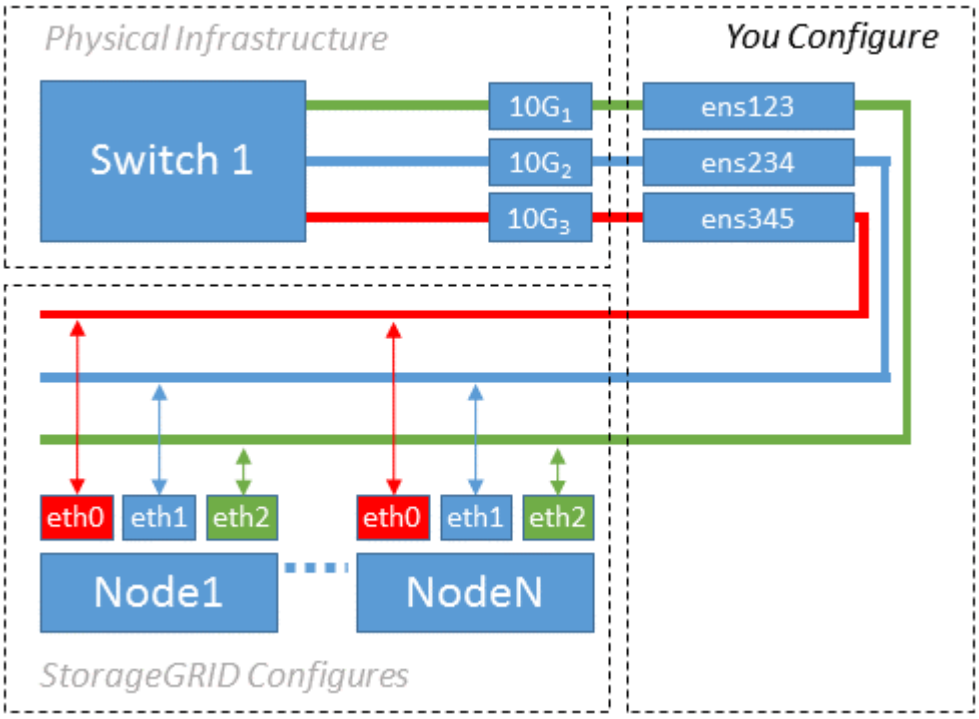
为主机启用MAC克隆的示例、其中、接口ens256的MAC地址为11：22：33：44：55：66、节点配置文件中的以下密钥为：

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

结果：ens256的主机MAC为b2：9c：02：C2：27：10、管理网络MAC为11：22：33：44：55：66

示例 **1** ： 映射到物理或虚拟 **NIC** 的一对一映射

示例 1 介绍了一个简单的物理接口映射，该映射只需要很少的主机端配置或根本不需要主机端配置。



Linux 操作系统创建 `ensXYZ`在安装或启动期间或热添加接口时自动添加接口。除了确保接口设置为启动后自动启动之外，不需要进行任何配置。您必须确定哪个 ensXYZ 对应哪个StorageGRID网络（网格、管理或客户端），以便您可以在稍后的配置过程中提供正确的映射。

请注意，此图显示了多个 StorageGRID 节点；但是，通常情况下，您会对单节点 VM 使用此配置。

如果交换机 1 是物理交换机，则应将连接到接口 10G1 到 10G3 的端口配置为访问模式，并将其放置在相应的 VLAN 上。

示例 **2** ： **LACP** 绑定传输 **VLAN**

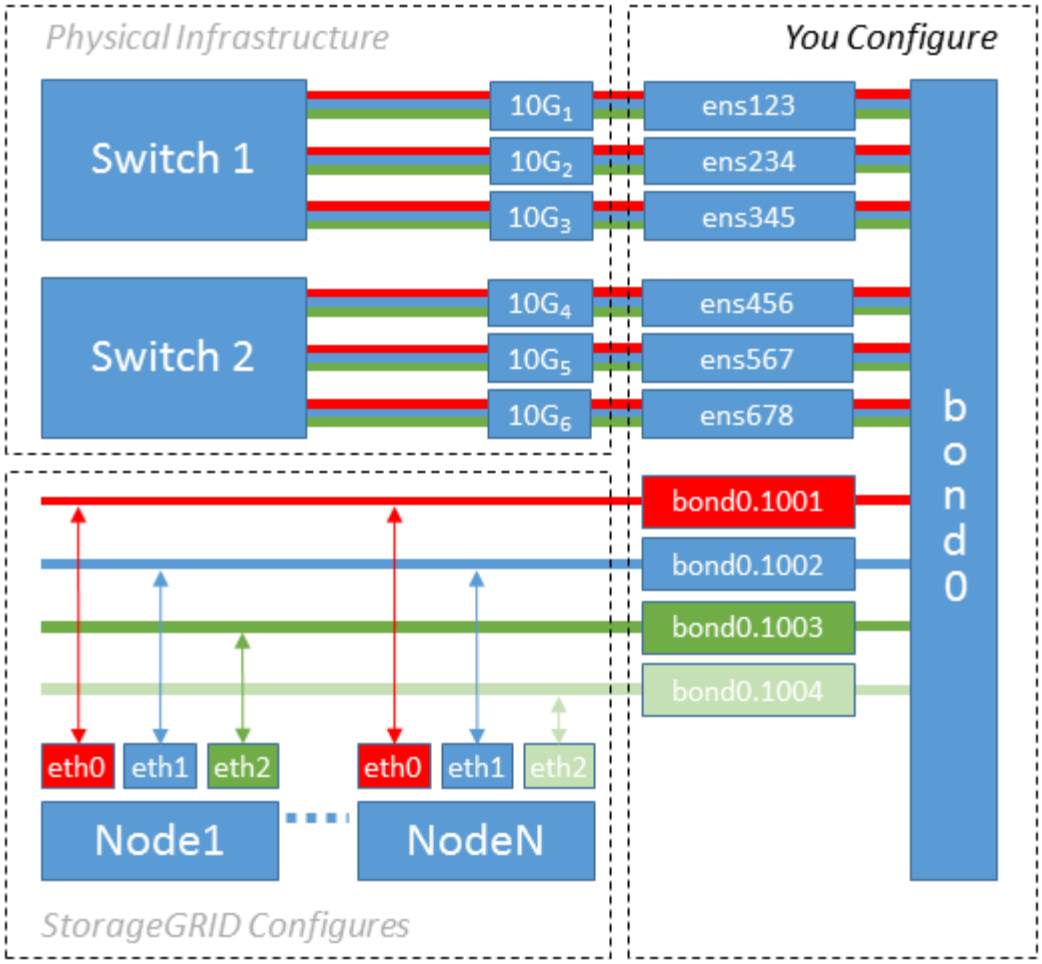
示例 2 假定您熟悉绑定网络接口以及在所使用的 Linux 分发版上创建 VLAN 接口。

关于此任务

示例 2 介绍了一种基于 VLAN 的通用灵活方案，该方案有助于在单个主机上的所有节点之间共享所有可用网络带宽。此示例尤其适用于裸机主机。

要了解此示例，假设每个数据中心有三个单独的网格网络，管理员网络和客户端网络子网。子网位于不同的 VLAN （ 1001 ， 1002 和 1003 ）上，并通过 LACP 绑定的中继端口（ bond0 ）提供给主机。您应在此绑定上配置三个 VLAN 接口： bond0.1001 ， bond0.1002 和 bond0.1003 。

如果同一主机上的节点网络需要单独的 VLAN 和子网，则可以在绑定上添加 VLAN 接口并将其映射到主机（如图中的 bond0.1004 所示）。



步骤

1. 将用于 StorageGRID 网络连接的所有物理网络接口聚合到一个 LACP 绑定中。

   在每个主机上对绑定使用相同的名称，例如， `bond0` 。

2. 按照标准VLAN接口命名约定，创建使用此绑定作为其关联“物理设备”的VLAN接口 `physdev-name.VLAN ID`。

   请注意，步骤 1 和 2 要求对终止网络链路另一端的边缘交换机进行适当配置。此外，边缘交换机端口还必须聚合到 LACP 端口通道中，并配置为中继，并允许通过所有必需的 VLAN 。

   本文档提供了此每主机网络配置方案的示例接口配置文件。

相关信息

- "Ubuntu 和 Debian 的示例 /etc/network/interfaces"
- "RHEL 的示例 /etc/sysconfig/network-scripts"

为 **Linux** 部署配置 **StorageGRID** 主机存储

您必须为每个 Linux 主机分配块存储卷。

开始之前

您已阅读以下主题，其中提供了完成此任务所需的信息：

- "存储和性能要求"
- "节点容器迁移要求"

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

关于此任务

将块存储卷(LUN)分配给主机时、请使用"存储要求"中的表确定以下内容：

- 每个主机所需的卷数（根据要在该主机上部署的节点的数量和类型）
- 每个卷的存储类别（即系统数据或对象数据）
- 每个卷的大小

在主机上部署 StorageGRID 节点时，您将使用此信息以及 Linux 为每个物理卷分配的永久性名称。

> 您无需对这些卷中的任何卷进行分区、格式化或挂载；只需确保它们对主机可见即可。

> 对于纯元数据存储节点、只需要一个对象数据LUN。

(`/dev/sdb`例如，在编写卷名称列表时，请避免使用“原始”特殊设备文件。这些文件可能会在主机重新启动后发生更改，从而影响系统的正常运行。如果使用的是`iSCSI LUN`和设备映射程序多路径、请考虑在目录中使用多路径别名 `/dev/mapper`、尤其是在SAN拓扑包含指向共享存储的冗余网络路径时。或者、您也可以在下使用系统创建的软链接 `/dev/disk/by-path/`作为永久性设备名称。

例如：

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

每个安装的结果会有所不同。

为每个块存储卷分配友好名称，以简化初始 StorageGRID 安装和未来维护过程。如果使用设备映射程序多路径驱动程序冗余访问共享存储卷、则可以使用文件中的 `alias`字段 `/etc/multipath.conf`。

例如：

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

以这种方式使用别名字段会使别名在主机上的目录中显示为块设备 `/dev/mapper`、这样、每当配置或维护操作需要指定块存储卷时、您就可以指定一个便于识别且易于验证的名称。

如果要设置共享存储以支持StorageGRID节点迁移并使用设备映射程序多路径、则可以在所有主机上创建并安装公用。 `/etc/multipath.conf`只需确保在每个主机上使用不同的容器引擎存储卷即可。使用别名并将目标主机名包含在每个容器引擎存储卷 LUN 的别名中，这样便于记住，建议这样做。

不再支持将Docker用作纯软件部署的容器引擎。在未来版本中、Docker将被另一个容器引擎取代。

相关信息

- "配置容器引擎存储卷"
- "存储和性能要求"
- "节点容器迁移要求"

在 **Linux** 上为 **StorageGRID** 配置容器引擎存储卷

在安装 Docker 或 Podman 容器引擎之前，您可能需要格式化存储卷并挂载它。

> 不再支持将Docker用作纯软件部署的容器引擎。在未来版本中、Docker将被另一个容器引擎取代。

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

关于此任务

如果您计划将根卷用于 Docker 或 Podman 存储卷，并且主机分区上有足够的可用空间，则可以跳过以下步骤：

- Podman： `/var/lib/containers`
- Docker： `/var/lib/docker`

步骤

1. 在容器引擎存储卷上创建文件系统：

RHEL

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

Ubuntu 或 Debian

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. 挂载容器引擎存储卷：

RHEL

- 对于 Docker：

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

- 对于 Podman：

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

Ubuntu 或 Debian

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

- 对于 Podman：

```
sudo mkdir -p /var/lib/podman
sudo mount container-storage-volume-device /var/lib/podman
```

3. 将容器存储卷设备的条目添加到 /etc/fstab。
   - RHEL：容器存储卷设备
   - Ubuntu 或 Debian：docker-storage-volume-device

   此步骤可确保存储卷将在主机重新启动后自动重新挂载。

安装 **Docker**

StorageGRID系统可以作为容器集合在 Linux 上运行。

- 在为 Ubuntu 或 Debian 安装StorageGRID之前，您必须安装 Docker。
- 如果您选择使用 Docker 容器引擎，请按照以下步骤安装 Docker。否则，安装 Podman 。

> 不再支持将Docker用作纯软件部署的容器引擎。在未来版本中、Docker将被另一个容器引擎取代。

步骤

1. 按照适用于您的 Linux 版本的说明安装 Docker 。

如果您的 Linux 分发版不包含 Docker ，您可以从 Docker 网站下载它。

2. 运行以下两个命令，确保已启用并启动 Docker：

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 输入以下命令确认您已安装预期版本的 Docker：

```
sudo docker version
```

客户端和服务器版本必须为1.11.0或更高版本。

安装 **Podman**

StorageGRID系统作为容器集合运行。如果您选择使用 Podman 容器引擎，请按照以下步骤安装 Podman。否则，安装 Docker 。

步骤

1. 按照适用于您的 Linux 版本的说明安装 Podman 和 Podman-Docker 。

安装 Podman 时，您还必须安装 Podman-Docker 软件包。

2. 输入以下命令，确认您已安装所需的 Podman 和 Podman-Docker 版本：

```
sudo docker version
```

通过 Podman-Docker 软件包，您可以使用 Docker 命令。

客户端和服务器版本必须为3.2.3或更高版本。

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

相关信息

"配置主机存储"

在 **Linux** 上安装 **StorageGRID** 主机服务

您可以使用适合您的操作系统类型的StorageGRID包来安装StorageGRID主机服务。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

RHEL

您可以使用 StorageGRID RPM 软件包安装 StorageGRID 主机服务。

关于此任务

以下说明介绍如何从 RPM 软件包安装主机服务。或者、您也可以使用安装归档文件中包含的DNF存储库元数据远程安装RPM包。请参见适用于 Linux 操作系统的 DNF 存储库说明。

步骤

1. 将 StorageGRID RPM 软件包复制到每个主机，或使其在共享存储上可用。

   例如、将其放置在目录中 `/tmp`、以便在下一步中使用示例命令。

2. 以 root 身份或使用具有 sudo 权限的帐户登录到每个主机，然后按指定顺序运行以下命令：

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
```

   您必须先安装映像软件包，然后再安装服务软件包。

   如果您将软件包放置在以外的目录中 `/tmp`，请修改命令以反映您使用的路径。

Ubuntu 或 Debian

您可以使用StorageGRID DEB 包为 Ubuntu 或 Debian 安装StorageGRID主机服务。

关于此任务

以下说明介绍如何从 Deb 软件包安装主机服务。或者，您也可以使用安装归档中包含的 APT 存储库元数据远程安装 Deb 软件包。请参见适用于 Linux 操作系统的 APT 存储库说明。

步骤

1. 将 StorageGRID Deb 软件包复制到每个主机，或使其在共享存储上可用。

   例如、将其放置在目录中 `/tmp`、以便在下一步中使用示例命令。

2. 以 root 身份或使用具有 sudo 权限的帐户登录到每个主机，然后运行以下命令。

   您必须先安装软件包、然后 `service`再安装 `images`软件包。如果您将软件包放置在以外的目录中 `/tmp`，请修改命令以反映您使用的路径。

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-
SHA.deb
```

在安装StorageGRID包之前，必须先安装 Python 3。这 `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb`直到您完成此操作后，命令才会失败。

自动化基于软件的节点安装

在 **Linux** 上自动安装 **StorageGRID** 主机服务和配置网格节点

您可以自动安装 StorageGRID 主机服务和配置网格节点。

关于此任务

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

在以下任一情况下，自动部署可能会很有用：

- 您已使用标准业务流程框架（例如 Ansible ， Puppet 或 Chef ）部署和配置物理或虚拟主机。
- 您打算部署多个 StorageGRID 实例。
- 您正在部署一个大型的复杂 StorageGRID 实例。

StorageGRID 主机服务由软件包安装，并由配置文件驱动。您可以使用以下方法之一创建配置文件：

- "创建配置文件"在手动安装期间以交互方式进行安装。
- 如本文所述，提前（或以编程方式）准备配置文件，以便使用标准业务流程框架实现自动安装。

  StorageGRID提供了可选的Python脚本、用于自动配置StorageGRID设备和整个StorageGRID系统("网格")。您可以直接使用这些脚本、也可以对其进行检查、以了解如何使用"StorageGRID 安装 REST API"您自己开发的网格部署和配置工具。

自动安装和配置 **StorageGRID** 主机服务

您可以使用 Ansible ， Puppet ， Chef ， Fabric 或 SaltStack 等标准业务流程框架自动安装 StorageGRID 主机服务。

StorageGRID主机服务打包在 DEB（Ubuntu 或 Debian）或 RPM（RHEL）中，并由您可以提前（或以编程方式）准备的配置文件驱动，以实现自动安装。如果您已经使用标准编排框架来安装和配置您的 Linux 部署，那么将StorageGRID添加到您的剧本或配方中应该很简单。

您可以自动执行准备主机和部署虚拟网格节点的所有步骤。

Ansible 角色和攻略手册示例

安装归档文件在文件夹中提供了示例Ansive角色和操作手册 `/extras`。《安可解决方案手册》介绍了该角色如何 `storagegrid`准备主机并将StorageGRID安装到目标服务器上。您可以根据需要自定义角色或攻略手册。

此示例攻略手册不包括在启动 StorageGRID 主机服务之前创建网络设备所需的步骤。在完成并使用攻略手册之前，请添加以下步骤。

RHEL

对于 RHEL，提供的安装任务 `storagegrid`角色示例使用 `ansible.builtin.dnf`模块从本地 RPM 文件或远程 Yum 存储库执行安装。如果模块不可用或不受支持，您可能需要编辑以下文件中的相应 Ansible 任务以使用 `yum`或者 `ansible.builtin.yum`模块：

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Ubuntu 或 Debian

对于 Ubuntu 或 Debian，提供的安装任务 `storagegrid`角色示例使用 `ansible.builtin.apt`模块从本地 DEB 文件或远程 apt 存储库执行安装。如果模块不可用或不受支持，您可能需要编辑以下文件中的相应 Ansible 任务以使用 `ansible.builtin.apt`模块：

- `roles/storagegrid/tasks/deb_install_from_repo.yml`
- `roles/storagegrid/tasks/deb_install_from_local.yml`

自动配置 StorageGRID

部署网格节点后，您可以自动配置 StorageGRID 系统。

开始之前

- 您可以从安装归档中了解以下文件的位置。

文件名	说明
configure-storagegrid.py	用于自动配置的 Python 脚本
configure-storaggrid.sample.json	用于脚本的配置文件示例
configure-storaggrid.blank.json	用于脚本的空配置文件

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

存储修改后的密码部分的管理密码和配置密码 `configure-storagegrid.json`配置文件保存在安全的位置。安装、扩展和维护过程都需要这些密码。您还应该备份修改后的 `configure-storagegrid.json`配置文件并将其存储在安全的位置。

关于此任务

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

您也可以使用网格管理器或安装 API 配置系统。

步骤

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

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中 `platform`是 `debs、 rpms`或 `vsphere。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

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

结果

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

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

如果您指定应生成随机密码、请打开 `Passwords.txt`文件并查找访问StorageGRID系统所需的密码。

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

系统会在显示确认消息时安装并配置 StorageGRID 系统。

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

您可以使用VMware OVF工具自动部署网格节点。您还可以自动配置 StorageGRID 。

自动部署网格节点

使用VMware OVF工具自动部署网格节点。

开始之前

- 您可以访问使用 Bash 3.2 或更高版本的 Linux/Unix 系统。
- 您已安装VMware vSphere和vCenter
- 您已安装并正确配置 VMware OVF Tool。
- 您知道使用VF工具访问VMware vSphere所需的用户名和密码
- 您具有足够的权限从OVF文件部署VM并启动VM、以及创建附加卷以连接到VM的权限。有关详细信息、请参见 `ovftool`文档。
- 您知道 vSphere 中要部署 StorageGRID 虚拟机的位置的虚拟基础架构（ VI ） URL 。此 URL 通常为 vApp 或资源池。例如： `vi://vcenter.example.com/vi/sgws`

  您可以使用VMware `ovftool`实用程序确定此值(有关详细信息、请参见 `ovftool`文档)。

  如果要部署到 vApp ，虚拟机不会首次自动启动，您必须手动启动它们。

- 您已收集部署配置文件的所有必需信息。有关信息、请参见。"收集有关部署环境的信息"
- 您可以从适用于 StorageGRID 的 VMware 安装归档文件访问以下文件：

文件名	说明
netapp-sg-version-sha.vmdk	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。 *注意：*此文件必须与和 `.mf`文件位于同一文件夹中`.ovf`。
vsphere-primary-admin.OVF vsphere-primary-admin.mf	(`.mf`用于部署主管理节点(`.ovf`的开放式虚拟化格式模板文件()和清单文件()。
vsphere-non-primary-admin.OVF vsphere-non-primary-admin.mf	(`.mf`用于部署非主管理节点(`.ovf`的模板文件()和清单文件()。
vsphere-gateway.OVF vsphere-gateway.mf	(`.mf`用于部署网关节点(`.ovf`的模板文件()和清单文件()。
vsphere-storage.OVF vsphere-storage.mf	(`.mf`用于部署基于虚拟机的存储节点的模板(`.ovf`文件()和清单文件()。
deploy-vsphere-ovftool.sh	Bash shell 脚本，用于自动部署虚拟网格节点。

文件名	说明
deploy-vsphere-ovftool-sample.ini	用于脚本的示例配置文件 `deploy-vsphere-ovftool.sh`。

定义部署的配置文件

您可以在配置文件中指定为StorageGRID部署虚拟网格节点所需的信息、此配置文件由bash脚本使用 `deploy-vsphere-ovftool.sh`。您可以修改示例配置文件、这样就不必从头开始创建该文件。

步骤

1. 为示例配置文件创建一份副本(`deploy-vsphere-ovftool.sample.ini`)。将新文件另存为，保存 `deploy-vsphere-ovftool.ini`在与相同的目录中 `deploy-vsphere-ovftool.sh`。
2. 打开 `deploy-vsphere-ovftool.ini`。
3. 输入部署 VMware 虚拟网格节点所需的所有信息。

   有关信息、请参见。配置文件设置

4. 输入并验证所有必要信息后，请保存并关闭此文件。

配置文件设置

`deploy-vsphere-ovftool.ini`配置文件包含部署虚拟网格节点所需的设置。

配置文件首先列出全局参数，然后在节点名称定义的部分中列出节点专用参数。使用文件时：

- 全局参数 _ 应用于所有网格节点。
- _Node-specific parameters_override 全局参数。

全局参数

全局参数将应用于所有网格节点，除非它们被各个部分中的设置所覆盖。将应用于多个节点的参数置于全局参数部分中，然后根据需要在各个节点的部分中覆盖这些设置。

- * OVFTOOL_FUFFESESESESES* ： 您可以将 OVFTOOL_FUFFICESPORITES* 指定为全局设置，也可以将参数单独应用于特定节点。例如：

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  您可以使用 `--powerOffTarget`和选项关闭和 `--overwrite`更换现有虚拟机。

  > 您应将节点部署到不同的数据存储库，并为每个节点指定 OVFTOOL_FUFFICESYUESYUESL ，而不是全局参数。

- **source**：StorageGRID虚拟机模板(`.vmdk`)文件以及 `.ovf`各个网格节点的和 `.mf`文件的路径。默认为当前目录。

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- * 目标 * ： 要部署 StorageGRID 的位置的 VMware vSphere 虚拟基础架构（ VI ） URL 。例如：

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- * 网格网络配置 * ： 用于获取静态或 DHCP IP 地址的方法。默认值为 static 。如果所有或大多数节点使用相同的方法获取 IP 地址，则可以在此处指定该方法。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_CONFIG = STATIC
```

- * 网格网络目标 * ： 要用于网格网络的现有 VMware 网络的名称。如果所有或大多数节点使用相同的网络名称，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_TARGET = SG Admin Network
```

- * 网格网络掩码 * ： 网格网络的网络掩码。如果所有或大多数节点使用相同的网络掩码，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_MASK = 255.255.255.0
```

- * 网格网络网关 * ： 网格网络的网络网关。如果所有或大多数节点使用同一个网络网关，则可以在此处指定此网关。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- * 网格网络 MTU * ： 可选。网格网络上的最大传输单元（ MTU ）。如果指定，则此值必须介于 1280 和 9216 之间。例如：

```
GRID_NETWORK_MTU = 9000
```

  如果省略，则使用 1400 。

  如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。

网络的MTU值必须与节点连接到的vSphere中虚拟交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

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

- * 管理网络配置 * ： 用于获取 IP 地址的方法，可以是禁用，静态或 DHCP 。默认值为 disabled 。如果所有或大多数节点使用相同的方法获取 IP 地址，则可以在此处指定该方法。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_CONFIG = STATIC
```

- * 管理网络目标 * ： 用于管理网络的现有 VMware 网络的名称。除非禁用管理网络，否则此设置为必填项。如果所有或大多数节点使用相同的网络名称，则可以在此处指定。与网格网络不同、所有节点都不需要连接到同一个管理网络。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- * 管理网络掩码 * ： 管理网络的网络掩码。如果使用的是静态 IP 寻址，则需要此设置。如果所有或大多数节点使用相同的网络掩码，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- * 管理网络网关 * ： 管理网络的网络网关。如果您使用的是静态 IP 寻址，并且在 admin_network_esl 设置中指定了外部子网，则需要此设置。(也就是说、如果admin_network_不必 为空。)如果所有或大多数节点使用同一个网络网关，则可以在此处指定此网关。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- * 管理网络 _NETWORK_ESL* ： 管理网络的外部子网列表（路由），指定为 CIDR 路由目标的逗号分隔列表。如果所有或大多数节点使用相同的外部子网列表，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- * 管理网络 MTU * ： 可选。管理网络上的最大传输单元（ MTU ）。如果admin_network_config = dhcp、请勿指定。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1400 。如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。如果所有或大多数节点对管理网络使用相同的 MTU ，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
ADMIN_NETWORK_MTU = 8192
```

- * 客户端网络配置 * ：用于获取 IP 地址的方法，可以是禁用，静态或 DHCP 。默认值为 disabled 。如果所有或大多数节点使用相同的方法获取 IP 地址，则可以在此处指定该方法。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_CONFIG = STATIC
```

- * 客户端网络目标 * ：用于客户端网络的现有 VMware 网络的名称。除非禁用客户端网络，否则此设置为必填项。如果所有或大多数节点使用相同的网络名称，则可以在此处指定。与网格网络不同、所有节点无需连接到同一客户端网络。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- * 客户端网络掩码 * ：客户端网络的网络掩码。如果使用的是静态 IP 寻址，则需要此设置。如果所有或大多数节点使用相同的网络掩码，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- * 客户端网络网关 * ：客户端网络的网络网关。如果使用的是静态 IP 寻址，则需要此设置。如果所有或大多数节点使用同一个网络网关，则可以在此处指定此网关。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- * 客户端网络 MTU * ：可选。客户端网络上的最大传输单元（ MTU ）。如果client_network_config = dhcp、请勿指定。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1400 。如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。如果所有或大多数节点对客户端网络使用相同的 MTU ，则可以在此处指定。然后，您可以通过为一个或多个节点指定不同的设置来覆盖全局设置。例如：

```
CLIENT_NETWORK_MTU = 8192
```

- * 端口重新映射 * ：重新映射节点用于内部网格节点通信或外部通信的任何端口。如果企业网络策略限制 StorageGRID 使用的一个或多个端口，则必须重新映射端口。有关StorageGRID使用的端口列表，请参见中的内部网格节点通信和外部通信"网络连接准则"。

> 不要重新映射计划用于配置负载平衡器端点的端口。

> 如果仅设置 port_remap ，则您指定的映射将同时用于入站和出站通信。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。

使用的格式为： *network type/protocol/default port used by grid node/new port*，其中网络类型为网格、管理或客户端，协议为TCP或UDP。

例如：

```
PORT_REMAP = client/tcp/18082/443
```

如果单独使用，则此示例设置会将网格节点的入站和出站通信从端口 18082 对称映射到端口 443 。如果与 port_remap_inbound 结合使用，则此示例设置会将出站通信从端口 18082 映射到端口 443 。

您还可以使用逗号分隔列表重新映射多个端口。

例如：

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- * 端口重新映射入站 * ：重新映射指定端口的入站通信。如果指定port_remap_inbound、但未指定port_remap值、则端口的出站通信将保持不变。

  不要重新映射计划用于配置负载平衡器端点的端口。

使用的格式为： *network type/protocol/_default port used by grid node/new port*，其中网络类型为网格、管理或客户端，协议为TCP或UDP。

例如：

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

此示例将接收发送到端口 443 以通过内部防火墙的流量，并将其定向到端口 18082 ，网格节点正在侦听 S3 请求。

您还可以使用逗号分隔列表重新映射多个入站端口。

例如：

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **temporal_password_type**：在节点加入网格之前访问VM控制台或StorageGRID安装API或使用SSH时要使用的临时安装密码类型。

  如果所有或大多数节点使用相同类型的临时安装密码、请在全局参数部分中指定类型。然后、可以选择对单个节点使用其他设置。例如，如果选择*全局使用自定义密码*，则可以使用<password>*来设置每个节点的密码。

*temporal_password_type*可以是以下项之一：

- 使用节点名称：节点名称用作临时安装密码、用于访问VM控制台、StorageGRID安装API和SSH。
- 禁用密码：不使用临时安装密码。如果您需要访问VM来调试安装问题，请参见"对安装问题进行故障排除"。
- 使用自定义密码：在*custom_temporal_password=SSH*中提供的值用作临时安装密码，并提供对VM控制台、安装<password>和StorageGRID的访问。

  或者，您可以省略*temporal_password_type*参数，而只指定<password>。

- **CUSTOM_Temporal_password=CUSTOM**<password>可选。访问VM控制台、StorageGRID安装API和SSH时要在安装期间使用的临时密码。如果将*temporal_password_type*设置为*use node name*或*Disable password*，则忽略此选项。

节点专用参数

每个节点都位于配置文件中各自的部分中。每个节点都需要以下设置：

- 此部分标题定义了将在网格管理器中显示的节点名称。您可以通过为节点指定可选的 node_name 参数来覆盖该值。
- **NODE_type**：VM_Admin_Node、VM_Storage_Node或VM_API_Gateway
- **storage_type**：组合、数据或元数据。如果未指定此存储节点可选参数、则默认为组合(数据和元数据)。有关详细信息，请参见 "存储节点的类型"。
- * 网格网络 IP ： 网格网络上节点的 IP 地址。
- * 管理网络 IP ： 管理网络上节点的 IP 地址。只有当节点已连接到管理网络且 admin_network_config 设置为 static 时才需要。
- * 客户端网络 IP* ： 客户端网络上节点的 IP 地址。只有当节点已连接到客户端网络且此节点的 client_network_config 设置为 static 时才需要此选项。
- * 管理 _IP* ： 网格网络上主管理节点的 IP 地址。使用指定的值作为主管理节点的 grid_network_IP 。如果省略此参数，则节点将尝试使用 mDNS 发现主管理节点 IP 。有关详细信息，请参见 "网格节点如何发现主管理节点"。

  对于主管理节点， admin_ip 参数将被忽略。

- 未全局设置的任何参数。例如，如果某个节点已连接到管理网络，而您未全局指定 admin_network 参数，则必须为此节点指定这些参数。

主管理节点

主管理节点需要以下附加设置：

- * 节点类型 * ： VM_Admin_Node
- * 管理角色 * ： 主

此示例条目适用于所有三个网络上的主管理节点：

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

以下附加设置对于主管理节点是可选的：

- * 磁盘 * ：默认情况下，会为管理节点另外分配两个 200 GB 的硬盘，以供审核和数据库使用。您可以使用 disk 参数增加这些设置。例如：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  对于管理节点，实例必须始终等于 2 。

存储节点

存储节点需要以下附加设置：

- * 节点类型 * ： VM_Storage_Node

  此示例条目适用于网格和管理网络上的存储节点，但不适用于客户端网络。此节点使用 admin_ip 设置指定网格网络上主管理节点的 IP 地址。

  ```
  [DC1-S1]
    NODE_TYPE = VM_Storage_Node

    GRID_NETWORK_IP = 10.1.0.3
    ADMIN_NETWORK_IP = 10.3.0.3

    ADMIN_IP = 10.1.0.2
  ```

  第二个示例条目适用于客户端网络上的存储节点，其中，客户的企业网络策略指出， S3 客户端应用程序仅允许使用端口 80 或 443 访问存储节点。示例配置文件使用 port_remap 使存储节点能够通过端口 443 发送和接收 S3 消息。

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

最后一个示例为从端口 22 到端口 3022 的 ssh 流量创建了对称重新映射，但明确设置了入站和出站流量的值。

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

以下附加设置对于存储节点是可选的：

- * 磁盘 * ：默认情况下，为存储节点分配三个 4 TB 磁盘，以供 RangeDB 使用。您可以使用 disk 参数增加这些设置。例如：

```
DISK = INSTANCES=16, CAPACITY=4096
```

- 存储类型：默认情况下、所有新存储节点均配置为同时存储对象数据和元数据、称为"组合存储节点"。您可以将存储节点类型更改为仅存储带有storage_type参数的数据或元数据。例如：

```
STORAGE_TYPE = data
```

网关节点

网关节点需要以下附加设置：

- * 节点类型 * ： VM_API_Gateway

此示例条目适用于所有三个网络上的示例网关节点。在此示例中，未在配置文件的全局部分中指定客户端网络参数，因此必须为节点指定这些参数：

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG Client Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

非主管理节点

非主管理节点需要以下附加设置：

- * 节点类型 * ： VM_Admin_Node
- * 管理角色 * ：非主要

此示例条目适用于不在客户端网络上的非主管理节点：

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG Grid Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

以下附加设置对于非主管理节点是可选的：

- * 磁盘 * ：默认情况下，会为管理节点另外分配两个 200 GB 的硬盘，以供审核和数据库使用。您可以使用 disk 参数增加这些设置。例如：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  对于管理节点，实例必须始终等于 2 。

运行 **Bash** 脚本

您可以使用 `deploy-vsphere-ovftool.sh`bash脚本和修改后的deploy-vsphere-ovftool.ini配置文件在VMware vSphere中自动部署StorageGRID节点。

开始之前

您已为您的环境创建 deploy-vsphere-ovftool.ini 配置文件。

您可以通过输入help命令来使用bash脚本中提供的帮助(`-h/--help`。例如：

```
./deploy-vsphere-ovftool.sh -h
```

或

```
./deploy-vsphere-ovftool.sh --help
```

步骤

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

   例如：

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. 要部署所有网格节点，请使用适用于您环境的选项运行 Bash 脚本。

   例如：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
   vsphere-ovftool.ini
   ```

4. 如果某个网格节点由于出现错误而无法部署，请解决此错误并仅为该节点重新运行 Bash 脚本。

   例如：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
   -node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

当每个节点的状态为"已传递"时、部署完成。

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

自动配置 StorageGRID

部署网格节点后，您可以自动配置 StorageGRID 系统。

开始之前

- 您可以从安装归档中了解以下文件的位置。

文件名	说明
configure-storagegrid.py	用于自动配置的 Python 脚本
configure-storaggrid.sample.json	用于脚本的配置文件示例
configure-storaggrid.blank.json	用于脚本的空配置文件

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

> 存储修改后的密码部分的管理密码和配置密码 `configure-storagegrid.json`配置文件保存在安全的位置。安装、扩展和维护过程都需要这些密码。您还应该备份修改后的 `configure-storagegrid.json`配置文件并将其存储在安全的位置。

关于此任务

您可以使用 `configure-storagegrid.py`Python脚本和 `configure-storagegrid.json`网格配置文件自动配置StorageGRID系统。

> 您也可以使用网格管理器或安装 API 配置系统。

步骤

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

   例如：

```
cd StorageGRID-Webscale-version/platform
```

其中 `platform`是Debs、rpms或vSphere。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

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

结果

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

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

如果您指定应生成随机密码、请打开 `Passwords.txt`文件并查找访问StorageGRID系统所需的密码。

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

系统会在显示确认消息时安装并配置 StorageGRID 系统。

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

相关信息

- "导航到网格管理器"
- "安装REST API"

部署虚拟网格节点

为 **StorageGRID** 收集有关 **VMware** 环境的信息

在部署网格节点之前，您必须收集有关网络配置和 VMware 环境的信息。

对所有节点执行一次安装比现在安装某些节点以及稍后安装某些节点更高效。

VMware 信息

您必须访问部署环境并收集以下信息： VMware 环境；为网格网络，管理网络和客户端网络创建的网络；以及计划用于存储节点的存储卷类型。

您必须收集有关 VMware 环境的信息，包括以下信息：

- 具有完成部署所需的适当权限的 VMware vSphere 帐户的用户名和密码。
- 每个StorageGRID节点虚拟机的主机、数据存储库和网络配置信息。

> VMware Live vMotion 会导致虚拟机时钟时间跳转，任何类型的网格节点均不支持此功能。尽管时钟时间不正确，但极少会导致数据丢失或配置更新。

网格网络信息

您必须收集有关为 StorageGRID 网格网络（必需）创建的 VMware 网络的信息，包括：

- 网络名称。
- 用于分配静态或 DHCP IP 地址的方法。
  - 如果使用的是静态 IP 地址，则为每个网格节点提供所需的网络详细信息（ IP 地址，网关，网络掩码）。
  - 如果使用DHCP、则为网格网络上主管理节点的IP地址。有关详细信息、请参见 "网格节点如何发现主管理节点" 。

管理网络信息

对于要连接到可选 StorageGRID 管理网络的节点，您必须收集有关为此网络创建的 VMware 网络的信息，包括：

- 网络名称。
- 用于分配静态或 DHCP IP 地址的方法。
  - 如果使用的是静态 IP 地址，则为每个网格节点提供所需的网络详细信息（ IP 地址，网关，网络掩码）。
  - 如果使用DHCP、则为网格网络上主管理节点的IP地址。有关详细信息、请参见 "网格节点如何发现主管理节点" 。
- 管理网络的外部子网列表（ ESL ）。

客户端网络信息

对于要连接到可选 StorageGRID 客户端网络的节点，您必须收集有关为此网络创建的 VMware 网络的信息，包括：

- 网络名称。
- 用于分配静态或 DHCP IP 地址的方法。
- 如果使用的是静态 IP 地址，则为每个网格节点提供所需的网络详细信息（ IP 地址，网关，网络掩码）。

有关其他接口的信息

安装节点后，您可以选择在 vCenter 中为虚拟机添加中继或访问接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

您添加的接口将显示在 "VLAN interfaces" 页面和网格管理器的 "HA Groups" 页面上。

- 如果要添加中继接口，请为每个新的父接口配置一个或多个 VLAN 接口。请参阅。 "配置 VLAN 接口"
- 如果添加访问接口，则必须将其直接添加到 HA 组。请参阅。 "配置高可用性组"

虚拟存储节点的存储卷

您必须收集基于虚拟机的存储节点的以下信息：

- 您计划添加的存储卷(存储LUN)的数量和大小。请参见。"存储和性能要求"

网格配置信息

您必须收集信息才能配置网格：

- 网格许可证
- 网络时间协议（ NTP ）服务器 IP 地址
- DNS服务器IP地址

为 **Linux** 部署创建 **StorageGRID** 节点配置文件

节点配置文件是一个小型文本文件，用于提供 StorageGRID 主机服务启动节点并将其连接到适当的网络和块存储资源所需的信息。节点配置文件用于虚拟节点、而不用于设备节点。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

节点配置文件的位置

将每个StorageGRID节点的配置文件放在要运行该节点的主机上的目录中 `/etc/storagegrid/nodes`。例如、如果您计划在HostA上运行一个管理节点、一个网关节点和一个存储节点、则必须将三个节点配置文件放在HostA上的中 `/etc/storagegrid/nodes`。

您可以使用文本编辑器（例如 vim 或 nanan ）在每个主机上直接创建配置文件，也可以在其他位置创建配置文件并将其移动到每个主机。

节点配置文件的命名

配置文件的名称非常重要。格式为 `node-name.conf`，其中 `node-name`是您分配给节点的名称。此名称显示在 StorageGRID 安装程序中，用于节点维护操作，例如节点迁移。

节点名称必须遵循以下规则：

- 必须是唯一的
- 必须以字母开头
- 可以包含字符 A 到 Z 和 a 到 z
- 可以包含数字 0 到 9
- 可以包含一个或多个连字符（ - ）
- 不得超过32个字符、不包括 `.conf`扩展名

主机服务不会解析中未遵循这些命名约定的任何文件 `/etc/storagegrid/nodes`。

如果您为网格规划了多站点拓扑，则典型的节点命名方案可能是：

```
site-nodetype-nodenumber.conf
```

例如、您可以为Data Center 1中的第一个管理节点和 `dc2-sn3.conf`Data Center 2中的第三个存储节点使用 `dc1-adm1.conf`。但是，只要所有节点名称都遵循命名规则，您就可以使用所需的任何方案。

节点配置文件的内容

配置文件包含密钥/值对、每行一个密钥和一个值。对于每个键/值对、请遵循以下规则：

- 键和值必须用等号(=()和可选空格分隔。
- 密钥不能包含空格。
- 这些值可以包含嵌入的空格。
- 忽略任何前导或尾随空格。

下表定义了所有受支持密钥的值。每个键都具有以下名称之一：

- 必需：每个节点或指定节点类型都需要此参数
- 最佳实践：可选、但建议使用
- 可选：对于所有节点均为可选

管理网络密钥

admin_ip

价值	名称
您要用于安装基于 Linux 的节点的管理节点的网格网络 IPv4 地址。对于恢复，如果可用，请使用主管理节点的 IP；否则，使用非主管理节点的 IP。如果省略此参数，节点将尝试使用 mDNS 发现主管理节点。 "网格节点如何发现主管理节点"	最佳实践

admin_network_config

价值	名称
DHCP ，静态或已禁用	可选

admin_network_esl

价值	名称
此节点应使用管理网络网关与之通信的子网的逗号分隔列表、采用CIDR表示法。 示例： `172.16.0.0/21,172.17.0.0/21`	可选

admin_network_gateway

价值	名称

此节点的本地管理网络网关的 IPv4 地址。必须位于 admin_network_ip 和 admin_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。
 	
示例
 	
`1.1.1.1`
 	
`10.224.4.81`
	如果指定为、则为必填项 `ADMIN_NETWORK_ESL`。否则为可选。

admin_network_ip

价值	名称

此节点在管理网络上的 IPv4 地址。只有在admin_network_config = static"时才需要此密钥；不要为其他值指定此密钥。
 	
示例
 	
`1.1.1.1`
 	
`10.224.4.81`
	admin_network_config = static"时为必需项。
	
	否则为可选。

admin_network_MAC

价值	名称
容器中管理网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `b2:9c:02:c2:27:10`	可选

admin_network_mask

价值	名称

此节点的 IPv4 网络掩码，位于管理网络上。当admin_network_config = static"时指定此密钥；不要为其他值指定此密钥。
 	
示例
 	
`255.255.255.0`
 	
`255.255.248.0`
	如果指定了admin_network_IP且admin_network_config = static"、则此字段为必需字段。
	
	否则为可选。

admin_network_mtu

价值	名称

管理网络上此节点的最大传输单元（ MTU ）。如果admin_network_config = dhcp、请勿指定。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
 	
如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
 	
• 重要信息 * ：网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
 	
示例
 	
`1500`
 	
`8192`
	可选

admin_network_target

价值	名称

StorageGRID 节点用于管理网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 grid_network_target 或 client_network_target 指定的接口名称不同。
 	
注意：不要使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
 	
• 最佳实践 * ：指定一个值，即使此节点最初不具有管理员网络 IP 地址也是如此。然后，您可以稍后添加管理员网络 IP 地址，而无需重新配置主机上的节点。
 	
示例
 	
`bond0.1002`
 	
`ens256`
	最佳实践

admin_network_target_type

价值	名称
DedicatedInterface （这是唯一支持的值。）	可选

admin_network_target_type_interface_clone_MAC

价值	名称
判断对错 将密钥设置为 "true" 以发生原因 StorageGRID 容器使用管理网络上主机主机目标接口的 MAC 地址。 有关 Linux 的 MAC 克隆的更多详细信息，请参阅"MAC 地址克隆的注意事项和建议"	最佳实践

管理角色

价值	名称
主要或非主要 只有当NODE_TYPE = VM_Admin_Node时、才需要此密钥；不要为其他节点类型指定此密钥。	当NODE_TYPE = VM_Admin_Node时为必需项 否则为可选。

块设备密钥

block_device_audit_logs

价值	名称

此节点将用于永久存储审核日志的块设备专用文件的路径和名称。
 	
示例
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	对于节点类型为VM_Admin_Node的节点为必需项。请勿为其他节点类型指定此名称。

block_device_RANGEDB_nnn

价值	名称

此节点将用于永久性对象存储的块设备专用文件的路径和名称。只有节点类型为VM_Storage_Node的节点才需要此密钥；请勿为其他节点类型指定此密钥。
 	
仅需要 block_device_RANGEDB_000 ； 其余为可选。为 block_device_RANGEDB_000 指定的块设备必须至少为 4 TB ； 其他块设备可以更小。
 	
不要留下空隙。如果指定 block_device_RANGEDB_005 ，则还必须指定 block_device_RANGEDB_004 。
 	
• 注 * ： 为了与现有部署兼容，升级后的节点支持两位数的密钥。
 	
示例
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	必填：
	
	BLOCK_DEVICE_RANGEDB_000
	
	可选：
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

block_device_tables

价值	名称

此节点将用于永久存储数据库表的块设备专用文件的路径和名称。只有节点类型为VM_Admin_Node的节点才需要此密钥；不要为其他节点类型指定此密钥。
 	
示例
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	必填

block_device_var_local

价值	名称

此节点将用于其永久性存储的块设备专用文件的路径和名称 `/var/local`。
 	
示例
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	必填

客户端网络密钥

client_network_config

价值	名称
DHCP ，静态或已禁用	可选

client_network_gateway

价值	名称

此节点的本地客户端网络网关的 IPv4 地址，该地址必须位于 client_network_ip 和 client_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。
 	
示例
 	
`1.1.1.1`
 	
`10.224.4.81`
	可选

client_network_IP

价值	名称

此节点在客户端网络上的 IPv4 地址。
 	
只有当client_network_config = static"时才需要此密钥；不要为其他值指定此密钥。
 	
示例
 	
`1.1.1.1`
 	
`10.224.4.81`
	当client_network_config = static"时为必需项
	
	否则为可选。

客户端网络 **MAC**

价值	名称
容器中客户端网络接口的 MAC 地址。 此字段为可选字段。如果省略此参数，则会自动生成 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `b2:9c:02:c2:27:20`	可选

client_network_mask

价值	名称

此节点在客户端网络上的 IPv4 网络掩码。
 	
当client_network_config = static"时指定此密钥；不要为其他值指定此密钥。
 	
示例
 	
`255.255.255.0`
 	
`255.255.248.0`
	如果指定了client_network_IP且client_network_config = static,则为必需项
	
	否则为可选。

client_network_mtu

价值	名称

客户端网络上此节点的最大传输单元（ MTU ）。如果client_network_config = dhcp、请勿指定。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
 	
如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
 	
• 重要信息 *： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
 	
示例
 	
`1500`
 	
`8192`
	可选

client_network_target

价值	名称

StorageGRID 节点用于客户端网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 grid_network_target 或 admin_network_target 指定的接口名称不同。
 	
注意：不要使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
 	
• 最佳实践： * 指定一个值，即使此节点最初不会具有客户端网络 IP 地址也是如此。然后，您可以稍后添加客户端网络 IP 地址，而无需重新配置主机上的节点。
 	
示例
 	
`bond0.1003`
 	
`ens423`
	最佳实践

client_network_target_type

价值	名称
DedicatedInterface（这是唯一支持的值。）	可选

client_network_target_type_interface_clone_MAC

价值	名称
判断对错 将密钥设置为 "true" ，以便对 StorageGRID 容器进行发生原因 处理，以使用客户端网络上主机目标接口的 MAC 地址。 有关 Linux 的 MAC 克隆的更多详细信息，请参阅"MAC 地址克隆的注意事项和建议"	最佳实践

网格网络密钥

grid_network_config

价值	名称
静态或 DHCP 如果未指定、则默认为static"。	最佳实践

grid_network_gateway

价值	名称
此节点的本地网格网络网关的 IPv4 地址，该网关必须位于 grid_network_ip 和 grid_network_mask 定义的子网上。对于配置了 DHCP 的网络，此值将被忽略。 如果网格网络是没有网关的单个子网，请使用该子网的标准网关地址（ X.y.Z.1 ）或此节点的 GRID_NETWORK_IP 值；任一值都将简化未来可能进行的网格网络扩展。	必填

GRID_NETWORK_IP

价值	名称

此节点在网格网络上的 IPv4 地址。只有当GRID_NETWORK_config = STATIC时、才需要此密钥；不要为其他值指定此密钥。
 	
示例
 	
`1.1.1.1`
 	
`10.224.4.81`
	如果grid network config = static,则需要此参数
	
	否则为可选。

GRID_NETWORK_MAC

价值	名称
容器中网格网络接口的 MAC 地址。 必须为 6 对十六进制数字，以冒号分隔。 示例： `b2:9c:02:c2:27:30`	可选 如果省略此参数，则会自动生成 MAC 地址。

grid_network_mask

价值	名称

此节点在网格网络上的 IPv4 网络掩码。如果grid network_config = static"、请指定此密钥；不要为其他值指定此密钥。
 	
示例
 	
`255.255.255.0`
 	
`255.255.248.0`
	如果指定了grid network_IP且grid network_config = static"、则此字段为必需字段。
	
	否则为可选。

grid_network_mtu

价值	名称

网格网络上此节点的最大传输单元（ MTU ）。如果grid network_config = dhcp、请勿指定。如果指定，则此值必须介于 1280 和 9216 之间。如果省略，则使用 1500 。
 	
如果要使用巨型帧，请将 MTU 设置为适合巨型帧的值，例如 9000 。否则，请保留默认值。
 	
• 重要信息 * ： 网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。
• 重要信息 * ： 为获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的MTU值都必须相同。
 	
示例
 	
`1500`
 	
`8192`
	可选

grid_network_target

价值	名称

StorageGRID 节点要用于网格网络访问的主机设备的名称。仅支持网络接口名称。通常，您使用的接口名称与为 admin_network_target 或 client_network_target 指定的接口名称不同。
 	
注意：不要使用绑定或网桥设备作为网络目标。可以在绑定设备上配置 VLAN （或其他虚拟接口），也可以使用网桥和虚拟以太网（ veth ）对。
 	
示例
 	
`bond0.1001`
 	
`ens192`
	必填

grid_network_target_type

价值	名称
DedicatedInterface （这是唯一支持的值。）	可选

grid_network_target_type_interface_clone_MAC

价值	名称
判断对错 将密钥值设置为 "true" ，以便对 StorageGRID 容器进行发生原因 处理，以使用网格网络上主机目标接口的 MAC 地址。 有关 Linux 的 MAC 克隆的更多详细信息，请参阅"MAC 地址克隆的注意事项和建议"	最佳实践

安装密码密钥(临时)

Custom_Temporal_password_Hash

价值	名称
对于主管理节点、请在安装期间为StorageGRID安装API设置默认临时密码。 注意：仅在主管理节点上设置安装密码。如果您尝试在其他节点类型上设置密码、则验证节点配置文件将失败。 安装完成后、设置此值不起作用。 如果省略此密钥、则默认情况下不会设置任何临时密码。或者、您也可以使用StorageGRID安装API设置临时密码。 必须为 `crypt()`SHA-512密码哈希、其格式至少为8个字符、并且 `$6$<salt>$<password hash>`不超过32个字符。 可以使用命令行界面工具(例如SHA-512模式下的命令)生成此哈希 `openssl passwd`。	最佳实践

接口密钥

interface_target_nnnnnn

价值	名称
要添加到此节点的额外接口的名称和可选问题描述 。您可以向每个节点添加多个额外接口。 对于_nnnn_、请为要添加的每个interface_target条目指定一个唯一编号。 对于此值，请指定裸机主机上物理接口的名称。然后，也可以添加一个逗号并提供接口的问题描述 ，该接口将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。 示例： `INTERFACE_TARGET_0001=ens256, Trunk` 如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口、则可以将该接口直接添加到HA组；无需配置VLAN接口。	可选

最大**RAM**密钥

最大 **RAM**

价值	名称
此节点允许使用的最大 RAM 量。如果省略此密钥，则节点不存在内存限制。在为生产级节点设置此字段时，请指定一个值，该值应至少比系统 RAM 总量少 24 GB ，并且要少 16 到 32 GB 。 • 注 * ： RAM 值会影响节点的实际元数据预留空间。请参见"什么是元数据预留空间的问题描述"。 此字段的格式为 *numberunit*，其中 *unit*`可以是 `b、、 `k m`或 `g。  示例  `24g`  `38654705664b` • 注 * ：如果要使用此选项，必须为内存 cgroups 启用内核支持。	可选

节点类型密钥

node_type

价值	名称
节点类型： • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway	必填

storage_type

价值	名称
定义存储节点包含的对象类型。有关详细信息，请参见 "存储节点的类型"。只有节点类型为VM_Storage_Node的节点才需要此密钥；请勿为其他节点类型指定此密钥。存储类型： • 综合 • 数据 • 元数据 注意：如果未指定storage_type、则存储节点类型默认设置为组合(数据和元数据)。	可选

端口重新映射密钥



对端口重新映射的支持已弃用，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除裸机主机上的端口重新映射"。

port_remap

价值	名称
重新映射节点用于内部网格节点通信或外部通信的任何端口。如果企业网络策略限制StorageGRID使用的一个或多个端口，则需要重新映射端口，如或中所述"内部网格节点通信""外部通信"。 重要：不要重新映射计划用于配置负载平衡器端点的端口。 • 注意 * ：如果仅设置 port_remap ，则指定的映射将同时用于入站和出站通信。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。 使用的格式为： *network type/protocol/default port used by grid node/new port*，其中 `*network type*`是网格、管理员或客户端， `*protocol*`是TCP或UDP。 示例： `PORT_REMAP = client/tcp/18082/443` 您还可以使用逗号分隔列表重新映射多个端口。 示例： `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	可选

port_remap_inbound

价值	名称
将入站通信重新映射到指定端口。如果指定port_remap_inbound、但未指定port_remap值、则端口的出站通信将保持不变。 重要：不要重新映射计划用于配置负载平衡器端点的端口。 使用的格式为： *network type/protocol/remapped port /default port used by grid node*，其中 `*network type*`是网格、管理员或客户端， `*protocol*`是TCP或UDP。 示例： `PORT_REMAP_INBOUND = grid/tcp/3022/22` 您还可以使用逗号分隔列表重新映射多个入站端口。 示例： `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	可选

网格节点如何发现 **StorageGRID** 中的主管理节点

网格节点与主管理节点进行通信以进行配置和管理。每个网格节点都必须知道网格网络上主管理节点的 IP 地址。

为了确保网格节点可以访问主管理节点，您可以在部署此节点时执行以下任一操作：

- 您可以使用 admin_ip 参数手动输入主管理节点的 IP 地址。
- 您可以省略 admin_ip 参数，以使网格节点自动发现该值。当网格网络使用 DHCP 为主管理节点分配 IP 地址时，自动发现尤其有用。

主管理节点的自动发现可通过多播域名系统(mDNS)来实现。主管理节点首次启动时，它会使用 mDNS 发布其 IP 地址。然后，同一子网上的其他节点可以查询 IP 地址并自动获取该地址。但是、由于多播IP流量通常不能在子网上路由、因此其他子网上的节点无法直接获取主管理节点的IP地址。

如果使用自动发现：

- 必须在主管理节点未直接连接到的任何子网上至少包含一个网格节点的 admin_IP 设置。然后，此网格节点将发布子网中其他节点的主管理节点 IP 地址，以便使用 mDNS 进行发现。
- 确保您的网络基础架构支持在子网内传递多播 IP 流量。

使用 **VMware vSphere** 将网格节点部署为 **StorageGRID** 的虚拟机

您可以使用 VMware vSphere Web Client 将每个网格节点部署为虚拟机。在部署期间，系统会创建每个网格节点并将其连接到一个或多个 StorageGRID 网络。

如果需要部署任何StorageGRID设备存储节点，请参见 "部署设备存储节点"。

您也可以在打开节点电源之前重新映射节点端口或增加节点的 CPU 或内存设置。

开始之前

- 您已经"规划并准备安装"了解了如何操作，并了解了软件、CPU和RAM以及存储和性能的要求。
- 您熟悉 VMware vSphere 虚拟机管理程序，并具有在此环境中部署虚拟机的经验。

该 `open-vm-tools`软件包是一种类似于VMware Tools的开源实施、随StorageGRID虚拟机一起提供。您无需手动安装VMware Tools。

- 您已下载并提取适用于 VMware 的正确版本的 StorageGRID 安装归档。

如果要在扩展或恢复操作中部署新节点，则必须使用网格上当前运行的 StorageGRID 版本。

- 您具有StorageGRID虚拟机磁盘(`.vmdk`)文件：

```
NetApp-SG-version-SHA.vmdk
```

- 您拥有 `.ovf`要部署的每种网格节点的和 `.mf`文件：

文件名	说明
vsphere-primary-admin.OVF vsphere-primary-admin.mf	主管理节点的模板文件和清单文件。

文件名	说明
vsphere-non-primary-admin.OVF vsphere-non-primary-admin.mf	非主管理节点的模板文件和清单文件。
vsphere-storage.OVF vsphere-storage.mf	存储节点的模板文件和清单文件。
vsphere-gateway.OVF vsphere-gateway.mf	网关节点的模板文件和清单文件。

- `.vdmk `.ovf`和 `.mf`文件都位于同一目录中。
- 您计划最大限度地减少故障域。例如、不应在一台vSphere ESXi主机上部署所有网关节点。

> 在生产部署中、不要在一个虚拟机上运行多个存储节点。请勿在同一ESXi主机上运行多个虚拟机、否则会导致不可接受的故障域问题。

- 如果要在扩展或恢复操作中部署节点，则可以使用"有关扩展 StorageGRID 系统的说明"或"恢复和维护说明"。
- 如果您要将StorageGRID 节点部署为虚拟机、并从NetApp ONTAP 系统分配存储、则表示您已确认卷未启用FabricPool 分层策略。例如、如果StorageGRID节点作为VMware主机上的虚拟机运行、请确保为该节点的数据存储库提供支持的卷未启用FabricPool分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

关于此任务

按照以下说明开始部署 VMware 节点，在扩展中添加新的 VMware 节点或在恢复操作中更换 VMware 节点。除步骤中所述之外、所有节点类型的节点部署过程都相同、包括管理节点、存储节点和网关节点。

如果要安装新的 StorageGRID 系统：

- 您可以按任意顺序部署节点。
- 您必须确保每个虚拟机均可通过网格网络连接到主管理节点。
- 在配置网格之前，必须部署所有网格节点。

如果要执行扩展或恢复操作：

- 您必须确保新虚拟机可以通过网格网络连接到所有其他节点。

如果需要重新映射节点的任何端口、请在端口重新映射配置完成之前、不要打开新节点的电源。

> 对端口重新映射的支持已弃用，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除裸机主机上的端口重新映射"。

步骤

1. 使用 vCenter 部署 OVF 模板。

如果指定 URL ，请指向包含以下文件的文件夹。否则，请从本地目录中选择其中每个文件。

```
NetApp-SG-version-SHA.vmdk
vsphere-node.ovf
vsphere-node.mf
```

例如，如果这是要部署的第一个节点，请使用以下文件为 StorageGRID 系统部署主管理节点：

```
NetApp-SG-version-SHA.vmdk
vsphere-primary-admin.ovf
vsphere-primary-admin.mf
```

2. 提供虚拟机的名称。

   标准做法是，对虚拟机和网格节点使用相同的名称。

3. 将虚拟机放置在相应的 vApp 或资源池中。
4. 如果要部署主管理节点，请阅读并接受最终用户许可协议。

   根据您的 vCenter 版本，在接受最终用户许可协议，指定虚拟机名称以及选择数据存储库方面，步骤顺序会有所不同。

5. 为虚拟机选择存储。

   如果要在恢复操作期间部署节点、请按照中的说明添加新虚拟磁盘、从故障网格节点重新连接虚拟硬盘或同时执行这两项操作存储恢复步骤。

   部署存储节点时，请使用 3 个或更多存储卷，每个存储卷的容量为 4 TB 或更大。您必须至少为卷 0 分配 4 TB 。

   > 存储节点 .OVF 文件为存储定义了多个 VMDK 。除非这些 VMDK 满足您的存储要求，否则应先将其删除，并为存储分配适当的 VMDK 或 RDM ，然后再启动节点。VMDK 在 VMware 环境中更常用，并且更易于管理，而 RDM 则可以为使用较大对象大小（例如大于 100 MB ）的工作负载提供更好的性能。

   > 某些 StorageGRID 安装可能会使用比典型虚拟化工作负载更大，更活跃的存储卷。您可能需要调整一些虚拟机管理程序参数，例如 `MaxAddressableSpaceTB`，以获得最佳性能。如果遇到性能不佳的问题，请联系虚拟化支持资源，以确定您的环境是否可以从特定于工作负载的配置调整中受益。

6. 选择网络。

   通过为每个源网络选择一个目标网络来确定节点要使用的 StorageGRID 网络。

   - 网格网络为必填项。您必须在 vSphere 环境中选择目标网络。+网格网络用于所有内部StorageGRID流量。它可以在网格中的所有节点之间、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。

- 如果使用管理网络，请在 vSphere 环境中选择其他目标网络。如果不使用管理网络、请选择为网格网络选择的同一目标。
- 如果您使用客户端网络，请在 vSphere 环境中选择其他目标网络。如果不使用客户端网络、请选择为网格网络选择的同一目标。
- 如果您使用的是管理或客户端网络、则节点不必位于同一管理或客户端网络上。

7. 对于*Customize Template (自定义模板)*，配置所需的StorageGRID节点属性。
   a. 输入 * 节点名称 * 。

      如果要恢复网格节点，则必须输入要恢复的节点的名称。

   b. 使用*临时安装密码*下拉列表指定临时安装密码，以便在新节点加入网格之前访问VM控制台或StorageGRID安装API，或者使用SSH。

      临时安装密码仅在节点安装期间使用。将节点添加到网格后，您可以使用("节点控制台密码"在恢复软件包的文件中列出) `Passwords.txt`来访问该节点。

      - 使用节点名称：您为*节点名称*字段提供的值用作临时安装密码。
      - 使用自定义密码：使用自定义密码作为临时安装密码。
      - 禁用密码：不使用临时安装密码。如果您需要访问VM来调试安装问题，请参见"对安装问题进行故障排除"。

   c. 如果选择了*使用自定义密码*，请在*自定义密码*字段中指定要使用的临时安装密码。
   d. 在 * 网格网络（ eth0 ） * 部分中，为 * 网格网络 IP 配置 * 选择静态或 DHCP 。
      - 如果选择静态，请输入 * 网格网络 IP* ， * 网格网络掩码 * ， * 网格网络网关 * 和 * 网格网络 MTU* 。
      - 如果选择 DHCP ，则会自动分配 * 网格网络 IP* ， * 网格网络掩码 * 和 * 网格网络网关 * 。

   e. 在 * 主管理 IP* 字段中，输入网格网络的主管理节点的 IP 地址。

      如果省略主管理节点 IP 地址，则如果主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上，则会自动发现此 IP 地址。但是，建议在此处设置主管理节点 IP 地址。

   f. 在 * 管理网络（ eth1 ） * 部分中，为 * 管理网络 IP 配置 * 选择静态， DHCP 或禁用。
      - 如果不想使用管理网络，请选择已禁用并输入*0.0.0.0*作为管理网络IP。您可以将其他字段留空。
      - 如果选择 static ，请输入 * 管理网络 IP* ， * 管理网络掩码 * ， * 管理网络网关 * 和 * 管理网络 MTU* 。
      - 如果选择 static ，请输入 * 管理网络外部子网列表 * 。您还必须配置网关。
      - 如果选择 DHCP ，则会自动分配 * 管理网络 IP* ， * 管理网络掩码 * 和 * 管理网络网关 * 。

   g. 在 * 客户端网络（ eth2 ） * 部分中，为 * 客户端网络 IP 配置 * 选择静态， DHCP 或禁用。
      - 如果不想使用客户端网络，请选择已禁用并输入*0.0.0.0*作为客户端网络IP。您可以将其他字段留空。
      - 如果选择 static ，请输入 * 客户端网络 IP* ， * 客户端网络掩码 * ， * 客户端网络网关 * 和 * 客户端网络 MTU* 。
      - 如果选择 DHCP ，则会自动分配 * 客户端网络 IP* ， * 客户端网络掩码 * 和 * 客户端网络网关 * 。

8. 查看虚拟机配置并进行必要的更改。
9. 准备好完成后，选择 * 完成 * 以开始上传虚拟机。
10. 如果您在恢复操作中部署了此节点，而此节点不是全节点恢复，请在部署完成后执行以下步骤：
    a. 右键单击虚拟机，然后选择 * 编辑设置 * 。
    b. 选择已指定用于存储的每个默认虚拟硬盘，然后选择 * 删除 * 。
    c. 根据您的数据恢复情况，根据您的存储要求添加新的虚拟磁盘，重新连接从先前删除的故障网格节点中保留的任何虚拟硬盘，或者同时重新连接这两者。

       请注意以下重要准则：

       - 如果要添加新磁盘，则应使用节点恢复之前使用的相同类型的存储设备。
       - 存储节点 .OVF 文件为存储定义了多个 VMDK 。除非这些 VMDK 满足您的存储要求，否则应先将其删除，并为存储分配适当的 VMDK 或 RDM ，然后再启动节点。VMDK 在 VMware 环境中更常用，并且更易于管理，而 RDM 则可以为使用较大对象大小（例如大于 100 MB ）的工作负载提供更好的性能。
11. 如果需要重新映射此节点使用的端口、请执行以下步骤。

    如果您的企业网络策略限制对 StorageGRID 使用的一个或多个端口的访问，您可能需要重新映射端口。有关 StorageGRID 使用的端口，请参阅 "网络连接准则"。

    不要重新映射负载平衡器端点中使用的端口。

    a. 选择新虚拟机。
    b. 从配置选项卡中，选择 * 设置 * > * vApp 选项 * 。* vApp Options* 的位置取决于 vCenter 的版本。
    c. 在 * 属性 * 表中，找到 port_remap_inbound 和 port_remap 。
    d. 要对称映射端口的入站和出站通信，请选择 * 端口重新映射 * 。

       对端口重新映射的支持已弃用，并将在未来的版本中删除。要删除重新映射的端口，请参阅"删除裸机主机上的端口重新映射"。

       如果仅设置 port_remap ，则表示您指定的适用场景 入站和出站通信映射。如果同时指定 port_remap_inbound ， port_remap 将仅应用于出站通信。

       i. 选择 * 设置值 * 。
       ii. 输入端口映射：

       ```
       <network type>/<protocol>/<default port used by grid node>/<new port>
       ```

       `<network type>`是网格、管理员或客户端、 `<protocol>`是TCP或UDP。

       例如，要将 ssh 流量从端口 22 重新映射到端口 3022 ，请输入：

       ```
       client/tcp/22/3022
       ```

       您可以使用逗号分隔列表重新映射多个端口。

例如：

```
client/tcp/18082/443, client/tcp/18083/80
```

i. 选择 * 确定 * 。

e. 要指定用于与节点的入站通信的端口，请选择 * 端口重新映射 _inbound* 。

如果指定port_remap_inbound但未指定port_remap值、则端口的出站通信将保持不变。

i. 选择 * 设置值 * 。

ii. 输入端口映射：

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port
used by grid node>
```

`<network type>`是网格、管理员或客户端、 `<protocol>`是TCP或UDP。

例如，要重新映射发送到端口 3022 的入站 SSH 流量，以便网格节点在端口 22 接收此流量，请输入以下内容：

```
client/tcp/3022/22
```

您可以使用逗号分隔列表重新映射多个入站端口。

例如：

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. 选择 * 确定 *

12. 如果要从默认设置中增加节点的 CPU 或内存：

a. 右键单击虚拟机，然后选择 * 编辑设置 * 。

b. 根据需要更改 CPU 数量或内存量。

将 * 内存预留 * 设置为与分配给虚拟机的 * 内存 * 大小相同的大小。

c. 选择 * 确定 * 。

13. 启动虚拟机。

完成后

如果将此节点部署为扩展或恢复操作步骤 的一部分，请返回到这些说明以完成此操作步骤 。

Linux 上 **StorageGRID** 节点的示例配置文件

您可以使用示例节点配置文件帮助设置 StorageGRID 系统的节点配置文件。这些示例显示了所有类型网格节点的节点配置文件。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

对于大多数节点，在使用网格管理器或安装 API 配置网格时，您可以添加管理员和客户端网络地址信息（ IP ，掩码，网关等）。主管理节点除外。如果要浏览到主管理节点的管理网络 IP 以完成网格配置（例如，由于网格网络未路由），则必须在主管理节点的节点配置文件中配置主管理节点的管理网络连接。示例显示了这一点。

在这些示例中，已将客户端网络目标配置为最佳实践，即使客户端网络默认处于禁用状态也是如此。

主管理节点的示例

示例文件名： `/etc/storagegrid/nodes/dc1-adm1.conf`

- 示例文件内容： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

存储节点示例

示例文件名: `/etc/storagegrid/nodes/dc1-sn1.conf`

- 示例文件内容： *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

网关节点示例

示例文件名: `/etc/storagegrid/nodes/dc1-gw1.conf`

- 示例文件内容： *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

非主管理节点的示例

示例文件名: `/etc/storagegrid/nodes/dc1-adm2.conf`

- 示例文件内容： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

在 **Linux** 上验证 **StorageGRID** 配置

在中为每个StorageGRID节点创建配置文件后 `/etc/storagegrid/nodes`、您必须验证这些文件的内容。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

要验证配置文件的内容，请在每个主机上运行以下命令：

```
sudo storagegrid node validate all
```

如果这些文件正确无误，则输出将为每个配置文件显示 * 已通过 * ，如示例所示。

如果在纯元数据节点上仅使用一个LUN、则可能会收到一条警告消息、您可以忽略此消息。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

对于自动安装，可以使用命令中的或 `--quiet`选项 `storagegrid`(例如 `storagegrid --quiet…`)禁止此输出 `-q`。如果禁止输出，则在检测到任何配置警告或错误时，命令的退出值将为非零。

如果配置文件不正确，则这些问题将显示为 * 警告 * 和 * 错误 * ，如示例所示。如果发现任何配置错误，则必须

先更正这些错误，然后再继续安装。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

在 **Linux** 上启动 **StorageGRID** 主机服务

要启动 StorageGRID 节点并确保它们在主机重新启动后重新启动，您必须启用并启动 StorageGRID 主机服务。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

步骤

1. 在每个主机上运行以下命令：

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 运行以下命令以确保部署正在进行：

```
sudo storagegrid node status node-name
```

3. 如果任何节点返回状态"Nnot running"(未运行)或"STOPPEed"(已停止)、请运行以下命令：

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

4. 如果您先前已启用并启动 StorageGRID 主机服务（或者不确定此服务是否已启用和启动），请同时运行以下命令：

```
sudo systemctl reload-or-restart storagegrid
```

了解 **StorageGRID** 安装 **REST API**

StorageGRID 提供了用于执行安装任务的 StorageGRID 安装 API 。

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

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

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

StorageGRID 安装 API

StorageGRID 安装API仅在最初配置StorageGRID 系统时以及需要执行主管理节点恢复时可用。可以从网格管理器通过 HTTPS 访问安装 API 。

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

StorageGRID 安装 API 包括以下部分：

- **config**：与产品发布和 API 版本相关的操作。您可以列出该版本支持的产品发布版本和 API 的主要版本。
- **grid**：网格级配置操作。您可以获取和更新网格设置，包括网格详细信息、Grid Network 子网、网格密码以及 NTP 和 DNS 服务器 IP 地址。
- **nodes**：节点级配置操作。您可以检索网格节点列表、删除网格节点、配置网格节点、查看网格节点以及重置网格节点的配置。
- **provision**：供应操作。您可以启动供应操作并查看供应操作的状态。

- **recovery**：主管理节点恢复操作。您可以重置信息、上传恢复包、启动恢复以及查看恢复操作的状态。
- **recovery-package**：下载 Recovery Package 的操作。
- **sites**：站点级配置操作。您可以创建、查看、删除和修改站点。
- **temporary-password**：在安装过程中对临时密码执行操作，以保护 mgmt-api。

对 **StorageGRID** 安装问题进行故障排除

如果在安装 StorageGRID 系统时出现任何问题，您可以访问安装日志文件。技术支持可能还需要使用安装日志文件来解决问题。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

Linux

运行每个节点的容器提供了以下安装日志文件：

- `/var/local/log/install.log`(在所有网格节点上均可找到)
- `/var/local/log/gdu-server.log`(位于主管理节点上)

主机上提供了以下安装日志文件：

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

要了解如何访问日志文件，请参见"收集日志文件和系统数据"。

VMware

以下是主要安装日志文件，技术支持可能需要这些文件来解决问题。

- `/var/local/log/install.log`(在所有网格节点上均可找到)
- `/var/local/log/gdu-server.log`(位于主管理节点上)

虚拟机资源预留需要调整

OVF 文件包含一个资源预留，用于确保每个网格节点都有足够的 RAM 和 CPU 来高效运行。如果通过在VMware上部署这些OVF文件来创建虚拟机、但预定义数量的资源不可用、则虚拟机将无法启动。

关于此任务

如果您确定 VM 主机具有足够的资源来支持每个网格节点，请手动调整为每个虚拟机分配的资源，然后尝试启动虚拟机。

步骤

1. 在 VMware vSphere 虚拟机管理程序客户端树中，选择未启动的虚拟机。
2. 右键 - 单击虚拟机，然后选择 * 编辑设置 * 。
3. 从虚拟机属性窗口中，选择 * 资源 * 选项卡。
4. 调整分配给虚拟机的资源：
   a. 选择 * CPU * ，然后使用预留滑块调整为此虚拟机预留的 MHz 。
   b. 选择 * 内存 * ，然后使用预留滑块调整为此虚拟机预留的 MB 。
5. 选择 * 确定 * 。
6. 根据需要对同一 VM 主机上托管的其他虚拟机重复上述步骤。

临时安装密码已禁用

在部署VMware节点时、您可以选择指定临时安装密码。要访问VM控制台或使用SSH、新节点必须具有此密码才能加入网格。

如果选择禁用临时安装密码、则必须执行其他步骤来调试安装问题。

您可以执行以下任一操作：

- 重新部署虚拟机、但指定一个临时安装密码、以便您可以访问控制台或使用SSH调试安装问题。
- 使用vCenter设置密码：
  a. 关闭虚拟机。
  b. 转到*VM*，选择*Config*选项卡，然后选择*vapp选项*。
  c. 指定要设置的临时安装密码类型：
     - 选择*custom_temporal_password*以设置自定义临时密码。
     - 选择*temporal_password_type*以使用节点名称作为临时密码。
  d. 选择 * 设置值 * 。
  e. 设置临时密码：
     - 将*custom_temporal_password*更改为自定义密码值。
     - 将*temporal_password_type*更新为*use node name*值。
  f. 重新启动虚拟机以应用新密码。

相关信息

- 要了解如何访问日志文件，请参见"日志文件参考"。
- "对 StorageGRID 系统进行故障排除"
- 如果您需要其他帮助，请联系 "NetApp 支持"。

脚本示例

在 **RHEL** 上将四个物理接口整合为一个绑定的 **StorageGRID** 示例

您可以使用示例文件将四个 Linux 物理接口聚合到一个 LACP 绑定中，然后建立三个 VLAN 接口，将此绑定分包为 StorageGRID 网格，管理和客户端网络接口。

物理接口

请注意，链路另一端的交换机还必须将这四个端口视为一个 LACP 中继或端口通道，并且必须至少通过三个带标记的参考 VLAN 。

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

绑定接口

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLAN 接口

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

在 **Ubuntu** 和 **Debian** 上聚合 **StorageGRID** 物理接口的示例

该 `/etc/network/interfaces`文件包括三个部分、分别定义了物理接口、绑定接口和VLAN接口。您可以将这三个示例部分合并为一个文件，该文件将四个 Linux 物理接口聚合为一个 LACP 绑定，然后建立三个 VLAN 接口，将此绑定分包为 StorageGRID 网格，管理和客户

端网络接口。

物理接口

请注意，链路另一端的交换机还必须将这四个端口视为一个 LACP 中继或端口通道，并且必须至少通过三个带标记的参考 VLAN 。

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

绑定接口

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLAN 接口

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

配置网格并完成安装

导航到 **StorageGRID** 网格管理器

您可以使用网格管理器定义配置 StorageGRID 系统所需的所有信息。

开始之前

必须部署主管理节点，并且已完成初始启动序列。

步骤

1. 打开Web浏览器并导航到：

   `https://primary_admin_node_ip`

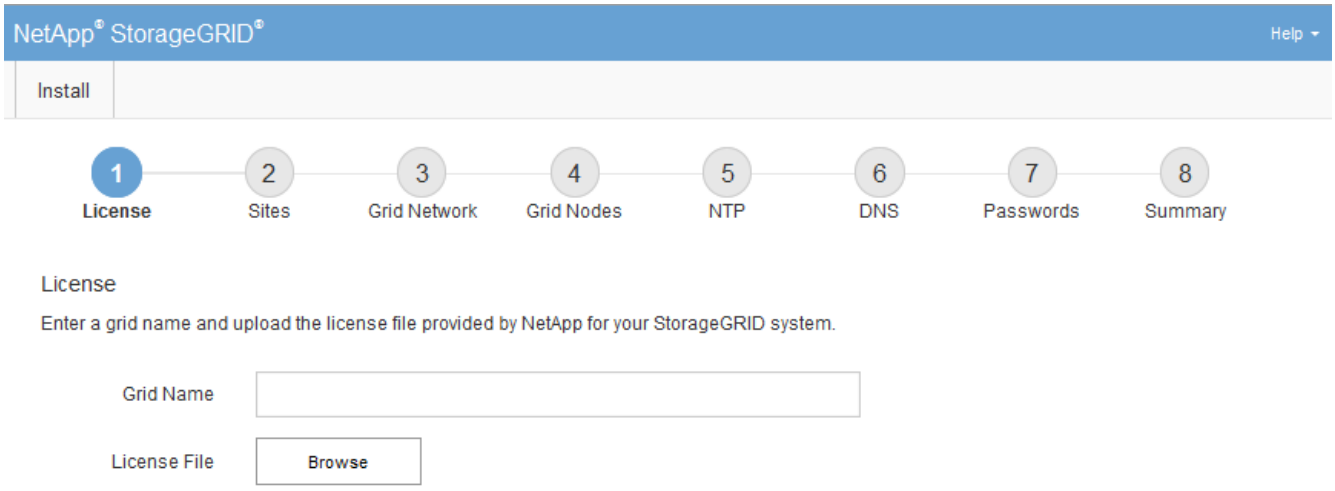
   或者，您也可以通过端口 8443 访问网格管理器：

   `https://primary_admin_node_ip:8443`

   根据您的网络配置，您可以使用网格网络或管理网络上的主管理节点 IP 的 IP 地址。您可能需要使用浏览器中的安全性/高级选项导航到不可信的证书。

2. 根据需要管理临时安装程序密码：
   - 如果已使用以下方法之一设置密码、请输入密码以继续。
     - 用户在先前访问安装程序时设置了密码
     - 对于 Linux，密码会自动从节点配置文件导入 `/etc/storagegrid/nodes/<node_name>.conf`
     - 对于 VMware，SSH/控制台密码已从 OVF 属性自动导入
   - 如果尚未设置密码、则可以选择设置密码以保护StorageGRID安装程序。
3. 选择*安装StorageGRID 系统*。

此时将显示用于配置 StorageGRID 网格的页面。



指定 **StorageGRID** 许可证信息

您必须指定 StorageGRID 系统的名称并上传 NetApp 提供的许可证文件。

步骤

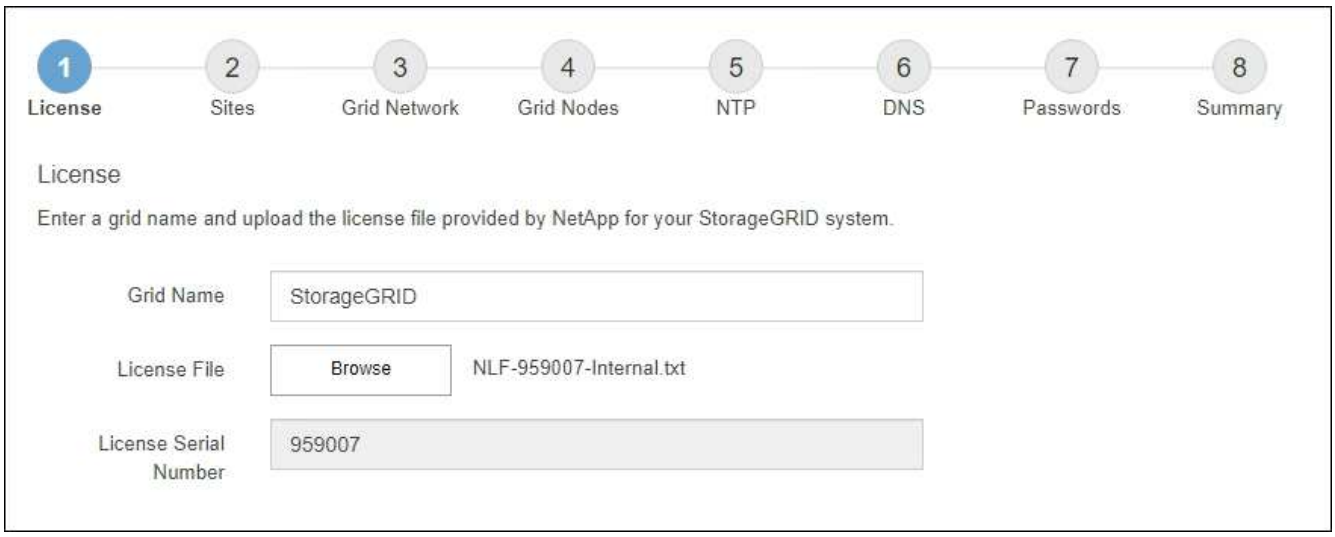
1. 在“许可证”页面的*网格名称*字段中，为StorageGRID 系统输入有意义的名称。

   安装后，此名称将显示在节点菜单的顶部。

2. 选择*浏览*，找到NetApp许可证文件(`NLF-unique-id.txt`)，然后选择*打开*。

   此时将验证许可证文件、并显示序列号。

   > StorageGRID 安装归档包含一个免费许可证，不提供产品的任何支持授权。您可以在安装后更新为提供支持的许可证。



3. 选择 * 下一步 * 。

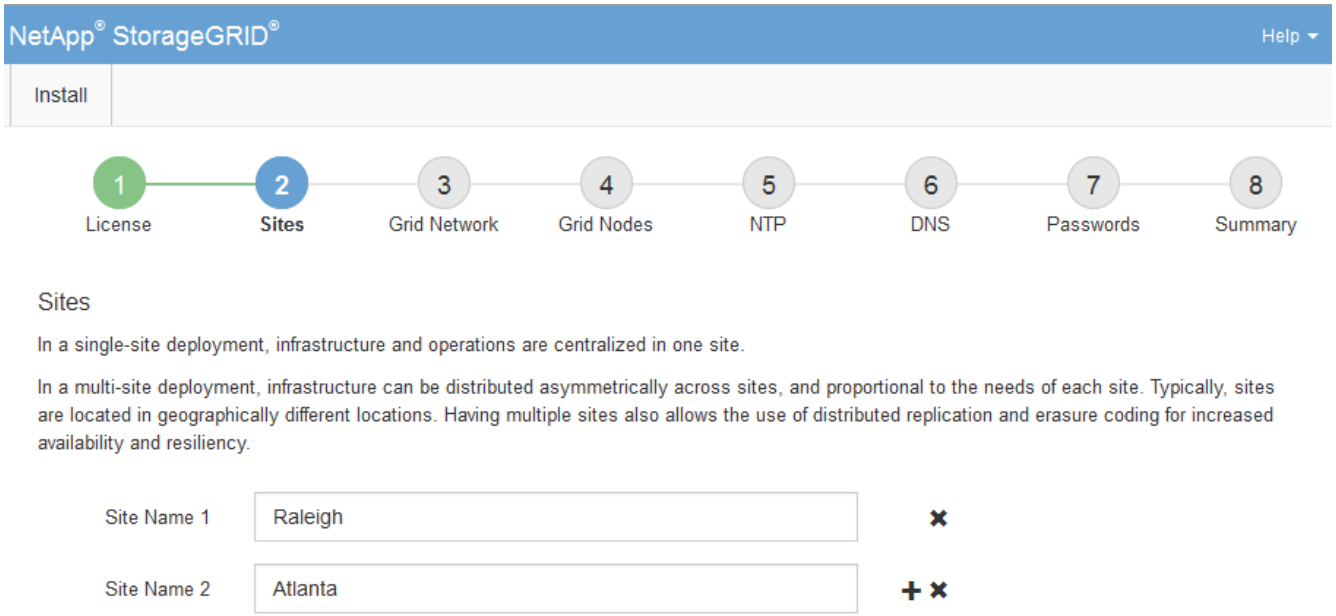
在 **StorageGRID** 中添加站点

安装 StorageGRID 时，必须至少创建一个站点。您可以创建其他站点来提高 StorageGRID 系统的可靠性和存储容量。

步骤

1. 在"站点"页面上，输入*站点名称*。
2. 要添加其他站点，请选择最后一个站点条目旁边的加号，然后在新的 **Site name** 文本框中输入名称。

   根据需要为网格拓扑添加尽可能多的其他站点。您最多可以添加 16 个站点。



3. 选择 * 下一步 * 。

为 **StorageGRID** 指定网格网络子网

您必须指定网格网络上使用的子网。

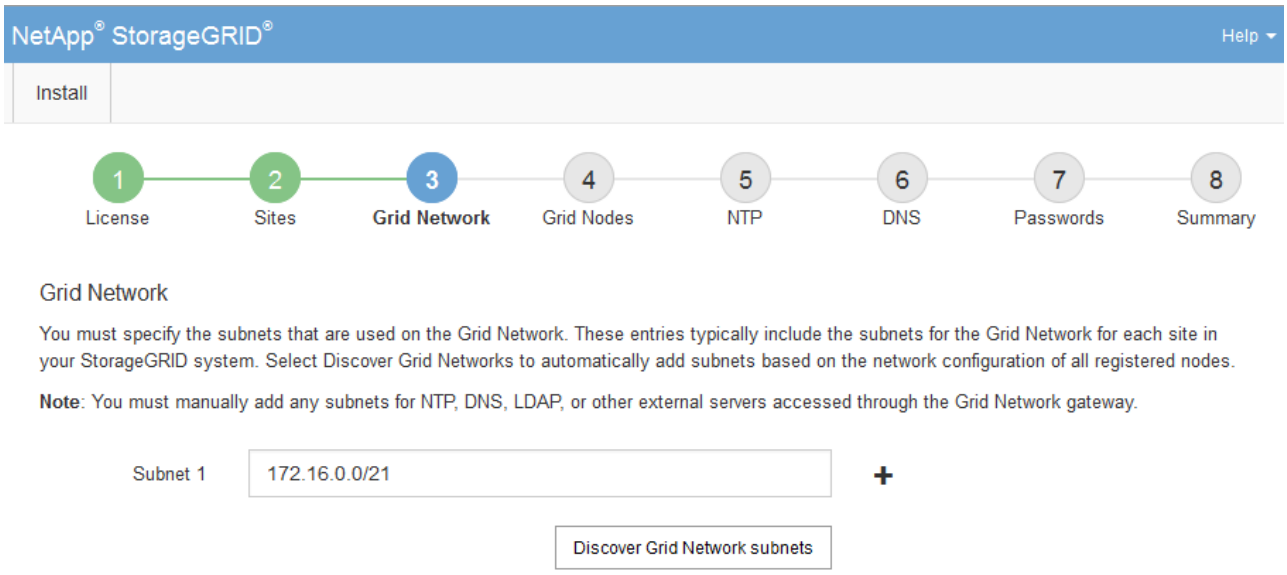
关于此任务

子网条目包括StorageGRID 系统中每个站点的网格网络子网以及需要通过网格网络访问的任何子网。

如果您有多个网格子网，则需要使用网格网络网关。指定的所有网格子网都必须可通过此网关访问。

步骤

1. 在 * 子网 1* 文本框中至少为一个网格网络指定 CIDR 网络地址。
2. 选择最后一个条目旁边的加号以添加其他网络条目。您必须为网格网络中的所有站点指定所有子网。
   - 如果您已经部署了至少一个节点，请选择 **Discover Grid Networks subnets** 以自动使用已向 Grid Manager 注册的网格节点报告的子网填充网格网络子网列表。
   - 您必须为NTP、DNS、LDAP或通过网格网络网关访问的其他外部服务器手动添加任何子网。



3. 选择 * 下一步 * 。

批准 **StorageGRID** 的待处理网格节点

您必须先批准每个网格节点，然后才能将其加入 StorageGRID 系统。

开始之前

您已部署所有虚拟设备和 StorageGRID 设备网格节点。

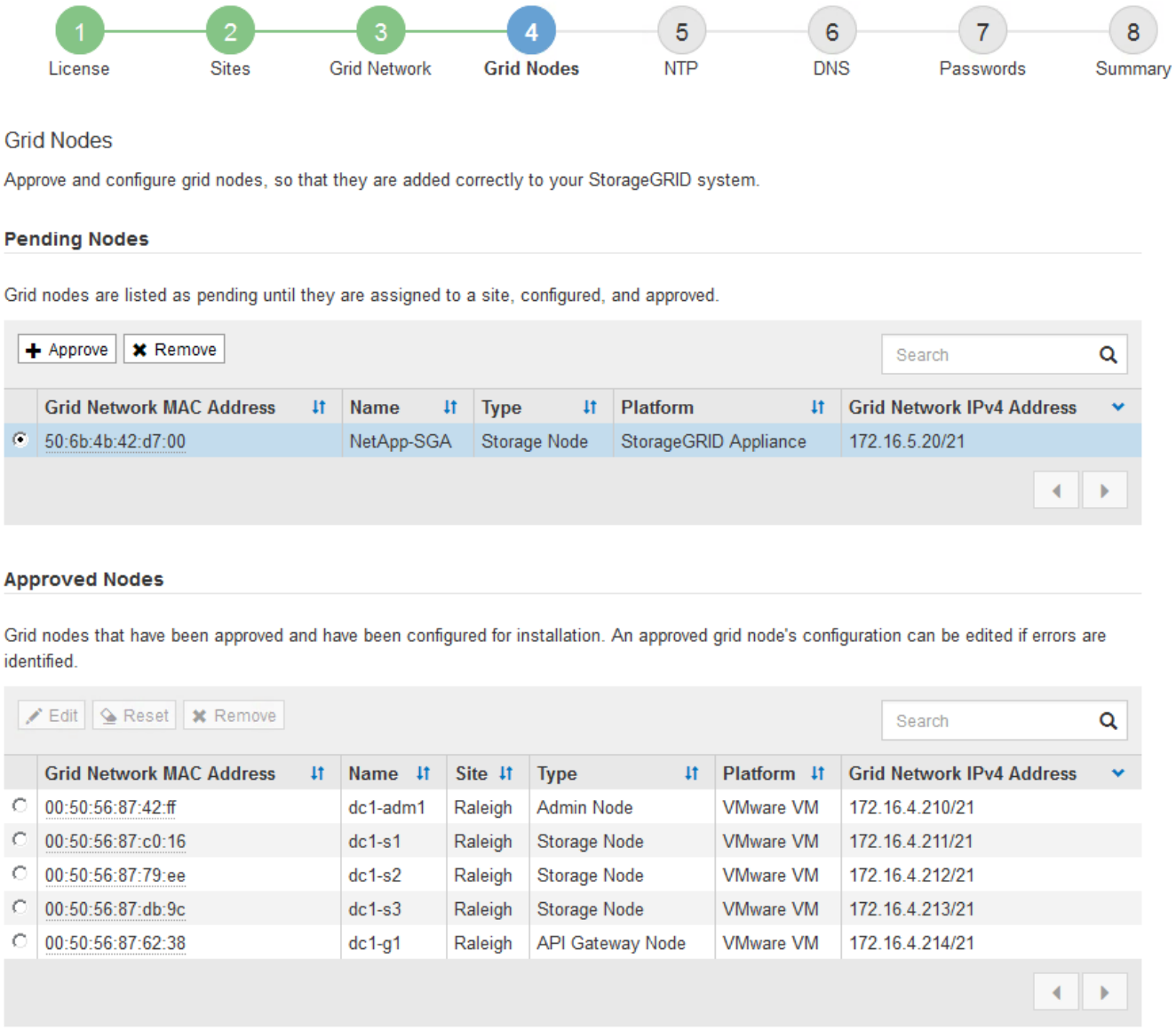
> 对所有节点执行一次安装比现在安装某些节点以及稍后安装某些节点更高效。

步骤

1. 查看 Pending Nodes 列表，并确认它显示了您部署的所有网格节点。

> 如果缺少网格节点、请确认已成功部署该节点、并且已为admin_IP设置主管理节点的正确网格网络IP。

2. 选择要批准的待定节点旁边的单选按钮。



3. 选择 * 批准 * 。
4. 在常规设置中，根据需要修改以下属性的设置：
   - **Site**：此网格节点的站点的系统名称。
   - **Name**：节点的系统名称。此名称默认为您在配置节点时指定的名称。

     内部StorageGRID 操作需要系统名称、完成安装后无法更改。但是、在安装过程的这一步中、您可以根据需要更改系统名称。

     对于 VMware 节点，您可以在此处更改名称，但此操作不会更改 vSphere 中虚拟机的名称。

   - * NTP 角色 * ：网格节点的网络时间协议（ NTP ）角色。选项包括 * 自动 * ， * 主 * 和 * 客户端 * 。选择 * 自动 * 会将主角色分配给管理节点，具有模板转换服务的存储节点，网关节点以及具有非静态 IP 地址的任何网格节点。所有其他网格节点都分配有客户端角色。

确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

- 存储类型(仅限存储节点)：指定新存储节点专用于数据、仅用于元数据或同时用于这两者。选项包括*数据和元数据*("组合")、仅数据*和*仅元数据。

  有关这些节点类型的要求的信息、请参见"存储节点的类型"。

- * ADC* 服务 * （仅限存储节点）：选择 * 自动 * ，让系统确定节点是否需要管理域控制器（ ADC* ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。每个站点至少有三个存储节点必须包含此 ADC-Service 。在部署后、您无法将ADC服务添加到节点。

5. 在网格网络中，根据需要修改以下属性的设置：

   - * IPv4 地址（ CIDR ） *：网格网络接口（容器中的 eth0 ）的 CIDR 网络地址。例如： 192.168.1.234/21
   - * 网关 *： 网格网络网关。例如： 192.168.0.1

     如果存在多个网格子网，则需要使用网关。

   如果您为网格网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保配置的IP地址不在DHCP地址池中。

6. 如果要为网格节点配置管理网络，请根据需要在管理网络部分中添加或更新设置。

   在 * 子网（ CIDR ） * 文本框中输入从此接口路由的目标子网。如果存在多个管理子网，则需要使用管理网关。

   如果您为管理网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保配置的IP地址不在DHCP地址池中。

   *Appliance：*对于StorageGRID 设备，如果在初始安装期间未使用StorageGRID 设备安装程序配置管理网络，则无法在此网格管理器对话框中配置管理网络。而是必须执行以下步骤：

   a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

      重新启动可能需要几分钟时间。

   b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。
   c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。
   d. 返回主页并选择*Start installation*。
   e. 在网格管理器中：如果已批准节点表中列出了该节点、请删除该节点。
   f. 从 Pending Nodes 表中删除此节点。
   g. 等待节点重新出现在 "Pending Nodes" 列表中。
   h. 确认您可以配置适当的网络。它们应已填充您在设备安装程序的IP配置页面上提供的信息。

有关详细信息、请参见 "硬件安装快速入门"以查找设备的说明。

7. 如果要为网格节点配置客户端网络，请根据需要在客户端网络部分中添加或更新设置。如果配置了客户端网络，则需要使用网关，安装后，它将成为节点的默认网关。

> 如果您为客户端网络配置选择了 DHCP 并在此更改了值，则新值将配置为节点上的静态地址。您必须确保配置的IP地址不在DHCP地址池中。

*设备:*对于StorageGRID 设备,如果在初始安装期间未使用StorageGRID 设备安装程序配置客户端网络,则无法在此网格管理器对话框中配置该网络。而是必须执行以下步骤：

a. 重新启动设备：在设备安装程序中，选择 * 高级 * > * 重新启动 * 。

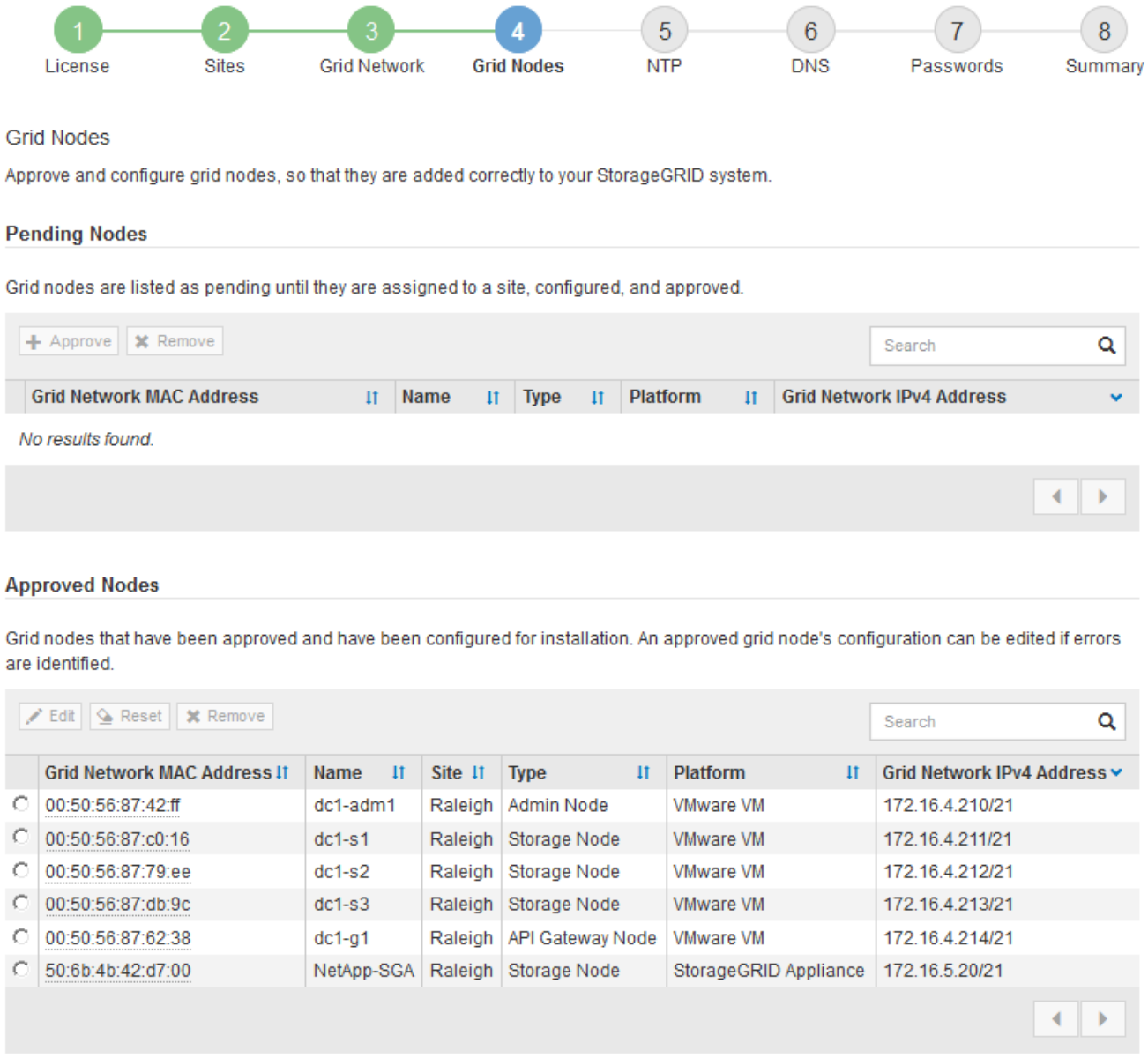
   重新启动可能需要几分钟时间。

b. 选择 * 配置网络 * > * 链路配置 * 并启用相应的网络。
c. 选择 * 配置网络 * > * IP 配置 * 并配置已启用的网络。
d. 返回主页并选择*Start installation*。
e. 在网格管理器中：如果已批准节点表中列出了该节点、请删除该节点。
f. 从 Pending Nodes 表中删除此节点。
g. 等待节点重新出现在 "Pending Nodes" 列表中。
h. 确认您可以配置适当的网络。它们应已填充您在设备安装程序的IP配置页面上提供的信息。

   有关详细信息、请参见 "硬件安装快速入门"以查找设备的说明。

8. 选择 * 保存 * 。

网格节点条目将移至 "Approved Nodes" 列表。



9. 对要批准的每个待定网格节点重复上述步骤。

   您必须批准您想要在网格中的所有节点。但是，在摘要页面上选择 **Install** 之前，您可以随时返回此页面。您可以通过选择其单选按钮并选择 **Edit** 来修改已批准网格节点的属性。

10. 审批完网格节点后，选择*下一步*。

为 **StorageGRID** 指定网络时间协议服务器信息

您必须为 StorageGRID 系统指定网络时间协议（ NTP ）配置信息，以便在不同服务器上执行的操作保持同步。

关于此任务

您必须为 NTP 服务器指定 IPv4 地址。

您必须指定外部 NTP 服务器。指定的 NTP 服务器必须使用 NTP 协议。

您必须指定四个引用 Stratum 3 或更高配置的 NTP 服务器，以防止出现时间偏差问题。

> 为生产级StorageGRID 安装指定外部NTP源时、请勿在早于Windows Server 2016的Windows版本上使用Windows时间(W32Time)服务。早期版本的 Windows 上的时间服务不够准确，Microsoft 不支持在 StorageGRID 等高精度环境中使用。
>
> "高精度时间的支持边界"

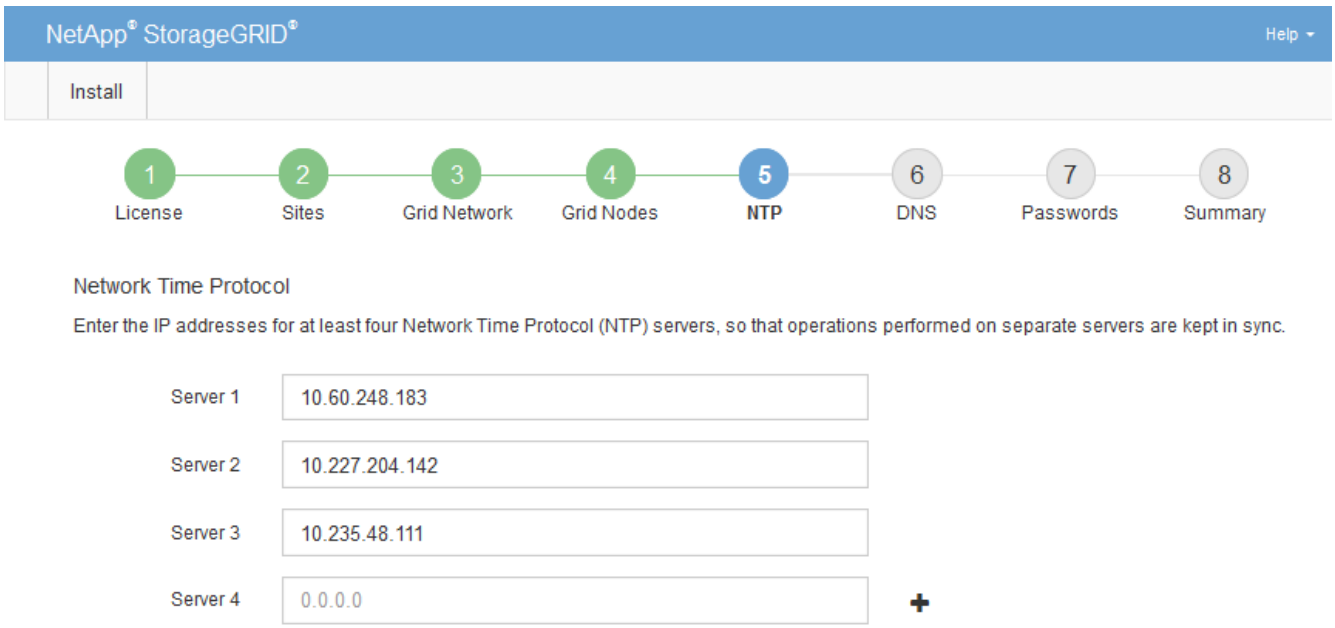
外部 NTP 服务器由先前分配了主 NTP 角色的节点使用。

> 确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

（仅限 VMware）对 VMware 执行额外检查，例如确保虚拟机管理程序使用与虚拟机相同的 NTP 源，并使用 VMTools 禁用虚拟机管理程序和StorageGRID虚拟机之间的时间同步。

步骤

1. 在 * 服务器 1* 到 * 服务器 4* 文本框中指定至少四个 NTP 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



3. 选择 * 下一步 * 。

相关信息

"网络连接准则"

为 **StorageGRID** 指定 **DNS** 服务器信息

您必须为StorageGRID 系统指定DNS信息、以便可以使用主机名而不是IP地址访问外部服务器。

关于此任务

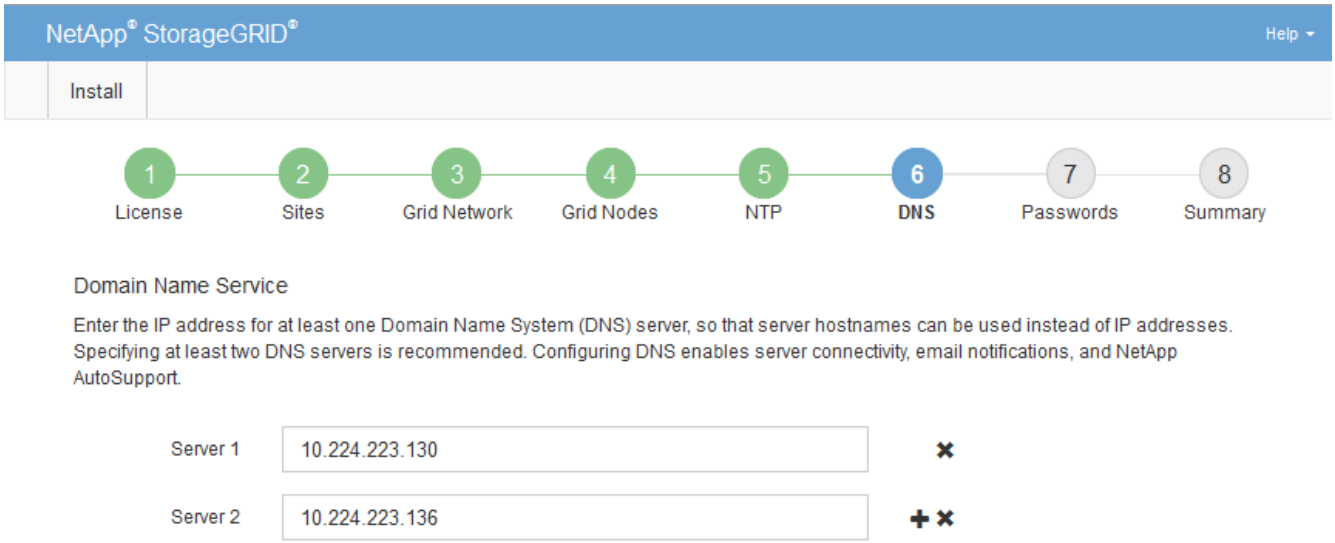
通过指定 "DNS服务器信息"、您可以在电子邮件通知和AutoSupport中使用完全限定域名(FQDN)主机名、而不是IP地址。

要确保正常运行、请指定两个或三个DNS服务器。如果指定的值超过三个、则可能仅使用三个、因为某些平台上存在已知的操作系统限制。如果您的环境存在路由限制、则各个节点(通常是站点上的所有节点)可以"自定义DNS服务器列表"使用一组不同的DNS服务器、最多可使用三个。

如果可能、请使用每个站点可以在本地访问的DNS服务器、以确保受支持的站点可以解析外部目标的FQDN。

步骤

1. 在 * 服务器 1* 文本框中至少指定一个 DNS 服务器的 IPv4 地址。
2. 如有必要，请选择最后一个条目旁边的加号以添加其他服务器条目。



最佳实践是至少指定两个 DNS 服务器。最多可以指定六个 DNS 服务器。

3. 选择 * 下一步 * 。

指定 **StorageGRID** 系统密码

在安装 StorageGRID 系统时，您需要输入密码以保护系统安全并执行维护任务。

关于此任务

使用安装密码页面指定配置密码短语和网格管理 root 用户密码。

- 配置密码短语用作加密密钥，不会由 StorageGRID 系统存储。
- 您必须具有用于安装，扩展和维护过程的配置密码短语，包括下载恢复软件包。因此，请务必将配置密码短语存储在安全位置。
- 如果您使用的是最新的网格管理器，则可以从网格管理器更改配置密码短语。
- 网格管理root用户密码可以使用网格管理器进行更改。
- 随机生成的命令行控制台和SSH密码存储在恢复软件包的文件中 `Passwords.txt`。

步骤

1. 在 **Provisioning passphrase** 中，输入更改 StorageGRID 系统的网格拓扑所需的配置密码短语。

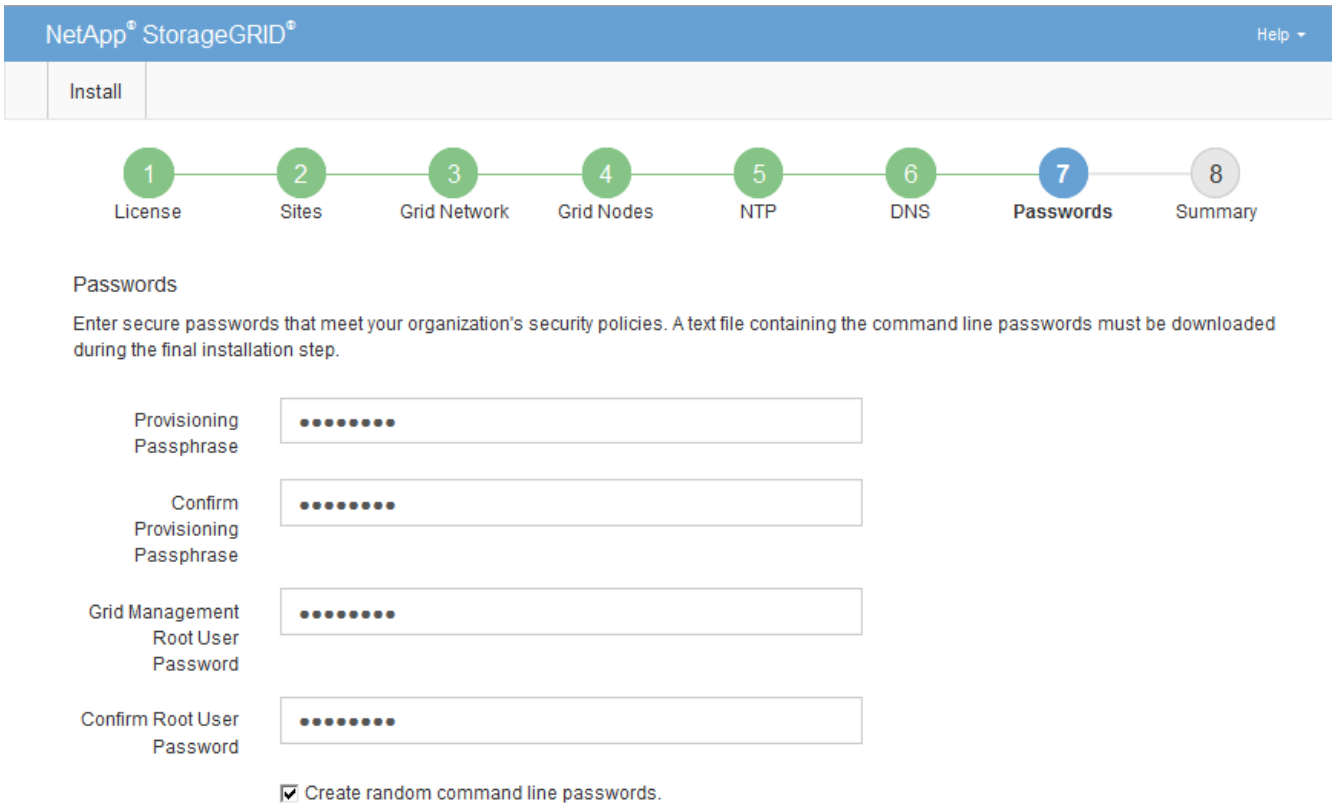
   将配置密码短语存储在安全位置。

   > 如果安装完成后您想稍后更改配置密码，则可以使用网格管理器。选择*配置* > 访问控制 > 电网密码。

2. 在 **Confirm provisioning passphrase** 中，重新输入配置密码进行确认。
3. 在*网格管理root用户密码*中，输入以"root"用户身份访问网格管理器所使用的密码。

   > 将配置密码存储在安全的位置。它是安装、扩展和维护过程所必需的。

4. 在 * 确认 root 用户密码 * 中，重新输入网格管理器密码进行确认。



5. 如果要安装网格以进行概念验证或演示，则可以选择清除*创建随机命令行密码*复选框。

   对于生产部署，出于安全原因，应始终使用随机密码。如果要使用默认密码通过命令行使用"root"或"admin"帐户访问网格节点，请清除*仅为演示网格创建随机命令行密码*。

   > 在"摘要"页面上选择 **Install** 后，系统会提示您下载"恢复包"文件 (`sgws-recovery-package-id-revision.zip`) 。您必须 "下载此文件" 才能完成安装。访问系统所需的密码存储在 `Passwords.txt` 文件中，该文件包含在恢复包文件中。

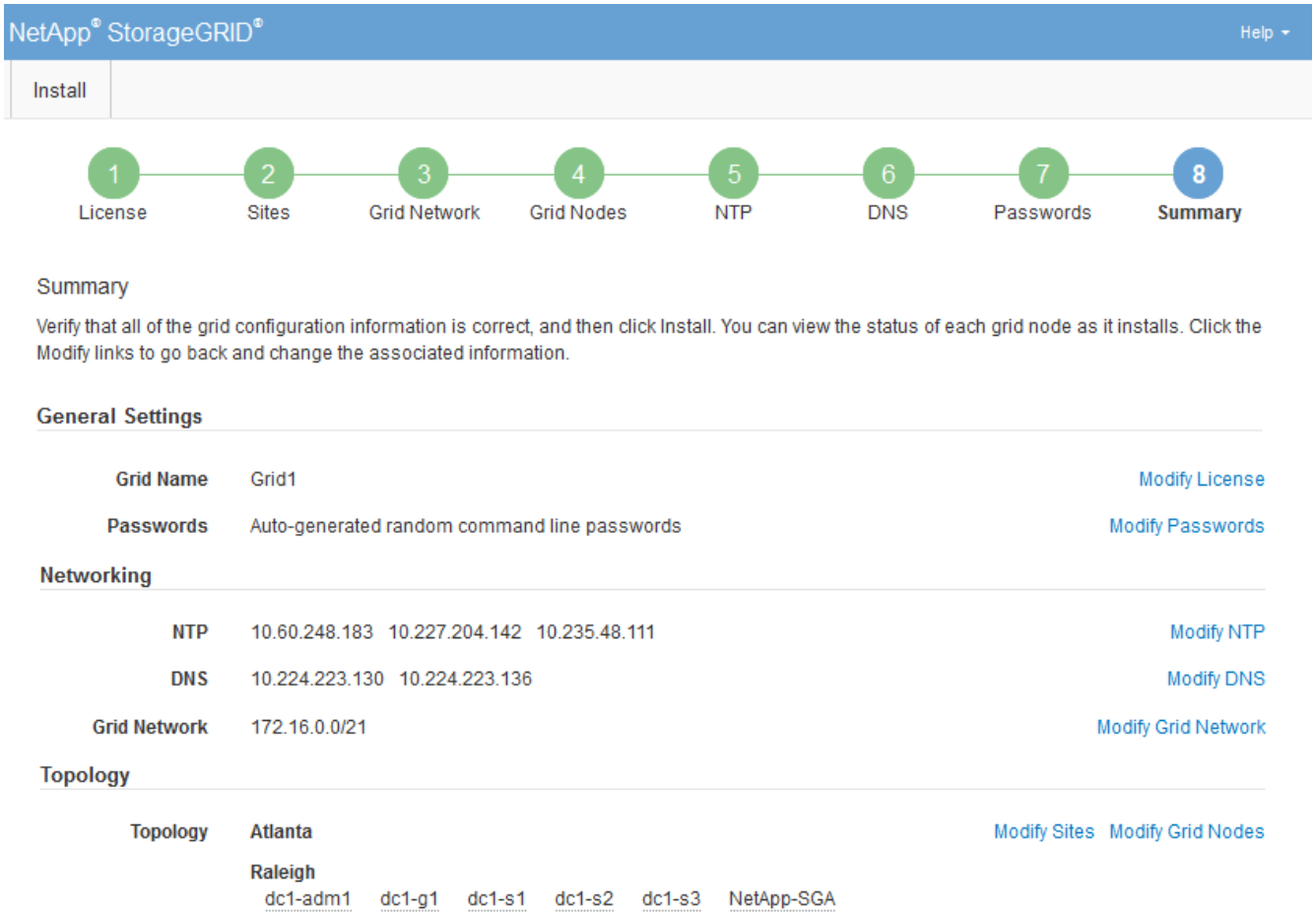
6. 选择 * 下一步 * 。

查看 StorageGRID 配置

您必须仔细查看输入的配置信息，以确保安装成功完成。

步骤

1. 查看 * 摘要 * 页面。



2. 验证所有网格配置信息是否正确。使用摘要页面上的修改链接返回并更正任何错误。
3. 选择*安装*。

> 如果节点配置为使用客户端网络，则当您选择*安装*时，该节点的默认网关将从网格网络切换到客户端网络。如果您失去连接，则必须确保您通过可访问的子网访问主管理节点。有关详细信息，请参阅"网络连接准则"。

4. 选择 * 下载恢复包 * 。

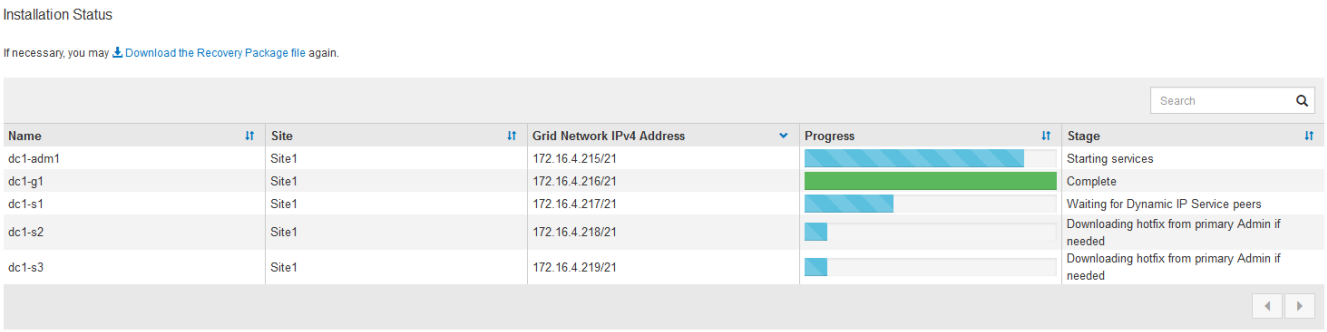
   安装过程中，如果网格拓扑已定义，系统将提示您下载恢复软件包文件(`.zip`，并确认您可以成功访问此文件的内容。您必须下载恢复软件包文件，以便在一个或多个网格节点出现故障时恢复 StorageGRID 系统。安装将在后台继续、但在下载并验证此文件之前、您无法完成安装并访问StorageGRID 系统。

5. 确认您可以提取文件的内容 `.zip`、然后将其保存在两个安全、独立的位置。

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

6. 选择*我已成功下载并验证恢复包文件*复选框，然后选择*下一步*。

   如果安装仍在进行中，则会显示状态页面。此页面指示每个网格节点的安装进度。



   当所有网格节点达到完成阶段后，将显示网格管理器的登录页面。

7. 使用 "root" 用户和您在安装期间指定的密码登录到网格管理器。

安装 **StorageGRID** 后的网络和 **DHCP** 要求

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 。配置期间无法设置DHCP。

  通过DHCP更改网格网络配置后、节点会重新启动、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，必须使用更改 IP 过程。请参阅。 "配置 IP 地址"
- 如果更改网络配置，包括更改路由和网关，则客户端与主管理节点和其他网格节点的连接可能会断开。根据应用的网络更改、您可能需要重新建立这些连接。

了解安装 **StorageGRID** 后所需的和可选的步骤

完成安装后、执行所需的集成和配置任务。您可以根据需要执行可选任务。

所需任务

- （仅限 VMware）配置 VMware vSphere Hypervisor 以实现自动重启。

  您必须将虚拟机管理程序配置为在服务器重新启动时重新启动虚拟机。如果不自动重新启动，虚拟机和网格节点将在服务器重新启动后保持关闭状态。有关详细信息，请参见 VMware vSphere 虚拟机管理程序文档。

- "创建租户帐户"用于在StorageGRID系统上存储对象的S3客户端协议。
- "控制系统访问"配置组和用户帐户。(可选)您可以"配置联合身份源"(例如Active Directory或OpenLDAP)导入

管理组和用户。或者，您可以"创建本地组和用户"。

- 集成并测试"S3 API"用于将对象上传到StorageGRID系统的客户端应用程序。
- "配置信息生命周期管理(ILM)规则和ILM策略"您希望使用来保护对象数据。
- 如果您的安装包含设备存储节点、请使用SANtricity OS完成以下任务：
  - 连接到每个 StorageGRID 设备。
  - 验证是否收到 AutoSupport 数据。

    请参阅。 "设置硬件"
- 查看并遵循"StorageGRID 系统强化准则"以消除安全风险。
- "为系统警报配置电子邮件通知"(英文)

可选任务

- "更新网格节点IP地址"如果自您计划部署并生成恢复包以来它们已经发生了变化。
- "配置存储加密"，如果需要。
- "配置存储压缩"根据需要减小已存储对象的大小。
- "配置 VLAN 接口"隔离网络流量并对其进行分区(如果需要)。
- "配置高可用性组"提高Grid Manager、租户管理器和S3客户端的连接可用性(如果需要)。
- "配置负载平衡器端点"用于S3客户端连接(如果需要)。

升级 StorageGRID 软件

升级 StorageGRID 软件

按照以下说明将 StorageGRID 系统升级到新版本。

执行升级时、StorageGRID系统中的所有节点都会升级。

> 如果您急需扩展存储以增加容量（如果您的存储几乎已满），请不要开始升级。及时完成升级程序。如果需要恢复，请联系技术支持。

升级之前

查看这些主题以了解 StorageGRID 12.1 中的新功能和增强功能，确定是否已弃用或删除任何功能，并了解 StorageGRID API 的更改。

- "升级期间对系统的影响"
- "StorageGRID 12.1 中的新增功能"
- "已删除或已弃用的功能"
- "对网格管理 API 进行的更改"
- "对租户管理 API 进行的更改"

规划和准备升级

估计完成 **StorageGRID** 升级的时间

根据升级可能需要的时间、考虑何时升级。了解在升级的每个阶段可以执行和不能执行的操作。

关于此任务

完成 StorageGRID 升级所需的时间取决于多种因素，例如客户端负载和硬件性能。

下表汇总了主要升级任务，并列出了每个任务所需的大致时间。下表后面的步骤提供了一些说明，您可以使用这些说明来估计系统的升级时间。

升级任务	说明	所需大致时间	执行此任务期间
运行预检并升级主管理节点	此时将运行升级预检、并停止、升级和重新启动主管理节点。	30分钟到1小时、服务设备节点所需时间最多。 未解决的预检错误将增加此时间。	您无法访问主管理节点。可能会报告连接错误、您可以忽略这些错误。 通过在开始升级之前运行升级预检、您可以在计划的升级维护窗口之前解决任何错误。
启动升级服务	此时将分发软件文件、并启动升级服务。	每个网格节点3分钟	
升级其他网格节点	所有其他网格节点上的软件均按照您批准节点的顺序进行升级。一个管理节点或网关节点与一个存储节点同时升级。	每个节点 15 分钟到 1 小时，设备节点所需时间最多 注意：对于设备节点，StorageGRID 设备安装程序会自动更新到最新版本。	• 请勿更改网格配置。 • 请勿更改审核级别配置。 • 请勿更新ILM配置。 • 系统会阻止您执行其他维护过程，例如修补程序，停用或扩展。 注：如果需要执行恢复，请与技术支持联系。
启用功能	新版本的新功能已启用。	最多 1 小时	• 请勿更改网格配置。 • 请勿更改审核级别配置。 • 请勿更新ILM配置。 • 您无法执行另一个维护操作步骤。
最终升级步骤	此时将删除临时文件，并完成到新版本的升级。	5 分钟	完成*最终升级步骤*任务后，您可以执行所有维护过程。

估计升级时间

步骤

1. 估计升级所有网格节点所需的时间。

a. 将 StorageGRID 系统中的节点数乘以每个节点 1 小时。

   一般来说，设备节点的升级时间比基于软件的节点要长。

b. 在此时间之外增加1小时、以说明下载文件、运行预检验证以及完成最终升级步骤所需的时间 `.upgrade`。

2. 如果您使用的是 Linux 节点，请为每个节点添加 15 分钟的时间，以考虑下载和安装 RPM 或 Deb 软件包所需的时间。
3. 通过添加步骤 1 和步骤 2 的结果来计算升级的总估计时间。

示例：升级到 **StorageGRID 12.1** 的估计时间

假设您的系统有 14 个网格节点，其中 8 个是 Linux 节点。

1. 将 14 乘以每个节点 1 小时。
2. 另外，还需要 1 小时的时间来说明下载，预检和最终步骤。

   升级所有节点的估计时间为15小时。

3. 将每个节点的 8 乘以 15 分钟，以说明在 Linux 节点上安装 RPM 或 Deb 软件包的时间。

   此步骤的估计时间为 2 小时。

4. 将这些值相加。

   您最多需要 18 小时才能完成系统升级到 StorageGRID 12.1.0。

> 根据需要、您可以通过批准要在多个会话中升级的网格节点子集来将维护窗口拆分为较小的窗口。例如、您可能希望在一个会话中升级站点A的节点、然后在以后的会话中升级站点B的节点。如果您选择在多个会话中执行升级、请注意、只有在升级完所有节点后、才能开始使用新功能。

StorageGRID 升级对系统的影响

了解StorageGRID系统在升级期间会受到什么影响。

升级完成前允许外部 **SSH** 访问

升级期间允许外部 SSH 访问。升级完成后，外部 SSH 访问默认被阻止。升级后，您可以使用“网格管理器”>“安全设置”页面上的“阻止 SSH”选项卡来"管理外部 SSH 访问"。网格节点之间的 SSH 访问不受影响。

StorageGRID 升级不会造成系统中断

StorageGRID 系统可以在整个升级过程中从客户端应用程序载入和检索数据。如果您批准所有类型相同的节点(例如存储节点)进行升级、则这些节点会一次关闭一个、因此、所有网格节点或特定类型的所有网格节点都不可用。

为了保证持续可用性、请确保ILM策略包含指定存储每个对象的多个副本的规则。此外、还必须确保所有外部S3客户端均配置为向以下项之一发送请求：

- 高可用性(HA)组虚拟IP地址

- 高可用性第三方负载平衡器
- 每个客户端具有多个网关节点
- 每个客户端具有多个存储节点

客户端应用程序可能会发生短期中断

StorageGRID系统可以在整个升级过程中从客户端应用程序中读取数据、但是、如果升级需要重新启动这些节点上的服务、则客户端与各个网关节点或存储节点的连接可能会暂时中断。升级过程完成后、连接将恢复、服务将在各个节点上恢复。

如果无法接受短时间断开连接、则可能需要计划停机时间才能应用升级。您可以使用选择性批准来计划某些节点的更新时间。

> 您可以使用多个网关和高可用性(HA)组在升级过程中提供自动故障转移。请参阅的说明"配置高可用性组"。

后台修复无法在具有混合版本节点的网格上运行

当网格包含混合版本节点时，升级期间不会运行后台修复。站点中断期间出现的任何不一致问题在升级完成之前都不会得到修复。

设备固件已升级

在 StorageGRID 12.1 升级期间：

- 所有 StorageGRID 设备节点都会自动升级到 StorageGRID Appliance Installer 固件版本 12.1。
- SG6060 和 SGF6024 设备自动升级到 BIOS 固件版本 3B08.EX 和BMC固件版本 4.01.07。
- SG100 和 SG1000 设备自动升级到 BIOS 固件版本 3B13.EC 和BMC固件版本 4.75.07。
- SGF6112、SG6160、SG110 和 SG1100 设备自动升级为 BIOS 固件版本 3A14.QD 和 BMC 固件版本 3.21.07。

ILM策略的处理方式会根据其状态而有所不同

- 升级后、活动策略将保持不变。
- 升级时仅保留最新的10个历史策略。
- 如果有建议的策略、则会在升级期间将其删除。

可能会触发警报

服务启动和停止以及 StorageGRID 系统作为混合版本环境运行时（某些网格节点运行早期版本，而其他网格节点已升级到更高版本），可能会触发警报。升级完成后，可能会触发其他警报。

例如，当服务停止时，您可能会看到*无法与节点通信*警报，或者当某些节点已升级到 StorageGRID 12.0 或更高版本，但其他节点仍在运行较早版本的 StorageGRID 时，您可能会看到 *Cassandra 通信错误*警报。通常，这些警报将在升级完成后清除。

在升级到 StorageGRID 12.0 或更高版本期间停止存储节点时，可能会触发 **ILM placement unachievable** 警报。升级完成后，此警报可能会持续 1 天。

升级完成后、您可以从Grid Manager信息板中选择*最近解决的警报*或*当前警报*来查看任何与升级相关的警报。

配置更改受限

> 配置更改限制是特定于版本的。如果要升级到其他 StorageGRID 版本，请参见该版本升级说明中的受限更改列表。

直到 * 启用新功能 * 任务完成：

- 请勿更改任何网格配置。
- 不要启用或禁用任何新功能。
- 请勿更新ILM配置。否则，您可能会遇到不一致的意外 ILM 行为。
- 请勿应用修补程序或恢复网格节点。

> 如果您需要在升级期间恢复节点、请联系技术支持。

- 升级时，不应管理 HA 组、VLAN 接口或负载平衡器端点。
- 在升级完成之前，请勿删除任何 HA 组。其他 HA 组中的虚拟 IP 地址可能无法访问。

完成 * 最终升级步骤 * 任务之前：

- 请勿执行扩展操作步骤。
- 请勿执行停用操作步骤。

升级前验证已安装的 **StorageGRID** 版本

在开始升级之前、请确认当前安装的是先前版本的StorageGRID、并应用了最新的可用修补程序。

关于此任务

在升级到 StorageGRID 12.1 之前，您的网格必须已安装 StorageGRID 12.0 或更高版本。如果您当前使用的是较早版本的 StorageGRID，则必须安装所有以前的升级文件及其最新修补程序（强烈建议），直到网格的当前版本至少为 StorageGRID 12.0.0。

中显示了一个可能的升级路径示例。

> NetApp强烈建议您在升级到下一个版本之前为每个StorageGRID版本应用最新的修补程序，并且还为您安装的每个新版本应用最新的修补程序。在某些情况下，您必须应用修补程序以避免数据丢失的风险。参考 "NetApp 下载： StorageGRID"以及每个修补程序的发行说明以了解更多信息。

验证已安装的版本

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 从网格管理器的顶部，选择 * 帮助 * > * 关于 * 。

3. 验证*版本*是否为 11.9.0.8 或更高版本。
4. 如果*版本*不是 11.9.0.8 或更高版本，请转到 "NetApp 下载： StorageGRID"下载您需要的升级和修补程序文件。
5. "按照升级说明进行操作"对于您下载的每个版本。"应用最新的修补程序"对于每个版本（强烈推荐）。

参考以下升级示例。

示例：从版本 **11.8** 升级到**StorageGRID 12.0**

以下示例显示了从 StorageGRID 版本 11.9 升级到版本 12.0 以准备 StorageGRID 12.1 升级的步骤。

按以下顺序下载并安装软件，以便为您的系统做好升级准备：

1. 升级到StorageGRID 11.8.0主要版本。
2. 应用最新的StorageGRID 11.8.0._y_修补程序。
3. 升级到StorageGRID 11.9.0 主要版本。
4. 应用StorageGRID 11.9.0.8 或更高版本的修补程序。

获取 **StorageGRID** 软件升级所需的材料

开始软件升级之前、请获取所有必需的材料。

项目	备注
服务笔记本电脑	服务笔记本电脑必须具有： • 网络端口 • SSH 客户端（例如 PuTTY ）
"支持的 Web 浏览器"	每个 StorageGRID 版本的浏览器支持通常会发生变化。确保您的浏览器与新的 StorageGRID 版本兼容。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语未在此文件中列出 `Passwords.txt`。
Linux RPM或Deb归档文件	如果在Linux主机上部署了任何节点、则必须"在所有主机上下载并安装RPM或DEB软件包"在开始升级之前先执行此操作。 确保您的 Linux 操作系统满足 StorageGRID 的最低内核版本要求。看"在 Linux 主机上安装StorageGRID" 。
StorageGRID 文档	• "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。在开始升级之前，请务必仔细阅读这些内容。 • "StorageGRID 软件升级解决方案指南" 对于要升级到的主要版本（需要登录） • 其他 "StorageGRID 文档"(根据需要)。

升级前请检查您的 **StorageGRID** 系统的状态

在升级StorageGRID系统之前、请确认系统已准备好进行升级。确保系统正常运行、并且所有网格节点均正常运行。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 检查并解决所有活动警报。
3. 请参阅"内部网格节点通信"和"外部通信"，以确保在升级之前打开 StorageGRID 12.1 的所有所需端口。

   升级到 StorageGRID 12.1 时不需要额外的端口。

升级软件

StorageGRID 升级快速入门

开始升级之前，请查看常规工作流。StorageGRID 升级页面将指导您完成每个升级步骤。

1 准备**Linux**主机

如果在Linux主机上部署了任何StorageGRID节点、"在每个主机上安装 RPM 或 Deb 软件包"请在开始升级之前执行此操作。

2 上传升级和修补程序文件

如果需要、从主管理节点访问StorageGRID 升级页面并上传升级文件和修补程序文件。

3 下载恢复包

在开始升级之前下载当前的恢复包。

4 运行升级预检

升级预检可帮助您检测问题、以便您可以在开始实际升级之前解决这些问题。

5 开始升级

开始升级时、将再次运行预检、并自动升级主管理节点。升级主管理节点时、您无法访问网格管理器。审核日志也将不可用。此升级可能需要长达 30 分钟的时间。

6 下载恢复包

主管理节点升级后，下载新的恢复包。

7 批准节点

您可以批准单个网格节点，一组网格节点或所有网格节点。

除非您确定网格节点已做好停止和重新启动的准备、否则请勿批准该节点的升级。

8 恢复操作

升级完所有网格节点后，将启用新功能，您可以恢复操作。您必须等待执行停用或扩展操作步骤 ，直到完成后台*升级数据库*任务和*最终升级步骤*任务。

相关信息

"估计完成升级所需的时间"

在所有 **Linux** 主机上下载并安装 **StorageGRID** 的 **RPM** 或 **DEB** 软件包

如果在Linux主机上部署了任何StorageGRID节点、请在开始升级之前、在每个主机上下载并安装额外的RPM或DEB软件包。

下载升级、**Linux**和修补程序文件

从网格管理器执行StorageGRID 升级时、系统会提示您首先下载升级归档和任何所需的修补程序。但是、如果您需要下载文件来升级Linux主机、则可以通过提前下载所有必需的文件来节省时间。

步骤

1. 转到。 "NetApp 下载： StorageGRID"
2. 选择用于下载最新版本的按钮，或者从下拉菜单中选择其他版本并选择 * 执行 * 。

   StorageGRID 软件版本采用以下格式： 11.*x.y* 。StorageGRID 修补程序采用以下格式： 11.*x.y.z* 。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 如果出现警告/须知通知，请记下热修补程序编号，然后选中该复选框。
5. 阅读最终用户许可协议(EUA)，选中复选框，然后选择*Accept & Continue*(接受并继续)。

   此时将显示选定版本的下载页面。此页面包含三列。
6. 从第二列(*升级StorageGRID *)下载两个文件：
   - 最新版本的升级归档文件(这是标记为*vmware、SG1000或SG100主管理节点*的部分中的文件)。虽然在执行升级之前不需要此文件、但现在下载它可以节省时间。
   - 或格式的RPM或 `.zip`DEB归档文件 `.tgz`。如果您在服务笔记本电脑上运行Windows、请选择此`.zip`文件。
     - RHEL

       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
     - Ubuntu或Debian

```
StorageGRID-Webscale-version-DEB-uniqueID.zip
StorageGRID-Webscale-version-DEB-uniqueID.tgz
```

7. 如果由于需要修补程序而需要同意警告/必须注意的通知，请下载该修补程序：
   a. 返回到 "NetApp 下载： StorageGRID"。
   b. 从下拉列表中选择修补程序编号。
   c. 再次同意警告通知和EULA。
   d. 下载并保存修补程序及其自述文件。

      开始升级时、系统将提示您上传StorageGRID 升级页面上的修补程序文件。

8. 代码签名验证在 Linux 节点上是手动的。或者，验证安装档案：
   a. 下载StorageGRID代码签名验证包。此软件包的文件名使用格式 `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`，其中 `<version-number>` 是StorageGRID软件版本。
   b. 按照步骤"手动验证安装文件"。

在所有**Linux**主机上安装归档文件

在升级StorageGRID 软件之前、请执行以下步骤。

步骤

1. 从安装文件中提取 RPM 或 Deb 软件包。
2. 在所有 Linux 主机上安装 RPM 或 Deb 软件包。

   请参阅安装 Linux StorageGRID主机服务的步骤"安装 StorageGRID 主机服务"。

   新软件包将作为附加软件包进行安装。

删除先前版本的安装归档

要释放Linux主机上的空间、您可以删除不再需要的早期StorageGRID版本的安装归档文件。

步骤

1. 删除旧的StorageGRID安装归档文件。

RHEL

1. 捕获已安装的StorageGRID软件包的列表： `dnf list | grep -i storagegrid`。

   示例：

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. 删除以前的StorageGRID软件包： `dnf remove images-package service-package`

   > 请勿删除当前正在运行的StorageGRID版本或计划升级到的StorageGRID版本的安装归档。

   您可以安全地忽略显示的警告。它们是指在安装较新的StorageGRID软件包时已被替换的文件。

   示例：

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
================================================================================
========
Package            Architecture      Version           Repository
```

```
Size
================================================================================
========
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
================================================================================
========
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
```

```
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory

  Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64   2/2
  Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  2/2
Installed products updated.
```

```
Removed:
  StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64
  StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64

Complete!
[root@rhel-example ~]#
```

Ubuntu 和 Debian

1. 捕获已安装的StorageGRID软件包列表： `dpkg -l | grep storagegrid`

   示例：

```
root@debian-example:~# dpkg -l | grep storagegrid
ii  storagegrid-webscale-images-11-6-0  11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale docker images for 11.6.0
ii  storagegrid-webscale-images-11-7-0  11.7.0-
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker
images for 11.7.0
ii  storagegrid-webscale-images-11-8-0  11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale docker images for 11.8.0
ii  storagegrid-webscale-images-11-9-0  11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale docker images for 11.9.0
ii  storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale host services for 11.6.0
ii  storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c
amd64 StorageGRID Webscale host services for 11.7.0
ii  storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale host services for 11.8.0
ii  storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale host services for 11.9.0
root@debian-example:~#
```

2. 删除以前的StorageGRID软件包： `dpkg -r images-package service-package`

   > 请勿删除当前正在运行的StorageGRID版本或计划升级到的StorageGRID版本的安装归档。

   示例：

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. 删除StorageGRID容器映像。

Docker

1. 捕获已安装容器映像的列表： `docker images`

   示例：

```
[root@docker-example ~]# docker images
REPOSITORY           TAG             IMAGE ID       CREATED
SIZE
storagegrid-11.9.0   Admin_Node      610f2595bcb4   2 days ago
2.77GB
storagegrid-11.9.0   Storage_Node    7f73d33eb880   2 days ago
2.65GB
storagegrid-11.9.0   API_Gateway     2f0bb79526e9   2 days ago
1.82GB
storagegrid-11.8.0   Storage_Node    7125480de71b   7 months ago
2.54GB
storagegrid-11.8.0   Admin_Node      404e9f1bd173   7 months ago
2.63GB
storagegrid-11.8.0   Archive_Node    c3294a29697c   7 months ago
2.39GB
storagegrid-11.8.0   API_Gateway     1f88f24b9098   7 months ago
1.74GB
storagegrid-11.7.0   Storage_Node    1655350eff6f   16 months ago
2.51GB
storagegrid-11.7.0   Admin_Node      872258dd0dc8   16 months ago
2.48GB
storagegrid-11.7.0   Archive_Node    121e7c8b6d3b   16 months ago
2.41GB
storagegrid-11.7.0   API_Gateway     5b7a26e382de   16 months ago
1.77GB
storagegrid-11.6.0   Admin_Node      ee39f71a73e1   2 years ago
2.38GB
storagegrid-11.6.0   Storage_Node    f5ef895dcad0   2 years ago
2.08GB
storagegrid-11.6.0   Archive_Node    5782de552db0   2 years ago
1.95GB
storagegrid-11.6.0   API_Gateway     cb480ed37eea   2 years ago
1.35GB
[root@docker-example ~]#
```

2. 删除先前StorageGRID版本的容器映像： `docker rmi image id`

   请勿删除当前正在运行的StorageGRID版本或计划升级到的StorageGRID版本的容器映像。

示例：

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051dd
f02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

Podman

1. 捕获已安装容器映像的列表： `podman images`

   示例：

```
[root@podman-example ~]# podman images
REPOSITORY                    TAG           IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0  Storage_Node  7125480de71b  7 months
ago   2.57 GB
localhost/storagegrid-11.8.0  Admin_Node    404e9f1bd173  7 months
ago   2.67 GB
localhost/storagegrid-11.8.0  Archive_Node  c3294a29697c  7 months
ago   2.42 GB
localhost/storagegrid-11.8.0  API_Gateway   1f88f24b9098  7 months
ago   1.77 GB
localhost/storagegrid-11.7.0  Storage_Node  1655350eff6f  16 months
ago  2.54 GB
localhost/storagegrid-11.7.0  Admin_Node    872258dd0dc8  16 months
ago  2.51 GB
localhost/storagegrid-11.7.0  Archive_Node  121e7c8b6d3b  16 months
ago  2.44 GB
localhost/storagegrid-11.7.0  API_Gateway   5b7a26e382de  16 months
ago  1.8 GB
localhost/storagegrid-11.6.0  Admin_Node    ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0  Storage_Node  f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0  Archive_Node  5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0  API_Gateway   cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. 删除先前StorageGRID版本的容器映像： `podman rmi image id`

> 请勿删除当前正在运行的StorageGRID版本或计划升级到的StorageGRID版本的容器映像。

示例：

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

执行 **StorageGRID** 升级

您可以升级到 StorageGRID 12.1 并同时应用该版本的最新修补程序。StorageGRID 升级页面提供建议的升级路径并直接链接到正确的下载页面。

开始之前

您已查看所有注意事项并完成所有规划和准备步骤。

> 如果您急需扩展存储以增加容量（如果您的存储几乎已满），请不要开始升级。及时完成升级程序。如果需要恢复，请联系技术支持。

访问**StorageGRID** 升级页面

首先、访问网格管理器中的StorageGRID 升级页面。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 选择*维护* > 系统 > 软件更新。
3. 从StorageGRID 升级磁贴中，选择*Upgrade*。

选择文件

StorageGRID 升级页面上的更新路径指示必须安装哪些主要版本（例如 12.1.0）和修补程序（例如 12.1.0.1）才能获取最新的 StorageGRID 版本。您应按所示顺序安装推荐的版本和修补程序。

> 如果没有显示更新路径，您的浏览器可能无法访问NetApp支持站点，或者AutoSupport页面（支持 > 工具 > **AutoSupport** > 设置）上的 *检查软件更新*复选框可能被禁用。

步骤

1. 对于*Select files*步骤，查看更新路径。
2. 从“下载文件”部分，选择每个*Download*链接，从NetApp 支持站点 下载所需的文件。

   如果未显示更新路径、请转到 "NetApp 下载： StorageGRID"以确定是否有新版本或修补程序可用、并下载所需的文件。

   > 如果您需要在所有Linux主机上下载并安装RPM或DEB软件包、则更新路径中可能已列出StorageGRID 升级文件和修补程序文件。

3. 选择*浏览*将版本升级文件上传到 StorageGRID：
   `NetApp_StorageGRID_12.1.0_Software_uniqueID.upgrade`

   上传和代码签名验证完成后，文件名旁边会出现一个绿色复选标记。

4. 如果您下载了一个修补程序文件，请选择*Browse*(浏览*)上传该文件。此修补程序将在版本升级过程中自动应用。
5. 选择 * 继续 * 。

运行预检

通过运行预检、您可以在开始升级网格之前检测并解决任何升级问题。

步骤

1. 对于*运行预检*步骤，首先输入网格的配置密码短语。
2. 选择 * 下载恢复包 * 。

   在升级主管理节点之前，您应该下载恢复包文件的当前副本。如果发生故障，恢复包文件可让您恢复系统。

3. 下载文件后、请确认您可以访问其中的内容、包括 `Passwords.txt`文件。
4. 将下载的文件(`.zip`()复制到两个安全、独立的位置。

   恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

5. 选择*运行预检*，并等待预检完成。
6. 查看每次报告的预检查的详细信息，并解决任何报告的错误。请参见 StorageGRID 12.1 版本的 "StorageGRID 软件升级解决方案指南"。

   在升级系统之前、您必须解决所有预检_errors_。但是、您不需要在升级之前解决precheck *WARNIS*。

   如果您已打开任何自定义防火墙端口，则会在预检验证期间收到通知。在继续升级之前，您必须联系技术支持。

7. 如果为解决报告的问题而对配置进行了任何更改，请再次选择*运行预检*以获取更新的结果。

   如果所有错误均已解决、系统将提示您开始升级。

开始升级并升级主管理节点

开始升级时、系统将再次运行升级预检、并自动升级主管理节点。此部分升级可能需要长达30分钟的时间。

升级主管理节点时、您将无法访问任何其他Grid Manager页面。审核日志也将不可用。

步骤

1. 选择*开始升级*。

   此时将显示一条警告、提醒您暂时无法访问网格管理器。

2. 选择*OK*确认警告并开始升级。
3. 等待执行升级预检并升级主管理节点。

   如果报告了任何预检错误，请解决这些错误，然后再次选择*Start upgrade。

   如果网格中的另一个管理节点联机且已准备就绪、则可以使用它来监控主管理节点的状态。升级主管理节点后、您可以批准其他网格节点。

4. 根据需要选择*CONTINUD*以访问*升级其他节点*步骤。

升级其他节点

您必须升级所有网格节点、但可以执行多个升级会话并自定义升级顺序。例如、您可能希望在一个会话中升级站点A的节点、然后在以后的会话中升级站点B的节点。如果您选择在多个会话中执行升级、请注意、只有在升级完所有节点后、才能开始使用新功能。

如果节点升级顺序非常重要，请逐个批准节点或节点组，并等待每个节点完成升级，然后再批准下一个节点或节点组。

> 在网格节点上开始升级时，该节点上的服务将停止。稍后，网格节点将重新启动。为避免与节点通信的客户端应用程序出现服务中断、请勿批准节点的升级、除非您确定节点已做好停止和重新启动的准备。根据需要计划维护时段或通知客户。

步骤

1. 对于*升级其他节点*步骤，请查看摘要，其中提供了整个升级的开始时间以及每个主要升级任务的状态。
   - *启动升级服务*是第一个升级任务。在此任务期间、软件文件将分发到网格节点、并在每个节点上启动升级服务。
   - 当*启动升级服务*任务完成后，*升级其他网格节点*任务启动，并提示您下载恢复包的新副本。
2. 出现提示时，输入您的配置密码并下载恢复包的新副本。

> 主管理节点升级后，您应该下载恢复包文件的新副本。如果发生故障，恢复包文件可让您恢复系统。

3. 查看每种节点类型的状态表。其中包含非主管理节点、网关节点和存储节点的表。

   当表首次出现时，网格节点可以处于以下阶段之一：

   - 解包升级
   - 正在下载
   - 正在等待批准
4. 当您准备好选择要升级的网格节点(或者如果您需要取消批准选定节点)时、请按照以下说明进行操作：

> 对于 StorageGRID 12.1 升级，如果要批准单个节点而不是所有节点，最佳做法是在转移到下一个站点之前升级整个站点。

任务	说明
搜索要批准的特定节点、例如特定站点上的所有节点	在*Search*字段中输入搜索字符串
选择要升级的所有节点	选择*批准所有节点*

任务	说明
选择要升级的相同类型的所有节点(例如、所有存储节点)	选择节点类型的*Approve All*按钮 如果您批准多个相同类型的节点，则这些节点将一次升级一个。
选择要升级的单个节点	选择节点的*Approve*按钮
延迟所有选定节点上的升级	选择*取消批准所有节点*
推迟对所有选定的相同类型节点执行升级	选择节点类型的*Unapprove All*按钮
延迟单个节点上的升级	选择节点的*Unapprove*按钮

5. 等待已批准的节点继续完成以下升级阶段：
   - 已批准且正在等待升级
   - 正在停止服务

     当节点的阶段达到*停止服务*时，无法删除该节点。取消批准*按钮被禁用。
   - 正在停止容器
   - 清理Docker映像
   - 正在升级基本操作系统软件包

     当设备节点达到此阶段时、设备上的StorageGRID 设备安装程序软件将会更新。此自动化过程可确保 StorageGRID 设备安装程序版本与 StorageGRID 软件版本保持同步。
   - 正在重新启动

     某些型号的设备可能会多次重新启动以升级固件和BIOS。
   - 重新启动后执行步骤
   - 正在启动服务
   - 完成
6. 根据需要重复审批步骤多次、直到所有网格节点均已升级为止。

完成升级

当所有网格节点均已完成升级阶段后，*升级其他网格节点*任务将显示为已完成。其余升级任务将在后台自动执行。

步骤

1. *启用功能*任务完成后（最多一小时），您可以开始使用升级后的 StorageGRID 版本中的 "新增功能"。

完成*最终升级步骤*后，即完成升级。第一步*选择文件*将重新显示绿色成功横幅。

2. 验证网格操作是否已恢复正常：
   a. 检查这些服务是否正常运行，以及是否没有意外警报。
   b. 确认客户端与 StorageGRID 系统的连接是否按预期运行。

相关信息

"升级期间对系统的影响"

对 StorageGRID 升级问题进行故障排除

如果在执行升级时出现问题、您可以自行解决问题描述 问题。如果无法解决问题描述 、请尽可能多地收集信息、然后联系技术支持。

升级未完成

以下各节介绍如何从升级部分失败的情况中恢复。

升级预检错误

要检测并解决问题，您可以在开始实际升级之前手动运行升级预检。大多数预检错误都提供了有关如何解决问题描述 的信息。

配置失败

如果自动配置过程失败，请联系技术支持。

网格节点崩溃或无法启动

如果网格节点在升级过程中崩溃或升级完成后无法成功启动，请联系技术支持以调查并更正任何潜在问题。

载入或数据检索中断

如果在不升级网格节点时意外中断数据加网或检索、请联系技术支持。

数据库升级错误

如果数据库升级失败并显示错误，请重试此升级。如果故障再次出现，请联系技术支持。

相关信息

"升级软件前检查系统状况"

用户界面问题

升级期间或之后、网格管理器或租户管理器可能会出现问题。

网格管理器在升级期间显示多条错误消息

如果在升级主管理节点时刷新浏览器或导航到另一个网格管理器页面、您可能会看到多条"503：服务不可用"和"连接到服务器时出现问题"消息。您可以安全地忽略这些消息、它们将在节点升级后立即停止显示。

如果在您开始升级后这些消息显示超过一个小时、则可能是由于某些原因导致主管理节点无法升级。如果您无法自行解决问题描述 问题、请联系技术支持。

Web 界面未按预期响应

升级 StorageGRID 软件后，网格管理器或租户管理器可能无法按预期做出响应。

如果您在使用 Web 界面时遇到问题：

- 确保您使用的是"支持的 Web 浏览器"。

  每个 StorageGRID 版本的浏览器支持通常会发生变化。

- 清除 Web 浏览器缓存。

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

"Docker映像可用性检查"错误消息

尝试启动升级过程时、您可能会收到一条错误消息、指出"以下问题已由Docker映像可用性检查验证套件确定"。必须先解决所有问题、然后才能完成升级。

如果您不确定解决所发现问题所需的更改，请联系技术支持。

消息	发生原因	解决方案
无法确定升级版本。升级版本信息文件 `{file_path}`与预期格式不匹配。	升级软件包已损坏。	请重新上传升级包，然后重试。如果问题仍然存在，请联系技术支持。
未找到升级版本信息文件 `{file_path}`。无法确定升级版本。	升级软件包已损坏。	请重新上传升级包，然后重试。如果问题仍然存在，请联系技术支持。
无法确定上当前安装的版本 `{node_name}`。	节点上的关键文件已损坏。	请联系技术支持。
尝试列出上的版本时出现连接错误 `{node_name}`	节点脱机或连接中断。	请检查以确保所有节点均联机并可从主管理节点访问，然后重试。
节点的主机 `{node_name}`未加载StorageGRID `{upgrade_version}`映像。必须先在主机上安装映像和服务，然后才能继续升级。	用于升级的 RPM 或 Deb 软件包未安装在运行节点的主机上，或者映像仍在导入过程中。 • 注： * 此错误仅适用于在 Linux 上作为容器运行的适用场景 节点。	检查以确保 RPM 或 Deb 软件包已安装在运行节点的所有 Linux 主机上。确保服务和映像文件的版本正确。请稍等几分钟，然后重试。 请参阅。 "Linux ： 在所有主机上安装 RPM 或 Deb 软件包"

消息	发生原因	解决方案
检查节点时出错 `{node_name}`	发生意外错误。	请稍等几分钟，然后重试。
运行预检时未捕获到错误。 `{error_string}`	发生意外错误。	请稍等几分钟，然后重试。

应用StorageGRID修补程序

StorageGRID 热修补程序操作步骤

如果检测到软件问题并在功能版本之间得到解决，则可能需要将修补程序应用于 StorageGRID 系统。

StorageGRID 修补程序包含在功能或修补程序版本之外进行的软件更改。未来版本也会进行同样的更改。此外，每个热修补程序版本都包含此功能或修补程序版本中所有以前的修补程序的汇总。

应用修补程序的注意事项

当另一个维护操作步骤 正在运行时、您无法应用StorageGRID 修补程序。例如、当停用、扩展或恢复操作步骤 正在运行时、您无法应用修补程序。

> 如果节点或站点停用操作步骤 已暂停，您可以安全地应用修补程序。此外，您还可以在 StorageGRID 升级操作步骤 的最后阶段应用修补程序。有关详细信息，请参见有关升级 StorageGRID 软件的说明。

在网格管理器中上传此修补程序后，此修补程序将自动应用于主管理节点。然后，您可以批准将此修补程序应用于 StorageGRID 系统中的其余节点。

如果某个修补程序无法应用到一个或多个节点，则失败的原因将显示在该修补程序进度表的详细信息列中。您必须解决导致失败的任何问题，然后重试整个过程。先前已成功应用此修补程序的节点将在后续应用程序中跳过。您可以根据需要安全地重试此修复程序多次，直到所有节点均已更新为止。要使应用程序完成，必须在所有网格节点上成功安装此修补程序。

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

如何应用修补程序进行恢复和扩展

将修补程序应用于网格后，主管理节点或非主管理节点会自动将相同的修补程序版本安装到通过恢复操作恢复或添加到扩展中的任何节点。登录到非主管理节点时，可以恢复任何节点（包括主管理节点）。如果从非主管理节点恢复节点，则该管理节点会将修补程序应用于已恢复的节点。

如果需要从自己的 StorageGRID 安装程序恢复主管理节点，则必须手动安装正确的 StorageGRID 版本，然后应用修补程序。主管理节点的最终 StorageGRID 版本必须与网格中其他节点的版本匹配。

以下示例说明了如何在登录到非主管理节点时恢复主管理节点的过程中应用修补程序：

1. 假设网格运行的是具有最新修补程序的 StorageGRID 11.*A.B* 版本。"网格版本"为11.*A.B.y*。

2. 主管理节点出现故障。
3. 您可以使用 StorageGRID 11.*A.B* 重新部署主管理节点，并执行恢复操作步骤 。

   根据与网格版本匹配的要求、您可以在部署节点时使用次要版本；您无需先部署主要版本。

4. 然后，将修补程序 11.*A.B.y* 应用于主管理节点。

应用修补程序时如何影响 **StorageGRID**

您必须了解应用修补程序时 StorageGRID 系统将受到什么影响。

StorageGRID修补程序无中断运行

在整个修复程序过程中、StorageGRID系统可以从客户端应用程序中加热和检索数据。如果您批准所有类型相同的节点加入修补程序(例如存储节点)、则这些节点一次关闭一个、因此所有网格节点或特定类型的所有网格节点都不可用。

为了保证持续可用性、请确保ILM策略包含指定存储每个对象的多个副本的规则。此外、还必须确保所有外部S3客户端均配置为向以下项之一发送请求：

- 高可用性(HA)组虚拟IP地址
- 高可用性第三方负载平衡器
- 每个客户端具有多个网关节点
- 每个客户端具有多个存储节点

客户端应用程序可能会发生短期中断

StorageGRID 系统可以在整个修补程序过程中从客户端应用程序载入和检索数据；但是，如果修补程序需要在各个网关节点或存储节点上重新启动服务，则客户端与这些节点的连接可能会暂时中断。修复程序过程完成并在各个节点上恢复服务后，连接将恢复。

如果无法接受短时间内断开连接，您可能需要计划停机时间以应用修补程序。您可以使用选择性批准来计划某些节点的更新时间。

您可以使用多个网关和高可用性（ High Availability ， HA ）组在修复程序过程中提供自动故障转移。请参阅的说明"配置高可用性组"。

可能会触发警报和 **SNMP** 通知

当服务重新启动以及 StorageGRID 系统作为混合版本环境运行时（某些网格节点运行早期版本，而另一些网格节点已升级到更高版本），可能会触发警报和 SNMP 通知。通常，这些警报和通知将在修复程序完成时清除。

配置更改受限

将修补程序应用于 StorageGRID 时：

- 在将修补程序应用于所有节点之前、请勿更改任何网格配置(例如、指定网格网络子网或批准待定网格节点)。

- 在将修补程序应用于所有节点之前、请勿更新ILM配置。

获取 StorageGRID 修补程序所需的材料

在应用修补程序之前，您必须获取所有必需的材料。

项目	备注
StorageGRID 修补程序文件	您必须下载 StorageGRID 修补程序文件。
• 网络端口 • "支持的 Web 浏览器" • SSH 客户端（例如 PuTTY ）	
Recovery package (`.zip`) 文件	在应用修补程序之前，"下载最新的恢复包文件"以防修复期间出现任何问题。然后，在应用修补程序后，下载恢复包文件的新副本并将其保存在安全的位置。更新后的恢复包文件允许您在发生故障时恢复系统。
Passwords.txt 文件	可选，仅当您使用 SSH 客户端手动应用修补程序时才使用。这 `Passwords.txt`文件是恢复包的一部分 `.zip`文件。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语未在此文件中列出 `Passwords.txt`。
相关文档	`readme.txt`文件。此文件包含在热修补程序下载页面中。在应用此修补程序之前，请务必仔细阅读此 `readme`文件。

下载 StorageGRID 修补程序文件

您必须先下载此修补程序文件，然后才能应用此修补程序。

步骤

1. 转到。 "NetApp 下载： StorageGRID"
2. 选择 * 可用软件 * 下的向下箭头可查看可供下载的修补程序列表。

   修补程序文件版本的格式为： 11.4_.x.y_ 。

3. 查看更新中包含的更改。

   如果您只安装了"已恢复主管理节点"、并且需要应用修补程序、请选择安装在其他网格节点上的相同修补程序版本。

   a. 选择要下载的热修补程序版本，然后选择 * 执行 * 。

   b. 使用您的 NetApp 帐户的用户名和密码登录。

c. 阅读并接受最终用户许可协议。

此时将显示选定版本的下载页面。

d. 下载修补程序 `readme.txt`文件以查看修补程序中所做更改的摘要。

4. 选择此修补程序的下载按钮，然后保存此文件。

请勿更改此文件的名称。

如果您使用的是macOS设备、修补程序文件可能会自动另存为 `.txt`文件。如果是、则必须重命名不带扩展名的文件 `.txt`。

5. 选择下载位置，然后选择 * 保存 * 。

在应用 StorageGRID 修补程序之前检查系统状况

您必须验证系统是否已准备好容纳此修补程序。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 如果可能，请确保系统运行正常，并且所有网格节点均已连接到网格。

连接的节点在"节点"页面上有绿色复选标记 。

3. 如果可能，请检查并解决任何当前警报。
4. 确保未执行任何其他维护过程，例如升级，恢复，扩展或停用操作步骤 。

应用修补程序之前，您应等待所有活动的维护过程完成。

当另一个维护操作步骤 正在运行时、您无法应用StorageGRID 修补程序。例如、当停用、扩展或恢复操作步骤 正在运行时、您无法应用修补程序。

如果是节点或站点"已暂停停用操作步骤"，则可以安全地应用修补程序。此外，您还可以在 StorageGRID 升级操作步骤 的最后阶段应用修补程序。请参阅的说明"正在升级StorageGRID 软件"。

在 StorageGRID 中应用热修复

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

开始之前

- 您已查看"应用修补程序的注意事项"。
- 您具有配置密码短语。

- 您具有root访问权限或维护权限。

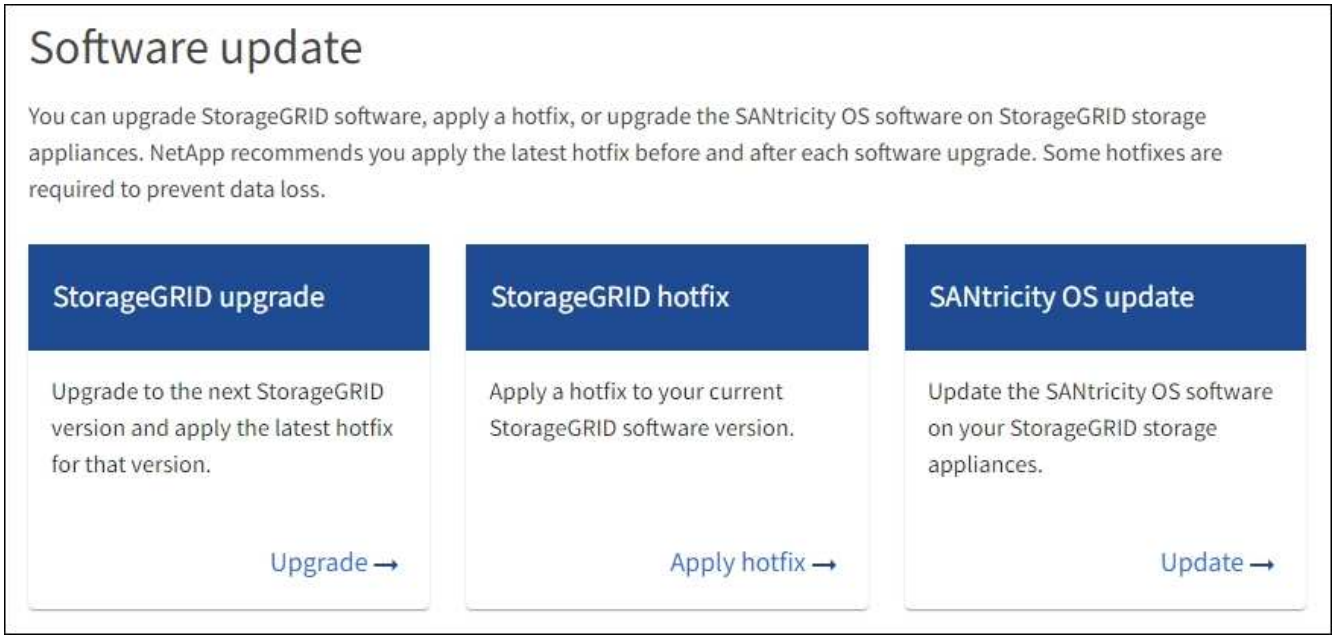
关于此任务

- 您可以延迟向节点应用修补程序，但只有在将修补程序应用到所有节点之后，此修补程序过程才会完成。
- 在完成修补程序过程之前、您无法执行StorageGRID 软件升级或SANtricity OS更新。

步骤

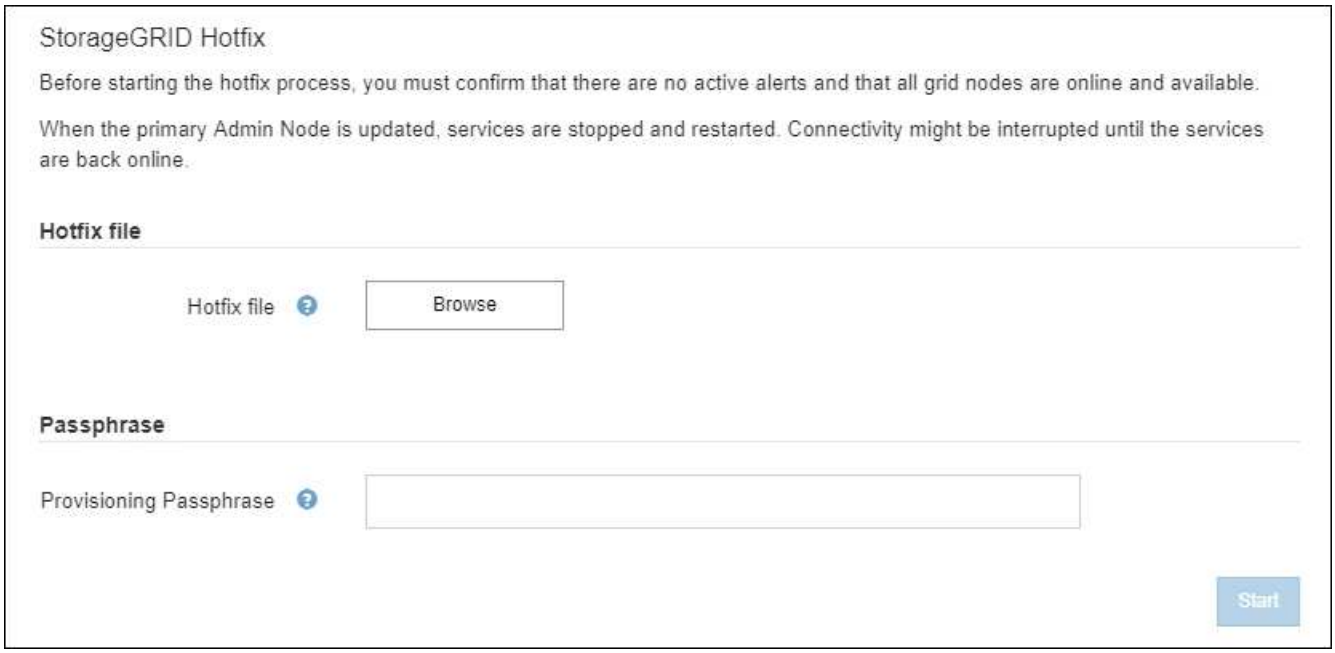
1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 选择*维护* > 系统 > 软件更新。

   此时将显示软件更新页面。



3. 选择 * 应用修补程序 * 。

   此时将显示 StorageGRID 热修补程序页面。



4. 选择从NetApp 支持站点 下载的修补程序文件。

   a. 选择 * 浏览 * 。

   b. 找到并选择文件。

      `hotfix-install-version`

   c. 选择 * 打开 * 。

      已上传此文件。上传完成后，文件名将显示在详细信息字段中。

      请勿更改文件名、因为它是验证过程的一部分。

5. 在文本框中输入配置密码短语。

   此时将启用 * 开始 * 按钮。

6. 选择 * 开始 * 。

   此时将显示一条警告，指出当主管理节点上的服务重新启动时，您的浏览器连接可能会暂时断开。

7. 选择 * 确定 * 开始将此修补程序应用于主管理节点。

   当修复程序启动时：

   a. 运行修补程序验证，包括代码签名验证。

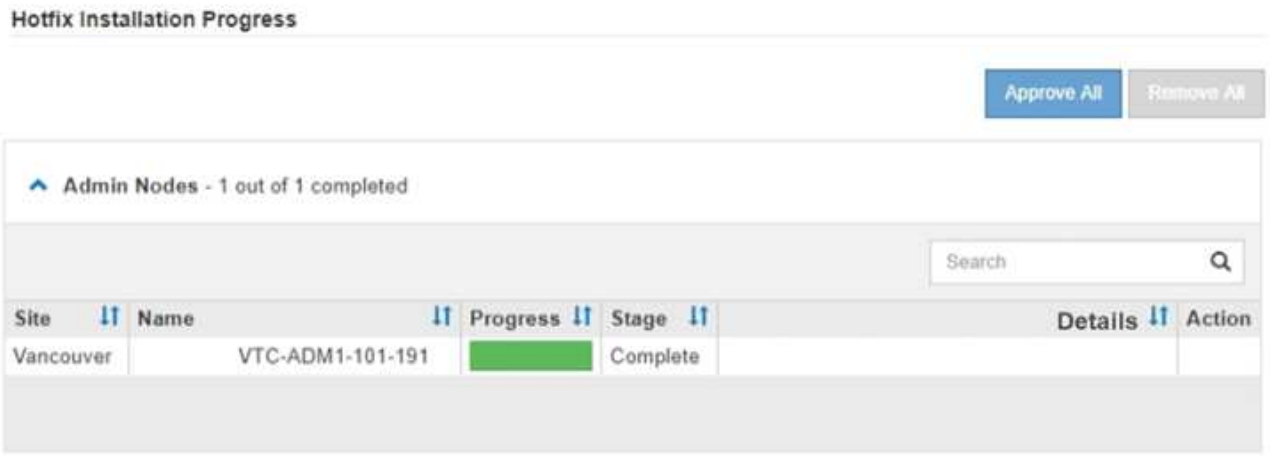
      如果报告了任何错误，请予以解决，重新上传此修复程序文件，然后再次选择 * 启动 * 。

   b. 此时将显示热修补程序安装进度表。

      此表显示了网格中的所有节点以及每个节点的修补程序安装的当前阶段。表中的节点按类型(管理节点、

网关节点和存储节点)进行分组。

c. 进度条完成后、主管理节点将显示为"完成"。



8. 或者，也可以按 * 站点 * ， * 名称 * ， * 进度 * ， * 阶段 * 或 * 详细信息 * 按升序或降序对每个分组中的节点列表进行排序。或者，在 * 搜索 * 框中输入一个术语以搜索特定节点。
9. 批准已准备好更新的网格节点。相同类型的已批准节点将一次升级一个。

除非您确定某个节点已准备好进行更新、否则请勿批准该节点的修补程序。将此修补程序应用于网格节点后、此节点上的某些服务可能会重新启动。对于与节点通信的客户端，这些操作可能会导致发生原因 服务中断。

- 选择一个或多个 * 批准 * 按钮将一个或多个单独的节点添加到修补程序队列。
- 在每个分组中选择 * 全部批准 * 按钮，将所有类型相同的节点添加到修补程序队列。如果您在 * 搜索 * 框中输入了搜索条件，则 * 全部批准 * 按钮将适用场景 所有搜索条件选择的节点。

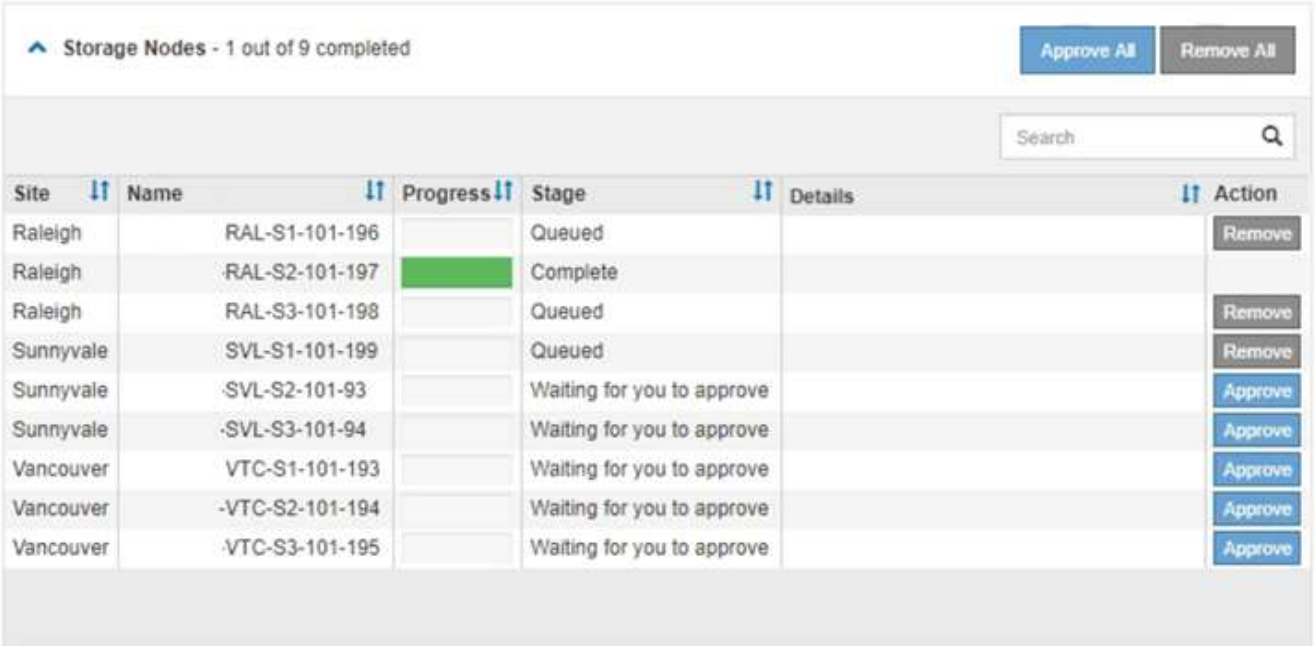
页面顶部的 * 全部批准 * 按钮批准页面上列出的所有节点，而分组表顶部的 * 全部批准 * 按钮仅批准该组中的所有节点。如果节点升级顺序非常重要，请一次批准一个节点或一组节点，并等待每个节点完成升级，然后再批准下一个节点。

- 选择页面顶部的顶级 * 全部批准 * 按钮，将网格中的所有节点添加到热修补程序队列。

您必须先完成 StorageGRID 热修补程序，然后才能启动其他软件更新。如果无法完成此修补程序，请联系技术支持。

- 选择 * 删除 * 或 * 全部删除 * 可从修补程序队列中删除一个节点或所有节点。

当此阶段进入"已排队"之后，*删除*按钮将隐藏，您无法再从修补程序进程中删除此节点。



10. 请稍候，此修补程序将应用于每个已批准的网格节点。

    在所有节点上成功安装此修复程序后，热修复程序安装进度表将关闭。绿色横幅显示了完成修补程序的日期和时间。

11. 如果无法将此修补程序应用于任何节点，请查看每个节点的错误，解决问题描述 ，然后重复上述步骤。

    只有在将此修补程序成功应用于所有节点之后，操作步骤 才会完成。您可以根据需要安全地重试此修复程序多次，直到其完成为止。

配置和管理StorageGRID系统

管理 StorageGRID

StorageGRID 管理快速入门

按照以下说明配置和管理 StorageGRID 系统。

确保您对 StorageGRID 系统有基本了解，并且对 Linux 命令行 Shell、网络以及服务器硬件设置和配置有相当详细的了解。

1 开始使用 **Grid Manager**

- "了解使用 Grid Manager 用户界面的基本步骤"
- "了解许可证信息"
- "了解如何使用网格管理API"

2 控制对 **StorageGRID** 的访问

- "了解密码短语、密码和权限"
- "配置身份联合"
- "管理管理组"
- "管理用户"
- "配置单点登录(SSO)"

3 使用网格联盟

- "配置网格联盟连接"
- "了解账号同步"
- "了解跨网格复制"
- "配置全局命名空间"

4 管理安全性

- "查看 StorageGRID 加密方法"
- "管理证书"
- "配置安全设置"
- "配置密钥管理服务器"
- "管理代理设置"

- "控制防火墙"

5 管理租户

- "了解并管理租户帐户"
- "管理租户的平台服务"
- "管理租户帐户的 S3 Select"

6 配置客户端连接

- "了解 S3 客户端的安全性"
- "使用S3设置向导"
- "管理高可用性组"
- "配置S3端点域名"

7 管理网络和连接

- "配置网络设置"
- "配置 VLAN 接口"
- "管理流量分类策略"
- "管理链路成本"

8 管理节点

- "管理存储节点"
- "管理管理节点"

开始使用Grid Manager

StorageGRID 的 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	138
Microsoft Edge	138
Mozilla Firefox	140

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

Sign in 到 StorageGRID 网格管理器

您可以通过在支持的 Web 浏览器的地址栏中输入管理节点的完全限定域名（ FQDN ）或 IP 地址来访问网格管理器登录页面。

每个 StorageGRID 系统都包括一个主管理节点和任意数量的非主管理节点。您可以登录到任何管理节点上的网格管理器来管理 StorageGRID 系统。但是、某些维护过程只能从主管理节点执行。

连接到**HA**组

如果管理节点包含在高可用性（ HA ）组中，则可以使用 HA 组的虚拟 IP 地址或映射到虚拟 IP 地址的完全限定域名进行连接。应选择主管理节点作为组的主接口，以便在访问网格管理器时，您可以在主管理节点上访问它，除非主管理节点不可用。请参阅。 "管理高可用性组"

使用**SSO**

如果"已配置单点登录(SSO)"。

在第一个管理节点上登录到网格管理器

开始之前

- 您已拥有登录凭据。
- 您正在使用"支持的 Web 浏览器"。
- 已在 Web 浏览器中启用 Cookie 。
- 您所属的用户组至少具有一个权限。
- 您有网格管理器的URL：

  `https://FQDN_or_Admin_Node_IP/`

  您可以使用完全限定域名、管理节点的IP地址或管理节点HA组的虚拟IP地址。

  要通过非HTTPS默认端口(443)访问网格管理器、请在URL中包含端口号：

  `https://FQDN_or_Admin_Node_IP:port/`

步骤

1. 启动受支持的 Web 浏览器。
2. 在浏览器的地址栏中、输入网格管理器的URL。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。请参阅。 "管理安全证书"
4. 登录到网格管理器。

显示的登录屏幕取决于是否已为StorageGRID 配置单点登录(Single Sign On、SSO)。

未使用**SSO**

a. 输入网格管理器的用户名和密码。
b. 选择 * 登录 * 。

使用**SSO**

- 如果StorageGRID 正在使用SSO、而这是您首次在此浏览器上访问此URL：
  i. 选择 * 登录 * 。您可以在帐户字段中保留0。
  ii. 在您组织的 SSO 登录页面上输入您的标准 SSO 凭据。

  例如，如果StorageGRID正在使用 SSO 并且您之前访问过网格管理器或租户帐户：

  A. 输入*0*(网格管理器的帐户ID)或选择*Grid Manager*(如果它出现在最近帐户列表中)。
  B. 选择 * 登录 * 。
  C. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。

登录后、将显示网格管理器的主页、其中包括信息板。要了解所提供的信息，请参见"查看和管理信息板"。

登录到其他管理节点

按照以下步骤登录到其他管理节点。

未使用**SSO**

步骤

1. 在浏览器的地址栏中，输入另一个管理节点的完全限定域名或 IP 地址。根据需要包括端口号。
2. 输入网格管理器的用户名和密码。
3. 选择 * 登录 * 。

使用**SSO**

如果StorageGRID 正在使用SSO、并且您已登录到一个管理节点、则可以访问其他管理节点、而无需重新登录。

步骤

1. 在浏览器的地址栏中输入另一个管理节点的完全限定域名或IP地址。
2. 如果您的SSO会话已过期、请重新输入您的凭据。

从 **StorageGRID Grid Manager** 中注销

使用网格管理器完成后、您必须注销以确保未经授权的用户无法访问StorageGRID 系统。根据浏览器 Cookie 设置，关闭浏览器可能无法将您从系统中注销。

步骤

1. 在右上角选择您的用户名。
2. 选择*注销*。

选项	说明
SSO 未使用	您已从管理节点注销。 此时将显示网格管理器登录页面。 • 注意： * 如果您已登录到多个管理节点，则必须从每个节点注销。
已启用SSO	您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。* 网格管理器 * 在 * 近期帐户 * 下拉列表中列为默认值， * 帐户 ID* 字段显示 0 。 *注意：*如果启用了 SSO 并且您也登录了租户管理器，您还必须"注销租户帐户"到"注销SSO"。

更改您的 **StorageGRID Grid Manager** 密码

如果您是网格管理器的本地用户，则可以更改自己的密码。

开始之前

您已使用登录到网格管理器"支持的 Web 浏览器"。

关于此任务

如果您以联盟用户身份登录到StorageGRID 、或者启用了单点登录(SSO)、则无法在网格管理器中更改密码。而是必须更改外部身份源中的密码，例如 Active Directory 或 OpenLDAP 。

步骤

1. 从网格管理器标题中，选择 * 。您的姓名 _* > * 更改密码 * 。
2. 输入当前密码。
3. 键入新密码。

   您的密码必须至少包含 8 个字符，并且不能超过 32 个字符。密码区分大小写。

4. 重新输入新密码。
5. 选择 * 保存 * 。

查看 **StorageGRID** 许可证信息

您可以根据需要查看 StorageGRID 系统的许可证信息，例如网格的最大存储容量。

开始之前

您已使用登录到网格管理器"支持的 Web 浏览器"。

关于此任务

如果某个问题描述 具有此StorageGRID 系统的软件许可证，信息板上的运行状况卡将包含一个许可证状态图标和一个*License*链接。此数字表示与许可证相关的问题数量。



步骤

1. 通过执行以下操作之一访问许可证页面：
   - 选择*维护* > 系统 > 许可证。
   - 从信息板上的运行状况卡中，选择许可证状态图标或*License*链接。

     只有当具有许可证的问题描述 时，才会显示此链接。
2. 查看当前许可证的只读详细信息：
   - StorageGRID 系统 ID ，此 ID 是此 StorageGRID 安装的唯一标识号
   - 许可证序列号
   - 许可证类型，永久*或*订阅
   - 网格的许可存储容量
   - 支持的存储容量
   - 许可证结束日期。*不适用*表示永久许可证。
   - 支持结束日期

     此日期是从当前许可证文件读取的，如果您在获取许可证文件后延长或续订支持服务合同，则此日期可能已过期。要更新此值，请参阅"更新 StorageGRID 许可证信息"。您还可以使用 Digital Advisor 查看实际合同结束日期。
   - 许可证文本文件的内容

更新 **StorageGRID** 许可证信息

您必须在许可证条款发生更改时随时更新 StorageGRID 系统的许可证信息。例如，如果为网格购买了额外的存储容量，则必须更新许可证信息。

开始之前

- 您有一个新的许可证文件可应用于 StorageGRID 系统。
- 您拥有 "特定访问权限"。
- 您具有配置密码短语。

步骤

1. 选择*维护* > 系统 > 许可证。
2. 在“更新许可证”部分中，选择*Browse*。
3. 找到并选择新的许可证文件(`.txt`)。

   此时将验证并显示新许可证文件。

4. 输入配置密码短语。
5. 选择 * 保存 * 。

使用API

使用 StorageGRID 网格管理 API

您可以使用网格管理 REST API 执行系统管理任务，而不是使用网格管理器用户界面。例如，您可能希望使用 API 来自动执行操作或更快地创建多个实体，例如用户。

顶级资源

网格管理 API 可提供以下顶级资源：

- `/grid`：访问仅限于Grid Manager用户，并且取决于配置的组权限。
- `/org`：访问仅限于属于租户帐户的本地或联合LDAP组的用户。有关详细信息，请参见 "使用租户帐户"。
- `/private`：访问仅限于Grid Manager用户，并且取决于配置的组权限。专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

问题描述 API 请求

网格管理 API 使用 Swagger 开源 API 平台。Swagger 提供了一个直观的用户界面，使开发人员和非开发人员能够使用 API 在 StorageGRID 中执行实时操作。

Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。

开始之前

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

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

步骤

1. 从网格管理器标题中，选择帮助图标 并选择 **API documentation**。

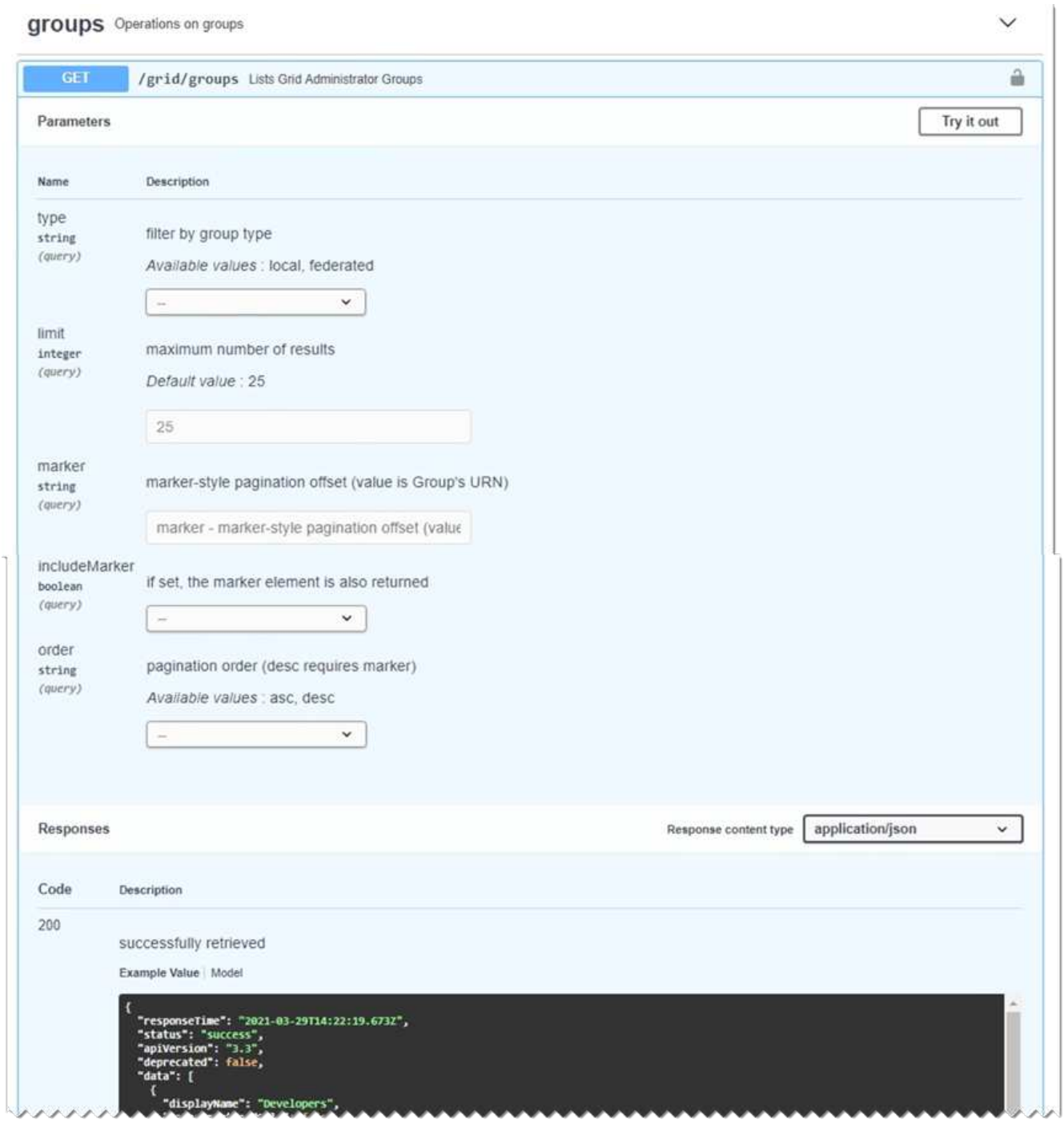
2. 要使用专用 API 执行操作，请在 StorageGRID 管理 API 页面上选择 * 转至专用 API 文档 * 。

   专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

3. 选择所需的操作。

   展开 API 操作时，您可以看到可用的 HTTP 操作，例如 GET ， PUT ， UPDATE 和 DELETE 。

4. 选择 HTTP 操作可查看请求详细信息，包括端点 URL ，任何必需或可选参数的列表，请求正文示例（如果需要）以及可能的响应。



5. 确定此请求是否需要其他参数，例如组或用户 ID 。然后，获取这些值。您可能需要先对其他 API 请求进行

问题描述 处理，以获取所需的信息。

6. 确定是否需要修改示例请求正文。如果是，您可以选择 * 型号 * 来了解每个字段的要求。
7. 选择 * 试用 * 。
8. 提供所需的任何参数，或根据需要修改请求正文。
9. 选择 * 执行 * 。
10. 查看响应代码以确定请求是否成功。

StorageGRID 中的网格管理 API 操作

网格管理 API 将可用操作组织到以下部分中。

此列表仅包含公有 API 中可用的操作。

- 帐户：用于管理存储租户帐户的操作、包括创建新帐户和检索给定帐户的存储使用量。
- **alerts**历史记录：对已解决的警报执行操作。
- 警报接收者：警报通知接收者操作(电子邮件)。
- 警报规则：对警报规则执行操作。
- 警报静音：警报静音操作。
- 警报：对警报执行操作。
- **audi**：列出和更新审核配置的操作。
- **auth**：执行用户会话身份验证的操作。

  网格管理 API 支持不可承载令牌身份验证方案。要登录，请在身份验证请求的JSON正文(即)中提供用户名和密码 `POST /api/v3/authorize`。如果用户已成功通过身份验证，则会返回一个安全令牌。此令牌必须在后续 API 请求的标题中提供（ "Authorization： bearer *token*" ）。令牌将在16小时后过期。

  如果为 StorageGRID 系统启用了单点登录，则必须执行不同的步骤进行身份验证。请参见"如果启用了单点登录、则在API中进行身份验证"。

  有关提高身份验证安全性的信息、请参见"防止跨站点请求伪造"。

- **client-certificates**：用于配置客户端证书的操作，以便使用外部监控工具安全地访问StorageGRID。
- **config**：与网格管理API的产品发行版和版本相关的操作。您可以列出该版本支持的网格管理 API 的产品版本和主要版本，并且可以禁用已弃用的 API 版本。
- *DEactive-Features *：用于查看可能已停用的功能的操作。
- **DNS-SERVERS**：列出和更改已配置的外部DNS服务器的操作。
- 驱动器详细信息：针对特定存储设备型号对驱动器执行的操作。
- **endpoint-domain-names**：列出和更改S3端点域名的操作。
- 纠删编码：对纠删编码配置文件的操作。
- 扩展：扩展操作(程序级)。
- 扩展节点：扩展操作(节点级)。

- 扩展站点：扩展操作(站点级)。
- *GRE-NETWORKS：列出和更改Grid Network List的操作。
- **GRID**密码：网格密码管理操作。
- 组：用于管理本地网格管理员组以及从外部LDAP服务器检索联合网格管理员组的操作。
- 身份源：用于配置外部身份源以及手动同步联盟组和用户信息的操作。
- *ILM：有关信息生命周期管理(ILM)的操作。
- *in-Progress－Procedures *：检索当前正在进行的维护程序。
- **license**：用于检索和更新StorageGRID 许可证的操作。
- **logs**：用于收集和下载日志文件的操作
- **metrics**：对StorageGRID 指标的操作，包括在某一时间点的即时指标查询和在一段时间内的范围指标查询。网格管理 API 使用 Prometheus 系统监控工具作为后端数据源。有关构建 Prometheus 查询的信息，请参见 Prometheus 网站。

> 名称中包含的指标*private*仅供内部使用。这些指标可能会在 StorageGRID 版本之间发生更改，恕不另行通知。

- 节点详细信息：对节点详细信息执行的操作。
- 节点运行状况：对节点运行状况执行的操作。
- **NONE-storage-state**：对节点存储状态执行的操作。
- **ntp-server**：列出或更新外部网络时间协议(NTP)服务器的操作。
- 对象：对对象和对象元数据执行的操作。
- 恢复：恢复操作步骤 的操作。
- **recovery-package**：下载恢复包的操作。
- 区域：用于查看和创建区域的操作。
- **s3-object-lock**：对全局S3对象锁定设置执行操作。
- **server-certificates**：用于查看和更新Grid Manager服务器证书的操作。
- **SNMP**：对当前SNMP配置执行的操作。
- **storage-**水 印：存储节点水印。
- **Traffic Classes**：流量分类策略的操作。
- 不可信客户端网络：对不可信客户端网络配置执行的操作。
- 用户：用于查看和管理Grid Manager用户的操作。

StorageGRID 中的网格管理 API 版本控制

网格管理 API 使用版本控制来支持无中断升级。

例如、此请求URL指定API版本4。

`https://hostname_or_ip_address/api/v4/authorize`

如果所做的更改与旧版本不兼容、则API的主要版本会发生碰撞。如果对_are compender_与旧版本进行了更改、则API的次要版本会发生碰撞。兼容的更改包括添加新端点或新属性。

以下示例说明了如何根据所做更改的类型对 API 版本进行递增。

API 的更改类型	旧版本	新版本
与旧版本兼容	2.1	2.2
与旧版本不兼容	2.1	3.0

首次安装StorageGRID软件时、仅会启用最新版本的API。但是，在升级到 StorageGRID 的新功能版本时，您仍可以访问至少一个 StorageGRID 功能版本的旧版 API 。

> 您可以配置受支持的版本。有关详细信息，请参见Swagger API文档的*config*部分"网格管理API"。在更新所有API客户端以使用较新版本后、您应停用对较旧版本的支持。

已过时的请求将通过以下方式标记为已弃用：

- 响应标头为 "depression: true"
- JSON 响应正文包含 "depressioned" ： true
- NMS.log 中会添加一个已弃用的警告。例如：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

确定当前版本支持哪些 **API** 版本

使用 `GET /versions`API请求返回受支持的API主要版本的列表。此请求位于Swagger API文档的*config*部分。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

指定请求的 **API** 版本

您可以使用路径参数(`/api/v4`()或标题(`Api-Version: 4`()指定API版本。如果同时提供这两个值，则标头值

将覆盖路径值。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

防止 **StorageGRID** 中的跨站请求伪造 **(CSRF)**

您可以通过使用 CSRF 令牌增强使用 Cookie 的身份验证，帮助防止 StorageGRID 受到跨站点请求伪造（ CSRF ）攻击。网格管理器和租户管理器会自动启用此安全功能；其他 API 客户端可以选择在登录时是否启用此功能。

如果攻击者可能触发对其他站点的请求（例如使用 HTTP 表单发布），则可以对使用已登录用户的 cookie 发出的某些请求进行发生原因 处理。

StorageGRID 可通过使用 CSRF 令牌帮助防止 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标题或特定后处理正文参数的内容匹配。

要启用此功能、请在身份验证期间将参数设置 `csrfToken`为 `true`。默认值为 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果为true、则会为Cookie设置一个 `GridCsrfToken`用于登录到网格管理器的随机值、并 `AccountCsrfToken`为Cookie设置一个用于登录到租户管理器的随机值。

如果存在 Cookie ，则可以修改系统状态的所有请求（ POST ， PUT ， patch ， delete ）都必须包括以下项之一：

- `X-Csrf-Token`标头、标头值设置为CRF令牌cookie的值。
- 对于接受窗体编码正文的端点： `csrfToken`窗体编码请求正文参数。

有关其他示例和详细信息，请参见联机 API 文档。

> 设置了CRF令牌Cookie的请求还会对任何希望使用JSON请求正文作为额外保护来抵御CRF攻击的请求强制实施"Contene-Type：application/json"标头。

如果启用了单点登录，请使用 **API**

如果已启用单一登录，请使用 **StorageGRID API**（**Active Directory**）

如果你有"已配置并启用单点登录（ SSO ）"并且您使用 Active Directory 作为 SSO 提供程序，则必须发出一系列 API 请求以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了单点登录，请登录到 **API**

如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用。

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- 这 `storagegrid-ssoauth.py`Python 脚本，位于StorageGRID安装文件目录中(./rpms`对于 RHEL ， `./debs`适用于 Ubuntu 或 Debian，以及 `./vsphere`对于 VMware)。
- cURL 请求的示例工作流。

  如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误： `A valid SubjectConfirmation was not found on this Response`。

  示例 cURL 工作流不会保护密码不会被其他用户看到。

如果存在URL编码问题，则可能会看到以下错误： `Unsupported SAML version`。

步骤

1. 选择以下方法之一以获取身份验证令牌：
   - 使用 `storagegrid-ssoauth.py`Python脚本。转至步骤 2 。
   - 使用 curl 请求。转至步骤 3 。
2. 如果要使用该 `storagegrid-ssoauth.py`脚本、请将该脚本传递给Python解释器并运行该脚本。

   出现提示时，输入以下参数的值：

   - SSO 方法。输入 ADFS 或 ADFS 。
   - SSO 用户名
   - 安装 StorageGRID 的域
   - StorageGRID 的地址
   - 要访问租户管理 API 的租户帐户 ID 。

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下操作步骤 。

   a. 声明登录所需的变量。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

   要访问网格管理API，请使用0作为 `TENANTACCOUNTID`。

   b. 要接收签名的身份验证URL，请向发出POST请求 `/api/v3/authorize-saml`，然后从响应中删除其他JSON编码。

   此示例显示了的签名身份验证URL的POST请求 `TENANTACCOUNTID`。结果将传递到 `python -m json.tool`以删除JSON编码。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 保存响应中的、 `SAMLRequest`以供后续命令使用。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. 从 AD FS 获取包含客户端请求 ID 的完整 URL 。

一种方法是使用上一响应中的 URL 请求登录表单。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

此响应包括客户端请求 ID ：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 保存响应中的客户端请求 ID 。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 将您的凭据发送到上一响应中的表单操作。

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS 返回 302 重定向，并在标题中显示追加信息 。

> 如果为 SSO 系统启用了多因素身份验证（ MFA ），则此表单发布还将包含第二个密码或其他凭据。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 保存 `MSISAuth`响应中的cookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 使用身份验证 POST 中的 Cookie 将 GET 请求发送到指定位置。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

响应标头将包含 AD FS 会话信息，以便日后注销时使用，而响应正文将 SAMLResponse 隐藏在一个格式的字段中。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 从隐藏字段保存 `SAMLResponse`：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用保存的 `SAMLResponse`，发出StorageGRID`/api/saml-response`请求以生成StorageGRID身份验证令牌。

对于 `RelayState`，请使用租户帐户ID；如果要登录到网格管理API，请使用0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

响应包括身份验证令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 将响应中的身份验证令牌另存为 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

现在、您可以对其他请求使用、与未使用SSO时使用 `MYTOKEN`API的方式类似。

如果启用了单点登录，请注销 API

如果已启用单点登录（ Single Sign-On ， SSO ），则必须对一系列 API 请求进行问题描述 ，才能注销网格管理 API 或租户管理 API 。如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要、您可以从组织的单点注销页面注销、以注销StorageGRID API。或者，您也可以从 StorageGRID 触发单点注销（ SLO ），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求、请将`cookie "sso=true "传递到SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回注销 URL ：

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 保存注销 URL 。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。如果未提供`cookie "sso=true "、则用户将从StorageGRID中注销、而不会影响SSO状态。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

`204 No Content`响应指示用户现在已注销。

```
HTTP/1.1 204 No Content
```

如果已启用单点登录，请使用 **StorageGRID API**（**Entra ID**）

如果你有"已配置并启用单点登录（ SSO ）"并且您使用 Entra ID 作为 SSO 提供程序，您可以使用两个示例脚本来获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了 **Entra ID** 单点登录，**Sign inAPI**

如果您使用 Entra ID 作为 SSO 身份提供商，则适用这些说明

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 电子邮件地址和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例脚本：

- `storagegrid-ssoauth-azure.py`Python脚本
- `storagegrid-ssoauth-azure.js`Node.js脚本

这两个脚本都位于StorageGRID安装文件目录中(`./rpms`对于 RHEL， `./debs`适用于 Ubuntu 或 Debian，以及`./vsphere`对于 VMware)。

要编写您自己的与 Entra ID 的 API 集成，请参阅 `storagegrid-ssoauth-azure.py`脚本。 Python 脚本直接向StorageGRID发出两个请求（首先获取 SAMLRequest，然后获取授权令牌），同时调用 Node.js 脚本与 Entra ID 交互以执行 SSO 操作。

SSO 操作可以通过一系列 API 请求来执行，但这样做并不简单。 Puppeteer Node.js 模块用于抓取 Entra ID SSO 接口。

如果存在URL编码问题，则可能会看到以下错误： `Unsupported SAML version`。

步骤

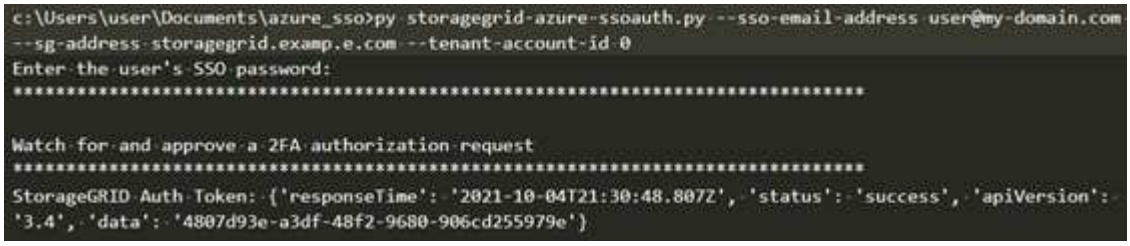
1. 安装所需的依赖关系，如下所示：
   a. 安装Node.js (请参见)。 "https://nodejs.org/en/download/"
   b. 安装所需的 Node.js 模块（ puppeteer 和 jsdom ）：

      ```
      npm install -g <module>
      ```

2. 将 Python 脚本传递给 Python 解释器以运行此脚本。

   然后，Python 脚本将调用相应的 Node.js 脚本来执行 Entra ID SSO 交互。

3. 出现提示时，输入以下参数的值（或使用参数传递这些值）：
   - 用于登录 Entra ID 的 SSO 电子邮件地址
   - StorageGRID 的地址
   - 要访问租户管理 API 的租户帐户 ID
4. 出现提示时，输入密码并准备在要求时向 Entra ID 提供 MFA 授权。



此脚本假定 MFA 是使用 Microsoft Authenticator 完成的。您可能需要修改脚本以支持其他形式的MFA (例如、输入在文本消息中收到的代码)。

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

如果已启用单一登录，请使用 **StorageGRID API (PingFederate)**

如果你有"已配置并启用单点登录（ SSO ）"并且您使用 PingFederate 作为 SSO 提供程序，则必须发出一系列 API 请求以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了单点登录，请登录到 **API**

如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- 这 `storagegrid-ssoauth.py`Python 脚本，位于StorageGRID安装文件目录中 (./rpms`对于 RHEL ， `./debs`适用于 Ubuntu 或 Debian，以及 `./vsphere`对于 VMware)。
- cURL 请求的示例工作流。

  如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误： `A valid SubjectConfirmation was not found on this Response`。

  示例 cURL 工作流不会保护密码不会被其他用户看到。

  如果存在URL编码问题，则可能会看到以下错误： `Unsupported SAML version`。

步骤

1. 选择以下方法之一以获取身份验证令牌：
   - 使用 `storagegrid-ssoauth.py`Python脚本。转至步骤 2 。
   - 使用 curl 请求。转至步骤 3 。
2. 如果要使用该 `storagegrid-ssoauth.py`脚本、请将该脚本传递给Python解释器并运行该脚本。

   出现提示时，输入以下参数的值：

   - SSO 方法。您可以输入"pingfederate"的任何变体(Pingfederate、pingfedate等)。
   - SSO 用户名
   - 安装 StorageGRID 的域。此字段不用于 PingFederate 。您可以将其留空或输入任何值。

- StorageGRID 的地址
- 要访问租户管理 API 的租户帐户 ID 。

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下操作步骤 。

   a. 声明登录所需的变量。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

   要访问网格管理API，请使用0作为 `TENANTACCOUNTID`。

   b. 要接收签名的身份验证URL，请向发出POST请求 `/api/v3/authorize-saml`，然后从响应中删除其他JSON编码。

   此示例显示了一个 POST 请求，用于为 TENANTACCOBTID 提供签名身份验证 URL 。结果将传递到 python -m json.tool 以删除 JSON 编码。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 保存响应中的、 `SAMLRequest`以供后续命令使用。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 导出响应和 cookie ，并对响应执行回显：

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 导出 "pf.adapterId" 值，并对响应执行回显：

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 导出 "href" 值（删除后斜杠 / ），并对响应执行回显：

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 导出 "act" 值：

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 发送 Cookie 以及凭据：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 从隐藏字段保存 `SAMLResponse`：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用保存的 `SAMLResponse`，发出StorageGRID`/api/saml-response`请求以生成StorageGRID身份验证令牌。

对于 `RelayState`，请使用租户帐户ID；如果要登录到网格管理API，请使用0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

响应包括身份验证令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 将响应中的身份验证令牌另存为 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

现在、您可以对其他请求使用、与未使用SSO时使用 `MYTOKEN`API的方式类似。

如果启用了单点登录，请注销 API

如果已启用单点登录（ Single Sign-On ， SSO ），则必须对一系列 API 请求进行问题描述 ，才能注销网格管理 API 或租户管理 API 。如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要、您可以从组织的单点注销页面注销、以注销StorageGRID API。或者，您也可以从 StorageGRID 触发单点注销（ SLO ），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求、请将`cookie "sso=true "传递到SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回注销 URL：

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 保存注销 URL 。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。如果未提供`cookie "sso=true "、则用户将从StorageGRID中注销、而不会影响SSO状态。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

`204 No Content`响应指示用户现在已注销。

```
HTTP/1.1 204 No Content
```

使用 **API** 停用 **StorageGRID** 功能

您可以使用网格管理 API 完全停用 StorageGRID 系统中的某些功能。停用某个功能后，不能为任何人分配执行与该功能相关的任务的权限。

关于此任务

停用的功能系统允许您阻止访问 StorageGRID 系统中的某些功能。停用某个功能是防止 root 用户或具有 * root 访问权限 * 的管理组中的用户能够使用该功能的唯一方法。

要了解此功能的有用程度，请考虑以下情形：

_Company A 是一家服务提供商，通过创建租户帐户租用其 StorageGRID 系统的存储容量。为了保护租户对象的安全， A 公司希望确保自己的员工在部署帐户后永远不能访问任何租户帐户。 _

Company A 可以通过使用网格管理 *API* 中的停用功能系统来实现此目标。通过完全停用网格管理器*(UI*和*API)*中的*更改租户*root*密码*功能，公司*A*可确保管理员用户*(*包括*root*用户和属于具有* *root*访问权限*的组的用户*)*不能更改任何租户帐户*root*用户的密码。

步骤

1. 访问网格管理 API 的 Swagger 文档。请参阅。 "使用网格管理 API"
2. 找到停用功能端点。
3. 要停用更改租户 root 密码等功能，请按如下所示向 API 发送正文：

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   请求完成后，更改租户根密码功能将被禁用。用户界面中不再显示*更改租户根密码*管理权限、任何尝试更改租户根密码的API请求都将失败、并显示"403禁止"。

重新激活已停用的功能

默认情况下，您可以使用网格管理 API 重新激活已停用的功能。但是，如果要防止重新激活已停用的功能，则可以停用 * 激活功能 * 功能本身。

无法重新激活*activateFeature*功能。如果您决定停用此功能，请注意，您将永远无法重新激活任何其他已停用的功能。要还原任何丢失的功能，您必须联系技术支持。

步骤

1. 访问网格管理 API 的 Swagger 文档。
2. 找到停用功能端点。
3. 要重新激活所有功能，请按如下所示将正文发送到 API：

```
{ "grid": null }
```

此请求完成后，包括更改租户 root 密码功能在内的所有功能都将重新激活。现在，" 更改租户根密码 " 管理权限将显示在用户界面中，如果用户具有 * 根访问权限 * 或 * 更改租户根密码 * 管理权限，则尝试更改租户根密码的任何 API 请求都将成功。

上一示例将重新激活 *all* 已停用的功能。如果其他功能已停用，而这些功能应保持停用状态，则必须在 PUT 请求中明确指定它们。例如、要重新激活更改租户root密码功能并继续停用存储管理员管理权限、请发送此放置请求：+

```
{ "grid": {"storageAdmin": true} }
```

控制对 StorageGRID 的访问

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。也可以启用单点登录 (SSO)、创建客户端证书、更改网格密码以及使用多管理员验证。

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 。

使用可以加快设置"组"速度、并"用户"允许用户使用"身份联合"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来确定每个用户可以执行的任务"权限"。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。他们无法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) 或 OpenID Connect (OIDC) 标准的单点登录 (SSO)。在您"配置并启用SSO"之后，所有用户都必须通过外部身份提供程序的身份验证，然后才能访问 Grid Manager、Tenant Manager、网格管理 API 或租户管理 API。本地用户无法登录 StorageGRID。

更改配置密码短语

许多安装和维护过程以及下载StorageGRID恢复包都需要配置密码。下载StorageGRID系统的网格拓扑信息和加密密钥的备份也需要密码。你可以"更改密码短语"按要求。

更改节点控制台密码

网格中的每个节点都有一个节点控制台密码，您需要使用 SSH 以“管理员”身份登录到节点，或者以 VM/物理控制台连接上的 root 用户身份登录。根据需要，您可以"更改节点控制台密码"对于每个节点。

使用多管理员验证

您可以使用多管理员验证 (MAV) 来确保只有在指定管理员批准后才能执行某些 StorageGRID 操作。MAV 可防止受损、恶意或缺乏经验的管理员进行不必要的更改或删除数据。

更改 **StorageGRID** 配置密码

使用此过程更改StorageGRID配置密码。恢复、扩展和维护过程都需要密码。下载恢复包备份也需要密码，其中包括网格拓扑信息、网格节点控制台密码和StorageGRID系统的加密密钥。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您具有维护或 root 访问权限。
- 您具有当前配置密码短语。

关于此任务

许多安装和维护过程都需要配置密码，并且"下载恢复包"。配置密码未在 `Passwords.txt`文件。确保记录配置密码并将其保存在安全的地方。

步骤

1. 选择*配置* > 访问控制 > 电网密码。
2. 在*更改配置密码短语*下，选择*进行更改*
3. 输入当前配置密码短语。
4. 输入新密码短语。密码短语必须至少包含 8 个字符，并且不能超过 32 个字符。密码短语区分大小写。

   将配置密码存储在安全的位置。它是安装、扩展和维护过程所必需的。

5. 重新输入新密码短语，然后选择 * 保存 * 。

   配置密码短语更改完成后，系统将显示一个绿色的成功横幅。

6. 选择 * 恢复包 * 。
7. 输入新的配置密码来下载新的恢复包。

更改配置密码后，您必须立即下载新的恢复包。如果发生故障，恢复包文件可让您恢复系统。

在 **StorageGRID** 中更改节点控制台密码

网格中的每个节点都有一个节点控制台密码，您可以使用该密码登录该节点。默认情况下，每个节点都有一个唯一的密码。您可以将每个密码更改为新的唯一密码，也可以将每个节点的密码更改为使用全局密码。密码存储在恢复包中。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有当前配置密码短语。

关于此任务

您可以使用节点控制台密码通过 SSH 以“管理员”身份登录到节点，或者通过 VM/物理控制台连接以 root 用户身份登录。您可以使用以下选项之一更改节点控制台密码：

- 自动对每个节点应用随机密码
- 指定一个全局密码并将其应用于所有节点
- 指定并将唯一密码应用于一个或多个节点

密码存储在更新的 `Passwords.txt`恢复包中的文件。密码列在文件的密码列中。

这"SSH 访问密码"用于节点间通信的 SSH 密钥与节点控制台密码是分开的。此过程不会更改 SSH 访问密码。

访问向导

步骤

1. 选择*配置* > 访问控制 > 电网密码。
2. 在*更改节点控制台密码*下、选择*进行更改*。

下载当前恢复软件包

在更改节点控制台密码之前，请下载当前的恢复包。如果任何节点的密码更改过程失败，您可以使用此文件中的密码。

步骤

1. 输入网格的配置密码短语。
2. 选择 * 下载恢复包 * 。
3. 复制恢复包文件(`.zip`）到两个安全、可靠且独立的位置。

恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

4. 选择 * 继续 * 。

提供新密码

1. 选择您想要使用的密码更改方法。
   - 自动： StorageGRID自动为所有节点分配一个新的随机控制台密码。
   - 自定义：您提供控制台密码。

自动

1. 选择 * 继续 * 。

自定义

1. 选择以下选项之一：
   - 全局控制台密码：对所有节点应用相同的控制台密码。
   - 唯一的控制台密码：在一个或多个节点上应用不同的密码。
2. 如果您选择了*全局控制台密码*，请输入您想要用于所有节点的密码。
3. 如果选择了“唯一控制台密码”，请为一个或多个节点输入唯一密码。
4. 选择 * 继续 * 。

完成密码修改

1. 当确认对话框出现时，如果您准备好让StorageGRID开始更改节点控制台密码，请选择 是。

   此过程启动后、您无法取消。

   StorageGRID生成一个包含新密码的新恢复包。

2. 当新的恢复包准备好后，选择*下载新的恢复包*并保存恢复包。
3. 打开 `.zip`文件。
4. 确认您可以访问包含新节点控制台密码的内容、包括 `Passwords.txt`文件。
5. 复制新的恢复包文件(`.zip`）到两个安全、可靠且独立的地点。

   不要覆盖旧的恢复包。

   您必须保护恢复文件，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

6. 选中复选框表示您已下载新的恢复包并验证了内容。
7. 选择 * 继续 * 。

   StorageGRID更新每个节点的密码。

   如果更新过程中出现错误，进度条会列出密码更改失败的节点数。系统将自动在密码更改失败的任何节点上重试该过程。如果该过程结束时某些节点仍未更改密码，则会出现“重试”按钮。

8. 如果一个或多个节点的密码更新失败：
   a. 查看表中列出的错误消息。
   b. 解决问题。
   c. 选择 * 重试 * 。

   重试仅会更改先前尝试更改密码期间失败的节点上的节点控制台密码。

9. 当进度条显示没有剩余更新时，选择*完成*。
10. 更改所有节点的节点控制台密码后，删除您下载的第一个恢复包。

更改 **StorageGRID** 管理节点的 **SSH** 访问密码

更改管理节点的SSH访问密码还会更新网格中每个节点的唯一内部SSH密钥集。主管理节点使用这些SSH密钥通过安全、无密码身份验证访问节点。

使用SSH密钥以root用户身份登录到节点、或者通过VM或物理控制台连接登录到 `admin`root用户。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有当前配置密码短语。

关于此任务

管理节点的新访问密码和每个节点的新内部密钥存储在 `Passwords.txt`恢复包中的文件。密钥列在该文件中的密码列中。

用于节点间通信的 SSH 密钥具有单独的 SSH 访问密码。此过程不会对其进行更改。

访问向导

步骤

1. 选择*配置* > 访问控制 > 电网密码。
2. 在*更改SSH密钥*下，选择*进行更改*。

下载当前恢复软件包

在更改 SSH 访问密钥之前，请下载当前的恢复包。如果任何节点的密钥更改过程失败，您可以使用此文件中的密钥。

步骤

1. 输入网格的配置密码短语。
2. 选择 * 下载恢复包 * 。
3. 复制恢复包文件(`.zip`）到两个安全、可靠且独立的位置。

恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

4. 选择 * 继续 * 。
5. 出现确认对话框时，如果您准备好开始更改SSH访问密钥，请选择*Yes*。

此过程启动后、您无法取消。

更改**SSH**访问密钥

当更改 SSH 访问密钥过程开始时，将生成一个包含新密钥的新恢复包。然后，在每个节点上更新密钥。

步骤

1. 等待新的恢复包生成，这可能需要几分钟。
2. 当“下载新的恢复包”按钮启用时，选择“下载新的恢复包”并保存新的恢复包文件(`.zip`）到两个安全、可靠且独立的地点。
3. 下载完成后：

   a. 打开 `.zip`文件。

   b. 确认您可以访问包含新SSH访问密钥的内容、包括 `Passwords.txt`文件。

   c. 复制新的恢复包文件(`.zip`）到两个安全、可靠且独立的地点。

   不要覆盖旧的恢复包。

   恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

4. 等待每个节点上的密钥更新、这可能需要几分钟时间。

   如果更改了所有节点的密钥、则会显示绿色成功横幅。

   如果在更新过程中出现错误、则会显示一条横幅消息、列出无法更改密钥的节点数量。系统将在任何未能更改密钥的节点上自动重试此过程。如果此过程结束时某些节点的密钥仍未更改，则会显示*Retry*按钮。

   如果一个或多个节点的密钥更新失败：

   a. 查看表中列出的错误消息。

   b. 解决问题。

   c. 选择 * 重试 * 。

      重试仅会更改先前尝试更改密钥期间失败的节点上的SSH访问密钥。

5. 在所有节点的 SSH 访问密钥更改后，删除您下载的第一个恢复包。
6. 或者，选择“维护”>“系统”>“恢复包”来下载新恢复包的附加副本。

使用身份联合可以加快设置组和用户的速度，并允许用户使用熟悉的凭据登录到 StorageGRID 。

为 **Grid Manager** 配置身份联合

如果您希望在另一个系统（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server ）中管理管理组和用户，则可以在网格管理器中配置身份联合。

开始之前

- 您已使用"支持的 Web 浏览器"。
- 你已经"特定访问权限"。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作为身份提供者。

  如果您想使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参阅。 配置 OpenLDAP 服务器的准则
- 如果您计划启用单点登录 (SSO)，您已查看"单点登录的要求和注意事项"。
- 如果您计划使用传输层安全（ Transport Layer Security ， TLS ）与 LDAP 服务器进行通信，则身份提供程序正在使用 TLS 1.2 或 1.3 。请参阅。 "支持传出 TLS 连接的密码"

关于此任务

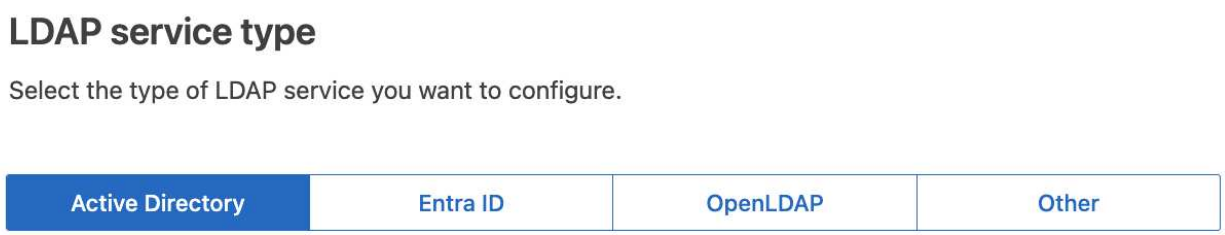
如果您想从其他系统（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）导入组，则可以为网格管理器配置身份源。您可以导入以下类型的组：

- 管理组。管理组中的用户可以登录到网格管理器并根据分配给该组的管理权限执行任务。
- 不使用自己的身份源的租户的租户用户组。租户组中的用户可以登录到租户管理器，并根据在租户管理器中为该组分配的权限执行任务。有关详细信息、请参见"创建租户帐户"和"使用租户帐户"。

输入配置

步骤

1. 选择*配置* > 访问控制 > 身份联合。
2. 选择 * 启用身份联合 * 。
3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - 用户唯一名称：包含 LDAP 用户唯一标识符的属性名称。此属性相当于 `sAMAccountName`对于 Active Directory 和 `uid`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `uid。
   - 用户 **UUID**：包含 LDAP 用户的永久唯一标识符的属性名称。此属性相当于 `objectGUID`对于 Active Directory 和 `entryUUID`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `nsuniqueid。每个用户的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数，其中连字符将被忽略。
   - 组唯一名称：包含 LDAP 组唯一标识符的属性的名称。此属性相当于 `sAMAccountName`对于 Active Directory 和 `cn`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `cn。
   - 组 **UUID**：包含 LDAP 组的永久唯一标识符的属性的名称。此属性相当于 `objectGUID`对于 Active Directory 和 `entryUUID`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `nsuniqueid。每个组的指定属性的值必须是 16 字节或字符串格式的 32 位十六进制数，其中连字符将被忽略。
5. 对于所有 LDAP 服务类型，请在配置 LDAP 服务器部分中输入所需的 LDAP 服务器和网络连接信息。
   - * 主机名 * ： LDAP 服务器的完全限定域名（ FQDN ）或 IP 地址。
   - * 端口 * ：用于连接到 LDAP 服务器的端口。

     STARTTLS 的默认端口为 389 ， LDAPS 的默认端口为 636 。但是，只要防火墙配置正确，您就可以使用任何端口。

   - * 用户名 * ：要连接到 LDAP 服务器的用户的可分辨名称（ DN ）的完整路径。

     对于 Active Directory ，您还可以指定低级别的登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

     - `sAMAccountName`或 `uid`
     - `objectGUID` `entryUUID`或 `nsuniqueid`
     - `cn`
     - `memberOf`或 `isMemberOf`
     - **Active Directory**： `objectSid`、 `primaryGroupID`、 `userAccountControl`和 `userPrincipalName`
     - 入口**ID**: `accountEnabled`和 `userPrincipalName`
   - * 密码 * ：与用户名关联的密码。

     如果您以后更改密码、则必须在此页面上更新密码。

   - * 组基本 DN* ：要搜索组的 LDAP 子树的可分辨名称（ DN ）的完整路径。在 Active Directory 示例（如下）中，可分辨名称相对于基础 DN （ DC=storagegrid ， DC=example ， DC=com ）的所有组均可用作联合组。

* 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

- * 用户基础 DN* ：要搜索用户的 LDAP 子树的可分辨名称（ DN ）的完整路径。

  用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

- 绑定用户名格式(可选)：如果无法自动确定模式，StorageGRID 应使用默认用户名模式。

  建议提供 * 绑定用户名格式 * ，因为如果 StorageGRID 无法绑定到服务帐户，它可以允许用户登录。

  输入以下模式之一：

  - **UserPrincipalName** 模式（**AD** 和 **Entra ID**）： `[USERNAME]@example.com`
  - 下级登录名称模式（**AD** 和 **Entra ID**）： `example\[USERNAME]`
  - 可分辨名称模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   - 使用 **STARTTLS**：使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是 Active Directory 、OpenLDAP 或其他的推荐选项，但 Microsoft Entra ID 不支持此选项。
   - 使用 **LDAPS**：LDAPS（通过 SSL 的 LDAP）选项使用 TLS 建立与 LDAP 服务器的连接。您必须为 Microsoft Entra ID 选择此选项。
   - 不要使用 **TLS**： StorageGRID系统和 LDAP 服务器之间的网络流量将不安全。 Microsoft Entra ID 不支持此选项。

     如果您的 Active Directory 服务器强制执行 LDAP 签名，则不支持使用 不使用 **TLS** 选项。您必须使用 STARTTLS 或 LDAPS。

7. 如果选择 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。
   - * 使用操作系统 CA 证书 * ：使用操作系统上安装的默认网格 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ：使用自定义安全证书。

     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

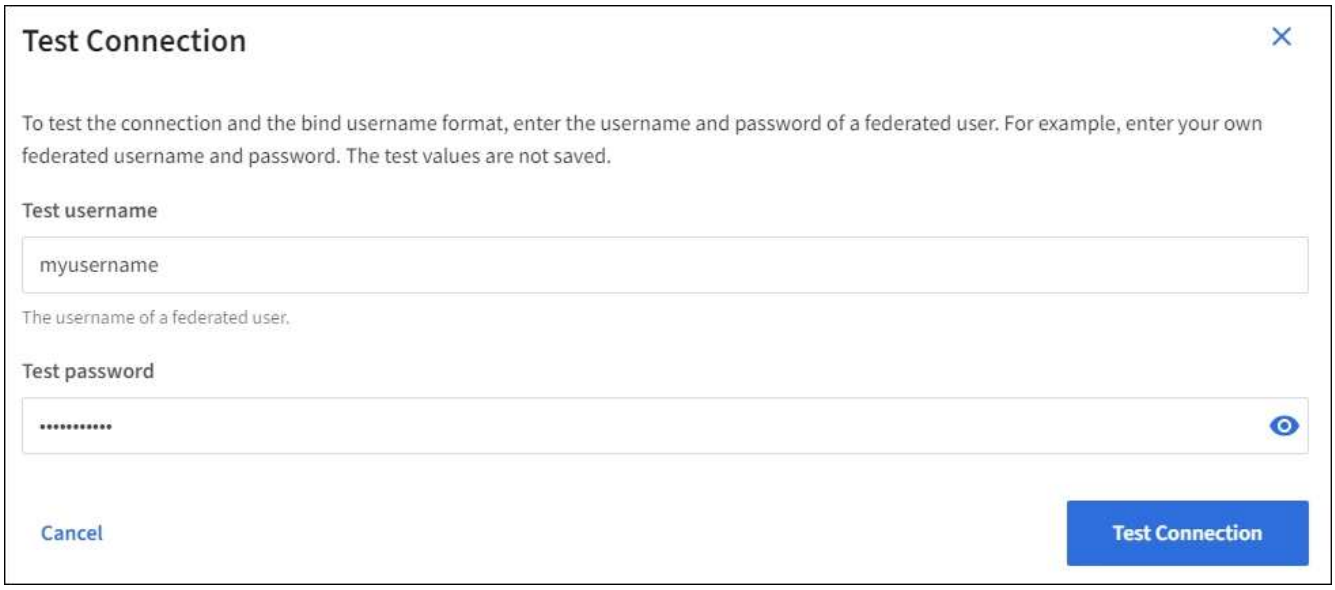
步骤

1. 选择 * 测试连接 * 。
2. 如果您没有提供绑定用户名格式：
   - 如果连接设置有效、则会显示"Test connection sule"(测试连接成功)消息。选择 * 保存 * 以保存配置。

- 如果连接设置无效、则会显示"无法建立测试连接"消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。

3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

   例如，输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符、例如@或/。



   - 如果连接设置有效、则会显示"Test connection sule"(测试连接成功)消息。选择 * 保存 * 以保存配置。
   - 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到身份联合页面。
2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以暂时或永久禁用群组和用户的身份联合。当身份联合被禁用时， StorageGRID和身份源之间就没有通信。但是，您配置的任何设置都会保留，以便您将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID系统和身份源之间不会发生同步，并且不会对尚未同步的帐户发出警报。
- 如果单点登录 (SSO) 状态为 已启用 或 沙盒模式，则 启用身份联合 复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 已禁用。看"禁用单点登录" 。

步骤

1. 转到身份联合页面。
2. 取消选中*启用身份联合*复选框。

配置 OpenLDAP 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于非 Active Directory 或 Microsoft Entra ID 的身份源， StorageGRID不会自动阻止外部禁用的用户访问 S3。要阻止 S3 访问，请删除用户的所有 S3 密钥或从所有组中删除该用户。

memberOf 和 fint 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

相关信息

"用于外部通信的端口"

管理 StorageGRID 中的管理员组

您可以创建管理组来管理一个或多个管理员用户的安全权限。用户必须属于要授予对 StorageGRID 系统访问权限的组。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

创建管理组

通过管理组，您可以确定哪些用户可以访问网格管理器和网格管理 API 中的哪些功能和操作。

访问向导

步骤

1. 选择*配置* > 访问控制 > 管理组。
2. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

- 如果要为本地用户分配权限，请创建本地组。
- 创建联合组以从身份源导入用户。

本地组

步骤

1. 选择 * 本地组 * 。
2. 输入组的显示名称，您可以稍后根据需要更新该名称。例如、"维护用户"或"ILM管理员"。
3. 输入组的唯一名称、此名称以后无法更新。
4. 选择 * 继续 * 。

联合组

步骤

1. 选择 * 联合组 * 。
2. 输入要导入的组的名称，与此名称在配置的身份源中显示的名称完全相同。
   - 对于 Active Directory 和 Microsoft Entra ID，使用 sAMAccountName。
   - 对于 OpenLDAP ，请使用 CN （公用名）。
   - 对于另一个 LDAP ，请为 LDAP 服务器使用适当的唯一名称。
3. 选择 * 继续 * 。

管理组权限

步骤

1. 对于 * 访问模式 * ，选择组中的用户是否可以在网格管理器和网格管理 API 中更改设置并执行操作，或者选择他们是否只能查看设置和功能。

- * 读写 *（默认）：用户可以更改其管理权限允许的设置并执行这些操作。
- * 只读 *：用户只能查看设置和功能。他们无法在网格管理器或网格管理API中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

> 如果用户属于多个组，并且任何组设置为 * 只读 * ，则用户将对所有选定设置和功能具有只读访问权限。

2. 选择一个或多个"管理员组权限"。

   您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到 StorageGRID 。

3. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

步骤

1. 或者，为此组选择一个或多个本地用户。

   如果尚未创建本地用户，则可以保存此组，而无需添加用户。您可以在用户页面上将此组添加到用户。有关详细信息、请参见。 "管理用户"

2. 选择 * 创建组 * 和 * 完成 * 。

查看和编辑管理组

您可以查看现有组的详细信息，修改组或复制组。

- 要查看所有组的基本信息，请查看组页面上的表。
- 要查看特定组的所有详细信息或编辑组，请使用 * 操作 * 菜单或详细信息页面。

任务	操作菜单	详细信息页面
查看组详细信息	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。	在表中选择组名称。
编辑显示名称（仅限本地组）	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 编辑组名称 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存更改 * 。
编辑访问模式或权限	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。 c. 也可以更改组的访问模式。 d. (可选)选择或清除"管理员组权限"。 e. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 也可以更改组的访问模式。 c. (可选)选择或清除"管理员组权限"。 d. 选择 * 保存更改 * 。

复制组

步骤

1. 选中组对应的复选框。
2. 选择 * 操作 * > * 复制组 * 。
3. 完成复制组向导。

删除组

如果要从系统中删除某个管理组，则可以删除该组，并删除与该组关联的所有权限。删除管理员组会从组中删除任何用户，但不会删除这些用户。

步骤

1. 在组页面中、选中要删除的每个组对应的复选框。
2. 选择 * 操作 * > * 删除组 * 。
3. 选择 * 删除组 * 。

StorageGRID 中的管理组权限

创建管理员用户组时，您可以选择一个或多个权限来控制对网格管理器特定功能的访问。然后，您可以将每个用户分配给一个或多个管理组，以确定用户可以执行的任务。

您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到网格管理器或网格管理 API 。

默认情况下，属于至少具有一个权限的组的任何用户均可执行以下任务：

- 登录到网格管理器
- 查看信息板
- 查看节点页面
- 查看当前警报和已解决警报
- 更改自己的密码（仅限本地用户）
- 查看配置和维护页面上提供的某些信息

权限与访问模式之间的交互

对于所有权限，组的 * 访问模式 * 设置将确定用户是否可以更改设置并执行操作，或者是否只能查看相关设置和功能。如果用户属于多个组，并且任何组设置为 * 只读 * ，则用户将对所有选定设置和功能具有只读访问权限。

以下各节介绍了在创建或编辑管理组时可以分配的权限。未明确提及的任何功能都需要具有 * 根访问权限 * 。

root 访问权限

通过此权限，可以访问所有网格管理功能。

更改租户 **root** 密码

通过此权限，您可以访问租户页面上的 * 更改 root 密码 * 选项，从而可以控制谁可以更改租户的本地 root 用户

的密码。启用 S3 密钥导入功能后，此权限也用于迁移 S3 密钥。没有此权限的用户看不到*更改root密码*选项。

要授予对包含 * 更改 root 密码 * 选项的租户页面的访问权限，还需要分配 * 租户帐户 * 权限。

ILM

通过此权限，您可以访问以下 * ILM * 菜单选项：

- 规则
- 策略
- 策略标记
- 存储池
- 存储等级
- regions
- 对象元数据查找

用户必须具有*其他网格配置*权限才能管理存储等级。

维护

用户必须具有维护权限才能使用以下选项：

- 配置 > 访问控制
  - 网格密码
- 配置 > 网络
  - S3端点域名
- 维护 > 任务
  - 停用
  - 扩展
  - 对象存在检查
  - 恢复
- 维护 > 系统
  - 恢复包
  - 软件更新
- 支持 > 工具
  - 日志

没有维护权限的用户可以查看但不能编辑以下页面：

- 维护 > 网络
  - DNS 服务器

- 网格网络
- NTP 服务器

- 维护 > 系统
  - 许可证
- 配置 > 网络
  - S3端点域名
- 配置 > 安全
  - 证书
- 配置 > 监控
  - 审核和系统日志服务器

管理警报

通过此权限，您可以访问用于管理警报的选项。用户必须具有此权限才能管理静音，警报通知和警报规则。

指标查询

此权限提供对以下内容的访问权限：

- 支持 > 工具 > *指标*页面
- 使用网格管理API的*Metrics*部分自定义Prometheus指标查询
- 包含指标的Grid Manager信息板卡

对象元数据查找

通过此权限，您可以访问 * ILM * > * 对象元数据查找 * 页面。

其他网格配置

此权限提供对这些附加网格配置选项的访问：

- **ILM**
  - 存储等级
- 配置 > 系统
- 支持 > 其他
  - I/O 优先级
  - 节点服务
  - 存储水印

链接成本需要 Root 访问。

存储设备管理员

此权限提供：

- 通过网格管理器访问存储设备上的E系列SANtricity System Manager。
- 能够在管理驱动器选项卡上对支持这些操作的设备执行故障排除和维护任务。

租户帐户

此权限可用于：

- 访问租户页面、在此可以创建、编辑和删除租户帐户
- 查看现有流量分类策略
- 查看包含租户详细信息的Grid Manager信息板卡

在 **StorageGRID** 中管理用户

您可以查看本地用户和联合用户。您还可以创建本地用户并将其分配给本地管理组，以确定这些用户可以访问哪些网格管理器功能。

开始之前

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

创建本地用户

您可以创建一个或多个本地用户，并将每个用户分配给一个或多个本地组。组的权限控制用户可以访问的网格管理器和网格管理 API 功能。

您只能创建本地用户。使用外部身份源管理联合用户和组。

网格管理器包括一个名为"root"的预定义本地用户。您无法删除root用户。

如果启用了单点登录(SSO)、则本地用户无法登录到StorageGRID。

访问向导

步骤

1. 选择*配置* > 访问控制 > 管理员用户。
2. 选择 * 创建用户 * 。

输入用户凭据

步骤

1. 输入用户的全名，唯一用户名和密码。
2. 或者，如果此用户不应访问网格管理器或网格管理 API ，请选择 * 是 * 。
3. 选择 * 继续 * 。

分配给组

步骤

1. （可选）将用户分配给一个或多个组以确定用户的权限。

   如果尚未创建组，则可以保存用户而不选择组。您可以在组页面上将此用户添加到组中。

   如果用户属于多个组，则权限是累积的。有关详细信息、请参见。 "管理管理组"

2. 选择 * 创建用户 * 并选择 * 完成 * 。

查看和编辑本地用户

您可以查看现有本地用户和联合用户的详细信息。您可以修改本地用户以更改用户的全名，密码或组成员资格。您还可以暂时阻止用户访问网格管理器和网格管理 API 。

您只能编辑本地用户。使用外部身份源管理联合用户。

- 要查看所有本地和联合用户的基本信息，请查看用户页面上的表。
- 要查看特定用户的所有详细信息，编辑本地用户或更改本地用户的密码，请使用 * 操作 * 菜单或详细信息页面。

  用户下次注销后重新登录到网格管理器时，系统将应用任何编辑。

  本地用户可以使用网格管理器横幅中的*更改密码*选项更改自己的密码。

任务	操作菜单	详细信息页面
查看用户详细信息	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。	在表中选择用户名。
编辑全名（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 编辑全名 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存更改 * 。
拒绝或允许 StorageGRID 访问	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择访问选项卡。 d. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 e. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择访问选项卡。 c. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 d. 选择 * 保存更改 * 。

任务	操作菜单	详细信息页面
更改密码（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择密码选项卡。 d. 输入新密码。 e. 选择 * 更改密码 * 。	a. 选择用户的名称以显示详细信息。 b. 选择密码选项卡。 c. 输入新密码。 d. 选择 * 更改密码 * 。
更改组（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择组选项卡。 d. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 e. 选择 * 编辑组 * 以选择不同的组。 f. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择组选项卡。 c. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 d. 选择 * 编辑组 * 以选择不同的组。 e. 选择 * 保存更改 * 。

导入联合用户

您可以将一个或多个联合用户（最多 100 个用户）直接导入“用户”页面。

步骤

1. 选择*配置* > 访问控制 > 管理员用户。
2. 选择*导入联合用户*。
3. 输入一个或多个联合用户的 UUID 或用户名。

   对于多个条目，请在新行上添加每个 UUID 或用户名。
4. 选择*导入*。

   如果将一个或多个用户导入“用户”字段失败，请执行以下步骤：

   a. 展开*未导入的用户*并选择*复制用户*。
   b. 通过选择“上一个”并将复制的用户粘贴到“导入联合用户”对话框中，重新尝试导入。

   关闭“导入联合用户”对话框后，成功导入的用户的联合用户信息将显示在“用户”页面上。

复制用户

您可以复制现有用户以创建具有相同权限的新用户。

步骤

1. 选中用户对应的复选框。
2. 选择 * 操作 * > * 复制用户 * 。
3. 完成复制用户向导。

删除用户

您可以删除本地用户，以便从系统中永久删除该用户。

> 您不能删除root用户。

步骤

1. 在用户页面中、选中要删除的每个用户对应的复选框。
2. 选择 * 操作 * > * 删除用户 * 。
3. 选择 * 删除用户 * 。

使用单点登录（ **SSO** ）

了解 **StorageGRID SSO**

启用单点登录 (SSO) 后，只有使用贵组织实施的 SSO 登录流程授权用户的凭据后，用户才可以访问网格管理器、租户管理器、网格管理 API 或租户管理 API。本地用户无法登录StorageGRID。

StorageGRID 系统支持使用安全断言标记语言 2.0 (SAML 2.0) 标准或 OpenID Connect 的单点登录 (SSO)。

在启用单点登录（ SSO ）之前，请查看启用 SSO 后 StorageGRID 登录和注销过程会受到什么影响。

启用 **SSO** 后登录

启用 SSO 并登录到 StorageGRID 后，系统会将您重定向到组织的 SSO 页面以验证您的凭据。

步骤

1. 在 Web 浏览器中输入任何 StorageGRID 管理节点的完全限定域名或 IP 地址。

   此时将显示 StorageGRID 登录页面。

   - 如果这是您第一次通过此浏览器访问该 URL，系统会提示您输入帐户 ID。
   - 如果您之前访问过网格管理器或租户管理器，系统将提示您选择最近的帐户或输入帐户 ID。

   > 如果输入租户帐户的完整StorageGRID (即完全限定域名或IP地址，后跟)，则不会显示“URL登录”页面 `/?accountId=20-digit-account-id`。而是会立即重定向到您所在组织的SSO登录页面，您可以在该页面中使用您的 SSO 凭据登录进行登录。

2. 指示您是要访问网格管理器还是租户管理器：
   - 要访问网格管理器，请将 * 帐户 ID* 字段留空，输入 * 0 * 作为帐户 ID ，或者选择 * 网格管理器 * （如果它显示在近期帐户列表中）。

◦ 要访问租户管理器，请输入 20 位租户帐户 ID ，或者如果某个租户显示在近期帐户列表中，则按名称选择此租户。

3. 选择 * 登录 *

   StorageGRID 会将您重定向到贵组织的 SSO 登录页面。例如：

4. 【签名 _sso]] 使用您的 SSO 凭据登录。

   如果您的 SSO 凭据正确：

   a. 身份提供程序（ IdP ）为 StorageGRID 提供身份验证响应。
   b. StorageGRID 将验证身份验证响应。
   c. 如果响应有效，并且您属于具有 StorageGRID 访问权限的联合组，则您将登录到网格管理器或租户管理器，具体取决于您选择的帐户。

   > 如果此服务帐户不可访问，则只要您是具有 StorageGRID 访问权限的联合组的现有用户，您仍可登录。

5. 或者，如果您拥有足够的权限，也可以访问其他管理节点，或者访问网格管理器或租户管理器。

   您无需重新输入SSO凭据。

启用 **SSO** 后注销

为 StorageGRID 启用 SSO 后，注销时会发生什么情况取决于您登录到的内容以及注销的位置。

步骤

1. 在用户界面右上角找到*Sign Out (注销)*链接。
2. 选择*注销*。

   此时将显示 StorageGRID 登录页面。更新了 * 近期帐户 * 下拉列表，其中包含 * 网格管理器 * 或租户名称，以便您将来可以更快地访问这些用户界面。

   > 下表总结了在使用单个浏览器会话时注销时会发生的情况。如果您通过多个浏览器会话登录到 StorageGRID ，则必须单独注销所有浏览器会话。

如果您已登录到 ...	您可以从以下位置注销 ...	您已注销 ...
一个或多个管理节点上的网格管理器	任何管理节点上的网格管理器	所有管理节点上的网格管理器 *注意：*如果您使用 Entra ID 进行 SSO，则可能需要几分钟才能退出所有管理节点。
一个或多个管理节点上的租户管理器	任何管理节点上的租户管理器	所有管理节点上的租户管理器

如果您已登录到 ...	您可以从以下位置注销 ...	您已注销 ...
网格管理器和租户管理器	网格管理器	仅限网格管理器。您还必须注销租户管理器才能注销 SSO 。

StorageGRID SSO 的要求和注意事项

在为StorageGRID 系统启用单点登录(Single Sign On、SSO)之前、请查看相关要求和注意事项。

身份提供程序要求

StorageGRID 支持多个 SSO 身份提供程序 (IdP)。

OIDC

以下 SSO IdPs 支持 OpenID Connect (OIDC)：

- Active Directory 联合身份验证服务（ AD FS ）
- 微软Entra ID
- Keycloak
- PingFederate
- Okta

SAML

以下 SSO IdPs 支持安全断言标记语言 2.0 (SAML 2.0)：

- Active Directory 联合身份验证服务（ AD FS ）
- 微软Entra ID
- PingFederate

您必须先为 StorageGRID 系统配置身份联合，然后才能配置 SSO 身份提供程序。用于身份联合的 LDAP 服务类型控制您可以实施的 SSO 类型。

已配置 **LDAP** 服务类型	**SSO** 身份提供程序的选项
Active Directory	• Active Directory • Keycloak • Okta • 进入 ID • PingFederate
进入 ID	进入 ID

AD FS 要求

您可以使用以下任意版本的 AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

Windows Server 2016应使用 "KB3201845 更新"、或更高版本。

其他要求

- 传输层安全（ Transport Layer Security ， TLS ） 1.2 或 1.3
- Microsoft .NET Framework 3.5.1 或更高版本

Entra ID 的注意事项

如果您使用 Entra ID 作为 SSO 类型，并且用户的用户主体名称不使用 sAMAccountName 作为前缀，则当StorageGRID与 LDAP 服务器失去连接时，可能会出现登录问题。要允许用户登录，您必须恢复与 LDAP 服务器的连接。

服务器证书要求

默认情况下， StorageGRID在每个管理节点上使用管理接口证书来保护对网格管理器、租户管理器、网格管理 API 和租户管理 API 的访问。为StorageGRID配置信赖方信任 (AD FS)、企业应用程序 (Entra ID) 或服务提供商连接 (PingFederate) 时，您可以使用服务器证书作为StorageGRID请求的签名证书。

如果您尚未"已为管理接口配置自定义证书"执行此操作，则应立即执行此操作。安装自定义服务器证书时，该证书将用于所有管理节点，您可以在所有 StorageGRID 依赖方信任关系，企业应用程序或 SP 连接中使用该证书。

建议不要在依赖方信任，企业应用程序或 SP 连接中使用管理节点的默认服务器证书。如果节点发生故障而您恢复了该节点，则会生成一个新的默认服务器证书。在登录到已恢复的节点之前，您必须使用新证书更新依赖方信任，企业应用程序或 SP 连接。

您可以通过登录到管理节点的命令Shell并转到目录来访问此节点的服务器证书 `/var/local/mgmt-api`。自定义服务器证书名为 `custom-server.crt`。此节点的默认服务器证书名为 `server.crt`。

端口要求

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。请参阅。 "在外部防火墙处控制访问"

确认联合用户可以登录到 **StorageGRID**

在启用单点登录（ SSO ）之前，您必须确认至少有一个联合用户可以登录到网格管理器以及任何现有租户帐户的租户管理器。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 您已配置身份联合。

步骤

1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

   启用 SSO 后，在租户管理器中配置的身份源将被网格管理器中配置的身份源覆盖。属于租户身份源的用户将无法再登录，除非他们拥有网格管理器身份源帐户。

   a. 登录到每个租户帐户的租户管理器。
   b. 选择*访问管理* > 身份联合。
   c. 确认未选中*启用身份联合*复选框。
   d. 如果是、请确认不再需要此租户帐户可能正在使用的任何联盟组、清除此复选框、然后选择*保存*。

2. 确认联合用户可以访问网格管理器：
   a. 从网格管理器中，选择*配置* > 访问控制 > 管理组。
   b. 确保已从 Active Directory 身份源导入至少一个联合组，并已为其分配 root 访问权限。
   c. 注销。
   d. 确认您可以以联合组中的用户身份重新登录到网格管理器。

3. 如果存在现有租户帐户，请确认具有 root 访问权限的联合用户可以登录：
   a. 从网格管理器中，选择*租户*。
   b. 选择租户帐户，然后选择 * 操作 * > * 编辑 * 。
   c. 在输入详细信息选项卡上，选择 * 继续 * 。
   d. 如果选中了*使用自己的身份源*复选框，请取消选中该复选框并选择*保存*。

      此时将显示租户页面。

   e. 选择租户帐户，选择 * 登录 * ，然后以本地 root 用户身份登录到租户帐户。
   f. 从租户管理器中，选择*访问管理*>*组*。
   g. 确保至少已为此租户为网格管理器中的一个联合组分配 root 访问权限。
   h. 注销。
   i. 确认您可以以联盟组中的用户身份重新登录到租户。

相关信息

- "单点登录的要求和注意事项"
- "管理管理组"
- "使用租户帐户"

了解如何使用 OIDC 在 StorageGRID 中设置 SSO

在 StorageGRID 中设置单点登录 (SSO) 后，StorageGRID（服务提供商）和 SSO 身份提供商可以安全地就用户身份验证请求进行通信。

您可以使用 OpenID Connect (OIDC) 或 SAML 在 StorageGRID 中设置 SSO。按照以下高级步骤使用 OIDC 在 StorageGRID 中设置 SSO，或了解 "使用 SAML 设置 SSO"。

1 配置身份提供程序

根据计划使用的 SSO 标识提供程序，您可以为标识联合 LDAP 服务类型选择 Active Directory 或 Entra ID。

- 对于 Active Directory Federation Service (AD FS)，您可以使用 AD FS、Entra ID、Keycloak、Okta 或 PingFederate 身份提供程序。
- 对于 Entra ID，您只能使用 Entra ID 身份提供程序。

使用 SSO 身份提供商的软件为网格中的每个管理节点配置 OIDC。

- 了解 Active Directory 中的 "为每个管理节点创建应用程序组"
- 了解 Entra ID 中的 "为每个管理节点创建应用程序"
- 了解 Keycloak 中的 "为每个管理节点创建客户端"
- 了解 "为每个管理节点创建一个 Okta 应用程序"
- 了解 "为每个管理节点创建服务提供商连接" 在 PingFederate 中的信息

2 配置 SSO

选择 OIDC 的配置 SSO 向导。然后，使用身份提供程序配置 SSO，并进入沙盒模式以配置和测试 SSO，然后再为 StorageGRID 用户启用 SSO。

了解 "使用 OIDC 配置 SSO"

3 启用 SSO

确认可以使用 SSO 登录到每个管理节点后，为所有 StorageGRID 用户启用 SSO。

了解 "为 StorageGRID 用户启用 SSO"

在 AD FS 中为 StorageGRID 中的 OIDC 创建应用程序组

必须使用 Active Directory Federation Services (AD FS) 为系统中每个管理节点的 OpenID Connect (OIDC) 创建应用程序组。

开始之前

- 您拥有系统中每个管理节点的完全限定域名（或 IP 地址）和依赖方标识符。

您的 StorageGRID 系统中的每个管理节点都必须有一个应用程序组。这可确保用户可以安全地登录和退出任何管理节点。您可以为所有管理节点创建单个应用程序组（推荐），也可以为每个管理节点创建不同的应用程序组。

- 您具有在 AD FS 中创建应用程序组的经验，或者您可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。

关于此任务

这些说明适用于 Windows Server 2022 AD FS。如果使用的是不同版本的 AD FS，您会注意到操作过程中的细微差异。如果有疑问，请参阅 Microsoft AD FS 文档。

步骤 **1**：创建应用程序组

您可以使用 Windows PowerShell 快速创建应用程序组。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * > * AD FS 管理 * 。
2. 选择*应用程序组* > 添加应用程序组
3. 对于 **Name**，输入信赖方标识符。
4. 在模板下，选择*客户端-服务器应用程序* > 访问 **Web API** 的服务器应用程序。
5. 选择 * 下一步 * 。
6. 记录*客户标识符*值。
7. 在 **Redirect URI** 下，输入管理节点的 FQDN（或 IP 地址） `callback` 和 `logged-out` URI：
   - `https://<FQDN>/api/v4/oidc-callback` 或 `https://<IP_address>/api/v4/oidc-callback`
   - `https://<FQDN>/api/v4/oidc-logged-out` 或 `https://<IP_address>/api/v4/oidc-logged-out`

   如果要对所有管理节点使用一个应用程序组，请输入每个管理节点的 URI。如果要为每个管理节点使用不同的应用程序组，请仅输入相应管理节点的 URI。
8. 选择 * 添加 * 。
9. 选择 **Generate a shared secret**，记录 **Secret** 的值，然后选择 **Next**。
10. 输入*标识符*的客户端标识符。
11. 选择*添加*，然后选择*下一步*。
12. 选择*Permit everyone*。
13. 验证是否在*客户端应用程序（调用方）*下选择了服务器应用程序。
14. 在*允许的范围*下，验证是否仅选择以下选项：
    - allatclaims
    - 电子邮件
    - openid

- 配置文件

15. 选择 **Next** > **Next**。
16. 选择 **Close**。

步骤 **2**：配置颁发转换规则

为每个应用程序组配置颁发转换规则。

步骤

1. 在 **AD FS Management** 页面中，右键选择应用程序组，然后选择 **Properties**。
2. 选择先前创建的 Web API，然后选择*编辑*。
3. 选择*颁发转换规则* > 添加规则……。
4. 在*声明规则模板：下，选择*将 **LDAP** 属性作为声明发送。
5. 选择 * 下一步 * 。
6. 输入声明规则名称。
7. 选择 **Active Directory** 作为属性存储。
8. 将 LDAP 属性映射添加到传出声明类型：
   - `E-Mail Addresses - E-Mail Address`
   - `Token-Groups - Unqualified Names - Group`
9. 选择 * 完成 * 。
10. 选择*Apply* > **OK** > **OK**。

下一步

创建应用程序组后，"使用 OIDC 配置 SSO"。

在 **StorageGRID** 中为 **OIDC** 创建 **Entra ID** 企业应用程序

使用 Entra ID 为系统中每个管理节点创建 OpenID Connect (OIDC) 企业应用程序。

开始之前

- 您拥有系统中每个管理节点的依赖方标识符和完全限定域名 (FQDN) 或 IP 地址。

> 您的 StorageGRID 系统中的每个管理节点都必须有一个企业应用程序。这可确保用户可以安全地登录和退出任何管理节点。您可以为所有管理节点创建单个企业应用程序（推荐），也可以为每个管理节点创建不同的企业应用程序。

- 您有在 Entra ID 中创建应用程序的经验。
- 您有一个具有有效订阅的 Entra ID 帐户。
- 您在 Entra ID 帐户中拥有以下角色之一：全局管理员、云应用程序管理员、应用程序管理员或服务主体的所有者。

步骤 **1**：访问 **Entra ID**

步骤

1. 登录到 "Azure 门户"。
2. 选择 "微软Entra ID"。
3. 选择 "应用注册"。

步骤**2**：注册新应用程序

为系统中的每个管理节点注册一个新的企业应用程序。

步骤

1. 在 Entra ID Enterprise 应用程序窗格中，选择 **Application registrations** > **New registration**。
2. 对于 **Name**，输入信赖方标识符。
3. 在*支持的帐户类型*下，选择可以使用应用程序或访问 API 的帐户类型，例如*仅限单个租户 - <tenant_name>*。
4. 在*重定向 URI* 下，选择*选择平台* > **Web**。
5. 输入管理节点的 FQDN（或 IP 地址）重定向 URI： `https://<FQDN>/api/v4/oidc-callback` 或 `https://<IP_address>/api/v4/oidc-callback`

   如果要对所有管理节点使用一个企业应用程序，请输入每个管理节点的 URI。如果要为每个管理节点使用不同的企业应用程序，请仅输入相应管理节点的 URI。

6. 选择*注册*。
7. 在新应用程序注册的"概述"页面上，记录*应用程序（客户端）ID* 和*目录（租户）ID*。

步骤 **3**：配置客户端密码

为每个新应用程序注册客户端密码。

步骤

1. 在新应用程序注册的"概述"页面上，选择 **Manage** > **Certificates and secrets** > **New client secret**。
2. 输入客户端密码并设置所需的到期日期。
3. 选择*添加*以创建客户端密码。
4. 复制密钥*值*。

   从客户端密钥页面刷新或导航后，密钥值将不可见。

步骤 **4**：设置 **API** 权限

为每个新应用程序设置 API 权限。

步骤

1. 在新应用程序注册的"概述"页面上，选择 管理 > **API** 权限 > 添加权限。

2. 选择 **Microsoft APIs** > **Microsoft Graph** > **Delegated permissions**。
3. 展开 **OpenId permissions**，然后选择 **email**、**offline_access**、**openid** 和 **profile**。
4. 选择*添加权限*。
5. 选择*授予管理员同意 <tenant>*，然后选择*是*。

第 **5** 步：添加注销重定向 **URI**

为每个新应用程序添加注销重定向 URI。

步骤

1. 在新应用程序注册的"概述"页面上，选择 **Manage** > **Authentication**。
2. 选择 **Add Redirect URI** > **Web**。
3. 输入管理节点的 FQDN（或 IP 地址）重定向 URI： `https://<FQDN>/api/v4/oidc-logged-out` 或 `https://<IP_address>/api/v4/oidc-logged-out`

   如果要对所有管理节点使用一个应用程序组，请输入每个管理节点的 URI。如果要为每个管理节点使用不同的应用程序组，请仅输入相应管理节点的 URI。

4. 选择*配置*。

下一步

创建企业应用程序后，"使用 OIDC 配置 SSO"。

在 **StorageGRID** 中为 **OIDC** 创建 **Keycloak** 客户端

使用 Keycloak 为 StorageGRID 系统中每个管理节点的 OpenID Connect (OIDC) 创建客户端连接。

开始之前

- 您具有在 Keycloak 中创建客户端的经验，或者您可以访问 Keycloak 文档。
- 您拥有用于目录查找和登录凭据的专用帐户（Bind DN）。
- 您拥有 Keycloak 管理员访问权限。

关于此任务

StorageGRID 系统中的每个管理节点都必须有一个客户端连接。这可确保用户可以安全地登录和退出任何管理节点。您可以为所有管理节点创建单个客户端连接（推荐），也可以为每个管理节点创建不同的客户端连接。

除非另有说明，否则请使用默认设置。在某些情况下，您可以使用贵组织要求的设置。

步骤 **1**：（可选）创建一个领域

创建 Keycloak 领域以配置 LDAP 提供程序和 OIDC 客户端，或使用 Keycloak 默认领域。

步骤

1. 选择 **Create Realm**。
2. 输入领域的名称。

3. 选择*已启用*。
4. 选择 * 创建 * 。

步骤 **2**：配置 **LDAP** 提供程序

请配置 LDAP 提供程序，以便 Keycloak 连接到 Active Directory Federation Service (AD FS) LDAP 服务器。

步骤

1. 选择 **User federation** > **Add Ldap providers**。
2. 在"设置"选项卡下：
   a. 输入以下推荐值：
      - UI 显示名称：输入唯一值。
      - 供应商：**Active Directory**
      - 连接 URL： `ldap://<ldap_IP_address>` 或 `ldaps://<ldap_IP_address>`
      - 连接池： **ON**
      - 绑定 DN：输入绑定 DN
      - 绑定凭据：输入密码
      - 编辑模式：**READ_ONLY**
      - 用户 DN：例如， `CN=Users、 DC=saml、 DC=sgws`
      - 用户名 LDAP 属性：**sAMAccountName**
      - RDN LDAP 属性：**cn**
      - UUID LDAP 属性：**objectGUID**
      - 用户对象类： `person、 organizationalPerson、 user`
      - 用户 LDAP 过滤器： `(sAMAccountName=*)`
      - 搜索范围：子树
      - 分页： **ON**
      - 导入用户： **ON**
      - 同步注册： **ON**
      - 在搜索过程中删除无效用户：**ON**
   b. 选择*测试连接*和*测试身份验证*。

      在继续之前，请解决可能发生的任何问题。
3. 选择 * 保存 * 。

步骤 **3**：配置 **LDAP** 映射

配置 LDAP 映射，将 AD 映射为 Keycloak 的属性。

步骤

1. 转至*用户联盟* > **LDAP**
2. 选择您创建的 LDAP 提供程序。
3. 在映射器选项卡上，选择*添加映射器* > 创建新映射器。
4. 对于映射器类型，选择 **user-attribute-ldap-mapper**。
5. 选择*保存*，然后输入以下信息：
   - 用户模型属性：**userPrincipalName**
   - LDAP 属性：**userPrincipalName**
   - 只读： **ON**
   - 始终从 LDAP 读取值： **ON**
   - 在 LDAP 中为必填项：**OFF**
   - 强制默认值： **ON**
   - 是二进制属性： **OFF**
6. 选择 * 保存 * 。

步骤 **4**：创建 **OIDC** 客户端

为您的系统创建 OIDC 客户端。

步骤

1. 转至 **Clients** > **Create client**。
2. 对于常规设置，输入以下信息：
   - 名称：输入客户端的显示名称。
   - 客户端类型：**OIDC Connect**
   - 客户端 ID：输入一个唯一值。保存此值以供以后使用。
3. 选择 * 下一步 * 。
4. 对于功能配置，输入以下信息：
   - 客户端身份验证：**ON**
   - 标准流程： 启用
   - 直接访问权限：启用
   - 服务帐户角色： **Enable**
5. 选择 * 下一步 * 。
6. 对于登录设置，输入重定向 URI：

> 如果为管理接口配置了一个或多个负载平衡器端点，请为每个端口添加重定向 URI。例如：`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback`和 `\https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

   - 有效的重定向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback` 和

`https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`

- 有效的注销后重定向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- 网页来源： `https://<Admin_IP_address_or_FQDN>`

7. 选择 * 保存 * 。

第 5 步：生成客户端密钥

为您创建的 OIDC 客户端生成客户端密码。

步骤

1. 转至 **Clients**，然后选择您创建的 OIDC 客户端。
2. 在凭据选项卡上，输入以下信息：
   - 客户端身份验证器： **Client Id and Secret**
   - 客户端密码：生成或设置客户端密码。保存此值以供以后使用。

第6步：定义范围

在 Keycloak 中定义作用域。

步骤

1. 转到 **Client scopes** > **Create client scope**，然后输入以下信息：
   - 类型： 无
   - 协议：**OpenID Connect**
   - 在同意屏幕上显示： 已启用
   - 包括在 OpenID Provider Metadata 中：已启用
2. 选择 * 保存 * 。
3. 在映射器选项卡上，选择*配置新映射器* > 用户属性，然后输入以下信息：
   - 名称：输入唯一值。
   - 用户属性：**userPrincipalName**
   - 令牌声明名称：**upn**
   - 声明 JSON 类型：**String**
   - 添加到ID令牌： **ON**
   - 添加到访问令牌： **ON**
   - 添加到userinfo：**ON**
   - 添加到令牌自省：**ON**
4. 选择 * 保存 * 。
5. 转到*客户*，然后选择您创建的OIDC 客户端。
6. 选择*Client Scopes* > **Add client scope**。

7. 选择您创建的客户端作用域。
8. 选择 * 添加 * 。

步骤 7：准备使用 OIDC 配置 SSO

保存在 StorageGRID 系统中使用 Keycloak 通过 OIDC 配置 SSO 所需的信息。

步骤

1. 请检查您是否已从创建的 OIDC 客户端保存了 客户端ID 和 客户端密钥。
2. 保存领域的 OpenID Connect 发现端点。此选项在 `well-known`配置端点中可用：

   ```
   https://<keycloak_host_ip/keycloak_host_name>/realms/<realm_name>/.well-known/openid-configuration
   ```

   可选地包括网络端口：

   ```
   https://<keycloak_host_ip/keycloak_host_name>:<https_port>/realms/<realm_name>/.well-known/openid-configuration
   ```

下一步

创建 OIDC 客户端后，"使用 OIDC 配置 SSO"。

在 StorageGRID 中为 OIDC 创建 Okta 应用程序

在 StorageGRID 系统中为 OpenID Connect (OIDC) 的所有管理节点创建 Okta 应用程序。

开始之前

- 您具有创建 Okta 应用程序的经验，或者您可以访问 Okta 文档。
- 您拥有 Okta 管理员访问权限。

关于此任务

Okta 应用程序必须包含所有管理节点的登录和注销重定向 URI。重定向 URI 可确保用户能够安全地登录和退出任何管理节点。您可以为所有管理节点创建单个 Okta 应用程序（推荐），也可以为每个管理节点创建不同的应用程序。

除非另有说明，否则请使用默认设置。在某些情况下，您可以使用贵组织要求的设置。

步骤 1：创建 Okta 应用程序

使用 Okta UI 创建 Okta 应用程序。

步骤

1. 在 Okta 中，转到 **Applications** > **Applications**。
2. 选择 **Create App Integration**，然后输入以下信息：
   - 登录方式：**OIDC - OpenID Connect**
   - 应用程序类型：**Web Application**

3. 选择 * 下一步 * 。
4. 在"应用集成"字段中输入应用程序的名称。
5. 验证是否为核心授权选择了授权代码（默认）。
6. 为每个管理节点添加登录和注销重定向 URI：
   - 登录重定向URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`
   - 注销重定向 URI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`

> 如果为管理接口配置了一个或多个负载平衡器端点，请为每个端口添加重定向 URI。例如：`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` 和 `\https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

7. 选择*保存*。保存客户端 ID 和客户端密钥值供以后使用。

步骤 **2**：添加联合组

从 Active Directory Federation Service (AD FS) 服务器为 StorageGRID 创建组或使用现有组。

步骤

1. 在 GRID Manager 中，选择 **Configuration** > **Admin groups** > **Create group** > **Federate Group**。
2. 输入 AD FS 服务器组名称。
3. 选择*读写*访问模式和*根访问*权限。
4. 选择 * 创建组 * 。

步骤 **3**：导入 **AD FS** 服务器组和用户

在 AD FS 服务器中安装 Okta Active Directory 客户端。然后，导入 AD FS 服务器组和用户。

步骤

1. 在 Okta 中，转到 目录 > 目录集成 > 添加目录 > 添加 **Active Directory**。
2. 选择 **Set Up Active Directory** > **Download Agent**。
3. 立即按照设置流程操作。

> 如果延迟，设置可能会停止，您需要重新开始。

   a. 选择 Active Directory 域。
   b. 创建 OktaService 帐户，而不是链接现有用户。
   c. 选择包含用户的组织单位和包含组的组织单位。
   d. 选择使用 AD UPN 作为 Okta 用户名的用户主体名称 (UPN)。例如：user@domain.com
4. 搜索 **Okta AD Agent Management Utility** 应用程序。然后，运行应用程序并确认状态消息 `The agent is running`显示。

每当要使用 Okta 执行 AD FS 服务器同步和导入时，都必须运行 Okta AD 客户端。

5. 在 Okta 中，转到 目录 > 目录集成。
6. 选择您创建的目录集成。
7. 选择*导入* > 立即导入。
8. 选择要导入的用户，然后选择*Confirm Assignments*。
9. 转到*目录* > *人员*并确认已成功导入用户。

   如果用户状态未激活，请选择 **Activate** 并继续刷新页面，直至用户处于激活状态。

10. 转到 目录 > 组，确认已自动导入该导入用户的组。
11. 选择该组并验证导入的用户是否属于该组。

步骤 **4**：设置申领

设置声明以在访问令牌中包含 AD FS 服务器组。然后，验证声明是否包含导入用户和 Okta 应用程序的导入组。

步骤

1. 在 Okta 中，转到 目录 > 组。
2. 为导入的用户选择导入的组。
3. 选择*应用程序* > 分配应用程序 > 分配。
4. 转至 **Security** > **API**。
5. 选择*默认*授权服务器。
6. 选择 **Claims** > **Add Claim**。然后，使用以下凭据创建声明：
   - 名称： **groups**
   - 包含在令牌类型中：**ID Token - Always**
   - 值类型：表达式
   - 值：**Groups.startsWith("active_directory","",100)**
   - 包括： 任何范围
7. 转至 **Security** > **API**。
8. 选择*默认*授权服务器。
9. 选择 **Token Preview** 选项卡，并为请求属性输入以下凭据：
   - OAuth/OIDC客户端：**<application name>**
   - 授予类型：**Authorization Code**
   - 用户：导入的用户（电子邮件地址）
   - 作用域：**email, profile, openid**
10. 选择 * 执行 * 。

导入的组显示在 Payload 的 Preview id_token 选项卡中。

下一步

创建 Okta 应用程序后，"使用 OIDC 配置 SSO"。

在 **StorageGRID** 中为 **OIDC** 创建 **PingFederate** 中的服务提供商连接

使用 PingFederate 为系统中每个管理节点的 OpenID Connect (OIDC) 创建服务提供商 (SP) 连接。

开始之前

- 您在 PingFederate 服务器中创建 SP 连接的经验。
- 您有https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["《管理员参考指南》"^]用于PingFedate服务器的。PingFederate 文档提供了详细的分步说明和说明。
- 你有"管理员权限"用于 PingFederate 服务器。

关于此任务

以下说明总结了如何将 PingFederate 服务器版本 12.1.10 配置为 StorageGRID 的 SSO 提供程序。如果您使用的是其他版本的 PingFederate，则可能需要调整这些说明。有关您的版本的详细说明，请参阅 PingFederate 服务器文档。

除非另有说明，否则请使用默认设置。在某些情况下，您可以使用组织要求的设置，例如身份验证方法的设置。

步骤 **1**：创建数据存储

如果尚未创建数据存储，请创建一个数据存储以将 PingFederate 连接到 AD FS LDAP 服务器。

步骤

1. 转到*系统* > 数据和凭据存储。
2. 选择*New Data Store*。
3. 对于类型，选择 **Directory (LDAP)**。
4. 选择 * 下一步 * 。
5. 在 LDAP 配置下：
   - 输入*主机名*、用户 **DN**（用户名）和*密码*的值。

     使用您在 StorageGRID 中"配置身份联合"时所用的值。
   - 对于 Active Directory，选择 **LDAP Type**。

步骤 **2**：创建密码凭据验证器

如果尚未创建密码凭据验证程序，请创建一个。

步骤

1. 选择*Password Credential Validators* > **Create New instance**。
2. 在类型选项卡上，输入以下信息：
   a. 实例名称和实例 ID：可以对两者使用相同的值。
   b. 类型：选择 **LDAP Username Password Credential Validator**。
3. 选择 * 下一步 * 。
4. 在 Instance Configuration （实例配置）选项卡上，输入以下信息：
   - LDAP 数据存储区：选择您创建的 数据存储。
   - SEARCH BASE：输入 LDAP 配置 的信息。
   - 搜索筛选器：输入 **sAMAccountName=${username}**。
   - 搜索范围：选择*子树*。
5. 选择 * 下一步 * 。
6. 在Extended Contract选项卡上，添加以下属性： `memberOf`、 `objectGUID`、 `sAMAccountName`、 `sn` 和 `userPrincipalName`
7. 选择*下一步* > 保存。

步骤 **3**：创建 **IdP** 适配器实例

如果尚未创建，请创建一个 IdP（身份提供程序）适配器实例。

> 您的 StorageGRID 系统中的每个管理节点都必须有一个 IdP 连接。这可确保用户可以安全地登录和退出任何管理节点。您可以为所有管理节点创建单个 IdP 连接（推荐），也可以为每个管理节点创建不同的 IdP 连接。

步骤

1. 转至 * 身份验证 * > * 集成 * > * IdP 适配器 * 。
2. 选择 * 创建新实例 * 。
3. 在类型选项卡上，输入以下信息：
   - 实例名称和实例 ID：可以对两者使用相同的值。
   - 类型：选择 **HTML Form IdP Adapter**。
4. 选择 * 下一步 * 。
5. 在 **IdP Adapter** 选项卡上，选择 **Add a new row to 'Credential Validators'**。
6. 选择您创建的 密码凭据验证程序。
7. 选择 * 下一步 * 。
8. 在Extended Contract选项卡上，添加为 密码凭据验证程序 映射的属性。
9. 选择 * 下一步 * 。
10. 在适配器属性选项卡上，为假名选择 **username** 属性。
11. 选择 **Next** > **Next**。
12. 查看摘要并选择*保存*。

步骤 4：配置 OAuth 服务器和授权服务器设置

配置授权服务器以支持 StorageGRID 接受的授权类型。

步骤

1. 转至*系统* > 授权服务器设置。
2. 验证是否已为授予类型选择以下选项以重用现有永久访问授予：
   - 隐含
   - 授权码
   - 资源所有者密码凭据

   > 如果贵公司限制使用 RESOURCE OWNER PASSWORD CREDENTIALS，则只能使用 AUTHORIZATION CODE。

3. 对于 OAuth 管理 Web 服务设置，请选择您创建的 密码凭据验证程序。

第5步：定义范围

在 PingFederate 中定义作用域。

步骤

1. 转到*系统* > **OAuth Settings** > 范围管理。
2. 在 Common Scopes 选项卡上，添加 **openid**、**email** 和 **profile** 的值（如果它们还不存在）。

第6步：配置 IdP 适配器映射

配置 IdP 适配器映射，以将 IdP 属性映射到颁发给客户端的永久授权，例如访问令牌或刷新令牌。

步骤

1. 转到 **Authentication** > **Policy Contract Grant Mapping**。
2. 选择 **IdP Adapter Grant Mapping**。
3. 从 SOURCE ADAPTER INSTANCE 下拉列表中，选择您创建的 HTML 表单适配器。
4. 选择*添加映射* > 合同履行。
5. 在源下，为 USER_KEY 和 USER_NAME 选择 **Adapter**。
6. 在"值"下，选择 **sAMAccountName** 作为 USER_KEY，选择 **username** 作为 USER_NAME。
7. 选择*下一步* > *下一步*以导航到摘要页面。
8. 选择 * 保存 * 。

第7步：设置资源所有者凭据映射

设置资源所有者凭据映射，以确保在身份验证期间正确验证用户凭据。

步骤

1. 转到 **Authentication** > **Policy Contract Grant Mapping**。

2. 选择*Resource Owner Credentials Grant Mapping*。
3. 从 SOURCE PASSWORD VALIDATOR INSTANCE 下拉列表中，选择您创建的 密码凭据验证程序。
4. 选择*添加映射* > 合同履行。
5. 为 USER_KEY 添加映射：
    - 在 Source 下，选择 **Password Credential Validator**。
    - 在值下，选择 **sAMAccountName**。
6. 选择*下一步* > *下一步*以导航到摘要页面。
7. 选择 * 保存 * 。

第**8**步：创建或导入签名证书

如果尚未创建，请创建或导入签名证书。

步骤

1. 转至 * 安全性 * > * 签名和解密密钥和证书 * 。
2. 选择*Create New*，然后输入以下信息：
    - 公用名 (CN)：这应该是服务器的完全限定域名 (FQDN)。
    - 组织（Org）：输入您的组织名称。
    - 国家/地区：提供两个字母的国家/地区代码，例如，US 代表美国。
    - 密钥算法：选择适当的密钥算法，例如 **RSA**。
    - 密钥大小：设置为 **2048** 位。
    - 签名算法：选择 **RSA with SHA256** 作为签名算法，以确保安全的加密操作。

第**9**步：配置访问令牌管理

StorageGRID 使用访问令牌对 PingFederate 中的 API 请求进行身份验证和授权。

步骤

1. 导航到*应用程序* > 访问令牌管理。
2. 选择 * 创建新实例 * 。
3. 在类型选项卡上，输入以下信息：
    - 实例名称和实例 ID：可以对两者使用相同的值。
    - 类型：验证值是否为 **JSON Web Tokens**。
4. 选择 * 下一步 * 。
5. 在"实例配置"选项卡上，输入证书的以下信息：
    - 密钥 ID：输入密钥的唯一标识符。
    - 证书：添加您创建的 证书。
    - JWS ALGORITHM：选择 **RSA using SHA256**。
    - 活动签名证书密钥 ID：选择您在此步骤中创建的 **KEY ID**。

6. 选择 **Next** > **Next**。
7. 在Access Token Attribute Contract选项卡上，为Subject Attribute Name选择*USER_KEY*，为Extend the Contract选择*username*。
8. 选择 * 添加 * 。
9. 选择*下一步* > 下一步 > *下一步*以导航到摘要页面。
10. 选择 * 保存 * 。

第10步：配置访问令牌映射

配置访问令牌映射以使用您创建的访问令牌。

步骤

1. 转到*应用程序* > 访问令牌映射。
2. 选择*访问令牌映射*。
3. 选择*添加映射*。
4. 对于上下文，选择*Default*。
5. 对于访问令牌管理器，请选择您创建的 访问令牌。
6. 选择*下一步* > 合同履行：
7. 在 Source 下，为用户名选择 **Persistent Grant**。
8. 在值下，选择 **USER_KEY** 作为用户名。
9. 选择*下一步* > 保存。

第11步：设置OpenID Connect策略

为客户端访问根据 OpenID 规范映射的属性定义 OpenID Connect 策略。

步骤

1. 转至*应用程序* > **OAuth Clients**。
2. 选择 **OpenId Connect Policy Management** > **Add Policy**。
3. 在"管理策略"选项卡上，输入以下信息：
   - 策略 ID：此策略的唯一标识符。
   - 策略名称：策略的描述性名称。
   - 访问令牌管理器：选择您创建的 访问令牌。
   - ID TOKEN LIFETIME：为 ID token 设置所需的生存期，例如 60 分钟或 1 小时。
   - 在 ID 令牌中包含用户信息：选中该框以在 ID 令牌中包含用户详细信息。
4. 选择 * 下一步 * 。
5. 在"属性合同"选项卡上，删除您创建的 数据存储 中不需要的任何现有属性。仅保留要从 Ping Authentication 传递到 StorageGRID 的属性。

这是关键的一步。它确定 ID 令牌中包括哪些属性值。StorageGRID 在身份验证过程中继承这些值。

6. 选择 **Next** > **Next**。
7. 在属性源和用户查找选项卡上，选择 添加属性源。然后输入下列信息：
   - ATTRIBUTE SOURCE ID 和 ATTRIBUTE SOURCE DESCRIPTION：可以对两者使用相同的值。
   - ACTIVE DATA STORE：选择您创建的 数据存储。
8. 选择 * 下一步 * 。
9. 在 LDAP 目录搜索选项卡上：
   a. 输入 * 基本 DN* ，该 DN 应与您在 StorageGRID 中为 LDAP 服务器输入的值完全匹配。
   b. 从根对象类下拉列表中选择 **objectClass**。
   c. 从 ATTRIBUTE 下拉列表中，为要映射的每个对象类添加属性。例如：
      - InetOrgPerson：添加 displayName、givenName 或 HomePhone。
      - user：添加 LocalID 或 userPrincipalName (upn)。
      - top：添加 memberOf 或名称。
      - person：添加 sn。
10. 选择 * 下一步 * 。
11. 在 LDAP 筛选器选项卡上，输入 * 。 sAMAccountName=$ ｛username｝ * 。

    您需要自定义 LDAP 筛选器，以确保 StorageGRID 根据贵组织特定的 Active Directory 或 LDAP 结构检索用户属性。请咨询您的 LDAP/AD 管理员，以获取适合您的设置的筛选器表达式。

12. 选择*保存*并查看摘要。
13. 在Contract Fulfillment （合同履行）选项卡上，输入以下信息：
    - 源：选择您创建的 LDAP 数据存储。
    - 值：将每个属性合约映射到相应的值。
14. 选择 **Next** > **Next**。
15. 查看摘要并选择*保存*。
16. 转到*应用程序* > **OAuth Clients** > **OpenID Connect Policy Management**。
17. 验证您创建的策略是否设置为默认策略。

步骤 **12**：为 **OAuth** 服务器创建 **OAuth** 客户端

创建新的 OAuth 客户端以配置必要的客户端凭据并授权 PingFederate 与 StorageGRID 之间的连接。

步骤

1. 转至*应用程序* > **OAuth Clients**。
2. 选择 **Add Client**，然后输入以下信息：
   - 客户端 ID：输入唯一值。

- 客户端身份验证：选择 **Client Secret**。
- CLIENT SECRET：选择 **CHANGE SECRET** > **Generate Secret**。

  这将为客户端生成密钥。保存此密钥供以后使用。

- REDIRECT URIS：在 **Redirect URI** 部分提供 StorageGRID 返回 URL。这些 URL 应与 StorageGRID 中为 OAuth 配置的 URL 匹配：例如：
- `https://<Admin IP or Hostname>/api/v4/oidc-callback`
- `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`
- 允许的授予类型：选择以下选项：
  - 授权码：这将启动 OAuth 流程。
  - **Refresh Token**：在访问令牌过期时获取新令牌。
  - **Resource Owner Password Credentials**：如果您需要直接访问用户凭据进行身份验证。
- OPENID CONNECT：选择 **RSA using SHA-256** 作为 ID 令牌签名算法。
- 注销模式：选择 **OIDC Back-Channel**。
- Front-Channel Logout URI、Back-Channel Logout URI 和 Post-Logout Redirect URI：添加 StorageGRID 注销 URI： `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`

3. 选择 * 保存 * 。

下一步

创建 SP 连接后，"使用 OIDC 配置 SSO"。

使用 **OIDC** 在 **StorageGRID** 中配置 **SSO**

按照为 OpenID Connect (OIDC) 配置 SSO 向导，进入沙盒模式配置和测试单点登录 (SSO)，然后为所有 StorageGRID 用户启用它。启用 SSO 后，您可以在需要更改或重新测试配置时返回沙盒模式。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 您已在 StorageGRID 系统的 SSO 身份提供程序中配置 OIDC 客户端。
- 您的 StorageGRID 系统有"已配置身份联合"。

步骤 **1**：提供身份提供程序详细信息

访问此向导并填写"提供身份提供商详细信息"页面上的字段。

步骤

1. 访问向导以配置SSO设置：
   a. 选择*配置* > 访问控制 > 单点登录。出现“单点登录”页面。

如果配置 SSO 设置按钮被禁用，请确认您已将身份提供者配置为联合身份源。请参阅"单点登录的要求和注意事项" 。

b. 选择*配置 SSO 设置*。出现提供身份提供者详细信息页面。

2. 在*协议*下，选择 **OIDC**。
3. 从下拉列表中选择 * SSO 类型 * 。
4. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置：

     i. 浏览到CA证书的位置。

     ii. 上传CA证书文件。
   - 不使用 **TLS**：不使用 TLS 证书来保护连接。

     如果更改了CA证书、请立即"在管理节点上重新启动mgmt-api服务"测试是否已成功通过SSO进入网格管理器。
5. 选择*继续*。出现“提供依赖方标识符”页面。

步骤 **2**：输入客户端信息

在向导的输入客户端信息步骤中填写字段。

步骤

1. 指定 StorageGRID 的 **Relying party identifier**。此值控制您用于每个 OIDC 配置的名称。
   - 例如，如果您的网格只有一个管理节点，并且您不希望将来添加更多管理节点，请输入 `SG`或 `StorageGRID`。
   - 如果您的网格包含多个管理节点，请在标识符中包含字符串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字符串后，将生成一个表，该表根据节点的主机名显示网格中每个管理节点的 OIDC 配置。

     您必须为 StorageGRID 系统中的管理节点配置 OIDC。这可以确保用户可以安全地登录和注销任何管理节点。您可以为所有管理节点使用相同的 OIDC 配置（推荐），也可以为每个管理节点设置不同的 OIDC 配置。
2. 为每个依赖方标识符输入 **Client ID**、**Client secret** 和 **OpenID endpoint URL**。
3. 选择*保存并进入沙盒模式*。

步骤 **3**：测试配置

进入沙盒模式后，您可以完成并测试所选 SSO 类型的配置。

沙盒模式可以轻松执行来回配置，并在启用 SSO 之前测试所有设置。StorageGRID 可以根据需要保持沙盒模

式。但是，只有联合用户和本地用户才能登录。

步骤

1. 在配置 SSO 页面上，找到向导的测试配置步骤上的链接。

   此 URL 是从您在 * 联合服务名称 * 字段中输入的值派生的。

2. 选择链接，或将网址复制并粘贴到新标签页中，以访问身份提供商的登录页面。
3. 请输入您的联合用户名和密码。
   - 如果 SSO 登录和注销操作成功，则会显示绿色横幅。
   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
4. 按照向导中的步骤访问网格中每个管理节点的测试配置页面。
5. 重复步骤 2 和 3，以验证每个管理节点的 SSO 连接。

步骤 **4**：启用单点登录

确认可以使用 SSO 登录每个管理节点后，即可为整个 StorageGRID 系统启用 SSO。

> 启用 SSO 后，所有用户都必须使用 SSO 访问网格管理器、租户管理器、网格管理 API 和租户管理 API。本地用户无法再访问 StorageGRID。StorageGRID 未为所有受支持的 SSO 提供程序提供示例身份验证脚本。

步骤

1. 从配置 SSO 向导的测试配置步骤中，选择*启用 SSO*。
2. 查看警告消息，然后选择*启用 SSO*。

   单点登录现已启用。出现“单点登录”页面，其中现在包含您刚刚配置的 SSO 的详细信息。

3. 要编辑配置，请选择*编辑*。
4. 要禁用单点登录，请选择*Disable*。

> 如果您使用 Azure 门户，并且从用于访问 Entra ID 的同一台计算机访问StorageGRID ，请确保 Azure 门户用户也是授权的StorageGRID用户（已导入StorageGRID 的联合组中的用户），或者在尝试登录StorageGRID之前注销 Azure 门户。

使用 **SAML** 设置 **SSO**

了解如何使用 **SAML** 在 **StorageGRID** 中设置 **SSO**

在 StorageGRID 中设置单点登录 (SSO) 后，StorageGRID（服务提供商）和 SSO 身份提供商可以安全地就用户身份验证请求进行通信。

您可以使用 OpenID Connect (OIDC) 或 SAML 在 StorageGRID 中设置 SSO。按照以下高级步骤使用 SAML 在 StorageGRID 中设置 SSO，或了解 "使用 OIDC 设置 SSO"。



配置 **SSO**

选择为 SAML 配置 SSO 向导。然后，使用身份提供程序配置 SSO 并进入沙盒模式。

了解 "使用 SAML 配置 SSO"



配置身份提供程序

根据计划使用的 SSO 标识提供程序，您可以为标识联合 LDAP 服务类型选择 Active Directory 或 Entra ID。

- 对于 Active Directory Federation Service (AD FS)，您可以使用 AD FS、Entra ID 或 PingFederate 身份提供程序。
- 对于 Entra ID，您只能使用 Entra ID 身份提供程序。

使用 SSO 身份提供商的软件为网格中的每个管理节点配置 SAML。

- 了解 Active Directory 中的 "为每个管理节点创建应用程序组"
- 了解 Entra ID 中的 "为每个管理节点创建应用程序"
- 了解 "为每个管理节点创建服务提供商连接" 在 PingFederate 中的信息



测试配置

为每个管理节点配置 SAML 后，返回配置 SSO 向导并测试配置。

了解 "测试 SSO 的配置"



启用 **SSO**

为所有 StorageGRID 用户启用 SSO。

了解 "为 StorageGRID 用户启用 SSO"

使用 **SAML** 在 **StorageGRID** 中配置 **SSO**

按照为 SAML 配置 SSO 向导并进入沙盒模式来配置和测试单点登录 (SSO)，然后再为所有 StorageGRID 用户启用它。启用 SSO 后，您可以在需要更改或重新测试配置时返回沙盒模式。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 您已为 StorageGRID 系统配置身份联合。
- 对于身份联合 **LDAP** 服务类型，您可以根据计划使用的 SSO 身份提供商选择 Active Directory 或 Entra ID。

已配置 **LDAP** 服务类型	**SSO** 身份提供程序的选项
Active Directory 联合身份验证服务（ AD FS ）	• Active Directory • 进入 ID • PingFederate
进入 ID	进入 ID

关于此任务

启用 SSO 后，如果用户尝试登录到管理节点，则 StorageGRID 会向 SSO 身份提供程序发送身份验证请求。然后， SSO 身份提供程序会向 StorageGRID 发回身份验证响应，指示身份验证请求是否成功。对于成功的请求：

- Active Directory 或 PingFederate 的响应包括用户的通用唯一标识符（ UUID ）。
- Entra ID 的响应包括用户主体名称 (UPN)。

要允许 StorageGRID （服务提供商）和 SSO 身份提供商安全地就用户身份验证请求进行通信，请完成以下任务：

1. 在StorageGRID中配置设置。
2. 使用 SSO 标识提供程序的软件为每个管理节点创建依赖方信任 (AD FS)、企业应用程序 (Entra ID) 或服务提供程序 (PingFederate)。
3. 返回StorageGRID以启用 SSO。

沙盒模式可以轻松执行这种来回配置，并在启用 SSO 之前测试所有设置。当您使用沙盒模式时，用户无法使用 SSO 登录。

步骤 **1**：提供身份提供程序详细信息

访问此向导并填写"提供身份提供商详细信息"页面上的字段。

步骤

1. 访问向导：
   a. 选择*配置* > 访问控制 > 单点登录。出现“单点登录”页面。

      如果配置 SSO 设置按钮被禁用，请确认您已将身份提供者配置为联合身份源。请参阅"单点登录的要求和注意事项" 。

   b. 选择*配置 SSO 设置*。出现提供身份提供者详细信息页面。
2. 在*协议*下，选择 **SAML**。
3. 从下拉列表中选择 * SSO 类型 * 。
4. 如果您选择 Active Directory 作为 SSO 类型，请输入身份提供者的 联合身份验证服务名称，与 Active Directory 联合身份验证服务 (AD FS) 中显示的完全一致。

要查找联合服务名称，请转到 Windows Server Manager 。选择 * 工具 * > * AD FS 管理 * 。从操作菜单中，选择 * 编辑联合身份验证服务属性 * 。联合服务名称显示在第二个字段中。

5. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - 不使用 **TLS**：不使用 TLS 证书来保护连接。

     如果更改了CA证书、请立即"在管理节点上重新启动mgmt-api服务"测试是否已成功通过SSO进入网格管理器。

6. 选择*继续*。出现“提供依赖方标识符”页面。

步骤 **2**：提供依赖方信任、企业应用程序或 **SP** 连接

根据您选择的 SSO 类型，填写向导第 2 步中的字段。

Active Directory

填写*提供依赖方标识符*步骤中的字段。

步骤

1. 指定StorageGRID的 依赖方标识符。此值控制您在 AD FS 中为每个信赖方信任所使用的名称。
   - 例如，如果您的网格只有一个管理节点，并且您不希望将来添加更多管理节点，请输入 `SG`或 `StorageGRID`。
   - 如果您的网格包含多个管理节点，请包含字符串 `[HOSTNAME]`在标识符中。例如， `SG-[HOSTNAME]` 。包含此字符串将生成一个表，该表根据节点的主机名显示网格中每个管理节点的依赖方标识符。

   > 您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

2. 选择*保存并进入沙盒模式*。

进入 **ID**

填写*配置企业应用程序*步骤中的字段。

步骤

1. 在企业应用程序部分，指定StorageGRID的 企业应用程序名称。此值控制您在 Entra ID 中为每个企业应用程序使用的名称。
   - 例如，如果您的网格只有一个管理节点，并且您不希望将来添加更多管理节点，请输入 `SG`或 `StorageGRID`。
   - 如果您的网格包含多个管理节点，请包含字符串 `[HOSTNAME]`在标识符中。例如， `SG-[HOSTNAME]` 。包含此字符串将生成一个表，该表根据节点的主机名显示系统中每个管理节点的企业应用程序名称。

   > 您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

2. 按照"在 Entra ID 中创建企业应用程序"中的步骤为表中列出的每个管理节点创建企业应用程序。
3. 从 Entra ID 复制每个企业应用程序的联合元数据 URL。然后，将此 URL 粘贴到StorageGRID中相应的 **Federation metadata URL** 字段中。
4. 复制并粘贴所有管理节点的联合元数据 URL 后，选择 保存并进入沙盒模式。

PingFederate

填写 **Provide SP connection ID** 步骤中的字段。

步骤

1. 在服务提供商（ SP ）部分中，为 StorageGRID 指定 * SP 连接 ID* 。此值控制 PingFederate 中每个 SP 连接使用的名称。
   - 例如，如果您的网格只有一个管理节点，并且您不希望将来添加更多管理节点，请输入 `SG`或 `StorageGRID`。

- 如果您的网格包含多个管理节点，请包含字符串 `[HOSTNAME]`在标识符中。例如， `SG-[HOSTNAME]` 。包含此字符串将生成一个表，该表根据节点的主机名显示系统中每个管理节点的SP连接 ID。

  > 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接。为每个管理节点建立 SP 连接可确保用户可以安全地登录和注销任何管理节点。

2. 在 * 联合元数据 URL* 字段中指定每个管理节点的联合元数据 URL 。

   请使用以下格式：

   ```
   https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
   ```

3. 选择*保存并进入沙盒模式*。

步骤 **3**：配置依赖方信任、企业应用程序或 **SP** 连接

保存配置并进入沙盒模式后，您可以完成并测试所选 SSO 类型的配置。

StorageGRID可以根据需要保持沙盒模式。但是，只有联合用户和本地用户可以登录。

Active Directory

步骤

1. 转至 Active Directory 联合身份验证服务（ AD FS ）。
2. 使用“配置 SSO”页面上的表格中显示的每个依赖方标识符，为StorageGRID创建一个或多个依赖方信任。

   您必须为表中所示的每个管理节点创建一个信任。

   有关说明，请转到 "在 AD FS 中创建依赖方信任"。

进入 **ID**

步骤

1. 从当前登录到的管理节点的单点登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到节点。
   b. 选择*配置* > 访问控制 > 单点登录。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 Azure 门户。
4. 按照 "在 Entra ID 中创建企业应用程序" 中的步骤，将每个管理节点的 SAML 元数据文件上传到其相应的 Entra ID 企业应用程序中。

PingFederate

步骤

1. 从当前登录到的管理节点的单点登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到节点。
   b. 选择*配置* > 访问控制 > 单点登录。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 PingFederate 。
4. "为 StorageGRID 创建一个或多个服务提供商（ SP ）连接"。使用每个管理节点的 SP 连接 ID（显示在配置 SSO 页面上的表格中）以及为该管理节点下载的 SAML 元数据。

   您必须为表中所示的每个管理节点创建一个 SP 连接。

步骤 **4**：测试配置

在强制整个StorageGRID系统使用单点登录之前，请确认每个管理节点的单点登录和单点注销均已正确配置。

Active Directory

步骤

1. 在配置 SSO 页面上，找到向导的测试配置步骤上的链接。

   此 URL 是从您在 * 联合服务名称 * 字段中输入的值派生的。

2. 选择此链接，或者将此 URL 复制并粘贴到浏览器中，以访问身份提供程序的登录页面。
3. 要确认您可以使用 SSO 登录到 StorageGRID ，请选择 * 登录到以下站点之一 * ，选择主管理节点的依赖方标识符，然后选择 * 登录 * 。
4. 输入您的联合用户名和密码。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。
   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
5. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

进入 **ID**

步骤

1. 转到 Azure 门户中的单点登录页面。
2. 选择 * 测试此应用程序 * 。
3. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。
   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
4. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

PingFederate

步骤

1. 在配置 SSO 页面中，选择沙盒模式消息中的第一个链接。

   一次选择并测试一个链路。

2. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。
   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
3. 选择下一个链接以验证网格中每个管理节点的 SSO 连接。

   如果您看到页面已过期消息，请在浏览器中选择 * 返回 * 按钮，然后重新提交您的凭据。

步骤 **5**：启用单点登录

确认可以使用 SSO 登录每个管理节点后，即可为整个 StorageGRID 系统启用 SSO。

启用 SSO 后，所有用户都必须使用 SSO 访问网格管理器，租户管理器，网格管理 API 和租户管理 API 。本地用户无法再访问 StorageGRID 。

步骤

1. 从配置 SSO 向导的测试配置步骤中，选择*启用 SSO*。
2. 查看警告消息，然后选择*启用 SSO*。

   单点登录现已启用。出现“单点登录”页面，其中现在包含您刚刚配置的 SSO 的详细信息。

3. 要编辑配置，请选择*编辑*。
4. 要禁用单点登录，请选择“禁用 **SSO**”。

如果您使用 Azure 门户，并且从用于访问 Entra ID 的同一台计算机访问StorageGRID ，请确保 Azure 门户用户也是授权的StorageGRID用户（已导入StorageGRID 的联合组中的用户），或者在尝试登录StorageGRID之前注销 Azure 门户。

下一步是什么?

使用 SAML 配置 SSO 后，为管理节点配置身份提供程序。

如果您的身份提供程序……	您需要……
Active directory	"为每个管理节点创建应用程序组"
进入 ID	"为每个管理节点创建应用程序"
PingFederate	"为每个管理节点创建服务提供商连接"

在 **StorageGRID** 中为 **SAML** 创建 **AD FS** 中的信赖方信任

必须使用 Active Directory 联合身份验证服务 (AD FS) 为系统中的每个 SAML 管理节点创建依赖方信任。您可以使用 PowerShell 命令、从 StorageGRID 导入 SAML 元数据或手动输入数据来创建依赖方信任。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择了 * AD FS* 作为 SSO 类型。
- 您在 Grid Manager 中拥有 "进入沙盒模式"。
- 您知道系统中每个管理节点的完全限定域名（或 IP 地址）和信赖方标识符。您可以在StorageGRID配置 SSO 页面上的管理节点详细信息表中找到这些值。

  您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

- 您有在 AD FS 中创建依赖方信任的经验，也可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。

- 如果您要手动创建依赖方信任，则可以获得为 StorageGRID 管理界面上传的自定义证书，或者知道如何从命令 Shell 登录到管理节点。

关于此任务

以下说明适用于 Windows Server 2016 AD FS 。如果您使用的是其他版本的 AD FS ，则会注意到操作步骤 略有不同。如果您有任何疑问，请参见 Microsoft AD FS 文档。

使用 **Windows PowerShell** 创建依赖方信任

您可以使用 Windows PowerShell 快速创建一个或多个依赖方信任。

步骤

1. 从 Windows 开始菜单中，右键选择 PowerShell 图标，然后选择 * 以管理员身份运行 * 。
2. 在 PowerShell 命令提示符处，输入以下命令：

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - 对于 *Admin_Node_Identifier*，输入管理节点的“依赖方标识符”，与它在“单一登录”页面上显示的完全相同。例如， `SG-DC1-ADM1`。
   - 对于 *Admin_Node_FQDN*，输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）
3. 在 Windows Server Manager 中，选择 * 工具 * > * AD FS 管理 * 。

   此时将显示 AD FS 管理工具。
4. 选择 * AD FS* > * 依赖方信任 * 。

   此时将显示依赖方信任列表。
5. 向新创建的依赖方信任添加访问控制策略：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击信任，然后选择 * 编辑访问控制策略 * 。
   c. 选择访问控制策略。
   d. 选择 * 应用 * ，然后选择 * 确定 *
6. 将款项申请发放策略添加到新创建的相关方信任：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   c. 选择 * 添加规则 * 。
   d. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。
   e. 在配置规则页面上，输入此规则的显示名称。

      例如，**ObjectGUID**到名称**ID***或***UPN**到名称**ID**。

f. 对于属性存储，选择 * Active Directory* 。

g. 在映射表的LDAP属性列中，键入*objectGUID*或选择*User-Principal-Name*。

h. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。

i. 选择 * 完成 * ，然后选择 * 确定 * 。

7. 确认元数据已成功导入。

a. 右键单击依赖方信任以打开其属性。

b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

如果缺少元数据、请确认联盟元数据地址是否正确、或者手动输入值。

8. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

9. 完成后，返回 StorageGRID 并 "测试所有依赖方信任" 以确认它们配置正确。

通过导入联合元数据创建依赖方信任

您可以通过访问每个管理节点的 SAML 元数据来导入每个依赖方信任的值。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。

2. 在操作下，选择 * 添加依赖方信任 * 。

3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。

4. 选择 * 导入有关依赖方的在线或本地网络上发布的数据 * 。

5. 在 * 联合元数据地址（主机名或 URL ） * 中，键入此管理节点的 SAML 元数据的位置：

```
https://Admin_Node_FQDN/api/saml-metadata
```

对于 *Admin_Node_FQDN*，输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

6. 完成依赖方信任向导，保存依赖方信任并关闭该向导。

输入显示名称时，请使用管理节点的相关方标识符，与网格管理器的 Single Sign-On 页面上显示的完全相同。例如， `SG-DC1-ADM1`。

7. 添加声明规则：

a. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。

b. 选择 * 添加规则 * ：

c. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。

d. 在配置规则页面上，输入此规则的显示名称。

例如，**ObjectGUID**到名称**ID***或***UPN**到名称**ID**。

e. 对于属性存储，选择 * Active Directory* 。

f. 在映射表的LDAP属性列中，键入*objectGUID*或选择*User-Principal-Name*。

g. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。

h. 选择 * 完成 * ，然后选择 * 确定 * 。

8. 确认元数据已成功导入。

a. 右键单击依赖方信任以打开其属性。

b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

如果缺少元数据、请确认联盟元数据地址是否正确、或者手动输入值。

9. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

10. 完成后，请返回 StorageGRID 并 "测试所有依赖方信任" 以确认它们配置正确。

手动创建依赖方信任

如果您选择不导入依赖部件信任的数据，则可以手动输入值。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。

2. 在操作下，选择 * 添加依赖方信任 * 。

3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。

4. 选择 * 手动输入有关依赖方的数据 * ，然后选择 * 下一步 * 。

5. 完成依赖方信任向导：

a. 输入此管理节点的显示名称。

为了确保一致性，请使用管理节点的依赖方标识符，与网格管理器的单点登录页面上显示的一致。例如， `SG-DC1-ADM1`。

b. 跳过此步骤可配置可选令牌加密证书。

c. 在配置URL页面上，选中*启用对SAML 2.0 WebSSO协议的支持*复选框。

d. 键入管理节点的 SAML 服务端点 URL：

`https://Admin_Node_FQDN/api/saml-response`

对于 *Admin_Node_FQDN*，输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

e. 在配置标识符页面上，指定同一管理节点的依赖方标识符：

Admin_Node_Identifier

对于 *Admin_Node_Identifier*，输入管理节点的“依赖方标识符”，与它在“单一登录”页面上显示的完全相同。例如， `SG-DC1-ADM1`。

f. 查看设置，保存依赖方信任并关闭向导。

此时将显示编辑款项申请发放策略对话框。

如果未显示此对话框，请右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。

6. 要启动 Claim Rule 向导，请选择 * 添加规则 * ：
   a. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。
   b. 在配置规则页面上，输入此规则的显示名称。

      例如，**ObjectGUID到名称ID*或*UPN到名称ID**。

   c. 对于属性存储，选择 * Active Directory* 。
   d. 在映射表的LDAP属性列中，键入*objectGUID*或选择*User-Principal-Name*。
   e. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。
   f. 选择 * 完成 * ，然后选择 * 确定 * 。
7. 右键单击依赖方信任以打开其属性。
8. 在 * 端点 * 选项卡上，为单点注销（ SLO ）配置端点：
   a. 选择 * 添加 SAML * 。
   b. 选择 * 端点类型 * > * SAML 注销 * 。
   c. 选择 * 绑定 * > * 重定向 * 。
   d. 在 * 可信 URL* 字段中，输入用于从此管理节点单点注销（ SLO ）的 URL ：

      ```
      https://Admin_Node_FQDN/api/saml-logout
      ```

   对于 *Admin_Node_FQDN*，输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

   a. 选择 * 确定 * 。
9. 在 * 签名 * 选项卡上，指定此依赖方信任的签名证书：
   a. 添加自定义证书：
      - 如果您已将自定义管理证书上传到 StorageGRID ，请选择此证书。
      - 如果您没有自定义证书、请登录到管理节点、转到管理节点的目录、 `/var/local/mgmt-api`然后添加 `custom-server.crt`证书文件。

        (`server.crt`不建议使用管理节点的默认证书)。如果管理节点出现故障，则在恢复节点时将重新生成默认证书，您需要更新依赖方信任。

   b. 选择 * 应用 * ，然后选择 * 确定 * 。

      依赖方属性将被保存并关闭。

10. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。
11. 完成后，请返回 StorageGRID 并 "测试所有依赖方信任" 以确认它们配置正确。

在 **StorageGRID** 中为 **SAML** 创建 **Entra ID** 企业应用程序

使用 Entra ID 为系统中每个用于 SAML 的管理节点创建企业应用程序。

开始之前

- 您已开始为StorageGRID配置单点登录，并选择 **Entra ID** 作为 SSO 类型。
- 您在 Grid Manager 中拥有 "进入沙盒模式"。
- 您的系统中的每个管理节点都有*企业应用程序名称*。您可以从配置 SSO 页面上的管理节点详细信息表中复制这些值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

- 您有在 Entra ID 中创建企业应用程序的经验。
- 您有一个具有有效订阅的 Entra ID 帐户。
- 您在 Entra ID 帐户中拥有以下角色之一：全局管理员、云应用程序管理员、应用程序管理员或服务主体的所有者。

步骤 **1**：访问 **Entra ID**

步骤

1. 登录到 "Azure 门户"。
2. 导航至 "进入 ID"。
3. 选择。 "企业级应用程序"

步骤**2**：创建企业应用程序并保存 **StorageGRID SSO** 配置

要在StorageGRID中保存 Entra ID 的 SSO 配置，您必须使用 Entra ID 为每个管理节点创建一个企业应用程序。您将从 Entra ID 复制联合元数据 URL，并将其粘贴到配置 SSO 页面上相应的 联合元数据 **URL** 字段中。

步骤

1. 对每个管理节点重复以下步骤。
   a. 在 Entra ID Enterprise 应用程序窗格中，选择 新应用程序。
   b. 选择 * 创建您自己的应用程序 * 。
   c. 对于名称，请输入从配置 SSO 页面上的管理节点详细信息表复制的*企业应用程序名称*。
   d. 保持选中 * 集成在库（非库）中找不到的任何其他应用程序 * 单选按钮。
   e. 选择 * 创建 * 。
   f. 选择 * 。 2.设置单点登录 * 框，或者选择左侧边距中的 * 单点登录 * 链接。
   g. 选择 * SAML * 框。

h. 复制 * 应用程序联合元数据 URL* ，该 URL 可在 * 步骤 3 SAML 签名证书 * 下找到。

i. 转到配置 SSO 页面，并将 URL 粘贴到与您使用的 企业应用程序名称 相对应的 联合元数据 **URL** 字段中。

2. 为每个管理节点粘贴联合元数据 URL 并对 SSO 配置进行所有其他必要的更改后，在配置 SSO 页面上选择保存。

步骤 **3**：为每个管理节点下载 **SAML** 元数据

保存 SSO 配置后，您可以为 StorageGRID 系统中的每个管理节点下载 SAML 元数据文件。

步骤

1. 对每个管理节点重复上述步骤。

a. 从管理节点登录到 StorageGRID 。

b. 选择*配置* > 访问控制 > 单点登录。

c. 选择按钮以下载此管理节点的 SAML 元数据。

d. 保存文件，然后将其上传到 Entra ID。

步骤 **4**：将 **SAML** 元数据上传到每个企业应用程序

为每个StorageGRID管理节点下载 SAML 元数据文件后，在 Entra ID 中执行以下步骤：

步骤

1. 返回到 Azure 门户。

2. 对每个企业级应用程序重复以下步骤：

> 您可能需要刷新 " 企业应用程序 " 页面才能查看先前在列表中添加的应用程序。

a. 转到企业应用程序的属性页面。

b. 将 * 需要分配 * 设置为 * 否 * （除非您要单独配置分配）。

c. 转到单点登录页面。

d. 完成 SAML 配置。

e. 选择 * 上传元数据文件 * 按钮，然后选择为相应管理节点下载的 SAML 元数据文件。

f. 加载文件后，选择 * 保存 * ，然后选择 * X * 以关闭窗格。此时将返回到使用 SAML 设置单点登录页面。

3. "测试每个应用程序"。

在 **StorageGRID** 中为 **SAML** 创建 **PingFederate** 服务提供商连接

使用 PingFederate 为系统中每个管理节点创建 SAML 服务提供商 (SP) 连接。为了加快此过程，您将从 StorageGRID 导入 SAML 元数据。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择了 * Ping 联邦 * 作为 SSO 类型。

- 您在 Grid Manager 中拥有 "进入沙盒模式"。
- 您系统中每个管理节点都有* SP连接 ID *。您可以在“配置 SSO”页面上的管理节点详细信息表中找到这些值。
- 您已为系统中的每个管理节点下载 * SAML 元数据 * 。
- 您在 PingFederate 服务器中创建 SP 连接的经验。
- 您有https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["《管理员参考指南》"^]用于PingFedate服务器的。PingFederate 文档提供了详细的分步说明和说明。
- 你有"管理员权限"用于 PingFederate 服务器。

关于此任务

以下说明总结了如何将 PingFederate 服务器 10.3 版配置为 StorageGRID 的 SSO 提供程序。如果您使用的是其他版本的 PingFederate ，则可能需要调整这些说明。有关您的版本的详细说明，请参见 PingFederate 服务器文档。

完成 **PingFederate** 中的前提条件

在创建要用于 StorageGRID 的 SP 连接之前，必须先在 PingFederate 中完成前提条件任务。配置 SP 连接时，您将使用这些前提条件中的信息。

创建数据存储库**[Data -store]]**

如果尚未创建数据存储库，请将 PingFederate 连接到 AD FS LDAP 服务器。使用您在StorageGRID中使用的值"配置身份联合"。

- * 类型 * ： 目录（ LDAP ）
- * LDAP 类型 * ： Active Directory
- * 二进制属性名称 * ： 在 "LDAP 二进制属性 " 选项卡上输入 * 对象 GUID* ，具体如图所示。

创建密码凭据验证器**[password-validator]]**

如果尚未创建密码凭据验证程序，请创建一个。

- * 类型 * ： LDAP 用户名密码凭据验证器
- * 数据存储 * ： 选择您创建的数据存储。
- * 搜索基础 * ： 输入 LDAP 中的信息（例如， DC=SAML ， DC=sgws ）。
- * 搜索筛选器 * ： sAMAccountName=$ ｛username｝
- * 范围 * ： 子树

创建**IdP**适配器实例**[adapter-instance]]**

如果尚未创建 IdP 适配器实例，请创建此实例。

步骤

1. 转至 * 身份验证 * > * 集成 * > * IdP 适配器 * 。

2. 选择 * 创建新实例 * 。
3. 在类型选项卡上，选择 * HTML 表单 IdP 适配器 * 。
4. 在 IdP 适配器选项卡上，选择 * 向 " 凭据验证器 "* 添加新行。
5. 选择密码凭据验证程序你创造的。
6. 在适配器属性选项卡上，为 * 伪名称 * 选择 * 用户名 * 属性。
7. 选择 * 保存 * 。

创建或导入签名证书

如果尚未创建，请创建或导入签名证书。

步骤

1. 转至 * 安全性 * > * 签名和解密密钥和证书 * 。
2. 创建或导入签名证书。

在 **PingFederate** 中创建 **SP** 连接

在 PingFederate 中创建 SP 连接时，您可以导入从 StorageGRID 为管理节点下载的 SAML 元数据。元数据文件包含您需要的许多特定值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接，以便用户可以安全地登录和注销任何节点。按照以下说明创建第一个 SP 连接。然后、转到创建其他 SP 连接创建所需的任何其他连接。

选择 **SP** 连接类型

步骤

1. 转至 * 应用程序 * > * 集成 * > * SP 连接 * 。
2. 选择 * 创建连接 * 。
3. 选择 * 不对此连接使用模板 * 。
4. 选择 * 浏览器 SSO 配置文件 * 和 * SAML 2.0* 作为协议。

导入 **SP** 元数据

步骤

1. 在导入元数据选项卡上，选择 * 文件 * 。
2. 选择从管理节点的配置 SSO 页面下载的 SAML 元数据文件。
3. 查看"元数据摘要"以及"常规信息"选项卡上提供的信息。

   合作伙伴的实体 ID 和连接名称设置为 StorageGRID SP 连接 ID 。（例如 10.96.105.200-DC1-ADM1-105-200 ）。基本 URL 是 StorageGRID 管理节点的 IP 。
4. 选择 * 下一步 * 。

配置 IdP 浏览器 SSO

步骤

1. 从浏览器 SSO 选项卡中，选择 * 配置浏览器 SSO* 。
2. 在 SAML 配置文件选项卡上，选择 * SP 启动的 SSO* ， * SP 初始 SLO* ， * IdP-Initiated SSO* 和 * IdP-Initiated SLO* 选项。
3. 选择 * 下一步 * 。
4. 在 Assertion Lifetime 选项卡上，不进行任何更改。
5. 在断言创建选项卡上，选择 * 配置断言创建 * 。
   a. 在身份映射选项卡上，选择 * 标准 * 。
   b. 在属性合同选项卡上，使用 * SAML 主题 * 作为属性合同以及导入的未指定名称格式。
6. 要延长合同，请选择*Delete*以删除未使用的 `urn:oid`。

映射适配器实例

步骤

1. 在身份验证源映射选项卡上，选择 * 映射新适配器实例 * 。
2. 在适配器实例选项卡上、选择您创建的适配器实例。
3. 在映射方法选项卡上，选择 * 从数据存储中检索其他属性 * 。
4. 在属性源和用户查找选项卡上，选择 * 添加属性源 * 。
5. 在数据存储选项卡上、提供说明并选择您添加的数据存储。
6. 在 LDAP 目录搜索选项卡上：
   - 输入 * 基本 DN* ，该 DN 应与您在 StorageGRID 中为 LDAP 服务器输入的值完全匹配。
   - 对于搜索范围，请选择 * 子树 * 。
   - 对于根对象类，搜索并添加以下属性之一：**objectGUUD***或***userPrincipalName**。
7. 在 LDAP 二进制属性编码类型选项卡上，为 * 对象 GUID* 属性选择 * Base64* 。
8. 在 LDAP 筛选器选项卡上，输入 * 。 sAMAccountName=$ ｛username｝ * 。
9. 在属性合同履行选项卡上，从来源下拉列表中选择*LDAP (属性)，然后从值下拉列表中选择***objectGUID*** 或***userPrincipalName**。
10. 查看并保存属性源。
11. 在故障保存属性源选项卡上，选择 * 中止 SSO 事务 * 。
12. 查看摘要并选择 * 完成 * 。
13. 选择 * 完成 * 。

配置协议设置

步骤

1. 在 * SP Connection* > * 浏览器 SSO* > * 协议设置 * 选项卡上，选择 * 配置协议设置 * 。
2. 在断言使用方服务URL选项卡上、接受从StorageGRID SAML元数据导入的默认值(绑定和端点URL的*post*

`/api/saml-response`)。

3. 在SLO服务URL选项卡上、接受从StorageGRID SAML元数据导入的默认值(*重定向*用于绑定和端点URL) `/api/saml-logout`。
4. 在允许的SAML绑定选项卡上、清除*项目*和* SOAP *。仅需要 * 发布 * 和 * 重定向 * 。
5. 在“签名策略”选项卡上，保持选中“要求对authn请求进行签名”和“始终签名断言”复选框。
6. 在加密策略选项卡上，选择 * 无 * 。
7. 查看摘要并选择 * 完成 * 以保存协议设置。
8. 查看摘要并选择 * 完成 * 以保存浏览器 SSO 设置。

配置凭据

步骤

1. 从 SP 连接选项卡中，选择 * 凭据 * 。
2. 从凭据选项卡中，选择 * 配置凭据 * 。
3. 选择正在签名证书您创建或导入的。
4. 选择 * 下一步 * 转到 * 管理签名验证设置 * 。
   a. 在信任模式选项卡上，选择 * 已取消锁定 * 。
   b. 在签名验证证书选项卡上，查看从 StorageGRID SAML 元数据导入的签名证书信息。
5. 查看摘要屏幕并选择 * 保存 * 以保存 SP 连接。

创建其他 **SP** 连接

您可以复制第一个 SP 连接，以便为网格中的每个管理节点创建所需的 SP 连接。您可以为每个副本上传新元数据。

> 不同管理节点的 SP 连接使用相同的设置，但合作伙伴的实体 ID ，基本 URL ，连接 ID ，连接名称，签名验证除外。 和 SLO 响应 URL 。

步骤

1. 选择 * 操作 * > * 复制 * 为每个附加管理节点创建初始 SP 连接的副本。
2. 输入副本的连接 ID 和连接名称，然后选择 * 保存 * 。
3. 选择与管理节点对应的元数据文件：
   a. 选择 * 操作 * > * 使用元数据更新 * 。
   b. 选择 * 选择文件 * 并上传元数据。
   c. 选择 * 下一步 * 。
   d. 选择 * 保存 * 。
4. 解决由于属性未使用而导致的错误：
   a. 选择新连接。
   b. 选择 * 配置浏览器 SSO > 配置断言创建 > 属性合同 * 。

c. 删除 * urn： oid* 的条目。

d. 选择 * 保存 * 。

在 StorageGRID 中禁用 SSO

如果您不再希望使用单点登录（ SSO ）功能，则可以禁用此功能。必须先禁用单点登录，然后才能禁用身份联合。

开始之前

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

步骤

1. 选择*配置* > 访问控制 > 单点登录。

   此时将显示 Single Sign-On 页面。

2. 选择*禁用*。
3. 选择 * 是 * 。

   此时将显示一条警告消息，指示本地用户现在可以登录。

下次登录到 StorageGRID 时，将显示 StorageGRID 登录页面，您必须输入本地或联合 StorageGRID 用户的用户名和密码。

暂时禁用和重新启用 StorageGRID 管理节点的 SSO

如果单点登录（ Single Sign-On ， SSO ）系统发生故障，您可能无法登录到网格管理器。在这种情况下，您可以为一个管理节点临时禁用并重新启用 SSO 。要禁用并重新启用 SSO ，必须访问节点的命令 Shell 。

开始之前

- 您拥有 "特定访问权限"。
- 您已获得 `Passwords.txt`文件。
- 您知道本地 root 用户的密码。

关于此任务

为一个管理节点禁用 SSO 后，您可以以本地 root 用户身份登录到网格管理器。要保护 StorageGRID 系统的安全，您必须在注销后立即使用节点的命令 Shell 在管理节点上重新启用 SSO 。

> 为一个管理节点禁用 SSO 不会影响网格中任何其他管理节点的 SSO 设置。网格管理器中单点登录页面上的*Enable SSO*复选框保持选中状态，所有现有SSO设置都将保持不变，除非您对其进行更新。

步骤

1. 登录到管理节点：

a. 输入以下命令： `ssh admin@Admin_Node_IP`
b. 输入文件中列出的密码 `Passwords.txt`。
c. 输入以下命令切换到root： `su -`
d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 根据您的 SSO 配置，运行以下命令之一：

   SAML

   ```
   disable-saml
   ```

   OIDC

   ```
   disable-oidc
   ```

   此时将显示一条消息，指出命令适用场景 this Admin Node only 。

3. 确认要禁用 SSO 。

   显示一条消息，指示节点上已禁用单点登录。

4. 从 Web 浏览器访问同一管理节点上的网格管理器。

   现在，由于已禁用 SSO ，将显示网格管理器登录页面。

5. 使用用户名 root 和本地 root 用户的密码登录。
6. 如果您因需要更正 SSO 配置而临时禁用 SSO ：
   a. 选择*配置* > 访问控制 > 单点登录。
   b. 更改不正确或过时的 SSO 设置。
   c. 选择 * 保存 * 。

      从 Single Sign-On 页面选择 * 保存 * 会自动为整个网格重新启用 SSO 。

7. 如果您因某些其他原因需要访问网格管理器而临时禁用 SSO ：
   a. 执行需要执行的任何任务。
   b. 选择*注销*，然后关闭网格管理器。
   c. 在管理节点上重新启用 SSO 。您可以执行以下任一步骤：

      - 运行以下命令： `enable-saml`

        此时将显示一条消息，指出命令适用场景 this Admin Node only 。

      确认要启用 SSO 。

显示一条消息，指示节点上已启用单点登录。

- 重新启动网格节点： `reboot`

8. 从 Web 浏览器中，从同一管理节点访问网格管理器。
9. 确认此时将显示 StorageGRID 登录页面，并且您必须输入 SSO 凭据才能访问网格管理器。

使用多管理员验证

了解 **StorageGRID** 多管理员验证

作为 StorageGRID 管理员，您可以使用多管理员验证 (MAV) 来确保某些操作只能在指定管理员批准后才能执行。MAV 有助于防止对您的 StorageGRID 系统进行意外或未经授权的更改。

默认情况下，MAV 处于禁用状态。

MAV 配置概述

要配置 MAV，您将执行以下任务：

- 创建一个或多个管理员组。MAV 管理员具有批准和否决权。
- 启用多管理员验证功能。
- 从一组受保护的操作中选择。

用户必须具有 Root 访问权限才能执行初始配置并在稍后进行修改。

如何在 **MAV** 下处理受保护的操作

启用 MAV 后，完成每个受保护的操作需要以下步骤：

1. 当用户启动操作时，会生成请求。
2. 在执行操作之前，必须至少有一个 MAV 管理员批准。
3. 获得批准后，将自动执行受 MAV 保护的操作。

配置 **StorageGRID** 多管理员验证

配置 StorageGRID 多管理员验证 (MAV) 系统涉及创建和管理 MAV 管理员组和用户、启用 MAV 功能以及选择或配置受保护的操作。

MAV管理员拥有受保护操作的批准和否决权。

开始之前

- 您拥有"root访问权限"。
- 您已从主管理节点登录到网格管理器。

步骤 1：创建 MAV 管理员组和用户

您可以将现有管理员添加到 MAV 组或创建新的管理员。

可以将 Active Directory (AD) 用户配置为 MAV 管理员。AD 用户必须配置为 StorageGRID 管理员。

步骤

1. 要创建 MAV 管理员组，请按照步骤 "创建本地或联合组"。
2. 对于组权限，请选择 **Root access** 或 **Multi-admin verification requests**。
3. 将本地用户或联合用户添加到组，或创建新的本地用户并按照步骤将其添加到组 "创建本地用户"。

步骤2：启用或禁用MAV

您必须明确启用多管理员验证 (MAV)。如果已启用 MAV，并且您决定在存在待处理的 MAV 请求时禁用它，系统将发出通知，说明待处理的请求将被删除。

步骤

1. 选择*配置* > 访问控制 > 多管理员验证 > **MAV** 设置。
2. 选中 **Enable MAV** 复选框以启用多管理员验证。
3. 审批人组部分列出了 MAV 管理组和审批人。
4. 在操作部分，选中要使用 MAV 保护的操作的复选框。
5. （可选）如果要使用电子邮件通知提醒 MAV 管理员待审批请求：
   a. 如果尚未配置电子邮件服务器，请按照步骤 "配置电子邮件服务器"。
   b. 输入发件人的电子邮件地址。
   c. 输入电子邮件通知的一个或多个收件人。
6. 选择*保存*以保存所做更改。

> 如果您决定不配置电子邮件通知，MAV 管理员可以查看 Grid Manager 仪表板或检查审批队列以查看待审批请求。要查看审批队列，请在多管理员验证页面上选择 **Other requests**。

步骤 3：管理受保护的操作

启用多管理员验证后，可以通过选中或清除要使用 MAV 保护的操作的复选框来管理受保护的操作。

> 对于 StorageGRID 12.1，唯一受保护的操作是 ILM 策略激活。如果要启用 MAV，则必须选中 ILM 策略激活的复选框。

MAV 请求可具有以下状态之一：

- 待处理。请求已启动。
- 已过期。请求未在 30 天内得到处理。或者具有 Root 访问权限的用户禁用了 MAV，这意味着所有待处理的请求均已过期。
- 已撤回。用户已撤回其请求。

- 已批准。MAV 管理员批准了待处理的请求。
- 已拒绝。MAV 管理员拒绝了待处理的请求。

对 **MAV** 电子邮件通知进行故障排除

如果 MAV 管理员未收到待处理请求的电子邮件通知，请按照以下步骤解决此问题。

开始之前

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

步骤

1. 验证设置。
   a. 选择*配置* > 监控 > 电子邮件服务器。
   b. 验证电子邮件（ SMTP ）服务器设置是否正确。
   c. 验证您是否为收件人指定了有效的电子邮件地址。
2. 检查垃圾邮件筛选器，确保电子邮件未发送到垃圾文件夹。
3. 请您的电子邮件管理员确认来自发件人地址的电子邮件未被阻止。
4. 收集管理节点的日志文件，然后联系技术支持。

   技术支持可以使用日志中的信息帮助确定出现问题的原因。例如， prometheus.log 文件在连接到您指定的服务器时可能会显示错误。

   请参阅 "收集日志文件和系统数据"。

请求批准 **StorageGRID** 中受 **MAV** 保护的操作

作为 StorageGRID 管理员或用户，当您在 StorageGRID 中启动受 MAV 保护的操作时，将自动生成一个请求。系统将显示一条消息，通知您该操作需要获得批准。

StorageGRID 系统定义哪些操作受 MAV 保护。当您启动受 MAV 保护的操作时，该请求将发送给 MAV 管理员进行审批。

步骤

StorageGRID 系统会通知您已启动受 MAV 保护的操作。

1. 根据需要，执行以下任一任务：
   a. 通过选择 **Configuration** > **Access control** > **Multi-admin verification** > **My requests** 来检查您的请求状态。
      - 待处理。请求已启动。
      - 已过期。请求未在 30 天内得到处理。或者具有 Root 访问权限的用户禁用了 MAV，这意味着所有待处理的请求均已过期。
      - 已撤回。用户已撤回其请求。
      - 已批准。MAV 管理员批准了待处理的请求。

- 已拒绝。MAV 管理员拒绝了待处理的请求。

b. 通过选择*配置* > 访问控制 > 多管理员验证 > 其他请求，检查其他用户的待处理请求。

c. 要取消操作，请选择*我的请求* > 要取消的请求 > 撤回。

MAV 管理员批准请求后，将自动执行此操作。

如果您的请求被拒绝，则不会执行该操作，如果需要，您可以提交新的请求。

管理 **StorageGRID** 中受 **MAV** 保护的操作请求

作为 MAV 管理员，您可以在 StorageGRID 中管理受 MAV 保护的操作请求。您可以查看自己或他人的待处理请求，批准或拒绝请求，并查看过去请求的历史记录。

开始之前

- 您属于 MAV 管理员组，并且具有 "root访问权限"。
- 您已从主管理节点登录到网格管理器。

步骤

1. 如果您收到有关 MAV 请求的电子邮件通知，请选择*配置* > 多管理员验证 > 其他请求。

   此外，Grid Manager 仪表板会显示待处理 MAV 请求的通知。

2. 选择要管理的每个请求的单选按钮。
3. 选择*批准*或*拒绝*以批准或拒绝选定请求。
4. 要查看过往请求的历史记录，请选择*History*。

使用网格联盟

了解 **StorageGRID** 网格联合

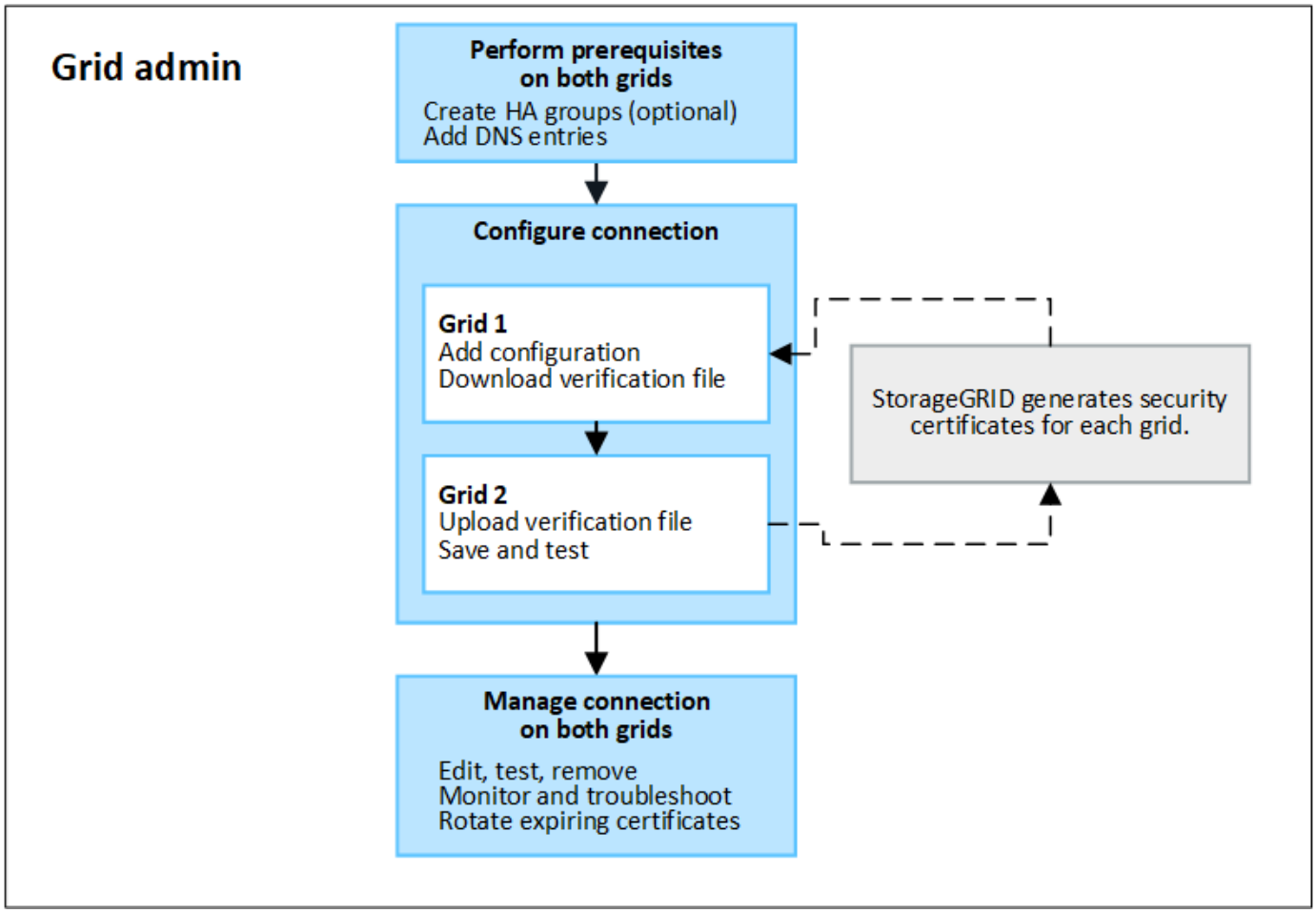
您可以使用网格联合在多个 StorageGRID 系统之间同步租户并复制其对象以进行灾难恢复。

什么是网格联合连接?

网格联合连接是两个StorageGRID 系统中的管理节点和网关节点之间的双向、可信且安全的连接。

网格联合工作流

此工作流图汇总了在两个网格之间配置网格联合连接的步骤。



网格联合连接的注意事项和要求

- 用于网格联合的网格必须运行相同的StorageGRID版本、或者两者之间的主要版本差异不超过一个。

  有关版本要求的详细信息，请参见 "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。

- 一个网格可以与其他网格建立一个或多个网格联合连接。每个网格联合连接都与任何其他连接无关。例如、如果网格1与网格2有一个连接、而与网格3有另一个连接、则网格2与网格3之间不存在隐含连接。
- 网格联合连接是双向的。建立连接后、您可以从任一网格监控和管理连接。
- 必须至少存在一个网格联盟连接，然后才能使用 "帐户同步" 或 "跨网格复制"。

网络和IP地址要求

- 网格联合连接可以在网格网络、管理网络或客户端网络上进行。
- 网格联合连接将一个网格连接到另一个网格。每个网格的配置用于在另一个网格上指定一个网格联合端点、此联合端点由管理节点、网关节点或这两者组成。
- 最佳做法是在每个网格上连接"高可用性(HA)组"网关节点和管理节点。使用HA组有助于确保网格联合连接在节点不可用时保持联机。如果任一HA组中的活动接口发生故障、则此连接可以使用备份接口。
- 建议不要创建使用单个管理节点或网关节点的IP地址的网格联合连接。如果节点不可用、网格联合连接也将不可用。
- "跨网格复制"的对象要求每个网格上的存储节点能够访问另一网格上配置的管理节点和网关节点。对于每个

网格、确认所有存储节点都具有一个高带宽路由、作为用于连接的管理节点或网关节点。

使用**FQDN**对连接进行负载平衡

对于生产环境、请使用完全限定域名(FQDN)标识连接中的每个网格。然后、创建相应的DNS条目、如下所示：

- 网格1的FQDN映射到网格1中HA组的一个或多个虚拟IP (VIP)地址、或者映射到网格1中一个或多个管理节点或网关节点的IP地址。
- 网格2的FQDN映射到网格2的一个或多个VIP地址、或者映射到网格2中一个或多个管理节点或网关节点的IP地址。

如果使用多个DNS条目、则会对使用此连接的请求进行负载平衡、如下所示：

- 映射到多个HA组的VIP地址的DNS条目会在HA组中的活动节点之间进行负载平衡。
- 映射到多个管理节点或网关节点的IP地址的DNS条目会在映射的节点之间进行负载平衡。

端口要求

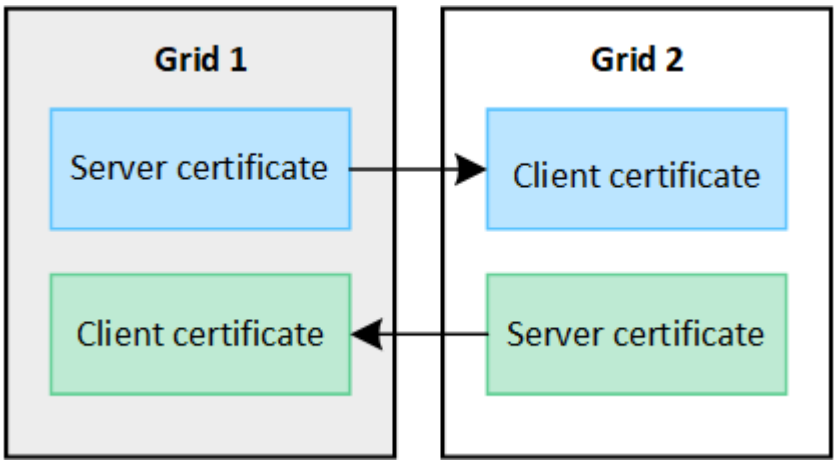
创建网格联合连接时、您可以指定介于23000到23999之间的任何未使用端口号。此连接中的两个网格将使用同一端口。

您必须确保任一网格中的任何节点都不会将此端口用于其他连接。

证书要求

配置网格联合连接时、StorageGRID 会自动生成四个SSL证书：

- 用于对从网格1发送到网格2的信息进行身份验证和加密的服务器和客户端证书
- 用于对从网格2发送到网格1的信息进行身份验证和加密的服务器和客户端证书



默认情况下、证书的有效期为730天(2年)。当这些证书接近到期日期时，“网格联合证书到期”警报会提醒您轮换证书，您可以使用网格管理器执行此操作。

如果连接任一端的证书过期、则连接将停止工作。数据复制将处于待定状态、直到证书更新为止。

了解更多信息。

- "创建网格联合连接"
- "管理网格联合连接"
- "对网格联合错误进行故障排除"

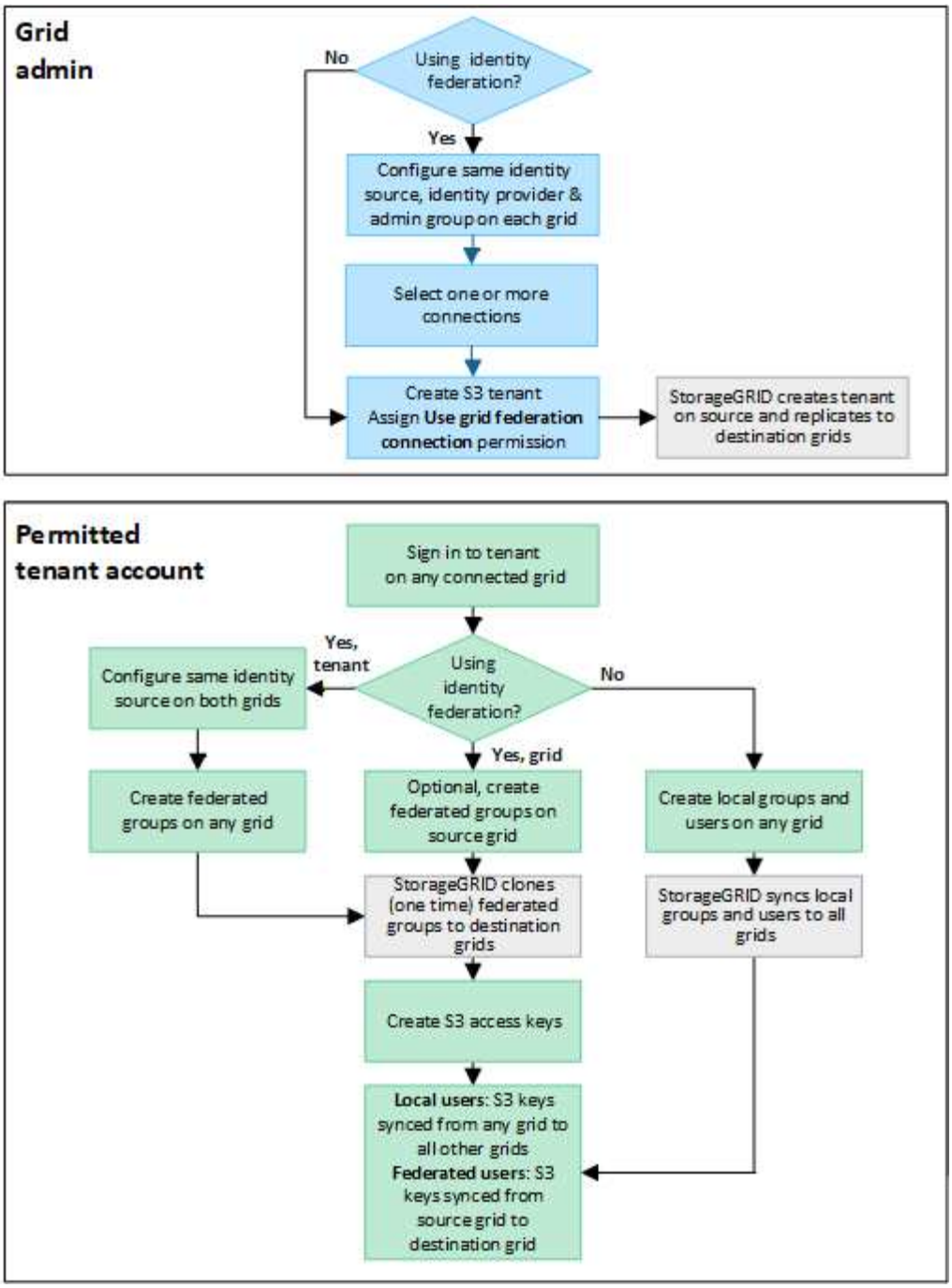
了解 **StorageGRID** 中的帐户同步

帐户同步是在一个或多个 "网格联合连接" 中的 StorageGRID 系统之间自动持续复制租户帐户、租户组、租户用户以及（可选）S3 访问密钥。

"跨网格复制" 需要帐户同步。在 StorageGRID 系统之间同步帐户信息可确保租户用户和组能够访问任何已连接网格上的相应存储桶和对象。

账号同步的工作流程

工作流程图显示网格管理员和允许的租户将执行的步骤，以设置帐户同步。这些步骤在 "已配置网格联合连接" 之后执行。



网格管理工作流

网格管理员执行的步骤取决于中的StorageGRID系统是"网格联合连接"使用单点登录(SSO)还是身份联合。

为帐户同步配置 SSO（可选）

如果网格联合连接中的任一StorageGRID 系统使用SSO、则两个网格都必须使用SSO。在为网格联盟创建租户帐户之前、租户的源网格和目标网格的网格管理员必须执行以下步骤。

步骤

1. 为两个网格配置相同的标识源。请参阅。 "使用身份联合"
2. 为两个网格配置相同的 SSO 身份提供者 (IdP)。看"配置单点登录" 。

3. "创建同一个管理员组"通过导入同一联盟组在两个网格上。

   创建租户时、您需要选择此组、以获得源租户帐户和目标租户帐户的初始root访问权限。

   > 如果在创建租户之前此管理员组不在两个网格上、则不会将租户复制到目标。

为帐户同步配置网格级身份联合（可选）

如果任一StorageGRID 系统使用无SSO的身份联合、则两个网格都必须使用身份联合。在为网格联盟创建租户帐户之前、租户的源网格和目标网格的网格管理员必须执行以下步骤。

步骤

1. 为两个网格配置相同的标识源。请参阅。 "使用身份联合"
2. (可选)如果联盟组对源租户帐户和目标租户帐户都具有初始root访问权限、则可通过导入同一联盟组在两个网格上进行访问"创建同一个管理员组"。

   > 如果为两个网格上都不存在的联盟组分配root访问权限、则租户不会复制到目标网格。

3. 如果您不希望联盟组对这两个帐户都具有初始root访问权限、请指定本地root用户的密码。

创建允许的**S3**租户帐户

根据需要配置SSO或身份联合之后、网格管理员可以执行以下步骤来确定哪些租户可以将存储分段对象复制到其他StorageGRID 系统。

步骤

1. 确定要作为帐户同步操作的租户源网格的网格。

   最初创建租户的网格称为租户的_ssource grid _。用于复制租户的网格称为租户的_Destination grid _。

2. 在此网格中、创建新的S3租户帐户或编辑现有帐户。
3. 分配*使用网格联合连接*权限。
4. 如果租户帐户要管理自己的联盟用户，请分配“使用自己的身份源”权限。

   如果分配此权限，源租户帐户和目标租户帐户在创建联合组之前必须配置相同的身份源。添加到源租户的联合组无法同步到目标租户，除非两个网格使用相同的身份源。

5. 选择特定的网格联合连接。
6. 保存新租户或修改后的租户。

   保存具有*使用网格联合连接*权限的新租户时、StorageGRID 会自动在另一个网格上创建该租户的副本、如下所示：

   - 这两个租户帐户具有相同的帐户ID、名称、存储配额和已分配权限。
   - 如果选择了具有租户 Root 访问权限的联合组，则会将该组克隆到目标租户。但是，不会对联合组和用户进行连续同步。仅发生一次性克隆。
   - 如果选择了具有租户 Root 访问权限的本地用户，则该用户将同步到目标租户。

有关详细信息，请参阅 "管理网格联盟的允许租户"。

允许的租户帐户工作流

将具有*使用网格联合连接*权限的租户复制到目标网格后，允许的租户帐户可以执行这些步骤来同步租户组、用户和 S3 访问密钥。

步骤

1. 在任何连接的网格上登录到租户帐户。
2. 如果允许，请在源和目标租户帐户上配置身份联盟。
3. 在任何连接的网格上创建组和用户。

   在租户上创建新组或用户时，StorageGRID 会自动将其同步到目标租户。

4. 创建S3访问密钥。
5. （可选）将 S3 访问密钥从源租户同步到目标租户。

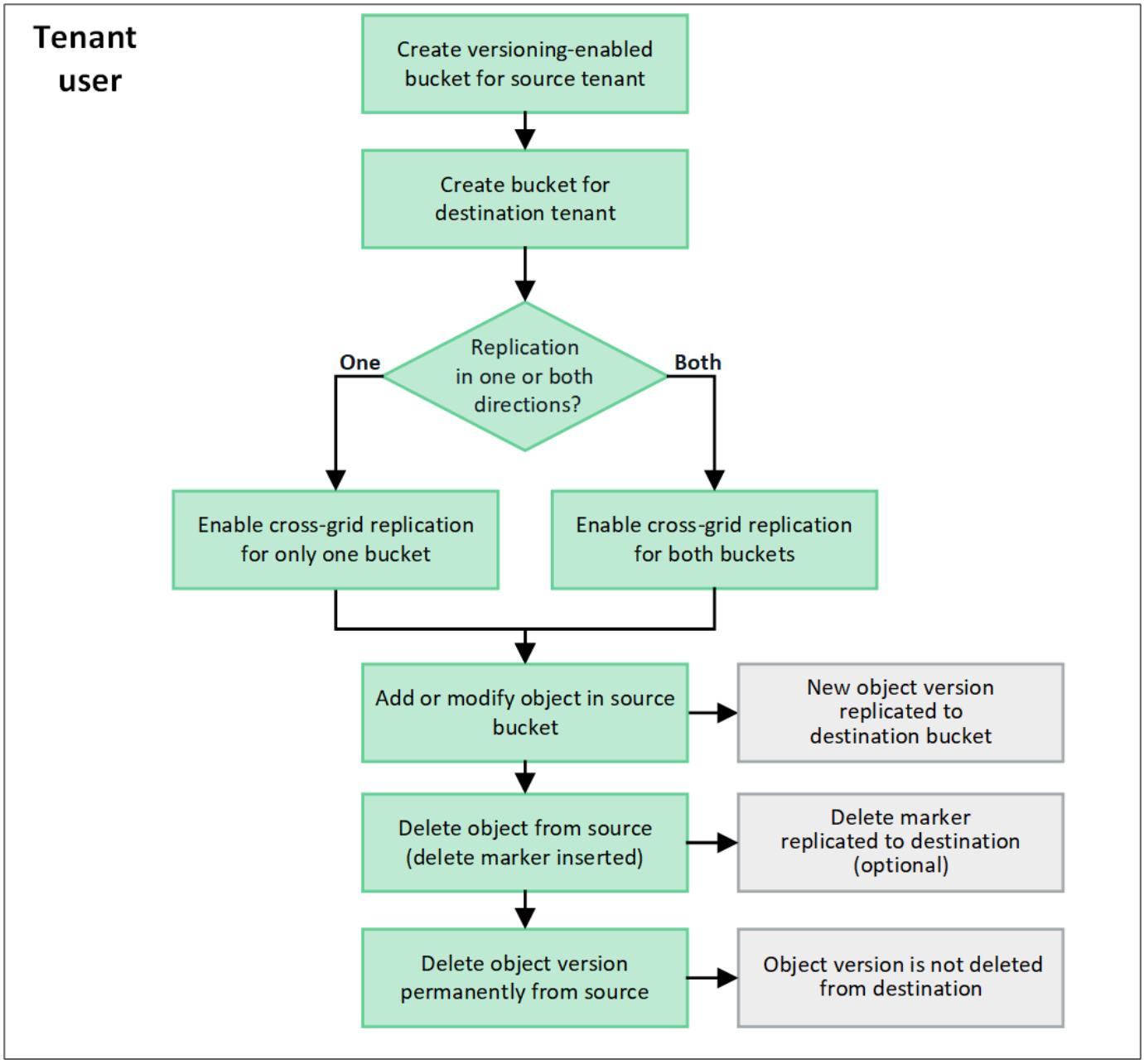
有关允许的租户帐户工作流的详细信息，以及要了解如何同步组、用户和 S3 访问密钥，请参阅 "同步租户组和用户"。

了解 **StorageGRID** 中的跨网格复制

跨网格复制是在连接于 "网格联合连接" 的两个 StorageGRID 系统中所选 S3 存储桶之间自动复制对象的功能。"帐户同步" 是跨网格复制所必需的。

跨网格复制工作流

工作流程图总结了在两个网格上的存储桶之间配置跨网格复制的步骤。



跨网格复制的要求

如果租户帐户具有*使用网格联合连接*权限以使用一个或多个 "网格联合连接"，则具有 Root 访问权限的租户用户可以在每个网格上的相应租户帐户中创建存储桶（"源"和"目标"存储桶）。这些存储桶：

- 可以有不同的名称
- 可以有不同的区域
- 必须启用版本控制
- 必须具有以下 S3 对象锁定配置之一：
  - 来源：已禁用，目的地：已禁用
  - 来源： 已启用 ，目的地： 已启用
  - 来源：已禁用，目的地：已启用

创建两个存储桶后，您可以为其中一个或两个存储桶配置跨网格复制。

了解更多信息。

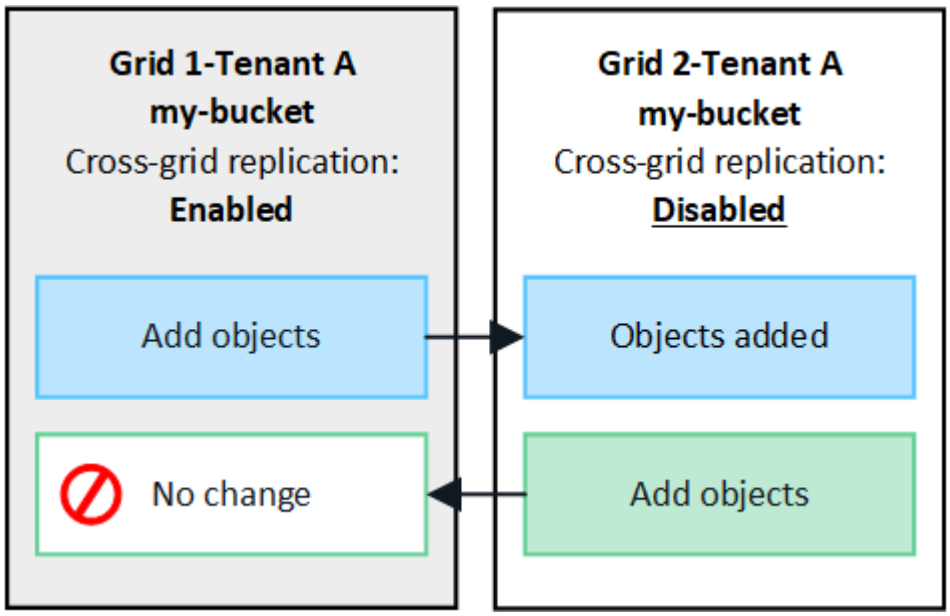
"管理跨网格复制"

跨网格复制的工作原理

您可以将跨网格复制配置为单向或双向进行。

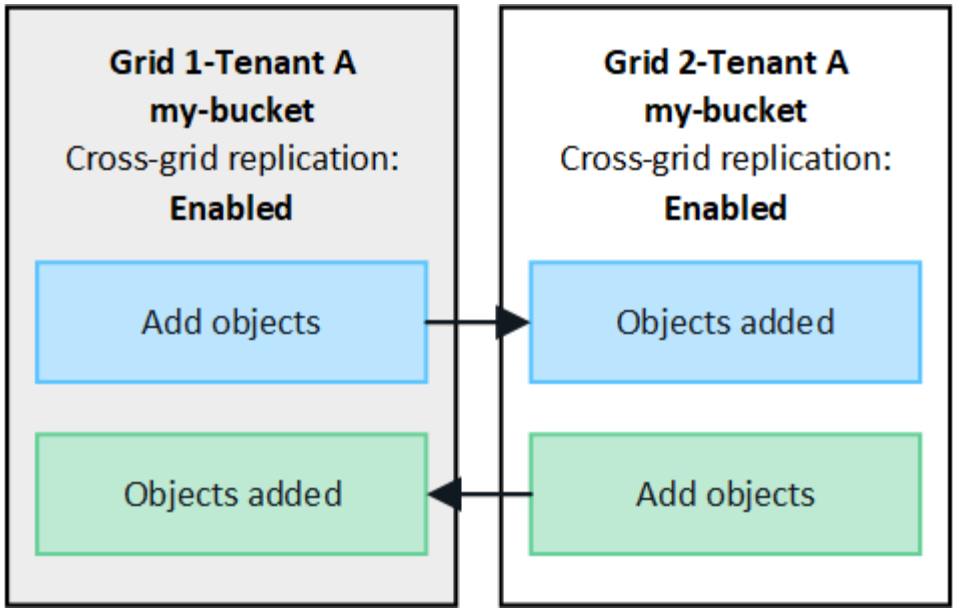
单向复制

如果仅为一个网格上的存储桶启用跨网格复制，则添加到该存储桶（源存储桶）的对象将被复制到另一个网格上的相应存储桶（目标存储桶）。但是，添加到目标存储桶的对象不会被复制回源。图中，启用了跨网格复制 `my-bucket`从网格 1 到网格 2，但在另一个方向则无法启用。



双向复制

如果为两个网格上的同一存储分段启用跨网格复制、则添加到任一存储分段的对象将复制到另一个网格。在图中、跨网格复制在两个方向上均已启用 `my-bucket`。



当对象被加热时会发生什么情况?

当S3客户端向启用了跨网格复制的存储分段添加对象时、会发生以下情况：

1. StorageGRID 会自动将对象从源存储分段复制到目标存储分段。执行此后台复制操作所需的时间取决于多个因素、包括待处理的其他复制操作的数量。

   S3 客户端可以通过发出 GetObject 或 HeadObject 请求来验证对象的复制状态。响应包括StorageGRID特定的 `x-ntap-sg-cgr-replication-status`响应头，其值为以下之一：

网格	复制状态
源	• **completed**：所有网格连接的复制均成功。 • *pending *：对象尚未复制到至少一个网格连接。 • 失败：复制未等待任何电网连接，并且至少有一个电网连接发生永久性故障。用户必须解决该错误。
目标	**REPRAM**：对象已从源网格复制。

   StorageGRID不支持 `x-amz-replication-status`标头。

2. StorageGRID使用每个网格的活动ILM策略来管理对象、就像管理任何其他对象一样。例如、网格1上的对象A可能会存储为两个复制副本并永久保留、而复制到网格2的对象A的副本可能会使用2+1纠删编码进行存储、并在三年后删除。

删除对象时会发生什么情况?

如中所述"删除数据流"，StorageGRID可以出于以下任一原因删除对象：

- S3客户端发出删除请求。
- 租户管理器用户"删除存储分段中的对象"可选择从存储分段中删除所有对象。

- 此存储分段具有生命周期配置、此配置将过期。
- 对象的ILM规则中的最后一个时间段结束、并且未指定其他放置位置。

如果StorageGRID 因"删除存储分段"操作中的对象、存储分段生命周期到期或ILM放置到期而删除对象、则不会从网格联合连接中的其他网格中删除复制的对象。但是、S3客户端删除操作添加到源存储分段的删除标记可以选择复制到目标存储分段。

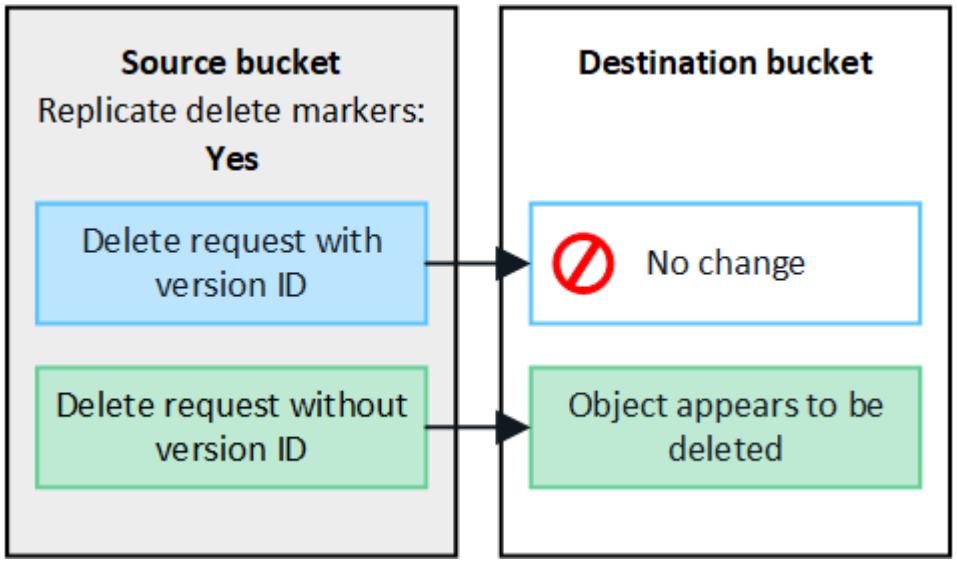
要了解S3客户端从启用了跨网格复制的存储分段中删除对象时会发生什么情况、请查看S3客户端如何从启用了版本控制的存储分段中删除对象、如下所示：

- 如果S3客户端发出包含版本ID的删除请求、则该对象的版本将被永久删除。不会向存储分段添加任何删除标记。
- 如果 S3 客户端发出不包含版本 ID 的删除请求， StorageGRID不会删除任何对象版本。相反，它会向存储桶添加一个删除标记。删除标记使StorageGRID表现得好像对象已被删除：
  - 没有版本 ID 的 GetObject 请求失败，并显示 `404 No Object Found`
  - 具有有效版本 ID 的 GetObject 请求成功并返回请求的对象版本。

当S3客户端从启用了跨网格复制的存储分段中删除对象时、StorageGRID 将确定是否将删除请求复制到目标、如下所示：

- 如果删除请求包含版本 ID，则该对象版本将从源网格中永久删除。但是， StorageGRID不会复制包含版本 ID 的删除请求，因此相同的对象版本不会从目标中删除。
- 如果删除请求不包含版本 ID， StorageGRID可以根据存储桶的跨网格复制配置方式选择性地复制删除标记：
  - 如果选择复制删除标记(默认)、则会将删除标记添加到源存储分段并复制到目标存储分段。实际上，该对象在两个网格上似乎都被删除。
  - 如果您选择不复制删除标记，则删除标记将添加到源存储桶，但不会复制到目标存储桶。实际上，在源网格上删除的对象不会在目标网格上删除。

在图中，当"已启用跨网格复制"。包含版本 ID 的源存储桶的删除请求不会从目标存储桶中删除对象。不包含版本 ID 的源存储桶的删除请求似乎会删除目标存储桶中的对象。



如果要使对象删除在网格之间保持同步、请为两个网格上的分段创建相应的"S3生命周期配置"。

如何复制加密对象

使用跨网格复制在网格之间复制对象时、您可以对单个对象进行加密、使用默认分段加密或配置网格范围的加密。在为存储分段启用跨网格复制之前或之后、您可以添加、修改或删除默认存储分段或网格范围的加密设置。

要对单个对象进行加密、可以在向源存储分段添加对象时使用SSE (使用StorageGRID托管密钥的服务器端加密)。使用 `x-amz-server-side-encryption`请求标头并指定 `AES256`。请参阅。 "使用服务器端加密"

跨网格复制不支持使用 SSE-C（使用客户提供的密钥的服务器端加密）。摄取操作将会失败。

要对存储分段使用默认加密，请使用PutBucketEncryption请求并将参数设置 `SSEAlgorithm`为 `AES256`。存储分段级加密适用于未包含请求标头的任何已加载对象 `x-amz-server-side-encryption`。请参阅。 "对存储分段执行的操作"

要使用网格级加密，请将*存储对象加密*选项设置为*AES-256*。网格级加密适用于未在存储分段级别进行加密的任何对象、或者不带请求标头的已加载对象 `x-amz-server-side-encryption`。请参阅。 "配置网络和对象选项"

SSE 不支持 AES-128。如果使用 **AES-128** 选项为源网格启用了 存储对象加密 选项，则 AES-128 算法的使用不会传播到复制的对象。相反，复制的对象使用目标的默认存储桶或网格级加密设置（如果可用）。

在确定如何对源对象进行加密时、StorageGRID 会应用以下规则：

1. 如果存在、请使用" `x-amz-server-side-encryption`加载"标题。
2. 如果不存在摄取标头，则使用存储桶默认加密设置（如果已配置）。
3. 如果未配置存储桶设置，则使用网格范围的加密设置（如果已配置）。
4. 如果不存在网格范围的设置，则不要加密源对象。

在确定如何对复制的对象进行加密时、StorageGRID 会按以下顺序应用这些规则：

1. 使用与源对象相同的加密、除非该对象使用AES-128加密。
2. 如果源对象未加密或使用 AES-128，则使用目标存储桶的默认加密设置（如果已配置）。
3. 如果目标存储桶没有加密设置，则使用目标的网格范围加密设置（如果已配置）。
4. 如果不存在网格范围的设置，则不要加密目标对象。

使用 **S3** 对象锁进行跨网格复制

您可以在以下情况下配置启用了 S3 对象锁定的StorageGRID桶之间的跨网格复制。

当源存储桶上的 **S3** 对象锁定是…	目标存储桶上的 **S3** 对象锁是…
已启用	已启用

当源存储桶上的 **S3** 对象锁定是…	目标存储桶上的 **S3** 对象锁是…
已禁用	已启用

您可以在现有存储桶上启用 S3 Object Lock，这可能会导致稍后出现配置错误。

如果在源存储桶上启用了 S3 对象锁定，请确保在目标存储桶上也启用了它。如果在目标存储桶上禁用了 S3 对象锁定，则在复制过程中会发生错误。请参阅 "跨网格复制警报和错误"。

当源存储桶上的 S3 对象锁定启用时：

- 对象按照以下顺序在目标处使用保留设置进行锁定：
  a. 源对象的保留标头值为：

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. 源存储桶的默认保留（如果设置）。
  c. 目标存储桶的默认保留（如果设置）。

  目标存储桶的默认保留不会覆盖从源对象复制的保留设置。
- 您可以使用以下方式设置目标对象的合法保留状态 `x-amz-object-lock-legal-hold`上传对象时。
- 如果目标租户或存储桶不支持源对象的 S3 对象锁定设置，则会发生错误。请参阅"跨网格复制警报和错误。"

当源存储桶上的 S3 对象锁定被禁用时：

- 您可以在目标存储桶上配置默认保留，以将 S3 对象锁定保留设置应用于目标对象。
- 目标对象无法设置合法保留状态。

不支持**PutObjectTaging.**和**DeleteObjectTaging**

启用了跨网格复制的分段中的对象不支持PutObjectTbaging和DeleteObjectTbagingrequests。

如果 S3 客户端发出 PutObjectTagging 或 DeleteObjectTagging 请求， `501 Not Implemented`被退回。消息是 `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured`。

不支持 **PutObjectRetention** 和 **PutObjectLegalHold**

对于启用了跨网格复制的存储桶中的对象，PutObjectRetention 和 PutObjectLegalHold 请求不完全支持。

如果 S3 客户端发出 PutObjectRetention 或 PutObjectLegalHold 请求，则会修改源对象的设置，但更改不会应用到目标。

分段对象的复制方式

源网格的最大段大小适用于复制到目标网格的对象。当对象被复制到另一个网格时，两个网格都会使用源网格的*最大段大小*设置（配置 > 系统 > 存储选项）。例如，假设源网格的最大段大小为 1 GB，而目标网格的最大段大小为 50 MB。如果您在源网格上提取一个 2 GB 的对象，则该对象将保存为两个 1 GB 的段。它还会作为两个 1 GB 的段复制到目标网格，尽管该网格的最大段大小为 50 MB。

比较 **StorageGRID** 中的跨网格复制和 **CloudMirror** 复制

开始使用网格联合时，请查看和之间的相似之处和不同之"跨网格复制""StorageGRID CloudMirror 复制服务"处。

> 您不能在通过跨网格复制复制的存储桶上使用 CloudMirror，反之亦然。

	跨网格复制	**CloudMirror** 复制服务
主要目的是什么？	一个StorageGRID 系统充当灾难恢复系统。分段中的对象可以在网格之间进行一个或两个方向的复制。	允许租户自动将对象从StorageGRID (源)中的存储分段复制到外部S3存储分段(目标)。 CloudMirror 复制在独立的 S3 基础架构中创建对象的独立副本。此独立副本不用作备份，但通常在云中进一步处理。
如何设置？	1. 配置两个网格之间的网格联合连接。 2. 添加新租户帐户，这些帐户会自动同步到其他网格。 3. 添加新的租户组和用户，这些内容也会同步。 4. 在每个网格上创建相应的存储分段、并允许跨网格复制在一个或两个方向进行。	1. 租户用户可通过使用租户管理器或S3 API定义CloudMirror端点(IP地址、凭据等)来配置CloudMirror复制。 2. 可以将该租户帐户拥有的任何存储分段配置为指向CloudMirror端点。
谁负责设置？	• 网格管理员配置连接和租户。 • 租户用户配置组、用户、密钥和分段。	通常指租户用户。
目标是什么？	网格联盟连接中另一个StorageGRID 系统上的相应且相同的S3存储分段。	• 任何兼容的S3基础架构(包括Amazon S3)。 • Google Cloud Platform （ GCP ）
是否需要对象版本控制？	是的、源分段和目标分段都必须启用对象版本控制。	不可以、CloudMirror复制支持源和目标上的任何未受版本控制的分段和受版本控制的分段组合。
将对象移动到目标的原因是什么？	将对象添加到启用了跨网格复制的存储分段时、系统会自动复制这些对象。	将对象添加到配置了CloudMirror端点的存储分段时、系统会自动复制这些对象。在为源存储分段配置CloudMirror端点之前、源存储分段中存在的对象不会进行复制、除非对其进行了修改。

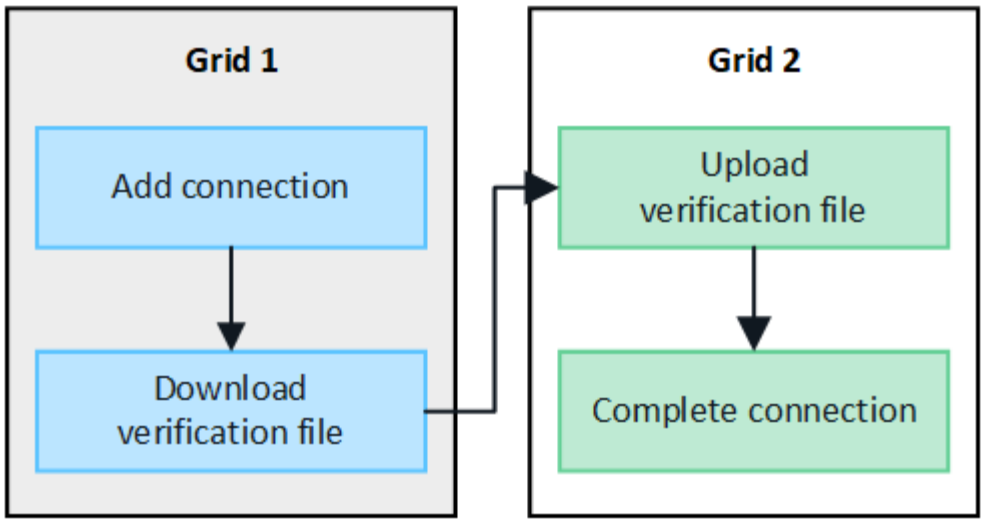
	跨网格复制	**CloudMirror** 复制服务
如何复制对象？	跨网格复制可创建版本控制对象、并将版本ID从源存储分段复制到目标存储分段。这样可以在两个网格之间保持版本顺序。	CloudMirror复制不需要启用了版本控制的分段、因此CloudMirror只能保持站点内密钥的顺序。对于向不同站点的对象发出的请求、不保证会保持排序。
如果无法复制对象、该怎么办？	对象将排队等待复制、但要遵守元数据存储限制。	对象将排队等待复制，但受平台服务限制的限制(请参见"使用平台服务的建议")。
是否复制了对象的系统元数据？	可以、当将对象复制到另一个网格时、也会复制其系统元数据。两个网格上的元数据将相同。	不可以、将对象复制到外部存储分段时、系统将更新其系统元数据。元数据因位置而异、具体取决于加数据时间以及独立S3基础架构的行为。
如何检索对象？	应用程序可以通过向任一网格上的存储分段发出请求来检索或读取对象。	应用程序可以通过向StorageGRID 或S3目标发出请求来检索或读取对象。例如，假设您使用 CloudMirror 复制将对象镜像到合作伙伴组织。配对节点可以使用自己的应用程序直接从 S3 目标读取或更新对象。不需要使用 StorageGRID 。
删除对象会发生什么情况？	• 包含版本ID的删除请求不会复制到目标网格。 • 如果删除请求不包含版本ID、请向源存储分段添加一个删除标记、此标记可以选择复制到目标网格。 • 如果只为一个方向配置了跨网格复制、则可以删除目标存储分段中的对象、而不会影响源。	根据源分段和目标分段的版本控制状态、结果会有所不同(不必相同)： • 如果这两个存储分段都已分版本、则删除请求将在这两个位置添加一个删除标记。 • 如果仅对源存储分段进行了版本控制、则删除请求会向源添加一个删除标记、但不会向目标添加此标记。 • 如果两个存储分段均未进行版本控制、则删除请求将从源中删除对象、而不是从目标中删除对象。 同样，可以删除目标分段中的对象而不影响源。

创建 **StorageGRID** 网格联合连接

如果要同步租户详细信息并复制对象数据，可以在 StorageGRID 系统之间创建网格联合连接。

如图所示、创建网格联合连接包括两个网格上的步骤。您可以在一个网格上添加连接、并在另一个网格上完成连接。您可以从任一网格开始。

或者，您也可以 "自动创建、编辑和维护网格联合连接"。



开始之前

- 您已查看"注意事项和要求"配置网格联合连接的。
- 如果您计划对每个网格使用完全限定域名(FQDN)、而不是IP或VIP地址、则您知道要使用哪些名称、并且已确认每个网格的DNS服务器具有相应的条目。
- 您正在使用"支持的 Web 浏览器"。
- 您具有两个网格的root访问权限和配置密码短语。

添加连接

在两个StorageGRID 系统中的任一系统上执行以下步骤。

步骤

1. 从任一网格上的主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 选择*添加连接*。
4. 输入连接名称，这是一个唯一的名称，可帮助您识别此连接。例如， `Grid 1-Grid 2`。
5. 如果需要"配置全局命名空间"，请选择*Enable global namespace*。
6. 选择 * 继续 * 。
7. 输入网格详细信息，如下：

字段	说明
此网格的FQDN或IP	以下选项之一： • 当前已登录到的网格的FQDN • 此网格上HA组的VIP地址 • 此网格上管理节点或网关节点的IP地址。IP可以位于目标网格可以访问的任何网络上。

字段	说明
端口	要用于此连接的端口。您可以输入介于23000到23999之间的任何未使用端口号。 此连接中的两个网格将使用同一端口。您必须确保任一网格中的任何节点都不会将此端口用于其他连接。
此网格的证书有效天数	希望此网格在连接中的安全证书有效的天数。默认值为730天(2年)、但您可以输入1到762天之间的任何值。 保存连接时、StorageGRID 会自动为每个网格生成客户端和服务器证书。
为此网格配置密码短语	要登录到的网格的配置密码短语。
其他网格的FQDN或IP	以下选项之一： • 要连接到的网格的FQDN • 另一个网格上HA组的VIP地址 • 另一网格上的管理节点或网关节点的IP地址。IP可以位于源网格可以访问的任何网络上。

1. 选择*保存并继续*。
2. 对于“下载验证文件”步骤，请选择*下载验证文件*。

   在另一个网格上完成连接后、您将无法再从任一网格下载验证文件。

3. 找到下载的文件(*connection-name*.grid-federation，并将其保存到安全的位置。

   此文件包含机密(屏蔽为 *)和其他敏感详细信息，必须安全地存储和传输。

4. 选择*Close*(关闭*)返回到Grid Federation (网格联合)页面。
5. 确认新连接已显示且其*Connection statues*为*waits to connect *。
6. 将文件提供 `*connection-name*.grid-federation`给另一个网格的网格管理员。

完成连接

在要连接的StorageGRID 系统(另一个网格)上执行这些步骤。

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 选择*上传验证文件*以访问上传页面。
4. 选择*上传验证文件*。然后，浏览并选择从第一个网格下载的文件(*connection-name*.grid-

federation)。

此时将显示此连接的详细信息。

5. (可选)为此网格输入不同的安全证书有效天数。“证书有效天数”条目默认为您在第一个网格中输入的值，但每个网格可以使用不同的到期日期。

   通常、对连接两端的证书使用相同天数。

   > 如果连接任一端的证书过期、则连接将停止工作、复制将处于待定状态、直到证书更新为止。

6. 输入当前已登录的网格的配置密码短语。
7. 选择*保存并测试*。

   此时将生成证书并测试连接。如果连接有效、则会显示一条成功消息、新连接将列在Grid Federation页面上。连接状态*将为*已连接。

   如果出现错误消息、请解决所有问题。请参阅。 "对网格联合错误进行故障排除"

8. 转到第一个网格上的"网格联合"页面并刷新浏览器。确认*连接状态*现在为*已连接*。
9. 建立连接后、安全地删除验证文件的所有副本。

   如果编辑此连接、则会创建一个新的验证文件。无法重复使用原始文件。

完成后

- 查看的注意事项"管理允许的租户"。
- "创建一个或多个新租户帐户"，分配*使用网格联合连接*权限，然后选择新连接。
- "管理连接"根据需要。您可以编辑连接值、测试连接、轮换连接证书或删除连接。
- "监控连接"作为常规StorageGRID监控活动的一部分。
- "排除连接故障"，包括解决与帐户同步和跨网格复制相关的任何警报和错误。

在 **StorageGRID** 中自动化网格联合连接

在安装和配置两个或多个运行 12.1 或更高版本的 StorageGRID 系统后，您可以使用 `manage-grid-federation.py` Python 脚本和 JSON 配置文件自动创建、编辑和维护网格联合连接。

开始之前

- 所有网格均运行StorageGRID 12.1或更高版本。
- 如果在任何网格上启用了单点登录 (SSO)，则表示已将其禁用。
- 您有一台安装了 Python 3.6 或更高版本的 Linux 计算机。
- 您从安装存档中知道以下文件的位置：

文件名	说明
manage-grid-federation.py	用于自动化网格联合连接管理的 Python 脚本
manage-grid-federation.sample.json	用于脚本的配置文件示例

- 您已创建 `manage-grid-federation.json`配置文件。要创建此文件，您可以修改示例配置文件，`manage-grid-federation.sample.json`。

> 将 `manage-grid-federation.json`配置文件中的网格管理员密码和配置密码存储在安全位置。如果文件中省略了凭据，脚本将以交互方式提示输入凭据。您还应将修改后的配置文件的备份存储在安全位置。

配置文件字段

JSON 配置文件是一个对象数组。每个对象表示一个网格，并支持以下字段：

字段	必填	说明
主机名	是	网格的管理节点主机名或 IP 地址
`grid_name`	是	网格的显示名称（最多 12 个字符）
用户名	否	网格管理员用户名（如果省略，则交互式提示）
`password`	否	网格管理员密码（如果省略，则交互式提示）
密码短语	否	配置密码短语（如果省略，则以交互方式提示）
`ca_bundle`	否	用于 SSL 验证的自定义 CA 证书捆绑包的路径
`region`	否	全局命名空间连接所需的默认 S3 区域
`CNAME`	否	全局命名空间连接所需的 CNAME
`globalEndpoint`	否	所需的全局命名空间端点

> 如果配置任何全局命名空间字段（(`region`、 `CNAME`、 `globalEndpoint`），则必须为每个网格提供所有三个字段。确保区域和 CNAME 在各网格中唯一，且所有网格的 `globalEndpoint` 值相同。

关于此任务

您可以使用 `manage-grid-federation.py` Python 脚本和 `manage-grid-federation.json`配置文件来自动化网格联合连接管理。该脚本执行以下操作：

- 使用 Grid Management API 对每个网格进行身份验证
- 验证所有网格是否正在运行 StorageGRID 12.1 或更高版本
- 验证是否在每个网格上禁用了单点登录
- 检索现有网格联合连接和 S3 配置
- 配置后更新 S3 区域、CNAME 和全局命名空间端点设置
- 为尚未连接的任何网格对创建新的网格联合连接

- 显示名称或全局命名空间设置更改时编辑现有连接
- 显示所有连接及其状态的摘要

您还可以直接使用 Grid Manager UI 或 Grid Management API 管理网格联合连接。

步骤

1. 登录到用于运行 Python 脚本的 Linux 计算机。
2. 更改为包含脚本的目录。

   例如：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   其中 **platform** 为 `debs`、 `rpms`或 `vsphere`。

3. 运行 Python 脚本并使用您创建的配置文件。

   例如：

   ```
   ./manage-grid-federation.py -i manage-grid-federation.json
   ```

   可以使用以下命令行选项：

选项	默认	说明
`-i, --input-json-file`	（必填）	包含网格列表的 JSON 配置文件的路径
`-b, --base-port`	23001	新网格联盟连接的起始端口号
`--no-verify-ssl`	SSL 验证已启用	禁用本地到网格连接的 SSL 证书验证

编辑现有连接

如果脚本检测到现有连接需要更改（例如，由于网格显示名称已更改或需要更新全局命名空间设置），它将在继续操作之前显示建议编辑的摘要并提示确认。

当启用了全局命名空间的网格上需要 S3 配置更新(`region`、 `CNAME`或 `globalEndpoint`）时，脚本必须暂时禁用全局命名空间以应用更改。在此情况下，确认提示将警告临时路由中断：

```
*** Global Namespace Disable Required ***
Global Namespace must be disabled to update region/CNAME/globalEndpoint
settings.
Routing requests will not work until Global Namespace is re-enabled.
Grids requiring S3 updates: grid1.example.com, grid2.example.com
Proceed with these edits and the temporary routing outage? [y/N]:
```

在 S3 配置更新期间，全局命名空间将暂时禁用，此时全局命名空间路由请求将无法正常工作。请在维护窗口期间执行此操作。

完成后

当脚本显示类似于以下内容的确认摘要时，您的网格联合连接即已建立和配置完成：

```
===== Newly Established Connections =====
 • Grid-A and Grid-B — grid-a.example.com and grid-b.example.com on port
23001

Total new connections: 1

===== All Grid-Federation Connections =====
  Name               Source                Target                Port
Status    Global Namespace
  ----------------  --------------------  --------------------  -----
--------  -----------------
  Grid-A and Grid-B grid-a.example.com    grid-b.example.com    23001  new
enabled

Total connections listed: 1

===== Grid S3 Configuration Summary =====
 grid-a.example.com:
    Default Region: us-east-1
    CNAME: s3-a.example.com
    Global namespace endpoint: gn.example.com
 grid-b.example.com:
    Default Region: us-west-1
    CNAME: s3-b.example.com
    Global namespace endpoint: gn.example.com
```

退出状态

代码	说明
0	脚本已成功完成
1	验证失败或网格 API 调用返回错误（检查日志输出）

如果任何连接失败，脚本将继续处理剩余对，并在输出的"失败的连接"部分报告所有失败。在重新运行脚本之前，请查看错误消息并解决任何问题。

了解网格联盟的全局命名空间

全局命名空间允许租户跨多个 StorageGRID 系统访问存储桶。当在网格联合连接上启用全

局命名空间时，可以将针对全局命名空间端点的 S3 CreateBucket 和 ListBuckets 请求发送到任何网格的负载均衡器端点，并根据请求中的签名区域自动路由到正确的网格。

什么是全局命名空间?

全局命名空间允许租户跨多个 StorageGRID 系统访问存储桶。当在网格联合连接上启用全局命名空间时，可以将针对全局命名空间端点的 S3 CreateBucket 和 ListBuckets 请求发送到任何网格的负载均衡器端点，并根据请求中的签名区域自动路由到正确的网格。

> 您应该设置 DNS 解析器，以执行存储桶 URL 到特定网格的 DNS 映射。根据需要，请咨询您的网络管理员，以确保 DNS 解析器设置正确。请参阅 "配置DNS解析"。

StorageGRID 不会在全局命名空间中跨网格强制使用唯一的存储桶名称，因此具有相同名称的存储桶可以存在于不同的网格中。请求中的签名区域用于确定哪个网格拥有该存储桶并应接收该请求。

例如，如果网格 A 使用区域 `us-east-1`，而网格 B 使用区域 `us-west-1`，则发送到具有该区域 `us-west-1`的任何网格的 CreateBucket 请求将自动路由到网格 B。

有关网格联合的详细信息，请参阅 "什么是网格联合？ "。

全局命名空间示例

网格 **1**

- 默认区域： `region-1`
- 默认 CNAME： `s3.region-1.company.com`
- 全局端点： `s3.company.com`

网格 **2**

- 默认区域： `region-2`
- 默认 CNAME： `s3.region-2.company.com`
- 全局端点： `s3.company.com`

Grid 3

- 默认区域： `region-3`
- 默认 CNAME： `s3.region-3.company.com`
- 全局端点： `s3.company.com`

CreateBucket 和 **ListBuckets** 操作

如果创建存储桶 (`bucket123`）时使用签名区域 `region-2` 并以全局端点 `s3.company.com` 为目标，则接收到请求的任何网格都将在 Grid 2 上创建存储桶。

特定于存储桶和一般对象操作

在给定网格上创建存储桶后，DNS 解析器会将存储桶 URL 解析为存储桶和网格 CNAME。

在 上面的示例 中，DNS 解析器应将 `bucket123.s3.company.com` 解析为

`bucket123.s3.grid3.company.com`（存储桶和网格的 CNAME）。换句话说，所有请求都直接发送到该网格，而无需额外的路由。

示例

`PutObject to bucket123.s3.company.com` 解析为 `bucket123.s3.grid3.company.com`

全局命名空间的 S3 行为

全局命名空间完全配置后，将应用以下 S3 行为。

区域强制执行

对全局命名空间端点的所有 S3 请求（"CreateBucket" 和 "List桶" 除外）都要求 V4 身份验证标头中的签名区域与网格的默认区域匹配。

- 如果签名区域不匹配，则请求将被拒绝，并显示以下错误：

```
An error occurred (AuthorizationHeaderMalformed) when calling the
<operation> operation: The authorization header is malformed; the region
'<signing-region>' is wrong; expecting '<grid-default-region>'
```

- 区域强制适用于网格上的所有存储桶，包括启用全局命名空间之前创建的存储桶。
- 区域强制执行仅适用于 V4 身份验证请求。匿名和 V2 请求不受区域强制执行约束。

CreateBucket 路由

CreateBucket 发送到全局命名空间端点(`s3.company.com`）的请求可以定向到任何网格的负载均衡器端点。请求将自动路由到其默认区域与请求中的签名区域匹配的网格。

例如：

- 网格A有默认区域 `us-east-1`，网格B有默认区域 `us-west-1`。
- 客户端向 `s3.company.com`发送 `CreateBucket` 请求，签名区域为 `us-west-1`。
- 轮询 DNS 将请求定向到 Grid A。
- 网格 A 将请求路由到网格 B。
- 该存储桶在网格 B 上创建。

有关 CreateBucket 的其他注意事项：

- `LocationConstraint` 元素可以设置为网格的任何默认或非默认区域。这只会影响 ILM 策略，而不会影响哪个网格创建存储桶（与 AWS 使用 `us-east-1` 的行为不同）。
- 请求中的签名区域确定哪个网格创建存储桶（签名区域必须与目标网格的默认区域相匹配）。
- 支持预先签名的 V4 请求。
- 全局命名空间路由不支持匿名和 V2 请求。

ListBuckets 路由

ListBuckets 发送到全局命名空间端点的请求的路由方式与 CreateBucket 请求类似，使用签名区域来确定正确的网格。

HEAD Bucket 和 ListBuckets 响应均不包含网格的默认区域。默认区域由签名区域隐含，签名区域强制与网格的默认区域匹配。

帐户和访问密钥管理

租户帐户和 S3 访问密钥可以使用 "帐户同步" 在所有网格之间进行同步，但当每个网格都有自己的单独访问密钥集时，全局命名空间也可以使用。如果使用单独的访问密钥，请确保 S3 客户端在向每个网格发送请求时使用正确的访问密钥。

下一步是什么?

现在，您已准备就绪 "配置全局命名空间"。

配置网格联盟的全局命名空间

配置全局命名空间，以允许租户访问跨多个 StorageGRID 系统的存储桶。

有关全局命名空间的详细信息，请参阅 "了解网格联盟的全局命名空间"。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到每个网格上的 Grid Manager。
- 每个网格都有 "root访问权限"。
- 您已查看网格联盟连接的 "注意事项和要求"。

配置全局命名空间的要求

- 全局命名空间中的所有网格必须在每对网格之间启用全局命名空间的网格联合连接。
- 可以参与单个全局命名空间的网格数上限为 11 个（本地网格和 10 个远程网格）。

> 10 网格限制受 StorageGRID 部署支持的网格联合连接的最大总数限制。总连接限制适用于部署中的*所有*网格联合连接，包括未启用全局命名空间的连接，因此您必须确保完全连接的全局命名空间和任何其他网格联合连接一起不超过此总限制。

- S3 客户端必须使用签名版本 4 (SigV4) 身份验证。全局命名空间路由操作不支持匿名和签名版本 2 请求。
  - 正常签名请求的指定方式如 "验证请求：使用授权标头（AWS Signature Version 4）"所述。
  - 预签名请求的指定方式如 "验证请求：使用查询参数（AWS Signature Version 4）"所述。

所需连接数

在全局命名空间中，必须连接每对网格。所需的连接数量取决于网格数量：

网格数	所需连接数
2	1
3	3
4	6
5	10
n	*n* × (*n* − 1) / 2

步骤 **1**：为每个网格设置唯一的默认区域

全局命名空间中的每个网格必须具有唯一的默认区域。默认区域标识拥有存储桶的网格。

CreateBucket 和 ListBuckets 请求基于此区域进行路由，所有其他请求必须与其发送到的默认区域匹配。

有关详细信息，请参阅 "配置 S3 区域"。

步骤

1. 在每个网格上"将默认区域设置为唯一值"。例如，将 Grid A 设置为 `us-east-1`，将 Grid B 设置为 `us-west-1`。

> 出于 ILM 策略的目的，您仍然可以使用非默认区域，这些区域通过 `LocationConstraint` 元素在 "CreateBucket 请求" 中设置。非默认区域不会在全局命名空间中跨网格验证唯一性。

2. 对全局命名空间中的每个网格重复此操作。每个网格必须具有不同的默认区域。
3. 根据需要设置更多区域。

步骤 **2**：配置 **S3** 全局命名空间设置

在全局命名空间的每个网格上，添加两个 S3 端点域名：

- 所有网格上相同的全局命名空间端点
- 网格的唯一 CNAME

您将配置外部 DNS，以便全局命名空间端点解析为一个或多个网格，并且唯一的 CNAME 端点解析为特定网格。

> 必须配置默认区域才能配置 S3 全局命名空间设置。启用全局命名空间设置后，如果 S3 请求未指定正确的区域，则请求将失败。所有 S3 请求都需要使用网格的默认区域进行签名。

步骤

1. 在每个网格上，选择*配置* > 网络 > **S3** 端点域名 > 域名。
2. 添加所有网格上相同的全局命名空间端点域名。例如： `s3.example.com`。
3. 为网格添加唯一的 CNAME。例如， `s3.company.com`。

4. 选择 * 保存 * 。
5. 选择*全局命名空间设置*。
   a. 选择全局命名空间端点。
   b. 选择网格的唯一 CNAME 域名。
6. 选择 * 保存 * 。
7. 确保客户端使用的服务器证书包括新的 S3 端点域名。
   - 如果客户端连接到使用自己的证书的负载平衡器端点，则"更新与此端点关联的证书"。
   - 如果客户端连接到使用全局S3 API证书的负载平衡器端点或直接连接到存储节点，"更新全局S3 API证书"。
8. 对全局命名空间中的每个网格重复这些步骤。

有关详细信息，请参阅 "配置S3端点域名"。

步骤 3：创建已启用全局命名空间的网格联合连接

在所有网格上配置 S3 端点域名和默认区域后，可以创建启用全局命名空间的网格联合连接。

关于此任务

当您创建网格联合连接并启用全局命名空间时，全局命名空间端点、CNAME 和默认区域字段将使用您在前面步骤中配置的值自动填充。如果未正确设置这些字段，Grid Manager 将阻止启用全局命名空间。

> 创建具有全局命名空间的网格联合连接后，无法更改该连接中网格的全局命名空间端点、CNAME 和默认区域。

步骤

1. 在第一个网格上，按照 "创建网格联合连接" 中所述的步骤进行操作。
2. 输入连接详细信息时，选择 启用全局命名空间。

   全局命名空间端点、CNAME 和默认区域的字段将自动填充您在前面的步骤中配置的值。如果任何值缺失或无效，则在解决问题之前无法启用全局命名空间。

3. 通过下载验证文件并将其上传到另一个网格来完成连接。
4. 对全局命名空间中的每对网格重复上述步骤。

   例如，使用 3 个网格，您需要 3 个连接（网格 A–网格 B、网格 A–网格 C、网格 B–网格 C）。使用 4 个网格，您需要 6 个连接。全局命名空间中最多可包含 10 个网格。请参阅 所需连接数。

步骤 4：配置负载均衡器端点

"配置负载平衡器端点" 全局命名空间中的每个网格。对这些端点中的每个端点使用相同的端口。

> 在配置 DNS 解析之前，请确保配置负载均衡器端点。

第 5 步：配置 DNS 解析

StorageGRID 不为全局命名空间提供内置 DNS 解析器。您必须配置外部 DNS 基础设施，以将 S3 请求路由到正确的网格。

您的 DNS 解析器应：

1. 将全局命名空间端点（例如， `s3.example.com`）解析为一个或多个网格的负载均衡器端点，通常使用轮询 DNS。
2. 将每个网格的唯一 CNAME（例如， `s3.grid-a.example.com`）解析为该特定网格的负载均衡器端点。
3. 对于虚拟托管风格的存储桶请求（例如 *`bucket`*`.s3.example.com`），请使用组织的路由策略将存储桶名称映射到相应网格的 CNAME。

   StorageGRID 不提供基于 DNS 的机制来发现哪个网格拥有存储桶。如果您需要基于存储桶所有权的自动路由，请使用"租户管理 API"发出 ListBucket 请求以返回存储桶 UUID。维护从存储桶 UUID 到网格的内部映射。您的外部 DNS 应使用该映射，而不是直接查询 StorageGRID。

相关信息

- "什么是网格联合？"
- "创建网格联合连接"
- "配置S3端点域名"
- "管理网格联合连接"

管理 **StorageGRID** 网格联合连接

管理StorageGRID 系统之间的网格联合连接包括编辑连接详细信息、轮换证书、删除租户权限以及删除未使用的连接。

开始之前

- 您已使用登录到任一网格上的网格管理器"支持的 Web 浏览器"。
- 您拥有已登录到的网格的"root访问权限"。

编辑网格联合连接

您可以通过登录到连接中任一网格上的主管理节点来编辑网格联合连接。更改第一个网格后、必须下载新的验证文件并将其上传到另一个网格。

> 在编辑连接时，帐户同步或跨网格复制请求将继续使用现有的连接设置。每次必须编辑一个连接，并为每个连接将一个验证文件上传到远程网格。编辑将在上传到远程网格后应用。

开始编辑连接

步骤

1. 从任一网格上的主管理节点登录到网格管理器。
2. 选择*节点*并确认系统中的所有其他管理节点都在线。

编辑网格联合连接时、StorageGRID 会尝试在第一个网格的所有管理节点上保存"候选配置"文件。如果无法将此文件保存到所有管理节点，则在选择*保存并测试*时会显示一条警告消息。

3. 选择*配置* > 系统 > 网格联合。
4. 使用“网格联合”页面或特定连接的详细信息页面上的*Actions*菜单编辑连接详细信息。请参见"创建网格联合连接"了解要输入的内容。

   操作菜单

   a. 选择连接的单选按钮。
   b. 选择*Actions*>*Edit*。
   c. 输入新信息。

   详细信息页面

   a. 选择连接名称以显示其详细信息。
   b. 选择 * 编辑 * 。
   c. 输入新信息。

5. 输入要登录到的网格的配置密码短语。
6. 选择*保存并继续*。

   新值将被保存、但在将新验证文件上传到另一个网格之前、这些值不会应用于连接。

7. 选择*下载验证文件*。

   要稍后下载此文件、请转到连接的详细信息页面。

8. 找到下载的文件(*connection-name*.grid-federation，并将其保存到安全的位置。

   验证文件包含机密信息、必须安全地存储和传输。

9. 选择*Close*(关闭*)返回到Grid Federation (网格联合)页面。
10. 确认*连接状态*为*待定编辑*。

    如果在开始编辑连接时连接状态不是*conned*，则不会更改为*Pending edit*。

11. 将文件提供 `*connection-name*.grid-federation`给另一个网格的网格管理员。

完成对连接的编辑

通过将验证文件上传到其他网格来完成对连接的编辑。

步骤

1. 从主管理节点登录到网格管理器。

2. 选择*配置* > 系统 > 网格联合。
3. 选择*上传验证文件*以访问上传页面。
4. 选择*上传验证文件*。然后、浏览并选择从第一个网格下载的文件。
5. 输入当前已登录的网格的配置密码短语。
6. 选择*保存并测试*。

   如果可以使用编辑的值建立连接、则会显示一条成功消息。否则、将显示错误消息。查看消息并解决任何问题。

7. 关闭向导以返回到"网格联盟"页面。
8. 确认*连接状态*为*已连接*。
9. 转到第一个网格上的"网格联合"页面并刷新浏览器。确认*连接状态*现在为*已连接*。
10. 建立连接后、安全地删除验证文件的所有副本。

[[test_grid _ FED_CONNECTION]]测试网格联合连接

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 使用“网格联合”页面或详细信息页面上的*Actions*菜单测试特定连接。

   操作菜单

   a. 选择连接的单选按钮。
   b. 选择*Actions*>*Test*。

   详细信息页面

   a. 选择连接名称以显示其详细信息。
   b. 选择 * 测试连接 * 。

4. 查看连接状态：

连接状态	说明
已连接	两个网格均已连接并正常通信。
错误	连接处于错误状态。例如、证书已过期或配置值不再有效。
待编辑	您已编辑此网格上的连接、但此连接仍在使用现有配置。要完成编辑、请将新验证文件上传到另一个网格。
正在等待连接	您已在此网格上配置连接、但在另一网格上连接尚未完成。从此网格下载验证文件并将其上传到另一个网格。

连接状态	说明
未知	连接处于未知状态、可能是由于网络问题描述 或脱机节点。

5. 如果连接状态为*Error*，请解决所有问题。然后，再次选择*测试连接*以确认问题描述 已修复。

[[rotate_grid _ FED_certificates]]旋转连接证书

每个网格联合连接都使用四个自动生成的SSL证书来保护此连接的安全。当每个网格的两个证书接近其到期日期时，“网格联合证书到期”警报将提醒您轮换证书。

如果连接任一端的证书过期、则连接将停止工作、复制将处于待定状态、直到证书更新为止。

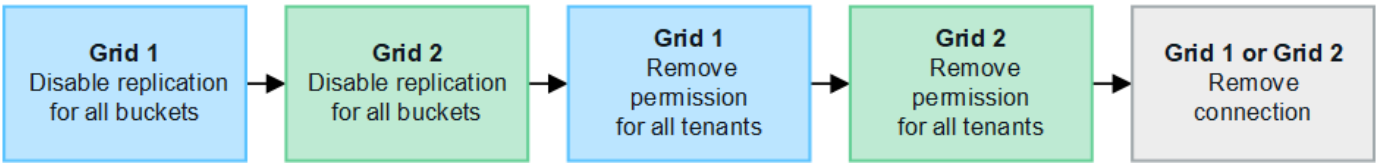
步骤

1. 从任一网格上的主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 从网格联盟页面上的任一选项卡中、选择连接名称以显示其详细信息。
4. 选择*证书*选项卡。
5. 选择*旋转证书*。
6. 指定新证书的有效天数。
7. 输入要登录到的网格的配置密码短语。
8. 选择*旋转证书*。
9. 根据需要、对连接中的另一个网格重复上述步骤。

   通常、对连接两端的证书使用相同天数。

[[remove_grid _ FED_CONNECTION]]删除网格联合连接

您可以从连接中的任一网格删除网格联合连接。如图所示、您必须在两个网格上执行前提条件步骤、以确认任一网格上的任何租户均未使用此连接。



删除连接之前、请注意以下事项：

- 删除连接不会删除已在网格之间复制的任何项目。例如、删除租户的权限后、不会从任一网格中删除存在于两个网格上的租户用户、组和对象。如果要删除这些项目、则必须手动将其从两个网格中删除。
- 删除连接后、任何正在等待复制的对象(已装载但尚未复制到另一个网格)的复制将永久失败。

对所有租户分段禁用复制

步骤

1. 从任一网格开始、从主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 选择连接名称以显示其详细信息。
4. 在*允许的租户*选项卡上、确定是否有任何租户正在使用此连接。
5. 如果列出了任何租户、则指示所有租户针对连接中两个网格上的所有分段执行"禁用跨网格复制"。

> 如果任何租户分段已启用跨网格复制、则无法删除*使用网格联合连接*权限。每个租户帐户都必须在两个网格上为其分段禁用跨网格复制。

删除每个租户的权限

对所有租户分段禁用跨网格复制后、从两个网格上的所有租户中删除*使用网格联合权限*。

步骤

1. 选择*配置* > 系统 > 网格联合。
2. 选择连接名称以显示其详细信息。
3. 对于*允许的租户*选项卡上的每个租户、从每个租户中删除*使用网格联合连接*权限。请参阅。 "管理允许的租户"
4. 对其他网格上允许的租户重复上述步骤。

断开连接

步骤

1. 如果任一网格上没有租户正在使用此连接，请选择*Remove*。
2. 查看确认消息，然后选择*Remove*。
   - 如果可以删除连接、则会显示一条成功消息。现在、两个网格中的网格联合连接均已删除。
   - 如果无法删除连接(例如、连接仍在使用中或出现连接错误)、则会显示一条错误消息。您可以执行以下任一操作：
     - 解决此错误(建议)。请参阅。 "对网格联合错误进行故障排除"
     - 强制断开连接。请参见下一节。

强制删除网格联合连接

如有必要，您可以强制删除未处于*已连接*状态的连接。

强制删除仅会从本地网格中删除此连接。要完全断开连接、请在两个滤线栅上执行相同的步骤。

步骤

1. 从确认对话框中，选择*Force remove*。

   此时将显示一条成功消息。无法再使用此网格联合连接。但是、租户分段可能仍会启用跨网格复制、并且某些对象副本可能已在连接中的网格之间进行复制。

2. 从连接中的另一个网格、从主管理节点登录到网格管理器。

3. 选择*配置* > 系统 > 网格联合。
4. 选择连接名称以显示其详细信息。
5. 选择*Remove*和*Yes*。
6. 选择*Force remove*以从该网格中删除连接。

管理 **StorageGRID** 网格联盟的允许租户

您可以允许 S3 租户帐户在多个 StorageGRID 系统之间使用一个或多个网格联合连接。当允许租户使用连接时，需要执行特殊步骤来编辑租户详细信息或永久删除租户使用连接的权限。

开始之前

- 您已使用登录到任一网格上的网格管理器"支持的 Web 浏览器"。
- 您拥有已登录到的网格的"root访问权限"。
- 两个网格之间存在"已创建网格联合连接"。
- 您已查看 "帐户同步" 和 "跨网格复制" 的工作流程。
- 根据需要，您已经为连接中的两个网格配置了单点登录 (SSO) 或身份联合。请参阅 "了解网格联盟的帐户同步"。

创建允许的租户

如果要允许新的或现有租户帐户使用网格联合连接进行帐户同步和跨网格复制，请按照"创建新的S3租户"或"编辑租户帐户"的一般说明进行操作，并注意以下事项：

- 您可以从连接中的任一网格创建租户。创建租户的网格是_租 户的源网格_。
- 连接状态必须为*已连接*。
- 在创建或编辑租户以启用*使用网格联合连接*权限并将其保存在第一个网格上后、相同的租户将自动复制到另一个网格。复制租户的网格是_租 户的目标网格_。
- 两个网格上的租户将具有相同的20位数帐户ID、名称、问题描述 、配额和权限。您也可以使用*问题描述 *字段帮助确定哪个是源租户、哪个是目标租户。例如、对于在网格1上创建的租户、如果该租户复制到网格2、则也会显示此问题描述： "This租户was created on Grid 1"(此租户已在网格1上创建)。
- 出于安全原因、本地root用户的密码不会复制到目标网格。

> 本地root用户登录到目标网格上的复制租户之前，该网格的网格管理员必须"更改本地root用户的密码"。

- 在两个网格上都有新租户或编辑过的租户后、租户用户可以执行以下操作：
  - 从任何连接的网格中，创建组和本地用户，这些组和本地用户会自动同步到所有其他连接的网格。请参阅 "同步租户组和用户"。
  - 为本地用户创建新的 S3 访问密钥，当为租户启用访问密钥同步时，这些密钥会自动同步到其他连接的网格。

> 联合用户的 S3 访问密钥在创建时从源克隆到目标一次。如果删除这些 S3 访问密钥，则这些更改不会同步到其他网格。您必须手动删除其他网格上的 S3 访问密钥。

- 在连接中的两个网格上创建相同的分段、并在一个方向或两个方向上启用跨网格复制。请参阅。 "管理跨网格复制"

查看允许的租户

您可以查看允许使用网格联盟连接的租户的详细信息。

步骤

1. 选择*租户*。
2. 从租户页面中、选择租户名称以查看租户详细信息页面。
3. （可选）选择 **Grid federation** 选项卡以 "监控网格联合连接"。

编辑允许的租户

如果您需要编辑具有*使用网格联合连接*权限的租户、请按照的常规说明进行操作"编辑租户帐户"、并注意以下事项：

- 如果租户具有*使用网格联合连接*权限：
- 您可以从连接中的任何网格编辑租户详细信息。对租户级别设置（如名称、描述或配额）以及本地用户拥有的组、本地用户和 S3 访问密钥的更改将自动同步到所有连接的网格。
- 您只能在源网格上更改*允许的网格联合连接*。
- 您可以添加新的网格联合连接。

> 您不能取消选择任何现有连接。要删除连接，请转到租户的详细信息页面，选择 **Grid federation** 选项卡，然后删除权限。

- 如果在编辑租户时添加新连接，则此租户将复制到由该新连接指定的远程网格。

删除允许的租户

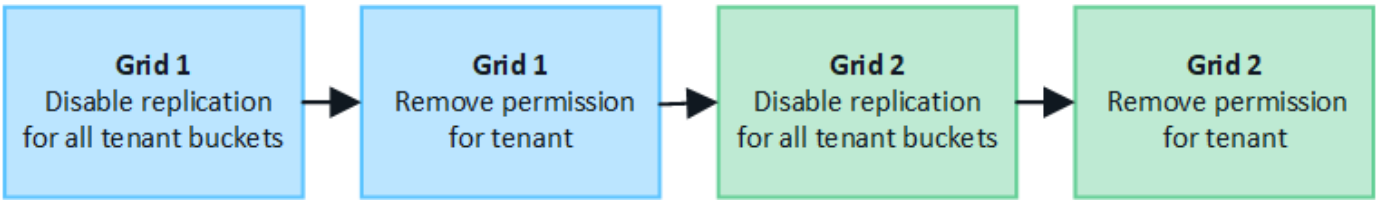
> 如果从源网格中删除原始租户或从目标网格中删除同步的租户，则会从所有网格中删除该租户，因此无法再使用该帐户。

如果您需要删除具有*使用网格联合连接*权限的租户、请按照的常规说明进行操作"删除租户帐户"、并注意以下事项：

- 在删除源网格上的租户之前，必须删除源网格上帐户的所有存储桶。
- 在删除目标网格上的同步租户之前，必须删除目标网格上帐户的所有存储桶。
- 如果删除原始租户或同步租户，则无法再将帐户用于跨网格复制。
- 如果要删除源网格或任何目标网格上的原始租户，则还会删除已同步到目标网格的租户组、用户和密钥。

删除使用网格联合连接权限

要防止租户使用网格联合连接、您必须删除*使用网格联合连接*权限。



在删除租户使用网格联合连接的权限之前、请注意以下事项：

- 如果租户的任何分段已启用跨网格复制、则无法删除*使用网格联合连接*权限。租户帐户必须先为其所有分段禁用跨网格复制。
- 删除*使用网格联合连接*权限不会删除已在网格之间复制的任何项目。例如、删除租户的权限后、不会从任一网格中删除存在于两个网格上的任何租户用户、组和对象。如果要删除这些项目、则必须手动将其从两个网格中删除。
- 如果要使用相同的网格联合连接重新启用此权限、请先删除目标网格上的此租户；否则、重新启用此权限将导致出现错误。

重新启用*使用网格联合连接*权限将使本地网格成为源网格，并触发同步到选定网格联合连接指定的远程网格。如果远程网格上已存在租户帐户，则同步将导致冲突错误。

开始之前

- 您正在使用"支持的 Web 浏览器"。
- 两个网格都有"root访问权限"。

禁用租户分段复制

首先、对所有租户分段禁用跨网格复制。

步骤

1. 从任一网格开始、从主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 选择连接名称以显示其详细信息。
4. 在*允许的租户*选项卡上、确定租户是否正在使用此连接。
5. 如果列出了租户、则指示其对连接中两个网格上的所有分段执行"禁用跨网格复制"。

如果任何租户分段已启用跨网格复制、则无法删除*使用网格联合连接*权限。租户必须在两个网格上为其分段禁用跨网格复制。

删除租户的权限

为租户分段禁用跨网格复制后、您可以删除租户使用网格联合连接的权限。

步骤

1. 从主管理节点登录到网格管理器。
2. 从"网格联盟"页面或"租户"页面中删除此权限。

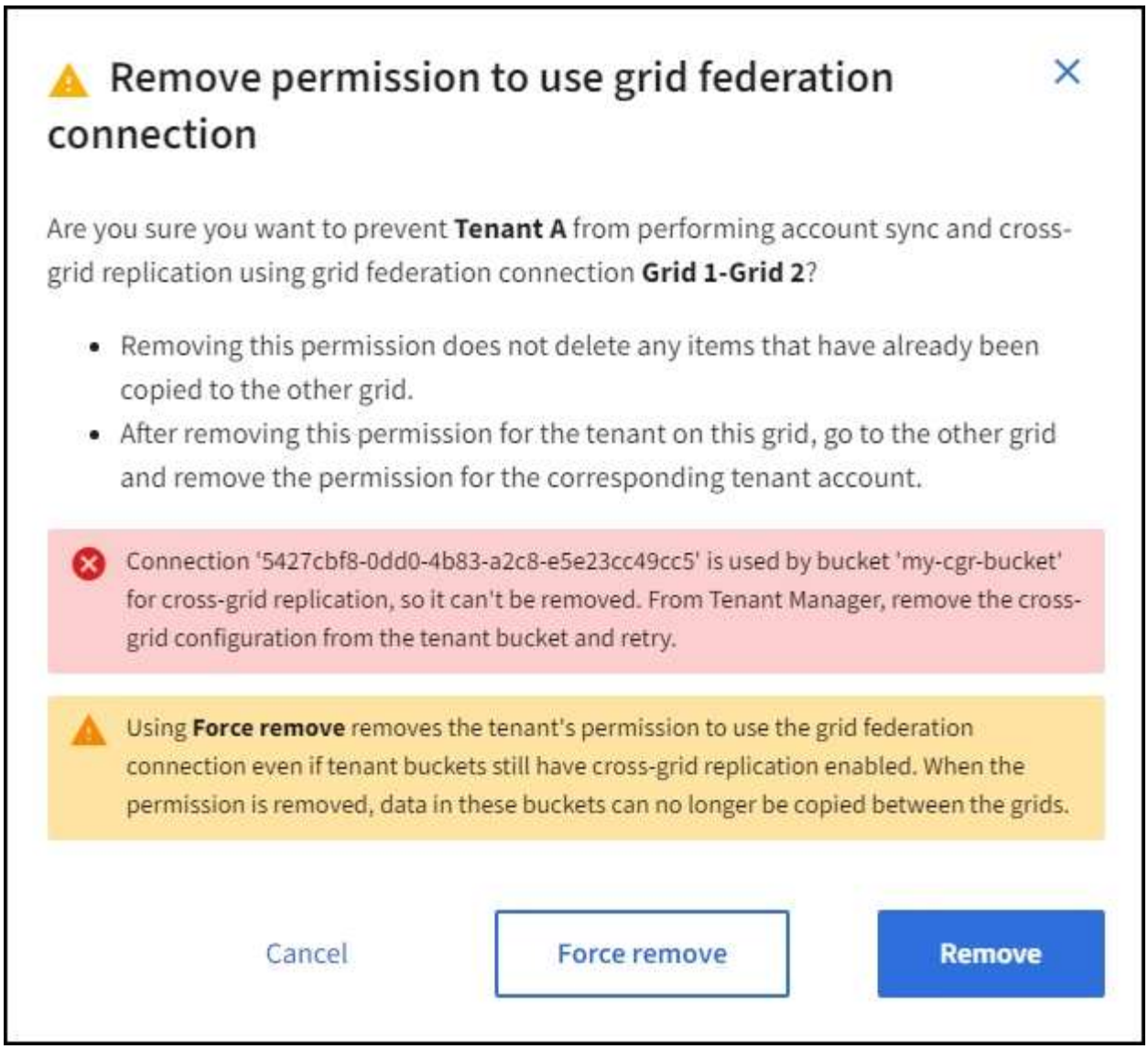
网格联合页面

a. 选择*配置* > 系统 > 网格联合。
b. 选择连接名称以显示其详细信息页面。
c. 在*允许的租户*选项卡上、选择租户的单选按钮。
d. 选择*删除权限*。

租户页面

a. 选择*租户*。
b. 选择租户的名称以显示详细信息页面。
c. 在*网格联盟*选项卡上，选择连接的单选按钮。
d. 选择*删除权限*。

3. 查看确认对话框中的警告，然后选择*Remove*。
   - 如果可以删除此权限、则会返回到详细信息页面、并显示一条成功消息。此租户无法再使用网格联合连接。
   - 如果一个或多个租户分段仍启用了跨网格复制、则会显示错误。



您可以执行以下任一操作：

- (建议。)登录到租户管理器并为租户的每个分段禁用复制。请参阅。 "管理跨网格复制"然后，重复这些步骤以删除*使用网格连接*权限。
- 强制删除权限。请参见下一节。

4. 转到另一个网格并重复这些步骤、以删除另一个网格上同一租户的权限。

强制删除权限

如有必要、您可以强制删除租户使用网格联合连接的权限、即使租户分段已启用跨网格复制也是如此。

在强制删除租户的权限之前、请注意的一般注意事项正在删除权限以及以下附加注意事项：

- 如果您强制删除*使用网格联合连接*权限，则所有正在等待复制到另一网格的对象(已加载但尚未复制)将继续被复制。为了防止这些进程中对象到达目标存储分段、您还必须删除租户对其他网格的权限。
- 删除*使用网格联合连接*权限后、插入到源存储分段中的任何对象都不会复制到目标存储分段。

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*配置* > 系统 > 网格联合。
3. 选择连接名称以显示其详细信息页面。
4. 在*允许的租户*选项卡上、选择租户的单选按钮。
5. 选择*删除权限*。
6. 查看确认对话框中的警告，然后选择*Force remove*。

   此时将显示一条成功消息。此租户无法再使用网格联合连接。

7. 根据需要、转到另一个网格并重复这些步骤、以强制删除另一个网格上同一租户帐户的权限。例如、您应在其他网格上重复这些步骤、以防止进程中对象到达目标分段。

对 **StorageGRID** 中的网格联合错误进行故障排除

您可能需要排除与网格联合连接、帐户同步和跨网格复制相关的警报和错误。

网格联合连接警报和错误

您可能会收到有关网格联盟连接的警报或遇到错误。

在进行任何更改以解析连接问题描述 后，请测试该连接以确保连接状态返回到*conn岗位*。有关说明，请参阅"管理网格联合连接"。

Grid Federation connection failure警报

问题描述

已触发*网格联合连接失败*警报。

详细信息

此警报表示网格之间的网格联合连接不起作用。

建议的操作

1. 查看两个网格的网格联合页面上的设置。确认所有值均正确无误。请参阅。 "管理网格联合连接"
2. 查看用于连接的证书。确保没有针对已过期的网格联合证书的警报、并且每个证书的详细信息有效。请参见中有关旋转连接证书的说明"管理网格联合连接"。
3. 确认两个网格中的所有管理节点和网关节点均已联机且可用。解决可能影响这些节点的所有警报、然后重试。
4. 如果您为本地或远程网格提供了完全限定域名(FQDN)、请确认DNS服务器联机且可用。有关网络连接、IP地址和DNS要求、请参见"什么是网格联合？"。

网格联合证书到期警报

问题描述

已触发*网格联合证书到期*警报。

详细信息

此警报指示一个或多个网格联合证书即将过期。

建议的操作

请参见中有关旋转连接证书的说明"管理网格联合连接"。

编辑网格联合连接时出错

问题描述

编辑网格联合连接时，如果选择*保存并测试*，则会看到以下警告消息："Ffailed to create a candidate configuration file on one or more Nides"(无法在一个或多个节点上创建候选配置文件)。

详细信息

编辑网格联合连接时、StorageGRID 会尝试在第一个网格的所有管理节点上保存"候选配置"文件。如果无法将此文件保存到所有管理节点(例如、由于某个管理节点脱机)、则会显示一条警告消息。

建议的操作

1. 从用于编辑连接的网格中，选择*节点*。
2. 确认该网格的所有管理节点均已联机。
3. 如果任何节点处于脱机状态、请将其恢复联机、然后重新尝试编辑连接。

帐户同步错误

无法登录到同步的租户帐户

问题描述

无法登录到已同步的租户帐户。租户管理器登录页面上的错误消息是"此帐户的凭据无效。请重试。"

详细信息

为租户的本地 root 用户和其他本地用户设置的密码将自动同步。但是，在登录到目标网格上的租户帐户之前，您可能需要更改目标网格上租户的本地 root 用户的密码。

建议的操作

在root用户登录到租户的目标网格之前、网格管理员必须首先登录到"更改本地root用户的密码"目标网格。

未同步创建的租户

问题描述

在创建具有*使用网格联合连接*权限的新租户后，您会看到消息"Tenant created without a sync"。

详细信息

如果连接状态更新延迟，发生原因 则可能会出现此问题描述 ，这可能会使运行状况不正常的连接显示为*conn象*。

建议的操作

1. 查看错误消息中列出的原因、并解决可能导致连接无法正常工作的任何网络或其他问题。请参阅。 网格联合连接警报和错误
2. 按照说明在中测试网格联合连接"管理网格联合连接"、以确认此问题已修复。

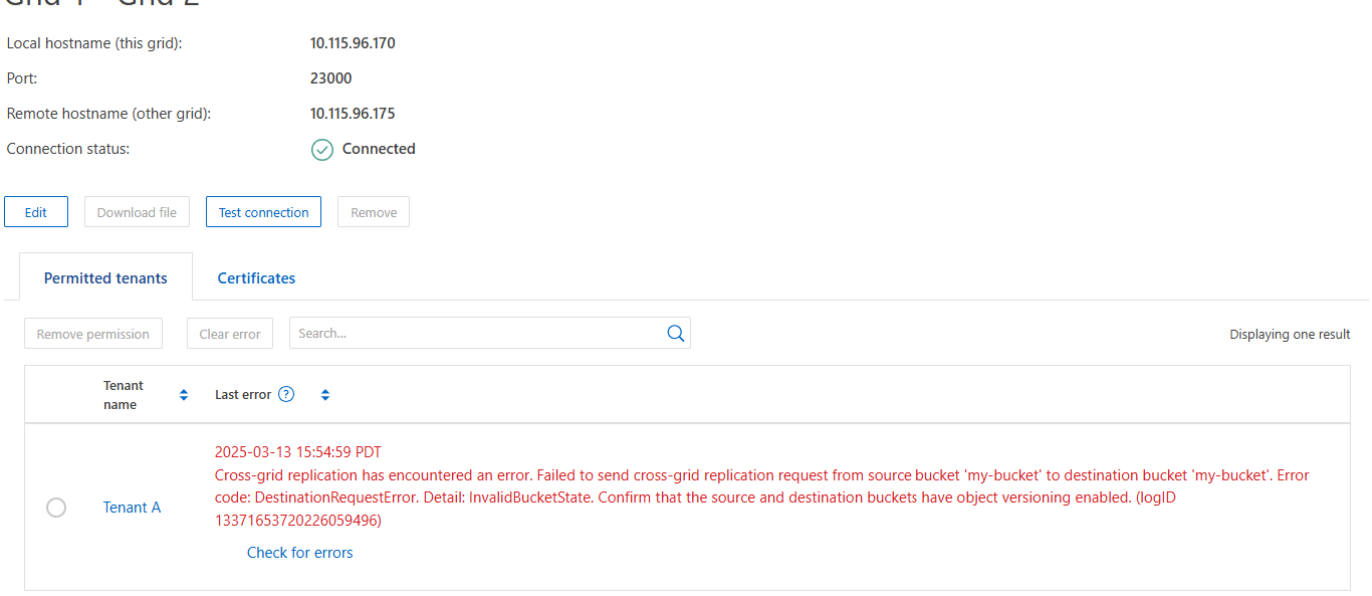
3. 从租户的源网格中，选择*租户*。
4. 找到无法同步的租户帐户。
5. 选择租户名称以显示详细信息页面。
6. 选择*重试同步*。如果错误已解决，租户帐户现在将同步到另一个网格。

跨网格复制警报和错误

为连接或租户显示的最后一个错误

问题描述

当"查看网格联合连接"(或连接时"管理允许的租户")您在连接详细信息页面的*上次错误*列中发现错误。例如：



详细信息

对于每个网格联合连接，*最后一个错误*列显示租户数据复制到另一个网格时发生的最近错误（如果有）。此列仅显示最后发生的跨网格复制错误；不会显示可能发生的先前错误。此列中的错误可能由于以下原因之一而发生：

- 未找到源对象版本。
- 未找到源存储桶。
- 已删除此目标存储分段。
- 目标存储分段已由其他帐户重新创建。
- 目标存储分段已暂停版本控制。
- 目标存储分段已由同一帐户重新创建、但现在已取消版本控制。
- 源对象的 S3 对象锁定设置不符合目标网格的租户级保留设置。
- 源对象具有 S3 对象锁定设置，并且目标存储桶上的 S3 对象锁定已禁用。

建议的操作

如果“上次错误”列中出现错误消息，请按照以下步骤操作：

1. 查看消息文本。
2. 执行任何建议的操作。

   例如，如果版本控制在目标存储桶上暂停以进行跨网格复制，请重新启用该存储桶的版本控制。或者，如果在跨网格复制的目标存储桶上禁用了 S3 对象锁定，则为该存储桶启用 S3 对象锁定。

3. 从表中选择连接或租户帐户。
4. 选择*清除错误*。
5. 选择*是*以清除消息并更新系统状态。
6. 等待5-6分钟、然后将新对象插入存储分段。确认错误信息不会再次出现。

   要确保清除错误消息、请在消息中的时间戳后至少等待5分钟、然后再输入新对象。

   清除错误后，如果在另一个存储分段中载入对象，并且该存储分段也存在错误，则可能会出现一个新的*last error*。

7. 要确定是否有任何对象因存储分段错误而无法复制，请参见"确定并重试失败的复制操作"。

跨网格复制永久故障警报

问题描述

已触发*跨网格复制永久失败*警报。

详细信息

此警报指示无法在两个网格上的分段之间复制租户对象、原因是需要用户干预才能解决。此警报通常是由源存储分段或目标存储分段的更改引起的。

建议的操作

1. 登录到触发警报的网格。
2. 转到*配置* > 系统 > 网格联合，然后找到警报中列出的连接名称。
3. 在允许的租户选项卡上、查看*上次错误*列以确定哪些租户帐户存在错误。
4. 要了解有关此故障的详细信息、请参见中的说明"监控网格联合连接"以查看跨网格复制指标。
5. 对于每个受影响的租户帐户：
   a. 请参见中的说明"监控租户活动"、确认租户未超过其在目标网格上用于跨网格复制的配额。
   b. 根据需要、增加目标网格上的租户配额、以允许保存新对象。
6. 对于每个受影响的租户、在两个网格上登录到租户管理器、以便比较存储分段列表。
7. 对于已启用跨网格复制的每个存储分段、请确认以下内容：
   - 同一租户在另一个网格上有对应的存储分段(必须使用确切名称)。
   - 这两个分段均已启用对象版本控制(不能在任一网格上暂停版本控制)。
   - 两个存储分段均未处于*删除对象：只读*状态。

8. 要确认问题已解决、请参见中的说明"监控网格联合连接"以查看跨网格复制指标、或者执行以下步骤：

   a. 返回到"网格联盟"页面。

   b. 选择受影响的租户、然后在*上次错误*列中选择*清除错误*。

   c. 选择*是*以清除消息并更新系统状态。

   d. 等待5-6分钟、然后将新对象插入存储分段。确认错误信息不会再次出现。

      要确保清除错误消息、请在消息中的时间戳后至少等待5分钟、然后再输入新对象。

   解决警报后、可能需要长达一天时间才能清除警报。

   a. 转到"确定并重试失败的复制操作"以确定未能复制到其他网格的任何对象或删除标记、并根据需要重试复制。

跨网格复制资源不可用警报

问题描述

已触发*跨网格复制资源不可用*警报。

详细信息

此警报表示跨网格复制请求处于待处理状态、因为资源不可用。例如、可能存在网络错误。

建议的操作

1. 监控警报以查看问题描述 是否自行解决。
2. 如果问题描述 仍然存在，请确定其中一个网格对于同一连接是否具有*Grid Federation connection failure*警报，或者对于某个节点是否具有*Unable to与节点*通信警报。当您解决这些警报时、可能会解决此警报。
3. 要了解有关此故障的详细信息、请参见中的说明"监控网格联合连接"以查看跨网格复制指标。
4. 如果无法解决此警报、请联系技术支持。

解决问题描述 后、跨网格复制将正常进行。

识别并重试失败的 **StorageGRID** 复制操作

解决*跨网格复制永久失败*警报后，您应确定是否有任何对象或删除标记无法复制到另一网格。然后、您可以重新创建这些对象或使用网格管理API重试复制。

*跨网格复制永久失败*警报指示无法在两个网格上的分段之间复制租户对象、原因是需要用户干预才能解决。此警报通常是由源存储分段或目标存储分段的更改引起的。有关详细信息，请参见 "对网格联合错误进行故障排除"。

确定是否有任何对象无法复制

要确定是否有任何对象或删除标记未复制到其他网格、您可以在审核日志中搜索"CGRR (跨网格复制请求)"消息。如果StorageGRID 无法将对象、多部分对象或删除标记复制到目标存储分段、则会将此消息添加到日志中。

您可以使用将结果转换为易于阅读的"Audy-讲解 工具"格式。

开始之前

- 您具有 root 访问权限。
- 您已获得 `Passwords.txt`文件。
- 您知道主管理节点的IP地址。

步骤

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

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 在audit.log中搜索CGRR消息、并使用audy-expand工具对结果进行格式化。

   例如、此命令将对过去30分钟内的所有CGRR消息进行greps、并使用audy-explast工具。

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   此命令的结果类似于此示例、其中包含六条CGRR消息的条目。在此示例中、所有跨网格复制请求均返回一个一般错误、因为无法复制对象。前三个错误用于"replicate object"操作、后三个错误用于"replicate delete marker"操作。

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

每个条目都包含以下信息：

字段	说明
CGRR跨网格复制请求	请求的名称
租户	租户的帐户ID
连接	网格联合连接的ID
操作	正在尝试的复制操作类型： • 复制对象 • 复制删除标记 • 复制多部分对象
存储分段	分段名称
对象	对象名称
version	对象的版本标识

字段	说明
错误	错误的类型。如果跨网格复制失败、则错误为"General error"。

重试失败的复制

生成对象列表并删除未复制到目标存储分段的标记并解决底层问题后、您可以通过以下两种方式之一重试复制：

- 将每个对象重新装入源存储分段。
- 使用网格管理专用API、如所述。

步骤

1. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
2. 选择*转至专用API文档*。

   标记为"专用"的StorageGRID API端点如有更改、恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

3. 在*cross-grid复制-高级*部分中，选择以下端点：

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. 选择 * 试用 * 。
5. 在*body文本框中，将*versionID*的示例条目替换为audit.log中与失败的跨网格复制请求对应的版本ID。

   请务必在字符串周围保留双引号。

6. 选择 * 执行 * 。
7. 确认服务器响应代码为*204*，表示对象或删除标记已标记为等待跨网格复制到另一网格。

   Pending表示跨网格复制请求已添加到内部队列进行处理。

监控复制重试次数

您应监控复制重试操作以确保其完成。

将对象或删除标记复制到另一个网格可能需要数小时甚至更长时间。

您可以通过以下两种方式之一监控重试操作：

- 使用S3"HeadObject"或"GetObject"请求。此响应包括StorageGRID专用的 `x-ntap-sg-cgr-replication-status` 响应标头、该标头将具有以下值之一：

网格	复制状态
源	• 已完成：复制成功。 • *pending *：对象尚未复制。 • 失败：复制失败并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

- 使用网格管理专用API、如所述。

步骤

1. 在专用API文档的*跨网格复制-高级*部分中，选择以下端点：

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. 选择 * 试用 * 。
3. 在参数部分中、输入您在请求中使用的版本ID `cross-grid-replication-retry-failed`。
4. 选择 * 执行 * 。
5. 确认服务器响应代码为*200*。
6. 查看复制状态、该状态为以下状态之一：
   - *pending *：对象尚未复制。
   - 已完成：复制成功。
   - **failer**：复制失败并出现永久故障。用户必须解决此错误。

管理安全性

管理 StorageGRID 中的安全性

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

管理加密

StorageGRID 提供了多种数据加密选项。您应"查看可用的加密方法"确定哪些符合数据保护要求。

管理证书

您可以"配置和管理服务器证书"使用HTTP连接或用于向服务器验证客户端或用户身份的客户端证书。

配置密钥管理服务器

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、您将无法访问设备上的任何数据、除非此节点可以与KMS进行通信。

> 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。

管理代理设置

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"存储代理服务器"。如果您使用HTTPS或HTTP发送AutoSupport软件包、则可以在管理节点和技术支持之间配置"管理代理服务器"。

控制防火墙

为了增强系统的安全性，您可以通过在打开或关闭特定端口来控制对StorageGRID管理节点的访问"外部防火墙"。您还可以通过配置每个节点来控制对其的网络访问"内部防火墙"。您可以阻止对除部署所需端口以外的所有端口进行访问。

查看 **StorageGRID** 加密方法

StorageGRID 提供了多种数据加密选项。您应查看可用的方法，以确定哪些方法符合数据保护要求。

下表简要总结了 StorageGRID 中可用的加密方法。

加密选项	工作原理	适用场景
网格管理器中的密钥管理服务器（ KMS ）	"配置密钥管理服务器"StorageGRID 站点和 "为此设备启用节点加密"。然后，设备节点将连接到 KMS 以请求密钥加密密钥（ Key Encryption Key ， KEK ）。此密钥用于对每个卷上的数据加密密钥（ DEK ）进行加密和解密。	安装期间启用了 * 节点加密 * 的设备节点。设备上的所有数据均可防止物理丢失或从数据中心删除。 注意：只有存储节点和服务设备才支持使用KMS管理加密密钥。
StorageGRID设备安装程序中的驱动器加密页面	如果此设备包含支持硬件加密的驱动器、您可以在安装期间设置驱动器密码短语。设置驱动器密码短语时、任何人都无法从已从系统中删除的驱动器中恢复有效数据、除非他们知道密码短语。开始安装之前，请转至*配置硬件*>*驱动器加密*以设置驱动器密码短语，该密码短语用于适用场景节点中所有StorageGRID管理的自加密驱动器。	包含自加密驱动器的设备。安全驱动器上的所有数据均可防止物理丢失或从数据中心中删除。 驱动器加密不适用于SANtricity-managed驱动器。如果您的存储设备具有自加密驱动器和SANtricity控制器、则可以在SANtricity中启用驱动器安全性。
SANtricity System Manager 中的驱动器安全性	如果为StorageGRID设备启用了驱动器安全功能、则可以使用"SANtricity 系统管理器"创建和管理安全密钥。要访问受保护驱动器上的数据，需要使用此密钥。	具有全磁盘加密(Full Disk Encryption、FD)驱动器或自加密驱动器的存储设备。安全驱动器上的所有数据均可防止物理丢失或从数据中心中删除。不能用于某些存储设备或任何服务设备。

加密选项	工作原理	适用场景
存储对象加密	您可以在网格管理器中启用该"存储对象加密"选项。启用后、在存储分段级别或对象级别未加密的任何新对象都会在数据导入期间进行加密。	新加存的S3对象数据。 现有存储对象未加密。对象元数据和其他敏感数据不会加密。
S3 存储分段加密	您可以通过问题描述a PutBucketEncryption请求为存储分段启用加密。在对象级别未加密的任何新对象都会在导入期间进行加密。	仅新载入的 S3 对象数据。 必须为存储分段指定加密。现有存储分段对象未加密。对象元数据和其他敏感数据不会加密。 "对存储分段执行的操作"
S3 对象服务器端加密（ SS3 ）	您发出S3请求来存储对象并包含 `x-amz-server-side-encryption`请求标头。	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据不会加密。 StorageGRID 负责管理密钥。 "使用服务器端加密"
使用客户提供的密钥（ SSI-C ）进行 S3 对象服务器端加密	您可以问题描述 S3 请求以存储一个对象并包含三个请求标头。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据不会加密。 密钥在 StorageGRID 之外进行管理。 "使用服务器端加密"
外部卷或数据存储库加密	如果您的部署平台支持，则可以在 StorageGRID 外部使用加密方法对整个卷或数据存储库进行加密。	所有对象数据，元数据和系统配置数据，假设每个卷或数据存储库都已加密。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。

加密选项	工作原理	适用场景
StorageGRID 外部的对象加密	在将对象数据和元数据载入 StorageGRID 之前，您可以在 StorageGRID 外部使用加密方法对这些数据和元数据进行加密。	仅限对象数据和元数据（系统配置数据不加密）。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。 "Amazon Simple Storage Service—用户指南：使用客户端加密保护数据"

使用多种加密方法

根据您的要求，您一次可以使用多种加密方法。例如：

- 您可以使用KMS保护设备节点、也可以使用SANtricity系统管理器中的驱动器安全功能对同一设备中自加密驱动器上的数据进行"双重加密"。
- 您可以使用KMS保护设备节点上的数据、也可以使用存储对象加密选项对所有对象进行加密。

如果只有一小部分对象需要加密，请考虑在存储分段或单个对象级别控制加密。启用多个级别的加密会产生额外的性能成本。

相关信息

"了解 FIPS 认证的加密选项"

管理证书

管理 **StorageGRID** 中的安全证书

安全证书是一个小型数据文件，用于在 StorageGRID 组件之间以及 StorageGRID 组件与外部系统之间创建安全可信的连接。

StorageGRID 使用两种类型的安全证书：

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

当客户端使用 HTTPS 连接到服务器时，服务器会使用包含公钥的服务器证书进行响应。客户端将服务器签名与其证书副本上的签名进行比较。如果签名匹配，客户端将使用相同的公钥与服务器开始会话。

StorageGRID 用作某些连接的服务器（例如负载平衡器端点）或其他连接的客户端（例如 CloudMirror 复制服务）。

- 默认网格 CA 证书 *

StorageGRID具有内置证书颁发机构 (CA)，可在系统安装期间生成内部 Grid CA 证书。默认情况下，使用 Grid

CA 证书来保护内部StorageGRID流量。外部证书颁发机构 (CA) 可以颁发完全符合您组织的信息安全策略的自定义证书。

在非生产环境中使用 Grid CA 证书。对于生产，请使用由外部证书颁发机构签署的自定义证书。支持但没有证书的不安全连接，但不推荐。

- 自定义CA证书不会删除内部证书；但是、自定义证书应是为验证服务器连接而指定的证书。
- 所有自定义证书都必须满足"服务器证书的系统强化准则"。
- StorageGRID 支持将 CA 中的证书捆绑到一个文件中（称为 CA 证书包）。

> StorageGRID 还包括在所有网格上相同的操作系统 CA 证书。在生产环境中，请确保指定一个由外部证书颁发机构签名的自定义证书，以替代操作系统 CA 证书。

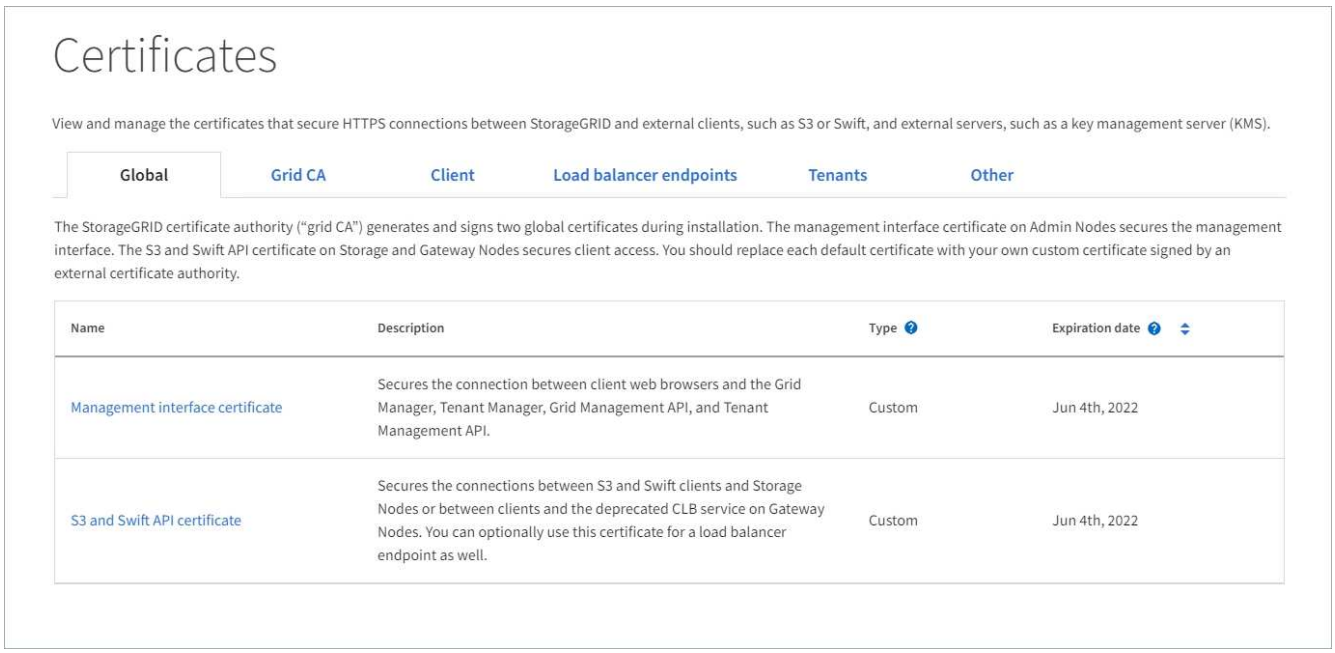
服务器和客户端证书类型的变体通过多种方式实现。在配置系统之前，您应准备好特定 StorageGRID 配置所需的所有证书。

访问安全证书

您可以在一个位置访问有关所有 StorageGRID 证书的信息，以及指向每个证书的配置工作流的链接。

步骤

1. 从网格管理器中，选择*配置* > 安全 > 证书。



2. 在证书页面上选择一个选项卡，以获取有关每个证书类别的信息并访问证书设置。如果您有，则可以访问选项卡"适当的权限"。
   - * 全局 * ： 确保从 Web 浏览器和外部 API 客户端访问 StorageGRID 的安全。
   - * 网格 CA* ： 保护内部 StorageGRID 流量的安全。
   - * 客户端 * ： 保护外部客户端与 StorageGRID Prometheus 数据库之间的连接。
   - 负载平衡器端点：保护S3客户端与StorageGRID负载平衡器之间的连接。

- * 租户 *： 保护与身份联合服务器或从平台服务端点到 S3 存储资源的连接。
- * 其他 *： 保护需要特定证书的 StorageGRID 连接。

下面介绍了每个选项卡，并提供了指向其他证书详细信息的链接。

全局

全局证书可确保从Web浏览器和外部S3 API客户端进行StorageGRID访问的安全。在安装期间，StorageGRID 证书颁发机构最初会生成两个全局证书。生产环境的最佳实践是使用由外部证书颁发机构签名的自定义证书。

- [管理接口证书]：确保客户端Web浏览器与StorageGRID管理界面的连接安全。
- S3 API证书：确保与存储节点、管理节点和网关节点的客户端API连接安全，S3客户端应用程序使用这些节点上传和下载对象数据。

有关已安装的全局证书的信息包括：

- * 名称 * ：证书名称，其中包含用于管理证书的链接。
- * 问题描述 *
- * 类型 * ：自定义或默认。+ 为了提高网格安全性，您应始终使用自定义证书。
- * 到期日期 * ：如果使用默认证书，则不会显示到期日期。

您可以：

- 将默认证书替换为由外部证书颁发机构签名的自定义证书，以提高网格安全性：
  - "替换由 StorageGRID 生成的默认管理接口证书"用于Grid Manager和租户管理器连接。
  - "替换S3 API证书"用于存储节点和负载平衡器端点(可选)连接。
- "还原默认管理接口证书"(英文)
- "还原默认S3 API证书"(英文)
- "使用脚本生成新的自签名管理接口证书"(英文)
- 复制或下载"管理接口证书"或"S3 API证书"。

网格 **CA**

网格 CA 证书由StorageGRID证书颁发机构在StorageGRID安装期间生成的可保护所有内部StorageGRID流量的安全。

证书信息包括证书到期日期和证书内容。

可以"复制或下载网格CA证书"，但不能更改。

客户端

客户端证书由外部证书颁发机构生成，用于保护外部监控工具与StorageGRID Prometheus数据库之间的连接。

证书表中的每个已配置客户端证书都有一行，用于指示此证书是否可用于 Prometheus 数据库访问以及证书到期日期。

您可以：

- "上传或生成新的客户端证书。"
- 选择一个证书名称以显示证书详细信息，您可以在其中执行以下操作：

- "更改客户端证书名称。"
- "设置 Prometheus 访问权限。"
- "上传并替换客户端证书。"
- "复制或下载客户端证书。"
- "删除客户端证书。"

◦ 选择*Actions*可快速"编辑"、"附加"或"删除"一个客户端证书。您最多可以选择 10 个客户端证书，并使用 * 操作 * > * 删除 * 一次删除这些证书。

负载平衡器端点

负载平衡器端点证书保护S3客户端与网关节点和管理节点上的StorageGRID负载平衡器服务之间的连接。

负载平衡器端点表中针对每个已配置的负载平衡器端点都有一行、用于指示此端点是使用全局S3 API证书还是自定义负载平衡器端点证书。此外，还会显示每个证书的到期日期。

对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

您可以：

◦ "查看负载平衡器端点"，包括其证书详细信息。

◦ "为 FabricPool 指定负载平衡器端点证书。"

◦ "使用全局S3 API证书"而不是生成新的负载平衡器端点证书。

租户

租户可以使用身份联合服务器证书或平台服务端点证书保护其与StorageGRID的连接。

租户表中的每个租户都有一行，用于指示每个租户是否有权使用自己的身份源或平台服务。

您可以：

◦ "选择一个租户名称以登录到租户管理器"

◦ "选择租户名称以查看租户身份联合详细信息"

◦ "选择租户名称以查看租户平台服务详细信息"

◦ "在创建端点期间指定平台服务端点证书"

其他

StorageGRID 会将其他安全证书用于特定目的。这些证书按其功能名称列出。其他安全证书包括：

◦ 云存储池证书

◦ 通过电子邮件发送警报通知证书

◦ 外部系统日志服务器证书

◦ 网格联合连接证书

◦ 身份联合证书

- 密钥管理服务器（ KMS ）证书
- 单点登录证书

信息指示函数使用的证书类型及其服务器和客户端证书的到期日期（如果适用）。选择功能名称将打开一个浏览器选项卡，您可以在此查看和编辑证书详细信息。

只有在具有的情况下，您才能查看和访问其他证书的信息"适当的权限"。

您可以：

- "为 S3 ， C2S S3 或 Azure 指定云存储池证书"
- "指定警报电子邮件通知的证书"
- "使用外部系统日志服务器的证书"
- "旋转网格联合连接证书"
- "查看和编辑身份联合证书"
- "上传密钥管理服务器（ KMS ）服务器和客户端证书"
- "手动为依赖方信任指定SSO证书"

安全证书详细信息

下面介绍了每种类型的安全证书、并提供了指向实施说明的链接。

管理接口证书

证书类型	说明	导航位置	详细信息
服务器	对客户端 Web 浏览器和 StorageGRID 管理界面之间的连接进行身份验证，使用户能够访问网格管理器和租户管理器，而不会出现安全警告。 此证书还会对网格管理 API 和租户管理 API 连接进行身份验证。 您可以使用安装期间创建的默认证书，也可以上传自定义证书。	配置 > 安全 > 证书，选择 全局 选项卡，然后选择 管理接口证书	"配置管理接口证书"

S3 API证书

证书类型	说明	导航位置	详细信息
服务器	对存储节点和负载平衡器端点的安全S3客户端连接进行身份验证(可选)。	配置 > 安全 > 证书，选择 全局 选项卡，然后选择 **S3 API** 证书	"配置S3 API证书"

网格 **CA** 证书

请参见默认网格 CA 证书问题描述。

管理员客户端证书

证书类型	说明	导航位置	详细信息
客户端	安装在每个客户端上，使 StorageGRID 能够对外部客户端访问进行身份验证。 • 允许授权的外部客户端访问 StorageGRID Prometheus 数据库。 • 允许使用外部工具安全监控 StorageGRID 。	配置 > 安全 > 证书，然后选择 客户端 选项卡	"配置客户端证书"

负载平衡器端点证书

证书类型	说明	导航位置	详细信息
服务器	对S3客户端与网关节点和管理节点上的StorageGRID负载平衡器服务之间的连接进行身份验证。您可以在配置负载平衡器端点时上传或生成负载平衡器证书。客户端应用程序在连接到StorageGRID 时使用负载平衡器证书来保存和检索对象数据。 您还可以使用自定义版本的全局S3 API证书证书对负载平衡器服务的连接进行身份验证。如果使用全局证书对负载平衡器连接进行身份验证、则无需为每个负载平衡器端点上载或生成单独的证书。 • 注意： * 用于负载平衡器身份验证的证书是正常 StorageGRID 操作期间使用量最多的证书。	配置 > 网络 > 负载均衡器端点	• "配置负载平衡器端点" • "为 FabricPool 创建负载平衡器端点"

云存储池端点证书

证书类型	说明	导航位置	详细信息
服务器	验证从 StorageGRID 云存储池到外部存储位置（如 S3 Glacier 或 Microsoft Azure Blob 存储）的连接。每种云提供商类型需要不同的证书。	• ILM * > * 存储池 *	"创建云存储池"

通过电子邮件发送警报通知证书

证书类型	说明	导航位置	详细信息
服务器和客户端	对 SMTP 电子邮件服务器与用于警报通知的 StorageGRID 之间的连接进行身份验证。 • 如果与 SMTP 服务器的通信需要传输层安全（ Transport Layer Security， TLS ），则必须指定电子邮件服务器 CA 证书。 • 仅当 SMTP 电子邮件服务器需要客户端证书进行身份验证时，才指定客户端证书。	警报 > 电子邮件设置	"为警报设置电子邮件通知"

外部系统日志服务器证书

证书类型	说明	导航位置	详细信息
服务器	对在 StorageGRID 中记录事件的外部系统日志服务器之间的 TLS 或 RELP/TLS 连接进行身份验证。 • 注： * 与外部系统日志服务器的 TCP ， RELP/TCP 和 UDP 连接不需要外部系统日志服务器证书。	配置 > 监控 > 审计和系统日志服务器	"使用外部系统日志服务器"

网格联合连接证书

证书类型	说明	导航位置	详细信息
服务器和客户端	对当前StorageGRID 系统与网格联合连接中的另一个网格之间发送的信息进行身份验证和加密。	配置 > 系统 > 电网联合	• "创建网格联合连接" • "轮换连接证书"

身份联合证书

证书类型	说明	导航位置	详细信息
服务器	对 StorageGRID 与外部身份提供程序（例如 Active Directory ， OpenLDAP 或 Oracle 目录服务器）之间的连接进行身份验证。用于身份联合，允许管理组和用户由外部系统管理。	配置 > 访问控制 > 身份联合	"使用身份联合"

密钥管理服务器（ **KMS** ）证书

证书类型	说明	导航位置	详细信息
服务器和客户端	对 StorageGRID 与外部密钥管理服务器（ KMS ）之间的连接进行身份验证，该服务器可为 StorageGRID 设备节点提供加密密钥。	配置 > 安全 > 密钥管理服务器	"添加密钥管理服务器（ KMS ）"

平台服务端点证书

证书类型	说明	导航位置	详细信息
服务器	对从 StorageGRID 平台服务到 S3 存储资源的连接进行身份验证。	• 租户管理器 * > * 存储（ S3 ） * > * 平台服务端点 *	"创建平台服务端点" "编辑平台服务端点"

单点登录（ **SSO** ）证书

证书类型	说明	导航位置	详细信息
服务器	对身份联合服务（例如 Active Directory 联合身份验证服务（ AD FS ））与用于单点登录（ SSO ）请求的 StorageGRID 之间的连接进行身份验证。	配置 > 访问控制 > 单点登录	"配置单点登录"

证书示例

示例 **1** ： 负载平衡器服务

在此示例中， StorageGRID 充当服务器。

1. 您可以在 StorageGRID 中配置负载平衡器端点并上传或生成服务器证书。
2. 您配置了与负载平衡器端点的S3客户端连接、并将同一证书上传到客户端。

3. 当客户端要保存或检索数据时，它会使用 HTTPS 连接到负载平衡器端点。
4. StorageGRID 会使用包含公有 密钥的服务器证书进行响应，并使用基于私钥的签名进行响应。
5. 客户端将服务器签名与其证书副本上的签名进行比较。如果签名匹配，客户端将使用相同的公钥开始会话。
6. 客户端将对象数据发送到 StorageGRID 。

示例 **2** ： 外部密钥管理服务器（ **KMS** ）

在此示例中， StorageGRID 充当客户端。

1. 您可以使用外部密钥管理服务器软件将 StorageGRID 配置为 KMS 客户端，并获取 CA 签名的服务器证书，公有 客户端证书以及客户端证书的专用密钥。
2. 使用网格管理器，您可以配置 KMS 服务器并上传服务器和客户端证书以及客户端专用密钥。
3. 当 StorageGRID 节点需要加密密钥时，它会向 KMS 服务器发出请求，请求包含证书中的数据以及基于私钥的签名。
4. KMS 服务器会验证证书签名，并决定它可以信任 StorageGRID 。
5. KMS 服务器使用经过验证的连接进行响应。

StorageGRID 中支持的服务器证书类型

StorageGRID 系统支持使用 RSA 或 ECDSA （椭圆曲线数字签名算法）加密的自定义证书。

安全策略的密码类型必须与服务器证书类型匹配。例如、RSA密钥需要RSA证书、而ECDSA密钥需要ECDSA证书。请参阅。 "管理安全证书"如果您配置的自定义安全策略与服务器证书不兼容，则可以"暂时还原为默认安全策略"。

有关StorageGRID如何保护客户端连接的详细信息，请参见"S3客户端的安全性"。

在 **StorageGRID** 中配置管理界面证书

您可以将默认管理接口证书替换为一个自定义证书，使用户可以访问 Grid Manager 和租户管理器，而不会遇到安全警告。您还可以还原到默认管理接口证书或生成新的管理接口证书。

关于此任务

默认情况下，每个管理节点都会获得一个由网格 CA 签名的证书。这些 CA 签名的证书可以替换为一个通用的自定义管理接口证书和相应的专用密钥。

由于所有管理节点都使用一个自定义管理接口证书，因此，如果客户端在连接到网格管理器和租户管理器时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有管理节点匹配。

您需要在服务器上完成配置，根据所使用的根证书颁发机构（ CA ），用户可能还需要在用于访问网格管理器和租户管理器的 Web 浏览器中安装网格 CA 证书。

为了确保操作不会因服务器证书失败而中断，当该服务器证书即将过期时，会触发*管理接口服务器证书过期*警报。根据需要，您可以通过选择“配置”>“安全”>“证书”并查看“全局”选项卡上管理接口证书的到期日期来查看当前证书的到期时间。

如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：

- 您的自定义管理接口证书将过期。
- 您。从自定义管理接口证书还原到默认服务器证书

添加自定义管理接口证书

要添加自定义管理接口证书，您可以提供自己的证书或使用网格管理器生成一个证书。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

- * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
- 证书专用密钥:自定义服务器证书专用密钥文件(`.key`)。

> EC 私钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

- * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

- 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

生成证书

生成服务器证书文件。

> 生产环境的最佳实践是使用由外部证书颁发机构签名的自定义管理接口证书。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

字段	说明
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。

字段	说明
有效天数	创建后证书过期的天数。
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

5. 刷新页面以确保 Web 浏览器已更新。

> 上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 添加自定义管理接口证书后， " 管理接口证书 " 页面将显示正在使用的证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认管理接口证书

您可以使用网格管理器和租户管理器连接的默认管理接口证书还原到。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用默认证书 * 。

   还原默认管理接口证书时、您配置的自定义服务器证书文件将被删除、并且无法从系统中恢复。默认管理接口证书将用于所有后续的新客户端连接。

4. 刷新页面以确保 Web 浏览器已更新。

使用脚本生成新的自签名管理接口证书

如果需要严格验证主机名，可以使用脚本生成管理接口证书。

开始之前

- 您拥有 "特定访问权限"。
- 您已获得 `Passwords.txt`文件。

关于此任务

生产环境的最佳实践是使用由外部证书颁发机构签名的证书。

步骤

1. 获取每个管理节点的完全限定域名（ FQDN ）。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
3. 使用新的自签名证书配置 StorageGRID 。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 对于 `--domains`，请使用通配符表示所有管理节点的完全限定域名。例如，`*.ui.storagegrid.example.com`使用*通配符表示`admin1.ui.storagegrid.example.com`和 `admin2.ui.storagegrid.example.com`。
   - 设置 `--type`为 `management`可配置网格管理器和租户管理器使用的管理接口证书。
   - 默认情况下，生成的证书有效期为一年（ 365 天），必须在证书过期之前重新创建。您可以使用 `--days`参数覆盖默认有效期。

   > 证书的有效期从运行时开始 `make-certificate`。您必须确保管理客户端与 StorageGRID 同步到同一个时间源；否则，客户端可能会拒绝此证书。

   ```
   $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
   management --days 720
   ```

   生成的输出包含管理 API 客户端所需的公有 证书。
4. 选择并复制证书。

   在您的选择中包括开始和结束标记。
5. 从命令Shell中注销。 `$ exit`

6. 确认已配置证书：
   a. 访问网格管理器。
   b. 选择“配置”>“安全”>“证书”
   c. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
7. 将管理客户端配置为使用您复制的公有 证书。包括开始和结束标记。

下载或复制管理接口证书

您可以保存或复制管理接口证书内容，以便在其他位置使用。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或CA包 `.pem`文件。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

在 **StorageGRID** 中配置 **S3 API** 证书

您可以替换或还原用于将S3客户端连接到存储节点或负载平衡器端点的服务器证书。替换的自定义服务器证书特定于您的组织。

Swift详细信息已从此版本的文档站点中删除。请参阅。 "StorageGRID 11.8：配置S3和Swift API证书"

关于此任务

默认情况下，每个存储节点都会获得一个由网格 CA 签名的 X.509 服务器证书。这些 CA 签名的证书可以替换为一个通用的自定义服务器证书和相应的专用密钥。

所有存储节点都使用一个自定义服务器证书，因此，如果客户端在连接到存储端点时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有存储节点匹配。

在服务器上完成配置后、您可能还需要在要用于访问系统的S3 API客户端中安装Grid CA证书、具体取决于您使用的根证书颁发机构(CA)。

为了确保操作不会因服务器证书失败而中断，当根服务器证书即将过期时，会触发*S3 API 的全局服务器证书过期*警报。根据需要，您可以通过选择“配置”>“安全”>“证书”并查看“全局”选项卡上 S3 API 证书的到期日期来查看当前证书的到期时间。

您可以上传或生成自定义S3 API证书。

添加自定义**S3 API**证书

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*S3 API certificer*。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - 证书专用密钥:自定义服务器证书专用密钥文件(`.key`)。

     EC 私钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 选择证书详细信息以显示已上传的每个自定义S3 API证书的元数据和PEM。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 保存 * 。

   自定义服务器证书将用于后续的新S3客户端连接。

生成证书

生成服务器证书文件。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

字段	说明
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。
有效天数	创建后证书过期的天数。

字段	说明
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择*Certificate Details*以显示生成的自定义S3 API证书的元数据和PEM。

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。

自定义服务器证书将用于后续的新S3客户端连接。

5. 选择一个选项卡以显示默认 StorageGRID 服务器证书，已上传的 CA 签名证书或已生成的自定义证书的元数据。

   上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 刷新页面以确保 Web 浏览器已更新。

7. 添加自定义S3 API证书后、S3 API证书页面将显示正在使用的自定义S3 API证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认**S3 API**证书

您可以还原为使用默认S3 API证书进行S3客户端与存储节点的连接。但是、不能对负载平衡器端点使用默认S3 API证书。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*S3 API certificer*。
3. 选择 * 使用默认证书 * 。

   还原全局S3 API证书的默认版本时、您配置的自定义服务器证书文件将被删除、并且无法从系统中恢复。默认的S3 API证书将用于后续与存储节点的新S3客户端连接。

4. 选择*OK*确认警告并还原默认S3 API证书。

如果您具有root访问权限、并且自定义S3 API证书已用于负载平衡器端点连接、则会显示一个列表、其中列出了无法再使用默认S3 API证书访问的负载平衡器端点。转到"配置负载平衡器端点"以编辑或删除受影响的端点。

5. 刷新页面以确保 Web 浏览器已更新。

下载或复制**S3 API**证书

您可以保存或复制S3 API证书内容以供其他地方使用。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*S3 API certificer*。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或CA包 `.pem`文件。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。

c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

相关信息

- "使用S3 REST API"
- "配置S3端点域名"

复制 **StorageGRID** 网格 **CA** 证书

StorageGRID 使用内部证书颁发机构（ CA ）来保护内部流量。如果您上传自己的证书，则此证书不会更改。

开始之前

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

关于此任务

如果配置了自定义服务器证书，则客户端应用程序应使用自定义服务器证书验证服务器。他们不应从 StorageGRID 系统复制 CA 证书。

步骤

1. 选择 配置 > 安全 > 证书，然后选择 **Grid CA** 选项卡。
2. 在*Certificate PEM*部分，下载或复制证书。

下载证书文件

下载证书 `.pem`文件。

a. 选择 * 下载证书 * 。
b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

例如： `storagegrid_certificate.pem`

复制证书 **PEM**

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

例如： `storagegrid_certificate.pem`

为 **FabricPool** 配置 **StorageGRID** 证书

对于执行严格主机名验证但不支持禁用严格主机名验证的S3客户端(例如使用FabricPool的ONTAP 客户端)、您可以在配置负载平衡器端点时生成或上传服务器证书。

开始之前

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

关于此任务

创建负载平衡器端点时，您可以生成自签名服务器证书或上传由已知证书颁发机构（ CA ）签名的证书。在生产环境中，您应使用由已知 CA 签名的证书。由 CA 签名的证书可以无中断地轮换。它们也更安全，因为它们可以更好地防止中间人攻击。

以下步骤为使用 FabricPool 的 S3 客户端提供了一般准则。有关更多详细信息和过程，请参见"为 FabricPool 配置 StorageGRID"。

步骤

1. （可选）配置一个高可用性（ High Availability ， HA ）组以供 FabricPool 使用。
2. 创建 S3 负载平衡器端点以供 FabricPool 使用。

   创建 HTTPS 负载平衡器端点时，系统会提示您上传服务器证书，证书专用密钥和可选的 CA 捆绑包。
3. 在 ONTAP 中将 StorageGRID 附加为云层。

   指定负载平衡器端点端口以及上载的 CA 证书中使用的完全限定域名。然后，提供 CA 证书。

> 如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。

在 **StorageGRID** 中配置客户端证书

客户端证书允许授权的外部客户端访问 StorageGRID Prometheus 数据库，从而为外部工具监控 StorageGRID 提供了一种安全的方式。

如果您需要使用外部监控工具访问StorageGRID 、则必须使用网格管理器上传或生成客户端证书、并将证书信息复制到外部工具。

请参阅"管理安全证书"和"配置自定义服务器证书"。

> 为了确保操作不会因服务器证书失败而中断，当此服务器证书即将过期时，将触发*证书页面上配置的客户端证书过期*警报。根据需要，您可以通过选择“配置”>“安全”>“证书”并查看“客户端”选项卡上客户端证书的到期日期来查看当前证书的到期时间。

> 如果使用密钥管理服务器(KMS)保护专门配置的设备节点上的数据，请参见有关的特定信息。"上传 KMS 客户端证书"

开始之前

- 您具有 root 访问权限。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 配置客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 如果已配置StorageGRID 管理接口证书、则可以使用CA、客户端证书和专用密钥来配置管理接口证书。
  - 要上传您自己的证书、您的本地计算机上提供了证书的专用密钥。
  - 私钥必须在创建时已保存或记录。如果您没有原始私钥、则必须创建一个新的私钥。

- 编辑客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 要上传您自己的证书或新证书、您的本地计算机上提供了私钥、客户端证书和CA (如果使用)。

添加客户端证书

要添加客户端证书、请使用以下过程之一：

- [已配置管理接口证书]
- CA颁发的客户端证书
- [从网格管理器生成的证书]

已配置管理接口证书

如果已使用客户提供的CA、客户端证书和专用密钥配置管理接口证书、请使用此操作步骤 添加客户端证书。

步骤

1. 在网格管理器中，选择*配置* > 安全 > 证书，然后选择*客户端*选项卡。
2. 选择 * 添加 * 。
3. 输入证书名称。
4. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
5. 选择 * 继续 * 。
6. 对于*attach certificates*步骤，请上传管理接口证书。
   a. 选择 * 上传证书 * 。
   b. 选择*浏览*并选择管理接口证书文件(`.pem`)。
      - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
      - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   c. 选择 * 创建 * 以在网格管理器中保存证书。

      新证书将显示在客户端选项卡上。
7. 配置外部监控工具，如Grafana。

CA颁发的客户端证书

如果未配置管理接口证书、并且您计划为使用CA颁发的客户端证书和专用密钥的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 执行步骤至"配置管理接口证书"。
2. 在网格管理器中，选择*配置* > 安全 > 证书，然后选择*客户端*选项卡。
3. 选择 * 添加 * 。

4. 输入证书名称。
5. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
6. 选择 * 继续 * 。
7. 对于*attach certificates*步骤，上传客户端证书、私钥和CA包文件：
   a. 选择 * 上传证书 * 。
   b. 选择*浏览*并选择客户证书、私钥和CA包文件(`.pem`)。
      - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
      - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   c. 选择 * 创建 * 以在网格管理器中保存证书。

      新证书将显示在客户端选项卡上。
8. 配置外部监控工具，如Grafana。

从网格管理器生成的证书

如果未配置管理接口证书、并且您计划为使用网格管理器中的生成证书功能的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 在网格管理器中，选择*配置* > 安全 > 证书，然后选择*客户端*选项卡。
2. 选择 * 添加 * 。
3. 输入证书名称。
4. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
5. 选择 * 继续 * 。
6. 对于*attach certificates*步骤，选择*Generate certificates*。
7. 指定证书信息：
   - 主题(可选)：证书所有者的X.509主题或可分辨名称(DN)。
   - 有效天数：生成的证书自生成之日起生效的天数。
   - 添加密钥用法扩展：如果选择(默认值和建议值)，则会将密钥用法扩展和扩展密钥用法扩展添加到生成的证书中。

     这些扩展定义了证书中所含密钥的用途。

     除非在证书包含这些扩展时遇到与旧客户端的连接问题、否则保持选中此复选框。
8. 选择 * 生成 * 。
9. 【客户端证书详细信息】选择*客户端证书详细信息*可显示证书元数据和证书PEM。

   关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
- 选择 * 下载私钥 * 将私钥另存为文件。

  指定私钥文件名和下载位置。

10. 选择 * 创建 * 以在网格管理器中保存证书。

    新证书将显示在客户端选项卡上。

11. 在网格管理器中，选择*配置* > 安全 > 证书，然后选择*全局*选项卡。
12. 选择*管理接口证书*。
13. 选择 * 使用自定义证书 * 。
14. 上传步骤中的certifice.pm和prived_key.pm文件客户端证书详细信息。无需上传CA捆绑包。
    a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
    b. 上传每个证书文件(`.pem`)。
    c. 选择*保存*以在网格管理器中保存证书。

       新证书将显示在管理接口证书页面上。

15. 配置外部监控工具，如Grafana。

[[configure-External monitoring-tool]]配置外部监控工具

步骤

1. 在外部监控工具上配置以下设置，例如 Grafana 。
   a. * 名称 * ： 输入连接的名称。

      StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。

   b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

      例如： `https://admin-node.example.com:9091`

   c. 启用 * TLS 客户端身份验证 * 和 * 使用 CA 证书 * 。
   d. 在TLS/SSL身份验证详细信息下、复制并粘贴：+
      - 管理接口CA证书到"** CA证书"
      - 到"Client Cert"的客户端证书
      - "**客户端密钥"的专用密钥

e. * 服务器名称 * ： 输入管理节点的域名。

servername 必须与管理接口证书中显示的域名匹配。

2. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

有关指标的信息，请参见"有关监控 StorageGRID 的说明"。

编辑客户端证书

您可以编辑管理员客户端证书以更改其名称，启用或禁用 Prometheus 访问，或者在当前证书已过期时上传新证书。

步骤

1. 选择“配置”>“安全”>“证书”，然后选择“客户端”选项卡。

表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择 * 编辑名称和权限 *
4. 输入证书名称。
5. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
6. 选择 * 继续 * 以在网格管理器中保存证书。

更新后的证书将显示在客户端选项卡上。

附加新的客户端证书

您可以在当前证书过期后上传新证书。

步骤

1. 选择“配置”>“安全”>“证书”，然后选择“客户端”选项卡。

表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择编辑选项。

上传证书

复制证书文本以粘贴到其他位置。

a. 选择 * 上传证书 * ，然后选择 * 继续 * 。

b. 上载客户端证书名称(`.pem`)。

选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

c. 选择 * 创建 * 以在网格管理器中保存证书。

更新后的证书将显示在客户端选项卡上。

生成证书

生成要粘贴到其他位置的证书文本。

a. 选择 * 生成证书 * 。

b. 指定证书信息：

- 主题(可选)：证书所有者的X.509主题或可分辨名称(DN)。
- 有效天数：生成的证书自生成之日起生效的天数。
- 添加密钥用法扩展：如果选择(默认值和建议值)，则会将密钥用法扩展和扩展密钥用法扩展添加到生成的证书中。

  这些扩展定义了证书中所含密钥的用途。

  除非在证书包含这些扩展时遇到与旧客户端的连接问题、否则保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

  关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

例如： `storagegrid_certificate.pem`

- 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
- 选择 * 下载私钥 * 将私钥另存为文件。

  指定私钥文件名和下载位置。

e. 选择 * 创建 * 以在网格管理器中保存证书。

新证书将显示在客户端选项卡上。

下载或复制客户端证书

您可以下载或复制客户端证书以供其他位置使用。

步骤

1. 选择“配置”>“安全”>“证书”，然后选择“客户端”选项卡。
2. 选择要复制或下载的证书。
3. 下载或复制证书。

下载证书文件

下载证书 `.pem`文件。

a. 选择 * 下载证书 * 。
b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

删除客户端证书

如果您不再需要管理员客户端证书，可以将其删除。

步骤

1. 选择“配置”>“安全”>“证书”，然后选择“客户端”选项卡。
2. 选择要删除的证书。

3. 选择 * 删除 * ，然后确认。

要删除最多 10 个证书，请在客户端选项卡上选择要删除的每个证书，然后选择 * 操作 * > * 删除 * 。

删除证书后，使用该证书的客户端必须指定一个新的客户端证书，才能访问 StorageGRID Prometheus 数据库。

配置安全设置

在 **StorageGRID** 中管理 **TLS** 和 **SSH** 策略

TLS和SSH策略用于确定使用哪些协议和加密方法与客户端应用程序建立安全TLS连接、以及与内部StorageGRID 服务建立安全SSH连接。

此安全策略控制TLS和SSH如何对移动数据进行加密。通常、请使用现代兼容性(默认)策略、除非您的系统需要符合通用标准或您需要使用其他密钥。

某些StorageGRID 服务尚未更新、无法在这些策略中使用这些加密方法。

开始之前

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

选择一个安全策略

步骤

1. 选择*配置* > 安全 > 安全设置。

   TLS和SSH策略*选项卡显示可用策略。当前活动的策略会在策略磁贴上标记为绿色复选标记。



2. 查看标签以了解可用的策略。

现代兼容性(默认)

如果您需要强加密并且没有特殊要求，请使用默认策略。此策略与大多数 TLS 和 SSH 客户端兼容。

传统兼容性

如果您需要为旧客户端提供额外的兼容性选项，请使用旧版兼容性策略。此策略中的附加选项可能会使其安全性低于现代兼容性策略。

通用标准

如果您需要通用标准认证，请使用通用标准政策。

FIPS严格

如果您需要通用标准认证，并且需要使用 NetApp 加密安全模块 (NCSM) 3.1.2 或 NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 模块进行与负载平衡器端点、租户管理器和网格管理器的外部客户端连接，请使用 FIPS 严格策略。使用此策略可能会降低性能。

NCSM 3.1.2 和 NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 模块用于以下操作：

- 全国运动医学委员会
  - 以下服务之间的 TLS 连接：ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api、nginx、nginx-gw 和 cache-svc
  - 客户端和 nginx-gw 服务（负载均衡器端点）之间的 TLS 连接
  - 客户端和 LDR 服务之间的 TLS 连接
  - SSE-S3、SSE-C 和存储对象加密设置的对象内容加密
  - SSH 连接

  有关详细信息，请参见 NIST Cryptographic Algorithm Validation Program "证书 #A7816"。
- NetApp StorageGRID内核加密 API 模块

  NetApp StorageGRID Kernel Crypto API 模块仅存在于 VM 和StorageGRID设备平台上。
  - 熵收集
  - 节点加密

    注：此模块尚未提交认证。

  有关详细信息，请参见 NIST Cryptographic Algorithm Validation Program "熵证书#E223"。

注意：选择此政策后，"执行滚动重启"所有节点均激活 NCSM。使用*维护* > *滚动重启*来启动和监控重启。

自定义

如果需要应用您自己的用户名或用户名、请创建自定义策略。

或者，如果您的 StorageGRID 具有 FIPS 140 加密要求，则启用 FIPS 模式功能以使用 NCSM 3.1.2 和 NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 模块：

a. 设置 `fipsMode`参数 `true`。

b. 当出现提示时，"执行滚动重启"所有节点都激活加密模块。使用*维护* > *滚动重启*来启动和监控重启。

c. 选择“支持”>“诊断”以查看活动的 FIPS 模块版本。

3. 要查看有关每个策略的加密、协议和算法的详细信息，请选择*查看详细信息*。
4. 要更改当前策略，请选择*使用策略*。

   策略磁贴上的*current policy*旁边会出现一个绿色复选标记。

创建自定义安全策略

如果需要应用自己的用户名、可以创建自定义策略。

步骤

1. 从与要创建的自定义策略最相似的策略的磁贴中，选择*查看详细信息*。
2. 选择*复制到剪贴板*，然后选择*取消*。



3. 从“自定义策略”磁贴中，选择“配置和使用”。
4. 粘贴您复制的JSON并进行所需的任何更改。
5. 选择*使用策略*。

   自定义策略磁贴上的*当前策略*旁边会出现一个绿色复选标记。

6. (可选)选择*Edit configuration*对新的自定义策略进行更多更改。

暂时还原为默认安全策略

如果配置了自定义安全策略，并且配置的TLS策略与不兼容，则可能无法登录到网格管理器"已配置服务器证书"。

您可以临时还原为默认安全策略。

步骤

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

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 运行以下命令：

   ```
   restore-default-cipher-configurations
   ```

3. 从 Web 浏览器访问同一管理节点上的网格管理器。
4. 按照中的步骤选择一个安全策略重新配置策略。

配置 **StorageGRID** 网络和对象安全性

您可以将网络和对象安全性配置为对存储的对象进行加密、防止某些S3请求、或者允许客户端使用HTTP而不是HTTPS连接到存储节点。

存储对象加密

通过存储对象加密、可以在通过S3读取所有对象数据时对这些数据进行加密。默认情况下、存储的对象不会进行加密、但您可以选择使用AES－128或AES－256加密算法对对象进行加密。启用此设置后，所有新载入的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密、则当前加密的对象仍会保持加密状态、但不会对新加装的对象进行加密。

存储的对象加密设置仅适用于尚未通过存储分段级或对象级加密进行加密的S3对象。

有关StorageGRID加密方法的更多详细信息，请参见"查看 StorageGRID 加密方法"。

防止修改客户端

防止客户端修改是一项系统范围的设置。如果选择了*prevent client修改*选项，则会拒绝以下请求。

S3 REST API

- DeleteBuckets请求
- 修改现有对象数据，用户定义的元数据或 S3 对象标记的任何请求

为存储节点连接启用**HTTP**

默认情况下、客户端应用程序会使用HTTPS网络协议直接连接到存储节点。您可以选择为这些连接启用 HTTP，例如在测试非生产网格时。

仅当S3客户端需要直接与存储节点建立HTTP连接时、才使用HTTP进行存储节点连接。对于仅使用HTTPS连接的客户端或连接到负载平衡器服务的客户端(因为可以使用HTTP或HTTPS)、您不需要使用此选项"配置每个负载平衡器端点"。

请参见"摘要：客户端连接的 IP 地址和端口"、了解S3客户端在使用HTTP或HTTPS连接到存储节点时使用的端口。

选择选项

开始之前

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

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择*网络和对象*选项卡。
3. 对于存储的对象加密，如果不希望对存储的对象进行加密，请使用*None*(默认)设置，或者选择*AES-128*或*AES-256*对存储的对象进行加密。
4. 如果要阻止S3客户端发出特定请求，可选择*prevent client修改*。

   如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

5. 如果客户端直接连接到存储节点并且您要使用HTTP连接，则可以选择*为存储节点连接启用HTTP *。

   为生产网格启用 HTTP 时请务必小心，因为请求会以未加密方式发送。

6. 选择 * 保存 * 。

更改 **StorageGRID** 接口安全设置

通过接口安全设置、您可以控制在用户处于非活动状态的时间超过指定时间时是否注销、以及是否在API错误响应中包含堆栈跟踪。

开始之前

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

关于此任务

“*安全设置”页面包括*浏览器非活动超时*和*管理API堆栈跟踪*设置。

浏览器非活动超时

指示用户的浏览器在注销前可以处于非活动状态的时间长度。默认值为 15 分钟。

浏览器非活动超时还受以下因素控制：

- 一个单独的不可配置 StorageGRID 计时器，其中包括用于系统安全保护的计时器。每个用户的身份验证

令牌将在用户登录后16小时过期。当用户的身份验证过期时、即使禁用了浏览器非活动超时或未达到浏览器超时值、该用户也会自动注销。要续订令牌，用户必须重新登录。

- 身份提供程序的超时设置(假设为StorageGRID 启用了单点登录(SSO))。

  如果启用了 SSO 并且用户的浏览器超时，则用户必须重新输入其 SSO 凭据才能再次访问StorageGRID 。看"SSO 的工作原理" 。

管理**API**堆栈跟踪

控制是否在Grid Manager和租户管理器API错误响应中返回堆栈跟踪。

默认情况下、此选项处于禁用状态、但您可能希望在测试环境中启用此功能。通常、您应在生产环境中禁用堆栈跟踪、以避免在发生API错误时泄露内部软件详细信息。

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择*Interface*选项卡。
3. 要更改浏览器非活动超时设置：
   a. 展开可展开面。
   b. 要更改超时期限、请指定一个介于60秒和7天之间的值。默认超时为15分钟。
   c. 要禁用此功能、请取消选中此复选框。
   d. 选择 * 保存 * 。

   新设置不会影响当前已登录的用户。用户必须重新登录或刷新其浏览器、新超时设置才能生效。
4. 要更改管理API堆栈跟踪设置、请执行以下操作：
   a. 展开可展开面。
   b. 选中此复选框可在Grid Manager和租户管理器API错误响应中返回堆栈跟踪。

      在生产环境中禁用堆栈跟踪、以避免在发生API错误时泄露内部软件详细信息。

   c. 选择 * 保存 * 。

在 **StorageGRID** 中管理外部 **SSH** 访问

通过阻止或允许外部访问来管理进入网格的入站流量的 SSH 访问。管理 SSH 外部访问不会影响网格中节点之间的流量。

开始之前

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

关于此任务

为了增强系统安全性，默认情况下会阻止外部 SSH 访问。如果您需要执行需要入站 SSH 访问的任务（例如故障排除），请暂时允许外部访问。完成任务后，阻止外部访问。

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择“阻止 **SSH**”选项卡。
3. 使用*阻止入站 SSH 访问*选项来管理外部 SSH 访问：
   a. 选中复选框以阻止访问（默认）。
   b. 取消选中复选框以允许访问。

   需要通过服务笔记本电脑和所有其他网格节点之间的端口 22 进行访问。维护任务完成后，移除对端口 22 的访问权限。

4. 选择 * 保存 * 。

配置密钥管理服务器

了解 **StorageGRID** 中的密钥管理服务器

密钥管理服务器（ Key Management Server ， KMS ）是一种外部第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为关联 StorageGRID 站点上的 StorageGRID 设备节点提供加密密钥。

StorageGRID仅支持某些密钥管理服务器。有关受支持产品和版本的列表，请使用 "NetApp 互操作性表工具（ IMT ）"。

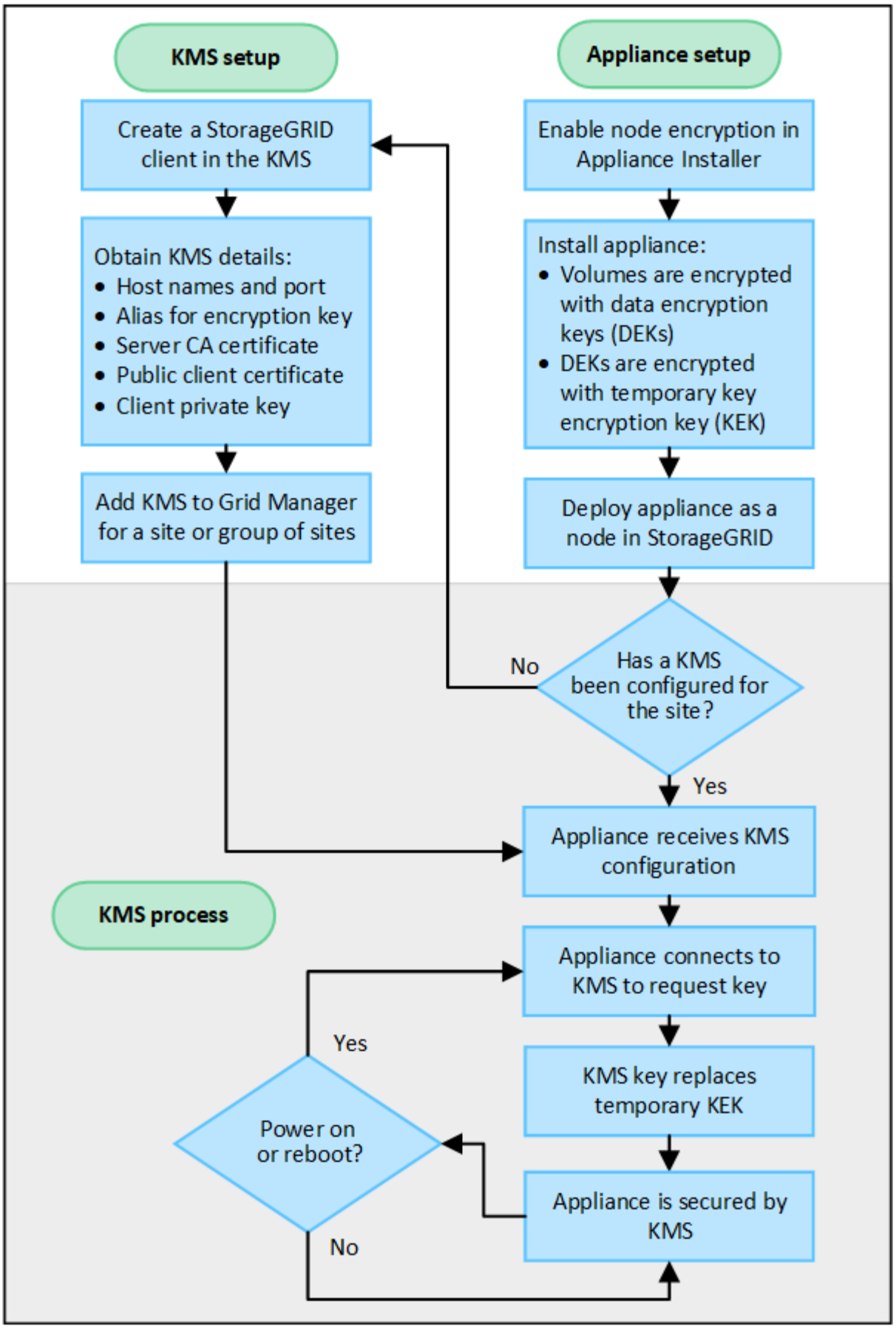
您可以使用一个或多个密钥管理服务器来管理安装期间启用了 * 节点加密 * 设置的任何 StorageGRID 设备节点的节点加密密钥。通过将密钥管理服务器与这些设备节点结合使用，您可以保护数据，即使设备已从数据中心中删除也是如此。对设备卷进行加密后、您将无法访问设备上的任何数据、除非此节点可以与KMS进行通信。

StorageGRID 不会创建或管理用于对设备节点进行加密和解密的外部密钥。如果您计划使用外部密钥管理服务器来保护 StorageGRID 数据，则必须了解如何设置该服务器，并且必须了解如何管理加密密钥。执行密钥管理任务不在本说明的范围之内。如果需要帮助，请参见密钥管理服务器的文档或联系技术支持。

StorageGRID 密钥管理服务器和设备配置

在使用密钥管理服务器（ KMS ）保护设备节点上的 StorageGRID 数据之前，必须完成两项配置任务：设置一个或多个 KMS 服务器以及为设备节点启用节点加密。完成这两项配置任务后，密钥管理过程将自动进行。

此流程图显示了使用 KMS 在设备节点上保护 StorageGRID 数据的高级步骤。



流程图显示了 KMS 设置和设备设置并行进行；但是，您可以根据需要在为新设备节点启用节点加密之前或之后

设置密钥管理服务器。

设置密钥管理服务器（ **KMS** ）

设置密钥管理服务器包括以下高级步骤。

步骤	请参见
访问 KMS 软件，并向每个 KMS 或 KMS 集群添加一个 StorageGRID 客户端。	"在 KMS 中将 StorageGRID 配置为客户端"
在 KMS 上获取 StorageGRID 客户端所需的信息。	"在 KMS 中将 StorageGRID 配置为客户端"
将 KMS 添加到网格管理器中，将其分配到一个站点或一组默认站点，上传所需的证书并保存 KMS 配置。	"添加密钥管理服务器（ KMS ）"

设置设备

设置要使用 KMS 的设备节点包括以下高级步骤。

1. 在设备安装的硬件配置阶段，使用 StorageGRID 设备安装程序为设备启用 * 节点加密 * 设置。

   将设备添加到网格后、您无法启用*节点加密*设置、并且无法对未启用节点加密的设备使用外部密钥管理。

2. 运行 StorageGRID 设备安装程序。在安装期间，系统会为每个设备卷分配一个随机数据加密密钥（ DEK ），如下所示：
   - 这些 DEks 用于对每个卷上的数据进行加密。这些密钥是在设备操作系统中使用Linux统一密钥设置(LUKS)磁盘加密生成的、无法更改。
   - 每个 DEK 都通过主密钥加密密钥（ KEK ）进行加密。初始 KEK 是一个临时密钥，用于对密钥进行加密，直到设备可以连接到 KMS 为止。
3. 将设备节点添加到 StorageGRID 。

有关详细信息、请参见。 "启用节点加密"

密钥管理加密过程（自动发生）

密钥管理加密包括以下高级步骤，这些步骤会自动执行。

1. 在网格中安装启用了节点加密的设备时， StorageGRID 会确定包含新节点的站点是否存在 KMS 配置。
   - 如果已为站点配置 KMS ，则设备将接收 KMS 配置。
   - 如果尚未为站点配置 KMS ，则设备上的数据将继续由临时 KEK 加密，直到您为站点配置 KMS 且设备收到 KMS 配置为止。
2. 设备使用 KMS 配置连接到 KMS 并请求加密密钥。
3. KMS 会向设备发送加密密钥。KMS 中的新密钥将取代临时的 KEK ，现在用于对设备卷的 DEK 进行加密和解密。

加密设备节点连接到配置的 KMS 之前存在的任何数据都将使用临时密钥进行加密。但是，在将临时密钥替换为 KMS 加密密钥之前，不应将设备卷视为不受从数据中心删除的保护。

4. 如果设备已启动或重新启动，它将重新连接到 KMS 以请求密钥。此密钥保存在易失性内存中、无法经受断电或重新启动的影响。

StorageGRID 密钥管理服务器要求和注意事项

在配置外部密钥管理服务器（ KMS ）之前，您必须了解注意事项和要求。

支持以下哪个版本的**KMIP**?

StorageGRID 支持 KMIP 1.4 版。

"密钥管理互操作性协议规范 1.4 版"

网络注意事项有哪些?

网络防火墙设置必须允许每个设备节点通过用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口进行通信。默认 KMIP 端口为 5696 。

您必须确保使用节点加密的每个设备节点都可以通过网络访问为站点配置的 KMS 或 KMS 集群。

支持哪些**TLS**版本?

设备节点与配置的 KMS 之间的通信使用安全 TLS 连接。StorageGRID在与KMS或KMS集群建立KMIP连接时、可以支持TLS 1.2或TLS 1.3协议、具体取决于KMS支持的内容以及您正在使用的协议"TLS和SSH策略"。

StorageGRID在建立连接时与 KMS 协商协议和密码（TLS 1.2）或密码套件（TLS 1.3）。要查看可用的协议版本和密码/密码套件，请查看 `tlsOutbound`网格的活动 TLS 和 SSH 策略部分（配置 > 安全 安全设置）。

支持哪些设备?

您可以使用密钥管理服务器（ Key Management Server ， KMS ）管理网格中启用了 * 节点加密 * 设置的任何 StorageGRID 设备的加密密钥。只有在使用 StorageGRID 设备安装程序安装设备的硬件配置阶段，才能启用此设置。

将设备添加到网格后、您无法启用节点加密、并且无法对未启用节点加密的设备使用外部密钥管理。

您可以对StorageGRID 设备和设备节点使用已配置的KMS。

您不能对基于软件(非设备)的节点使用已配置的KMS、包括以下节点：

- 部署为虚拟机（ VM ）的节点
- 在 Linux 主机上的容器引擎中部署的节点

在这些其他平台上部署的节点可以在数据存储库或磁盘级别使用 StorageGRID 外部的加密。

应在何时配置密钥管理服务器?

对于新安装，通常应在创建租户之前在网格管理器中设置一个或多个密钥管理服务器。此顺序可确保节点在存储任何对象数据之前受到保护。

您可以在安装设备节点之前或之后在网格管理器中配置密钥管理服务器。

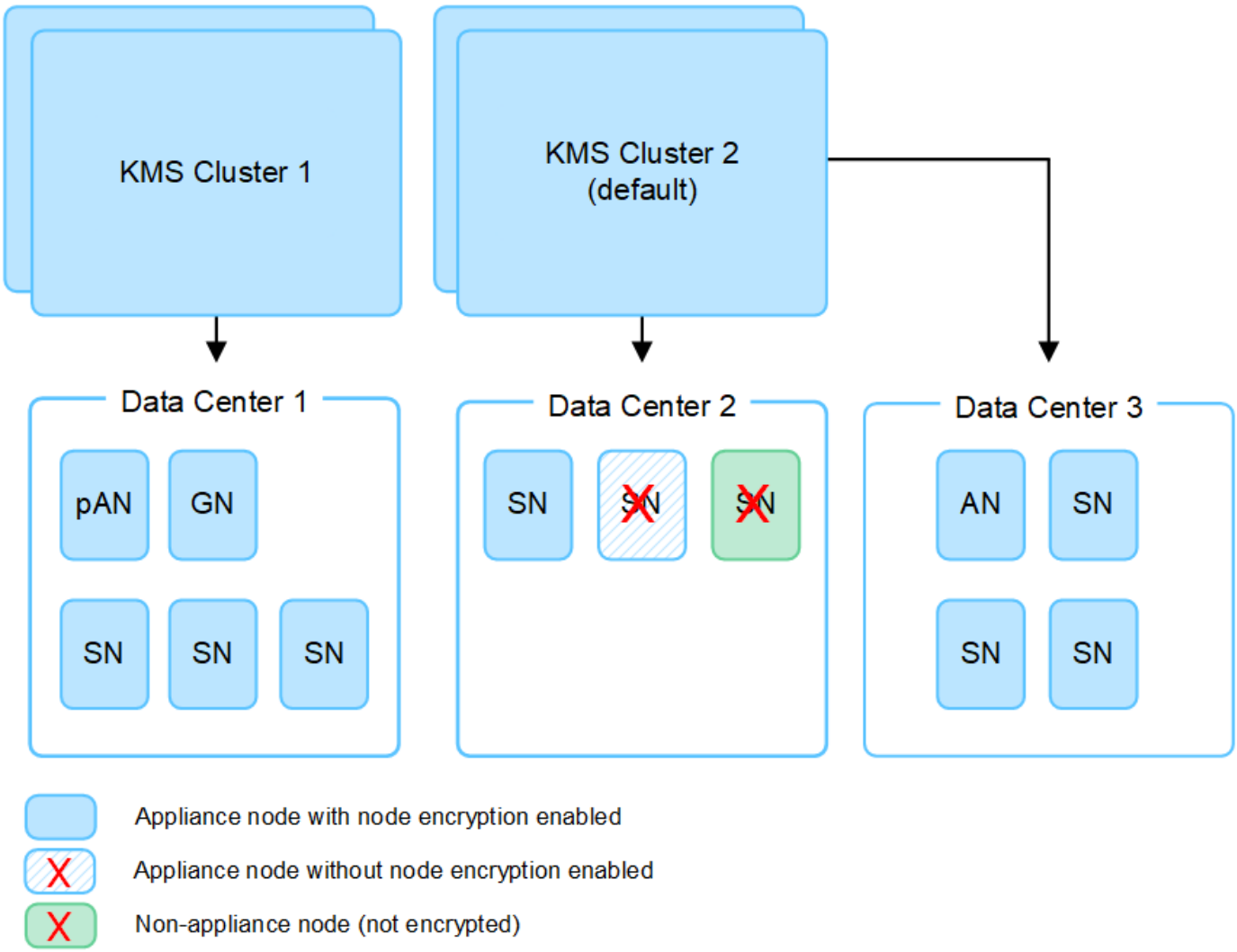
我需要多少个密钥管理服务器?

您可以配置一个或多个外部密钥管理服务器，以便为 StorageGRID 系统中的设备节点提供加密密钥。每个 KMS 都为单个站点或一组站点上的 StorageGRID 设备节点提供一个加密密钥。

StorageGRID 支持使用 KMS 集群。每个 KMS 集群都包含多个复制的密钥管理服务器，这些服务器共享配置设置和加密密钥。建议使用 KMS 集群进行密钥管理，因为它可以提高高可用性配置的故障转移功能。

例如，假设您的 StorageGRID 系统有三个数据中心站点。您可以将一个 KMS 集群配置为为为 Data Center 1 上的所有设备节点提供密钥，而将另一个 KMS 集群配置为为为所有其他站点上的所有设备节点提供密钥。添加第二个 KMS 集群时，您可以为 Data Center 2 和 Data Center 3 配置默认 KMS 。

请注意，不能对非设备节点或安装期间未启用*Node Encryption设置的任何设备节点使用KMS。



轮换密钥时会发生什么情况?

作为安全最佳实践、每个已配置的KMS都应定期"旋转加密密钥"使用。

新密钥版本可用时：

- 它会自动分发到与 KMS 关联的站点上的加密设备节点。分发应在轮换密钥后的一小时内完成。
- 如果在分发新密钥版本时加密设备节点脱机，则该节点将在重新启动后立即收到新密钥。
- 如果由于任何原因无法使用新密钥版本对设备卷进行加密、则会为此设备节点触发* KMS加密密钥轮换失败*警报。您可能需要联系技术支持以帮助解决此警报。

是否可以在设备节点加密后重复使用它?

如果需要将加密设备安装到另一个 StorageGRID 系统中，则必须先停用网格节点，才能将对象数据移动到另一个节点。然后，您可以使用StorageGRID设备安装程序 "清除KMS配置"。清除 KMS 配置将禁用 * 节点加密 * 设置，并删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。

如果无法访问 KMS 加密密钥，则设备上保留的任何数据将无法再访问并永久锁定。

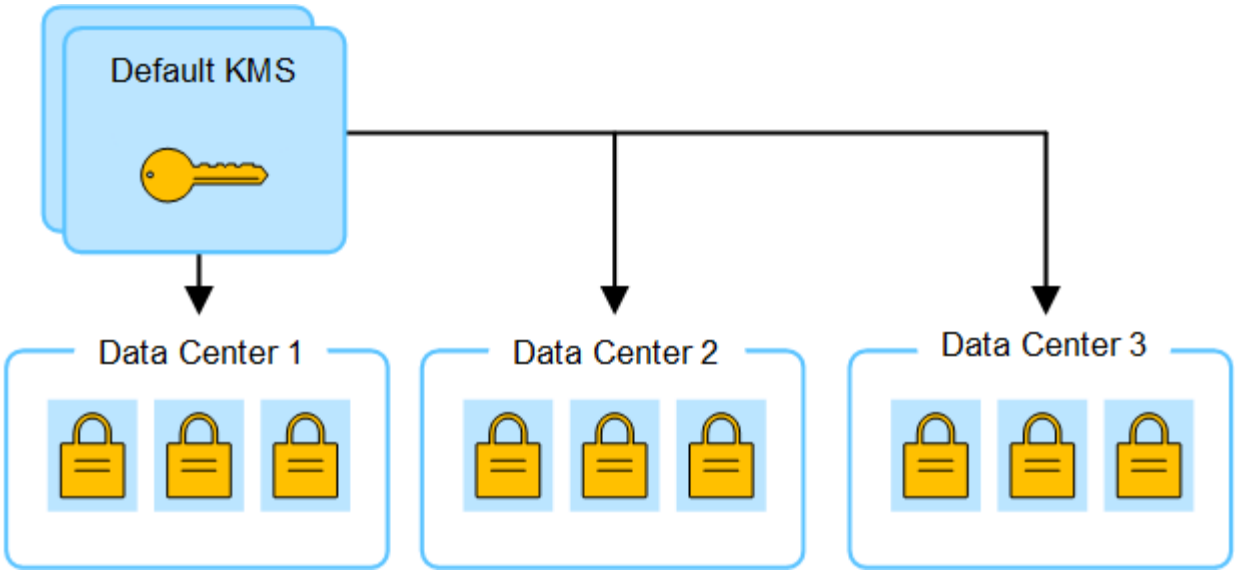
更改 **StorageGRID** 站点 **KMS** 的注意事项

每个密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群都会为单个站点或一组站点上的所有设备节点提供一个加密密钥。如果需要更改站点使用的 KMS ，则可能需要将加密密钥从一个 KMS 复制到另一个 KMS 。

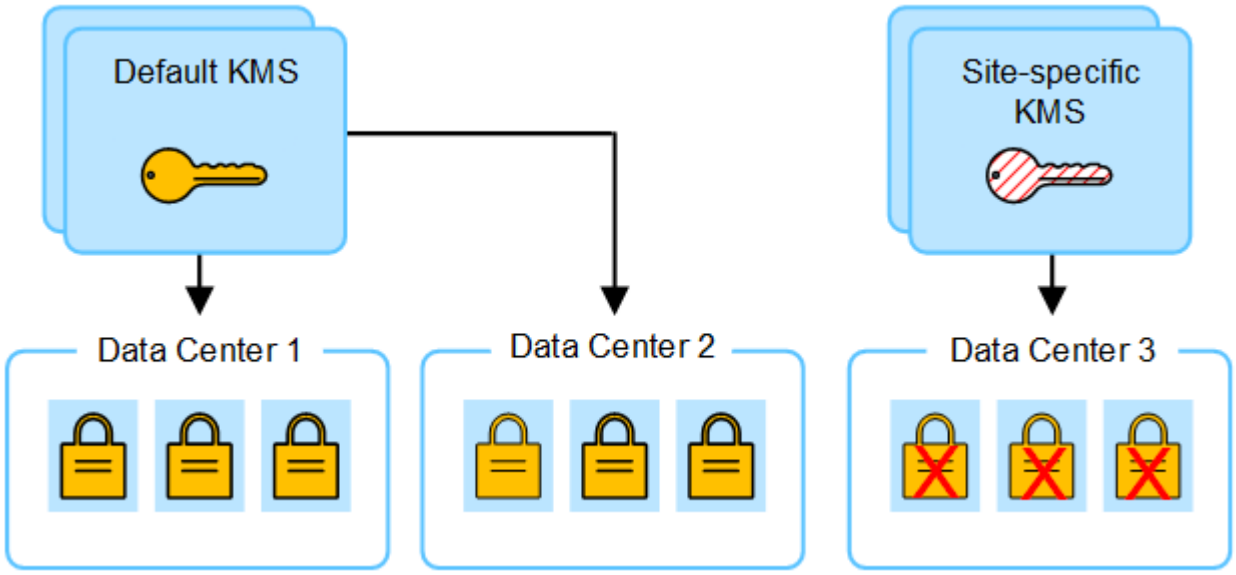
如果更改站点使用的 KMS ，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS 。您必须确保 KMS 具有正确的密钥，以便对站点上的加密设备节点进行解密。

例如：

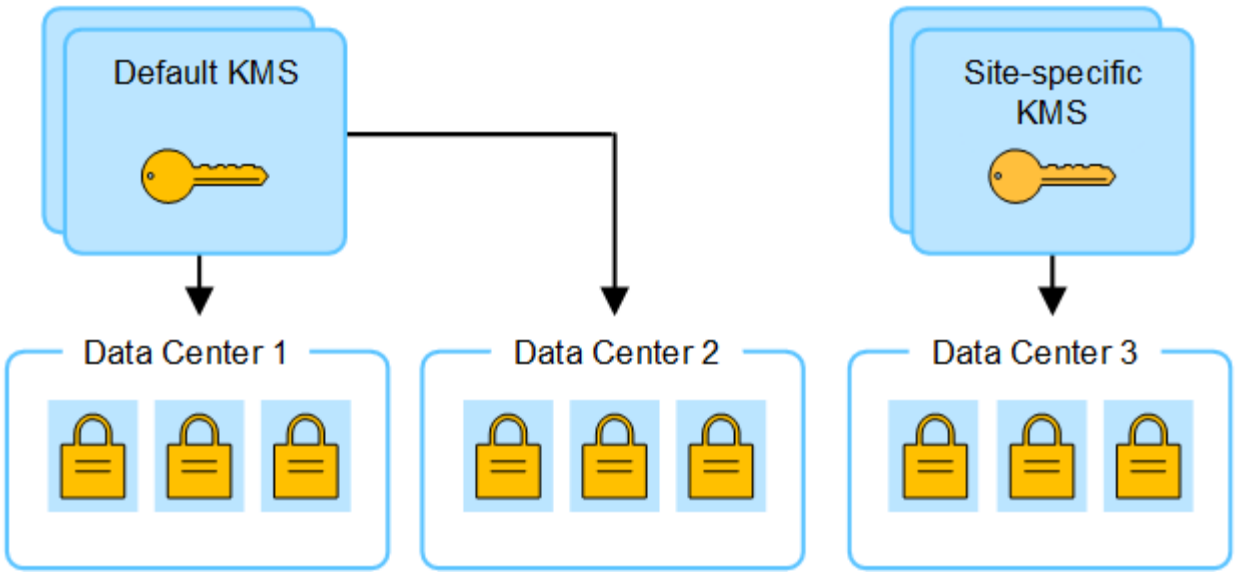
1. 您最初会配置一个默认KMS、用于适用场景 所有没有专用KMS的站点。
2. 保存 KMS 后，所有启用了 * 节点加密 * 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于对所有站点上的设备节点进行加密。此外，还必须使用此相同密钥对这些设备进行解密。



3. 您决定为一个站点（图中的数据中心 3 ）添加站点专用的 KMS 。但是，由于设备节点已加密，因此在尝试保存站点专用 KMS 的配置时会发生验证错误。之所以出现此错误，是因为站点特定的 KMS 没有正确的密钥来对该站点上的节点进行解密。



4. 要解决问题描述 问题，请将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。（从技术上讲，您可以将原始密钥复制到具有相同别名的新密钥。原始密钥将成为新密钥的先前版本。)现在、站点专用的KMS具有正确的密钥、可用于对数据中心3上的设备节点进行解密、因此可以将其保存在StorageGRID中。



更改站点使用的 **KMS** 的用例

下表总结了更改站点 KMS 的最常见情况下所需的步骤。

更改站点 **KMS** 的用例	所需步骤
您有一个或多个站点特定的 KMS 条目，并且希望使用其中一个条目作为默认 KMS 。	编辑站点特定的 KMS 。在 * 管理密钥 * 字段中，选择 * 不受其他 KMS （默认 KMS ）管理的站点 * 。现在，站点专用的 KMS 将用作默认 KMS 。它将适用于没有专用KMS的任何站点。 "编辑密钥管理服务器（ KMS ）"
您有一个默认 KMS ，并且在扩展中添加了一个新站点。您不想对新站点使用默认KMS。	1. 如果新站点上的设备节点已被默认 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从默认 KMS 复制到新 KMS 。 2. 使用网格管理器添加新的 KMS 并选择站点。 "添加密钥管理服务器（ KMS ）"
您希望站点的 KMS 使用其他服务器。	1. 如果站点上的设备节点已由现有 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从现有 KMS 复制到新 KMS 。 2. 使用网格管理器编辑现有 KMS 配置并输入新的主机名或 IP 地址。 "添加密钥管理服务器（ KMS ）"

在 **KMS** 中将 **StorageGRID** 配置为客户端

您必须将 StorageGRID 配置为每个外部密钥管理服务器或 KMS 集群的客户端，然后才能将 KMS 添加到 StorageGRID 。

这些说明适用于These CipherTrust Manager和Hashitorp Vault。有关受支持产品和版本的列表，请使用 "NetApp 互操作性表工具（ IMT ）"。

步骤

1. 在 KMS 软件中，为计划使用的每个 KMS 或 KMS 集群创建一个 StorageGRID 客户端。

   每个 KMS 都会为单个站点或一组站点上的 StorageGRID 设备节点管理一个加密密钥。

2. [[crea-key-with -kms-product]]使用以下两种方法之一创建密钥：
   - 使用KMS产品的密钥管理页面。为每个KMS或KMS集群创建AES加密密钥。

     加密密钥必须为2、048位或更多、并且必须可导出。

   - 让StorageGRID创建密钥。测试并保存后，系统将提示您"正在上传客户端证书"。
3. 记录每个 KMS 或 KMS 集群的以下信息。

   将KMS添加到StorageGRID时需要此信息：

   - 每个服务器的主机名或 IP 地址。
   - KMS 使用的 KMIP 端口。
   - KMS 中加密密钥的密钥别名。
4. 对于每个 KMS 或 KMS 集群，获取一个由证书颁发机构（ CA ）签名的服务器证书，或者一个包含 PEM 编码的每个 CA 证书文件的证书捆绑包，这些证书按证书链顺序串联。

   通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

   - 证书必须使用 Privacy Enhanced Mail （ PEM ） Base — 64 编码的 X.509 格式。
   - 每个服务器证书中的 " 使用者备用名称（ SAN ） " 字段必须包含 StorageGRID 要连接到的完全限定域名（ FQDN ）或 IP 地址。

     > 在 StorageGRID 中配置 KMS 时，必须在 * 主机名 * 字段中输入相同的 FQDN 或 IP 地址。

   - 服务器证书必须与 KMS 的 KMIP 接口使用的证书匹配，该接口通常使用端口 5696 。
5. 获取外部 KMS 颁发给 StorageGRID 的公有 客户端证书以及客户端证书的专用密钥。

   客户端证书允许 StorageGRID 向 KMS 进行身份验证。

在 **StorageGRID** 中添加密钥管理服务器

您可以使用 StorageGRID 密钥管理服务器向导添加每个 KMS 或 KMS 集群。

开始之前

- 您已查看"使用密钥管理服务器的注意事项和要求"。
- 您拥有"已在 KMS 中将 StorageGRID 配置为客户端"，并且您拥有每个KMS或KMS群集所需的信息。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

关于此任务

如果可能，请先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对所有不受另一个 KMS 管理的站点进行适用场景 。如果首先创建默认 KMS ，则网格中所有节点加密的设备都将使用默认 KMS 进行加密。如果要稍后创建站点专用的 KMS ，则必须先将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。有关详细信息、请参见。 "更改站点的 KMS 的注意事项"

第**1**步：公里详细信息

在添加密钥管理服务器向导的步骤1 (KMS详细信息)中、您可以提供有关KMS或KMS集群的详细信息。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。

   此时将显示密钥管理服务器页面、并选中配置详细信息选项卡。

2. 选择 * 创建 * 。

   此时将显示"Add a Key Management Server"(添加密钥管理服务器)向导的第1步(KMS详细信息)。

3. 为 KMS 和您在该 KMS 中配置的 StorageGRID 客户端输入以下信息。

字段	说明
Kms名称	一个描述性名称，可帮助您标识此 KMS 。必须介于 1 到 64 个字符之间。
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。 注意：如果您尚未使用KMS产品创建密钥，系统将提示您让StorageGRID创建密钥。
管理的密钥	将与此 KMS 关联的 StorageGRID 站点。如果可能，您应先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对不受另一个 KMS 管理的所有站点进行适用场景 。 • 如果此 KMS 将管理特定站点上设备节点的加密密钥，请选择一个站点。 • 选择*不由其他KMS管理的站点(默认KMS)*以配置默认KMS，该KMS将应用于任何没有专用KMS的站点以及您在后续扩展中添加的任何站点。 ◦ 注意： * 如果您选择的站点先前已被默认 KMS 加密，但未向新 KMS 提供当前版本的原始加密密钥，则保存 KMS 配置时将发生验证错误。
端口	KMS 服务器用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口。默认为 5696 ，即 KMIP 标准端口。

字段	说明
主机名	KMS 的完全限定域名或 IP 地址。 *注意：*服务器证书的使用者替代名称(SAN)字段必须包含您在此处输入的FQDN或IP地址。否则， StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。
5. 选择 * 继续 * 。

第**2**步：上传服务器证书

在添加密钥管理服务器向导的步骤2 (上传服务器证书)中、您可以上传KMS的服务器证书(或证书包)。通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

步骤

1. 从*步骤2 (上载服务器证书)*中，浏览到保存的服务器证书或证书包所在的位置。
2. 上传证书文件。

   此时将显示服务器证书元数据。

   如果您上传的是证书捆绑包，则每个证书的元数据将显示在其自己的选项卡上。

3. 选择 * 继续 * 。

第**3**步：上传客户端证书

在添加密钥管理服务器向导的步骤3 (上传客户端证书)中、您可以上传客户端证书和客户端证书专用密钥。客户端证书允许 StorageGRID 向 KMS 进行身份验证。

步骤

1. 从*步骤3 (上传客户端证书)*中，浏览到客户端证书的位置。
2. 上传客户端证书文件。

   此时将显示客户端证书元数据。

3. 浏览到客户端证书的专用密钥位置。
4. 上传私钥文件。
5. 选择*测试并保存*。

   如果密钥不存在、系统将提示您创建一个StorageGRID密钥。

   测试密钥管理服务器与设备节点之间的连接。如果所有连接均有效，并且在 KMS 上找到正确的密钥，则新的密钥管理服务器将添加到密钥管理服务器页面上的表中。

添加 KMS 后，密钥管理服务器页面上的证书状态将立即显示为未知。StorageGRID 可能需要长达 30 分钟才能获取每个证书的实际状态。您必须刷新 Web 浏览器才能查看当前状态。

6. 如果在选择*测试并保存*时出现错误信息，请查看消息详细信息，然后选择*OK*。

   例如，如果连接测试失败，您可能会收到 422： Unprocessable Entity 错误。

7. 如果需要在不测试外部连接的情况下保存当前配置，请选择*Force save*。

   选择*强制保存*可保存KMS配置，但不会测试从每个设备到该KMS的外部连接。如果具有此配置的问题描述 ，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

8. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 * 。

   已保存 KMS 配置，但未测试与 KMS 的连接。

在 **StorageGRID** 中管理密钥管理服务器

管理密钥管理服务器(KMS)包括查看或编辑详细信息、管理证书、查看加密节点以及删除不再需要的KMS。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。

查看 **KMS** 详细信息

您可以查看有关StorageGRID系统中每个密钥管理服务器(KMS)的信息、包括密钥详细信息以及服务器和客户端证书的当前状态。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。

   此时将显示密钥管理服务器页面、并显示以下信息：

   - 配置详细信息选项卡列出了已配置的任何密钥管理服务器。
   - 加密节点选项卡列出了已启用节点加密的所有节点。

2. 要查看特定KMS的详细信息并对该KMS执行操作、请选择KMS的名称。KMS的详细信息页面列出了以下信息：

字段	说明
管理的密钥	与 KMS 关联的 StorageGRID 站点。 此字段显示特定 StorageGRID 站点的名称或 * 不由其他 KMS （默认 KMS ）管理的站点。 *

字段	说明
主机名	KMS 的完全限定域名或 IP 地址。 如果集群包含两个密钥管理服务器，则会列出这两个服务器的完全限定域名或 IP 地址。如果集群中有两个以上的密钥管理服务器，则会列出第一个 KMS 的完全限定域名或 IP 地址以及集群中其他密钥管理服务器的数量。 例如： `10.10.10.10 and 10.10.10.11`或 `10.10.10.10 and 2 others`。 要查看集群中的所有主机名，请选择一个KMS，然后选择*Edit*或*Actions*>*Edit*。

3. 在KMS详细信息页面上选择一个选项卡以查看以下信息：

选项卡	字段	说明
密钥详细信息	密钥名称	KMS 中 StorageGRID 客户端的密钥别名。
密钥 UID	最新版本密钥的唯一标识符。	上次修改时间
最新版本密钥的日期和时间。	服务器证书	元数据
证书的元数据、例如序列号、到期日期和时间以及证书PEM。	证书PEM	证书的PEM (隐私增强邮件)文件的内容。
客户端证书	元数据	证书的元数据、例如序列号、到期日期和时间以及证书PEM。

4. 根据组织的安全实践要求，只要经常选择*Rotate key*，或使用KMS软件，即可创建新版本的密钥。

成功轮换密钥后、密钥UID和上次修改字段将更新。

> 如果使用KMS软件旋转加密密钥、请将其从上次使用的密钥版本旋转到同一密钥的新版本。不要旋转到完全不同的键。
>
> 切勿尝试通过更改 KMS 的密钥名称（别名）来旋转密钥。StorageGRID 要求使用相同密钥别名从 KMS 访问以前使用的所有密钥版本（以及将来的任何密钥版本）。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。

管理证书

及时解决任何服务器或客户端证书问题。如果可能、请在证书过期之前进行更换。

要保持数据访问，您必须尽快解决任何证书问题。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。
2. 在表中、查看每个KMS的证书到期时间值。
3. 如果任何KMS的证书到期时间为未知、请等待30分钟、然后刷新Web浏览器。
4. 如果证书到期列指示证书已到期或即将到期、请选择KMS以转到KMS详细信息页面。
   a. 选择*服务器证书*并验证"到期日期"字段的值。
   b. 要替换证书，请选择*编辑证书*以上传新证书。
   c. 重复这些子步骤，并选择*Client certifice*，而不是服务器证书。
5. 触发*KMS CA证书到期*、*KMS客户端证书到期*和*KMS服务器证书到期*警报时，请记下每个警报的问题描述 并执行建议的操作。

   StorageGRID可能需要长达30分钟才能获取证书到期更新。刷新Web浏览器以查看当前值。

如果状态为*服务器证书状态未知*，请确保KMS允许在不需要客户证书的情况下获取服务器证书。

查看加密节点

您可以查看有关 StorageGRID 系统中已启用 * 节点加密 * 设置的设备节点的信息。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。

   此时将显示密钥管理服务器页面。配置详细信息选项卡显示已配置的任何密钥管理服务器。

2. 从页面顶部选择*加密节点*选项卡。

   加密节点选项卡列出了StorageGRID 系统中启用了*Node Encryption *设置的设备节点。

3. 查看表中每个设备节点的信息。

列	说明
节点名称	设备节点的名称。
节点类型	节点的类型：存储，管理或网关。
站点	安装节点的 StorageGRID 站点的名称。

列	说明
Kms名称	用于节点的 KMS 的描述性名称。 如果未列出KMS、请选择配置详细信息选项卡以添加KMS。 "添加密钥管理服务器（ KMS ）"
密钥 UID	用于对设备节点上的数据进行加密和解密的加密密钥的唯一 ID 。要查看整个密钥UID、请选择文本。 短划线（ - ）表示密钥 UID 未知，可能是因为设备节点和 KMS 之间存在连接问题描述 。
状态	KMS 与设备节点之间的连接状态。如果节点已连接，则时间戳每 30 分钟更新一次。更改 KMS 配置后，可能需要几分钟才能更新连接状态。 *注意:*刷新您的Web浏览器以查看新值。

4. 如果状态列指示 KMS 问题描述 ，请立即解决此问题描述 。

   在正常的 KMS 操作期间，状态将为 * 已连接到 KMS* 。如果节点与网格断开连接，则会显示节点连接状态（ administratively down 或 Unknown ）。

   其他状态消息对应于同名的 StorageGRID 警报：

   - 无法加载 Kms 配置
   - Kms 连接错误
   - 未找到 Kms 加密密钥名称
   - Kms 加密密钥轮换失败
   - Kms 密钥无法对设备卷进行解密
   - 未配置公里

   对这些警报执行建议的操作。

   ! 您必须立即解决任何问题，以确保您的数据得到完全保护。

编辑KMS

例如，如果证书即将到期，您可能需要编辑密钥管理服务器的配置。

开始之前

- 如果您计划更新为KMS选择的站点，则已查看"更改站点的 KMS 的注意事项"。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。

   此时将显示密钥管理服务器页面、并显示已配置的所有密钥管理服务器。

2. 选择要编辑的KMS，然后选择*Actions*>*Edit*。

   您也可以通过在表中选择KMS名称并在KMS详细信息页面上选择*Edit*来编辑KMS。

3. (可选)更新编辑密钥管理服务器向导的*步骤1 (KMS详细信息)*中的详细信息。

字段	说明
Kms名称	一个描述性名称，可帮助您标识此 KMS 。必须介于 1 到 64 个字符之间。
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。 在极少数情况下，您只需要编辑密钥名称。例如，如果在 KMS 中重命名了别名，或者先前密钥的所有版本都已复制到新别名的版本历史记录中，则必须编辑密钥名称。
管理的密钥	如果您正在编辑特定于站点的KMS，并且还没有默认的KMS，则可以选择*不由另一个KMS管理的站点(默认KMS)*。此选择会将特定于站点的KMS转换为默认KMS、这将应用于没有专用KMS的所有站点以及扩展中添加的任何站点。 *注:*如果您正在编辑特定于站点的KMS，则不能选择其他站点。如果您正在编辑默认KMS、则无法选择特定站点。
端口	KMS 服务器用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口。默认为 5696 ，即 KMIP 标准端口。
主机名	KMS 的完全限定域名或 IP 地址。 *注意：*服务器证书的使用者替代名称(SAN)字段必须包含您在此处输入的FQDN或IP地址。否则， StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。
5. 选择 * 继续 * 。

   此时将显示编辑密钥管理服务器向导的第2步(上传服务器证书)。

6. 如果需要替换服务器证书，请选择 * 浏览 * 并上传新文件。
7. 选择 * 继续 * 。

   此时将显示编辑密钥管理服务器向导的第3步(上传客户端证书)。

8. 如果需要替换客户端证书和客户端证书专用密钥，请选择 * 浏览 * 并上传新文件。

9. 选择*测试并保存*。

   测试密钥管理服务器与受影响站点上的所有节点加密设备节点之间的连接。如果所有节点连接均有效，并且在 KMS 上找到正确的密钥，则密钥管理服务器将添加到密钥管理服务器页面上的表中。

10. 如果显示错误消息，请查看消息详细信息，然后选择 * 确定 * 。

    例如，如果为此 KMS 选择的站点已由另一个 KMS 管理，或者连接测试失败，则可能会收到 422 ： Unprocessable Entity 错误。

11. 如果需要在解决连接错误之前保存当前配置，请选择*Force save*。

    > 选择*强制保存*可保存KMS配置，但不会测试从每个设备到该KMS的外部连接。如果具有此配置的问题描述 ，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

    此时将保存 KMS 配置。

12. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 * 。

    此时将保存KMS配置、但不会测试与KMS的连接。

删除密钥管理服务器（ **KMS** ）

在某些情况下，您可能需要删除密钥管理服务器。例如，如果您已停用站点，则可能需要删除站点专用的 KMS 。

开始之前

- 您已查看"使用密钥管理服务器的注意事项和要求"。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

关于此任务

在以下情况下，您可以删除 KMS ：

- 如果站点已停用，或者站点中没有启用节点加密的设备节点，则可以删除站点专用的 KMS 。
- 如果每个站点已存在站点专用的 KMS ，并且已启用设备节点加密，则可以删除默认 KMS 。

步骤

1. 选择*配置* > 安全 > 密钥管理服务器。

   此时将显示密钥管理服务器页面、并显示已配置的所有密钥管理服务器。

2. 选择要删除的KMS，然后选择*Actions*>*Remove*。

   您也可以通过在表中选择KMS名称并从KMS详细信息页面中选择*Remove*来删除KMS。

3. 确认满足以下条件：
   - 您要删除某个站点的特定于站点的KMS、而此站点没有启用节点加密的设备节点。

◦ 您要删除默认KMS、但每个站点都已存在具有节点加密的站点专用KMS。

4. 选择 * 是 * 。

   此时将删除 KMS 配置。

管理代理设置

配置 StorageGRID 存储代理

如果您使用的是平台服务或云存储池，则可以在存储节点和外部 S3 端点之间配置非透明代理。例如，您可能需要一个非透明代理来允许将平台服务消息发送到外部端点，例如 Internet 上的端点。

配置的存储代理设置不适用于Kafka平台服务端点。

开始之前

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

关于此任务

您可以为单个存储代理配置设置。

步骤

1. 选择*配置* > 安全 > 代理设置。
2. 在*存储*选项卡上，选中*启用存储代理*复选框。
3. 选择存储代理的协议。
4. 输入代理服务器的主机名或 IP 地址。
5. （可选）输入用于连接到代理服务器的端口。

   将此字段留空以使用协议的默认端口：80表示HTTP、1080表示SOCK5。

6. 选择 * 保存 * 。

   保存存储代理后、可以配置和测试平台服务或云存储池的新端点。

   代理更改可能需要长达 10 分钟才能生效。

7. 检查代理服务器的设置，以确保不会阻止来自 StorageGRID 的平台服务相关消息。
8. 如果需要禁用存储代理，请清除该复选框，然后选择*Save*。

相关信息

"用于外部通信的端口"

如果使用HTTP或HTTPS发送AutoSupport软件包、则可以在管理节点和技术支持(AutoSupport)之间配置非透明代理服务器。

有关 AutoSupport 的详细信息，请参见 "配置 AutoSupport"。

开始之前

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

关于此任务

您可以为单个管理代理配置设置。

步骤

1. 选择*配置* > 安全 > 代理设置。

   此时将显示代理设置页面。默认情况下、存储在选项卡菜单中处于选中状态。

2. 选择*Admin*选项卡。
3. 选中*启用管理员代理*复选框。
4. 输入代理服务器的主机名或 IP 地址。
5. 输入用于连接到代理服务器的端口。
6. (可选)输入代理服务器的用户名和密码。

   如果代理服务器不需要用户名或密码、请将这些字段留空。

7. 选择以下选项之一：

   ◦ 如果要保护与管理员代理的连接，请选择*验证代理证书*。上传CA分发包以验证管理代理服务器提供的SSL证书的真实性。

   > 如果验证了代理证书、则AutoSupport On Demand、E系列AutoSupport到StorageGRID以及StorageGRID升级页面上的更新路径确定将不起作用。

   上载CA分发包后、将显示其元数据。

   ◦ 如果在与管理代理服务器通信时不想验证证书，请选择*不验证代理证书*。

8. 选择 * 保存 * 。

   保存管理代理后、将配置管理节点与技术支持之间的代理服务器。

   > 代理更改可能需要长达 10 分钟才能生效。

9. 如果需要禁用管理员代理，请清除*启用管理员代理*复选框，然后选择*保存*。

在外部防火墙处控制 **StorageGRID** 访问

您可以在外部防火墙处打开或关闭特定端口。

您可以通过在外部防火墙中打开或关闭特定端口来控制对 StorageGRID 管理节点上用户界面和 API 的访问。例如，除了使用其他方法控制系统访问之外，您可能还希望防止租户能够在防火墙处连接到网格管理器。

如果要配置StorageGRID内部防火墙，请参见"配置内部防火墙"。

端口	说明	端口是否已打开 ...
443	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问网格管理器，网格管理 API ，租户管理器和租户管理 API 。 • 注： * 端口 443 也用于某些内部流量。
8443	管理节点上的网格管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问网格管理器和网格管理 API 。 • Web浏览器和管理API客户端无法访问租户管理器或租户管理API。 • 请求内部内容将被拒绝。
9443	管理节点上的租户管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问租户管理器和租户管理 API 。 • Web浏览器和管理API客户端无法访问网格管理器或网格管理API。 • 请求内部内容将被拒绝。

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

相关信息

- "登录到网格管理器"
- "创建租户帐户"
- "外部通信"

管理 **StorageGRID** 中的内部防火墙控制

StorageGRID 在每个节点上都包含一个内部防火墙、可通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止对特定网格部署所需端口以外的所有端口进行网络访问。在防火墙控制页面上所做的配置更改将部署到每个节点。

使用防火墙控制页面上的三个选项卡自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡允许对关闭的端口进行选定访问。您可以使用CIDR表示法添加IP地址或子网、以访问使用管理外部访问选项卡关闭的端口。
- 管理外部访问：使用此选项卡关闭默认打开的端口，或重新打开先前关闭的端口。
- 不可信客户端网络：使用此选项卡指定节点是否信任来自客户端网络的入站流量。

  此选项卡上的设置将覆盖管理外部访问选项卡中的设置。

  - 具有不可信客户端网络的节点仅接受在该节点上配置的负载平衡器端点端口(全局端点、节点接口和受节点类型制约的端点)上的连接。
  - 负载平衡器端点端口_是不可信客户端网络上唯一打开的端口_、与管理外部网络选项卡上的设置无关。
  - 如果受信任、则可以访问在"管理外部访问"选项卡下打开的所有端口以及在客户端网络上打开的任何负载平衡器端点。

> 您在一个选项卡上所做的设置可能会影响您在另一个选项卡上所做的访问更改。请务必检查所有选项卡上的设置、以确保您的网络按预期方式运行。

要配置内部防火墙控制，请参见"配置防火墙控件"。

有关外部防火墙和网络安全的详细信息，请参阅"在外部防火墙处控制访问"。

特权地址列表和管理外部访问选项卡

通过特权地址列表选项卡、您可以注册一个或多个被授予对关闭的网格端口访问权限的IP地址。通过"管理外部访问"选项卡、您可以关闭对选定外部端口或所有打开的外部端口的外部访问(默认情况下、外部端口可由非网格节点访问)。这两个选项卡通常可结合使用来定制网格所需的确切网络访问。

> 默认情况下、有权限的IP地址不具有内部网格端口访问权限。

示例**1**：使用跳转主机执行维护任务

假设您要使用跳转主机(一个增强安全的主机)进行网络管理。您可以使用以下常规步骤：

1. 使用特权地址列表选项卡添加跳转主机的IP地址。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后、网格中管理节点上的所有外部端口都将被阻止用于除跳转主机之外的所有主机。然后、您可以使用跳转主机更安全地在网格上执行维护任务。

示例**2**：锁定敏感端口

假设您想要锁定敏感端口和该端口上的服务。您可以使用以下一般步骤：

1. 使用特权地址列表选项卡仅向需要访问服务的主机授予访问权限。
2. 使用管理外部访问选项卡阻止所有端口。

在阻止访问分配给网格管理器和租户管理器的任何端口之前、请添加特权IP地址(预设端口为443和8443)。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后，敏感端口和该端口上的服务可供特权地址列表中的主机使用。无论请求来自哪个接口，所有其他主机都被拒绝访问该服务。

示例**3**：禁止访问未使用的服务

在网络级别、您可以禁用一些不打算使用的服务。例如、要阻止HTTP S3客户端流量、您可以使用管理外部访问选项卡上的切换来阻止端口18084。

不可信客户端网络选项卡

如果您使用的是客户端网络，则可以通过仅在显式配置的端点上接受入站客户端流量来帮助保护 StorageGRID 免受恶意攻击。

默认情况下，每个网格节点上的客户端网络均为 *trusted* 。也就是说，默认情况下，StorageGRID信任所有上每个网格节点的入站连接"可用外部端口"。

您可以通过指定每个节点上的客户端网络为 *untrused_* 来减少对 StorageGRID 系统的恶意攻击威胁。如果节点的客户端网络不可信，则节点仅接受显式配置为负载平衡器端点的端口上的入站连接。请参阅"配置负载平衡器端点"和"配置防火墙控件"。

示例 **1** ： 网关节点仅接受 **HTTPS S3** 请求

假设您希望网关节点拒绝客户端网络上除 HTTPS S3 请求以外的所有入站流量。您应执行以下常规步骤：

1. 在页面中"负载平衡器端点"、通过端口443为基于HTTPS的S3配置负载平衡器端点。
2. 在防火墙控制页面中、选择不可信以指定网关节点上的客户端网络不可信。

保存配置后，网关节点客户端网络上的所有入站流量都会被丢弃，但端口 443 上的 HTTPS S3 请求和 ICMP 回显（ ping ）请求除外。

示例 **2** ： 存储节点发送 **S3** 平台服务请求

假设您要启用来自存储节点的出站S3平台服务流量、但要阻止客户端网络上与该存储节点的任何入站连接。您应执行此常规步骤：

- 在防火墙控制页面的不可信客户端网络选项卡中、指示存储节点上的客户端网络不可信。

保存配置后、存储节点将不再接受客户端网络上的任何传入流量、但仍允许向已配置的平台服务目标发出出站请求。

示例**3**：限制对网格管理器的子网访问

假设您希望仅允许对特定子网进行网格管理器访问。您应执行以下步骤：

1. 将管理节点的客户端网络连接到子网。
2. 使用不可信客户端网络选项卡将客户端网络配置为不可信。

3. 创建管理接口负载平衡器端点时、输入port并选择端口要访问的管理接口。
4. 对不可信客户端网络选择*Yes*。
5. 使用管理外部访问选项卡阻止所有外部端口(无论是否为该子网以外的主机设置了特权IP地址)。

保存配置后、只有指定子网上的主机才能访问网格管理器。所有其他主机均被阻止。

配置 **StorageGRID** 内部防火墙

您可以配置StorageGRID 防火墙以控制对StorageGRID 节点上特定端口的网络访问。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 您已查看和中的信息"管理防火墙控制""网络连接准则"。
- 如果您希望管理节点或网关节点仅在显式配置的端点上接受入站流量，则已定义负载平衡器端点。

> 更改客户端网络的配置时、如果未配置负载平衡器端点、现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上都有一个内部防火墙、可用于打开或关闭网格节点上的部分端口。您可以使用防火墙控制选项卡打开或关闭网格网络、管理网络和客户端网络上默认打开的端口。您还可以创建一个可访问关闭的网格端口的特权IP地址列表。如果您使用的是客户端网络、则可以指定节点是否信任客户端网络的入站流量、并且可以配置客户端网络上特定端口的访问。

将向网格外部的IP地址开放的端口数限制为仅限绝对必要的端口、可增强网格的安全性。您可以使用三个防火墙控制选项卡中每个选项卡上的设置来确保仅打开所需的端口。

有关使用防火墙控件的详细信息，包括示例，请参阅 "管理防火墙控制"。

有关外部防火墙和网络安全的详细信息，请参阅 "在外部防火墙处控制访问"。

访问防火墙控件

步骤

1. 选择*配置* > 安全 > 防火墙控制。

   此页面上的三个选项卡在中"管理防火墙控制"进行了介绍。

2. 选择任何选项卡以配置防火墙控件。

   您可以按任意顺序使用这些选项卡。您在一个选项卡上设置的配置不会限制在其他选项卡上可以执行的操作；但是、在一个选项卡上进行的配置更改可能会更改在其他选项卡上配置的端口的行为。

特权地址列表

您可以使用特权地址列表选项卡授予主机对默认关闭或通过管理外部访问选项卡上的设置关闭的端口的访问权限。

默认情况下、有权限的IP地址和子网不具有内部网格访问权限。此外、即使在"管理外部访问"选项卡中阻止了负载平衡器端点和在"特权地址列表"选项卡中打开的其他端口、也可以访问。

"特权地址列表"选项卡上的设置可以覆盖"不受信任的客户端网络"选项卡上的设置。

步骤

1. 在特权地址列表选项卡上、输入要授予对已关闭端口的访问权限的地址或IP子网。
2. （可选）选择 **Add another IP or a subnet in CIDR notation** 以添加其他特权客户端。

   向特权列表中添加尽可能少的地址。

3. 可选，选择*允许特权 IP 地址访问 StorageGRID 内部端口*。请参阅 "StorageGRID 内部端口"。

   此选项会删除对内部服务的一些保护。如果可能、请将其禁用。

4. 选择 * 保存 * 。

管理外部访问

在"管理外部访问"选项卡中关闭某个端口后、任何非网格IP地址都无法访问该端口、除非您将该IP地址添加到特权地址列表中。您只能关闭默认情况下处于打开状态的端口、并且只能打开已关闭的端口。

"管理外部访问"选项卡上的设置无法覆盖"不可信客户端网络"选项卡上的设置。例如、如果节点不可信、则客户端网络上会阻止端口SSH/ 22、即使此端口在管理外部访问选项卡上打开也是如此。不可信客户端网络选项卡上的设置会覆盖客户端网络上已关闭的端口(例如443、8443、9443)。

步骤

1. 选择*管理外部访问*。此选项卡将显示一个表、其中包含网格中节点的所有外部端口(默认情况下可由非网格节点访问的端口)。
2. 使用以下选项配置要打开和关闭的端口：
   - 使用每个端口旁边的切换键打开或关闭选定端口。
   - 选择*打开所有显示的端口*以打开表中列出的所有端口。
   - 选择*关闭所有显示的端口*以关闭表中列出的所有端口。

     如果关闭 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。

   使用表右侧的滚动条确保您已查看所有可用端口。使用搜索字段输入端口号以查找任何外部端口的设置。您可以输入部分端口号。例如，如果输入*2*，则会显示名称中包含字符串“2”的所有端口。

3. 选择 * 保存 *

不可信客户端网络

如果节点的客户端网络不可信、则该节点仅接受配置为负载平衡器端点的端口以及您在此选项卡上选择的其他端口(可选)上的入站流量。您还可以使用此选项卡为扩展中添加的新节点指定默认设置。

如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

在*不可信客户端网络*选项卡上所做的配置更改将覆盖*管理外部访问*选项卡上的设置。

步骤

1. 选择*不可信客户端网络*。
2. 在设置新节点默认值部分中、指定在扩展操作步骤 中向网格添加新节点时的默认设置。
   - 可信(默认)：在扩展中添加节点时、其客户端网络是可信的。
   - * 不可信 * ：在扩展中添加节点时，其客户端网络不可信。

   您可以根据需要返回此选项卡来更改特定新节点的设置。

   此设置不会影响 StorageGRID 系统中的现有节点。
3. 使用以下选项选择仅允许在显式配置的负载平衡器端点或其他选定端口上进行客户端连接的节点：
   - 选择*在显示的节点上取消信任*，将表中显示的所有节点添加到不可信客户端网络列表中。
   - 选择*在显示的节点上信任*，从不可信客户端网络列表中删除表中显示的所有节点。
   - 使用每个节点旁边的切换功能将选定节点的客户端网络设置为可信或不可信。

   例如，您可以选择*Untrust on displayed N点*将所有节点添加到Untrusted Client Network列表中，然后使用单个节点旁边的切换将该单个节点添加到Trusted Client Network列表中。

   使用表右侧的滚动条确保您已查看所有可用节点。使用搜索字段输入节点名称以查找任何节点的设置。您可以输入部分名称。例如，如果输入*GW*，则会显示名称中包含字符串"gw"的所有节点。
4. 选择 * 保存 * 。

   新的防火墙设置将立即应用和实施。如果尚未配置负载均衡器端点，现有客户端连接可能会失败。

管理租户

StorageGRID 中的租户帐户

租户帐户允许您使用简单存储服务(S3) REST API在StorageGRID系统中存储和检索对象。

Swift详细信息已从此版本的文档站点中删除。请参阅。 "StorageGRID 11.8:管理租户"

作为网格管理员、您可以创建和管理S3客户端用于存储和检索对象的租户帐户。

每个租户帐户都具有联合组或本地组、用户、S3分段和对象。

租户帐户可用于按不同实体隔离存储的对象。例如，以下任一使用情形均可使用多个租户帐户：

- * 企业用例： * 如果您在企业应用程序中管理 StorageGRID 系统，则可能需要按组织中的不同部门隔离网格的对象存储。在这种情况下，您可以为营销部门，客户支持部门，人力资源部门等创建租户帐户。

> 如果您使用 S3 客户端协议，则可以使用 S3 存储桶和存储桶策略在企业各部门之间隔离对象。您不需要使用租户帐户。请参阅实施说明"S3存储分段和存储分段策略"了解更多信息。

- * 服务提供商用例： * 如果您将 StorageGRID 系统作为服务提供商进行管理，则可以按要在网格上租用存储的不同实体来隔离网格的对象存储。在这种情况下，您将为公司 A ，公司 B ，公司 C 等创建租户帐户。

有关详细信息，请参见 "使用租户帐户"。

如何创建租户帐户？

使用网格管理器创建租户帐户。创建租户帐户时，您可以指定以下信息：

- 基本信息、包括租户名称、客户端类型(S3)和可选存储配额。
- 租户帐户的权限、例如租户帐户是否可以使用S3平台服务、配置自己的身份源、使用S3 Select或使用网格联盟连接。
- 租户的初始root访问权限、具体取决于StorageGRID 系统是使用本地组和用户、身份联合还是单点登录(SSO)。

此外、如果S3租户帐户需要符合法规要求、您可以为StorageGRID 系统启用S3对象锁定设置。启用 S3 对象锁定后，所有 S3 租户帐户均可创建和管理合规的存储分段。

租户管理器的用途是什么？

创建租户帐户后、租户用户可以登录到租户管理器来执行如下任务：

- 设置身份联合(除非身份源与网格共享)
- 管理组和用户
- 使用网格联合进行帐户同步和跨网格复制
- 管理 S3 访问密钥
- 创建和管理S3存储分段
- 使用S3平台服务
- 使用 S3 Select
- 监控存储使用情况

> 虽然S3租户用户可以使用租户管理器创建和管理S3访问密钥和存储分段、但他们必须使用S3客户端应用程序来加存和管理对象。有关详细信息、请参见。 "使用S3 REST API"

创建 **StorageGRID** 租户帐户

您必须至少创建一个租户帐户，才能控制对 StorageGRID 系统中存储的访问。

创建租户帐户的步骤取决于"身份联合"和"单点登录"是否配置，以及用于创建租户帐户的网格管理器帐户是否属于具有 Root 访问权限的管理员组。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限或租户帐户权限"。
- 如果租户帐户将使用为网格管理器配置的身份源，并且您要将租户帐户的 root 访问权限授予某个联合组，则您已将该联合组导入到网格管理器中。您无需为此管理员组分配任何网格管理器权限。请参阅。 "管理管理组"
- 如果要允许 S3 租户使用网格联合连接同步帐户数据并将存储区对象复制到另一个网格：
  - 您拥有 "已配置网格联合连接"。
  - 连接状态为*已连接*。
  - 您具有 root 访问权限。
  - 您已查看的注意事项"管理网格联盟允许的租户"。
  - 如果租户帐户将使用为Grid Manager配置的身份源、则您已将同一联盟组导入到两个网格上的Grid Manager中。

    创建租户时、您需要选择此组、以获得源租户帐户和目标租户帐户的初始root访问权限。

    如果在创建租户之前此管理员组不在两个网格上、则不会将租户复制到目标。

访问向导

步骤

1. 选择*租户*。
2. 选择 * 创建 * 。

输入详细信息

步骤

1. 输入租户的详细信息。

字段	说明
名称	租户帐户的名称。租户名称不需要唯一。创建租户帐户时、它会收到一个唯一的20位数帐户ID。

字段	说明
问题描述 (可选)	用于帮助识别租户的问题描述。 如果您要创建将使用网格联合连接的租户、也可以使用此字段帮助确定哪个是源租户、哪个是目标租户。例如、对于在网格1上创建的租户、如果该租户复制到网格2、则也会显示此问题描述： "This租户was created on Grid 1"(此租户已在网格1上创建)。
客户端类型	必须为*S3*。
存储配额(可选)	如果希望此租户具有存储配额、则为配额和单位指定一个数值。

2. 选择 * 继续 * 。

[[admin-租 户**-Select-permissions]]**选择权限

步骤

1. (可选)选择希望此租户具有的基本权限。

   其中某些权限还有其他要求。有关详细信息、请选择每个权限的帮助图标。

权限	如果选择...
允许平台服务	租户可以使用CloudMirror等S3平台服务。请参阅。 "管理 S3 租户帐户的平台服务"
使用自己的身份源	租户可以为联合组和用户配置和管理自己的身份源。如果您有以下情况，则此选项被禁用"已配置SSO"适用于您的StorageGRID系统。
允许S3选择	租户可以通过问题描述 S3选择对象内容API请求筛选和检索对象数据。请参阅。 "管理租户帐户的 S3 Select" 重要：选择对象内容请求会降低所有S3客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。

2. (可选)选择希望此租户具有的高级权限。

权限	如果选择...
网格联合连接	租户可以使用网格联合连接，这些连接： • 使此租户帐户以及所有租户组、用户和 S3 访问密钥在此网格与选定连接中的其他网格之间同步。 如果出于安全或合规原因需要，您可以取消选择*启用访问密钥同步*。 • 允许此租户在每个网格上的相应分段之间配置跨网格复制。 请参阅。 "管理网格联盟允许的租户"
S3 对象锁定	允许租户使用S3对象锁定的特定功能： • *设置最长保留期限*用于定义添加到此存储分段的新对象应保留多长时间、从其被插入开始。 • *允许兼容模式*可防止用户在保留期间覆盖或删除受保护的对象版本。

3. 选择 * 继续 * 。

定义**root**访问权限并创建租户

步骤

1. 根据您的StorageGRID 系统是使用身份联合、单点登录(SSO)还是同时使用这两者、定义租户帐户的root访问权限。

选项	执行此操作 ...
如果未启用身份联合	指定以本地root用户身份登录租户时要使用的密码。
如果启用了身份联合	a. 选择一个现有联盟组、以便对租户具有root访问权限。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择一个现有联盟组、以便对租户具有root访问权限。没有本地用户可以登录。

2. 选择 * 创建租户 * 。

   此时将显示一条成功消息、新租户将列在租户页面上。要了解如何查看租户详细信息和监控租户活动，请参见"监控租户活动"。

   根据网络连接、节点状态和cassandr操作、在网格中应用租户设置可能需要15分钟或更长时间。

3. 如果您为租户选择了*使用网格联合连接*权限，请确认已将相同的租户复制到连接中的另一个网格。两个网

格上的租户将具有相同的 20 位帐户 ID、名称、描述、配额和权限。

> 如果您看到一条错误消息，指出租户帐户是在此网格上创建的，但未同步到其他网格，请参阅 "对网格联合错误进行故障排除" 中的说明。

登录到租户(可选)

您可以根据需要立即登录到新租户以完成配置、也可以稍后登录到租户。登录步骤取决于您是使用默认端口(443)还是使用受限端口登录到网格管理器。请参阅。 "在外部防火墙处控制访问"

立即登录

如果使用的是...	操作
端口443、并且您为本地root用户设置了密码	1. 选择*以root身份登录*。 登录时、将显示用于配置分段、身份联合、组和用户的链接。 2. 选择用于配置租户帐户的链接。 每个链接都会在租户管理器中打开相应的页面。要完成此页面，请参见"有关使用租户帐户的说明"。
端口443、并且您没有为本地root用户设置密码	选择*Sign In*，然后输入root访问联合组中用户的凭据。
受限端口	1. 选择*完成* 2. 在租户表中选择*受限*、了解有关访问此租户帐户的更多信息。 租户管理器的 URL 格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`是管理节点的完全限定域名或IP地址 ◦ `port`是仅租户端口 ◦ `20-digit-account-id`是租户的唯一帐户ID

请稍后登录

如果使用的是...	执行以下操作之一 ...
端口 443	• 从网格管理器中，选择“租户”，然后选择租户名称右侧的“Sign in”。 • 在 Web 浏览器中输入租户的 URL： `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`是管理节点的完全限定域名或IP地址 ◦ `20-digit-account-id`是租户的唯一帐户ID
受限端口	• 从网格管理器中，选择*租户*，然后选择*受限*。 • 在 Web 浏览器中输入租户的 URL： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `FQDN_or_Admin_Node_IP`是管理节点的完全限定域名或IP地址 ◦ `port`是仅租户受限端口 ◦ `20-digit-account-id`是租户的唯一帐户ID

配置租户

按照 "使用租户帐户" 中的说明管理租户组和用户、S3 访问密钥、存储桶、平台服务以及帐户同步和跨网格复制。

编辑 **StorageGRID** 租户帐户

您可以编辑租户帐户以更改显示名称、存储配额或租户权限。

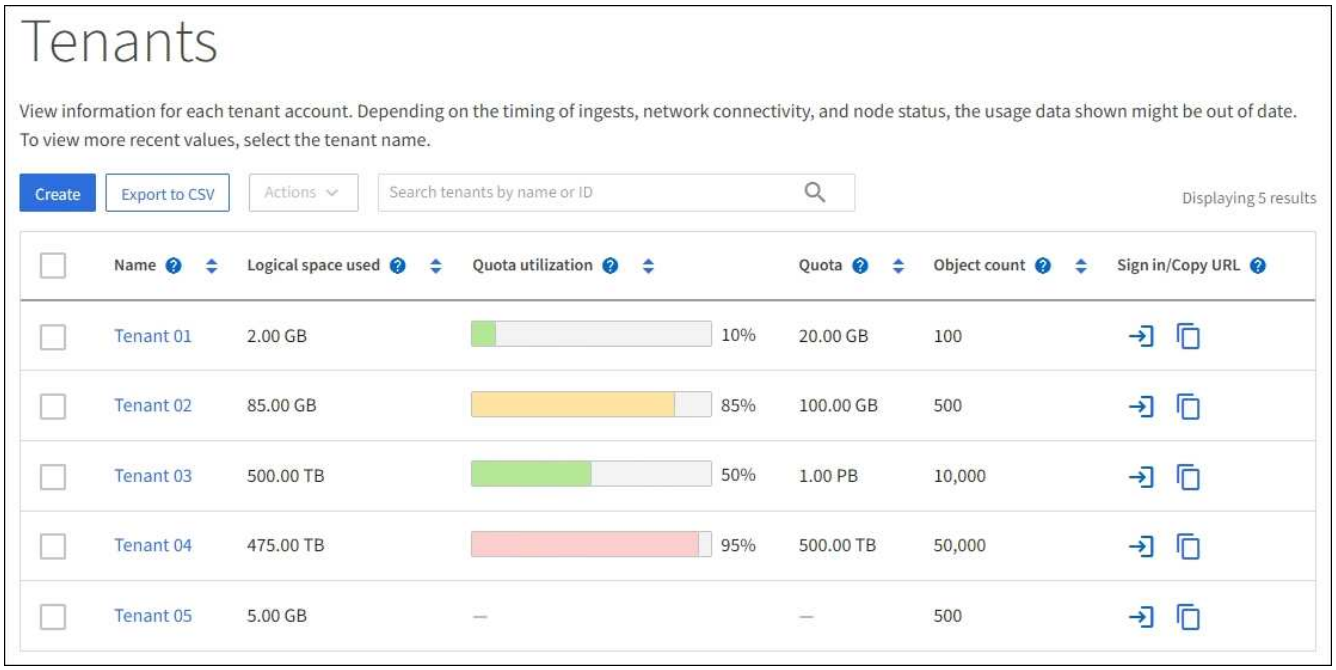
开始之前

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

根据网络连接、节点状态和cassandr操作、在网格中应用租户设置可能需要15分钟或更长时间。

步骤

1. 选择*租户*。



2. 找到要编辑的租户帐户。

   使用搜索框按名称或租户ID搜索租户。

3. 选择租户。您可以执行以下任一操作：
   - 选中租户对应的复选框，然后选择*Actions*>*Edit*。
   - 选择租户名称以显示详细信息页面，然后选择*Edit*。
4. (可选)更改以下字段的值：
   - * 名称 *
   - * 问题描述 *
   - * 存储配额 *
5. 选择 * 继续 * 。
6. 选择或清除租户帐户的权限。
   - 如果对已在使用 * 平台服务 * 的租户禁用此服务，则其为 S3 分段配置的服务将停止工作。不会向租户发送任何错误消息。例如，如果租户已为 S3 存储分段配置了 CloudMirror 复制，则他们仍可将对象存储在存储分段中，但这些对象的副本将不再创建在已配置为端点的外部 S3 存储分段中。请参阅。 "管理 S3 租户帐户的平台服务"
   - 更改*使用自己的身份源*设置以确定租户帐户是使用自己的身份源还是使用为网格管理器配置的身份源。

     如果*使用自己的身份源*是：

     - 已禁用并选中、租户已启用自己的身份源。租户必须先禁用其身份源，然后才能使用为网格管理器配置的身份源。
     - 已禁用但未选中、已为StorageGRID 系统启用SSO。租户必须使用为网格管理器配置的身份源。
   - 根据需要选中或清除*允许S3 Select*权限。请参阅。 "管理租户帐户的 S3 Select"

- 删除*使用网格联合连接*权限：
  i. 在租户详细信息页面上选择网格联合选项卡。
  ii. 选择要删除的连接。
  iii. 选择*删除权限*。
- 要添加*使用网格联合连接*权限：
  i. 选择*网格联盟*选项卡。
  ii. 选中*使用网格联合连接*复选框。
  iii. (可选)选择*克隆现有本地用户和组*将其克隆到远程网格。如果需要、您可以停止正在进行的克隆、或者在上次克隆操作完成后克隆某些本地用户或组失败时重试克隆。

  如果出于安全或合规原因需要，您可以取消选择*启用访问密钥同步*。

- 要设置最长保留期限或允许合规模式、请执行以下操作：

  必须先在网格上启用S3对象锁定、然后才能使用这些设置。

  i. 选择*S3对象锁定*选项卡。
  ii. 对于*设置最大保留期限*，请输入一个值，然后从下拉列表中选择时间段。
  iii. 对于*允许兼容模式*，选中复选框。

更改 **StorageGRID** 租户的本地 **root** 用户密码

如果 root 用户被锁定在帐户之外，您可能需要更改租户的本地 root 用户的密码。

开始之前

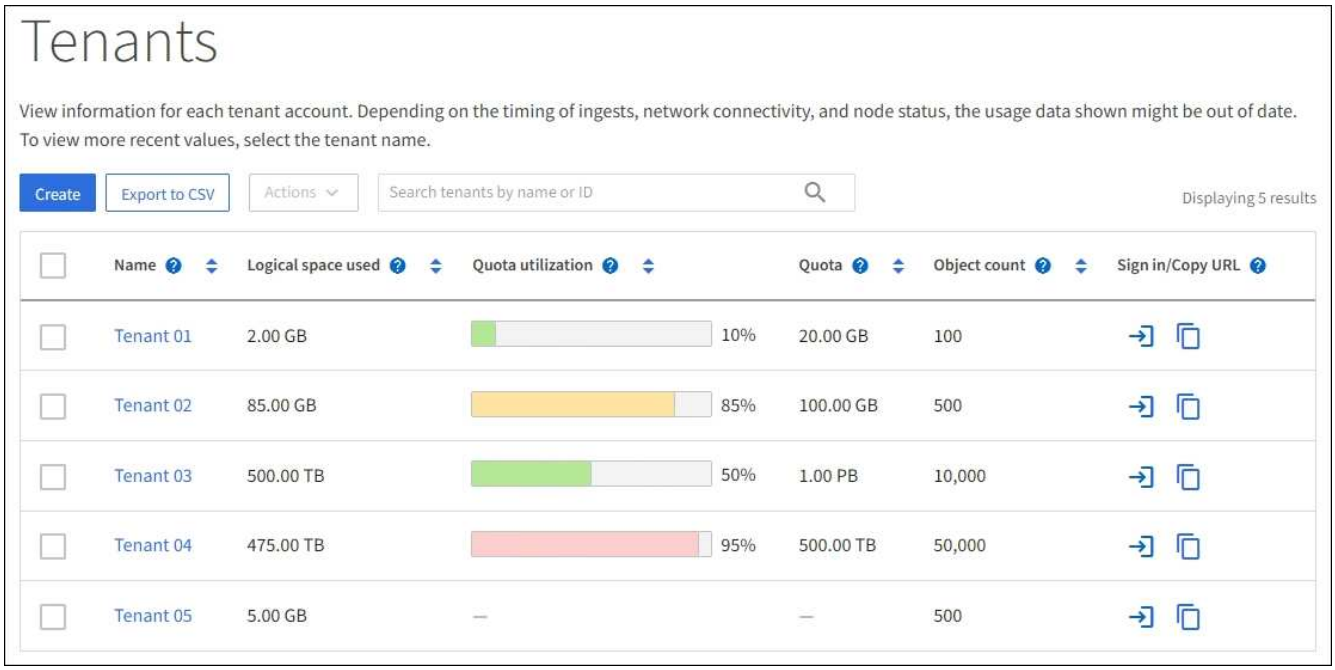
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。

关于此任务

如果为StorageGRID 系统启用了单点登录(SSO)、则本地root用户无法登录到租户帐户。要执行 root 用户任务，用户必须属于对租户具有 root 访问权限的联合组。

步骤

1. 选择*租户*。



2. 选择租户帐户。您可以执行以下任一操作：
   - 选中租户对应的复选框，然后选择*Actions*>*更改root密码*。
   - 选择租户的名称以显示详细信息页面，然后选择*Actions*>*更改root密码*。
3. 输入租户帐户的新密码。
4. 选择 * 保存 * 。

删除 **StorageGRID** 租户帐户

如果要永久删除租户对系统的访问权限，可以删除租户帐户。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 您已删除与租户帐户关联的所有S3存储分段和对象。
- 如果允许租户使用网格联合连接，您已查看了"删除具有使用网格联盟连接权限的租户"的注意事项。删除操作会同步，因此如果在任何网格上删除租户，该租户将在所有选定的网格上被删除。

步骤

1. 选择*租户*。
2. 找到要删除的租户帐户。

   使用搜索框按名称或租户ID搜索租户。
3. 要删除多个租户，请选中复选框，然后选择*Actions*>*Delete*。
4. 要删除单个租户、请执行以下操作之一：
   - 选中该复选框，然后选择*Actions*>*Delete*。

- 选择租户名称以显示详细信息页面、然后选择*操作*>*删除*。

5. 选择 * 是 * 。

管理平台服务

了解 **StorageGRID** 平台服务

平台服务包括 CloudMirror 复制，事件通知和搜索集成服务。

如果为 S3 租户帐户启用平台服务，则必须配置网格，以便租户可以访问使用这些服务所需的外部资源。

平台服务不支持"分支桶"。

CloudMirror 复制

StorageGRID CloudMirror复制服务用于将特定对象从StorageGRID存储分段镜像到指定的外部目标。

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

CloudMirror复制与跨网格复制功能有一些重要的相似之处和不同之处。要了解更多信息，请参阅"请比较跨网格复制和CloudMirror复制"。

通知

每个存储桶事件通知用于将有关对对象执行的特定操作的通知发送到指定的外部 Kafka 集群、webhook 端点或 Amazon Simple Notification Service。

例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

> 虽然可以在启用了 S3 对象锁定的存储分段上配置事件通知，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留至日期和合法保留状态）。

搜索集成服务

搜索集成服务用于将S3对象元数据发送到指定的EI路径 搜索索引、在该索引中、可以使用外部服务搜索或分析元数据。

例如，您可以将存储分段配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 跨存储分段执行搜索，并对对象元数据中存在的模式执行复杂的分析。

> 虽然可以在启用了 S3 对象锁定的情况下在存储分段上配置 Elasticsearch 集成，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留截止日期和合法保留状态）。

通过平台服务，租户可以对其数据使用外部存储资源，通知服务以及搜索或分析服务。由于平台服务的目标位置通常位于 StorageGRID 部署外部，因此您必须确定是否要允许租户使用这些服务。如果是，则必须在创建或编辑租户帐户时启用平台服务。您还必须配置网络，使租户生成的平台服务消息能够访问其目标。

使用平台服务的建议

在使用平台服务之前，请注意以下建议：

- 如果 StorageGRID 系统中的 S3 存储分段同时启用了版本控制和 CloudMirror 复制，则还应为目标端点启用 S3 存储分段版本控制。这样， CloudMirror 复制就可以在端点上生成类似的对象版本。
- 如果 S3 请求需要进行 CloudMirror 复制，通知和搜索集成，则使用的活动租户不应超过 100 个。如果活动租户超过 100 个，则可能会导致 S3 客户端性能下降。
- 发送到无法完成的端点的请求最多将排队到500、000个请求。此限制在活动租户之间平均共享。允许新租户暂时超过此500、000限制、以便新创建的租户不会受到不公平的处罚。

相关信息

- "管理平台服务"
- "配置存储代理设置"
- "监控StorageGRID"

StorageGRID 平台服务的网络和端口

如果允许 S3 租户使用平台服务，则必须为网格配置网络连接，以确保平台服务消息可以传送到其目标。

在创建或更新 S3 租户帐户时，您可以为该租户帐户启用平台服务。如果启用了平台服务，则租户可以创建端点，用作 CloudMirror 复制，事件通知或从其 S3 存储分段搜索集成消息的目标。这些平台服务消息会从运行此 ADA 服务的存储节点发送到目标端点。

例如，租户可以配置以下类型的目标端点：

- 本地托管的 Elasticsearch 集群
- 支持接收Amazon Simple Notification Service消息的本地应用程序
- 本地托管的Kafka集群
- 支持 HTTP POST 通知请求的外部或本地托管的 webhook 端点。

  该端点可以托管在各种 Web 服务器、框架或数据处理工具（例如 Fluentd）上。
- 同一个或另一个 StorageGRID 实例上本地托管的 S3 存储分段
- 外部端点，例如 Amazon Web Services 上的端点。

要确保可以传送平台服务消息，您必须配置一个或多个包含此 ADA 存储节点的网络。您必须确保可使用以下端口向目标端点发送平台服务消息。

默认情况下，平台服务消息在以下端口上发送：

- **80**：对于以http开头的端点URI (大多数端点)
- **443**：对于以https开头的端点URL (大多数端点)
- **9092**：对于以http或https开头的端点URL (仅限Kafka端点)

租户可以在创建或编辑端点时指定其他端口。

如果使用 StorageGRID 部署作为 CloudMirror 复制的目标，则可能会在 80 或 443 以外的端口上收到复制消息。确保已在端点中指定目标 StorageGRID 部署用于 S3 的端口。

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

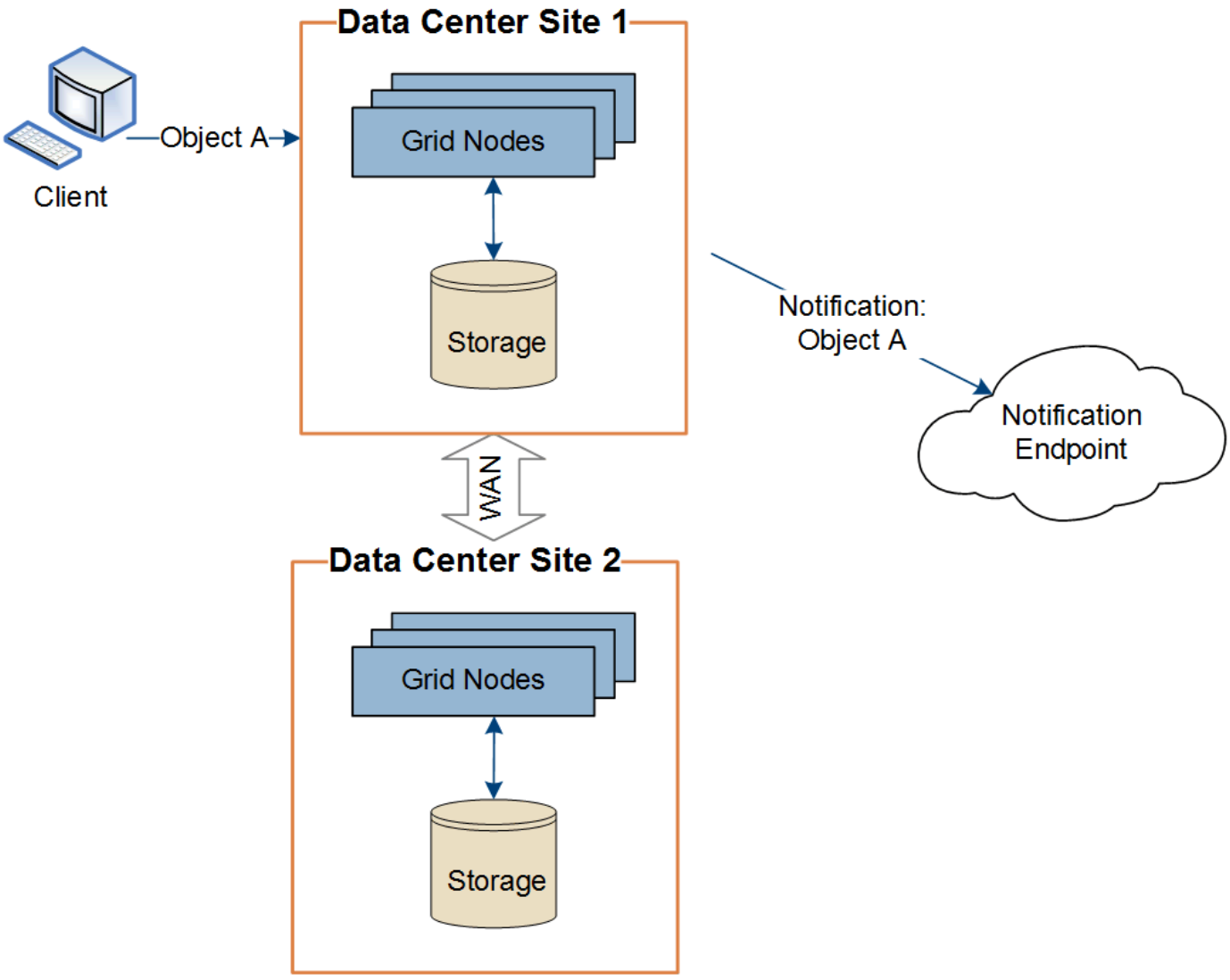
相关信息

- "使用租户帐户"
- "用于外部通信的端口"

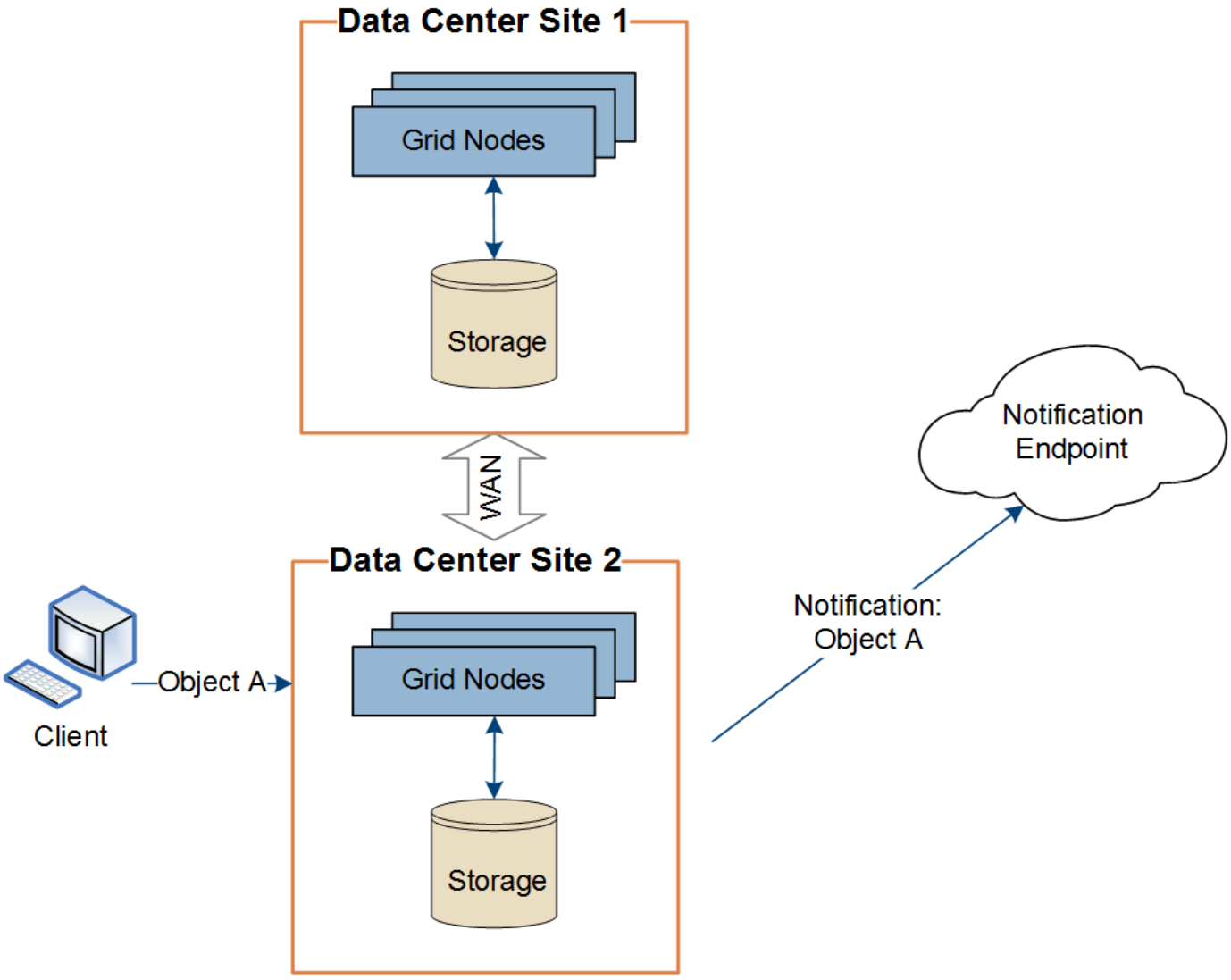
按站点交付 **StorageGRID** 平台服务消息

所有平台服务操作均按站点执行。

也就是说，如果租户使用客户端通过连接到数据中心站点 1 的网关节点对对象执行 S3 API 创建操作，则会从数据中心站点 1 触发并发送有关该操作的通知。



如果客户端随后从数据中心站点 2 对同一对象执行 S3 API 删除操作，则会从数据中心站点 2 触发并发送有关删除操作的通知。



请确保在每个站点上配置网络，以便平台服务消息可以传送到其目标。

StorageGRID 平台服务故障排除

平台服务中使用的端点由租户管理器中的租户用户创建和维护。但是，如果租户在配置或使用平台服务时遇到问题，则可以使用网格管理器来帮助解决此问题。

新端点出现问题

租户必须先使用租户管理器创建一个或多个端点，才能使用平台服务。每个端点代表一个平台服务的外部目标、例如StorageGRID S3存储分段、Amazon Web Services存储分段、Amazon Simple Notification Service主题、Kafka主题或本地或AWS上托管的ElanicSearch集群。每个端点都包括外部资源的位置以及访问该资源所需的凭据。

租户创建端点时， StorageGRID 系统会验证此端点是否存在，以及是否可以使用指定的凭据访问此端点。系统会从每个站点的一个节点验证与端点的连接。

如果端点验证失败，则会显示一条错误消息，说明端点验证失败的原因。租户用户应解析问题描述 ，然后重新尝试创建端点。

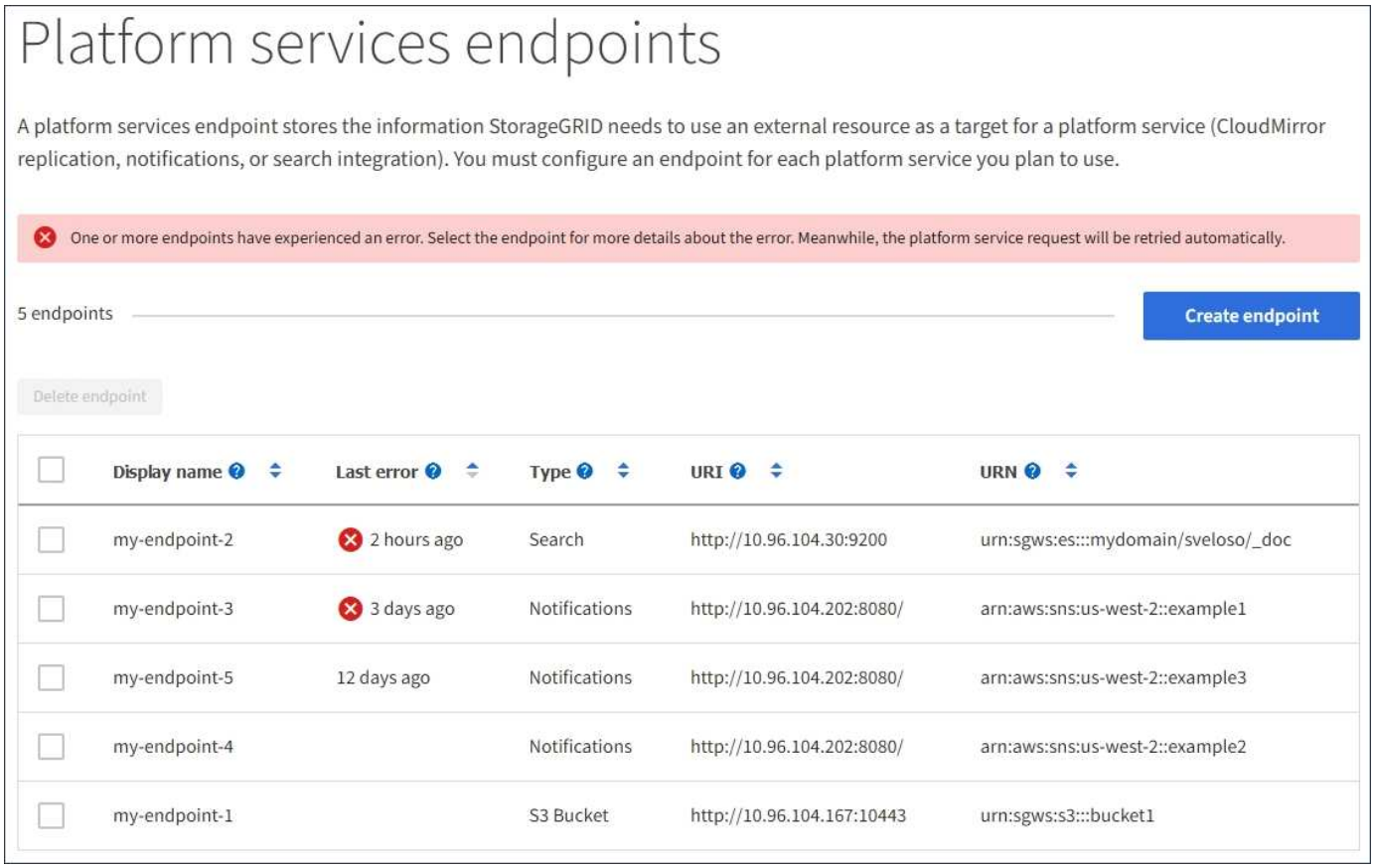
如果未为租户帐户启用平台服务、则端点创建将失败。

现有端点存在问题

如果在StorageGRID 尝试访问现有端点时发生错误、租户管理器的信息板上将显示一条消息。

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

租户用户可以转到"端点"页面，查看每个端点的最新错误消息，并确定发生错误的时间。*上一个错误*列显示每个端点的最新错误消息，并指示错误发生的时间。包含 图标的错误发生在过去 7 天内。



* 最后一个错误 * 列中的某些错误消息可能会在圆括号中包含日志 ID 。网格管理员或技术支持可以使用此 ID 在 bycast.log 中查找有关此错误的更多详细信息。

与代理服务器相关的问题

如果您已配置"存储代理"存储节点和平台服务端点之间，如果您的代理服务不允许来自StorageGRID的消息，则可能会发生错误。要解决这些问题，请检查代理服务器的设置，以确保平台服务相关的消息不会被阻止。

确定是否发生错误

如果在过去7天内发生任何端点错误、租户管理器中的信息板将显示警报消息。您可以转到 " 端点 " 页面以查看有关此错误的更多详细信息。

客户端操作失败

某些平台服务问题可能会导致 S3 存储分段上的发生原因 客户端操作失败。例如，如果内部复制状态计算机（ RSM ）服务停止，或者排队等待传送的平台服务消息太多， S3 客户端操作将失败。

要检查服务状态，请执行以下操作：

1. 选择 节点 > 站点 > 存储节点 > 概览*。
2. 检查警报表中的活动警报。
3. 解决所有活动警报。如有需要，请联系技术支持。

可恢复和不可恢复的端点错误

创建端点后，平台服务请求错误可能会因各种原因而发生。某些错误可通过用户干预进行恢复。例如，可能会发生可恢复的错误，原因如下：

- 用户凭据已删除或已过期。
- 目标存储桶不存在。
- 无法传送通知。

如果 StorageGRID 遇到可恢复的错误，将重试平台服务请求，直到成功。

其他错误是无法恢复的。例如，以下原因可能会发生不可恢复的错误：

- 端点已删除。
- Webhook 端点目标通过以下方式响应通知请求 `400 Bad Request`错误。

如果StorageGRID遇到不可恢复的端点错误：

- 在网格管理器中，转至*Support*>*Tools*>*Metrics *>*Grafana *>*Platform Services Overview*以查看错误详细信息。
- 在租户管理器中，转至*存储(S3)*>*平台服务端点*以查看错误详细信息。
- 检查 `/var/local/log/bycast-err.log`是否存在相关错误。具有ADC服务的存储节点包含此日志文件。

无法传送平台服务消息

如果目标遇到问题而无法接受平台服务消息，则存储桶上的客户端操作会成功，但平台服务消息不会被传递。例如，如果在目标上更新凭据，使得StorageGRID无法再对目标服务进行身份验证，则可能会发生此错误。

检查相关警报。

降低平台服务请求的性能

如果发送请求的速率超过目标端点接收请求的速率， StorageGRID 软件可能会限制传入的存储分段 S3 请求。只有在等待发送到目标端点的请求积压时，才会发生限制。

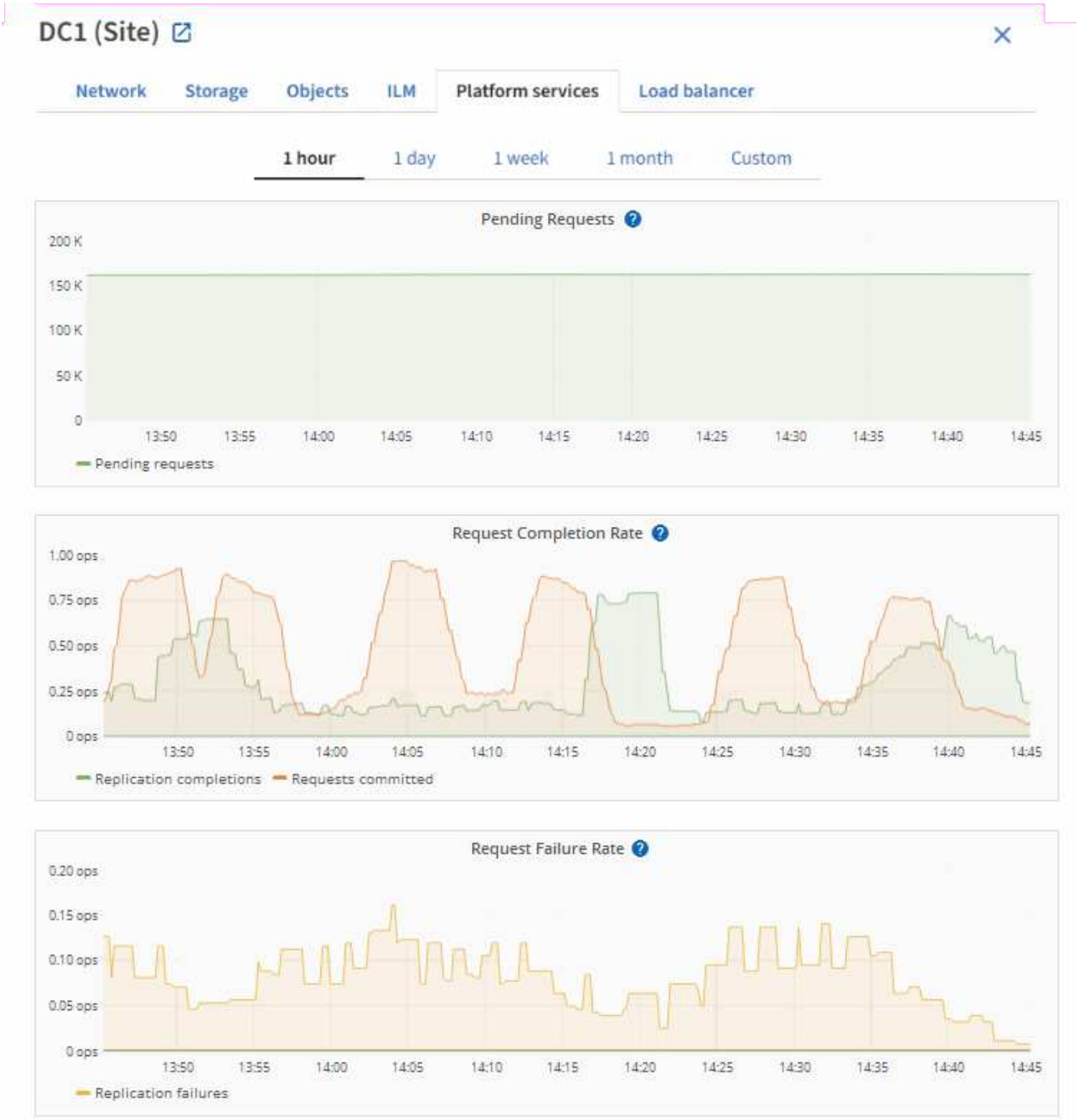
唯一明显的影响是，传入的 S3 请求执行时间较长。如果您开始检测到性能明显较慢，则应降低载入速率或使用容量较高的端点。如果积压的请求持续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。

CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求所涉及的数据传输通常多于搜索集成或事件通知请求。

平台服务请求失败

要查看平台服务的请求失败率，请执行以下操作：

1. 选择*节点*。
2. 选择 ***site*** > * 平台服务 * 。
3. 查看请求错误率图表。



平台服务不可用警报

" 平台服务不可用 * " 警报表示无法在站点上执行平台服务操作，因为运行或可用的 RSM 服务存储节点太少。

RSM 服务可确保将平台服务请求发送到其各自的端点。

要解决此警报，请确定站点上的哪些存储节点包含 RSM 服务。(RSM服务位于同时包含ADC服务的存储节点上。)然后、确保这些存储节点中的大多数节点正在运行且可用。

> 如果某个站点上有多个包含 RSM 服务的存储节点出现故障，则该站点的任何待定平台服务请求都将丢失。

有关平台服务端点的其他故障排除指南

有关更多信息，请参见"使用租户帐户gt；对平台服务端点进行故障排除"。

相关信息

"排除StorageGRID 系统故障"

管理 **StorageGRID** 中租户帐户的 **S3 Select**

您可以允许某些 S3 租户对单个对象使用 S3 Select 到问题描述 SelectObjectContent 请求。

S3 Select 可以高效地搜索大量数据，而无需部署数据库和相关资源即可启用搜索。它还可以降低检索数据的成本和延迟。

什么是 **S3 Select** ？

S3 Select 允许 S3 客户端使用 SelectObjectContent 请求仅筛选和检索对象所需的数据。S3 Select 的 StorageGRID 实施包括部分 S3 Select 命令和功能。

使用 **S3 Select** 的注意事项和要求

网格管理要求

网格管理员必须授予租户S3选择功能。选择*在或时允许S3选择*"创建租户""编辑租户"。

对象格式要求

要查询的对象必须采用以下格式之一：

- **CSX**。可以按原样使用、也可以压缩到GZIP或bzip2归档中。
- 镶木地板。对镶木地板对象的其他要求：
  - S3 Select仅支持使用GZIP或Snappy进行列式压缩。S3 Select不支持对镶木地板对象进行整体对象压缩。
  - S3 Select不支持镶木地板输出。必须将输出格式指定为CSV或JSON。
  - 最大未压缩行组大小为512 MB。
  - 您必须使用对象架构中指定的数据类型。

- 不能使用间隔、JSON、列表、时间或UUID逻辑类型。

端点要求

必须将选择对象内容请求发送到"StorageGRID 负载平衡器端点"。

端点使用的管理节点和网关节点必须为以下选项之一：

- 服务设备节点
- 基于VMware的软件节点
- 运行已启用cgroup v2的内核的裸机节点

一般注意事项

查询不能直接发送到存储节点。

SelectObjectContent 请求会降低所有 S3 客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。

请参见"有关使用 S3 Select 的说明"。

查看"Grafana 图表"对于 S3 选择随时间推移的操作，在网格管理器中选择 支持 > 工具 > 指标。

配置客户端连接

配置 **S3** 客户端到 **StorageGRID** 的连接

作为网格管理员、您可以管理一些配置选项、这些配置选项用于控制S3客户端应用程序如何连接到StorageGRID系统以存储和检索数据。

Swift详细信息已从此版本的文档站点中删除。请参阅。 "StorageGRID 11.8:配置S3和Swift客户端连接"

配置任务

1. 根据客户端应用程序连接到StorageGRID 的方式、在StorageGRID 中执行必备任务。

所需任务

您必须获得：

- IP 地址
- 域名
- SSL 证书

可选任务

(可选)配置：

- 身份联合
- SSO

1. 使用StorageGRID 获取应用程序连接到网格所需的值。您可以使用S3设置向导、也可以手动配置每个StorageGRID 实体。+

使用**S3**设置向导

按照S3设置向导中的步骤进行操作。

手动配置

1. 创建高可用性组
2. 创建负载平衡器端点
3. 创建租户帐户
4. 创建存储分段和访问密钥
5. 配置ILM规则和策略

1. 使用S3应用程序完成与StorageGRID 的连接。创建DNS条目以将IP地址与计划使用的任何域名关联起来。

   根据需要执行其他应用程序设置。

2. 在应用程序和StorageGRID 中执行持续任务、以管理和监控一段时间内的对象存储。

将**StorageGRID** 连接到客户端应用程序所需的信息

在将StorageGRID连接到S3客户端应用程序之前、您必须在StorageGRID中执行配置步骤并获取特定值。

我需要什么值?

下表显示了您必须在StorageGRID中配置的值、以及S3应用程序和DNS服务器使用这些值的位置。

价值	其中、值已配置	使用值的位置
虚拟IP (VIP)地址	StorageGRID > HA组	DNS条目

价值	其中、值已配置	使用值的位置
端口	StorageGRID >负载平衡器端点	客户端应用程序
SSL 证书	StorageGRID >负载平衡器端点	客户端应用程序
服务器名称(FQDN)	StorageGRID >负载平衡器端点	• 客户端应用程序 • DNS条目
S3访问密钥ID和机密访问密钥	StorageGRID >租户和存储分段	客户端应用程序
存储分段/容器名称	StorageGRID >租户和存储分段	客户端应用程序

如何获取这些值?

根据您的要求、您可以执行以下任一操作来获取所需信息：

- *使用*"S3设置向导"。S3设置向导可帮助您在StorageGRID 中快速配置所需的值、并输出一个或两个文件、您可以在配置S3应用程序时使用这些文件。此向导将指导您完成所需的步骤、并帮助您确保设置符合StorageGRID 最佳实践。

  如果要配置S3应用程序、建议使用S3设置向导、除非您知道自己有特殊要求、否则实施需要大量自定义。

- *使用*"FabricPool 设置向导"。与S3设置向导类似、FabricPool 设置向导可帮助您快速配置所需值并输出一个文件、您可以在ONTAP 中配置FabricPool 云层时使用该文件。

  如果您计划使用StorageGRID 作为FabricPool 云层的对象存储系统、建议使用FabricPool 设置向导、除非您知道自己有特殊要求或实施需要大量自定义。

- 手动配置项目。如果您要连接到S3应用程序而不想使用S3设置向导、则可以通过手动执行配置来获取所需的值。请按照以下步骤操作：

  a. 配置要用于S3应用程序的高可用性(HA)组。请参阅。 "配置高可用性组"
  b. 创建S3应用程序要使用的负载平衡器端点。请参阅。 "配置负载平衡器端点"
  c. 创建S3应用程序要使用的租户帐户。请参阅。 "创建租户帐户"
  d. 对于S3租户、请登录到租户帐户、并为要访问该应用程序的每个用户生成访问密钥ID和机密访问密钥。请参阅。 "创建您自己的访问密钥"
  e. 在租户帐户中创建一个或多个S3存储分段。对于S3，请参见"创建 S3 存储分段"。
  f. 要为属于新租户或存储分段/容器的对象添加特定放置说明、请创建新的ILM规则并激活新的ILM策略以使用该规则。请参阅"创建 ILM 规则"和"创建 ILM 策略"。

StorageGRID 中 S3 客户端的安全性

StorageGRID租户帐户使用S3客户端应用程序将对象数据保存到StorageGRID。您应查看为客户端应用程序实施的安全措施。

摘要

以下列表总结了如何为S3 REST API实施安全性：

连接安全性
: TLS

服务器身份验证
: 系统 CA 签名的 X.509 服务器证书或管理员提供的自定义服务器证书

客户端身份验证
: S3帐户访问密钥ID和机密访问密钥

客户端授权
: 存储分段所有权和所有适用的访问控制策略

StorageGRID如何为客户端应用程序提供安全性

S3客户端应用程序可以连接到网关节点或管理节点上的负载平衡器服务、也可以直接连接到存储节点。

- 连接到负载平衡器服务的客户端可以根据您的方式使用HTTPS或HTTP"配置负载平衡器端点"。

  建议使用HTTPS提供安全的TLS加密通信。您必须向端点附加安全证书。

  HTTP提供的未加密通信安全性较低、只能用于非生产或测试网格。

- 连接到存储节点的客户端也可以使用HTTPS或HTTP。

  HTTPS是默认设置、建议使用。

  HTTP提供的未加密通信安全性较低、但对于非生产网格或测试网格、也可以选择使用"已启用"它。

- StorageGRID 与客户端之间的通信使用 TLS 进行加密。
- 无论将负载平衡器端点配置为接受 HTTP 或 HTTPS 连接，网格中的负载平衡器服务和存储节点之间的通信都会进行加密。
- 客户端必须向StorageGRID提供"HTTP身份验证标头"才能执行REST API操作。

安全证书和客户端应用程序

在所有情况下，客户端应用程序都可以使用网格管理员上传的自定义服务器证书或 StorageGRID 系统生成的证书进行 TLS 连接：

- 当客户端应用程序连接到负载平衡器服务时、它们将使用为负载平衡器端点配置的证书。每个负载平衡器端点都有自己的证书##8212;网格管理员上传的自定义服务器证书，或者网格管理员在配置端点时在StorageGRID中生成的证书。

  请参阅。 "负载平衡注意事项"

- 当客户端应用程序直接连接到存储节点时、它们会使用系统生成的服务器证书、这些证书是在安装StorageGRID 系统时为存储节点生成的(由系统证书颁发机构签名)。 或网格管理员为网格提供的单个自定义服务器证书。请参阅。 "添加自定义S3 API证书"

应将客户端配置为信任对用于建立 TLS 连接的任何证书签名的证书颁发机构。

支持 **TLS** 库的哈希和加密算法

StorageGRID系统支持一组客户端应用程序在建立 TLS 会话时可以使用的密码套件。要配置密码，请转到*配置*>*安全*>*安全设置*并选择*TLS 和 SSH 策略*。

支持的 **TLS** 版本

StorageGRID 支持 TLS 1.2 和 TLS 1.3 。

> 不再支持 SSLv3 和 TLS 1.1 （或更早版本）。

使用**S3**设置向导

StorageGRID S3 设置向导注意事项和要求

您可以使用S3设置向导将StorageGRID 配置为S3应用程序的对象存储系统。

何时使用**S3**设置向导

S3设置向导将指导您完成配置StorageGRID 以用于S3应用程序的每个步骤。完成此向导期间、您可以下载一些文件、用于在S3应用程序中输入值。使用向导可以更快地配置系统、并确保您的设置符合StorageGRID 最佳实践。

如果您有"root访问权限"，则可以在开始使用StorageGRID网格管理器时完成S3设置向导，也可以稍后访问并完成该向导。根据您的要求、您还可以手动配置部分或全部所需项、然后使用向导收集S3应用程序所需的值。

在使用向导之前

在使用向导之前、请确认您已满足这些前提条件。

获取**IP**地址并设置**VLAN**接口

如果要配置高可用性(HA)组、您就知道S3应用程序要连接到哪些节点以及要使用哪些StorageGRID 网络。您还知道要为子网CIDR、网关IP地址和虚拟IP (VIP)地址输入哪些值。

如果您计划使用虚拟LAN将流量与S3应用程序隔离、则已配置VLAN接口。请参阅。 "配置 VLAN 接口"

配置身份联合和**SSO**

如果您计划对StorageGRID系统使用身份联合或单点登录 (SSO)，则您已启用这些功能。您还知道哪个联合组应该对 S3 应用程序将使用的租户帐户具有根访问权限。看"使用身份联合"和"配置单点登录"。

获取并配置域名

您知道要用于StorageGRID 的完全限定域名(FQDN)。域名服务器(DNS)条目会将此FQDN映射到您使用向导创建的HA组的虚拟IP (VIP)地址。

如果您计划使用 S3 虚拟托管风格的请求，则应该使用"已配置S3端点域名"。建议使用虚拟托管风格的请求。

查看负载平衡器和安全证书要求

如果您计划使用StorageGRID 负载平衡器、则已查看负载平衡的一般注意事项。您拥有要上传的证书或生成证书所需的值。

如果您计划使用外部(第三方)负载平衡器端点、则具有该负载平衡器的完全限定域名(FQDN)、端口和证书。

配置任何网格联合连接

如果要允许 S3 租户使用网格联合连接同步帐户数据并将存储区对象复制到另一个网格，请在启动向导之前确认以下内容：

- 您拥有 "已配置网格联合连接"。
- 连接状态为*已连接*。
- 您具有 root 访问权限。

访问并完成 **StorageGRID** 中的 **S3** 设置向导

您可以使用S3设置向导配置StorageGRID 以用于S3应用程序。设置向导提供了应用程序访问StorageGRID 存储分段和保存对象所需的值。

开始之前

- 您拥有"root访问权限"。
- 您已查看"注意事项和要求"以使用向导。

访问向导

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 如果仪表板上出现 **FabricPool and S3 setup wizard** 横幅，请选择横幅中的链接。如果横幅不再出现，请从 Grid Manager 标题栏中选择帮助图标 ，然后选择 **FabricPool and S3 setup wizard**。
3. 在FabricPool and S3设置向导页面的S3应用程序部分中，选择*立即配置*。

第1步(共6步)：配置HA组

HA组是一组节点、每个节点都包含StorageGRID 负载平衡器服务。HA组可以包含网关节点、管理节点或同时包含这两者。

您可以使用HA组帮助保持S3数据连接可用。如果HA组中的活动接口发生故障、备份接口可以管理工作负载、而对S3操作的影响微乎其微。

有关此任务的详细信息，请参见"管理高可用性组"。

步骤

1. 如果您计划使用外部负载平衡器、则无需创建HA组。选择*跳过此步骤*并转到[第2步(共6步)：配置负载平衡器端点]。
2. 要使用StorageGRID 负载平衡器、您可以创建新的HA组或使用现有HA组。

创建 **HA** 组

a. 要创建新的HA组，请选择*创建HA组*。

b. 对于“输入详细信息”步骤，请填写以下字段。

字段	说明
HA组名称	此HA组的唯一显示名称。
问题描述 (可选)	此HA组的问题描述。

c. 对于*Add interfaces*步骤，选择要在此HA组中使用的节点接口。

使用列标题对行进行排序，或者输入搜索词以更快地找到接口。

您可以选择一个或多个节点、但只能为每个节点选择一个接口。

d. 对于“确定接口优先级”步骤，请确定此HA组的主接口和任何备份接口。

拖动行以更改*优先级顺序*列中的值。

列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。

如果HA组包含多个接口、而活动接口发生故障、则虚拟IP (VIP)地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。解决故障后、VIP地址将移回可用的最高优先级接口。

e. 对于“输入**IP**地址”步骤，请填写以下字段。

字段	说明
Subnet CIDR	采用CIDR表示法的VIP子网地址&#8212；后跟斜杠的IPv4地址和子网长度(0-32)。 网络地址不能设置任何主机位。例如， `192.16.0.0/22`。
网关IP地址(可选)	如果用于访问StorageGRID 的S3 IP地址与StorageGRID VIP地址不在同一子网上、请输入StorageGRID VIP本地网关IP地址。本地网关 IP 地址必须位于 VIP 子网中。
虚拟IP地址	为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网内。 必须至少有一个地址为IPv4。您也可以指定其他 IPv4 和 IPv6 地址。

f. 选择*创建HA组*，然后选择*完成*返回S3设置向导。

g. 选择*继续*以转到负载平衡器步骤。

使用现有**HA**组

a. 要使用现有HA组，请从*选择HA组*中选择HA组名称。

b. 选择*继续*以转到负载平衡器步骤。

第2步(共6步)：配置负载平衡器端点

StorageGRID 使用负载平衡器管理客户端应用程序中的工作负载。负载平衡可最大限度地提高多个存储节点的速度和连接容量。

您可以使用所有网关和管理节点上的StorageGRID 负载平衡器服务、也可以连接到外部(第三方)负载平衡器。建议使用StorageGRID 负载平衡器。

有关此任务的详细信息，请参见"负载平衡注意事项"。

要使用StorageGRID 负载平衡器服务，请选择StorageGRID 负载平衡器*选项卡，然后创建或选择要使用的负载平衡器端点。要使用外部负载平衡器，请选择*外部负载平衡器*选项卡，并提供有关已配置的系统的详细信息。

创建端点

步骤

1. 要创建负载平衡器端点，请选择*Create endpoint*。
2. 对于*输入端点详细信息*步骤，请填写以下字段。

字段	说明
名称	端点的描述性名称。
端口	要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入任何未使用的外部端口。如果输入80或443、则仅在网关节点上配置端点、因为这些端口是在管理节点上预留的。 *注意：*不允许使用其他网格服务使用的端口。看"StorageGRID 内部端口" 。
客户端类型	必须为*S3*。
网络协议	选择 * HTTPS * 。 注意：支持在不使用TLS加密的情况下与StorageGRID 通信，但不建议这样做。

3. 对于*选择绑定模式*步骤，指定绑定模式。绑定模式控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

模式	说明
全局（默认）	客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。 除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。
HA 组的虚拟 IP	客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。 具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。
节点接口	客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。
节点类型	根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。

4. 对于租户访问步骤、选择以下选项之一：

字段	说明
允许所有租户(默认)	所有租户帐户都可以使用此端点来访问其分段。
允许选定租户	只有选定租户帐户才能使用此端点访问其分段。
阻止选定租户	选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。

5. 对于*attach certificer*步骤，选择以下选项之一：

字段	说明
上传证书(建议)	使用此选项可上传CA签名的服务器证书、证书专用密钥和可选的CA包。
生成证书	使用此选项可生成自签名证书。有关输入内容的详细信息、请参见"配置负载平衡器端点"。
使用StorageGRID S3证书	仅当您已上传或生成自定义版本的StorageGRID 全局证书时、才使用此选项。有关详细信息、请参见。 "配置S3 API证书"

6. 选择*完成*以返回S3设置向导。
7. 选择*继续*转到租户和存储分段步骤。

对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

使用现有负载平衡器端点

步骤

1. 要使用现有端点，请从*选择负载平衡器端点*中选择其名称。
2. 选择*继续*转到租户和存储分段步骤。

使用外部负载平衡器

步骤

1. 要使用外部负载平衡器、请填写以下字段。

字段	说明
FQDN	外部负载平衡器的完全限定域名(FQDN)。
端口	S3应用程序将用于连接到外部负载平衡器的端口号。
证书	复制外部负载平衡器的服务器证书并将其粘贴到此字段中。

2. 选择*继续*转到租户和存储分段步骤。

第3步(共6步)：创建租户和存储分段

租户是一种可以使用S3应用程序在StorageGRID 中存储和检索对象的实体。每个租户都有自己的用户、访问密钥、分段、对象和一组特定功能。

分段是一种用于存储租户对象和对象元数据的容器。尽管租户可能具有许多存储分段、但此向导可帮助您以最快、最简单的方式创建租户和存储分段。如果稍后需要添加存储分段或设置选项、可以使用租户管理器。

有关此任务的详细信息，请参见"创建租户帐户"和"创建 S3 存储分段"。

步骤

1. 输入租户帐户的名称。

   租户名称不需要唯一。创建租户帐户时，它会收到一个唯一的数字帐户 ID 。

2. 根据您的StorageGRID系统是否使用，定义租户帐户的根访问权限"身份联合"，"单点登录(SSO)" ，或两者兼而有之。

选项	执行此操作 ...
如果未启用身份联合	指定以本地root用户身份登录租户时要使用的密码。
如果启用了身份联合	a. 选择租户要拥有的现有联盟组"root访问权限"。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择租户要拥有的现有联盟组"root访问权限"。没有本地用户可以登录。

3. 如果希望向导为root用户创建访问密钥ID和机密访问密钥，请选择*自动创建root用户S3访问密钥*。

   如果租户的唯一用户是root用户、请选择此选项。如果其他用户要使用此租户、则"使用租户管理器"配置密钥和权限。

4. 如果要立即为此租户创建存储分段，请选择*为此租户创建存储分段*。

   如果为网格启用了S3对象锁定、则在此步骤中创建的分段不会启用S3对象锁定。如果您需要对此S3应用程序使用S3对象锁定分段、请勿选择立即创建分段。请稍后使用租户管理器"创建存储分段"。

   a. 输入S3应用程序要使用的存储分段的名称。例如， `s3-bucket`。

      创建存储分段后、无法更改存储分段名称。

   b. 为此存储分段选择*区域*。

      使用默认区域(`us-east-1`)，除非您希望将来使用ILM根据存储分段的区域过滤对象。

5. 选择*创建并继续*。

第4步(共6步)：下载数据

在下载数据步骤中、您可以下载一个或两个文件以保存刚刚配置的内容的详细信息。

步骤

1. 如果选择了*自动创建root用户S3访问密钥*，请执行以下一项或两项操作：
   - 选择*下载访问密钥*可下载 `.csv`包含租户帐户名称、访问密钥ID和机密访问密钥的文件。
   - 选择复制图标（）将访问密钥 ID 和秘密访问密钥复制到剪贴板。
2. 选择*下载配置值*可下载 `.txt`包含负载平衡器端点、租户、分段和root用户设置的文件。
3. 将此信息保存到安全位置。

> 在复制两个访问密钥之前、请勿关闭此页面。关闭此页面后、密钥将不可用。请确保将此信息保存在安全位置、因为此信息可用于从StorageGRID 系统获取数据。

4. 如果出现提示、请选中此复选框以确认您已下载或复制密钥。
5. 选择*继续*以转到ILM规则和策略步骤。

第5步(共6步)：查看S3的ILM规则和ILM策略

信息生命周期管理(ILM)规则控制StorageGRID 系统中所有对象的放置、持续时间和加载行为。StorageGRID 附带的ILM策略会为所有对象创建两个复制副本。此策略在您至少激活一个新策略之前有效。

步骤

1. 查看页面上提供的信息。
2. 如果要为属于新租户或存储分段的对象添加特定说明、请创建新规则和新策略。请参阅"创建 ILM 规则"和"使用ILM策略"。
3. 选择*我已查看这些步骤并了解我需要执行的操作*。
4. 选中此复选框以指示您了解下一步要做什么。
5. 选择*继续*以转到*摘要*。

第6步(共6步)：查看摘要

步骤

1. 查看摘要。
2. 记下后续步骤中的详细信息、这些详细信息介绍了在连接到S3客户端之前可能需要的其他配置。例如，选择*以root身份登录*将转到租户管理器，您可以在其中添加租户用户、创建其他存储分段以及更新存储分段设置。
3. 选择 * 完成 * 。
4. 使用从StorageGRID 下载的文件或手动获取的值配置应用程序。

管理HA组

高可用性(HA)组可为S3客户端提供高可用性数据连接、并可为网格管理器和租户管理器提供高可用性连接。

您可以将多个管理节点和网关节点的网络接口分组到一个高可用性（ HA ）组中。如果 HA 组中的活动接口发生故障，则备份接口可以管理工作负载。

每个 HA 组均可访问选定节点上的共享服务。

- 包含网关节点和/或管理节点的HA组可为S3客户端提供高可用性数据连接。
- 仅包含管理节点的 HA 组可提供与网格管理器和租户管理器的高可用性连接。
- 仅包含服务设备和基于VMware的软件节点的HA组可以为提供高可用性连接"使用 S3 Select 的 S3 租户"。建议在使用 S3 Select 时使用 HA 组，但不要求使用 HA 组。

如何创建 **HA** 组?

1. 您可以为一个或多个管理节点或网关节点选择一个网络接口。您可以使用网格网络（ eth0 ）接口，客户端网络（ eth2 ）接口， VLAN 接口或已添加到节点的访问接口。

   如果某个接口具有DHCP分配的IP地址、则无法将其添加到HA组。

2. 您可以指定一个接口作为主接口。主接口是活动接口，除非发生故障。
3. 您可以确定任何备份接口的优先级顺序。
4. 您可以为组分配 1 到 10 个虚拟 IP （ VIP ）地址。客户端应用程序可以使用其中任何 VIP 地址连接到 StorageGRID 。

有关说明，请参阅"配置高可用性组"。

什么是活动接口?

在正常操作期间， HA 组的所有 VIP 地址都会添加到主接口，这是优先级顺序中的第一个接口。只要主接口保持可用，客户端就会连接到组的任何 VIP 地址。也就是说、在正常操作期间、主接口是组的"活动"接口。

同样、在正常操作期间、HA组中任何优先级较低的接口都会充当"备份"接口。除非主(当前处于活动状态)接口不可用、否则不会使用这些备份接口。

查看节点的当前 **HA** 组状态

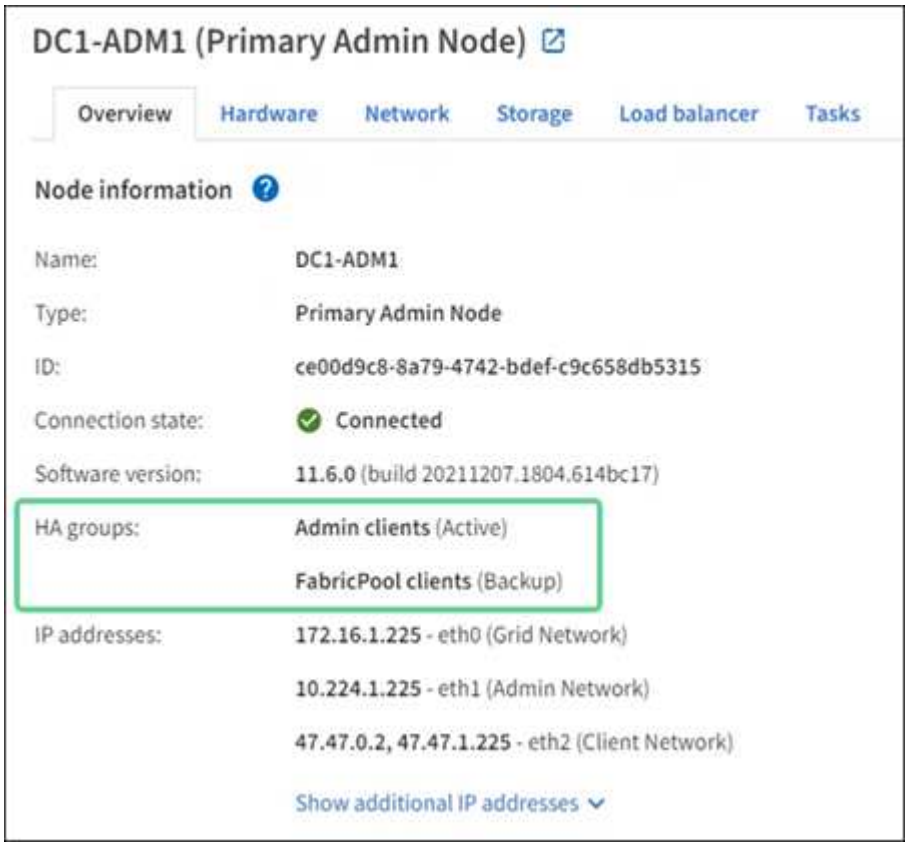
要查看某个节点是否已分配给 HA 组并确定其当前状态，请选择 **Nodes** > ***node***。

如果 * 概述 * 选项卡包含 * HA 组 * 的条目，则节点将分配给列出的 HA 组。组名称后面的值是 HA 组中节点的当前状态：

- * 活动 * ： HA 组当前正在此节点上托管。
- * 备份 * ： HA 组当前未使用此节点；这是一个备份接口。
- 已停止：无法在此节点上托管HA组、因为已手动停止高可用性(keepalived)服务。
- 故障：由于以下一项或多项原因、无法在此节点上托管HA组：

- 此节点上未运行负载平衡器（ nginx -gw ）服务。
- 节点的 eth0 或 VIP 接口已关闭。
- 此节点已关闭。

在此示例中，主管理节点已添加到两个 HA 组中。此节点当前是管理客户端组的活动接口，也是 FabricPool 客户端组的备份接口。



活动接口发生故障时会发生什么情况?

当前托管 VIP 地址的接口是活动接口。如果 HA 组包含多个接口且活动接口发生故障，则 VIP 地址将按优先级顺序移至第一个可用的备份接口。如果该接口发生故障， VIP 地址将移至下一个可用备份接口，依此类推。

触发故障转移的原因如下：

- 配置接口的节点将关闭。
- 配置了该接口的节点与所有其他节点的连接至少断开 2 分钟。
- 活动接口关闭。
- 负载平衡器服务将停止。
- 高可用性服务将停止。

> 托管活动接口的节点外部的网络故障可能不会触发故障转移。同样、网格管理器或租户管理器的服务也不会触发故障转移。

故障转移过程通常只需几秒钟，并且速度足以使客户端应用程序不会受到任何影响，并且可以依靠正常的重试行

为来继续运行。

解决故障后，如果更高优先级的接口再次可用，则 VIP 地址会自动移至可用的最高优先级接口。

StorageGRID HA 组如何提供高可用性

您可以使用高可用性（ High Availability ， HA ）组提供与 StorageGRID 的高可用性连接，以用于对象数据和管理目的。

- HA 组可以为网格管理器或租户管理器提供高度可用的管理连接。
- HA组可以为S3客户端提供高可用性数据连接。
- 如果 HA 组仅包含一个接口，则可以提供多个 VIP 地址并明确设置 IPv6 地址。

只有当 HA 组中包含的所有节点都提供相同的服务时， HA 组才能提供高可用性。创建 HA 组时，请从提供所需服务的节点类型中添加接口。

- * 管理节点 * ：包括负载平衡器服务，并允许访问网格管理器或租户管理器。
- 网关节点：包括负载平衡器服务。

HA 组的用途	将此类型的节点添加到 **HA** 组
访问 Grid Manager	• 主管理节点（ * 主 * ） • 非主管理节点 • 注： * 主管理节点必须为主接口。某些维护过程只能从主管理节点执行。
仅访问租户管理器	• 主管理节点或非主管理节点
S3客户端访问—负载均衡器服务	• 管理节点 • 网关节点
的S3客户端访问"S3 Select"	• 服务设备 • 基于 VMware 的软件节点 • 注 * ： 使用 S3 Select 时建议使用 HA 组，但不要求使用 HA 组。

将 **HA** 组与 **Grid Manager** 或租户管理器结合使用的限制

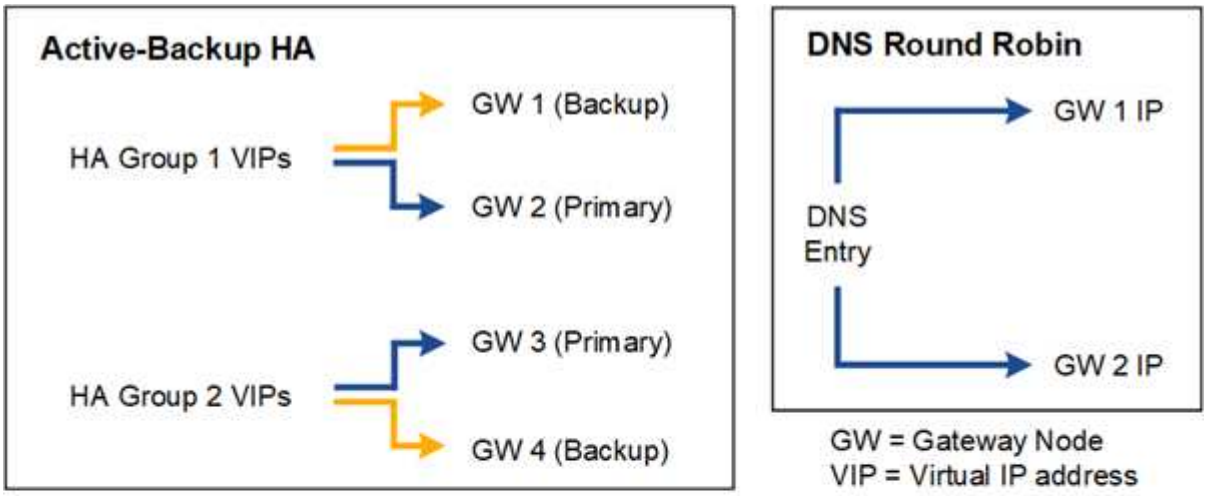
如果 Grid Manager 或租户管理器服务失败，则不会触发 HA 组故障转移。

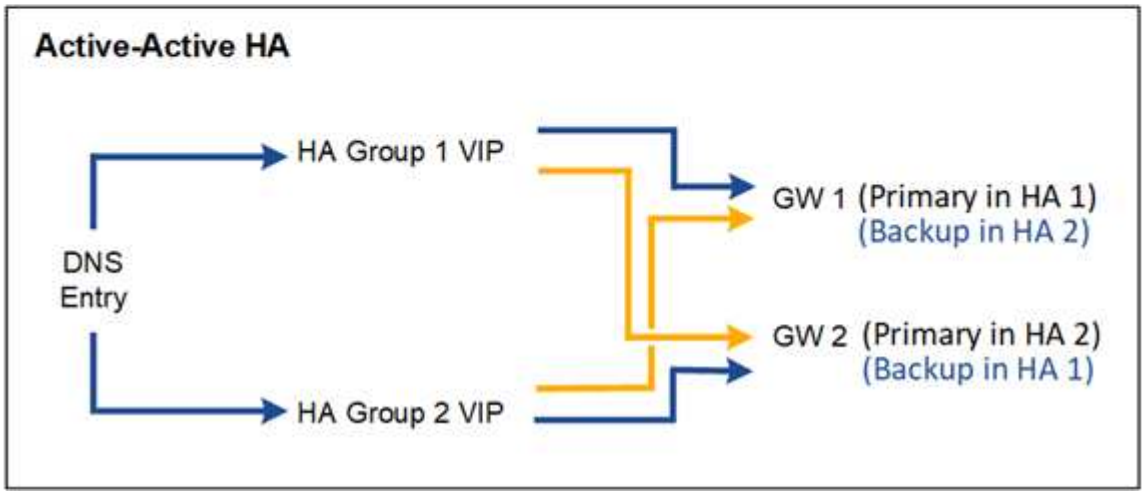
如果在发生故障转移时登录到网格管理器或租户管理器，则您将注销并必须重新登录才能恢复任务。

当主管理节点不可用时、无法执行某些维护过程。在故障转移期间，您可以使用网格管理器监控 StorageGRID 系统。

以下图表提供了配置高可用性 (HA) 组的不同方法的示例。每个选项都有优点和缺点。

在图中，蓝色表示 HA 组中的主接口，黄色表示 HA 组中的备份接口。





下表总结了图中所示每个 HA 配置的优势。

配置	优势	劣势
主动备份 HA	• 由 StorageGRID 管理，无外部依赖关系。 • 快速故障转移。	• 一个 HA 组中只有一个节点处于活动状态。每个 HA 组至少有一个节点处于空闲状态。
DNS 轮循	• 提高聚合吞吐量。 • 无闲置主机。	• 故障转移速度较慢，这可能取决于客户端行为。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。

配置	优势	劣势
主动 - 主动 HA	• 流量分布在多个 HA 组中。 • 可随 HA 组数量扩展的高聚合吞吐量。 • 快速故障转移。	• 配置更复杂。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。

在 **StorageGRID** 中配置高可用性组

您可以配置高可用性（ High Availability ， HA ）组，以提供对管理节点或网关节点上服务的高可用性访问。

StorageGRID系统最多可以有 255 个 HA 组。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 如果您计划在 HA 组中使用 VLAN 接口，则已创建 VLAN 接口。请参阅。 "配置 VLAN 接口"
- 如果您计划对 HA 组中的节点使用访问接口，则已创建此接口：
  - **Linux**（安装节点之前）："创建节点配置文件"
  - **Linux**（安装节点后）："向节点添加中继或访问接口"
  - **VMware**（安装节点后）："向节点添加中继或访问接口"

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

创建高可用性组

创建高可用性组时，您可以选择一个或多个接口并按优先级顺序对其进行组织。然后，您将一个或多个 VIP 地址分配给该组。

接口必须是要将网关节点或管理节点包含在 HA 组中的接口。一个 HA 组只能对任何给定节点使用一个接口；但是，同一节点的其他接口也可以在其他 HA 组中使用。

访问向导

步骤

1. 选择*配置* > 网络 > 高可用性组。
2. 选择 * 创建 * 。

输入 **HA** 组的详细信息

步骤

1. 为 HA 组提供一个唯一名称。

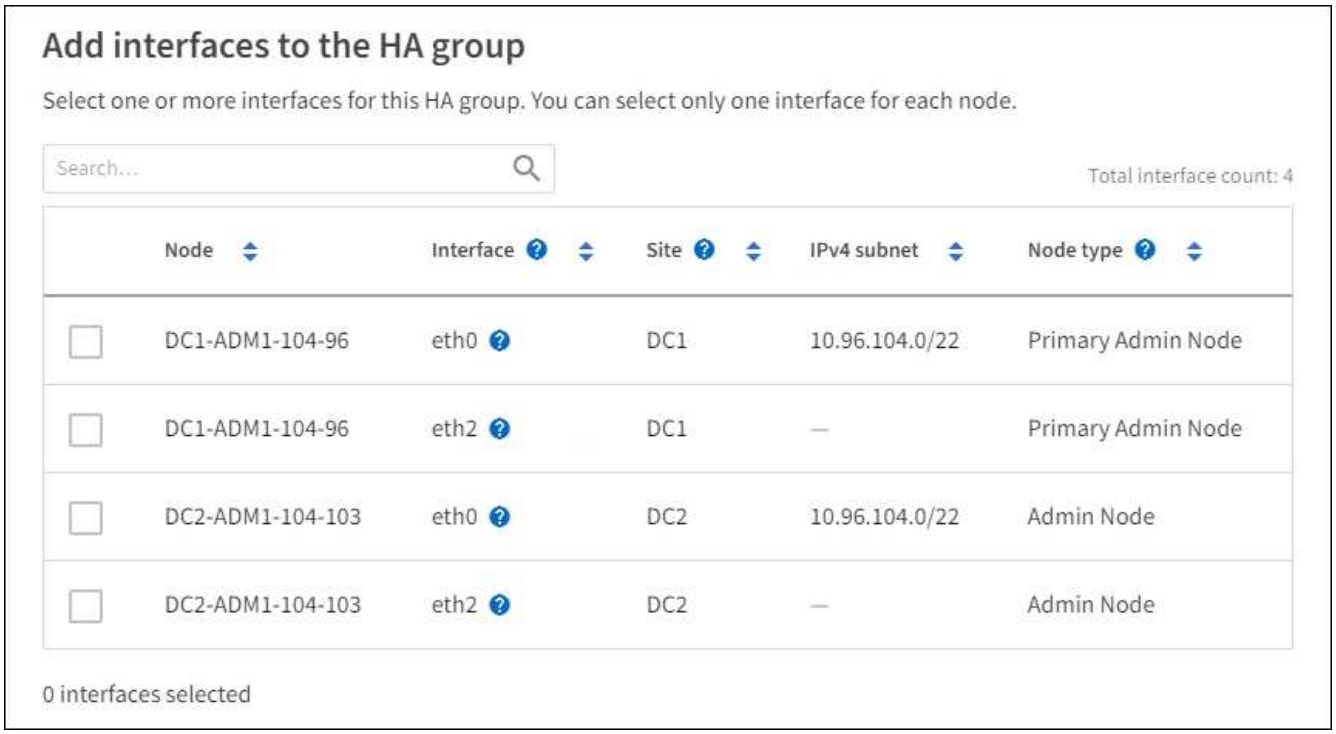
2. 或者，输入 HA 组的问题描述 。
3. 选择 * 继续 * 。

向 **HA** 组添加接口

步骤

1. 选择一个或多个接口以添加到此 HA 组。

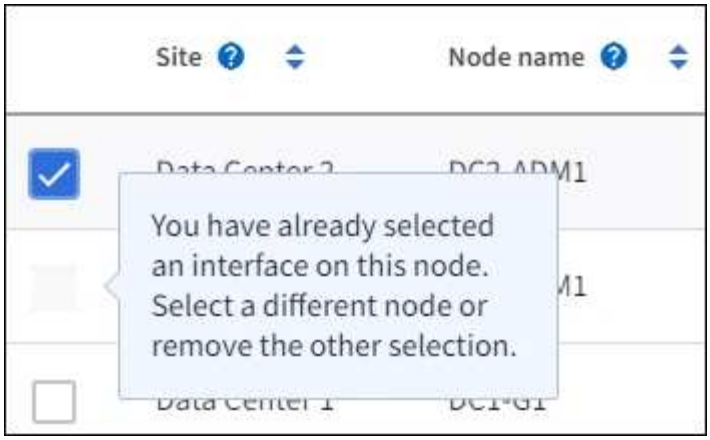
   使用列标题对行进行排序，或者输入搜索词以更快地找到接口。



   创建 VLAN 接口后，请等待最多 5 分钟，使新接口显示在表中。

   选择接口的准则

   - 必须至少选择一个接口。
   - 您只能为一个节点选择一个接口。
   - 如果 HA 组用于管理节点服务（包括网格管理器和租户管理器）的 HA 保护，请仅选择管理节点上的接口。
   - 如果HA组用于对S3客户端流量进行HA保护、请选择管理节点和/或网关节点上的接口。
   - 如果选择不同类型节点上的接口，则会显示一条信息性注释。系统会提醒您，如果发生故障转移，则新活动节点上可能无法使用先前活动节点提供的服务。例如、备份网关节点无法为管理节点服务提供HA保护。同样、备份管理节点无法执行主管理节点可以提供的所有维护过程。
   - 如果无法选择接口、则会禁用其复选框。工具提示提供了更多信息。



- 如果某个接口的子网值或网关与另一个选定接口冲突、则无法选择该接口。
- 如果已配置接口没有静态IP地址、则无法选择该接口。

2. 选择 * 继续 * 。

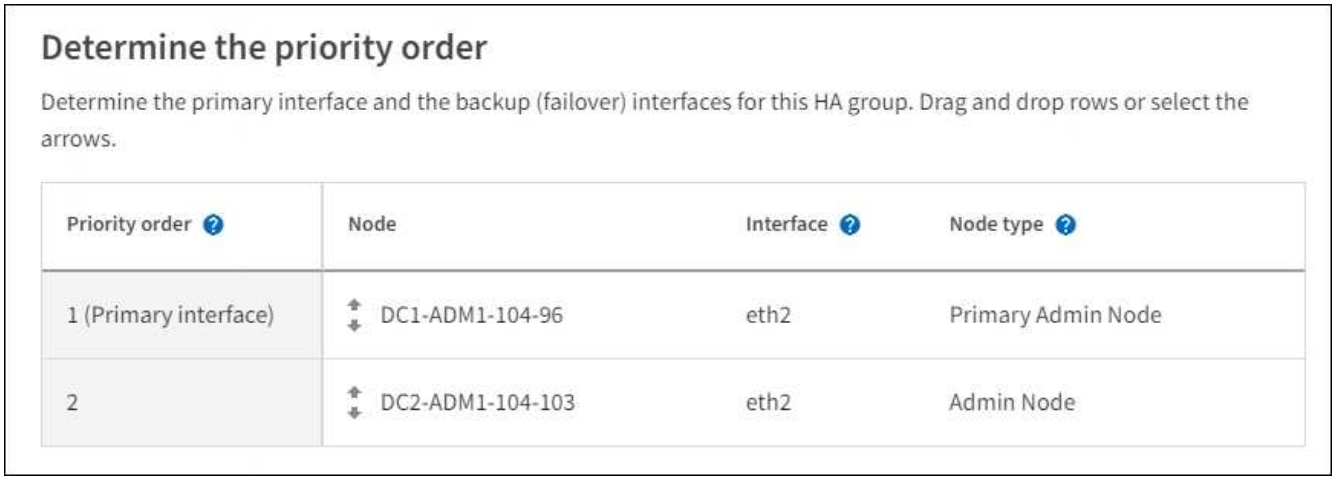
确定优先级顺序

如果HA组包含多个接口、则可以确定哪个是主接口、哪些是备份(故障转移)接口。如果主接口发生故障、VIP地址将移至可用的最高优先级接口。如果该接口发生故障， VIP 地址将移至可用的下一个最高优先级接口，依此类推。

步骤

1. 拖动*优先级顺序*列中的行以确定主接口和任何备份接口。

   列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。



> 如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行。

2. 选择 * 继续 * 。

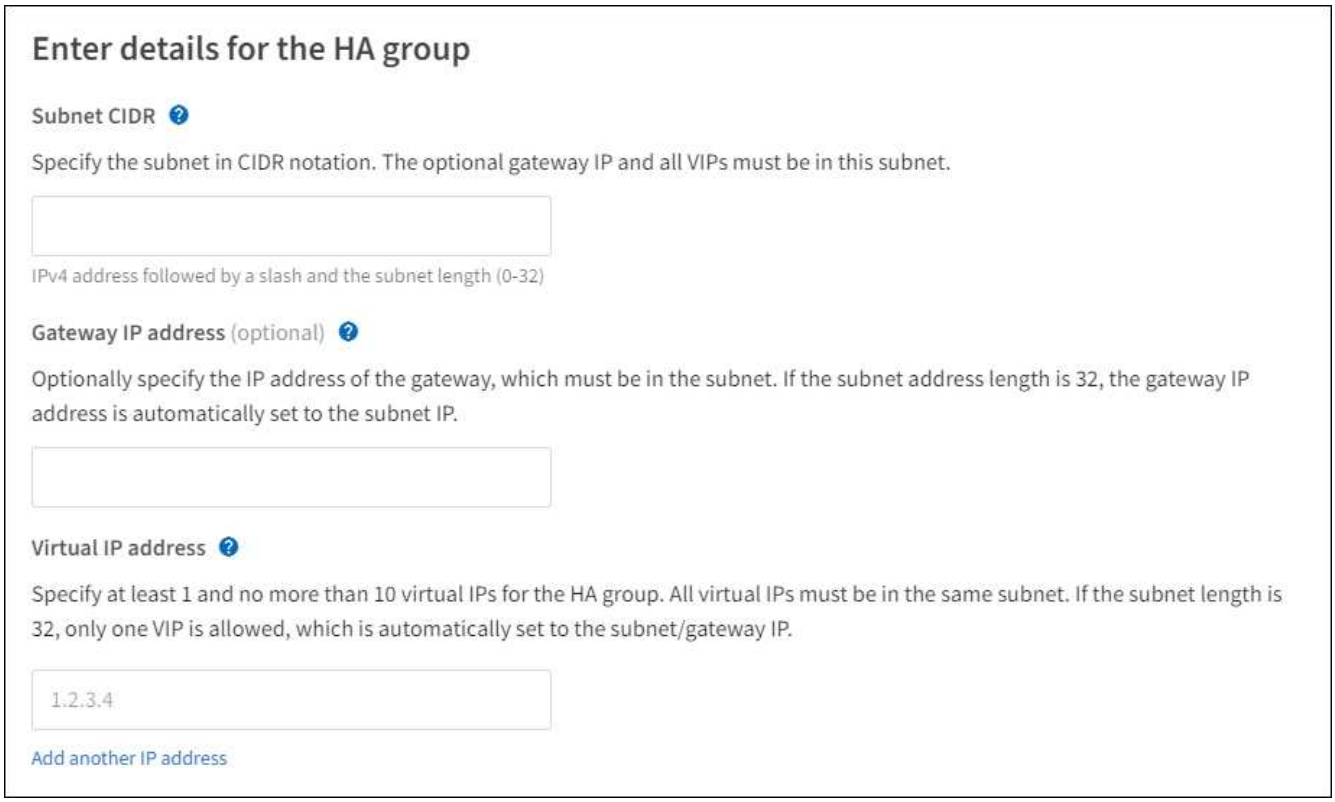
输入 **IP** 地址

步骤

1. 在 * 子网 CIDR * 字段中，以 CIDR 表示法指定 VIP 子网— IPv4 地址后跟斜杠和子网长度（ 0-32 ）。

   网络地址不能设置任何主机位。例如， `192.16.0.0/22`。

   如果使用 32 位前缀，则 VIP 网络地址也会用作网关地址和 VIP 地址。



2. (可选)如果任何S3管理或租户客户端要从其他子网访问这些VIP地址，请输入*网关IP地址*。网关地址必须在 VIP 子网中。

   客户端和管理员用户将使用此网关访问虚拟 IP 地址。

3. 为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网中、并且所有VIP地址都将在活动接口上同时处于活动状态。

   您必须至少提供一个 IPv4 地址。您也可以指定其他 IPv4 和 IPv6 地址。

4. 选择 * 创建 HA 组 * 并选择 * 完成 * 。

   此时将创建 HA 组，您现在可以使用已配置的虚拟 IP 地址。

后续步骤

如果要使用此 HA 组进行负载平衡，请创建一个负载平衡器端点以确定端口和网络协议并附加任何所需的证书。请参阅。 "配置负载平衡器端点"

编辑高可用性组

您可以编辑高可用性（ High Availability ， HA ）组以更改其名称和问题描述 ，添加或删除接口，更改优先级顺

序或添加或更新虚拟 IP 地址。

例如，如果要删除与站点或节点停用操作步骤 中选定接口关联的节点，则可能需要编辑 HA 组。

步骤

1. 选择*配置* > 网络 > 高可用性组。

   " 高可用性组 " 页面显示所有现有的 HA 组。

2. 选中要编辑的HA组对应的复选框。
3. 根据要更新的内容执行以下操作之一：
   - 选择 * 操作 * > * 编辑虚拟 IP 地址 * 以添加或删除 VIP 地址。
   - 选择 * 操作 * > * 编辑 HA 组 * 可更新组的名称或问题描述 ，添加或删除接口，更改优先级顺序或添加或删除 VIP 地址。
4. 如果选择了 * 编辑虚拟 IP 地址 * ：
   a. 更新 HA 组的虚拟 IP 地址。
   b. 选择 * 保存 * 。
   c. 选择 * 完成 * 。
5. 如果选择了 * 编辑 HA 组 * ：
   a. （可选）更新组的名称或问题描述 。
   b. (可选)选中或清除相应复选框以添加或删除接口。

      如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行

   c. (可选)拖动行以更改此HA组的主接口和任何备份接口的优先级顺序。
   d. 也可以更新虚拟 IP 地址。
   e. 选择 * 保存 * ，然后选择 * 完成 * 。

删除高可用性组

您可以一次删除一个或多个高可用性（ HA ）组。

如果HA组绑定到负载平衡器端点、则无法删除该HA组。要删除HA组、必须将其从使用该组的任何负载平衡器端点中删除。

要防止客户端中断、请在删除HA组之前更新任何受影响的S3客户端应用程序。更新每个客户端以使用其他 IP 地址进行连接，例如，安装期间为接口配置的不同 HA 组的虚拟 IP 地址或 IP 地址。

步骤

1. 选择*配置* > 网络 > 高可用性组。
2. 查看要删除的每个HA组的*负载平衡器端点*列。如果列出了任何负载平衡器端点：
   a. 转到*配置* > 网络 > 负载均衡器端点。

b. 选中此端点对应的复选框。

c. 选择 * 操作 * > * 编辑端点绑定模式 * 。

d. 更新绑定模式以删除HA组。

e. 选择 * 保存更改 * 。

3. 如果未列出负载平衡器端点、请选中要删除的每个HA组对应的复选框。
4. 选择*Actions*>*Remove HA group*。
5. 查看此消息并选择 * 删除 HA 组 * 以确认您的选择。

   选定的所有 HA 组都将被删除。高可用性组页面上会显示一个绿色的成功横幅。

管理负载平衡

了解 **StorageGRID** 负载平衡

您可以使用负载平衡处理S3客户端的载入和检索工作负载。

什么是负载平衡?

当客户端应用程序从StorageGRID 系统保存或检索数据时、StorageGRID 使用负载平衡器管理载入和检索工作负载。负载平衡通过在多个存储节点之间分布工作负载、最大限度地提高速度和连接容量。

StorageGRID 负载平衡器服务安装在所有管理节点和所有网关节点上，并提供第 7 层负载平衡。它会终止客户端请求，检查请求并与存储节点建立新的安全连接。

将客户端流量转发到存储节点时，每个节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。

> 尽管StorageGRID负载均衡器服务是推荐的负载均衡机制，但您可能希望集成第三方负载均衡器。如需了解更多信息，请联系您的NetApp客户代表或参考以下内容： "将第三方负载均衡器与StorageGRID结合使用"。

我需要多少个负载平衡节点?

作为一般最佳实践， StorageGRID 系统中的每个站点都应包含两个或更多具有负载平衡器服务的节点。例如，一个站点可能包含两个网关节点，或者同时包含一个管理节点和一个网关节点。无论您使用的是服务设备、裸机节点还是基于虚拟机(VM)的节点、请确保每个负载平衡节点都有足够的网络、硬件或虚拟化基础架构。

什么是负载平衡器端点?

负载平衡器端点定义了传入和传出客户端应用程序请求用来访问包含负载平衡器服务的节点的端口和网络协议(HTTPS或HTTP)。此外、此端点还可以定义客户端类型(S3)、绑定模式以及允许或阻止的租户列表(可选)。

要创建负载均衡器端点，请使用网格管理器或完成 S3 设置和FabricPool向导：

- "配置负载平衡器端点"
- "使用S3设置向导"
- "使用FabricPool 设置向导"

负载均衡器缓存的注意事项

当工作负载对数据子集进行操作并多次访问对象时，缓存可以显著提高性能。此外，缓存无需完整的网格部署即可提供对对象存储的远程访问。负载均衡器缓存仅适用于网关节点。

在创建负载均衡器端点时：

- 仅为可缓存的工作负载启用缓存。如果工作负载访问未缓存的数据的频率高于访问缓存的数据的频率，那么其性能将比未使用缓存提供服务时的性能更差。在某些情况下，覆盖率和驱逐率较高的工作负载也可能超过保证的驱动器写入耐久性。
- 考虑添加额外的端点或节点来缓存适合缓存的单个工作负载。
- 对可缓存和不可缓存的工作负载使用不同的端点。这种分离确保缓存机制得到适当应用并且不会干扰不可缓存的数据处理。
- 通过将潜在的可缓存工作负载定向到启用缓存的端点来评估它。监视并验证缓存命中率以确定工作负载是否适合缓存。此评估有助于优化性能并确保有效利用缓存资源。
- "查看审核日志"确定现有工作负载是否适合缓存。对于给定的时间段，确定针对唯一对象的 GET 百分比。为了适合缓存，该值应低于 50%。

适合缓存的工作负载示例

- 数据湖
- 高性能计算 (HPC)
- AI/ML 训练
- 内容分发网络（CDN）
- 媒体资产管理
- 视频制作

- 可以缓存多个对象版本。
- 支持范围读取操作。

不适合缓存的工作负载示例

- Fabric Pool
- 备份应用程序
- 存储分层

如果缓存提供的任何内容需要静态加密， "启用节点或驱动器加密"在缓存节点上。

不会被缓存的对象和请求类型

- 这 `response-content-encoding`查询参数
- 这 `partNumber`查询参数
- 条件标题

- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

- 使用以下任意方式静态加密的请求：
  - SSE（使用StorageGRID管理密钥的服务器端加密）
  - SSE-C（使用客户提供的密钥进行服务器端加密）
  - 存储对象加密

任何未缓存的请求都会被转发到上游 LDR，就好像未启用缓存一样。

相关信息

- "排查负载均衡器缓存问题"
- 有关负载均衡器缓存的更多信息，请联系技术支持。

端口注意事项

对于您创建的第一个端点、负载平衡器端点的端口默认为10433、但您可以指定介于1到65535之间的任何未使用的外部端口。如果使用端口80或443、则端点将仅在网关节点上使用负载平衡器服务。这些端口在管理节点上预留。如果对多个端点使用同一端口、则必须为每个端点指定不同的绑定模式。

不允许使用其他网格服务使用的端口。看"StorageGRID 内部端口" 。

网络协议注意事项

在大多数情况下、客户端应用程序和StorageGRID 之间的连接应使用传输层安全(Transport Layer Security 、TLS)加密。支持在不使用TLS加密的情况下连接到StorageGRID 、但不建议这样做、尤其是在生产环境中。为StorageGRID 负载平衡器端点选择网络协议时，应选择*HTTPS*。

负载平衡器端点证书的注意事项

如果选择*HTTPS*作为负载平衡器端点的网络协议，则必须提供安全证书。在创建负载平衡器端点时、您可以使用以下三个选项中的任何一个：

- 上传签名证书(建议)。此证书可以由公共信任的证书颁发机构(CA)或私有证书颁发机构(CA)签名。最佳做法是、使用公共信任的CA服务器证书来保护连接安全。与生成的证书不同、由CA签名的证书可以无干扰地轮换、这有助于避免过期问题。

  在创建负载平衡器端点之前、您必须获取以下文件：

  - 自定义服务器证书文件。
  - 自定义服务器证书专用密钥文件。
  - (可选)来自每个中间颁发证书颁发机构的证书的CA包。
- 生成自签名证书。
- 使用全局**StorageGRID S3**证书。您必须先上传或生成此证书的自定义版本、然后才能为负载平衡器端点选择此证书。请参阅。 "配置S3 API证书"

我需要什么值?

要创建证书、您必须知道S3客户端应用程序将用于访问此端点的所有域名和IP地址。

证书的*Subject DN*(可分辨名称)条目必须包含客户端应用程序将用于StorageGRID 的完全限定域名。例如:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

根据需要、此证书可以使用通配符来表示运行负载平衡器服务的所有管理节点和网关节点的完全限定域名。例如，`*.storagegrid.example.com`使用*通配符表示`adm1.storagegrid.example.com`和`gn1.storagegrid.example.com`。

如果您计划使用 S3 虚拟托管样式请求，则证书还必须为您配置的每个 "S3端点域名" 包含一个*备用名称*条目，包括任何通配符名称。例如:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

如果域名使用通配符，请查看"服务器证书的强化准则"。

您还必须为安全证书中的每个名称定义一个DNS条目。

如何管理即将到期的证书?

如果用于保护S3应用程序和StorageGRID 之间连接的证书到期、则该应用程序可能会暂时无法访问StorageGRID。

要避免证书到期问题、请遵循以下最佳实践:

- 请仔细监控任何警告证书到期日期即将到来的警报，例如*负载平衡器端点证书到期*和* S3 API*警报的全局服务器证书到期。
- 请始终保持StorageGRID 和S3应用程序的证书版本同步。如果要替换或续订用于负载平衡器端点的证书、则必须替换或续订S3应用程序使用的等效证书。
- 使用公共签名的CA证书。如果使用由CA签名的证书、则可以无系统地替换即将到期的证书。
- 如果您已生成自签名StorageGRID 证书、并且该证书即将过期、则必须在现有证书过期之前手动替换StorageGRID 和S3应用程序中的证书。

绑定模式的注意事项

通过绑定模式、您可以控制可用于访问负载平衡器端点的IP地址。如果端点使用绑定模式、则客户端应用程序仅在使用允许的IP地址或其对应的完全限定域名(FQDN)时才能访问该端点。使用任何其他IP地址或FQDN的客户端应用程序无法访问此端点。

您可以指定以下任意绑定模式:

- 全局(默认):客户端应用程序可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP

(VIP)地址或相应的FQDN访问端点。除非需要限制端点的可访问性、否则请使用此设置。

- * HA组的虚拟IP *。客户端应用程序必须使用HA组的虚拟IP地址(或相应的FQDN)。
- 节点接口。客户端必须使用选定节点接口的IP地址(或相应FQDN)。
- 节点类型。根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)。

租户访问注意事项

租户访问是一项可选的安全功能、可用于控制哪些StorageGRID 租户帐户可以使用负载平衡器端点来访问其分段。您可以允许所有租户访问某个端点(默认)、也可以为每个端点指定允许或阻止的租户列表。

您可以使用此功能在租户及其端点之间提供更好的安全隔离。例如、您可以使用此功能来确保一个租户所拥有的绝密或高度机密材料始终不会被其他租户完全访问。

> 出于访问控制的目的、租户是根据客户端请求中使用的访问密钥来确定的、如果在请求中未提供访问密钥(例如匿名访问)、则使用存储分段所有者来确定租户。

租户访问示例

要了解此安全功能的工作原理、请考虑以下示例：

1. 您已创建两个负载平衡器端点、如下所示：
   - *公共*端点：使用端口10443并允许所有租户访问。
   - *top密钥*端点：使用端口10444并仅允许访问*top密钥*租户。系统将阻止所有其他租户访问此端点。
2. `top-secret.pdf`位于*top密钥*租户拥有的存储分段中。

要访问 `top-secret.pdf`，*top密钥*租户中的用户可以向发出获取请求 `https://w.x.y.z:10444/top-secret.pdf`。由于允许此租户使用10444端点、因此用户可以访问此对象。但是、如果属于任何其他租户的用户向同一URL发出相同请求、他们将收到"立即拒绝访问"消息。即使凭据和签名有效、访问也会被拒绝。

CPU 可用性

在将S3流量转发到存储节点时、每个管理节点和网关节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。节点 CPU 负载信息每隔几分钟更新一次，但权重可能会更频繁地更新。即使节点报告利用率为 100% 或未能报告利用率，也会为所有存储节点分配最小基本权重值。

在某些情况下，有关 CPU 可用性的信息仅限于负载平衡器服务所在的站点。

配置 **StorageGRID** 负载均衡器端点

负载平衡器端点用于确定S3客户端在连接到网关和管理节点上的StorageGRID负载平衡器时可以使用的端口和网络协议。您还可以使用端点访问网格管理器、租户管理器或这两者。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。

- 您拥有"root访问权限"。
- 您已查看"负载平衡注意事项"。
- 如果先前已重新映射要用于负载平衡器端点的端口，则已创建"已删除端口重新映射"。
- 您已创建计划使用的任何高可用性（ HA ）组。建议使用 HA 组，但不要求使用 HA 组。请参阅。 "管理高可用性组"
- 如果负载平衡器端点将由使用"S3 Select 的 S3 租户"，则不能使用任何裸机节点的IP地址或FQDN。用于S3 Select的负载平衡器端点仅允许使用服务设备和基于VMware的软件节点。
- 您已配置计划使用的任何 VLAN 接口。请参阅。 "配置 VLAN 接口"
- 如果要创建 HTTPS 端点（建议），则您具有服务器证书的信息。

  对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

  - 要上传证书，您需要服务器证书，证书专用密钥以及 CA 捆绑包（可选）。
  - 要生成证书、您需要S3客户端用于访问此端点的所有域名和IP地址。您还必须知道主题（可分辨名称）。
  - 如果要使用StorageGRID S3 API证书(也可用于直接连接到存储节点)、则表示您已将默认证书替换为由外部证书颁发机构签名的自定义证书。请参阅。 "配置S3 API证书"

创建负载平衡器端点

每个 S3 客户端负载均衡器端点指定一个端口、一个客户端类型（S3）和一个网络协议（HTTP 或 HTTPS）。管理接口负载均衡器端点指定端口、接口类型和不受信任的客户端网络。

访问向导

步骤

1. 选择*配置* > 网络 > 负载均衡器端点。
2. 要为 S3 客户端创建端点，请选择 **S3** 客户端 选项卡。
3. 要创建端点以访问网格管理器、租户管理器或这两者，请选择*管理接口*选项卡。
4. 选择 * 创建 * 。

输入端点详细信息

步骤

1. 选择相应的说明、为要创建的端点类型输入详细信息。

S3 客户端

字段	说明
名称	端点的描述性名称，将显示在负载平衡器端点页面的表中。
端口	要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入介于1到65535之间的任何未使用的外部端口。 如果输入*80*或*8443*，则仅在网关节点上配置端点，除非释放端口8443。然后、您可以使用端口8443作为S3端点、此端口将同时在网关节点和管理节点上进行配置。 如果要为 "全局命名空间" 配置负载平衡器端点，请对每个端点使用相同的端口。
客户端类型	必须为*S3*。
网络协议	客户端在连接到此端点时将使用的网络协议。 • 选择 * HTTPS * 可进行安全的 TLS 加密通信（建议）。您必须附加安全证书，然后才能保存此端点。 • 选择 * HTTP * 可实现不太安全的未加密通信。对于非生产网格，请仅使用 HTTP 。
启用缓存	启用或禁用"网关节点上的缓存"用于此负载均衡器端点。 如果出现缓存问题，请参阅"排查负载均衡器缓存问题"。

管理接口

字段	说明
名称	端点的描述性名称，将显示在负载平衡器端点页面的表中。
端口	要用于访问网格管理器和/或租户管理器的StorageGRID端口。 • 网格管理器：**8443** • 租户管理器：**9443** • 网格管理器和租户管理器：**443** 注：您可以使用这些预设端口或其他可用端口。
接口类型	选择要使用此端点访问的StorageGRID接口对应的单选按钮。

字段	说明
不可信客户端网络	如果此端点应可供不可信的客户端网络访问，请选择*是*。否则，请选择*No*。 选择*是*时，端口在所有不可信的客户端网络上打开。 注意：创建负载平衡器端点时，只能将端口配置为对不可信客户端网络开放或关闭。

1. 选择 * 继续 * 。

选择绑定模式

步骤

1. 为端点选择绑定模式、以控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

   某些绑定模式可用于客户端端点或管理接口端点。此处列出了这两种端点类型的所有模式。

模式	说明
全局(默认用于客户端端点)	客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。 除非需要限制此端点的可访问性，否则请使用*Global"设置。
HA 组的虚拟 IP	客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。 具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。
节点接口	客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。
节点类型(仅限客户端端点)	根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。
所有管理节点(默认用于管理接口端点)	客户端必须使用任何管理节点的IP地址(或相应的FQDN)才能访问此端点。

   如果多个端点使用同一端口，StorageGRID 将使用此优先级顺序来确定要使用的端点：**HA**组的虚拟**IP *>*Node interfaces**>*Node type*>*Global"。

   如果要创建管理接口端点、则仅允许使用管理节点。

2. 如果选择了 * HA 组的虚拟 IP * ，请选择一个或多个 HA 组。

   如果要创建管理接口端点、请选择仅与管理节点关联的VIP。

3. 如果选择了 * 节点接口 * ，请为要与此端点关联的每个管理节点或网关节点选择一个或多个节点接口。
4. 如果选择了*Node type*，请选择管理节点(包括主管理节点和任何非主管理节点)或网关节点。

控制租户访问

只有当管理接口端点具有时，该端点才能控制租户访问租户管理器的接口类型。

步骤

1. 对于*租户访问*步骤，请选择以下选项之一：

字段	说明
允许所有租户(默认)	所有租户帐户都可以使用此端点来访问其分段。 如果尚未创建任何租户帐户、则必须选择此选项。添加租户帐户后、您可以编辑负载平衡器端点以允许或阻止特定帐户。
允许选定租户	只有选定租户帐户才能使用此端点访问其分段。
阻止选定租户	选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。

2. 如果要创建*HTTP*端点，则不需要附加证书。选择 * 创建 * 以添加新的负载平衡器端点。然后，转到完成后。否则，请选择 * 继续 * 以附加证书。

附加证书

步骤

1. 如果要创建 * HTTPS * 端点，请选择要附加到该端点的安全证书类型。

   此证书可确保S3客户端与管理节点或网关节点上的负载平衡器服务之间的连接安全。

   - * 上传证书 * 。如果您要上传自定义证书，请选择此选项。
   - * 生成证书 * 。如果您具有生成自定义证书所需的值，请选择此选项。
   - 使用**StorageGRID S3**证书。如果要使用全局S3 API证书、则选择此选项、此证书也可用于直接连接到存储节点。

     您无法选择此选项、除非已将默认S3 API证书(由网格CA签名)替换为由外部证书颁发机构签名的自定义证书。请参阅。 "配置S3 API证书"

   - 使用管理接口证书。如果要使用全局管理接口证书、则选择此选项、此证书也可用于直接连接到管理节点。
2. 如果您未使用StorageGRID S3证书、请上传或生成此证书。

上传证书

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

- * 服务器证书 * ： PEM 编码的自定义服务器证书文件。
- 证书专用密钥:自定义服务器证书专用密钥文件(`.key`)。

> EC 私钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

- * CA bundle* ：一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

- 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 创建 * 。+ 已创建负载平衡器端点。自定义证书将用于S3客户端或管理接口与端点之间的所有后续新连接。

生成证书

a. 选择 * 生成证书 * 。

b. 指定证书信息：

字段	说明
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。
有效天数	创建后证书过期的天数。

字段	说明
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 创建 * 。

此时将创建负载平衡器端点。自定义证书将用于S3客户端或管理接口与此端点之间的所有后续新连接。

完成后

步骤

1. 如果使用DNS、请确保DNS包含一条记录、用于将StorageGRID 完全限定域名(FQDN)与客户端用于建立连接的每个IP地址相关联。

   在 DNS 记录中输入的 IP 地址取决于您是否使用的是由负载平衡节点组成的 HA 组：

   - 如果已配置HA组、则客户端将连接到该HA组的虚拟IP地址。
   - 如果不使用HA组、则客户端将使用网关节点或管理节点的IP地址连接到StorageGRID 负载平衡器服务。

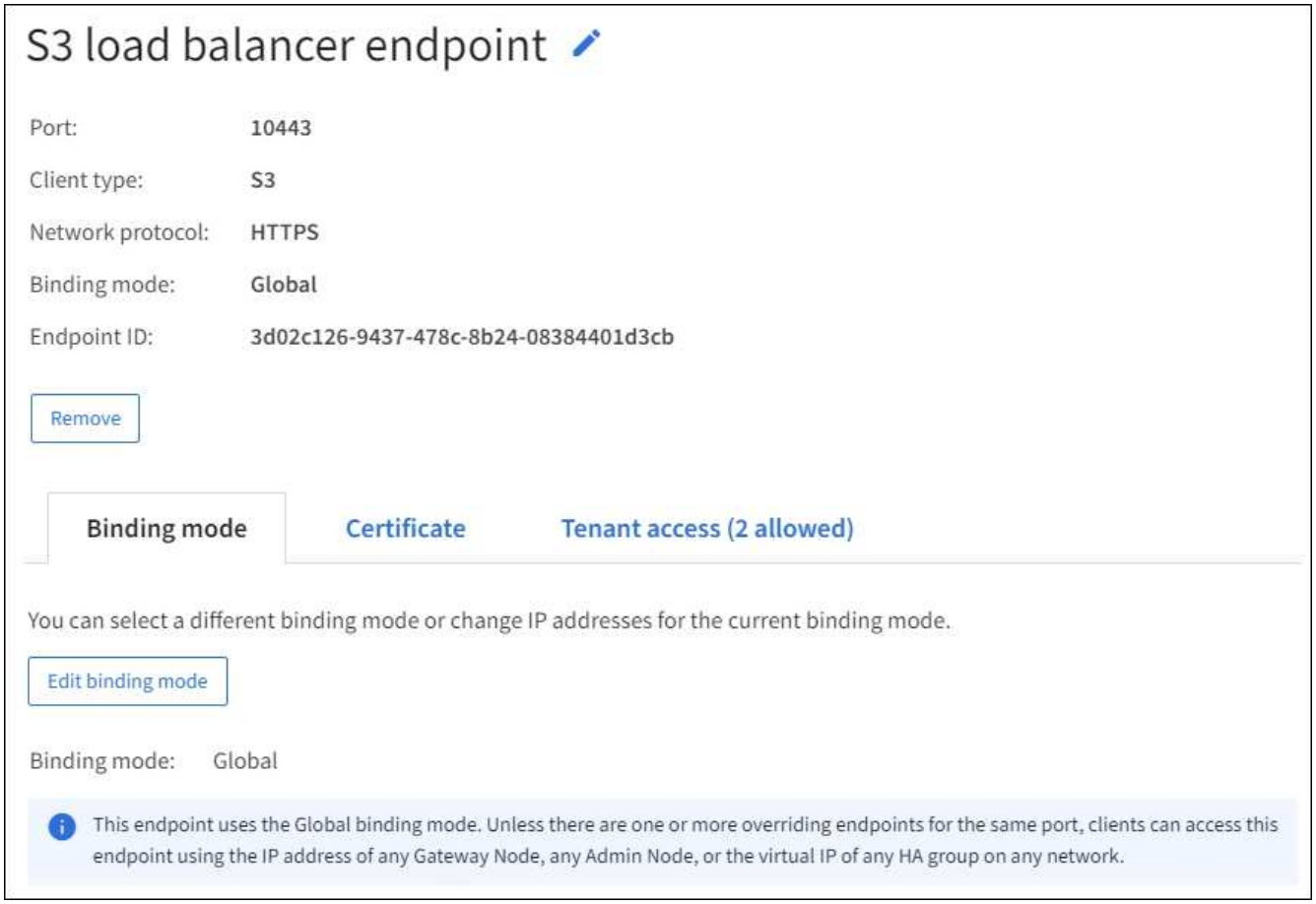
     此外，还必须确保 DNS 记录引用所有必需的端点域名，包括任何通配符名称。

2. 为S3客户端提供连接到端点所需的信息：
   - 端口号
   - 完全限定域名或 IP 地址
   - 任何必需的证书详细信息

查看和编辑负载平衡器端点

您可以查看现有负载平衡器端点的详细信息，包括安全端点的证书元数据。您可以更改端点的某些设置。

- 要查看所有负载平衡器端点的基本信息、请查看"负载平衡器端点"页面上的表。
- 要查看有关特定端点的所有详细信息，包括证书元数据，请在表中选择端点的名称。显示的信息因端点类型及其配置方式而异。



- 要编辑端点，请使用“负载平衡器端点”页面上的*Actions*菜单。

如果在编辑管理接口端点的端口时无法访问网格管理器、请更新URL和端口以重新获取访问权限。

编辑端点后，您可能需要等待长达 15 分钟，才能将所做的更改应用于所有节点。

任务	操作菜单	详细信息页面
编辑端点名称	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点名称 * 。 c. 输入新名称。 d. 选择 * 保存 * 。	a. 选择端点名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存 * 。

任务	操作菜单	详细信息页面
编辑端点端口	a. 选中此端点对应的复选框。 b. 选择*Actions*>*编辑端点端口* c. 输入有效的端口号。 d. 选择 * 保存 * 。	*n/A*
编辑端点绑定模式	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 编辑绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。
编辑端点证书	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点证书 * 。 c. 根据需要上传或生成新的自定义证书、或者开始使用全局S3证书。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 证书 * 选项卡。 c. 选择 * 编辑证书 * 。 d. 根据需要上传或生成新的自定义证书、或者开始使用全局S3证书。 e. 选择 * 保存更改 * 。
编辑租户访问	a. 选中此端点对应的复选框。 b. 选择*操作*>*编辑租户访问*。 c. 选择其他访问选项、从列表中选择或删除租户、或者同时执行这两项操作。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择*租户访问*选项卡。 c. 选择*编辑租户访问*。 d. 选择其他访问选项、从列表中选择或删除租户、或者同时执行这两项操作。 e. 选择 * 保存更改 * 。

删除负载平衡器端点

您可以使用 * 操作 * 菜单删除一个或多个端点，也可以从详细信息页面中删除单个端点。

为防止客户端中断、请在删除负载平衡器端点之前更新任何受影响的S3客户端应用程序。更新每个客户端以使用分配给另一个负载平衡器端点的端口进行连接。请务必同时更新所需的任何证书信息。

如果在删除管理接口端点时无法访问网格管理器、请更新此URL。

- 删除一个或多个端点：
  a. 在"负载平衡器"页面中、选中要删除的每个端点对应的复选框。

b. 选择 * 操作 * > * 删除 * 。

c. 选择 * 确定 * 。

- 从详细信息页面中删除一个端点：

a. 从"负载平衡器"页面中、选择端点名称。

b. 在详细信息页面上选择 * 删除 * 。

c. 选择 * 确定 * 。

在 **StorageGRID** 中配置 **S3** 端点域名

要支持S3虚拟托管模式请求、必须使用网格管理器配置S3客户端连接到的S3端点域名列表。

不支持使用IP地址作为端点域名。未来版本将禁止此配置。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 您已确认网格升级未在进行中。

在进行网格升级时、请勿对域名配置进行任何更改。

关于此任务

要使客户端能够使用 S3 端点域名，您必须执行以下所有操作：

- 使用网格管理器将 S3 端点域名添加到 StorageGRID 系统。
- 确保已为客户端所需的"客户端用于与StorageGRID 进行HTTPS连接的证书"所有域名签名。

  例如，如果端点为 `s3.company.com`，则必须确保用于HTTPS连接的证书包括 `s3.company.com`端点和端点的通配符主题替代名称(`Subject`备用名称，`SAN`)： `*.s3.company.com`。

- 配置客户端使用的 DNS 服务器。包括客户端用于建立连接的IP地址的DNS记录、并确保这些记录引用所有必需的S3端点域名、包括任何通配符名称。

客户端可以使用网关节点，管理节点或存储节点的 IP 地址或连接到高可用性组的虚拟 IP 地址连接到 StorageGRID 。您应了解客户端应用程序如何连接到网格，以便在 DNS 记录中包含正确的 IP 地址。

使用 HTTPS 连接（建议）连接到网格的客户端可以使用以下任一证书：

- 连接到负载平衡器端点的客户端可以对该端点使用自定义证书。可以对每个负载平衡器端点进行配置、使其能够识别不同的S3端点域名。
- 连接到负载平衡器端点或直接连接到存储节点的客户端可以自定义全局S3 API证书、以包含所有必需的S3端点域名。

如果不添加S3端点域名且此列表为空、则会禁用对S3虚拟托管模式请求的支持。

添加S3端点域名

步骤

1. 选择*配置* > 网络 > **S3** 端点域名。
2. 在*域名1*字段中输入域名。选择*添加其他域名*以添加更多域名。
3. 选择 * 保存 * 。
4. 确保客户端使用的服务器证书与所需的S3端点域名匹配。
   - 如果客户端连接到使用自己的证书的负载平衡器端点，则"更新与此端点关联的证书"。
   - 如果客户端连接到使用全局S3 API证书的负载平衡器端点或直接连接到存储节点，"更新全局S3 API证书"。
5. 添加所需的 DNS 记录，以确保可以解决端点域名请求。

结果

现在，当客户端使用端点时 *bucket.s3.company.com*，DNS服务器解析到正确的端点，证书按预期对端点进行身份验证。

重命名S3端点域名

如果更改S3应用程序使用的名称、虚拟托管模式请求将失败。

步骤

1. 选择*配置* > 网络 > **S3** 端点域名。
2. 选择要编辑的域名字段并进行必要的更改。
3. 选择 * 保存 * 。
4. 选择*是*确认更改。

删除S3端点域名

如果删除S3应用程序使用的名称、虚拟托管模式请求将失败。

步骤

1. 选择*配置* > 网络 > **S3** 端点域名。
2. 选择域名旁边的删除图标 ✕。
3. 选择*是*确认删除。

相关信息

- "使用S3 REST API"
- "查看 IP 地址"
- "配置高可用性组"

StorageGRID 客户端连接的 **IP** 地址和端口

要存储或检索对象、S3客户端应用程序会连接到负载平衡器服务(包含在所有管理节点和网关节点上)或本地分发路由器(LDR)服务(包含在所有存储节点上)。

客户端应用程序可以使用网格节点的IP地址以及该节点上服务的端口号连接到StorageGRID。或者、您也可以为负载平衡节点创建高可用性(HA)组、以提供使用虚拟IP (VIP)地址的高可用性连接。如果要使用完全限定域名(FQDN)而不是IP或VIP地址连接到StorageGRID 、则可以配置DNS条目。

此表总结了客户端连接到 StorageGRID 的不同方式以及每种连接类型所使用的 IP 地址和端口。如果已创建负载平衡器端点和高可用性(HA)组、请参见从何处查找IP地址以在网格管理器中查找这些值。

建立连接的位置	客户端连接到的服务	**IP** 地址	端口
HA组	负载平衡器	HA 组的虚拟 IP 地址	分配给负载平衡器端点的端口
管理节点	负载平衡器	管理节点的 IP 地址	分配给负载平衡器端点的端口
网关节点	负载平衡器	网关节点的 IP 地址	分配给负载平衡器端点的端口
存储节点	LDR	存储节点的 IP 地址	默认 S3 端口： • HTTPS：18082 • HTTP：18084

示例**URL**

要将客户端应用程序连接到网关节点HA组的负载平衡器端点、请使用如下所示的URL结构：

```
https://VIP-of-HA-group:LB-endpoint-port
```

例如、如果HA组的虚拟IP地址为192.0.2.5、负载平衡器端点的端口号为10443、则应用程序可以使用以下URL连接到StorageGRID ：

```
https://192.0.2.5:10443
```

从何处查找**IP**地址

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 要查找网格节点的 IP 地址，请执行以下操作：
   a. 选择*节点*。
   b. 选择要连接到的管理节点，网关节点或存储节点。
   c. 选择 * 概述 * 选项卡。
   d. 在节点信息部分中，记下节点的 IP 地址。

e. 选择 * 显示更多 * 可查看 IPv6 地址和接口映射。

您可以建立从客户端应用程序到列表中任何 IP 地址的连接：

- * eth0： * 网格网络
- * eth1： * 管理网络（可选）
- * eth2： * 客户端网络（可选）

> 如果您正在查看管理节点或网关节点，并且该节点是高可用性组中的活动节点，则 eth2 上会显示 HA 组的虚拟 IP 地址。

3. 要查找高可用性组的虚拟 IP 地址，请执行以下操作：
   a. 选择*配置* > 网络 > 高可用性组。
   b. 在表中，记下 HA 组的虚拟 IP 地址。
4. 查找负载平衡器端点的端口号：
   a. 选择*配置* > 网络 > 负载均衡器端点。
   b. 记下要使用的端点的端口号。

> 如果端口号为80或443、则仅在网关节点上配置端点、因为这些端口是在管理节点上预留的。所有其他端口都在网关节点和管理节点上进行配置。

   c. 从表中选择端点的名称。
   d. 确认*客户端类型*(S3)与要使用端点的客户端应用程序匹配。

管理网络和连接

配置 **StorageGRID** 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。

配置 **VLAN** 接口

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

流量分类策略

您可以使用来"流量分类策略"标识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。

StorageGRID 网络准则

您可以使用网格管理器配置和管理 StorageGRID 网络和连接。

请参见"配置S3客户端连接"、了解如何连接S3客户端。

默认 StorageGRID 网络

默认情况下， StorageGRID 支持每个网格节点使用三个网络接口，从而可以根据您的安全和访问要求为每个网格节点配置网络。

有关网络拓扑的详细信息，请参见"网络连接准则"。

网格网络

必填。网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。

管理网络

可选。管理网络通常用于系统管理和维护。它也可用于客户端协议访问。管理网络通常是一个专用网络，不需要在站点之间进行路由。

客户端网络

可选。客户端网络是一种开放式网络、通常用于提供对S3客户端应用程序的访问、因此可以隔离网格网络并确保其安全。客户端网络可以与可通过本地网关访问的任何子网进行通信。

准则

- 每个StorageGRID节点为其分配的每个网络都需要一个专用网络接口、IP地址、子网掩码和网关。
- 一个网格节点不能在一个网络上具有多个接口。
- 支持每个网格节点在每个网络上使用一个网关，并且该网关必须与节点位于同一子网中。如果需要，您可以在网关中实施更复杂的路由。
- 在每个节点上，每个网络都映射到一个特定的网络接口。

网络	接口名称
网格	eth0
admin （可选）	eth1
客户端（可选）	eth2

- 如果节点连接到 StorageGRID 设备，则每个网络都使用特定端口。有关详细信息，请参见适用于您的设备的安装说明。
- 每个节点都会自动生成默认路由。如果启用了 eth2 ，则 0.0.0.0/0 将在 eth2 上使用客户端网络。如果未启用 eth2 ，则 0.0.0.0/0 将在 eth0 上使用网格网络。
- 只有在网格节点加入网格后，客户端网络才会正常运行
- 可以在网格节点部署期间配置管理网络，以便在网格完全安装之前能够访问安装用户界面。

可选接口

您也可以向节点添加额外的接口。例如、您可能希望向管理节点或网关节点添加中继接口、以便使用"VLAN 接

口"隔离属于不同应用程序或租户的流量。或者，您可能需要添加要在中使用的访问接口"高可用性（ HA ）组"。

要添加中继或访问接口，请参见以下内容：

- **VMware (**安装节点后**)**："VMware ： 向节点添加中继或访问接口"
  - **Linux**（安装节点之前）："创建节点配置文件"
  - **Linux**（安装节点后）："向节点添加中继或访问接口"

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

在 **StorageGRID** 中查看 **IP** 地址

您可以查看 StorageGRID 系统中每个网格节点的 IP 地址。然后、您可以使用此IP地址通过命令行登录到网格节点并执行各种维护过程。

开始之前

您已使用登录到网格管理器"支持的 Web 浏览器"。

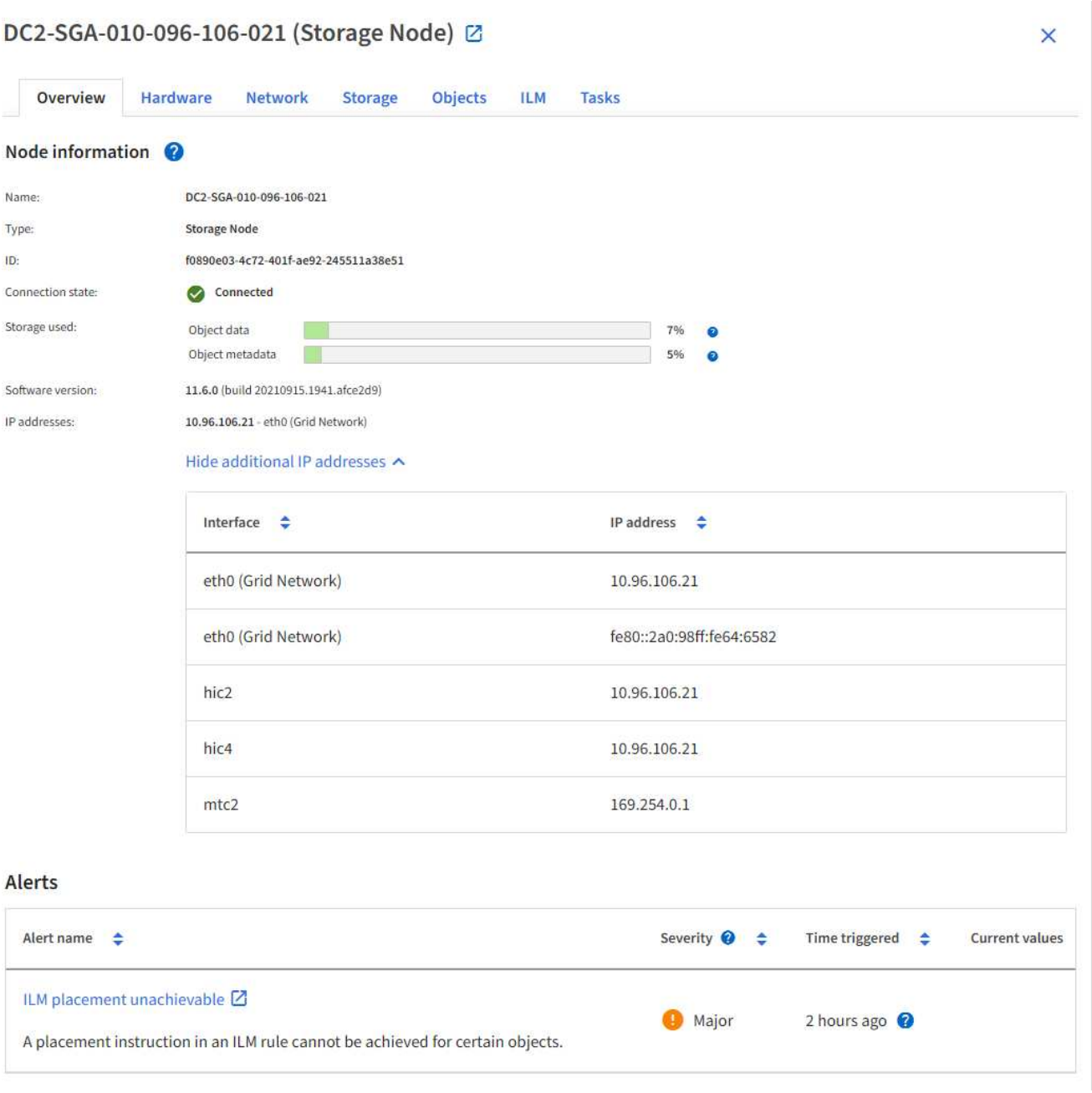
关于此任务

有关更改IP地址的信息，请参见"配置 IP 地址"。

步骤

1. 选择*节点* > ***grid node*** > 概览。
2. 选择 IP 地址标题右侧的 * 显示更多 * 。

   此网格节点的 IP 地址会在表中列出。



在 **StorageGRID** 中配置 **VLAN** 接口

在管理节点和网关节点上创建虚拟 LAN (VLAN) 接口，并在 HA 组和负载均衡器端点中使用它们来隔离和分区流量，从而实现安全性、灵活性和性能。HA 组中选定的节点可以使用 VLAN 接口共享最多 10 个虚拟 IP 地址，这样，如果一个节点出现故障，另一个节点将接管往返于虚拟 IP 地址的流量。

VLAN 接口注意事项

- 您可以通过输入 VLAN ID 并在一个或多个节点上选择父接口来创建 VLAN 接口。
- 必须在交换机上将父接口配置为中继接口。
- 父接口可以是网格网络（ eth0 ），客户端网络（ eth2 ），也可以是虚拟机或裸机主机的附加中继接口（例

如 ens256 ）。

- 对于每个 VLAN 接口，您只能为给定节点选择一个父接口。例如、不能将同一网关节点上的网格网络接口和客户端网络接口用作同一VLAN的父接口。
- 如果 VLAN 接口用于管理节点流量，其中包括与网格管理器和租户管理器相关的流量，请仅选择管理节点上的接口。
- 如果VLAN接口用于S3客户端流量、请选择管理节点或网关节点上的接口。
- 如果需要添加中继接口，请参见以下内容了解详细信息：
  - **VMware (**安装节点后)：“VMware ： 向节点添加中继或访问接口”
  - **Linux**（安装节点之前）：“创建节点配置文件”
  - **Linux**（安装节点后）：“向节点添加中继或访问接口”

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

创建 **VLAN** 接口

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 已在网络中配置中继接口并将其连接到 VM 或 Linux 节点。您知道中继接口的名称。
- 您知道要配置的 VLAN 的 ID 。

关于此任务

网络管理员可能已配置一个或多个中继接口以及一个或多个 VLAN ，以隔离属于不同应用程序或租户的客户端或管理流量。每个 VLAN 都通过一个数字 ID 或标记来标识。例如，您的网络可能使用 VLAN 100 传输 FabricPool 流量，而使用 VLAN 200 传输归档应用程序。

您可以使用网格管理器创建 VLAN 接口，以允许客户端访问特定 VLAN 上的 StorageGRID 。创建 VLAN 接口时，您可以指定 VLAN ID 并选择一个或多个节点上的父（中继）接口。

访问向导

步骤

1. 选择*配置* > 网络 > **VLAN** 接口。
2. 选择 * 创建 * 。

输入 **VLAN** 接口的详细信息

步骤

1. 指定网络中 VLAN 的 ID 。您可以输入 1 到 4094 之间的任何值。

   VLAN ID不需要唯一。例如，您可以对一个站点的管理流量使用 VLAN ID 200 ，而对另一个站点的客户端流量使用相同的 VLAN ID 。您可以在每个站点使用不同的父接口集创建单独的 VLAN 接口。但是、具有相同ID的两个VLAN接口不能在一个节点上共享同一个接口。如果指定的 ID 已被使用，则会显示一条消息。

2. 或者，输入 VLAN 接口的短问题描述 。
3. 选择 * 继续 * 。

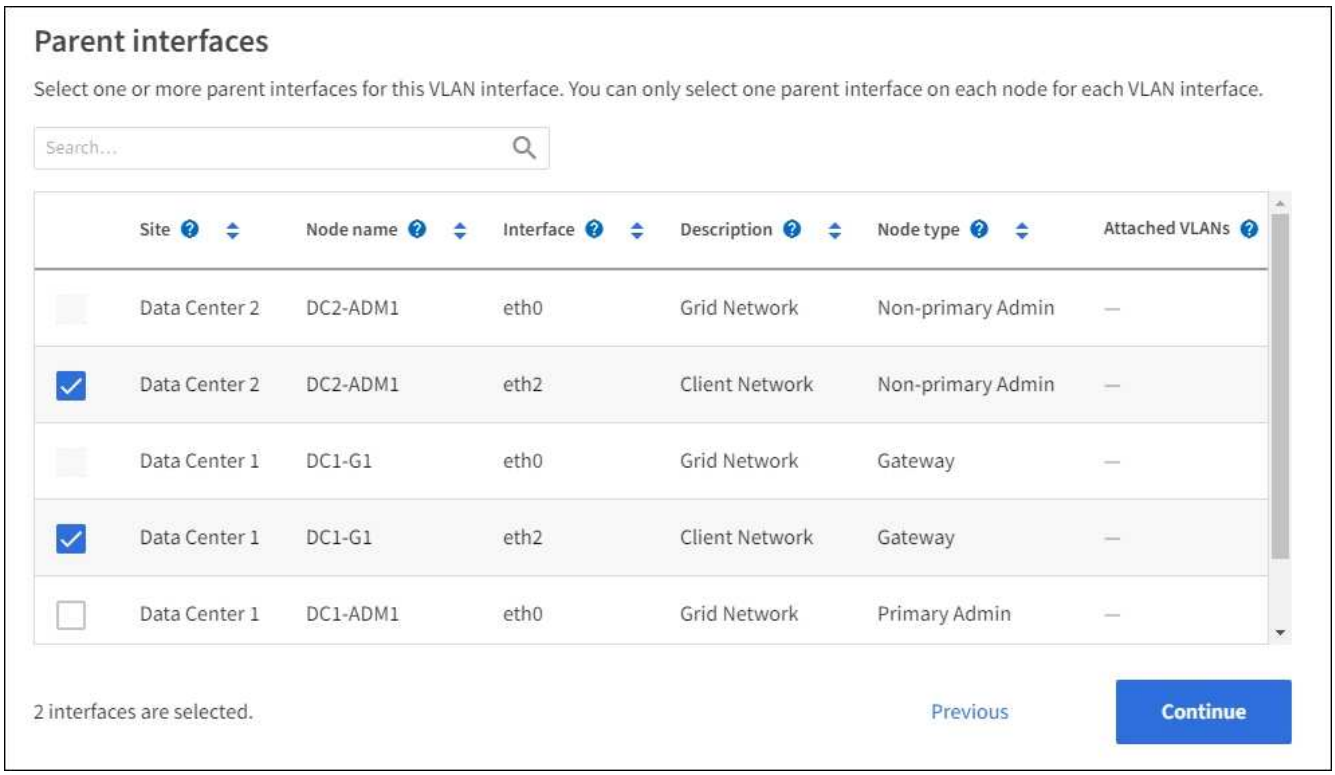
选择父接口

下表列出了网格中每个站点上所有管理节点和网关节点的可用接口。管理网络(eth1)接口不能用作父接口、因此不会显示出来。

步骤

1. 选择一个或多个要将此 VLAN 连接到的父接口。

   例如，您可能希望将 VLAN 连接到网关节点和管理节点的客户端网络（ eth2 ）接口。



2. 选择 * 继续 * 。

确认设置

步骤

1. 查看配置并进行任何更改。
   - 如果需要更改 VLAN ID 或问题描述 ，请选择页面顶部的 * 输入 VLAN 详细信息 * 。
   - 如果需要更改父接口，请选择页面顶部的 * 选择父接口 * 或选择 * 上一个 * 。
   - 如果需要删除父接口，请选择垃圾桶 。
2. 选择 * 保存 * 。
3. 等待最多 5 分钟，新的接口才会作为选择出现在“高可用性组”页面上，并列在节点的 网络接口 表中（节点 > 父接口节点 > 网络）。

编辑 **VLAN** 接口

编辑 VLAN 接口时，可以进行以下类型的更改：

- 更改 VLAN ID 或问题描述 。
- 添加或删除父接口。

例如，如果您计划停用关联节点，则可能需要从 VLAN 接口中删除父接口。

请注意以下事项：

- 如果在 HA 组中使用 VLAN 接口，则无法更改 VLAN ID 。
- 如果父接口在 HA 组中使用，则不能删除该父接口。

  例如、假设VLAN 200连接到节点A和B上的父接口。如果HA组对节点A使用VLAN 200接口、对节点B使用eth2接口、则可以删除节点B未使用的父接口、但不能删除节点A已使用的父接口

步骤

1. 选择*配置* > 网络 > **VLAN** 接口。
2. 选中要编辑的VLAN接口对应的复选框。然后，选择 * 操作 * > * 编辑 * 。
3. 也可以更新 VLAN ID 或问题描述 。然后，选择 * 继续 * 。

   如果在 HA 组中使用 VLAN ，则无法更新 VLAN ID 。

4. (可选)选中或清除相应复选框以添加父接口或删除未使用的接口。然后，选择 * 继续 * 。
5. 查看配置并进行任何更改。
6. 选择 * 保存 * 。

删除 **VLAN** 接口

您可以删除一个或多个 VLAN 接口。

如果 VLAN 接口当前正在 HA 组中使用，则无法将其删除。必须先从 HA 组中删除 VLAN 接口，然后才能将其删除。

要避免客户端流量发生任何中断，请考虑执行以下操作之一：

- 在删除此 VLAN 接口之前，请向 HA 组添加一个新的 VLAN 接口。
- 创建不使用此 VLAN 接口的新 HA 组。
- 如果要删除的 VLAN 接口当前为活动接口，请编辑 HA 组。将要删除的 VLAN 接口移至优先级列表的底部。等待新主接口建立通信，然后从 HA 组中删除旧接口。最后，删除该节点上的 VLAN 接口。

步骤

1. 选择*配置* > 网络 > **VLAN** 接口。
2. 选中要删除的每个VLAN接口对应的复选框。然后，选择 * 操作 * > * 删除 * 。
3. 选择 * 是 * 确认您的选择。

选定的所有 VLAN 接口都将被删除。VLAN 接口页面上会显示一个绿色的成功横幅。

为管理接口启用StorageGRID CORS

作为网格管理员，如果您希望另一个域可以使用管理 API 访问StorageGRID中的数据，则可以为对StorageGRID 的管理 API 请求启用跨域资源共享 (CORS)。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 这"root访问权限"提供对所有 CORS 配置请求的访问。

关于此任务

CORS 是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如，假设您想在域中为StorageGRID构建一个监控仪表板 `http://www.example.com`。通过在StorageGRID中启用 CORS `http://www.example.com`和"网格管理器"， StorageGRID域响应来自 `\http://www.example.com`。

管理 API (mgmt-api) 请求 `application/json`或者 `multipart/formdata`请求 `Content-Type`支持 CORS。

步骤

1. 在网格管理器中，转到*配置* > 网络 > 管理界面 **CORS** 设置。
2. 选择*网格管理器*、*租户管理器*或两个选项。
   - 网格管理器：为跨域网格管理 API 请求启用 CORS。
   - 租户管理器：为跨域租户管理 API 请求启用 CORS。
3. 在"域"字段中输入其他域的 URL。

   如果您想在StorageGRID中为多个域启用 CORS，请选择"添加另一个域"。
4. 选择 * 保存 * 。

相关信息

"为存储桶和对象配置StorageGRID CORS"

管理流量分类策略

StorageGRID 中的流量分类策略

通过流量分类策略、您可以识别和监控不同类型的网络流量。这些策略可以帮助您进行流量限制和监控、以增强服务质量(QoS)产品。

流量分类策略应用于网关节点和管理节点的 StorageGRID 负载平衡器服务上的端点。要创建流量分类策略，必须已创建负载平衡器端点。

匹配规则

每个流量分类策略都包含一个或多个匹配规则，用于标识与以下一个或多个实体相关的网络流量：

- 存储分段
- 子网
- 租户
- 负载平衡器端点

StorageGRID 会根据规则的目标监控与策略中任何规则匹配的流量。与某个策略的任何规则匹配的任何流量均由该策略处理。相反，您可以设置规则来匹配除指定实体之外的所有流量。

流量限制

您也可以将以下限制类型添加到策略中：

- 聚合带宽
- 每个请求的带宽
- 并发请求
- 请求率

限制值按负载平衡器强制实施。如果流量同时分布在多个负载平衡器上，则总最大速率是您指定的速率限制的倍数。

> 您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是、StorageGRID 不能同时限制这两种类型的带宽。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。

对于聚合或每个请求的带宽限制，请求以您设置的速率流入或流出。StorageGRID 只能强制执行一种速度，因此最具体的策略匹配（按匹配器类型）是强制执行的策略匹配。请求消耗的带宽不计入包含总带宽限制策略的其他不太具体的匹配策略。对于所有其他限制类型，客户端请求将延迟 250 毫秒，并且对于超过任何匹配策略限制的请求，将收到 503 Slow Down 响应。

在 Grid Manager 中，您可以查看流量图表并验证策略是否执行了预期的流量限制。

使用具有 **SLA** 的流量分类策略

您可以将流量分类策略与容量限制和数据保护结合使用来实施服务级别协议（ SLA ），这些协议提供了有关容量，数据保护和性能的具体信息。

以下示例显示了一个 SLA 的三个层。您可以创建流量分类策略以实现每个 SLA 层的性能目标。

服务级别层	容量	数据保护	允许的最高性能	成本
金牌	允许 1 PB 存储	3 复制 ILM 规则	25 K 请求 / 秒 5 GB/ 秒（ 40 Gbps ）带宽	每月 $$
银牌	允许 250 TB 存储	2 复制 ILM 规则	10 K 请求 / 秒 1.25 GB/ 秒（ 10 Gbps ）带宽	每月 $$

服务级别层	容量	数据保护	允许的最高性能	成本
铜牌	允许 100 TB 存储	2 复制 ILM 规则	5 K 请求 / 秒 1 GB/ 秒（ 8 Gbps ）带宽	每月 $

创建 **StorageGRID** 流量分类策略

如果要监控网络流量、您可以创建流量分类策略、也可以选择按分段、分段正则表达式、CIDR、负载平衡器端点或租户限制网络流量。您也可以根据带宽，并发请求数或请求率为策略设置限制。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 您已创建要匹配的任何负载平衡器端点。
- 您已创建要匹配的任何租户。

步骤

1. 选择*配置* > 网络 > 流量分类。
2. 选择 * 创建 * 。
3. 为策略输入名称和问题描述 (可选)，然后选择*CONTINUE*。

   例如，描述此流量分类策略适用场景 及其限制。

4. 选择*添加规则*并指定以下详细信息，为策略创建一个或多个匹配规则。您创建的任何策略都应至少具有一个匹配规则。选择 * 继续 * 。

字段	说明
键入	选择与规则适用场景 匹配的流量类型。流量类型包括存储分段、存储分段正则表达式、CIDR、负载平衡器端点和租户。

字段	说明
匹配值	输入与选定类型匹配的值。 • 存储分段：输入一个或多个存储分段名称。 • b分 段正则表达式：输入用于匹配一组分段名称的一个或多个正则表达式。 正则表达式已取消锁定。在分段名称的开头使用^锚定进行匹配、在名称的结尾使用$锚定进行匹配。正则表达式匹配支持PCRE (Perl兼容正则表达式)语法的子集。 • cidr：以CIDR表示法输入一个或多个与所需子网匹配的IPv4子网。 • 负载平衡器端点：选择端点名称。这些是您在上定义的负载平衡器端点"配置负载平衡器端点"。 • 租户：租户匹配使用访问密钥ID。如果此请求不包含访问密钥ID (例如、匿名访问)、则会使用所访问存储分段的所有权来确定租户。
反向匹配	如果要匹配与刚刚定义的类型和匹配值一致的所有网络流量_例外_流量，请选中*反向匹配*复选框。否则、请清除此复选框。 例如，如果要将此策略应用于除一个负载平衡器端点之外的所有端点，请指定要排除的负载平衡器端点，然后选择*Inverse Match*。 对于包含多个匹配器且至少有一个是反向匹配器的策略，请注意不要创建与所有请求匹配的策略。

5. (可选)选择*添加限制*，然后选择以下详细信息以添加一个或多个限制，以控制规则匹配的网络流量。

   即使您未添加任何限制、StorageGRID 也会收集指标、以便您了解流量趋势。

字段	说明
键入	要应用于规则匹配的网络流量的限制类型。例如、您可以限制带宽或请求速率。 注意：您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是、StorageGRID 不能同时限制这两种类型的带宽。使用聚合带宽时、每个请求的带宽不可用。相反、如果正在使用每个请求的带宽、则聚合带宽将不可用。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。 对于带宽限制， StorageGRID 会应用与设置的限制类型最匹配的策略。例如，如果您的策略仅限制一个方向的流量，则相反方向的流量将是无限制的，即使存在与具有带宽限制的其他策略匹配的流量也是如此。StorageGRID 按以下顺序实施带宽限制的"最佳"匹配： • 确切的 IP 地址（ /32 掩码） • 确切的存储分段名称 • 分段正则表达式 • 租户 • 端点 • 非精确的 CIDR 匹配项（非 /32 ） • 反向匹配
适用场景	这是否会限制适用场景 客户端读取请求(GET或HEAD)或写入请求(Put、POST或DELETE)。
价值	根据您选择的单位、网络流量将限制为的值。例如、输入10并选择MiB/秒、以防止与此规则匹配的网络流量超过10 MiB/秒 注意：根据单位设置，可用单位可以是二进制(例如GiB)或十进制(例如GB)。要更改单位设置，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。
Unit	描述您输入的值的单位。

例如，如果您想为 SLA 层创建 4 GB/s 的带宽限制，请创建两个聚合带宽限制：GET/HEAD 为 4 GB/s ，PUT/POST/DELETE 为 4 GB/s。

6. 选择 * 继续 * 。
7. 阅读并查看流量分类策略。使用*上一步*按钮返回并根据需要进行更改。对策略满意后，选择*保存并继续*。

   现在、S3客户端流量将根据流量分类策略进行处理。

完成后

"查看网络流量指标"验证策略是否强制实施了预期的流量限制。

编辑 StorageGRID 流量分类策略

您可以编辑流量分类策略以更改其名称或问题描述，或者创建，编辑或删除此策略的任何规则或限制。

开始之前

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

步骤

1. 选择*配置* > 网络 > 流量分类。

   此时将显示"流量分类策略"页面、并在表中列出现有策略。

2. 使用操作菜单或详细信息页面编辑策略。请参见"创建流量分类策略"了解要输入的内容。

   操作菜单

   a. 选中策略对应的复选框。

   b. 选择*Actions*>*Edit*。

   详细信息页面

   a. 选择策略名称。

   b. 选择策略名称旁边的*Edit*按钮。

3. 对于输入策略名称步骤，可选择编辑策略名称或问题描述，然后选择*CONTINUOD*。
4. 对于添加匹配规则步骤，可选择添加规则或编辑现有规则的*Type*和*Match Value*，然后选择*Continue*。
5. 对于“设置限制”步骤，可以选择添加、编辑或删除限制，然后选择*CONTINUOD*。
6. 查看更新后的策略，然后选择*保存并继续*。

   您对策略所做的更改将被保存，网络流量现在将根据流量分类策略进行处理。您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

删除 StorageGRID 流量分类策略

您可以删除不再需要的流量分类策略。请确保删除正确的策略、因为删除策略后无法检索到该策略。

开始之前

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

步骤

1. 选择*配置* > 网络 > 流量分类。

此时将显示"流量分类策略"页面、其中的现有策略在表中列出。

2. 使用操作菜单或详细信息页面删除策略。

操作菜单

a. 选中策略对应的复选框。

b. 选择 * 操作 * > * 删除 * 。

策略详细信息页面

a. 选择策略名称。

b. 选择策略名称旁边的*Remove*按钮。

3. 选择*是*确认要删除策略。

此策略将被删除。

在 **StorageGRID** 中查看网络流量指标

您可以通过查看"流量分类策略"页面中提供的图形来监控网络流量。

开始之前

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

关于此任务

对于任何现有流量分类策略、您可以查看负载平衡器服务的指标、以确定该策略是否成功限制网络中的流量。图形中的数据可以帮助您确定是否需要调整策略。

即使没有为流量分类策略设置限制，也会收集指标，并且图形可提供有用的信息来了解流量趋势。

步骤

1. 选择*配置* > 网络 > 流量分类。

此时将显示"流量分类策略"页面、表中将列出现有策略。

2. 选择要查看其指标的流量分类策略名称。

3. 选择*Metrics *选项卡。

此时将显示流量分类策略图形。这些图形仅显示与选定策略匹配的流量的指标。

页面上包含以下图形。

- 请求速率：此图提供与所有负载平衡器处理的此策略匹配的带宽量。收到的数据包括所有请求的请求标头以及包含正文数据的响应的正文数据大小。Sent包括所有请求的响应标头以及响应中包含正文数据的请求的响应正文数据大小。

请求完成后、此图表仅显示带宽使用量。对于速度较慢或较大的对象请求、实际瞬时带宽可能与此图中报告的值不同。

- 错误响应率：此图提供了与此策略匹配的请求向客户端返回错误(HTTP状态代码>= 400)的大致速率。
- 平均请求持续时间(无错误)：此图形提供与此策略匹配的成功请求的平均持续时间。
- 策略带宽使用量：此图提供与所有负载平衡器处理的此策略匹配的带宽量。收到的数据包括所有请求的请求标头以及包含正文数据的响应的正文数据大小。Sent包括所有请求的响应标头以及响应中包含正文数据的请求的响应正文数据大小。

4. 将光标置于折线图上方、可查看该图特定部分上的值弹出窗口。
5. 选择指标标题下方的* Grafana DDashboard *以查看策略的所有图形。除了*Metrics *选项卡中的四个图形之外，您还可以查看另外两个图形：
   - Write Request Rate by object size：与此策略匹配的放置/后置/删除请求的速率。单个单元格上的定位显示每秒的速率。悬停视图中显示的速率会被截断为整数、如果存储分段中存在非零请求、则可能会报告0。
   - 按对象大小划分的读取请求速率：与此策略匹配的GET或HEAD请求的速率。单个单元格上的定位显示每秒的速率。悬停视图中显示的速率会被截断为整数、如果存储分段中存在非零请求、则可能会报告0。
6. 或者，从*支持*菜单访问图表。
   a. 选择*支持* > 工具 > 指标。
   b. 从* Grafana 部分选择*交通分类政策。
   c. 从页面左上角的菜单中选择策略。
   d. 将光标置于图形上方可查看一个弹出窗口、其中显示了样本的日期和时间、汇总到计数中的对象大小以及该时间段内每秒的请求数。

      流量分类策略通过其 ID 进行标识。策略ID将在"流量分类策略"页面上列出。
7. 分析图形以确定策略限制流量的频率以及是否需要调整策略。

StorageGRID 中传出 **TLS** 连接支持的密码

StorageGRID 系统支持一组有限的密码套件，用于将传输层安全（ Transport Layer Security ， TLS ）连接到用于身份联合和云存储池的外部系统。

支持的 **TLS** 版本

StorageGRID 支持使用 TLS 1.2 和 TLS 1.3 连接到用于身份联合和云存储池的外部系统。

已选择支持与外部系统一起使用的 TLS 密码，以确保与一系列外部系统兼容。该列表大于支持与 S3 客户端应用程序一起使用的密码列表。要配置密码，请转到*配置*>*安全*>*安全设置*并选择*TLS 和 SSH 策略*。

在StorageGRID 中、无法配置协议版本、密码、密钥交换算法和MAC算法等TLS配置选项。如果您对这些设置有特定要求，请联系您的 NetApp 客户代表。

StorageGRID 中活动、空闲和并发 **HTTP** 连接的优势

如何配置 HTTP 连接可能会影响 StorageGRID 系统的性能。根据 HTTP 连接是活动连接

还是空闲连接，或者您有多个并发连接，配置会有所不同。

您可以确定以下类型的 HTTP 连接的性能优势：

- 空闲 HTTP 连接
- 活动 HTTP 连接
- 并发 HTTP 连接

保持空闲 **HTTP** 连接处于打开状态的优势

当客户端应用程序空闲时，保持 HTTP 连接打开以允许后续事务。保持空闲 HTTP 连接打开最多 10 分钟。StorageGRID可能会自动关闭处于打开状态且空闲时间超过 10 分钟的 HTTP 连接。

开放式和空闲 HTTP 连接具有以下优势：

- 从 StorageGRID 系统确定必须执行 HTTP 事务的时间缩短到 StorageGRID 系统可以执行此事务的时间

  缩短延迟是主要优势，尤其是在建立 TCP/IP 和 TLS 连接所需的时间方面。

- 通过在先前执行的传输中填充 TCP/IP 慢速启动算法来提高数据传输速率
- 瞬时通知多种中断客户端应用程序与 StorageGRID 系统之间连接的故障情况

通过平衡慢启动优势和资源分配来决定保持空闲连接打开的时间。

活动 **HTTP** 连接的优势

对于直接连接到存储节点的连接、应将活动HTTP连接的持续时间限制为最长10分钟、即使HTTP连接持续执行事务也是如此。

- 连接应保持打开状态的最长持续时间是为了权衡连接持久性的优势与将连接分配给内部系统资源的理想方式。

对于客户端与存储节点的连接、限制活动HTTP连接具有以下优势：

- 在 StorageGRID 系统之间实现最佳负载平衡。

  随着时间的推移，由于负载平衡要求的变化，HTTP 连接可能不再是最佳的。当客户端应用程序为每个事务建立单独的 HTTP 连接时，系统会执行最佳的负载平衡，但这种方法会抵消与持久连接相关的宝贵收益。

- 允许客户端应用程序将 HTTP 事务定向到具有可用空间的 LDR 服务。
- 允许开始维护过程。

  某些维护过程仅在所有正在进行的 HTTP 连接完成后才会启动。

对于客户端与负载平衡器服务的连接，限制打开连接的持续时间对于允许某些维护过程立即启动非常有用。如果客户端连接的持续时间不受限制、则可能需要几分钟的时间、活动连接才会自动终止。

并发 **HTTP** 连接的优势

您应保持与 StorageGRID 系统的多个 TCP/IP 连接处于开放状态，以实现并行处理，从而提高性能。并行连接的最佳数量取决于多种因素。

并发 HTTP 连接具有以下优势：

- 缩短延迟

  事务可以立即启动，而不是等待其他事务完成。

- 提高吞吐量

  StorageGRID 系统可以执行并行事务并提高聚合事务吞吐量。

客户端应用程序应建立多个 HTTP 连接。当客户端应用程序必须执行事务时，它可以选择并立即使用当前未处理事务的任何已建立连接。

每个StorageGRID系统的拓扑对于并发事务和连接都有不同的峰值吞吐量。峰值吞吐量取决于计算、网络、存储资源、WAN 链接以及StorageGRID系统支持的服务器、服务和应用程序的数量。

StorageGRID系统通常支持多个客户端应用程序。在确定最大并发连接数时请记住这一点。如果客户端应用程序由多个软件实体组成，每个实体都与StorageGRID系统建立连接，则将跨实体的所有连接加起来。在以下情况下，您可能需要调整最大并发连接数：

- StorageGRID 系统的拓扑会影响系统可以支持的并发事务和连接的最大数量。
- 如果客户端应用程序通过带宽有限的网络与 StorageGRID 系统进行交互，则可能需要降低并发程度，以确保各个事务在合理时间内完成。
- 当许多客户端应用程序共享 StorageGRID 系统时，您可能需要降低并发程度，以避免超过系统限制。

为读取和写入操作分隔 **HTTP** 连接池

您可以使用单独的 HTTP 连接池执行读写操作，并控制每个连接池要使用的池容量。通过单独的 HTTP 连接池，您可以更好地控制事务并平衡负载。

客户端应用程序可以创建检索占主导地位（读取）或存储占主导地位（写入）的负载。由于读取和写入事务使用单独的 HTTP 连接池，因此您可以调整每个池中用于读取或写入事务的数量。

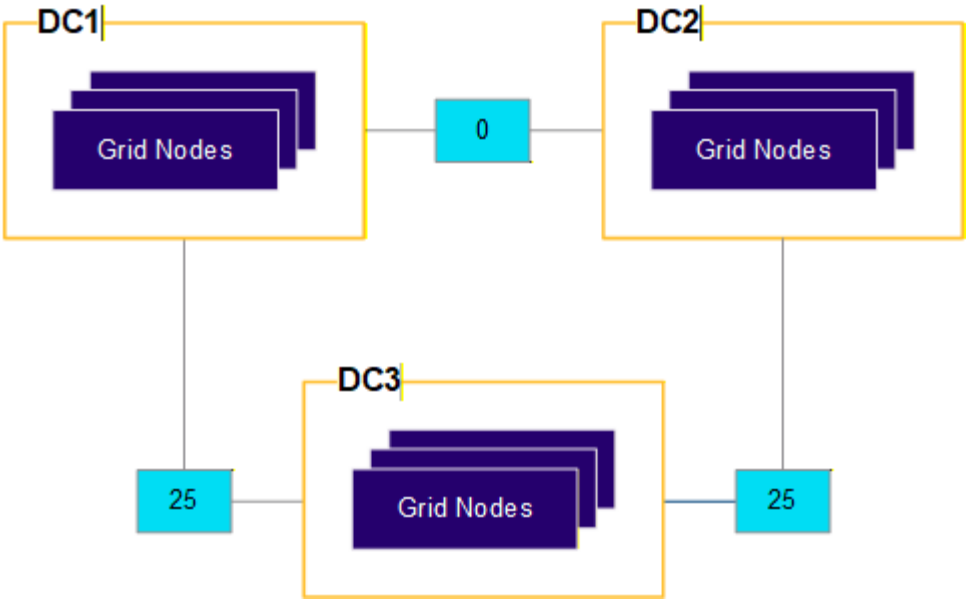
在 **StorageGRID** 中管理链路成本

链路成本可用于确定存在两个或更多数据中心站点时哪个数据中心站点提供请求的服务的优先级。您可以调整链路成本以反映站点之间的延迟。

什么是链路成本？

- 链接成本用于确定用于实现对象检索的对象副本的优先级。
- 网格管理 API 和租户管理 API 使用链路成本来确定要使用的内部 StorageGRID 服务。
- 链路开销由管理节点和网关节点上的负载平衡器服务用于引导客户端连接。请参阅 "负载平衡注意事项"。

该图显示了一个三站点网格，该网格在站点之间配置了链接成本：



- 管理节点和网关节点上的负载平衡器服务会将客户端连接平均分布到同一数据中心站点上的所有存储节点以及链路成本为0的任何数据中心站点。

  在此示例中，数据中心站点 1 （ DC1 ）的网关节点会将客户端连接平均分布到 DC1 的存储节点和 DC2 的存储节点。DC3 上的网关节点仅向 DC3 上的存储节点发送客户端连接。

- 在检索作为多个复制副本存在的对象时， StorageGRID 会在链路成本最低的数据中心检索此副本。

  在此示例中、如果DC2的客户端应用程序检索到同时存储在DC1和DC3的对象、则会从DC1检索该对象、因为从DC1到DC2的链路成本为0、低于从DC3到DC2的链路成本(25)。

链路成本是任意的相对数字，没有特定的度量单位。例如，使用链路成本 50 比使用链路成本 25 更低。下表显示了常用链路成本。

链路	链路成本	备注
物理数据中心站点之间	25 (默认)	通过 WAN 链路连接的数据中心。
位于同一物理位置的逻辑数据中心站点之间	0	逻辑数据中心位于通过 LAN 连接的同一物理建筑或园区中。

更新链路成本

您可以更新数据中心站点之间的链路成本，以反映站点之间的延迟。

开始之前

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

步骤

1. 选择*支持* > 其他 > 链接成本。

2. 对于"站点/链接成本"列中列出的每个站点，为其他站点输入一个介于 0 到 100 之间的成本值。

   如果源与目标相同、则无法更改链接成本。

3. 放弃或保存更改：
   - 要放弃更改，请选择*清除更改*。
   - 要保存更改，请选择*保存*。

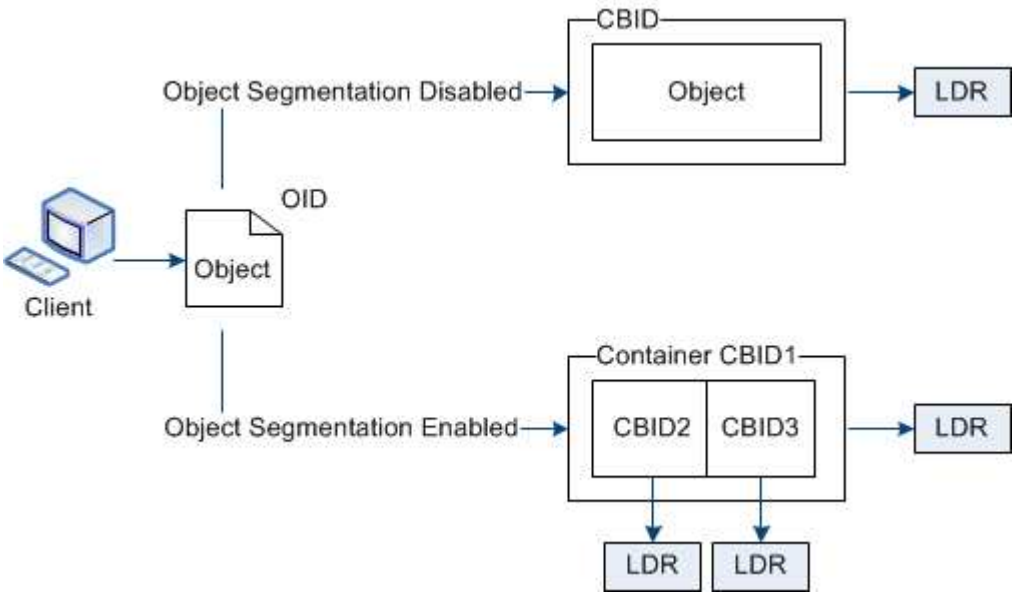
管理存储节点

使用存储选项

了解 StorageGRID 中的对象分段

对象分段是指将对象拆分为一组大小固定的较小对象的过程、用于优化大型对象的存储和资源使用。S3 多部分上传还会创建分段对象，其中每个部分都有一个对象。

将对象载入 StorageGRID 系统后， LDR 服务会将该对象拆分为多个区块，并创建一个区块容器，其中会将所有区块的标题信息列为内容。



检索分段容器时， LDR 服务会从其分段中汇集原始对象并将该对象返回给客户端。

容器和区块不一定存储在同一个存储节点上。容器和分段可以存储在 ILM 规则中指定的存储池中的任何存储节点上。

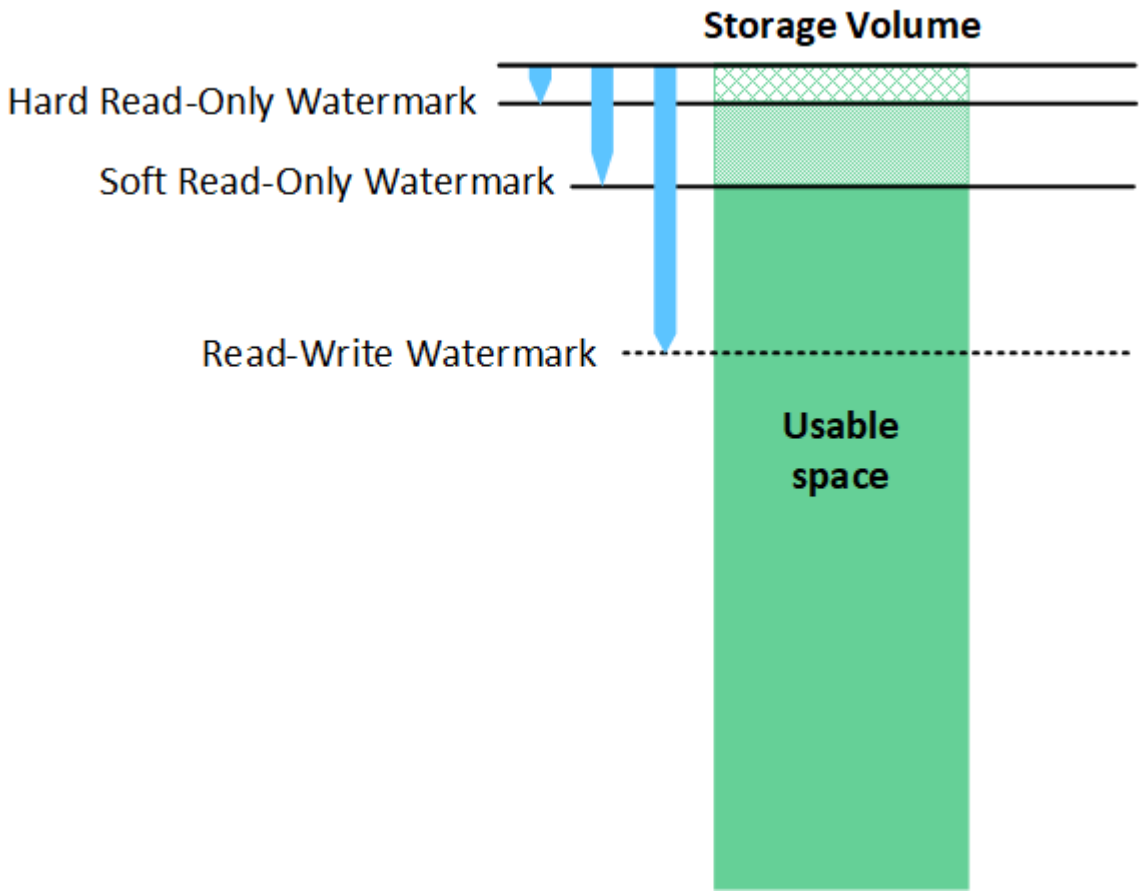
StorageGRID 系统会单独处理每个区块，并计入受管对象和存储对象等属性的数量。例如，如果存储在 StorageGRID 系统中的对象拆分为两个区块，则在载入完成后，受管对象的值将增加三个，如下所示：

```
segment container + segment 1 + segment 2 = three stored objects
```

了解 StorageGRID 中的存储卷水印

StorageGRID 使用三个存储卷水印来确保存储节点在空间严重不足之前安全地过渡到只读

状态，并允许已过渡到只读状态的存储节点再次变为读写状态。



存储卷水印仅适用于用于复制和擦除编码对象数据的空间。要了解为卷0上的对象元数据预留的空间，请转至"管理对象元数据存储"。

什么是软只读水印?

*存储卷软只读水印*是第一个水印、用于指示存储节点用于对象数据的可用空间已满。

如果存储节点中每个卷的可用空间小于该卷的软只读水印、则该存储节点将过渡到_read-only mode_。只读模式表示存储节点向 StorageGRID 系统的其余部分公布只读服务，但满足所有待处理的写入请求。

例如、假设存储节点中的每个卷都具有10 GB的软只读水印。一旦每个卷的可用空间小于 10 GB ，存储节点就会过渡到软只读模式。

什么是硬只读水印?

下一个水印是*存储卷硬只读水印*，表示节点用于对象数据的可用空间已满。

如果卷上的可用空间小于该卷的硬只读水印、则对该卷的写入将失败。但是、可以继续向其他卷写入数据、直到这些卷上的可用空间小于硬只读水印为止。

例如、假设存储节点中的每个卷都有一个硬只读水印、即5 GB。一旦每个卷的可用空间小于 5 GB ，存储节点就不再接受任何写入请求。

硬只读水印始终小于软只读水印。

什么是读写水印?

存储卷读写水印*仅适用于已转换为只读模式的存储节点。它可确定节点何时可以重新变为读写状态。如果存储节点中任一存储卷上的可用空间大于该卷的读写水印、则该节点会自动转换回读写状态。

例如，假设存储节点已过渡到只读模式。此外、还假设每个卷都有一个读写水印、大小为30 GB。任何卷的可用空间增加到 30 GB 后，节点将再次变为读写状态。

读写水印始终大于软只读水印和硬只读水印。

查看存储卷水印

您可以查看当前水印设置和系统优化的值。如果未使用优化水印、您可以确定是否可以或应该调整设置。

开始之前

- 您已完成StorageGRID 11.6或更高版本的升级。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

查看当前水印设置

您可以在网格管理器中查看当前存储水印设置。

步骤

1. 选择*支持* > 其他 > 存储水印。
2. 在存储水印页面上、查看使用优化值复选框。
   - 如果选中此复选框、则会根据存储节点的大小和卷的相对容量为每个存储节点上的每个存储卷优化所有三个水印。

     这是默认的建议设置。请勿更新这些值。您也可以选择查看优化的存储水印。
   - 如果未选中使用优化值复选框、则会使用自定义(非优化)水印。不建议使用自定义水印设置。按照的说明"对低只读水印覆盖警报进行故障排除"确定您是否可以或应该调整设置。

     指定自定义水印设置时、必须输入大于0的值。

[[view-优化 的存储水印**]]**查看优化的存储水印

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

1. 选择*支持* > 工具 > 指标。
2. 在 Prometheus 部分中，选择用于访问 Prometheus 用户界面的链接。
3. 要查看建议的最小软只读水印，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

管理 **StorageGRID** 中的对象元数据存储

StorageGRID 系统的对象元数据容量用于控制可存储在该系统上的最大对象数。为了确保 StorageGRID 系统有足够的空间来存储新对象，您必须了解 StorageGRID 在何处以及如何存储对象元数据。

什么是对象元数据?

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

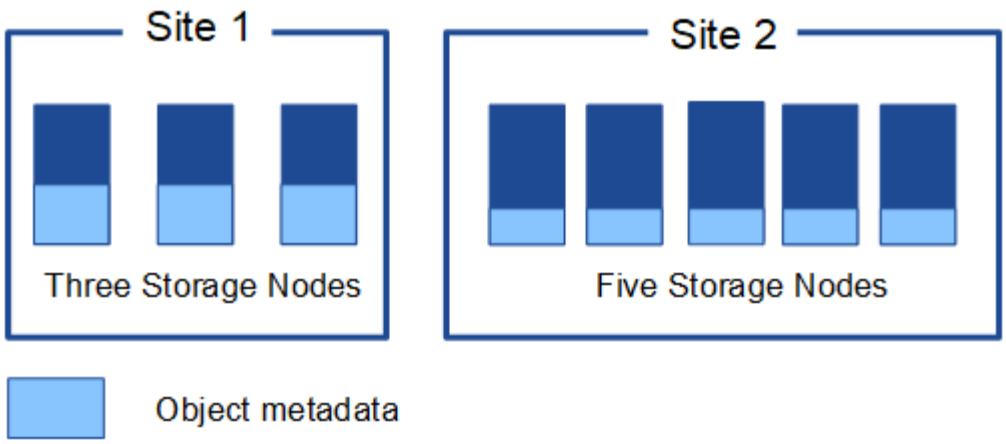
对于 StorageGRID 中的对象，对象元数据包括以下类型的信息：

- 系统元数据、包括每个对象的唯一ID (UUID)、对象名称、S3存储分段的名称、租户帐户名称或ID、对象的逻辑大小、首次创建对象的日期和时间以及上次修改对象的日期和时间。
- 与对象关联的任何自定义用户元数据键值对。
- 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
- 对于复制的对象副本，为每个副本提供当前存储位置。
- 对于经过擦除编码的对象副本，为每个片段的当前存储位置。
- 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。
- 对于分段对象和多部分对象，分段标识符和数据大小。

如何存储对象元数据?

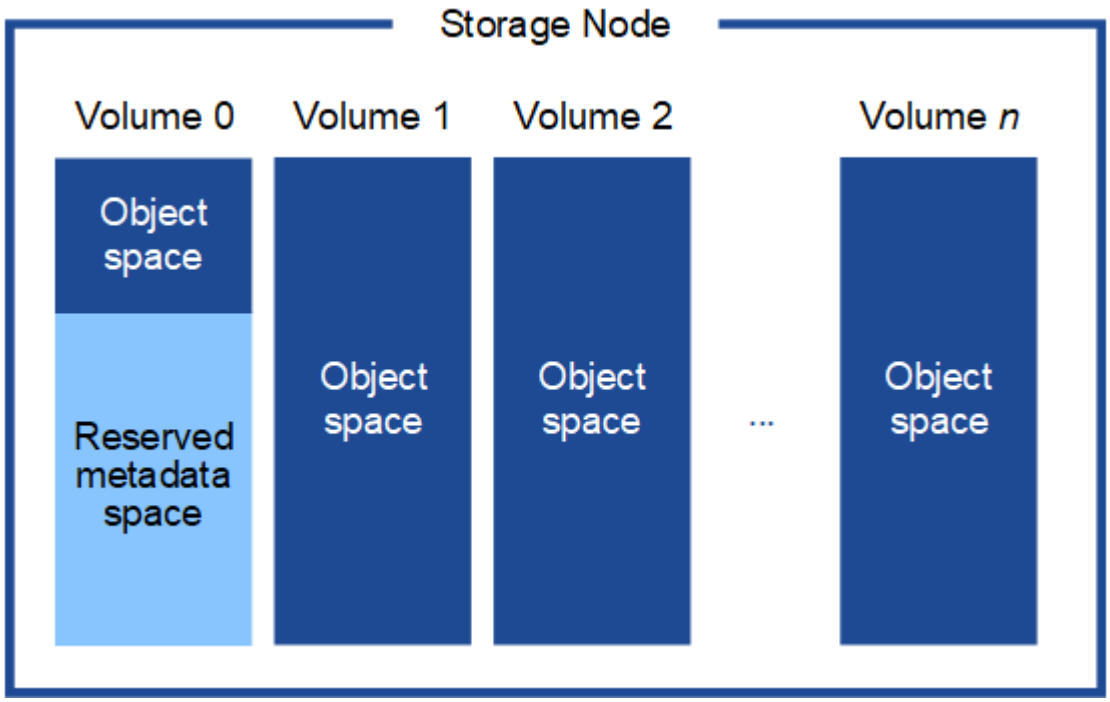
StorageGRID 在 Cassandra 数据库中维护对象元数据，该数据库独立于对象数据进行存储。为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。

此图表示两个站点上的存储节点。每个站点都具有相同数量的对象元数据、每个站点的元数据会细分为该站点的所有存储节点。



对象元数据存储在何处?

此图表示单个存储节点的存储卷。



如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。它会使用预留空间存储对象元数据并执行基本数据库操作。存储卷 0 和存储节点中所有其他存储卷上的任何剩余空间仅用于对象数据（复制的副本和经过纠删编码的片段）。

在特定存储节点上为对象元数据预留的空间量取决于多个因素、如下所述。

元数据预留空间设置

Metadata"预留空间"是一个系统范围的设置、表示每个存储节点的卷0上要为元数据预留的空间量。如表所示、此设置的默认值基于：

- 最初安装 StorageGRID 时使用的软件版本。
- 每个存储节点上的 RAM 量。

用于初始 **StorageGRID** 安装的版本	存储节点上的 **RAM** 量	默认元数据预留空间设置
12.1	网格中的每个存储节点上的容量为 128 GB 或更大	20 TB (20,000 GB)
	网格中任何存储节点上的容量小于 128 GB	3 TB （ 3 ， 000 GB ）
11.5 至 12.0	网格中的每个存储节点上的容量为 128 GB 或更大	8 TB （ 8 ， 000 GB ）
	网格中任何存储节点上的容量小于 128 GB	3 TB （ 3 ， 000 GB ）
11.1 到 11.4	任何一个站点的每个存储节点上的容量为 128 GB 或更大	4 TB （ 4 ， 000 GB ）
	每个站点的任何存储节点上的容量小于 128 GB	3 TB （ 3 ， 000 GB ）
11.0或更早版本	任意数量	2 TB （ 2 ， 000 GB ）

查看元数据预留空间设置

按照以下步骤查看StorageGRID系统的元数据预留空间设置。

步骤

1. 选择*配置* > 系统 > 存储设置。
2. 在存储设置页面上，展开*元数据预留空间*部分。

对于StorageGRID 11.8.或更高版本、元数据预留空间值必须至少为100 GB且不超过1 PB。

新 StorageGRID 12.1 或更高版本安装的默认设置（其中每个存储节点具有 128 GB 或更多 RAM）为 20,000 GB（20 TB）。

元数据的实际预留空间

与系统范围的元数据预留空间设置不同、为每个存储节点确定对象元数据的_쪵 뵆 预留空间_。对于任何给定存储节点、为元数据预留的实际空间取决于该节点的卷0大小以及系统范围的元数据预留空间设置。

节点的卷 **0** 大小	元数据的实际预留空间
小于500 GB (非生产环境使用)	卷 0 的 10%

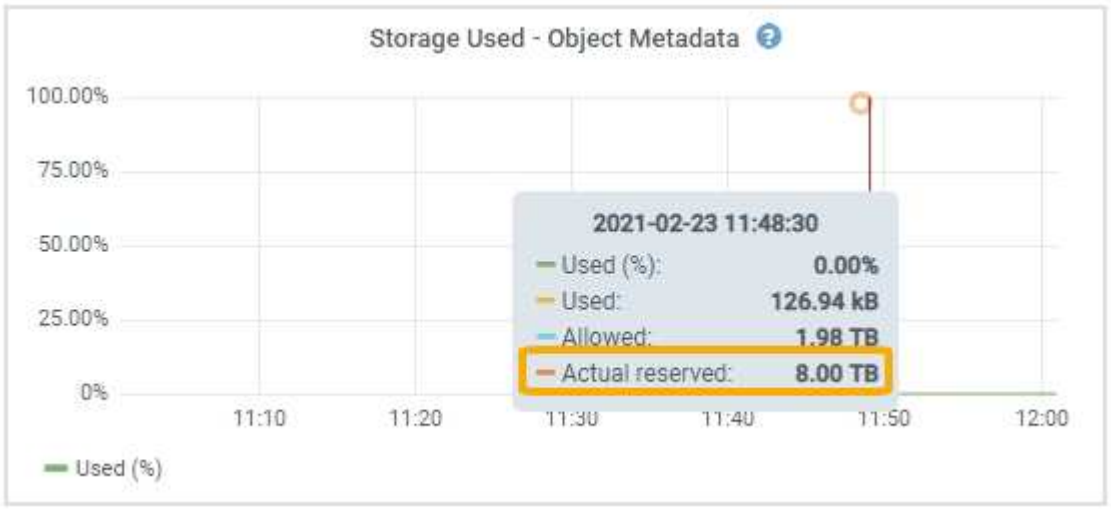
节点的卷 **0** 大小	元数据的实际预留空间
500 GB或更多+或+仅元数据存储节点	这些值中较小的值： • 卷0 • 元数据预留空间设置 注意：对于纯元数据存储节点、只需要一个rangedb。

查看元数据的实际预留空间

按照以下步骤查看特定存储节点上为元数据预留的实际空间。

步骤

1. 从网格管理器中，选择*节点* > 存储节点。
2. 选择 * 存储 * 选项卡。
3. 将光标置于"已用存储-对象元数据"图表上、然后找到*实际预留*值。



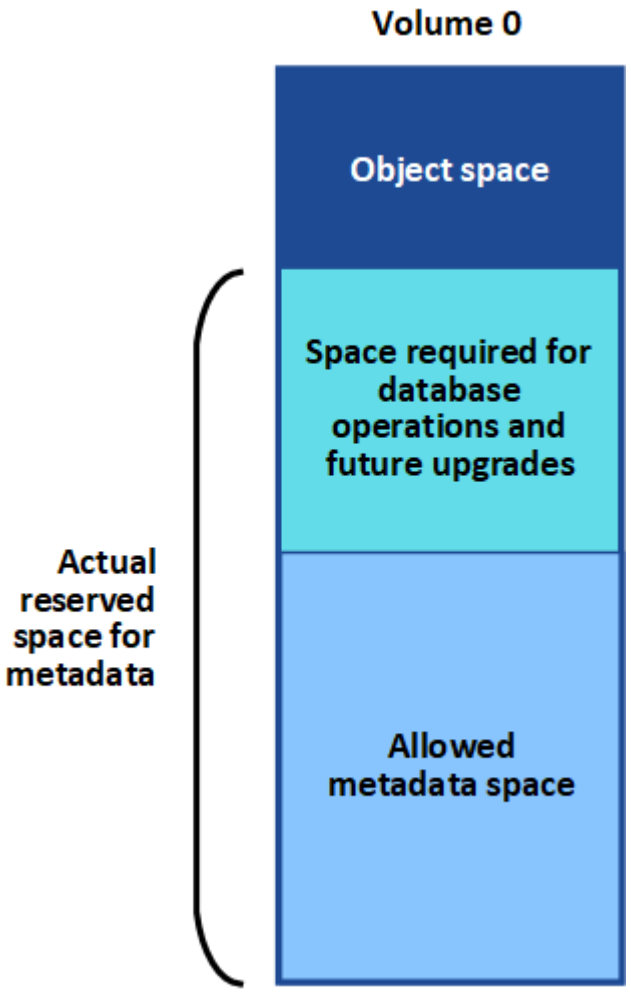
在屏幕截图中，实际保留值为 20 TB。此屏幕截图适用于新 StorageGRID 12.1 安装中的大型存储节点。卷 0 至少为 20 TB，因此它使用默认的系统范围元数据保留空间设置。

实际保留元数据空间示例

假设您使用 12.1 版或更高版本安装新的 StorageGRID 系统。在此示例中，假设每个存储节点的 RAM 超过 128 GB，并且存储节点 1 (SN1) 的卷 0 为 6 TB。基于这些值：

- 全系统*元数据保留空间*设置为 20 TB。（如果每个存储节点的 RAM 超过 128 GB，这是新 StorageGRID 12.1 或更高版本安装的默认值。）
- SN1 元数据的*实际保留*空间为 6 TB。（整个卷被保留，因为卷 0 小于*元数据保留空间*设置。）

每个存储节点为元数据实际预留的空间细分为可用于对象元数据的空间（允许的元数据空间 _ ）以及基本数据库操作（如数据缩减和修复）以及未来硬件和软件升级所需的空间。允许的元数据空间用于控制整体对象容量。



下表显示了StorageGRID 如何根据不同存储节点的内存量和元数据的实际预留空间计算不同存储节点的*允许元数据空间*。

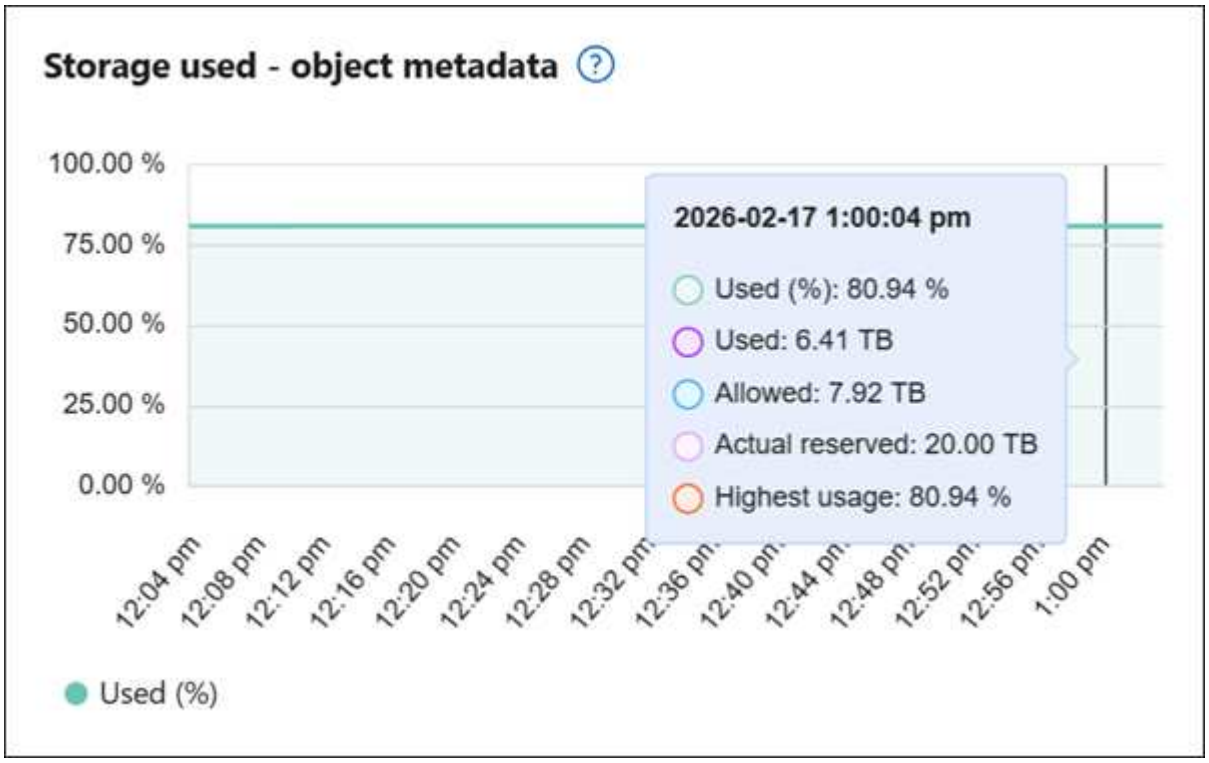
		存储节点上的内存量	
	&lt； 128 GB	&gt； = 128 GB	元数据的实际预留空间
&lt； = 4 TB	元数据实际预留空间的 75%，最高可达 1.32 TB	元数据实际保留空间的 75%，最多 1.98 TB	管理； 4 TB

查看允许的元数据空间

按照以下步骤查看存储节点允许的元数据空间。

步骤

1. 从网格管理器中选择*节点*。
2. 选择存储节点。
3. 选择 * 存储 * 选项卡。
4. 将光标置于已用存储-对象元数据图表上、然后找到*允许*值。



在屏幕截图中，*允许*值为 7.92 TB，这是元数据实际保留空间超过 4 TB 的 Storage Node 的最大值。

- 允许 * 值对应于此 Prometheus 指标：

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

允许的元数据空间示例

假设您使用 12.1 版或更高版本安装新的 StorageGRID 系统。在此示例中，假设每个存储节点的 RAM 超过 128 GB，并且存储节点 1 (SN1) 的卷 0 为 6 TB。基于这些值：

- 全系统*元数据保留空间*设置为 20 TB。（如果每个存储节点的 RAM 超过 128 GB，这是新 StorageGRID 12.1 或更高版本安装的默认值。）
- SN1 元数据的*实际保留*空间为 6 TB。（整个卷被保留，因为卷 0 小于*元数据保留空间*设置。）
- SN1 上元数据的*允许*空间为 3.75 TB，基于元数据允许的空间表中所示的计算：（元数据的实际保留空间 − 1 TB）× 75%，最多 7.92 TB。

不同大小的存储节点如何影响对象容量

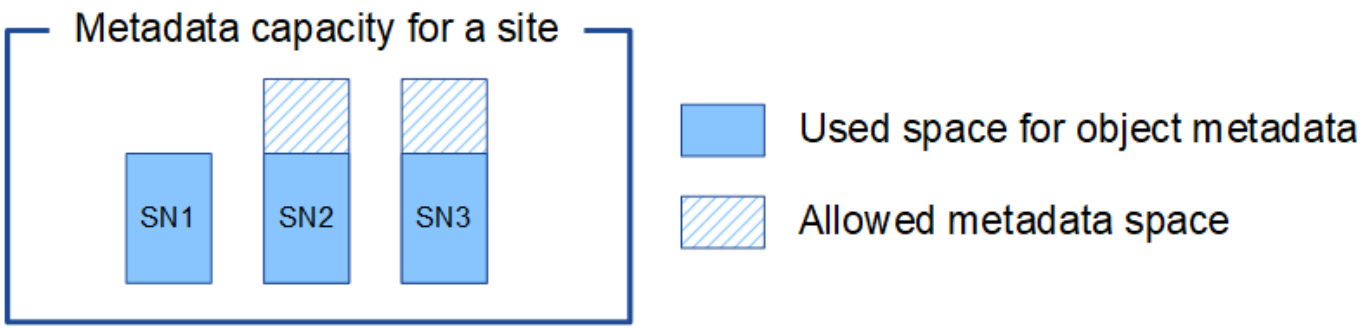
如上所述， StorageGRID 会在每个站点的存储节点之间均匀分布对象元数据。因此，如果某个站点包含不同大小的存储节点，则该站点上最小的节点将决定该站点的元数据容量。

请考虑以下示例：

- 您有一个单站点网格，其中包含三个大小不同的存储节点。
- *元数据预留空间*设置为4 TB。
- 对于实际预留的元数据空间和允许的元数据空间，存储节点具有以下值。

存储节点	卷 **0** 的大小	实际预留的元数据空间	允许的元数据空间
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

由于对象元数据在站点的存储节点之间平均分布，因此本示例中的每个节点只能持有 1.32 TB 的元数据。无法使用SN2和SN3允许的额外0.66 TB元数据空间。



同样，由于 StorageGRID 会维护每个站点上 StorageGRID 系统的所有对象元数据，因此 StorageGRID 系统的整体元数据容量取决于最小站点的对象元数据容量。

由于对象元数据容量控制最大对象数，因此当一个节点用尽元数据容量时，网格实际上已满。

相关信息

- 要了解如何监控每个存储节点的对象元数据容量，请参见的说明"监控StorageGRID"。
- 通过添加新存储节点来增加系统的对象元数据容量"扩展网格"。

增加 **StorageGRID** 中的 **Metadata Reserved Space** 设置

如果存储节点满足特定的RAM和可用空间要求、则可以增加"元数据预留空间"系统设置。

您需要的内容

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 你有"Root 访问权限或其他网格配置权限"。

关于此任务

您可以手动将系统范围的元数据预留空间设置增加到8 TB。

只有当以下两项陈述均为 true 时，才能增加系统范围的元数据预留空间设置的值：

- 系统中任何站点的存储节点均具有 128 GB 或更多 RAM 。
- 系统中任何站点的存储节点在存储卷 0 上都有足够的可用空间。

请注意，如果增加此设置，则会同时减少所有存储节点的存储卷 0 上可用于对象存储的空间。因此，您可能希望根据预期对象元数据要求将元数据预留空间设置为小于 8 TB 的值。

> 一般来说，最好使用较高的值，而不是较低的值。如果 " 元数据预留空间 " 设置过大，您可以稍后减小此设置。相比之下，如果稍后增加该值，系统可能需要移动对象数据以释放空间。

有关“元数据预留空间”设置如何影响特定存储节点上对象元数据存储的允许空间的详细说明，请参见"管理对象元数据存储"。

步骤

1. 确定当前的元数据预留空间设置。
   a. 选择*配置* > 系统 > 存储设置。
   b. 注意*元数据保留空间*的值。
2. 确保每个存储节点的存储卷 0 上有足够的可用空间来增加此值。
   a. 选择*节点*。
   b. 选择网格中的第一个存储节点。
   c. 选择存储选项卡。
   d. 在卷部分中，找到 * /var/local/rangedb/0* 条目。
   e. 确认可用值等于或大于要使用的新值与当前元数据预留空间值之间的差值。

      例如，如果元数据预留空间设置当前为 4 TB ，而您希望将其增加到 6 TB ，则可用值必须为 2 TB 或更大。

   f. 对所有存储节点重复上述步骤。
      - 如果一个或多个存储节点没有足够的可用空间，则无法增加元数据预留空间值。请勿继续使用此操作步骤。
      - 如果每个存储节点在卷 0 上都有足够的可用空间，请转至下一步。
3. 确保每个存储节点上至少有 128 GB 的 RAM 。
   a. 选择*节点*。
   b. 选择网格中的第一个存储节点。
   c. 选择 * 硬件 * 选项卡。
   d. 将光标悬停在 " 内存使用量 " 图表上。确保 * 总内存 * 至少为 128 GB 。
   e. 对所有存储节点重复上述步骤。
      - 如果一个或多个存储节点没有足够的可用总内存，则无法增加元数据预留空间值。请勿继续使用此操作步骤。
      - 如果每个存储节点的总内存至少为 128 GB ，请转至下一步。

4. 更新元数据预留空间设置。
   a. 选择*配置* > 系统 > 存储设置。
   b. 选择*元数据保留空间*。
   c. 输入新值。

      例如，要输入 8 TB 作为支持的最大值，请输入 * 80000000000000000* （ 8 ，后跟 12 个零）

   d. 选择 * 保存 * 。

压缩 **StorageGRID** 中存储的对象

您可以启用对象压缩以减小StorageGRID 中存储的对象大小、从而减少对象占用的存储空间。

开始之前

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

关于此任务

默认情况下、对象压缩处于禁用状态。如果启用数据压缩、则StorageGRID 会在保存每个对象时尝试使用无结果压缩。

> 如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

启用对象压缩之前、请注意以下事项：

- 除非您知道所存储的数据是可压缩的，否则不应选择*压缩存储的对象*。
- 将对象保存到 StorageGRID 的应用程序可能会在保存对象之前对其进行压缩。如果客户端应用程序在将对象保存到StorageGRID 之前已经对其进行了压缩、则选择此选项不会进一步减小对象的大小。
- 如果将NetApp FabricPool 与StorageGRID 结合使用、请勿选择*压缩存储的对象*。
- 如果选择*压缩存储的对象*，S3客户端应用程序应避免执行指定返回字节数范围的GetObject操作。这些"范围读取"操作效率低下、因为StorageGRID必须有效地解压缩对象才能访问请求的字节。从非常大的对象请求少量字节的GetObject操作效率特别低；例如、从50 GB压缩对象读取10 MB的范围是效率低下的。

  如果从压缩对象读取范围，则客户端请求可能会超时。

  > 如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

步骤

1. 选择*配置* > 系统 > 存储设置 > 对象压缩。
2. 选中*压缩存储的对象*复选框。
3. 选择 * 保存 * 。

在 **StorageGRID** 中管理完整存储节点

当存储节点达到容量时，您必须通过添加新存储来扩展 StorageGRID 系统。有三种选项可供选择：添加存储卷，添加存储扩展架和添加存储节点。

添加存储卷

每个存储节点均支持最大数量的存储卷。定义的最大值因平台而异。如果存储节点包含的存储卷数少于最大数量，则可以添加卷以增加其容量。请参阅的说明"扩展 StorageGRID 系统"。

添加存储扩展架

某些StorageGRID设备存储节点(例如SG6060或SG6160)可以支持更多存储架。如果您的 StorageGRID 设备具有扩展功能，但尚未扩展到最大容量，则可以添加存储架以增加容量。请参阅的说明"扩展 StorageGRID 系统"。

添加存储节点

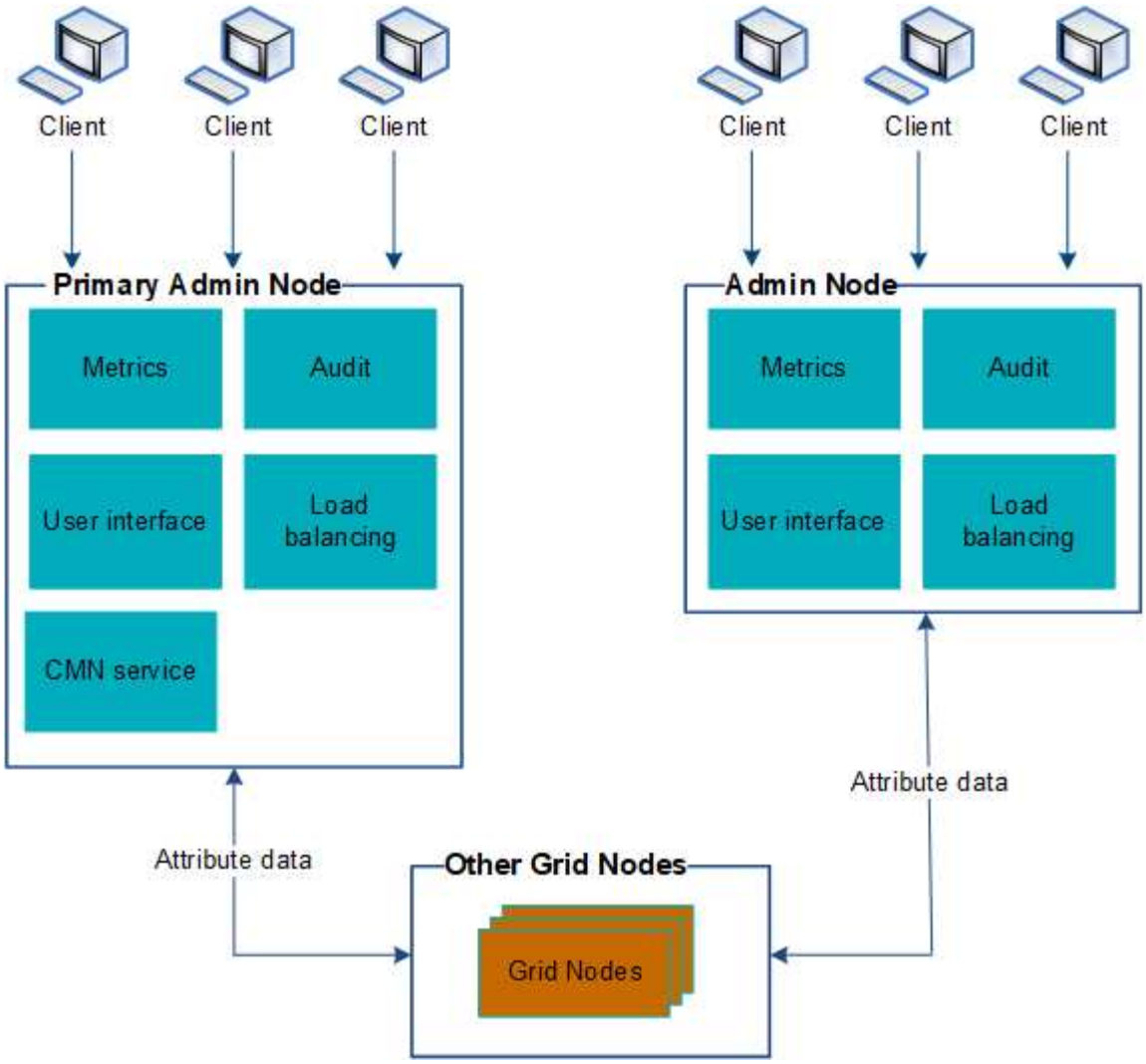
您可以通过添加存储节点来增加存储容量。添加存储时，必须仔细考虑当前活动的 ILM 规则和容量要求。请参阅的说明"扩展 StorageGRID 系统"。

管理管理节点

在 **StorageGRID** 中使用多个管理节点

一个 StorageGRID 系统可以包含多个管理节点，这样，即使一个管理节点出现故障，您也可以持续监控和配置 StorageGRID 系统。

如果某个管理节点不可用、则属性处理将继续、系统仍会触发警报、并且仍会发送电子邮件通知和AutoSupport软件包。但是、拥有多个管理节点不会提供故障转移保护、但通知和AutoSupport软件包除外。



如果管理节点出现故障，可以通过两种方法继续查看和配置 StorageGRID 系统：

- Web 客户端可以重新连接到任何其他可用的管理节点。
- 如果系统管理员配置了高可用性管理节点组，则 Web 客户端可以继续使用 HA 组的虚拟 IP 地址访问网格管理器或租户管理器。请参阅。 "管理高可用性组"

> 使用HA组时、如果活动管理节点发生故障、则访问将中断。用户必须在 HA 组的虚拟 IP 地址故障转移到组中的另一个管理节点后重新登录。

某些维护任务只能使用主管理节点执行。如果主管理节点出现故障，则必须先对其进行恢复，然后 StorageGRID 系统才能重新完全正常运行。

识别 **StorageGRID** 中的主管理节点

主管理节点提供的功能比非主管理节点更多。例如、某些维护过程必须使用主管理节点来执行。

有关管理节点的详细信息，请参见"什么是管理节点"。

开始之前

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

步骤

1. 选择*节点*。
2. 在搜索框中输入*primary*。

   在搜索结果中、确定Type列中显示"Primary Admin Ne"的节点。应列出一个主管理节点。

使用 ILM 管理对象

使用 ILM 在 StorageGRID 中管理对象

ILM策略中的信息生命周期管理(ILM)规则指示StorageGRID如何创建和分发对象数据副本以及如何长期管理这些副本。

关于这些说明

设计和实施ILM规则和策略需要仔细规划。您必须了解操作要求， StorageGRID 系统的拓扑结构，对象保护需求以及可用存储类型。然后，您必须确定希望如何复制，分发和存储不同类型的对象。

按照以下说明执行以下操作：

- 了解StorageGRID ILM，包括"ILM如何在对象的整个生命周期内运行"。
- 了解如何配置"存储池"、"云存储池"和"ILM 规则"。
- 了解如何"创建、模拟和激活ILM策略"保护一个或多个站点上的对象数据。
- 了解如何"使用S3对象锁定管理对象"，这有助于确保特定S3存储分段中的对象在指定的时间内不会被删除或覆盖。

了解更多信息。

要了解更多信息，请查看以下视频：

ILM 规则概述

ILM 策略概述

ILM 和对象生命周期

ILM 如何在 StorageGRID 中对象的整个生命周期内运行

了解 StorageGRID 如何在对象生命周期的每个阶段使用 ILM 管理对象，有助于您设计更有效的策略。

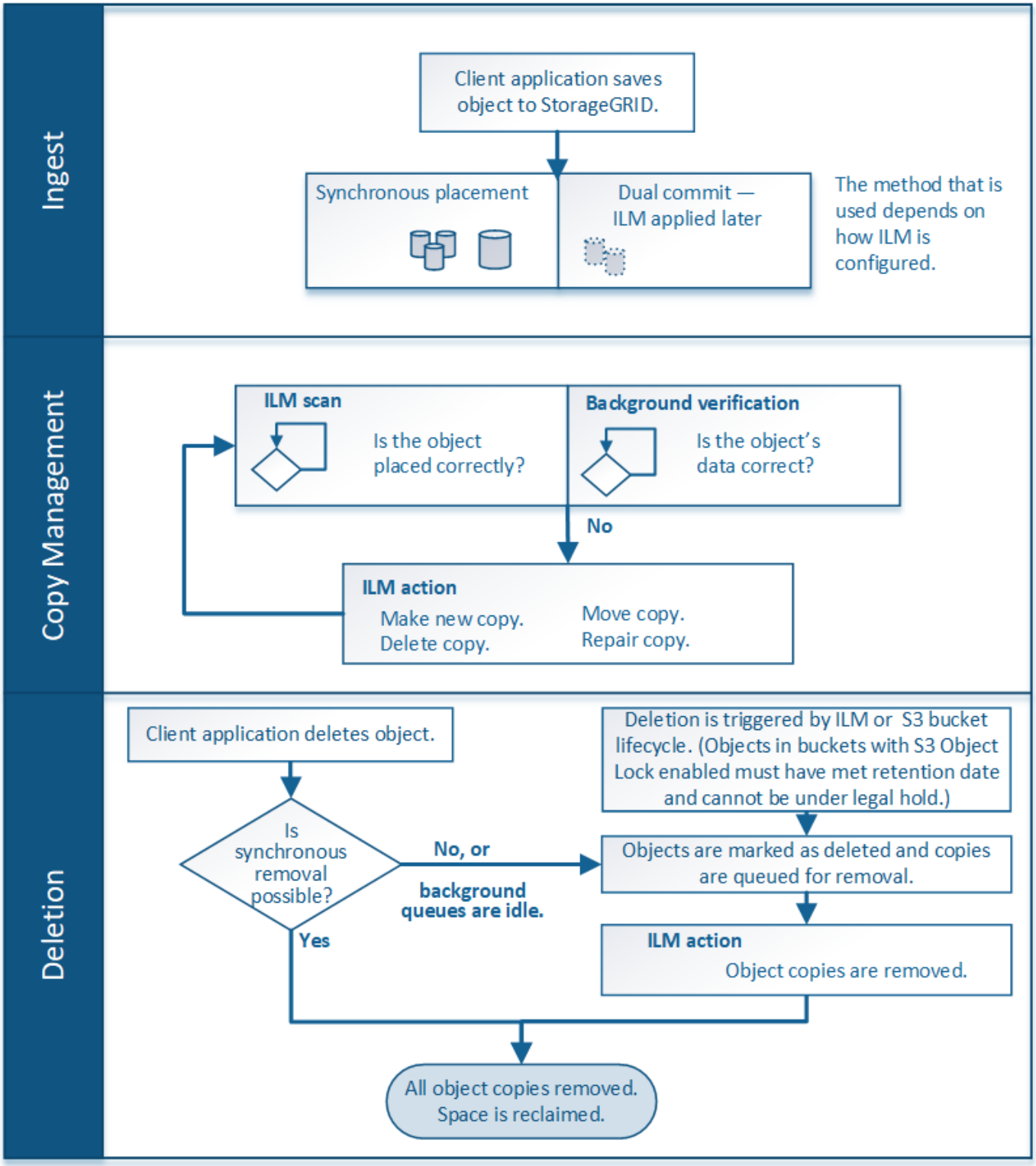
- **Ingest**：当S3客户端应用程序建立连接以将对象保存到StorageGRID系统时、将开始执行加注；当StorageGRID向客户端返回"ining suced"消息时、加注操作完成。根据 ILM 要求的指定方式，在载入期间

通过立即应用 ILM 指令（同步放置）或创建临时副本并稍后应用 ILM （双提交）来保护对象数据。

- * 副本管理 * ： 创建 ILM 放置说明中指定的对象副本数量和类型后， StorageGRID 可管理对象位置并防止对象丢失。
  - **ILM**扫描和评估：StorageGRID会持续扫描存储在网格中的对象列表，并检查当前副本是否符合ILM要求。如果需要不同类型，数字或位置的对象副本， StorageGRID 会根据需要创建，删除或移动副本。
  - 后台验证：StorageGRID持续执行后台验证以检查对象数据的完整性。如果发现问题， StorageGRID 会自动在满足当前 ILM 要求的位置创建一个新的对象副本或替换的擦除编码对象片段。请参阅。 "验证对象完整性"
- * 对象删除 * ： 从 StorageGRID 系统中删除所有副本后，对象管理将结束。可以根据客户端的删除请求删除对象，也可以通过 ILM 删除对象或因 S3 存储分段生命周期到期而删除对象。

> 如果存储分段中已启用S3对象锁定的对象处于合法保留状态、或者已指定保留截止日期但尚未满足、则无法删除这些对象。

该图总结了 ILM 在对象的整个生命周期中的运行方式。



如何载入对象

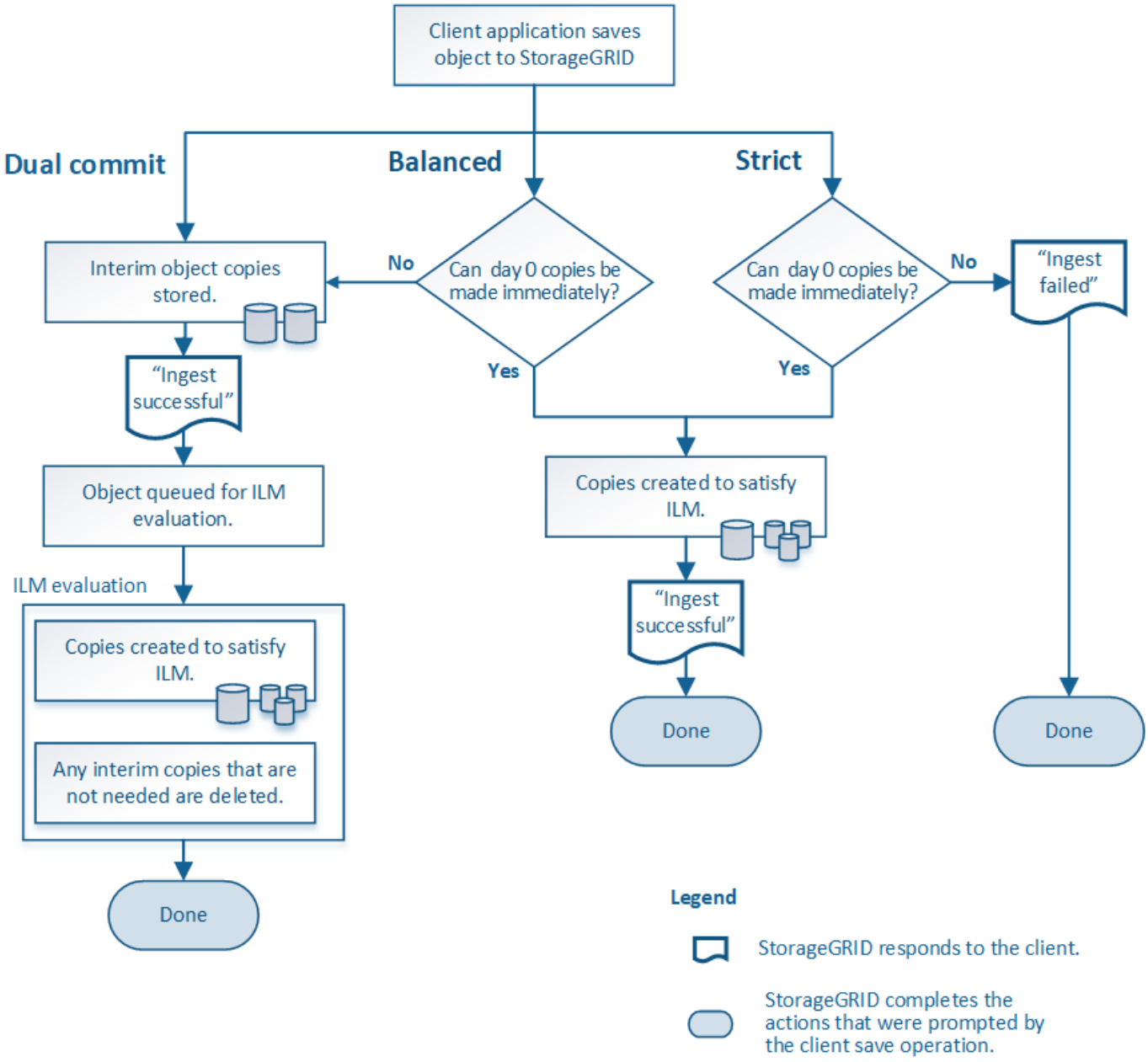
StorageGRID 中的 **ILM** 摄取选项

在创建ILM规则时、您可以指定以下三个选项之一来保护对象：双重提交、严格或平衡。

根据您的选择， StorageGRID 会创建临时副本并将对象排队，以便稍后进行 ILM 评估，或者使用同步放置并立即创建副本以满足 ILM 要求。

加热选项流程图

此流程图显示了在对象与 ILM 规则匹配时会发生的情况，该规则使用三个载入选项中的每一个选项。



双提交

选择双重提交选项后、StorageGRID会立即在两个不同的存储节点上创建临时对象副本、并向客户端返回"INGEST S晒"消息。对象将排队等待 ILM 评估，满足规则放置说明的副本将在稍后创建。如果无法在双重提交后立即处理ILM策略、则可能需要一些时间才能实现站点丢失保护。

在以下任一情况下，请使用双提交选项：

- 您正在使用多站点 ILM 规则，客户端载入延迟是您的主要考虑因素。使用双提交时、您必须确保网格能够执行额外的工作、即创建和删除不满足ILM要求的双提交副本。具体而言：
  - 网格上的负载必须足够低，以防止 ILM 积压。

- 网格必须具有多余的硬件资源（ IOPS ， CPU ，内存，网络带宽等）。

- 您正在使用多站点 ILM 规则，并且站点之间的 WAN 连接通常具有较高的延迟或有限的带宽。在这种情况下，使用双提交选项有助于防止客户端超时。在选择双提交选项之前，您应使用实际工作负载测试客户端应用程序。

已平衡(默认)

选择 Balified 选项时， StorageGRID 还会在载入时使用同步放置，并立即创建规则放置说明中指定的所有副本。与严格选项不同、如果StorageGRID 无法立即创建所有副本、则会改用双提交。如果ILM策略使用放置在多个站点上、但无法实现即时站点丢失保护、则会触发*无法实现ILM放置*警报。

使用平衡选项可实现数据保护，网格性能和载入成功的最佳组合。已平衡是创建ILM规则向导中的默认选项。

严格

如果选择 strict 选项，则 StorageGRID 会在载入时使用同步放置，并立即创建规则放置说明中指定的所有对象副本。如果StorageGRID 无法创建所有副本、例如、由于所需的存储位置暂时不可用、则加热操作将失败。客户端必须重试此操作。

如果您在操作或法规要求中要求仅将对象立即存储在 ILM 规则中所述的位置，请使用 strict 选项。例如、为了满足法规要求、您可能需要使用stricted选项和Location约束高级筛选器来保证对象永远不会存储在某些数据中心。

请参阅。 "示例 5 ： 用于严格载入行为的 ILM 规则和策略"

StorageGRID 中 **ILM** 摄取选项的优势、劣势和限制

了解在载入时保护数据的三个选项（平衡，严格或双重提交）中每一个选项的优缺点有助于您确定要为 ILM 规则选择哪个选项。

有关安装选项的概述，请参见"加热选项"。

平衡而严格的选项的优势

与在载入期间创建临时副本的双提交相比，这两个同步放置选项具有以下优势：

- * 更好的数据安全性 * ： 对象数据会按照 ILM 规则放置说明中的说明立即受到保护，可以对其进行配置，以防止出现多种故障情况，包括多个存储位置发生故障。双提交只能防止丢失一个本地副本。
- * 更高效的网格操作 * ： 每个对象仅在载入时进行一次处理。由于 StorageGRID 系统不需要跟踪或删除中间副本，因此处理负载较低，数据库空间占用较少。
- * （平衡）建议 * ： 平衡选项可提供最佳 ILM 效率。除非需要严格的加载行为或网格满足使用双重提交的所有标准、否则建议使用均衡选项。
- * （严格）对象位置的确定性 * ： strict 选项可确保根据 ILM 规则中的放置说明立即存储对象。

平衡而严格的选项的缺点

与双提交相比，平衡和严格选项存在一些缺点：

- * 客户端载入时间更长 * ： 客户端载入延迟可能更长。使用均衡或严格选项时、只有在创建和存储所有经过删除的片段或复制的副本之后、才会向客户端返回"成功地执行"消息。但是，对象数据很可能会更快地到达最终放置位置。

- **(**严格**)**更高的加载失败率：使用严格选项、只要StorageGRID 无法立即创建ILM规则中指定的所有副本、加载就会失败。如果所需存储位置暂时脱机或网络问题发生原因 在站点之间复制对象时出现延迟，则可能会出现较高的载入失败率。
- 在某些情况下 *（严格） S3 多部分上传放置可能与预期不同 *：严格地说，您希望对象按照 ILM 规则的说明放置，或者载入操作失败。但是、对于S3多部分上传、载入对象时会针对对象的每个部分评估ILM、多部分上传完成后、会针对整个对象评估ILM。在以下情况下，这可能会导致放置方式与您预期不同：
  - * 如果在 S3 多部件上传过程中 ILM 发生变化 *：由于每个部件都是根据在载入部件时处于活动状态的规则放置的，因此在多部件上传完成后，对象的某些部分可能不符合当前的 ILM 要求。在这些情况下，对象的载入不会失败。相反、未正确放置的任何部件将排队等待ILM重新评估、并在稍后移动到正确的位置。
  - * 当 ILM 规则按大小筛选时 *：在评估某个部件的 ILM 时， StorageGRID 会按部件的大小进行筛选，而不是按对象的大小进行筛选。这意味着、对象的某些部分可以存储在不满足对象整体ILM要求的位置。例如，如果规则指定所有 10 GB 或更大的对象都存储在 DC1 中，而所有较小的对象存储在 DC2 中，则在载入时， 10 部分多部分上传的每个 1 GB 部分都存储在 DC2 中。评估对象的 ILM 时，对象的所有部分都会移至 DC1 。
- *（严格）更新对象标记或元数据后，如果无法进行新要求的放置，则载入不会失败 *：严格地说，您希望按照 ILM 规则的说明放置对象，或者使载入失败。但是，在更新网格中已存储的对象的元数据或标记时，不会重新载入该对象。这意味着、更新触发的任何对象放置更改不会立即生效。如果通过正常后台 ILM 流程重新评估 ILM ，则会进行放置更改。如果无法进行所需的放置更改(例如、由于新需要的位置不可用)、更新后的对象将保留其当前放置位置、直到可以进行放置更改为止。

使用平衡和严格选项对对象放置的限制

对于具有以下任何放置说明的ILM规则、不能使用"平衡"或"严格"选项：

- 第 0 天放置在云存储池中。
- 规则将用户定义的创建时间作为其参考时间时放置在云存储池中。

之所以存在这些限制、是因为StorageGRID无法同步向云存储池创建副本、而用户定义的创建时间可以解析为当前时间。

ILM规则和一致性如何相互作用以影响数据保护

ILM规则和一致性选择都会影响对象的保护方式。这些设置可以进行交互。

例如、为ILM规则选择的加载行为会影响对象副本的初始放置、而存储对象时使用的一致性会影响对象元数据的初始放置。由于StorageGRID需要同时访问对象的数据和元数据才能满足客户端请求、因此为一致性和载入行为选择匹配的保护级别可以提供更好的初始数据保护、并提高系统响应的可预测性。

下面简要总结了StorageGRID中提供的一致性值：

- **all**：所有节点都会立即接收对象元数据、否则请求将失败。
- 强全局：保证所有站点上所有客户端请求的读写一致性。配置 Quorum 语义时，将应用以下行为：
  - 当网格具有三个或更多站点时，允许对客户端请求进行站点故障容忍。双站点电网不具备站点故障容忍能力。
  - 如果一个站点发生故障，以下 S3 操作将无法成功：
    - DeleteBucketEncryption

- PutBucketBranch
- PutBucketEncryption
- PutBucketVersioning
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObject保留

如果需要，您可以 "配置StorageGRID Quorum 语义以实现强全局一致性"。

- **strong-sit**：对象元数据会立即分发到站点上的其他节点。保证站点内所有客户端请求的写入后读一致性。
- **read-after-new-write**：为新对象提供写入后读取一致性，并最终为对象更新提供一致性。提供高可用性和数据保护保证。建议用于大多数情况。
- 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。

> 在选择一致性值之前，"阅读完整的一致性问题描述" 。在更改默认值之前，您应该了解其优点和局限性。

示例：如何交互一致性和**ILM**规则

假设您有一个三站点网格，具有以下 ILM 规则和以下一致性：

- **ILM** 规则：创建三个对象副本，一个在本地站点，另一个在每个远程站点。使用严格的摄取行为。
- 一致性：强全局（对象元数据立即分发到多个站点）。

当客户端将对象存储到网格时， StorageGRID会复制所有三个对象并将元数据分发到多个站点，然后再将成功返回给客户端。

在接收成功消息时，对象将受到完全保护，不会丢失。例如，如果本地站点在摄取后不久丢失，对象数据和对象元数据的副本仍然存在于远程站点。该对象可以从其他站点完全检索。

如果您使用相同的 ILM 规则和强站点一致性，则客户端可能会在对象数据复制到远程站点之后但在对象元数据分发到那里之前收到成功消息。在这种情况下，对象元数据的保护级别与对象数据的保护级别不匹配。如果本地站点在摄取后不久丢失，对象元数据就会丢失。无法检索该对象。

一致性和ILM规则之间的相互关系可能很复杂。如果需要帮助、请联系NetApp。

相关信息

"示例 5： 用于严格载入行为的 ILM 规则和策略"

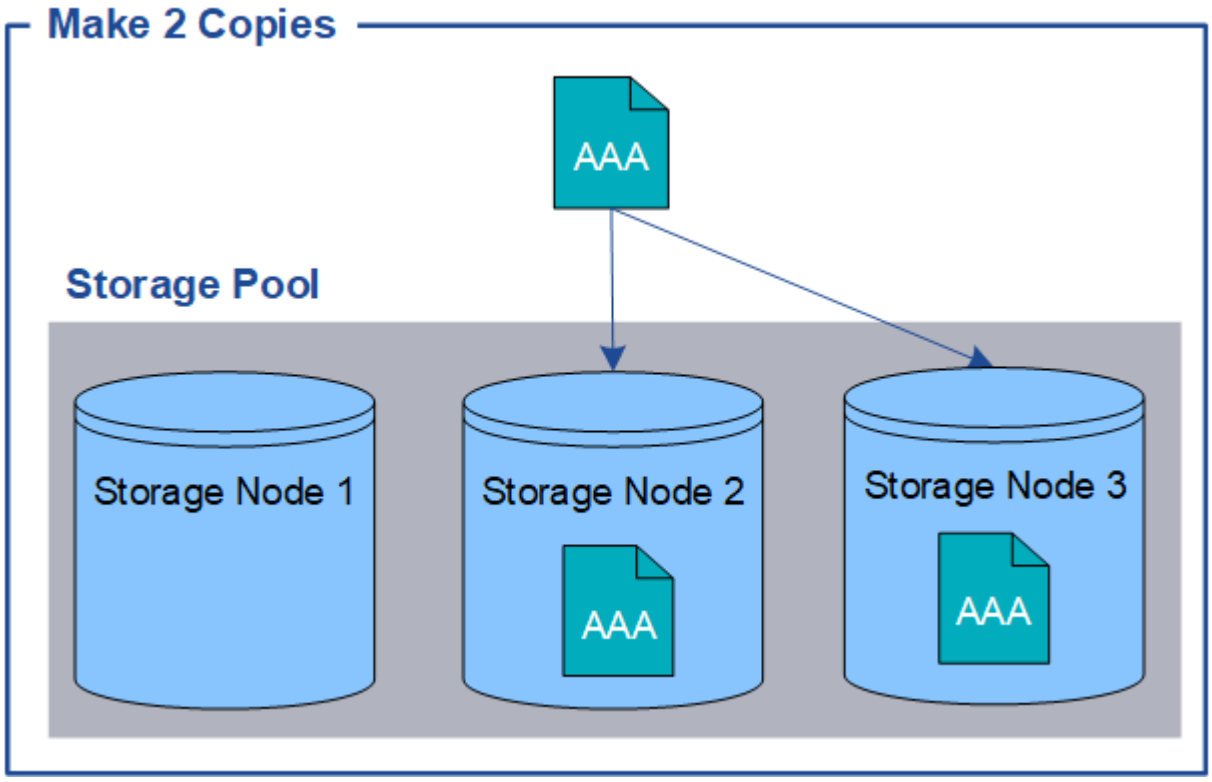
对象的存储方式（复制或纠删编码）

了解 **StorageGRID** 中的复制

复制是StorageGRID用于存储对象数据的两种方法之一(纠删编码是另一种方法)。如果对象与使用复制的ILM规则匹配、则系统会为对象数据创建精确副本、并将这些副本存储在存储节点上。

在配置创建复制副本的 ILM 规则时，您可以指定应创建多少个副本，这些副本应放置在何处以及应将这些副本存储在每个位置的时间长度。

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



当 StorageGRID 将对象与此规则匹配时，它会为该对象创建两个副本，并将每个副本放置在存储池中的不同存储节点上。这两个副本可以放置在三个可用存储节点中的任意两个上。在这种情况下，规则会将对象副本放置在存储节点 2 和 3 上。由于有两个副本，因此，如果存储池中的任何节点出现故障，可以检索此对象。

StorageGRID 只能在任何给定存储节点上存储一个对象的一个复制副本。如果您的网格包含三个存储节点，并且您创建了一个 4 副本 ILM 规则，则只会创建三个副本—每个存储节点一个副本。系统将触发 * 无法实现 ILM 放置 * 警报，以指示无法完全应用 ILM 规则。

相关信息

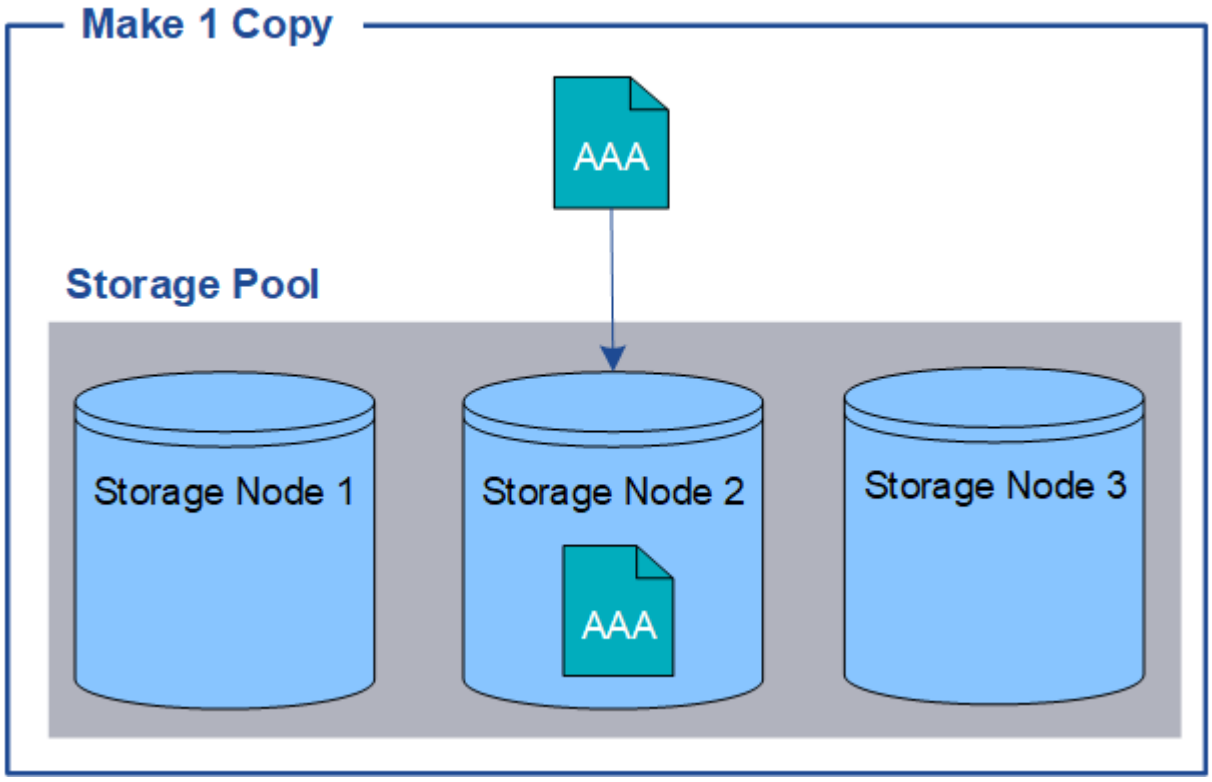
- "什么是纠删编码"
- "什么是存储池"
- "通过复制和纠删编码实现站点丢失保护"

StorageGRID 中单副本复制的风险

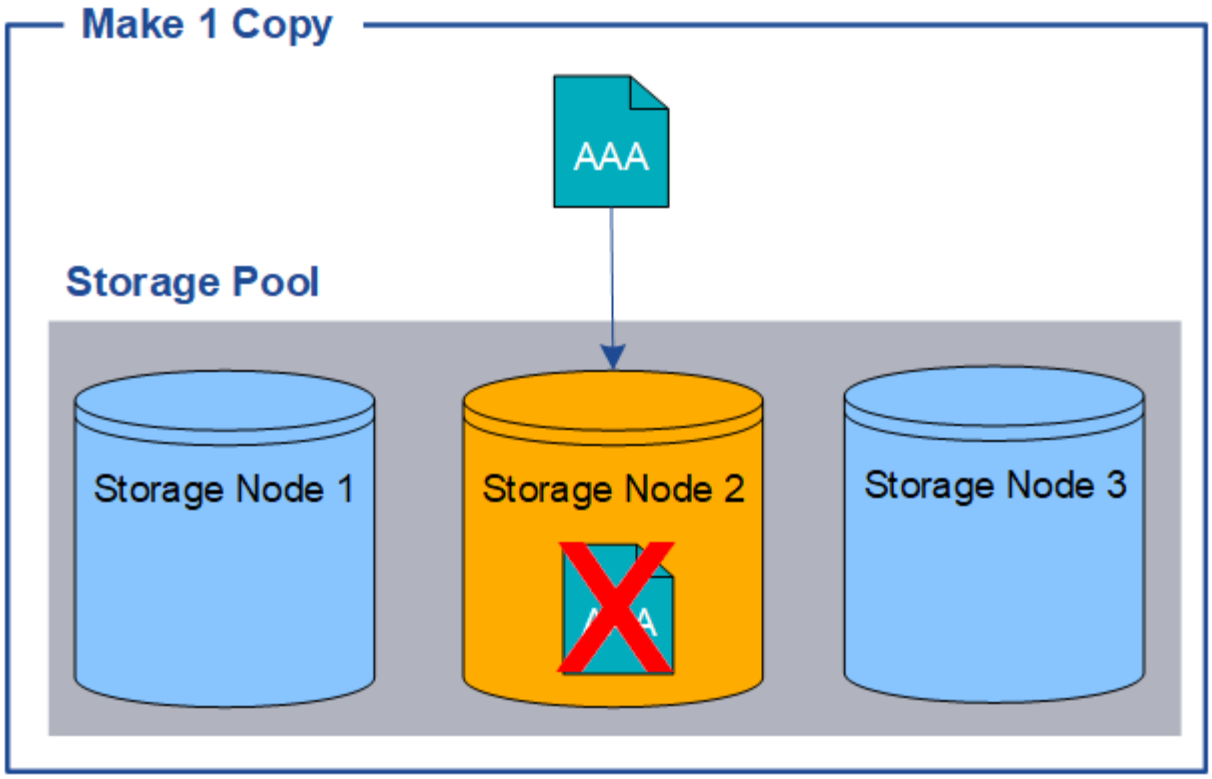
在创建 ILM 规则以创建复制副本时，您应始终在放置说明中指定至少两个副本，以便在任意时间段内使用。

请勿使用在任何时间段内仅创建一个复制副本的ILM规则。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

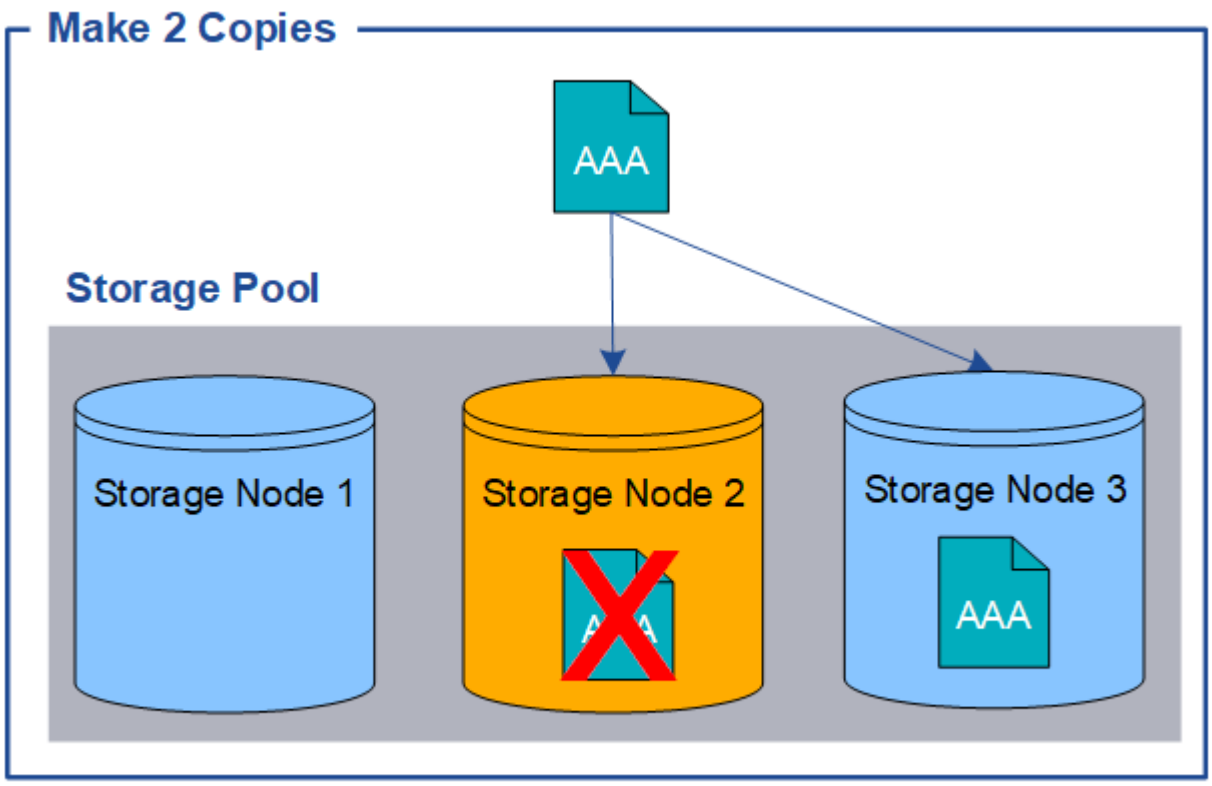
在以下示例中， Make 1 Copy ILM 规则指定将对象的一个复制副本放置在包含三个存储节点的存储池中。如果载入的对象与此规则匹配，则 StorageGRID 仅会在一个存储节点上放置一个副本。



如果 ILM 规则仅创建一个对象的一个复制副本，则在存储节点不可用时，此对象将无法访问。在此示例中，只要存储节点 2 脱机，例如在升级或其他维护操作步骤 期间，您将暂时无法访问对象 AAA 。如果存储节点 2 发生故障，您将完全丢失对象 AAA 。



为了避免丢失对象数据，您应始终为要通过复制保护的所有对象创建至少两个副本。如果存在两个或更多副本，则在一个存储节点出现故障或脱机时，您仍可以访问此对象。

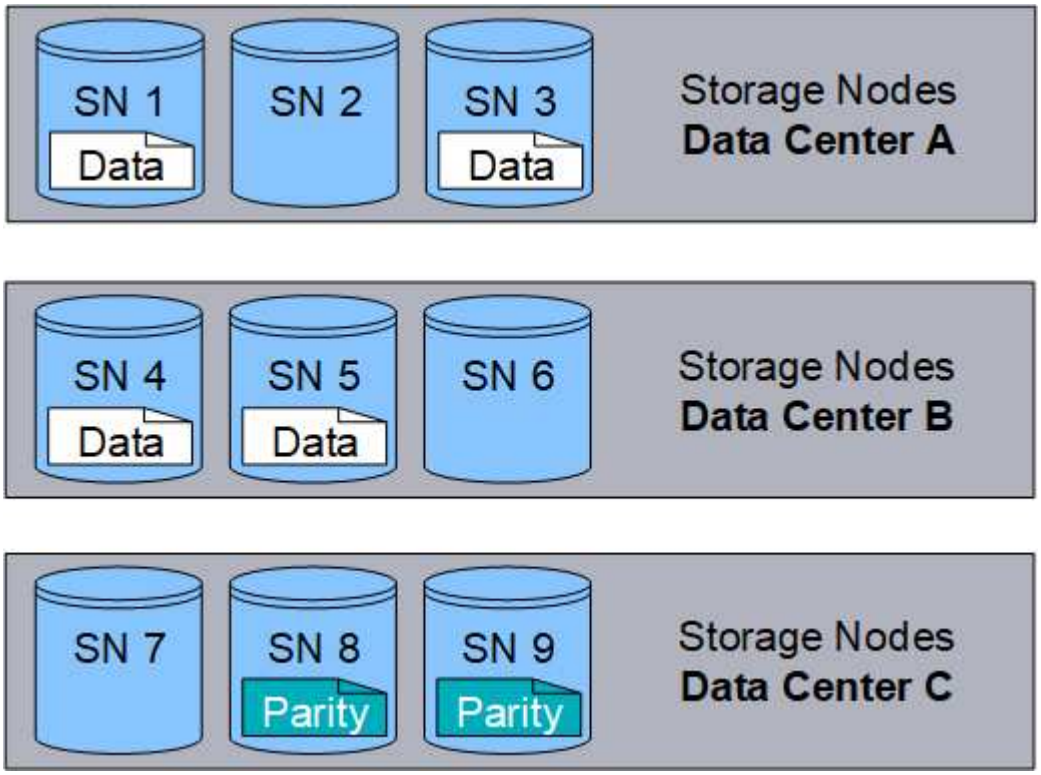


纠删编码是StorageGRID用于存储对象数据的两种方法之一(复制是另一种方法)。如果对象与使用纠删编码的ILM规则匹配、则这些对象会划分为数据片段、并计算额外的奇偶校验片段、每个片段会存储在不同的存储节点上。

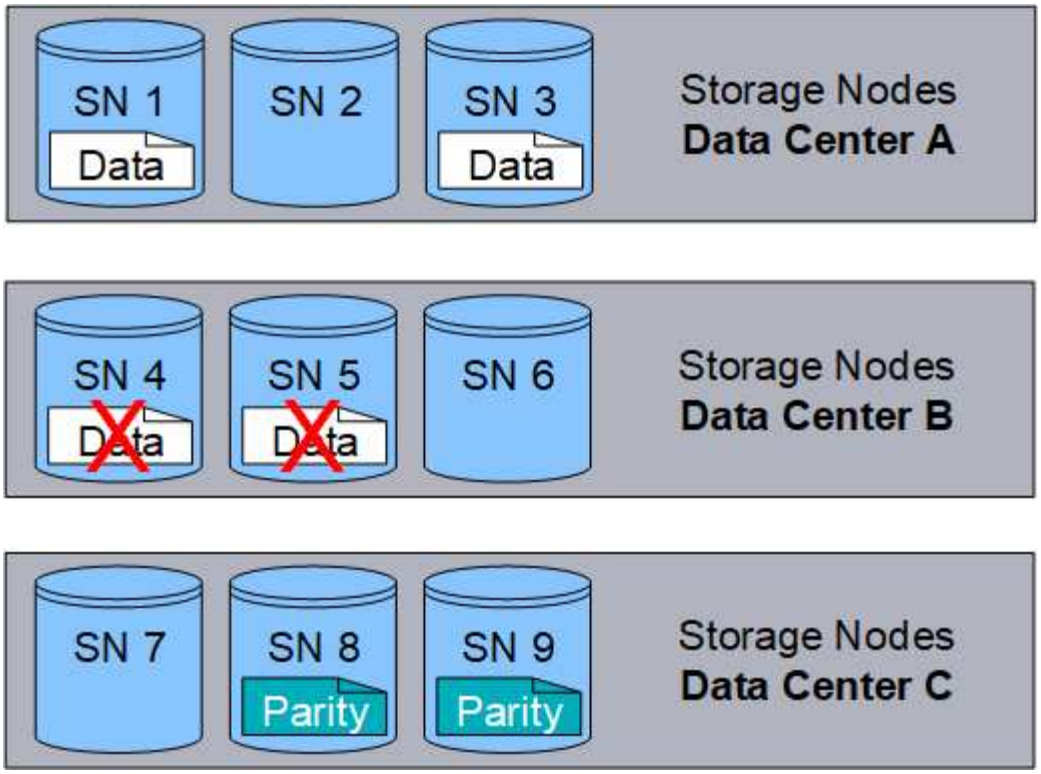
访问某个对象时，系统会使用存储的片段重新组合该对象。如果数据或奇偶校验片段损坏或丢失，则纠删编码算法可以使用剩余数据和奇偶校验片段的子集重新创建该片段。

创建ILM规则时、StorageGRID会创建支持这些规则的纠删编码配置文件。您可以查看纠删编码配置文件、"重命名纠删编码配置文件"或"如果纠删编码配置文件当前未在任何ILM规则中使用、则停用该配置文件"的列表。

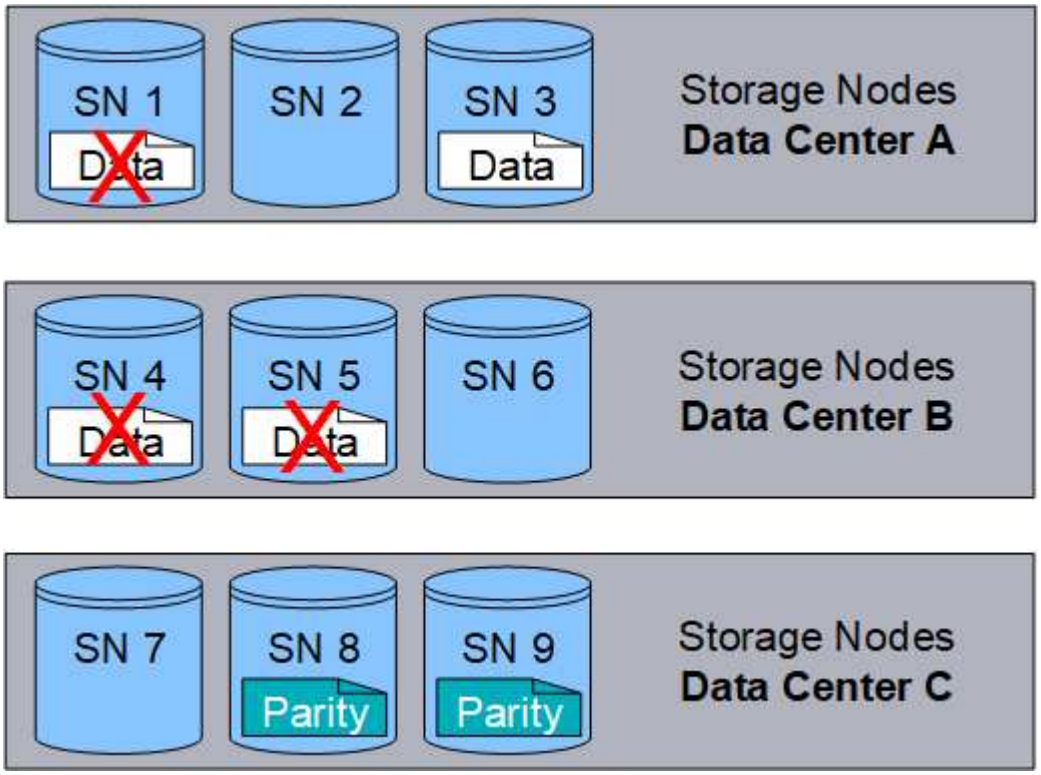
以下示例说明了如何对对象数据使用纠删编码算法。在此示例中， ILM 规则使用 4+2 纠删编码方案。每个对象都会被划分为四个相等的数据片段，并根据对象数据计算两个奇偶校验片段。六个片段中的每个片段都存储在三个数据中心站点的不同节点上，以便为节点故障或站点丢失提供数据保护。



4+2纠删编码方案可以通过多种方式进行配置。例如、您可以配置一个包含六个存储节点的单站点存储池。对于"站点丢失保护"，您可以使用包含三个站点的存储池，每个站点上有三个存储节点。只要六个片段中的任意四个（数据或奇偶校验）仍然可用，就可以检索对象。最多可以丢失两个片段，而不会丢失对象数据。如果整个站点丢失、只要所有其他碎片仍可访问、就可以检索或修复对象。



如果丢失两个以上的存储节点，则无法检索此对象。



相关信息

- "什么是复制"
- "什么是存储池"
- "什么是纠删编码方案"

- "重命名纠删编码配置文件"
- "停用纠删编码配置文件"

了解 **StorageGRID** 中的纠删编码方案

纠删编码方案可控制为每个对象创建的数据片段数量和奇偶校验片段数量。

创建或编辑ILM规则时、您可以选择可用的纠删编码方案。StorageGRID会根据您计划使用的存储池中的存储节点和站点数量自动创建纠删编码方案。

数据保护

StorageGRID 系统使用 Reed-Solomon 纠删编码算法。该算法会将对象分区为 `k`数据片段并计算奇偶校验片段 `m`。

这些 `k + m = n`片段会分布在多个存储节点中 `n`、以提供如下数据保护：

- 要检索或修复对象、 `k`需要使用片段。
- 一个对象可以承受多达 `m`丢失或损坏的碎片。的值越高 `m`，故障容错越高。

通过纠删编码方案提供最佳数据保护、该方案在存储池中具有最高的节点或卷容错能力。

存储开销

纠删编码方案的存储开销是通过奇偶校验片段数除(`m`以数据片段数计算得出的(`k`。您可以使用存储开销计算每个擦除编码对象所需的磁盘空间量：

```
disk space = object size + (object size * storage overhead)
```

例如，如果使用 4+2 方案存储一个 10 MB 的对象（存储开销为 50% ），则该对象将占用 15 MB 的网格存储。如果使用 6+2 方案存储同一个 10 MB 对象（存储开销为 33% ），则该对象将占用大约 13.3 MB 的空间。

选择总价值最低的纠删编码方案、以 `k+m`满足您的需求。具有较少片段数量的纠删编码方案在计算上效率更高、原因是：

- 每个对象创建和分布(或检索)的片段较少
- 它们的性能较高、因为片段大小较大
- 在中添加的节点可能更少"需要更多存储时进行扩展"

存储池准则

如果要为创建经过删除编码的副本的规则选择要使用的存储池、请对存储池使用以下准则：

- 存储池必须包含三个或更多站点，或者只包含一个站点。

  > 如果存储池包含两个站点、则不能使用纠删编码。

  - 包含三个或更多站点的存储池的纠删编码方案

- 单站点存储池的纠删编码方案

- 请勿使用包含"所有站点"站点的存储池。
- 存储池应至少包含 `*k+m* +1`可存储对象数据的存储节点。

> 可以在安装期间配置存储节点以包含对象数据和元数据（“组合”存储节点）、仅包含对象元数据或仅包含对象数据。有关详细信息，请参阅"存储节点的类型" 。

所需的最小存储节点数为 `k+m`。但是，如果所需的存储节点暂时不可用，则至少添加一个存储节点有助于防止载入失败或 ILM 回退。

包含三个或更多站点的存储池的纠删编码方案

下表介绍了 StorageGRID 当前支持的纠删编码方案，该方案适用于包含三个或更多站点的存储池。所有这些方案都提供站点丢失保护。一个站点可能会丢失，但对象仍可访问。

对于提供站点丢失保护的纠删编码方案、存储池中建议的存储节点数超过 `*k+m* +1`、因为每个站点至少需要三个存储节点。

纠删编码方案（ *k+m* ）	已部署站点的最小数量	每个站点的建议存储节点数	建议的存储节点总数	站点丢失保护？	存储开销
4+2.	3	3	9	是	50%
6+2.	4	3	12	是	33%
8+2.	5	3	15	是	25%
6+3.	3	4	12	是	50%
9+3.	4	4	16	是	33%
2+1.	3	3	9	是	50%
4+1.	5	3	15	是	25%
6+1.	7	3	21	是	17%
7+5.	3	5	15	是	71%

> StorageGRID 要求每个站点至少有三个存储节点。要使用 7+5 方案，每个站点至少需要四个存储节点。建议每个站点使用五个存储节点。

在选择提供站点保护的纠删编码方案时，请平衡以下因素的相对重要性：

- * 碎片数量 * ： 当碎片总数减少时，性能和扩展灵活性通常会提高。

- 容错：容错通过具有更多奇偶校验段(即值更高时)来提高 `m`。
- 网络流量：从故障中恢复时，使用具有更多片段的方案(即，的总数更高 `k+m`)会产生更多网络流量。
- * 存储开销 * ： 开销较高的方案需要每个对象更多的存储空间。

例如，在选择 4+2 方案和 6+3 方案（两者都有 50% 的存储开销）时，如果需要额外的容错功能，请选择 6+3 方案。如果网络资源受限，请选择 4+2 方案。如果所有其他因素相等，请选择 4+2 ，因为其碎片总数较低。

如果您不确定要使用的方案，请选择 4+2 或 6+3 ，或者联系技术支持。

单站点存储池的纠删编码方案

单站点存储池支持为三个或更多站点定义的所有纠删编码方案，但前提是该站点具有足够的存储节点。

所需的最小存储节点数为 `k+m`，但建议使用包含存储节点的存储池 `k+m +1`。例如， 2+1 纠删编码方案要求一个存储池至少包含三个存储节点，但建议使用四个存储节点。

纠删编码方案（ *k+m* ）	存储节点的最小数量	建议的存储节点数	存储开销
4+2.	6	7	50%
6+2.	8	9	33%
8+2.	10	11	25%
6+3.	9	10	50%
9+3.	12	13	33%
2+1.	3	4	50%
4+1.	5	6	25%
6+1.	7	8	17%
7+5.	12	13	71%

StorageGRID 中纠删编码的优势、劣势和要求

在决定是使用复制还是纠删编码来保护对象数据不会丢失之前，您应了解纠删编码的优点，缺点和要求。

纠删编码的优势

与复制相比，纠删编码可提高可靠性，可用性和存储效率。

- 可靠性：以在不丢失数据的情况下可以承受的同时故障次数来衡量。

- 复制：多个相同的对象副本存储在不同的节点和跨站点上。
- 擦除编码：将对象编码为数据和奇偶校验片段，并分布在许多节点和站点上。这种分散提供了站点和节点故障保护。

- 可用性：当存储节点发生故障或无法访问时获取对象的能力。与复制相比，擦除编码在相当的存储成本下提供了更高的可用性。
- 存储效率：在可用性和可靠性相似的情况下，擦除编码对象比复制对象占用更少的磁盘空间。例如，复制到两个站点的 10 MB 对象将消耗 20 MB 磁盘空间（两个副本），而使用 6+3 擦除编码方案在三个站点上进行擦除编码的对象仅消耗 15 MB 磁盘空间。

> 擦除编码对象的磁盘空间计算为对象大小加上存储开销。存储开销百分比是奇偶校验片段数除以数据片段数。

纠删编码的缺点

与复制相比，纠删编码具有以下缺点：

- 建议增加存储节点和站点的数量、具体取决于纠删编码方案。相比之下、如果复制对象数据、则每个副本只需要一个存储节点。请参阅"包含三个或更多站点的存储池的纠删编码方案"和"单站点存储池的纠删编码方案"。
- 存储扩展的成本和复杂性增加。要扩展使用复制的部署、您需要在创建对象副本的每个位置添加存储容量。要扩展使用纠删编码的部署，您必须同时考虑使用的纠删编码方案以及现有存储节点的容量。例如、如果您等待现有节点达到100%全满、则必须至少添加 `k+m`存储节点、但如果在现有节点达到70%全满时进行扩展、则可以为每个站点添加两个节点、同时仍可最大程度地提高可用存储容量。有关详细信息，请参见 "为经过纠删编码的对象添加存储容量"。
- 在分布在不同地理位置的站点之间使用纠删编码时，检索延迟会增加。通过WAN连接检索经过验证编码并分布在远程站点上的对象片段比复制并在本地可用的对象(客户端连接到的同一站点)所需时间更长。
- 在地理位置分散的站点之间使用纠删编码时，检索和修复的 WAN 网络流量使用率较高，尤其是频繁检索的对象或通过 WAN 网络连接进行对象修复。
- 当您跨站点使用擦除编码时，随着站点间网络延迟的增加，最大对象吞吐量会急剧下降。这种下降是由于 TCP 网络吞吐量下降造成的，这影响了StorageGRID系统存储和检索对象片段的速度。
- 提高计算资源的利用率。

何时使用纠删编码

使用擦除编码来满足以下要求：

- 大于 1 MB 的对象。

> 纠删编码最适合大于 1 MB 的对象。不要对小于200 KB的对象使用纠删编码、以避免管理非常小的经过纠删编码的片段所产生的开销。

- 长期或冷存储，用于存储不经常检索的内容。
- 高数据可用性和可靠性。
- 防止发生完整的站点和节点故障。
- 存储效率。

- 需要高效数据保护的单站点部署，只需一个纠删编码副本，而不是多个复制副本。
- 站点间延迟小于 100 毫秒的多站点部署。

StorageGRID 如何确定对象保留

StorageGRID 为网格管理员和单个租户用户提供了指定对象存储时间的选项。通常，租户用户提供的任何保留指令优先于网格管理员提供的保留指令。

租户用户如何控制对象保留

租户用户可以使用以下方法控制其对象在StorageGRID中存储的时间：

- 如果为网格启用了全局S3对象锁定设置、S3租户用户可以在启用S3对象锁定的情况下创建存储分段、然后为每个存储分段选择*默认保留期限*。
- 如果为网格启用了全局 S3 对象锁定设置，则 S3 租户用户可以在启用了 S3 对象锁定的情况下创建分段，然后使用 S3 REST API 为添加到该分段的每个对象版本指定保留日期和合法保留设置。
  - 无法通过任何方法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、任何方法都无法删除该版本。
  - 启用了S3对象锁定的分段中的对象将由ILM "永久"保留。但是，在达到保留截止日期后，可以通过客户端请求或存储分段生命周期到期来删除对象版本。请参阅。 "使用 S3 对象锁定管理对象"
- S3 租户用户可以将生命周期配置添加到其分段中，以指定到期操作。如果存在分段生命周期，则 StorageGRID 会存储一个对象，直到满足到期操作中指定的日期或天数为止，除非客户端先删除该对象。请参阅。 "创建 S3 生命周期配置"
- S3客户端可以发出删除对象请求。在确定是删除还是保留对象时， StorageGRID 始终会优先处理客户端删除请求，而不是 S3 存储分段生命周期或 ILM 。

网格管理员如何控制对象保留

网格管理员可以使用以下方法控制对象保留：

- 为每个租户设置S3对象锁定最长保留期限。然后、租户用户可以为其每个存储分段设置默认保留期限。此外、还会对该存储分段(对象的保留截止日期)中新加载的任何对象强制实施最长保留期限。
- 创建ILM放置指令以控制对象的存储时间长度。如果对象与 ILM 规则匹配，则 StorageGRID 会存储这些对象，直到 ILM 规则中的最后一个时间段结束为止。如果为放置指令指定了"永久"、则对象将无限期保留。
- 无论谁控制对象的保留时间、ILM设置都控制存储哪些类型的对象副本(已复制或已删除编码)以及副本的位置(存储节点或云存储池)。

S3 存储分段生命周期和 ILM 如何交互

配置S3存储分段生命周期后、对于与生命周期筛选器匹配的对象、生命周期到期操作将覆盖ILM策略。因此，即使有关放置对象的任何 ILM 指令已失效，该对象也可能会保留在网格中。

对象保留示例

要更好地了解 S3 对象锁定，存储分段生命周期设置，客户端删除请求和 ILM 之间的交互，请考虑以下示例。

示例 **1**： **S3** 存储分段生命周期将对象保留的时间超过 **ILM**

ILM

将两个副本存储 1 年（ 365 天）

分段生命周期

对象在 2 年（ 730 天）后过期

结果

StorageGRID 会将对象存储 730 天。StorageGRID 使用存储分段生命周期设置来确定是删除还是保留对象。

> 如果存储分段生命周期指定对象的保留时间应超过 ILM 指定的时间，则 StorageGRID 在确定要存储的副本数量和类型时会继续使用 ILM 放置说明。在此示例中，从第 366 天到第 730 天，此对象的两个副本将继续存储在 StorageGRID 中。

示例 **2**： **S3** 存储分段生命周期将对象在 **ILM** 之前过期

ILM

将两个副本存储 2 年（ 730 天）

分段生命周期

对象在 1 年（ 365 天）后过期

结果

StorageGRID 将在 365 天后删除此对象的两个副本。

示例 **3**： 客户端删除将覆盖存储分段生命周期和 **ILM**

ILM

"永久"在存储节点上存储两个副本

分段生命周期

对象在 2 年（ 730 天）后过期

客户端删除请求

发布日期：第 400 天

结果

StorageGRID 会在第 400 天删除此对象的两个副本，以响应客户端删除请求。

示例 **4**： **S3** 对象锁定会覆盖客户端删除请求

S3 对象锁定

对象版本的保留截止日期为 2026-03-31 。合法保留无效。

符合 **ILM** 规则

"永久"在存储节点上存储两个副本

客户端删除请求

于2024-03-31发布

结果

StorageGRID 不会删除此对象版本，因为保留截止日期仍在 2 年后。

StorageGRID 如何删除对象

StorageGRID 可以直接响应客户端请求删除对象，也可以因 S3 存储分段生命周期到期或 ILM 策略要求而自动删除对象。了解可删除对象的不同方式以及 StorageGRID 如何处理删除请求有助于您更有效地管理对象。

StorageGRID 可以使用以下两种方法之一删除对象：

- 同步删除：当 StorageGRID 收到客户端删除请求时，将立即删除所有对象副本。删除副本后，系统会通知客户端删除操作成功。
- 对象将排队等待删除：当 StorageGRID 收到删除请求时，该对象将排队等待删除，并且系统会立即通知客户端删除已成功。对象副本稍后将通过后台 ILM 处理进行删除。

删除对象时， StorageGRID 会使用方法来优化删除性能，最大限度地减少潜在的删除积压并以最快的速度释放空间。

下表总结了 StorageGRID 何时使用每种方法。

执行删除的方法	使用时
对象已排队等待删除	当满足以下条件中的 * 任意 * 时： • 以下事件之一已触发自动对象删除： ◦ 已达到 S3 存储分段的生命周期配置中的到期日期或天数。 ◦ ILM 规则中指定的最后一个时间段已过。 *注意：*如果存储分段中启用了S3对象锁定的对象处于合法保留状态、或者指定了保留截止日期但尚未满足、则无法删除这些对象。 • S3客户端请求删除、并且满足以下一个或多个条件： ◦ 无法在30秒内删除副本、例如、某个对象位置暂时不可用。 ◦ 后台删除队列处于空闲状态。
立即删除对象（同步删除）	当S3客户端发出删除请求且满足以下*全部*条件时： • 可以在 30 秒内删除所有副本。 • 后台删除队列包含要处理的对象。

当S3客户端发出删除请求时、StorageGRID会首先将对象添加到删除队列中。然后，它会切换到执行同步删除。确保后台删除队列包含要处理的对象，这样 StorageGRID 可以更高效地处理删除，尤其是对于低并发性客户端，同时有助于防止客户端删除积压。

StorageGRID 删除对象的方式可能会影响系统的执行方式：

- 当 StorageGRID 执行同步删除时， StorageGRID 可能需要长达 30 秒才能将结果返回给客户端。这意味着删除的速度可能会更慢，即使副本的实际删除速度比 StorageGRID 将对象排队等待删除时要快。
- 如果您在批量删除期间密切监控删除性能、则可能会注意到、删除一定数量的对象后、删除率似乎很慢。当 StorageGRID 从对要删除的对象进行排队转移到执行同步删除时，会发生此更改。删除率明显降低并不意味着删除对象副本的速度较慢。相反，它表明平均而言，空间释放速度更快。

如果要删除大量对象，并且您的优先级是快速释放空间，请考虑使用客户端请求删除对象，而不是使用 ILM 或其他方法删除这些对象。通常，当客户端执行删除时，空间释放速度会更快，因为 StorageGRID 可以使用同步删除。

删除对象后释放空间所需的时间取决于多个因素：

- 对象副本是同步删除还是稍后排队等待删除（对于客户端删除请求）。
- 其他因素包括网格中的对象数或对象副本排队等待删除时网格资源的可用性（对于客户端删除和其他方法）。

如何删除受版本控制的 S3 对象

如果为 S3 存储分段启用了版本控制，则无论这些请求来自 S3 客户端， S3 存储分段生命周期到期还是 ILM 策略要求， StorageGRID 都会在响应删除请求时遵循 Amazon S3 的行为。

对对象进行版本管理时、对象删除请求不会删除对象的当前版本、也不会释放空间。相反、对象删除请求会创建一个零字节删除标记作为对象的当前版本、从而使对象的上一个版本"非当前"。如果对象删除标记为当前版本且没有非当前版本、则它将成为过期的对象删除标记。

即使尚未删除此对象， StorageGRID 的行为仍会使当前版本的对象不再可用。对该对象的请求将返回 404 NotFound 。但是，由于未删除非当前对象数据，因此指定非当前对象版本的请求可能会成功。

如果客户端从"分支桶"， StorageGRID隐藏了对象版本的存在，但不会在分支存储桶中创建删除标记。如果客户端从分支存储桶中删除没有版本 ID 的对象， StorageGRID会根据标准 S3 行为在分支存储桶中创建删除标记。

要在删除分版本对象时释放空间或删除删除标记、请使用以下方法之一：

- **S3**客户端请求:在S3删除对象请求中指定对象版本ID (`DELETE /object?versionId=ID`)。请注意，此请求仅删除指定版本的对象副本（其他版本仍占用空间）。
- 存储分段生命周期：在存储分段生命周期配置中使用此 `NoncurrentVersionExpiration`操作。满足指定的非当前磁盘数后， StorageGRID 将永久删除非当前对象版本的所有副本。无法恢复这些对象版本。

  > `NewerNoncurrentVersions`存储分段生命周期配置中的操作指定受版本控制的S3存储分段中保留的非最新版本数。如果非最新版本比指定的版本多`NewerNoncurrentVersions`、则在非当前天数值已过时、StorageGRID将删除旧版本。此`NewerNoncurrentVersions`阈值将覆盖ILM提供的生命周期规则、这意味着、如果ILM请求删除版本在阈值内的非当前对象、则会保留此对象 `NewerNoncurrentVersions`。

  要删除过期的对象删除标记，请使用 `Expiration`带有以下标记之一的操作：`ExpiredObjectDeleteMarker`、 `Days`或 `Date`。

- *ILM："克隆活动策略"并向新策略中添加两个ILM规则：
  - 第一条规则：使用"非当前时间"作为参考时间、以匹配对象的非当前版本。在中"创建ILM规则向导的第1步(输入详细信息)"，为问题“Apply this Rule to older object versions only (in S3 bu桶with versioning enabled)？(仅将此规则应用于旧对象版本(在启用了版本控制的S3存储分段中)？)”选择*Yes*。
  - 第二条规则：使用*Ingesgite time*与当前版本匹配。"非当前时间"规则必须显示在策略中、高于*载入时间*规则。

    要删除已过期的对象删除标记、请使用*内嵌时间*规则匹配当前的删除标记。只有当*时间段****天*已过且当前删除程序已过期(没有非当前版本)时、删除标记才会被删除。
- 删除"删除所有对象版本"存储分段中的对象：使用租户管理器从存储分段中删除标记(包括删除标记)。

删除受版本控制的对象后、StorageGRID会创建一个零字节删除标记作为对象的当前版本。必须先删除所有对象和删除标记、然后才能删除分版本存储分段。

- 在StorageGRID 11.7或更早版本中创建的删除标记只能通过S3客户端请求删除、而不能通过ILM、存储分段生命周期规则或删除存储分段操作中的对象来删除。
- 可以通过ILM、存储分段生命周期规则、删除存储分段操作中的对象或显式S3客户端删除功能从在StorageGRID 11.8或更高版本中创建的存储分段中删除标记。

相关信息

- "使用S3 REST API"
- "示例 4： S3 版本对象的 ILM 规则和策略"

在 StorageGRID 中创建和分配存储等级

存储级别用于确定存储节点使用的存储类型。如果希望ILM规则将某些对象放置在特定存储节点上、则可以创建存储级别。

开始之前

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

关于此任务

首次安装StorageGRID 时，系统会自动为系统中的每个存储节点分配*Default*存储级别。您可以根据需要定义自定义存储级别并将其分配给不同的存储节点。

通过使用自定义存储等级、您可以创建仅包含特定类型存储节点的ILM存储池。例如，您可能希望某些对象存储在速度最快的存储节点上，例如 StorageGRID 全闪存存储设备。

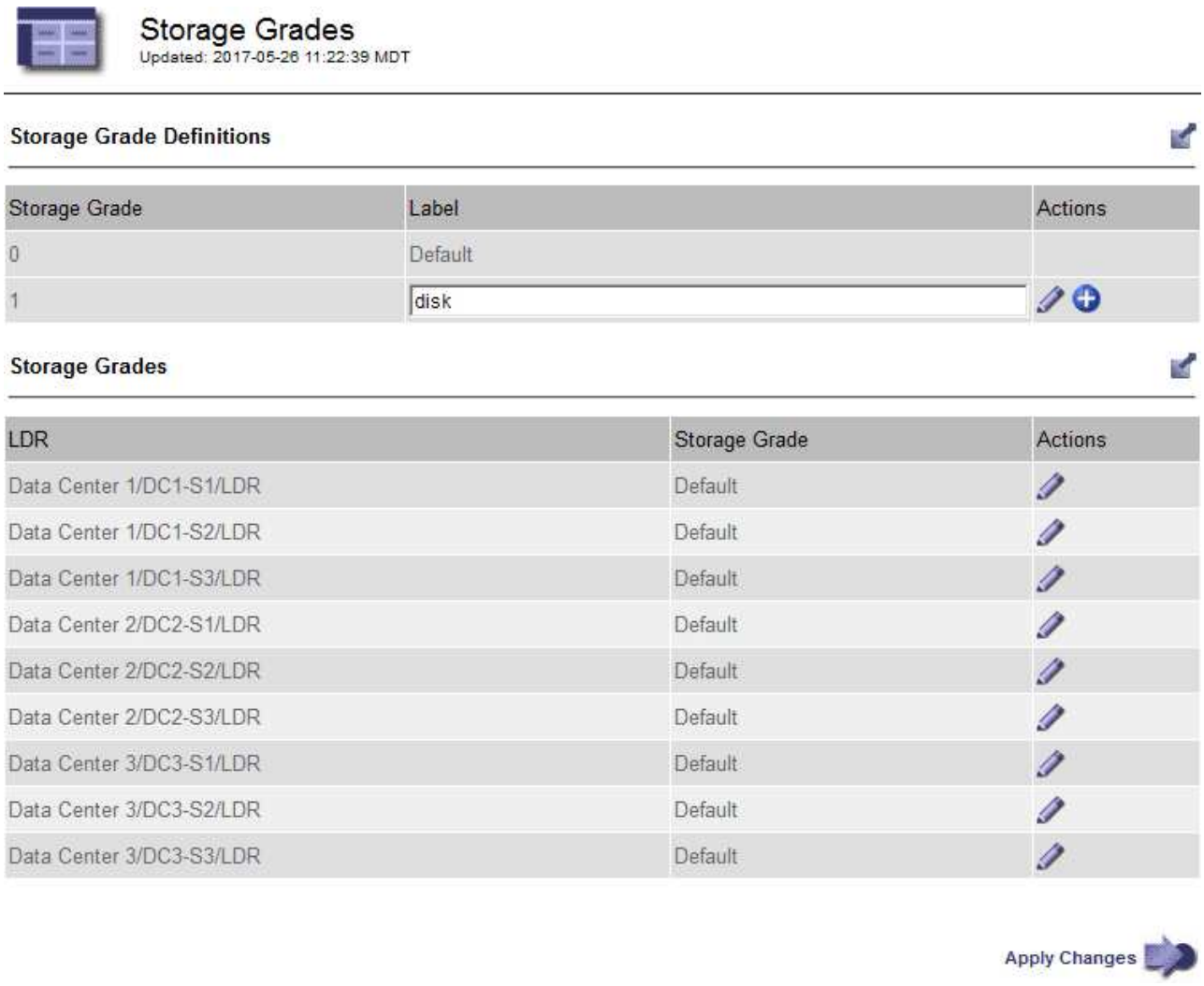
仅元数据存储节点不能分配存储等级。有关详细信息，请参阅"存储节点的类型" 。

如果不需要考虑存储级别(例如，所有存储节点都相同)，则可以跳过此过程，并在使用时对存储级别使用"创建存储池""“包括所有存储级别”选项。使用此选项可确保存储池包含站点上的每个存储节点、而不管其存储级别如何。

请勿创建超出所需数量的存储等级。例如、不要为每个存储节点创建存储级别。而是将每个存储级别分配给两个或更多节点。如果仅分配给一个节点的存储级别不可用，则发生原因 ILM 会回退日志。

步骤

1. 选择 * ILM * > * 存储级别 * 。
2. 定义自定义存储等级：
   a. 对于要添加的每个自定义存储等级，选择 **Insert** 以添加行。
   b. 输入描述性标签。

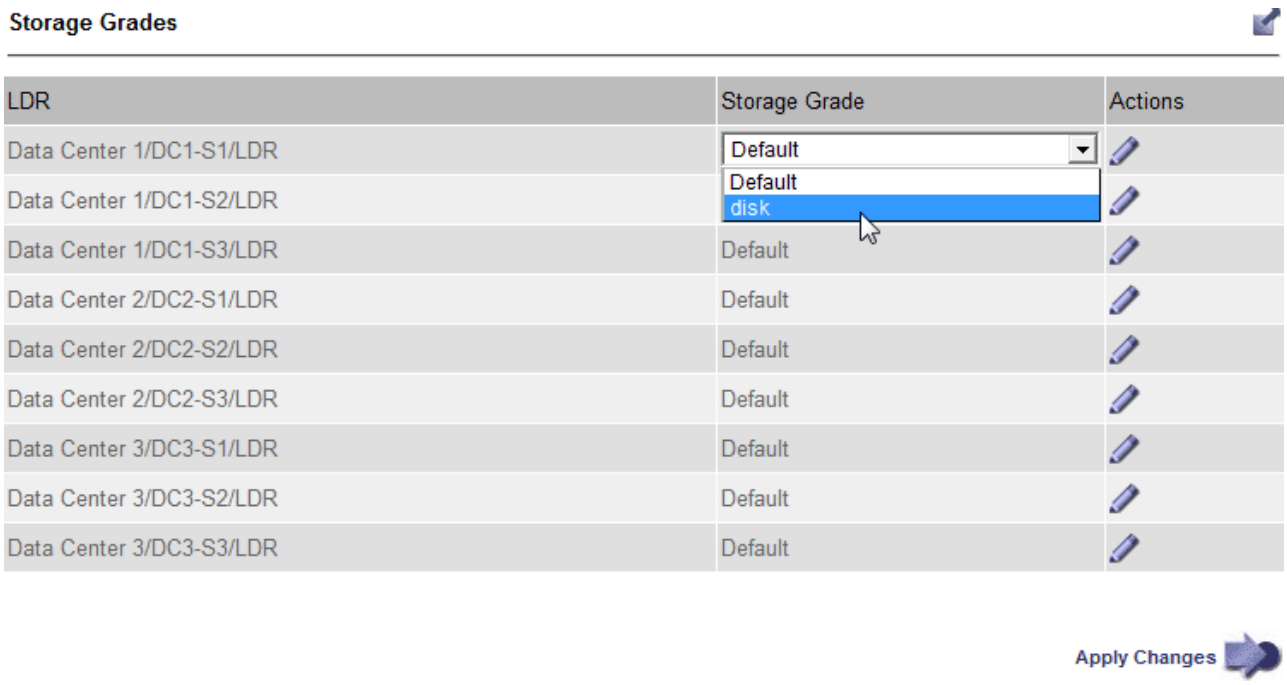


   c. 选择 * 应用更改 * 。
   d. 或者，如果您需要修改已保存的标签，请选择*编辑*并选择*应用更改*。

   您无法删除存储等级。

3. 为存储节点分配新的存储级别：
   a. 在 LDR 列表中找到存储节点，然后选择其*编辑*图标。

b. 从列表中选择适当的存储级别。



只需为给定存储节点分配一次存储级别。从故障中恢复的存储节点将保持先前分配的存储级别。激活ILM策略后、请勿更改此分配。如果分配发生更改，则会根据新的存储级别存储数据。

a. 选择 * 应用更改 * 。

使用存储池

了解 StorageGRID 中的存储池

存储池是存储节点的逻辑分组。

安装StorageGRID 时、系统会自动为每个站点创建一个存储池。您可以根据存储需求配置其他存储池。

可以在安装期间配置存储节点以包含对象数据和元数据（“组合”存储节点）、仅包含对象元数据或仅包含对象数据。仅元数据存储节点不能在存储池中使用。有关详细信息，请参阅"存储节点的类型" 。

存储池具有两个属性：

- * 存储级别 * ：对于存储节点，是指后备存储的相对性能。
- 站点：存储对象的数据中心。

存储池在ILM规则中用于确定对象数据的存储位置以及所使用的存储类型。配置用于复制的ILM规则时、请选择一个或多个存储池。

StorageGRID 中的存储池配置准则

配置和使用存储池、通过在多个站点之间分布数据来防止数据丢失。复制的副本和经过删除编码的副本需要不同的存储池配置。

请参阅 "使用复制和纠删编码启用站点丢失保护的示例"。

所有存储池的准则

- 尽可能简化存储池配置。请勿创建超出所需数量的存储池。
- 创建具有尽可能多节点的存储池。每个存储池应包含两个或更多节点。如果节点不可用，则节点不足的存储池可以对发生原因 ILM 进行回退。
- 避免创建或使用重叠的存储池（包含一个或多个相同节点）。如果存储池重叠，则可能会在同一节点上保存多个对象数据副本。
- 通常、不要使用所有存储节点存储池(StorageGRID 11.6及更早版本)或所有站点站点。这些项会自动更新、以包括您在扩展中添加的任何新站点、而这可能不是您想要的行为。

用于复制副本的存储池准则

- 对于使用的站点丢失保护"复制"，请在中指定一个或多个特定于站点的存储池"每个ILM规则的放置说明"。

  在StorageGRID 安装期间、系统会自动为每个站点创建一个存储池。

  对每个站点使用存储池可确保复制的对象副本准确放置在所需位置（例如，每个站点上的每个对象一个副本，以实现站点丢失保护）。

- 如果要在扩展中添加站点、请创建一个仅包含新站点的新存储池。然后、"更新ILM规则"控制在新站点上存储哪些对象。
- 如果副本数小于存储池数、则系统会分布这些副本、以平衡各个池之间的磁盘使用量。
- 如果存储池重叠（包含相同的存储节点），则对象的所有副本可能只保存在一个站点上。您必须确保选定存储池不包含相同的存储节点。

用于擦除编码副本的存储池准则

- 对于使用的站点丢失保护"纠删编码"，请创建至少包含三个站点的存储池。如果存储池仅包含两个站点、则不能使用该存储池进行纠删编码。对于具有两个站点的存储池，没有可用的纠删编码方案。
- 存储池中包含的存储节点和站点数量决定了哪些"纠删编码方案"可用。
- 如果可能，存储池中的存储节点数应超过您选择的纠删编码方案所需的最小存储节点数。例如，如果您使用 6+3 纠删编码方案，则必须至少有九个存储节点。但是，建议每个站点至少另外配置一个存储节点。
- 尽可能均匀地在各个站点之间分布存储节点。例如，要支持 6+3 纠删编码方案，请配置一个存储池，使其在三个站点中至少包含三个存储节点。
- 如果吞吐量要求较高、则在站点之间的网络延迟超过100毫秒时、不建议使用包含多个站点的存储池。随着延迟增加， StorageGRID 创建，放置和检索对象片段的速率会因 TCP 网络吞吐量降低而大幅下降。

  吞吐量的降低会影响对象摄取和检索的最大可实现速率（当选择 Balanced 或 Strict 作为摄取行为时），或可能导致 ILM 队列积压（当选择 Dual commit 作为摄取行为时）。请参阅 "ILM规则加热行为"。

如果您的网格仅包含一个站点、则系统将阻止您使用纠删编码配置文件中的所有存储节点存储池(StorageGRID 11.5及更早版本)或所有站点站点。此行为可防止在添加第二个站点时配置文件变得无效。

利用 **StorageGRID** 中的存储池进行站点丢失保护

如果您的StorageGRID 部署包含多个站点、则可以对已正确配置的存储池使用复制和纠删编码来启用站点丢失保护。

复制和纠删编码需要不同的存储池配置：

- 要使用复制保护站点丢失、请使用在StorageGRID 安装期间自动创建的站点专用存储池。然后、使用创建ILM规则以"放置说明"指定多个存储池、以便在每个站点上放置每个对象的一个副本。
- 要使用纠删编码保护站点丢失，请"创建包含多个站点的存储池"。然后、创建ILM规则、这些规则使用一个存储池、其中包含多个站点和任何可用的纠删编码架构。

在配置StorageGRID部署以进行站点丢失保护时，还必须考虑以下因素的影响"加热选项"和"一致性"。

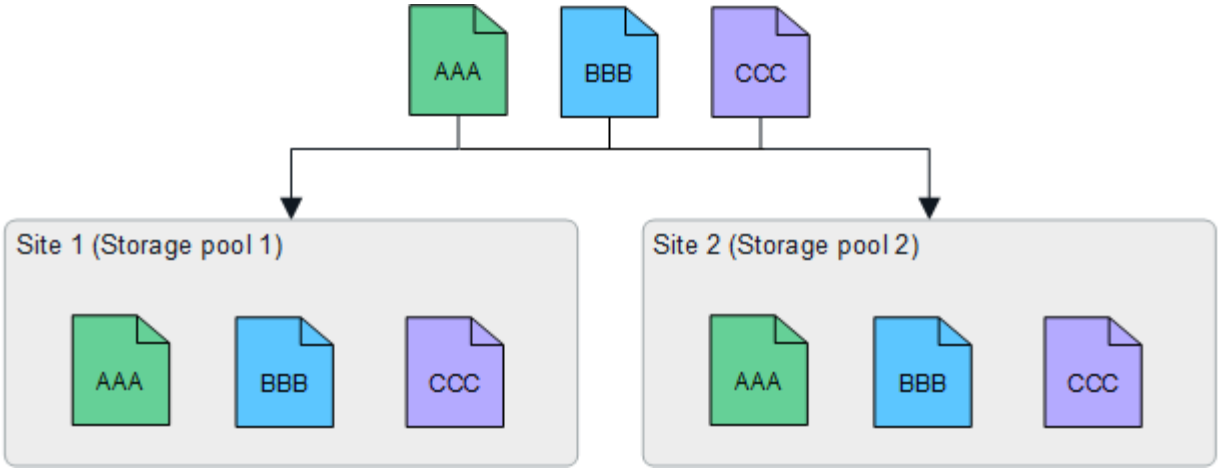
复制示例

默认情况下、在StorageGRID 安装期间、系统会为每个站点创建一个存储池。如果存储池仅包含一个站点、则可以配置使用复制来保护站点丢失的ILM规则。在此示例中：

- 存储池1包含站点1
- 存储池2包含站点2
- ILM规则包含两个放置位置：
  - 通过在站点1复制1个副本来存储对象
  - 通过在站点2复制1个副本来存储对象

ILM规则放置：





如果一个站点丢失、则另一个站点上可以提供对象副本。

纠删编码示例

如果存储池中的每个存储池包含多个站点、则可以配置使用纠删编码保护站点丢失的ILM规则。在此示例中：

- 存储池1包含站点1到3
- ILM规则包含一个放置位置：在存储池1 (包含三个站点)上使用4+2 EC方案通过纠删编码存储对象

ILM规则放置：

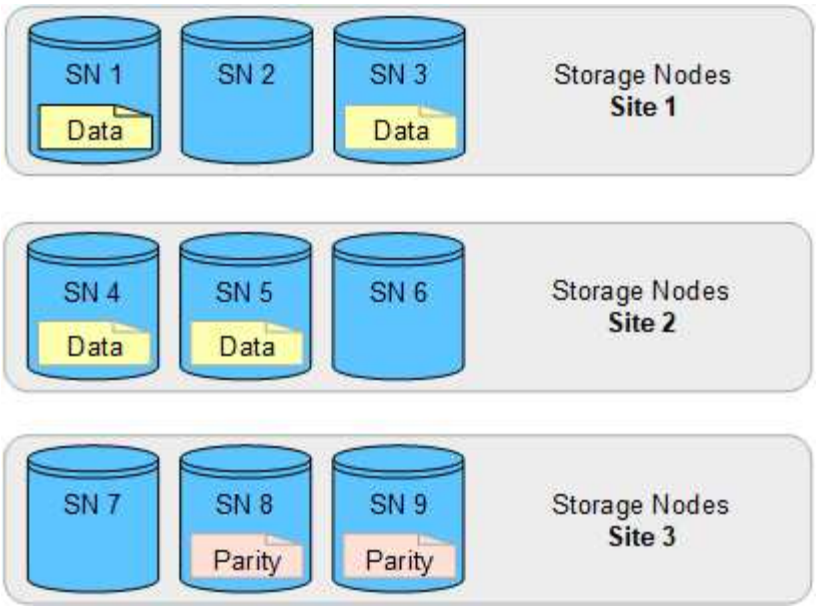


在此示例中：

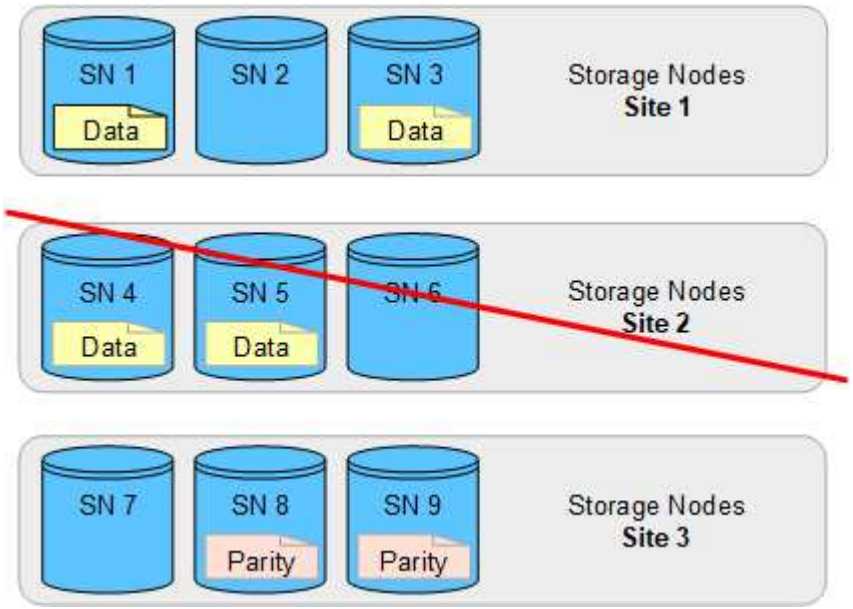
- ILM规则使用4+2纠删编码方案。
- 每个对象都会被划分为四个相等的数据片段，并根据对象数据计算两个奇偶校验片段。
- 六个片段中的每个片段都存储在三个数据中心站点的不同节点上，以便为节点故障或站点丢失提供数据保护。

允许在包含任意数量站点的存储池中进行纠删编码、但两个站点除外。

使用4+2纠删编码方案的ILM规则：



如果一个站点丢失、数据仍可恢复：



在 **StorageGRID** 中创建存储池

您可以创建存储池来确定 StorageGRID 系统存储对象数据的位置以及使用的存储类型。每个存储池包括一个或多个站点以及一个或多个存储级别。

> 在新网格上安装 StorageGRID 12.0 或更高版本时，系统会自动为每个站点创建存储池。但是，如果您最初安装了 StorageGRID 11.6 或更早版本，则不会自动为每个站点创建存储池。

如果要创建云存储池以将对象数据存储在StorageGRID系统之外，请参见"有关使用云存储池的信息"。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。

- 您拥有 "特定访问权限"。
- 您已查看创建存储池的准则。

关于此任务

存储池用于确定对象数据的存储位置。所需的存储池数量取决于网格中的站点数量以及所需的副本类型：复制副本或经过纠删编码的副本。

- 对于复制和单站点纠删编码，请为每个站点创建一个存储池。例如，如果要将复制的对象副本存储在三个站点上，请创建三个存储池。
- 要在三个或更多站点上进行纠删编码，请创建一个存储池，其中包含每个站点的条目。例如，如果要跨三个站点擦除代码对象，请创建一个存储池。

> 请勿将所有站点包含在要在纠删编码配置文件中使用的存储池中。而是为每个要存储经过数据经过了数据经过了数据经过了数据迁移的站点在存储池中添加一个单独的条目。有关示例、请参见此步骤。

- 如果您有多个存储级别、请勿在一个站点上创建包含不同存储级别的存储池。请参见"创建存储池的准则"。

步骤

1. 选择 * ILM * > * 存储池 * 。

   存储池选项卡列出了所有已定义的存储池。

   > 对于全新安装的StorageGRID 11.6或更早版本、每当添加新数据中心站点时、所有存储节点存储池都会自动更新。请勿在ILM规则中使用此池。

2. 要创建新存储池，请选择 * 创建 * 。
3. 输入存储池的唯一名称。请使用一个在配置纠删编码配置文件和ILM规则时易于识别的名称。
4. 从 * 站点 * 下拉列表中，为此存储池选择一个站点。

   选择站点后、此表中的存储节点数将自动更新。

   通常、不要使用任何存储池中的所有站点站点。使用所有站点存储池的 ILM 规则会将对象放置在任何可用站点上，从而减少对对象放置的控制。此外，所有站点存储池会立即使用新站点上的存储节点，这可能不是您所期望的行为。

5. 从*存储级别*下拉列表中、选择ILM规则使用此存储池时要使用的存储类型。

   存储级别(*all*包括 所有存储级别)包括选定站点上的所有存储节点。如果您为网格中的存储节点创建了其他存储级别，则这些存储级别将在下拉列表中列出。

6. 如果要在多站点纠删编码配置文件中使用存储池、请选择*添加更多节点*、以便为每个站点向存储池添加一个条目。

   > 如果您为一个站点添加多个具有不同存储等级的条目、则系统会向您发出警告。

   要删除条目，请选择删除图标 ✕。

7. 如果您对所做的选择感到满意，请选择 * 保存 * 。

   此时，新存储池将添加到此列表中。

在 StorageGRID 中查看存储池详细信息

您可以查看存储池的详细信息以确定存储池的使用位置，并查看包含哪些节点和存储级别。

开始之前

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

步骤

1. 选择 * ILM * > * 存储池 * 。

   "存储池"表包含每个包含存储节点的存储池的以下信息：

   - * 名称 * ：存储池的唯一显示名称。
   - **Node COUNT**：存储池中的节点数。
   - 存储使用量：已用于此节点上的对象数据的总可用空间的百分比。此值不包括对象元数据。
   - 总容量：存储池的大小、等于存储池中所有节点可用于对象数据的总空间量。
   - **ILM usage**：存储池的当前使用方式。存储池可能未使用、也可能用于一个或多个ILM规则、纠删编码配置文件或这两者。
2. 要查看特定存储池的详细信息、请选择其名称。

   此时将显示存储池的详细信息页面。

3. 查看*节点*选项卡以了解存储池中包含的存储节点。

   此表包含每个节点的以下信息：

   - 节点名称
   - 站点名称
   - 存储级
   - 存储使用量：已用于存储节点的对象数据在总可用空间中所占的百分比。

   > 每个存储节点的“已用存储 - 对象数据”图表中也显示相同的存储使用情况（%）值（选择“节点”>“存储节点”>“存储”）。

4. 查看*ILM usage*选项卡以确定存储池当前是否正在任何ILM规则或纠删编码配置文件中使用。
5. (可选)转到* ILM规则页面*、了解并管理使用存储池的任何规则。

   请参见"有关使用ILM规则的说明"。

在 StorageGRID 中编辑存储池

您可以编辑存储池以更改其名称或更新站点和存储级别。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 您已查看"创建存储池的准则"。
- 如果您计划编辑由活动 ILM 策略中的规则使用的存储池，则已考虑所做的更改将如何影响对象数据放置。

关于此任务

如果要向活动ILM策略中使用的存储池添加新站点或存储级别、请注意、新站点或存储级别中的存储节点不会自动使用。要强制StorageGRID 使用新站点或存储级别、您必须在保存编辑后激活新的ILM策略。

步骤

1. 选择 * ILM * > * 存储池 * 。
2. 选中要编辑的存储池对应的复选框。

   您不能编辑所有存储节点存储池(StorageGRID 11.6及更早版本)。

3. 选择 * 编辑 * 。
4. 根据需要更改存储池名称。
5. 根据需要选择其他站点和存储级别。

   如果在纠删编码配置文件中使用存储池、并且此更改可能会发生原因使纠删编码方案无效、则您将无法更改站点或存储级别。例如、如果纠删编码配置文件中使用的存储池当前仅包含一个站点的存储级别、则您将无法对两个站点使用存储级别、因为此更改会使纠删编码方案无效。

   > 从现有存储池添加或删除站点不会移动任何现有的经过删除编码的数据。如果要从站点移动现有数据、则必须创建新的存储池和EC配置文件、以便对数据重新编码。

6. 选择 * 保存 * 。

完成后

如果将新站点或存储级别添加到活动 ILM 策略中使用的存储池，请激活新的 ILM 策略，以强制 StorageGRID 使用新站点或存储级别。例如，克隆现有的 ILM 策略，然后激活克隆。请参阅 "使用 ILM 规则和 ILM 策略"。

删除 StorageGRID 中的存储池

您可以删除未使用的存储池。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。

步骤

1. 选择 * ILM * > * 存储池 * 。
2. 查看表中的ILM使用情况列、确定是否可以删除存储池。

   如果存储池正在ILM规则或纠删编码配置文件中使用、则不能将其删除。根据需要选择*_storage pool name_*>*ILM usage*以确定存储池的使用位置。

3. 如果未使用要删除的存储池、请选中此复选框。
4. 选择 * 删除 * 。
5. 选择 * 确定 * 。

使用云存储池

了解 **StorageGRID** 中的云存储池

云存储池允许您使用 ILM 将对象数据移动到 StorageGRID 系统之外。例如，您可能希望将不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 Storage 中的存档访问层。或者，您可能需要维护 StorageGRID 对象的云备份以增强灾难恢复。

从 ILM 的角度来看，云存储池类似于存储池。要将对象存储在任一位置，请在为 ILM 规则创建放置说明时选择池。但是，存储池由 StorageGRID 系统内的存储节点组成，而云存储池由外部存储桶 (S3) 或容器 (Azure Blob Storage) 组成。

下表将存储池与云存储池进行了比较、并显示了一些高级别的相似之处和不同之处。

	存储池	云存储池
如何创建?	使用网格管理器中的 * ILM * > * 存储池 * 选项。	使用网格管理器中的*ILM >*存储池*>*云存储池*选项。 您必须先设置外部存储分段或容器，然后才能创建云存储池。
您可以创建多少个池?	无限制。	最多 10 个。

	存储池	云存储池
对象存储在何处?	在StorageGRID中的一个或多个存储节点上。	在 StorageGRID 系统外部的 Amazon S3 桶、Azure Blob Storage 容器或 Google Cloud 中。 如果云存储池是 Amazon S3 存储分段： • 您可以选择配置存储分段生命周期，以便将对象过渡到低成本的长期存储，例如 Amazon S3 Glacier 或 S3 Glacier Deep Archive 。外部存储系统必须支持Glacierar存储类和S3 Restore-Object API。 • 您可以创建云存储池，以便与支持 AWS 机密区域的 AWS 商用云服务（ C2S ）结合使用。 如果云存储池是 Azure Blob 存储容器，StorageGRID 会将对象转换到存档层。 注意： 一般来说，不要为用于云存储池的容器配置 Azure Blob Storage 生命周期管理。对云存储池中对象执行 RestoreObject 操作可能会受到已配置的生命周期的影响。
什么控制对象放置?	活动ILM策略中的ILM规则。	活动ILM策略中的ILM规则。
使用以下哪种数据保护方法?	复制或纠删编码。	复制。
每个对象允许多少个副本?	多个。	一个副本位于云存储池中，一个或多个副本也位于 StorageGRID 中。 *注意：*在任何给定时间、都不能将对象存储在多个云存储池中。
有哪些优势?	可以随时快速访问对象。	低成本存储。 注意：FabricPool 数据无法分层到云存储池。

StorageGRID 中云存储池对象的生命周期

在实施云存储池之前，请查看存储在每种类型的云存储池中的对象的生命周期。

S3 ： 云存储池对象的生命周期

这些步骤介绍了S3云存储池中存储的对象的生命周期阶段。

"Glaciere"是指Glacier存储类和Glacier深度归档存储类、但有一个例外：Glacier深度归档存储类不支持加缓还原层。仅支持批量或标准检索。

Google Cloud Platform （ GCP ）支持从长期存储中检索对象，而无需执行还原后操作。

1. * 存储在 StorageGRID 中的对象 *

   要开始生命周期，客户端应用程序会将对象存储在 StorageGRID 中。

2. * 对象已移至 S3 云存储池 *

   - 如果对象与使用 S3 云存储池作为其放置位置的 ILM 规则匹配，则 StorageGRID 会将此对象移动到云存储池指定的外部 S3 存储分段。
   - 将对象移动到S3云存储池后、客户端应用程序可以使用StorageGRID的S3 GetObject请求检索该对象、除非该对象已转移到Glacier.存储。

3. * 已过渡到 Glacier 的对象（无法检索状态） *

   - 也可以将对象过渡到 Glacier 存储。例如，外部 S3 存储分段可能会使用生命周期配置立即或在一定天数后将对象过渡到 Glacier 存储。

     如果要过渡对象、则必须为外部S3存储分段创建生命周期配置、并且必须使用实施Glacier"存储类并支持S3 Restore-Object API的存储解决方案。

   - 过渡期间、客户端应用程序可以使用S3 HeadObject请求监控对象的状态。

4. * 对象已从 Glacier 存储还原 *

   如果某个对象已转移到Glacier"存储、则客户端应用程序可以对S3 Restore-Object请求执行问题描述操作、以便将可检索副本还原到S3云存储池。此请求指定在云存储池和数据访问层中应使用多少天的副本来执行还原操作（加急，标准或批量）。达到可检索副本的到期日期后，该副本将自动恢复为无法检索的状态。

   如果StorageGRID中的存储节点上也存在对象的一个或多个副本、则无需发出Restore-Object请求来从Glacier恢复 对象。而是可以使用GetObject请求直接检索本地副本。

5. * 已检索对象 *

   还原对象后、客户端应用程序可以问题描述一个GetObject请求来检索还原的对象。

Azure： Cloud Storage Pool 对象的生命周期

这些步骤介绍了存储在Azure云存储池中的对象的生命周期阶段。

1. * 存储在 StorageGRID 中的对象 *

   要开始生命周期，客户端应用程序会将对象存储在 StorageGRID 中。

2. * 对象已移至 Azure Cloud Storage Pool*

   当此对象与使用 Azure 云存储池作为其放置位置的 ILM 规则匹配时，StorageGRID 会将此对象移动到由云存储池指定的外部 Azure Blob 存储容器。

3. * 已过渡到归档层的对象（无法检索状态） *

   将此对象移动到 Azure 云存储池后，StorageGRID 会立即自动将此对象转换到 Azure Blob 存储存档层。

4. * 对象已从归档层还原 *

   如果某个对象已转移到归档层、则客户端应用程序可以对S3 Restore"对象请求执行问题描述操作、以便将可检索副本还原到Azure云存储池。

   当 StorageGRID 收到 RestoreObject 时，它会暂时将此对象转换到 Azure Blob Storage Cool 层。一旦到达 RestoreObject 请求中的到期日期，StorageGRID 会将此对象转换回存档层。

   > 如果StorageGRID中的存储节点上也存在对象的一个或多个副本、则无需发出Restore"对象请求、即可从归档访问层还原对象。而是可以使用GetObject请求直接检索本地副本。

5. * 已检索对象 *

   将对象还原到Azure云存储池后、客户端应用程序可以通过问题描述发出GetObject请求来检索还原的对象。

相关信息

"使用S3 REST API"

StorageGRID 中的云存储池用例

使用云存储池、您可以将数据备份或分层到外部位置。此外、您还可以将数据备份或分层到多个云。

将**StorageGRID** 数据备份到外部位置

您可以使用云存储池将 StorageGRID 对象备份到外部位置。

如果无法访问 StorageGRID 中的副本，则可以使用云存储池中的对象数据来处理客户端请求。但是、要访问云存储池中的备份对象副本、您可能需要问题描述S3 RestoreObject请求。

云存储池中的对象数据也可用于恢复因存储卷或存储节点故障而从 StorageGRID 丢失的数据。如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 会临时还原该对象，并在已恢复的存储节点上创建一个新副本。

要实施备份解决方案 ，请执行以下操作：

1. 创建一个云存储池。
2. 配置一个 ILM 规则，以便在存储节点上同时存储对象副本（以复制或擦除编码的副本的形式），并在云存储池中存储单个对象副本。
3. 将规则添加到 ILM 策略中。然后，模拟并激活策略。

将数据从**StorageGRID** 分层到外部位置

您可以使用云存储池将对象存储在 StorageGRID 系统之外。例如，假设您需要保留大量对象，但您希望很少访问这些对象（如果有）。您可以使用云存储池将对象分层以降低存储成本并释放 StorageGRID 中的空间。

要实施分层解决方案 ，请执行以下操作：

1. 创建一个云存储池。

2. 配置一个 ILM 规则，以便将很少使用的对象从存储节点移动到云存储池。
3. 将规则添加到 ILM 策略中。然后，模拟并激活策略。

维护多个云端点

如果要将对象数据分层或备份到多个云，则可以配置多个云存储池端点。ILM 规则中的筛选器允许您指定存储在每个云存储池中的对象。例如，您可能希望将来自某些租户或存储桶的对象存储在 Amazon S3 Glacier 中，并将来自其他租户或存储桶的对象存储在 Azure Blob Storage 中。或者，您可能希望在 Amazon S3 Glacier 和 Azure Blob Storage 之间移动数据。

使用多个云存储池端点时、请记住、一个对象一次只能存储在一个云存储池中。

实施多个云端点：

1. 最多创建 10 个云存储池。
2. 配置 ILM 规则，以便在每个云存储池中的适当时间存储相应的对象数据。例如、将存储分段A中的对象存储在云存储池A中、将存储分段B中的对象存储在云存储池B中。或者、将对象存储在云存储池A中一段时间、然后将其移动到云存储池B
3. 将规则添加到 ILM 策略中。然后，模拟并激活策略。

StorageGRID 中的云存储池要求和限制

如果您计划使用云存储池将对象移出 StorageGRID 系统，则必须查看配置和使用云存储池的注意事项。

一般注意事项

- 一般来说，云存档存储（例如 Amazon S3 Glacier 或 Azure Blob Storage）是存储对象数据的低成本场所。但是，从云存档存储中检索数据的成本相对较高。为了实现最低的总体成本，您必须考虑何时以及多久访问一次云存储池中的对象。建议仅对您希望不经常访问的内容使用云存储池。
- 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。
- 无法将启用了S3对象锁定的对象放置在云存储池中。
- 云存储池不支持以下平台、身份验证和协议与S3对象锁定的组合：
  - 平台：Google Cloud Platform和Azure
  - 身份验证类型：匿名访问
  - 协议：HTTP

用于云存储池的端口的注意事项

要确保 ILM 规则可以将对象移入和移出指定的云存储池，您必须配置包含系统存储节点的一个或多个网络。您必须确保以下端口可以与云存储池进行通信。

默认情况下，云存储池使用以下端口：

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

您可以在创建或编辑云存储池时指定其他端口。

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

成本注意事项

使用云存储池访问云中的存储需要通过网络连接到云。您必须根据希望使用云存储池在 StorageGRID 和云之间移动的数据量，考虑用于访问云并适当配置云的网络基础架构的成本。

当 StorageGRID 连接到外部云存储池端点时，它会发出各种请求来监控连接并确保它可以执行所需的操作。虽然这些请求会产生一些额外成本，但监控云存储池的成本只能是在 S3 或 Azure 中存储对象的总成本的一小部分。

如果您需要将对象从外部云存储池端点移回 StorageGRID ，可能会产生更显著的成本。在以下任一情况下，对象可能会移回 StorageGRID ：

- 此对象的唯一副本位于云存储池中，您决定将此对象存储在 StorageGRID 中。在这种情况下、您需要重新配置ILM规则和策略。进行 ILM 评估时， StorageGRID 会发出多个请求，以便从云存储池中检索对象。然后， StorageGRID 会在本地创建指定数量的复制副本或经过纠删编码的副本。将对象移回 StorageGRID 后，云存储池中的副本将被删除。
- 由于存储节点故障，对象丢失。如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 会临时还原该对象，并在已恢复的存储节点上创建一个新副本。

> 当对象从云存储池移回 StorageGRID 时， StorageGRID 会为每个对象向云存储池端点发出多个请求。在移动大量对象之前，请联系技术支持以帮助估算时间范围和相关成本。

S3 ： 云存储池存储分段所需的权限

用于云存储池的外部S3存储分段的策略必须授予StorageGRID权限、以便将对象移动到该存储分段、获取对象的状态、根据需要从Glacier"存储中还原对象等。理想情况下，StorageGRID应具有对存储分段(`s3:*`的完全控制访问权限；但是，如果不可能，存储分段策略必须向StorageGRID授予以下S3权限：

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3：外部存储分段的生命周期注意事项

StorageGRID与云存储池中指定的外部S3存储分段之间的对象移动由StorageGRID中的ILM规则和活动ILM策略控制。相比之下，对象从云存储池中指定的外部 S3 存储分段过渡到 Amazon S3 Glacier 或 S3 Glacier 深度归档（或过渡到实施 Glacier 存储类的存储解决方案 ）则由该分段的生命周期配置控制。

如果要从云存储池过渡对象、则必须在外部S3存储分段上创建适当的生命周期配置、并且必须使用实施Glacier"

存储类并支持S3 RestorerObject API的存储解决方案。

例如，假设您希望将从 StorageGRID 移动到云存储池的所有对象立即过渡到 Amazon S3 Glacier 存储。您应在外部 S3 存储分段上创建一个生命周期配置，用于指定单个操作（ * 过渡 * ），如下所示：

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

此规则会在创建所有存储分段对象的日期（即从 StorageGRID 迁移到云存储池的日期）将这些对象过渡到 Amazon S3 Glacier 。

> 配置外部存储分段的生命周期时，切勿使用 * 到期 * 操作来定义对象何时过期。到期操作发生原因 外部存储系统以删除已过期的对象。如果稍后尝试从 StorageGRID 访问已过期的对象，则无法找到已删除的对象。

如果要将云存储池中的对象过渡到S3 Glacier"深度归档"(而不是Amazon S3 Glacier")、请在存储分段生命周期中指定 `<StorageClass>DEEP_ARCHIVE</StorageClass>`。但是、请注意、您不能使用该 `Expedited`层从S3 Glaciereep Archive还原对象。

Azure： 访问层注意事项

配置 Azure 存储帐户时，您可以将默认访问层设置为热或冷。创建用于云存储池的存储帐户时，应使用热层作为默认层。即使 StorageGRID 在将对象移动到云存储池时会立即将层设置为归档，但使用默认设置 " 热 " 可确保在至少 30 天之前从冷层中删除的对象不会收到提前删除费用。

Azure： 不支持生命周期管理

不要对与 Cloud Storage Pool 一起使用的容器使用 Azure Blob Storage 生命周期管理。生命周期操作可能会干扰 Cloud Storage Pool 操作。

相关信息

"创建云存储池"

StorageGRID 中的云存储池和 **CloudMirror** 复制

在开始使用云存储池时，了解云存储池与 StorageGRID CloudMirror 复制服务之间的相似之处和不同之处可能会很有帮助。

	云存储池	**CloudMirror** 复制服务
主要目的是什么?	用作归档目标。云存储池中的对象副本可以是对象的唯一副本，也可以是其他副本。也就是说、您可以在StorageGRID 中保留一个副本并将一个副本发送到云存储池、而不是在现场保留两个副本。	允许租户自动将对象从StorageGRID (源)中的存储分段复制到外部S3存储分段(目标)。在独立的S3基础架构中为对象创建一个独立副本。
如何设置?	使用网格管理器或网格管理API以与存储池相同的方式进行定义。可选择作为ILM规则中的放置位置。虽然存储池包含一组存储节点，但云存储池是使用远程 S3 或 Azure 端点（ IP 地址，凭据等）定义的。	租户用户、方法是使用租"配置 CloudMirror 复制"户管理器或S3 API定义CloudMirror端点(IP地址、凭据等)。设置 CloudMirror 端点后，可以将该租户帐户拥有的任何分段配置为指向 CloudMirror 端点。
谁负责设置?	通常是网格管理员	通常是租户用户
目标是什么?	• 任何兼容的 S3 基础架构（包括 Amazon S3 ） • Azure Blob 归档层 • Google Cloud Platform （ GCP ）	• 任何兼容的 S3 基础架构（包括 Amazon S3 ） • Google Cloud Platform （ GCP ）
将对象移动到目标的原因是什么?	活动ILM策略中的一个或多个ILM规则。ILM 规则定义 StorageGRID 将哪些对象移动到云存储池以及何时移动这些对象。	将新对象插入已配置CloudMirror端点的源存储分段的操作。在为源存储分段配置CloudMirror端点之前、源存储分段中存在的对象不会进行复制、除非对其进行了修改。
如何检索对象?	应用程序必须向 StorageGRID 发出请求，以检索已移动到云存储池的对象。如果某个对象的唯一副本已过渡到归档存储，则 StorageGRID 会管理还原该对象的过程，以便可以检索该对象。	由于目标存储分段中的镜像副本是一个独立的副本，因此应用程序可以通过向 StorageGRID 或 S3 目标发出请求来检索对象。例如，假设您使用 CloudMirror 复制将对象镜像到合作伙伴组织。配对节点可以使用自己的应用程序直接从 S3 目标读取或更新对象。不需要使用 StorageGRID 。
是否可以直接从目标读取?	不可以。移动到云存储池的对象由StorageGRID管理。读取请求必须定向到 StorageGRID （ StorageGRID 将负责从云存储池中检索）。	可以，因为镜像副本是一个独立副本。
如果从源中删除对象，会发生什么情况?	此对象也会从云存储池中删除。	不会复制删除操作。已删除的对象不再位于 StorageGRID 存储分段中，但它仍位于目标存储分段中。同样，可以删除目标分段中的对象而不影响源。

	云存储池	**CloudMirror** 复制服务
发生灾难后如何访问对象（ StorageGRID 系统无法运行）？	必须恢复发生故障的 StorageGRID 节点。在此过程中，复制对象的副本可能会使用云存储池中的副本进行还原。	CloudMirror 目标中的对象副本独立于 StorageGRID ，因此可以在恢复 StorageGRID 节点之前直接访问这些副本。

在 **StorageGRID** 中创建云存储池

云存储池指定单个外部 Amazon S3 存储桶或其他 S3 兼容提供商或 Azure Blob Storage 容器。

创建云存储池时，您需要指定 StorageGRID 用于存储对象的外部存储分段或容器的名称和位置、云提供商类型（Amazon S3/GCP 或 Azure Blob Storage），以及 StorageGRID 访问该外部存储分段或容器所需的信息。

StorageGRID 会在您保存云存储池后立即对其进行验证，因此您必须确保云存储池中指定的存储分段或容器存在且可访问。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。
- 您已查看"云存储池注意事项"。
- 云存储池引用的外部存储分段或容器已存在，并且您已具有服务端点信息。
- 要访问存储分段或容器、您可以身份验证类型的帐户信息选择。

步骤

1. 选择* ILM **>***存储池>*云存储池*。
2. 选择*创建*，然后输入以下信息：

字段	说明
云存储池名称	一个名称，用于简要说明云存储池及其用途。在配置 ILM 规则时，请使用易于识别的名称。
提供程序类型	您将在此云存储池中使用哪个云提供商： • * Amazon S3/GCP*：为Amazon S3、Commercial Cloud Services (C2S) S3、Google Cloud Platform (GCP)或其他S3兼容提供商选择此选项。 • * Azure Blob 存储 *
存储分段或容器	外部S3存储分段或Azure容器的名称。保存云存储池后、您无法更改此值。

3. 根据您选择的Provider类型、输入服务端点信息。

Amazon S3/GCP

a. 对于协议、请选择HTTPS或HTTP。

> 不要对敏感数据使用HTTP连接。

b. 输入主机名。示例：

```
s3-aws-region.amazonaws.com
```

c. 选择URL样式：

选项	说明
自动检测	尝试根据提供的信息自动检测要使用的 URL 模式。例如，如果指定 IP 地址， StorageGRID 将使用路径模式的 URL 。仅当您不知道要使用哪种特定模式时，才选择此选项。
虚拟托管模式	使用虚拟托管样式的URL访问存储分段。虚拟托管样式的URL会在域名中包含分段名称。示例： `https://bucket-name.s3.company.com/key-name`
路径样式	使用路径模式 URL 访问存储分段。路径样式的URL末尾包含分段名称示例： `https://s3.company.com/bucket-name/key-name` *注意：*不建议使用路径样式的URL选项，此选项将在StorageGRID 的未来版本中弃用。

d. (可选)输入端口号、或者使用默认端口：443表示HTTPS、80表示HTTP。

Azure Blob存储

a. 使用以下格式之一输入服务端点的URI。

- `https://host:port`
- `http://host:port`

示例： `https://myaccount.blob.core.windows.net:443`

如果未指定端口、则默认情况下、端口443用于HTTPS、端口80用于HTTP。

4. [[authentication－account－info]]选择*继续*。然后选择身份验证类型、并为云存储池端点输入所需信息：

访问密钥

*for Amazon S3/GCP*或其他与*S3*兼容的提供程序

a. 访问密钥**ID**：输入拥有外部存储分段的帐户的访问密钥ID。
b. 机密访问密钥：输入机密访问密钥。

IAM角色无处不在

*for AWS IAM roles Anywhere*服务

StorageGRID可使用AWS安全令牌服务(STS)动态生成短生命令牌以访问AWS资源。

a. **AWS IAM**角色无处不在区域：选择云存储池所在的区域。例如， `us-east-1`。
b. 信任锚点**URN**：输入用于验证短期STS凭据请求的信任锚点的URN。可以是根CA、也可以是中间CA。
c. 配置文件**URN**：输入IAM角色Anywhere配置文件的URN，该配置文件列出了可假设任何受信任的角色。
d. 角色**URN**：输入IAM角色的URN、该URN可假设任何受信任的人。
e. 会话持续时间：输入临时安全凭据和角色会话的持续时间。输入至少15分钟且不超过12小时。
f. 服务器**CA**证书(可选)：一个或多个PEM格式的可信CA证书，用于在任意位置验证IAM角色。如果省略、则不会验证服务器。
g. **end-**实体 证书:由信任锚点签名的X509证书的公共密钥，采用PEM格式。AWS IAM roles Anywhere使用此密钥颁发STS令牌。
h. **end-**实体 专用密钥:最终实体证书的专用密钥。

CAP (C2S访问门户**)**

for Commercial Cloud Services (C2S) S3 service

a. 临时凭据**URL**：输入StorageGRID将用于从CAP服务器获取临时凭据的完整URL，包括分配给您的C2S帐户的所有必需和可选API参数。
b. 服务器**CA**证书：选择*浏览*并上传StorageGRID将用于验证CAP服务器的CA证书。证书必须采用PEM编码、并由相应的政府证书颁发机构(CA)颁发。
c. 客户端证书：选择*浏览*并将StorageGRID用于标识自身的证书上传到CAP服务器。客户端证书必须采用PEM编码、由相应的政府证书颁发机构(CA)颁发、并授予对C2S帐户的访问权限。
d. 客户端专用密钥：选择*浏览*并上传PEM编码的客户端证书专用密钥。
e. 如果客户端专用密钥已加密，请输入用于对客户端专用密钥进行解密的密码短语。否则，请将*客户端专用密钥密码短语*字段留空。

如果要对客户端证书进行加密、请使用传统格式进行加密。不支持PKCS #8加密格式。

Azure Blob存储

对于*Azure Blb*存储、仅共享密钥

a. 帐户名称：输入拥有外部容器的存储帐户的名称

b. 帐户密钥：输入存储帐户的机密密钥

您可以使用 Azure 门户查找这些值。

匿名

不需要追加信息。

5. 选择 * 继续 * 。然后选择要使用的服务器验证类型：

选项	说明
在存储节点操作系统中使用根CA证书	使用操作系统上安装的网格 CA 证书确保连接安全。
使用自定义 CA 证书	使用自定义 CA 证书。选择*浏览*并上传PEM编码的证书。
请勿验证证书	选择此选项意味着与云存储池的TLS连接不安全。

6. 选择 * 保存 * 。

保存云存储池时， StorageGRID 将执行以下操作：

- 验证存储分段或容器以及服务端点是否存在、以及是否可以使用您指定的凭据访问它们。
- 将标记文件写入存储分段或容器、以将其标识为云存储池。请勿删除名为的此文件 `x-ntap-sgws-cloud-pool-uuid`。

如果云存储池验证失败，您将收到一条错误消息，说明验证失败的原因。例如、如果存在证书错误或指定的存储分段或容器尚不存在、则可能会报告错误。

7. 如果发生错误，请参见"有关对云存储池进行故障排除的说明"，解决所有问题，然后再次尝试保存云存储池。

相关信息

"用于外部通信的端口"

在 StorageGRID 中查看云存储池详细信息

您可以查看云存储池的详细信息、以确定其使用位置以及包含哪些节点和存储级别。

开始之前

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

步骤

1. 选择* ILM >*存储池>*云存储池*。

"云存储池"表包含包含包含存储节点的每个云存储池的以下信息：

- **Name**：池的唯一显示名称。
- **URI**：云存储池的统一资源标识符。
- 提供商类型：此云存储池使用哪个云提供商。
- 容器：用于云存储池的存储分段的名称。
- **ILM usage**：当前使用池的方式。一个云存储池可能未使用、也可能用于一个或多个ILM规则、纠删编码配置文件或这两者。
- 上次错误：对此云存储池执行运行状况检查期间检测到的最后一次错误。

2. 要查看特定云存储池的详细信息、请选择其名称。

   此时将显示池的详细信息页面。

3. 查看*身份验证*选项卡、了解此云存储池的身份验证类型并编辑身份验证详细信息。
4. 查看*服务器验证*选项卡可了解验证详细信息、编辑验证、下载新证书或复制证书PEM。
5. 查看* ILM使用情况*选项卡以确定云存储池当前是否正在任何ILM规则或纠删编码配置文件中使用。
6. (可选)转到使用云存储池的* ILM规则页面*"了解并管理任何规则"。

在 **StorageGRID** 中编辑云存储池

您可以编辑云存储池以更改其名称、服务端点或其他详细信息；但是、您不能更改云存储池的S3存储分段或Azure容器。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 您已查看"云存储池注意事项"。

步骤

1. 选择* ILM >*存储池>*云存储池*。

   " 云存储池 " 表列出了现有的云存储池。

2. 选中要编辑的云存储池对应的复选框、然后选择*操作*>*编辑*。

   或者、选择云存储池的名称、然后选择*编辑*。

3. 根据需要更改云存储池名称、服务端点、身份验证凭据或证书验证方法。

   > 您不能更改云存储池的提供程序类型、S3存储分段或Azure容器。

   如果您以前上载了服务器证书或客户端证书，则可以展开“证书详细信息”可面面面面面，查看当前正在使用的证书。

4. 选择 * 保存 * 。

   保存云存储池时， StorageGRID 会验证存储分段或容器以及服务端点是否存在，以及是否可以使用您指定

的凭据访问它们。

如果云存储池验证失败，则会显示一条错误消息。例如，如果存在证书错误，则可能会报告错误。

请参见中的说明"对云存储池进行故障排除"、解决此问题、然后再次尝试保存云存储池。

删除 StorageGRID 中的云存储池

如果云存储池未在ILM规则中使用并且不包含对象数据、则可以将其删除。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。

如果需要、请使用ILM移动对象数据

如果要删除的云存储池包含对象数据、则必须使用ILM将数据移动到其他位置。例如、您可以将数据移动到网格上的存储节点或其他云存储池。

步骤

1. 选择* ILM >*存储池>*云存储池*。
2. 查看表中的ILM使用情况列、确定是否可以删除云存储池。

   如果云存储池正在ILM规则或纠删编码配置文件中使用、则不能将其删除。

3. 如果正在使用云存储池、请选择*云存储池名称_*>* ILM usage*。
4. "克隆每个ILM规则"此操作当前会将对象放置在要删除的云存储池中。
5. 确定要将由您克隆的每个规则管理的现有对象移动到的位置。

   您可以使用一个或多个存储池、也可以使用其他云存储池。

6. 编辑已克隆的每个规则。

   对于创建ILM规则向导的步骤2、请从*副本位置*字段中选择新位置。

7. "创建新的ILM策略"并将每个旧规则替换为克隆的规则。
8. 激活新策略。
9. 等待ILM从云存储池中删除对象并将其放置在新位置。

删除云存储池

如果云存储池为空且未在任何ILM规则中使用、则可以将其删除。

开始之前

- 您已删除可能已使用该池的任何ILM规则。
- 您已确认 S3 存储分段或 Azure 容器不包含任何对象。

如果您尝试删除包含对象的云存储池，则会发生错误。请参阅。 "对云存储池进行故障排除"

> 创建云存储池时， StorageGRID 会将标记文件写入存储分段或容器，以将其标识为云存储池。不要删除名为的文件 `x-ntap-sgws-cloud-pool-uuid`。

步骤

1. 选择* ILM >*存储池>*云存储池*。
2. 如果ILM使用情况列指示未使用云存储池、请选中此复选框。
3. 选择 * 操作 * > * 删除 * 。
4. 选择 * 确定 * 。

对 **StorageGRID** 中的云存储池进行故障排除

使用这些故障排除步骤可帮助解决在创建、编辑或删除云存储池时可能遇到的错误。

确定是否发生错误

StorageGRID通过读取已知对象对每个云存储池执行简单的运行状况检查 `x-ntap-sgws-cloud-pool-uuid`、以确保可以访问云存储池且该池运行正常。当StorageGRID在端点上遇到错误时、它会每分钟从每个存储节点执行一次运行状况检查。解决错误后、运行状况检查将停止。如果运行状况检查检测到问题、则会在"存储池"页面上的"云存储池"表的"最后一个错误"列中显示一条消息。

此表显示了为每个云存储池检测到的最新错误，并指示错误发生的时间。

此外，如果运行状况检查检测到在过去 5 分钟内发生了一个或多个新的 Cloud Storage Pool 错误，则会触发 * 云存储池连接错误 * 警报。如果您收到有关此警报的电子邮件通知、请转到存储池页面(选择* ILM >*存储池)、查看最后一个错误列中的错误消息、并参阅下面的故障排除准则。

检查错误是否已解决

解决任何底层问题后，您可以确定错误是否已解决。从云存储池页面中、选择端点、然后选择*清除错误*。确认消息指示 StorageGRID 已清除云存储池的错误。

如果根本问题已解决，则不再显示此错误消息。但是、如果根本问题尚未修复(或者遇到其他错误)、则错误消息将在几分钟内显示在Last error列中。

错误：运行状况检查失败。端点出错

在以下情况下，您可能会遇到此错误：

- 当您开始将此存储桶用于云存储池后，为 Amazon S3 存储桶启用具有默认保留的 S3 对象锁定时。当 PUT 操作没有包含有效负载校验和值的 HTTP 标头（例如 `Content-MD5`）时，会出现此错误。AWS 要求将此标头值用于对启用了 S3 对象锁定的存储桶执行的 PUT 操作。

  要解决此问题，请按照 "编辑云存储池" 中的步骤操作，无需进行任何更改。此操作会触发对云存储池配置的验证，该配置会自动检测和更新云存储池端点配置上的 S3 对象锁定标志。

- 当您开始将此存储桶用于云存储池后，为 StorageGRID S3 存储桶启用具有默认保留的 S3 对象锁定时。

  要解决此问题：

- 如果您使用的是 HTTP：不支持启用 S3 对象锁定的云存储池。请编辑端点连接以改用 HTTPS。
- 如果您使用的是 HTTPS：请按照 "编辑云存储池" 中的步骤操作，无需进行任何更改。此操作将触发对云存储池配置的验证，该验证会自动检测并更新云存储池端点配置上的 S3 Object Lock 标志。

如果还有其他问题，请与技术支持联系。

错误：此云存储池包含意外内容

尝试创建，编辑或删除云存储池时，可能会遇到此错误。如果存储分段或容器包含标记文件、但该文件的元数据字段不具有预期的UUID、则会发生此错误 `x-ntap-sgws-cloud-pool-uuid`。

通常，只有在创建新的云存储池且另一个 StorageGRID 实例已使用同一个云存储池时，您才会看到此错误。

请尝试以下步骤之一来解决此问题：

- 如果要配置新的云存储池、并且存储分段包含与以下示例类似的文件和其他对象密钥、请创建一个新存储分段并改用此新存储 `x-ntap-sgws-cloud-pool-uuid`分段。

  附加对象键的示例： `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- 如果 `x-ntap-sgws-cloud-pool-uuid`文件是存储分段中的唯一对象、请删除此文件。

如果这些步骤不适用于您的情形、请联系支持部门。

错误：无法创建或更新云存储池。端点出错

在以下情况下、您可能会遇到此错误：

- 尝试创建或编辑云存储池时。
- 在配置新的云存储池期间选择不受支持的平台、身份验证或协议与S3对象锁定的组合。请参阅。 "云存储池注意事项"

此错误表示连接或配置问题导致StorageGRID无法写入云存储池。

要更正问题描述 ，请查看来自端点的错误消息。

- 如果错误消息包含 `Get *url*: EOF`，请检查用于云存储池的服务端点是否不对需要HTTPS的容器或分段使用HTTP。
- 如果错误消息包含 `Get *url*: net/http: request canceled while waiting for connection` ，请验证网络配置是否允许存储节点访问用于云存储池的服务端点。
- 如果此错误是由于不受支持的平台、身份验证或协议导致的、请使用S3对象锁定更改为受支持的配置、然后再次尝试保存新的云存储池。
- 对于所有其他端点错误消息，请尝试以下一项或多项操作：
  - 创建一个与您为云存储池输入的名称相同的外部容器或存储分段，然后再次尝试保存新的云存储池。
  - 更正为云存储池指定的容器或存储分段名称，然后重新尝试保存新的云存储池。

错误：无法解析 **CA** 证书

在尝试创建或编辑云存储池时，您可能会遇到此错误。如果 StorageGRID 无法解析您在配置云存储池时输入的

证书，则会发生此错误。

要更正问题描述 ，请检查您提供的 CA 证书是否存在问题。

错误：未找到具有此 ID 的云存储池

尝试编辑或删除云存储池时，可能会遇到此错误。如果端点返回 404 响应，则会发生此错误，这可能表示以下任一项：

- 用于云存储池的凭据没有此存储分段的读取权限。
- 用于云存储池的存储分段不包括 `x-ntap-sgws-cloud-pool-uuid`标记文件。

尝试以下一个或多个步骤以更正问题描述：

- 检查与配置的访问密钥关联的用户是否具有所需权限。
- 使用具有所需权限的凭据编辑云存储池。
- 如果权限正确，请联系支持部门。

错误：无法检查云存储池的内容。端点出错

在尝试删除云存储池时，您可能会遇到此错误。此错误表示某种类型的连接或配置问题描述 正在阻止 StorageGRID 读取云存储池存储分段的内容。

要更正问题描述 ，请查看来自端点的错误消息。

错误：对象已放置在此存储分段中

在尝试删除云存储池时，您可能会遇到此错误。如果云存储池包含通过ILM移动到该存储池的数据、在配置云存储池之前存储分段中的数据或在创建云存储池之后由其他源放置在分段中的数据、则不能删除该数据。

尝试以下一个或多个步骤以更正问题描述：

- 按照"云存储池对象的生命周期"中有关将对象移回StorageGRID的说明进行操作。
- 如果您确定其余对象未被 ILM 放置在云存储池中，请手动从存储分段中删除这些对象。

> 切勿手动删除云存储池中可能已由 ILM 放置的对象。如果稍后尝试从 StorageGRID 访问手动删除的对象，则找不到已删除的对象。

错误：代理尝试访问云存储池时遇到外部错误

如果您在存储节点与用于云存储池的外部S3端点之间配置了非透明存储代理、则可能会遇到此错误。如果外部代理服务器无法访问云存储池端点、则会发生此错误。例如， DNS 服务器可能无法解析主机名，或者可能存在外部网络问题描述 。

尝试以下一个或多个步骤以更正问题描述：

- 检查云存储池（ * ILM * > * 存储池 * ）的设置。
- 检查存储代理服务器的网络配置。

错误：**X.509**证书已超出有效期

在尝试删除云存储池时，您可能会遇到此错误。如果身份验证需要X.509证书来确保正确的外部云存储池已通过验证、并且在删除云存储池配置之前外部池为空、则会发生此错误。

请尝试以下步骤以更正问题描述：

- 更新为向云存储池进行身份验证而配置的证书。
- 确保已解决此云存储池上的任何证书到期警报。

相关信息

"云存储池对象的生命周期"

在 StorageGRID 中管理纠删编码配置文件

您可以查看纠删编码配置文件的详细信息、并根据需要重命名配置文件。如果纠删编码配置文件当前未在任何ILM规则中使用、则可以停用该配置文件。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。

查看纠删编码配置文件详细信息

您可以查看纠删编码配置文件的详细信息、以确定其状态、使用的纠删编码方案以及其他信息。

步骤

1. 选择*配置* > 系统 > 擦除编码。
2. 选择配置文件。此时将显示配置文件的详细信息页面。
3. (可选)查看ILM规则选项卡、查看使用配置文件的ILM规则列表以及使用这些规则的ILM策略。
4. (可选)查看存储节点选项卡、以了解有关配置文件存储池中每个存储节点的详细信息、例如存储节点所在的站点以及存储使用情况。

重命名纠删编码配置文件

您可能需要重命名纠删编码配置文件、使其更清楚地显示该配置文件的功能。

步骤

1. 选择*配置* > 系统 > 擦除编码。
2. 选择要重命名的配置文件。
3. 选择 * 重命名 * 。
4. 为纠删编码配置文件输入一个唯一名称。

   纠删编码配置文件名称会附加到ILM规则放置指令中的存储池名称中。

纠删编码配置文件名称必须唯一。如果您使用现有配置文件的名称，则会发生验证错误，即使该配置文件已停用也是如此。

5. 选择 * 保存 * 。

停用纠删编码配置文件

如果您不再计划使用纠删编码配置文件、并且该配置文件当前未在任何ILM规则中使用、则可以停用该配置文件。

确认当前未执行任何经过删除编码的数据修复操作或停用过程。如果在执行其中任一操作期间尝试停用纠删编码配置文件、则会返回错误消息。

关于此任务

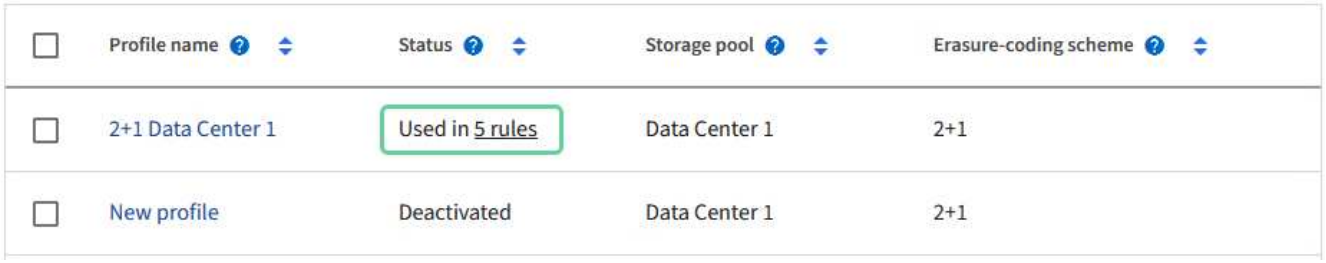
如果满足以下任一条件、StorageGRID将阻止您停用纠删编码配置文件：

- 纠删编码配置文件当前在ILM规则中使用。
- 纠删编码配置文件不再用于任何ILM规则、但该配置文件的对象数据和奇偶校验片段仍然存在。

步骤

1. 选择*配置* > 系统 > 擦除编码。
2. 在Active选项卡上、查看*状态*列、确认要停用的纠删编码配置文件未在任何ILM规则中使用。

   如果纠删编码配置文件在任何ILM规则中使用、则无法停用该配置文件。在此示例中、至少在一个ILM规则中使用2+1数据中心1配置文件。



3. 如果在 ILM 规则中使用配置文件，请执行以下步骤：
   a. 选择 * ILM * > * 规则 * 。
   b. 选择每个规则并查看保留图、以确定该规则是否使用要停用的纠删编码配置文件。
   c. 如果ILM规则使用要停用的纠删编码配置文件、请确定是否在任何ILM策略中使用此规则。
   d. 根据纠删编码配置文件的使用位置、完成表中的其他步骤。

此配置文件已在何处使用？	停用配置文件前要执行的其他步骤	请参见这些附加说明
从不在任何 ILM 规则中使用	无需执行其他步骤。继续执行此操作步骤。	无 _

此配置文件已在何处使用?	停用配置文件前要执行的其他步骤	请参见这些附加说明
在从未在任何 ILM 策略中使用过的 ILM 规则中	i. 编辑或删除所有受影响的 ILM 规则。如果编辑规则、请删除使用纠删编码配置文件的所有放置。 ii. 继续执行此操作步骤。	"使用 ILM 规则和 ILM 策略"
在当前处于活动状态的ILM策略中的ILM规则中	i. 克隆策略。 ii. 删除使用纠删编码配置文件的ILM规则。 iii. 添加一个或多个新 ILM 规则以确保对象受到保护。 iv. 保存，模拟和激活新策略。 v. 等待应用新策略，并根据添加的新规则将现有对象移动到新位置。 ◦ 注意： * 根据对象数量和 StorageGRID 系统的大小， ILM 操作可能需要数周甚至数月才能根据新的 ILM 规则将对象移动到新位置。 虽然您可以安全地尝试停用仍与数据关联的纠删编码配置文件、但停用操作将失败。如果配置文件尚未准备好停用，则会显示一条错误消息通知您。 vi. 编辑或删除从策略中删除的规则。如果编辑规则、请删除使用纠删编码配置文件的所有放置。 vii. 继续执行此操作步骤。	"创建ILM策略" "使用 ILM 规则和 ILM 策略"
在ILM策略中的当前ILM规则中	i. 编辑策略。 ii. 删除使用纠删编码配置文件的ILM规则。 iii. 添加一个或多个新的 ILM 规则以确保所有对象均受保护。 iv. 保存策略。 v. 编辑或删除从策略中删除的规则。如果编辑规则、请删除使用纠删编码配置文件的所有放置。 vi. 继续执行此操作步骤。	"创建ILM策略" "使用 ILM 规则和 ILM 策略"

e. 刷新纠删编码配置文件页面、以确保此配置文件未在ILM规则中使用。

4. 如果在 ILM 规则中未使用该配置文件，请选择单选按钮并选择 * 停用 * 。此时将显示停用纠删编码配置文件对话框。

   您可以同时选择多个要停用的配置文件、只要每个配置文件未在任何规则中使用即可。

5. 如果确实要停用此配置文件，请选择 * 停用 * 。

结果

- 如果StorageGRID能够停用纠删编码配置文件、则其状态为已停用。您不能再为任何 ILM 规则选择此配置文件。您无法重新激活已停用的配置文件。
- 如果 StorageGRID 无法停用此配置文件，则会显示一条错误消息。例如，如果对象数据仍与此配置文件关联，则会显示一条错误消息。您可能需要等待几周才能再次尝试停用过程。

为StorageGRID配置 S3 区域

ILM 规则可以根据创建 S3 存储桶的可选区域过滤对象，从而允许您将来自不同区域的对象存储在不同的存储位置。

如果要在规则中使用 S3 分段区域作为筛选器，则必须先创建可由系统中的分段使用的区域。

> 创建存储分段后、您不能更改存储分段的区域。

开始之前

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

关于此任务

创建 S3 存储分段时，您可以指定在特定区域创建存储分段。通过指定区域，存储分段可以在地理位置上靠近用户，从而有助于优化延迟，最大限度地降低成本并满足法规要求。

创建 ILM 规则时，您可能需要使用与 S3 存储分段关联的区域作为高级筛选器。例如、您可以设计一个仅适用于在区域中创建的S3存储分段中的对象的规则 `us-west-2`。然后，您可以指定将这些对象的副本放置在该区域内数据中心站点的存储节点上，以优化延迟。

配置区域时，请遵循以下准则：

- 默认情况下、所有存储分段均视为属于该 `us-east-1`区域。
- 您必须先使用网格管理器创建区域，然后才能在使用租户管理器或租户管理 API 创建存储桶时指定非默认区域，或者使用 S3 PUT Bucket API 请求的 LocationConstraint 请求元素指定非默认区域。如果 PUT Bucket 请求使用StorageGRID中未定义的区域，则会发生错误。
- 创建 S3 存储分段时，必须使用确切的区域名称。区域名称区分大小写。有效字符包括数字，字母和连字符。

  > EU 不被视为 eu-west-1 的别名。如果您想使用 EU 或 eu-west-1 区域，则必须使用准确的名称。

- 如果某个区域在分配给任何策略(活动或非活动)的规则中使用、则无法删除或修改该区域。
- 如果在ILM规则中使用无效区域作为高级筛选器、则无法将该规则添加到策略中。

  如果您在 ILM 规则中使用某个区域作为高级过滤器但后来删除了该区域，或者您使用网格管理 API 创建规则并指定了未定义的区域，则可能会导致区域无效。

- 如果在使用某个区域创建 S3 存储分段后将其删除，则如果您要使用位置限制高级筛选器查找该存储分段中的对象，则需要重新添加该区域。

步骤

1. 选择 * ILM * > * 区域 * 。

   出现“区域”页面。

2. 选择“所有区域”或“默认区域”选项卡。

   所有地区

   *所有区域*选项卡列出了当前定义的区域，包括定义的默认区域。

   > 您无法删除或修改“所有区域”选项卡中的默认区域。使用“默认区域”选项卡来更改默认区域。

   a. 要添加区域，请选择“添加另一个区域”。
   b. 输入要在创建 S3 存储分段时使用的区域名称。

      在创建相应的 S3 存储分段时，您必须使用此确切的区域名称作为 LocationConstraint 请求元素。

   c. 要删除未使用的区域，请选择删除图标 ✕。

      如果您尝试删除当前在任何策略(活动或非活动)中使用的区域、则会显示一条错误消息。

   d. 完成更改后，选择 * 保存 * 。

      现在、您可以从创建ILM规则向导的步骤1中的高级筛选器部分选择这些区域。请参阅。 "在 ILM 规则中使用高级筛选器"

   默认区域

   *默认区域*选项卡显示当前定义的默认区域，您可以修改它。

   a. 要更改默认区域，请从“默认区域”下拉列表中的可用选项中选择区域名称。
   b. 选择 * 保存 * 。

创建 **ILM** 规则

了解 **StorageGRID** 中的 **ILM** 规则

要管理对象，您需要创建一组信息生命周期管理（ ILM ）规则，并将其组织到 ILM 策略中。

系统中载入的每个对象都会根据活动策略进行评估。如果策略中的规则与对象的元数据匹配，则规则中的说明将确定 StorageGRID 复制和存储该对象所采取的操作。

> 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。

ILM 规则的要素

ILM 规则包含三个要素：

- * 筛选条件 * ：规则的基本和高级筛选器用于定义规则适用场景 的对象。如果某个对象与所有筛选器匹配，则 StorageGRID 将应用此规则并创建在规则的放置说明中指定的对象副本。
- * 放置说明 * ：规则的放置说明用于定义对象副本的数量，类型和位置。每个规则都可以包含一系列放置说明，以便随着时间的推移更改对象副本的数量，类型和位置。一个放置的时间段到期后，下一个放置中的说明将自动应用于下一个 ILM 评估。
- *Ingest behavior *：通过规则的加网行为、您可以选择在加网时(S3客户端将对象保存到网格时)如何保护按规则筛选的对象。

ILM规则筛选

创建 ILM 规则时，您可以指定筛选器来标识规则适用场景 的对象。

最简单的情况是，规则可能不使用任何筛选器。任何不使用筛选器适用场景 all 对象的规则，因此它必须是 ILM 策略中的最后一个（默认）规则。默认规则为与其他规则中的筛选器不匹配的对象提供存储指令。

- 通过基本筛选器，您可以对不同的大型对象组应用不同的规则。通过这些筛选器、您可以将规则应用于特定租户帐户、特定S3存储分段或这两者。

  通过基本筛选器、您可以轻松地将不同的规则应用于大量对象。例如，您公司的财务记录可能需要存储以满足法规要求，而营销部门的数据则可能需要存储以方便日常运营。在为每个部门创建单独的租户帐户后，或者将不同部门的数据隔离到单独的 S3 存储分段后，您可以轻松创建适用场景 一个规则来记录所有财务记录，并创建另一个适用场景 规则来记录所有营销数据。

- 高级筛选器让您可以进行精细控制。您可以创建筛选器，以便根据以下对象属性选择对象：
  - 载入时间
  - 上次访问时间
  - 全部或部分对象名称（密钥）
  - 位置限制(仅限S3)
  - 对象大小
  - 用户元数据
  - 对象标记(仅限S3)

您可以按非常具体的条件筛选对象。例如，医院成像部门存储的对象在使用不到 30 天时可能会频繁使用，而在使用之后则很少使用，而包含患者就诊信息的对象可能需要复制到健康网络总部的计费部门。您可以创建筛选器，根据对象名称，大小， S3 对象标记或任何其他相关标准来标识每种类型的对象，然后创建单独的规则以适当存储每组对象。

您可以根据需要在一个规则中组合筛选器。例如，营销部门可能希望以不同于供应商记录的方式存储大型映像文件，而人力资源部门可能需要将人员记录集中存储在特定地理位置和策略信息中。在这种情况下、您可以创建按租户帐户筛选的规则、以便将记录与每个部门隔离、同时在每个规则中使用筛选器来标识规则适用场景 所对应的特定对象类型。

放置说明用于确定对象数据的存储位置，存储时间和存储方式。一个 ILM 规则可以包含一个或多个放置指令。每个放置指令适用场景 都有一段时间。

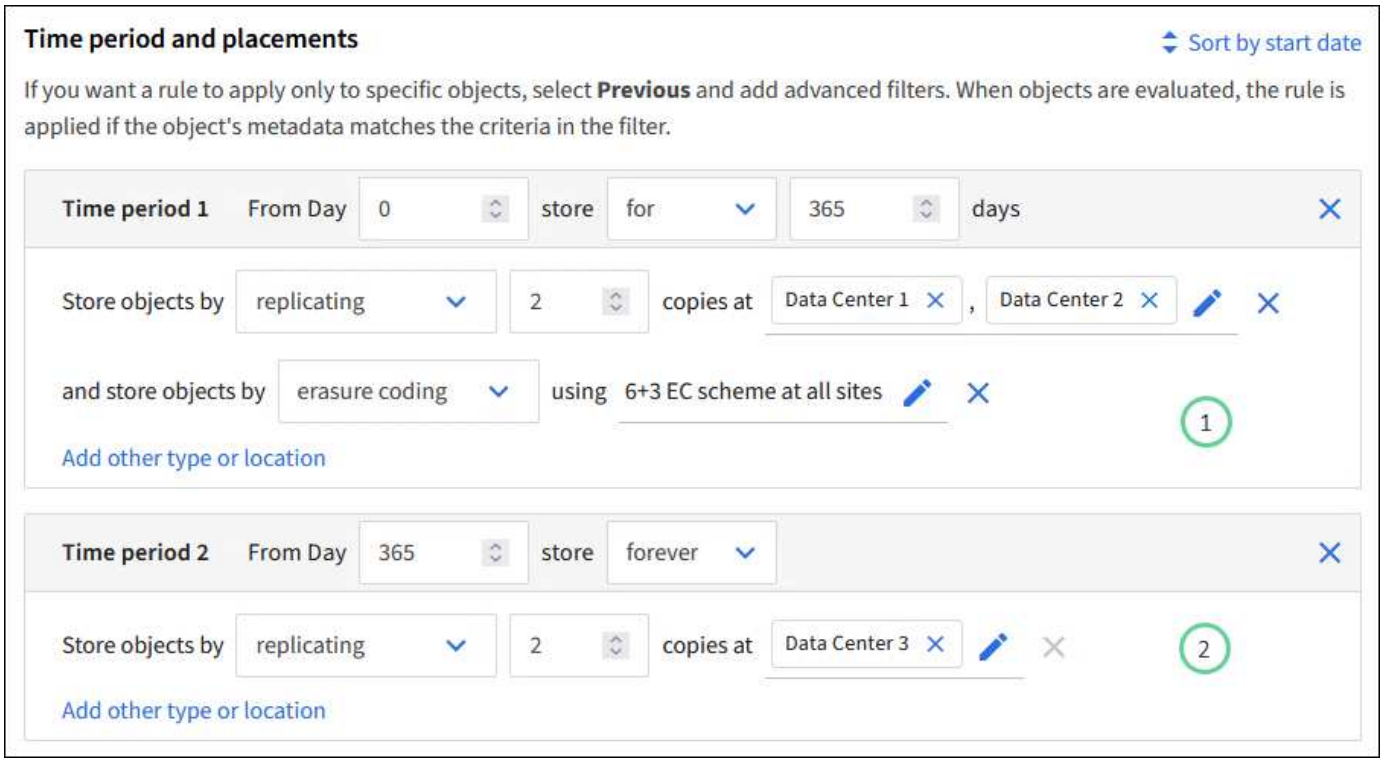
创建放置说明时：

- 首先指定参考时间，该时间决定放置指令的开始时间。参考时间可能是：载入对象时，访问对象时，受版本控制的对象变为非当前状态时或用户定义的时间。
- 接下来，您可以指定相对于参考时间应用放置的时间。例如，放置可能从第 0 天开始，并持续 365 天，与对象载入的时间相关。
- 最后，您可以指定副本的类型（复制或纠删编码）以及副本的存储位置。例如，您可能希望将两个复制副本存储在两个不同的站点上。

每个规则可以定义一个时间段内的多个放置位置，也可以定义不同时间段的不同放置位置。

- 要在一个时间段内将对象放置在多个位置，请选择*添加其他类型或位置*，为该时间段添加多行。
- 要将对象放置在不同时间段的不同位置，请选择*添加另一时间段*以添加下一时间段。然后，指定时间段内的一个或多个行。

此示例在创建ILM规则向导的定义放置页面上显示了两个放置说明。



第一个放置指令 (1) 在第一年有两行：

- 第一行会在两个数据中心站点创建两个复制的对象副本。
- 第二行使用所有数据中心站点创建6+3经过删除的副本。

第二份放置说明 (2) 在一年后创建两份副本，并永久保留这些副本。

为规则定义一组放置指令时，必须确保至少有一个放置指令从第 0 天开始，并且定义的时间段之间没有空隙，最终放置指令将永久持续，或者一直持续到您不再需要任何对象副本为止。

规则中的每个时间段到期后，将应用下一时间段的内容放置说明。此时将创建新的对象副本，并删除任何不需要的副本。

ILM规则加热行为

载入行为用于控制是否按照规则中的说明立即放置对象副本，或者是否创建了临时副本并稍后应用放置说明。ILM 规则可以使用以下载入行为：

- * 平衡 * ： StorageGRID 尝试在载入时创建 ILM 规则中指定的所有副本；如果无法创建，则创建临时副本并将成功返回给客户端。在可能的情况下，将创建 ILM 规则中指定的副本。
- * 严格 * ：必须创建 ILM 规则中指定的所有副本，才能将成功返回给客户端。
- *Dual Commit *：StorageGRID 会立即创建对象的临时副本并将成功结果返回给客户端。如果可能，将创建 ILM 规则中指定的副本。

相关信息

- "加热选项"
- "加热选项的优点、缺点和限制"
- "一致性和ILM规则如何相互作用以影响数据保护"

ILM 规则示例

例如、ILM规则可以指定以下内容：

- 仅应用于属于租户A的对象
- 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。
- 将这两个副本保留为"永久"、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。
- 使用均衡选项进行加载行为：租户A将对象保存到StorageGRID 后立即应用双站点放置指令、除非无法立即创建两个所需的副本。

  例如，如果租户 A 保存对象时无法访问站点 2 ，则 StorageGRID 将在站点 1 的存储节点上创建两个临时副本。一旦站点 2 可用， StorageGRID 就会在该站点创建所需的副本。

相关信息

- "什么是存储池"
- "什么是云存储池"

访问 StorageGRID 中的创建 ILM 规则向导

您可以通过 ILM 规则管理对象数据随时间的放置。要创建ILM规则、请使用创建ILM规则向导。

如果要为策略创建默认ILM规则、请改用。"有关创建默认ILM规则的说明"

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。
- 如果要指定此规则适用于哪些租户帐户、您拥有"租户帐户权限"或知道每个帐户的帐户ID。
- 如果希望规则按上次访问时间元数据筛选对象、则必须通过S3存储分段启用上次访问时间更新。
- 您已配置计划使用的任何云存储池。请参阅。 "创建云存储池"
- 您熟悉"加热选项"。
- 如果需要创建与S3对象锁定配合使用的合规规则，则您熟悉"S3 对象锁定的要求"。
- 或者，您已经观看了视频：

  ILM 规则概述

关于此任务

创建 ILM 规则时：

- 请考虑 StorageGRID 系统的拓扑和存储配置。
- 考虑要创建哪些类型的对象副本(复制或删除编码)以及所需的每个对象的副本数。
- 确定连接到 StorageGRID 系统的应用程序中使用的对象元数据类型。ILM 规则根据对象的元数据筛选对象。
- 请考虑随时间推移对象副本的放置位置。
- 确定要使用的加网选项(均衡、严格或双重提交)。

步骤

1. 选择 * ILM * > * 规则 * 。
2. 选择 * 创建 * 。"第1步(输入详细信息)"的创建ILM规则向导。

输入 **StorageGRID ILM** 规则的详细信息和筛选器

通过创建ILM规则向导的*输入详细信息*步骤、您可以输入规则的名称和问题描述 、并为规则定义筛选器。

输入问题描述 并为规则定义筛选器是可选的。

关于此任务

根据评估对象时"ILM规则"，StorageGRID会将对象元数据与规则的筛选器进行比较。如果对象元数据与所有筛选器匹配， StorageGRID 将使用规则放置对象。您可以设计一个规则以应用于所有对象，也可以指定基本筛选器，例如一个或多个租户帐户或分段名称，或者指定高级筛选器，例如对象的大小或用户元数据。

步骤

1. 在 * 名称 * 字段中输入规则的唯一名称。
2. 或者，也可以在 * 问题描述 * 字段中为此规则输入一个短问题描述 。

   您应说明此规则的目的或功能，以便稍后识别此规则。

3. (可选)选择一个或多个应用此规则的S3租户帐户。如果此规则为所有租户添加适用场景 ，请将此字段留空。

   如果您既没有root访问权限、也没有租户帐户权限、则无法从列表中选择租户。而是输入租户 ID 或输入多个 ID 作为逗号分隔的字符串。

4. (可选)指定此规则适用的S3分段。

   如果选择了*应用于所有存储分段*(默认)、则此规则将应用于所有S3存储分段。

5. 对于S3租户、可选择*是*以仅将此规则应用于已启用版本控制的S3存储分段中的较早对象版本。

   如果您选择*Yes*，将自动为中的参考时间选择“非当前时间”"创建ILM规则向导的第2步"。

   > 非当前时间仅适用于启用了版本控制的分段中的S3对象。请参阅"存储分段操作、PutBucketVersioning"和"使用 S3 对象锁定管理对象"。

   您可以使用此选项通过筛选非当前对象版本来减少受版本控制的对象的存储影响。请参阅。 "示例 4： S3 版本对象的 ILM 规则和策略"

6. (可选)选择*添加高级筛选器*以指定其他筛选器。

   如果不配置高级筛选、则规则适用场景 all objects that match the Basic Filters.有关高级筛选的详细信息，请参见在 ILM 规则中使用高级筛选器和[指定多个元数据类型和值]。

7. 选择 * 继续 * 。"第2步(定义放置位置)"的创建ILM规则向导。

在 **ILM** 规则中使用高级筛选器

通过高级筛选功能，您可以创建仅根据特定对象的元数据应用于特定对象的 ILM 规则。为规则设置高级筛选时，您可以选择要匹配的元数据类型，选择运算符并指定元数据值。评估对象时， ILM 规则仅应用于元数据与高级筛选器匹配的对象。

下表显示了您可以在高级筛选器中指定的元数据类型，可用于每种元数据类型的运算符以及预期的元数据值。

元数据类型	支持的运算符	元数据值
载入时间	• 为 • 不是 • 之前 • 已开启或早于 • 之后 • 开启或之后	载入对象的时间和日期。 *注意：*为避免激活新ILM策略时出现资源问题、您可以在任何可能更改大量现有对象位置的规则中使用"Ingesg"时间高级筛选器。将"Inged Time (启动时间)"设置为大于或等于新策略生效的大致时间、以确保现有对象不会发生不必要的移动。

元数据类型	支持的运算符	元数据值
密钥	• 等于 • 不等于 • 包含 • 不包含 • 开头为 • 不以开头 • 结尾为 • 结尾不为	唯一S3对象密钥的全部或部分。 例如，您可能希望匹配以结尾或以开头的 `test-object/`对象 `.txt`。
上次访问时间	• 为 • 不是 • 之前 • 已开启或早于 • 之后 • 开启或之后	上次检索（读取或查看）对象的时间和日期。 *注意：*如果您计划"使用上次访问时间"作为高级筛选器、则必须为S3存储分段启用上次访问时间更新。
位置限制(仅限S3)	• 等于 • 不等于	创建 S3 存储分段的区域。使用 * ILM * > * 区域 * 定义显示的区域。 注意： us-east-1 的值将匹配在 us-east-1 区域创建的存储桶中的对象以及未指定区域的存储桶中的对象。看"配置 S3 区域" 。
对象大小	• 等于 • 不等于 • 小于 • 小于或等于 • 大于 • 大于或等于	对象的大小。 纠删编码最适合大于 1 MB 的对象。不要对小于200 KB的对象使用纠删编码、以避免管理非常小的经过纠删编码的片段所产生的开销。

元数据类型	支持的运算符	元数据值
用户元数据	• 包含 • 结尾为 • 等于 • exists • 开头为 • 不包含 • 结尾不为 • 不等于 • 不存在 • 不以开头	键值对，其中*User metadata"是键，*Metadata"是值。 例如，要按用户元数据为的对象进行筛选 `color=blue`，请为*用户元数据名称*、 `equals`运算符和 `blue`*元数据值*指定 `color`。 *注意：*用户元数据名称不区分大小写；用户元数据值区分大小写。
对象标记(仅限S3)	• 包含 • 结尾为 • 等于 • exists • 开头为 • 不包含 • 结尾不为 • 不等于 • 不存在 • 不以开头	键值对，其中*Object tag name*是键，*Object tag value*是值。 例如，要筛选对象标记为的对象 `Image=True`，请指定 `Image`**Object tag name**、运算符和*Object tag value* `equals`。 `True` • 注： * 对象标记名称和对象标记值区分大小写。您必须严格按照为对象定义的方式输入这些项。

指定多个元数据类型和值

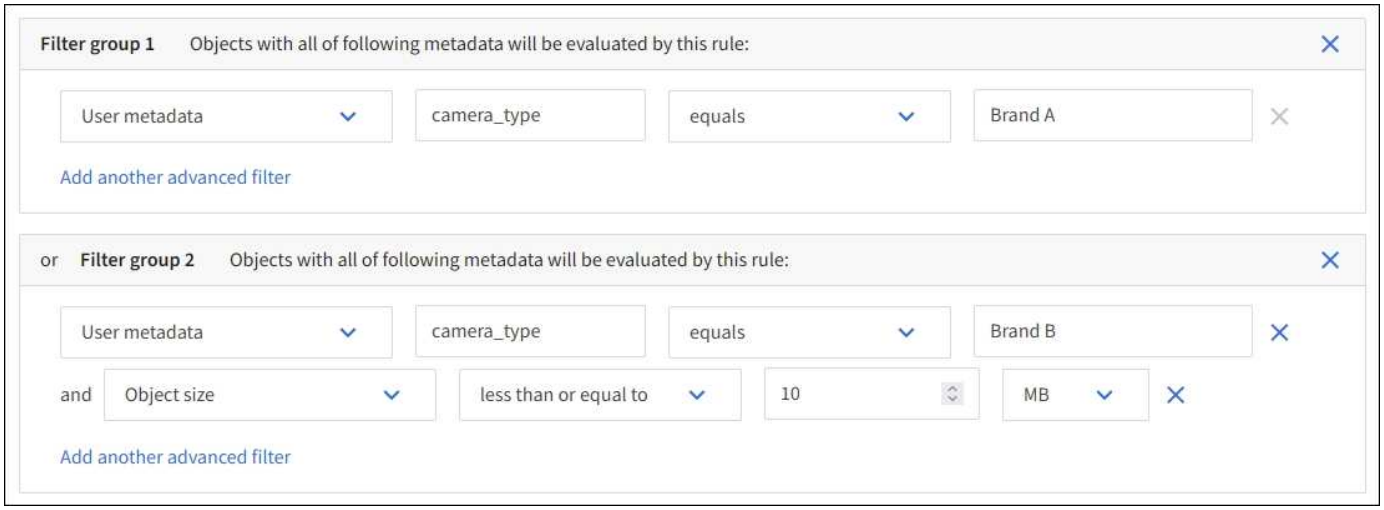
定义高级筛选时，您可以指定多种类型的元数据和多个元数据值。例如，如果希望规则匹配大小介于10 MB到100 MB之间的对象，则应选择*Object Size*元数据类型并指定两个元数据值。

- 第一个元数据值用于指定大于或等于 10 MB 的对象。
- 第二个元数据值用于指定小于或等于 100 MB 的对象。



使用多个条目可以精确控制匹配的对象。在以下示例中、规则适用场景对象使用品牌A或品牌B作为摄像机类型

用户元数据的值。但是，规则仅对小于 10 MB 的品牌 B 对象执行适用场景 。



定义 **StorageGRID ILM** 规则的放置说明

通过创建ILM规则向导的*定义放置位置*步骤、您可以定义放置说明、这些放置说明确定对象的存储时长、副本类型(已复制或已删除编码)、存储位置以及副本数量。

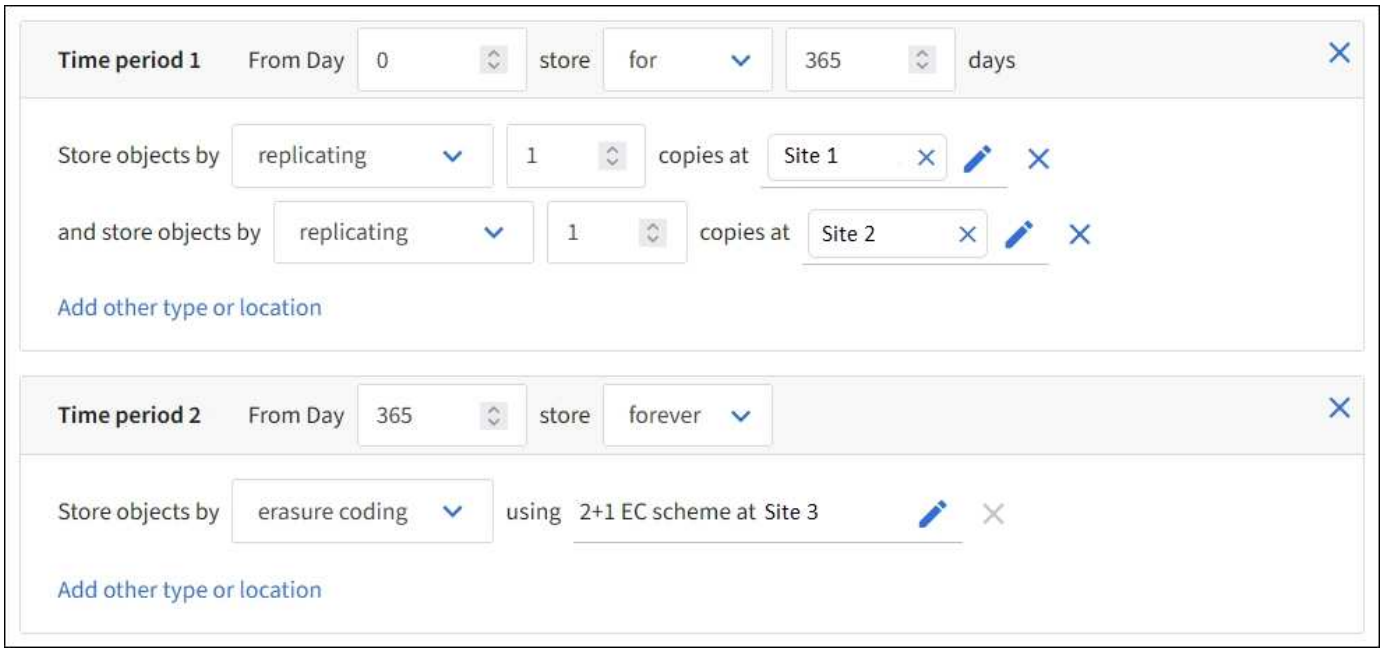
所示屏幕截图仅为示例。结果可能因StorageGRID版本而异。

关于此任务

一个 ILM 规则可以包含一个或多个放置指令。每个放置指令适用场景 都有一段时间。如果使用多个指令，则时间段必须是连续的，并且至少有一个指令必须从第 0 天开始。这些说明可以永久继续，也可以一直持续到不再需要任何对象副本为止。

如果要在该时间段内创建不同类型的副本或使用不同的位置，则每个放置指令可以包含多行。

在此示例中、ILM规则会在第一年将一个复制副本存储在站点1中、并将一个复制副本存储在站点2中。一年后，将创建 2+1 纠删编码副本，并仅保存在一个站点上。



步骤

1. 对于*参考时间*，选择在计算放置指令的开始时间时要使用的时间类型。

选项	说明
载入时间	对象的载入时间。
上次访问时间	上次检索（读取或查看）对象的时间。 要使用此选项、必须为S3存储分段启用上次访问时间更新。请参阅 "在ILM规则中使用上次访问时间"。
用户定义的创建时间	在用户定义的元数据中指定的时间。
非当前时间	如果您在中为问题“仅将此规则应用于较旧的对象版本(在启用了版本控制的S3存储分段中)？”选择了*是*，则会自动选择“非当前时间”"创建ILM规则向导的第1步"。

如果要创建_PROMENTINY_规则、则必须选择*内嵌时间*。请参阅 "使用 S3 对象锁定管理对象"。

2. 在*时间段和位置*部分中，输入第一个时间段的开始时间和持续时间。

例如、您可能希望指定第一年的对象存储位置(*from day 0 store for 365 days*）。至少有一个指令必须从第 0 天开始。

3. 如果要创建复制的副本：
   a. 从*存储对象依据*下拉列表中，选择*复制*。
   b. 选择要创建的副本数。

如果将副本数更改为 1 ，则会显示一条警告。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会

使数据面临永久丢失的风险。请参阅 "为什么不应使用单副本复制"。

要避免此风险、请执行以下一项或多项操作：

- 增加时间段内的副本数。
- 向其他存储池或云存储池添加副本。
- 选择*纠删编码*，而不选择*复制*。

  如果此规则已在所有时间段创建多个副本，则可以安全地忽略此警告。

c. 在*副本位置*字段中、选择要添加的存储池。

- 如果仅指定一个存储池 * ，请注意， StorageGRID 只能在任何给定存储节点上存储一个对象的一个复制副本。如果您的网格包含三个存储节点、而您选择4作为副本数、则只会创建三个副本&#8212；每个存储节点一个副本。

  系统将触发 * 无法实现 ILM 放置 * 警报，以指示无法完全应用 ILM 规则。

- 如果指定多个存储池 * ，请记住以下规则：
  - 副本数不能大于存储池数。
  - 如果副本数等于存储池数，则每个存储池中将存储一个对象副本。
  - 如果副本数小于存储池数、则会在载入站点存储一个副本、然后系统会分发其余副本、以保持池中的磁盘使用量保持平衡、同时确保任何站点都不会获得一个对象的多个副本。
  - 如果存储池重叠（包含相同的存储节点），则对象的所有副本可能只保存在一个站点上。因此、请勿指定所有存储节点存储池(StorageGRID 11.6及更早版本)和其他存储池。

4. 如果要创建经过纠删编码的副本：

a. 从*存储对象依据*下拉列表中，选择*纠删编码*。

> 纠删编码最适合大于 1 MB 的对象。不要对小于200 KB的对象使用纠删编码、以避免管理非常小的经过纠删编码的片段所产生的开销。

b. 如果没有为大于200 KB的值添加对象大小筛选器，请选择*Previer*返回到步骤1。然后，选择*添加高级筛选器*并将*对象大小*筛选器设置为大于200 KB的任何值。

c. 选择要添加的存储池以及要使用的纠删编码方案。

纠删编码副本的存储位置包括纠删编码方案的名称、后跟存储池的名称。

可用的纠删编码方案受所选存储池中存储节点的数量限制。提供的方案旁边会出现一个 `Recommended`标志"提供最佳保护或最低存储开销"。

5. (可选)：

a. 选择*添加其他类型或位置*可在不同位置创建其他副本。

b. 选择*添加其他时间段*以添加不同的时间段。

对象删除基于以下设置进行：

- 除非另一个时间段以*forever *结尾、否则对象将在最后一个时间段结束时自动删除。
- 根据"存储分段和租户保留期限设置"，即使ILM保留期限结束，也可能不会删除对象。

6. 如果要将对象存储在云存储池中：
   a. 在*存储对象依据*下拉列表中，选择*复制*。
   b. 选择*复制位置*字段、然后选择云存储池。

      使用云存储池时，请记住以下规则：

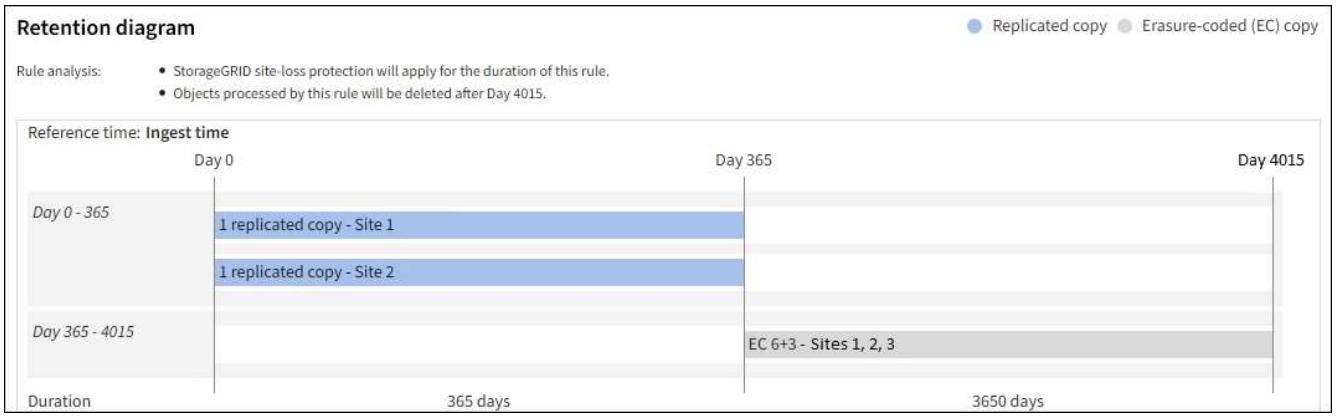
      - 您不能在一个放置说明中选择多个云存储池。同样、您也不能在同一放置说明中选择云存储池和存储池。
      - 您只能在任何给定的云存储池中存储一个对象的一个副本。如果将 * 副本 * 设置为 2 或更多，则会显示一条错误消息。
      - 不能同时在任何云存储池中存储多个对象副本。如果使用云存储池的多个放置位置的日期重叠，或者同一放置中的多个行使用云存储池，则会显示错误消息。
      - 您可以将对象存储在云存储池中、同时将该对象存储为StorageGRID中的复制副本或经过删除编码的副本。但是、您必须在该时间段的放置说明中包含多行、才能指定每个位置的副本数量和类型。
7. 在保留图中、确认您的放置说明。

   在此示例中、ILM规则会在第一年将一个复制副本存储在站点1中、并将一个复制副本存储在站点2中。一年后、再过10年、三个站点将保存一份6+3经过删除的副本。总共11年后、这些对象将从StorageGRID 中删除。

   保留图的规则分析部分指出：

   - 在此规则有效期内、StorageGRID 站点丢失保护将适用。
   - 此规则处理的对象将在第4015天后删除。

     请参见 "启用站点丢失保护。"



8. 选择 * 继续 * 。"第3步(选择加热行为)"的创建ILM规则向导。

在 StorageGRID ILM 规则中使用上次访问时间

您可以在ILM规则中使用上次访问时间作为参考时间。例如，您可能希望将过去三个月查看过的对象保留在本地存储节点上，同时将最近未查看过的对象移动到异地位置。如果您希望ILM规则仅应用于上次在特定日期访问的对象、也可以使用上次访问时间作为高级筛选器。

关于此任务

在ILM规则中使用上次访问时间之前、请查看以下注意事项：

- 使用上次访问时间作为参考时间时、请注意、更改对象的上次访问时间不会立即触发ILM评估。而是在后台 ILM 评估对象时评估对象的放置位置，并根据需要移动对象。访问对象后，此操作可能需要两周或更长时间。

  在根据上次访问时间创建ILM规则时、请考虑此延迟、并避免放置使用较短时间段(少于一个月)的位置。

- 如果将上次访问时间用作高级筛选器或参考时间、则必须为S3存储分段启用上次访问时间更新。您可以使用"租户管理器"或"租户管理 API"。

  默认情况下、S3存储分段会禁用上次访问时间更新。

  请注意，启用上次访问时间更新可能会降低性能，尤其是在对象较小的系统中。之所以会影响性能，是因为每次检索对象时， StorageGRID 都必须使用新的时间戳更新对象。

下表汇总了是否针对不同类型的请求更新存储分段中所有对象的上次访问时间。

请求类型	上次访问时间更新被禁用时是否更新上次访问时间	上次访问时间更新启用后是否更新上次访问时间
请求检索对象，其访问控制列表或其元数据	否	是
请求更新对象的元数据	是	是
请求将对象从一个存储分段复制到另一个存储分段	• 否，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本
请求完成多部分上传	是，对于已组装的对象	是，对于已组装的对象

选择 StorageGRID ILM 规则的接收行为

创建ILM规则向导的*选择导出行为*步骤允许您选择在导出时如何保护通过此规则筛选的对象。

关于此任务

StorageGRID 可以创建临时副本并将对象排入队列，以便稍后进行 ILM 评估，也可以立即创建副本以满足规则的放置说明。

步骤

1. 选择要使用的。"加热行为"

   有关详细信息，请参见 "加热选项的优点、缺点和限制"。

   > 如果规则使用以下放置方式之一、则不能使用"平衡"或"严格"选项：
   >
   > - 第 0 天的云存储池
   > - 规则使用用户定义的创建时间作为参考时间时的云存储池
   >
   > 请参阅。 "示例 5 ： 用于严格载入行为的 ILM 规则和策略"

2. 选择 * 创建 * 。

   此时将创建ILM规则。只有在将规则添加到中并激活该策略后、此规则才会处于活动"ILM策略"状态。

   要查看规则的详细信息、请在ILM规则页面上选择规则的名称。

在 **StorageGRID** 中创建默认 **ILM** 规则

在创建 ILM 策略之前，您必须创建一个默认规则，以便将其他规则不匹配的任何对象放置在此策略中。默认规则不能使用任何筛选器。它必须应用于所有租户，所有分段和所有对象版本。

开始之前

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

关于此任务

默认规则是ILM策略中要评估的最后一个规则、因此不能使用任何筛选器。默认规则的放置说明将应用于策略中其他规则未匹配的任何对象。

在此示例策略中、第一条规则仅适用于属于test-租 户-1的对象。默认规则，即属于所有其他租户帐户的适用场景 对象的最后一个规则。



创建默认规则时，请记住以下要求：

- 将默认规则添加到策略时、该规则将自动作为最后一个规则。
- 默认规则不能使用任何基本或高级筛选器。
- 默认规则必须应用于所有对象版本。
- 默认规则应创建复制的副本。

> 请勿使用创建经过删除编码的副本的规则作为策略的默认规则。纠删编码规则应使用高级筛选器、以防止对较小的对象进行纠删编码。

- 通常，默认规则应永久保留对象。
- 如果您正在使用(或计划启用)全局S3对象锁定设置、则默认规则必须合规。

步骤

1. 选择 * ILM * > * 规则 * 。
2. 选择 * 创建 * 。

   此时将显示创建ILM规则向导的第1步(输入详细信息)。

3. 在*Rule name*字段中输入规则的唯一名称。
4. 或者，也可以在 * 问题描述 * 字段中为此规则输入一个短问题描述 。
5. 将*租户帐户*字段留空。

   默认规则必须应用于所有租户帐户。

6. 保留“存储分段名称”下拉选项的*适用场景all存储分段*。

   默认规则必须应用于所有S3存储分段。

7. 对于"仅将此规则应用于较旧的对象版本(在启用了版本控制的S3存储分段中)？"的问题、保留默认问题解答*否*。
8. 请勿添加高级筛选器。

   默认规则无法指定任何筛选器。

9. 选择 * 下一步 * 。

   此时将显示第2步(定义放置位置)。

10. 对于"参考时间"、请选择任何选项。

    如果您保留了问题的默认答案*No*，“仅将此规则应用于旧对象版本？”非当前时间不会包括在下拉列表中。默认规则必须应用所有对象版本。

11. 指定默认规则的放置说明。
    - 默认规则应永久保留对象。如果默认规则不会永久保留对象，则在激活新策略时会显示警告。您必须确认这是您期望的行为。
    - 默认规则应创建复制的副本。

      请勿使用创建经过删除编码的副本的规则作为策略的默认规则。纠删编码规则应包括大于200 KB*的*对象大小(MB)高级筛选器，以防止对较小的对象进行纠删编码。

    - 如果您正在使用（或计划启用）全局 S3 对象锁定设置，则默认规则必须符合：
      - 它必须至少创建两个复制的对象副本或一个经过纠删编码的副本。
      - 这些副本必须在放置说明中每行的整个持续时间内存在于存储节点上。
      - 无法将对象副本保存在云存储池中。
      - 至少一行放置说明必须从第0天开始、并使用Ingast时间作为参考时间。
      - 放置说明中至少有一行必须为"永久"。
12. 查看保留图以确认放置说明。
13. 选择 * 继续 * 。

    此时将显示第3步(选择加载行为)。

14. 选择要使用的加注选项，然后选择*Create*。

管理ILM策略

了解 StorageGRID 中的 ILM 策略

信息生命周期管理（ ILM ）策略是一组有序的 ILM 规则，用于确定 StorageGRID 系统如何在一段时间内管理对象数据。

配置不正确的 ILM 策略可能导致无法恢复的数据丢失。激活 ILM 策略之前，请仔细查看 ILM 策略及其 ILM 规则，然后模拟 ILM 策略。请始终确认 ILM 策略将按预期运行。

默认**ILM**策略

安装StorageGRID并添加站点时、系统会自动创建默认ILM策略、如下所示：

- 如果网格包含一个站点、则默认策略包含一个默认规则、用于复制该站点上每个对象的两个副本。
- 如果网格包含多个站点、则默认规则会复制每个站点上每个对象的一个副本。

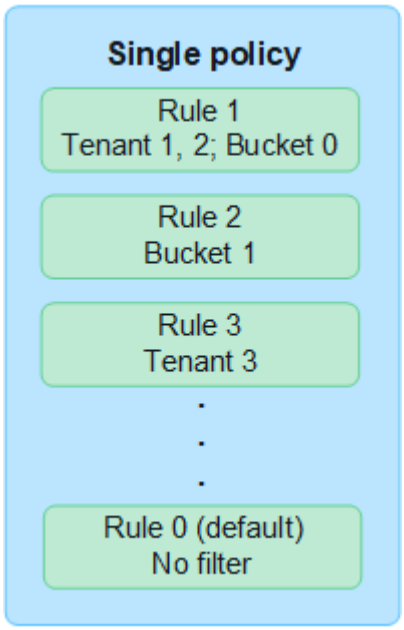
如果默认策略不能满足您的存储要求，您可以创建自己的规则和策略。看"创建ILM规则"和"创建ILM策略"。

一个或多个活动**ILM**策略?

一次可以有一个或多个活动ILM策略。

一个策略

如果您的网格将使用简单的数据保护方案、其中包含一些租户专用和存储分段专用的规则、请使用一个活动ILM策略。ILM规则可以包含用于管理不同存储分段或租户的筛选器。



如果只有一个策略、而租户的要求发生变化、则必须创建新的ILM策略或克隆现有策略、以应用更改、模拟并激活新的ILM策略。对ILM策略进行更改可能会导致对象移动需要数天时间、并导致发生原因系统延迟。

多个策略

要为租户提供不同的服务质量选项、一次可以有多个活动策略。每个策略都可以管理特定租户、S3分段和对象。为一组特定租户或对象应用或更改一个策略时、应用于其他租户和对象的策略不受影响。

ILM策略标记

如果要允许租户在每个存储分段的多个数据保护策略之间轻松切换、请使用多个带有_ILM policy tags_的ILM策略。您可以将每个ILM策略分配给一个标记、然后租户标记一个存储分段以将此策略应用于该存储分段。您

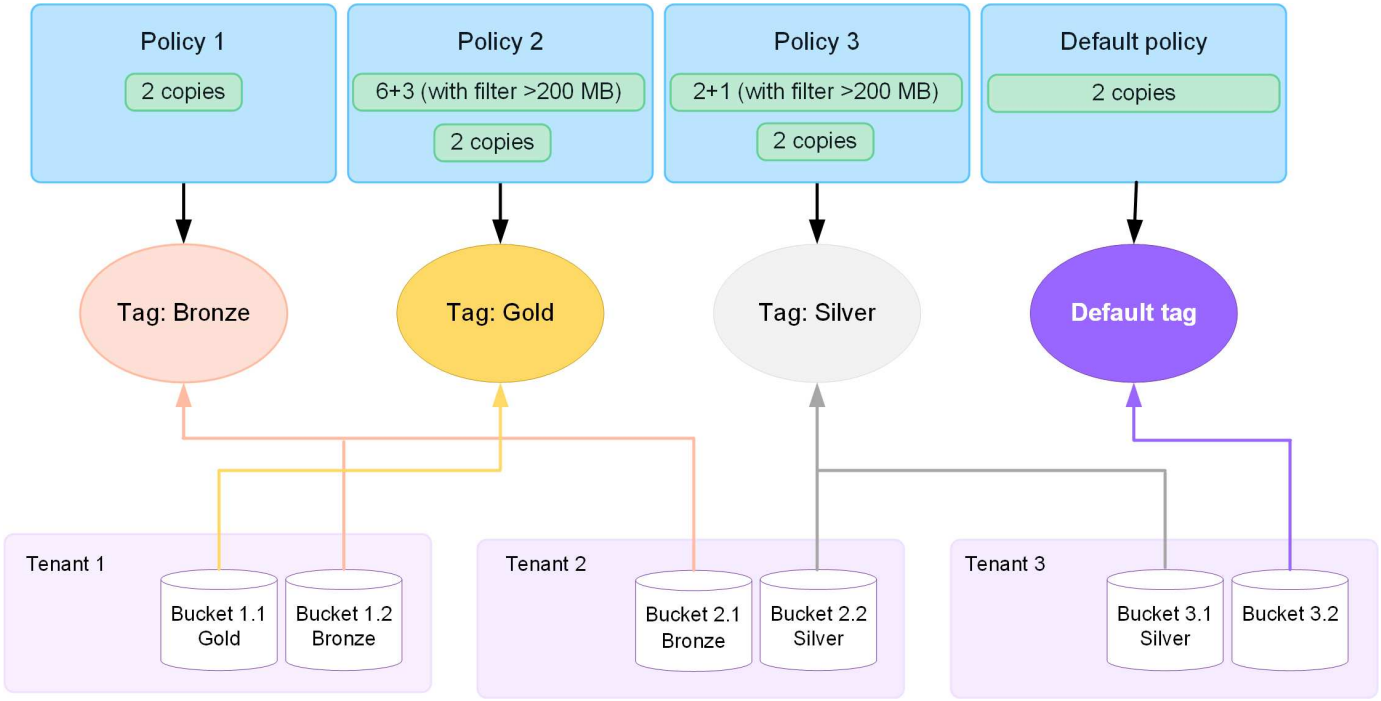
只能在S3存储分段上设置ILM策略标记。

例如、您可能有三个标记、分别名为Gold、Silver和Bronze。您可以根据ILM策略存储对象的时长和位置为每个标记分配ILM策略。租户可以通过标记其存储分段来选择要使用的策略。标记为Gold的存储分段由Gold策略管理、并获得Gold级别的数据保护和性能。

> 你可以"最多创建 10 个策略标签"为您的网格。

默认ILM策略标记

安装StorageGRID时、系统会自动创建默认ILM策略标记。每个网格都必须有一个分配给默认标记的活动策略。默认策略适用于任何未标记的S3存储分段。



ILM 策略如何评估对象?

活动ILM策略用于控制对象的放置、持续时间和数据保护。

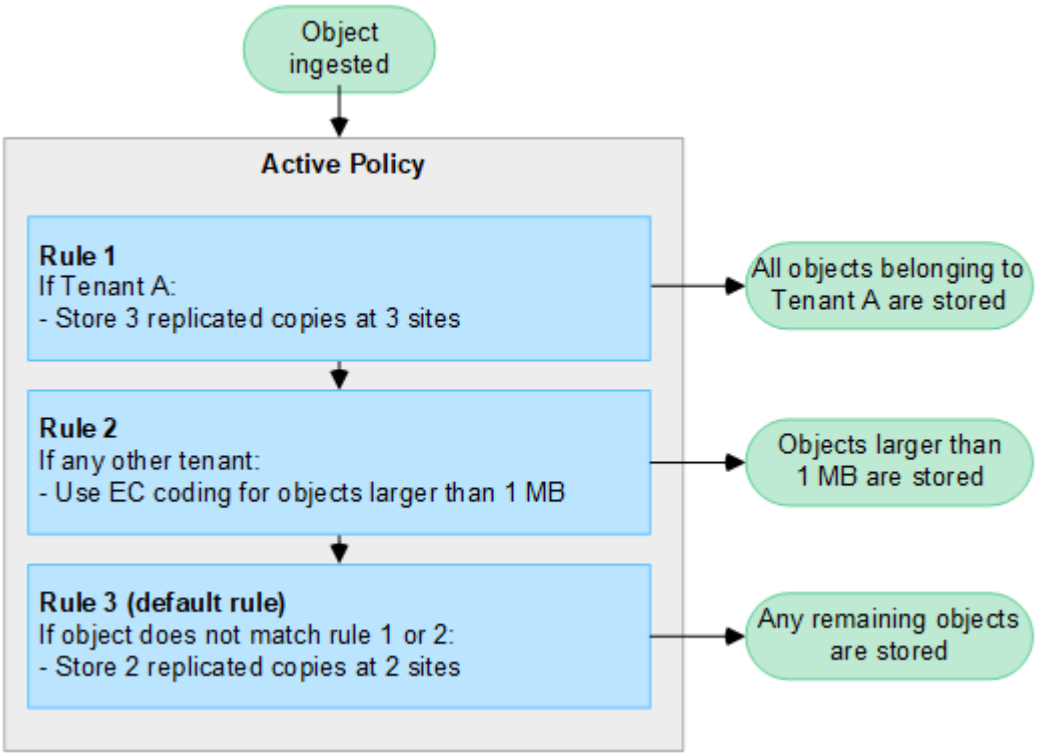
当客户端将对象保存到StorageGRID时、系统将根据策略中按顺序排列的一组ILM规则对对象进行评估、如下所示：

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、则系统将根据策略中的每个后续规则评估对象、直到进行匹配为止。
3. 如果没有与对象匹配的规则，则会应用策略中默认规则的载入行为和放置说明。默认规则是策略中的最后一个规则。默认规则必须应用于所有租户、所有S3分段和所有对象版本、并且不能使用任何高级筛选器。

ILM 策略示例

例如、一个ILM策略可以包含三个ILM规则、这些规则可指定以下内容：

- *规则1：为租户A*复制的副本
  - 匹配属于租户A的所有对象
  - 将这些对象作为三个复制副本存储在三个站点上。
  - 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：对大于1 MB*的对象进行纠删编码
  - 匹配其他租户的所有对象、但前提是这些对象大于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。
  - 与小于或等于1 MB的对象不匹配、因此将根据规则3评估这些对象。
- 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。不使用筛选器。
  - 为规则1或规则2不匹配的所有对象创建两个复制副本(不属于租户A且小于或等于1 MB的对象)。



什么是活动策略和非活动策略?

每个StorageGRID系统必须至少具有一个活动ILM策略。如果您希望有多个活动ILM策略、请创建ILM策略标记并为每个标记分配一个策略。然后、租户将标记应用于S3存储分段。默认策略将应用于存储分段中未分配策略标记的所有对象。

首次创建ILM策略时、您可以选择一个或多个ILM规则并按特定顺序进行排列。在模拟策略以确认其行为后、您可以将其激活。

激活一个ILM策略后、StorageGRID将使用该策略来管理所有对象、包括现有对象和新加入的对象。实施新策略中的 ILM 规则后，现有对象可能会移至新位置。

如果一次激活多个ILM策略、而租户将策略标记应用于S3存储分段、则每个存储分段中的对象将根据分配给该标记的策略进行管理。

StorageGRID系统会跟踪已激活或停用的策略的历史记录。

创建 ILM 策略的注意事项

- 仅在测试系统中使用系统提供的策略基线2副本策略。对于StorageGRID 11.6及更早版本、此策略中的"创建2个副本"规则将使用包含所有站点的所有存储节点存储池。如果 StorageGRID 系统具有多个站点，则一个对象的两个副本可能会放置在同一站点上。

> 在安装StorageGRID 11.6及更早版本期间、系统会自动创建所有存储节点存储池。如果升级到更高版本的StorageGRID 、则所有存储节点池仍将存在。如果全新安装StorageGRID 11.7或更高版本、则不会创建所有存储节点池。

- 在设计新策略时，请考虑可能会输入到网格中的所有不同类型的对象。确保此策略包含与这些对象匹配并根据需要放置这些对象的规则。
- 尽量使 ILM 策略简单。这样可以避免在随时间推移对 StorageGRID 系统进行更改时，对象数据无法按预期得到保护的潜在危险情况。
- 确保策略中的规则顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。例如、如果策略中的第一个规则与某个对象匹配、则该对象不会由任何其他规则进行评估。
- 每个ILM策略中的最后一条规则是默认ILM规则、不能使用任何筛选器。如果某个对象未被其他规则匹配，则默认规则将控制该对象的放置位置以及保留时间。
- 在激活新策略之前，请查看此策略对现有对象的放置所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

在 StorageGRID 中创建 ILM 策略

创建一个或多个ILM策略以满足您的服务质量要求。

通过一个有效的ILM策略、您可以将相同的ILM规则应用于所有租户和存储分段。

通过使用多个活动ILM策略、您可以将适当的ILM规则应用于特定租户和存储分段、以满足多项服务质量要求。

创建ILM策略

关于此任务

在创建您自己的策略之前、请确认"默认ILM策略"不满足您的存储要求。

> 在测试系统中、仅使用系统提供的策略：2个副本策略(对于单站点网格)或每个站点1个副本(对于多站点网格)。对于StorageGRID 11.6及更早版本、此策略中的默认规则将使用所有存储节点存储池、其中包含所有站点。如果 StorageGRID 系统具有多个站点，则一个对象的两个副本可能会放置在同一站点上。

> 如果是"已启用全局S3对象锁定设置"，则必须确保 ILM 策略符合启用了 S3 Object Lock 的存储桶的要求。在本节中，请按照提及启用 S3 Object Lock 的说明进行操作。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。

- 您已"已创建ILM规则"根据是否启用S3对象锁定来确定。

  未启用**S3**对象锁定

  - 您是否"已创建ILM规则"要添加到策略中。您可以根据需要保存策略、创建其他规则、然后编辑策略以添加新规则。
  - 您的"已创建默认 ILM 规则"不包含任何筛选器。

  已启用**S3**对象锁定

  - StorageGRID 系统的 "已启用全局S3对象锁定设置"。
  - 您是否"创建了合规和不合规的ILM规则"要添加到策略中。您可以根据需要保存策略、创建其他规则、然后编辑策略以添加新规则。
  - 您的"已创建默认 ILM 规则"策略符合要求。

- 或者，您已经观看了视频：

ILM 策略概述

另请参见"使用ILM策略"。

步骤

1. 选择 * ILM * > * 策略 * 。

   如果启用了全局S3对象锁定设置、则"ILM策略"页面将指示哪些ILM规则合规。

2. 确定希望如何创建ILM策略。

   创建新策略

   a. 选择*创建策略*。

   克隆现有策略

   a. 选中要开头的策略对应的复选框，然后选择*Clone。

   编辑现有策略

   a. 如果策略处于非活动状态、您可以对其进行编辑。选中要开始的非活动策略对应的复选框，然后选择*Edit*。

3. 在*策略名称*字段中，为策略输入一个唯一名称。
4. (可选)在*reason for change*字段中，输入创建新策略的原因。
5. 要向策略中添加规则，请选择*选择规则*。选择规则名称以查看该规则的设置。

   如果要克隆策略：

   - 此时将选择要克隆的策略使用的规则。
   - 如果要克隆的策略使用了任何不含筛选器的规则，而这些规则不是默认规则，则系统会提示您删除除其

中一个规则之外的所有规则。

- 如果默认规则使用筛选器、系统将提示您选择新的默认规则。
- 如果默认规则不是最后一条规则、则可以将此规则移至新策略的末尾。

未启用**S3**对象锁定

a. 为此策略选择一个默认规则。要创建新的默认规则，请选择*ILM规则页*。

   默认规则适用场景 与策略中的其他规则不匹配的任何对象。此默认规则不能使用任何筛选器、并且始终最后评估。

   > 请勿使用"创建2个副本"规则作为策略的默认规则。" 创建 2 个副本 " 规则使用一个存储池 " 所有存储节点 " ，其中包含所有站点。如果 StorageGRID 系统具有多个站点，则一个对象的两个副本可能会放置在同一站点上。

已启用**S3**对象锁定

a. 为此策略选择一个默认规则。要创建新的默认规则，请选择*ILM规则页*。

   规则列表仅包含合规的规则、不使用任何筛选器。

   > 请勿使用"创建2个副本"规则作为策略的默认规则。" 创建 2 个副本 " 规则使用一个存储池 " 所有存储节点 " ，其中包含所有站点。如果使用此规则，则一个对象的多个副本可能会放置在同一站点上。

b. 如果需要为不合规S3存储分段中的对象设置不同的"默认"规则、请选择*为不合规S3存储分段添加不带筛选器的规则*、然后选择一个不使用筛选器的不合规规则。

   例如、您可能希望使用云存储池将对象存储在未启用S3对象锁定的存储分段中。

   > 您只能选择一个不使用筛选器的不合规规则。

另请参见"示例 7： S3 对象锁定的兼容 ILM 策略"。

6. 选择完默认规则后，选择*CONTINU*。
7. 对于其他规则步骤、请选择要添加到策略中的任何其他规则。这些规则至少使用一个筛选器(租户帐户、存储分段名称、高级筛选器或非当前引用时间)。然后选择*Select*。

   此时、创建策略窗口将列出您选择的规则。默认规则位于末尾，上面有其他规则。

   如果启用了S3对象锁定、并且您还选择了不合规的"默认"规则、则该规则将作为策略中倒数第二条规则添加。

   > 如果任何规则不永久保留对象、则会显示警告。激活此策略后、您必须确认希望StorageGRID 在默认规则的放置说明过期后删除对象(除非分段生命周期将对象保留较长时间)。

8. 拖动非默认规则的行以确定评估这些规则的顺序。

您无法移动默认规则。如果启用了S3对象锁定、则如果选择了不合规的"默认"规则、则也无法移动该规则。

> 您必须确认 ILM 规则的顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。

9. 根据需要选择*选择规则*以添加或删除规则。
10. 完成后，选择 * 保存 * 。
11. 重复这些步骤以创建其他ILM策略。
12. 模拟 ILM 策略(英文)您应始终在激活策略之前模拟该策略、以确保其按预期工作。

模拟策略

在激活策略并将其应用于生产数据之前、模拟测试对象上的策略。

开始之前

您知道要测试的每个对象的S3分段/对象密钥。

步骤

1. 使用S3客户端或"S3控制台"，加载测试每个规则所需的对象。
2. 在ILM策略页面上，选中策略对应的复选框，然后选择*silmate*。
3. 在*Object*字段中，输入测试对象的S3 `bucket/object-key`。例如， `bucket-01/filename.png`。
4. 如果启用了S3版本控制，可以选择在*Version ID*字段中输入对象的版本ID。
5. 选择 * 模拟 * 。
6. 在Simulation Results部分中、确认每个对象都使用正确的规则进行匹配。
7. 要确定哪个存储池或纠删编码配置文件有效、请选择匹配规则的名称以转到规则详细信息页面。

> 查看对现有复制对象和经过重复数据和经过重复数据处理的对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

结果

对策略规则所做的任何编辑都将反映在模拟结果中，并显示新的匹配项和之前的匹配项。模拟策略窗口将保留您测试的对象，直到您选择 全部清除 或为模拟结果列表中的每个对象选择删除图标 ✕。

相关信息

"ILM策略模拟示例"

激活策略

激活一个新ILM策略后、现有对象和新加索的对象将由该策略进行管理。激活多个策略时、分配给存储分段的ILM策略标记将确定要管理的对象。

在激活新策略之前：

1. 模拟策略以确认其行为符合您的预期。
2. 查看对现有复制对象和经过重复数据和经过重复数据处理的对象的放置方式所做的任何更改。在评估和实施

新放置时，更改现有对象的位置可能会导致临时资源问题。

ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。

关于此任务

激活 ILM 策略时，系统会将新策略分发到所有节点。但是，只有在所有网格节点均可接收新策略之后，新的活动策略才会实际生效。在某些情况下、系统会等待实施新的活动策略、以确保网格对象不会意外删除。具体而言：

- 如果您进行的策略更改*增加数据冗余或持久性*，这些更改将立即实施。例如，如果您激活包含三个副本规则而不是双个副本规则的新策略，则该策略将立即实施，因为它会增加数据冗余。
- 如果所做的策略更改*可能会降低数据冗余或持久性*，则在所有网格节点可用之前，不会实施这些更改。例如、如果您激活的新策略使用的是双副本规则、而不是三个副本规则、则新策略将显示在Active policy选项卡中、但只有在所有节点均已联机且可用后、此策略才会生效。

步骤

按照以下步骤激活一个或多个策略：

激活一个策略

如果只有一个活动策略、请执行以下步骤。如果您已有一个或多个活动策略、并且要激活其他策略、请按照步骤激活多个策略。

1. 准备好激活策略后，选择*ILM >*Policies*。

   或者，您也可以从*ILM >*Policy tags*页面激活单个策略。

2. 在策略选项卡上，选中要激活的策略对应的复选框，然后选择*Activate*。
3. 按照相应步骤操作：
   - 如果警告消息提示您确认要激活策略，请选择*OK*。
   - 如果显示包含策略详细信息的警告消息：
     i. 查看详细信息、确保策略按预期管理数据。
     ii. 如果默认规则将对象存储的天数有限、请查看保留图、然后在文本框中键入此天数。
     iii. 如果默认规则永久存储对象，但一个或多个其他规则的保留时间有限，请在文本框中键入*yes*。
     iv. 选择*激活策略*。

激活多个策略

要激活多个策略，您必须创建策略标签并为每个标签分配一个策略。您最多可以为网格创建 10 个策略标签。

> 当使用多个策略标签时，如果租户频繁地将策略标签重新分配给存储桶，则网格性能可能会受到影响。如果您有不受信任的租户，请考虑仅使用默认策略标签。

1. 选择*ILM >*Policy tags*。
2. 选择 * 创建 * 。
3. 在创建策略标记对话框中、键入标记名称以及标记的问题描述(可选)。

   > 标记名称和说明对租户可见。选择有助于租户在选择要分配给其存储分段的策略标记时做出明智决策的值。例如、如果分配的策略将在一段时间后删除对象、您可以在问题描述中进行通信。请勿在这些字段中包含敏感信息。

4. 选择*创建标记*。
5. 在ILM策略标记表中、使用下拉列表选择要分配给该标记的策略。
6. 如果“策略限制”列中出现警告，请选择*查看策略详细信息*以查看策略。
7. 确保每个策略都能按预期管理数据。
8. 选择*激活指派的策略*。或者，选择*clear changes*以删除策略分配。
9. 在使用新标记激活策略对话框中、查看每个标记、策略和规则如何管理对象的说明。根据需要进行更改、以确保策略按预期管理对象。
10. 如果确定要激活策略，请在文本框中键入*yes*，然后选择*Activate Policies*。

相关信息

"示例 6： 更改 ILM 策略"

StorageGRID 中的 **ILM** 策略模拟示例

ILM策略模拟示例提供了为您的环境构建和修改模拟的准则。

示例**1**：模拟**ILM**策略时验证规则

此示例介绍了如何在模拟策略时验证规则。

在此示例中，正在针对两个分段中的输入对象模拟 * 示例 ILM 策略 * 。此策略包括三个规则，如下所示：

- 第一条规则 * 两个副本，即 bucket-A* 两年，仅适用于 bucket-a 中的对象
- 第二条规则 * EC 对象 > 1 MB* ，适用场景 all b桶 but filters on objects 大于 1 MB 。
- 第三条规则为 * 两个副本，两个数据中心 * 。它不包含任何筛选器，也不使用非当前参考时间。

模拟策略后、确认每个对象均符合正确的规则。



在此示例中：

- `bucket-a/bucket-a object.pdf`正确匹配了第一个规则，该规则按中的对象进行筛选 `bucket-a。
- `bucket-b/test object greater than 1 MB.pdf`是中的 `bucket-b，因此与第一个规则不匹配。而是通过第二条规则正确匹配，该规则会对大于 1 MB 的对象进行筛选。
- `bucket-b/test object less than 1 MB.pdf`与前两个规则中的筛选器不匹配、因此它将由默认规则放置、该规则不包含任何筛选器。

示例**2**：模拟**ILM**策略时对规则重新排序

此示例显示了在模拟策略时如何重新排列规则以更改结果。

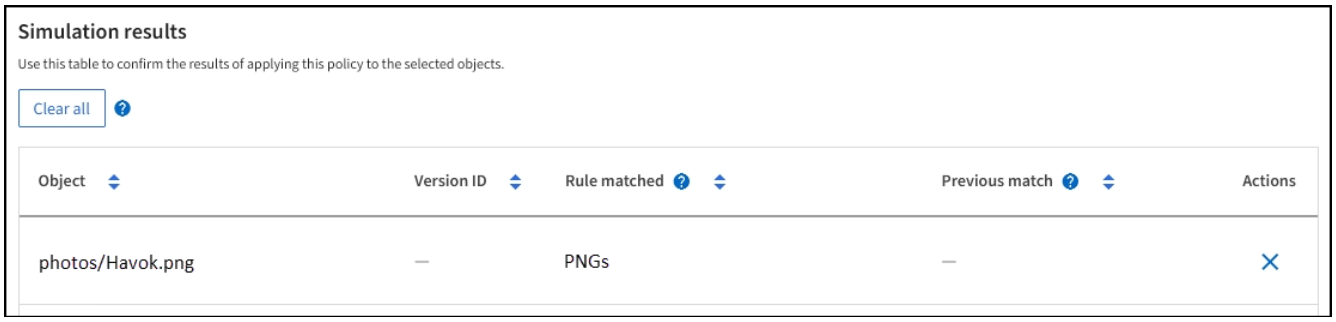
在此示例中，正在模拟 * 演示 * 策略。此策略用于查找具有 series=x-men 用户元数据的对象，它包含以下三个规则：

- 第一个规则*PNGs*过滤以结尾的键名 `.png`。
- 第二条规则*X-men*仅适用于租户A的对象并筛选 `series=x-men`用户元数据。
- 最后一条规则*two copes two data centres *是默认规则，它匹配与前两条规则不匹配的任何对象。

步骤

1. 添加规则并保存策略后，选择 * 模拟 * 。
2. 在*Object*字段中，输入测试对象的S3存储分段/object-key，然后选择*sobject*。

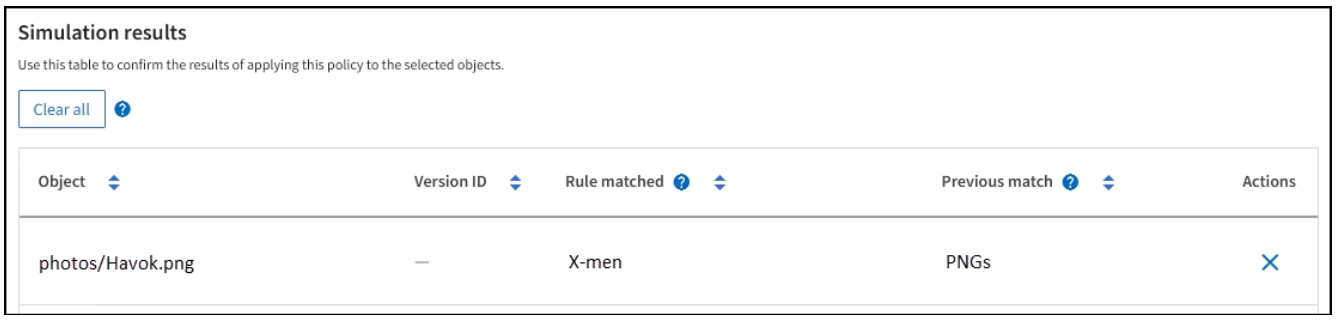
   此时将显示模拟结果，显示 `Havok.png`对象已与*PNGs*规则匹配。



   但是， `Havok.png`是为了测试*X-men*规则。

3. 要解析问题描述 ，请对规则重新排序。
   a. 选择*完成*以关闭模拟ILM策略窗口。
   b. 选择 * 编辑 * 以编辑策略。
   c. 将 **X-men** 规则拖动到列表顶部。
   d. 选择 * 保存 * 。
4. 选择 * 模拟 * 。

   系统会根据更新后的策略重新评估先前测试的对象，并显示新的模拟结果。在此示例中、"规则匹配"列显示`Havok.png`对象现在与X-MEN元数据规则符合预期。上一个匹配列显示了与上一个模拟中的对象匹配的PNG规则。

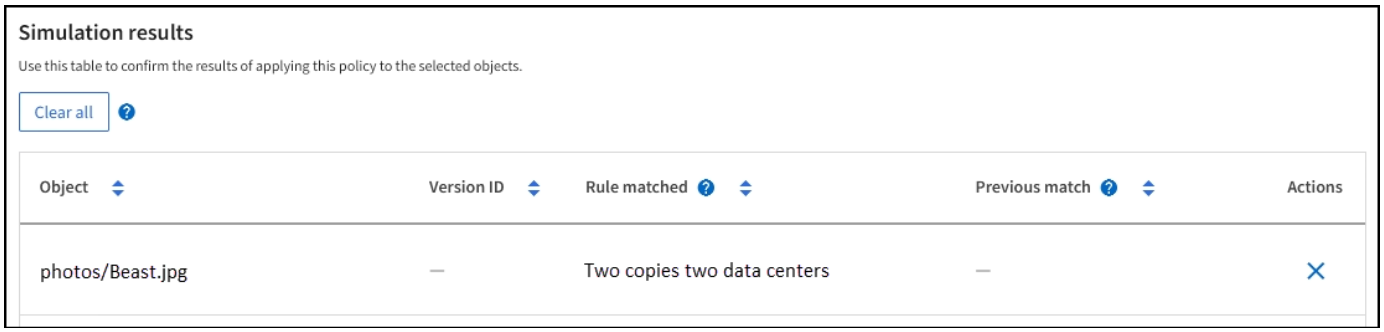


示例**3**：模拟**ILM**策略时更正规则

此示例显示了如何模拟策略，更正策略中的规则以及继续模拟。

在此示例中，正在模拟 * 演示 * 策略。此策略用于查找包含用户元数据的对象 `series=x-men`。但是、针对对

象模拟此策略时会出现意外结果 `Beast.jpg`。该对象与默认规则匹配，而不是与 X-men 元数据规则匹配，而是复制两个数据中心。



如果测试对象与策略中的预期规则不匹配，则必须检查策略中的每个规则并更正任何错误。

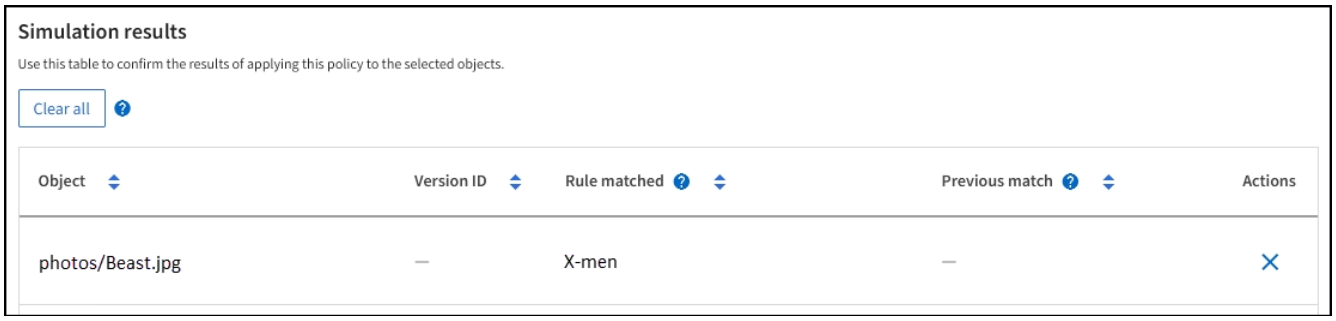
步骤

1. 选择*完成*以关闭模拟策略对话框。在策略的详细信息页面上，选择*保留图*。然后根据需要为每个规则选择*全部展开*或*查看详细信息*。
2. 查看规则的租户帐户，参考时间和筛选条件。

   例如、假设X-men规则的元数据输入为"x-men01"、而不是"x-men"。

3. 要解决此错误、请按如下所示更正此规则：
   - 如果规则属于策略的一部分、您可以克隆规则、也可以从策略中删除规则、然后对其进行编辑。
   - 如果规则是活动策略的一部分，则必须克隆此规则。您不能编辑或删除活动策略中的规则。
4. 再次执行模拟。

   在此示例中、更正后的X-MEN规则现在会按预期根据用户元数据匹配 `Beast.jpg`对象 `series=x-men`。



管理 **StorageGRID** 中的 **ILM** 策略标签

您可以查看ILM策略标记详细信息、编辑标记或删除标记。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"所需的访问权限"。

查看ILM策略标记详细信息

要查看标记的详细信息：

1. 选择*ILM >*Policy tags*。
2. 从表中选择策略的名称。此时将显示此标记的详细信息页面。
3. 在详细信息页面上、查看已分配策略的先前历史记录。
4. 通过选择策略来查看策略。

编辑ILM策略标记

> 标记名称和说明对租户可见。选择有助于租户在选择要分配给其存储分段的策略标记时做出明智决策的值。例如、如果分配的策略将在一段时间后删除对象、您可以在问题描述中进行通信。请勿在这些字段中包含敏感信息。

要编辑现有标记的问题描述：

1. 选择*ILM >*Policy tags*。
2. 选中标记的复选框，然后选择*Edit*。

   或者、选择标记的名称。此时将显示标签的详细信息页面，您可以在该页面上选择*Edit*。
3. 根据需要更改标记问题描述
4. 选择 * 保存 * 。

删除ILM策略标记

删除策略标记后、分配有该标记的任何分段都将应用默认策略。

删除标记：

1. 选择*ILM >*Policy tags*。
2. 选中标记的复选框，然后选择*Remove*。此时将显示确认对话框。

   或者、选择标记的名称。此时将显示标签的详细信息页面，您可以在该页面上选择*Remove*。
3. 选择*是*以删除标记。

相关信息

"了解如何创建 ILM 策略标签"

使用 StorageGRID 中的对象元数据查找验证 ILM 策略

激活ILM策略后、将代表性测试对象插入StorageGRID系统、然后执行对象元数据查找以确认副本是否按预期创建并放置在正确的位置。

开始之前

您有一个对象标识符，它可以是以下之一：

- **UUID**：对象的通用唯一标识符。
- **CBID**： StorageGRID内对象的唯一标识符。您可以从审计日志中获取对象的 CBID。以全部大写的形式输入 CBID。
- **S3** 存储桶和对象键：当通过 S3 接口提取对象时，客户端应用程序使用存储桶和对象键组合来存储和识别该对象。如果 S3 存储桶已版本化，并且您想要使用存储桶和对象键查找 S3 对象的特定版本，那么您就有*版本 ID*。

步骤

1. 正在载入对象。
2. 选择 * ILM * > * 对象元数据查找 * 。
3. 在 * 标识符 * 字段中键入对象的标识符。您可以输入UUID、CBID或S3存储分段/对象密钥。
4. 或者，输入对象的版本 ID （仅限 S3 ）。
5. 选择 * 查找 * 。

   此时将显示对象元数据查找结果。此页面列出了以下类型的信息：

   - 系统元数据、例如对象ID (UUID)、结果类型(对象、删除标记、S3存储分段)以及对象的逻辑大小。有关详细信息、请参见以下示例屏幕截图。
   - 与对象关联的任何自定义用户元数据键值对。
   - 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
   - 对于复制的对象副本，为每个副本提供当前存储位置。
   - 对于经过擦除编码的对象副本，为每个片段的当前存储位置。
   - 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。
   - 对于分段对象和多部分对象，包含分段标识符和数据大小的对象分段列表。对于包含 100 个以上区块的对象，仅显示前 100 个区块。
   - 所有对象元数据均采用未处理的内部存储格式。此原始元数据包括内部系统元数据，不能保证这些元数据在版本之间持续存在。
6. 确认对象存储在正确的位置、并且副本类型正确。

   如果启用了 Audit 选项，则还可以监控审核日志中是否显示了 "ORLM Object Rules" 消息。ORLM审核消息可以为您提供有关ILM评估过程状态的更多信息、但不能为您提供有关对象数据放置是否正确或ILM策略是否完整的信息。您必须自己进行评估。有关详细信息，请参见 "查看审核日志"。

以下示例显示了存储为两个复制副本的 S3 测试对象的对象元数据查找结果。

以下屏幕截图是一个示例。您的结果因StorageGRID版本而异。

System Metadata

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

Replicated Copies

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

Raw Metadata


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


相关信息

"使用S3 REST API"

在 StorageGRID 中使用 ILM 策略和 ILM 规则

随着存储要求的变化、您可能需要制定其他策略或修改与策略关联的ILM规则。您可以查看ILM指标来确定系统性能。

开始之前

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

查看ILM策略

要查看活动和非活动ILM策略以及策略激活历史记录、请执行以下操作：

1. 选择 * ILM * > * 策略 * 。
2. 选择*策略*可查看活动和非活动策略列表。此表列出了每个策略的名称、将策略分配到的标记以及策略是处于活动状态还是处于非活动状态。
3. 选择*激活历史记录*可查看策略的激活开始和结束日期列表。
4. 选择策略名称以查看策略的详细信息。

如果您查看状态为已编辑或已删除的策略的详细信息、则会显示一条消息、说明您正在查看在指定时间段内处于活动状态且此后已被编辑或删除的策略版本。

编辑**ILM**策略

您只能编辑非活动策略。如果要编辑活动策略、请将其停用、或者创建克隆并编辑此克隆。

编辑策略：

1. 选择 * ILM * > * 策略 * 。
2. 选中要编辑的策略对应的复选框，然后选择*Edit*。
3. 按照中的说明编辑策略"创建ILM策略"。
4. 在重新激活策略之前、请对其进行模拟。

配置不正确的 ILM 策略可能导致无法恢复的数据丢失。激活 ILM 策略之前，请仔细查看 ILM 策略及其 ILM 规则，然后模拟 ILM 策略。请始终确认 ILM 策略将按预期运行。

克隆**ILM**策略

克隆ILM策略：

1. 选择 * ILM * > * 策略 * 。
2. 选中要克隆的策略对应的复选框，然后选择*Clone。
3. 按照中的说明"创建ILM策略"，从已克隆的策略开始创建新策略。

配置不正确的 ILM 策略可能导致无法恢复的数据丢失。激活 ILM 策略之前，请仔细查看 ILM 策略及其 ILM 规则，然后模拟 ILM 策略。请始终确认 ILM 策略将按预期运行。

删除**ILM**策略

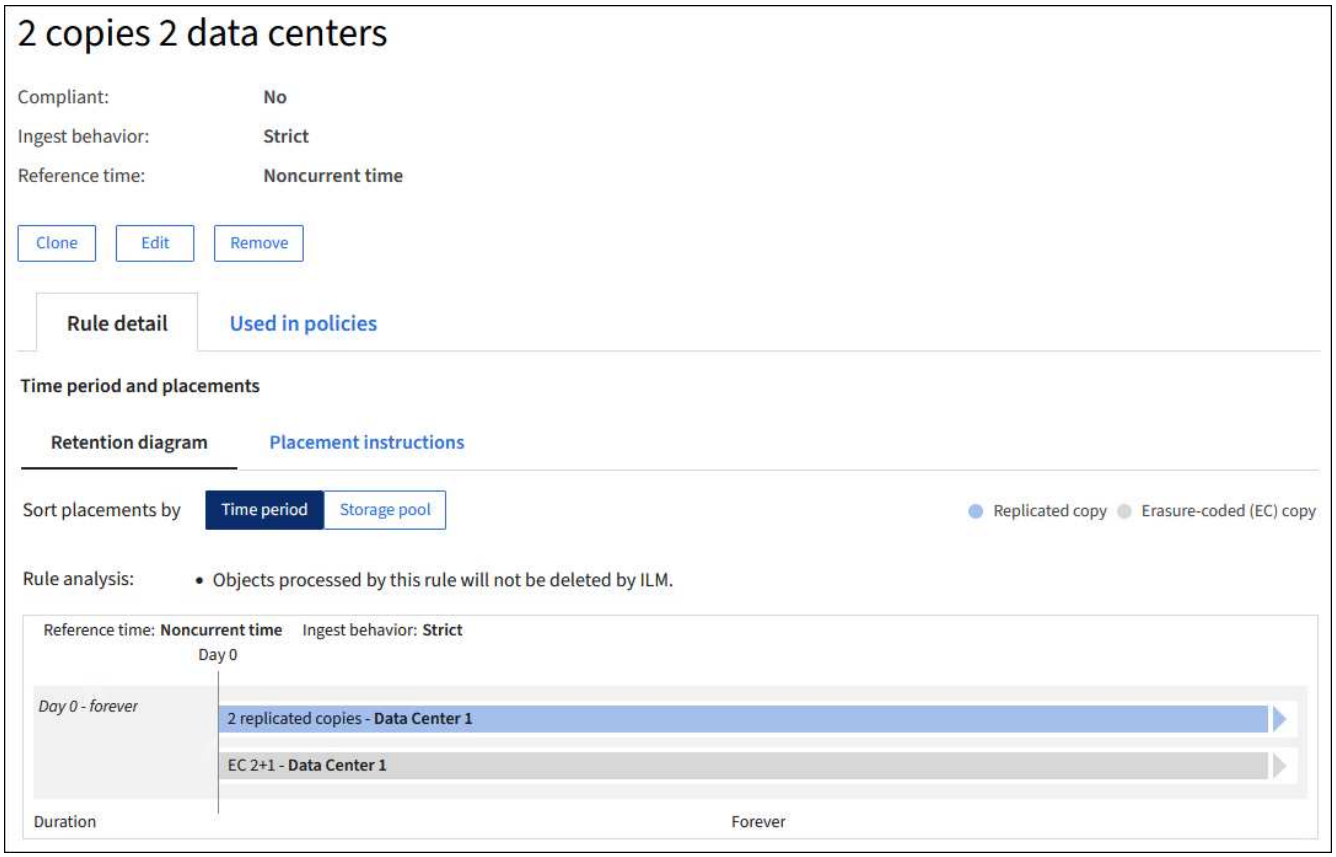
您只能删除处于非活动状态的ILM策略。删除策略：

1. 选择 * ILM * > * 策略 * 。
2. 选中要删除的非活动策略对应的复选框。
3. 选择 * 删除 * 。

查看ILM规则详细信息

要查看ILM规则的详细信息、包括规则的保留图和放置说明、请执行以下操作：

1. 选择 * ILM * > * 规则 * 。
2. 选择要查看其详细信息的规则的名称。示例：



此外、您还可以使用详细信息页面克隆、编辑或删除规则。如果某个规则在任何策略中使用、则无法编辑或删除该规则。

克隆 ILM 规则

如果要创建使用现有规则的某些设置的新规则、可以克隆现有规则。如果您需要编辑任何策略中使用的规则、则可以克隆该规则并对克隆进行更改。对克隆进行更改后、您可以从策略中删除原始规则、并根据需要将其替换为修改后的版本。

如果ILM规则是使用StorageGRID 10.2或更早版本创建的、则无法克隆该规则。

步骤

1. 选择 * ILM * > * 规则 * 。
2. 选中要克隆的规则对应的复选框，然后选择*Clone。或者，也可以选择规则名称，然后从规则详细信息页面中选择*Clone。
3. 按照和"在ILM规则中使用高级筛选器"的步骤更新克隆的规则编辑ILM规则。

   克隆 ILM 规则时，必须输入新名称。

编辑 ILM 规则

要更改筛选器或放置指令，您可能需要编辑 ILM 规则。

如果某个规则已在任何ILM策略中使用、则无法编辑此规则。而是可以克隆规则对克隆的副本进行任何必要的更改。

> 配置不正确的 ILM 策略可能导致无法恢复的数据丢失。激活 ILM 策略之前，请仔细查看 ILM 策略及其 ILM 规则，然后模拟 ILM 策略。请始终确认 ILM 策略将按预期运行。

步骤

1. 选择 * ILM * > * 规则 * 。
2. 确认要编辑的规则未在任何ILM策略中使用。
3. 如果要编辑的规则未在使用中，请选中该规则的复选框，然后选择*Actions*>*Edit*。或者，选择规则的名称，然后在规则详细信息页面上选择*Edit*。
4. 完成编辑ILM规则向导的步骤。如有必要，请按照和中的步骤"在ILM规则中使用高级筛选器"进行操作"创建 ILM 规则"。

   编辑ILM规则时、不能更改其名称。

删除ILM规则

要使当前ILM规则列表易于管理、请删除您不可能使用的任何ILM规则。

步骤

要删除当前在活动策略中使用的ILM规则、请执行以下操作：

1. 克隆策略。
2. 从策略克隆中删除ILM规则。
3. 保存，模拟和激活新策略，以确保对象按预期受到保护。
4. 转到删除当前在非活动策略中使用的ILM规则的步骤。

要删除当前在非活动策略中使用的ILM规则、请执行以下操作：

1. 选择非活动策略。
2. 从策略或中删除ILM规则删除策略。
3. 转到删除当前未使用的ILM规则的步骤。

删除当前未使用的ILM规则：

1. 选择 * ILM * > * 规则 * 。
2. 确认要删除的规则未在任何策略中使用。
3. 如果要删除的规则未在使用中，请选择该规则并选择*Actions*>*Remove*。您可以选择多个规则并同时删除所有规则。
4. 选择*是*确认要删除ILM规则。

查看ILM指标

您可以查看ILM的指标、例如队列中的对象数量和评估速率。您可以监控这些指标以确定系统性能。队列或评估速率较高可能表示系统无法跟上载入速率、客户端应用程序的负载过大或存在某些异常情况。

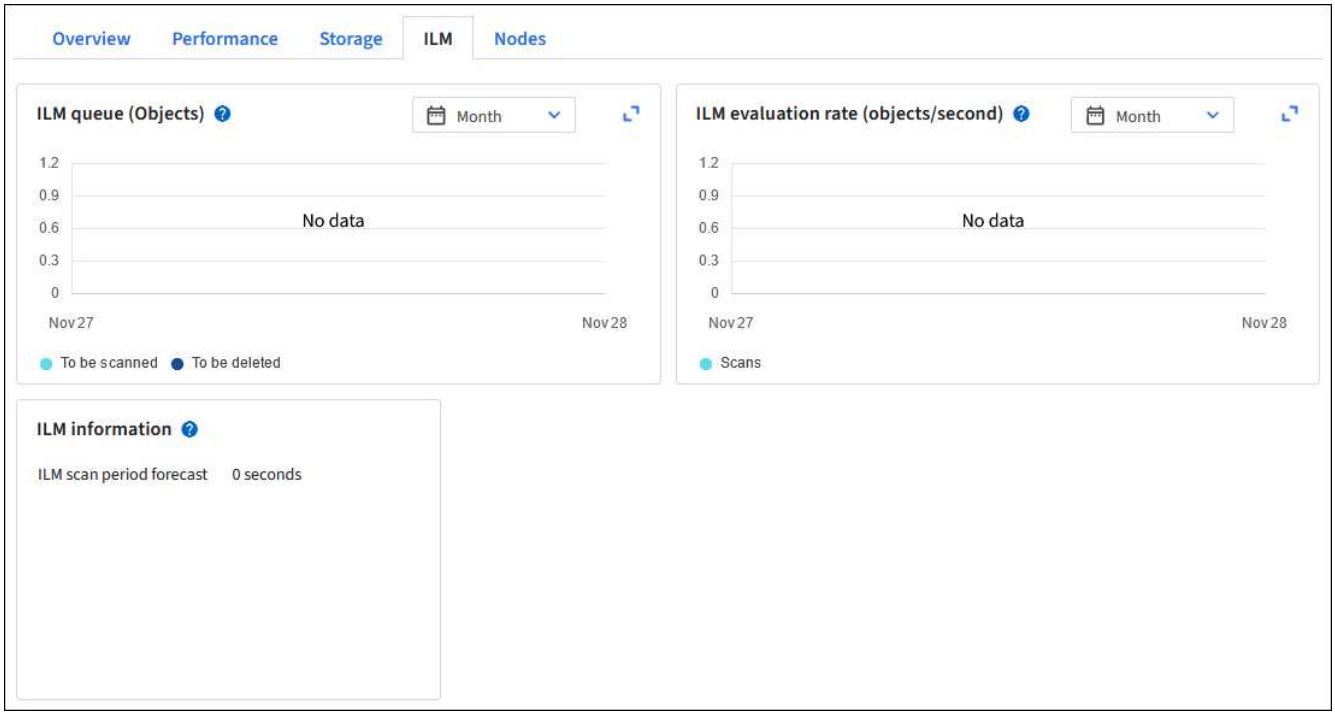
步骤

1. 选择*信息板*>* ILM *。

   由于可以自定义信息板、因此ILM选项卡可能不可用。

2. 监控ILM选项卡上的指标。

   您可以选择问号 以查看 ILM 选项卡上各项目的说明。



使用 S3 对象锁定

S3 对象锁定如何保护 StorageGRID 中的对象

作为网格管理员、您可以为StorageGRID 系统启用S3对象锁定、并实施合规的ILM策略、以帮助确保特定S3存储分段中的对象在指定时间内不会被删除或覆盖。

什么是 S3 对象锁定?

StorageGRID S3 对象锁定功能是一种对象保护解决方案，相当于 Amazon Simple Storage Service （Amazon S3 ）中的 S3 对象锁定。

当为 StorageGRID 系统启用全局 S3 对象锁定设置时，S3 租户帐户可以创建启用或未启用 S3 对象锁定的存储桶。启用现有存储桶的允许 S3 对象锁定设置后，S3 租户帐户可以为现有存储桶启用 S3 对象锁定。如果存储桶已启用 S3 对象锁定，则需要存储桶版本控制并自动启用。在 S3 租户帐户为新的或现有存储桶启用 S3 对象锁定后，无法禁用它。

*没有S3对象锁定的存储分段*只能包含没有指定保留设置的对象。任何已加热的对象都不具有保留设置。

*具有S3对象锁定*的存储分段可以包含具有和不具有S3客户端应用程序指定的保留设置的对象。已加热的某些对象将具有保留设置。

*配置了S3对象锁定和默认保留的存储分段*可以上传具有指定保留设置的对象以及没有保留设置的新对象。新对象使用默认设置、因为尚未在对象级别配置保留设置。

配置默认保留后、所有新加的对象都会具有保留设置、这一点很有效。没有对象保留设置的现有对象不受影响。

保留模式

StorageGRID S3对象锁定功能支持两种保留模式、可对对象应用不同级别的保护。这些模式相当于Amazon S3保留模式。

- 在合规模式下：
  - 在达到保留截止日期之前、无法删除此对象。
  - 对象的保留截止日期可以增加、但不能减少。
  - 在达到该日期之前、无法删除对象的保留截止日期。
- 在监管模式下：
  - 具有特殊权限的用户可以在请求中使用旁路标头来修改某些保留设置。
  - 这些用户可以在达到保留截止日期之前删除对象版本。
  - 这些用户可以增加、减少或删除对象的保留截止日期。

对象版本的保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以使用S3客户端应用程序为添加到该存储分段的每个对象指定以下保留设置(可选)：

- 保留模式：合规性或监管。
- **retain**至日期：如果某个对象版本的retain至日期为未来版本，则可以检索该对象，但不能将其删除。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。合法保留与保留日期无关。

  如果某个对象处于合法保留状态、则无论其保留模式如何、任何人都无法删除该对象。

  要了解有关对象设置的详细信息，请参阅 "使用S3 REST API配置S3对象锁定"。

存储分段的默认保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以选择为此存储分段指定以下默认设置：

- 默认保留模式：合规或监管。
- 默认保留期限：添加到此存储分段的新对象版本应保留多长时间、从添加之日开始。

默认分段设置仅适用于没有自己的保留设置的新对象。添加或更改这些默认设置时、现有存储分段对象不会受到

影响。

请参阅 "创建 S3 存储区。" 和 "更新S3对象锁定默认保留"。

比较 S3 对象锁定与原有合规性

S3 对象锁定取代了早期 StorageGRID 版本中提供的合规性功能。由于S3对象锁定功能符合Amazon S3要求、因此会弃用专有的StorageGRID合规性功能、该功能现在称为"原有合规性"。

> 全局合规性设置已弃用。如果使用以前版本的 StorageGRID 启用了此设置，则会自动启用 S3 对象锁定设置。您可以继续使用 StorageGRID 来管理现有合规存储桶的设置；但是，您无法创建新的合规存储桶。有关详细信息，请参阅 "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"。

如果您在先前版本的 StorageGRID 中使用了原有的合规性功能，请参见下表，了解它与 StorageGRID 中的 S3 对象锁定功能的比较情况。

	S3 对象锁定	合规性（原有）
如何全局启用此功能？	从网格管理器中，选择*配置* > 系统 > **S3** 对象锁。	不再支持。
如何为存储分段启用此功能？	在使用租户管理器，租户管理 API 或 S3 REST API 创建新存储分段时，用户必须启用 S3 对象锁定。	不再支持。
是否支持存储分版本控制？	是。需要分段版本控制，并且在为分段启用 S3 对象锁定时会自动启用分段版本控制。	否
如何设置对象保留？	用户可以为每个对象版本设置保留截止日期、也可以为每个存储分段设置默认保留期限。	用户必须为整个存储分段设置一个保留期限。保留期限适用场景 存储分段中的所有对象。
是否可以更改保留期限？	• 在合规模式下、对象版本的保留截止日期可以增加、但不能减少。 • 在监管模式下、具有特殊权限的用户可以减少甚至删除对象的保留设置。	存储分段的保留期限可以延长、但不能缩短。
合法保留在何处？	用户可以对存储分段中的任何对象版本进行合法保留或取消合法保留。	合法保留放置在存储分段上，并影响存储分段中的所有对象。

	S3 对象锁定	合规性（原有）
何时可以删除对象？	• 在合规模式下、可以在达到保留截止日期后删除对象版本、前提是对象不处于合法保留状态。 • 在监管模式下、具有特殊权限的用户可以在达到保留截止日期之前删除对象、前提是该对象不处于合法保留状态。	可以在保留期限到期后删除对象，前提是存储分段未处于合法保留状态。可以自动或手动删除对象。
是否支持存储分段生命周期配置？	是	否

StorageGRID 中的 **S3 Object Lock** 工作流

作为网格管理员，您必须与租户用户密切协调，以确保对象受到保护，并满足其保留要求。

根据网络连接、节点状态和cassandr操作、在网格中应用租户设置可能需要15分钟或更长时间。

以下网格管理员和租户用户列表包含使用S3对象锁定功能的高级别任务。

网格管理员

- 为整个StorageGRID系统启用全局S3对象锁定设置。
- 允许用户为现有存储桶启用 S3 对象锁定。
- 确保信息生命周期管理(ILM)策略符合_合规_，即符合"启用了S3对象锁定的分段的要求"。
- 根据需要、允许租户使用合规性作为保留模式。否则、仅允许使用监管模式。
- 根据需要为租户设置最长保留期限。

租户用户

- 查看使用S3对象锁定的存储分段和对象的注意事项。
- 根据需要，联系网格管理员以启用以下设置之一：
  - 全局 S3 对象锁定
  - 允许为现有存储桶启用 S3 对象锁定
- 创建启用了S3对象锁定的分段。
- 在现有存储桶上启用 S3 对象锁定。
- (可选)配置存储分段的默认保留设置：
  - 默认保留模式：监管或合规(如果网格管理员允许)。
  - 默认保留期限：必须小于或等于网格管理员设置的最长保留期限。
- 使用S3客户端应用程序添加对象并可选择设置对象专用保留：
  - 保留模式。监管或合规性(如果网格管理员允许)。
  - 保留截止日期：必须小于或等于网格管理员设置的最长保留期限所允许的值。

相关信息

了解 "S3 Object Lock 要求"

StorageGRID 中的 **S3** 对象锁定要求

您必须查看启用全局 S3 对象锁定设置的要求，创建合规 ILM 规则和 ILM 策略的要求以及 StorageGRID 对使用 S3 对象锁定的分段和对象所施加的限制。

使用全局 **S3** 对象锁定设置的要求

- 您必须先使用网格管理器或网格管理 API 启用全局 S3 对象锁定设置，然后任何 S3 租户才能创建启用了 S3 对象锁定的分段。
- 启用全局 S3 对象锁定设置后，所有 S3 租户帐户都可以在启用了 S3 对象锁定的情况下创建存储分段。
- 启用全局S3对象锁定设置后、无法禁用该设置。
- 除非所有活动ILM策略中的默认规则均为_兼容_(即、默认规则必须符合启用了S3对象锁定的分段的要求)、否则无法启用全局S3对象锁定。
- 启用全局S3对象锁定设置后、您无法创建新的ILM策略或激活现有ILM策略、除非该策略中的默认规则合规。启用全局S3对象锁定设置后、ILM规则和ILM策略页面将指示哪些ILM规则合规。

允许在现有存储桶上启用 **S3** 对象锁定的要求

启用全局 S3 对象锁定设置后，您可以选择允许所有具有权限的 S3 租户帐户或 S3 用户在现有存储桶上启用 S3 对象锁定。当 S3 租户帐户或 S3 用户在现有存储桶上启用 S3 对象锁定时，可能会导致意外的数据从云存储池迁移回 StorageGRID，具体取决于您的 ILM 规则。

意外数据迁移启动后无法停止。

符合 **ILM** 规则的要求

如果要启用全局S3对象锁定设置、则必须确保所有活动ILM策略中的默认规则合规。合规规则可满足启用了 S3 对象锁定的两个存储分段以及启用了旧合规性的任何现有存储分段的要求：

- 它必须至少创建两个复制的对象副本或一个经过纠删编码的副本。
- 这些副本必须在放置说明中每行的整个持续时间内存在于存储节点上。
- 无法将对象副本保存在云存储池中。
- 至少一行放置指令必须从第0天开始、并使用*内嵌时间*作为参考时间。
- 放置说明中至少有一行必须为"永久"。

ILM策略的要求

启用全局S3对象锁定设置后、活动和非活动ILM策略可以同时包含合规和不合规规则。

- 活动或非活动ILM策略中的默认规则必须合规。
- 不合规规则仅适用于未启用S3对象锁定或未启用原有合规性功能的分段中的对象。
- 合规规则可以应用于任何存储分段中的对象；不需要为此存储分段启用 S3 对象锁定或原有合规性。

"S3对象锁定的合规ILM策略示例"

启用了 **S3** 对象锁定的存储分段的要求

- 如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以使用租户管理器，租户管理 API 或 S3 REST API 创建启用了 S3 对象锁定的分段。
- 为存储分段启用 S3 对象锁定后， StorageGRID 会自动为该存储分段启用版本控制。您不能禁用存储分段的S3对象锁定或暂停版本控制。
- 您也可以使用租户管理器、租户管理API或S3 REST API为每个存储分段指定默认保留模式和保留期限。存储分段的默认保留设置仅适用于添加到存储分段中但没有自己的保留设置的新对象。您可以通过在上传每个对象版本时为其指定保留模式和保留截止日期来覆盖这些默认设置。
- 启用了S3对象锁定的分段支持分段生命周期配置。

启用了 **S3** 对象锁定的分段中的对象的要求

- 要保护对象版本、您可以为存储分段指定默认保留设置、也可以为每个对象版本指定保留设置。可以使用S3客户端应用程序或S3 REST API指定对象级保留设置。
- 保留设置适用于各个对象版本。对象版本可以同时具有保留截止日期和合法保留设置，但不能具有其他设置，或者两者均不具有。为对象指定保留日期或合法保留设置仅保护请求中指定的版本。您可以创建新版本的对象，而先前版本的对象仍保持锁定状态。

启用了 **S3** 对象锁定的存储分段中的对象生命周期

在启用了S3对象锁定的情况下保存在存储分段中的每个对象都会经历以下阶段：

1. * 对象载入 *

   将对象版本添加到启用了S3对象锁定的存储分段时、将按如下所示应用保留设置：

   - 如果为对象指定了保留设置、则会应用对象级别设置。系统将忽略任何默认存储分段设置。
   - 如果没有为对象指定保留设置、则会应用默认存储分段设置(如果存在)。
   - 如果没有为对象或存储分段指定保留设置、则对象不受S3对象锁定保护。

   如果应用了保留设置、则对象和任何S3用户定义的元数据都会受到保护。

2. 对象保留和删除

   StorageGRID 会在指定的保留期限内存储每个受保护对象的多个副本。对象副本的确切数量和类型以及存储位置由活动ILM策略中的合规规则决定。是否可以在达到保留截止日期之前删除受保护对象取决于其保留模式。

   - 如果某个对象处于合法保留状态、则无论其保留模式如何、任何人都无法删除该对象。

相关信息

- "创建 S3 存储区。"
- "更新S3对象锁定默认保留"
- "使用S3 REST API配置S3对象锁定"
- "示例 7： S3 对象锁定的兼容 ILM 策略"

在 StorageGRID 中启用 S3 Object Lock

如果 S3 租户帐户在保存对象数据时需要遵守法规要求，则必须为整个 StorageGRID 系统启用 S3 对象锁定。启用全局 S3 对象锁定设置后，任何 S3 租户用户都可以使用 S3 对象锁定创建和管理存储分段和对象。

开始之前

- 您拥有"root访问权限"。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您已查看S3对象锁定工作流、并了解注意事项。
- 您已确认活动 ILM 策略中的默认规则是合规的。有关详细信息，请参见 "创建默认 ILM 规则"。

关于此任务

网格管理员必须启用全局 S3 对象锁定设置，以允许租户用户创建启用了 S3 对象锁定的新分段。启用此设置后、将无法禁用它。

启用 S3 对象锁定后，网格管理员还可以允许租户用户在现有存储桶上启用 S3 对象锁定。网格管理员启用此设置后，可以将其禁用。有关详细信息，请参阅"S3 Object Lock 要求"。

启用全局S3对象锁定设置后、请查看现有租户的合规性设置。启用此设置时、每个租户的S3对象锁定设置取决于创建租户时的StorageGRID版本。

> 全局合规性设置已弃用。如果使用以前版本的 StorageGRID 启用了此设置，则会自动启用 S3 对象锁定设置。您可以继续使用 StorageGRID 来管理现有合规存储桶的设置；但是，您无法创建新的合规存储桶。有关详细信息，请参阅 "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"。

步骤

1. 选择*配置* > 系统 > **S3** 对象锁。

   此时将显示 "S3 Object Lock Settings" 页面。

2. 选择 **Enable S3 Object Lock** 为您的整个 StorageGRID 系统启用 S3 对象锁定。
3. （可选）选择 **Allow S3 Object Lock to be enabled on existing buckets**。

   > 在现有存储桶上启用 S3 对象锁定可能会导致数据意外从云存储池迁移回 StorageGRID，具体取决于您的 ILM 规则。此迁移启动后无法停止。有关详细信息，请参阅 "S3 Object Lock 要求"。

4. 选择 * 应用 * 。

   此时将显示一个确认对话框、提醒您在启用S3对象锁定后无法禁用它。

5. 如果确实要为整个系统永久启用 S3 对象锁定，请选择 * 确定 * 。

   选择 * 确定 * 时：

   - 如果活动ILM策略中的默认规则合规、则会为整个网格启用S3对象锁定、并且无法禁用。

- 如果默认规则不合规，则会出现错误。您必须创建并激活一个新的 ILM 策略，其中包含一个合规规则作为其默认规则。选择 **OK**。然后，创建新策略，模拟并激活它。有关说明，请参阅 "创建 ILM 策略"。

解决在 **StorageGRID** 中更新 **S3 Object Lock** 或旧版合规性设置时的一致性错误

如果一个站点上的一个数据中心站点或多个存储节点不可用，您可能需要帮助 S3 租户用户对 S3 对象锁定或原有合规性配置进行更改。

启用了 S3 对象锁定（或原有合规性）的存储分段的租户用户可以更改某些设置。例如，使用 S3 对象锁定的租户用户可能需要将对象版本置于合法保留状态。

当租户用户更新 S3 存储分段或对象版本的设置时， StorageGRID 会尝试立即更新整个网格中的存储分段或对象元数据。如果由于数据中心站点或多个存储节点不可用而导致系统无法更新元数据、则系统将返回错误：

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

要解决此错误，请执行以下步骤：

1. 尝试尽快使所有存储节点或站点重新可用。
2. 如果您无法在每个站点提供足够的存储节点，请联系技术支持，他们可以帮助您恢复节点并确保在网格中一致地应用更改。
3. 解决底层问题描述 后，提醒租户用户重试其配置更改。

相关信息

- "使用租户帐户"
- "使用S3 REST API"
- "恢复和维护"

ILM 规则和策略示例

StorageGRID 中基本对象保护和保留的 **ILM** 规则和策略

在定义 ILM 策略以满足对象保护和保留要求时，您可以使用以下示例规则和策略作为起点。

> 以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

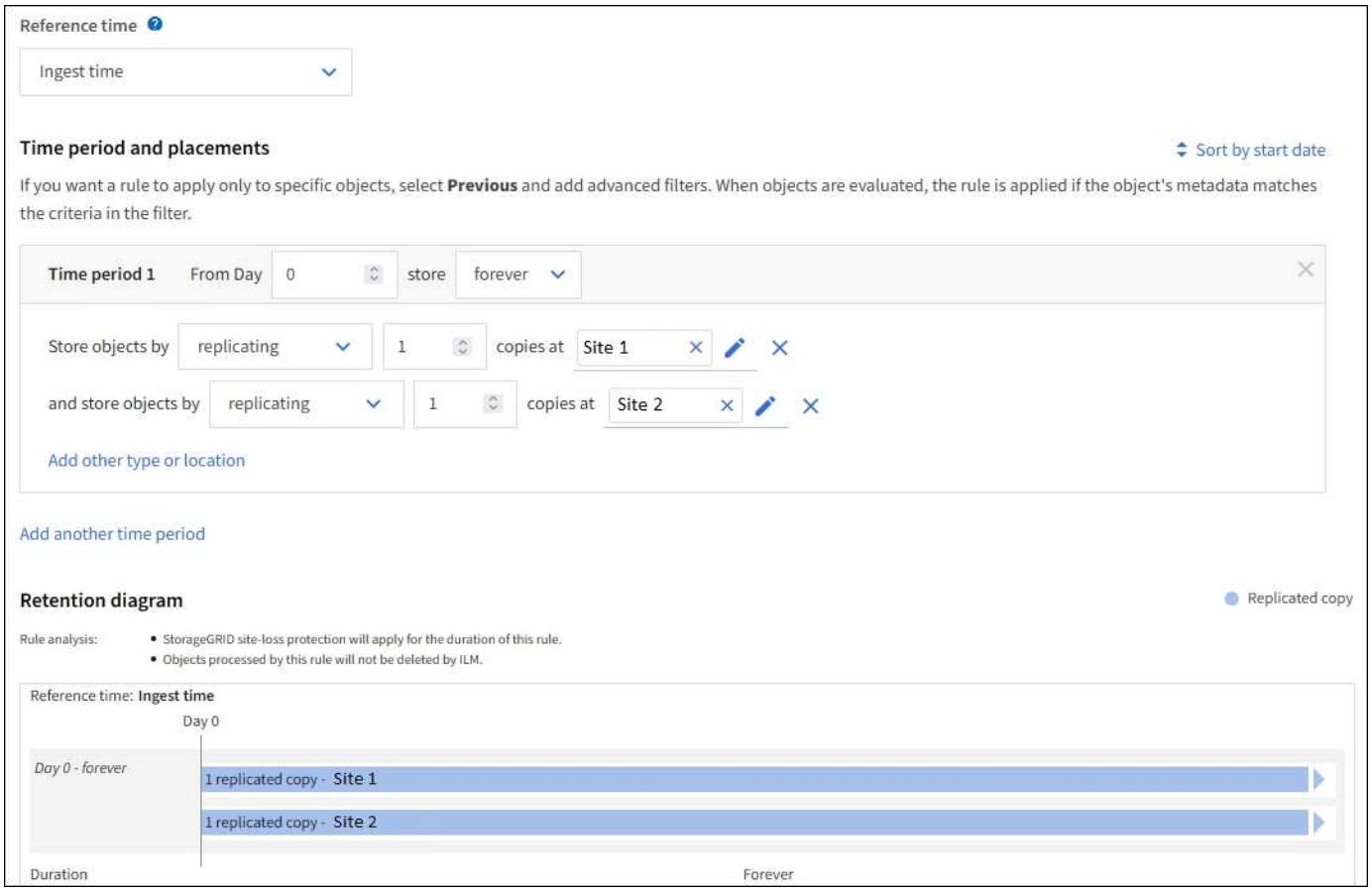
ILM规则**1**示例**1**：将对象数据复制到两个站点

此示例ILM规则会将对象数据复制到两个站点中的存储池。

规则定义	示例值
单站点存储池	两个存储池、每个存储池包含不同的站点、分别名为站点1和站点2。
规则名称	两个副本两个站点
参考时间	载入时间
放置	在Day 0 to Forever、在站点1和站点2各保留一个复制副本。

保留图的规则分析部分指出：

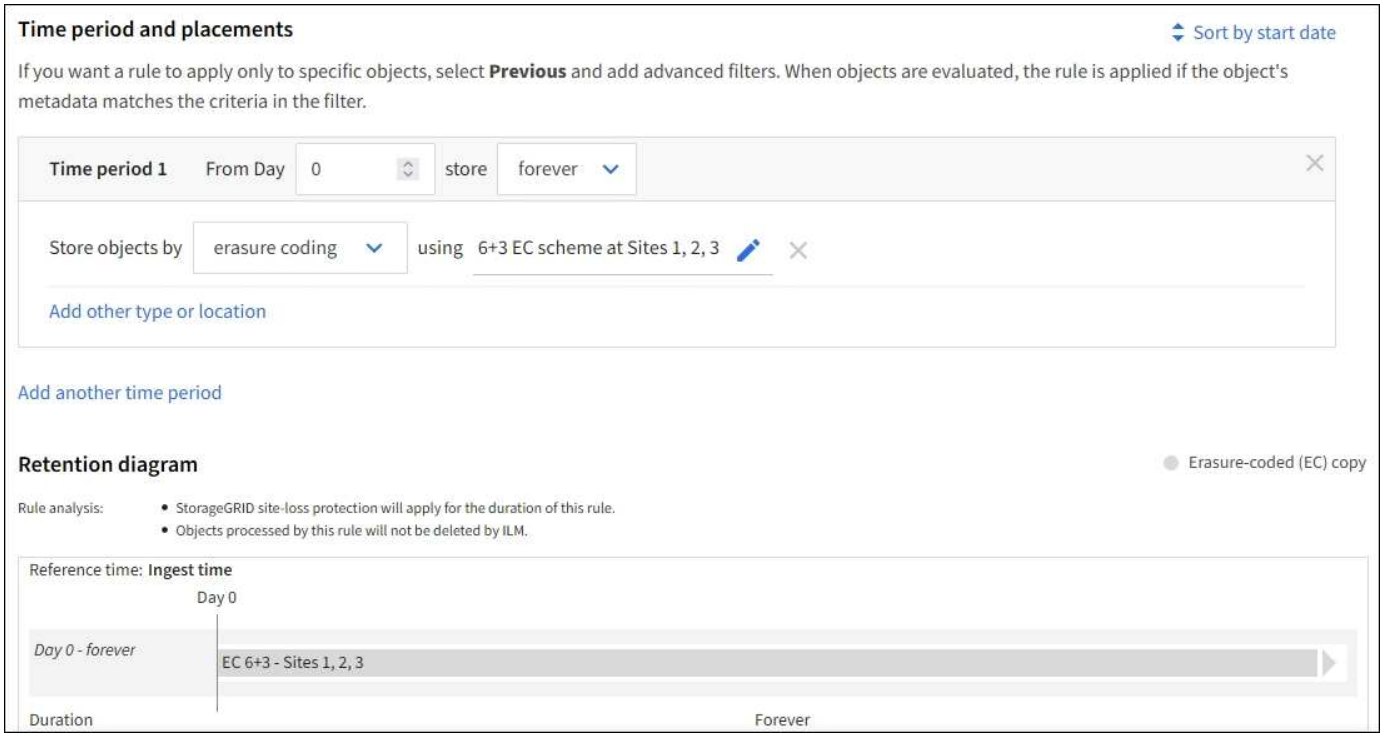
- 在此规则有效期内、StorageGRID 站点丢失保护将适用。
- ILM不会删除此规则处理的对象。



ILM规则**2**示例**1**：具有存储分段匹配的纠删编码配置文件

此示例ILM规则使用纠删编码配置文件和S3存储分段来确定对象的存储位置和时长。

规则定义	示例值
包含多个站点的存储池	• 三个站点(站点1、2、3)中的一个存储池 • 使用 6+3 纠删编码方案
规则名称	S3存储分段财务记录
参考时间	载入时间
放置	对于S3存储分段中名为Finance—记录的对象、请在纠删编码配置文件指定的池中创建一个纠删编码副本。请永久保留此副本。

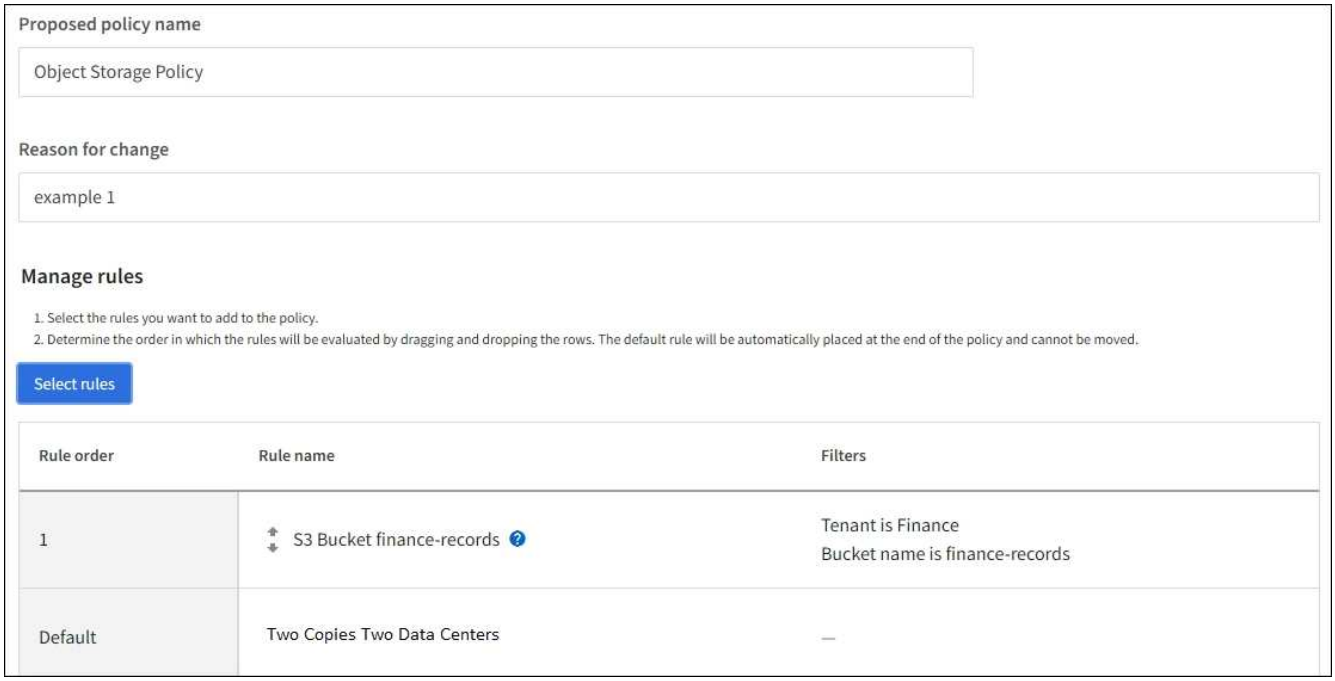


ILM 策略示例 **1**

实际上、大多数ILM策略都很简单、即使StorageGRID 系统允许您设计复杂的ILM策略也是如此。

多站点网格的典型ILM策略可能包括以下ILM规则：

- 载入时、将属于S3存储分段的所有对象存储 `finance-records`在包含三个站点的存储池中。使用6+3纠删编码。
- 如果某个对象与第一个ILM规则不匹配、请使用策略的默认ILM规则、两个副本两个数据中心、以便在站点1中存储该对象的一个副本、在站点2中存储一个副本。



相关信息

- "使用ILM策略"
- "创建ILM策略"

StorageGRID 中用于 **EC** 对象大小过滤的 **ILM** 规则和策略

您可以使用以下示例规则和策略作为起点来定义一个 ILM 策略，该策略按对象大小进行筛选以满足建议的 EC 要求。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

ILM 规则 **1** 示例 **2**： 对大于 **1 MB** 的对象使用 **EC**

此示例中的 ILM 规则擦除将对大于 1 MB 的对象进行编码。

纠删编码最适合大于 1 MB 的对象。不要对小于200 KB的对象使用纠删编码、以避免管理非常小的经过纠删编码的片段所产生的开销。

规则定义	示例值
规则名称	仅EC对象> 1 MB
参考时间	载入时间
对象大小高级筛选器	对象大小大于1 MB

规则定义	示例值
放置	使用三个站点创建 2+1 纠删编码副本



ILM 规则 **2** 示例 **2**： 两个复制副本

此示例 ILM 规则将创建两个复制副本，而不按对象大小进行筛选。此规则是策略的默认规则。由于第一个规则会筛选出大于 1 MB 的所有对象，因此此规则仅筛选 1 MB 或更小的适用场景 对象。

规则定义	示例值
规则名称	两个复制副本
参考时间	载入时间
对象大小高级筛选器	无
放置	在Day 0 to Forever、在站点1和站点2各保留一个复制副本。

示例 **2** 中的 **ILM** 策略：对大于 **1 MB** 的对象使用 **EC**

此示例 ILM 策略包括两个 ILM 规则：

- 第一个规则擦除将对大于 1 MB 的所有对象进行编码。
- 第二个（默认） ILM 规则会创建两个复制副本。由于规则 1 已筛选出大于 1 MB 的对象，因此规则 2 仅筛选 1 MB 或更小的适用场景 对象。

用于在 **StorageGRID** 中保护映像文件的 **ILM** 规则和策略

您可以使用以下示例规则和策略来确保对大于1 MB的映像进行了删除编码、并使用较小的映像创建两个副本。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

ILM 规则 **1** ，例如 **3**： 对大于 **1 MB** 的映像文件使用 **EC**

此示例 ILM 规则使用高级筛选功能对大于 1 MB 的所有映像文件进行擦除代码。

纠删编码最适合大于 1 MB 的对象。不要对小于200 KB的对象使用纠删编码、以避免管理非常小的经过纠删编码的片段所产生的开销。

规则定义	示例值
规则名称	EC映像文件> 1 MB
参考时间	载入时间
对象大小高级筛选器	对象大小大于1 MB
密钥的高级筛选器	• 以.jpg结尾 • 以.png结尾
放置	使用三个站点创建 2+1 纠删编码副本



由于此规则已配置为策略中的第一个规则、因此纠删编码放置指令仅适用于大于1 MB的适用场景 .jpg和.jpg文件。

ILM 规则 **2** 示例 **3**： 为其余所有映像文件创建 **2** 个复制副本

此示例 ILM 规则使用高级筛选来指定复制较小的映像文件。由于策略中的第一个规则已与大于 1 MB 的映像文件匹配，因此此规则会对 1 MB 或更小的适用场景 映像文件进行匹配。

规则定义	示例值
规则名称	2个映像文件副本
参考时间	载入时间
密钥的高级筛选器	• 以.jpg结尾 • 以.png结尾
放置	在两个存储池中创建2个复制副本

示例 3 中的 ILM 策略：更好地保护映像文件

此示例 ILM 策略包括三个规则：

- 第一个规则擦除会对大于 1 MB 的所有映像文件进行编码。
- 第二条规则会为任何剩余映像文件（即 1 MB 或更小的映像）创建两个副本。
- 默认规则适用场景 所有剩余对象（即任何非映像文件）。

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

StorageGRID 中非当前 S3 对象版本的 ILM 规则和策略

如果您的S3存储分段启用了版本控制、则可以通过在ILM策略中包含使用"非当前时间"作为参考时间的规则来管理非当前对象版本。

如果为对象指定了有限的保留时间、则在达到该时间段后、这些对象将被永久删除。确保您了解对象的保留时间。

如本示例所示，您可以通过对非当前对象版本使用不同的放置说明来控制受版本控制的对象使用的存储量。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

要对非最新版本的对象执行ILM策略模拟、您必须知道对象版本的UUID或CBID。要查找UUID和CBID、请在对象仍为最新时使用"对象元数据查找"。

ILM 规则 1 示例 4： 保存三个副本并保留 10 年

此示例ILM规则会将每个对象的副本存储在三个站点上、为期10年。

此规则将适用场景 所有对象，无论它们是否已受版本控制。

规则定义	示例值
存储池	三个存储池、每个存储池由不同的数据中心组成、分别命名为站点1、站点2和站点3。

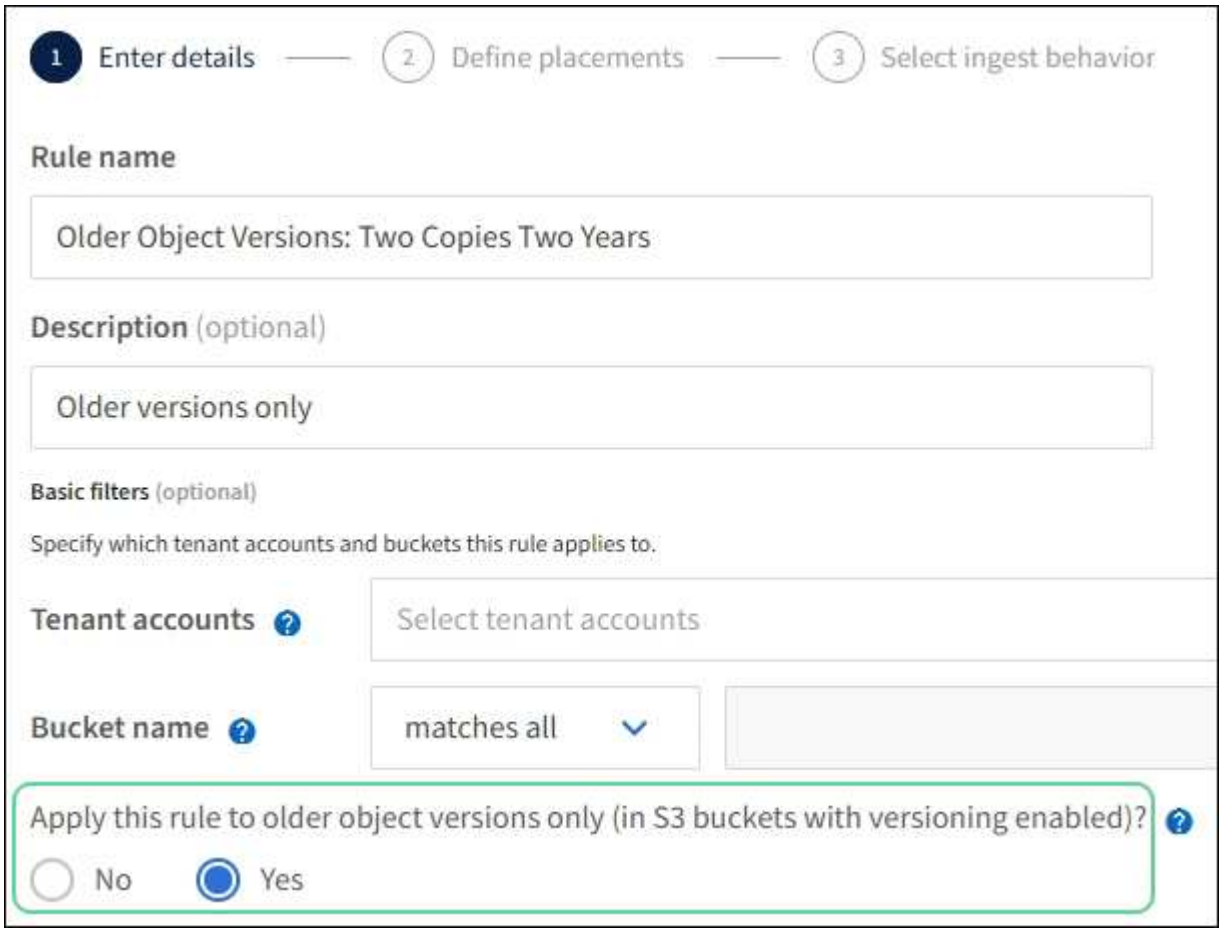
规则定义	示例值
规则名称	三个副本十年
参考时间	载入时间
放置	在第0天、将三个复制副本保留10年(3、752天)、一个在站点1、一个在站点2、一个在站点3。10 年后，删除对象的所有副本。

ILM 规则 **2** 示例 **4**： 将两个非最新版本副本保存 **2** 年

此示例 ILM 规则会将 S3 版本对象的两个非最新版本副本存储 2 年。

由于 ILM 规则 1 会对对象的所有版本进行适用场景 处理，因此您必须创建另一个规则来筛选出任何非最新版本。

要创建使用"非当前时间"作为参考时间的规则、请为问题"仅将此规则应用于较旧的对象版本(在启用了版本控制的S3存储分段中)？"选择*是* 在创建ILM规则向导的步骤1 (输入详细信息)中。选择*是*时，系统会自动为参考时间选择_noncurrent time_，您不能选择其他参考时间。



在此示例中，仅存储两个非最新版本副本，这些副本将存储两年。

规则定义	示例值
存储池	两个存储池、分别位于不同的数据中心站点1和站点2。
规则名称	非最新版本：两个副本，两年
参考时间	非当前时间 当您为"仅将此规则应用于较旧的对象版本(在启用了版本控制的S3存储分段中)？"问题选择*是*时、系统会自动选中此选项 在创建ILM规则向导中。
放置	在相对于非当前时间的第0天(即、从对象版本成为非当前版本之日开始)、将非当前对象版本的两个复制副本保留2年(730天)、一个在站点1、一个在站点2。2 年后，删除非最新版本。

ILM 策略示例 **4**： **S3** 版本对象

如果要以与当前版本不同的方式管理对象的旧版本、则使用"非当前时间"作为参考时间的规则必须显示在ILM策略中、然后才会显示应用于当前对象版本的规则。

S3 版本对象的 ILM 策略可能包括以下 ILM 规则：

- 从每个对象的任何较旧（非最新）版本变为非最新版本之日起，保留两年。

> 策略中必须先显示"非当前时间"规则、然后再显示应用于当前对象版本的规则。否则、"非当前时间"规则将永远无法匹配非当前对象版本。

- 在执行数据加热时、创建三个复制副本、并在三个站点中的每个站点上存储一个副本。将当前对象版本的副本保留 10 年。

模拟此示例策略时，您希望按如下所示评估测试对象：

- 第一个规则将匹配任何非最新的对象版本。如果非当前对象版本超过 2 年，则 ILM 会将其永久删除（非当前版本的所有副本都会从网格中删除）。
- 当前对象版本将与第二个规则匹配。当当前对象版本已存储10年时、ILM过程会添加一个删除标记作为对象的当前版本、并使以前的对象版本"非当前"。下次进行ILM评估时、此非最新版本将与第一条规则匹配。因此、站点3上的副本将被清除、站点1和站点2上的两个副本将再存储2年。

相关信息

"如何删除对象"

StorageGRID 中严格摄取行为的 **ILM** 规则和策略

您可以在规则中使用位置筛选器和严格的载入行为来防止对象保存在特定数据中心位置。

在本示例中，基于巴黎的租户出于监管方面的考虑，不希望在欧盟以外存储某些对象。其他对象，包括来自其他租户帐户的所有对象，可以存储在巴黎数据中心或美国数据中心。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

相关信息

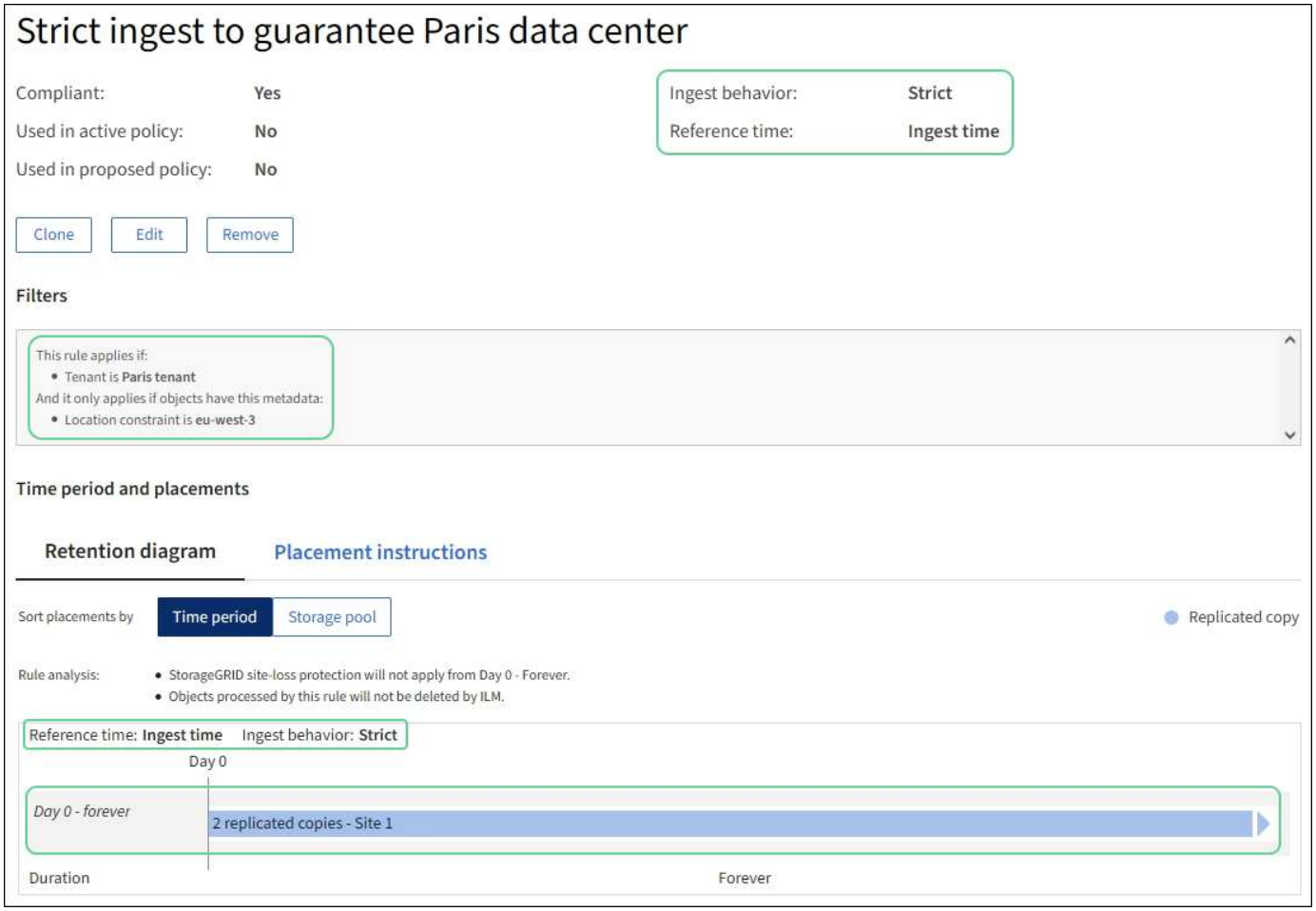
- "加热选项"
- "创建ILM规则：选择加热行为"

ILM 规则 **1** 示例 **5**： 严格载入以保证巴黎数据中心

此示例 ILM 规则使用严格的载入行为来保证，在将区域设置为 EU-west-3 区域（巴黎）的情况下，基于巴黎的租户保存到 S3 分段的对象永远不会存储在美国数据中心。

此规则属于巴黎租户且 S3 分段区域设置为 EU-west-3 （巴黎）的适用场景 对象。

规则定义	示例值
租户帐户	巴黎租户
高级筛选器	位置约束等于EU-w西-3
存储池	站点1 (巴黎)
规则名称	严格载入以保证巴黎数据中心的安全
参考时间	载入时间
放置	在第0天、在站点1 (巴黎)中永久保留两个复制的副本
加热行为	严格。请始终在载入时使用此规则的放置位置。如果无法在巴黎数据中心存储对象的两个副本，则载入将失败。



ILM 规则 **2** 示例 **5**： 平衡其他对象的载入

此示例 ILM 规则使用平衡载入行为为第一个规则不匹配的任何对象提供最佳 ILM 效率。将存储与此规则匹配的所有对象的两个副本—一个在美国数据中心，一个在巴黎数据中心。如果无法立即满足规则、临时副本将存储在任何可用位置。

此规则适用于属于任何租户和任何区域的适用场景 对象。

规则定义	示例值
租户帐户	忽略
高级筛选器	未指定 _
存储池	站点1 (巴黎)和站点2 (美国)
规则名称	2 个副本 2 个数据中心
参考时间	载入时间
放置	在第 0 天，将两个复制副本永久保留在两个数据中心

规则定义	示例值
加热行为	平衡。如果可能，与此规则匹配的对象将根据规则的放置说明进行放置。否则，会在任何可用位置创建临时副本。

ILM 策略示例 **5** ： 结合载入行为

示例 ILM 策略包括两个具有不同载入行为的规则。

使用两种不同载入行为的 ILM 策略可能包括以下 ILM 规则：

- 仅在巴黎数据中心存储属于 PARIS 租户且 S3 存储分段区域设置为 EU-west-3 （ PARIS ）的对象。如果 PARIS 数据中心不可用，则无法载入。
- 将所有其他对象（包括属于巴黎租户但具有不同分段区域的对象）存储在美国数据中心和巴黎数据中心。如果放置说明不能满足要求、请在任何可用位置创建临时副本。

模拟示例策略时，您希望按如下所示评估测试对象：

- 属于 PARIS 租户且 S3 存储分段区域设置为 EU-west-3 的任何对象均按第一个规则匹配，并存储在 PARIS 数据中心。由于第一个规则使用严格的载入，因此这些对象永远不会存储在美国数据中心。如果巴黎数据中心的存储节点不可用、则加载将失败。
- 第二个规则将匹配所有其他对象、包括属于PARIS租户且未将S3存储分段区域设置为EU-WEI-3的对象。每个对象的一份副本保存在每个数据中心。但是，由于第二条规则使用平衡载入，因此，如果一个数据中心不可用，则会在任何可用位置保存两个临时副本。

更改 **ILM** 策略如何影响 **StorageGRID** 性能

如果需要更改数据保护或添加新站点、则可以创建并激活新的ILM策略。

在更改策略之前，您必须了解 ILM 放置的更改如何临时影响 StorageGRID 系统的整体性能。

在此示例中、扩展中添加了一个新的StorageGRID 站点、需要实施一个新的活动ILM策略、以便在新站点上存储数据。要实施新的活动策略，请首先"创建策略"。之后、您必须"模拟"先执行新策略、然后再"激活"执行新策略。

> 以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

更改**ILM**策略如何影响性能

激活新的 ILM 策略时， StorageGRID 系统的性能可能会暂时受到影响，尤其是在新策略中的放置说明要求将许多现有对象移动到新位置时。

激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

要确保新的ILM策略不会影响现有复制的和经过删除编码的对象的放置，您可以"创建具有"加网时间"筛选器的ILM规则"。例如，**Ingt time _is on or after _<date and time> _**，这样新规则只适用于在指定日期和时间或之后插入的对象。

可能会暂时影响 StorageGRID 性能的 ILM 策略更改类型包括：

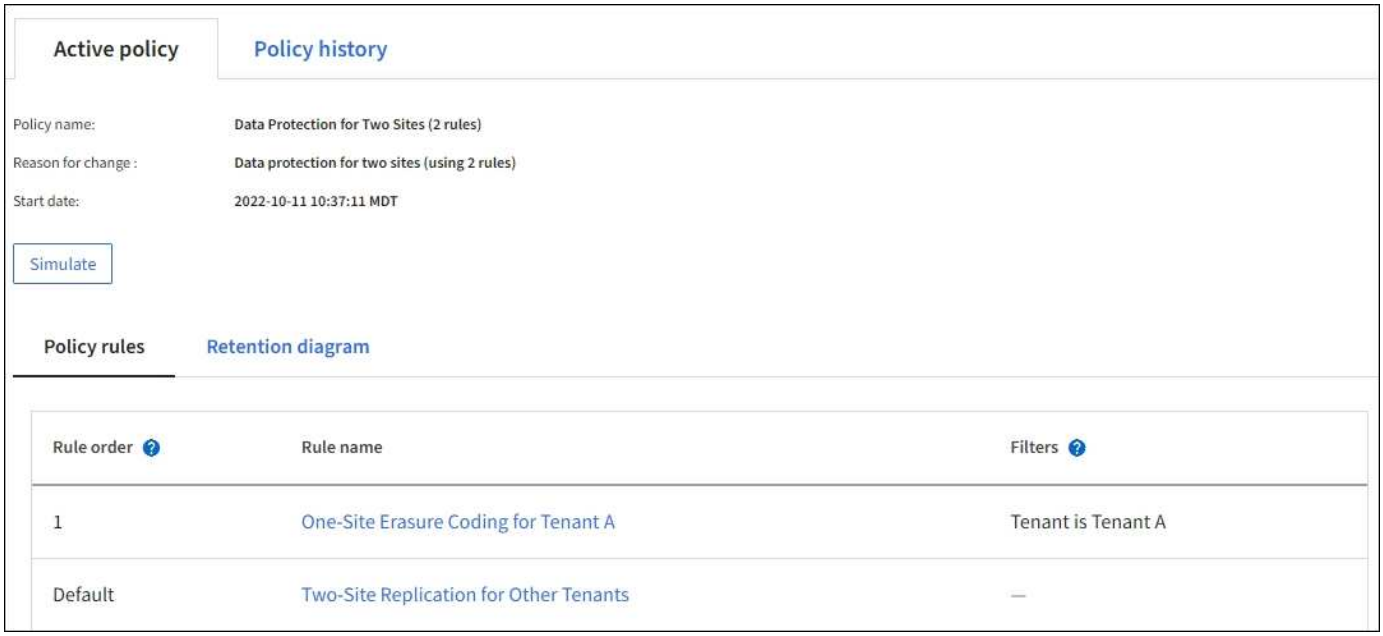
- 将不同的纠删编码配置文件应用于现有的纠删编码对象。

> StorageGRID认为每个纠删编码配置文件都是唯一的、在使用新配置文件时不会重复使用纠删编码片段。

- 更改现有对象所需的副本类型；例如，将大量复制对象转换为经过纠删编码的对象。
- 将现有对象的副本移动到完全不同的位置；例如，将大量对象移入或移出云存储池，或者移动到远程站点或从远程站点移动。

示例 **6** 中的活动 **ILM** 策略：两个站点的数据保护

在此示例中，活动 ILM 策略最初是为双站点 StorageGRID 系统设计的，并使用两个 ILM 规则。



在此 ILM 策略中，属于租户 A 的对象在一个站点上通过 2+1 纠删编码进行保护，而属于所有其他租户的对象则通过双副本复制在两个站点之间进行保护。

规则 **1**： 租户 **A** 的单站点纠删编码

规则定义	示例值
规则名称	租户 A 的单站点擦除编码
租户帐户	租户 A
存储池	站点1
放置	站点1中2+1纠删编码从第0天到永久

规则 **2**： 为其他租户进行双站点复制

规则定义	示例值
规则名称	适用于其他租户的双站点复制
租户帐户	忽略
存储池	站点1和站点2
放置	从Day 0到Forever的两个复制副本：一个副本位于站点1、一个副本位于站点2。

ILM策略例如示例**6**：在三个站点上保护数据

在此示例中、三站点StorageGRID 系统的ILM策略将被替换为新策略。

在执行扩展以添加新站点后、网格管理员创建了两个新存储池：站点3的存储池和包含所有三个站点的存储池(与所有存储节点的默认存储池不同)。然后、管理员创建了两个新的ILM规则和一个新的ILM策略、旨在保护所有三个站点的数据。

激活此新 ILM 策略后，属于租户 A 的对象将在三个站点上通过 2+1 纠删编码得到保护，而属于其他租户（以及属于租户 A 的较小对象）的对象将通过三个副本复制在三个站点上得到保护。

规则 **1**： 租户 **A** 的三站点纠删编码

规则定义	示例值
规则名称	租户 A 的三站点擦除编码
租户帐户	租户 A
存储池	所有3个站点(包括站点1、站点2和站点3)
放置	从第0天到永远、在所有3个站点中执行2+1纠删编码

规则 **2**： 对其他租户进行三站点复制

规则定义	示例值
规则名称	适用于其他租户的三站点复制
租户帐户	忽略
存储池	站点1、站点2和站点3

规则定义	示例值
放置	从Day 0到Forever的三个复制副本：一个副本位于站点1、一个副本位于站点2、一个副本位于站点3。

激活**ILM**策略、例如**6**

激活新ILM策略时、根据任何新规则或更新规则中的放置说明、现有对象可能会移动到新位置、或者可能会为现有对象创建新的对象副本。

ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。在激活策略之前，请仔细查看并模拟策略，以确认策略将按预期运行。

激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

擦除编码指令发生变化时会发生什么情况

在本示例的当前活动ILM策略中、属于租户A的对象将在站点1上使用2+1纠删编码进行保护。在新的ILM策略中、属于租户A的对象将在站点1、2和3上使用2+1纠删编码进行保护。

激活新的 ILM 策略后，将执行以下 ILM 操作：

- 租户 A 输入的新对象将拆分为两个数据片段，并添加一个奇偶校验片段。然后、这三个片段中的每一个都存储在不同的站点上。
- 属于租户 A 的现有对象将在进行 ILM 扫描过程中重新评估。由于ILM放置指令使用新的纠删编码配置文件、因此会创建全新的纠删编码片段并将其分发到三个站点。

站点1上的现有2+1片段不会重复使用。StorageGRID认为每个纠删编码配置文件都是唯一的、在使用新配置文件时不会重复使用纠删编码片段。

复制指令发生变化时会发生什么情况

在此示例中、在当前活动的ILM策略中、属于其他租户的对象将通过站点1和2的存储池中的两个复制副本受到保护。在新的ILM策略中、属于其他租户的对象将使用站点1、2和3的存储池中的三个复制副本进行保护。

激活新的 ILM 策略后，将执行以下 ILM 操作：

- 当租户A以外的任何租户都加入新对象时、StorageGRID 会创建三个副本、并在每个站点保存一个副本。
- 属于这些其他租户的现有对象将在进行中的 ILM 扫描过程中重新评估。由于站点1和站点2上的现有对象副本仍然满足新ILM规则的复制要求、因此StorageGRID 只需要为站点3创建一个新的对象副本。

激活此策略对性能的影响

激活此示例中的ILM策略后、此StorageGRID系统的整体性能将暂时受到影响。要为租户A的现有对象创建新的已删除编码片段、并在站点3为其他租户的现有对象创建新的复制副本、需要使用高于正常级别的网格资源。

由于 ILM 策略发生更改，客户端读取和写入请求可能会暂时出现比正常延迟高的情况。在整个网格中完全实施放置说明后，延迟将恢复到正常水平。

为了避免激活新ILM策略时出现资源问题、您可以在任何可能更改大量现有对象位置的规则中使用"IngTime advanced"筛选器。将"Inged Time (启动时间)"设置为大于或等于新策略生效的大致时间、以确保现有对象不会发生不必要的移动。

如果在 ILM 策略更改后需要降低或提高对象的处理速度，请联系技术支持。

StorageGRID 中 **S3 Object Lock** 的合规 **ILM** 策略

在定义 ILM 策略以满足启用了 S3 对象锁定的存储分段中对象的对象保护和保留要求时，您可以在此示例中使用 S3 存储分段， ILM 规则和 ILM 策略作为起点。

如果您在先前的 StorageGRID 版本中使用了原有合规性功能，则也可以使用此示例来帮助管理启用了原有合规性功能的任何现有存储分段。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。

相关信息

- "使用 S3 对象锁定管理对象"
- "创建ILM策略"

S3 对象锁定的分段和对象示例

在此示例中，名为 Bank of ABC 的 S3 租户帐户使用租户管理器创建了一个启用了 S3 对象锁定的存储分段，用于存储重要的银行记录。

存储分段定义	示例值
租户帐户名称	ABC 银行
分段名称	银行记录
存储分段区域	us-east-1 （默认）

添加到银行记录分段的每个对象和对象版本将对和 `legal hold`设置使用以下值 `retain-until-date。

为每个对象设置	示例值
`retain-until-date`	"2030-12-30T23：59：59Z"(2030年12月30日) 每个对象版本都有自己的 `retain-until-date`设置。此设置可以增加，但不能减少。

为每个对象设置	示例值
`legal hold`	"Off"(关闭)(无效) 在保留期限内，可以随时对任何对象版本进行合法保留或取消合法保留。如果对象处于合法保留状态、则即使已访问、也无法删除该对象 `retain-until-date`。

适用于**S3**对象锁定的**ILM**规则**1**示例：具有存储分段匹配的纠删编码配置文件

此示例 ILM 规则仅适用于名为 ABC 银行的 S3 租户帐户。它会匹配存储分段中的任何对象 `bank-records`、然后使用纠删编码将对象存储在三个数据中心站点上、并使用6+3纠删编码配置文件。此规则可满足启用了S3对象锁定的存储分段的要求：使用"数据加载时间"作为参考时间、从第0天到永远在存储节点上保留一个副本。

规则定义	示例值
规则名称	合规规则：银行记录分段中的EC对象- ABC银行
租户帐户	ABC 银行
分段名称	`bank-records`
高级筛选器	对象大小（ MB ）大于 1 *注：*此筛选器可确保擦除编码不会用于1 MB或更小的对象。

规则定义	示例值
参考时间	载入时间
放置	从 Day 0 存储永久存储
纠删编码配置文件	• 在三个数据中心站点的存储节点上创建经过擦除编码的副本 • 使用 6+3 纠删编码方案

适用于 **S3** 对象锁定的 **ILM** 规则 **2** 示例：不合规规则

此示例 ILM 规则最初会将两个复制的对象副本存储在存储节点上。一年后，它会将一个副本永久存储在云存储池中。由于此规则使用云存储池，因此它不符合要求，并且不会应用于启用了 S3 对象锁定的分段中的对象。

规则定义	示例值
规则名称	不合规规则：使用云存储池
租户帐户	未指定

规则定义	示例值
Bucket Name	未指定、但仅适用于未启用S3对象锁定(或原有合规性功能)的分段。
高级筛选器	未指定

规则定义	示例值
参考时间	载入时间
放置	• 在第 0 天，在数据中心 1 和数据中心 2 的存储节点上保留两个复制副本 365 天 • 1 年后，将一个复制副本永久保留在云存储池中

适用于 **S3** 对象锁定的 **ILM** 规则 **3** 示例：默认规则

此示例 ILM 规则会将对象数据复制到两个数据中心中的存储池。此合规规则是 ILM 策略中的默认规则。它不包括任何筛选器，不使用非当前参考时间，并满足启用了 S3 对象锁定的存储分段的要求：从 0 天到永久，存储节点上保留两个对象副本，并使用 Ingest 作为参考时间。

规则定义	示例值
规则名称	默认合规规则：两个副本两个数据中心
租户帐户	未指定
Bucket Name	未指定
高级筛选器	未指定

规则定义	示例值
参考时间	载入时间
放置	从 0 天到永久，请保留两个复制副本—一个在数据中心 1 的存储节点上，一个在数据中心 2 的存储节点上。

S3 对象锁定的兼容 **ILM** 策略示例

要创建有效保护系统中所有对象的 ILM 策略，包括启用了 S3 对象锁定的分段中的对象，您必须选择满足所有对象存储要求的 ILM 规则。然后、您必须模拟并激活此策略。

向策略中添加规则

在此示例中， ILM 策略包括三个 ILM 规则，其顺序如下：

1. 一种使用纠删编码保护启用了 S3 对象锁定的特定分段中大于 1 MB 的对象的合规规则。从 0 天到永久，对象存储在存储节点上。
2. 一种不合规的规则，在存储节点上创建两个复制的对象副本一年，然后将一个对象副本永久移动到云存储池。此规则不适用于启用了 S3 对象锁定的存储分段，因为它使用的是云存储池。
3. 一种默认合规规则，用于在存储节点上创建从 0 天到永久的两个复制对象副本。

模拟策略

在向策略添加规则、选择默认合规规则并排列其他规则之后、您应通过测试启用了S3对象锁定的存储分段中的对象以及其他存储分段中的对象来模拟策略。例如，在模拟示例策略时，您希望按如下所示评估测试对象：

- 第一个规则仅与 ABC 银行租户的存储分段记录中大于 1 MB 的测试对象匹配。
- 第二个规则将匹配所有其他租户帐户的所有不合规分段中的所有对象。
- 默认规则将与以下对象匹配：
  - ABC银行租户的存储分段库记录中的对象不超过1 MB。
  - 为所有其他租户帐户启用了 S3 对象锁定的任何其他分段中的对象。

激活策略

如果您完全确信新策略会按预期保护对象数据，则可以激活此策略。

S3 存储桶生命周期和 **ILM** 策略在 **StorageGRID** 中如何交互

根据您的生命周期配置、对象会遵循S3存储分段生命周期或ILM策略的保留设置。

分段生命周期优先于**ILM**策略的示例

ILM策略

- 基于非当前时间引用的规则：在第0天、保留X个副本20天
- 基于写入时间引用的规则(默认)：在第0天、将X个副本保留50天

存储分段生命周期

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

结果

- 此时将读取名为"docs/text"的对象。它与前缀"docs/"的存储分段生命周期筛选器匹配。
  - 100天后、系统将创建一个删除标记、"docs/text"将变为非最新。
  - 5天后、"文档/文本"将在自加载以来总共105天内被删除。
  - 在自数据加载以来总共200天以及自删除标记创建以来总共100天的95天后、过期的删除标记将被删除。
- 此时会摄录一个名为"Video/move"的对象。它与筛选器不匹配、并使用ILM保留策略。
  - 50天后、系统将创建删除标记、并且"视频/电影"将变为非当前状态。
  - 20天后、"视频/电影"将自加载后总共删除70天。

- 在自数据加载以来总共100天以及自删除标记创建以来的50天之后、过期的删除标记将被删除。

存储分段生命周期隐式永久保留的示例

ILM策略

- 基于非当前时间引用的规则：在第0天、保留X个副本20天
- 基于写入时间引用的规则(默认)：在第0天、将X个副本保留50天

存储分段生命周期

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

结果

- 此时将读取名为"docs/text"的对象。它与前缀"docs/"的存储分段生命周期筛选器匹配。

  此 `Expiration`操作仅适用于已过期的删除标记、这意味着将其他所有内容永久保留(以"docs/"开头)。

  删除以"docs/"开头的标记将在过期后被删除。

- 此时会摄录一个名为"Video/move"的对象。它与筛选器不匹配、并使用ILM保留策略。
  - 50天后、系统将创建删除标记、并且"视频/电影"将变为非当前状态。
  - 20天后、"视频/电影"将自加载后总共删除70天。
  - 在自数据加载以来总共100天以及自删除标记创建以来的50天之后、过期的删除标记将被删除。

使用存储分段生命周期复制**ILM**并清除过期删除标记的示例

ILM策略

- 基于非当前时间引用的规则：在第0天、保留X个副本20天
- 基于写入时间引用的规则(默认)：在第0天、永久保留X个副本

存储分段生命周期

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

结果

- ILM策略会在存储分段生命周期中重复。
  - ILM策略的永久规则旨在手动删除对象并在20天后清理非最新版本。因此、"加载时间"规则将永久保留已过期的删除标记。
  - 存储分段生命周期会在添加时复制ILM策略的行为 `"ExpiredObjectDeleteMarker": true`，这会在标记过期后删除标记
- 已加热对象。无筛选器意味着存储分段生命周期会适用场景所有对象并覆盖ILM保留设置。
  - 当租户发出对象删除请求时、系统将创建一个删除标记、并且该对象将变为非当前对象。
  - 20天后、非当前对象将被删除、并且删除标记将过期。
  - 之后不久、过期的删除标记将被删除。

StorageGRID 系统加固

了解 StorageGRID 的系统加固

系统强化是指尽可能消除 StorageGRID 系统中的安全风险的过程。

在安装和配置StorageGRID时、请遵循这些准则来帮助您满足任何规定的机密性、完整性和可用性安全目标。

您应该已经在使用行业标准的最佳实践来强化系统。例如，您对StorageGRID使用强密码，使用 HTTPS 而不是 HTTP，并在可用的情况下启用基于证书的身份验证。这些最佳实践必须包括限制物理访问以及保护物理数据中心和支持基础设施的物理和环境安全。您还必须参考适用于您的业务和地理位置的任何适用监管标准和建议。

StorageGRID遵循 "NetApp漏洞处理策略"。报告的漏洞会根据产品安全意外事件响应流程进行验证和解决。

强化StorageGRID系统时、请考虑以下事项：

- 您实施了三个**StorageGRID**网络中的哪一个网络。所有 StorageGRID 系统都必须使用网格网络，但您也可以使用管理网络，客户端网络或这两者。每个网络都有不同的安全注意事项。
- 用于**StorageGRID**系统中各个节点的平台类型。StorageGRID 节点可以部署在 VMware 虚拟机上， Linux 主机上的容器引擎中或作为专用硬件设备。每种类型的平台都有自己的一套强化最佳实践。
- 租户帐户的信任程度。如果您是使用不可信租户帐户的服务提供商，则与仅使用可信的内部租户相比，您将面临不同的安全问题。
- 您的组织遵循哪些安全要求和约定。您可能需要遵守特定的法规或企业要求。

StorageGRID 软件升级的强化准则

您必须使 StorageGRID 系统和相关服务保持最新，以抵御攻击。

升级到 StorageGRID 软件

您应尽可能将 StorageGRID 软件升级到最新的主要版本或先前的主要版本。使 StorageGRID 保持最新有助于缩短已知漏洞处于活动状态的时间，并减少整体攻击面。此外、StorageGRID 的最新版本通常包含早期版本中未包含的安全强化功能。

请参考 "NetApp 互操作性表工具"(IMT)确定您应使用的StorageGRID软件版本。如果需要修补程序， NetApp 会优先为最新版本创建更新。某些修补程序可能与早期版本不兼容。

- 要下载最新的StorageGRID版本和修补程序，请访问 "NetApp 下载： StorageGRID"。
- 要升级StorageGRID软件，请参见"升级说明"。
- 要应用修补程序，请参见"StorageGRID 热修补程序操作步骤"。

升级到外部服务

外部服务可能存在间接影响StorageGRID 的漏洞。确保StorageGRID所依赖的服务保持最新。这些服务包括 LDAP、KMS（或 KMIP 服务器）、DNS 和 NTP。

有关支持的版本列表，请参见 "NetApp 互操作性表工具"。

升级到虚拟机管理程序

如果您的 StorageGRID 节点正在 VMware 或其他虚拟机管理程序上运行，则必须确保虚拟机管理程序软件和固件是最新的。

有关支持的版本列表，请参见 "NetApp 互操作性表工具"。

升级到**Linux**节点

如果 StorageGRID 节点使用的是 Linux 主机平台，则必须确保将安全更新和内核更新应用于主机操作系统。此外，如果存在固件更新，则必须将这些更新应用于容易受到影响的硬件。

有关支持的版本列表，请参见 "NetApp 互操作性表工具"。

StorageGRID 网络强化准则

StorageGRID 系统支持每个网格节点最多三个网络接口，使您可以根据安全和访问要求为每个网格节点配置网络。

有关StorageGRID网络的详细信息，请参见"StorageGRID 网络类型"。

网格网络准则

您必须为所有内部 StorageGRID 流量配置网格网络。所有网格节点均位于网格网络上，它们必须能够与所有其他节点进行通信。

配置网格网络时，请遵循以下准则：

- 确保网络不受不可信客户端的保护，例如在开放式互联网上的客户端。
- 如果可能，请仅对内部流量使用网格网络。管理网络和客户端网络都具有其他防火墙限制，可阻止外部向内部服务发送流量。支持对外部客户端流量使用网格网络，但这种使用可提供更少的保护层。
- 如果 StorageGRID 部署跨越多个数据中心，请使用网格网络上的虚拟专用网络（ VPN ）或等效网络为内部流量提供额外保护。
- 某些维护过程要求在主管理节点与所有其他网格节点之间的端口 22 上进行安全 Shell （ SSH ）访问。使用外部防火墙将 SSH 访问限制为受信任的客户端。

管理网络准则

管理网络通常用于执行管理任务（使用网格管理器或 SSH 的受信任员工）以及与 LDAP ， DNS ， NTP 或 KMS （或 KMIP 服务器）等其他受信任服务进行通信。但是， StorageGRID 不会在内部强制使用此用法。

如果您使用的是管理网络，请遵循以下准则：

- 阻止管理网络上的所有内部流量端口。请参见"列出内部端口"。
- 如果不可信的客户端可以访问管理网络，请使用外部防火墙阻止对管理网络上 StorageGRID 的访问。

客户端网络准则

客户端网络通常用于租户以及与外部服务（例如 CloudMirror 复制服务或其他平台服务）进行通信。但是， StorageGRID 不会在内部强制使用此用法。

如果您使用的是客户端网络，请遵循以下准则：

- 阻止客户端网络上的所有内部流量端口。请参见"列出内部端口"。
- 仅接受显式配置的端点上的入站客户端流量。请参见有关的信息"管理防火墙控制"。

StorageGRID 节点的强化准则

StorageGRID 节点可以部署在 VMware 虚拟机上， Linux 主机上的容器引擎中或作为专用硬件设备。每种类型的平台和每种类型的节点都有自己的一组强化最佳实践。

控制远程 IPMI 对BMC的访问

您可以为所有包含 BMC 的设备启用或禁用远程 IPMI 访问。远程 IPMI 接口允许任何拥有 BMC 帐户和密码的人对您的 StorageGRID 设备进行低级硬件访问。如果您不需要远程 IPMI 访问 BMC，请禁用此选项。

- 要在 Grid Manager 中控制对 BMC 的远程 IPMI 访问，请转到 **Configuration** > **Security** > **Security settings** > **Appliances** > **Remote IPMI access**：
  - 清除*启用远程IPMI访问*复选框以禁用对BMC的IPMI访问。
  - 选中*启用远程IPMI访问*复选框以启用对BMC的IPMI访问。

有关BMC强化的更多信息，请参阅 "强化基板管理控制器"网络安全信息表 "国家安全局（NSA）"和 "网络安全和基础设施安全局（CISA）"。

更改设备 BMC 密码

您可以更改设备的 BMC 密码，以限制访问并提高系统安全性。

1. 在 Grid Manager 中，转到 节点 > 网格节点 > **BMC** 设置。
2. 在更改密码部分，在*新密码*中输入一个长度在 8 到 16 个字符之间的新 BMC 密码，然后在*确认新密码*中再次输入。
3. 选择 * 保存 * 。

您还可以使用 `PUT /bmc-configuration/root-password` API 更改 BMC 密码。

控制设备上的外部 USB 端口访问

您可以启用设备上的 USB 端口，以允许技术支持访问以进行诊断和故障排除。如果您不需要 USB 端口访问，请禁用端口以确保安全。初始安装或升级后，默认情况下会启用 USB 端口。

- 在 Grid Manager 中，转到 **Configuration** > **Security** > **Security settings** > **Appliances** > **USB port access** 以启用或禁用 USB 端口：
  - 选中*启用USB端口*复选框并保存以启用端口。

    如果先前未选中USB复选框并已保存，请选中*启用USB端口*复选框并保存以再次启用USB端口。
  - 清除*启用 USB 端口*复选框并保存以禁用端口。

防火墙配置

在系统强化过程中，您必须查看外部防火墙配置并对其进行修改，以便仅接受来自 IP 地址和严格需要的端口的流量。

StorageGRID 在每个节点上都包含一个内部防火墙、可通过控制对节点的网络访问来增强网格的安全性。您应"管理内部防火墙控制"禁止对特定网格部署所需端口以外的所有端口进行网络访问。在防火墙控制页面上所做的配置更改将部署到每个节点。

具体来说、您可以管理以下方面：

- 特权地址：您可以允许所选IP地址或子网访问通过管理外部访问选项卡上的设置关闭的端口。
- 管理外部访问：您可以关闭默认打开的端口，也可以重新打开先前关闭的端口。
- 不可信客户端网络：您可以指定节点是否信任来自客户端网络的入站流量以及在配置不可信客户端网络时要打开的其他端口。

虽然此内部防火墙可为应对某些常见威胁提供额外的保护层，但它不会消除对外部防火墙的需求。

有关StorageGRID使用的所有内部和外部端口的列表，请参阅"StorageGRID 内部端口"和"用于外部通信的端口"。

禁用未使用的服务

对于所有StorageGRID节点，您应该禁用或阻止对未使用的服务的访问。例如，如果您不打算使用 DHCP，请使用网格管理器关闭端口 68。选择*配置* > 防火墙控制 > 管理外部访问。然后将端口 68 的状态切换从 打开 更改为 关闭。

虚拟化，容器和共享硬件

对于所有 StorageGRID 节点，请避免在与不可信软件相同的物理硬件上运行 StorageGRID 。不要假设虚拟机管理程序保护将阻止恶意软件访问受StorageGRID保护的数据、前提是StorageGRID 和恶意软件位于同一物理硬件上。例如， Meltdown 和 Spectre 攻击会利用现代处理器中的关键漏洞，并允许程序在同一台计算机的内存中窃取数据。

在安装期间保护节点

安装StorageGRID 节点时、不允许不可信用户通过网络访问这些节点。节点只有在加入网格后才会完全安全。

限制对硬件的物理访问

您必须将对StorageGRID硬件设备节点以及运行StorageGRID 的VMware 虚拟机主机和 Linux 主机的物理访问限制为仅限授权管理员。物理访问控制的一些示例包括锁、警卫、物理屏障和视频监控。

硬件设备节点设计为仅由授权管理员安装和操作。不允许未经授权的管理员访问硬件设备节点。

管理节点准则

管理节点可提供系统配置，监控和日志记录等管理服务。登录到网格管理器或租户管理器时，您正在连接到管理节点。

请按照以下准则保护 StorageGRID 系统中的管理节点：

- 保护所有管理节点不受不可信客户端的安全，例如在开放式 Internet 上的客户端。确保任何不可信的客户端都不能访问网格网络，管理网络或客户端网络上的任何管理节点。
- StorageGRID 组控制对网格管理器和租户管理器功能的访问。为每个用户组授予其角色所需的最低权限，并使用只读访问模式防止用户更改配置。
- 在使用 StorageGRID 负载平衡器端点时，请对不可信的客户端流量使用网关节点，而不是管理节点。
- 如果您有不受信任的租户、请勿允许他们直接访问租户管理器或租户管理API。相反，让任何不可信的租户使用与租户管理 API 交互的租户门户或外部租户管理系统。
- (可选)使用管理员代理更好地控制从管理节点到NetApp支持的AutoSupport通信。请参见的步骤"创建管理员代理"。
- 或者，也可以使用受限的 8443 和 9443 端口分隔 Grid Manager 和租户管理器通信。阻止共享端口 443 并将租户请求限制为端口 9443 以提供额外保护。
- 也可以为网格管理员和租户用户使用单独的管理节点。

有关详细信息，请参阅的说明"管理 StorageGRID"。

存储节点准则

存储节点可管理和存储对象数据和元数据。请按照以下准则保护 StorageGRID 系统中的存储节点。

- 不允许不受信任的客户端直接连接到存储节点。使用由网关节点或第三方负载平衡器提供的负载平衡器端点。
- 不要为不可信租户启用出站服务。例如、在为不可信租户创建帐户时、不允许租户使用自己的身份源、也不允许使用平台服务。请参见的步骤"创建租户帐户"。
- 对不可信的客户端流量使用第三方负载平衡器。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。
- (可选)使用存储代理更好地控制云存储池以及从存储节点到外部服务的平台服务通信。请参见的步骤"创建存储代理"。
- 或者，使用客户端网络连接到外部服务。然后，选择*配置*>*安全*>*防火墙控制*>*不受信任的客户端网络*，并指示存储节点上的客户端网络不受信任。存储节点不再接受客户端网络上的任何传入流量，但它继续允许平台服务的出站请求。

网关节点准则

网关节点提供了一个可选的负载平衡接口，客户端应用程序可以使用该接口连接到 StorageGRID 。请按照以下准则保护 StorageGRID 系统中的所有网关节点：

- 配置和使用负载平衡器端点。请参阅。 "负载平衡注意事项"
- 在客户端和网关节点或存储节点之间使用第三方负载平衡器处理不可信的客户端流量。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。如果您使用的是第三方负载平衡器，则仍然可以选择将网络流量配置为通过内部负载平衡器端点或直接发送到存储节点。
- 如果您使用负载均衡器端点，则可以选择让客户端通过客户端网络连接。然后，选择*配置*>*安全*>*防火墙控制*>*不受信任的客户端网络*，并指示网关节点上的客户端网络不受信任。网关节点仅接受明确配置为负载均衡器端点的端口上的入站流量。

硬件设备节点准则

StorageGRID 硬件设备经过专门设计，可在 StorageGRID 系统中使用。某些设备可用作存储节点。其他设备可以用作管理节点或网关节点。您可以将设备节点与基于软件的节点结合使用，也可以部署经过全面设计的全设备网格。

请按照以下准则保护 StorageGRID 系统中的所有硬件设备节点：

- 如果设备使用 SANtricity 系统管理器管理存储控制器，请防止不可信的客户端通过网络访问 SANtricity 系统管理器。
- 如果设备具有基板管理控制器 (BMC)，请注意BMC管理端口允许低级硬件访问。仅将BMC管理端口连接到安全、可信的内部管理网络。

  您可以建立 VLAN 来隔离BMC网络连接并限制BMC对受信任网络的互联网访问。有关强制 VLAN 分离的更多信息，请参阅 "强化基板管理控制器"网络安全信息表 "国家安全局（NSA）"和 "网络安全和基础设施安全局（CISA）"。

  如果没有安全、可信的内部管理网络，请将BMC管理端口保持未连接或阻塞状态。技术支持可能会在支持案例期间请求临时访问权限。

- 如果设备支持使用智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）标准通过以太网远程管理控制器硬件，请阻止端口 623 上的不可信流量。

  您也可以 禁用远程 IPMI 访问。

> 您可以为所有包含BMC 的设备启用或禁用远程 IPMI 访问。远程 IPMI 接口允许任何拥有BMC帐户和密码的人对您的StorageGRID设备进行低级硬件访问。如果您不需要远程 IPMI 访问BMC，请使用以下方法之一禁用此选项：+ 在 Grid Manager 中，转到 配置 > 安全 > 安全设置 > 设备，然后清除 *启用远程 IPMI 访问*复选框。 + 在网格管理 API 中，使用私有端点： `PUT /private/bmc` 。

- 对于包含使用SANtricity系统管理器管理的SED、FDE或FIPS NL)驱动器的设备型号， "启用并配置SANtricity驱动器安全性"。
- 对于包含使用StorageGRID Appliance Installer 和 Grid Manager 管理的 SED 或 FIPS NVMe SSD 的设备型号， "启用并配置StorageGRID驱动器加密" 。
- 对于没有 SED、FDE 或 FIPS 驱动器的设备，使用密钥管理服务器 (KMS) "启用并配置StorageGRID软件节点加密" 。

相关信息

"了解SANtricity System Manager 中的驱动器安全性"

StorageGRID 中 TLS 和 SSH 的强化准则

您应该控制 SSH 访问，替换默认 TLS 证书，并为 TLS 和 SSH 连接选择适当的安全策略。

证书强化准则

您应将安装期间创建的默认证书替换为您自己的自定义证书。

对于许多组织来说，用于 StorageGRID Web 访问的自签名数字证书不符合其信息安全策略。在生产系统上，您应安装 CA 签名的数字证书以用于对 StorageGRID 进行身份验证。

具体而言，您应使用自定义服务器证书，而不是这些默认证书：

- * 管理接口证书 * ：用于确保对网格管理器，租户管理器，网格管理 API 和租户管理 API 的访问安全。
- **S3 API certifice**：用于保护对存储节点和网关节点的访问，S3客户端应用程序使用这些节点上传和下载对象数据。

有关详细信息和说明、请参见"管理安全证书"。

> StorageGRID 单独管理用于负载平衡器端点的证书。要配置负载平衡器证书，请参见"配置负载平衡器端点"。

使用自定义服务器证书时，请遵循以下准则：

- 证书应具有与StorageGRID的DNS条目匹配的 *subjectAltName*。有关详细信息，请参见中的第4.2.1.6节“使用者替代名称” "RFC 5280： PKIX 证书和 CRL 配置文件"。
- 尽可能避免使用通配符证书。此准则的一个例外是S3虚拟托管模式端点的证书、如果事先不知道分段名称、则需要使用通配符。
- 如果必须在证书中使用通配符，则应执行其他步骤以降低风险。请使用通配符模式(如 `*.s3.example.com`)，而不要对其他应用程序使用 `s3.example.com`后缀。此模式也适用于路径模式的S3访问，例如 `dc1-s1.s3.example.com/mybucket`。
- 将证书到期时间设置为较短（例如 2 个月），并使用网格管理 API 自动轮换证书。这对于通配符证书尤其重要。

此外，客户端在与 StorageGRID 通信时应使用严格的主机名检查。

TLS和SSH策略强化准则

您可以选择一个安全策略、以确定使用哪些协议和加密方法与客户端应用程序建立安全TLS连接、以及与内部StorageGRID 服务建立安全SSH连接。

安全策略控制 TLS 和 SSH 如何加密传输中的数据。作为最佳实践，您应该禁用应用程序兼容性不需要的加密选项。使用默认的现代策略，除非您的系统需要符合通用标准、符合 FIPS 140-2，或者您需要使用其他密码

有关详细信息和说明、请参见"管理TLS和SSH策略"。

管理外部 **SSH** 访问

为了增强系统安全性，默认情况下会阻止外部 SSH 访问。仅当需要执行需要入站 SSH 访问的任务（例如故障排除）时才启用 SSH 访问。参考"管理外部 SSH 访问"了解详细信息和说明。

StorageGRID 中日志、密码和审核消息的加固准则

除了遵循 StorageGRID 网络和节点的强化准则之外，您还应遵循 StorageGRID 系统其他方面的强化准则。

临时安装密码

要在安装期间保护StorageGRID系统的安全、请在StorageGRID安装UI或安装API中的临时安装程序密码页面上设置密码。设置后、此密码将应用于所有StorageGRID安装方法、包括用户界面、安装API和 `configure-storagegrid.py`脚本。

有关详细信息、请参见：

- "在基于软件的节点上安装StorageGRID"
- "安装StorageGRID设备"

日志和审核消息

始终以安全的方式保护 StorageGRID 日志和审核消息输出。从支持和系统可用性角度来看， StorageGRID 日志和审核消息可提供宝贵的信息。此外， StorageGRID 日志和审核消息输出中包含的信息和详细信息通常具有敏感性。

将 StorageGRID 配置为向外部系统日志服务器发送安全事件。如果使用系统日志导出，请为传输协议选择 TLS 和 RELP/TLS 。

有关StorageGRID日志的详细信息、请参见"日志文件参考"。有关StorageGRID审核消息的详细信息、请参见"审核消息"。

NetApp AutoSupport

通过StorageGRID的AutoSupport功能、您可以主动监控系统的运行状况、并自动将软件包发送给NetApp 支持站点、组织的内部支持团队或支持合作伙伴。默认情况下、首次配置StorageGRID时、向NetApp发送AutoSupport软件包处于启用状态。

可以禁用 AutoSupport 功能。但是， NetApp 建议启用此功能，因为如果您的 StorageGRID 系统上出现问题描述 ， AutoSupport 有助于加快识别和解决问题的速度。

对于传输协议， AutoSupport 支持 HTTPS ， HTTP 和 SMTP 。由于AutoSupport软件包的敏感性、NetApp强烈建议使用HTTPS作为向NetApp发送AutoSupport软件包的默认传输协议。

跨源资源共享**(CORS)**

如果您希望S3存储分段和该存储分段中的对象可供其他域中的Web应用程序访问、则可以为该存储分段配置跨源站资源共享(CORS)。通常、除非需要、否则不要启用CORS。如果需要 CORS ，请将其限制为可信源。

请参阅"为存储桶和对象配置 CORS"。

外部安全设备

全面强化的解决方案 必须解决 StorageGRID 之外的安全机制问题。使用其他基础架构设备筛选和限制对 StorageGRID 的访问是建立和保持严格安全防护的有效方法。这些外部安全设备包括防火墙，入侵防护系统（ IP ）和其他安全设备。

对于不可信的客户端流量，建议使用第三方负载平衡器。第三方负载平衡可提供更多控制和更多保护层，防止受到攻击。

勒索软件防护

按照中的建议帮助保护对象数据免受勒索软件攻击 "利用StorageGRID 防御勒索软件"。

StorageGRID 与 FabricPool

使用 StorageGRID 与 FabricPool 的配置工作流程

如果您使用NetApp ONTAP 软件、则可以使用NetApp FabricPool 将非活动数据分层到NetApp StorageGRID 对象存储系统。

按照以下说明执行以下操作：

- 了解为FabricPool 工作负载配置StorageGRID 的注意事项和最佳实践。
- 了解如何配置StorageGRID 对象存储系统以用于FabricPool。
- 了解在将StorageGRID 作为FabricPool 云层附加时如何为ONTAP 提供所需的值。

快速入门、了解如何为**FabricPool** 配置**StorageGRID**

1 规划您的配置

- 确定要使用哪个 FabricPool 卷分层策略将非活动 ONTAP 数据分层到 StorageGRID 。
- 规划和安装 StorageGRID 系统以满足您的存储容量和性能需求。
- 熟悉StorageGRID系统软件，包括"网格管理器"和"租户管理器"。
- 查看"HA组"、、"负载平衡" "ILM"和的FabricPool最佳实践"更多内容"。
- 查看以下附加资源、其中提供了有关使用和配置ONTAP 和FabricPool 的详细信息：

  "TR-4598：《ONTAP 中的FabricPool 最佳实践》"

  "适用于FabricPool的ONTAP文档"

2 执行前提任务

获取，"将StorageGRID 附加为云层所需的信息"包括：

- IP 地址
- 域名
- SSL 证书

可选地，配置"身份联合"和"单点登录"。

3 配置**StorageGRID**设置

使用StorageGRID 获取ONTAP 连接到网格所需的值。

建议也是配置所有项的"FabricPool 设置向导"最快方式、但您也可以根据需要手动配置每个实体。

4 配置**ONTAP**和**DNS**

使用ONTAP以"添加云层"使用StorageGRID值。然后、"配置DNS条目"将IP地址与您计划使用的任何域名关联。

5 监控和管理

系统启动并运行后、在ONTAP 和StorageGRID 中执行持续任务、以管理和监控FabricPool 数据分层。

什么是 **FabricPool** ？

FabricPool 是一种 ONTAP 混合存储解决方案 ，它使用高性能闪存聚合作为性能层，使用对象存储作为云层。使用启用了 FabricPool 的聚合有助于降低存储成本，而不会影响性能，效率或保护。

FabricPool 会将云层(外部对象存储、例如StorageGRID)与本地层(ONTAP 存储聚合)关联起来、以创建光盘的复合集合。然后、FabricPool 中的卷可以利用分层功能、将活动(热)数据保留在高性能存储(本地层)上、并将停用(冷)数据分层到外部对象存储(云层)。

无需更改架构，您可以继续从中央 ONTAP 存储系统管理数据和应用程序环境。

什么是 **StorageGRID** ？

NetApp StorageGRID 是一种存储架构、与文件或块存储等其他存储架构不同、它将数据作为对象进行管理。对象保留在单个容器(如分段)中、不会作为文件嵌套在其他目录中的目录中。虽然对象存储的性能通常低于文件或块存储，但其可扩展性明显更高。StorageGRID 存储分段可以容纳数 PB 的数据和数十亿个对象。

为什么使用 **StorageGRID** 作为 **FabricPool** 云层?

FabricPool 可以将ONTAP 数据分层到多个对象存储提供程序、包括StorageGRID。公有 云可能会在存储分段或容器级别设置支持的每秒输入 / 输出操作数上限（ IOPS ），而 StorageGRID 性能则会随系统中的节点数进行扩展。使用 StorageGRID 作为 FabricPool 云层，您可以将冷数据保存在自己的私有云中，以获得最高性能并全面控制数据。

此外，如果使用 StorageGRID 作为云层，则不需要 FabricPool 许可证。

将 **StorageGRID** 作为 **FabricPool** 云层连接所需的信息

在将StorageGRID 附加为FabricPool 的云层之前、您必须在StorageGRID 中执行配置步骤并获取要在ONTAP 中使用的特定值。

我需要什么值?

下表显示了必须在StorageGRID 中配置的值以及ONTAP 和DNS服务器如何使用这些值。

价值	其中、值已配置	使用值的位置
虚拟IP (VIP)地址	StorageGRID > HA组	DNS条目

价值	其中、值已配置	使用值的位置
端口	StorageGRID >负载平衡器端点	ONTAP 系统管理器>添加云层
SSL 证书	StorageGRID >负载平衡器端点	ONTAP 系统管理器>添加云层
服务器名称(FQDN)	StorageGRID >负载平衡器端点	DNS条目
访问密钥ID和机密访问密钥	StorageGRID >租户和存储分段	ONTAP 系统管理器>添加云层
存储分段/容器名称	StorageGRID >租户和存储分段	ONTAP 系统管理器>添加云层

如何获取这些值?

根据您的要求、您可以执行以下任一操作来获取所需信息：

- 使用"FabricPool 设置向导"。FabricPool 设置向导可帮助您在StorageGRID 中快速配置所需的值、并输出一个文件、您可以使用该文件配置ONTAP System Manager。此向导将指导您完成所需的步骤、并帮助您确保设置符合StorageGRID 和FabricPool 最佳实践。
- 手动配置每个项目。然后、在ONTAP 系统管理器或ONTAP 命令行界面中输入值。请按照以下步骤操作：
  a. "为FabricPool 配置高可用性(HA)组"(英文)
  b. "为 FabricPool 创建负载平衡器端点"(英文)
  c. "为 FabricPool 创建租户帐户"(英文)
  d. 登录到租户帐户、和"为root用户创建存储分段和访问密钥"。
  e. 为FabricPool数据创建ILM规则、并将其添加到活动ILM策略中。请参阅。 "为FabricPool 数据配置ILM"
  f. (可选)"为FabricPool 创建流量分类策略"。

使用**FabricPool** 设置向导

了解 **StorageGRID FabricPool** 设置向导

您可以使用FabricPool 设置向导将StorageGRID 配置为FabricPool 云层的对象存储系统。完成设置向导后、您可以在ONTAP 系统管理器中输入所需的详细信息。

何时使用**FabricPool** 设置向导

FabricPool 设置向导将指导您完成配置StorageGRID 以用于FabricPool 的每个步骤、并自动为您配置某些实体、例如ILM和流量分类策略。完成此向导期间、您可以下载一个文件、用于在ONTAP 系统管理器中输入值。使用向导可以更快地配置系统、并确保您的设置符合StorageGRID 和FabricPool 最佳实践。

如果您拥有root访问权限、则可以在开始使用StorageGRID 网格管理器时完成FabricPool 设置向导、也可以稍后访问并完成该向导。根据您的要求、您还可以手动配置部分或全部所需项、然后使用向导将ONTAP 所需的值汇编到一个文件中。

除非您知道自己有特殊要求、或者您的实施需要大量自定义、否则请使用FabricPool 设置向导。

在使用向导之前

确认您已完成这些前提条件步骤。

查看最佳实践

- 您大致了解了"将StorageGRID 附加为云层所需的信息"。
- 您已经查看了以下方面的FabricPool 最佳实践：
  - "高可用性(HA)组"
  - "负载平衡"
  - "ILM规则和策略"

获取**IP**地址并设置**VLAN**接口

如果要配置HA组、您就会知道ONTAP 要连接到哪些节点以及要使用哪些StorageGRID 网络。您还知道要为子网CIDR、网关IP地址和虚拟IP (VIP)地址输入哪些值。

如果您计划使用虚拟LAN隔离FabricPool 流量、则已配置VLAN接口。请参阅。 "配置 VLAN 接口"

配置身份联合和**SSO**

如果您计划对StorageGRID系统使用身份联合或单点登录 (SSO)，则您已启用这些功能。您还知道哪个联合组应该对ONTAP将使用的租户帐户具有 root 访问权限。看"使用身份联合"和"配置单点登录"。

获取并配置域名

- 您知道要用于StorageGRID 的完全限定域名(FQDN)。域名服务器(DNS)条目会将此FQDN映射到您使用向导创建的HA组的虚拟IP (VIP)地址。请参阅。 "配置 DNS 服务器"
- 如果您计划使用 S3 虚拟托管式请求，则需要 "已配置S3端点域名"。ONTAP 默认使用路径样式的 URL，但建议使用虚拟托管样式的请求。

查看负载平衡器和安全证书要求

如果您计划使用StorageGRID负载平衡器，则已查看常规"负载平衡注意事项"。您拥有要上传的证书或生成证书所需的值。

如果您计划使用外部(第三方)负载平衡器端点、则具有该负载平衡器的完全限定域名(FQDN)、端口和证书。

确认**ILM**存储池配置

如果您最初安装的是StorageGRID 11.5或更早版本、则已配置要使用的存储池。通常、您应为要用于存储ONTAP 数据的每个StorageGRID 站点创建一个存储池。

> 如果您最初安装的是StorageGRID 11.7或11.8.首次安装上述任一版本时、系统会自动为每个站点创建存储池。

ONTAP 与**StorageGRID** 云层之间的关系

FabricPool 向导将指导您完成创建一个StorageGRID 云层的过程、此云层包含一个StorageGRID 租户、一组访

问密钥和一个StorageGRID 存储分段。您可以将此StorageGRID 云层附加到一个或多个ONTAP 本地层。

通常、最佳做法是将一个云层附加到集群中的多个本地层。但是、根据您的要求、您可能希望对单个集群中的本地层使用多个分段甚至多个StorageGRID 租户。通过使用不同的分段和租户、您可以在ONTAP 本地层之间隔离数据和数据访问、但配置和管理有点复杂。

NetApp建议不要将一个云层附加到多个集群中的本地层。

> 有关将StorageGRID与NetApp MetroCluster™和FabricPool镜像结合使用的最佳实践，请参见"TR-4598：《ONTAP 中的FabricPool 最佳实践》"。

可选：为每个本地层使用不同的分段

要对ONTAP 集群中的本地层使用多个分段、请在ONTAP 中添加多个StorageGRID 云层。每个云层共享同一个HA组、负载平衡器端点、租户和访问密钥、但使用不同的容器(StorageGRID 存储分段)。请遵循以下常规步骤：

1. 在StorageGRID 网格管理器中、完成第一个云层的FabricPool 设置向导。
2. 在ONTAP 系统管理器中、添加云层并使用从StorageGRID 下载的文件来提供所需的值。
3. 从StorageGRID 租户管理器中、登录到由向导创建的租户、然后创建第二个分段。
4. 再次完成FabricPool 向导。选择现有HA组、负载平衡器端点和租户。然后、选择您手动创建的新存储分段。为新存储分段创建新的ILM规则、并激活ILM策略以包含该规则。
5. 在ONTAP 中、添加第二个云层、但提供新存储分段名称。

可选：为每个本地层使用不同的租户和存储分段

要对ONTAP 集群中的本地层使用多个租户和不同的访问密钥集、请在ONTAP 中添加多个StorageGRID 云层。每个云层共享同一个HA组、负载平衡器端点、但使用不同的租户、访问密钥和容器(StorageGRID 存储分段)。请遵循以下常规步骤：

1. 在StorageGRID 网格管理器中、完成第一个云层的FabricPool 设置向导。
2. 在ONTAP 系统管理器中、添加云层并使用从StorageGRID 下载的文件来提供所需的值。
3. 再次完成FabricPool 向导。选择现有HA组和负载平衡器端点。创建新租户和存储分段。为新存储分段创建新的ILM规则、并激活ILM策略以包含该规则。
4. 在ONTAP 中、添加第二个云层、但提供新的访问密钥、机密密钥和存储分段名称。

访问并完成 **StorageGRID FabricPool** 设置向导

您可以使用FabricPool 设置向导将StorageGRID 配置为FabricPool 云层的对象存储系统。

开始之前

- 您已查看"注意事项和要求"以使用FabricPool设置向导。

> 如果要配置StorageGRID以与任何其他S3客户端应用程序结合使用，请转至"使用S3设置向导"。

- 您拥有"root访问权限"。

访问向导

您可以在开始使用StorageGRID 网格管理器时完成FabricPool 设置向导、也可以稍后访问并完成该向导。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 如果仪表板上出现 **FabricPool and S3 setup wizard** 横幅，请选择横幅中的链接。如果横幅不再出现，请从 Grid Manager 标题栏中选择帮助图标  ，然后选择 **FabricPool and S3 setup wizard**。
3. 在FabricPool and S3设置向导页面的FabricPool 部分中，选择*立即配置*。

   *Step 1 of 9：Configure HA group*出现。

第1步(共9步)：配置HA组

高可用性(HA)组是一组节点、每个节点都包含StorageGRID 负载平衡器服务。HA组可以包含网关节点、管理节点或同时包含这两者。

您可以使用HA组帮助保持FabricPool 数据连接可用。HA组使用虚拟IP地址(VIP)提供对负载平衡器服务的高可用性访问。如果HA组中的活动接口发生故障、则备份接口可以管理工作负载、而对FabricPool 操作的影响微乎其微

有关此任务的详细信息，请参见"管理高可用性组"和"高可用性组的最佳实践"。

步骤

1. 如果您计划使用外部负载平衡器、则无需创建HA组。选择*跳过此步骤*并转到[第2步(共9步)：配置负载平衡器端点]。
2. 要使用StorageGRID 负载平衡器、请创建新的HA组或使用现有HA组。

创建 **HA** 组

a. 要创建新的HA组，请选择*创建HA组*。

b. 对于“输入详细信息”步骤，请填写以下字段。

字段	说明
HA组名称	此HA组的唯一显示名称。
问题描述 (可选)	此HA组的问题描述。

c. 对于*Add interfaces*步骤，选择要在此HA组中使用的节点接口。

使用列标题对行进行排序，或者输入搜索词以更快地找到接口。

您可以选择一个或多个节点、但只能为每个节点选择一个接口。

d. 对于“确定接口优先级”步骤，请确定此HA组的主接口和任何备份接口。

拖动行以更改*优先级顺序*列中的值。

列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。

如果HA组包含多个接口、而活动接口发生故障、则虚拟IP (VIP)地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。解决故障后， VIP 地址将移回可用的最高优先级接口。

e. 对于“输入**IP**地址”步骤，请填写以下字段。

字段	说明
Subnet CIDR	采用CIDR表示法的VIP子网的地址##8212;后跟斜杠的IPv4地址和子网长度(0-32)。 网络地址不能设置任何主机位。例如， `192.16.0.0/22`。
网关IP地址(可选)	可选。如果用于访问StorageGRID 的ONTAP IP地址与StorageGRID VIP地址不在同一子网上、请输入StorageGRID VIP本地网关IP地址。本地网关 IP 地址必须位于 VIP 子网中。
虚拟IP地址	为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网中、并且所有VIP地址都将在活动接口上同时处于活动状态。 必须至少有一个地址为IPv4。您也可以指定其他 IPv4 和 IPv6 地址。

f. 选择*创建HA组*，然后选择*完成*返回FabricPool 设置向导。

g. 选择*继续*以转到负载平衡器步骤。

使用现有**HA**组

a. 要使用现有HA组，请从*选择HA组*下拉列表中选择HA组名称。

b. 选择*继续*以转到负载平衡器步骤。

第2步(共9步)：配置负载平衡器端点

StorageGRID 使用负载平衡器管理客户端应用程序(如FabricPool)的工作负载。负载平衡可最大限度地提高多个存储节点的速度和连接容量。

您可以使用所有网关和管理节点上的StorageGRID 负载平衡器服务、也可以连接到外部(第三方)负载平衡器。建议使用StorageGRID 负载平衡器。

有关此任务的详细信息，请参见常规"负载平衡注意事项"和"FabricPool 负载平衡最佳实践"。

步骤

1. 选择或创建StorageGRID 负载平衡器端点、或者使用外部负载平衡器。

创建端点

a. 选择 * 创建端点 * 。

b. 对于*输入端点详细信息*步骤，请填写以下字段。

字段	说明
名称	端点的描述性名称。
端口	要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入任何未使用的外部端口。如果输入80或443、则仅在网关节点上配置端点、因为这些端口是在管理节点上预留的。 *注意：*不允许使用其他网格服务使用的端口。请参见"网络端口参考"。
客户端类型	必须为*S3*。
网络协议	选择 * HTTPS * 。 注意：支持在不使用TLS加密的情况下与StorageGRID 通信，但不建议这样做。

c. 对于*选择绑定模式*步骤，指定绑定模式。绑定模式控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

模式	说明
全局（默认）	客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。 除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。
HA 组的虚拟 IP	客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。 具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。
节点接口	客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。
节点类型	根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。

d. 对于*租户访问*步骤，请选择以下选项之一：

字段	说明
允许所有租户(默认)	所有租户帐户都可以使用此端点来访问其分段。 对于用于FabricPool 的负载平衡器端点，*允许所有租户*几乎始终是适当的选项。 如果要对新的StorageGRID 系统使用FabricPool 设置向导、并且尚未创建任何租户帐户、则必须选择此选项。
允许选定租户	只有选定租户帐户才能使用此端点访问其分段。
阻止选定租户	选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。

e. 对于*attach certificer*步骤，选择以下选项之一：

字段	说明
上传证书(建议)	使用此选项可上传CA签名的服务器证书、证书专用密钥和可选的CA包。
生成证书	使用此选项可生成自签名证书。有关输入内容的详细信息、请参见"配置负载平衡器端点"。
使用StorageGRID S3 证书	只有在您已上传或生成自定义版本的StorageGRID 全局证书时、此选项才可用。有关详细信息、请参见。 "配置S3 API证书"

f. 选择*完成*以返回FabricPool 设置向导。

g. 选择*继续*转到租户和存储分段步骤。

对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

使用现有负载平衡器端点

a. 从*选择负载平衡器端点*下拉列表中选择现有端点的名称。

b. 选择*继续*转到租户和存储分段步骤。

使用外部负载平衡器

a. 完成外部负载平衡器的以下字段。

字段	说明
FQDN	外部负载平衡器的完全限定域名(FQDN)。
端口	FabricPool 将用于连接到外部负载平衡器的端口号。

字段	说明
证书	复制外部负载平衡器的服务器证书并将其粘贴到此字段中。

b. 选择*继续*转到租户和存储分段步骤。

第3步(共9步)：租户和存储分段

租户是一种可以使用S3应用程序在StorageGRID 中存储和检索对象的实体。每个租户都有自己的用户、访问密钥、分段、对象和一组特定功能。您必须先创建StorageGRID 租户、然后才能创建FabricPool 要使用的存储分段。

分段是一种用于存储租户对象和对象元数据的容器。尽管某些租户可能具有多个分段、但此向导一次只允许您创建或选择一个租户和一个分段。您可以稍后使用租户管理器添加所需的任何其他分段。

您可以创建新租户和存储分段以供FabricPool 使用、也可以选择现有租户和存储分段。如果您创建新租户、系统会自动为租户的root用户创建访问密钥ID和机密访问密钥。

有关此任务的详细信息，请参见"为 FabricPool 创建租户帐户"和"创建 S3 存储分段并获取访问密钥"。

步骤

创建新租户和存储分段或选择现有租户。

新租户和存储分段

1. 要创建新租户和存储分段，请输入*租户名称*。例如， `FabricPool tenant`。
2. 根据您的StorageGRID系统是否使用，定义租户帐户的根访问权限"身份联合"，"单点登录(SSO)" ，或两者兼而有之。

选项	执行此操作 ...
如果未启用身份联合	指定以本地root用户身份登录租户时要使用的密码。
如果启用了身份联合	a. 选择一个现有联盟组、以便对租户具有root访问权限。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择一个现有联盟组、以便对租户具有root访问权限。没有本地用户可以登录。

3. 对于*Bucketname*，输入FabricPool 将用于存储ONTAP 数据的存储分段的名称。例如，`fabricpool-bucket`。

   创建存储分段后、无法更改存储分段名称。

4. 为此存储分段选择*区域*。

   使用默认区域(`us-east-1`)，除非您希望将来使用ILM根据存储分段的区域过滤对象。

5. 选择*创建并继续*以创建租户和存储分段并转到下载数据步骤

选择租户和存储分段

现有租户帐户必须至少具有一个未启用版本控制的存储分段。如果现有租户不存在存储分段、则无法选择该租户帐户。

1. 从*租户名称*下拉列表中选择现有租户。
2. 从*存储分段名称*下拉列表中选择现有存储分段。

   FabricPool 不支持对象版本控制、因此不会显示已启用版本控制的分段。

   请勿选择已启用S3对象锁定的存储分段以用于FabricPool。

3. 选择*CONTINUD*进入下载数据步骤。

第4步(共9步)：下载ONTAP 设置

在此步骤中、您将下载一个文件、可使用此文件在ONTAP 系统管理器中输入值。

步骤

1. （可选）选择复制图标（  ），将访问密钥 ID 和秘密访问密钥复制到剪贴板。

这些值包含在下载文件中、但您可能需要单独保存它们。

2. 选择*下载ONTAP 设置*以下载包含到目前为止输入的值的文本文件。

   此 `ONTAP_FabricPool_settings_*bucketname*.txt`文件包含将StorageGRID配置为FabricPool云层的对象存储系统所需的信息、其中包括：

   - 负载平衡器连接详细信息、包括服务器名称(FQDN)、端口和证书
   - Bucket Name
   - 租户帐户的root用户的访问密钥ID和机密访问密钥

3. 将复制的密钥和下载的文件保存到安全位置。

   > 在复制两个访问密钥或下载ONTAP 设置或同时复制这两者之前、请勿关闭此页面。关闭此页面后、密钥将不可用。请确保将此信息保存在安全位置、因为此信息可用于从StorageGRID系统获取数据。

4. 选中此复选框以确认您已下载或复制访问密钥ID和机密访问密钥。
5. 选择*继续*以转到ILM存储池步骤。

第5步(共9步)：选择存储池

存储池是指一组存储节点。选择存储池时、您可以确定StorageGRID 将使用哪些节点来存储从ONTAP 分层的数据。

有关此步骤的详细信息，请参见"创建存储池"。

步骤

1. 从*站点*下拉列表中，选择要用于从ONTAP 分层的数据的StorageGRID 站点。
2. 从*存储池*下拉列表中、选择该站点的存储池。

   站点的存储池包括该站点的所有存储节点。

3. 选择*继续*以转到ILM规则步骤。

第6步(共9步)：查看FabricPool 的ILM规则

信息生命周期管理(ILM)规则控制StorageGRID 系统中所有对象的放置、持续时间和加载行为。

FabricPool 设置向导会自动创建建议的ILM规则以供FabricPool 使用。此规则仅适用于您指定的存储分段。它在单个站点上使用2+1纠删编码来存储从ONTAP 分层的数据。

有关此步骤的详细信息，请参见"创建 ILM 规则"和"对FabricPool 数据使用ILM的最佳实践"。

步骤

1. 查看规则详细信息。

字段	说明
规则名称	自动生成、无法更改
说明	自动生成、无法更改
筛选器	分段名称 此规则仅适用于保存在指定分段中的适用场景 对象。
参考时间	载入时间 当对象最初保存到存储分段时、放置指令开始。
放置说明	使用2+1纠删编码

2. 按*时间段*和*存储池*对保留图进行排序以确认放置说明。
   - 此规则的*时间段*为*第0天-永久*。*Day 0*表示从ONTAP 分层数据时应用此规则。*Forever *表示StorageGRID ILM不会删除已从ONTAP分层的数据。
   - 此规则的*存储池*是您选择的存储池。*EC 2+1*表示数据将使用2+1纠删编码进行存储。每个对象将保存为两个数据片段和一个奇偶校验片段。每个对象的三个片段将保存到单个站点的不同存储节点。
3. 选择*创建并继续*以创建此规则并转到ILM策略步骤。

第7步(共9步)：查看并激活ILM策略

FabricPool设置向导创建供FabricPool使用的ILM规则后、将创建ILM策略。激活此策略之前、必须仔细模拟并查看此策略。

有关此步骤的详细信息，请参见"创建 ILM 策略"和"对FabricPool 数据使用ILM的最佳实践"。

> 激活新的ILM策略后、StorageGRID 将使用该策略来管理网格中所有对象(包括现有对象和新加载的对象)的放置、持续时间和数据保护。在某些情况发生原因 下、激活新策略可以将现有对象移动到新位置。

> 为避免数据丢失、请勿使用将过期的ILM规则或删除FabricPool云层数据。将保留期限设置为*永久*、以确保StorageGRID ILM不会删除FabricPool对象。

步骤

1. (可选)更新系统生成的*Policy name*。默认情况下、系统会在活动或非活动策略的名称后附加"+" FabricPool、但您可以提供自己的名称。
2. 查看非活动策略中的规则列表。
   - 如果您的网格没有非活动ILM策略、则向导会通过克隆活动策略并将新规则添加到顶部来创建非活动策略。
   - 如果您的网格已具有非活动ILM策略、并且该策略使用的规则和顺序与活动ILM策略相同、则该向导会将新规则添加到非活动策略的顶部。

- 如果您的非活动策略包含与活动策略不同的规则或顺序、则向导会通过克隆活动策略并将新规则添加到顶部来创建一个新的非活动策略。

3. 查看新非活动策略中规则的顺序。

   由于FabricPool 规则是第一个规则、因此FabricPool 分段中的任何对象都会置于评估策略中的其他规则之前。任何其他分段中的对象将由策略中的后续规则放置。

4. 查看保留图、了解如何保留不同的对象。
   a. 选择*全部展开*可查看非活动策略中每个规则的保留图。
   b. 选择*时间段*和*存储池*以查看保留图。确认应用于FabricPool存储分段或租户的任何规则将保留对象*永久*。
5. 查看非活动策略后，选择*激活并继续*以激活策略并转到流量分类步骤。

> ILM策略中的错误可能会导致发生原因 无法修复的数据丢失。激活之前、请仔细查看策略。

第8步(共9步)：创建流量分类策略

您可以选择使用FabricPool 设置向导创建一个流量分类策略、以监控FabricPool 工作负载。系统创建的策略使用匹配规则来标识与您创建的存储分段相关的所有网络流量。此策略仅监控流量；它不会限制FabricPool 或任何其他客户端的流量。

有关此步骤的详细信息，请参见"为 FabricPool 创建流量分类策略"。

步骤

1. 查看策略。
2. 如果要创建此流量分类策略，请选择*创建并继续*。

   FabricPool 开始将数据分层到StorageGRID 后、您可以转到"流量分类策略"页面查看此策略的网络流量指标。之后、您还可以添加规则来限制其他工作负载、并确保FabricPool 工作负载具有大部分带宽。

3. 否则，请选择*跳过此步骤*。

第9步(共9步)：查看摘要

此摘要提供了有关您配置的项目的详细信息、包括负载平衡器、租户和存储分段的名称、流量分类策略以及活动ILM策略。

步骤

1. 查看摘要。
2. 选择 * 完成 * 。

后续步骤

完成FabricPool 向导后、请执行以下附加步骤。

步骤

1. 转到"配置ONTAP 系统管理器"以输入保存的值、并完成连接的ONTAP端。您必须将StorageGRID 添加为云层、将此云层附加到本地层以创建FabricPool 、并设置卷分层策略。

2. 转到"配置DNS服务器"并确保DNS包含一条记录、用于将StorageGRID服务器名称(完全限定域名)与您要使用的每个StorageGRID IP地址相关联。
3. 请访问"StorageGRID 和 FabricPool 的其他最佳实践"、了解StorageGRID审核日志和其他全局配置选项的最佳实践。

手动配置StorageGRID

在 StorageGRID 中为 FabricPool 创建高可用性 (HA) 组

在配置 StorageGRID 以与 FabricPool 结合使用时，您可以选择创建一个或多个高可用性（ HA ）组。HA组是一组节点、每个节点都包含StorageGRID 负载平衡器服务。HA组可以包含网关节点、管理节点或同时包含这两者。

您可以使用HA组帮助保持FabricPool 数据连接可用。HA组使用虚拟IP地址(VIP)提供对负载平衡器服务的高可用性访问。如果HA组中的活动接口发生故障、则备份接口可以管理工作负载、而对FabricPool 操作的影响微乎其微。

有关此任务的详细信息，请参见"管理高可用性组"。要使用FabricPool设置向导完成此任务，请转至"访问并完成FabricPool 设置向导"。

开始之前

- 您已查看"高可用性组的最佳实践"。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 如果您计划使用 VLAN ，则已创建 VLAN 接口。请参阅。 "配置 VLAN 接口"

步骤

1. 选择*配置* > 网络 > 高可用性组。
2. 选择 * 创建 * 。
3. 对于“输入详细信息”步骤，请填写以下字段。

字段	说明
HA组名称	此HA组的唯一显示名称。
问题描述 (可选)	此HA组的问题描述。

4. 对于*Add interfaces*步骤，选择要在此HA组中使用的节点接口。

   使用列标题对行进行排序，或者输入搜索词以更快地找到接口。

   您可以选择一个或多个节点、但只能为每个节点选择一个接口。

5. 对于“确定接口优先级”步骤，请确定此HA组的主接口和任何备份接口。

   拖动行以更改*优先级顺序*列中的值。

列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。

如果HA组包含多个接口、而活动接口发生故障、则虚拟IP (VIP)地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。解决故障后， VIP 地址将移回可用的最高优先级接口。

6. 对于“输入**IP**地址”步骤，请填写以下字段。

字段	说明
Subnet CIDR	采用CIDR表示法的VIP子网的地址##8212;后跟斜杠的IPv4地址和子网长度(0-32)。 网络地址不能设置任何主机位。例如， `192.16.0.0/22`。
网关IP地址(可选)	可选。如果用于访问StorageGRID 的ONTAP IP地址与StorageGRID VIP地址不在同一子网上、请输入StorageGRID VIP本地网关IP地址。本地网关 IP 地址必须位于 VIP 子网中。
虚拟IP地址	为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网内。 必须至少有一个地址为IPv4。您也可以指定其他 IPv4 和 IPv6 地址。

7. 选择 * 创建 HA 组 * ，然后选择 * 完成 * 。

在 **StorageGRID** 中为 **FabricPool** 创建负载平衡器端点

StorageGRID 使用负载平衡器管理客户端应用程序(如FabricPool)的工作负载。负载平衡可最大限度地提高多个存储节点的速度和连接容量。

在配置StorageGRID 以与FabricPool 结合使用时、您必须配置负载平衡器端点、并上传或生成负载平衡器端点证书、此证书用于保护ONTAP 和StorageGRID 之间的连接。

要使用FabricPool设置向导完成此任务，请转至"访问并完成FabricPool 设置向导"。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。
- 您已查看常规"负载平衡注意事项"以及"FabricPool 负载平衡最佳实践"。

步骤

1. 选择*配置* > 网络 > 负载均衡器端点。
2. 选择 * 创建 * 。
3. 对于*输入端点详细信息*步骤，请填写以下字段。

字段	说明
名称	端点的描述性名称。
端口	要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入任何未使用的外部端口。如果输入80或443、则仅在网关节点上配置端点。这些端口在管理节点上预留。 *注意：*不允许使用其他网格服务使用的端口。请参见"网络端口参考"。 将StorageGRID 附加为FabricPool 云层时、您需要向ONTAP 提供此编号。
客户端类型	选择 * 。 s3* 。
网络协议	选择 * HTTPS * 。 注意：支持在不使用TLS加密的情况下与StorageGRID 通信，但不建议这样做。

4. 对于*选择绑定模式*步骤，指定绑定模式。绑定模式控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

模式	说明
全局（默认）	客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。 除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。
HA 组的虚拟 IP	客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。 具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。
节点接口	客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。
节点类型	根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。

5. 对于*租户访问*步骤，请选择以下选项之一：

字段	说明
允许所有租户(默认)	所有租户帐户都可以使用此端点来访问其分段。 对于用于FabricPool 的负载平衡器端点，*允许所有租户*几乎始终是适当的选项。 如果尚未创建任何租户帐户、则必须选择此选项。
允许选定租户	只有选定租户帐户才能使用此端点访问其分段。
阻止选定租户	选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。

6. 对于*attach certificer*步骤，选择以下选项之一：

字段	说明
上传证书(建议)	使用此选项可上传CA签名的服务器证书、证书专用密钥和可选的CA包。
生成证书	使用此选项可生成自签名证书。有关输入内容的详细信息、请参见"配置负载平衡器端点"。
使用StorageGRID S3证书	只有在您已上传或生成自定义版本的StorageGRID 全局证书时、此选项才可用。有关详细信息、请参见。 "配置S3 API证书"

7. 选择 * 创建 * 。

对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

在 **StorageGRID** 中为 **FabricPool** 创建租户帐户

您必须在网格管理器中创建一个租户帐户以供 FabricPool 使用。

租户帐户允许客户端应用程序在 StorageGRID 上存储和检索对象。每个租户帐户都有自己的帐户 ID ，授权组和用户，分段和对象。

有关此任务的详细信息，请参见"创建租户帐户"。要使用FabricPool设置向导完成此任务，请转至"访问并完成FabricPool 设置向导"。

开始之前

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

步骤

1. 选择*租户*。

2. 选择 * 创建 * 。
3. 对于输入详细信息步骤、请输入以下信息。

字段	说明
名称	租户帐户的名称。租户名称不需要唯一。创建租户帐户时，它会收到一个唯一的数字帐户 ID 。
问题描述 (可选)	用于帮助识别租户的问题描述。
客户端类型	对于FabricPool ，必须为*S3*。
存储配额(可选)	对于FabricPool 、将此字段留空。

4. 对于选择权限步骤：
   a. 不要选择*允许平台服务*。

      FabricPool 租户通常不需要使用CloudMirror复制等平台服务。

   b. (可选)选择*使用自己的身份源*。
   c. 不要选择*允许S3选择*。

      FabricPool 租户通常不需要使用S3 Select。

   d. （可选）选择 **Use grid federation connection** 以允许租户使用 "网格联合连接" 进行帐户同步和跨网格复制。然后，选择要使用的网格联合连接。
5. 对于定义根访问权限步骤，根据您的StorageGRID系统是否使用"身份联合"，"单点登录(SSO)" ，或两者兼而有之。

选项	执行此操作 ...
如果未启用身份联合	指定以本地root用户身份登录租户时要使用的密码。
如果启用了身份联合	a. 选择一个现有联盟组、以便对租户具有root访问权限。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择一个现有联盟组、以便对租户具有root访问权限。没有本地用户可以登录。

6. 选择 * 创建租户 * 。

在 **StorageGRID** 中为 **FabricPool** 创建 **S3** 存储桶并获取访问密钥

在将 StorageGRID 与 FabricPool 工作负载结合使用之前，您必须为 FabricPool 数据创建一个 S3 存储分段。您还需要为要用于 FabricPool 的租户帐户获取访问密钥和机密访问密钥。

有关此任务的详细信息，请参见"创建 S3 存储分段"和"创建您自己的 S3 访问密钥"。要使用FabricPool设置向导完成此任务，请转至"访问并完成FabricPool 设置向导"。

开始之前

- 您已创建一个租户帐户供 FabricPool 使用。
- 您对租户帐户具有root访问权限。

步骤

1. 登录到租户管理器。

   您可以执行以下任一操作：

   - 从网格管理器的租户帐户页面中，选择此租户的 * 登录 * 链接，然后输入您的凭据。
   - 在 Web 浏览器中输入租户帐户的 URL ，然后输入凭据。

2. 为 FabricPool 数据创建 S3 存储分段。

   您必须为计划使用的每个 ONTAP 集群创建一个唯一的存储分段。

   a. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
   b. 选择 * 创建存储分段 * 。
   c. 输入要用于FabricPool 的StorageGRID 存储分段的名称。例如， `fabricpool-bucket`。

      创建存储分段后、无法更改存储分段名称。

   d. 为此存储分段选择区域。

      默认情况下，所有存储桶均在 `us-east-1`地区。如果默认区域配置为 `us-east-1`，该其他区域最初是在下拉菜单中选择的。

   e. 选择 * 继续 * 。
   f. 选择 * 创建存储分段 * 。

      不要为FabricPool 存储分段选择*启用对象版本控制*。同样、请勿编辑FabricPool分段以使用*可用*或非默认一致性。FabricPool存储分段的建议一致性为*read-after-new-write*，这是新存储分段的默认一致性。

3. 创建访问密钥和机密访问密钥。

   a. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。
   b. 选择 * 创建密钥 * 。
   c. 选择 * 创建访问密钥 * 。
   d. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

      将 StorageGRID 配置为 FabricPool 云层时，您将在 ONTAP 中输入这些值。

如果您将来在StorageGRID 中生成新的访问密钥和机密访问密钥、请在ONTAP 中输入新密钥、然后再从StorageGRID 中删除旧值。否则、ONTAP 可能会暂时失去对StorageGRID 的访问权限。

为 FabricPool 数据配置 StorageGRID ILM

您可以使用此简单示例策略作为自己ILM规则和策略的起点。

本示例假设您正在为一个 StorageGRID 系统设计 ILM 规则和 ILM 策略，该系统在科罗拉多州丹佛的一个数据中心内有四个存储节点。此示例中的FabricPool数据使用名为的分段 `fabricpool-bucket`。

以下 ILM 规则和策略仅为示例。配置 ILM 规则的方法有多种。在激活新策略之前、请对其进行模拟、以确认其是否按预期工作、以防止内容丢失。要了解更多信息，请参阅"使用 ILM 管理对象"。

为避免数据丢失、请勿使用将过期的ILM规则或删除FabricPool云层数据。将保留期限设置为*永久*、以确保StorageGRID ILM不会删除FabricPool对象。

开始之前

- 您已查看"对FabricPool 数据使用ILM的最佳实践"。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"ILM或root访问权限"。
- 如果从 11.7 之前的 StorageGRID 版本升级到 StorageGRID 12.1，则已配置要使用的存储池。一般来说，您应该为要用于存储数据的每个 StorageGRID 站点创建一个存储池。（从版本 11.7 开始，系统会自动为每个站点创建存储池。）

如果您最初安装的是StorageGRID 11.7或11.8.首次安装上述任一版本时、系统会自动为每个站点创建存储池。

步骤

1. 创建一个仅适用于中数据的ILM规则 `fabricpool-bucket`。此示例规则将创建经过删除编码的副本。

规则定义	示例值
规则名称	2 + 1 FabricPool 数据纠删编码
Bucket Name	`fabricpool-bucket` 您也可以筛选 FabricPool 租户帐户。
高级筛选器	对象大小大于0.2 MB。 注意： FabricPool 仅写入4 MB对象，但必须添加对象大小筛选器，因为此规则使用纠删编码。

规则定义	示例值
参考时间	载入时间
时间段和放置位置	从第0天存储到永久存储 在丹佛使用2+1 EC方案通过纠删编码存储对象、并将这些对象永久保留在StorageGRID中。 为避免数据丢失、请勿使用将过期的ILM规则或删除FabricPool云层数据。
加热行为	平衡

2. 创建一个默认ILM规则、以便为第一个规则不匹配的任何对象创建两个复制副本。请勿选择基本筛选器(租户帐户或存储分段名称)或任何高级筛选器。

规则定义	示例值
规则名称	两个复制副本
Bucket Name	无 _
高级筛选器	无 _
参考时间	载入时间
时间段和放置位置	从第0天存储到永久存储 通过在Denver复制2个副本来存储对象。
加热行为	平衡

3. 创建ILM策略并选择两个规则。由于复制规则不使用任何筛选器，因此它可以是策略的默认（最后）规则。
4. 将测试对象载入网格。
5. 使用测试对象模拟策略以验证此行为。
6. 激活策略。

激活此策略后， StorageGRID 将按如下所示放置对象数据：

- 中从FabricPool分层的数据 `fabricpool-bucket`将使用2+1纠删编码方案进行纠删编码。两个数据片段和一个奇偶校验片段将放置在三个不同的存储节点上。
- 所有其他分段中的所有对象都将被复制。将创建两个副本并将其放置在两个不同的存储节点上。
- 这些副本将永久保留在StorageGRID中。StorageGRID ILM不会删除这些对象。

在 StorageGRID 中为 FabricPool 创建流量分类策略

您可以选择设计 StorageGRID 流量分类策略，以优化 FabricPool 工作负载的服务质量。

有关此任务的详细信息，请参见"管理流量分类策略"。要使用FabricPool设置向导完成此任务，请转至"访问并完成FabricPool 设置向导"。

开始之前

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

关于此任务

为 FabricPool 创建流量分类策略的最佳实践取决于工作负载，如下所示：

- 如果您计划将FabricPool 主工作负载数据分层到StorageGRID 、则应确保FabricPool 工作负载具有大部分带宽。您可以创建流量分类策略来限制所有其他工作负载。

  一般来说， FabricPool 读取操作比写入操作更重要。

  例如，如果其他 S3 客户端使用此 StorageGRID 系统，则应创建流量分类策略。您可以限制其他分段，租户， IP 子网或负载平衡器端点的网络流量。

- 通常、您不应对任何FabricPool工作负载实施服务质量限制、而应仅对其他工作负载实施限制。
- 对其他工作负载的限制应考虑这些工作负载的行为。根据网格的规模估算和功能以及预期利用率，施加的限制也会有所不同。

步骤

1. 选择*配置* > 网络 > 流量分类。
2. 选择 * 创建 * 。
3. 为策略输入名称和问题描述 (可选)，然后选择*CONTINUE*。
4. 对于添加匹配规则步骤、请至少添加一个规则。
   a. 选择*添加规则*
   b. 对于类型，选择*负载平衡器端点*，然后选择为FabricPool 创建的负载平衡器端点。

      您也可以选择 FabricPool 租户帐户或存储分段。

   c. 如果希望此流量策略限制其他端点的流量，请选择*反向匹配*。
5. (可选)添加一个或多个限制、以控制规则匹配的网络流量。

   即使您未添加任何限制、StorageGRID 也会收集指标、以便您了解流量趋势。

   a. 选择*添加限制*。
   b. 选择要限制的流量类型以及要应用的限制。
6. 选择 * 继续 * 。

7. 阅读并查看流量分类策略。使用*上一步*按钮返回并根据需要进行更改。对策略满意后，选择*保存并继续*。

完成后

"查看网络流量指标"验证策略是否强制实施了预期的流量限制。

配置 ONTAP System Manager 以将 StorageGRID 添加为 FabricPool 云层

获取所需的StorageGRID 信息后、您可以转到ONTAP 将StorageGRID 添加为云层。

开始之前

- 完成FabricPool设置向导后、您将 `ONTAP_FabricPool_settings_*bucketname*.txt`下载文件。
- 如果您手动配置了StorageGRID 、则您拥有用于StorageGRID 的完全限定域名(FQDN)或StorageGRID HA组的虚拟IP (VIP)地址、负载平衡器端点的端口号、负载平衡器证书、 租户帐户的root用户的访问密钥ID和机密密钥、以及ONTAP 将在该租户中使用的分段名称。

访问ONTAP 系统管理器

以下说明介绍如何使用ONTAP 系统管理器将StorageGRID 添加为云层。您可以使用ONTAP 命令行界面完成相同的配置。有关说明，请转至 "适用于FabricPool的ONTAP文档"。

步骤

1. 访问要分层到StorageGRID 的ONTAP 集群的System Manager。
2. 以集群管理员身份登录。
3. 导航到*存储*>*层*>*添加云层*。
4. 从对象存储提供程序列表中选择* StorageGRID *。

输入StorageGRID 值

有关详细信息、请参见 "适用于FabricPool的ONTAP文档" 。

步骤

1. 使用您手动获取的文件或值填写"添加云层"表单 `ONTAP_FabricPool_settings_*bucketname*.txt`。

字段	说明
名称	输入此云层的唯一名称。您可以接受默认值。
URL模式	如果是"已配置S3端点域名"，请选择*Virtual-Hosted-Style URL*。 路径样式 **URL** 是 ONTAP 的默认设置，但建议对 StorageGRID 使用虚拟托管样式请求。如果为*服务器名称 (FQDN)* 字段提供的是 IP 地址而非域名，则必须使用*路径样式 URL*。

字段	说明
服务器名称(FQDN)	输入用于StorageGRID 的完全限定域名(FQDN)或StorageGRID HA组的虚拟IP (VIP)地址。例如， `s3.storagegrid.company.com`。 请注意以下事项： • 此处指定的IP地址或域名必须与您为StorageGRID 负载平衡器端点上传或生成的证书匹配。 • 如果您提供了域名、则DNS记录必须映射到要用于连接到StorageGRID 的每个IP地址。请参阅。 "配置DNS服务器"
SSL	Enabled (已启用)(默认)。
对象存储证书	粘贴要用于StorageGRID负载平衡器端点的PEM证书，包括：`-----BEGIN CERTIFICATE-----`和 `-----END CERTIFICATE-----`。 • 注意： * 如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。
端口	输入StorageGRID 负载平衡器端点使用的端口。ONTAP 将在连接到StorageGRID 时使用此端口。例如、10433.
访问密钥和机密密钥	输入StorageGRID 租户帐户的root用户的访问密钥ID和机密访问密钥。 提示：如果您将来在StorageGRID 中生成新的访问密钥和机密访问密钥，请在从StorageGRID 中删除旧值之前在ONTAP 中输入新密钥。否则、ONTAP 可能会暂时失去对StorageGRID 的访问权限。
容器名称	输入您创建的用于此ONTAP 层的StorageGRID 存储分段的名称。

2. 在ONTAP 中完成最终的FabricPool 配置。
   a. 将一个或多个聚合附加到云层。
   b. (可选)创建卷分层策略。

使用 FabricPool 为 StorageGRID 配置 DNS 服务器条目

配置高可用性组、负载平衡器端点和S3端点域名后、必须确保DNS包含StorageGRID 的必要条目。您必须为安全证书中的每个名称以及可能使用的每个IP地址提供一个DNS条目。

请参阅。 "负载平衡注意事项"

StorageGRID 服务器名称的DNS条目

添加DNS条目以将StorageGRID 服务器名称(完全限定域名)与要使用的每个StorageGRID IP地址相关联。在DNS中输入的IP地址取决于您是否使用负载平衡节点的HA组：

- 如果您已配置HA组、则ONTAP 将连接到该HA组的虚拟IP地址。
- 如果您不使用HA组、则ONTAP 可以使用任何网关节点或管理节点的IP地址连接到StorageGRID 负载平衡器服务。
- 如果服务器名称解析为多个IP地址、ONTAP 将使用所有IP地址(最多16个IP地址)建立客户端连接。建立连接后， IP 地址将以轮循方式进行选取。

虚拟托管式请求的 **DNS** 条目

如果您已定义"S3端点域名"并且将使用虚拟托管样式的请求，请为所有必需的 S3 端点域名添加 DNS 条目，包括任何通配符名称。

适用于**FabricPool** 的**StorageGRID** 最佳实践

StorageGRID 高可用性 **(HA)** 组与 **FabricPool** 的最佳实践

在将StorageGRID 作为FabricPool 云层附加之前、请了解StorageGRID 高可用性(HA)组并查看将HA组与FabricPool 结合使用的最佳实践。

什么是 **HA** 组?

高可用性(HA)组是来自多个StorageGRID 网关节点和/或管理节点的一组接口。HA组有助于保持客户端数据连接可用。如果HA组中的活动接口发生故障、则备份接口可以管理工作负载、而对FabricPool 操作的影响微乎其微。

每个 HA 组均可提供对关联节点上共享服务的高可用性访问。例如，如果 HA 组仅包含网关节点上的接口，或者同时包含管理节点和网关节点上的接口，则可以对共享负载平衡器服务进行高可用性访问。

要了解有关高可用性组的更多信息，请参见"管理高可用性(HA)组"。

使用**HA**组

为FabricPool 创建StorageGRID HA组的最佳实践取决于工作负载。

- 如果您计划将FabricPool 与主工作负载数据结合使用、则必须创建一个至少包含两个负载平衡节点的HA组、以防止数据检索中断。
- 如果您计划使用 FabricPool snapshot-only 卷分层策略或非主本地性能层（例如，灾难恢复位置或 NetApp SnapMirror ® 目标），则只能为 HA 组配置一个节点。

以下说明介绍如何为主动备份 HA 设置 HA 组（一个节点为活动节点，一个节点为备份节点）。但是，您可能更喜欢使用 DNS 轮循或主动 - 主动 HA 。要了解这些其他HA配置的优势，请参见"HA 组的配置选项"。

StorageGRID 负载平衡与 **FabricPool** 的最佳实践

在将StorageGRID 作为FabricPool 云层附加之前、请查看将负载平衡器与FabricPool 结合使用的最佳实践。

要了解有关StorageGRID负载平衡器和负载平衡器证书的常规信息，请参见"负载平衡注意事项"。

您可以控制哪些租户可以使用特定负载平衡器端点来访问其分段。您可以允许所有租户、允许某些租户或阻止某些租户。创建供FabricPool 使用的负载平衡端点时，请选择*允许所有租户*。ONTAP 会对StorageGRID 存储分段中的数据进行加密、因此这一额外的安全层几乎不会提供额外的安全性。

安全证书的最佳实践

在创建供FabricPool 使用的StorageGRID 负载平衡器端点时、您需要提供安全证书、以使ONTAP 能够向StorageGRID 进行身份验证。

大多数情况下、ONTAP 和StorageGRID 之间的连接应使用传输层安全(Transport Layer Security、TLS)加密。支持使用不带TLS加密的FabricPool 、但不建议这样做。为StorageGRID 负载平衡器端点选择网络协议时，请选择*HTTPS*。然后、提供允许ONTAP 向StorageGRID 进行身份验证的安全证书。

要了解有关负载平衡端点的服务器证书的详细信息，请执行以下操作：

- "管理安全证书"
- "负载平衡注意事项"
- "服务器证书的强化准则"

将证书添加到**ONTAP**

将StorageGRID 添加为FabricPool 云层时、必须在ONTAP 集群上安装相同的证书、包括根证书颁发机构(CA)证书和任何从属证书颁发机构(CA)证书。

管理证书到期时间



如果用于保护ONTAP 和StorageGRID 之间连接的证书到期、FabricPool 将暂时停止工作、并且ONTAP 将暂时无法访问分层到StorageGRID 的数据。

要避免证书到期问题、请遵循以下最佳实践：

- 请仔细监控任何警告证书到期日期即将到来的警报，例如*负载平衡器端点证书到期*和* S3 API*警报的全局服务器证书到期。
- 请始终保持证书的StorageGRID 和ONTAP 版本同步。如果要替换或续订用于负载平衡器端点的证书、则必须替换或续订ONTAP 用于云层的等效证书。
- 使用公共签名的CA证书。如果您使用的是由CA签名的证书、则可以使用网格管理API自动轮换证书。这样、您就可以无干扰地替换即将到期的证书。
- 如果您已生成自签名StorageGRID 证书、并且该证书即将过期、则必须在现有证书过期之前手动替换StorageGRID 和ONTAP 中的证书。如果自签名证书已过期、请在ONTAP 中关闭证书验证以防止访问丢失。

  有关说明、请参见。 "NetApp知识库：如何在现有ONTAP FabricPool 部署上配置新的StorageGRID 自签名服务器证书"

使用 **StorageGRID ILM** 处理 **FabricPool** 数据的最佳实践

如果要使用FabricPool 将数据分层到StorageGRID 、则必须了解对FabricPool 数据使

用StorageGRID 信息生命周期管理(ILM)的要求。

> FabricPool 不了解 StorageGRID ILM 规则或策略。如果 StorageGRID ILM 策略配置不当，可能会发生数据丢失。有关详细信息，请参见"使用ILM规则管理对象"和"创建ILM策略"。

将**ILM**与**FabricPool** 结合使用的准则

使用FabricPool设置向导时、该向导会自动为您创建的每个S3存储分段创建一个新的ILM规则、并将该规则添加到非活动策略中。系统将提示您激活此策略。自动创建的规则遵循建议的最佳实践：在单个站点上使用2+1纠删编码。

如果您要手动配置StorageGRID 、而不是使用FabricPool 设置向导、请查看这些准则、以确保您的ILM规则和ILM策略适合FabricPool 数据和您的业务需求。您可能需要创建新规则并更新活动ILM策略、以符合这些准则。

- 您可以使用复制和纠删编码规则的任意组合来保护云层数据。

  建议的最佳实践是，在站点内使用 2+1 纠删编码，以实现经济高效的数据保护。纠删编码使用的 CPU 较多，但提供的存储容量明显低于复制。4+1 和 6+1 方案使用的容量小于 2+1 方案。但是，如果您需要在网格扩展期间添加存储节点， 4+1 和 6+1 方案的灵活性将会降低。有关详细信息，请参见 "为经过纠删编码的对象添加存储容量"。

- 应用于 FabricPool 数据的每个规则都必须使用纠删编码，或者必须至少创建两个复制副本。

  > 如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

- 如果需要"从StorageGRID中删除FabricPool数据"，请使用ONTAP检索FabricPool卷的所有数据并将其提升到性能层。

  > 为避免数据丢失、请勿使用将过期的ILM规则或删除FabricPool云层数据。将每个ILM规则中的保留期限设置为*永久*、以确保StorageGRID ILM不会删除FabricPool对象。

- 请勿创建将FabricPool 云层数据从存储分段移动到其他位置的规则。您不能使用云存储池将FabricPool 数据移动到其他对象存储。

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

- 从 ONTAP 9.8 开始，您可以选择创建对象标记来帮助对分层数据进行分类和排序，以便于管理。例如，您只能在连接到 StorageGRID 的 FabricPool 卷上设置标记。然后，在 StorageGRID 中创建 ILM 规则时，您可以使用对象标记高级筛选器选择并放置此数据。

StorageGRID 全局设置与 **FabricPool** 的最佳实践

在配置StorageGRID 系统以与FabricPool 结合使用时、您可能需要更改其他StorageGRID 选项。在更改全局设置之前、请考虑此更改会对其他S3应用程序产生何种影响。

审核消息和日志目标

FabricPool 工作负载的读取操作率通常较高、从而可能会生成大量审核消息。

- 如果您不需要记录FabricPool或任何其他 S3 应用程序的客户端读取操作，则可以选择转到 配置 > 监控 > 审计和系统日志服务器。将 客户端读取 设置更改为 错误 以减少审计日志中记录的审计消息数量。看"配置日志管理和外部系统日志服务器"了解详情。
- 如果您的网格很大、可以使用多种类型的S3应用程序、也可以保留所有审核数据、配置外部系统日志服务器并远程保存审核信息。使用外部服务器可以最大限度地降低审核消息日志记录对性能的影响、而不会降低审核数据的完整性。有关详细信息、请参见。 "外部系统日志服务器的注意事项"

对象加密

配置StorageGRID时、如果其他StorageGRID客户端需要数据加密、您可以选择启用"用于存储对象加密的全局选项"。从 FabricPool 分层到 StorageGRID 的数据已加密，因此不需要启用 StorageGRID 设置。客户端加密密钥归 ONTAP 所有。

对象压缩

配置StorageGRID时，请勿启用"用于压缩存储对象的全局选项"。已对从 FabricPool 分层到 StorageGRID 的数据进行压缩。使用StorageGRID 选项不会进一步减小对象的大小。

S3 对象锁定

如果您的StorageGRID系统启用了全局 S3 对象锁定设置，请不要启用"S3 对象锁定"当您创建FabricPool存储桶时。 FabricPool存储桶不支持 S3 对象锁定。

存储分段一致性

对于FabricPool存储分段、建议的存储分段一致性为*新写入后读取*、这是新存储分段的默认一致性。请勿编辑FabricPool存储分段以使用*可用*或*强站点*。

FabricPool 分层

如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。例如，如果 StorageGRID 节点正在 VMware 主机上运行，请确保为 StorageGRID 节点的数据存储库提供支持的卷未启用 FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

从**StorageGRID**中删除**FabricPool**数据

如果需要删除当前存储在StorageGRID中的FabricPool数据、则必须使用ONTAP检索FabricPool卷的所有数据并将其提升到性能层。

开始之前

- 您已查看中的说明和注意事项 "将数据提升到性能层"。
- 您正在使用ONTAP 9.8或更高版本。

- 您正在使用"支持的 Web 浏览器"。
- 您属于具有的FabricPool租户帐户的StorageGRID用户组"管理所有分段或root访问权限"。

关于此任务

以下说明介绍了如何将数据从StorageGRID移回FabricPool。您可以使用ONTAP和StorageGRID租户管理器执行此操作步骤。

步骤

1. 在ONTAP中、发出 `volume modify`命令。

   设置 `tiering-policy`为 `none`可停止新的分层、而设置为 `promote`可返回先前分 `cloud-retrieval-policy`层到StorageGRID的所有数据。

   请参阅。 "将 FabricPool 卷中的所有数据提升到性能层"

2. 等待此操作完成。

   您可以使用 `volume object-store`命令和 `tiering`选项 "检查性能层促销的状态"。

3. 提升操作完成后、登录到StorageGRID租户管理器的FabricPool租户帐户。
4. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
5. 确认FabricPool存储分段现在为空。
6. 如果存储分段为空，"删除存储分段"。

完成后

删除存储分段后、无法再继续从FabricPool到StorageGRID的分层。但是、由于本地层仍附加到StorageGRID云层、ONTAP系统管理器将返回错误消息、指示存储分段不可访问。

要防止出现这些错误消息、请执行以下操作之一：

- 使用FabricPool镜像将其他云层附加到聚合。
- 将FabricPool聚合中的数据移动到非FabricPool聚合、然后删除未使用的聚合。

有关说明、请参见。 "适用于FabricPool的ONTAP文档"

使用StorageGRID租户和客户端

使用租户帐户

使用 StorageGRID 租户帐户

租户帐户允许您使用简单存储服务(S3) REST API在StorageGRID系统中存储和检索对象。

什么是租户帐户？

每个租户帐户都有自己的联合组或本地组、用户、S3分段和对象。

租户帐户可用于按不同实体隔离存储的对象。例如，以下任一使用情形均可使用多个租户帐户：

- * 企业用例： * 如果在企业中使用 StorageGRID 系统，则网格的对象存储可能会被组织中的不同部门隔离。例如，可能存在营销部门，客户支持部门，人力资源部门等的租户帐户。

  > 如果您使用 S3 客户端协议，您还可以使用 S3 存储桶和存储桶策略在企业各部门之间隔离对象。您不需要创建单独的租户帐户。请参阅实施说明"S3存储分段和存储分段策略"了解更多信息。

- * 服务提供商用例： * 如果服务提供商正在使用 StorageGRID 系统，则网格的对象存储可能会被租用该存储的不同实体分隔。例如，可能存在公司 A ，公司 B ，公司 C 等的租户帐户。

如何创建租户帐户

租户帐户由创建"使用网格管理器的 StorageGRID 网格管理员"。创建租户帐户时、网格管理员指定以下内容：

- 基本信息、包括租户名称、客户端类型(S3)和可选存储配额。
- 租户帐户的权限、例如租户帐户是否可以使用S3平台服务、配置自己的身份源、使用S3 Select或使用网格联盟连接。
- 租户的初始root访问权限、具体取决于StorageGRID 系统是使用本地组和用户、身份联合还是单点登录(SSO)。

此外，如果 S3 租户帐户需要符合法规要求，网格管理员可以为 StorageGRID 系统启用 S3 对象锁定设置。启用 S3 对象锁定后，所有 S3 租户帐户均可创建和管理合规的存储分段。

配置 S3 租户

完成后"已创建 S3 租户帐户"，您可以访问租户管理器来执行如下任务：

- 设置身份联合(除非身份源与网格共享)
- 管理组和用户
- 使用网格联合进行帐户同步和跨网格复制
- 管理 S3 访问密钥

- 创建和管理S3存储分段
- 使用S3平台服务
- 使用 S3 Select
- 监控存储使用情况

虽然您可以使用租户管理器创建和管理S3存储分段、但必须使用"S3 客户端"或"S3控制台"来加存和管理对象。

如何登录和注销

Sign in 到 StorageGRID 租户管理器

您可以通过在的地址栏中输入租户的URL来访问租户管理器"支持的 Web 浏览器"。

开始之前

- 您已拥有登录凭据。
- 网格管理员提供了一个用于访问租户管理器的URL。URL 将类似于以下示例之一：

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  此URL始终包括完全限定域名(FQDN)、管理节点的IP地址或管理节点HA组的虚拟IP地址。它可能还包括端口号、20位租户帐户ID或这两者。

- 如果URL不包括租户的20位帐户ID、则您具有此帐户ID。
- 您正在使用"支持的 Web 浏览器"。
- 已在 Web 浏览器中启用 Cookie 。
- 您属于具有"特定访问权限"的用户组。

步骤

1. 启动"支持的 Web 浏览器"。
2. 在浏览器的地址栏中，输入用于访问租户管理器的 URL 。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。
4. 登录到租户管理器。

   显示的登录屏幕取决于您输入的URL以及是否已为StorageGRID 配置单点登录(Single Sign On、SSO)。

未使用**SSO**

如果StorageGRID 未使用SSO、则会显示以下屏幕之一：

- 网格管理器登录页面。选择*租户登录*链接。
- 租户管理器登录页面。 *帐户*字段可能已经填写完毕。
  i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。
  ii. 输入用户名和密码。
  iii. 选择 * 登录 * 。

  此时将显示租户管理器信息板。

  iv. 如果您收到了其他人的初始密码，请选择*_USERNAME_*>*更改密码*以保护您的帐户。

使用**SSO**

如果StorageGRID 正在使用SSO、则会显示以下屏幕之一：

- 您组织的 SSO 页面。

  输入您的标准SSO凭据，然后选择*登录*。

- 租户管理器 SSO 登录页面。
  i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。
  ii. 选择 * 登录 * 。
  iii. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。

  此时将显示租户管理器信息板。

Sign out StorageGRID 租户管理器

使用租户管理器完成操作后、您必须注销以确保未经授权的用户无法访问StorageGRID 系统。根据浏览器 Cookie 设置，关闭浏览器可能无法将您从系统中注销。

步骤

1. 找到用户界面右上角的用户名下拉列表。
2. 选择用户名，然后选择*Sign Out。
   - 如果未使用 SSO：

     您已从管理节点注销。此时将显示租户管理器登录页面。

     如果您已登录到多个管理节点，则必须从每个节点注销。

◦ 如果启用了 SSO：

您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。您刚刚访问的租户帐户的名称将在 * 近期帐户 * 下拉列表中列为默认名称，并显示租户的 * 帐户 ID* 。

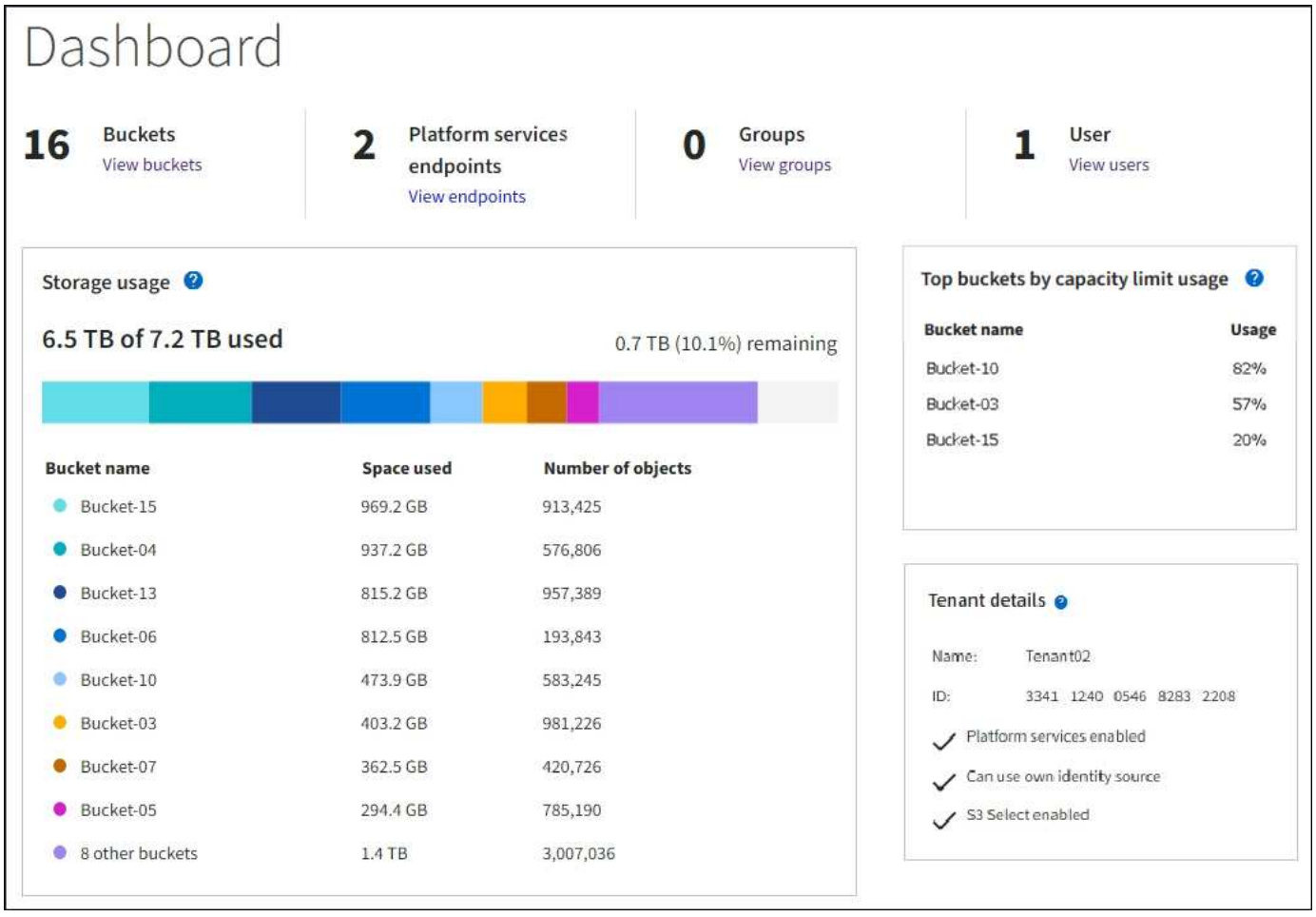
如果启用了 SSO ，并且您还登录到网格管理器，则还必须注销网格管理器才能注销 SSO 。

StorageGRID 中的租户管理器信息板

租户管理器仪表板概述了租户帐户的配置以及租户 S3 存储桶中对象使用的空间量。如果租户有配额，仪表板会显示已使用的配额量以及剩余的配额量。如果存在与租户帐户相关的任何错误，则错误将显示在仪表板上。

属于该租户的所有对象的逻辑大小包括未完成和正在进行的分段上传。该大小不包括用于 ILM 策略的额外物理空间。已用空间值是估计值。这些估计受到摄取时间、网络连接和节点状态的影响。

上载对象后、信息板将类似于以下示例：



租户帐户信息

信息板顶部显示已配置的分段或容器、组和用户的数量。此外、它还会显示平台服务端点的数量(如果已配置)。

选择链接以查看详细信息。

根据"租户管理权限"您拥有的以及您配置的选项、信息板的其余部分将显示准则、存储使用情况、对象信息和租户详细信息的各种组合。

存储和配额使用量

存储使用情况面板包含以下信息：

- 租户的对象数据量。

  此值表示已上传的对象数据总量，不表示用于存储这些对象及其元数据副本的空间。

- 如果设置了配额，则表示可用于对象数据的总空间量以及剩余空间量和百分比。配额限制了可载入的对象数据量。

  > 配额使用量基于内部估计值、在某些情况下可能会超过此值。例如，当租户开始上传对象时， StorageGRID 会检查配额，如果租户超过配额，则会拒绝新的载入。但是，在确定是否超过配额时， StorageGRID 不会考虑当前上传的大小。如果删除了对象、则可能会暂时阻止租户上传新对象、直到重新计算配额使用量为止。计算配额使用量可能需要10分钟或更长时间。

- 一个条形图，表示最大分段或容器的相对大小。

  您可以将光标置于任何图表区块上方，以查看该分段或容器占用的总空间。



- 要与条形图相对应，需要列出最大的分段或容器，包括对象数据总量以及每个分段或容器的对象数量。

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

如果租户具有九个以上的分段或容器，则所有其他分段或容器将合并到列表底部的一个条目中。

要更改租户管理器中显示的存储值的单位、请选择租户管理器右上角的用户下拉列表、然后选择*用户首选项*。

配额使用情况警报

如果已在网格管理器中启用配额使用情况警报、则在配额较低或超过配额时、这些警报将显示在租户管理器中、如下所示：

- 如果已使用租户配额的 90% 或更多，则会触发 * 租户配额使用量高 * 警报。

  请考虑让网格管理员增加配额。

- 如果超过配额、则会显示一条通知、告知您无法上传新对象。

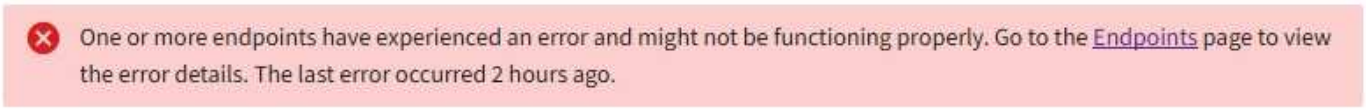
[[bket-Capacity -usage]]容量限制使用量

如果您已为存储分段设置容量限制、则租户管理器信息板将按容量限制使用量显示前几个存储分段的列表。

如果没有为存储分段设置限制、则其容量将无限制。但是、如果租户帐户具有总存储配额、并且已达到该配额、则无论存储分段上的剩余容量限制如何、您都无法加载更多对象。

端点错误

如果已使用网格管理器配置一个或多个端点以用于平台服务、则租户管理器信息板会在过去七天内发生任何端点错误时显示警报。



要查看有关的详细信息"平台服务端点错误"，请选择*端点*以显示端点页面。

租户管理 API

了解 StorageGRID 租户管理 API

您可以使用租户管理 REST API 执行系统管理任务，而不是使用租户管理器用户界面。例如，您可能希望使用 API 来自动执行操作或更快地创建多个实体，例如用户。

租户管理 API：

- 使用 Swagger 开源 API 平台。Swagger 提供了一个直观的用户界面，支持开发人员和非开发人员与 API 进行交互。Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。
- 使用"版本控制以支持无中断升级"。

要访问租户管理 API 的 Swagger 文档，请执行以下操作：

1. 登录到租户管理器。
2. 从租户管理器的顶部、选择帮助图标并选择* API文档*。

API操作

租户管理 API 将可用的 API 操作组织到以下部分中：

- 帐户：对当前租户帐户执行的操作、包括获取存储使用情况信息。
- **auth**：执行用户会话身份验证的操作。

  租户管理 API 支持不承载令牌身份验证方案。对于租户登录，您需要在身份验证请求的JSON正文(即)中提供用户名、密码和帐户ID `POST /api/v3/authorize`。如果用户已成功通过身份验证，则会返回一个安全令牌。此令牌必须在后续 API 请求的标题中提供（ " 授权：承载令牌 " ）。

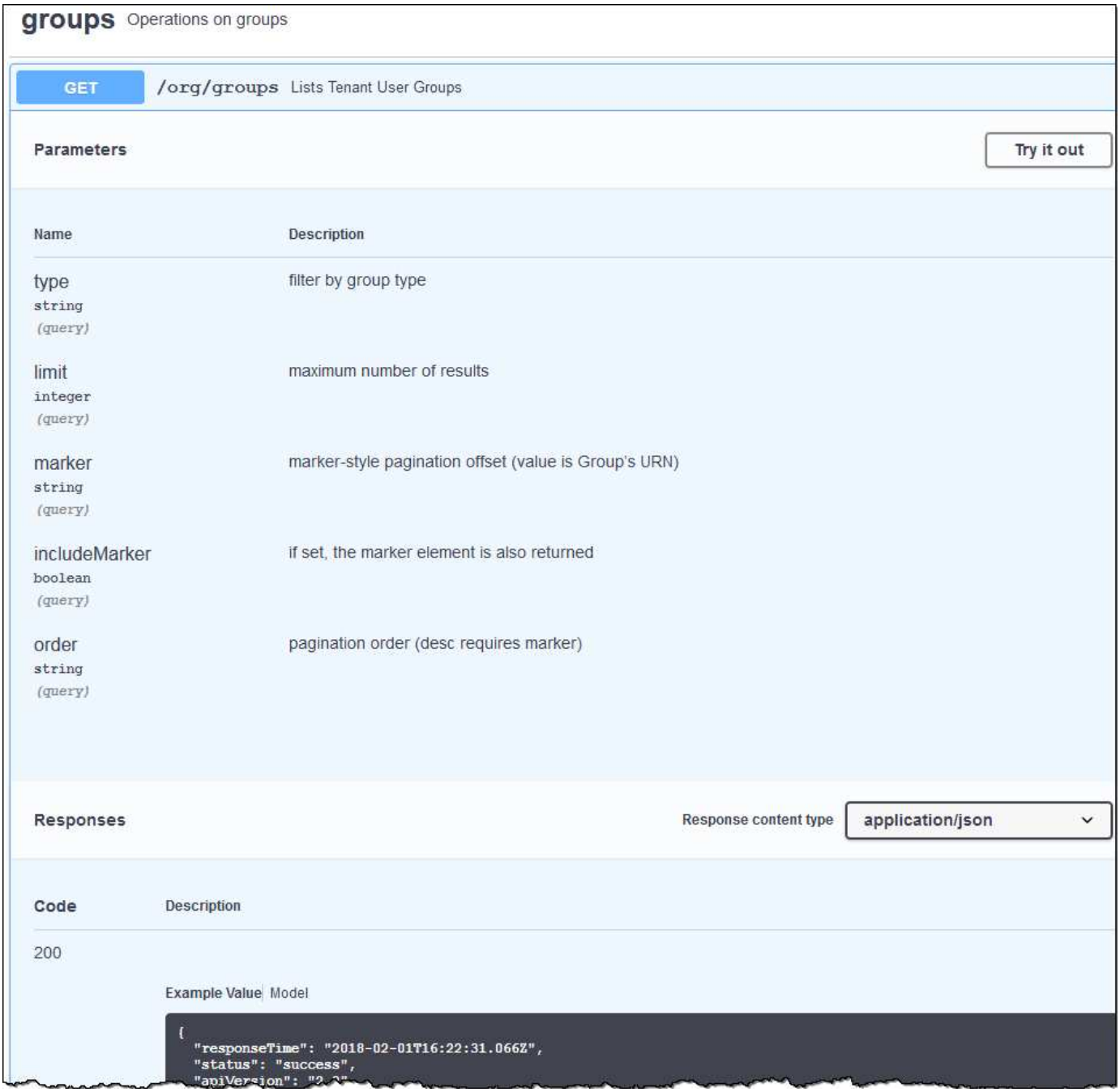
  有关提高身份验证安全性的信息，请参见"防止跨站点请求伪造"。

  > 如果为 StorageGRID 系统启用了单点登录（ SSO ），则必须执行不同的步骤进行身份验证。请参见"有关使用网格管理 API 的说明"。

- **config**：与租户管理API的产品版本和版本相关的操作。您可以列出该版本支持的产品版本和主要 API 版本。
- 容器：对 S3 存储桶的操作。
- *DEactive-Features *：用于查看可能已停用的功能的操作。
- 端点：用于管理端点的操作。通过端点， S3 存储分段可以使用外部服务进行 StorageGRID CloudMirror 复制，通知或搜索集成。
- 网格联合连接：对网格联合连接和跨网格复制的操作。
- 组：用于管理本地租户组和从外部身份源检索联合租户组的操作。
- 身份源：用于配置外部身份源以及手动同步联盟组和用户信息的操作。
- *ILM：有关信息生命周期管理(ILM)设置的操作。
- 区域：用于确定已为StorageGRID 系统配置了哪些区域的操作。
- **S3**：用于管理租户用户的S3访问密钥的操作。
- **s3-configurations**：检索 S3 全局配置的操作。
- **S3-object-lock**：对全局S3对象锁定设置执行操作，用于支持合规性。
- 用户：用于查看和管理租户用户的操作。

操作详细信息

展开每个 API 操作时，您可以看到其 HTTP 操作，端点 URL ，任何必需或可选参数的列表，请求正文示例（如果需要）以及可能的响应。



问题描述 **API** 请求

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

步骤

1. 选择 HTTP 操作以查看请求详细信息。
2. 确定此请求是否需要其他参数，例如组或用户 ID 。然后，获取这些值。您可能需要先对其他 API 请求进行问题描述 处理，以获取所需的信息。
3. 确定是否需要修改示例请求正文。如果是，您可以选择 * 型号 * 来了解每个字段的要求。
4. 选择 * 试用 * 。

5. 提供所需的任何参数，或根据需要修改请求正文。
6. 选择 * 执行 * 。
7. 查看响应代码以确定请求是否成功。

StorageGRID 租户管理 API 版本控制

租户管理 API 使用版本控制来支持无中断升级。

例如、此请求URL指定API版本4。

`https://hostname_or_ip_address/api/v4/authorize`

如果所做的更改与旧版本不兼容、则API的主要版本会发生碰撞。如果对_are compender_与旧版本进行了更改、则API的次要版本会发生碰撞。兼容的更改包括添加新端点或新属性。

以下示例说明了如何根据所做更改的类型对 API 版本进行递增。

API 的更改类型	旧版本	新版本
与旧版本兼容	2.1	2.2
与旧版本不兼容	2.1	3.0

首次安装StorageGRID软件时、仅会启用最新版本的API。但是，在升级到 StorageGRID 的新功能版本时，您仍可以访问至少一个 StorageGRID 功能版本的旧版 API 。

> 您可以配置受支持的版本。有关详细信息，请参见Swagger API文档的*config*部分"网格管理API"。在更新所有API客户端以使用较新版本后、您应停用对较旧版本的支持。

已过时的请求将通过以下方式标记为已弃用：

- 响应标头为 "depression: true"
- JSON 响应正文包含 "depressioned" ： true
- NMS.log 中会添加一个已弃用的警告。例如：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

确定当前版本支持哪些 API 版本

使用 `GET /versions`API请求返回受支持的API主要版本的列表。此请求位于Swagger API文档的*config*部分。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

指定请求的 **API** 版本

您可以使用路径参数(`/api/v4`()或标题(`Api-Version: 4`()指定API版本。如果同时提供这两个值，则标头值将覆盖路径值。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

防止 **StorageGRID** 中的跨站请求伪造

您可以通过使用 CSRF 令牌增强使用 Cookie 的身份验证，帮助防止 StorageGRID 受到跨站点请求伪造（ CSRF ）攻击。网格管理器和租户管理器会自动启用此安全功能；其他 API 客户端可以选择在登录时是否启用此功能。

如果攻击者可能触发对其他站点的请求（例如使用 HTTP 表单发布），则可以对使用已登录用户的 cookie 发出的某些请求进行发生原因 处理。

StorageGRID 可通过使用 CSRF 令牌帮助防止 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标题或特定后处理正文参数的内容匹配。

要启用此功能、请在身份验证期间将参数设置 `csrfToken`为 `true`。默认值为 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果为true、则会为Cookie设置一个 `GridCsrfToken`用于登录到网格管理器的随机值、并 `AccountCsrfToken`

为Cookie设置一个用于登录到租户管理器的随机值。

如果存在 Cookie ，则可以修改系统状态的所有请求（ POST ， PUT ， patch ， delete ）都必须包括以下项之一：

- `X-Csrf-Token`标头、标头值设置为CRF令牌cookie的值。
- 对于接受窗体编码正文的端点： `csrfToken`窗体编码请求正文参数。

要配置CRF保护，请使用"网格管理 API"或"租户管理 API"。

> 设置了CRF令牌Cookie的请求还会对任何希望使用JSON请求正文作为额外保护来抵御CRF攻击的请求强制实施"Contene-Type：application/json"标头。

使用网格联合连接

同步 **StorageGRID** 中的租户组和用户

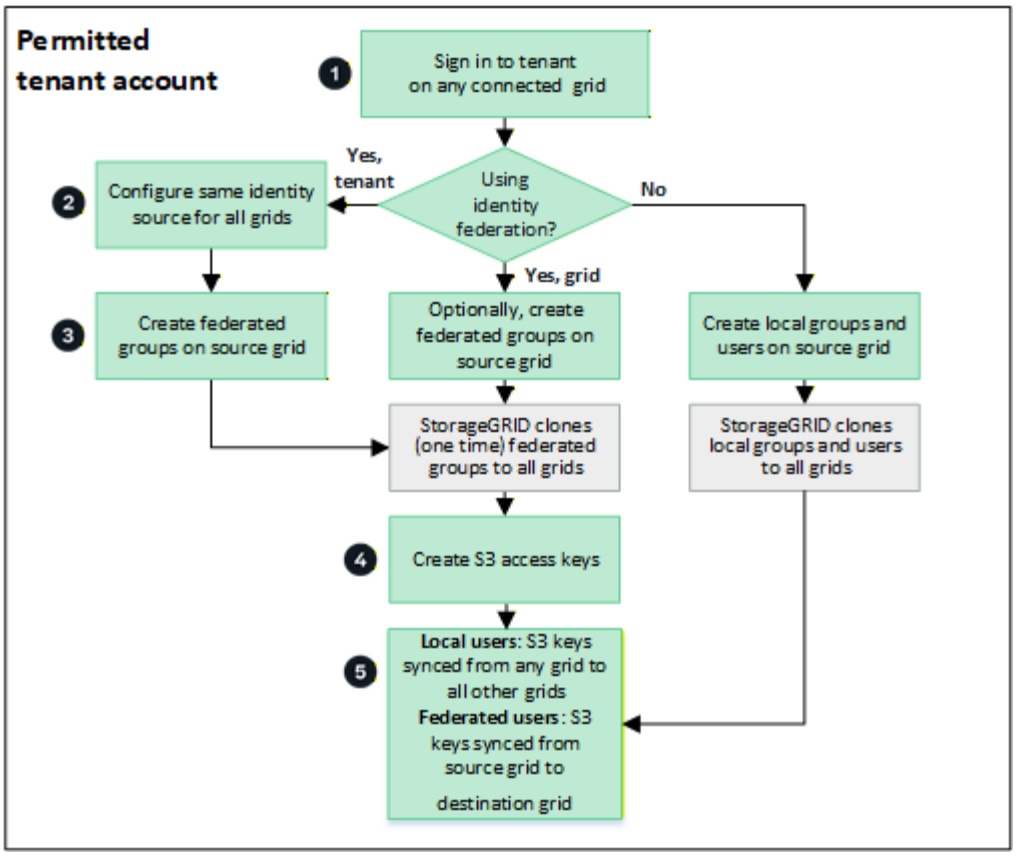
如果创建或编辑租户以使用网格联合连接，则该租户将从一个 StorageGRID 系统（源租户）复制到所有其他连接的 StorageGRID 系统（副本租户）。租户复制后，租户组、用户和 S3 访问密钥将在连接的网格中同步。

最初创建租户的 StorageGRID 系统是租户的_源网格_。租户将复制到一个或多个_目标网格_。所有已连接网格上的租户帐户具有相同的帐户 ID、名称、描述、存储配额、分配的权限和 root 用户密码。有关详细信息，请参阅 "了解网格联盟的帐户同步" 和 "管理允许的租户"。

需要同步租户帐户信息，以便对存储桶对象执行 "跨网格复制" 操作。在所有网格上拥有相同的租户组和用户，可确保您能够访问任何已连接网格上的相应存储桶和对象。

用于帐户同步的租户工作流程

如果您的租户帐户具有*使用网格联合连接*权限，请查看工作流程图，了解同步组、用户和 S3 访问密钥所需执行的步骤。



以下是工作流中的主要步骤：

1 登录到租户

在任何连接的网格上登录到租户帐户。

2 (可选)配置身份联合

如果您的租户帐户具有*使用自己的身份源*权限以使用联合组和用户，请为源和一个或多个目标租户帐户配置相同的身份源（使用相同的设置）。联合组在创建时克隆，联合用户在创建密钥时克隆。要进行克隆，必须在所有网格上配置相同的身份源。有关说明，请参阅 "使用身份联合"。

3 创建组和用户

您可以从任何连接的网格创建组和用户。添加新本地组时，StorageGRID 会自动将其同步到所有连接的网格。对本地组（编辑、删除）的更改也会持续同步。联合组在创建时克隆一次。

- 如果为整个StorageGRID系统或租户帐户配置了身份联合、"创建新租户组"可通过从身份源导入联合组来实现。
- 如果您不使用身份联合，"创建新的本地组"进而"创建本地用户"。

4 创建**S3**访问密钥

您可以"创建您自己的访问密钥"或在任何网格上"创建其他用户的访问密钥"以访问所有连接网格上的存储桶。

5 同步 **S3** 访问密钥

如果需要在所有网格上使用相同的访问密钥访问存储桶，请在其中一个网格上创建访问密钥。对于本地用户，默认情况下会自动同步访问密钥。对于联合用户，您必须在源网格上创建 S3 访问密钥，并选择 **Enable access key sync** 以将密钥同步到所有目标网格。

如何同步组、用户和 **S3** 访问密钥?

查看此部分，了解如何跨连接的网格同步组、用户和 S3 访问密钥。

本地组会持续同步

创建租户帐户并将其复制到目标网格后，StorageGRID 会持续同步所有已连接网格中的本地组。在任何网格上对本地组所做的所有更改（包括创建、编辑和删除操作）都会自动复制到所有其他已连接的网格。

原始组及其同步副本都具有相同的访问模式、组权限和 S3 组策略。有关说明，请参阅"为 S3 租户创建组"。

本地用户会不断同步

当您在任何已连接的网格上创建新的本地用户时，StorageGRID 会自动将该用户同步到所有其他已连接的网格。后续更改（包括编辑、删除和密码重置）也会持续同步。原始用户及其同步副本具有相同的全名、用户名和 * 拒绝访问 * 设置。每个网格上的相同用户也属于相同的组。有关说明，请参见 "管理用户"。

联合组在创建时同步一次

假设使用帐户同步的 "单点登录" 和 "身份联合" 要求已满足，您为网格上的租户创建（导入）的联合组将自动同步到所有其他连接网格上的租户。

这两个组具有相同的访问模式、组权限和 S3 组策略。

为源租户创建联合组并同步到其他网格后，联合用户可以在任何连接的网格上登录到租户。联合组的后续更改不会在网格之间自动同步。

S3 访问密钥可以自动或手动同步

默认情况下，StorageGRID 会自动同步 S3 访问密钥。出于安全考虑，您可以为每个租户禁用 S3 访问密钥的自动同步，并为每个网格上的每个租户提供不同的密钥。

要管理已连接网格上的访问密钥，您可以执行以下操作之一：

- 如果不需要对每个网格使用相同的密钥，则可以禁用自动访问密钥同步，并在每个网格上"创建您自己的访问密钥"或"创建其他用户的访问密钥"。

同步联合用户的 S3 访问密钥时，用户和 S3 访问密钥都将同步到目标租户。

本地用户拥有的 S3 访问密钥在连接的网格之间持续同步，包括在删除密钥时。联合用户拥有的 S3 访问密钥在创建时同步一次；后续更改（包括删除）不会被复制。您可以为每个租户连接启用或禁用访问密钥同步。

添加到目标网格的组和用户已同步

在任何连接的网格上所做的更改，包括创建或导入本地组和用户，都会自动同步到所有其他连接的网格。

已编辑或删除的本地组、用户和访问密钥已同步

对本地用户拥有的本地组、本地用户和 S3 访问密钥的更改在所有连接的网格中持续同步。同步操作包括编辑、删除和密码重置。

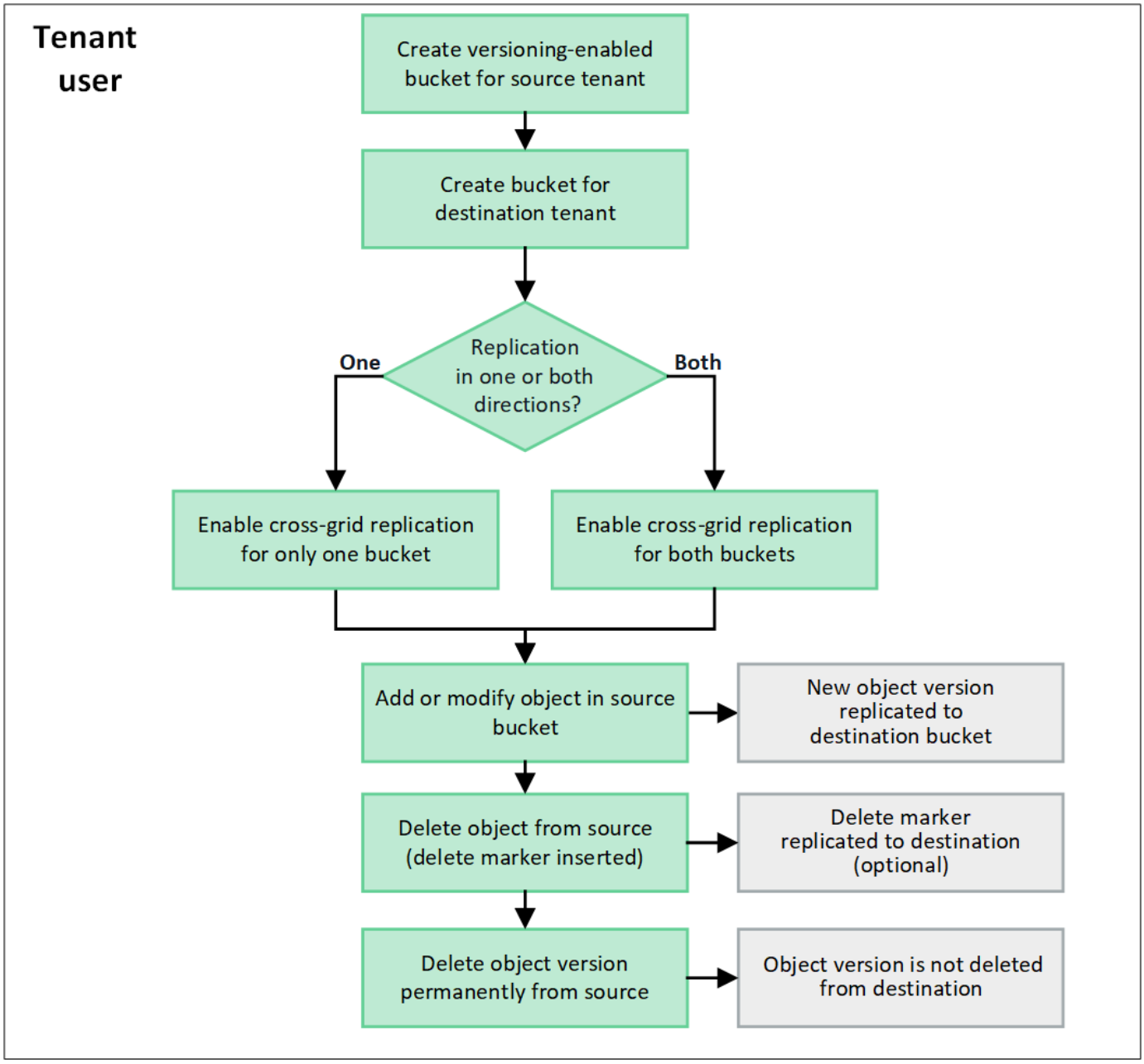
初始创建后，对联合用户拥有的联合组和 S3 访问密钥的更改不会同步。

在 **StorageGRID** 中管理跨网格复制

如果在创建租户帐户时为其分配了*使用网格联合连接*权限、则可以使用跨网格复制在租户源网格上的分段和租户目标网格上的分段之间自动复制对象。跨网格复制可以在一个方向或两个方向上进行。

跨网格复制工作流

工作流程图总结了配置两个网格上的存储桶之间的跨网格复制所执行的步骤。图表下方对这些步骤进行了更详细的描述。



配置跨网格复制

在使用跨网格复制之前，您必须登录每个网格上相应的租户帐户并创建两个存储桶。然后，您可以在一个或两个存储桶上启用跨网格复制。

开始之前

- 您已经查看了跨网格复制的要求。请参阅"什么是跨网格复制" 。
- 您正在使用"支持的 Web 浏览器"。
- 租户帐户具有*使用网格联合连接*权限，并且两个网格上都存在相同的租户帐户。请参阅"管理网格联盟连接允许的租户" 。
- 您登录的租户用户已存在于两个网格中，并且属于具有"root访问权限"。
- 如果您以本地用户身份登录到租户的目标网格，则租户帐户的根用户已为您在该网格上的用户帐户设置了密码。

创建两个存储桶

第一步，登录每个网格上相应的租户帐户，并在每个网格上创建一个存储桶。

步骤

1. 从网格联合连接中的任一网格开始、创建一个新存储分段：
   a. 使用两个网格上的租户用户凭据登录到租户帐户。

      如果您无法以本地用户身份登录租户的目标网格，请确认租户帐户的根用户已为您的用户帐户设置密码。

   b. 按照的说明进行操作"创建S3存储分段"。

      每个网格上的存储桶名称和区域可以不同。

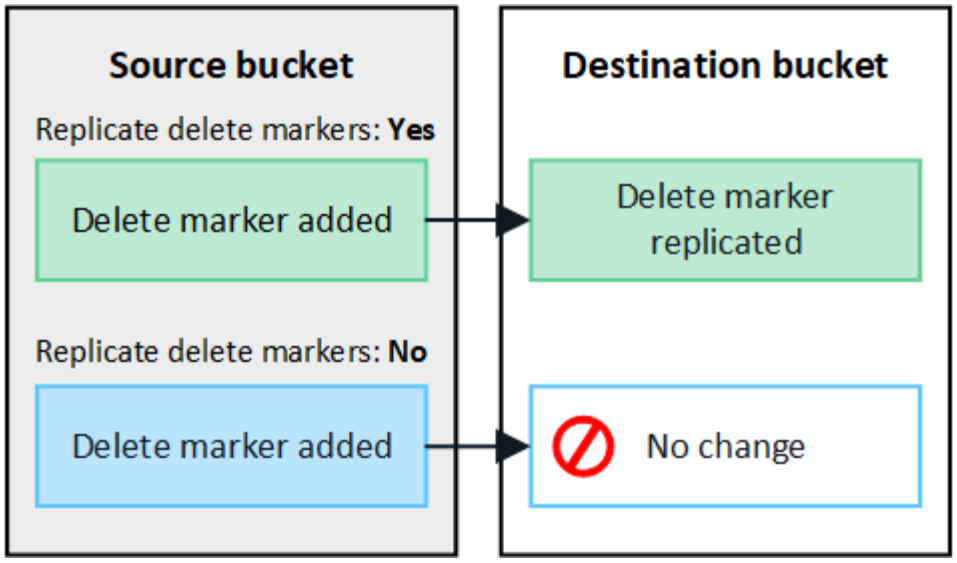
   c. 在*管理对象设置*选项卡上，选择*启用对象版本控制*。
   d. 如果您的StorageGRID系统启用了 S3 对象锁定，请参阅"使用 S3 对象锁进行跨网格复制"。
   e. 选择 * 创建存储分段 * 。
   f. 选择 * 完成 * 。
2. 重复这些步骤，在网格联合连接中的另一个网格上为同一租户帐户创建存储桶。

   根据需要、每个存储分段可以使用不同的区域。

启用跨网格复制

步骤

1. 从要复制其对象的网格开始，启用"跨网格单向复制"：
   a. 登录到存储分段的租户帐户。
   b. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
   c. 从表中选择存储分段名称以访问存储分段详细信息页面。
   d. 选择*跨网格复制*选项卡。
   e. 选择*Enable*，然后查看要求列表。
   f. 如果满足所有要求、请选择要使用的网格联合连接。
   g. (可选)更改*复制删除标记*的设置，以确定S3客户端向不包含版本ID的源网格发出删除请求时目标网格上会发生什么情况：
      - **Yes**(默认)：将删除标记添加到源存储分段并复制到目标存储分段。
      - 否：删除标记已添加到源存储桶，但未复制到目标存储桶。



如果删除请求包含版本 ID，则该对象版本将从源存储桶中永久删除。 StorageGRID不会复制包含版本 ID 的删除请求，因此相同的对象版本不会从目标中删除。

参考"什么是跨网格复制"了解详情。

a. (可选)更改*跨网格复制*审核类别的设置以管理审核消息的数量：
   - 错误(默认)：审核输出中仅包含失败的跨网格复制请求。
   - 正常：包括所有跨网格复制请求，这会显著增加审核输出的量。

b. 选择*启用并测试*。

   片刻之后，会出现一条成功消息。添加到此存储桶的对象现在会自动复制到另一个网格。 *跨网格复制*在存储桶详细信息页面上显示为已启用的功能。

2. (可选)转至另一网格和上的相应"在两个方向上启用跨网格复制"存储分段。

测试网格之间的复制

如果为存储分段启用了跨网格复制、则可能需要验证连接和跨网格复制是否正常工作、以及源存储分段和目标存储分段是否仍满足所有要求(例如、版本控制仍处于启用状态)。

开始之前

- 您正在使用"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。

步骤

1. 登录到存储分段的租户帐户。
2. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
3. 从表中选择存储分段名称以访问存储分段详细信息页面。
4. 选择*跨网格复制*选项卡。
5. 选择 * 测试连接 * 。

如果连接正常，则会出现成功横幅。否则，会出现一条错误消息，您和网格管理员可以使用它来解决问题。有关详细信息，请参阅"对网格联合错误进行故障排除"。

6. 如果跨网格复制配置为双向进行，请转到另一网格上的相应分段，然后选择*测试连接*，以验证跨网格复制是否在另一个方向工作。

禁用跨网格复制

如果不再需要将对象复制到另一个网格、则可以永久停止跨网格复制。

禁用跨网格复制之前、请注意以下事项：

- 禁用跨网格复制不会删除任何已在网格之间复制的对象。例如， `my-bucket`网格 1 上已复制到 `my-bucket` 如果您禁用该存储桶的跨网格复制，则网格 2 上的数据不会被删除。如果要删除这些对象，则必须手动将其删除。
- 如果为每个分段启用了跨网格复制(即、如果是双向复制)、则可以为其中一个分段或这两个分段禁用跨网格复制。例如、您可能希望禁用将对象从网格1复制到网格 `my-bucket`2、同时继续将对象从 `my-bucket`网格2复制 `my-bucket`到网格 `my-bucket`1。
- 您必须先禁用跨网格复制，然后才能删除租户使用网格联合连接的权限。请参阅"管理允许的租户" 。

开始之前

- 您正在使用"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。

步骤

1. 从不再需要复制对象的网格开始、停止对分段的跨网格复制：
   a. 登录到存储分段的租户帐户。
   b. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
   c. 从表中选择存储分段名称以访问存储分段详细信息页面。
   d. 选择*跨网格复制*选项卡。
   e. 选择*禁用复制*。
   f. 如果您确定要禁用此存储桶的跨网格复制，请在文本框中键入*是*，然后选择*禁用*。

      片刻后、将显示一条成功消息。添加到此存储分段的新对象无法再自动复制到其他网格。*跨网格复制*不再显示为"分段"页面上的"已启用"功能。

2. 如果跨网格复制配置为双向进行、请转到另一个网格上的相应存储分段、并停止另一个方向的跨网格复制。

在 **StorageGRID** 中查看网格联合连接

如果您的租户帐户具有*使用网格联合连接*权限、则可以查看允许的连接。

开始之前

- 租户帐户具有*使用网格联合连接*权限。
- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。

步骤

1. 选择*存储(S3)>*网格联合连接。

   此时将显示"网格联合连接"页面、其中包含一个表、其中汇总了以下信息：

列	说明
连接名称	此租户有权使用的网格联盟连接。
具有跨网格复制的存储分段	对于每个网格联合连接、是指启用了跨网格复制的租户分段。添加到这些分段的对象将复制到连接中的其他网格。
上次错误	对于每个网格联合连接、在将数据复制到另一个网格时发生的最新错误(如果有)。请参阅。 清除上一个错误

2. (可选)为选择存储分段名称"查看存储分段详细信息"。

清除上一个错误

由于以下原因之一，“上次错误”列中可能会出现错误：

- 未找到源对象版本。
- 未找到源存储分段。
- 已删除此目标存储分段。
- 目标存储分段已由其他帐户重新创建。
- 目标存储分段已暂停版本控制。
- 目标存储分段已由同一帐户重新创建、但现在已取消版本控制。

此列仅显示上次发生的跨网格复制错误；不会显示先前可能发生的错误。

步骤

1. 如果*last error*列中显示消息，请查看消息文本。

   例如、此错误表示跨网格复制的目标分段处于无效状态、可能是因为版本控制已暂停或启用了S3对象锁定。



2. 执行任何建议的操作。例如、如果在目标存储分段上暂停版本控制以进行跨网格复制、请为此存储分段重新启用版本控制。
3. 从表中选择连接。
4. 选择*清除错误*。
5. 选择*是*以清除消息并更新系统状态。
6. 等待5-6分钟、然后将新对象插入存储分段。确认错误信息不会再次出现。

   要确保清除错误消息、请在消息中的时间戳后至少等待5分钟、然后再输入新对象。

7. 要确定是否有任何对象因存储分段错误而无法复制，请参见"确定并重试失败的复制操作"。

管理组和用户

在 StorageGRID 中使用身份联合

使用身份联合可以加快租户组和用户的设置速度，并允许租户用户使用熟悉的凭据登录到租户帐户。

为租户管理器配置身份联合

如果您希望在另一个系统（例如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server ）中管理租户组和用户，则可以为租户管理器配置身份联合。

开始之前

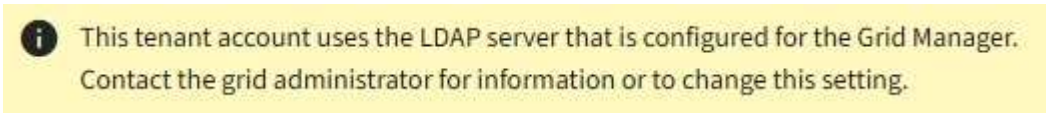
- 您已使用"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作为身份提供者。

  如果您想使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参阅。 配置 OpenLDAP 服务器的准则
- 如果您计划使用传输层安全（ Transport Layer Security ， TLS ）与 LDAP 服务器进行通信，则身份提供程序必须使用 TLS 1.2 或 1.3 。请参阅。 "支持传出 TLS 连接的密码"

关于此任务

是否可以为租户配置身份联合服务取决于租户帐户的设置方式。您的租户可能会共享为网格管理器配置的身份联合服务。如果在访问"身份联合"页面时看到此消息、则无法为此租户配置单独的联合身份源。

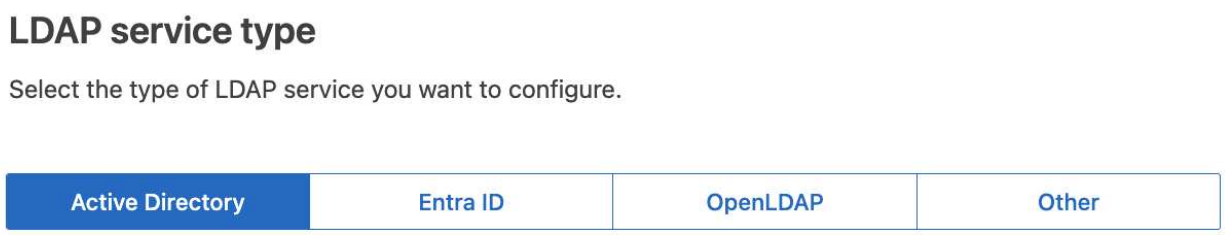


进入配置

在配置"标识联盟"时、您可以提供StorageGRID 连接到LDAP服务所需的值。

步骤

1. 选择*访问管理* > 身份联合。
2. 选择 * 启用身份联合 * 。
3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - 用户唯一名称：包含 LDAP 用户唯一标识符的属性名称。此属性相当于 `sAMAccountName`对于 Active Directory 和 `uid`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `uid。
   - 用户 **UUID**：包含 LDAP 用户的永久唯一标识符的属性名称。此属性相当于 `objectGUID`对于 Active Directory 和 `entryUUID`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `nsuniqueid。每个用户的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数，其中连字符将被忽略。
   - 组唯一名称：包含 LDAP 组唯一标识符的属性的名称。此属性相当于 `sAMAccountName`对于 Active Directory 和 `cn`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `cn。
   - 组 **UUID**：包含 LDAP 组的永久唯一标识符的属性的名称。此属性相当于 `objectGUID`对于 Active Directory 和 `entryUUID`对于 OpenLDAP。如果您正在配置 Oracle Directory Server，请输入 `nsuniqueid。每个组的指定属性的值必须是 16 字节或字符串格式的 32 位十六进制数，其中连字符将被忽略。
5. 对于所有 LDAP 服务类型，请在配置 LDAP 服务器部分中输入所需的 LDAP 服务器和网络连接信息。
   - * 主机名 * ： LDAP 服务器的完全限定域名（ FQDN ）或 IP 地址。
   - * 端口 * ：用于连接到 LDAP 服务器的端口。

     STARTTLS 的默认端口为 389 ， LDAPS 的默认端口为 636 。但是，只要防火墙配置正确，您就可以使用任何端口。

   - * 用户名 * ：要连接到 LDAP 服务器的用户的可分辨名称（ DN ）的完整路径。

     对于 Active Directory ，您还可以指定低级别的登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

     - `sAMAccountName`或 `uid

- `objectGUID` `entryUUID`或 `nsuniqueid`
- `cn`
- `memberOf`或 `isMemberOf`
- **Active Directory**： `objectSid`、 `primaryGroupID`、 `userAccountControl`和 `userPrincipalName`
- 入口**ID**: `accountEnabled`和 `userPrincipalName`

◦ * 密码 * ： 与用户名关联的密码。

> 如果您以后更改密码、则必须在此页面上更新密码。

◦ * 组基本 DN* ： 要搜索组的 LDAP 子树的可分辨名称（ DN ）的完整路径。在 Active Directory 示例（如下）中，可分辨名称相对于基础 DN （ DC=storagegrid ， DC=example ， DC=com ）的所有组均可用作联合组。

> * 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

◦ * 用户基础 DN* ： 要搜索用户的 LDAP 子树的可分辨名称（ DN ）的完整路径。

> 用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

◦ 绑定用户名格式(可选)：如果无法自动确定模式，StorageGRID 应使用默认用户名模式。

建议提供 * 绑定用户名格式 * ，因为如果 StorageGRID 无法绑定到服务帐户，它可以允许用户登录。

输入以下模式之一：

- **UserPrincipalName** 模式（**AD** 和 **Entra ID**）： `[USERNAME]@example.com`
- 下级登录名称模式（**AD** 和 **Entra ID**）： `example\[USERNAME]`
- 可分辨名称模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

  与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   ◦ 使用 **STARTTLS**：使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是 Active Directory 、OpenLDAP 或其他的推荐选项，但 Microsoft Entra ID 不支持此选项。
   ◦ 使用 **LDAPS**：LDAPS（通过 SSL 的 LDAP）选项使用 TLS 建立与 LDAP 服务器的连接。您必须为 Microsoft Entra ID 选择此选项。
   ◦ 不要使用 **TLS**： StorageGRID系统和 LDAP 服务器之间的网络流量将不安全。 Microsoft Entra ID 不支持此选项。

> 如果您的 Active Directory 服务器强制执行 LDAP 签名，则不支持使用 不使用 **TLS** 选项。您必须使用 STARTTLS 或 LDAPS。

7. 如果选择 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。

- * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认网格 CA 证书确保连接安全。
- * 使用自定义 CA 证书 * ： 使用自定义安全证书。

  如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

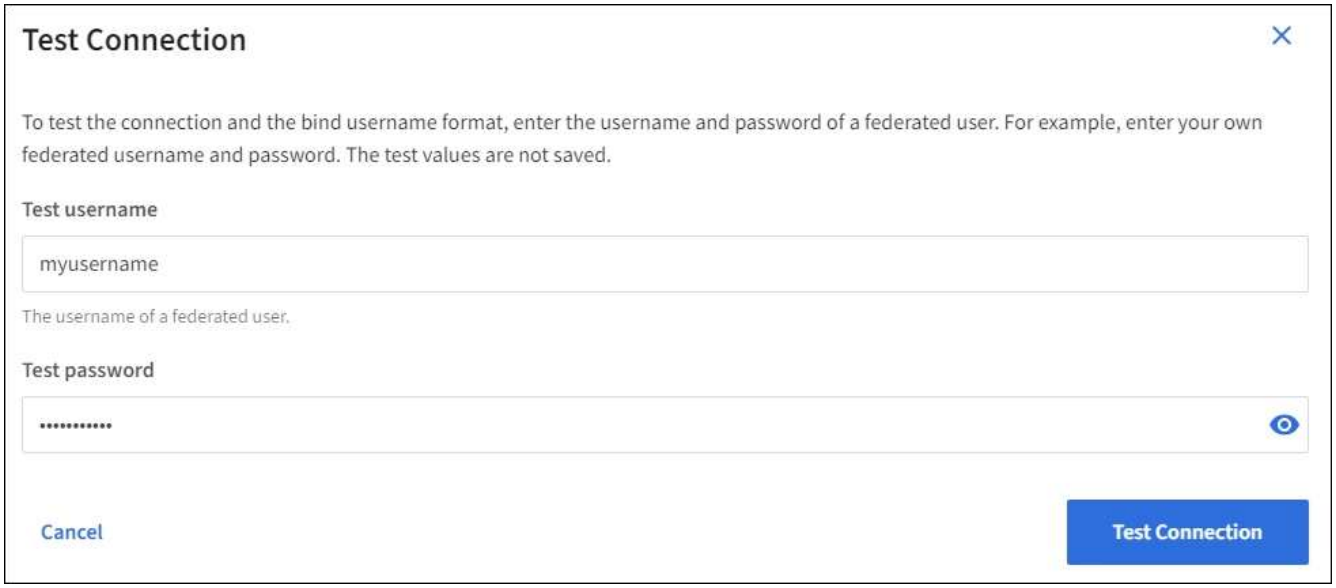
测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

步骤

1. 选择 * 测试连接 * 。
2. 如果您没有提供绑定用户名格式：
   - 如果连接设置有效、则会显示"Test connection sule"(测试连接成功)消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效、则会显示"无法建立测试连接"消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

   例如，输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符、例如@或/。



   - 如果连接设置有效、则会显示"Test connection sule"(测试连接成功)消息。选择 * 保存 * 以保存配置。
   - 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到身份联合页面。

2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以暂时或永久禁用群组和用户的身份联合。当身份联合被禁用时， StorageGRID和身份源之间就没有通信。但是，您配置的任何设置都会保留，以便您将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID系统和身份源之间不会发生同步，并且不会对尚未同步的帐户发出警报。
- 如果单点登录 (SSO) 状态为 已启用 或 沙盒模式，则 启用身份联合 复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 已禁用。看"禁用单点登录" 。

步骤

1. 转到身份联合页面。
2. 取消选中*启用身份联合*复选框。

配置 **OpenLDAP** 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

对于非 Active Directory 或 Microsoft Entra ID 的身份源， StorageGRID不会自动阻止外部禁用的用户访问 S3。要阻止 S3 访问，请删除用户的所有 S3 密钥或从所有组中删除该用户。

memberOf 和 **fint** 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

管理租户组

在 **StorageGRID** 中为 **S3** 租户创建组

您可以通过导入联合组或创建本地组来管理 S3 用户组的权限。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。
- 如果您计划导入联盟组，则已导入"已配置身份联合"，并且已配置的身份源中已存在联盟组。
- 如果您的租户帐户具有*使用网格联合连接*权限，则表示您已查看"同步租户组和用户"的工作流程和注意事项，并且您已登录到租户的源网格。

访问创建组向导

首先、访问创建组向导。

步骤

1. 选择“访问管理”>“组”。
2. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

步骤

1. 选择 * 本地组 * 选项卡以创建本地组，或者选择 * 联合组 * 选项卡以从先前配置的身份源导入组。

   如果为 StorageGRID 系统启用了单点登录（ SSO ），则属于本地组的用户将无法登录到租户管理器，但他们可以根据组权限使用客户端应用程序管理租户的资源。

2. 输入组的名称。
   - * 本地组 * ： 输入显示名称和唯一名称。您可以稍后编辑显示名称。

     如果您的租户帐户具有*使用网格联合连接*权限、并且目标网格上的租户已存在相同的*唯一名称*、则会发生克隆错误。

   - * 联合组 * ： 输入唯一名称。对于Active Directory、唯一名称是与属性关联的名称 `sAMAccountName`。对于OpenLDAP、唯一名称是与属性关联的名称 `uid`。
3. 选择 * 继续 * 。

管理组权限

组权限控制用户可在租户管理器和租户管理API中执行的任务。

步骤

1. 对于*Access mode*，请选择以下选项之一：
   - 读写(默认)：用户可以登录到租户管理器并管理租户配置。
   - * 只读 * ：用户只能查看设置和功能。他们无法在租户管理器或租户管理API中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

   > 如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。

2. 为此组选择一个或多个权限。

   请参阅。 "租户管理权限"

3. 选择 * 继续 * 。

设置**S3**组策略

组策略用于确定用户将拥有哪些S3访问权限。

步骤

1. 选择要用于此组的策略。

组策略	说明
无S3访问	默认。此组中的用户无权访问S3资源、除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
只读访问	此组中的用户对S3资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
完全访问	此组中的用户对S3资源(包括分段)具有完全访问权限。选择此选项后，完全访问组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
勒索软件防护	此示例策略适用场景此租户的所有分段。此组中的用户可以执行常见操作、但无法从启用了对象版本控制的分段中永久删除对象。 具有*管理所有存储分段*权限的租户管理器用户可以覆盖此组策略。将"管理所有分段"权限限制为受信任用户、并在可用时使用多因素身份验证(Multi-FactorAuthentication、MFA)。
自定义	组中的用户将被授予您在文本框中指定的权限。

2. 如果选择 * 自定义 * ，请输入组策略。每个组策略的大小限制为 5 ， 120 字节。您必须输入有效的 JSON 格式字符串。

   有关组策略的详细信息(包括语言语法和示例)，请参见"组策略示例"。

3. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

您可以保存组而不添加用户、也可以选择添加任何已存在的本地用户。

步骤

1. 或者，为此组选择一个或多个本地用户。
2. 选择 * 创建组 * 和 * 完成 * 。

   您创建的组将显示在组列表中。

   如果您的租户帐户具有 **Use grid federation connection** 权限，并且您在租户的源网格上，则新组将同步到租户的目标网格。**Succeeded** 在组的详细信息页面的"概览"部分显示为同步状态。

StorageGRID 租户管理权限

在创建租户组之前，请考虑要分配给该组的权限。租户管理权限用于确定用户可以使用租户管理器或租户管理 API 执行的任务。一个用户可以属于一个或多个组。如果用户属于多个组，则权限是累积的。

要登录到租户管理器或使用租户管理 API ，用户必须属于至少具有一个权限的组。所有可以登录的用户均可执行以下任务：

- 查看信息板
- 更改自己的密码（适用于本地用户）

对于所有权限，组的访问模式设置将确定用户是否可以更改设置并执行操作，或者是否只能查看相关设置和功能。

> 如果用户属于多个组，并且任何组设置为只读，则用户将对所有选定设置和功能具有只读访问权限。

您可以为组分配以下权限。

权限	说明	详细信息
root 访问权限	提供对租户管理器和租户管理 API 的完全访问权限。	
管理您自己的S3凭据	允许用户创建和删除自己的 S3 访问密钥。	没有此权限的用户看不到*storage (S3)*>*My S3 access keys*菜单选项。

权限	说明	详细信息
查看所有存储分段	允许用户查看所有存储桶和存储桶配置。	没有“查看所有存储分段”或“管理所有存储分段”权限的用户不会看到“存储分段”菜单选项。 此权限已被“管理所有存储桶”权限取代。它不会影响 S3 客户端或 S3 控制台使用的 S3 存储桶或组策略。
管理所有存储分段	允许用户使用租户管理器和租户管理 API 创建和删除 S3 存储桶并管理租户帐户中所有 S3 存储桶的设置，而无需考虑 S3 存储桶或组策略。	没有“查看所有存储分段”或“管理所有存储分段”权限的用户不会看到“存储分段”菜单选项。 此权限取代了查看所有存储桶的权限。它不会影响 S3 客户端或 S3 控制台使用的 S3 存储桶或组策略。
管理端点	允许用户使用租户管理器或租户管理API创建或编辑平台服务端点、这些端点用作StorageGRID 平台服务的目标。	没有此权限的用户看不到“平台服务端点”菜单选项。
使用S3控制台选项卡	与查看所有存储分段或管理所有存储分段权限结合使用时、用户可以从存储分段详细信息页面上的S3控制台选项卡查看和管理对象。	

管理 **StorageGRID** 租户组

根据需要管理租户组以查看、编辑或复制组等。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。

查看或编辑组

您可以查看和编辑每个组的基本信息和详细信息。

步骤

1. 选择“访问管理”>“组”。
2. 查看"组"页面上提供的信息、其中列出了此租户帐户的所有本地组和联盟组的基本信息。

   如果租户帐户具有*使用网格联合连接*权限、而您正在查看租户源网格上的组：

   - 如果任何组未同步到目标网格上的租户，请按照步骤 重试组同步。
3. 如果要更改组的名称：
   a. 选中组对应的复选框。
   b. 选择 * 操作 * > * 编辑组名称 * 。

c. 输入新名称。

d. 选择*保存更改。*

4. 如果要查看更多详细信息或进行其他编辑、请执行以下操作之一：

   - 选择组名称。
   - 选中组对应的复选框，然后选择*Actions*>*查看组详细信息*。

5. 查看概述部分、其中显示了每个组的以下信息：

   - 显示名称
   - 唯一名称
   - 键入
   - 访问模式
   - 权限
   - S3策略
   - 此组中的用户数
   - 如果租户帐户具有*使用网格联合连接*权限且您正在查看租户源网格上的组、则添加以下字段：
     - 同步状态，成功*或*失败
     - 对于联合组，蓝色横幅表示如果您编辑或删除此组，您的更改将不会同步到其他网格。

6. 根据需要编辑组设置。参考"为 S3 租户创建组"了解有关输入内容的详细信息。

   a. 在概述部分，通过选择名称或编辑图标 来更改显示名称。

   b. 在*组权限*选项卡上，更新权限，然后选择*保存更改*。

   c. 在*组策略*选项卡上，进行任何更改，然后选择*保存更改*。

      根据需要选择不同的 S3 组策略或输入自定义策略的 JSON 字符串。

7. 要将一个或多个现有本地用户添加到组、请执行以下操作：

   a. 选择用户选项卡。



   b. 选择*添加用户*。

   c. 选择要添加的现有用户，然后选择*添加用户*。

      右上角将显示一条成功消息。

8. 要从组中删除本地用户、请执行以下操作：

a. 选择用户选项卡。
b. 选择*删除用户*。
c. 选择要去除的用户，然后选择*Remove Users *。

   右上角将显示一条成功消息。

9. 确认您为每个更改的部分选择了*保存更改*。

重复的组

您可以复制现有组、以更快地创建新组。

> 如果您的租户帐户具有*使用网格联合连接*权限，并且您从租户的源网格复制了一个组，则复制的组将同步到租户的目标网格。

步骤

1. 选择“访问管理”>“组”。
2. 选中要复制的组对应的复选框。
3. 选择 * 操作 * > * 复制组 * 。
4. 看"为 S3 租户创建组"了解有关输入内容的详细信息。
5. 选择 * 创建组 * 。

重试组同步

如果任何组未能同步，则该组的"同步状态"列中将显示"已失败"。表格上方会显示横幅，指示一个或多个组无法同步。

步骤

要重试同步：

1. 在横幅上，选择 **Retry sync**。此操作会重试无法同步的所有组的同步。
2. 要重试同步单个组，请选择组名称。在组详细信息页面上，选择*Retry sync*。
3. 从正在同步的每个组的详细信息页面查看同步操作的状态。

如果重试成功，则每个成功同步的组的"同步状态"列中将显示"Succeeded"，横幅将消失。

有关更多信息，请参见 "同步租户组和用户"。

删除一个或多个组

您可以删除一个或多个组。仅属于已删除组的任何用户将无法再登录到租户管理器或使用租户帐户。

步骤

1. 选择“访问管理”>“组”。
2. 选中要删除的每个组对应的复选框。

3. 选择*Actions*>*Delete group*或*Actions*>*Delete Groups*。

   此时将显示确认对话框。

4. 选择*删除组*或*删除组*。

设置 **AssumeRole**

开始之前

您必须是管理员才能设置 AssumeRole。

关于此任务

要设置 AssumeRole，请创建要假定的目标组（如果该组尚不存在）。编辑该组的 S3 策略以指定假设该组允许的操作。编辑组的 S3 信任策略以指定允许使用 AssumeRole API 承担该组的可信用户。

假设该组创建的临时安全凭证在有限的时间内有效。会话时长为15分钟到12小时，默认会话时长为1小时。当您从组的 S3 信任策略中删除用户时，该用户将无法再承担该组。

步骤

1. 选择“访问管理”>“组”。
2. 选择组名称。
3. 选择“**S3** 信任策略”选项卡。
4. 添加您的 S3 信任策略，包括可以执行 AssumeRole 的用户列表。
5. 选择 * 保存更改 * 。
6. 选择“**S3** 组策略”选项卡。
7. 编辑 S3 策略以仅为该组的 S3 信任策略中添加的受信任用户指定所需的 S3 操作。
8. 选择 * 保存更改 * 。

AssumeRole S3 信任策略示例

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

委托人：

- `"Principal": "*"` 匹配所有人，包括匿名（未签名）请求
- `"Principal": { "AWS": "*" }` 匹配任何经过身份验证的身份或用户（与匿名请求不匹配）
- 仅适用于存储桶策略
- 主体是被授予或拒绝权限的帐户/用户

配置完成后，S3 信任策略中列出的用户可以执行 AssumeRole 并接收凭证。最终的权限由组策略、bucket策略、session策略决定。有关更多信息，请参阅"使用访问策略" 。

管理 **StorageGRID** 租户用户

您可以创建本地用户并将其分配给本地组，以确定这些用户可以访问哪些功能。您还可以导入联合用户。租户管理器包括一个名为 *root* 的预定义本地用户。虽然您可以添加和删除本地用户，但无法删除 root 用户。

如果为 StorageGRID 系统启用了单一登录 (SSO)，本地用户将无法登录到 Tenant Manager 或 Tenant Management API，但他们可以根据组权限使用客户端应用程序访问租户的资源。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。
- 如果您的租户帐户具有*使用网格联合连接*权限，则表示您已查看"同步租户组和用户"的工作流程和注意事项，并且您已登录到租户的源网格。

创建本地用户

您可以创建本地用户并将其分配给一个或多个本地组、以控制其访问权限。

不属于任何组的S3用户不具有管理权限或应用了S3组策略。这些用户可能已通过存储分段策略授予 S3 存储分段访问权限。

访问创建用户向导

步骤

1. 选择“访问管理”>“用户”。
2. 选择 * 创建用户 * 。

输入凭据

步骤

1. 对于*输入用户凭据*步骤，请填写以下字段。

字段	说明
全名	此用户的全名、例如、人员的名字和姓氏或应用程序的名称。

字段	说明
用户名	此用户用于登录的名称。用户名必须唯一、并且无法更改。 注意：如果您的租户帐户具有*使用网格联合连接*权限、则如果目标网格上的租户已存在相同的*用户名*、则会发生克隆错误。
密码和确认密码	用户在登录时最初使用的密码。
拒绝访问	选择*是*可防止此用户登录到租户帐户、即使他们可能仍属于一个或多个组也是如此。 例如，选择*Yes*可暂时暂停用户的登录能力。

2. 选择 * 继续 * 。

分配给组

步骤

1. 将用户分配给一个或多个本地组、以确定他们可以执行哪些任务。

   将用户分配到组是可选的。如果您愿意、可以在创建或编辑组时选择用户。

   不属于任何组的用户将无管理权限。权限是累积的。用户将对其所属的所有组拥有所有权限。请参阅。 "租户管理权限"

2. 选择 * 创建用户 * 。

   如果您的租户帐户具有*使用网格联合连接*权限，并且您在租户的源网格上，则新的本地用户将同步到租户的目标网格。**Succeeded** 在用户详细信息页面的"概览"部分显示为 **Sync status**。

3. 选择*完成*返回用户页。

查看或编辑本地用户

步骤

1. 选择“访问管理”>“用户”。
2. 查看"用户"页面上提供的信息、其中列出了此租户帐户的所有本地和联盟用户的基本信息。
3. 如果要更改用户的全名：
   a. 选中用户对应的复选框。
   b. 选择 * 操作 * > * 编辑全名 * 。
   c. 输入新名称。
   d. 选择*保存更改。*
4. 如果要查看更多详细信息或进行其他编辑、请执行以下操作之一：
   - 选择用户名。

- 选中用户对应的复选框，然后选择*Actions*>*查看用户详细信息*。

5. 查看概述部分、其中显示了每个用户的以下信息：
   - 全名
   - 用户名
   - 用户类型
   - 拒绝访问
   - 访问模式
   - 组成员资格
6. 根据需要编辑用户设置。有关输入内容的详细信息、请参见创建本地用户。
   a. 在概述部分，通过选择名称或编辑图标 更改全名。

      您不能更改用户名。

   b. 在*密码*选项卡上，更改用户的密码，然后选择*保存更改*。
   c. 在*访问*选项卡上，选择*否*允许用户登录，或选择*是*阻止用户登录。然后，选择*保存更改*。
   d. 在*Access keys*选项卡上，选择*Create key*并按照的说明"正在创建其他用户的S3访问密钥"进行操作。
   e. 在*组*选项卡上，选择*编辑组*将用户添加到组或从组中删除用户。然后，选择*保存更改*。
7. 确认您为每个更改的部分选择了*保存更改*。

导入联合用户

您可以将一个或多个联合用户（最多 100 个用户）直接导入“用户”页面。

步骤

1. 选择“访问管理”>“用户”。
2. 选择*导入联合用户*。
3. 输入一个或多个联合用户的 UUID 或用户名。

   对于多个条目，请在新行上添加每个 UUID 或用户名。

4. 选择*导入*。

   如果将一个或多个用户导入“用户”字段失败，请执行以下步骤：

   a. 展开*未导入的用户*并选择*复制用户*。
   b. 通过选择“上一个”并将复制的用户粘贴到“导入联合用户”对话框中，重新尝试导入。

   关闭“导入联合用户”对话框后，成功导入的用户的联合用户信息将显示在“用户”页面上。

本地用户重复

您可以复制本地用户以更快地创建新用户。

如果您的租户帐户具有*使用网格联合连接*权限，并且您从租户的源网格复制了用户，则复制的用户将同步到租户的目标网格。

步骤

1. 选择“访问管理”>“用户”。
2. 选中要复制的用户对应的复选框。
3. 选择 * 操作 * > * 复制用户 * 。
4. 有关输入内容的详细信息、请参见创建本地用户。
5. 选择 * 创建用户 * 。

重试用户同步

如果任何用户未能同步，则在用户的"同步状态"列中显示"已失败"。表格上方会显示一个横幅，指示一个或多个用户未能同步。

步骤

要重试同步：

1. 在横幅上，选择*重试同步*。此操作将重试同步所有未能同步的用户。
2. 要重试同步单个用户，请选择用户名。在用户详细信息页面上，选择 **Retry sync**。
3. 从您正在同步的每个用户的详细信息页面查看同步操作的状态。

如果重试成功，则成功同步的每个用户的"同步状态"列中都会显示"Succeeded"，横幅将消失。

有关更多信息，请参见 "同步租户组和用户"。

删除一个或多个本地用户

您可以永久删除一个或多个不再需要访问StorageGRID 租户帐户的本地用户。

如果您的租户帐户具有*使用网格联合连接*权限，并且您删除了本地用户，则 StorageGRID 将删除连接中其他网格上的相应用户，除非该用户是目标网格上的联合用户。您必须使用联合身份源删除联合用户。

步骤

1. 选择“访问管理”>“用户”。
2. 选中要删除的每个用户对应的复选框。
3. 选择*Actions*>*Delete user*或*Actions*>*Delete user*。

   此时将显示确认对话框。
4. 选择*删除用户*或*删除用户*。

管理 S3 访问密钥

管理 **StorageGRID** 中的 **S3** 访问密钥

S3 租户帐户的每个用户都必须具有访问密钥，才能在 StorageGRID 系统中存储和检索对象。访问密钥由访问密钥 ID 和机密访问密钥组成。

S3 访问密钥可按如下方式进行管理：

- 拥有*管理您自己的S3凭据*权限的用户可以创建或删除自己的S3访问密钥。
- 拥有* root访问权限*的用户可以管理S3 root帐户和所有其他用户的访问密钥。除非存储分段策略明确禁用，否则根访问密钥可为租户提供对所有存储分段和对象的完全访问权限。

StorageGRID 支持签名版本 2 和签名版本 4 身份验证。除非存储分段策略明确启用，否则不允许跨帐户访问。

在 **StorageGRID** 中创建您自己的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以创建自己的 S3 访问密钥。您必须具有访问密钥才能访问分段和对象。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理您自己的S3凭据或root访问权限"。

关于此任务

您可以创建一个或多个 S3 访问密钥，以便为租户帐户创建和管理存储分段。创建新的访问密钥后，使用新的访问密钥 ID 和机密访问密钥更新应用程序。为了安全起见、请勿创建超出所需数量的密钥、并删除未使用的密钥。如果只有一个密钥，并且该密钥即将到期，请在旧密钥到期之前创建一个新密钥，然后删除旧密钥。

每个密钥可以有特定的到期时间，也可以无到期时间。请遵循以下到期时间准则：

- 为密钥设置到期时间，以将访问权限限制为特定时间段。设置较短的到期时间有助于降低访问密钥 ID 和机密访问密钥意外暴露时的风险。过期密钥将自动删除。
- 如果环境中的安全风险较低、并且您不需要定期创建新密钥、则不必设置密钥的到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。



您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。

   此时将显示 My access keys 页面，其中列出了所有现有访问密钥。

2. 选择 * 创建密钥 * 。
3. 执行以下操作之一：
   - 选择 * 不设置到期时间 * 可创建不会过期的密钥。（默认）
   - 选择 * 设置到期时间 * ，然后设置到期日期和时间。

到期日期最多可以是自当前日期起五年。到期时间至少可以是当前时间之后的一分钟。

4. 选择 * 创建访问密钥 * 。

   此时将显示 Download access key 对话框，其中列出了您的访问密钥 ID 和机密访问密钥。

5. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

   复制或下载此信息之前、请勿关闭此对话框。关闭对话框后、您无法复制或下载密钥。

6. 选择 * 完成 * 。

   新密钥将列在 " 我的访问密钥 " 页面上。

在 StorageGRID 中查看您的 S3 访问密钥

如果您使用的是S3租户，并且拥有"适当的权限"，则可以查看S3访问密钥列表。您可以按到期时间对列表进行排序，以便确定哪些密钥不久将过期。根据需要、您可以"创建新密钥"或"删除密钥"不再使用。

您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您所属的用户组具有管理您自己的S3凭据"权限"。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。
2. 在“我的访问密钥”页面中，按*Expiration time*或*Access key ID*对任何现有访问密钥进行排序。
3. 根据需要创建新密钥或删除不再使用的任何密钥。

   如果在现有密钥到期之前创建新密钥，则可以开始使用新密钥，而不会暂时丢失对帐户中对象的访问权限。

   过期密钥将自动删除。

在 StorageGRID 中删除您自己的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以删除您自己的 S3 访问密钥。删除访问密钥后，无法再使用它访问租户帐户中的对象和分段。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。

- 您拥有"管理您自己的S3凭据权限"。

> 您可以使用租户管理器中为您的帐户显示的访问密钥 ID 和机密访问密钥来访问属于您帐户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从您的帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择 * 存储（ S3 ） * > * 我的访问密钥 * 。
2. 在我的访问密钥页面中、选中要删除的每个访问密钥对应的复选框。
3. 选择 * 删除密钥 * 。
4. 从确认对话框中，选择*Delete key*。

   页面右上角将显示一条确认消息。

在 **StorageGRID** 中创建其他用户的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以为其他用户创建 S3 访问密钥，例如需要访问存储分段和对象的应用程序。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。

关于此任务

您可以为其他用户创建一个或多个 S3 访问密钥，以便他们可以为其租户帐户创建和管理存储分段。创建新的访问密钥后，使用新的访问密钥 ID 和机密访问密钥更新应用程序。为了安全起见、请不要创建超出用户需要的密钥、并删除未使用的密钥。如果只有一个密钥，并且该密钥即将到期，请在旧密钥到期之前创建一个新密钥，然后删除旧密钥。

每个密钥可以有特定的到期时间，也可以无到期时间。请遵循以下到期时间准则：

- 设置密钥的到期时间，以将用户的访问限制为特定时间段。如果访问密钥 ID 和机密访问密钥意外暴露，则设置较短的到期时间有助于降低风险。过期密钥将自动删除。
- 如果环境中的安全风险较低、并且您不需要定期创建新密钥、则不必设置密钥的到期时间。如果您稍后决定创建新密钥，请手动删除旧密钥。

> 可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择“访问管理”>“用户”。
2. 选择要管理其 S3 访问密钥的用户。

   此时将显示用户详细信息页面。

3. 选择 * 访问密钥 * ，然后选择 * 创建密钥 * 。
4. 执行以下操作之一：
   - 选择*不设置到期时间*以创建不到期的密钥。（默认）
   - 选择 * 设置到期时间 * ，然后设置到期日期和时间。

     到期日期最多可以是自当前日期起五年。到期时间至少可以是当前时间之后的一分钟。
5. 选择 * 创建访问密钥 * 。

   此时将显示 Download access key 对话框，其中列出了访问密钥 ID 和机密访问密钥。
6. 将访问密钥 ID 和机密访问密钥复制到安全位置，或者选择 * 下载 .csv * 以保存包含访问密钥 ID 和机密访问密钥的电子表格文件。

   复制或下载此信息之前、请勿关闭此对话框。关闭对话框后、您无法复制或下载密钥。
7. 选择 * 完成 * 。

   新密钥将列在用户详细信息页面的访问密钥选项卡中。

在 **StorageGRID** 中查看其他用户的 **S3** 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以查看其他用户的 S3 访问密钥。您可以按到期时间对列表进行排序，以便确定哪些密钥不久将过期。您可以根据需要创建新密钥并删除不再使用的密钥。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择“访问管理”>“用户”。
2. 从用户页面中、选择要查看其S3访问密钥的用户。
3. 从“用户详细信息”页面中，选择*访问密钥*。
4. 按 * 到期时间 * 或 * 访问密钥 ID* 对密钥进行排序。
5. 根据需要创建新密钥并手动删除不再使用的密钥。

   如果在现有密钥到期之前创建新密钥，则用户可以开始使用新密钥，而不会暂时丢失对帐户中对象的访问权限。

   过期密钥将自动删除。

相关信息

- "创建其他用户的 S3 访问密钥"
- "删除其他用户的 S3 访问密钥"

在 StorageGRID 中删除其他用户的 S3 访问密钥

如果您使用的是 S3 租户，并且您拥有相应的权限，则可以删除其他用户的 S3 访问密钥。删除访问密钥后，无法再使用它访问租户帐户中的对象和分段。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

> 可以使用租户管理器中为用户显示的访问密钥 ID 和机密访问密钥来访问属于用户的 S3 存储分段和对象。因此，请像使用密码一样保护访问密钥。定期轮换访问密钥，从帐户中删除任何未使用的密钥，并且切勿与其他用户共享这些密钥。

步骤

1. 选择“访问管理”>“用户”。
2. 从用户页面中、选择要管理其S3访问密钥的用户。
3. 在“用户详细信息”页面中，选择*访问密钥*，然后选中要删除的每个访问密钥对应的复选框。
4. 选择 * 操作 * > * 删除选定密钥 * 。
5. 从确认对话框中，选择*Delete key*。

   页面右上角将显示一条确认消息。

管理 S3 存储分段

创建 StorageGRID S3 存储桶

您可以使用租户管理器为对象数据创建 S3 分段。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有root访问权限或管理所有存储分段的用户组"权限"。这些权限将覆盖组或存储分段策略中的权限设置。

> 设置或修改存储桶或对象的 S3 对象锁定属性的权限可以通过以下方式授予"存储分段策略或组策略"。

- 如果您计划为存储分段启用S3对象锁定、则网格管理员已为StorageGRID 系统启用全局S3对象锁定设置、并且您已查看S3对象锁定分段和对象的要求。
- 如果多个租户每个都有多达 5,000 个存储桶，则网格中的每个存储节点至少有 64 GB 的 RAM。

StorageGRID 系统为每个 S3 租户帐户最多支持 20,000 个存储桶。每个网格最多可包含 100,000 个存储桶，包括"分支桶"。还有一个限制"分支铲斗深度"。

访问向导

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 选择 * 创建存储分段 * 。

输入详细信息

步骤

1. 输入存储分段的详细信息。

字段	说明
Bucket Name	符合以下规则的存储分段名称： • 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。 • 必须符合 DNS 要求。 • 必须包含至少3个且不超过63个字符。 • 每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。 • 在虚拟托管模式请求中不得包含句点。句点会在验证服务器通配符证书时出现发生原因 问题。 有关详细信息，请参阅 "有关存储分段命名规则的 Amazon Web Services （ AWS ）文档"。 注意:创建存储分段后不能更改存储分段名称。
区域	存储分段的区域。 您的StorageGRID管理员管理可用区域。存储桶的区域会影响应用于对象的数据保护策略。默认情况下，所有存储桶均在 `us-east-1`地区。如果默认区域配置为 `us-east-1`，该其他区域最初是在下拉菜单中选择的。 注意：创建存储分段后无法更改区域。

2. 选择 * 继续 * 。

管理设置

步骤

1. （可选）为存储分段启用对象版本控制。

   如果要将每个对象的每个版本存储在此存储分段中，请启用对象版本控制。然后，您可以根据需要检索对象

的先前版本。

如果出现以下情况，则必须启用对象版本控制：

- 该存储桶将用于跨网格复制。
- 你想创建一个"分支桶"从这个桶里。

2. 如果启用了全局S3对象锁定设置、则可以选择为存储分段启用S3对象锁定、以便使用一次写入、多次读取(WORM)模型存储对象。

   只有在需要将对象保留固定时间(例如为了满足特定法规要求)时、才为存储分段启用S3对象锁定。S3对象锁定是一种永久设置、可帮助您防止在固定时间内或无限期删除或覆盖对象。

   > 为存储分段启用S3对象锁定设置后、便无法将其禁用。具有正确权限的任何人都可以向此存储分段添加无法更改的对象。您可能无法删除这些对象或存储分段本身。

   如果为存储分段启用 S3 对象锁定，则会自动启用存储分段版本控制。

3. 如果选择了*启用S3对象锁定*，则可以选择为此存储分段启用*默认保留*。

   > 网格管理员必须授予您访问的权限"使用S3对象锁定的特定功能"。

   启用*默认保留*后，添加到存储分段的新对象将自动受到保护，不会被删除或覆盖。*默认保留*设置不适用于具有自己保留期限的对象。

   a. 如果启用了*默认保留*，请为存储分段指定*默认保留模式*。

默认保留模式	说明
监管	• 具有权限的用户 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`请求标头绕过保留设置。 • 这些用户可以在达到保留截止日期之前删除对象版本。 • 这些用户可以增加、减少或删除对象的保留截止日期。
合规性	• 在达到保留截止日期之前、无法删除此对象。 • 对象的保留截止日期可以增加、但不能减少。 • 在达到该日期之前、无法删除对象的保留截止日期。 注意：网格管理员必须允许您使用兼容模式。

   b. 如果启用了*默认保留*，请指定存储分段的*默认保留期限*。

      *默认保留期限*表示添加到此存储分段的新对象应保留多长时间、从其被插入开始。指定一个小于或等于网格管理员设置的租户最长保留期限的值。

网格管理员创建租户时会设置一个_maximum _保留期限、该保留期限的值可以介于1天到100年之间。如果设置了_default_保留期限、则该保留期限不能超过为最长保留期限设置的值。如果需要、请让网格管理员增加或减少最长保留期限。

4. 可选地，选择*启用容量限制*，输入一个值，然后选择容量单位。

   容量限制是指可用于此存储分段对象的最大容量。此值表示逻辑数量(对象大小)、而不是物理数量(磁盘上的大小)。

   如果未设置限制、则此存储分段的容量为无限制。有关详细信息、请参见 "容量限制使用量" 。

5. 可选地，选择*启用对象计数限制*。

   对象数量限制是此存储桶可以包含的最大对象数量。该值代表逻辑数量（对象计数）。如果没有设置限制，则对象数量不受限制。

6. 选择 * 创建存储分段 * 。

   此时将创建存储分段并将其添加到 " 存储分段 " 页面上的表中。

7. (可选)选择*转至存储分段详细信息页面*"查看存储分段详细信息"并执行其他配置。

您还可以"创建分支存储桶"根据需要。

在 **StorageGRID** 中查看 **S3** 存储桶详细信息

您可以查看租户帐户中的存储分段。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限、管理所有分段权限或查看所有分段权限"。这些权限会覆盖组或存储分段策略中的权限设置。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

   此时将显示"分段"页面。

2. 查看每个存储分段的摘要表。

   您可以根据需要按任何列对信息进行排序，也可以在列表中向前和向后翻页。

   > 显示的对象计数、已用空间和使用量值均为估计值。这些估计值受载入时间，网络连接和节点状态的影响。如果分段启用了版本控制，则删除的对象版本将包含在对象计数中。

   名称
   存储分段的唯一名称、无法更改。

   已启用的功能
   为存储分段启用的功能列表。

   S3 对象锁定
   是否为存储分段启用S3对象锁定。

只有在为网格启用了S3对象锁定时、才会显示此列。此列还会显示任何旧版合规存储分段的信息。

区域

无法更改的存储分段区域。默认情况下、此列处于隐藏状态。

对象计数

此分段中的对象数。如果分段启用了版本控制、则此值将包含非当前对象版本。

添加或删除对象时、此值可能不会立即更新。

已用空间

分段中所有对象的逻辑大小。逻辑大小不包括复制的或经过纠删编码的副本或对象元数据所需的实际空间。

此值可能需要长达10分钟才能更新。

使用情况

存储分段容量限制的已用百分比(如果已设置)。

此使用量值基于内部估计值、在某些情况下可能会超过此值。例如、StorageGRID会在租户开始上传对象时检查容量限制(如果已设置)、如果租户已超过容量限制、则会拒绝向此存储分段载入新内容。但是、在确定是否已超过容量限制时、StorageGRID不会考虑当前上传的大小。如果删除了对象、则可能会暂时阻止租户将新对象上传到此存储分段、直到重新计算容量限制使用量为止。计算可能需要10分钟或更长时间。

此值表示存储对象及其元数据所需的逻辑大小、而不是物理大小。

容量

如果设置、则表示存储分段的容量限制。

创建日期

创建存储分段的日期和时间。默认情况下、此列处于隐藏状态。

3. 要查看特定存储分段的详细信息、请从表中选择存储分段名称。
   a. 查看网页顶部的摘要信息以确认存储分段的详细信息、例如区域和对象计数。
   b. 查看容量限制使用情况和对象数量限制使用情况条。如果使用率达到或接近 100%，请考虑增加限制或删除一些对象。
   c. 根据需要选择*删除存储分段中的对象*和*删除存储分段*。

> 请密切注意选择其中每个选项时显示的注意事项。有关详细信息、请参见：
>
> - "删除存储分段中的所有对象"
> - "删除存储分段"(存储分段必须为空)

   d. 根据需要查看或更改每个选项卡中存储分段的设置。
      - **S3**控制台：查看存储分段的对象。有关详细信息，请参阅 "使用S3控制台"。
      - 存储分段选项：查看或更改选项设置。创建存储分段后、无法更改某些设置、例如S3对象锁定。

        - "管理存储分段一致性"
        - "上次访问时间更新"
        - "Capacity limit"
        - "对象数量限制"
        - "对象版本控制"
        - "S3 对象锁定"
        - "默认存储分段保留"
        - "管理跨网格复制"(如果允许租户使用)
    - 平台服务："管理平台服务"(如果租户允许)
    - 存储分段访问：查看或更改选项设置。您必须具有特定的访问权限。
        - 配置"存储桶和对象的 CORS"因此其他域中的 Web 应用程序可以访问该存储桶和存储桶中的对象。
        - "控制用户访问"S3存储分段和该存储分段中的对象。
    - 分支：查看存储桶的分支存储桶列表。"创建新的分支存储桶或管理分支存储桶" 。

了解 **StorageGRID** 分支存储桶

分支存储桶提供对存储桶中在特定时间存在的对象的访问。

您可以从现有存储桶创建分支存储桶。创建分支存储桶后，创建该存储桶的原始存储桶称为_基本存储桶_。此外，您可以从另一个分支存储桶创建一个分支存储桶。

分支存储桶提供对受保护数据的访问，但不作为备份。要继续保护数据，请在基本存储桶上使用这些功能：

- "S3 对象锁定"
- "跨网格复制"用于基础桶
- "存储桶策略"用于版本化存储桶，以清理旧对象版本

请注意分支桶的以下特征：

- 您可以使用以下方式访问分支存储桶中的对象"S3 控制台下载对象"。
- 当客户端访问分支存储桶中的对象时，该分支存储桶的"访问策略"，而不是基本存储桶的策略，决定是否允许或拒绝访问。
- 在基础存储桶中创建的对象是根据"ILM 规则"适用于底部桶。根据 ILM 规则如何应用于分支存储桶来评估在分支存储桶中创建的对象。
- 分支存储桶不支持跨网格复制。
- 分支存储桶不支持平台服务。

分支存储桶使用示例

- 您可以使用分支存储桶来删除损坏的对象，方法是从损坏发生之前的时间点创建一个分支存储桶，然后将应用程序指向该分支存储桶而不是包含损坏对象的基本存储桶。

- 您正在将数据保存在版本控制的存储桶中。存在一个意外的漏洞，导致许多不需要的对象在时间_T_之后被摄取。您可以为之前时间值 *T* 创建一个分支存储桶，并将客户端操作重定向到该分支存储桶。然后，只有早于时间 *T* 摄取的对象才会暴露给客户端。
- 您正在将数据保存在版本化的存储桶中。存在一个意外漏洞，导致许多不需要的对象在 *T1* 和 *T2* 之间被摄取。您可以为 *Exclude* 时间值 *T1* 和 *T2* 创建分支存储桶，并将客户端操作重定向到该分支存储桶。然后，只有在 *T1* 之前和 *T2* 之后摄取的对象才会向客户端公开。

对分支存储桶中的对象进行操作

- 对分支存储桶执行 PUT 对象操作会在分支中创建一个对象。
- 对分支存储桶执行 GET 对象操作将从分支中检索对象。如果分支存储桶中不存在该对象，则从基本存储桶中检索该对象。
- 分支存储桶中的对象删除如下：

操作	目标	结果	基本存储桶中的对象可见性	分支存储桶中的对象可见性
删除没有版本 ID 的	基础桶	仅为基本存储桶创建删除标记	HEAD/GET 返回对象不存在，但特定版本仍可访问	HEAD/GET 返回对象存在，且特定版本仍可访问 删除标记将在分支存储桶之后创建 `beforeTime`。
根据版本 ID 删除	基础桶	删除了基本存储桶和分支存储桶的特定对象版本	HEAD/GET 返回对象版本不存在	HEAD/GET 返回对象版本不存在
删除没有版本 ID 的	分支桶	仅为分支存储桶创建删除标记	HEAD/GET 返回对象（基本 bucket 对象不受影响）	HEAD/GET 返回对象不存在
根据版本 ID 删除	分支桶	仅删除分支存储桶的特定对象版本	HEAD/GET 返回特定对象版本（基本存储桶对象不受影响）	HEAD/GET 返回对象版本不存在

另请参阅"如何删除受版本控制的 S3 对象"。

管理 **StorageGRID** 分支存储桶

使用租户管理器创建和查看分支存储桶的详细信息。

开始之前

- 您已使用"支持的 Web 浏览器"。
- 您属于具有 Root 访问权限的用户组，或者"管理所有存储分段权限"。这些权限将覆盖组或存储桶策略中的权限设置。
- 您要从中创建分支的基本存储桶具有"已启用版本控制"。

- 您是基本存储桶的所有者。

关于此任务

请注意分支存储桶的以下信息：

分支存储桶深度限制

一个分支桶最多可包含 20 个基本桶。随着分支桶深度的增加，S3 访问延迟可能会增加，尤其是对于 ListObjectVersions 调用。

- 如果从作为常规存储桶的基本存储桶（最初创建为基本存储桶的存储桶）创建分支存储桶，则新的分支存储桶具有一个基本存储桶。
- 如果基本桶本身就是一个分支桶，则新的分支桶将继承该分支桶的所有基本桶。用户仅直接指定一个基本桶；继承的基本桶是隐含的。
- 基本桶（显式和隐式）的总数不能超过 20 个。

  例如，假定 Bucket **A** 是启用了版本控制的常规 Bucket：

  - 从 **A** 创建的分支桶 **B** 有一个基本桶：**A**。
  - 从 **B** 创建的分支桶 **C** 有两个基本桶：**B**（显式）和 **A**（隐式）。
  - 从 **C** 创建的分支桶 **D** 有三个基本桶：**C**（显式）、**B**（隐式）和 **A**（隐式）。
  - 此模式最多可延续至 20 个基本桶的最大深度。

S3 对象锁定权限

可以通过 "存储分段策略或组策略" 授予设置存储桶或对象的 S3 Object Lock 属性的权限。

暂停版本控制

如果您暂停对基本存储桶进行版本控制，则基本存储桶的内容将不再在其分支存储桶中可见。

配置并创建分支存储桶后，您无法更改该配置。

创建分支存储桶

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 选择要从中创建分支的存储桶（“基本存储桶”）。
3. 在存储桶详情页面，选择*分支* > 创建分支存储桶。

   如果基本存储桶未启用版本控制，则“创建分支存储桶”按钮将被禁用。

输入详细信息

步骤

1. 输入分支存储桶的详细信息。

字段	说明
分支存储桶名称	符合以下规则的分支存储桶的名称： • 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。 • 必须符合 DNS 要求。 • 必须包含至少3个且不超过63个字符。 • 每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。 • 在虚拟托管模式请求中不得包含句点。句点会在验证服务器通配符证书时出现发生原因 问题。 有关详细信息，请参见 "有关存储分段命名规则的 Amazon Web Services （ AWS ）文档"。 注意：创建分支存储桶后，您无法更改名称。
区域（无法修改分支存储桶）	分支存储桶的区域。 分支存储桶的区域必须与基本存储桶的区域匹配，因此该字段对于分支存储桶是禁用的。
分支桶类型	• 读写：您可以在分支存储桶中添加或删除对象或对象版本。 • 只读：您不能修改分支存储桶中的对象。 注意：仅当分支存储桶为空时，您才可以将分支存储桶类型设置为只读。如果现有分支存储桶的类型设置为读写，而您尚未写入，则可以将类型更改为只读。

2. 选择 * 继续 * 。

时间筛选器

选择时间范围以包括基本桶中的对象版本。对于任何时间筛选器，请选择以下范围内的任何日期：

- 最小日期：2010年1月1日（UTC）
- 最大日期：从今天的日期起五年（UTC）

执行前
: 分支存储桶提供对早于 *Before* time 创建的对象版本的访问。

执行后
: 分支存储桶提供对在 *After* 时间之后创建的对象版本的访问。

介于
: 分支存储桶提供对 *From* 和 *To* 时间之间创建的对象版本的访问。

排除

分支存储桶不提供对_Exclude from_和_Exclude to_时间之间创建的对象版本的访问权限。

管理对象设置（可选）

分支存储桶的对象设置不会影响基础存储桶中的对象版本。

步骤

1. 如果启用了全局 S3 对象锁定设置，则可以选择为分支存储桶启用 S3 对象锁定。要启用 S3 对象锁，分支存储桶必须是读写存储桶。

   仅当您需要将对象保留一段固定的时间（例如，为了满足某些监管要求）时，才为分支存储桶启用 S3 对象锁定。 S3 对象锁定是一种永久性设置，可帮助您防止对象在固定时间内或无限期内被删除或覆盖。

   > 一旦为存储桶启用 S3 对象锁定设置，就无法禁用它。任何拥有正确权限的人都可以将对象添加到无法更改的分支存储桶中。您可能无法删除这些对象或分支存储桶本身。

2. 如果您选择了“启用 S3 对象锁定”，则可以选择为分支存储桶启用“默认保留”。

   > 网格管理员必须授予您访问的权限"使用S3对象锁定的特定功能"。

   当启用*默认保留*时，添加到分支存储桶的新对象将自动受到保护，免遭删除或覆盖。 *默认保留*设置不适用于具有自己的保留期的对象。

   a. 如果启用了*默认保留*，请为分支存储桶指定*默认保留模式*。

默认保留模式	说明
监管	• 具有权限的用户 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`请求标头绕过保留设置。 • 这些用户可以在达到保留截止日期之前删除对象版本。 • 这些用户可以增加、减少或删除对象的保留截止日期。
合规性	• 在达到保留截止日期之前、无法删除此对象。 • 对象的保留截止日期可以增加、但不能减少。 • 在达到该日期之前、无法删除对象的保留截止日期。 注意：网格管理员必须允许您使用兼容模式。

   b. 如果启用了*默认保留*，请指定分支存储桶的*默认保留期*。

      *默认保留期*表示从提取新对象开始，添加到分支存储桶中的新对象应保留多长时间。指定一个小于或等于网格管理员设置的租户最大保留期的值。

网格管理员创建租户时会设置一个_maximum _保留期限、该保留期限的值可以介于1天到100年之间。如果设置了_default_保留期限、则该保留期限不能超过为最长保留期限设置的值。如果需要、请让网格管理员增

加或减少最长保留期限。

3. 或者，选择“启用容量限制”。

   容量限制是分支桶可用的最大容量。该值代表逻辑量（对象大小），而不是物理量（磁盘上的大小）。

   如果没有设置限制，则分支桶的容量是无限的。请参阅"容量限制使用量"了解更多信息。

   > 此设置仅适用于直接提取到分支存储桶中的对象，而不适用于通过分支存储桶从基础存储桶中可见的对象。

4. 或者，选择“启用对象计数限制”。

   对象计数限制是分支存储桶可以包含的最大对象数。该值代表逻辑数量（对象计数）。如果没有设置限制，则对象数量不受限制。

   > 此设置仅适用于直接提取到分支存储桶中的对象，而不适用于通过分支存储桶从基础存储桶中可见的对象。

5. 选择 * 创建存储分段 * 。

   分支存储桶已创建并添加到“存储桶”页面上的表中。

6. 或者，选择“转到存储桶详细信息页面”"查看分支存储桶详细信息"并执行额外的配置。

   在 Bucket 详情页面，对于只读 Bucket，一些与修改对象相关的配置选项被禁用。

将 **ILM** 策略标记应用于 **StorageGRID** 存储区

根据对象存储要求选择要应用于存储分段的ILM策略标记。

ILM策略控制对象数据的存储位置以及是否在特定时间段后将其删除。网格管理员创建ILM策略、并在使用多个活动策略时将其分配给ILM策略标记。

> 避免频繁重新分配存储分段的策略标记。否则、可能会发生性能问题。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限、管理所有分段权限或查看所有分段权限"。这些权限会覆盖组或存储分段策略中的权限设置。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

   此时将显示"分段"页面。您可以根据需要按任何列对信息进行排序，也可以在列表中向前和向后翻页。

2. 选择要将ILM策略标记分配到的存储分段的名称。

   您还可以更改已分配标记的存储分段的ILM策略标记分配。

显示的对象计数和已用空间值为估计值。这些估计值受载入时间，网络连接和节点状态的影响。如果分段启用了版本控制，则删除的对象版本将包含在对象计数中。

3. 在存储分段选项选项卡中、展开ILM策略标记可展开框。只有当网格管理员启用了自定义策略标记的使用时、才会显示此可风框。
4. 阅读每个策略标记的问题描述以确定应将哪个标记应用于存储分段。

更改存储分段的ILM策略标记将触发存储分段中所有对象的ILM重新评估。如果新策略将对象保留一段有限的时间、则较早的对象将被删除。

5. 选择要分配给存储分段的标记对应的单选按钮。
6. 选择 * 保存更改 * 。此时将使用ILM策略标记名称的密钥和值在此存储分段上设置一个新的S3存储分段标记 `NTAP-SG-ILM-BUCKET-TAG`。

确保S3应用程序不会意外覆盖或删除新存储分段标记。如果在向存储分段应用新标记集时省略此标记、则存储分段中的对象将还原为根据默认ILM策略进行评估。

仅使用已验证ILM策略标记的租户管理器或租户管理器API设置和修改ILM策略标记。请勿使用S3 PutBucketTag API或S3 DeleteBucketTag API修改 `NTAP-SG-ILM-BUCKET-TAG`ILM策略标记。

在使用新ILM策略重新评估对象时、更改分配给存储分段的策略标记会暂时影响性能。

管理 **StorageGRID** 存储桶策略

您可以控制用户对S3存储分段以及该存储分段中的对象的访问。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。查看所有存储分段和管理所有存储分段权限仅允许查看。
- 您已确认已满足所需数量的存储节点和站点。如果任何站点中没有两个或更多存储节点、或者某个站点不可用、则可能无法对这些设置进行更改。

步骤

1. 选择*Buckets*，然后选择要管理的存储分段。
2. 在存储分段详细信息页面上、选择*存储分段访问*>*存储分段策略*。
3. 执行以下操作之一：
   - 选中*启用策略*复选框以输入存储分段策略。然后输入有效的JSON格式字符串。

     每个分段策略的大小限制为20、480字节。
   - 通过编辑字符串来修改现有策略。
   - 通过取消选择*Enable policy*来禁用策略。

有关存储分段策略的详细信息(包括语言语法和示例)，请参见"存储分段策略示例"。

管理 **StorageGRID** 存储桶一致性

一致性值可用于指定存储分段设置更改的可用性、并在存储分段中对象的可用性与这些对象在不同存储节点和站点之间的一致性之间实现平衡。您可以将一致性值更改为与默认值不同的值、以便客户端应用程序可以满足其运行需求。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

存储分段一致性准则

分段一致性用于确定影响该S3分段中对象的客户端应用程序的一致性。通常，存储分段应使用*read-after-new-write*一致性。

更改存储分段一致性

如果*read-after-new-write*一致性不符合客户端应用程序的要求，您可以通过设置分段一致性或使用标头来更改一致性 `Consistency-Control`。 `Consistency-Control`标题将覆盖存储分段一致性。

如果更改存储分段的一致性、则只有在更改后被加载的对象才能保证满足修订后的设置。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从*存储分段选项*选项卡中，选择**可选框。
4. 为此存储分段中的对象执行的操作选择一致性。
   - 全部：提供最高级别的一致性。所有节点都会立即接收数据，否则请求将失败。
   - 强-全局：保证所有站点中所有客户端请求的写入后读一致性。
   - 强站点：保证站点内所有客户端请求的写入后读一致性。
   - 读后新写入(默认)：为新对象提供读后写入一致性、并最终为对象更新提供一致性。提供高可用性和数据保护保证。建议用于大多数情况。
   - 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。
5. 选择 * 保存更改 * 。

更改存储分段设置时会发生什么情况

分段具有多个设置、这些设置会影响分段的行为以及这些分段中的对象。

默认情况下，以下存储分段设置使用*强*一致性。如果任何站点中没有两个或更多存储节点、或者某个站点不可用、则对这些设置所做的任何更改可能不可用。

- "后台空分段删除"
- "上次访问时间"
- "分段生命周期"
- "存储分段策略"
- "存储分段标记"
- "存储分段版本控制"
- "S3 对象锁定"
- "存储分段加密"

分段版本控制、S3对象锁定和分段加密的一致性值不能设置为高度一致的值。

以下存储分段设置不会使用较强的一致性、因此更改可用性较高。对这些设置所做的更改可能需要一段时间才能生效。

- "平台服务配置：通知、复制或搜索集成"
- "为存储桶和对象配置StorageGRID CORS"
- 更改存储分段一致性

如果更改存储分段设置时使用的默认一致性不符合客户端应用程序的要求，则可以使用的标题"S3 REST API"或 `force`中的或 `reducedConsistency`选项来更改一致性 `Consistency-Control`"租户管理 API"。

在 **StorageGRID** 中启用或禁用上次访问时间更新

当网格管理员为 StorageGRID 系统创建信息生命周期管理（ ILM ）规则时，他们可以选择指定对象的最后访问时间来确定是否将该对象移动到其他存储位置。如果您使用的是 S3 租户，则可以通过为 S3 存储分段中的对象启用上次访问时间更新来利用此类规则。

这些说明仅适用于至少包含一个使用*上次访问时间*选项作为高级筛选器或参考时间的ILM规则的StorageGRID系统。如果您的 StorageGRID 系统不包含此类规则，则可以忽略这些说明。有关详细信息、请参见。 "在ILM规则中使用上次访问时间"

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。

关于此任务

*上次访问时间*是ILM规则的*参考时间*放置指令的可用选项之一。通过将规则的"参考时间"设置为上次访问时间、网格管理员可以根据上次检索(读取或查看)对象的时间指定将对象放置在某些存储位置。

例如，为了确保最近查看的对象保持在较快的存储上，网格管理员可以创建一个 ILM 规则，指定以下内容：

- 过去一个月检索到的对象应保留在本地存储节点上。
- 过去一个月未检索到的对象应移至异地位置。

默认情况下，对上次访问时间的更新处于禁用状态。如果您的StorageGRID 系统包含使用*上次访问时间*选项的ILM规则、而您希望此选项应用于此存储分段中的对象、则必须为该规则中指定的S3存储分段启用上次访问时间更新。

在检索对象时更新上次访问时间会降低 StorageGRID 性能，尤其是对于小型对象。

上次访问时间更新会影响性能，因为每次检索对象时， StorageGRID 都必须执行以下附加步骤：

- 使用新的时间戳更新对象
- 将对象添加到 ILM 队列，以便根据当前 ILM 规则和策略对其进行重新评估

下表汇总了禁用或启用上次访问时间时应用于存储分段中所有对象的行为。

请求类型	禁用上次访问时间时的行为（默认）		启用上次访问时间时的行为	
	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?	上次访问时间是否已更新?	对象是否已添加到 ILM 评估队列?
发出 HEAD 操作时请求检索对象的元数据	否	否	否	否
请求检索对象，其访问控制列表或其元数据	否	否	是	是
请求更新对象的元数据	是	是	是	是
列出对象或对象版本的请求	否	否	否	否
请求将对象从一个存储分段复制到另一个存储分段	• 否，对于源副本 • 是，对于目标副本	• 否，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本	• 是，对于源副本 • 是，对于目标副本
请求完成多部分上传	是，对于已组装的对象	是，对于已组装的对象	是，对于已组装的对象	是，对于已组装的对象

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

此时将显示存储分段详细信息页面。

3. 从*存储分段选项*选项卡中，选择*上次访问时间更新*可接触框。
4. 启用或禁用上次访问时间更新。
5. 选择 * 保存更改 * 。

更改 **StorageGRID** 中 **S3** 存储桶的对象版本控制

如果您使用的是S3租户、则可以更改S3存储分段的版本控制状态。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。
- 您已确认已满足所需数量的存储节点和站点。如果任何站点中没有两个或更多存储节点、或者某个站点不可用、则可能无法对这些设置进行更改。

关于此任务

您可以为存储分段启用或暂停对象版本控制。为存储分段启用版本控制后、存储分段无法恢复为未受版本控制的状态。但是，您可以暂停存储分段的版本控制。

- Disabled ： 从未启用版本控制
- Enabled ： 已启用版本控制
- suspended ： 先前已启用版本控制并已暂停

有关详细信息，请参见以下内容：

- "对象版本控制"
- "S3 版本对象的 ILM 规则和策略（示例 4 ）"
- "如何删除对象"

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从“存储分段选项”选项卡中，选择“对象版本控制”可选框。
4. 为此存储分段中的对象选择版本控制状态。

   对于用于跨网格复制的存储分段、必须始终启用对象版本控制。如果启用了 S3 对象锁定或原有合规性，则会禁用 * 对象版本控制 * 选项。

选项	说明
启用版本控制	如果要将每个对象的每个版本存储在此存储分段中，请启用对象版本控制。然后，您可以根据需要检索对象的先前版本。 用户修改存储分段中已存在的对象时，这些对象将进行版本控制。
暂停版本控制	如果您不再需要创建新的对象版本，请暂停对象版本控制。您仍然可以检索任何现有对象版本。

5. 选择 * 保存更改 * 。

使用 **S3 Object Lock** 将对象保留在 **StorageGRID** 中

如果存储分段和对象必须符合保留法规要求、则可以使用S3对象锁定。

网格管理员必须授予您使用S3对象锁定特定功能的权限。

什么是 **S3** 对象锁定?

StorageGRID S3 对象锁定功能是一种对象保护解决方案，相当于 Amazon Simple Storage Service （ Amazon S3 ）中的 S3 对象锁定。

当为 StorageGRID 系统启用全局 S3 对象锁定设置时，S3 租户帐户可以创建启用或未启用 S3 对象锁定的存储桶。启用现有存储桶的允许 S3 对象锁定设置后，S3 租户帐户可以为现有存储桶启用 S3 对象锁定。如果存储桶已启用 S3 对象锁定，则需要存储桶版本控制并自动启用。在 S3 租户帐户为新的或现有存储桶启用 S3 对象锁定后，无法禁用它。

*没有S3对象锁定的存储分段*只能包含没有指定保留设置的对象。任何已加热的对象都不具有保留设置。

*具有S3对象锁定*的存储分段可以包含具有和不具有S3客户端应用程序指定的保留设置的对象。已加热的某些对象将具有保留设置。

*配置了S3对象锁定和默认保留的存储分段*可以上传具有指定保留设置的对象以及没有保留设置的新对象。新对象使用默认设置、因为尚未在对象级别配置保留设置。

配置默认保留后、所有新加的对象都会具有保留设置、这一点很有效。没有对象保留设置的现有对象不受影响。

保留模式

StorageGRID S3对象锁定功能支持两种保留模式、可对对象应用不同级别的保护。这些模式相当于Amazon S3保留模式。

- 在合规模式下：
  - 在达到保留截止日期之前、无法删除此对象。
  - 对象的保留截止日期可以增加、但不能减少。
  - 在达到该日期之前、无法删除对象的保留截止日期。
- 在监管模式下：

- 具有特殊权限的用户可以在请求中使用旁路标头来修改某些保留设置。
- 这些用户可以在达到保留截止日期之前删除对象版本。
- 这些用户可以增加、减少或删除对象的保留截止日期。

对象版本的保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以使用S3客户端应用程序为添加到该存储分段的每个对象指定以下保留设置(可选):

- 保留模式：合规性或监管。
- **retain**至日期：如果某个对象版本的retain至日期为未来版本，则可以检索该对象，但不能将其删除。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。合法保留与保留日期无关。

> 如果某个对象处于合法保留状态、则无论其保留模式如何、任何人都无法删除该对象。

要了解有关对象设置的详细信息，请参阅 "使用S3 REST API配置S3对象锁定"。

存储分段的默认保留设置

如果在创建存储分段时启用了S3对象锁定、则用户可以选择为此存储分段指定以下默认设置：

- 默认保留模式：合规或监管。
- 默认保留期限：添加到此存储分段的新对象版本应保留多长时间、从添加之日开始。

默认分段设置仅适用于没有自己的保留设置的新对象。添加或更改这些默认设置时、现有存储分段对象不会受到影响。

请参阅 "创建 S3 存储区。" 和 "更新S3对象锁定默认保留"。

S3对象锁定任务

以下网格管理员和租户用户列表包含使用S3对象锁定功能的高级别任务。

网格管理员

- 为整个StorageGRID系统启用全局S3对象锁定设置。
- 允许用户为现有存储桶启用 S3 对象锁定。
- 确保信息生命周期管理(ILM)策略符合_合规_，即符合"启用了S3对象锁定的分段的要求"。
- 根据需要、允许租户使用合规性作为保留模式。否则、仅允许使用监管模式。
- 根据需要为租户设置最长保留期限。

租户用户

- 查看使用S3对象锁定的存储分段和对象的注意事项。
- 根据需要，联系网格管理员以启用以下设置之一：
  - 全局 S3 对象锁定

- 允许为现有存储桶启用 S3 对象锁定

- 创建启用了S3对象锁定的分段。
- 在现有存储桶上启用 S3 对象锁定。
- (可选)配置存储分段的默认保留设置：
  - 默认保留模式：监管或合规(如果网格管理员允许)。
  - 默认保留期限：必须小于或等于网格管理员设置的最长保留期限。
- 使用S3客户端应用程序添加对象并可选择设置对象专用保留：
  - 保留模式。监管或合规性(如果网格管理员允许)。
  - 保留截止日期：必须小于或等于网格管理员设置的最长保留期限所允许的值。

启用了 **S3** 对象锁定的存储分段的要求

- 如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以使用租户管理器，租户管理 API 或 S3 REST API 创建启用了 S3 对象锁定的分段。
- 为存储分段启用 S3 对象锁定后， StorageGRID 会自动为该存储分段启用版本控制。您不能禁用存储分段的S3对象锁定或暂停版本控制。
- 您也可以使用租户管理器、租户管理API或S3 REST API为每个存储分段指定默认保留模式和保留期限。存储分段的默认保留设置仅适用于添加到存储分段中但没有自己的保留设置的新对象。您可以通过在上传每个对象版本时为其指定保留模式和保留截止日期来覆盖这些默认设置。
- 启用了S3对象锁定的分段支持分段生命周期配置。

启用了 **S3** 对象锁定的分段中的对象的要求

- 要保护对象版本、您可以为存储分段指定默认保留设置、也可以为每个对象版本指定保留设置。可以使用S3客户端应用程序或S3 REST API指定对象级保留设置。
- 保留设置适用于各个对象版本。对象版本可以同时具有保留截止日期和合法保留设置，但不能具有其他设置，或者两者均不具有。为对象指定保留日期或合法保留设置仅保护请求中指定的版本。您可以创建新版本的对象，而先前版本的对象仍保持锁定状态。

启用了 **S3** 对象锁定的存储分段中的对象生命周期

在启用了S3对象锁定的情况下保存在存储分段中的每个对象都会经历以下阶段：

1. * 对象载入 *

   将对象版本添加到启用了S3对象锁定的存储分段时、将按如下所示应用保留设置：

   - 如果为对象指定了保留设置、则会应用对象级别设置。系统将忽略任何默认存储分段设置。
   - 如果没有为对象指定保留设置、则会应用默认存储分段设置(如果存在)。
   - 如果没有为对象或存储分段指定保留设置、则对象不受S3对象锁定保护。

   如果应用了保留设置、则对象和任何S3用户定义的元数据都会受到保护。

2. 对象保留和删除

   StorageGRID 会在指定的保留期限内存储每个受保护对象的多个副本。对象副本的确切数量和类型以及存储

位置由活动ILM策略中的合规规则决定。是否可以在达到保留截止日期之前删除受保护对象取决于其保留模式。

- 如果某个对象处于合法保留状态、则无论其保留模式如何、任何人都无法删除该对象。

是否仍可管理旧版合规存储分段?

S3 对象锁定功能取代了先前 StorageGRID 版本中提供的合规性功能。如果您使用早期版本的 StorageGRID 创建了合规的存储分段，则可以继续管理这些存储分段的设置；但是，您无法再创建新的合规存储分段。有关说明，请参阅https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"^]。

相关信息

了解 "S3 Object Lock 要求"

在 **StorageGRID** 中更新 **S3** 对象锁定默认保留

如果您在创建存储分段时启用了S3对象锁定、则可以编辑存储分段以更改默认保留设置。您可以启用(或禁用)默认保留并设置默认保留模式和保留期限。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。
- 系统会为您的StorageGRID 系统全局启用S3对象锁定、您可以在创建存储分段时启用S3对象锁定。请参阅。 "使用S3对象锁定保留对象"

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
2. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

3. 从*存储分段选项*选项卡中，选择*S3对象锁定*可触摸板。
4. (可选)为此存储分段启用或禁用*默认保留*。

   对此设置所做的更改不会应用于存储分段中已有的对象或可能具有自己保留期限的任何对象。

5. 如果启用了*默认保留*，请为存储分段指定*默认保留模式*。

默认保留模式	说明
监管	• 具有权限的用户 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true`请求标头绕过保留设置。 • 这些用户可以在达到保留截止日期之前删除对象版本。 • 这些用户可以增加、减少或删除对象的保留截止日期。

默认保留模式	说明
合规性	• 在达到保留截止日期之前、无法删除此对象。 • 对象的保留截止日期可以增加、但不能减少。 • 在达到该日期之前、无法删除对象的保留截止日期。 注意：网格管理员必须允许您使用兼容模式。

6. 如果启用了*默认保留*，请指定存储分段的*默认保留期限*。

   *默认保留期限*表示添加到此存储分段的新对象应保留多长时间、从其被插入开始。指定一个小于或等于网格管理员设置的租户最长保留期限的值。

   网格管理员创建租户时会设置一个_maximum _保留期限、该保留期限的值可以介于1天到100年之间。如果设置了_default_保留期限、则该保留期限不能超过为最长保留期限设置的值。如果需要、请让网格管理员增加或减少最长保留期限。

7. 选择 * 保存更改 * 。

在 StorageGRID 中为 S3 存储桶配置 CORS

如果您希望S3存储分段和该存储分段中的对象可供其他域中的Web应用程序访问、则可以为该存储分段配置跨源站资源共享(CORS)。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 对于GET CORS配置请求，您属于具有的用户组"管理所有存储分段或查看所有存储分段权限"。这些权限将覆盖组或存储分段策略中的权限设置。
- 对于Put CORS配置请求，您属于具有的用户组"管理所有存储分段权限"。此权限将覆盖组或存储分段策略中的权限设置。
- 提供对所有CORS配置请求的"root访问权限"访问权限。

关于此任务

跨源资源共享（ CORS ）是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如、假设您使用名为的S3存储分段 `Images`来存储图形。通过为存储分段配置CORS `Images`，您可以允许该存储分段中的图像显示在网站上 `http://www.example.com`。

为存储分段启用CORS

步骤

1. 使用文本编辑器创建所需的XML。此示例显示了用于为 S3 存储分段启用 CORS 的 XML 。具体而言：
   - 允许任何域向存储分段发送GET请求
   - 仅允许 `http://www.example.com`域发送GET、POST和DELETE请求
   - 允许所有请求标头

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

有关CORS配置XML的详细信息，请参见 "Amazon Web Services (AWS)文档：《Amazon Simple Storage Service用户指南》"。

2. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
3. 从表中选择分段名称。

   此时将显示存储分段详细信息页面。

4. 从*存储分段访问*选项卡中，选择*跨源资源共享(CORS)*可接触式。
5. 选中*启用CORS*复选框。
6. 将CORS配置XML粘贴到文本框中。
7. 选择 * 保存更改 * 。

修改CORS设置

步骤

1. 更新文本框中的CORS配置XML，或选择*Clear*重新开始。
2. 选择 * 保存更改 * 。

禁用CORS设置

步骤

1. 清除*启用CORS*复选框。
2. 选择 * 保存更改 * 。

相关信息

"为管理接口配置StorageGRID CORS"

从 **StorageGRID S3** 存储桶中删除对象

您可以使用租户管理器删除一个或多个存储分段中的对象。

注意事项和要求

在执行这些步骤之前、请注意以下事项：

- 删除存储分段中的对象后、StorageGRID 会从StorageGRID 系统中的所有节点和站点中永久删除每个选定存储分段中的所有对象和所有对象版本。StorageGRID 还会删除任何相关的对象元数据。您将无法恢复此信息。
- 根据对象数、对象副本数和并发操作数、删除存储分段中的所有对象可能需要几分钟、几天甚至几周时间。
- 如果存储分段具有"已启用S3对象锁定"，则它可能会在_yrees_状态下保持*Deleting objects: read-only。

> 使用S3对象锁定的存储分段将保持*删除对象：只读*状态、直到达到所有对象的保留日期并删除任何合法保留为止。

- 删除对象时，存储分段的状态为*删除对象：只读*。在这种状态下、您不能向存储分段添加新对象。
- 删除所有对象后、存储分段将保持只读状态。您可以执行以下操作之一：
  - 将存储分段恢复为写入模式、并将其用于新对象
  - 删除存储分段
  - 保持存储分段处于只读模式、以保留其名称供将来使用
- 如果存储分段启用了对象版本控制、则可以使用删除存储分段中的对象操作删除在StorageGRID 11.8或更高版本中创建的标记。
- 如果存储分段启用了对象版本控制、则删除对象操作不会删除在StorageGRID 11.7或更早版本中创建的删除标记。有关删除存储分段中对象的信息，请参见"如何删除受版本控制的 S3 对象"。
- 如果使用"跨网格复制"，请注意以下事项：
  - 使用此选项不会从其他网格的存储分段中删除任何对象。
  - 如果为源分段选择此选项，则在将对象添加到另一网格上的目标分段时，将触发*跨网格复制失败*警报。如果无法保证没有人会在删除所有存储分段对象之前将对象添加到另一网格上的存储分"禁用跨网格复制"段中。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"root访问权限"。此权限将覆盖组或存储分段策略中的权限设置。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

   此时将显示 " 分段 " 页面，其中会显示所有现有的 S3 分段。

2. 使用*操作*菜单或特定存储分段的详细信息页面。

操作菜单

a. 选中要从中删除对象的每个存储分段对应的复选框。
b. 选择*操作*>*删除存储分段中的对象*。

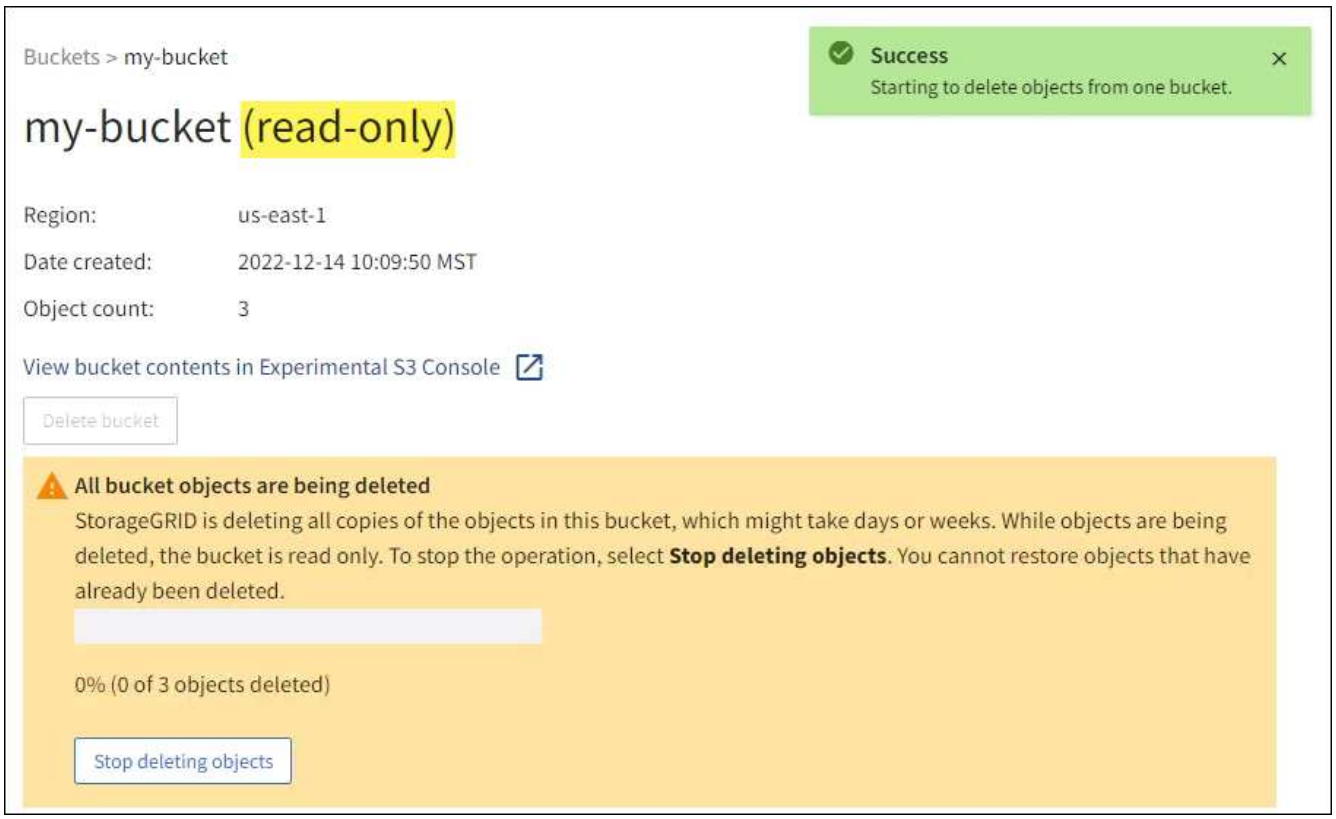
详细信息页面

a. 选择存储分段名称以显示其详细信息。
b. 选择*删除存储分段中的对象*。

3. 出现确认对话框时，查看详细信息，输入*Yes*，然后选择*OK*。
4. 等待删除操作开始。

   几分钟后：

   - 此时、存储分段详细信息页面上将显示一个黄色状态横幅。进度条表示已删除的对象百分比。
   - 在存储分段详细信息页面上、*(只读)*显示在存储分段名称后面。
   - *(删除对象：只读)*出现在"分段"页的分段名称旁边。

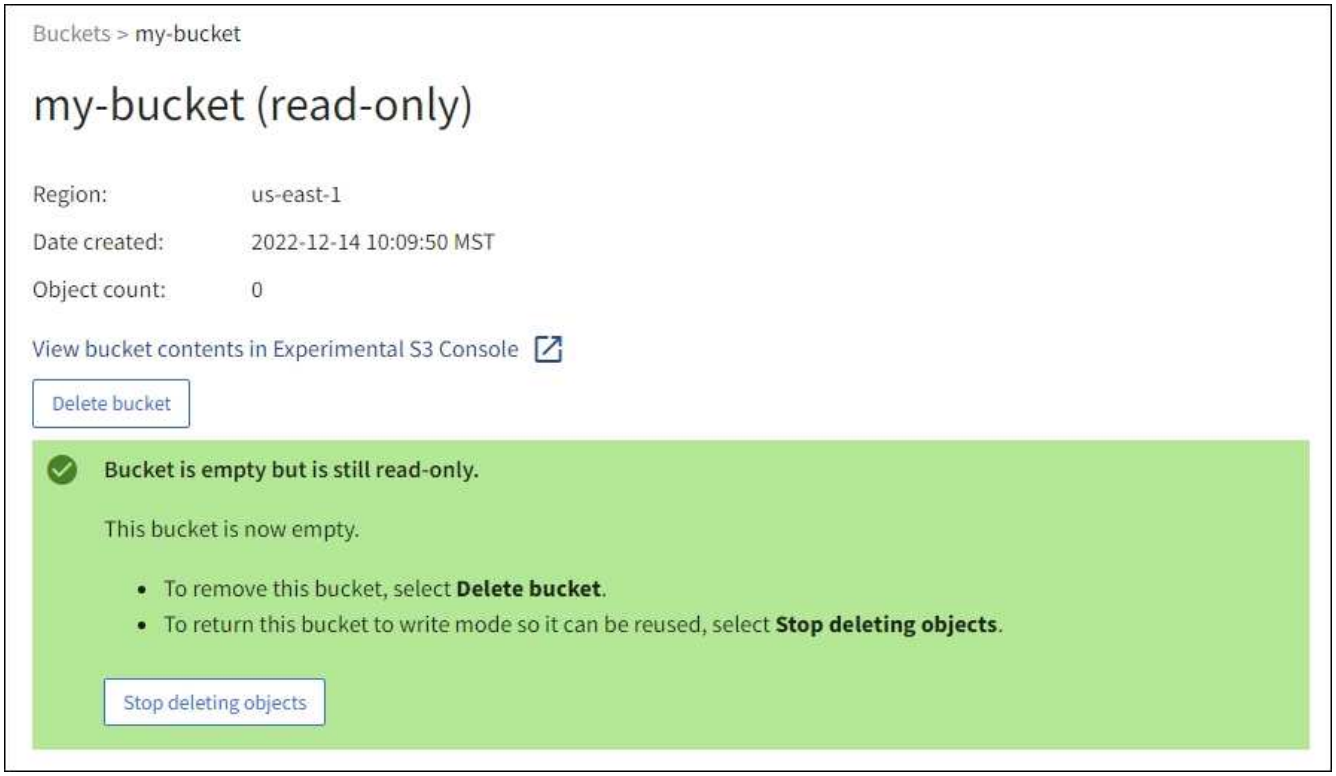


5. 在运行操作时，根据需要选择*停止删除对象*以暂停进程。然后，选择*删除存储分段中的对象*以恢复此过程。

   选择*停止删除对象*时，存储分段将返回到写入模式；但是，您无法访问或恢复已删除的任何对象。

6. 等待此操作完成。

当存储分段为空时、状态横幅将更新、但存储分段仍保持只读状态。



7. 执行以下操作之一：
   - 退出页面以使存储分段保持只读模式。例如、您可以将一个空分段保留为只读模式、以保留该分段名称供将来使用。
   - 删除存储分段。您可以选择*删除存储分段*来删除单个存储分段，也可以返回“存储分段”页面并选择*操作*>*删除*存储分段来删除多个存储分段。

     如果在删除所有对象后无法删除分版本存储分段、则删除标记可能会保留下来。要删除存储分段、必须删除所有剩余的删除标记。

   - 将存储分段恢复为写入模式、并可选择将其用于新对象。您可以为单个存储分段选择*停止删除对象*，也可以返回到“存储分段”页面，并为多个存储分段选择*操作*>*停止删除对象*。

删除 **StorageGRID S3** 存储桶

您可以使用租户管理器删除一个或多个空的 S3 分段。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理所有分段或root访问权限"。这些权限将覆盖组或存储分段策略中的权限设置。
- 要删除的存储分段为空。如果要删除的分段为_NOT _空，"从存储分段中删除对象"。

关于此任务

以下说明介绍如何使用租户管理器删除 S3 存储分段。您也可以使用或删除S3存储分段"租户管理 API""S3 REST API"。

如果S3存储分段包含对象、非当前对象版本或删除标记、则不能将其删除。有关如何删除S3版本控制对象的信息，请参见"如何删除对象"。

步骤

1. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。

   此时将显示 " 分段 " 页面，其中会显示所有现有的 S3 分段。

2. 使用*操作*菜单或特定存储分段的详细信息页面。

   操作菜单

   a. 选中要删除的每个存储分段对应的复选框。
   b. 选择*Actions*>*Delete Buc分 段*。

   详细信息页面

   a. 选择存储分段名称以显示其详细信息。
   b. 选择*删除存储分段*。

3. 出现确认对话框时，选择*Yes*。

   StorageGRID 会确认每个存储分段均为空，然后删除每个存储分段。此操作可能需要几分钟时间。

   如果存储分段不为空，则会显示一条错误消息。必须"删除存储分段中的所有对象和任何删除标记"先删除存储分段。

在 **StorageGRID** 中使用 **S3 Console**

您可以使用S3控制台查看和管理S3存储分段中的对象。

S3控制台允许您：

- 上传、下载、重命名、复制、移动、 并删除对象
- 查看、还原、下载和删除对象版本
- 按前缀搜索对象
- 管理对象标记
- 查看对象元数据
- 查看、创建、重命名、复制、移动、 和删除文件夹

> S3控制台可为大多数常见情形提供更好的用户体验。它并不能在所有情况下替代CLI或API操作。
>
> 如果使用S3控制台导致操作时间过长(例如、几分钟或几小时)、请考虑：
>
> - 减少选定对象的数量
> - 使用非图形(API或CLI)方法访问数据

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 如果您要管理对象、则属于具有root访问权限的用户组。或者、您属于具有"使用S3控制台"选项卡权限以及"查看所有分段"或"管理所有分段"权限的用户组。请参阅。 "租户管理权限"
- 已为用户配置 S3 组或存储桶策略。看"使用存储分段和组访问策略" 。
- 您知道用户的访问密钥 ID 和机密访问密钥。(可选)您有一个 `.csv`包含此信息的文件。请参见"创建访问密钥的说明"。

步骤

1. 选择 存储 > 存储桶 > 存储桶名称。
2. 选择S3控制台选项卡。
3. 将访问密钥ID和机密访问密钥粘贴到字段中。否则，请选择*上传访问密钥*并选择您的 `.csv`文件。
4. 选择 * 登录 * 。
5. 此时将显示存储分段对象表。您可以根据需要管理对象。

追加信息

- 按前缀搜索：前缀搜索功能仅搜索以当前文件夹的特定词开头的对象。搜索不包括在其他位置包含单词的对象。此规则也包括文件夹中的适用场景对象。例如，搜索 `folder1/folder2/somefile-`将返回文件夹中以单词开头的 `somefile-`对象 `folder1/folder2/`。
- 拖放：您可以将文件从计算机的文件管理器拖放到S3控制台。但是、您不能上传文件夹。
- 对文件夹的操作：移动、复制或重命名文件夹时，文件夹中的所有对象一次更新一个，这可能需要一段时间。
- 禁用存储分段版本控制时永久删除：在禁用了版本控制的情况下覆盖或删除存储分段中的对象时、此操作将永久生效。请参阅。 "更改存储分段的对象版本控制"

管理 S3 平台服务

S3 平台服务

了解 StorageGRID 的平台服务

在实施平台服务之前、请查看使用这些服务的概述和注意事项。

有关S3的信息，请参见"使用S3 REST API"。

平台服务概述

StorageGRID 平台服务允许您向外部目标发送事件通知以及S3对象和对象元数据的副本、从而帮助您实施混合云战略。

由于平台服务的目标位置通常不在 StorageGRID 部署中，因此平台服务可以为您提供使用外部存储资源，通知服务以及数据搜索或分析服务所带来的强大功能和灵活性。

可为单个 S3 存储桶配置任何平台服务组合。例如，您可以在 StorageGRID S3 存储桶上同时配置 "CloudMirror 服务" 和 "通知"，以便将特定对象镜像到 Amazon Simple Storage Service (S3)，同时向第三方监控应用程序发送有关此类对象的通知，以帮助您跟踪 AWS 费用。

StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。

如何配置平台服务

平台服务与您使用配置的外部端点进行通信"租户管理器"或"租户管理 API"。每个端点代表一个外部目标，例如StorageGRID S3 存储桶、Amazon Web Services 存储桶、Amazon SNS 主题、webhook 端点或在本地、AWS 或其他地方托管的 Elasticsearch 集群。

创建外部端点后、您可以通过向存储分段添加XML配置来为该存储分段启用平台服务。XML 配置可确定存储分段应处理的对象，存储分段应执行的操作以及存储分段应用于服务的端点。

您必须为要配置的每个平台服务添加单独的 XML 配置。例如：

- 如果要将密钥以开头的所有对象 `/images`复制到Amazon S3存储分段、则必须向源存储分段添加复制配置。
- 如果您还希望在这些对象存储到存储分段时发送通知，则必须添加通知配置。
- 如果要为这些对象的元数据编制索引、则必须添加用于实施搜索集成的元数据通知配置。

配置 XML 的格式由用于实施 StorageGRID 平台服务的 S3 REST API 控制：

平台服务	**S3 REST API**	请参见
CloudMirror 复制	• GetBucketReplication • PutBucketReplication	• "CloudMirror 复制" • "对存储分段执行的操作"
通知	• GetBucketNotizationConfiguration • PutBucketNotizationConfiguration	• "通知" • "对存储分段执行的操作"
搜索集成	• 获取存储分段元数据通知配置 • PUT 存储分段元数据通知配置	• "搜索集成" • "StorageGRID自定义操作"

使用平台服务的注意事项

注意事项	详细信息
目标端点监控	您必须监控每个目标端点的可用性。如果与目标端点的连接长时间断开，并且存在大量请求积压，则向 StorageGRID 发出的其他客户端请求（例如 PUT 请求）将失败。当端点可访问时，您必须重试这些失败的请求。

注意事项	详细信息
目标端点限制	如果发送请求的速率超过目标端点接收请求的速率， StorageGRID 软件可能会限制传入的存储分段 S3 请求。只有在等待发送到目标端点的请求积压时，才会发生限制。 唯一明显的影响是，传入的 S3 请求执行时间较长。如果您开始检测到性能明显较慢，则应降低载入速率或使用容量较高的端点。如果积压的请求持续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。 CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求所涉及的数据传输通常多于搜索集成或事件通知请求。
订购担保	StorageGRID 保证对站点中的对象执行操作的顺序。只要针对某个对象的所有操作都位于同一站点内，最终对象状态（用于复制）就始终等于 StorageGRID 中的状态。 在跨 StorageGRID 站点执行操作时， StorageGRID 会尽力订购请求。例如，如果您先将某个对象写入站点 A ，然后覆盖站点 B 上的同一个对象，则 CloudMirror 复制到目标分段的最终对象不能保证为较新的对象。
ILM 驱动的对象删除	为了匹配AWS CRR和Amazon Simple Notification Service的删除行为、在因StorageGRID ILM规则而删除源存储分段中的对象时、不会发送CloudMirror和事件通知请求。例如，如果 ILM 规则在 14 天后删除某个对象，则不会发送 CloudMirror 或事件通知请求。 相反，在因 ILM 而删除对象时，系统会发送搜索集成请求。
使用Kafka端点	Kafka端点的身份验证使用以下身份验证类型。这些类型与用于对其他端点(如Amazon SNS)进行身份验证的类型不同、需要用户名和密码凭据。 • SASL/普通 • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 *注意:*配置的存储代理设置不适用于Kafka平台服务端点。

使用 **CloudMirror** 复制服务的注意事项

注意事项	详细信息
复制状态	StorageGRID不支持此 `x-amz-replication-status`标题。
对象大小	CloudMirror 复制服务可复制到目标分段的对象的最大大小为 5 TiB ，与最大 _supported 对象大小相同。 注意：单个PutObject操作的最大_Recommended_大小为5 GiB (5、368、709、120字节)。如果对象大于 5 GiB ，请改用多部分上传。

注意事项	详细信息
存储分段版本控制和版本ID	如果 StorageGRID 中的源 S3 存储分段已启用版本控制，则还应为目标存储分段启用版本控制。 使用版本控制时，请注意，由于 S3 协议的限制，目标存储桶中对象版本的排序是尽力而为的，CloudMirror 服务不对此提供保证。此外，目标存储桶将维护其自身设置，可能不提供版本控制。 注意：StorageGRID 中源存储分段的版本ID与目标存储分段的版本ID无关。
标记对象版本	由于S3协议中的限制、CloudMirror服务不会复制提供版本ID的任何PutObjectTaging或DeleteObjectTagingRequests。由于源和目标的版本ID不相关、因此无法确保复制对特定版本ID的标记更新。 相反、CloudMirror服务会复制未指定版本ID的PutObjectTastingclaingRequests或DeleteObjectTastingcling请求。这些请求会更新最新密钥的标记（如果分段已受版本控制，则更新最新版本的标记）。此外，还会复制具有标记（而不是标记更新）的常规载入。
多部分上传和 `ETag`值	镜像使用多部分上传方式上传的对象时， CloudMirror 服务不会保留这些部分。因此、 `ETag`镜像对象的值将与原始对象的值不同 `ETag`。
使用 SSI-C 加密的对象（使用客户提供的密钥进行服务器端加密）	CloudMirror服务不支持使用SSE-C加密的对象。如果您尝试将对象插入源存储分段以进行CloudMirror复制、并且该请求包含SSE-C请求标头、则操作将失败。
已启用 S3 对象锁定的存储分段	如果 StorageGRID 中的源 S3 存储桶已启用 S3 Object Lock，则还应为配置了默认保留的目标存储桶启用 S3 Object Lock。 对于启用了 S3 Object Lock 的源和目标存储桶，支持复制_对象数据_。但是，目标存储桶将维护其自己的对象保留设置，并且它们可能不提供合规性或版本控制。

了解 **StorageGRID CloudMirror** 复制服务

如果您希望StorageGRID将添加到S3存储分段的指定对象复制到一个或多个外部目标存储分段、则可以为该存储分段启用CloudMirror复制。

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。

> CloudMirror 复制仅在源存储桶启用了 S3 对象锁定且端点为 Amazon 或 StorageGRID S3 存储桶时才受支持。对象锁定设置不会复制到存储桶端点。

CloudMirror和ILM

CloudMirror复制独立于网格的活动ILM策略运行。CloudMirror 服务会在将对象存储到源存储分段时复制这些对象，并尽快将其交付到目标存储分段。对象载入成功后，系统将触发复制对象的传送。

CloudMirror和跨网格复制

CloudMirror复制与跨网格复制功能有重要的相似之处和不同之处。请参阅 "请比较跨网格复制和CloudMirror复制"。

CloudMirror和S3存储分段

CloudMirror 复制通常配置为使用外部 S3 存储分段作为目标。但是，您也可以将复制配置为使用另一个 StorageGRID 部署或任何与 S3 兼容的服务。

现有存储分段

如果为现有存储分段启用了CloudMirror复制、则只会复制添加到该存储分段的新对象。不会复制存储分段中的任何现有对象。要强制复制现有对象，您可以通过执行对象复制来更新现有对象的元数据。

> 如果您使用CloudMirror复制将对象复制到Amazon S3目标、请注意、Amazon S3会将每个Put请求标头中用户定义的元数据的大小限制为2 KB。如果对象的用户定义元数据大于 2 KB ，则不会复制该对象。

多个目标分段

要将单个分段中的对象复制到多个目标分段、请在复制配置XML中为每个规则指定目标。不能同时将一个对象复制到多个分段。

分版本或未分版本的分段

您可以在受版本管理或未受版本管理的分段上配置CloudMirror复制。目标分段可以是版本控制、也可以是未版本控制。您可以使用版本控制和未版本控制的分段的任意组合。例如，您可以将版本控制的存储分段指定为未版本控制的源存储分段的目标，反之亦然。您还可以在未版本控制的存储分段之间进行复制。

删除、复制环路和事件

删除行为

与Amazon S3服务跨区域复制(CRR)的删除行为相同。删除源存储分段中的对象绝不会删除目标中复制的对象。如果源和目标存储分段都已进行版本控制，则会复制删除标记。如果目标存储分段未进行版本控制、则删除源存储分段中的对象不会将删除标记复制到目标存储分段或删除目标对象。

防止复制环路

当对象复制到目标分段时、StorageGRID会将其标记为"副本"。目标StorageGRID分段不会再次复制标记为副本的对象、从而防止您出现意外复制环路。此副本标记是StorageGRID的内部标记、不会妨碍您在使用Amazon S3存储分段作为目标时利用AWS CRR。

> 用于标记复本的自定义标头为 `x-ntap-sg-replica`。此标记可防止级联镜像。StorageGRID 支持在两个网格之间使用双向CloudMirror。

目标存储分段中的事件

无法保证目标存储分段中事件的唯一性和顺序。由于为确保成功交付而执行的操作，可能会将一个源对象的多个相同副本传送到目标。在极少数情况下，如果从两个或更多不同的 StorageGRID 站点同时更新同一对象，则目标存储分段上的操作顺序可能与源存储分段上的事件顺序不匹配。

了解 S3 存储桶的 StorageGRID 事件通知

如果您希望StorageGRID将有关指定事件的通知发送到目标 Kafka 集群、webhook 端点或

Amazon Simple Notification Service，则可以为 S3 存储桶启用事件通知。

例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

事件通知在通知配置中指定的源存储分段处创建，并传送到目标。如果与某个对象关联的事件成功，则会创建有关该事件的通知并排队等待传送。

不能保证通知的唯一性和顺序。由于为保证成功交付而执行的操作，可能会向目标发送多个事件通知。由于交付是异步的，因此无法保证目标上通知的时间顺序与源存储分段上事件的顺序一致，尤其是对于来自不同 StorageGRID 站点的操作。您可以在事件消息中使用 `sequencer`键来确定特定对象的事件顺序、如Amazon S3文档中所述。

StorageGRID事件通知遵循Amazon S3 API、但存在一些限制。

- 支持以下事件类型：
  - S3：已创建对象：
  - S3：对象创建：放置
  - S3：对象创建：发布
  - S3：对象创建：复制
  - S3：ObjectCreated：CompleteMultipartUpload
  - S3：已删除对象：
  - S3：ObjectRemoved：Delete
  - S3：ObjectRemoved：DeleteMarkerCreated
  - S3：ObjectRestore：POST
- 从StorageGRID 发送的事件通知使用标准JSON格式、但不包括某些密钥、而对其他密钥使用特定值、如表所示：

密钥名称	**StorageGRID** 值
事件源	`sgws:s3`
awsRegion	不包括
X-AMZ-ID-2	不包括
ARN	`urn:sgws:s3:::bucket_name`

了解 **StorageGRID** 搜索集成服务

如果要对对象元数据使用外部搜索和数据分析服务，则可以为 S3 存储分段启用搜索集成。

搜索集成服务是一种自定义StorageGRID服务、每当创建或删除对象或更新其元数据或标记时、该服务都会自动异步将S3对象元数据发送到目标端点。然后，您可以使用目标服务提供的复杂搜索，数据分析，可视化或机器

学习工具来搜索，分析对象数据并从中获得洞察力。

例如，您可以将存储分段配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 跨存储分段执行搜索，并对对象元数据中存在的模式执行复杂的分析。

虽然可以在启用了S3对象锁定的存储分段上配置Ela才 搜索集成、但对象的S3对象锁定元数据(包括"保留到日期"和"合法保留状态")不会包含在发送到Ela才 搜索的元数据中。

> 由于搜索集成服务会将对象元数据发送到目标、因此其配置XML称为"_metadata_Notification configuration XML"。此配置XML与用于启用_event_通知的"通知配置XML"不同。

搜索集成和**S3**存储分段

您可以为任何版本控制或未版本控制的存储分段启用搜索集成服务。搜索集成是通过将元数据通知配置 XML 与用于指定要对哪些对象执行操作的存储分段以及对象元数据的目标进行关联来配置的。

元数据通知以JSON文档的形式生成、该文档使用存储分段名称、对象名称和版本ID (如果有)命名。除了对象的所有标记和用户元数据之外，每个元数据通知还包含一组标准的对象系统元数据。

> 对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后、无法在索引中编辑文档的域类型。

搜索通知

在以下情况下、系统会生成元数据通知并将其排队以供传送：

- 已创建对象。
- 删除对象，包括因网格的 ILM 策略操作而删除对象的时间。
- 添加，更新或删除对象元数据或标记。更新时始终会发送一组完整的元数据和标记，而不仅仅是更改后的值。

将元数据通知配置 XML 添加到存储分段后，系统会为您创建的任何新对象以及您通过更新其数据，用户元数据或标记来修改的任何对象发送通知。但是、不会为存储分段中已有的任何对象发送通知。要确保将存储分段中所有对象的对象元数据发送到目标，应执行以下任一操作：

- 创建存储分段后以及添加任何对象之前，请立即配置搜索集成服务。
- 对存储分段中已有的所有对象执行操作，此操作将触发元数据通知消息以发送到目标。

搜索集成服务和**El**在职 搜索

StorageGRID 搜索集成服务支持将 Elasticsearch 集群作为目标。与其他平台服务一样，目标也会在端点中指定，而此端点的 URN 会在该服务的配置 XML 中使用。使用 "NetApp 互操作性表工具"确定受支持的ElASISearch版本。

管理平台服务端点

在为存储分段配置平台服务之前，必须至少将一个端点配置为平台服务的目标。

StorageGRID 管理员可以按租户访问平台服务。要创建或使用平台服务端点、您必须是具有"管理端点"或"根"访问权限的租户用户、并且网格中的网络连接已配置为允许存储节点访问外部端点资源。对于单个租户、您最多可以配置500个平台服务端点。有关详细信息，请与 StorageGRID 管理员联系。

什么是平台服务端点?

平台服务端点用于指定StorageGRID访问外部目标所需的信息。

例如、如果要将对象从StorageGRID 存储分段复制到Amazon S3存储分段、则需要创建一个平台服务端点、其中包含StorageGRID 访问Amazon上的目标存储分段所需的信息和凭据。

每种类型的平台服务都需要自己的端点，因此您必须为计划使用的每个平台服务至少配置一个端点。定义平台服务端点后，您可以在用于启用此服务的配置 XML 中使用此端点的 URN 作为目标。

您可以对多个源存储分段使用与目标相同的端点。例如，您可以配置多个源分段，将对象元数据发送到同一搜索集成端点，以便可以跨多个分段执行搜索。您还可以将源存储分段配置为使用多个端点作为目标、这样、您可以执行以下操作：将有关对象创建的通知发送到一个Amazon Simple Notification Service (Amazon SNS)主题、将有关对象删除的通知发送到另一个Amazon SNS主题。

用于 **CloudMirror** 复制的端点

StorageGRID 支持表示 S3 存储分段的复制端点。这些存储分段可能托管在 Amazon Web Services ，相同或远程 StorageGRID 部署或其他服务上。

通知的端点

StorageGRID支持 Amazon SNS、Kafka 和 webhook 端点。不支持简单队列服务 (SQS) 和 AWS Lambda 端点。

搜索集成服务的端点

StorageGRID 支持表示 Elasticsearch 集群的搜索集成端点。这些EI路径 搜索集群可以位于本地数据中心、也可以托管在AWS云或其他位置。

搜索集成端点是指特定的 Elasticsearch 索引和类型。您必须先在 Elasticsearch 中创建索引，然后才能在 StorageGRID 中创建端点，否则端点创建将失败。在创建端点之前、无需创建类型。如果需要， StorageGRID 将在向端点发送对象元数据时创建此类型。

相关信息

"管理 StorageGRID"

创建平台服务端点时，必须指定唯一资源名称（ URN ）。在为平台服务创建配置XML时、您将使用URN引用此端点。每个端点的 URN 必须是唯一的。

StorageGRID 会在您创建平台服务端点时对其进行验证。在创建平台服务端点之前，请确认此端点中指定的资源存在且可访问。

urn 元素

平台服务端点的URN必须以或 `urn:mysite`开头 `arn:aws`，如下所示：

- 如果服务托管在Amazon Web Services (AWS)上、请使用 `arn:aws`
- 如果服务托管在Google Cloud Platform (GCP)上、请使用 `arn:aws`
- 如果服务托管在本地、请使用 `urn:mysite`

例如、如果为StorageGRID上托管的CloudMirror端点指定URN、则URN可能以开头 `urn:sgws`。

URN 的下一个元素用于指定平台服务的类型，如下所示：

服务	键入
CloudMirror 复制	`s3`
通知	`sns`， `kafka` ， 或者 `webhook`
搜索集成	`es`

例如，要继续为StorageGRID上托管的CloudMirror端点指定URN，您可以添加 `s3`到`get `urn:sgws:s3`。

对于大多数端点来说，URN 的最后一个元素标识目标 URI 处的特定目标资源，例如， `sns-topic-name` 。

对于 webhook 端点，目标资源就是目标 URI 本身。

服务	特定资源
CloudMirror 复制	`bucket-name`
通知	`sns-topic-name`或 `kafka-topic-name` *注意：*对于 webhook 端点，URN 的最后一个元素可以是任何字符串，只要端点的 URN 是唯一的。
搜索集成	`domain-name/index-name/type-name` • 注意： * 如果 Elasticsearch 集群已配置为 * 不 * 自动创建索引，则必须在创建端点之前手动创建索引。

AWS 和 **GCP** 上托管的服务的 **urns**

对于 AWS 和 GCP 实体，完整的 URN 是有效的 AWS ARN 。例如：

- CloudMirror 复制：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 搜索集成：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> 对于AWS搜索集成端点， `domain-name`必须包括文字字符串 `domain/`，如下所示。

用于本地托管服务的 **urns**

使用本地托管的服务而非云服务时，只要 URN 在第三个和最后一个位置包含所需的元素，您就可以以任何方式指定 URN 以创建有效且唯一的 URN 。您可以将可选元素留空，也可以通过任何方式指定这些元素，以帮助您标识资源并使 URN 具有唯一性。例如：

- CloudMirror 复制：

```
urn:mysite:s3:::bucket-name
```

对于StorageGRID上托管的CloudMirror端点、您可以指定以开头的有效URN `urn:sgws`：

```
urn:sgws:s3:::bucket-name
```

- 通知：

指定Amazon Simple Notification Service端点：

```
urn:aws:sns:region:account-id:sns-topic-name
```

指定Kafka端点：

```
urn::kafka:::kafka-topic-name
```

> 或者，您可以在指定 Kafka 端点时包含以下内容 `mysite`：
> `urn:mysite:kafka:::kafka-topic-name`

指定 webhook 端点：

```
urn:mysite:webhook:::webhook-name
```

- 搜索集成：

```
urn:mysite:es:::domain-name/index-name/type-name
```

> 对于本地托管的搜索集成端点、元素可以是任意字符串、 `domain-name`只要端点的URN是唯一的。

创建 **StorageGRID** 平台服务端点

必须至少创建一个正确类型的端点，然后才能启用平台服务。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- StorageGRID 管理员已为租户帐户启用平台服务。
- 您属于具有的用户组"管理端点或root访问权限"。
- 平台服务端点引用的资源已创建：
  - CloudMirror 复制： S3 存储分段
  - 事件通知：Amazon Simple Notification Service (Amazon SNS) 主题、Kafka 主题或 Webhook 终端节点
  - 搜索通知：Elasticsearch 索引，如果目标集群未配置为自动创建索引。
- 您知道有关目标资源的信息：
  - 统一资源标识符（ URI ）的主机和端口

    > 如果您计划使用 StorageGRID 系统上托管的存储分段作为 CloudMirror 复制的端点，请联系网格管理员以确定需要输入的值。

  - 唯一资源名称（ URN ）

    "为平台服务端点指定 URN"

  - 身份验证凭据（如果需要）：

搜索集成端点

对于搜索集成端点、您可以使用以下凭据：

- 访问密钥：访问密钥 ID 和机密访问密钥
- 基本 HTTP ： 用户名和密码

CloudMirror复制端点

对于CloudMirror复制端点、您可以使用以下凭据：

- 访问密钥：访问密钥 ID 和机密访问密钥
- CAP （ C2S 访问门户）： 临时凭据 URL ，服务器和客户端证书，客户端密钥以及可选的客户端专用密钥密码短语。

Amazon SNS端点

对于Amazon SNS端点、您可以使用以下凭据：

- 访问密钥：访问密钥 ID 和机密访问密钥

Kafka端点

对于Kafka端点、您可以使用以下凭据：

- SASL/PLAIN：用户名和密码
- SASL/SCRAM-SHA-256：用户名和密码
- SASL/SCRAM-SHA-512：用户名和密码

  - 安全证书（如果需要证书验证）

- 如果启用了EI在任 一EI在任 一安全功能中、您将拥有用于连接测试的监控集群权限、以及用于文档更新的写入索引权限或同时具有索引和删除索引权限。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。此时将显示平台服务端点页面。
2. 选择 * 创建端点 * 。
3. 输入显示名称以简要说明端点及其用途。

   当端点在“端点”页面上列出时，端点支持的平台服务类型会显示在端点名称旁边，因此您不需要在名称中包含该信息。

4. 在 * URI * 字段中，指定端点的唯一资源标识符（ URI ）。

   请使用以下格式之一：

```
https://host:port
http://host:port
```

如果未指定端口、则会使用以下默认端口：

- 端口443用于HTTPS URL、端口80用于HTTP URL (大多数端点)
- 用于HTTPS和HTTP URI的端口9092 (仅限Kafka端点)

例如， StorageGRID 上托管的存储分段的 URI 可能为：

```
https://s3.example.com:10443
```

在此示例中、 `s3.example.com`表示StorageGRID高可用性(HA)组的虚拟IP (VIP)的DNS条目、并 `10443` 表示负载平衡器端点中定义的端口。

应尽可能连接到负载平衡节点的HA组、以避免单点故障。

同样， AWS 上托管的存储分段的 URI 可能为：

```
https://s3-aws-region.amazonaws.com
```

如果此端点用于CloudMirror复制服务、请勿在URI中包含存储分段名称。您可以在 * URN* 字段中包含分段名称。

5. 输入端点的唯一资源名称（ URN ）。

   创建端点后、您无法更改此端点的URN。

6. 选择 * 继续 * 。
7. 为*身份验证类型*选择一个值。

   如果您需要对 webhook 端点进行身份验证，请在第 9 步。

搜索集成端点

输入或上传搜索集成端点的凭据。

您提供的凭据必须具有目标资源的写入权限。

Authentication type	说明	凭据
匿名	提供对目标的匿名访问。仅适用于已禁用安全性的端点。	无身份验证。
访问密钥	使用 AWS 模式的凭据对与目标的连接进行身份验证。	• 访问密钥 ID • 机密访问密钥
基本 HTTP	使用用户名和密码对目标连接进行身份验证。	• 用户名 • 密码

CloudMirror复制端点

输入或上传CloudMirror复制端点的凭据。

您提供的凭据必须具有目标资源的写入权限。

Authentication type	说明	凭据
匿名	提供对目标的匿名访问。仅适用于已禁用安全性的端点。	无身份验证。
访问密钥	使用 AWS 模式的凭据对与目标的连接进行身份验证。	• 访问密钥 ID • 机密访问密钥
CAP （ C2S 访问门户）	使用证书和密钥对目标连接进行身份验证。	• 临时凭据 URL • 服务器 CA 证书（ PEM 文件上传） • 客户端证书（ PEM 文件上传） • 客户端专用密钥（ PEM 文件上传，OpenSSL 加密格式或未加密的专用密钥格式） • 客户端专用密钥密码短语（可选）

Amazon SNS端点

输入或上传Amazon SNS端点的凭据。

您提供的凭据必须具有目标资源的写入权限。

Authentication type	说明	凭据
匿名	提供对目标的匿名访问。仅适用于已禁用安全性的端点。	无身份验证。
访问密钥	使用 AWS 模式的凭据对与目标的连接进行身份验证。	• 访问密钥 ID • 机密访问密钥

Kafka端点

输入或上传Kafka端点的凭据。

您提供的凭据必须具有目标资源的写入权限。

Authentication type	说明	凭据
匿名	提供对目标的匿名访问。仅适用于已禁用安全性的端点。	无身份验证。
SASL/普通	使用带有纯文本的用户名和密码对目标连接进行身份验证。	• 用户名 • 密码
SASL/SCRAM-SHA-256	使用用户名和密码并使用质询响应协议和SHA-256哈希对目标连接进行身份验证。	• 用户名 • 密码
SASL/SCRAM-SHA-512	使用用户名和密码并使用质询响应协议和SHA-512哈希对目标连接进行身份验证。	• 用户名 • 密码

如果用户名和密码源自从Kafka集群获取的委派令牌，请选择*使用委派进行身份验证*。

8. 选择 * 继续 * 。
9. 选择*验证证书*单选按钮来选择如何验证与端点的 TLS 连接。

大多数端点

验证搜索集成、CloudMirror 复制、Amazon SNS 或 Kafka 端点的 TLS 连接。

证书验证的类型	说明
TLS	验证与端点资源的 TLS 连接的服务器证书。
已禁用	证书验证已禁用。此选项不安全。
使用自定义 CA 证书	自定义 CA 证书用于在连接到端点时验证服务器的身份。
使用操作系统 CA 证书	使用操作系统上安装的默认网格 CA 证书来保护连接。

Webhook 和 **Kafka** 端点

验证 Webhook 或 Kafka 端点的 TLS 连接。

证书验证的类型	说明
TLS	验证与端点资源的 TLS 连接的服务器证书。
移动TLS	验证与端点资源的相互 TLS 连接的客户端和服务器证书。
已禁用	证书验证已禁用。此选项不安全。
使用自定义 CA 证书	自定义 CA 证书用于在连接到端点时验证服务器的身份。
使用操作系统 CA 证书	使用操作系统上安装的默认网格 CA 证书来保护连接。 注意：Webhook 端点没有此选项。

当您选择 **mTLS** 时，这些选项变为可用。

证书验证的类型	说明
不验证服务器证书	禁用服务器证书验证，这意味着服务器的身份未经验证。此选项不安全。
客户端证书	客户端证书用于在连接到端点时验证客户端的身份。
客户端私钥	客户端证书的私钥。如果加密，则必须使用传统格式 PKCS #1（不支持 PKCS #8 格式）。
客户端私钥密码	用于解密客户端私钥的密码。如果私钥未加密，请将此处留空。

10. 选择 * 测试并创建端点 * 。
    - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
    - 如果端点验证失败，则会显示一条错误消息。如果需要修改端点以更正错误，请选择 * 返回到端点详细信息 * 并更新此信息。然后，选择 * 测试并创建端点 * 。

    如果未为租户帐户启用平台服务、则端点创建将失败。请与 StorageGRID 管理员联系。

配置端点后，您可以使用其 URN 配置平台服务。

相关信息

- "为平台服务端点指定 URN"
- "配置 CloudMirror 复制"
- "配置事件通知"
- "配置搜索集成服务"
- "用于外部通信的端口"

测试 **StorageGRID** 平台服务端点的连接

如果与平台服务的连接发生更改，您可以测试端点的连接，以验证目标资源是否存在以及是否可以使用您指定的凭据访问它。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理端点或root访问权限"。

关于此任务

StorageGRID 不会验证这些凭据是否具有正确的权限。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。

2. 选择要测试其连接的端点。

   此时将显示端点详细信息页面。

3. 选择 * 测试连接 * 。
    - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
    - 如果端点验证失败，则会显示一条错误消息。如果需要修改端点以更正错误，请选择 * 配置 * 并更新信息。然后，选择 * 测试并保存更改 * 。

在 **StorageGRID** 中编辑平台服务端点

您可以编辑平台服务端点的配置以更改其名称， URI 或其他详细信息。例如，您可能需要更新已过期的凭据或更改 URI 以指向备份 Elasticsearch 索引以进行故障转移。您不能更改平台服务端点的URN。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理端点或root访问权限"。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。

2. 选择要编辑的端点。

   此时将显示端点详细信息页面。

3. 选择 * 配置 * 。
4. 根据需要更改端点的配置。

   创建端点后、您无法更改此端点的URN。

   a. 要更改终结点的显示名称，请选择编辑图标 。
   b. 根据需要更改 URI 。
   c. 根据需要更改身份验证类型。
      - 对于访问密钥身份验证，请根据需要更改密钥，方法是选择 * 编辑 S3 密钥 * 并粘贴新的访问密钥 ID 和机密访问密钥。如果需要取消所做的更改，请选择 * 还原 S3 密钥编辑 * 。
      - 对于 CAP （ C2S 访问门户）身份验证，更改临时凭据 URL 或可选客户端专用密钥密码短语，并根据需要上传新的证书和密钥文件。

        客户端专用密钥必须采用 OpenSSL 加密格式或未加密的专用密钥格式。

   d. 根据需要，更改验证证书的方法。
5. 选择 * 测试并保存更改 * 。
   - 如果可以使用指定凭据访问端点，则会显示一条成功消息。系统会从每个站点的一个节点验证与端点的连接。
   - 如果端点验证失败，则会显示一条错误消息。修改端点以更正错误，然后选择 * 测试并保存更改 * 。

删除 **StorageGRID** 平台服务端点

如果您不想再使用关联的平台服务，可以删除端点。

开始之前

- 您已使用登录到租户管理器"支持的 Web 浏览器"。
- 您属于具有的用户组"管理端点或root访问权限"。

步骤

1. 选择 * 存储（ S3 ） * > * 平台服务端点 * 。

   此时将显示平台服务端点页面，其中显示了已配置的平台服务端点列表。

2. 选中要删除的每个端点对应的复选框。

   如果删除正在使用的平台服务端点，则使用此端点的任何分段都将禁用关联的平台服务。任何尚未完成的请求都将被丢弃。所有新请求都将继续生成，直到您更改存储分段配置以不再引用已删除的 URN 为止。StorageGRID 会将这些请求报告为不可恢复的错误。

3. 选择 * 操作 * > * 删除端点 * 。

   此时将显示一条确认消息。

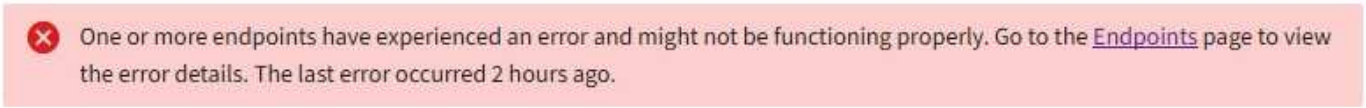
4. 选择 * 删除端点 * 。

StorageGRID 平台服务端点错误故障排除

如果在StorageGRID 尝试与平台服务端点通信时发生错误、则信息板上会显示一条消息。在平台服务端点页面上，最后一个错误列指示错误发生多长时间前。如果与端点凭据关联的权限不正确，则不会显示任何错误。

确定是否发生错误

如果在过去7天内发生任何平台服务端点错误、租户管理器信息板将显示警报消息。您可以转到平台服务端点页面以查看有关此错误的更多详细信息。



信息板上显示的同一错误也会显示在平台服务端点页面的顶部。要查看更详细的错误消息，请执行以下操作：

步骤

1. 从端点列表中，选择出现错误的端点。
2. 在端点详细信息页面上，选择*连接*。此选项卡仅显示端点的最新错误，并指示错误发生的时间。包含红色 X 图标 的错误发生在过去 7 天内。

检查错误是否仍然是最新的

即使解决了某些错误， * 最后一个错误 * 列也可能会继续显示这些错误。要查看错误是否为当前错误或强制从表中删除已解决的错误，请执行以下操作：

步骤

1. 选择端点。

   此时将显示端点详细信息页面。

2. 选择 * 连接 * > * 测试连接 * 。

选择 * 测试连接 * 将使 StorageGRID 验证平台服务端点是否存在以及是否可以使用当前凭据访问它。系统会从每个站点的一个节点验证与端点的连接。

解决端点错误

您可以使用端点详细信息页面上的 * 最后一个错误 * 消息来帮助确定导致错误的原因。某些错误可能需要编辑端点才能解决问题描述 。例如，如果 StorageGRID 由于没有正确的访问权限或访问密钥已过期而无法访问目标 S3 存储分段，则可能会发生 CloudMirrorbuc2 错误。消息为"端点凭据或目标访问需要更新"、详细信息为"AccessDenied"或"InvvalidAccessKeyId"。

如果您需要编辑端点以解决错误，则选择 * 测试并保存更改 * 会使 StorageGRID 验证更新后的端点，并确认可以使用当前凭据访问它。系统会从每个站点的一个节点验证与端点的连接。

步骤

1. 选择端点。
2. 在端点详细信息页面上，选择 * 配置 * 。
3. 根据需要编辑端点配置。
4. 选择 * 连接 * > * 测试连接 * 。

权限不足的端点凭据

当 StorageGRID 验证平台服务端点时，它会确认端点的凭据可用于联系目标资源，并执行基本权限检查。但是， StorageGRID 不会验证某些平台服务操作所需的所有权限。因此、如果在尝试使用平台服务时收到错误(例如"403禁止")、请检查与端点凭据关联的权限。

相关信息

- "管理StorageGRID ()；对平台服务进行故障排除"
- "创建平台服务端点"
- "测试平台服务端点的连接"
- "编辑平台服务端点"

在 **StorageGRID** 中配置 **CloudMirror** 复制

要为存储分段启用CloudMirror复制、请创建并应用有效的存储分段复制配置XML。

开始之前

- StorageGRID 管理员已为租户帐户启用平台服务。
- 您已创建一个存储分段以用作复制源。
- 要用作CloudMirror复制目标的端点已存在、并且您具有其URN。
- 您属于具有的用户组"管理所有分段或root访问权限"。使用租户管理器配置存储分段时，这些权限会覆盖组

或存储分段策略中的权限设置。

关于此任务

CloudMirror 复制会将对象从源存储分段复制到端点中指定的目标存储分段。

有关存储分段复制及其配置方法的一般信息，请参见 "Amazon Simple Storage Service (S3)文档：复制对象"。有关StorageGRID如何实施GetBucketReplication、DeleteBucketReplication和PutBucketReplication的信息，请参见"对存储分段执行的操作"。

> CloudMirror复制与跨网格复制功能有重要的相似之处和不同之处。要了解更多信息，请参阅"请比较跨网格复制和CloudMirror复制"。

配置CloudMirror复制时、请注意以下要求和特征：

- 在创建和应用有效的存储分段复制配置XML时、它必须对每个目标使用S3存储分段端点的URN。
- 只有为 Amazon S3 或 StorageGRID S3 存储桶启用了 S3 Object Lock 的源或目标存储桶才支持复制。对象锁标头未复制到目标对象。
- 如果在包含对象的存储分段上启用CloudMirror复制、则会复制添加到该存储分段的新对象、但不会复制该存储分段中的现有对象。您必须更新现有对象才能触发复制。
- 如果在配置 CloudMirror 复制后在目标存储桶上启用 S3 对象锁定，则可能需要 "重新保存端点" 以允许复制恢复。
- 如果在复制配置 XML 中指定存储类，则 StorageGRID 在对目标 S3 端点执行操作时会使用该类。目标端点还必须支持指定的存储类。请务必遵循目标系统供应商提供的任何建议。

步骤

1. 为源存储分段启用复制：
   - 使用文本编辑器创建在 S3 复制 API 中指定的启用复制所需的复制配置 XML 。
   - 配置 XML 时：
     - 请注意， StorageGRID 仅支持复制配置的 V1 。这意味着StorageGRID不支持在规则中使用 `Filter` 元素、而是遵循V1约定来删除对象版本。有关详细信息，请参见有关复制配置的 Amazon 文档。
     - 使用 S3 存储分段端点的 URN 作为目标。
     - (可选)添加元素、并指定以下选项 `<StorageClass>`之一：
       - `STANDARD`：默认存储类。如果在上传对象时未指定存储类、则会使用此 `STANDARD`存储类。
       - `STANDARD_IA`：(标准—访问频率不高。)此存储类用于访问频率较低但仍需要在需要时快速访问的数据。
       - `REDUCED_REDUNDANCY`：使用此存储类存储非关键、可重现的数据，这些数据的冗余程度低于存储 `STANDARD`类。
     - 如果在配置XML中指定、 `Role`则会忽略它。StorageGRID 不使用此值。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. 从信息板中选择*查看存储分段*，或选择*存储(S3)>*存储分段。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 复制 * 。
5. 选中*启用复制*复选框。
6. 将复制配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。

   StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证复制配置是否正确：
   a. 向源存储分段添加一个对象，以满足复制配置中指定的复制要求。

      在前面所示的示例中、将复制与前缀"2020"匹配的对象。

   b. 确认对象已复制到目标存储分段。

      对于小型对象，复制操作会快速进行。

相关信息

"创建平台服务端点"

在 **StorageGRID** 中配置事件通知

您可以通过创建通知配置XML并使用租户管理器将XML应用于存储分段来为存储分段启用通知。

开始之前

- StorageGRID 管理员已为租户帐户启用平台服务。
- 您已创建一个存储分段来用作通知源。

- 要用作事件通知目标的端点已存在、并且您具有其URN。
- 您属于具有的用户组"管理所有分段或root访问权限"。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

您可以通过将通知配置 XML 与源存储桶关联来配置事件通知。通知配置 XML 遵循 S3 约定来配置存储桶通知，并将目标 Amazon SNS 主题、Kafka 主题或 webhook 端点指定为端点的 URN。

有关事件通知以及如何配置事件通知的一般信息，请参阅 "Amazon文档"。有关StorageGRID如何实施S3存储分段通知配置API的信息，请参阅"有关实施 S3 客户端应用程序的说明"。

为存储分段配置事件通知时、请注意以下要求和特征：

- 在创建和应用有效通知配置XML时、它必须对每个目标使用事件通知端点的URN。
- 虽然可以在启用了S3对象锁定的存储分段上配置事件通知、但通知消息中不会包含对象的S3对象锁定元数据(包括保留到日期和合法保留状态)。
- 配置事件通知后，每当源存储桶中的对象发生指定事件时，都会生成通知并将其发送到用作目标的 Amazon SNS 主题、Kafka 主题或 webhook 终端节点。
- 如果为包含对象的存储分段启用事件通知，则仅会为保存通知配置后执行的操作发送通知。

步骤

1. 为源存储分段启用通知：
   - 使用文本编辑器创建启用 S3 通知 API 中指定的事件通知所需的通知配置 XML 。
   - 配置 XML 时，请使用事件通知端点的 URN 作为目标主题。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 事件通知 * 。
5. 选中*启用事件通知*复选框。
6. 将通知配置 XML 粘贴到文本框中，然后选择 * 保存更改 * 。

> StorageGRID 管理员必须使用网格管理器或网格管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证是否已正确配置事件通知：
   a. 对源存储分段中符合配置 XML 中配置的触发通知要求的对象执行操作。

      在此示例中、每当创建带有前缀的对象时、都会发送事件通知 `images/`。

   b. 确认通知已传送至目标 Amazon SNS 主题、Kafka 主题或 webhook 终端节点。

      例如、如果您的目标主题托管在Amazon SNS上、则可以将此服务配置为在发送通知时向您发送电子邮件。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+
如果在目标主题收到通知，则表示您已成功为 StorageGRID 通知配置源存储分段。

相关信息

- "了解存储分段通知"
- "使用S3 REST API"
- "创建平台服务端点"

在 **StorageGRID** 中配置搜索集成服务

您可以通过创建搜索集成XML并使用租户管理器将XML应用于存储分段来为存储分段启用搜索集成。

开始之前

- StorageGRID 管理员已为租户帐户启用平台服务。
- 您已创建要为其内容编制索引的S3存储分段。
- 要用作搜索集成服务目标的端点已存在、并且您具有其URN。
- 您属于具有的用户组"管理所有分段或root访问权限"。使用租户管理器配置存储分段时，这些权限会覆盖组或存储分段策略中的权限设置。

关于此任务

为源存储分段配置搜索集成服务后，创建对象或更新对象的元数据或标记会触发要发送到目标端点的对象元数据。

如果为已包含对象的存储分段启用搜索集成服务、则不会自动为现有对象发送元数据通知。更新这些现有对象、以确保将其元数据添加到目标搜索索引中。

步骤

1. 为存储分段启用搜索集成：

   - 使用文本编辑器创建启用搜索集成所需的元数据通知 XML 。
   - 配置 XML 时，请使用搜索集成端点的 URN 作为目标。

     可以按对象名称的前缀筛选对象。例如、可以将带有前缀的对象的元数据发送到一个目标、将带有前缀的对象的元数据发送 `images`到另一个目标 `videos`。前缀重叠的配置无效、提交后将被拒绝。例如、不允许配置为带有前缀的对象使用一个规则、为带有前缀的对象使用另一个 `test2`规则 `test`。

     根据需要，请参阅元数据配置XML的示例。

     ```
     <MetadataNotificationConfiguration>
      <Rule>
         <Status>Enabled</Status>
         <Prefix></Prefix>
         <Destination>
            <Urn>/Urn>
            </Destination>
      </Rule>
     </MetadataNotificationConfiguration>
     ```

     元数据通知配置XML中的元素：

名称	说明	必填
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
状态	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是
目标	规则目标的容器标记。 包含在 Rule 元素中。	是

名称	说明	必填
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN ： • `es`必须是第三个元素。 • URN必须以索引结尾，并以形式键入元数据的存储位置 `domain-name/myindex/mytype`。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是

2. 在租户管理器中，选择 * 存储（ S3 ） * > * 分段 * 。
3. 选择源存储分段的名称。

   此时将显示存储分段详细信息页面。

4. 选择 * 平台服务 * > * 搜索集成 *
5. 选中*启用搜索集成*复选框。
6. 将元数据通知配置粘贴到文本框中，然后选择 * 保存更改 * 。

   StorageGRID 管理员必须使用网格管理器或管理 API 为每个租户帐户启用平台服务。如果保存配置 XML 时发生错误，请联系 StorageGRID 管理员。

7. 验证是否已正确配置搜索集成服务：
   a. 向源存储分段添加一个对象，以满足配置 XML 中指定的元数据通知触发要求。

      在前面显示的示例中，添加到存储分段的所有对象都会触发元数据通知。

   b. 确认包含对象元数据和标记的 JSON 文档已添加到端点中指定的搜索索引中。

完成后

根据需要，您可以使用以下任一方法禁用存储分段的搜索集成：

- 选择*storage (S3)*>*Bucbes*并清除*Enable search integration*复选框。
- 如果您直接使用 S3 API ，请使用删除分段元数据通知请求。请参见有关实施 S3 客户端应用程序的说明。

示例：应用于所有对象的元数据通知配置

在此示例中，所有对象的对象元数据都将发送到同一目标。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

示例：具有两个规则的元数据通知配置

在此示例中、与前缀匹配的对象的对象元数据 `/images`将发送到一个目标、而与前缀匹配的对象的对象元数据 `/videos`将发送到另一个目标。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

元数据通知格式

为存储分段启用搜索集成服务后，每次添加，更新或删除对象元数据或标记时，系统都会生成一个 JSON 文档并将其发送到目标端点。

此示例显示了在名为的分段中创建 `test`具有密钥的对象时可能生成的JSON示例 `SGWS/Tagging.txt`。`test`存储分段未进行版本控制、因此 `versionId`标记为空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

JSON文档中包含的字段

文档名称包括存储分段名称，对象名称和版本 ID （如果存在）。

存储分段和对象信息

`bucket`:存储分段的名称

`key`:对象键名

`versionID`：对象版本、用于版本分段中的对象

`region`：例如，存储分段区域 `us-east-1`

系统元数据

`size`：HTTP客户端可见的对象大小(以字节为单位)

`md5`:对象哈希

用户元数据

`metadata`：对象的所有用户元数据，以键值对的形式显示

`key:value`

Tags

`tags`：为对象定义的所有对象标记，以键值对的形式

`key:value`

如何在**EIASITSEearch**中查看结果

对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前、请启用索引上的动态字段映射。为文档编制索引后、无法在索引中编辑文档的域类型。

使用S3 REST API

StorageGRID S3 REST API 支持的版本和更新

StorageGRID 支持简单存储服务（ S3 ） API ，该 API 作为一组表示状态传输（ Representational State Transfer ， REST ） Web 服务来实施。

通过对S3 REST API的支持、您可以将为S3 Web服务开发的面向服务的应用程序与使用StorageGRID 系统的内部对象存储连接起来。需要对客户端应用程序当前使用S3 REST API调用的情况进行最小更改。

支持的版本

StorageGRID支持以下特定版本的 STS、S3 和 HTTP：

项目	版本
STS AssumeRole API 规范	"Amazon Web Services (AWS) 文档：Amazon Assumerole API 参考" 有关 AssumeRole 的更多信息，请参阅"设置 AssumeRole"。
S3 API规范	"AWS 文档：Amazon Simple Storage Service API 参考"
HTTP	1.1 有关 HTTP 的详细信息，请参见 HTTP/1.1 （ RFC 7230-35 ）。 "IETF RFC 2616 ： 超文本传输协议（ HTTP/1.1 ）" • 注 * ： StorageGRID 不支持 HTTP/1.1 管道化。

对**S3 REST API**支持进行了更新

版本	注释
12.1.0	• `If-Match` 根据您的 StorageGRID 配置， `If-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。 • `If-None-Match` 根据您的 StorageGRID 配置， `If-None-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-None-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。 • 为以下请求和支持的标头添加了对预先计算的校验和值的支持： ◦ CompleteMultipartUpload: `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` ◦ CreateMultipartUpload: `CRC32`, `CRC32C`,以及 `CRC64NVME`用于 `x-amz-checksum-algorithm` ◦ CopyObject: `CRC32`, `CRC32C`, `CRC64NVME`,以及 `SHA256`用于 `x-amz-checksum-algorithm` ◦ PutObject: `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` ◦ UploadPart: `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`和 `x-amz-checksum-crc64nvme` • 添加了对 `x-amz-checksum-type`的支持，适用于 CreateMultipartUpload 和 CompleteMultipartUpload。 • 增加了对 `s3:x-amz-copy-source`策略条件键的支持。 • 允许在现有存储桶上启用 S3 对象锁定。
12.0	• 增加了对管理接口的跨域资源共享 (CORS) 支持，允许另一个域使用管理 API 访问StorageGRID中的数据。"了解更多信息。"。 • 添加了对 STS AssumeRole 和会话策略的支持。请参阅"会话策略示例"。您可以在租户组下设置 AssumeRole。

版本	注释
11.9	• 增加了对以下请求和支持的标头预先计算的SHA-256校验和值的支持。您可以使用此功能验证已上传对象的完整性： ◦ CompleteMultipartUpload： `x-amz-checksum-sha256` ◦ CreateMultipartUpload： `x-amz-checksum-algorithm` ◦ GetObject： `x-amz-checksum-mode` ◦ 标题对象： `x-amz-checksum-mode` ◦ ListParts ◦ PutObject： `x-amz-checksum-sha256` ◦ 上传部件： `x-amz-checksum-sha256` • 增加了网格管理员控制租户级别保留和合规性设置的功能。这些设置会影响S3对象锁定设置。 ◦ 分段默认保留模式和对象保留模式：监管或合规(如果网格管理员允许)。 ◦ 存储分段默认保留期限和对象保留截止日期：必须小于或等于网格管理员设置的最长保留期限所允许的值。 • 改进了对内容编码和流 `x-amz-content-sha256`值的支持 `aws-chunked`。限制： ◦ 如果存在、 `chunk-signature`则为可选且不经过验证 ◦ 如果存在、 `x-amz-trailer`则忽略内容
11.8	更新了S3操作的名称，使其与中使用的名称一致 "Amazon Web Services （AWS）文档： Amazon Simple Storage Service API 参考"。
11.7	• 已添加 "快速参考：支持的S3 API请求"。 • 增加了对将监管模式与S3对象锁定结合使用的支持。 • 增加了对GET对象和HEAD对象请求的StorageGRID专用响应标头的支持 `x-ntap-sg-cgr-replication-status`。此标头可提供跨网格复制的对象复制状态。 • 现在，选择对象内容请求支持镶木图对象。
11.6	• 增加了对在GET对象和HEAD对象请求中使用Request参数的支持 `partNumber`。 • 增加了对 S3 对象锁定的默认保留模式和存储分段级别的默认保留期限的支持。 • 增加了对策略条件密钥的支持 `s3:object-lock-remaining-retention-days`、用于设置对象允许的保留期限。 • 已将单个Put对象操作的最大_Recommended_大小更改为5 GiB (5、368、709、120字节)。如果对象大于 5 GiB ，请改用多部分上传。

版本	注释
11.5	• 增加了对管理存储分段加密的支持。 • 增加了对 S3 对象锁定和已弃用旧合规性请求的支持。 • 增加了对在版本控制的存储分段上使用删除多个对象的支持。 • 现在已正确支持此 `Content-MD5`请求标头。
11.4	• 增加了对删除存储分段标记，获取存储分段标记和放置存储分段标记的支持。不支持成本分配标记。 • 对于在 StorageGRID 11.4 中创建的分段，不再需要限制对象密钥名称以满足性能最佳实践。 • 增加了对事件类型分段通知的支持 `s3:ObjectRestore:Post`。 • 现在，多部件的 AWS 大小限制已强制实施。多部分上传中的每个部件必须介于 5 MiB 和 5 GiB 之间。最后一个部件可以小于 5 MiB 。 • 增加了对TLS 1.3的支持
11.3	• 增加了对使用客户提供的密钥（ SSI-C ）对对象数据进行服务器端加密的支持。 • 增加了对删除、获取和放置存储分段生命周期操作(仅限到期操作)以及响应标头的支持 `x-amz-expiration`。 • 更新了 PUT 对象， PUT 对象 - 复制和多部件上传，以说明在载入时使用同步放置的 ILM 规则的影响。 • 不再支持 TLS 1.1 密码。
11.2	增加了对用于云存储池的后对象还原的支持。增加了对在组和存储分段策略中使用 AWS 语法来处理 ARN ，策略条件密钥和策略变量的支持。仍支持使用 StorageGRID 语法的现有组和存储分段策略。 • 注意： * 在其他配置 JSON/XML 中使用 ARN/URN 的情况没有改变，包括在自定义 StorageGRID 功能中使用的情况。
11.1	增加了对跨源站资源共享(CORS)、用于S3客户端连接到网格节点的HTTP以及分段合规性设置的支持。
11.0	增加了对为存储分段配置平台服务（ CloudMirror 复制，通知和 Elasticsearch 搜索集成）的支持。此外、还增加了对存储分段的对象标记位置限制以及可用一致性的支持。
10.4	增加了对版本控制，端点域名页面更新，策略中的条件和变量，策略示例以及 PutOverwriteObject 权限的 ILM 扫描更改的支持。
10.3	增加了对版本控制的支持。
10.2	增加了对组和存储分段访问策略以及多部件副本（上传部件 - 复制）的支持。

版本	注释
10.1	增加了对多部分上传、虚拟托管式请求和 v4 身份验证的支持。
10.0	StorageGRID系统初步支持 S3 REST API。 _简单存储服务 API 参考_当前支持的版本是 2006-03-01。

StorageGRID 中支持的 S3 API 请求

此页面汇总了StorageGRID 如何支持Amazon Simple Storage Service (S3) API。

此页面仅包含 StorageGRID 支持的 S3 操作。任何未列出的 S3 操作都可能返回 `501 Not Implemented`或导致意外行为。

要查看每个操作的AWS文档、请选择标题中的链接。

通用**URI**查询参数和请求标头

除非另有说明、否则支持以下通用URI查询参数：

- `versionId`(根据对象操作的需要)

除非另有说明、否则支持以下通用请求标头：

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

相关信息

- "S3 REST API实施详细信息"
- "Amazon Simple Storage Service API参考：通用请求标头"

"AbortMultipartUpload"

URI查询参数和请求标头

StorageGRID支持对此请求使用all、并支持通用参数和标头以下附加URI查询参数：

- `uploadId`

请求正文

无

StorageGRID 文档

"多部分上传操作"

"CompleteMultipartUpload"

URI查询参数和请求标头

StorageGRID支持对此请求使用all、并支持通用参数和标头以下附加URI查询参数：

- `uploadId`
- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-checksum-type`
- `x-amz-storage-class`

请求正文**XML**标记

StorageGRID 支持以下请求正文XML标记：

- `ChecksumCRC32`
- `ChecksumCRC32C`
- `ChecksumCRC64NVME`
- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

StorageGRID 文档

"CompleteMultipartUpload"

"CopyObject"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加标头：

- `x-amz-checksum-algorithm`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`

- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

请求正文

无

StorageGRID 文档

"CopyObject"

"CreateBucket"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加标头：

- `x-amz-bucket-object-lock-enabled`

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"对存储分段执行的操作"

"CreateMultipartUpload"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加标头：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-checksum-type`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

请求正文

无

StorageGRID 文档

"CreateMultipartUpload"

"DeleteBucket"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

StorageGRID 文档

"对存储分段执行的操作"

"DeleteBucketCors"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"DeleteBucketEncryption"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"DeleteBucketLifecycle"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

- "对存储分段执行的操作"
- "创建 S3 生命周期配置"

"DeleteBucketPolicy"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"DeleteBucketReplication"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"DeleteBucketTbaging"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"DeleteObject"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求以及此附加请求标头：

- `x-amz-bypass-governance-retention`

请求正文

无

StorageGRID 文档

"对对象执行的操作"

"DeleteObjects"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求以及此附加请求标头：

- `x-amz-bypass-governance-retention`

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"对对象执行的操作"

"DeleteObjectTagging"

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对对象执行的操作"

"GetBucketAcl"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketCors"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketEncryption"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketLifecycleConfiguration"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

- "对存储分段执行的操作"
- "创建 S3 生命周期配置"

"GetBucketLocation"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketNotizationConfiguration"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketPolicy"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketReplication"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketTaging"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetBucketVersioning"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"GetObject"

URI查询参数和请求标头

StorageGRID支持此请求的所有、通用参数和标头以及以下附加URI查询参数：

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

以及以下附加请求标头：

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

请求正文

无

StorageGRID 文档

"GetObject"

"GetObjectAcl"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对对象执行的操作"

"GetObjectLegalHold"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"使用S3 REST API配置S3对象锁定"

"GetObjectLockConfiguration"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"使用S3 REST API配置S3对象锁定"

"GetObject保留"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"使用S3 REST API配置S3对象锁定"

"GetObjectTagging"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对对象执行的操作"

"HeadBucket"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"HeadObject"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加标头：

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

请求正文

无

StorageGRID 文档

"HeadObject"

"List桶"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

无

StorageGRID 文档

"服务 上的操作"

"ListMultipartUploads"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加参数：

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

请求正文

无

StorageGRID 文档

"ListMultipartUploads"

"ListObjects"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加参数：

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"ListObjectsV2"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加参数：

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"ListObjectVersies"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加参数：

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

请求正文

无

StorageGRID 文档

"对存储分段执行的操作"

"ListParts"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加参数：

- `max-parts`
- `part-number-marker`

- `uploadId`

请求正文

无

StorageGRID 文档

"ListMultipartUploads"

"PutBucketCors"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"对存储分段执行的操作"

"PutBucketEncryption"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文**XML**标记

StorageGRID 支持以下请求正文XML标记：

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

StorageGRID 文档

"对存储分段执行的操作"

"PutBucketLifecycleConfiguration"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文**XML**标记

StorageGRID 支持以下请求正文XML标记：

- `And`
- `Days`
- `Expiration`

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

StorageGRID 文档

- "对存储分段执行的操作"
- "创建 S3 生命周期配置"

"PutBucketNotizationConfiguration"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文**XML**标记

StorageGRID 支持以下请求正文XML标记：

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

StorageGRID 文档

"对存储分段执行的操作"

"PutBucketPolicy"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

有关支持的 JSON 主体字段的详细信息，请参阅"使用存储分段和组访问策略"。

"PutBucketReplication"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文**XML**标记

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

StorageGRID 文档

"对存储分段执行的操作"

"PutBucketTaging"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"对存储分段执行的操作"

"PutBucketVersioning"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文参数

StorageGRID 支持以下请求正文参数：

- `VersioningConfiguration`
- `Status`

StorageGRID 文档

"对存储分段执行的操作"

"PutObject"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加标头：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

请求正文

- 对象的二进制数据

StorageGRID 文档

"PutObject"

"PutObjectLegalHold"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"使用S3 REST API配置S3对象锁定"

"PutObjectLockConfiguration"

URI查询参数和请求标头

StorageGRID 支持此请求的_大多数_通用参数和标头。

请求正文

StorageGRID 支持 Amazon S3 REST API 在实施时定义的_大多数_请求正文参数，但以下情况除外：

除非网格管理员授予权限，否则无法使用 PutObjectLockConfiguration 在现有存储桶上启用 S3 对象锁定。

StorageGRID 文档

"使用S3 REST API配置S3对象锁定"

"PutObject保留"

URI查询参数和请求标头

StorageGRID支持此请求的所有通用参数和标头以及以下附加标头：

- `x-amz-bypass-governance-retention`

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"使用S3 REST API配置S3对象锁定"

"PutObjectTagging"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

StorageGRID 支持在实施时由Amazon S3 REST API定义的所有请求正文参数。

StorageGRID 文档

"对对象执行的操作"

"RestorEObject"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

有关支持的正文字段的详细信息，请参见"RestorEObject"。

"SelectObjectContent"

URI查询参数和请求标头

StorageGRID支持所有通用参数和标头此请求。

请求正文

有关支持的正文字段的详细信息、请参见以下内容：

- "使用 S3 Select"
- "SelectObjectContent"

"上传部件"

URI查询参数和请求标头

StorageGRID支持此请求的所有、通用参数和标头以及以下附加URI查询参数：

- `partNumber`
- `uploadId`

以及以下附加请求标头：

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

请求正文

- 零件的二进制数据

StorageGRID 文档

"上传部件"

"上传PartCopy"

URI查询参数和请求标头

StorageGRID支持此请求的所有、通用参数和标头以及以下附加URI查询参数：

- `partNumber`
- `uploadId`

以及以下附加请求标头：

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

请求正文

无

StorageGRID 文档

"上传PartCopy"

测试 StorageGRID S3 REST API 配置

您可以使用Amazon Web Services命令行界面(AWS CLI)测试与系统的连接、并验证是否可以读取和写入对象。

开始之前

- 您已从下载并安装AWS命令行界面 "aws.amazon.com/cli"。
- 您也可以选择"已创建负载平衡器端点"。否则、您知道要连接到的存储节点的IP地址以及要使用的端口号。请参阅。 "客户端连接的IP地址和端口"
- 您拥有 "已创建S3租户帐户"。
- 您已登录到租户和"已创建访问密钥"。

有关这些步骤的详细信息，请参见"配置客户端连接"。

步骤

1. 配置AWS命令行界面设置以使用您在StorageGRID 系统中创建的帐户：
   a. 进入配置模式： `aws configure`
   b. 输入您创建的帐户的访问密钥ID。
   c. 输入您创建的帐户的机密访问密钥。
   d. 输入要使用的默认区域。例如， `us-east-1`。
   e. 输入要使用的默认输出格式，或者按 * 输入 * 选择 JSON 。
2. 创建存储分段。

   此示例假设您已将负载平衡器端点配置为使用IP地址10.96.101.17和端口10443。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   如果已成功创建存储分段，则会返回存储分段的位置，如以下示例所示：

   ```
   "Location": "/testbucket"
   ```

3. 上传对象。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

   如果对象上传成功，则返回一个 Etag ，该 Etag 是对象数据的哈希。

4. 列出存储分段的内容以验证是否已上传此对象。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   list-objects --bucket testbucket
   ```

5. 删除对象。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   delete-object --bucket testbucket --key s3.pdf
   ```

6. 删除存储分段。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID 如何实施 S3 REST API

StorageGRID S3 REST API 如何解决冲突的客户端请求

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。

" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

StorageGRID S3 REST API 如何平衡可用性和一致性

一致性可在不同存储节点和站点之间的对象可用性与这些对象的一致性之间实现平衡。您可以根据应用程序的要求更改一致性。

默认情况下， StorageGRID保证新创建对象的读写一致性。成功完成 PUT 之后的任何 GET 都将能够读取新写入的数据。现有对象的覆盖、元数据更新和删除最终是一致的。

如果要以不同的一致性执行对象操作、您可以：

- 指定一致性每个存储分段。
- 为指定一致性每个API操作。
- 通过执行以下任务之一更改默认的网格范围一致性：
  - 在网格管理器中，转到*配置* > 系统 > 存储设置 > 默认存储桶一致性。
  - (英文)

> 对网格范围一致性的更改仅适用于在更改设置后创建的分段。要确定更改的详细信息，请参见位于的审核日志 `/var/local/log`(搜索*consencyLevel*)。

一致性值

一致性会影响StorageGRID用于跟踪对象的元数据在节点之间的分布方式。一致性影响对象对于客户端请求的可用性。

您可以将存储分段或API操作的一致性设置为以下值之一：

- **all**：所有节点都会立即接收对象元数据、否则请求将失败。
- 强全局：保证所有站点上所有客户端请求的读写一致性。配置 Quorum 语义时，将应用以下行为：
  - 当网格具有三个或更多站点时，允许对客户端请求进行站点故障容忍。双站点电网不具备站点故障容忍能力。
  - 如果一个站点发生故障，以下 S3 操作将无法成功：

- DeleteBucketEncryption
- PutBucketBranch
- PutBucketEncryption
- PutBucketVersioning
- PutObjectLegalHold
- PutObjectLockConfiguration
- PutObject保留

如果需要，您可以 "配置StorageGRID Quorum 语义以实现强全局一致性"。

- **strong-sit**：对象元数据会立即分发到站点上的其他节点。保证站点内所有客户端请求的写入后读一致性。
- **read-after-new-write**：为新对象提供写入后读取一致性，并最终为对象更新提供一致性。提供高可用性和数据保护保证。建议用于大多数情况。
- 可用：为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。

使用"新写后读取"和"可用"一致性

如果head或get操作使用"新写入后读取"一致性、则StorageGRID会通过多个步骤执行查找、如下所示：

- 它首先使用低一致性查找对象。
- 如果此查找失败、它将在下一个一致性值处重复此查找、直到达到与强全局行为等效的一致性为止。

如果head或get操作使用"新写入后读取"一致性、但对象不存在、则对象查找将始终达到与强全局行为等效的一致性。由于这种一致性要求每个站点上都有多个对象元数据副本、因此、如果同一站点上的两个或更多存储节点不可用、您可能会收到大量500个内部服务器错误。

除非您需要与Amazon S3类似的一致性保证、否则可以通过将一致性设置为"available "来防止HEAD和GET操作出现这些错误。如果head或get操作使用"可用"一致性、则StorageGRID仅提供最终的一致性。它不会在一致性提高时重试失败的操作、因此不需要提供对象元数据的多个副本。

[[API-operation]指定**API**操作的一致性

要为单个API操作设置一致性、此操作必须支持一致性值、并且必须在请求标头中指定一致性。此示例将GetObject操作的一致性设置为"strong-site"。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

对于PutObject和GetObject操作、必须使用相同的一致性。

指定 bucket 的一致性

要设置存储分段的一致性、可以使用StorageGRID"PUT 存储分段一致性"请求。或者、也可以"更改存储分段的一致性"从租户管理器中执行此操作。

设置存储分段的一致性时、请注意以下事项：

- 设置存储分段的一致性可确定对存储分段或存储分段配置中的对象执行的S3操作所使用的一致性。它不会影响存储分段本身的操作。
- 单个API操作的一致性会覆盖存储分段的一致性。
- 通常、分段应使用默认一致性"read-after-new-write"。如果请求无法正常工作、请尽可能更改应用程序客户端的行为。或者、将客户端配置为为为每个API请求指定一致性。只能在最后一种方法下、在存储分段级别设置一致性。

一致性和 ILM 规则如何相互作用以影响数据保护

您选择的一致性和ILM规则都会影响对象的保护方式。这些设置可以进行交互。

例如、存储对象时使用的一致性会影响对象元数据的初始放置、而为ILM规则选择的加载行为会影响对象副本的初始放置。由于StorageGRID需要同时访问对象的元数据及其数据才能满足客户端请求、因此为一致性和载入行为选择匹配的保护级别可以提供更好的初始数据保护、并提高系统响应的可预测性。

以下内容"加热选项"适用于ILM规则：

双提交
: StorageGRID会立即创建对象的临时副本、并将成功结果返回给客户端。如果可能，将创建 ILM 规则中指定的副本。

严格
: 必须先创建ILM规则中指定的所有副本、然后才能将成功返回到客户端。

平衡
: StorageGRID会在加载时尝试创建ILM规则中指定的所有副本；如果无法创建、则会创建临时副本、并将成功结果返回给客户端。在可能的情况下，将创建 ILM 规则中指定的副本。

一致性规则和ILM规则如何交互的示例

假设您有一个三站点网格，具有以下 ILM 规则和以下一致性：

- **ILM** 规则：创建三个对象副本，一个在本地站点，另一个在每个远程站点。使用严格的摄取行为。
- 一致性：强全局（对象元数据立即分发到多个站点）。

当客户端将对象存储到网格时， StorageGRID会复制所有三个对象并将元数据分发到多个站点，然后再将成功返回给客户端。

在接收成功消息时，对象将受到完全保护，不会丢失。例如，如果本地站点在摄取后不久丢失，对象数据和对象元数据的副本仍然存在于远程站点。该对象可以从其他站点完全检索。

如果您使用相同的 ILM 规则和强站点一致性，则客户端可能会在对象数据复制到远程站点之后但在对象元数据分发到那里之前收到成功消息。在这种情况下，对象元数据的保护级别与对象数据的保护级别不匹配。如果本地站点在摄取后不久丢失，对象元数据就会丢失。无法检索该对象。

一致性和ILM规则之间的相互关系可能很复杂。如果需要帮助、请联系NetApp。

StorageGRID 如何使用对象版本控制

如果要保留每个对象的多个版本、可以设置分段的版本控制状态。为分段启用版本控制有助于防止意外删除对象、并可用于检索和还原对象的早期版本。

StorageGRID 系统实施版本控制，并支持大多数功能，但存在一些限制。StorageGRID最多支持每个对象10、000个版本。

对象版本控制可以与 StorageGRID 信息生命周期管理（ ILM ）或 S3 存储分段生命周期配置结合使用。您必须明确为每个存储分段启用版本控制。为分段启用版本控制后、添加到分段的每个对象都会分配一个版本ID、该ID由StorageGRID系统生成。

不支持使用 MFA （多因素身份验证） Delete 。

> 只能在使用 StorageGRID 10.3 或更高版本创建的存储分段上启用版本控制。

ILM 和版本控制

ILM 策略将应用于对象的每个版本。ILM 扫描过程会持续扫描所有对象，并根据当前 ILM 策略重新评估这些对象。对 ILM 策略所做的任何更改都会应用于先前载入的所有对象。如果启用了版本控制，则包括先前载入的版本。ILM 扫描会将新的 ILM 更改应用于先前输入的对象。

对于启用了版本控制的分段中的S3对象，版本控制支持允许您创建使用"非当前时间"作为参考时间的ILM规则(在中为问题"仅将此规则应用于旧对象版本？"选择*是*"创建ILM规则向导的第1步")。对象更新后，其先前版本将变为非最新版本。通过使用"非当前时间"筛选器、您可以创建可减少先前版本对象对存储的影响的策略。

> 使用多部分上传操作上传新版本的对象时，原始版本对象的非当前时间反映为新版本创建多部分上传的时间，而不是多部分上传完成的时间。在有限情况下，原始版本的非当前时间可能比当前版本的时间早数小时或数天。

相关信息

- "如何删除受版本控制的 S3 对象"
- "S3 版本对象的 ILM 规则和策略（示例 4 ）"(英文)

使用 S3 REST API 配置 StorageGRID S3 对象锁定

如果为StorageGRID 系统启用了全局S3对象锁定设置、则可以在启用S3对象锁定的情况下创建分段。您可以为每个存储分段指定默认保留、也可以为每个对象版本指定保留设置。

> StorageGRID 不支持 `x-amz-sdk-checksum-algorithm`请求标头。

如何为存储分段启用S3对象锁定

如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以选择在创建每个分段时启用 S3 对象锁定。

S3对象锁定是一种永久性设置、只有在创建存储分段时才能启用。创建分段后、您无法添加或禁用S3对象锁

定。

要为存储桶启用 S3 Object Lock，请使用以下方法之一：

- 使用租户管理器创建存储分段。请参阅。 "创建 S3 存储分段"
- 使用带有请求标头的CreateBucket.创建存储分段 `x-amz-bucket-object-lock-enabled`。请参阅。 "对存储分段执行的操作"
- 从租户管理器管理存储桶设置。请参阅 "更新S3对象锁定默认保留"。

S3对象锁定需要分段版本控制、创建分段时会自动启用此功能。您不能暂停分段的版本控制。请参阅。 "对象版本控制"

存储分段的默认保留设置

为存储分段启用S3对象锁定后、您可以选择为存储分段启用默认保留、并指定默认保留模式和默认保留期限。

默认保留模式

- 在合规模式下：
  - 在达到保留截止日期之前、无法删除此对象。
  - 对象的保留截止日期可以增加、但不能减少。
  - 在达到该日期之前、无法删除对象的保留截止日期。
- 在监管模式下：
  - 具有权限的用户 `s3:BypassGovernanceRetention`可以使用 `x-amz-bypass-governance-retention: true` 请求标头绕过保留设置。
  - 这些用户可以在达到保留截止日期之前删除对象版本。
  - 这些用户可以增加、减少或删除对象的保留截止日期。

默认保留期限

每个存储分段都可以指定默认保留期限(以年或天为单位)。

如何设置存储分段的默认保留

要设置存储分段的默认保留时间、请使用以下方法之一：

- 通过租户管理器管理存储分段设置。请参阅"创建 S3 存储区。"和"更新S3对象锁定默认保留"。
- 问题描述存储分段的PutObjectLockConfiguration请求、用于指定默认模式和默认天数或年数。

PutObjectLockConfiguration

通过PutObjectLockConfiguration请求、您可以设置和修改启用了S3对象锁定的存储分段的默认保留模式和默认保留期限。您还可以删除先前配置的默认保留设置。

当新对象版本被摄取到存储桶时，如果未指定 `x-amz-object-lock-mode`和 `x-amz-object-lock-retain-until-date`，则应用默认保留模式。如果未指定 `x-amz-object-lock-retain-until-date`，则使用默认保留期限来计算保留截止日期。

如果在接收对象版本后修改了默认保留期限，则对象版本的 retain-until-date 保持不变，并且不会使用新的默认保留期限重新计算。

要完成此操作、您必须 `s3:PutBucketObjectLockConfiguration`具有权限或帐户root。

必须在 PutObjectLockConfiguration 请求中指定以下请求标头之一：

```
Content-MD5
x-amz-checksum-*
```

StorageGRID 不验证此操作的 x-amz-checksum-* 标头的内容。

请求示例

此示例为存储桶启用 S3 对象锁定（如果网格管理员已授予权限），并将默认保留模式设置为 COMPLIANCE，将默认保留期限设置为 6 年。

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

如何确定存储分段的默认保留

要确定是否为存储分段启用了S3对象锁定并查看默认保留模式和保留期限、请使用以下方法之一：

- 在租户管理器中查看存储分段。请参阅。 "查看S3存储分段"
- 问题描述一个GetObjectLockConfiguration请求。

GetObjectLockConfiguration

通过GetObjectLockConfiguration请求、您可以确定是否为存储分段启用了S3对象锁定、如果已启用、则查看是否为存储分段配置了默认保留模式和保留期限。

当新对象版本被摄取到存储桶时，如果未指定 `x-amz-object-lock-mode`，则应用默认保留模式。如果未指定 `x-amz-object-lock-retain-until-date`，则使用默认保留期限来计算保留截止日期。

要完成此操作、您必须 `s3:GetBucketObjectLockConfiguration`具有权限或帐户root。

请求示例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

响应示例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

启用了S3对象锁定的存储分段可以包含具有和不具有S3对象锁定保留设置的对象组合。

对象级保留设置可通过S3 REST API来指定。对象的保留设置将覆盖存储分段的任何默认保留设置。

您可以为每个对象指定以下设置：

- 保留模式：合规性或监管。
- *retain－until－date *：指定StorageGRID 必须保留对象版本多长时间的日期。
  - 在合规模式下、如果保留截止日期为未来日期、则可以检索对象、但无法修改或删除它。保留截止日期可以增加、但不能减少或删除此日期。
  - 在监管模式下、具有特殊权限的用户可以绕过保留截止日期设置。他们可以在对象版本的保留期限到期之前将其删除。它们还可以增加、减少甚至删除保留截止日期。
- * 合法保留 * ：对对象版本应用合法保留时，会立即锁定该对象。例如，您可能需要对与调查或法律争议相关的对象进行法律保留。合法保留没有到期日期，但在明确删除之前始终有效。

  对象的合法保留设置与保留模式和保留截止日期无关。如果某个对象版本处于合法保留状态、则任何人都无法删除该版本。

要在向存储分段添加对象版本时指定S3对象锁定设置，请发出"PutObject"、"CopyObject"或"CreateMultipartUpload"请求。

您可以使用以下命令：

- `x-amz-object-lock-mode`，可以是合规性或监管(区分大小写)。

  > 如果指定 `x-amz-object-lock-mode`，则还必须指定 `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
  - 保留截止日期值的格式必须为 `2020-08-10T21:46:00Z`。允许使用小数秒，但仅保留 3 位小数（精确度为毫秒）。不允许使用其他ISO 8601格式。
  - 保留截止日期必须为未来日期。
- `x-amz-object-lock-legal-hold`

  如果处于合法保留状态（区分大小写），则对象将置于合法保留状态。如果关闭了合法保留，则不会进行合法保留。任何其他值都会导致 400 错误请求（ InvalidArgument ）错误。

如果您使用上述任一请求标头，请注意以下限制：

- 如果 PutObject 请求中存在任何 x-amz-object-lock-* 请求标头，则必须包含以下请求标头之一：

```
Content-MD5
x-amz-checksum-*
```

这些标头不是 CopyObject 或 CreateMultipartUpload 所必需的。

- 如果存储桶未启用 S3 对象锁定并存在 x-amz-object-lock-* 请求标头，则返回 400 Bad Request (InvalidRequest) 错误。
- PutObject请求支持使用 `x-amz-storage-class: REDUCED_REDUNDANCY`匹配AWS行为。但是，如果在启用了 S3 对象锁定的情况下将对象载入存储分段，则 StorageGRID 将始终执行双提交载入。
- 如果配置了标题、和，并且请求发送者具有正确的权限，则 `s3:Get*`后续的`GET`或`HeadObject`版本响应将包括标题 `x-amz-object-lock-mode`、 `x-amz-object-lock-retain-until-date`和 `x-amz-object-lock-legal-hold`。

您可以使用 `s3:object-lock-remaining-retention-days`策略条件密钥来限制对象允许的最短和最长保留期限。

如何更新对象的保留设置

如果需要更新现有对象版本的合法保留或保留设置，可以执行以下对象子资源操作：

- `PutObjectLegalHold`

  如果新的合法保留值为 on ，则对象将置于合法保留状态。如果合法保留值为 off ，则取消合法保留。

- `PutObjectRetention`
  - 模式值可以是合规性或监管(区分大小写)。
  - 保留截止日期值的格式必须为 `2020-08-10T21:46:00Z`。允许使用小数秒，但仅保留 3 位小数（精确度为毫秒）。不允许使用其他ISO 8601格式。
  - 如果对象版本具有现有的保留日期，则只能增加此保留日期。新的价值必须是未来的。

必须在请求中指定以下请求标头之一：

```
Content-MD5
x-amz-checksum-*
```

StorageGRID 不验证这些操作的 x-amz-checksum-* 标头的内容。

如何使用监管模式

具有权限的用户 `s3:BypassGovernanceRetention`可以绕过使用监管模式的对象的活动保留设置。任何删除或PutObject保留 操作都必须包含 `x-amz-bypass-governance-retention:true`请求标头。这些用户可以执行以下附加操作：

- 执行DeleteObject或DeleteObjects操作以在对象保留期限到期之前删除该对象版本。

  无法删除处于合法保留状态的对象。合法保留必须关闭。

  The `x-amz-bypass-governance-retention` 标头对没有 S3 Object Lock 的对象无效。

- 执行PutObject锟 剁 操作、以便在对象的保留期限结束之前将对象版本的模式从监管更改为合规。

  绝不允许将模式从合规性更改为监管。

- 执行PutObject铻 刭 操作以增加、减少或删除对象版本的保留期限。

相关信息

- "使用 S3 对象锁定管理对象"
- "使用S3对象锁定保留对象"
- "《Amazon Simple Storage Service用户指南：锁定对象》"

了解 **StorageGRID** 的 **S3** 生命周期配置

您可以创建 S3 生命周期配置，以控制何时从 StorageGRID 系统中删除特定对象。

本节中的简单示例说明了 S3 生命周期配置如何控制从特定 S3 存储桶删除（过期）某些对象的时间。本节中的示例仅用于说明目的。有关创建 S3 生命周期配置的完整详细信息，请参阅 "Amazon Simple Storage Service 用户指南：管理对象的生命周期"。请注意，StorageGRID 仅支持到期操作；不支持过渡操作。

什么是生命周期配置

生命周期配置是一组应用于特定 S3 分段中的对象的规则。每个规则都指定受影响的对象以及这些对象的到期时间（在特定日期或一定天数后）。

StorageGRID 在一个生命周期配置中最多支持 1 ， 000 条生命周期规则。每个规则可以包含以下 XML 元素：

- 到期日期：从对象载入开始，在达到指定日期或达到指定天数时删除对象。
- NoncurrentVersionExpiration ：从对象变为非最新状态开始，在达到指定天数时删除对象。
- 筛选器（前缀，标记）
- 状态
- ID

每个对象都遵循S3存储分段生命周期或ILM策略的保留设置。配置S3存储分段生命周期后、对于与存储分段生命周期筛选器匹配的对象、生命周期到期操作将覆盖ILM策略。与存储分段生命周期筛选器不匹配的对象将使用ILM策略的保留设置。如果某个对象与存储分段生命周期筛选器匹配、并且未明确指定到期操作、则不会使用ILM策略的保留设置、这意味着对象版本将永久保留。请参阅。 "S3存储分段生命周期和ILM策略的优先级示例"

因此，即使 ILM 规则中的放置说明仍适用于某个对象，该对象也可能会从网格中删除。或者，即使对象的任何 ILM 放置指令已失效，该对象也可能会保留在网格中。有关详细信息，请参见 "ILM 如何在对象的整个生命周期内运行"。

> 存储分段生命周期配置可用于启用了 S3 对象锁定的存储分段，但旧版合规存储分段不支持存储分段生命周期配置。

StorageGRID 支持使用以下存储分段操作来管理生命周期配置：

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

作为创建生命周期配置的第一步，您需要创建一个包含一个或多个规则的 JSON 文件。例如，此 JSON 文件包含三个规则，如下所示：

1. 规则1仅适用于与前缀/匹配且 `key2`值为 `tag2`的对象 `category1`。`Expiration`参数用于指定与筛选器匹配的对象将在2020年8月22日午夜过期。
2. 规则2仅适用于与前缀/匹配的对象 `category2`。`Expiration`参数用于指定与筛选器匹配的对象将在其被加热100天后过期。

   > 指定天数的规则与对象的载入时间相关。如果当前日期超过载入日期加上天数，则在应用生命周期配置后，可能会立即从存储分段中删除某些对象。

3. 规则3仅适用于与前缀/匹配的对象 `category3`。`Expiration`参数用于指定任何非最新版本的匹配对象将在变为非最新状态50天后过期。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

将生命周期配置应用于存储分段

创建生命周期配置文件后、您可以通过发出PutBucketLifecycleConfiguration请求将其应用于存储分段。

此请求将示例文件中的生命周期配置应用于名为的分段中的对象 `testbucket`。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

要验证生命周期配置是否已成功应用于存储分段、请发送问题描述a GetBucketLifecycleConfiguration请求。例如：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功的响应将列出您刚刚应用的生命周期配置。

验证存储分段生命周期到期适用场景 对象

在发出PutObject、HeadObject或GetObject请求时、您可以确定生命周期配置适用场景中的到期规则是否为特定对象。如果规则适用、则响应会包含一个 `Expiration`参数、用于指示对象何时到期以及匹配了哪个到期规则。

> 由于存储分段生命周期会覆盖ILM、因此 `expiry-date`显示的是要删除对象的实际日期。有关详细信息，请参见 "如何确定对象保留"。

例如、此PutObject请求是在2020年6月22日发出的、并将对象放置在存储分段中 `testbucket`。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功响应表示此对象将在 100 天后（ 2020 年 10 月 1 日）过期，并且与生命周期配置的规则 2 匹配。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

例如、此HeadObject请求用于获取testb分 段中同一对象的元数据。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功响应包括对象的元数据，并指示对象将在 100 天后过期，并且与规则 2 匹配。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

对于启用了版本控制的分段、 `x-amz-expiration`响应标头仅适用于当前版本的对象。

使用 **StorageGRID** 实施 **S3 REST API** 的建议

在实施用于 StorageGRID 的 S3 REST API 时，应遵循以下建议。

针对不存在的对象的建议

如果您的应用程序定期检查某个对象是否存在于您认为该对象实际上不存在的路径中，则应使用“可用”"一致性"。例如，如果您的应用程序在 PUT 之前 HEAD 某个位置，则您应该使用“可用”一致性。

否则、如果HEAD操作未找到对象、则在同一站点上的两个或更多存储节点不可用或某个远程站点不可访问时、您可能会收到大量500个内部服务器错误。

您可以使用请求为每个存储分段设置"可用"一致性"PUT 存储分段一致性"、也可以在单个API操作的请求标头中指定一致性。

对象密钥建议

根据首次创建分段的时间、请遵循这些对象键名建议。

在**StorageGRID 11.4**或更早版本中创建的分段

- 不要使用随机值作为对象键的前四个字符。这与 AWS 以前针对密钥前缀的建议不同。请改用非随机、非唯一的前缀，如 `image`。
- 如果按照以前的AWS建议在密钥前缀中使用随机和唯一字符、请在对象密钥前添加目录名称。也就是说，请使用以下格式：

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  而不是以下格式：

```
mybucket/f8e3-image3132.jpg
```

在**StorageGRID 11.4**或更高版本中创建的分段

不需要限制对象密钥名称以满足性能最佳实践。在大多数情况下、对象密钥名称的前四个字符可以使用随机值。

> 但S3工作负载例外、它会在短时间后持续删除所有对象。为了最大限度地降低此使用情形对性能的影响、请每隔数千个对象更改一次密钥名称的前导部分、并使用日期之类的内容。例如、假设S3客户端通常每秒写入2、000个对象、而ILM或存储分段生命周期策略将在三天后删除所有对象。为了最大限度地降低对性能的影响、您可以使用如下模式命名密钥：
>
> `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

"范围读取"建议

如果"用于压缩存储对象的全局选项"已启用、S3客户端应用程序应避免执行指定要返回的字节数范围的GetObject操作。这些"范围读取"操作效率低下、因为StorageGRID必须有效地解压缩对象才能访问请求的字节。从非常大的对象请求少量字节的GetObject操作效率特别低；例如、从50 GB压缩对象读取10 MB的范围是效率低下的。

如果从压缩对象读取范围，则客户端请求可能会超时。

> 如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

支持Amazon S3 REST API

StorageGRID 中 **S3 REST API** 支持的操作和限制

StorageGRID 系统实施简单存储服务 API （API 版本 2006-03-01 ），支持大多数操作，但有一些限制。在集成 S3 REST API 客户端应用程序时，您需要了解实施详细信息。

StorageGRID 系统支持虚拟托管风格的请求和路径风格的请求。

日期处理

S3 REST API 的 StorageGRID 实施仅支持有效的 HTTP 日期格式。

对于接受日期值的任何标头， StorageGRID 系统仅支持有效的 HTTP 日期格式。日期的时间部分可以使用格林威治标准时间（ GMT ）格式或通用协调时间（ UTC ）格式指定，并且不存在时区偏移（必须指定 +0000 ）。如果您在请求中包括 `x-amz-date`标题，则它将覆盖在“日期请求”标题中指定的任何值。使用AWS签名版本4时、 `x-amz-date`由于不支持日期标头、因此签名请求中必须存在标头。

通用请求标头

StorageGRID系统支持由定义的通用请求标头 "Amazon Simple Storage Service API参考：通用请求标头"，但有一个例外。

请求标题	实施
Authorization	完全支持 AWS 签名版本 2 支持 AWS 签名版本 4 ，但以下情况除外： • 在中提供实际有效负载校验和值时 `x-amz-content-sha256`，该值将被接受而不进行验证，就像为标头提供了该值一样 `UNSIGNED-PAYLOAD`。如果您提供的 `x-amz-content-sha256`标头值表示 `aws-chunked`流式传输(例如、STAVAMMA-AWS4-HMAC-SHA256-payload)、则不会根据区块数据验证区块签名。

通用响应标头

StorageGRID 系统支持由 _Simple Storage Service API 参考 _ 定义的所有通用响应标头，但有一个例外。

响应标头	实施
X-AMZ-ID-2	未使用

StorageGRID S3 REST API 如何验证请求

StorageGRID 系统支持使用 S3 API 对对象进行身份验证和匿名访问。

S3 API 支持签名版本 2 和签名版本 4 对 S3 API 请求进行身份验证。

经过身份验证的请求必须使用您的访问密钥 ID 和机密访问密钥进行签名。

StorageGRID系统支持两种身份验证方法：HTTP `Authorization`标头和使用查询参数。

使用 **HTTP** 授权标头

HTTP `Authorization`标头由所有S3 API操作使用、但在存储分段策略允许的情况下匿名请求除外。`Authorization`标头包含对请求进行身份验证所需的所有签名信息。

使用查询参数

您可以使用查询参数向 URL 添加身份验证信息。这称为对 URL 进行预签名，可用于授予对特定资源的临时访问权限。具有预先签名URL的用户无需知道访问资源的机密访问密钥、这样您就可以为资源提供第三方受限访问权限。

StorageGRID 中支持的服务操作

StorageGRID 系统支持对该服务执行以下操作。

操作	实施
List桶 (以前称为GET服务)	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。

操作	实施
获取存储使用量	StorageGRID"获取存储使用量"请求会告知您某个帐户以及与该帐户关联的每个存储分段使用的总存储量。这是对服务执行的操作，其路径为/，并(`?x-ntap-sg-usage`添加了自定义查询参数)。
选项 /	客户端应用程序可以向存储节点上的S3端口发出 `OPTIONS /`请求、而无需提供S3身份验证凭据、从而确定存储节点是否可用。您可以使用此请求进行监控，也可以允许外部负载平衡器确定存储节点何时关闭。

StorageGRID 中的 **S3** 存储桶操作和实施详细信息

StorageGRID 系统为每个 S3 租户帐户最多支持 20,000 个存储桶。

每个网格最多可以包含100、000个分段。

如果多个租户每个都有多达 5,000 个存储桶，则网格中的每个存储节点必须至少有 64 GB 的 RAM。

存储桶名称限制遵循 AWS US Standard 区域限制，但应进一步将其限制为 DNS 命名约定，以支持 S3 虚拟托管风格的请求。

有关详细信息，请参见以下内容：

- "《Amazon Simple Storage Service用户指南：存储分段配额、限制和限制》"
- "配置S3端点域名"

ListObjects（获取 Bucket）和 ListObjectVersions（获取 Bucket 对象版本）操作支持StorageGRID"一致性值"。

您可以检查是否为单个存储区启用或禁用了对上次访问时间的更新。请参阅 "获取存储分段上次访问时间"。

下表介绍了 StorageGRID 如何实施 S3 REST API 存储分段操作。要执行其中任何操作，必须为帐户提供必要的访问凭据。

操作	实施
CreateBucket	创建新存储分段。创建存储分段后，您就会成为存储分段所有者。 注意：不支持 S3 目录存储桶。 • 存储分段名称必须符合以下规则： ◦ 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。 ◦ 必须符合 DNS 要求。 ◦ 必须包含至少3个且不超过63个字符。 ◦ 可以是一个或多个标签的序列，并使用一个句点分隔相邻标签。每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母，数字和连字符。 ◦ 不能与文本格式的 IP 地址类似。 ◦ 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。 • 默认情况下，分段是在区域中创建的 `us-east-1`；但是，您可以在请求正文中使用 `LocationConstraint`请求元素来指定其他区域。使用元素时 `LocationConstraint`、必须指定已使用网格管理器或网格管理API定义的区域的确切名称。如果您不知道应使用的区域名称、请联系您的系统管理员。 注意：如果您的 CreateBucket 请求使用的区域尚未在 StorageGRID 中定义，则会发生错误。 • 您可以包含 `x-amz-bucket-object-lock-enabled`请求标头以创建启用了 S3 Object Lock 的存储桶。请参阅"使用S3 REST API配置S3对象锁定"。 S3 Object Lock 需要存储桶版本控制，在创建启用了 S3 Object Lock 的存储桶时会自动启用。 您可以在创建存储桶时或稍后启用 S3 Object Lock。
DeleteBucket	删除存储分段。
DeleteBucketCors	删除存储分段的CORS配置。
DeleteBucketEncryption	从存储分段中删除默认加密。现有加密对象将保持加密状态、但添加到存储分段的任何新对象不会加密。
DeleteBucketLifecycle	从存储桶中删除生命周期配置。请参阅"创建 S3 生命周期配置"。
DeleteBucketPolicy	删除附加到存储分段的策略。
DeleteBucketReplication	删除附加到存储分段的复制配置。

操作	实施
DeleteBucketTbaging	使用 `tagging`子资源从存储分段中删除所有标记。 注意：如果为此存储桶设置了非默认 ILM 策略标记，则将存在一个分配了值的 `NTAP-SG-ILM-BUCKET-TAG`存储桶标记。如果有 `NTAP-SG-ILM-BUCKET-TAG`存储桶标记，请勿发出 DeleteBucketTagging 请求。相反，仅使用 `NTAP-SG-ILM-BUCKET-TAG`标记及其分配的值发出 PutBucketTagging 请求，以从存储桶中删除所有其他标记。请勿修改或删除 `NTAP-SG-ILM-BUCKET-TAG`存储桶标记。
GetBucketAcl	返回肯定响应以及存储分段所有者的ID、DisplayName和权限、指示所有者对存储分段具有完全访问权限。
GetBucketCors	返回 `cors`存储分段的配置。
GetBucketEncryption	返回存储分段的默认加密配置。
GetBucketLifecycleConfiguration (以前称为GET分段生命周期)	返回存储区的生命周期配置。请参阅 "创建 S3 生命周期配置"。
GetBucketLocation	返回使用 `LocationConstraint` 元素在 CreateBucket 请求中设置的区域。如果存储桶的区域为 `us-east-1`（默认），则会为 `LocationConstraint` 返回空值。
GetBucketNotizationConfiguration (以前称为GET分段通知)	返回附加到存储分段的通知配置。
GetBucketPolicy	返回附加到存储分段的策略。
GetBucketReplication	返回附加到存储分段的复制配置。
GetBucketTaging	使用 `tagging`子资源返回存储分段的所有标记。 注意：如果为此存储桶设置了非默认 ILM 策略标记，则将存在一个 `NTAP-SG-ILM-BUCKET-TAG`存储桶标记，并为其分配了值。请勿修改或删除此标签。
GetBucketVersioning	此实现使用 `versioning`子资源返回存储分段的版本控制状态。 • *blank*：从未启用版本控制(分段已"取消版本控制") • Enabled ： 已启用版本控制 • suspended ： 先前已启用版本控制并已暂停

操作	实施
GetObjectLockConfiguration	返回存储分段默认保留模式和默认保留期限(如果已配置)。 请参阅 "使用S3 REST API配置S3对象锁定"。
HeadBucket	确定存储分段是否存在、以及您是否有权访问该存储分段。 此操作将返回： • `x-ntap-sg-bucket-id`：UUID格式的存储分段的UUID。 • `x-ntap-sg-trace-id`：关联请求的唯一跟踪ID。
ListObjects和ListObjectsV2 (以前称为GET分段)	返回分段中的部分或全部对象(最多1、000个)。对象的存储类可以具有两个值之一、即使对象是使用存储类选项获取的也是 `REDUCED_REDUNDANCY`如此： • `STANDARD`，表示对象存储在由存储节点组成的存储池中。 • `GLACIER`，表示对象已移至云存储池指定的外部存储分段。 如果存储分段包含大量具有相同前缀的已删除密钥、则响应可能包含一些`CommonPrefixes`不包含密钥的密钥。 对于 HeadObject 和 ListObject 请求， StorageGRID返回具有不同精度的 LastModified 时间戳，而 AWS 返回具有相同精度的时间戳，如以下示例所示： • StorageGRID HeadObject：“LastModified”：“2024-09-26T16：43：24 + 00：00” • StorageGRID ListObject：“LastModified”：“2024-09-26T16：43：24.931000 + 00：00” • AWS HeadObject：“LastModified”：“2023-10-17T00：19：54 + 00：00” • AWS ListObject：“LastModified”：“2023-10-17T00：19：54 + 00：00”
ListObjectVersies (以前称为Get BucketObject Version)	如果对存储分段具有读取访问权限、则对子资源使用此操作 `versions`可列出存储分段中所有版本对象的元数据。
PutBucketCors	设置存储分段的CORS配置、以便存储分段可以处理跨源站请求。跨源资源共享（CORS）是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如、假设您使用名为的S3存储分段 `images`来存储图形。通过设置存储分段的CORS配置 `images`，您可以允许该存储分段中的图像显示在网站上 `http://www.example.com`。

操作	实施
PutBucketEncryption	设置现有存储分段的默认加密状态。启用存储分段级别加密后，添加到存储分段中的任何新对象都会进行加密。 StorageGRID 支持使用 StorageGRID 管理的密钥进行服务器端加密。指定服务器端加密配置规则时，请将参数设置 `SSEAlgorithm` 为 `AES256`，而不要使用 `KMSMasterKeyID`参数。 如果对象上传请求已指定加密(即、如果请求包含请求标头)、则会忽略存储分段默认加密配置 `x-amz-server-side-encryption-*`。
PutBucketLifecycleConfiguration (以前称为"放置分段生命周期")	为存储分段创建新的生命周期配置或替换现有生命周期配置。StorageGRID 在一个生命周期配置中最多支持 1 ， 000 条生命周期规则。每个规则可以包含以下 XML 元素： • 到期日期(天数、日期、ExpireObjectDeleteMarker) • 非当前版本到期(新非当前版本、非当前日期) • 筛选器（前缀，标记） • 状态 • ID StorageGRID 不支持以下操作： • AbortIncompleteMultipartUpload • 过渡 请参阅"创建 S3 生命周期配置"。要了解存储桶生命周期中的到期操作如何与 ILM 放置说明交互，请参阅"ILM 如何在对象的整个生命周期内运行"。 • 注 * ：存储分段生命周期配置可用于启用了 S3 对象锁定的存储分段，但传统合规存储分段不支持存储分段生命周期配置。

操作	实施

PutBucketNotizationConfiguration
 	
(以前称为Put Bucket"通知)
	使用请求正文中包含的通知配置XML配置分段的通知。您应了解以下实施详细信息：
	
	• StorageGRID支持 Amazon Simple Notification Service (Amazon SNS) 主题、Kafka 主题或 webhook 端点作为目的地。不支持简单队列服务 (SQS) 或 AWS Lambda 端点。
	• 必须将通知目标指定为 StorageGRID 端点的 URN 。可以使用租户管理器或租户管理 API 创建端点。
	
	要成功配置通知，端点必须存在。如果端点不存在， `400 Bad Request`则返回错误代码 `InvalidArgument`。
	
	• 您不能为以下事件类型配置通知。这些事件类型 * 不 * 受支持。
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• 从StorageGRID 发送的事件通知使用标准JSON格式、不同之处在于它们不包含某些密钥、而对其他密钥使用特定值、如以下列表所示：
	◦ * 事件源 *
	
	`sgws:s3`
	
	◦ * awsRegion*
	
	不包括
	
	◦ * 。 x-AMZ-id-2*
	
	不包括
	
	◦ * arn*
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	设置附加到存储桶的策略。请参阅 "使用存储分段和组访问策略"。

操作	实施
PutBucketReplication	使用请求正文中提供的复制配置"StorageGRID CloudMirror复制"XML配置存储分段。对于 CloudMirror 复制，您应了解以下实施详细信息： • StorageGRID 仅支持复制配置的 V1。这意味着 StorageGRID 不支持对规则使用 `Filter`元素，并遵循 V1 约定删除对象版本。有关详细信息，请参阅 "《Amazon Simple Storage Service用户指南：复制配置》"。 • 分段复制可以在分版本或未分版本的分段上配置。 • 您可以在复制配置 XML 的每个规则中指定不同的目标存储分段。一个源存储分段可以复制到多个目标存储分段。 • 目标存储桶必须指定为租户管理器或租户管理 API 中指定的 StorageGRID 终结点的 URN。请参阅 "配置 CloudMirror 复制"。 要成功进行复制配置，必须存在此端点。如果端点不存在，则请求将作为失败 `400 Bad Request`。错误消息指出： `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • 您无需在配置XML中指定 `Role`。StorageGRID 不使用此值，如果提交，则会忽略此值。 • 如果在配置XML中省略该存储类、则默认情况下、StorageGRID将使用该 `STANDARD`存储类。 • 如果从源存储分段中删除对象或删除源存储分段本身，则跨区域复制行为如下： ◦ 如果在复制对象或存储分段之前将其删除、则不会复制该对象或存储分段、也不会通知您。 ◦ 如果您在复制对象或存储分段后将其删除，则 StorageGRID 会对跨区域复制的 V1 遵循标准 Amazon S3 删除行为。
PutBucketTaging	使用 `tagging`子资源为存储分段添加或更新一组标记。添加存储分段标记时，请注意以下限制： • StorageGRID 和 Amazon S3 为每个存储分段最多支持 50 个标签。 • 与存储分段关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可包含 128 个 Unicode 字符。 • 标记值的长度最多可以为 256 个 Unicode 字符。 • 密钥和值区分大小写。 注意：如果为此存储桶设置了非默认 ILM 策略标记，则将存在一个 `NTAP-SG-ILM-BUCKET-TAG`存储桶标记，并为其分配了值。确保在所有 PutBucketTagging 请求中包含带有分配值的 `NTAP-SG-ILM-BUCKET-TAG`存储桶标记。请勿修改或删除此标记。 注意：此操作将覆盖存储分段已有的任何当前标记。如果在集合中省略了任何现有标记、则会删除存储分段中的这些标记。

操作	实施
PutBucketVersioning	使用 `versioning`子资源设置现有存储分段的版本控制状态。您可以使用以下值之一设置版本控制状态： • Enabled ： 为存储分段中的对象启用版本控制。添加到存储分段中的所有对象都会收到唯一的版本 ID 。 • suspended ： 为存储分段中的对象禁用版本控制。添加到存储分段的所有对象都会收到版本ID `null`。
PutObjectLockConfiguration	• 配置或删除存储分段默认保留模式和默认保留期限。 • 如果网格管理员已授予权限，则在现有存储桶上启用 S3 对象锁定。 如果修改了默认保留期限，现有对象版本的 retain-until-date 将保持不变，并且不会使用新的默认保留期限重新计算。 有关详细信息，请参见 "使用S3 REST API配置S3对象锁定"。

对对象执行的操作

StorageGRID 如何实现对象的 **S3 REST API** 操作

本节介绍 StorageGRID 系统如何对对象实施 S3 REST API 操作。

以下条件适用于所有对象操作：

- StorageGRID"一致性值"所有对象操作均支持，但以下操作除外：
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObject保留
  - SelectObjectContent
- 冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。
- StorageGRID 存储分段中的所有对象均归存储分段所有者所有，包括由匿名用户或其他帐户创建的对象。

下表介绍了 StorageGRID 如何实施 S3 REST API 对象操作。

操作	实施
DeleteObject	处理DeleteObject请求时、StorageGRID会尝试立即从所有存储位置删除对象的所有副本。如果成功， StorageGRID 会立即向客户端返回响应。如果无法在30秒内删除所有副本(例如、由于某个位置暂时不可用)、则StorageGRID 会将这些副本排队等待删除、然后向客户端指示删除成功。 限制 • 不支持多因素身份验证(MFA)和响应标头 `x-amz-mfa`。 • `If-Match`和 `If-None-Match`标头的行为因您的 StorageGRID 配置而异。提供这些标头可能会返回错误消息（501 Not Implemented）。如果 `If-Match`或 `If-None-Match`标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。 The `x-amz-bypass-governance-retention` 标头对没有 S3 Object Lock 的对象无效。 版本控制 要删除特定版本、此应用程序必须是存储分段所有者并使用 `versionId`子资源。使用此子资源将永久删除此版本。如果 `versionId`对应于删除标记，则返回的响应标头 `x-amz-delete-marker`将设置为 `true`。 • 如果在启用了版本控制的存储分段上删除对象时未显示 `versionId`子资源、则会生成删除标记。使用响应标头返回删除标记 `x-amz-version-id`的， `versionId`并将 `x-amz-delete-marker`响应标头设置为 `true`。 • 如果删除的对象没有分段上的子资源、而 `versionId`版本控制已暂停、则会永久删除已有的"`null`"版本或"`null`"删除标记、并生成新的"`null`"删除标记。 `x-amz-delete-marker`返回的响应标头设置为 `true`。 • 注意 * ：在某些情况下，一个对象可能存在多个删除标记。 请参见"使用S3 REST API配置S3对象锁定"、了解如何在监管模式下删除对象版本。
DeleteObjects (以前称为删除多个对象)	不支持多因素身份验证(MFA)和响应标头 `x-amz-mfa`。 可以在同一请求消息中删除多个对象。 The `x-amz-bypass-governance-retention` 标头对没有 S3 Object Lock 的对象无效。 请参见"使用S3 REST API配置S3对象锁定"、了解如何在监管模式下删除对象版本。

操作	实施
DeleteObjectTagging	使用 `tagging`子资源从对象中删除所有标记。 版本控制 如果 `versionId`未在请求中指定查询参数、则此操作将从受版本控制的分段中的对象的最新版本中删除所有标记。如果对象的当前版本是删除标记，则返回"方法NotAllowed"状态，并 `x-amz-delete-marker`将响应标头设置为 `true。
GetObject	"GetObject"
GetObjectAcl	如果为帐户提供了必要的访问凭据，则此操作将返回肯定响应以及对象所有者的 ID ， DisplayName 和权限，指示所有者对对象具有完全访问权限。
GetObjectLegalHold	"使用S3 REST API配置S3对象锁定"
GetObject保留	"使用S3 REST API配置S3对象锁定"
GetObjectTagging	使用 `tagging`子资源返回对象的所有标记。 版本控制 如果 `versionId`未在请求中指定查询参数、则此操作将返回受版本控制的分段中对象的最新版本中的所有标记。如果对象的当前版本是删除标记，则返回"方法NotAllowed"状态，并 `x-amz-delete-marker`将响应标头设置为 `true。
HeadObject	"HeadObject"
RestorEObject	"RestorEObject"
PutObject	"PutObject"
CopyObject (以前称为Put Object - Copy)	"CopyObject"
PutObjectLegalHold	"使用S3 REST API配置S3对象锁定"
PutObject保留	"使用S3 REST API配置S3对象锁定"

操作	实施
PutObjectTagging	使用 `tagging`子资源向现有对象添加一组标记。 对象标记限制 您可以在上传新对象时为其添加标记，也可以将其添加到现有对象中。StorageGRID 和 Amazon S3 对每个对象最多支持 10 个标记。与对象关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可以是 128 个 Unicode 字符，而标记值的长度最多可以是 256 个 Unicode 字符。密钥和值区分大小写。 标记更新和加热行为 使用PutObjectTags更新对象的标记时、StorageGRID不会重新加载对象。这意味着不会使用匹配 ILM 规则中指定的 " 载入行为 " 选项。通过正常后台 ILM 进程重新评估 ILM 时，更新触发的任何对象放置更改都会进行。 这意味着、如果ILM规则使用stricting选项执行加数据操作、则在无法放置所需对象(例如、新需要的位置不可用)时不会执行任何操作。更新后的对象会保留其当前位置，直到可以进行所需的位置为止。 解决冲突 冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。 版本控制 如果 `versionId`未在请求中指定查询参数、则此操作会将标记添加到受版本控制的分段中对象的最新版本。如果对象的当前版本是删除标记，则返回"方法`NotAllowed`"状态，并 `x-amz-delete-marker`将响应标头设置为 `true`。
SelectObjectContent	"SelectObjectContent"

StorageGRID 中支持的 **Amazon S3 Select** 操作

StorageGRID支持的以下Amazon S3 Select子句、数据类型和运算符"SelectObjectContent 命令"。

不支持未列出的任何项目。

有关语法，请参见"SelectObjectContent"。有关S3 Select的详细信息，请参见 "适用于 S3 Select 的 AWS 文档"。

只有启用了 S3 Select 的租户帐户才能进行问题描述 SelectObjectContent 查询。请参见"使用 S3 Select 的注意事项和要求"。

条款

- 选择列表
- from 子句
- Where 子句
- Limit 子句

数据类型

- 池
- 整型
- string
- 浮动
- 小数点，数字
- timestamp

运算符

逻辑运算符

- 和
- 不是
- 或

比较运算符

- <
- >
- &lt； =
- &gt； =
- =
- =
- <>
- ！ =
- 介于之间
- 在中

模式匹配运算符

- 例如
- _
- %

统一运算符

- 为空
- 不为空

数学运算符

- +
- -
- *
- /
- %

StorageGRID 遵循Amazon S3 Select操作员优先级。

聚合函数

- 平均（）
- 计数（ * ）
- 最大值（）
- 最小值（）
- sum（ ）

条件函数

- 案例
- 合并
- NULLIF

转换函数

- cast （用于受支持的数据类型）

date 函数

- 日期添加
- 日期差异
- 提取
- to_string
- to_timestamp
- UTCNOW

字符串函数

- char_length ， character_length
- 更低
- 子字符串
- 剪切
- 上限

StorageGRID 如何使用服务器端加密

服务器端加密可用于保护空闲对象数据。StorageGRID 会在写入对象时对数据进行加密，并在您访问对象时对数据进行解密。

如果要使用服务器端加密，可以根据加密密钥的管理方式从两个互斥选项中选择任一选项：

- *SSE （使用 StorageGRID 管理的密钥进行服务器端加密） *：在问题描述 S3 请求以存储对象时，StorageGRID 会使用唯一密钥对对象进行加密。在问题描述 S3 请求以检索对象时， StorageGRID 会使用存储的密钥对对象进行解密。
- * SSI-C （使用客户提供的密钥进行服务器端加密） *：在问题描述 S3 请求以存储对象时，您可以提供自己的加密密钥。检索对象时，您可以在请求中提供相同的加密密钥。如果这两个加密密钥匹配，则会对对象进行解密，并返回您的对象数据。

  虽然 StorageGRID 负责管理所有对象加密和解密操作，但您必须管理提供的加密密钥。

  > 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。

  > 如果使用 SSE 或 SSI-C 对对象进行加密，则会忽略任何分段级别或网格级别的加密设置。

使用 **SS**

要使用 StorageGRID 管理的唯一密钥对对象进行加密，请使用以下请求标头：

```
x-amz-server-side-encryption
```

以下对象操作支持此命令头：

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

使用 **SSI-C**

要使用您管理的唯一密钥对对象进行加密，请使用三个请求标头：

请求标题	说明
`x-amz-server-side-encryption-customer-algorithm`	指定加密算法。标题值必须为 `AES256`。
`x-amz-server-side-encryption-customer-key`	指定用于对对象进行加密或解密的加密密钥。密钥的值必须为 256 位 base64 编码。
`x-amz-server-side-encryption-customer-key-MD5`	根据 RFC 1321 指定加密密钥的 MD5 摘要，用于确保加密密钥的传输没有错误。MD5 摘要的值必须为 base64 编码的 128 位。

以下对象操作支持 SSI-C 请求标头：

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "上传部件"
- "上传PartCopy"

将服务器端加密与客户提供的密钥（ **SSI-C** ）结合使用的注意事项

在使用 SSI-C 之前，请注意以下注意事项：

- 必须使用 https 。

> 使用SSE-C时、StorageGRID会拒绝通过http发出的任何请求。出于安全考虑、您应考虑损坏使用http意外发送的任何密钥。丢弃该密钥，并根据需要旋转。

- 响应中的 ETag 不是对象数据的 MD5 。
- 您必须管理加密密钥到对象的映射。StorageGRID 不存储加密密钥。您负责跟踪为每个对象提供的加密密钥。
- 如果您的存储分段已启用版本控制，则每个对象版本都应具有自己的加密密钥。您负责跟踪每个对象版本使用的加密密钥。
- 由于您在客户端上管理加密密钥，因此您还必须在客户端上管理任何其他保护措施，例如密钥轮换。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。

- 如果为存储分段配置了跨网格复制或CloudMirror复制、则无法加载SSE-C对象。载入操作将失败。

相关信息

"Amazon S3用户指南：使用客户提供的密钥进行服务器端加密(SSE-C)"

您可以使用S3 CopyObject请求为已存储在S3中的对象创建副本。CopyObject操作与依次执行GetObject和PutObject相同。

解决冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

对象大小

一个PutObject操作的最大_Recommended_大小为5 GiB (5、368、709、120字节)。如果您的对象大于5 GiB、请改用"多部分上传"。

一个PutObject操作的最大_supported_大小为5 TiB (5、497、555、138、880字节)。

> 如果您从StorageGRID 11.5或更早版本升级、则在尝试上传超过5 GiB的对象时、将触发S3 Put Object Size Too Liger警报。如果您全新安装了StorageGRID 11.7或11.7、则在这种情况下不会触发警报。但是、为了符合AWS S3标准、未来版本的StorageGRID不支持上传超过5 GiB的对象。

用户元数据中的 **UTF-8** 字符

如果某个请求在用户定义的元数据的密钥名称或值中包含（未转义） UTF-8 值，则会未定义 StorageGRID 行为。

StorageGRID 不解析或解释用户定义元数据的键名或值中包含的转义 UTF-8 字符。转义 UTF-8 字符被视为 ASCII 字符：

- 如果用户定义的元数据包含转义的 UTF-8 字符，则请求将成功。
- 如果键名称或值的解释值包含不可打印的字符，StorageGRID 不会返回 `x-amz-missing-meta`标头。

支持的请求标头

支持以下请求标头：

- `Content-Type`
- `x-amz-checksum-algorithm`：指定 `CRC32`、 `CRC32C`、 `CRC64NVME`或 `SHA256`

  复制对象时，如果源对象具有 `checksum`或包含 `x-amz-checksum-algorithm`，则复制的对象具有 FULL_OBJECT 校验和。

  如果源对象具有校验和，但请求不包括 `x-amz-checksum-algorithm`或它使用不受支持的校验和值，则复制的对象与源对象具有相同类型的校验和。StorageGRID 忽略无效或不受支持的 `x-amz-checksum-algorithm`值。

  如果源对象没有校验和，并且没有包含 `x-amz-checksum-algorithm`或使用不受支持的校验和值，则复制对象没有校验和。

如果 CopyObject 请求未指定校验和，并且源对象没有校验和，则 StorageGRID 不会计算对象的默认 CRC-64/NVME 校验和。

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`，后跟一个包含用户定义的元数据的名称-值对
- `x-amz-metadata-directive`：默认值为 `COPY`，可用于复制对象和关联元数据。

  您可以指定 `REPLACE`在复制对象时覆盖现有元数据、或者更新对象元数据。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：默认值为 `COPY`，可用于复制对象和所有标记。

  您可以指定 `REPLACE`在复制对象时覆盖现有标记、或者更新标记。

- S3 对象锁定请求标头：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果在发出请求时没有这些标头、则会使用存储分段默认保留设置来计算对象版本模式和保留截止日期。请参阅。 "使用S3 REST API配置S3对象锁定"

- SSA 请求标头：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    请参见 [服务器端加密的请求标头]

请求标头不受支持

不支持以下请求标头：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

  根据您的 StorageGRID 配置， If-Match 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 If-Match 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。

- If-None-Match

  根据您的 StorageGRID 配置， If-None-Match 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 If-None-Match 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。

- x-amz-website-redirect-location

存储类选项

`x-amz-storage-class`如果匹配的ILM规则使用link:../ilm/data-protection-options-for-ingest.html[""INGest"选项"]"双提交"或"已平衡"，则请求标头受支持，并会影响StorageGRID创建的对象副本数。

- STANDARD

  （默认）指定在 ILM 规则使用双提交选项或 balanced-option 回退到创建中间副本时执行双提交载入操作。

- REDUCED_REDUNDANCY

  指定在 ILM 规则使用双提交选项或 balanced-option 回退为创建中间副本时执行单提交载入操作。

  如果在启用了S3对象锁定的情况下将对象导入存储分段、则会忽略此`REDUCED_REDUNDANCY`选项。如果要将对象移入旧的兼容存储分段、则此`REDUCED_REDUNDANCY`选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

在**CopyObject**中使用**x-AMZ-copy-source**

如果标题中指定的源分段和密钥 `x-amz-copy-source`与目标分段和密钥不同、则会将源对象数据的副本写入目标。

如果源和目标匹配，并且 x-amz-metadata-directive`标头指定为 `REPLACE，则会使用请求中提供的元数据值更新对象的元数据。在此情况下，StorageGRID 不会重新载入对象。这有两个重要后果：

- 不能使用CopyObject原位加密现有对象、也不能更改原位现有对象的加密。如果提供 x-amz-server-

side-encryption`标题或 `x-amz-server-side-encryption-customer-algorithm`标题，StorageGRID将拒绝请求并返回 `XNotImplemented。

- 未使用匹配的 ILM 规则中指定的导入行为选项。当正常后台 ILM 流程重新评估 ILM 时，将对更新触发的对象放置进行任何更改。

  这意味着、如果ILM规则使用stricting选项执行加数据操作、则在无法放置所需对象(例如、新需要的位置不可用)时不会执行任何操作。更新后的对象会保留其当前位置，直到可以进行所需的位置为止。

服务器端加密的请求标头

如果是"使用服务器端加密"，则提供的请求标头取决于源对象是否已加密以及是否计划对目标对象进行加密。

- 如果源对象使用客户提供的密钥(SSE-C)进行加密、则必须在CopyObject请求中包含以下三个标头、以便可以对该对象进行解密、然后进行复制：
  - x-amz-copy-source-server-side-encryption-customer-algorithm：指定 AES256。
  - x-amz-copy-source-server-side-encryption-customer-key：指定创建源对象时提供的加密密钥。
  - x-amz-copy-source-server-side-encryption-customer-key-MD5：指定创建源对象时提供的MD5摘要。
- 如果要使用您提供和管理的唯一密钥对目标对象（副本）进行加密，请包含以下三个标题：
  - x-amz-server-side-encryption-customer-algorithm：指定 AES256。
  - x-amz-server-side-encryption-customer-key：为目标对象指定新的加密密钥。
  - x-amz-server-side-encryption-customer-key-MD5：指定新加密密钥的MD5摘要。

  > 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看的注意事项"使用服务器端加密"。

- 如果要使用由StorageGRID (SSE)管理的唯一密钥对目标对象(副本)进行加密，请在CopyObject请求中包括此标头：
  - x-amz-server-side-encryption

  > server-side-encryption`无法更新此对象的值。而是使用： `REPLACE`创建具有新值的 `x-amz-metadata-directive`副本 `server-side-encryption。

版本控制

如果源分段已进行版本控制、则可以使用 x-amz-copy-source`标题复制对象的最新版本。要复制对象的特定版本，必须明确指定使用子资源复制的版本 `versionId。如果目标分段已进行版本控制、则生成的版本将返回到响应标头中 x-amz-version-id。如果暂停目标存储分段的版本控制、则 `x-amz-version-id`返回"null"值。

使用 **GetObject** 请求从 **StorageGRID** 中的存储桶检索对象

您可以使用S3 GetObject请求从S3存储分段中检索对象。

GetObject和多部分对象

您可以使用 `partNumber`request参数检索多部分或分段对象的特定部分。 `x-amz-mp-parts-count`响应元素指示对象有多少个零件。

分段/多部分对象和非分段/非多部分对象均可设置 `partNumber`为1；但是、 `x-amz-mp-parts-count`仅为分段或多部分对象返回响应元素。

用户元数据中的 UTF-8 字符

StorageGRID 不会解析或解释用户定义的元数据中的转义 UTF-8 字符。如果密钥名称或值包含不可打印字符、则对用户定义的元数据中具有转义UTF-8字符的对象的获取请求不会返回 `x-amz-missing-meta`标题。

支持的请求标头

支持以下请求标头：

- `Accept-Encoding`

  当对象没有存储的 `Content-Encoding`时，带有 `Accept-Encoding: gzip`的 `GET` 请求会对响应实时应用压缩。只有 `gzip`会影响 `GET` 响应编码； `deflate`、 `br`和 `identity`不会影响。对于已存储 `Content-Encoding`的对象，StorageGRID 返回存储的编码，不会基于 `Accept-Encoding`应用额外的实时压缩。StorageGRID 不支持带有 `Accept-Encoding: gzip`的 GET 请求的范围读取操作。

- `x-amz-checksum-mode`：请指定 `ENABLED`

  GetObject不支持此 `Range`标题 `x-amz-checksum-mode`。如果在请求中包含 `Range`并 `x-amz-checksum-mode`启用、则StorageGRID不会在响应中返回校验和值。

请求标头不受支持

不支持以下请求标头并返回 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本控制

如果 `versionId`未指定子资源、则此操作将提取受版本控制的分段中对象的最新版本。如果对象的当前版本是删除标记，则返回"未找到"状态，并 `x-amz-delete-marker`将响应标头设置为 `true`。

使用客户提供的加密密钥（ SSI-C ）进行服务器端加密的请求标头

如果使用您提供的唯一密钥对对象进行加密，请使用所有三个标头。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定对象的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定对象加密密钥的MD5摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看中的注意事项"使用服务器端加密"。

GetObject for Cloud Storage Pool对象的行为

如果对象已存储在中"云存储池"，GetObject请求的行为取决于对象的状态。有关详细信息、请参见"HeadObject"。

> 如果对象存储在云存储池中、并且该对象的一个或多个副本也位于网格中、则GetObject请求将尝试从网格中检索数据、然后再从云存储池中检索数据。

对象的状态	**GetObject**的行为
对象已载入 StorageGRID 但尚未通过 ILM 进行评估，或者存储在传统存储池中的对象或使用纠删编码	`200 OK` 检索对象的副本。
云存储池中的对象，但尚未过渡到无法检索的状态	`200 OK` 检索对象的副本。
对象已过渡到无法检索的状态	`403 Forbidden、 InvalidObjectState` 使用"RestorEObject"请求将对象还原到可检索状态。
正在从不可检索状态还原的对象	`403 Forbidden、 InvalidObjectState` 等待RestorEObject请求完成。
对象已完全还原到云存储池	`200 OK` 检索对象的副本。

云存储池中的多部分或分段对象

如果您上传的是多部分对象或 StorageGRID 将一个大型对象拆分为多个区块，则 StorageGRID 会通过取样该对象的部分或区块来确定该对象是否在云存储池中可用。在某些情况下、如果对象的某些部分已转换为不可检索状态、或者对象的某些部分尚未还原、则GetObject请求可能会错误地返回 `200 OK`。

在这些情况下：

- GetObject请求可能会返回一些数据、但会在传输中途停止。
- 后续GetObject请求可能会返回 `403 Forbidden`。

GetObject和跨网格复制

如果您正在使用"网格联盟"、并且"跨网格复制"已为存储分段启用、则S3客户端可以通过发出GetObject请求来验证对象的复制状态。此响应包括StorageGRID专用的 `x-ntap-sg-cgr-replication-status`响应标头、该标头将具有以下值之一：

网格	复制状态
源	• 已完成：复制成功。 • *pending *：对象尚未复制。 • 失败：复制失败并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

StorageGRID不支持此 `x-amz-replication-status`标题。

使用 **S3 HeadObject** 请求从 **StorageGRID** 中的对象检索元数据

您可以使用S3 HeadObject请求从对象中检索元数据、而无需返回对象本身。如果对象存储在云存储池中、则可以使用HeadObject确定对象的过渡状态。

HeadObject和多部分对象

您可以使用 `partNumber`request参数检索多部分或分段对象特定部分的元数据。 `x-amz-mp-parts-count`响应元素指示对象有多少个零件。

分段/多部分对象和非分段/非多部分对象均可设置 `partNumber`为1；但是、 `x-amz-mp-parts-count`仅为分段或多部分对象返回响应元素。

用户元数据中的 **UTF-8** 字符

StorageGRID 不会解析或解释用户定义的元数据中的转义 UTF-8 字符。如果密钥名称或值包含不可打印的字符、则对用户定义的元数据中具有转义UTF-8字符的对象发出的HEAD请求不会返回 `x-amz-missing-meta`标题。

支持的请求标头

支持以下请求标头：

- `x-amz-checksum-mode`

  `partNumber`对于HeadObject、不支持参数和 `Range`标头 `x-amz-checksum-mode`。如果在启用的情况下将其包含在请求中 `x-amz-checksum-mode`、则StorageGRID不会在响应中返回校验和值。

请求标头不受支持

以下请求标头不受支持并返回 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本控制

如果 `versionId`未指定子资源、则此操作将提取受版本控制的分段中对象的最新版本。如果对象的当前版本是删除标记，则返回"未找到"状态，并 `x-amz-delete-marker`将响应标头设置为 `true。

使用客户提供的加密密钥（ **SSI-C** ）进行服务器端加密的请求标头

如果对象使用您提供的唯一密钥进行加密，请使用所有这三个标头。

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定对象的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定对象加密密钥的MD5摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看中的注意事项"使用服务器端加密"。

云存储池对象的**HeadObject**响应

如果对象存储在中"云存储池"，则返回以下响应标头：

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

响应标头提供了有关对象移动到云存储池，可选择过渡到不可检索状态并已还原时的状态的信息。

对象的状态	对**HeadObject**的响应
对象已载入 StorageGRID 但尚未通过 ILM 进行评估，或者存储在传统存储池中的对象或使用纠删编码	`200 OK`(不会返回特殊的响应标头。)

云存储池中的对象，但尚未过渡到无法检索的状态	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	在将对象转换为不可检索状态之前、的值 `expiry-date`将设置为未来某个较远的时间。确切的过渡时间不受 StorageGRID 系统控制。

对象的状态	对**HeadObject**的响应

对象已过渡到不可检索状态，但网格上至少也存在一个副本	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	的值设置为未来的 `expiry-date`某个遥远时间。
	
	注意：如果网格上的副本不可用(例如、存储节点已关闭)、您必须先发出"RestorEObject"请求、从云存储池中还原副本、然后才能成功检索对象。

对象已过渡到无法检索的状态，网格上不存在任何副本	`200 OK`
	
	`x-amz-storage-class: GLACIER`

正在从不可检索状态还原的对象	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

对象已完全还原到云存储池	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	`expiry-date`指示云存储池中的对象何时将返回到不可检索状态。

云存储池中的多部分或分段对象

如果您上传的是多部分对象或 StorageGRID 将一个大型对象拆分为多个区块，则 StorageGRID 会通过取样该对象的部分或区块来确定该对象是否在云存储池中可用。在某些情况下、当某个对象的某些部分已转换为不可检索状态或该对象的某些部分尚未还原时、HeadObject请求可能会错误地返回 `x-amz-restore: ongoing-request="false"`。

HeadObject和跨网格复制

如果您正在使用"网格联盟"、并且"跨网格复制"已为存储分段启用、则S3客户端可以通过发出HeadObject请求来

验证对象的复制状态。此响应包括StorageGRID专用的 `x-ntap-sg-cgr-replication-status`响应标头、该标头将具有以下值之一：

网格	复制状态
源	• 已完成：复制成功。 • *pending *：对象尚未复制。 • 失败：复制失败并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

StorageGRID不支持此 `x-amz-replication-status`标题。

使用 **S3 PutObject** 请求将对象添加到 **StorageGRID** 中的存储桶

您可以使用S3 PutObject请求将对象添加到分段。

解决冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

对象大小

一个PutObject操作的最大_Recommended_大小为5 GiB (5、368、709、120字节)。如果您的对象大于5 GiB、请改用"多部分上传"。

一个PutObject操作的最大_supported_大小为5 TiB (5、497、555、138、880字节)。

如果您从StorageGRID 11.5或更早版本升级、则在尝试上传超过5 GiB的对象时、将触发S3 Put Object Size Too Liger警报。如果您全新安装了StorageGRID 11.7或11.7、则在这种情况下不会触发警报。但是、为了符合AWS S3标准、未来版本的StorageGRID不支持上传超过5 GiB的对象。

用户元数据大小

Amazon S3 将每个 PUT 请求标头中用户定义的元数据的大小限制为 2 KB 。StorageGRID 将用户元数据限制为 24 KiB 。用户定义的元数据的大小是通过采用 UTF-8 编码的每个键和值的字节数之和来衡量的。

用户元数据中的 **UTF-8** 字符

如果某个请求在用户定义的元数据的密钥名称或值中包含（未转义） UTF-8 值，则会未定义 StorageGRID 行为。

StorageGRID 不会解析或解释用户定义的元数据的密钥名称或值中包含的转义 UTF-8 字符。转义的 UTF-8 字符被视为 ASCII 字符：

- 如果用户定义的元数据包含转义的UTF-8字符、则PutObject、CopyObject、GetObject和HeadObject请求会成功。

- 如果键名或值的解释值包含不可打印字符、则StorageGRID不会返回 `x-amz-missing-meta`标题。

对象标记限制

您可以在上传新对象时为其添加标记，也可以将其添加到现有对象中。StorageGRID 和 Amazon S3 对每个对象最多支持 10 个标记。与对象关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可以是 128 个 Unicode 字符，而标记值的长度最多可以是 256 个 Unicode 字符。密钥和值区分大小写。

对象所有权

在 StorageGRID 中，所有对象均归存储分段所有者帐户所有，包括由非所有者帐户或匿名用户创建的对象。

支持的请求标头

支持以下请求标头：

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  当您为 `aws-chunked`指定 `Content-Encoding`时，StorageGRID 不会验证以下项目：

  - StorageGRID 不会根据分块数据验证 `chunk-signature`。
  - StorageGRID 不会针对对象验证您为 `x-amz-decoded-content-length`提供的值。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  如果同时使用有效负载签名、则支持分块传输编码 `aws-chunked`。

- 校验和请求标头：

  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`

  > 如果 PutObject 请求未指定校验和，StorageGRID 不会计算对象的默认 CRC-64/NVME 校验和。

- `x-amz-meta-`，后跟一个包含用户定义的元数据的名称-值对。

为用户定义的元数据指定名称 - 值对时，请使用以下通用格式：

```
x-amz-meta-name: value
```

如果要使用*用户定义的创建时间*选项作为ILM规则的参考时间，则必须使用 `creation-time`作为创建对象时记录的元数据的名称。例如：

```
x-amz-meta-creation-time: 1443399726
```

自1970年1月1日以来、的值 `creation-time`以秒为单位进行评估。

> ILM规则不能同时使用*用户定义的创建时间*作为参考时间和平衡或严格的加注选项。创建 ILM 规则时返回错误。

- `x-amz-tagging`
- S3 对象锁定请求标头
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果在发出请求时没有这些标头、则会使用存储分段默认保留设置来计算对象版本模式和保留截止日期。请参阅。 "使用S3 REST API配置S3对象锁定"
- SSA 请求标头：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    请参见 [服务器端加密的请求标头]

请求标头不受支持

不支持以下请求标头：

- `If-Match`

  根据您的 StorageGRID 配置， `If-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。

- `If-None-Match`

  根据您的 StorageGRID 配置， `If-None-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息

（501 Not Implemented）。如果 `If-None-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。

- `x-amz-acl`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

> `x-amz-website-redirect-location`标题返回 `XNotImplemented`。

存储类选项

> `x-amz-storage-class`支持请求标头。为提交的值 `x-amz-storage-class` 会影响StorageGRID在加载期间保护对象数据的方式、而不会影响StorageGRID系统中存储对象的永久性副本数(由ILM确定)。

如果匹配已加数据对象的ILM规则使用了严格加数据选项、则标头将 `x-amz-storage-class`不起作用。

以下值可用于 `x-amz-storage-class`：

- `STANDARD`(默认)
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则在载入对象后，系统会立即创建该对象的第二个副本并将其分发到其他存储节点（双提交）。评估ILM时、StorageGRID 会确定这些初始临时副本是否符合规则中的放置说明。否则、可能需要在不同位置创建新对象副本、并且可能需要删除初始临时副本。
  - 已平衡：如果ILM规则指定了已平衡选项、而StorageGRID 无法立即创建规则中指定的所有副本、则StorageGRID 会在不同的存储节点上创建两个临时副本。

    如果StorageGRID可以立即创建ILM规则(同步放置)中指定的所有对象副本、则标头无效。 `x-amz-storage-class`
- `REDUCED_REDUNDANCY`
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则 StorageGRID 会在载入对象时创建一个临时副本（单个提交）。

- 均衡：如果ILM规则指定了均衡选项，则只有当系统无法立即创建规则中指定的所有副本时，StorageGRID 才会创建一个临时副本。如果 StorageGRID 可以执行同步放置，则此标头不起作用。如果与对象匹配的ILM规则创建单个复制副本、则最好使用此 `REDUCED_REDUNDANCY`选项。在这种情况下、使用 `REDUCED_REDUNDANCY`可避免在每次执行加载操作时不必要地创建和删除额外的对象副本。

在其他情况下、不建议使用 `REDUCED_REDUNDANCY`选项。 `REDUCED_REDUNDANCY`增加了在加数据过程中对象数据丢失的风险。例如，如果最初将单个副本存储在发生故障的存储节点上，而此存储节点未能进行 ILM 评估，则可能会丢失数据。

> 在任何一段时间内只复制一个副本会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

指定 `REDUCED_REDUNDANCY`仅会影响在首次应用对象时创建的副本数。它不会影响通过活动ILM策略评估对象时为对象创建的副本数、也不会导致数据在StorageGRID系统中以较低的冗余级别进行存储。

> 如果在启用了S3对象锁定的情况下将对象导入存储分段、则会忽略此`REDUCED_REDUNDANCY`选项。如果要将对象移入旧的兼容存储分段、则此`REDUCED_REDUNDANCY`选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

服务器端加密的请求标头

您可以使用以下请求标头通过服务器端加密对对象进行加密。SSE 和 SSI-C 选项是互斥的。

- * SSE* ： 如果要使用 StorageGRID 管理的唯一密钥对对象进行加密，请使用以下标题。
  - `x-amz-server-side-encryption`

    如果 `x-amz-server-side-encryption`PutObject请求中未包含标题、则PutObject响应将省略网格范围"存储对象加密设置"。

- * SSI-C* ： 如果要使用您提供和管理的唯一密钥对对象进行加密，请使用所有这三个标头。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新对象的加密密钥。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新对象的加密密钥的MD5摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看的注意事项"使用服务器端加密"。

> 如果使用 SSE 或 SSI-C 对对象进行加密，则会忽略任何分段级别或网格级别的加密设置。

版本控制

如果为存储分段启用了版本控制、则会自动为所存储对象的版本生成唯一的 `versionId`。此消息 `versionId`也会通过响应标头在响应中返回 `x-amz-version-id`。

如果版本控制已暂停、则对象版本将使用空进行存储 `versionId`、如果已存在空版本、则会被覆盖。

授权标题的签名计算

使用标头对请求进行身份验证时 `Authorization`、StorageGRID与AWS在以下方面有所不同：

- StorageGRID不要求 `host`标题包含在中 `CanonicalHeaders`。
- StorageGRID不需要 `Content-Type`包含在中 `CanonicalHeaders`。
- StorageGRID不要求 `x-amz-*`标题包含在中 `CanonicalHeaders`。

> 作为一般最佳实践、请始终将这些标头包含在中 `CanonicalHeaders`以确保它们经过验证；但是、如果排除这些标头、StorageGRID不会返回错误。

有关详细信息，请参见 "授权标头的签名计算：传输单个区块中的有效负载(AWS签名版本4)"。

相关信息

- "使用 ILM 管理对象"
- "Amazon Simple Storage Service API参考：PutObject"

使用 **S3 RestoreObject** 请求在 **StorageGRID** 中还原对象

您可以使用S3 RestorEObject请求还原存储在云存储池中的对象。

支持的请求类型

StorageGRID仅支持用于还原对象的RestorEObject请求。它不支持此 `SELECT`类型的还原。选择请求返回。`XNotImplemented`

版本控制

(可选)指定 `versionId`以还原受版本控制分段中某个对象的特定版本。如果未指定 `versionId`，则会还原对象的最新版本

云存储池对象上的**RestorEObject**的行为

如果对象已存储在中"云存储池"，则根据对象的状态，RestorEObject请求具有以下行为。有关详细信息、请参见"HeadObject"。

> 如果某个对象存储在云存储池中、并且该对象的一个或多个副本也位于网格中、则无需发出RestorEObject请求来还原该对象。而是可以使用GetObject请求直接检索本地副本。

对象的状态	**RestorEObject**的行为
对象已载入 StorageGRID ，但尚未通过 ILM 进行评估，或者对象不在云存储池中	`403 Forbidden、 InvalidObjectState`

对象的状态	**RestorEObject**的行为
云存储池中的对象，但尚未过渡到无法检索的状态	`200 OK`不进行任何更改。 注意：在将对象转换为不可检索状态之前，您不能更改其 `expiry-date`。
对象已过渡到无法检索的状态	`202 Accepted`在请求正文中指定的天数内将对象的可检索副本还原到云存储池。在此期间结束时，对象将返回到无法检索的状态。 (可选)使用 `Tier`请求元素确定完成（`Expedited`、 `Standard`或 `Bulk`所需的恢复作业时间。如果未指定 `Tier`，则使用该 `Standard`层。 重要提示：如果对象已过渡到 S3 Glacier Deep Archive 或云存储池使用 Azure Blob Storage，则无法使用 `Expedited`层还原该对象。将返回以下错误 `403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class`。
正在从不可检索状态还原的对象	`409 Conflict`、 `RestoreAlreadyInProgress`
对象已完全还原到云存储池	`200 OK` *注意：*如果对象已还原到可检索状态，您可以使用的新值重新发出RestoreObject请求来 `Days`更改它 `expiry-date`。还原日期将相对于请求时间进行更新。

使用 **S3 SelectObjectContent** 请求过滤 **StorageGRID** 中的对象数据

您可以使用 S3 SelectObjectContent 请求根据简单的 SQL 语句筛选 S3 对象的内容。

有关详细信息，请参阅 "Amazon Simple Storage Service API参考：选择对象内容"。

开始之前

- 此租户帐户具有 S3 Select 权限。
- 您有权 `s3:GetObject`查询要查询的对象。
- 要查询的对象必须采用以下格式之一：
  - **CSX**。可以按原样使用、也可以压缩到GZIP或bzip2归档中。
  - 镶木地板。对镶木地板对象的其他要求：
    - S3 Select仅支持使用GZIP或Snappy进行列式压缩。S3 Select不支持对镶木地板对象进行整体对象压缩。
    - S3 Select不支持镶木地板输出。必须将输出格式指定为CSV或JSON。
    - 最大未压缩行组大小为512 MB。
    - 您必须使用对象架构中指定的数据类型。
    - 不能使用间隔、JSON、列表、时间或UUID逻辑类型。

- SQL 表达式的最大长度为 256 KB 。
- 输入或结果中的任何记录的最大长度为 1 MiB 。

CSV请求语法示例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

镶木地板请求语法示例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL 查询示例

此查询可从美国人口统计数据中获取状态名称， 2010 年人口， 2015 年估计人口以及变更百分比。文件中非状态的记录将被忽略。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

要查询的文件的前几行，如下所 `SUB-EST2020_ALL.csv`示：

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS命令行界面使用示例(CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

输出文件的前几行 `changes.csv`，如下所示：

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS命令行界面使用示例(镶木地板)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

输出文件的前几行changes.csv如下所示：

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

多部分上传操作

StorageGRID 中支持的分段上传操作

本节介绍 StorageGRID 如何支持多部件上传操作。

以下条件和注释适用于所有多部件上传操作：

- 一个分段的并发多部分上传不应超过1、000次、因为ListMultipartUploADS查询结果可能返回不完整的结果。
- StorageGRID 对多部件部件强制实施 AWS 大小限制。S3 客户端必须遵循以下准则：
  - 多部分上传中的每个部分必须介于 5 MiB （ 5 ， 242 ， 880 字节）和 5 GiB （ 5 ， 368 ， 709 ， 120 字节）之间。
  - 最后一部分可以小于 5 MiB （ 5 ， 242 ， 880 字节）。
  - 通常，部件大小应尽可能大。例如，对于 100 GiB 对象，请使用部件大小 5 GiB 。由于每个部件都被视为唯一的对象、因此使用较大的部件可降低StorageGRID 元数据开销。
  - 对于小于 5 GiB 的对象，请考虑使用非多部分上传。
- 如果ILM规则使用""INGest"选项""“平衡”或“严格”，则载入多部分对象时会针对该对象的每个部分以及多部分上传完成后对该对象作为一个整体进行ILM评估。您应了解这会对对象和部件放置产生何种影响：
  - 如果在进行S3多部分上传时ILM发生更改、则在多部分上传完成后、对象的某些部分可能无法满足当前ILM要求。未正确放置的任何部件将排队等待ILM重新评估、并在稍后移至正确位置。
  - 在评估某个部件的 ILM 时， StorageGRID 会筛选该部件的大小，而不是对象的大小。这意味着、对象的某些部分可以存储在不满足对象整体ILM要求的位置。例如、如果规则指定所有10 GB或更大的对象存储在DC1、而所有较小的对象存储在DC2、则载入时、10部分多部分上传的每个1 GB部分都存储在DC2。但是、在为对象整体评估ILM时、对象的所有部分都会移至DC1。

- 所有分段上传操作都支持StorageGRID"一致性值" 。
- 使用多部分上传载入对象时、不会应用。"对象分段阈值(1 GiB)"
- 根据需要、您可以使用"服务器端加密"多部分上传。要使用SSE (带有StorageGRID管理的密钥的服务器端加密)、请仅在CreateMultipartUpload请求中包含 `x-amz-server-side-encryption`请求标头。要使用SSE-C (使用客户提供的密钥进行服务器端加密)、您可以在CreateMultipartUpload请求和后续每个UploadPart请求中指定相同的三个加密密钥请求标头。
- 多部分上传的对象是否包含在 "分支桶" 中取决于初始化摄取的时间和分支存储桶的时间筛选器：
  - **Before**。如果提取是在分支存储桶的 *Before* 时间戳之前启动的，则无论上传何时完成，都会包含多部分上传的对象。
  - **After**。如果提取是在分支桶的 *After* 时间戳之后启动的，则包括多部分上传的对象。
  - **Between**。如果提取是在分支存储桶的 *From* 和 *To* 时间戳之间启动的，则无论上传何时完成，都会包含多部分上传的对象。
  - 排除。如果提取是在分支桶的 *Exclude from* 时间之前或 *Exclude to* 时间之后启动的，则会包含多部分上传的对象。

操作	实施
AbortMultipartUpload	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。
CompleteMultipartUpload	请参见 "CompleteMultipartUpload"
CreateMultipartUpload (以前称为"启动多部分上传")	请参见 "CreateMultipartUpload"
ListMultipartUploads	请参见 "ListMultipartUploads"
ListParts	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。
上传部件	请参见 "上传部件"
上传PartCopy	请参见 "上传PartCopy"

StorageGRID S3 REST API 如何完成多部分上传

CompleteMultipartUpload操作通过整合先前上传的部件来完成对象的多部分上传。

> 对于CompleteMultipartUpload中的请求参数、StorageGRID支持按升序排列的非连续值 `partNumber`。参数可以以任何值开头。

解决冲突

冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

支持的请求标头

支持以下请求标头：

- 校验和请求标头：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`
  - `x-amz-checksum-type`

  如果 CreateMultipartUpload 请求未指定校验和，StorageGRID 不会计算对象的默认 CRC-64/NVME 校验和。

- `x-amz-storage-class`

  `x-amz-storage-class`如果匹配的ILM规则指定，则标头将影响StorageGRID创建的对象副本数link:../ilm/data-protection-options-for-ingest.html["双提交或平衡加热选项"]。

- `STANDARD`

  （默认）指定在 ILM 规则使用双提交选项或 balanced-option 回退到创建中间副本时执行双提交载入操作。

- `REDUCED_REDUNDANCY`

  指定在 ILM 规则使用双提交选项或 balanced-option 回退为创建中间副本时执行单提交载入操作。

  如果在启用了S3对象锁定的情况下将对象导入存储分段、则会忽略此`REDUCED_REDUNDANCY`选项。如果要将对象移入旧的兼容存储分段、则此`REDUCED_REDUNDANCY`选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

如果多部分上传未在 15 天内完成，则此操作将标记为非活动，并从系统中删除所有关联数据。

`ETag`返回的值不是数据的MD5和、而是遵循多部分对象的值的Amazon S3 API实施 `ETag。

请求标头不受支持

不支持以下请求标头：

- `If-Match`

  根据您的 StorageGRID 配置， `If-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。

- `If-None-Match`

  根据您的 StorageGRID 配置， `If-None-Match` 标头的行为会有所不同。提供此标头可能会返回错误消息（501 Not Implemented）。如果 `If-None-Match` 标头被接受但不起作用，则可能会触发警报，其中包含有关启用更严格的 501 Not Implemented 错误行为的说明。

- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

版本控制

此操作将完成多部分上传。如果为分段启用了版本控制、则在完成多部分上传后创建对象版本。

如果为存储分段启用了版本控制、则会自动为所存储对象的版本生成唯一的 `versionId`。此消息 `versionId` 也会通过响应标头在响应中返回 `x-amz-version-id`。

如果版本控制已暂停、则对象版本将使用空进行存储 `versionId`、如果已存在空版本、则会被覆盖。

> 如果为存储分段启用了版本控制，则完成多部分上传始终会创建新版本，即使在同一对象密钥上同时完成多部分上传也是如此。如果某个存储分段未启用版本控制，则可以先启动多部分上传，然后再对同一对象密钥启动并完成另一个多部分上传。在非版本控制的存储分段上，最后完成的多部分上传将优先。

复制，通知或元数据通知失败

如果为平台服务配置了进行多部分上传的存储分段，则即使关联的复制或通知操作失败，多部分上传也会成功。

租户可以通过更新对象的元数据或标记来触发失败的复制或通知。租户可以重新提交现有值，以避免进行不必要的更改。

请参阅 "对平台服务进行故障排除"。

StorageGRID 中的 S3 CreateMultipartUpload 请求标头和选项

CreateMultipartUpload (以前称为启动多部分上传)操作会为对象启动多部分上传、并返回

上传ID。

`x-amz-storage-class`支持请求标头。为提交的值 `x-amz-storage-class` 会影响StorageGRID在加载期间保护对象数据的方式、而不会影响StorageGRID系统中存储对象的永久性副本数(由ILM确定)。

如果与所含对象匹配的ILM规则使用了""INGest"选项""严格"，则 `x-amz-storage-class`标头将不起作用。

以下值可用于 `x-amz-storage-class`：

- `STANDARD`(默认)
  - *Dual Commit *：如果ILM规则指定了Dual Commit INGEST选项、则在一个对象被加注后、系统将创建该对象的第二个副本并将其分发到其他存储节点(Dual Commit)。评估ILM时、StorageGRID 会确定这些初始临时副本是否符合规则中的放置说明。否则、可能需要在不同位置创建新对象副本、并且可能需要删除初始临时副本。
  - 已平衡：如果ILM规则指定了已平衡选项、而StorageGRID 无法立即创建规则中指定的所有副本、则StorageGRID 会在不同的存储节点上创建两个临时副本。

    如果StorageGRID可以立即创建ILM规则(同步放置)中指定的所有对象副本、则标头无效。 `x-amz-storage-class`
- `REDUCED_REDUNDANCY`
  - *Dual Commit *：如果ILM规则指定了Dual Commit选项、则StorageGRID会在对象被引入时创建一个临时副本(单个提交)。
  - 均衡：如果ILM规则指定了均衡选项，则只有当系统无法立即创建规则中指定的所有副本时，StorageGRID 才会创建一个临时副本。如果 StorageGRID 可以执行同步放置，则此标头不起作用。如果与对象匹配的ILM规则创建单个复制副本、则最好使用此 `REDUCED_REDUNDANCY`选项。在这种情况下、使用 `REDUCED_REDUNDANCY`可避免在每次执行加载操作时不必要地创建和删除额外的对象副本。

  在其他情况下、不建议使用 `REDUCED_REDUNDANCY`选项。 `REDUCED_REDUNDANCY`增加了在加数据过程中对象数据丢失的风险。例如，如果最初将单个副本存储在发生故障的存储节点上，而此存储节点未能进行 ILM 评估，则可能会丢失数据。

> 在任何一段时间内只复制一个副本会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

指定 `REDUCED_REDUNDANCY`仅会影响在首次应用对象时创建的副本数。它不会影响通过活动ILM策略评估对象时为对象创建的副本数、也不会导致数据在StorageGRID系统中以较低的冗余级别进行存储。

> 如果在启用了S3对象锁定的情况下将对象导入存储分段、则会忽略此 `REDUCED_REDUNDANCY`选项。如果要将对象移入旧的兼容存储分段、则此 `REDUCED_REDUNDANCY`选项将返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

支持的请求标头

支持以下请求标头：

- `Content-Type`
- `x-amz-checksum-algorithm`：指定 `CRC32`、 `CRC32C`、 `CRC64NVME`或 `SHA256`

> 如果 CreateMultipartUpload 请求未指定校验和，StorageGRID 不会计算对象的默认 CRC-64/NVME 校验和。StorageGRID 忽略无效或不受支持的 `x-amz-checksum-algorithm`值。

- `x-amz-checksum-type`
- `x-amz-meta-`，后跟一个包含用户定义的元数据的名称-值对

  为用户定义的元数据指定名称 - 值对时，请使用以下通用格式：

  ```
  x-amz-meta-_name_: `value`
  ```

  如果要使用*用户定义的创建时间*选项作为ILM规则的参考时间，则必须使用 `creation-time`作为创建对象时记录的元数据的名称。例如：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  自1970年1月1日以来、的值 `creation-time`以秒为单位进行评估。

> 如果要将对象添加到已启用原有合规性的存储分段、则不允许将其添加 `creation-time`为用户定义的元数据。此时将返回错误。

- S3 对象锁定请求标头：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    如果在不使用这些标题的情况下发出请求，则存储分段默认保留设置用于计算对象版本 retain-until 日期。

  "使用S3 REST API配置S3对象锁定"

- SSA 请求标头：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

[服务器端加密的请求标头]

有关StorageGRID如何处理UTF-8字符的信息，请参见"PutObject"。

服务器端加密的请求标头

您可以使用以下请求标头通过服务器端加密对多部分对象进行加密。SSE 和 SSI-C 选项是互斥的。

- **SSE**：如果要使用由StorageGRID管理的唯一密钥对对象进行加密，请在CreateMultipartUpload请求中使用以下标头。请勿在任何UploadPart请求中指定此标题。
  - `x-amz-server-side-encryption`
- **SSE-C**：如果要使用提供和管理的唯一密钥对对象进行加密，请在CreateMultipartUpload请求(以及后续的每个UploadPart请求)中使用所有这三个标头。
  - `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
  - `x-amz-server-side-encryption-customer-key`：指定新对象的加密密钥。
  - `x-amz-server-side-encryption-customer-key-MD5`：指定新对象的加密密钥的MD5摘要。

您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看的注意事项"使用服务器端加密"。

请求标头不受支持

不支持以下请求标头：

- `x-amz-website-redirect-location`

`x-amz-website-redirect-location`标题返回 `XNotImplemented`。

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。执行CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

StorageGRID 中的 S3 ListMultipartUploads 操作和支持的参数

ListMultipartUploads操作可列出分段的正在进行的多部分上传。

支持以下请求参数：

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`

- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。执行CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

StorageGRID 中 S3 UploadPart 操作支持和不支持的请求标头

UploadPart操作在对象的多部分上传中上传部件。

支持的请求标头

支持以下请求标头：

- 校验和请求标头：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`

  如果在 CreateMultipartUpload 请求期间指定了 CRC-32、CRC-32C、CRC-64/NVME 或 SHA-256 校验和，则还必须在每个 UploadPart 请求中包含校验和请求标头。

  > 如果 CreateMultipartUpload 请求未指定校验和，StorageGRID 不会计算对象的默认 CRC-64/NVME 校验和。

- `Content-Length`
- `Content-MD5`

服务器端加密的请求标头

如果为CreateMultipartUpload请求指定了SSE-C加密、则还必须在每个UploadPart请求中包含以下请求标头：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定与CreateMultipartUpload请求中提供的加密密钥相同的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定与CreateMultipartUpload请求中提供的MD5摘要相同的MD5摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看中的注意事项"使用服务器端加密"。

请求标头不受支持

不支持以下请求标头：

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。执行CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

使用 **S3 UploadPartCopy** 操作在 **StorageGRID** 中上传对象的一部分

UploadPartCopy操作通过从现有对象作为数据源复制数据来上传部分对象。

所有Amazon S3 REST API行为均会实施UploadPartCopy操作。如有更改、恕不另行通知。

此请求读取和写入StorageGRID系统中指定的对象数据 `x-amz-copy-source-range`。

支持的请求标头

支持以下请求标头：

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

服务器端加密的请求标头

如果为CreateMultipartUpload请求指定了SSE-C加密、则还必须在每个UploadPartCopy请求中包含以下请求标头：

- `x-amz-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-server-side-encryption-customer-key`：指定与CreateMultipartUpload请求中提供的加密密钥相同的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定与CreateMultipartUpload请求中提供的MD5摘要相同的MD5摘要。

如果源对象使用客户提供的密钥(SSE-C)进行加密、则必须在UploadPartCopy请求中包含以下三个标头、以便可以解密并复制该对象：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 `AES256`。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定创建源对象时提供的加密密钥。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定创建源对象时提供的MD5摘要。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看中的注意事项"使用服务器端加密"。

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。执行CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

S3校验和支持

StorageGRID 会自动检测在 CreateMultipartUpload 请求期间是否指定了校验和，并在 UploadPartCopy 操作中使用此校验和。您无需在 UploadPartCopy 请求中指定校验和。如果 CreateMultipartUpload 请求未指定校验和，StorageGRID 不会计算对象的默认 CRC-64/NVME 校验和。当 CreateMultipartUpload 未指定校验和时，StorageGRID 不包括复制部件的校验和。

StorageGRID S3 REST API 错误响应

StorageGRID 系统支持所有适用的标准 S3 REST API 错误响应。此外， StorageGRID 实施还添加了多个自定义响应。

支持的 **S3 API** 错误代码

名称	**HTTP**状态
ACCESSDENIED	403 已禁用
BadDigest	400 个错误请求
BucketAlreadyExists	409 冲突
BucketNotEmpagty	409 冲突
实体不完整	400 个错误请求
内部错误	500 内部服务器错误
InvalidAccessKeyId	403 已禁用

名称	**HTTP**状态
InvalidArgument	400 个错误请求
InvalidBucketName	400 个错误请求
InvalidBucketState	409 冲突
InvalidDigest	400 个错误请求
InvalidEncryptionAlgorithmError	400 个错误请求
InvalidPart	400 个错误请求
InvalidPartOrder	400 个错误请求
InvalidRange	416 无法满足请求的范围
InvalidRequest	400 个错误请求
InvalidStorageClass	400 个错误请求
InvalidTag	400 个错误请求
InvalidURI	400 个错误请求
KeyTooLong	400 个错误请求
MalformedXML	400 个错误请求
MetadataTooLarge	400 个错误请求
方法未使用	不允许使用 405 方法
MissingContent长度	411 需要长度
MissingRequestBodyError	400 个错误请求
MissingSecurityHeader	400 个错误请求
NoSuchBucket	未找到 404
NoSuchKey	未找到 404

名称	**HTTP**状态
NoSuchUpload	未找到 404
未实施	501 未实施
NoSuchBucketPolicy	未找到 404
ObjectLockConfigurationNotFoundError	未找到 404
预条件已启用	412- 前提条件失败
已请求超时	403 已禁用
服务不可用	503 服务不可用
SignatureDoesNotMatch	403 已禁用
TooMany桶	400 个错误请求
用户密钥已规范	400 个错误请求

StorageGRID 自定义错误代码

名称	说明	**HTTP**状态
XBucketLifeycleNotAllowed	旧版合规存储分段不支持存储分段生命周期配置	400 个错误请求
XBucketPolicyParseException	无法解析收到的存储分段策略 JSON 。	400 个错误请求
XComplianceConflict	操作因原有合规性设置而被拒绝。	403 已禁用
XComplianceReducedRedundancyFor禁用	原有的合规存储分段不允许减少冗余	400 个错误请求
XMaxBucketPolicyLengthExceeded	您的策略超出了允许的最大存储分段策略长度。	400 个错误请求
XMissingInternalRequestHeader	缺少内部请求的标题。	400 个错误请求
XNoSuchBucketCompliance	指定的存储分段未启用原有合规性。	未找到 404
XNotAcceptable	此请求包含一个或多个无法满足的接受标头。	406 不可接受

名称	说明	HTTP状态
未实施	您提供的请求意味着未实施的功能。	501 未实施

StorageGRID自定义操作

StorageGRID 中支持的自定义存储桶操作

StorageGRID系统支持添加到S3 REST API中的自定义操作。

下表列出了StorageGRID支持的自定义操作。

操作	说明
"获取存储分段一致性"	返回应用于特定存储分段的一致性。
"PUT 存储分段一致性"	设置应用于特定存储分段的一致性。
"获取存储分段上次访问时间"	返回为特定存储分段启用还是禁用上次访问时间更新。
"PUT 分段上次访问时间"	用于启用或禁用特定存储分段的上次访问时间更新。
"删除存储分段元数据通知配置"	删除与特定存储分段关联的元数据通知配置 XML 。
"获取存储分段元数据通知配置"	返回与特定存储分段关联的元数据通知配置 XML 。
"PUT 存储分段元数据通知配置"	配置存储分段的元数据通知服务。
"获取存储使用量"	告诉您某个帐户以及与该帐户关联的每个存储分段使用的总存储量。
"已弃用：具有合规性设置的CreateBucket"	已弃用且不支持：您无法再在启用合规性的情况下创建新存储分段。
"已弃用：GET分段合规性"	已弃用但受支持：返回当前对现有旧版合规存储分段有效的合规性设置。
"已弃用：Put Bucket"	已弃用但受支持：允许您修改现有旧版合规存储分段的合规性设置。

使用 **GET Bucket** 一致性请求检索 **StorageGRID** 中的存储桶一致性级别

通过GET分段一致性请求、您可以确定应用于特定分段的一致性。

默认一致性设置为保证新创建的对象在写入后进行读取。

要完成此操作、您必须具有S3：GetBucketConsistency权限或帐户root。

请求示例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

响应

在响应XML中、 `<Consistency>`将返回以下值之一：

一致性	说明
全部	所有节点都会立即接收数据，否则请求将失败。
强大的全局功能	保证所有站点中所有客户端请求的写入后读一致性。
强大的站点	保证站点内所有客户端请求的写入后读一致性。
读后写	（默认）为新对象提供写入后读一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。建议用于大多数情况。
可用	为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。

响应示例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

相关信息

"一致性"

使用 **PUT Bucket** 一致性请求在 **StorageGRID** 中指定一致性级别

通过"放置分段一致性请求"、您可以指定要应用于对分段执行的操作的一致性。

默认一致性设置为保证新创建的对象在写入后进行读取。

开始之前

要完成此操作、您必须具有S3：PutBucketConsistency权限或帐户root。

请求

`x-ntap-sg-consistency`参数必须包含以下值之一：

一致性	说明
全部	所有节点都会立即接收数据，否则请求将失败。
强大的全局功能	保证所有站点中所有客户端请求的写入后读一致性。
强大的站点	保证站点内所有客户端请求的写入后读一致性。
读后写	（默认）为新对象提供写入后读一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。建议用于大多数情况。
可用	为新对象和对象更新提供最终一致性。对于S3存储分段、请仅在需要时使用(例如、对于包含很少读取的日志值的存储分段、或者对于不存在的密钥执行HEAD或GET操作)。S3 FabricPool 存储分段不支持。

*注意：*通常、应使用"新写入后读取"一致性。如果请求无法正常工作、请尽可能更改应用程序客户端的行为。或者、将客户端配置为为为每个API请求指定一致性。只能在最后一种方法下、在存储分段级别设置一致性。

请求示例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

相关信息

"一致性"

使用 **GET Bucket** 上次访问时间请求检索 **StorageGRID** 中的存储桶上次访问时间状态

通过获取分段上次访问时间请求，您可以确定是为单个分段启用还是禁用了上次访问时间更新。

要完成此操作、您必须具有S3：GetBucketLastAccessTime权限或帐户root。

请求示例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

响应示例

此示例显示已为存储分段启用上次访问时间更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

使用 **PUT Bucket** 上次访问时间请求在 **StorageGRID** 中启用和禁用上次访问时间更新

通过 PUT 分段上次访问时间请求，您可以为各个分段启用或禁用上次访问时间更新。禁用上次访问时间更新可提高性能，它是使用 10.3.0 或更高版本创建的所有存储分段的默认设置。

要完成此操作、您必须对某个存储分段拥有S3：PutBucketLastAccessTime权限、或者以root帐户身份登录。

> 从 StorageGRID 10.3 版开始，默认情况下，所有新存储分段都会禁用对上次访问时间的更新。如果您的存储分段是使用早期版本的 StorageGRID 创建的，并且您希望与新的默认行为匹配，则必须明确禁用上述每个存储分段的上次访问时间更新。您可以使用"放置分段上次访问时间"请求或从租户管理器中某个分段的详细信息页面启用或禁用对上次访问时间的更新。请参阅。 "启用或禁用上次访问时间更新"

如果禁用了某个存储分段的上次访问时间更新，则会对存储分段上的操作应用以下行为：

- GetObject、GetObjectAcl、GetObjectTaging和HeadObject请求不更新上次访问时间。此对象不会添加到用于信息生命周期管理（ ILM ）评估的队列中。
- 仅更新元数据的CopyObject和PutObjectTagingRequests也会更新上次访问时间。对象将添加到队列中以进行 ILM 评估。

- 如果对源存储分段禁用了对上次访问时间的更新、则CopyObject请求不会更新源存储分段的上次访问时间。复制的对象不会添加到源存储分段的 ILM 评估队列中。但是、对于目标、CopyObject请求始终会更新上次访问时间。对象副本将添加到队列中以进行 ILM 评估。
- CompleteMultipartUpload请求更新上次访问时间。已完成的对象将添加到队列中以进行 ILM 评估。

请求示例

此示例将为存储分段启用上次访问时间。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

此示例将禁用存储分段的上次访问时间。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

使用 **StorageGRID** 中的 **DELETE Bucket** 元数据通知配置请求禁用搜索集成服务

通过删除存储分段元数据通知配置请求，您可以通过删除配置 XML 来禁用各个存储分段的搜索集成服务。

要完成此操作、您必须对某个存储分段拥有S3：DeleteBucketMetadataNotification权限、或者以root帐户身份登录。

请求示例

此示例显示了禁用存储分段的搜索集成服务。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

使用 **GET Bucket** 元数据通知配置请求在 **StorageGRID** 中配置搜索集成

使用获取分段元数据通知配置请求，您可以检索用于为各个分段配置搜索集成的配置 XML 。

要完成此操作、您必须具有S3：GetBucketMetadataNotification权限或帐户root。

请求示例

此请求检索名为的存储分段的元数据通知配置 `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

响应

响应正文包括存储分段的元数据通知配置。通过元数据通知配置，您可以确定如何配置存储分段以进行搜索集成。也就是说，您可以通过它确定哪些对象已编制索引，以及将其对象元数据发送到哪些端点。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

每个元数据通知配置都包含一个或多个规则。每个规则都指定其适用场景 的对象以及 StorageGRID 应将对象元数据发送到的目标。必须使用 StorageGRID 端点的 URN 指定目标。

名称	说明	必填
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是

名称	说明	必填
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
状态	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是
目标	规则目标的容器标记。 包含在 Rule 元素中。	是
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN ： • `es`必须是第三个元素。 • URN必须以索引结尾，并以形式键入元数据的存储位置 `domain-name/myindex/mytype`。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是

响应示例

标记之间包含的XML
<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`显示了如何为存储分段配置与搜索集成端点的集成。在此示例中、对象元数据将发送到名为的Elan才 搜索索引并键入名为的 `2017`索引、该索引 `current`托管在名为的AWS域中 `records。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

相关信息

"使用租户帐户"

使用 **PUT Bucket** 元数据通知配置请求在 **StorageGRID** 中启用搜索集成服务

通过 PUT Bucket 元数据通知配置请求，您可以为各个存储分段启用搜索集成服务。您在请求正文中提供的元数据通知配置 XML 用于指定将其元数据发送到目标搜索索引的对象。

要完成此操作、您必须对某个存储分段拥有S3：PutBucketMetadataNotification权限、或者以root帐户身份登录。

请求

此请求必须在请求正文中包含元数据通知配置。每个元数据通知配置都包含一个或多个规则。每个规则都指定其适用场景 的对象以及 StorageGRID 应将对象元数据发送到的目标。

可以按对象名称的前缀筛选对象。例如、可以将带有前缀的对象的元数据发送到一个目标、将带有前缀的对象发送 /images`到另一个目标 `/videos。

前缀重叠的配置无效、在提交时将被拒绝。例如、如果配置中包含一个用于带有前缀的对象的规则、而包含另一个用于带有前缀的对象的规则、 test2`则不允许执行此配置 `test。

必须使用 StorageGRID 端点的 URN 指定目标。提交元数据通知配置时，端点必须存在，否则请求将作为失败 `400 Bad Request`。错误消息指出： `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

下表介绍了元数据通知配置 XML 中的元素。

名称	说明	必填
MetadataNotificationConfiguration	用于指定元数据通知的对象和目标的规则的容器标记。 包含一个或多个规则元素。	是
规则	用于标识应将其元数据添加到指定索引中的对象的规则的容器标记。 拒绝前缀重叠的规则。 包含在 MetadataNotificationConfiguration 元素中。	是
ID	规则的唯一标识符。 包含在 Rule 元素中。	否
状态	状态可以是 " 已启用 " 或 " 已禁用 " 。不会对已禁用的规则执行任何操作。 包含在 Rule 元素中。	是

名称	说明	必填
前缀	与前缀匹配的对象受此规则的影响，其元数据将发送到指定目标。 要匹配所有对象，请指定一个空前缀。 包含在 Rule 元素中。	是
目标	规则目标的容器标记。 包含在 Rule 元素中。	是
URN	发送对象元数据的目标的 urn 。必须是具有以下属性的 StorageGRID 端点的 URN： • `es`必须是第三个元素。 • URN必须以索引结尾，并以形式键入元数据的存储位置 `domain-name/myindex/mytype`。 端点使用租户管理器或租户管理 API 进行配置。它们的形式如下： • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 必须在提交配置 XML 之前配置端点，否则配置将失败并显示 404 错误。 urn 包含在目标元素中。	是

请求示例

此示例显示了为存储分段启用搜索集成。在此示例中，所有对象的对象元数据都将发送到同一目标。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

在此示例中、与前缀匹配的对象的对象元数据 `/images`将发送到一个目标、而与前缀匹配的对象的对象元数据 `/videos`将发送到另一个目标。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

由搜索集成服务生成的 **JSON**

为存储分段启用搜索集成服务后，每次添加，更新或删除对象元数据或标记时，系统都会生成一个 JSON 文档并将其发送到目标端点。

此示例显示了在名为的分段中创建 `test`具有密钥的对象时可能生成的JSON示例 `SGWS/Tagging.txt`。`test`存储分段未进行版本控制、因此 `versionId`标记为空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

元数据通知中包含的对象元数据

下表列出了启用搜索集成后发送到目标端点的 JSON 文档中包含的所有字段。

文档名称包括存储分段名称，对象名称和版本 ID （如果存在）。

键入	项目名称	说明
存储分段和对象信息	存储分段	存储分段的名称
存储分段和对象信息	密钥	对象密钥名称
存储分段和对象信息	版本 ID	对象版本，用于受版本控制的分段中的对象
存储分段和对象信息	region	存储分段区域、例如 `us-east-1`
系统元数据	大小	HTTP 客户端可见的对象大小（以字节为单位）
系统元数据	md5	对象哈希

键入	项目名称	说明
用户元数据	元数据 *key:value*	对象的所有用户元数据，作为键值对
Tags	标记 *key:value*	为对象定义的所有对象标记，作为键值对

> 对于标记和用户元数据， StorageGRID 会将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch 。要配置 Elasticsearch 以将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后、无法在索引中编辑文档的域类型。

相关信息

"使用租户帐户"

使用 **GET Storage Usage** 请求检索 **StorageGRID** 中的帐户和存储桶存储使用情况

" 获取存储使用量 " 请求会告知您帐户正在使用的存储总量以及与帐户关联的每个存储分段的存储总量。

可以通过使用查询参数修改后的ListBuc桶 请求来获取帐户及其存储分段所使用的存储量 `x-ntap-sg-usage`。存储分段使用量与系统处理的 PUT 和 DELETE 请求分开跟踪。根据请求处理情况，使用量值与预期值匹配可能会有一定的延迟，尤其是在系统负载较重时。

默认情况下， StorageGRID 会尝试使用强全局一致性检索使用情况信息。如果无法实现强全局一致性、StorageGRID 会尝试在强站点一致性处检索使用情况信息。

要完成此操作、您必须具有S3：ListAllMy桶 权限或帐户root。

请求示例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

响应示例

此示例显示了一个帐户，该帐户在两个存储分段中包含四个对象和 12 字节的数据。每个存储分段包含两个对象和六个字节的数据。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

版本控制

存储的每个对象版本都会对响应中的和 `DataBytes`值产生影响 `ObjectCount。删除标记不会添加到总数中 ObjectCount。

相关信息

"一致性"

已弃用旧合规性存储分段请求

旧版 **StorageGRID** 合规性的已弃用存储桶请求

您可能需要使用 StorageGRID S3 REST API 来管理使用原有合规性功能创建的分段。

已弃用合规性功能

先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。

如果您之前启用了全局合规性设置，则会在 StorageGRID 11.6 中启用全局 S3 对象锁定设置。您不能再在启用

了合规性的情况下创建新的存储分段；但是，您可以根据需要使用 StorageGRID S3 REST API 管理任何现有的旧合规存储分段。

- "使用S3 REST API配置S3对象锁定"
- "使用 ILM 管理对象"
- "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

已弃用的合规性请求：

- "已弃用 - 为符合性修改存储分段请求"

  SGCompliance XML 元素已弃用。以前，您可以将此 StorageGRID 自定义元素包含在 PUT 存储分段请求的可选 XML 请求正文中，以创建合规存储分段。

- "已弃用—获取存储分段合规性"

  获取存储分段合规性请求已弃用。但是，您可以继续使用此请求来确定当前对现有旧版合规存储分段有效的合规性设置。

- "已弃用—放置分段合规性"

  已弃用Put Bucket. Compliance请求。但是，您可以继续使用此请求修改现有旧版合规存储分段的合规性设置。例如，您可以将现有存储分段置于合法保留状态或延长其保留期限。

StorageGRID 中已弃用的 **SGCompliance** 元素

SGCompliance XML 元素已弃用。以前、您可以将此StorageGRID自定义元素包含在CreateBuckets请求的可选XML请求正文中、以创建兼容分段。

> 先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。有关详细信息、请参见以下内容：
>
> - "使用S3 REST API配置S3对象锁定"
> - "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

您不能再在已启用合规性的情况下创建新存储分段。如果尝试使用CreateBucket"请求修改以实现合规性"来创建新的合规分段、则会返回以下错误消息：

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

StorageGRID 中已弃用的 **GET Bucket compliance** 请求

获取存储分段合规性请求已弃用。但是，您可以继续使用此请求来确定当前对现有旧版合规存储分段有效的合规性设置。

先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。有关详细信息、请参见以下内容：

- "使用S3 REST API配置S3对象锁定"
- "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

要完成此操作、您必须具有S3：GetBucketCompliance权限或帐户root。

请求示例

通过此示例请求，您可以确定名为的分段的合规性设置 `mybucket`。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

响应示例

在响应XML中、 `<SGCompliance>`列出了对分段有效的合规性设置。此示例响应显示了一个存储分段的合规性设置，从将对象载入网格开始，每个对象将保留一年（ 525600 分钟）。此存储分段当前没有法律上的保留。每个对象将在一年后自动删除。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名称	说明
RetentionPeriodMinutes	添加到此存储分段的对象的保留期限长度，以分钟为单位。保留期限从将对象载入网格时开始。

名称	说明
乐高积木	• true ： 此存储分段当前处于合法保留状态。在解除合法保留之前、无法删除此存储分段中的对象、即使其保留期限已到期也是如此。 • false ： 此存储分段当前未处于合法保留状态。此存储分段中的对象可以在保留期限到期时删除。
自动删除	• true ： 此存储分段中的对象将在保留期限到期时自动删除，除非此存储分段处于合法保留状态。 • false ： 保留期限到期后，不会自动删除此存储分段中的对象。如果需要删除这些对象，必须手动将其删除。

错误响应

如果创建的存储分段不符合要求，则响应的HTTP状态代码为，其中S3错误代码 `XNoSuchBucketCompliance`为 `404 Not Found`。

StorageGRID 中已弃用的 **PUT Bucket compliance** 请求

已弃用Put Bucket. Compliance请求。但是，您可以继续使用此请求修改现有旧版合规存储分段的合规性设置。例如，您可以将现有存储分段置于合法保留状态或延长其保留期限。

> 先前 StorageGRID 版本中提供的 StorageGRID 合规性功能已弃用，并已被 S3 对象锁定取代。有关详细信息、请参见以下内容：
>
> • "使用S3 REST API配置S3对象锁定"
>
> • "NetApp 知识库：如何在 StorageGRID 11.5 中管理原有的合规存储分段"

要完成此操作、您必须具有S3：PutBucketCompliance权限或帐户root。

发出 PUT 存储分段合规性请求时，必须为合规性设置的每个字段指定一个值。

请求示例

此示例请求修改名为的分段的合规性设置 `mybucket`。在此示例中、中的对象 `mybucket`现在将保留两年(1、051、200分钟)、而不是一年、从将对象插入网格时开始。此存储分段没有法律上的保留。每个对象将在两年后自动删除。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名称	说明
RetentionPeriodMinutes	添加到此存储分段的对象的保留期限长度，以分钟为单位。保留期限从将对象载入网格时开始。 *重要*为RettionPeriodMinutes指定新值时、必须指定一个等于或大于存储分段的当前保留期限的值。设置存储分段的保留期限后、您不能减小该值、只能增加该值。
乐高积木	• true ： 此存储分段当前处于合法保留状态。在解除合法保留之前、无法删除此存储分段中的对象、即使其保留期限已到期也是如此。 • false ： 此存储分段当前未处于合法保留状态。此存储分段中的对象可以在保留期限到期时删除。
自动删除	• true ： 此存储分段中的对象将在保留期限到期时自动删除，除非此存储分段处于合法保留状态。 • false ： 保留期限到期后，不会自动删除此存储分段中的对象。如果需要删除这些对象，必须手动将其删除。

合规性设置的一致性

当您使用 PUT 存储分段合规性请求更新 S3 存储分段的合规性设置时， StorageGRID 会尝试更新整个网格中存储分段的元数据。默认情况下、StorageGRID会使用*强-全局*一致性来保证所有数据中心站点和包含存储分段元数据的所有存储节点在更改合规性设置后都具有读写后一致性。

如果由于一个数据中心站点或一个站点上的多个存储节点不可用而导致StorageGRID无法实现*强全局*一致性、则响应的HTTP状态代码为 `503 Service Unavailable.`

如果收到此响应，您必须联系网格管理员，以确保所需的存储服务尽快可用。如果网格管理员无法使每个站点上的存储节点足够可用、技术支持可能会通过强制保持*强站点*一致性来指示您重试失败的请求。

除非技术支持指示您执行此操作、并且您了解使用此级别可能会产生的后果、否则切勿强制实施*强站点*一致性以满足放入存储分段合规性要求。

当一致性降低到*强站点*时，StorageGRID保证更新后的合规性设置将仅对站点内的客户端请求具有写后读的一致性。这意味着，在所有站点和存储节点均可用之前， StorageGRID 系统可能会暂时为此存储分段设置多个不一致的设置。设置不一致可能导致意外和意外的行为。例如、如果您将存储分段置于合法保留状态、而您强制实施较低的一致性、则存储分段的先前合规性设置(即合法保留)可能仍会在某些数据中心站点有效。因此，您认为处于合法保留状态的对象可能会在保留期限到期时被用户删除，或者如果启用了自动删除，也可以删除。

要强制使用*strong-sit*一致性，请重新发出Put Bucket*兼容性请求并包括HTTP请求 `Consistency-Control`标头，如下所示：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

错误响应

- 如果创建的存储分段不符合要求，则响应的HTTP状态代码为 `404 Not Found`。
- 如果 `RetentionPeriodMinutes`在请求中小于存储分段的当前保留期限，则HTTP状态代码为 `400 Bad Request`。

相关信息

"已弃用：为满足合规性而修改存储分段请求"

管理访问策略

StorageGRID 如何使用 **AWS** 策略来控制对 **S3** 存储桶和对象的访问

StorageGRID 使用 Amazon Web Services （ AWS ）策略语言允许 S3 租户控制对这些存储分段和对象的访问。StorageGRID 系统实施 S3 REST API 策略语言的一个子集。S3 API 的访问策略以 JSON 格式写入。

访问策略概述

StorageGRID支持三种访问策略：

- 存储分段策略，使用GetBucketPolicy、PutBucketPolicy和DeleteBucketPolicy S3 API操作或租户管理器或租户管理API进行管理。存储分段策略附加到存储分段，因此，可以对其进行配置，以控制存储分段所有者帐户或其他帐户中的用户对存储分段及其对象的访问。一个存储分段策略适用场景 只能包含一个存储分段，并且可能包含多个组。
- * 组策略 * ，使用租户管理器或租户管理 API 配置。组策略会附加到帐户中的某个组，因此，这些策略会配置为允许该组访问该帐户拥有的特定资源。一个组策略只对一个组进行适用场景 ，并且可能对多个存储分段进行。
- 会话策略，包含在 AssumeRole 请求中。会话策略仅适用于给定的会话，进一步定义用户除了组和存储桶策略授予的权限之外还拥有的权限。

> 组、桶和会话策略之间的优先级没有区别。

StorageGRID 存储分段和组策略遵循由 Amazon 定义的特定语法。每个策略中都包含一组策略语句，每个语句都包含以下元素：

- 语句 ID （ SID ）（可选）
- 影响
- 主体 / 不重要
- 资源 /NotResource
- 操作 / 未操作
- 条件（可选）

策略语句是使用此结构构建的，用于指定权限： Grant <Effic> to allow/deny <Principe> to Perform <Action> on <Resource> when <condition> applies 。

每个策略元素都用于特定功能：

Element	说明
SID	Sid 元素是可选的。SID 仅用作用户的问题描述 。它会被存储，但不会被 StorageGRID 系统解释。
影响	使用 Effect 元素确定是否允许或拒绝指定的操作。您必须使用支持的 Action Element 关键字来确定允许（或拒绝）对存储分段或对象执行的操作。
主体 / 不重要	您可以允许用户，组和帐户访问特定资源并执行特定操作。如果请求中不包含 S3 签名，则可以通过指定通配符（ * ）作为主体来进行匿名访问。默认情况下，只有帐户 root 有权访问该帐户拥有的资源。 委托人： • `"Principal": "*"` 匹配所有人，包括匿名（未签名）请求 • `"Principal": { "AWS": "*" }` 匹配任何经过身份验证的身份或用户（与匿名请求不匹配） • 仅适用于存储桶策略 • 主体是被授予或拒绝权限的帐户/用户 您只需要在存储分段策略中指定主体元素。对于组策略，附加该策略的组为隐式主体元素。
资源 /NotResource	资源元素用于标识分段和对象。您可以使用 Amazon 资源名称（ ARN ）来标识资源，从而允许或拒绝对存储分段和对象的权限。
操作 / 未操作	操作和效果元素是权限的两个组成部分。当组请求资源时，它们会被授予或拒绝访问该资源。除非您明确分配权限，否则访问将被拒绝，但您可以使用显式拒绝覆盖由其他策略授予的权限。
条件	条件元素是可选的。通过条件，您可以构建表达式以确定何时应用策略。

在 Action 元素中，您可以使用通配符（ * ）指定所有操作或部分操作。例如，此操作与 S3： GetObject ， S3

： PutObject 和 S3： DeleteObject 等权限匹配。

```
s3:*Object
```

在资源元素中，可以使用通配符（*）和（？）。星号（*）与 0 个或更多字符匹配时，问号（？） 匹配任意单个字符。

在Principal元素 中、不支持使用通配符、但设置匿名访问除外、此操作会向所有人授予权限。例如，您将通配符（*）设置为 Principal 值。

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

在以下示例中，该语句使用的是 " 影响 " ， " 主体 " ， " 操作 " 和 " 资源 " 元素。此示例显示了一个完整的存储分段策略语句，该语句使用“允许”效应授予Principals、admin组和Finance组 `federated-group/finance`对名为的存储分段执行操作的权限，并 `s3:GetObject`授予 `federated-group/admin`对该存储分 `mybucket`段中所有对象执行操作的权限 `s3:ListBucket`。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

存储分段策略的大小限制为 20 ， 480 字节，而组策略的大小限制为 5 ， 120 字节。

策略一致性

默认情况下，对组策略所做的任何更新最终都是一致的。当组策略保持一致时、由于策略缓存、更改可能需要额外15分钟才能生效。默认情况下、您对存储分段策略进行的任何更新都具有强烈的一致性。

您可以根据需要更改存储分段策略更新的一致性保证。例如、您可能希望在站点中断期间对存储分段策略进行更改。

在这种情况下、您可以在PutBucketPolicy请求中设置 `Consistency-Control`标题、也可以使用Put BucketPolicy一致性请求。如果存储分段策略保持一致、则由于策略缓存、所做的更改可能需要额外8秒才能生效。

> 如果您将一致性设置为其他值以解决临时情况、请务必在完成后将存储分段级别设置恢复为其原始值。否则、所有未来存储分段请求都将使用修改后的设置。

什么是会话策略?

会话策略是一种访问策略，它暂时限制特定会话期间可用的权限，例如当用户加入某个组时。会话策略只能允许一部分权限，并且不能授予额外的权限。该组本身可能拥有更广泛的权限。

在策略语句中使用 **ARN**

在策略语句中， ARN 用于 Principal 和 Resource Element 。

- 使用以下语法指定 S3 资源 ARN ：

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 使用以下语法指定身份资源 ARN （用户和组）：

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

其他注意事项：

- 您可以使用星号（ * ）作为通配符，以匹配对象密钥中的零个或多个字符。
- 可以在对象键中指定的国际字符应使用 JSON UTF-8 或使用 JSON \u 转义序列进行编码。不支持百分比编码。

  "RFC 2141 URN 语法"

  PutBucketPolicy操作的HTTP请求正文必须使用charset=UTF-8进行编码。

在策略中指定资源

在策略语句中，您可以使用资源元素指定允许或拒绝权限的分段或对象。

- 每个策略语句都需要一个资源元素。在策略中，资源用元素表示，或者以排除方式 `NotResource`表示 `Resource`。
- 您可以使用 S3 资源 ARN 指定资源。例如：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 您也可以在对象密钥中使用策略变量。例如：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 资源值可以指定在创建组策略时尚不存在的存储区。

指定策略中的主体

使用 Principal 元素标识策略语句允许 / 拒绝访问资源的用户，组或租户帐户。

- 存储分段策略中的每个策略语句都必须包含一个主体元素。组策略中的策略语句不需要Principal元素、因为该组被理解为主体。
- 在策略中、主体由元素"Principal"或"NotPrincipal"表示以供排除。
- 必须使用 ID 或 ARN 指定基于帐户的身份：

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 此示例使用租户帐户 ID 27233906934684427525 ，其中包括帐户 root 和帐户中的所有用户：

```
 "Principal": { "AWS": "27233906934684427525" }
```

- 您只能指定帐户 root ：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 您可以指定一个特定的联合用户（ "Alex" ）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 您可以指定特定的联合组（ "Managers" ）：

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers"  }
```

- 您可以指定匿名主体：

```
"Principal": "*"
```

- 为避免歧义，您可以使用用户 UUID ，而不是用户名：

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

  例如、假设Alex离开了组织、用户名 `Alex`被删除。如果新的Alex加入组织并分配了相同的 `Alex`用户名、则新用户可能会无意中继承授予给原始用户的权限。

- 主体值可以指定在创建存储桶策略时尚不存在的组/用户名。

在策略中指定权限

在策略中， Action 元素用于允许 / 拒绝对资源的权限。您可以在策略中指定一组权限，这些权限由元素 "Action" 或 "NotAction" 表示以表示排除。其中每个元素都映射到特定的 S3 REST API 操作。

下表列出了应用于存储分段的权限以及应用于对象的权限。

> 现在、Amazon S3会对PutBucketReplication和DeleteBucketReplication操作使用S3：PutReplication配置权限。StorageGRID 对每个操作使用单独的权限，这些权限与原始 Amazon S3 规范匹配。

> 使用放置覆盖现有值时执行删除。

应用于存储分段的权限

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： CreateBucket	CreateBucket	是。 注意：仅用于组策略。
S3： DeleteBucket	DeleteBucket	
S3： DeleteBucketMetadataNotification	删除存储分段元数据通知配置	是

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： DeleteBucketPolicy	DeleteBucketPolicy	
S3： DeleteReplicationConfiguration	DeleteBucketReplication	可以、分开放置和删除权限
S3： GetBucketAcl	GetBucketAcl	
S3： GetBucketCompliance	获取存储分段合规性（已弃用）	是
S3： GetBucketConsistency	获取存储分段一致性	是
S3： GetBucketCORS	GetBucketCors	
S3： GetEncryptionConfiguration	GetBucketEncryption	
S3： GetBucketLastAccessTime	获取存储分段上次访问时间	是
S3： GetBucketLocation	GetBucketLocation	
S3： GetBucketMetadataNotification	获取存储分段元数据通知配置	是
S3： GetBucketNotification	GetBucketNotizationConfiguration	
S3： GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3： GetBucketPolicy	GetBucketPolicy	
S3： GetBucketTagging	GetBucketTaging	
S3： GetBucketVersioning	GetBucketVersioning	
S3： GetLifeycleConfiguration	GetBucketLifecycleConfiguration	
S3： GetReplicationConfiguration	GetBucketReplication	
S3： ListAllMy桶	• List桶 • 获取存储使用量	是、对于GET存储使用情况。 注意：仅用于组策略。

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： ListBucket	• GetObject • HeadBucket • HeadObject • ListObjects	
S3： ListBucketMultipartUploads	• ListMultipartUploads	
S3： ListBucketVersions	获取存储分段版本	
S3： PutBucketCompliance	PUT 存储分段合规性（已弃用）	是
S3： PutBucketConsistency	PUT 存储分段一致性	是
S3： PutBucketCORS	• DeleteBucketCors†ñ a • PutBucketCors	
S3： PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
S3： PutBucketLastAccessTime	PUT 分段上次访问时间	是
S3： PutBucketMetadataNotification	PUT 存储分段元数据通知配置	是
S3： PutBucketNotification	PutBucketNotizationConfiguration	
S3： PutBucketObjectLockConfiguration	• 具有请求标头的CreateBucket(`x-amz-bucket-object-lock-enabled: true`还需要S3：CreateBucket)权限 • PutObjectLockConfiguration	
S3： PutBucketPolicy	PutBucketPolicy	
S3： PutBucketTagging	• DeleteBucketTbaging*LW_AT*† • PutBucketTaging	
S3： PutBucketVersioning	PutBucketVersioning	
S3： PutLifeycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： PutReplicationConfiguration	PutBucketReplication	可以、分开放置和删除权限

应用于对象的权限

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： AbortMultipartUpload	• AbortMultipartUpload	
S3：BypassGovernanceRetention	• DeleteObject • DeleteObjects • PutObject保留	
S3： DeleteObject	• DeleteObject • DeleteObjects	
S3： DeleteObjectTagging	DeleteObjectTagging	
S3： DeleteObjectVersionTagging	DeleteObjectTaging(对象的特定版本)	
S3： DeleteObjectVersion	DeleteObject (对象的特定版本)	
S3： GetObject	• GetObject • HeadObject • SelectObjectContent	
S3： GetObjectAcl	GetObjectAcl	
S3： GetObjectLegend	GetObjectLegalHold	
S3： GetObjectRetention	GetObject保留	
S3： GetObjectTagging	GetObjectTagging	
S3： GetObjectVersionTagging	GetObjectTaging(对象的特定版本)	
S3： GetObjectVersion	GetObject (对象的特定版本)	
S3： ListMultipartUploadPart	ListParts	

权限	S3 REST API 操作	为 StorageGRID 自定义
S3： PutObject	• CopyObject • CompleteMultipartUpload • CreateMultipartUpload • PutObject • 上传部件 • 上传PartCopy	
S3： PutObjectLegend	PutObjectLegalHold	
S3： PutObjectRetention	PutObject保留	
S3： PutObjectTagging	PutObjectTagging	
S3： PutObjectVersionTagging	PutObjectTaging(对象的特定版本)	
S3： PutOverwriteObject	• CompleteMultipartUpload • CopyObject • DeleteObjectTagging • PutObject • PutObjectTagging	是
S3： RestoreObject	RestorEObject	

使用 **PutOverwriteObject** 权限

S3： PutOverwriteObject 权限是一种自定义 StorageGRID 权限，适用场景 可通过此权限创建或更新对象。此权限的设置可确定客户端是否可以覆盖对象的数据，用户定义的元数据或 S3 对象标记。

此权限的可能设置包括：

- * 允许 *： 客户端可以覆盖对象。这是默认设置。
- **deny**:客户端无法覆盖对象。如果设置为 deny ，则 PutOverwriteObject 权限的工作原理如下：
  - 如果在同一路径中找到现有对象：
    - 无法覆盖对象的数据、用户定义的元数据或S3对象标记。
    - 正在执行的任何载入操作均会取消，并返回错误。
    - 如果启用了S3版本控制、则拒绝设置将阻止PutObjectTaging或DeleteObjectTaging操作修改对象及其非最新版本的标记集。
  - 如果找不到现有对象，此权限无效。
- 当此权限不存在时，效果与"允许"设置的效果相同。

如果当前 S3 策略允许覆盖，并且 PutOverwriteObject 权限设置为 Deny，则客户端无法覆盖对象的数据、用户定义的元数据或对象标记。此外，如果选中“防止客户端修改”复选框（配置 > 安全设置 > 网络和对象），则该设置将覆盖 PutOverwriteObject 权限的设置。

指定策略中的条件

条件用于定义策略何时生效。条件包括运算符和键值对。

条件使用键值对进行评估。一个条件元素可以包含多个条件，每个条件可以包含多个键值对。条件块使用以下格式：

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

在以下示例中， ipaddress 条件使用 SourceIp 条件密钥。

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

支持的条件运算符

条件运算符分为以下几类：

- 字符串
- 数字
- 布尔值
- IP 地址
- 空检查

条件运算符	说明
StringEquals	根据完全匹配（区分大小写）将键与字符串值进行比较。
StringNotEquals	根据否定匹配（区分大小写）将键与字符串值进行比较。
StringEqualsIgnoreCase	根据完全匹配将键与字符串值进行比较（忽略大小写）。
StringNotEqualsIgnoreCase	根据否定的匹配将键与字符串值进行比较（忽略大小写）。

条件运算符	说明
StringLike	根据完全匹配（区分大小写）将键与字符串值进行比较。可以包含*和?通配符。
StringNotLike	根据否定匹配（区分大小写）将键与字符串值进行比较。可以包含*和?通配符。
数值方程式	根据精确匹配将键与数字值进行比较。
NumericNotEquals	根据否定匹配将键与数字值进行比较。
数值 GreaterThan	将键与基于"大于"匹配的数值进行比较。
NumericGreaterThals.	将键与基于"大于或等于"匹配的数值进行比较。
数值细小	将键与基于"小于"匹配的数值进行比较。
数值 ThalEquals	将键与基于"小于或等于"匹配的数值进行比较。
池	根据"true或false"匹配将键与布尔值进行比较。
IP 地址	将密钥与 IP 地址或 IP 地址范围进行比较。
NotIpAddress	根据否定匹配将密钥与 IP 地址或 IP 地址范围进行比较。
空	检查当前请求上下文中是否存在条件密钥。
如果存在	附加到任何条件运算符（Null 条件除外），以检查该条件键是否不存在。如果条件键不存在，则返回 TRUE。

支持的条件密钥

条件键	操作	说明
AWS ： 源 Ip	IP 运算符	与发送请求的 IP 地址进行比较。可用于存储桶或对象操作。 注意： 如果 S3 请求是通过管理节点和网关节点上的负载平衡器服务发送的，则与负载平衡器服务上游的 IP 地址进行比较。 **Note**：如果使用第三方非透明负载均衡器，则与该负载均衡器的 IP 地址进行比较。任何 `X-Forwarded-For`标头都将被忽略，因为无法确定其有效性。

条件键	操作	说明
AWS ： 用户名	资源 / 身份	与发送请求的发件人的用户名进行比较。可用于存储桶或对象操作。
S3 ： 分隔符	S3 ： ListBucket 和 S3 ： ListBucketVersions 权限	与ListObjects 或 ListObjectVersions 请求中指定的分隔符参数进行比较。
S3：<tag-key>	S3 ： DeleteObjectTagging S3 ： DeleteObjectVersionTagging S3 ： GetObject S3 ： GetObjectAcl 3：GetObjectTaging S3 ： GetObjectVersion S3：GetObjectVersionAcl S3 ： GetObjectVersionTagging S3：PutObjectAcl S3 ： PutObjectTagging S3：PutObjectVersion对象 S3 ： PutObjectVersionTagging	要求现有对象具有特定的标记键和值。
S3 ： 最大密钥	S3 ： ListBucket 和 S3 ： ListBucketVersions 权限	与ListObjects 或 ListObjectVersions 请求中指定的 max-keys 参数进行比较。
s3：对象锁定模式	S3 ： PutObject	相比 `object-lock-mode`从PutObject、CopyObject 、CreateMultipartUpload请求中的请求头展开。
s3：对象锁定模式	S3 ： PutObjectRetention	相比 `object-lock-mode`从 PutObjectRetention 请求中的 XML 主体扩展而来。

条件键	操作	说明
S3： object-lock-real-retenation-days	S3： PutObject	与请求标头中指定的保留截止日期或根据存储分段默认保留期限计算得出的保留截止日期进行比较 `x-amz-object-lock-retain-until-date`、以确保这些值处于以下请求允许的范围内： • PutObject • CopyObject • CreateMultipartUpload
S3： object-lock-real-retenation-days	S3： PutObjectRetention	与PutObjectRetain请求中指定的保留截止日期进行比较、以确保该日期在允许的范围内。
S3：前缀	S3： ListBucket 和 S3： ListBucketVersions 权限	与 ListObjects 或 ListObjectVersions 请求中指定的前缀参数，或为 GetObject 或 HeadObject 指定的键进行比较。
S3：<tag-key>	S3： PutObject S3： PutObjectTagging S3： PutObjectVersionTagging	当对象请求包括标记时，需要特定的标记键和值。
s3:x-amz-copy-source	S3： PutObject	与从 PutObject 和 UploadPartCopy 请求中的请求标头展开的 x-amz-copy-source 进行比较。
s3:x-amz-服务器端加密客户算法	S3： PutObject	相比 `sse-customer-algorithm`或 `copy-source-sse-customer-algorithm`从 PutObject、CopyObject 、CreateMultipartUpload、UploadPart、UploadPartCopy、CompleteMultipartUpload 请求中的请求头展开。

指定策略中的变量

您可以在策略中使用变量填充可用的策略信息。您可以在元素中以及元素的字符串比较中 `Condition`使用策略变量 `Resource`。

在此示例中，变量 `${aws:username}`是Resource元素的一部分：

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

在此示例中、变量 `${aws:username}`是条件块中条件值的一部分：

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

变量	说明
`${aws:SourceIp}`	使用 SourceIp 键作为提供的变量。
`${aws:username}`	使用 username 密钥作为提供的变量。
`${s3:prefix}`	使用特定于服务的前缀密钥作为提供的变量。
`${s3:max-keys}`	使用特定于服务的 max-keys 键作为提供的变量。
`${*}`	特殊字符。使用字符作为文字 * 字符。
`${?}`	特殊字符。使用字符作为文字?字符。
`${$}`	特殊字符。使用字符作为文字 $ 字符。

创建需要特殊处理的策略

有时，策略可能会授予对安全性有危险或对持续操作（例如锁定帐户的 root 用户）有危险的权限。在策略验证期间， StorageGRID S3 REST API 实施的限制性要低于 Amazon ，但在策略评估期间同样严格。

策略问题描述	**Policy type**	**Amazon** 行为	**StorageGRID** 行为
拒绝向自己授予对 root 帐户的任何权限	存储分段	有效且强制实施，但 root 用户帐户保留所有 S3 存储分段策略操作的权限	相同
拒绝用户 / 组的任何权限	组	有效且强制实施	相同
允许外部帐户组拥有任何权限	存储分段	主体无效	有效，但如果某个策略允许，则所有 S3 存储分段策略操作的权限均会返回 405 Method not allowed 错误
允许外部帐户 root 或用户拥有任何权限	存储分段	有效，但如果某个策略允许，则所有 S3 存储分段策略操作的权限均会返回 405 Method not allowed 错误	相同

策略问题描述	**Policy type**	**Amazon** 行为	**StorageGRID** 行为
允许所有人对所有操作拥有权限	存储分段	有效，但对所有 S3 存储分段策略操作的权限会为外部帐户 root 和用户返回 405 Method not allowed 错误	相同
拒绝任何人对所有操作的权限	存储分段	有效且强制实施，但 root 用户帐户保留所有 S3 存储分段策略操作的权限	相同
主体是不存在的用户或组	存储分段	主体无效	有效
资源不是 S3 存储分段	组	有效	相同
主体是一个本地组	存储分段	主体无效	有效
策略授予非所有者帐户(包括匿名帐户)放置对象的权限。	存储分段	有效。对象由创建者账户所有，存储桶策略不适用。创建者账户必须使用对象 ACL 授予对象的访问权限。	有效。对象由存储分段所有者帐户拥有。存储分段策略适用。

一次写入多读（**WORM**）保护

您可以创建一次写入多读（ Write Once Read-Many ， WORM ）分段来保护数据，用户定义的对象元数据和 S3 对象标记。您可以配置 WORM 分段，以便创建新对象并防止覆盖或删除现有内容。请使用此处所述的方法之一。

为了确保覆盖始终被拒绝，您可以：

- 从网格管理器中，转到*配置* > 安全 > 安全设置 > 网络和对象，然后选择*防止客户端修改*复选框。
- 应用以下规则和 S3 策略：
  - 向 S3 策略添加 PutOverwriteObject deny 操作。
  - 将 DeleteObject deny 操作添加到 S3 策略中。
  - 将PutObject Allow操作添加到S3策略中。

> 在 S3 策略中将 DeleteObject 设置为 DENY 不会阻止 ILM 在存在"30 天后零副本"等规则时删除对象。

> 即使应用了所有这些规则和策略、它们也无法防止并发写入(请参见情形A)。它们可以防止顺序完成的覆盖（请参见情况 B ）。

- 情形 A* ： 并发写入（不受保护）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 情形 B*： 顺序完成的覆盖（防止）

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

相关信息

- "StorageGRID ILM 规则如何管理对象"
- "存储分段策略示例"
- "组策略示例"
- "会话策略示例"
- "使用 ILM 管理对象"
- "使用租户帐户"

StorageGRID S3 REST API 会话策略示例

使用以下示例构建StorageGRID会话策略。

示例：设置允许对象检索的会话策略

在此示例中，会话的主体仅允许从 bucket1 检索对象。所有其他操作都会被隐式拒绝，除了特定于 StorageGRID 的操作（例如使用 "S3： PutOverwriteObject" 权限）。调用 AssumeRole API 时，可以以 JSON 文件的形式提供会话策略。

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

StorageGRID S3 REST API 存储桶策略示例

使用本节中的示例为分段构建StorageGRID 访问策略。

存储分段策略用于指定附加此策略的存储分段的访问权限。您可以通过以下工具之一使用S3 PutBucketPolicy

API配置存储分段策略：

- "租户管理器"(英文)
- 使用此命令的AWS CLI (请参见"对存储分段执行的操作")：

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

在 StorageGRID 中，委托人：

- `"Principal": "*"` 匹配所有人，包括匿名（未签名）请求
- `"Principal": { "AWS": "*" }` 匹配任何经过身份验证的身份或用户（与匿名请求不匹配）
- 仅适用于存储桶策略
- 主体是被授予或拒绝权限的帐户/用户

示例：允许每个人对某个存储分段进行只读访问

在此示例中、允许所有人(包括匿名用户)列出分段中的对象、并对分段中的所有对象执行GetObject操作。所有其他操作都将被拒绝。请注意、此策略可能并不特别有用、因为除了帐户root之外、没有其他人有权向存储分段写入数据。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

示例：允许一个帐户中的每个人完全访问某个存储分段，而另一帐户中的每个人只读访问某个存储分段

在此示例中、一个指定帐户中的每个人都可以完全访问某个分段、而另一个指定帐户中的每个人只能列出该分段并对以对象密钥前缀开头的分段中的对象执行GetObject操作 `shared/`。

> 在 StorageGRID 中，非所有者帐户创建的对象（包括匿名帐户）归存储分段所有者帐户所有。存储分段策略适用场景 这些对象。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

示例：允许每个人对某个存储分段进行只读访问，并允许指定组进行完全访问

在此示例中、允许包括匿名用户在内的所有人列出分段并对分段中的所有对象执行GetObject操作、而仅允许属于指定帐户中组的用户 `Marketing`进行完全访问。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

示例：如果客户端位于 **IP** 范围内，则允许每个人对存储分段进行读写访问

在此示例中，允许包括匿名用户在内的所有人列出存储分段并对存储分段中的所有对象执行任何对象操作，前提是这些请求来自指定的 IP 范围（ 54.240.143.0 到 54.240.143.255 ，但 54.240.143.188 除外）。所有其他操作都将被拒绝，并且 IP 范围以外的所有请求都将被拒绝。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

示例：允许指定的联合用户完全访问某个存储分段

在此示例中、联盟用户Alex有权对存储分段及其对象进行完全访问 `examplebucket`。包括 "`root` " 在内的所有其他用户均被明确拒绝所有操作。但请注意， "`root` " 从不会被拒绝 PUT ， Get/DeleteBucketPolicy 的权限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

示例： **PutOverwriteObject** 权限

在此示例中、 `Deny`PutOverwriteObject和DeleteObject的影响可确保任何人都无法覆盖或删除对象的数据、用户定义的元数据和S3对象标记。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

StorageGRID S3 REST API 组策略示例

使用本节中的示例为组构建StorageGRID 访问策略。

组策略用于指定附加此策略的组的访问权限。此策略中没有任何 `Principal`元素、因为它是隐式的。组策略可使用租户管理器或 API 进行配置。

示例：使用租户管理器设置组策略

在租户管理器中添加或编辑组时、您可以选择组策略来确定此组的成员将具有哪些S3访问权限。请参阅。 "为 S3 租户创建组"

- * 无 S3 访问 *：默认选项。此组中的用户无权访问S3资源、除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
- * 只读访问 *：此组中的用户对 S3 资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
- * 完全访问 *：此组中的用户对 S3 资源（包括分段）具有完全访问权限。选择此选项后，完全访问组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
- **Ransmans**要 缓解：此示例策略适用场景 all b分 段for this租户。此组中的用户可以执行常见操作、但无法从启用了对象版本控制的分段中永久删除对象。

  具有"管理所有存储分段"权限的租户管理器用户可以覆盖此组策略。将"管理所有分段"权限限制为受信任用户、并在可用时使用多因素身份验证(Multi-FactorAuthentication、MFA)。

- * 自定义 *：组中的用户将获得您在文本框中指定的权限。

示例：允许组完全访问所有存储分段

在此示例中，除非 bucket 策略明确拒绝，否则允许组中的所有成员对租户帐户拥有的所有分段进行完全访问。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

示例：允许组对所有分段进行只读访问

在此示例中，组的所有成员都对 S3 资源具有只读访问权限，除非 bucket 策略明确拒绝。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

示例：仅允许组成员对存储分段中的"文件夹"具有完全访问权限

在此示例中，组成员只能列出并访问指定存储分段中的特定文件夹（密钥前缀）。请注意，在确定其他组策略和存储分段策略的隐私时，应考虑这些文件夹的访问权限。

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

StorageGRID 审核日志中跟踪的 S3 操作

审核消息由 StorageGRID 服务生成并存储在文本日志文件中。您可以在审核日志中查看特定于S3的审核消息、以获取有关分段和对象操作的详细信息。

审核日志中跟踪的存储分段操作

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- DeleteBucketTbaging
- DeleteObjects
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketTaging
- HeadBucket
- ListObjects
- ListObjectVersies
- PUT 存储分段合规性
- PutBucketLifecycleConfiguration

- PutBucketPolicy
- PutBucketTaging
- PutBucketVersioning

审核日志中跟踪的对象操作

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestorEObject
- 选择对象
- UploadPart (当ILM规则使用平衡或严格的加载时)
- UploadPartCopy (当ILM规则使用平衡或严格的加载时)

相关信息

- "访问审核日志文件"
- "客户端写入审核消息"
- "客户端读取审核消息"

使用Swift REST API (使用寿命结束)

StorageGRID 中的 Swift REST API 支持

对Swift API的支持已终止、将在未来版本中删除。

Swift详细信息已从此版本的文档站点中删除。请参阅。 "StorageGRID 11.8:使用Swift REST API"

监控StorageGRID系统并对其进行故障排除

监控StorageGRID 系统

使用 AutoSupport

了解 StorageGRID 中的 AutoSupport

通过AutoSupport功能、StorageGRID可以向NetApp技术支持发送运行状况和状态包。

使用AutoSupport有助于更快地解决问题。技术支持可以监控您系统的存储需求并帮助确定是否需要添加新节点或站点。或者， AutoSupport可以将软件包发送到另一个目的地。

StorageGRID具有两种类型的AutoSupport：

- **Windows** StorageGRID AutoSupport报告StorageGRID软件问题。首次安装StorageGRID时、默认情况下处于启用状态。您可以"更改默认AutoSupport配置"根据需要执行此操作。

> 如果未启用StorageGRID AutoSupport ，则网格管理器仪表板上会出现一条消息。该消息包含指向AutoSupport配置页面的链接。如果您关闭该消息，即使AutoSupport保持禁用状态，它也不会再次出现，直到您的浏览器缓存被清除。

- *设备硬件AutoSupport *报告StorageGRID设备问题。您必须"在每个设备上配置硬件AutoSupport"。

什么是 Digital Advisor?

Active IQ Digital Advisor（也称为 Digital Advisor）是基于云的，利用了 NetApp 已安装基础中的预测分析和社区智慧。其持续的风险评估、预测性警报、规范性指导和自动化操作可帮助您在问题发生之前进行预防，从而改善系统健康状况并提高系统可用性。

如果您想在 NetApp 支持站点上使用 Digital Advisor 仪表板和功能，则必须启用 AutoSupport。

"Digital Advisor 文档"

AutoSupport软件包中包含的信息

AutoSupport软件包包含以下文件和详细信息。

文件名	字段	说明
AutoSupport-history.XML	AutoSupport序列号+ 此AutoSupport的目标+交付状态+交付尝试次数+ AutoSupport主题+交付URI 上次错误 AutoSupport放置文件名+生成时间+ AutoSupport压缩大小+ AutoSupport解压缩大小+总收集时间(毫秒)	AutoSupport历史记录文件。

文件名	字段	说明
AutoSupport．XML	节点+用于联系支持的协议+HTTP/HTTPS的支持URL 支持地址 AutoSupport按需状态+AutoSupport按需服务器URL + AutoSupport按需轮询间隔	AutoSupport状态文件。提供有关所用协议、技术支持URL和地址、轮询间隔以及OnDemand AutoSupport (如果已启用或已禁用)的详细信息。
存储分段.XML	分段ID +帐户ID +内部版本+位置约束配置+启用合规性+启用合规性配置+启用S3对象锁定+启用S3对象锁定配置+一致性配置+启用CORS配置+上次访问时间+启用策略+启用策略配置+通知+启用云镜像+启用云镜像配置+启用搜索+搜索配置+启用分段标记配置+分段标记配置+版本控制配置	提供存储分段级别的配置详细信息和统计信息。存储分段配置的示例包括平台服务、合规性和存储分段一致性。
grid配置.XML	属性ID +属性名称+值+索引+表ID +表名称	网格范围的配置信息文件。包含有关网格证书、元数据预留空间、网格范围配置设置(合规性、S3对象锁定、对象压缩、警报、系统日志和ILM配置)、纠删编码配置文件详细信息、DNS名称和"NMS名称"的信息。
GRE-SPEC.XML	网格规范、原始XML	用于配置和部署StorageGRID。包含节点的网格规格、NTP服务器IP、DNS服务器IP、网络拓扑和硬件配置文件。
grid－Tasks．XML	节点+服务路径+属性ID +属性名称+值+索引+表ID +表名称	网格任务(维护过程)状态文件。提供网格的活动任务、已终止任务、已完成任务、失败任务和待定任务的详细信息。
GRI.JSON	网格+修订版+软件版本+说明+许可证+密码+ DNS + NTP +站点+节点	网格信息。
ILM配置.XML	属性ID +属性名称+值+索引+表ID +表名称	ILM配置的属性列表。
ILM状态.XML	节点+服务路径+属性ID +属性名称+值+索引+表ID +表名称	ILM指标信息文件。包含每个节点的ILM评估速率以及网格范围指标。
ILM。XML	ILM原始XML	ILM活动策略文件。包含有关活动ILM策略的详细信息、例如存储池ID、载入行为、筛选器、规则和问题描述。
Log.TGZ	*n/A*	可下载的日志文件。包含 `bycast-err.log` 每个节点的和 `servermanager.log`。

文件名	字段	说明
Manifest.XML	收集顺序+此数据的AutoSupport内容文件名+此数据项的说明+收集的字节数+收集所用时间+此数据项的状态+错误说明+此数据的AutoSupport内容类型+	包含AutoSupport元数据以及所有AutoSupport文件的简要说明。
NMS-实体.XML	属性索引+实体OID +节点ID +设备型号ID +设备型号版本+实体名称	中的组和服务实体"NMS树"。提供网格拓扑详细信息。可以根据节点上运行的服务来确定节点。
objects-statues.XML	节点+服务路径+属性ID +属性名称+值+索引+表ID +表名称	对象状态、包括后台扫描状态、活动传输、传输速率、总传输量、删除速率、损坏的片段、丢失的对象、丢失的对象、尝试修复的对象、扫描速率、估计扫描期限以及修复完成状态。
server-stats.XML	节点+服务路径+属性ID +属性名称+值+索引+表ID +表名称	服务器配置。包含每个节点的以下详细信息：平台类型、操作系统、已安装内存、可用内存、存储连接、存储设备机箱序列号、存储控制器故障驱动器计数、计算控制器机箱温度、计算硬件、计算控制器序列号、电源、驱动器大小和驱动器类型。
service-stats.XML	节点+服务路径+属性ID +属性名称+值+索引+表ID +表名称	服务节点信息文件。包含分配的表空间、可用表空间、数据库的Reaper指标、区块修复持续时间、修复作业持续时间、自动作业重新启动和自动作业终止等详细信息。
storage-Greds.XML	存储级别ID +存储级别名称+存储节点ID +存储节点路径	每个存储节点的存储级别定义文件。
摘要属性.XML	组OID +组路径+摘要属性ID +摘要属性名称+值+索引+表ID +表名称	汇总StorageGRID使用情况信息的高级系统状态数据。提供网格名称、站点名称、每个网格和每个站点的存储节点数量、许可证类型、许可证容量和使用情况、软件支持条款以及S3操作详细信息等详细信息。
system-alerts．XML	名称+严重性+节点名称+警报状态+站点名称+警报触发时间+警报解决时间+规则ID +节点ID +站点ID +已关闭+其他标注+其他标签	指示StorageGRID系统中潜在问题的当前系统警报。

文件名	字段	说明
USERAGENTS.XML	用户代理+天数+总HTTP请求数+载入的总字节数+检索的总字节数+放置请求数+获取请求数+删除请求数+机头请求数+POST请求数+平均请求时间(毫秒)+平均放置请求时间(毫秒)+平均删除请求时间(毫秒)+平均机头请求时间(毫秒)+平均后请求时间(毫秒)+平均选项请求时间(毫秒)	基于应用程序用户代理的统计信息。例如、每个用户代理的放置/获取/删除/机头操作数以及每个操作的总字节数。
X-header-data	X-SAP-ASUP生成的-ON + NetApp X-SAP-ASUP主机名+ NetApp X-SAP-ASUP OS版本+ X-SAP-ASUP序列号+ X-SAP-ASUP序列号NetApp + X-SAP-ASUP主题NetApp + X-SAP-ASUP系统ID + X-SAP-ASUP型号名称+ NetApp NetApp NetApp	AutoSupport标头数据。

在 **StorageGRID** 中配置 **AutoSupport**

该 AutoSupport 功能使您的 StorageGRID 系统能够向技术支持发送定期和事件驱动的运行状况和状态消息，以进行主动监控和故障排除。StorageGRID AutoSupport 还支持使用 Digital Advisor 进行预测性建议。

默认情况下，首次安装 StorageGRID 时，系统会为基于软件的 StorageGRID 系统启用每周和事件触发的 AutoSupport 功能。但是，您必须在每个设备上 配置硬件AutoSupport。您可以根据需要更改 AutoSupport 配置。

如果要更改 StorageGRID AutoSupport 的配置，请仅在主管理节点上进行更改。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到主管理节点上的 Grid Manager。
- 您拥有"root访问权限"。
- 如果您将使用 HTTPS 发送 AutoSupport 软件包，则您已直接或"使用代理服务器"向主管理节点提供出站互联网访问权限（不需要入站连接）。
- 如果在 StorageGRID AutoSupport 页面上选择了 HTTP，则必须将 AutoSupport 包"已配置代理服务器"转发为 HTTPS。NetApp 的 AutoSupport 服务器将拒绝使用 HTTP 发送的包。
- 如果您将使用 SMTP 作为 AutoSupport 包的协议，则有 "已配置电子邮件服务器"。

关于此任务

您可以使用以下选项的任意组合将AutoSupport软件包发送给技术支持：

- 每周：每周自动发送一次AutoSupport软件包。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软件包。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软件包、这在他们正在使用问题描述时非常有用(需要HTTPS AutoSupport传输协议)。默认设置： disabled 。
- 用户触发：随时手动发送AutoSupport软件包。
- 日志收集："手动收集日志文件和系统数据并发送AutoSupport包" 。

配置 AutoSupport

要更改 AutoSupport 的安装默认配置，或在每个 StorageGRID 设备上配置硬件 AutoSupport：

步骤

1. 选择 支持 > 工具 > **AutoSupport** > 设置。
2. 选择要用于发送AutoSupport软件包的协议。
   - * HTTPS ： 这是新安装的默认和建议设置。此协议使用端口443。如果需要启用AutoSupport On Demand功能，则必须使用HTTPS。
   - **HTTP**：如果选择 HTTP，则必须"配置代理服务器"将 AutoSupport 包转发为 HTTPS。NetApp 的 AutoSupport 服务器拒绝使用 HTTP 发送的包。此协议使用端口 80。
   - **SMTP**：如果您希望通过电子邮件发送 AutoSupport 包，请使用此选项。您必须先 "配置电子邮件服务器"。

   您设置的协议用于发送除按需 AutoSupport 之外的所有 AutoSupport 软件包，按需功能需要 HTTPS 协议。
3. 如果选择了*HTTPS*，请选择是否使用NetApp支持证书(TLS证书)来保护与技术支持服务器的连接。
   - 验证证书(默认)：确保AutoSupport软件包的传输安全。NetApp 支持证书已随 StorageGRID 软件一起安装。
   - * 不验证证书 * ： 只有当您有充分理由不使用证书验证时，例如证书出现临时问题时，才选择此选项。
4. 如果您选择了 **SMTP**，请使用*发件人*字段输入您之前配置的电子邮件服务器的地址。
5. 选择 * 保存 * 。所有每周、用户触发和事件触发的软件包都会使用选定协议进行发送。

禁用每周AutoSupport

默认情况下、StorageGRID系统配置为每周向技术支持发送一次AutoSupport软件包。

要确定每周AutoSupport软件包的发送时间，请转到* AutoSupport *>*结果*选项卡。在*Weekly AutoSupport (每周计划时间)*部分，查看*Next Scheduled Time (下一个计划时间)*的值。

您可以随时禁用每周AutoSupport软件包的自动发送功能。

步骤

1. 选择 支持 > 工具 > **AutoSupport** > 设置。
2. 清除*启用每周AutoSupport *复选框。
3. 选择 * 保存 * 。

禁用事件触发的**AutoSupport**

默认情况下、StorageGRID系统配置为每小时向技术支持发送一次AutoSupport软件包。

您可以随时禁用事件触发的AutoSupport。

步骤

1. 选择 支持 > 工具 > **AutoSupport** > 设置。
2. 清除*启用事件触发的AutoSupport *复选框。
3. 选择 * 保存 * 。

启用 **AutoSupport On Demand**

AutoSupport On Demand 可帮助解决技术支持正在积极处理的问题。

默认情况下， AutoSupport On Demand 处于禁用状态。启用此功能后、技术支持可以请求StorageGRID系统自动发送AutoSupport软件包。技术支持还可以为 AutoSupport On Demand 查询设置轮询时间间隔。

技术支持无法启用或禁用AutoSupport On Demand。

步骤

1. 选择 支持 > 工具 > **AutoSupport** > 设置。
2. 为协议选择 * HTTPS * 。
3. 选中*启用每周AutoSupport *复选框。
4. 选中*启用AutoSupport On Demand*复选框。
5. 选择 * 保存 * 。

   已启用 AutoSupport On Demand ，技术支持可以将 AutoSupport On Demand 请求发送到 StorageGRID 。

禁用软件更新检查

默认情况下， StorageGRID 会联系 NetApp 以确定您的系统是否有可用的软件更新。如果提供了 StorageGRID 修补程序或新版本，则新版本将显示在 StorageGRID 升级页面上。

根据需要，您可以选择禁用软件更新检查。例如，如果您的系统无法访问 WAN ，则应禁用此检查以避免下载错误。

步骤

1. 选择 支持 > 工具 > **AutoSupport** > 设置。
2. 清除*检查软件更新*复选框。
3. 选择 * 保存 * 。

添加其他 **AutoSupport** 目标

启用AutoSupport后、运行状况和状态软件包将发送给技术支持。您可以为所有AutoSupport软件包指定一个额外的目标。

要验证或更改用于发送 AutoSupport 软件包的协议，请参见 配置 AutoSupport 中的说明。

您不能使用SMTP协议将AutoSupport软件包发送到其他目标。

步骤

1. 选择 支持 > 工具 > **AutoSupport** > 设置。
2. 选择*启用其他AutoSupport 目标*。
3. 指定以下内容：

主机名

附加AutoSupport 目标服务器的服务器主机名或IP地址。

您只能输入一个附加目标。

端口

用于连接到其他AutoSupport 目标服务器的端口。对于HTTP、默认为端口80；对于HTTPS、默认为端口443。

证书验证

是否使用TLS证书来保护与其他目标的连接。

- 选择*验证证书*以使用证书验证。
- 选择*不验证证书*发送AutoSupport包而不验证证书。

  只有当您有充分的理由不使用证书验证时，例如证书出现临时问题时，才选择此选项。

4. 如果选择了*验证证书*，请执行以下操作：
   a. 浏览到CA证书的位置。
   b. 上传CA证书文件。

   此时将显示CA证书元数据。
5. 选择 * 保存 * 。

所有未来的每周、事件触发和用户触发的AutoSupport软件包都将发送到其他目标。

[[autocsupport-for -eliance]]为设备配置**AutoSupport**

适用于设备的AutoSupport报告StorageGRID硬件问题、而StorageGRID AutoSupport报告StorageGRID软件问题、但有一个例外：对于SGF6112、StorageGRID AutoSupport同时报告硬件和软件问题。您必须在每个设备上配置AutoSupport、但SGF6112除外、它不需要额外配置。对于服务设备和存储设备、AutoSupport的实施方式有所不同。

您可以使用SANtricity为每个存储设备启用AutoSupport。您可以在初始设备设置期间或安装设备后配置SANtricity AutoSupport：

- 对于SG6000和SG5700设备、 "在SANtricity 系统管理器中配置AutoSupport"

如果您在 "SANtricity 系统管理器" 中配置通过代理进行 AutoSupport 传输，则可以将 E-Series 设备的

AutoSupport 包包含在 StorageGRID AutoSupport 中。

StorageGRID AutoSupport 不会报告硬件问题、例如DIMM或主机接口卡(Host Interface Card、HIC)故障。但是，某些组件故障可能会触发"硬件警报"。对于带有底板管理控制器(BMC)的StorageGRID设备、您可以配置电子邮件和SNMP陷阱来报告硬件故障：

- "为BMC警报设置电子邮件通知"
- "配置BMC的SNMP设置"

相关信息

- "用于外部通信的端口"
- "NetApp 支持"

手动触发 **StorageGRID** 中的 **AutoSupport** 包

要帮助技术支持解决StorageGRID系统的问题、您可以手动触发要发送的AutoSupport软件包。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您具有 Root 访问权限或其他网格配置权限。

步骤

1. 选择 支持 > 工具 > **AutoSupport**。
2. 在*操作*选项卡上，选择*发送用户触发的AutoSupport *。

   StorageGRID尝试将AutoSupport包发送到NetApp支持站点。如果尝试成功，则*结果*选项卡上的*最近结果*和*上次成功时间*值将会更新。如果出现问题，*最新结果*值将更新为“失败”，并且StorageGRID不会再次尝试发送AutoSupport包。

3. 1 分钟后，刷新浏览器中的AutoSupport页面以访问最新结果。

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

StorageGRID 如何处理 **AutoSupport** 包故障

查看 StorageGRID 在尝试发送 AutoSupport 软件包失败时所执行的操作列表。

StorageGRID 会根据 AutoSupport 软件包的类型采取不同的操作。可以通过选择 支持 > 工具 > **AutoSupport** > 结果 来检查 AutoSupport 软件包的状态。

如果AutoSupport软件包无法发送，“Failed”(失败)将显示在AutoSupport页的*results*选项卡上。

如果将代理服务器配置为将 AutoSupport 包转发到 NetApp，"验证代理服务器配置设置是否正确"。

每周**AutoSupport**软件包失败

如果每周AutoSupport软件包无法发送、StorageGRID系统将执行以下操作：

1. 更新最新的 result 属性以重试。
2. 尝试每四分钟重新发送15次AutoSupport软件包、持续一小时。
3. 发送失败一小时后，将最新结果属性更新为 Failed 。
4. 尝试在下次计划的时间再次发送AutoSupport软件包。
5. 如果软件包因NMS服务不可用而失败、并且软件包在七天之后发送、则保留常规AutoSupport计划。
6. 当NMS服务再次可用时、如果某个软件包在七天或更长时间内未发送、则会立即发送AutoSupport软件包。

用户触发或事件触发的**AutoSupport**软件包故障

如果用户触发或事件触发的AutoSupport软件包无法发送、StorageGRID系统将执行以下操作：

1. 如果已知错误，则显示错误消息。例如、如果用户在选择SMTP协议时未提供正确的电子邮件配置设置、则会显示以下错误： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 不再尝试发送软件包。
3. 将错误记录在中 `nms.log`。

如果出现故障，并且 SMTP 是所选协议，则 AutoSupport 页面上可能会显示以下错误消息： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

了解如何"配置电子邮件服务器设置"。

更正**AutoSupport**软件包故障

如果发生故障，并且 SMTP 是所选协议，请验证 StorageGRID 系统的电子邮件服务器是否正确配置，以及您的电子邮件服务器是否正在运行。AutoSupport 页面上可能会出现以下错误消息：由于"电子邮件服务器"页面上的设置不正确，无法使用 SMTP 协议发送 AutoSupport 包。

通过**StorageGRID**发送**E**系列**AutoSupport**软件包

您可以通过StorageGRID管理节点(而不是存储设备管理端口)向技术支持发送E系列SANtricity System Manager AutoSupport软件包。

有关将AutoSupport与E系列设备结合使用的详细信息、请参见 "E系列硬件AutoSupport"。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您有 "存储设备管理员或root访问权限"。
- 您已配置SANtricity AutoSupport：
  - 对于SG6000和SG5700设备、 "在SANtricity 系统管理器中配置AutoSupport"

要使用网格管理器访问 SANtricity 系统管理器，您必须具有 SANtricity 固件 8.70 或更高版本。

关于此任务

E系列AutoSupport软件包包含存储硬件的详细信息、比StorageGRID系统发送的其他AutoSupport软件包更具体。

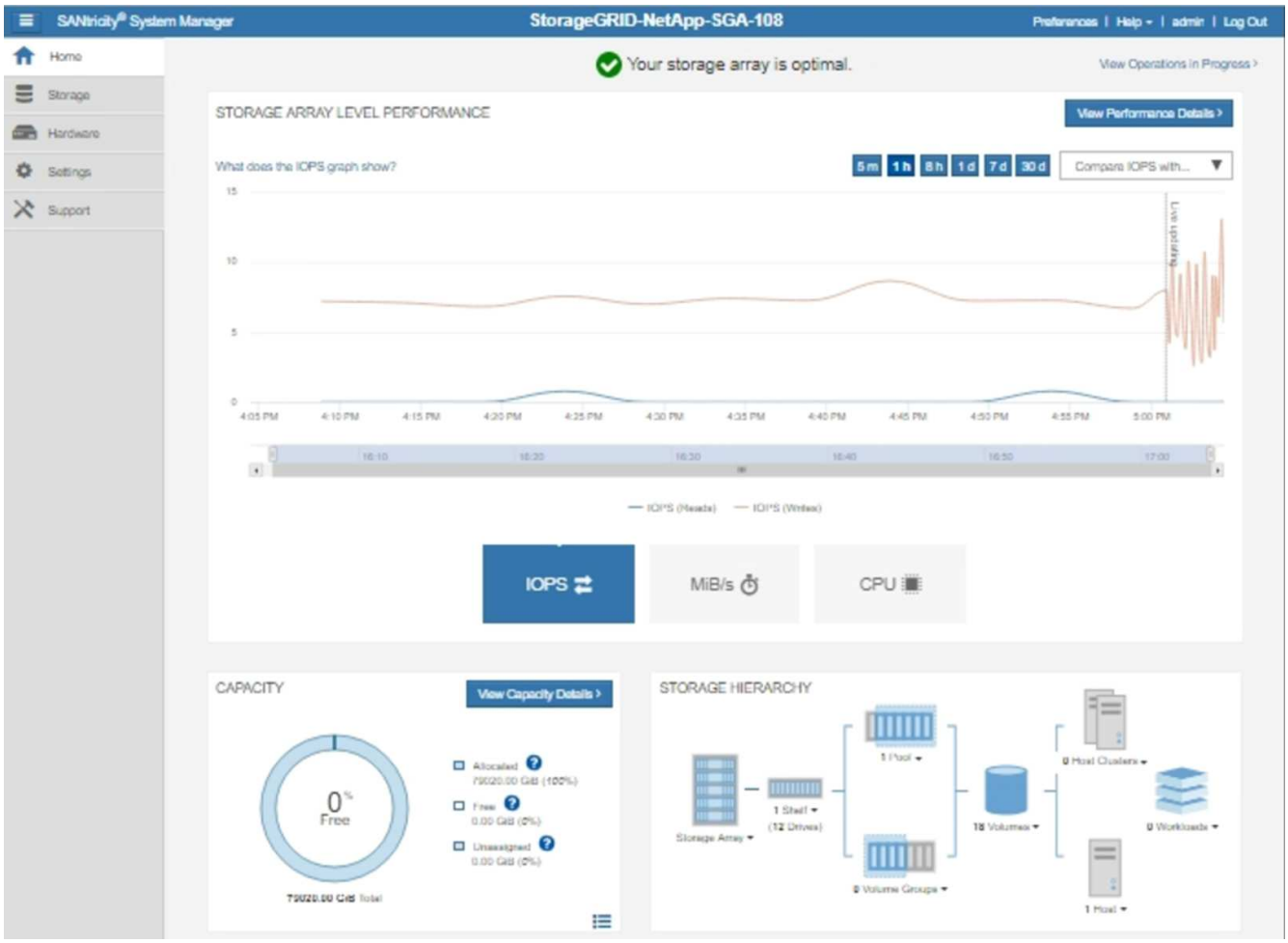
您可以在SANtricity系统管理器中配置一个特殊的代理服务器地址、以便在不使用设备管理端口的情况下通过StorageGRID管理节点传输AutoSupport软件包。以这种方式传输的AutoSupport软件包由发送"首选发件人管理节点"，它们使用在网格管理器中配置的任何"管理代理设置"软件包。

此操作步骤仅用于为E系列AutoSupport软件包配置StorageGRID代理服务器。有关E系列AutoSupport配置的更多详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

步骤

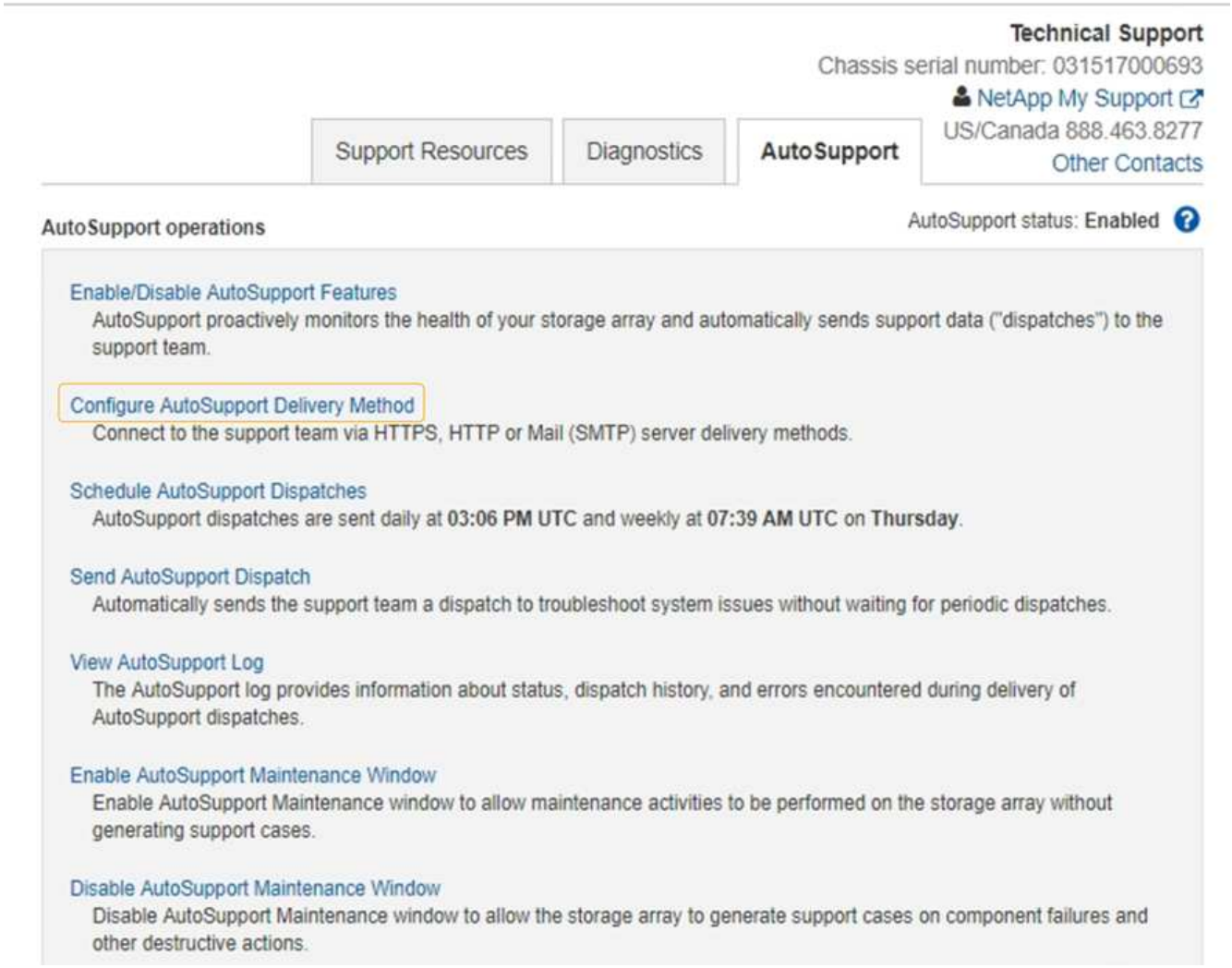
1. 在网格管理器中，选择*节点*。
2. 从左侧的节点列表中，选择要配置的存储设备节点。
3. 选择 * SANtricity 系统管理器 * 。

   此时将显示 SANtricity System Manager 主页。



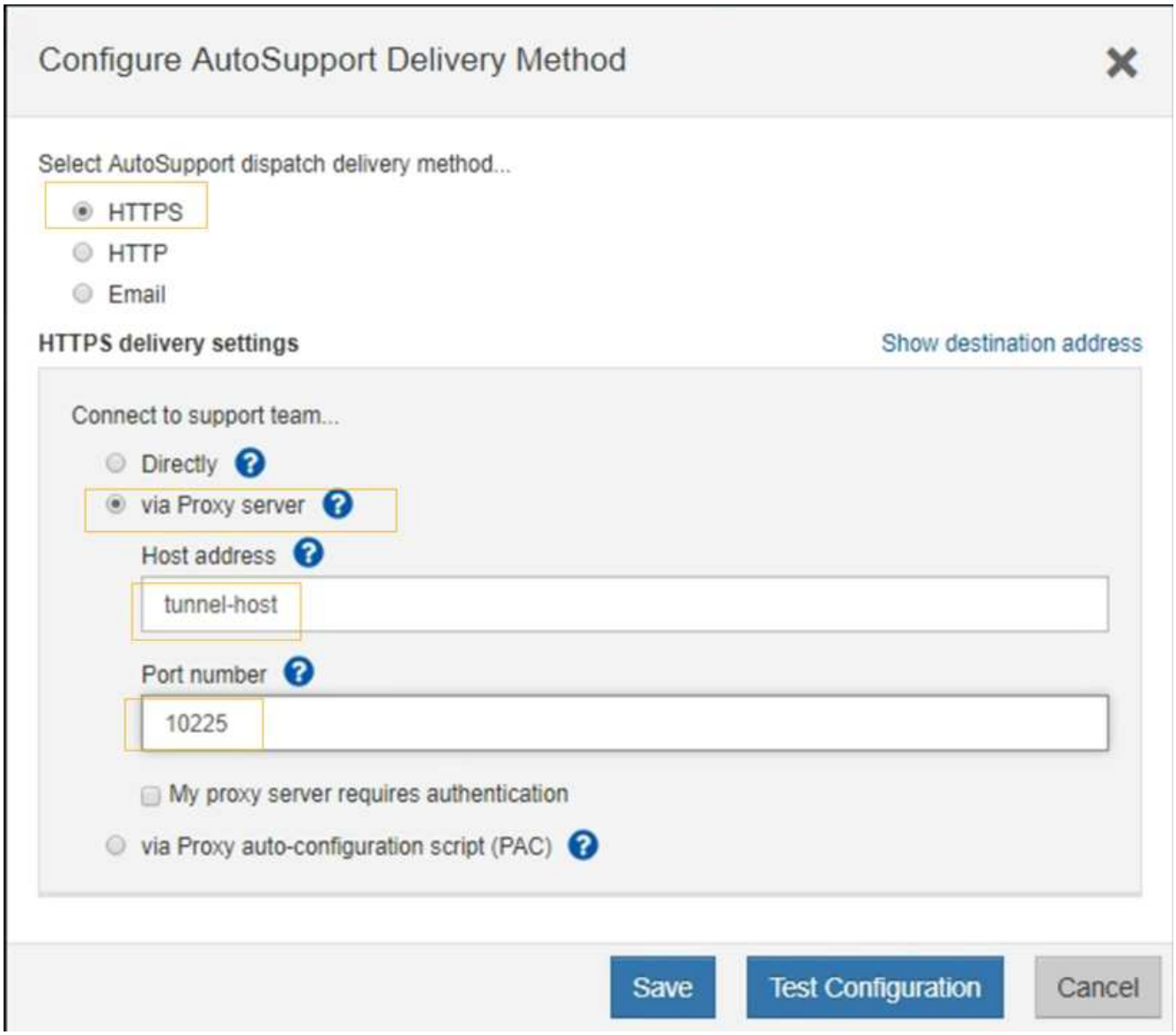
4. 选择*支持* > 支持中心 > **AutoSupport**。

此时将显示 AutoSupport 操作页面。



5. 选择 * 配置 AutoSupport 交付方法 * 。

此时将显示配置 AutoSupport 交付方法页面。



6. 选择 * HTTPS * 作为传送方法。

   已预安装启用HTTPS的证书。

7. 选择 * 通过代理服务器 * 。
8. 输入 `tunnel-host`作为*主机地址*。

   `tunnel-host`是使用管理节点发送E系列AutoSupport软件包的特殊地址。

9. 输入 `10225`作为*端口号*。

   `10225`是从设备中的E系列控制器接收AutoSupport软件包的StorageGRID代理服务器上的端口号。

10. 选择 * 测试配置 * 以测试 AutoSupport 代理服务器的路由和配置。

    如果正确、则绿色横幅中会显示一条消息："Your AutoSupport configuration has been verified。"

    如果测试失败，则会在红色横幅中显示一条错误消息。请检查您的StorageGRID DNS设置和网络连接、确

保"首选发件人管理节点"可以连接到NetApp支持站点、然后重试此测试。

11. 选择 * 保存 * 。

此时将保存配置、并显示一条确认消息：AutoSupport delDelivery Method has been configured.(已配置传输方法。)

监控StorageGRID 系统

定期监控StorageGRID系统以确保其按预期运行。

开始之前

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

> 要更改网格管理器中显示的存储值的单位，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。

关于此任务

这些说明介绍了如何：

- "查看和管理信息板"
- "查看节点页面"
- "定期监控系统的以下方面："
  - "系统运行状况"
  - "存储容量"
  - "信息生命周期管理"
  - "网络和系统资源"
  - "租户活动"
  - "负载平衡操作"
  - "网格联合连接"
- "管理警报"
- "查看日志文件"
- "配置日志管理和外部系统日志服务器"
- "使用外部系统日志服务器"收集审核信息
- "使用SNMP进行监控"
- "更改 I/O 优先级"改变 I/O 操作的相对优先级

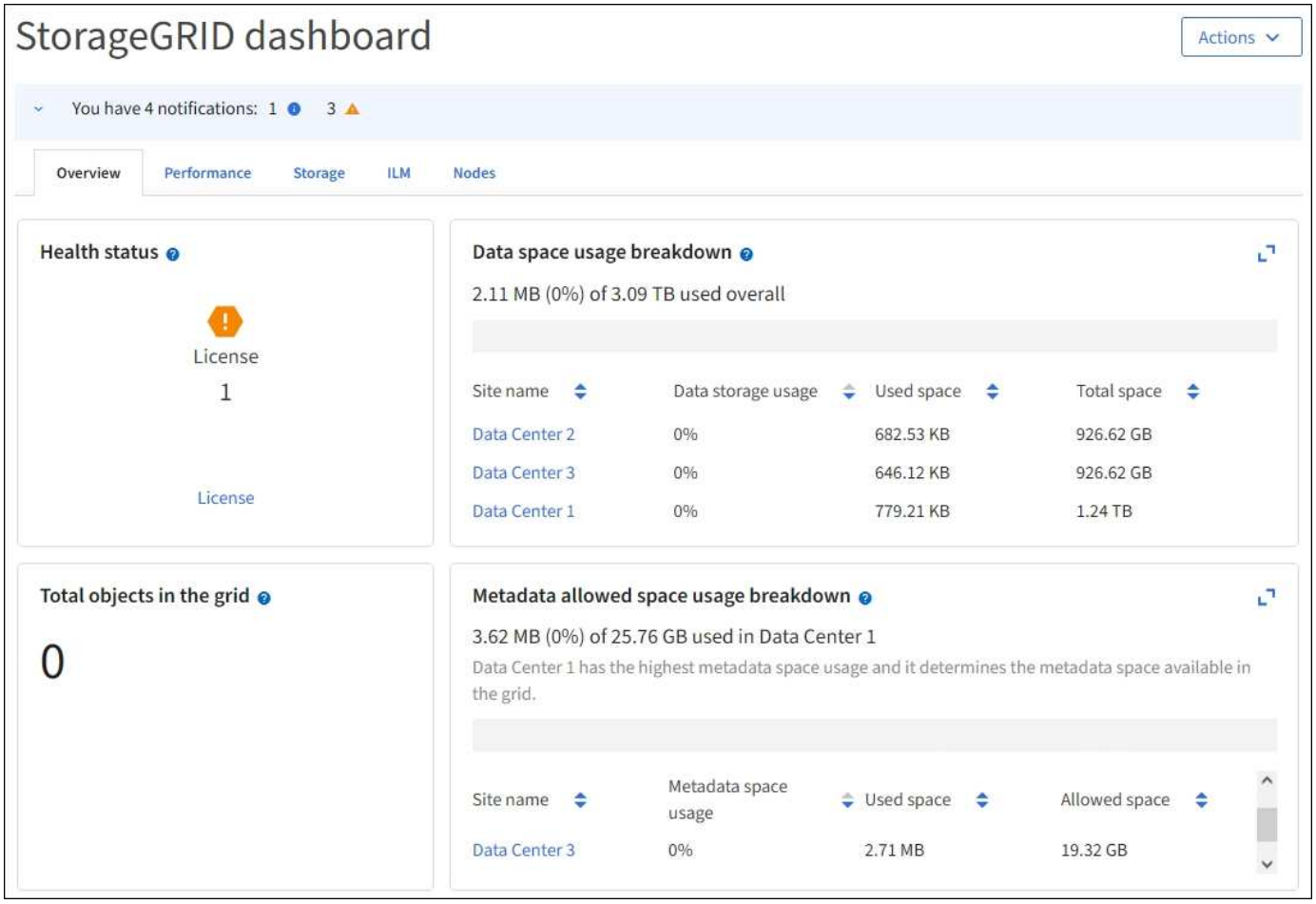
在 StorageGRID 中查看和管理信息板

您可以使用信息板一目了然地监控系统活动。您可以创建自定义信息板来监

控StorageGRID 的实施。

要更改网格管理器中显示的存储值的单位，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。

您的信息板可能会因系统配置而有所不同。



查看信息板

信息板包含多个选项卡、其中包含有关StorageGRID 系统的特定信息。每个选项卡都包含卡片上显示的信息类别。

您可以按原样使用系统提供的信息板。此外、您还可以创建仅包含与监控StorageGRID 实施相关的选项卡和卡片的自定义信息板。

系统提供的信息板选项卡包含具有以下类型信息的卡：

选项卡	包含
概述	有关网格的常规信息、例如活动警报、空间使用量和网格中的总对象数。
性能	空间使用量、一段时间内使用的存储、S3操作、请求持续时间、错误率。

选项卡	包含
存储	租户配额使用量和逻辑空间使用量。预测用户数据和元数据的空间使用量。
ILM	信息生命周期管理队列和评估率。
节点	按节点显示的CPU、数据和内存使用情况。按节点执行S3操作。节点到站点分布。

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

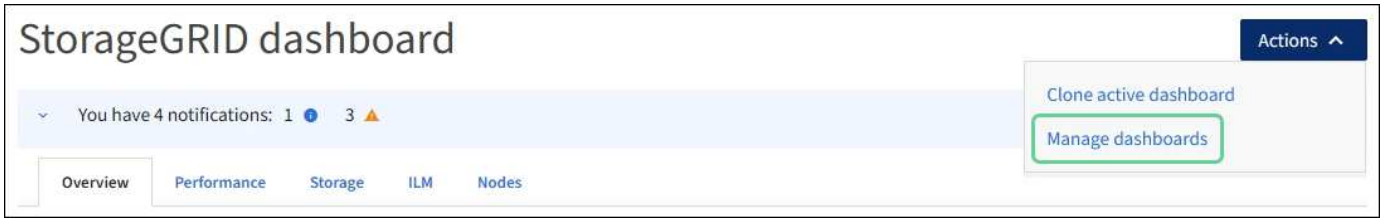
管理信息板

如果您具有root访问权限(请参见"管理组权限")，则可以对信息板执行以下管理任务：

- 从头开始创建自定义信息板。您可以使用自定义信息板控制显示的StorageGRID 信息以及该信息的组织方式。
- 克隆信息板以创建自定义信息板。
- 为用户设置活动信息板。活动信息板可以是系统提供的信息板、也可以是自定义信息板。
- 设置默认信息板、除非用户激活自己的信息板、否则所有用户都会看到该信息板。
- 编辑信息板名称。
- 编辑信息板以添加或删除选项卡和卡。您至少可以有1个选项卡、最多可以有20个选项卡。
- 删除信息板。

如果您拥有除root访问权限之外的任何其他权限、则只能设置活动信息板。

要管理信息板，请选择*Actions*>*Manage Dards*。



配置信息板

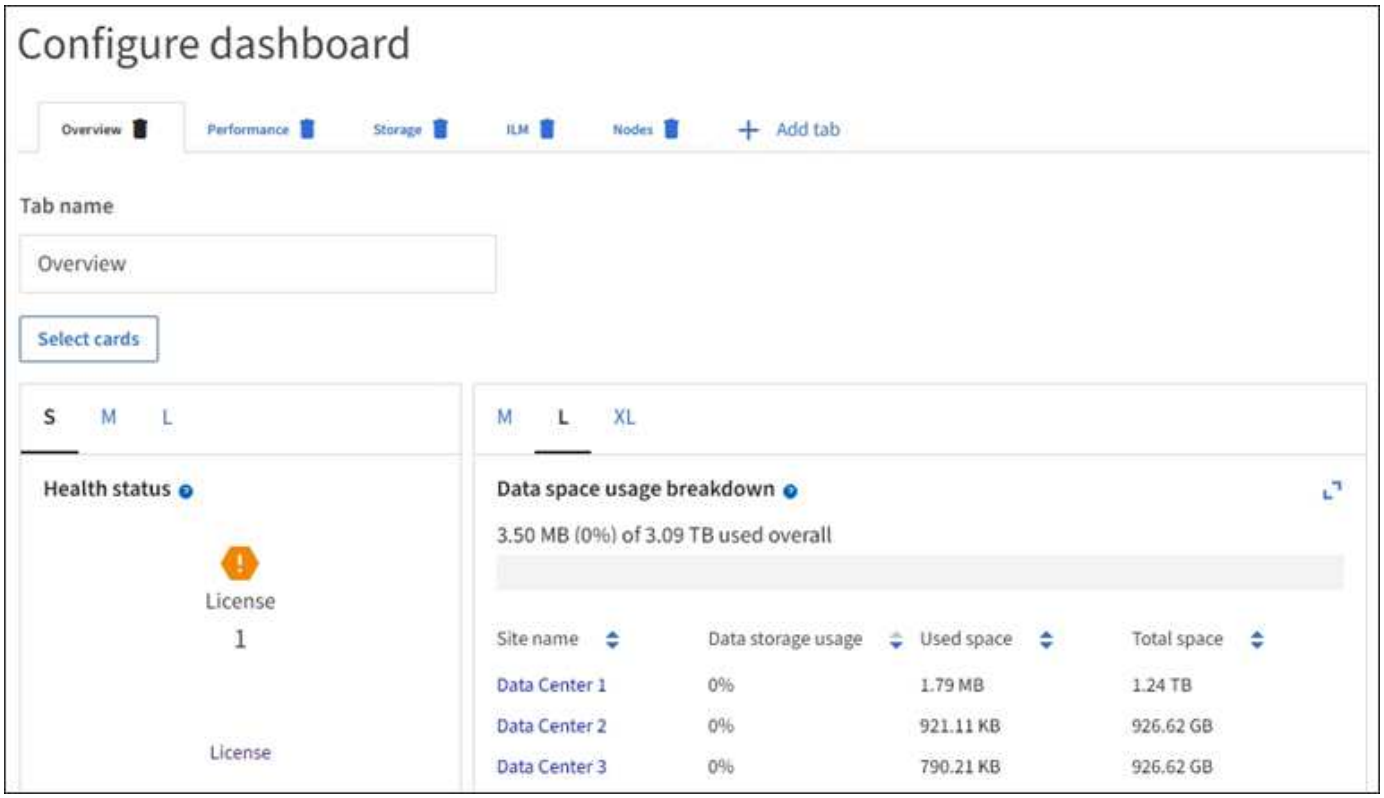
要通过克隆活动信息板来创建新信息板，请选择*Actions*>*Clone active DDashboard *。

要编辑或克隆现有信息板，请选择*Actions*>*Manage Dards*。

无法编辑或删除系统提供的信息板。

配置信息板时、您可以：

- 添加或删除选项卡
- 重命名选项卡并为新选项卡指定唯一名称
- 为每个选项卡添加、删除或重新排列(拖动)卡片
- 选择卡片顶部的*S*、**M**、**L***或***XL**，选择单张卡片的大小



查看节点页面

查看 **StorageGRID** 节点页面

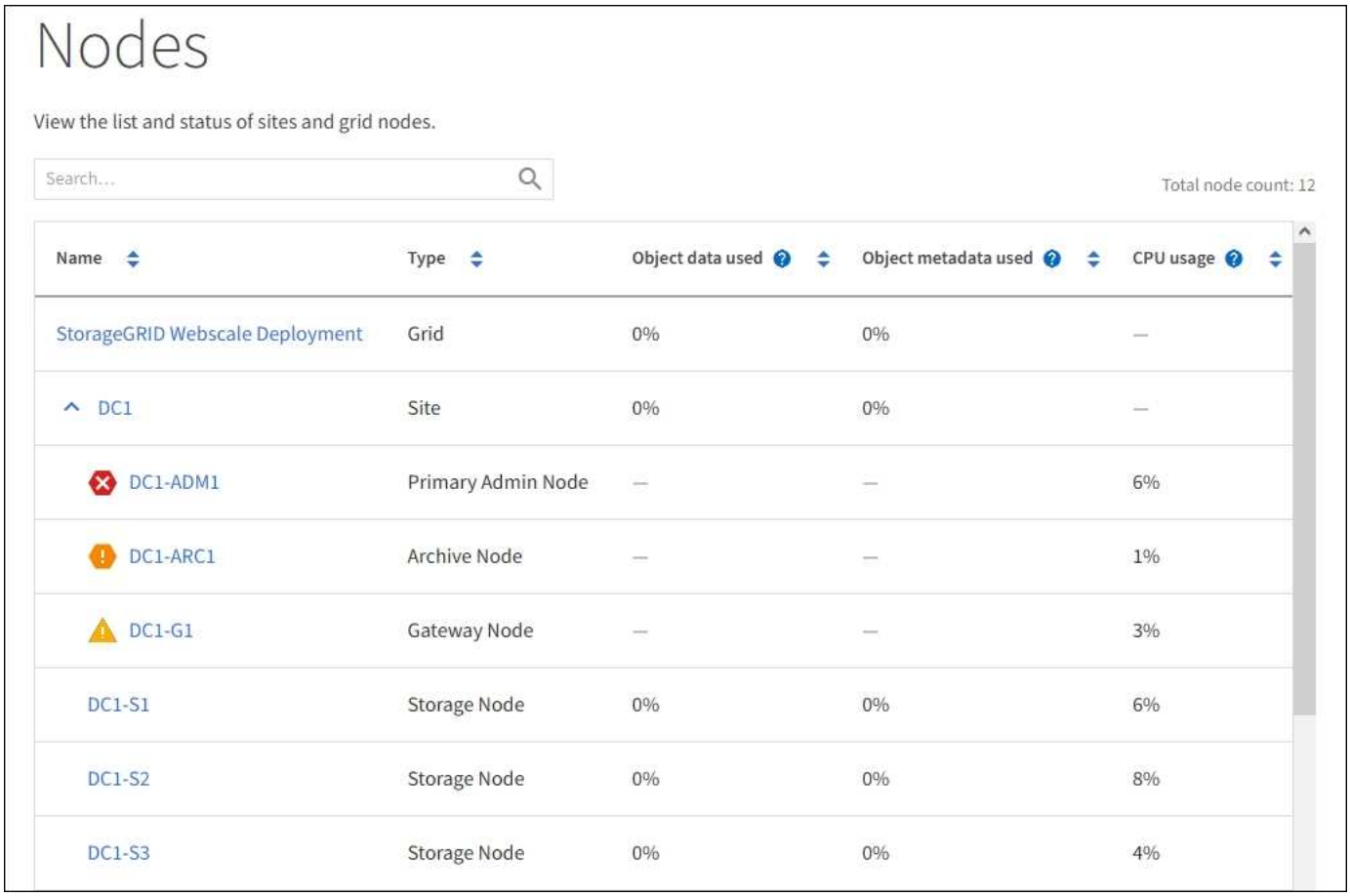
如果您需要的StorageGRID 系统信息比信息板提供的信息更详细、可以使用节点页面查看整个网格、网格中的每个站点以及站点中的每个节点的指标。

节点表列出了整个网格、每个站点和每个节点的摘要信息。如果节点已断开连接或存在活动警报、则节点名称旁边会显示一个图标。如果节点已连接且没有活动警报，则不会显示任何图标。

如果节点未连接到网格、例如在升级期间或处于断开状态时、某些指标可能不可用或不在站点和网格总数中。节点重新连接到网格后、请等待几分钟、使值稳定下来。

要更改网格管理器中显示的存储值的单位，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。

所示屏幕截图仅为示例。结果可能因StorageGRID版本而异。



连接状态图标

如果节点与网格断开连接、则节点名称旁边会显示以下任一图标。

图标	说明	需要执行操作
	• 未连接 - 未知 * 由于未知原因、节点已断开连接或节点上的服务意外关闭。例如，节点上的服务可能已停止，或者节点可能已因电源故障或意外中断而丢失网络连接。 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。	需要立即关注。"选择每个警报"并按照建议的操作进行操作。 例如，您可能需要重新启动已停止的服务或重新启动节点的主机。 注意：在受管关闭操作期间，节点可能显示为未知。在这些情况下，您可以忽略未知状态。

图标	说明	需要执行操作
	• 未连接 - 已管理员关闭 * 出于预期原因、节点未连接到网格。 例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。一个或多个警报可能也处于活动状态。 根据底层问题描述 、这些节点通常无需任何干预即可恢复联机。	确定是否有任何警报正在影响此节点。 如果一个或多个警报处于活动状态、"选择每个警报"请按照建议的操作进行操作。

如果节点与网格断开连接、则可能会出现底层警报、但仅会显示"未连接"图标。要查看节点的活动警报，请选择节点。

警报图标

如果节点存在活动警报，则节点名称旁边会显示以下图标之一：

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

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

Minor：系统正常运行，但存在异常情况，如果继续运行，可能会影响系统的运行能力。您应该监控并解决未自行清除的轻微警报，以确保它们不会导致更严重的问题。

查看系统、站点或节点的详细信息

要筛选节点表中显示的信息，请在*Search*字段中输入搜索字符串。您可以按系统名称、显示名称或类型进行搜索(例如，输入*gat*以快速查找所有网关节点)。

要查看网格、站点或节点的信息、请执行以下操作：

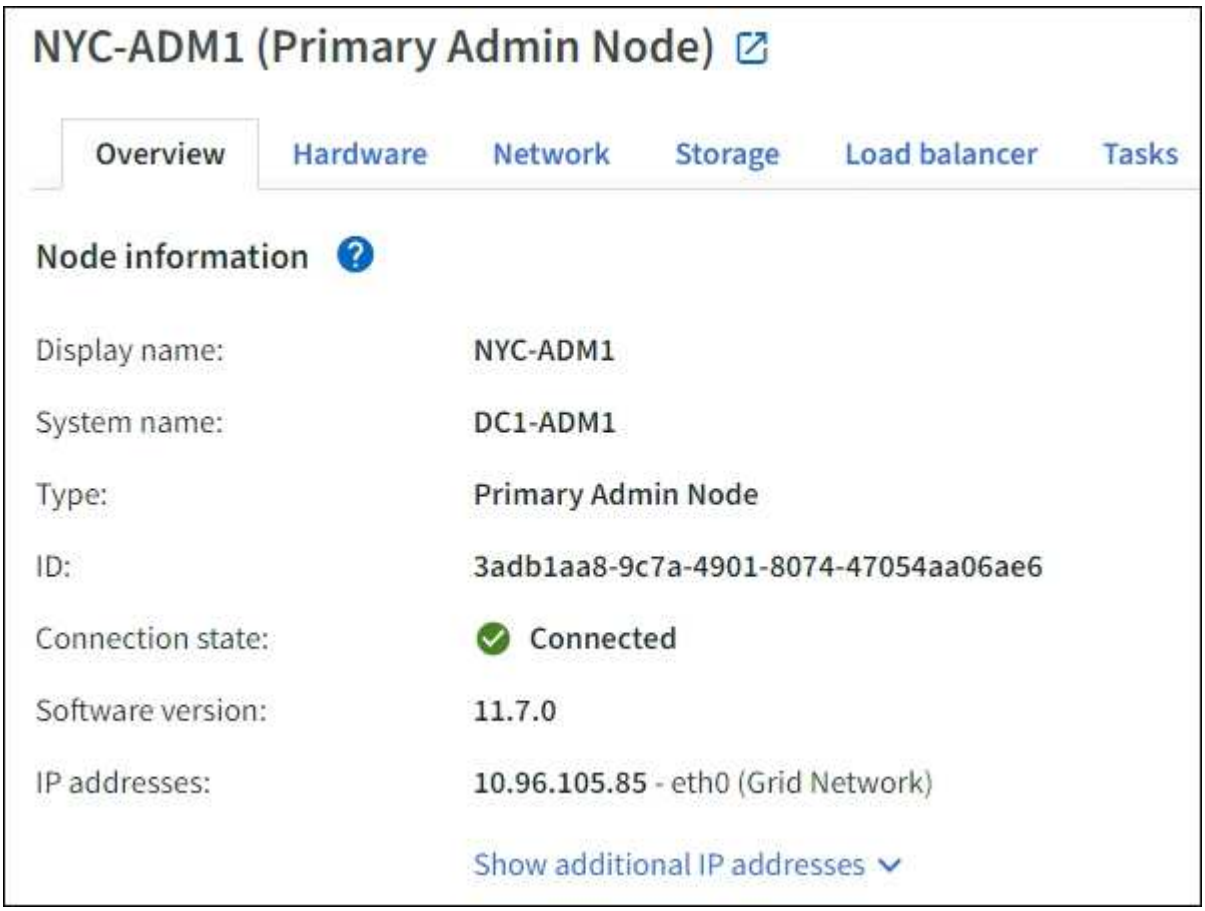
- 选择网格名称可查看整个 StorageGRID 系统统计信息的聚合摘要。
- 选择一个特定的数据中心站点，以查看该站点上所有节点的统计信息的聚合摘要。
- 选择一个特定节点以查看该节点的详细信息。

查看 **StorageGRID Overview** 选项卡

概述选项卡提供了有关每个节点的基本信息。此外，它还会显示当前影响节点的任何警报。

此时将显示所有节点的概述选项卡。

概述选项卡的节点信息部分列出了有关节点的基本信息。



节点的概述信息包括：

- **Display name**(仅在节点已重命名时显示)：节点的当前显示名称。使用"重命名网格、站点和节点"步骤更新此值。
- 系统名称：您在安装期间为节点输入的名称。系统名称用于内部StorageGRID 操作、无法更改。
- 类型：节点的类型—管理节点、主管理节点、存储节点或网关节点。
- * ID * ：节点的唯一标识符，也称为 UUID 。
- * 连接状态 * ：三种状态之一。此时将显示最严重状态的图标。
  - 未知 ：由于未知原因，节点未连接到网格，或者一个或多个服务意外关闭。例如，节点之间的网络连接已丢失、电源已关闭或服务已关闭。*无法与节点通信*警报也可能被触发。其他警报也可能处于活动状态。这种情况需要立即关注。

    在受管关闭操作期间，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。

  - 管理性关闭 ：由于预期的原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭、节点正在重新启动或软件正在升级。一个或多个警报也可能处于活动状态。
  - 已连接 ：节点已连接到网格。

- * 已用存储 * ： 仅适用于存储节点。
  - * 对象数据 * ： 存储节点上已使用的对象数据总可用空间的百分比。
  - * 对象元数据 * ： 存储节点上已使用的对象元数据的总允许空间百分比。
- * 软件版本 * ： 节点上安装的 StorageGRID 版本。
- * HA 组 * ： 仅适用于管理节点和网关节点。如果节点上的网络接口包含在高可用性组中，并且该接口是否为主接口，则显示此信息。
- **IP addresses**：节点的 IP 地址。选择 **Show additional IP addresses** 以查看节点的 IPv4 和 IPv6 地址以及接口映射。

警报

“概述”选项卡的“警报”部分列出了任何"当前影响此节点且尚未被禁止的警报"。选择警报名称可查看其他详细信息和建议的操作。



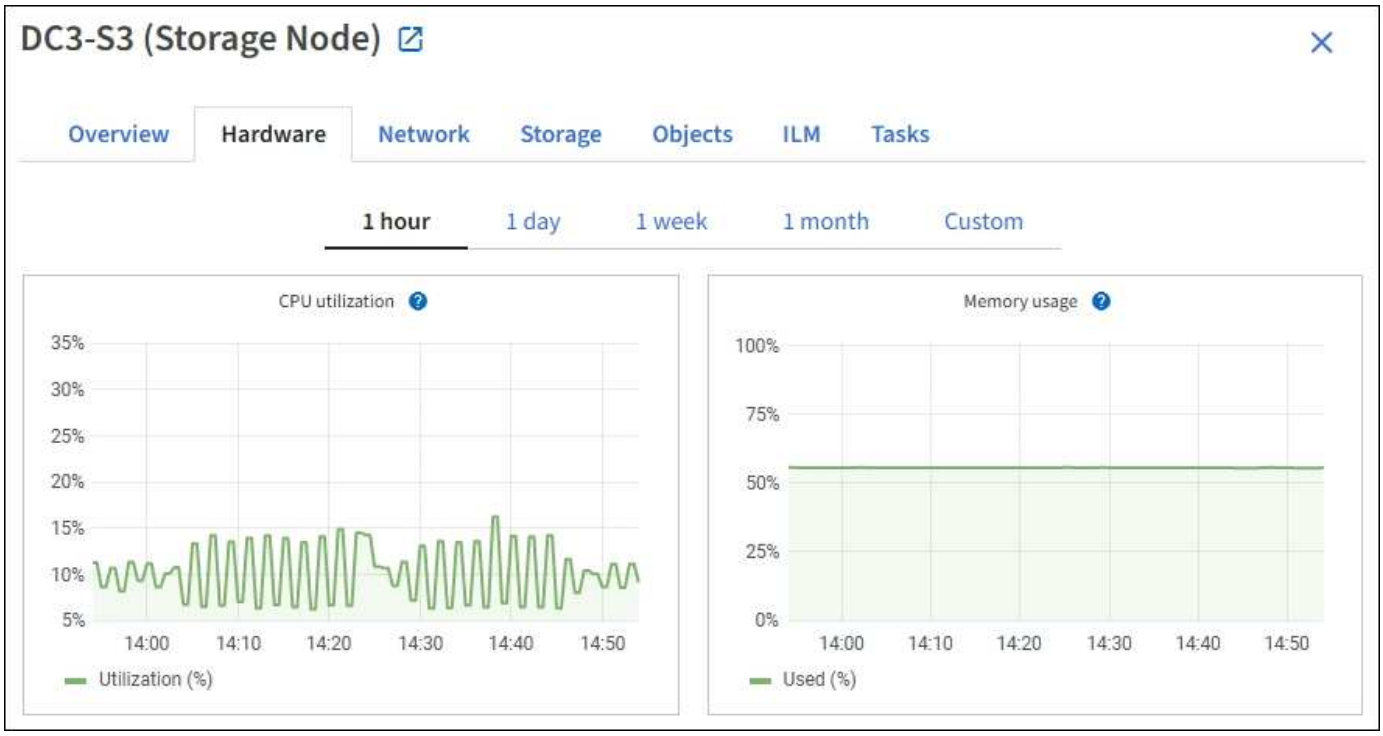
警报也包括在"节点连接状态"中。

查看 **StorageGRID** 硬件选项卡

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

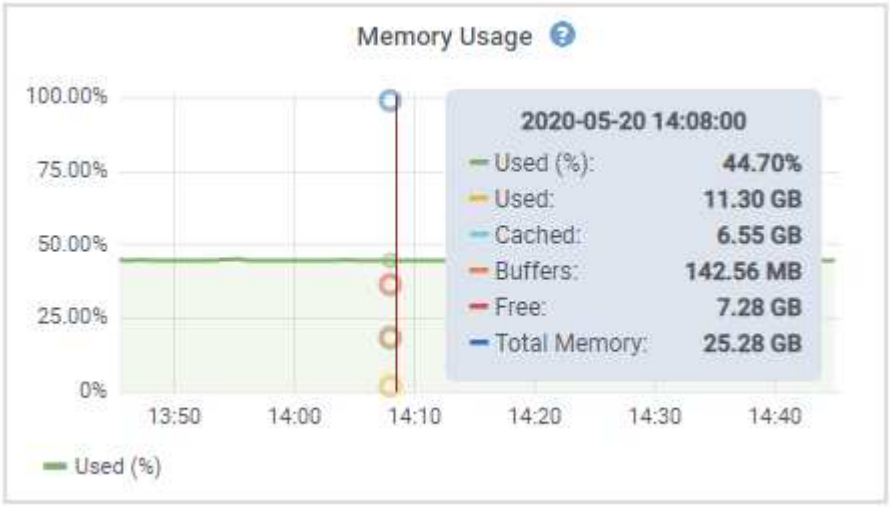
Grid Manager随每个版本更新、可能与此页面上的示例屏幕截图不匹配。

此时将显示所有节点的硬件选项卡。



要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。

要查看CPU利用率和内存使用情况的详细信息、请将光标置于每个图形上方。



如果节点是设备节点，则此选项卡还会包含一个部分，其中包含有关设备硬件的详细信息。

查看有关设备存储节点的信息

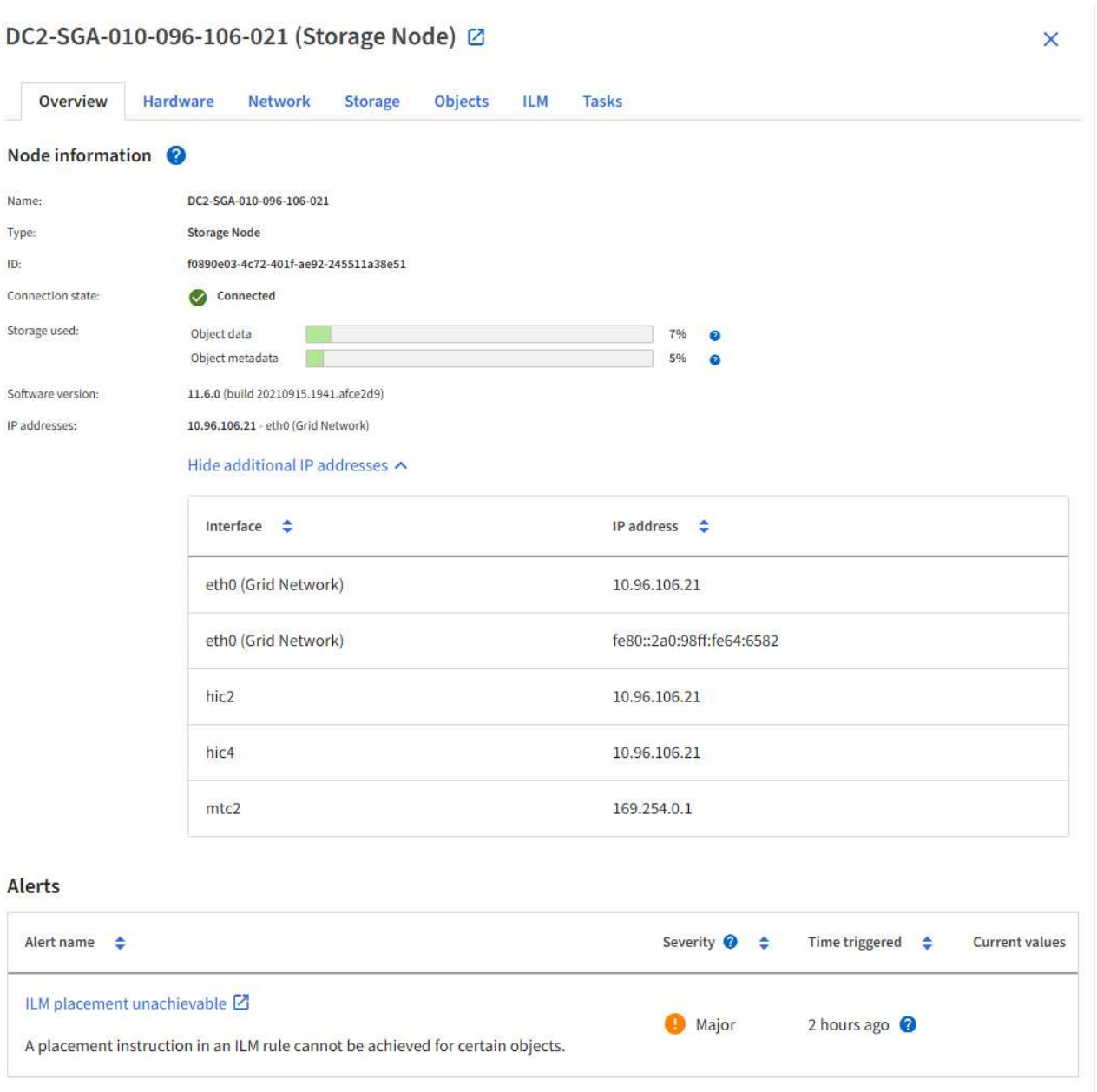
节点页面列出了有关每个设备存储节点的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，控制器固件版本，网络资源，网络接口， 网络地址以及接收和传输数据。

步骤

1. 从节点页面中，选择设备存储节点。
2. 选择 * 概述 * 。

" 概述 " 选项卡的 " 节点信息 " 部分显示节点的摘要信息，例如节点的名称，类型， ID 和连接状态。IP 地址列表包括每个地址的接口名称，如下所示：

- * eth * ： 网格网络，管理网络或客户端网络。
- * hic* ： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
- * MTC* ： 设备上的一个物理 1 GbE 端口。一个或多个 MTC 接口已绑定，以构成 StorageGRID 管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。

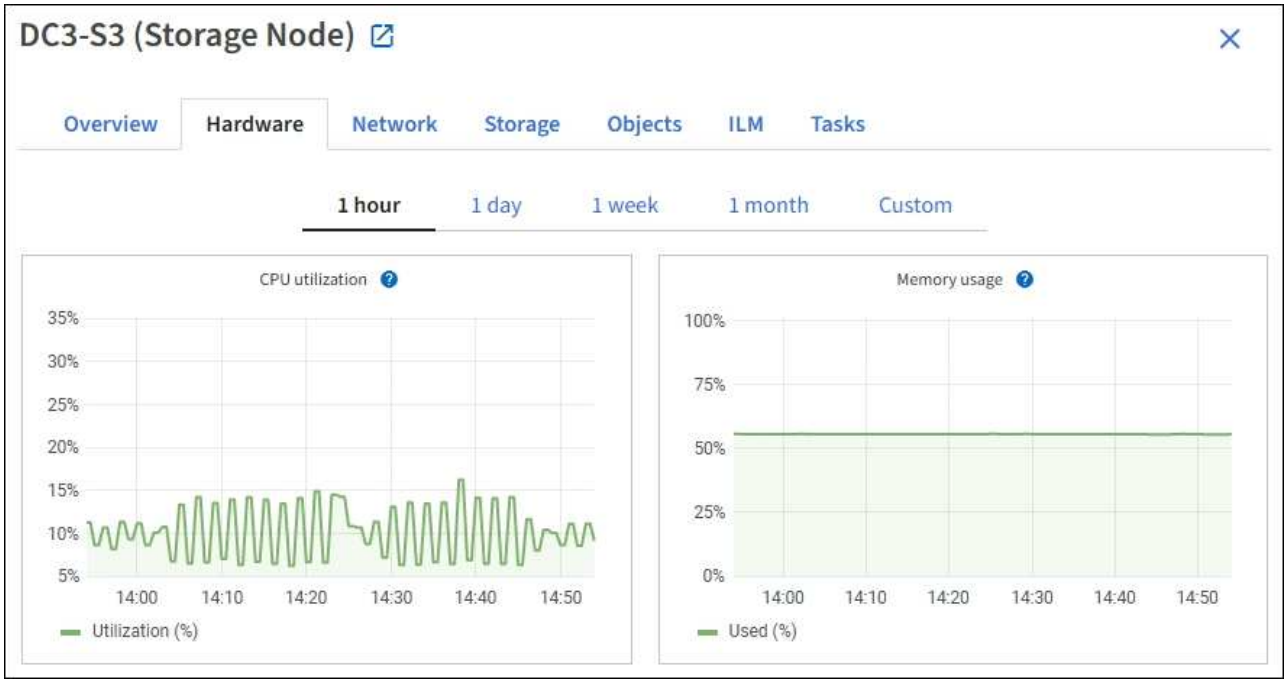


" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

3. 选择 * 硬件 * 可查看有关此设备的详细信息。

   a. 查看 CPU 使用率和内存使用率图表，以确定一段时间内 CPU 和内存使用率的百分比。要显示不同的时间间隔，请选择图表或图形上方的一个控件。您可以显示间隔为 1 小时、1 天、1 周或 1 个月的可用信

息。您还可以设置自定义间隔，以便指定日期和时间范围。



b. 向下滚动以查看设备组件表。此表包含设备的型号名称，控制器名称，序列号和 IP 地址以及每个组件的状态等信息。

某些字段（例如计算控制器 BMC IP 和计算硬件）仅针对具有此功能的设备显示。

存储架和扩展架（如果是安装的一部分）的组件会显示在设备表下方的单独表中。

字段	说明
设备型号	SANtricity OS中显示的此StorageGRID 设备的型号。
存储控制器名称	SANtricity OS中显示的此StorageGRID 设备的名称。
存储控制器 A 管理 IP	存储控制器A上管理端口1的IP地址。您可以使用此IP访问SANtricity操作系统来解决存储问题。
存储控制器 B 的管理 IP	存储控制器B上管理端口1的IP地址。您可以使用此IP访问SANtricity操作系统来解决存储问题。 某些设备型号没有存储控制器B
存储控制器 WWID	SANtricity 操作系统中显示的存储控制器的全球通用标识符。
存储设备机箱序列号	设备的机箱序列号。
存储控制器固件版本	此设备的存储控制器上的固件版本。

字段	说明
存储控制器SANtricity操作系统版本	存储控制器A的SANtricity操作系统版本
存储控制器NVstoragean版本	系统管理器报告的存储控制器的SANtricity版本。 对于SG6060和SG6160、如果这两个控制器之间的NVSG版本不匹配、则会显示控制器A的版本。如果控制器A未安装或未正常运行、则会显示控制器B的版本。
存储硬件	存储控制器硬件的整体状态。如果 SANtricity System Manager 报告存储硬件的状态为 "Needs Attention （需要注意） "，则 StorageGRID 系统也会报告此值。 如果状态为"需要引起注意"、请首先使用SANtricity操作系统检查存储控制器。然后、确保不存在适用于此计算控制器的其他警报。
存储控制器故障驱动器计数	不是最佳驱动器的数量。
存储控制器 A	存储控制器 A 的状态
存储控制器 B	存储控制器B的状态。某些设备型号没有存储控制器B
存储控制器电源 A	存储控制器的电源 A 的状态。
存储控制器电源 B	存储控制器的电源 B 的状态。
存储数据驱动器类型	设备中的驱动器类型、例如HDD (硬盘驱动器)或SSD (固态驱动器)。
存储数据驱动器大小	一个数据驱动器的有效大小。 对于SG6160、还会显示缓存驱动器的大小。 注意：对于带有扩展架的节点、请改用每个磁盘架的数据驱动器大小。有效驱动器大小可能因磁盘架而异。
存储 RAID 模式	为设备配置的 RAID 模式。
存储连接	存储连接状态。
整体电源	设备的所有电源的状态。

字段	说明
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller ， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含BMC的设备型号、不会显示此字段。
计算控制器序列号	计算控制器的序列号。
计算硬件	计算控制器硬件的状态。对于没有单独计算硬件和存储硬件的设备型号、不会显示此字段。
计算控制器 CPU 温度	计算控制器 CPU 的温度状态。
计算控制器机箱温度	计算控制器的温度状态。
计算控制器电源 A	计算控制器电源 A 的状态。
计算控制器电源B	计算控制器的电源 B 状态。

+

存储架表中的列	说明
磁盘架机箱序列号	存储架机箱的序列号。
磁盘架 ID	存储架的数字标识符。 • 99 ： 存储控制器架 • 0 ： 第一个扩展架 • 1 ： 第二个扩展架 *注：*扩展架仅适用于SG6060和SG6160。
磁盘架状态	存储架的整体状态。
IOM状态	任何扩展架中的输入 / 输出模块（ IOM ）的状态。不适用于扩展架。
电源状态	存储架电源的整体状态。
抽盒状态	存储架中抽盒的状态。不适用，如果磁盘架不包含抽盒。
风扇状态	存储架中的散热风扇的整体状态。

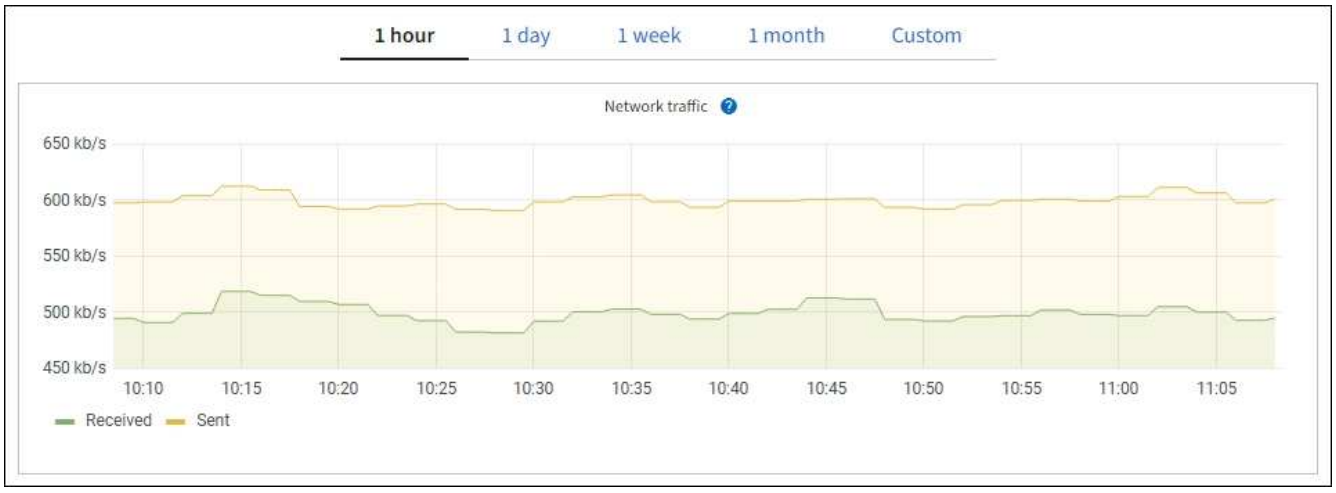
存储架表中的列	说明
驱动器插槽	存储架中的驱动器插槽总数。
数据驱动器	存储架中用于数据存储的驱动器数量。
【磁盘架数据驱动器大小】数据驱动器大小	存储架中一个数据驱动器的有效大小。
缓存驱动器	存储架中用作缓存的驱动器数量。
缓存驱动器大小	存储架中最小缓存驱动器的大小。通常，缓存驱动器的大小相同。
配置状态	存储架的配置状态。

a. 确认所有状态均为"标称"。

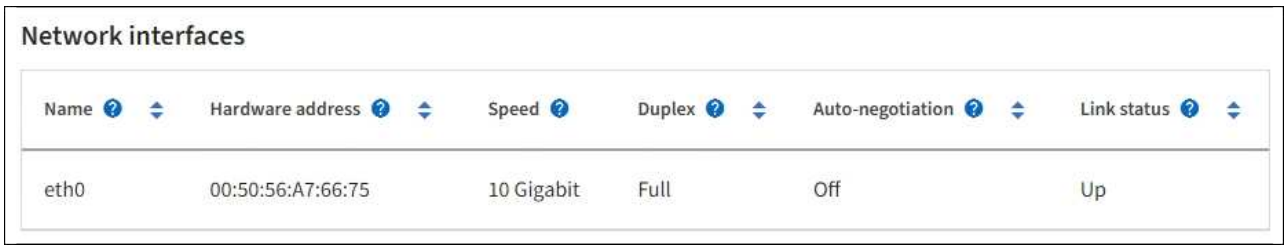
如果状态不是"标称"、请查看任何当前警报。您还可以使用 SANtricity 系统管理器详细了解其中一些硬件值。请参见有关安装和维护设备的说明。

4. 选择 * 网络 * 可查看每个网络的信息。

网络流量图提供了整体网络流量的摘要。



a. 请查看"网络接口"部分。



使用下表以及网络接口表中*速度*列中的值，确定设备上的 10/25-GbE 网络端口是否配置为使用主动/备

份模式或 LACP 模式。

表中显示的值假定使用了所有四个链路。

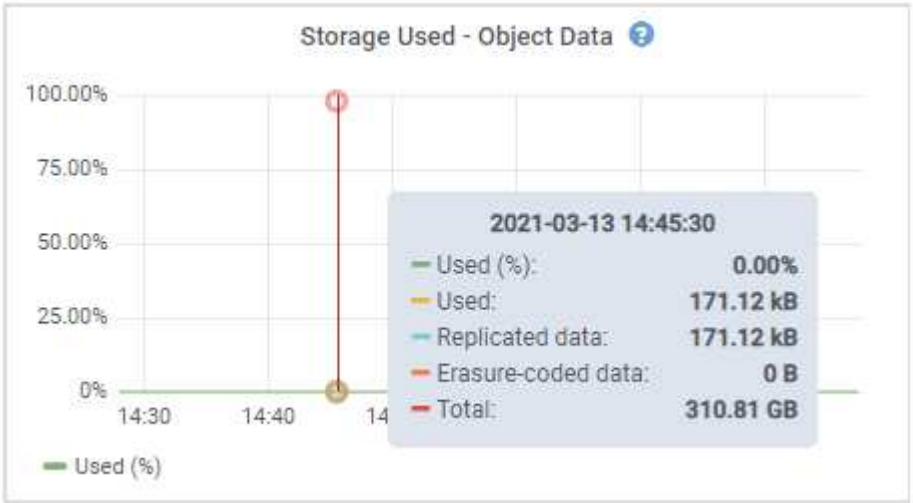
链路模式	绑定模式	单个 **HIC** 链路速度（ **hic1** ， **hic2** ， **hic3** ， **hic4** ）	预期网格 / 客户端网络速度（ **eth0** ， **eth2** ）
聚合	LACP	25	100
已修复	LACP	25	50
已修复	主动 / 备份	25	25
聚合	LACP	10	40
已修复	LACP	10	20
已修复	主动 / 备份	10	10

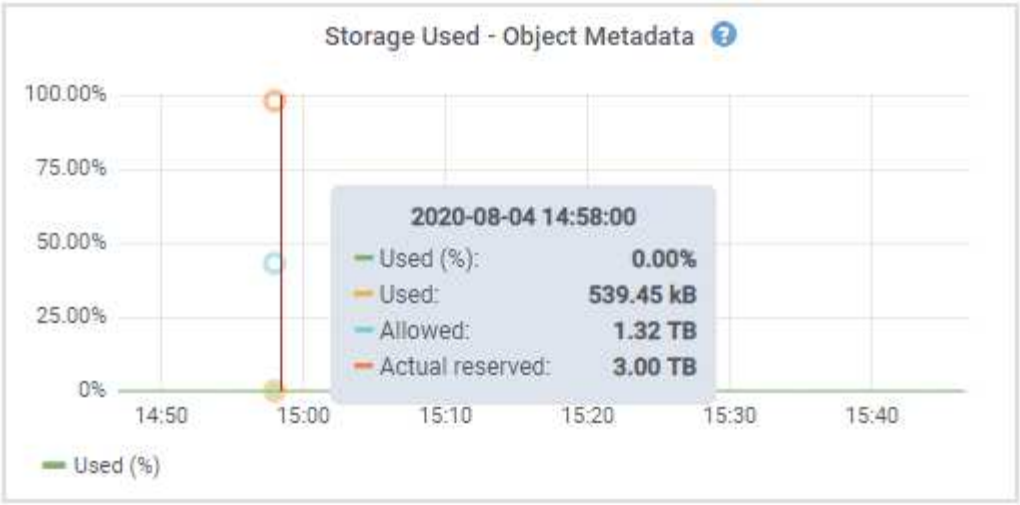
+
有关配置10/C5-GbE端口的详细信息、请参见 "配置网络链路"。

a. 请查看"网络通信"部分。

   接收和传输表显示了通过每个网络接收和发送的字节数和数据包数，以及其他接收和传输指标。

5. 选择 * 存储 * 可查看显示对象数据和对象元数据在一段时间内所用存储百分比的图形，以及有关磁盘设备，卷和对象存储的信息。





a. 向下滚动以查看每个卷和对象存储的可用存储容量。

   每个磁盘的全球通用名称与在SANtricity OS (连接到设备存储控制器的管理软件)中查看标准卷属性时显示的卷全球通用标识符(WWID)匹配。

为了帮助您解释与卷挂载点相关的磁盘读取和写入统计信息，磁盘设备表的 * 名称 * 列（即 *sdc* ， *sdd* ， *sde* 等）中显示的名称的第一部分与卷表的 * 设备 * 列中显示的值匹配。

查看有关设备管理节点和网关节点的信息

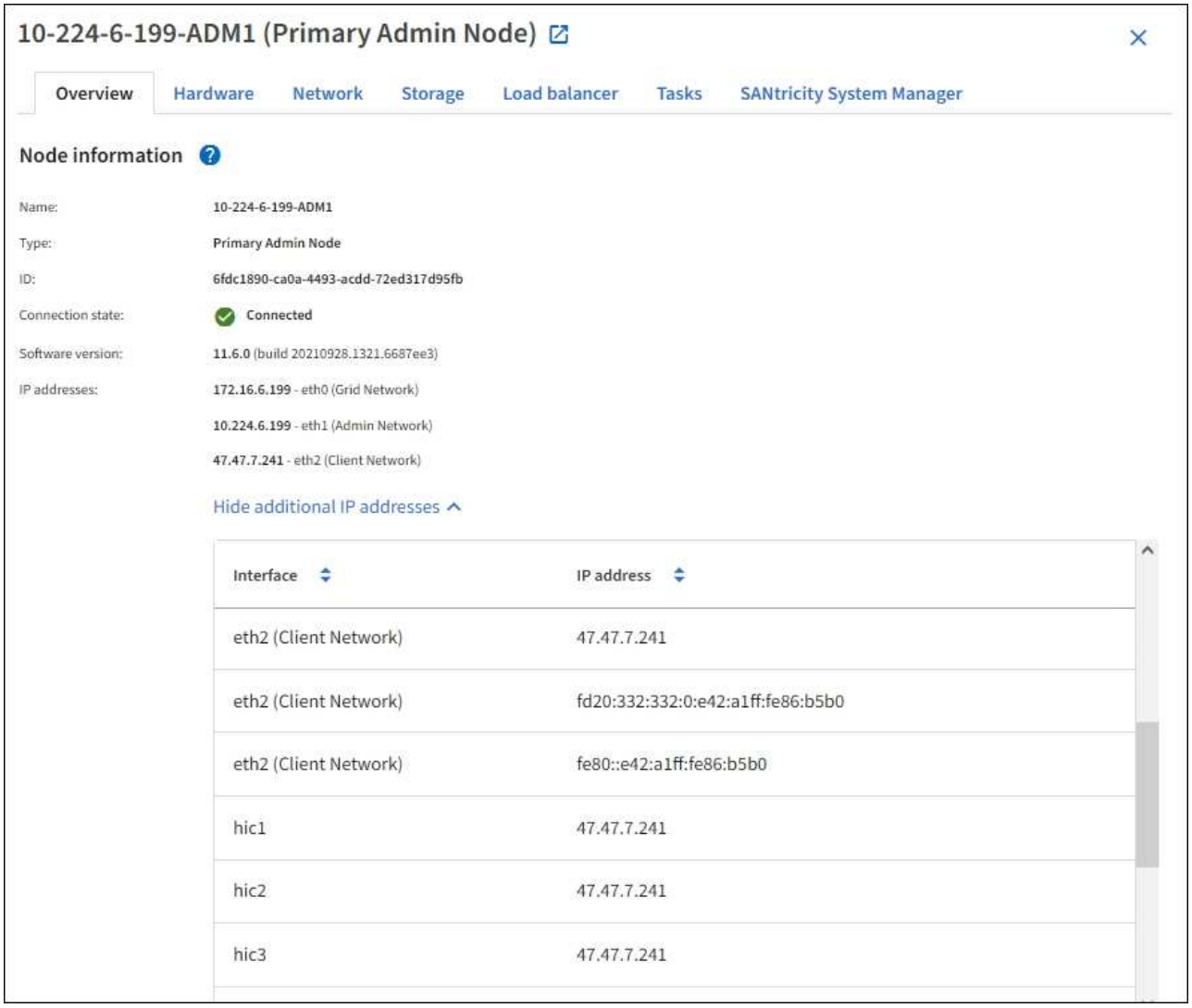
节点页面列出了有关用作管理节点或网关节点的每个服务设备的服务运行状况以及所有计算，磁盘设备和网络资源的信息。您还可以查看内存，存储硬件，网络资源，网络接口，网络地址， 以及接收和传输数据。

步骤

1. 从节点页面中，选择设备管理节点或设备网关节点。
2. 选择 * 概述 * 选项卡。

   " 概述 " 选项卡的 " 节点信息 " 部分显示节点的摘要信息，例如节点的名称，类型， ID 和连接状态。IP 地址列表包括每个地址的接口名称，如下所示：

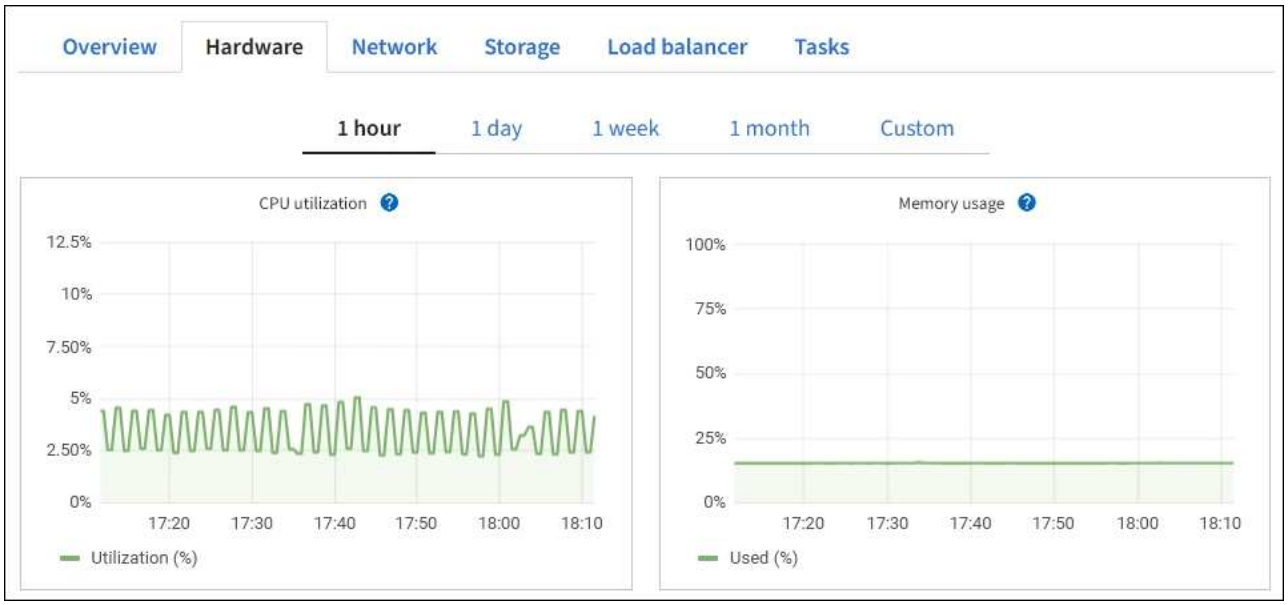
   - * adllb* 和 * adlli* ： 如果对管理网络接口使用主动 / 备份绑定，则显示此信息
   - * eth * ： 网格网络，管理网络或客户端网络。
   - * hic* ： 设备上的一个物理 10 ， 25 或 100 GbE 端口。这些端口可以绑定在一起，并连接到 StorageGRID 网格网络（ eth0 ）和客户端网络（ eth2 ）。
   - * MTC* ： 设备上的一个物理 1-GbE 端口。一个或多个 MTC 接口已绑定，以构成管理网络接口（ eth1 ）。您可以保留其他 MTC 接口，以便数据中心的技术人员临时进行本地连接。



" 概述 " 选项卡的 " 警报 " 部分显示节点的任何活动警报。

3. 选择*硬件*选项卡以查看有关设备的详细信息。

   a. 查看 CPU 利用率和内存图形，确定 CPU 和内存使用量随时间的变化所占百分比。要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。



b. 向下滚动以查看设备的组件表。该表包含型号名称、序列号、控制器固件版本以及每个组件的状态等信息。

字段	说明
设备型号	此 StorageGRID 设备的型号。
存储控制器故障驱动器计数	不是最佳驱动器的数量。
存储数据驱动器类型	设备中的驱动器类型、例如HDD (硬盘驱动器)或SSD (固态驱动器)。
存储数据驱动器大小	一个数据驱动器的有效大小。
存储 RAID 模式	设备的 RAID 模式。
整体电源	设备中所有电源的状态。
计算控制器 BMC IP	计算控制器中的基板管理控制器（ Baseboard Management Controller， BMC ）端口的 IP 地址。您可以使用此 IP 连接到 BMC 界面来监控和诊断设备硬件。 对于不包含BMC的设备型号、不会显示此字段。
计算控制器序列号	计算控制器的序列号。
计算硬件	计算控制器硬件的状态。
计算控制器 CPU 温度	计算控制器 CPU 的温度状态。

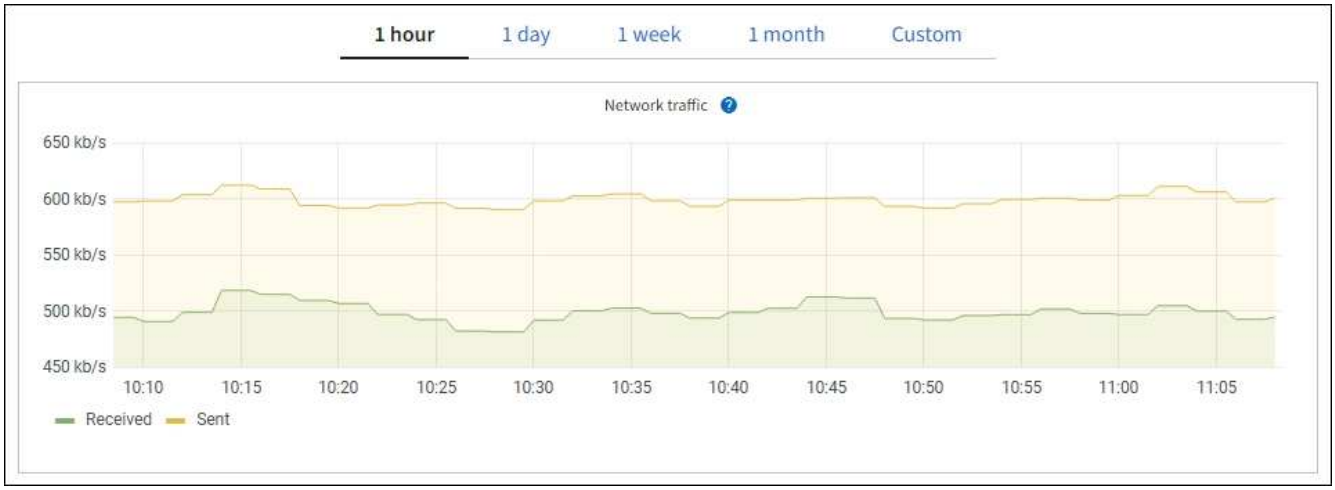
字段	说明
计算控制器机箱温度	计算控制器的温度状态。

c. 确认所有状态均为"标称"。

如果状态不是"标称"、请查看任何当前警报。

4. 选择*网络*选项卡可查看每个网络的信息。

网络流量图提供了整体网络流量的摘要。



a. 请查看"网络接口"部分。

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

表中显示的值假定使用了所有四个链路。

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

a. 请查看"网络通信"部分。

   接收和传输表显示了通过每个网络接收和发送的字节数和数据包数，以及其他接收和传输指标。

5. 选择*存储*选项卡以查看有关服务设备上磁盘设备和卷的信息。

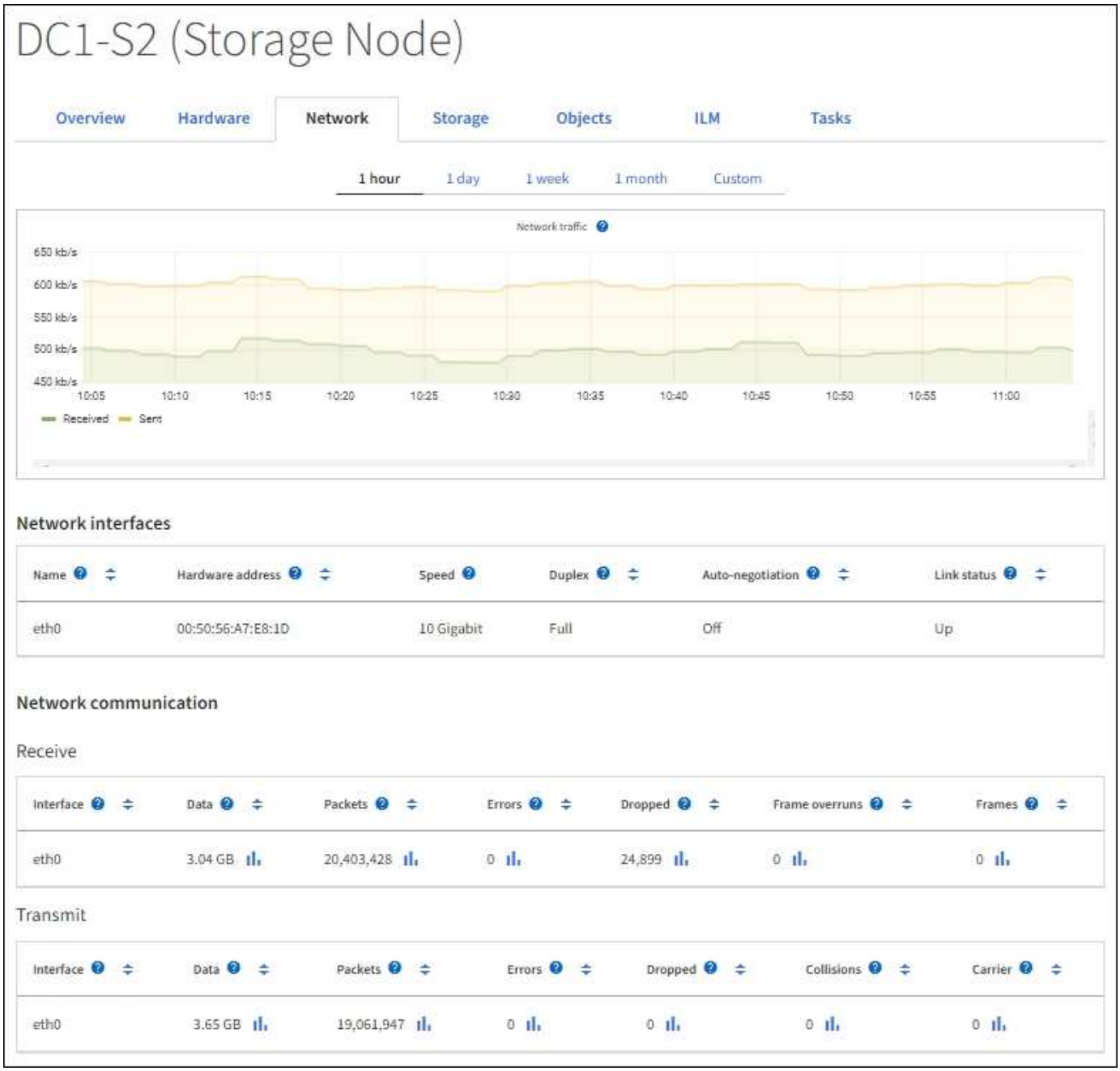
查看 **StorageGRID Network** 选项卡

网络选项卡显示一个图形，其中显示了通过节点，站点或网格上的所有网络接口接收和发送的网络流量。

此时将显示所有节点，每个站点和整个网格的网络选项卡。

要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。

对于节点，网络接口表提供了有关每个节点的物理网络端口的信息。网络通信表提供了有关每个节点的接收和传输操作以及任何驱动程序报告的故障计数器的详细信息。



相关信息

"监控网络连接和性能"

查看 **StorageGRID Storage** 选项卡

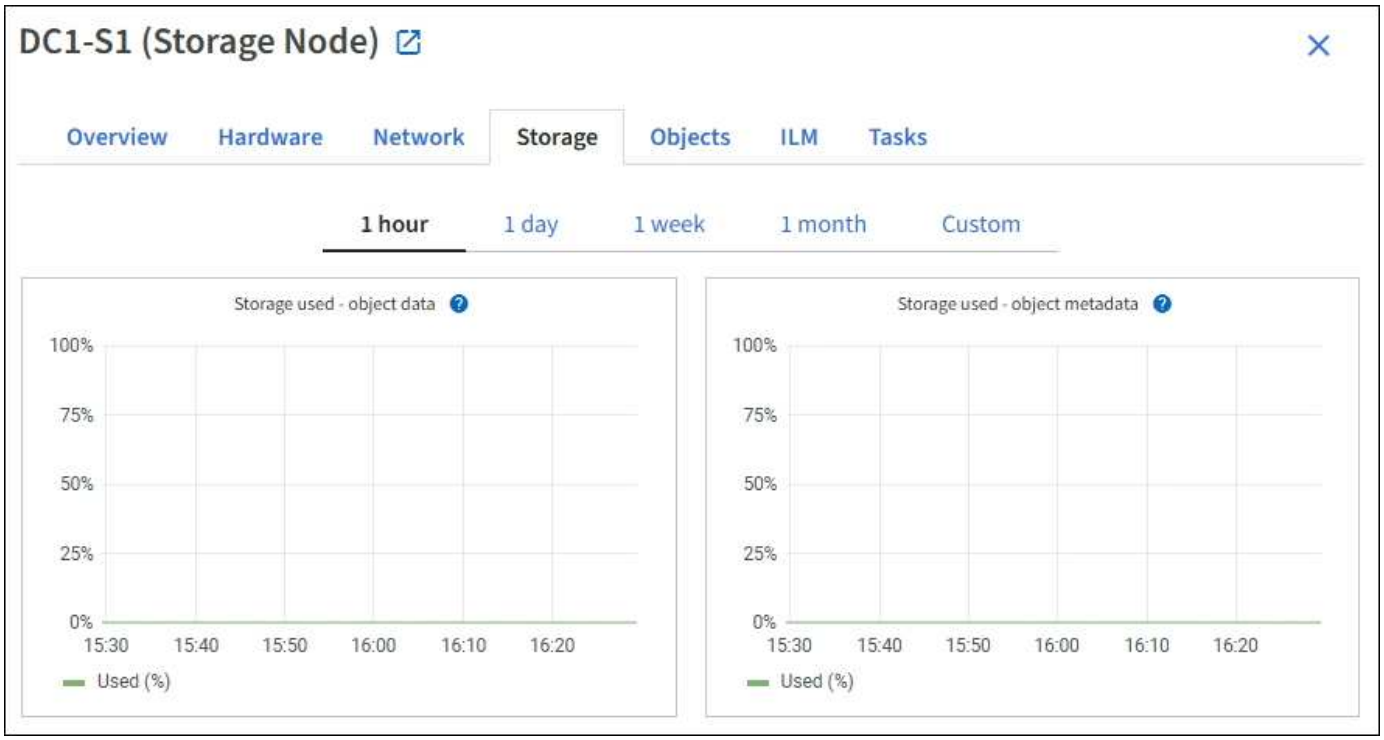
存储选项卡汇总了存储可用性和其他存储指标。

显示所有节点、每个站点和整个网格的"存储"选项卡。此选项卡包含以下信息：

已用存储图

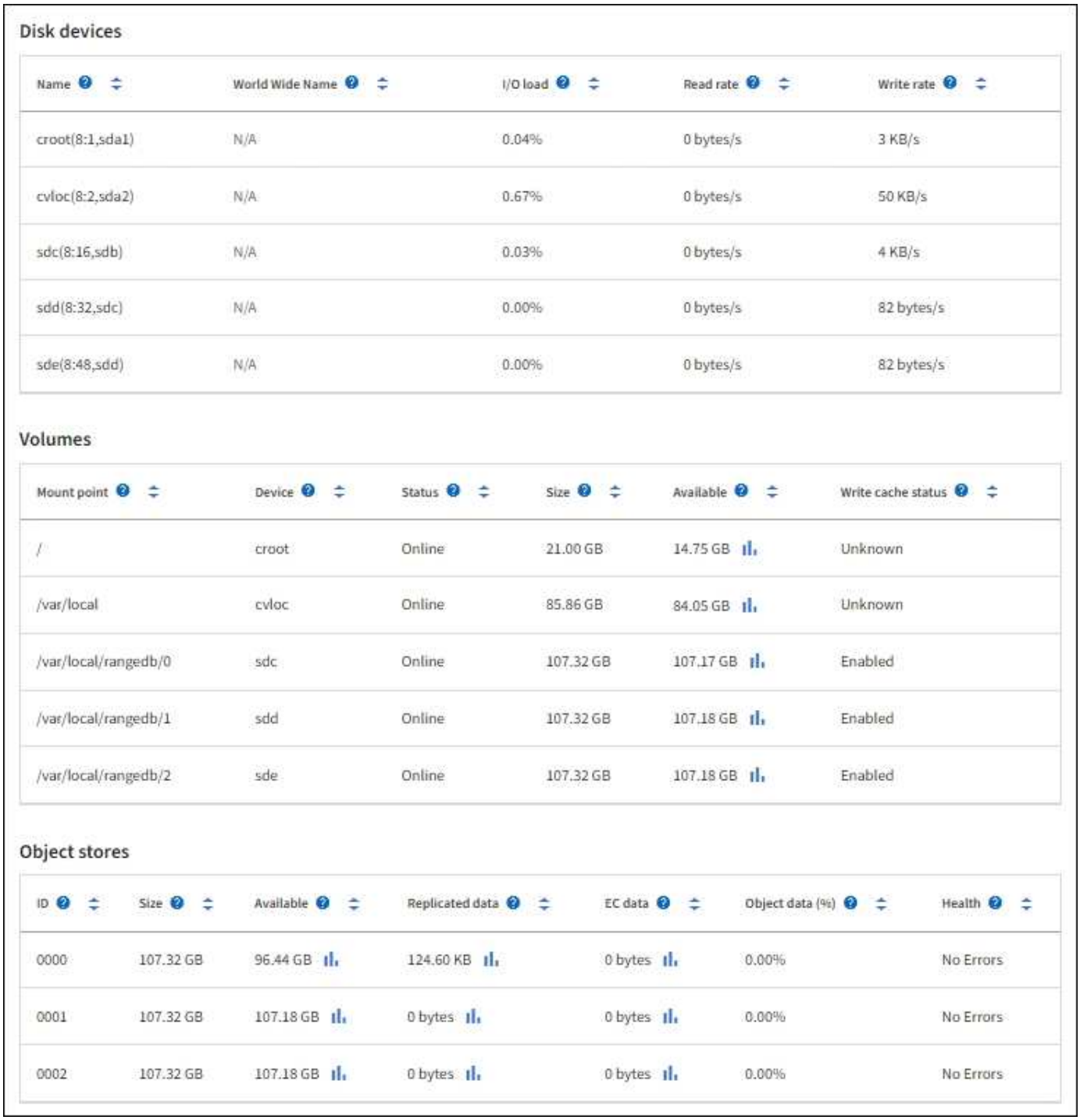
对于存储节点，每个站点和整个网格， " 存储 " 选项卡包含一些图形，用于显示对象数据和对象元数据在一段时间内使用了多少存储。

如果节点未连接到网格、例如在升级期间或处于断开状态时、某些指标可能不可用或不在站点和网格总数中。节点重新连接到网格后、请等待几分钟、使值稳定下来。



磁盘设备，卷和对象存储表

对于所有节点，存储选项卡包含节点上磁盘设备和卷的详细信息。对于存储节点，对象存储表提供了有关每个存储卷的信息。



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

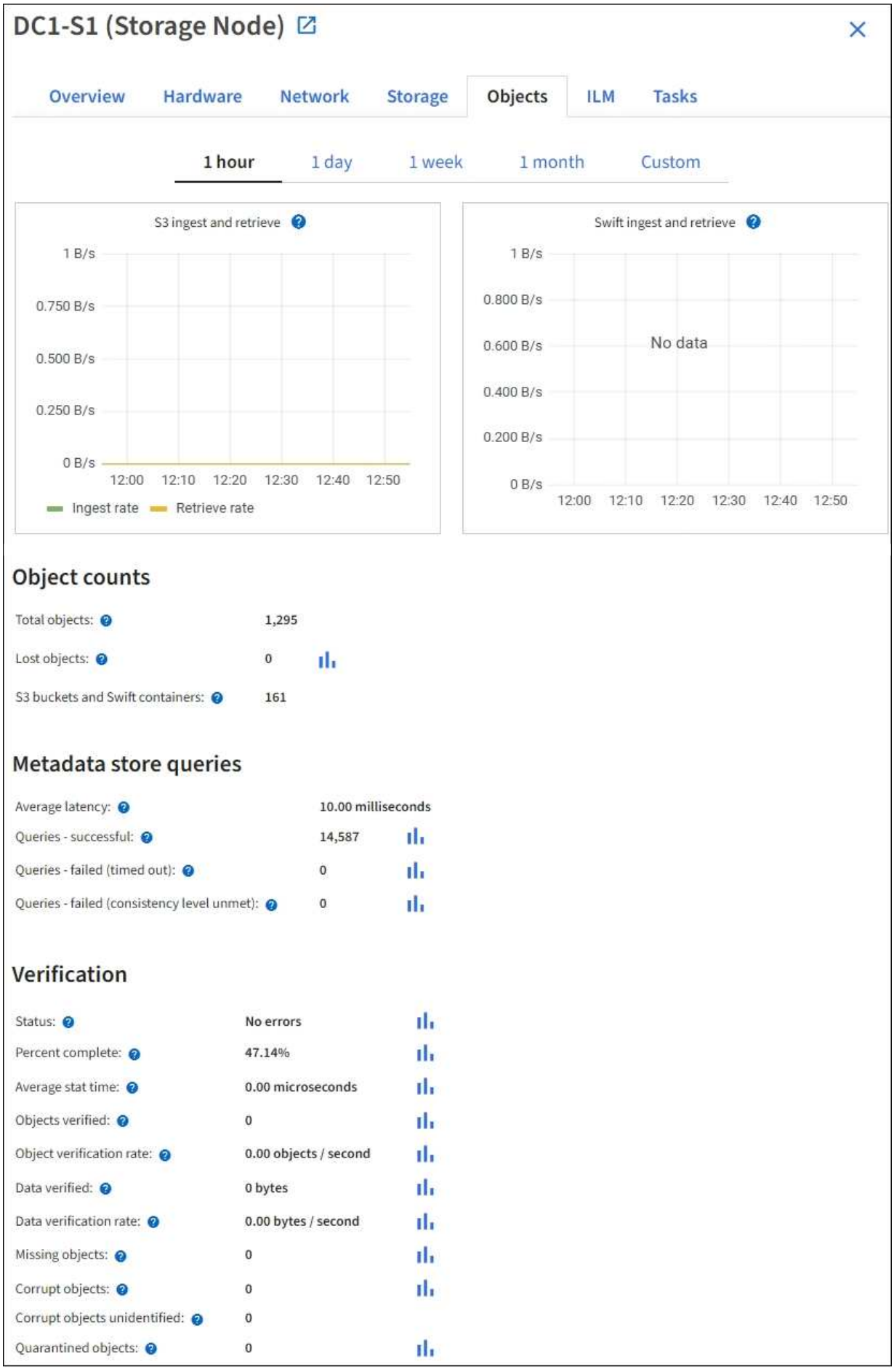
相关信息

"监控存储容量"

查看 **StorageGRID Objects** 选项卡

对象选项卡提供了有关的信息"S3读取和读取速率"。

此时将显示每个存储节点，每个站点和整个网格的对象选项卡。对于存储节点，对象选项卡还提供对象计数以及有关元数据查询和后台验证的信息。

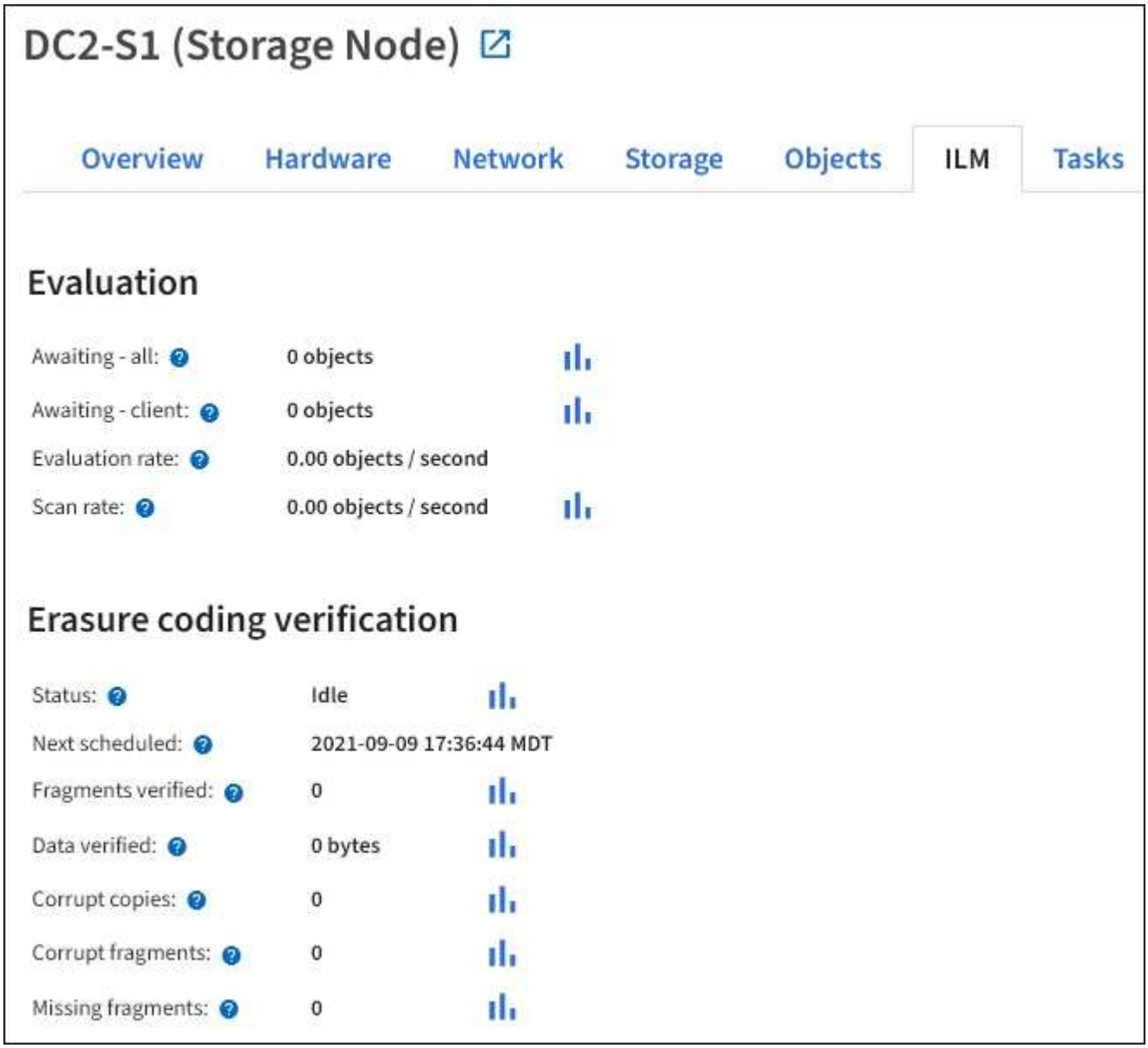

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

查看 **StorageGRID ILM** 选项卡

ILM选项卡提供了有关信息生命周期管理(ILM)操作的信息。

此时将显示每个存储节点，每个站点和整个网格的 ILM 选项卡。对于每个站点和网格， "ILM " 选项卡会显示一个 ILM 队列随时间变化的图形。对于网格，此选项卡还提供完成对所有对象的完整 ILM 扫描的估计时间。

对于存储节点、ILM选项卡提供了有关对已进行过身份验证的对象进行ILM评估和后台验证的详细信息。



相关信息

- "监控信息生命周期管理"
- "管理 StorageGRID"

使用 **StorageGRID** 任务选项卡

所有节点均显示“任务”选项卡。您可以使用此选项卡重命名或重新启动节点，或者将设备

节点置于维护模式。对于存储节点，您可以设置存储状态。

有关此选项卡上每个选项的完整要求和说明、请参见以下内容：

- "重命名网格、站点和节点"
- "重新启动网格节点"
- "将设备置于维护模式"
- 在将直接连接或 SAN 卷添加到存储节点后，或者在恢复存储节点后，您可以验证或设置存储节点的存储状态。这些说明可以在描述这些任务的主题中找到。

查看 **StorageGRID** 负载平衡器选项卡

" 负载平衡器 " 选项卡包含与负载平衡器服务的运行相关的性能和诊断图。

此时将为管理节点和网关节点，每个站点和整个网格显示负载平衡器选项卡。对于每个站点， " 负载平衡器 " 选项卡提供该站点所有节点的统计信息的聚合摘要。对于整个网格， " 负载平衡器 " 选项卡提供了所有站点统计信息的聚合摘要。

如果未通过负载平衡器服务运行任何I/O、或者未配置任何负载平衡器、则图形将显示"无数据"。



请求流量

此图提供了负载平衡器端点与发出请求的客户端之间传输的数据吞吐量的 3 分钟移动平均值，以每秒位数为单位。

此值将在每个请求完成时更新。因此，此值可能与请求率较低或请求寿命较长时的实时吞吐量不同。您可以查看 " 网络 " 选项卡，更真实地查看当前网络行为。

传入请求速率

此图按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分，提供每秒新请求数的 3 分钟移动平均值。验证新请求的标头后，此值将更新。

平均请求持续时间（非错误）

此图提供了按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分的 3 分钟移动平均请求持续时间。每个请求持续时间从负载平衡器服务解析请求标头时开始，到将完整的响应正文返回给客户端时结束。

错误响应率

此图提供了每秒返回给客户端的错误响应数的 3 分钟移动平均值，并按错误响应代码进行细分。

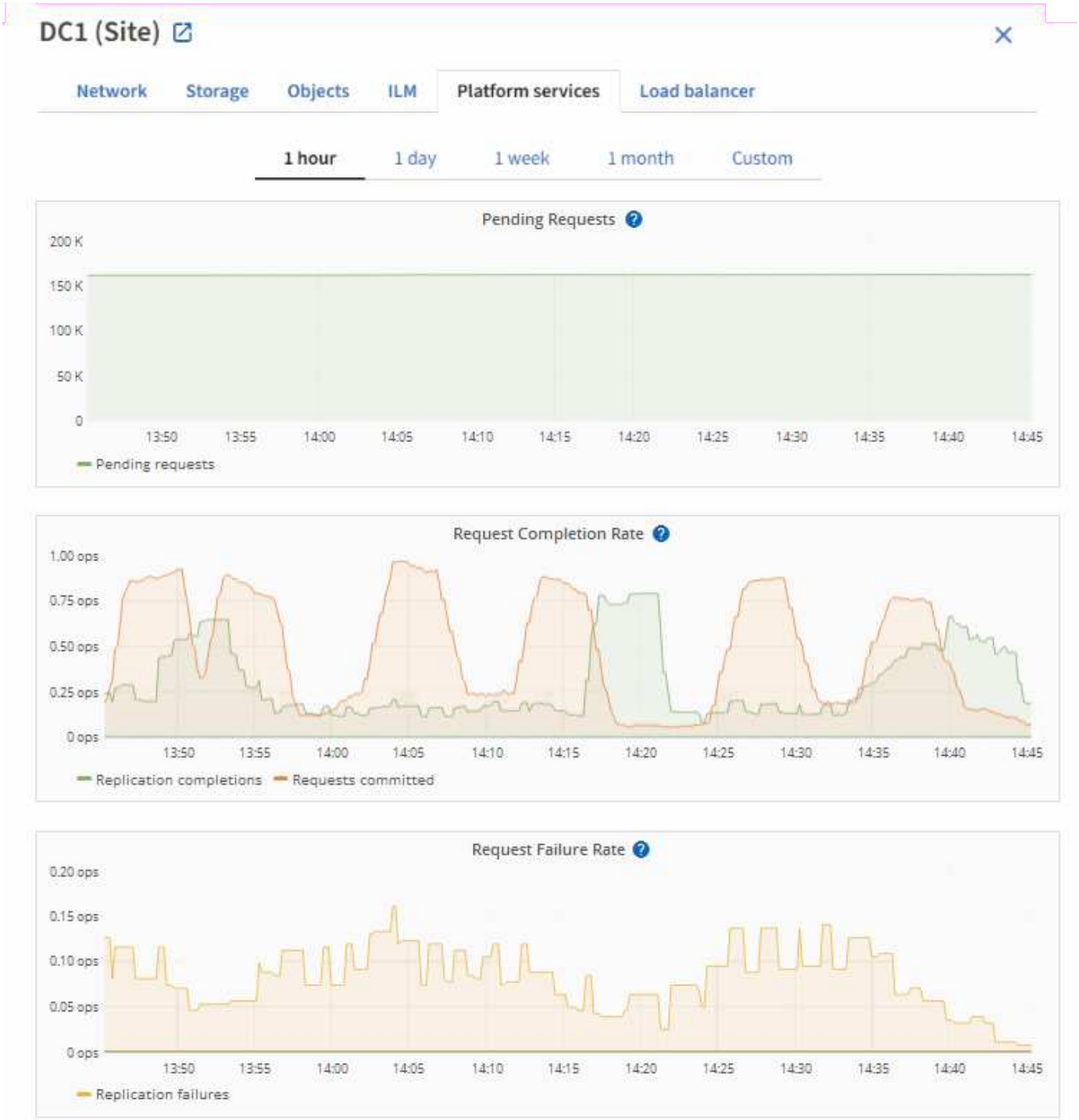
相关信息

- "监控负载平衡操作"
- "管理 StorageGRID"

查看 **StorageGRID** 平台服务选项卡

平台服务选项卡提供了有关站点上任何 S3 平台服务操作的信息。

此时将显示每个站点的平台服务选项卡。此选项卡提供了有关 S3 平台服务的信息，例如 CloudMirror 复制和搜索集成服务。此选项卡上的图形显示了待处理请求数，请求完成率和请求失败率等指标。



有关S3平台服务的详细信息(包括故障排除详细信息)，请参见"有关管理 StorageGRID 的说明"。

查看 **StorageGRID** 管理驱动器选项卡

通过管理驱动器选项卡、您可以访问详细信息、并对支持此功能的设备中的驱动器执行故障排除和维护任务。

使用管理驱动器选项卡、您可以执行以下操作：

- 查看设备中的数据存储驱动器布局

- 查看一个表、其中列出了每个驱动器位置、类型、状态、固件版本和序列号
- 对每个驱动器执行故障排除和维护功能

要访问“管理驱动器”选项卡，您必须拥有"存储设备管理员或root访问权限"。

有关使用管理驱动器选项卡的信息，请参阅 "使用管理驱动器选项卡"。

查看 **StorageGRID SANtricity System Manager** 选项卡

通过 SANtricity 系统管理器选项卡，您可以访问 SANtricity 系统管理器，而无需配置或连接存储设备的管理端口。您可以使用此选项卡查看硬件诊断和环境信息以及与驱动器相关的问题。

> 从网格管理器访问 SANtricity 系统管理器通常仅用于监控设备硬件和配置 E 系列 AutoSupport 。SANtricity 系统管理器中的许多功能和操作(例如升级固件)不适用于监控StorageGRID 设备。为避免出现问题、请始终按照设备的硬件维护说明进行操作。要升级SANtricity固件、请参见 "维护配置过程"适用于您的存储设备的。

> 只有使用E系列硬件的存储设备节点才会显示SANtricity 系统管理器选项卡。

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

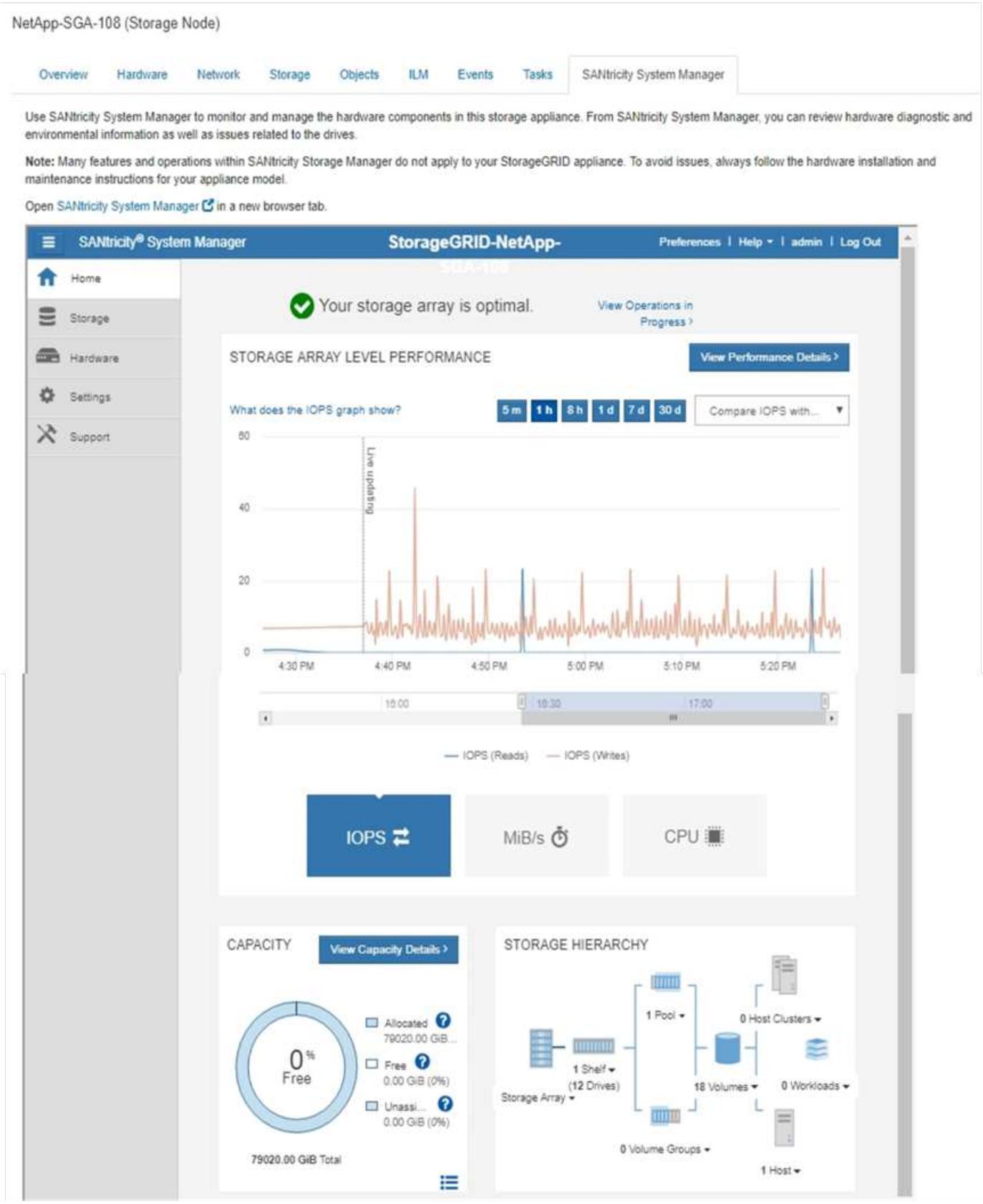
- 查看性能数据、例如存储阵列级别的性能、I/O延迟、存储控制器CPU利用率和吞吐量。
- 检查硬件组件状态。
- 执行支持功能、包括查看诊断数据和配置E系列AutoSupport。

> 要使用 SANtricity System Manager 为 E 系列 AutoSupport 配置代理，请参阅 "通过StorageGRID发送E系列AutoSupport软件包"。

要通过网格管理器访问SANtricity系统管理器，您必须拥有"存储设备管理员或root访问权限"。

> 要使用网格管理器访问 SANtricity 系统管理器，您必须具有 SANtricity 固件 8.70 或更高版本。

此选项卡将显示 SANtricity 系统管理器的主页。



您可以使用 SANtricity 系统管理器链接在新浏览器窗口中打开 SANtricity 系统管理器，以便于查看。

要查看存储阵列级别性能和容量使用情况的详细信息、请将光标置于每个图形上方。

有关查看可从SANtricity系统管理器选项卡访问的信息的详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

要定期监控的信息

在 **StorageGRID** 中监控什么以及何时监控

即使发生错误或部分网格不可用时StorageGRID 系统仍可继续运行、您也应监控并解决潜在问题、以免影响网格的效率或可用性。

开始之前

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

关于监控任务

繁忙的系统会生成大量信息。以下列表提供了有关需要持续监控的最重要信息的指导。

要监控的内容	频率
"系统运行状况"	每天
正在消耗的速率"存储节点对象和元数据容量"	每周
"信息生命周期管理操作"	每周
"网络和系统资源"	每周
"租户活动"	每周
"S3客户端操作"	每周
"负载平衡操作"	在初始配置之后以及任何配置更改之后
"网格联合连接"	每周

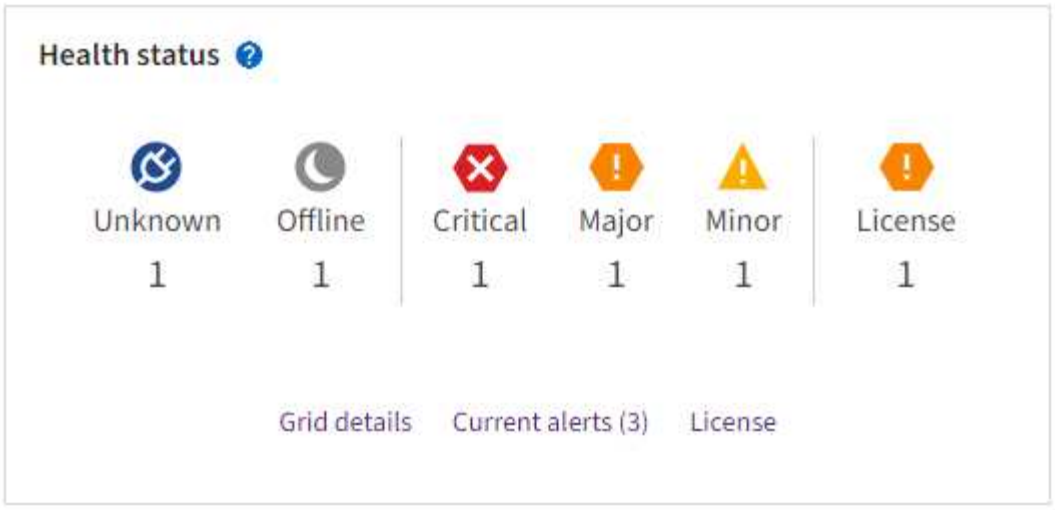
在 **StorageGRID** 中监控系统运行状况

每天监控StorageGRID 系统的整体运行状况。

关于此任务

StorageGRID 系统可在部分网格不可用时继续运行。警报指示的潜在问题不一定是系统操作的问题。调查Grid Manager信息板的运行状况卡上汇总的问题。

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



如果存在问题，则会显示一些链接，您可以通过这些链接查看其他详细信息：

链路	出现以下情况时显示...
网格详细信息	所有节点均已断开连接(连接状态未知或已被管理员关闭)。
当前警报(严重、主要、次要)	警报为当前处于活动状态。
最近解决的警报	过去一周触发的警报现已解决。
许可证	此StorageGRID 系统具有一个具有软件许可证的问题描述。您可以"根据需要更新许可证信息"。

监控节点连接状态

如果一个或多个节点与网格断开连接，则关键 StorageGRID 操作可能会受到影响。监控节点连接状态并及时解决任何问题。

图标	说明	需要执行操作
	• 未连接 - 未知 * 由于未知原因、节点已断开连接或节点上的服务意外关闭。例如，节点上的服务可能已停止，或者节点可能已因电源故障或意外中断而丢失网络连接。 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。	需要立即关注。选择每个警报并按照建议的操作进行操作。 例如，您可能需要重新启动已停止的服务或重新启动节点的主机。 注意：在受管关闭操作期间，节点可能显示为未知。在这些情况下，您可以忽略未知状态。

图标	说明	需要执行操作
	• 未连接 - 已管理员关闭 * 出于预期原因、节点未连接到网格。 例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。一个或多个警报可能也处于活动状态。 根据底层问题描述 、这些节点通常无需任何干预即可恢复联机。	确定是否有任何警报正在影响此节点。 如果一个或多个警报处于活动状态、选择每个警报请按照建议的操作进行操作。
	• 已连接 * 节点已连接到网格。	无需执行任何操作。

查看当前警报和已解决警报

当前警报：触发警报时、信息板上会显示警报图标。节点页面上还会显示节点的警报图标。如果"已配置警报电子邮件通知"是，则还会发送电子邮件通知，除非警报已被禁用。

已解决警报：您可以搜索和查看已解决警报的历史记录。

或者，您已经观看了视频：

警报概述

下表介绍了网格管理器中显示的当前警报和已解决警报的信息。

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

列标题	说明
时间已触发	当前警报：在您的本地时间和UTC时间内触发警报的日期和时间。如果对多个警报进行了分组，则标题行将显示警报的最新实例（ *lates* ）和最旧的警报实例（ *oldest* ）的时间。 已解决警报：警报在多长时间前触发。
站点 / 节点	正在或已发生警报的站点和节点的名称。
状态	警报处于活动状态、已被关闭还是已解决。如果对多个警报进行分组，并在下拉列表中选择了 * 所有警报 * ，则标题行将显示该警报处于活动状态的实例数以及已静音的实例数。
解决时间(仅限已解决警报)	警报解决多长时间前。
Current Values或_data values"	导致触发警报的度量值。对于某些警报，还会显示其他值，以帮助您了解和调查此警报。例如，为 "* 对象数据存储空间不足 * " 警报显示的值包括已用磁盘空间百分比，磁盘空间总量和已用磁盘空间量。 *注意：*如果对多个当前警报进行了分组，则当前值不会显示在标题行中。
触发值(仅限已解决警报)	导致触发警报的度量值。对于某些警报，还会显示其他值，以帮助您了解和调查此警报。例如，为 "* 对象数据存储空间不足 * " 警报显示的值包括已用磁盘空间百分比，磁盘空间总量和已用磁盘空间量。

步骤

1. 选择*当前警报*或*已解决警报*链接可查看这些类别的警报列表。您也可以通过选择*N节点*>* *NODE*>*Overview*并从“警报”表中选择警报来查看警报的详细信息。

   默认情况下、当前警报显示如下：

   - 首先显示最近触发的警报。
   - 同一类型的多个警报显示为一个组。
   - 未显示已被设置为"已被设置为"状态的警报。
   - 对于特定节点上的特定警报，如果达到阈值的严重性超过一个，则仅显示最严重的警报。也就是说，如果达到次要，主要和严重严重性的警报阈值，则仅显示严重警报。

     当前警报页面每两分钟刷新一次。

2. 要展开警报组，请选择向下插入符号 ⌄。要折叠组中的单个警报，请选择向上插入符号 ⌃，或选择组的名称。
3. 要显示单个警报而不是一组警报，请清除*组警报*复选框。
4. 要对当前警报或警报组进行排序，请选择每个列标题中的向上/向下箭头 ⇅。
   - 如果选择 * 组警报 * ，则会对每个组中的警报组和各个警报进行排序。例如，您可能希望按 * 时间触发 * 对组中的警报进行排序，以查找特定警报的最新实例。

- 清除*组警报*后，将对整个警报列表进行排序。例如，您可能希望按 * 节点 / 站点 * 对所有警报进行排序，以查看影响特定节点的所有警报。

5. 要按状态(所有警报、活动*或*已关闭)过滤当前警报，请使用表顶部的下拉菜单。

   请参阅。 "静默警报通知"

6. 对已解决的警报进行排序：
   - 从*触发时*下拉菜单中选择一个时间段。
   - 从*严重性*下拉菜单中选择一个或多个严重性。
   - 从 * 警报规则 * 下拉菜单中选择一个或多个默认或自定义警报规则，以筛选与特定警报规则相关的已解决警报。
   - 从 * 节点 * 下拉菜单中选择一个或多个节点，以筛选与特定节点相关的已解决警报。
7. 要查看特定警报的详细信息、请选择该警报。此时将显示一个对话框、其中提供了选定警报的详细信息和建议操作。
8. (可选)对于特定警报、选择SILENCE this alAlert,以使导致触发此警报的警报规则静音。

   您必须具有"管理警报或root访问权限"才能使警报规则静音。

   在决定静默警报规则时，请务必小心。如果某个警报规则已静音，则在阻止完成关键操作之前，您可能无法检测到潜在问题。

9. 要查看警报规则的当前条件，请执行以下操作：
   a. 从警报详细信息中选择*查看条件*。

      此时将显示一个弹出窗口，其中列出了每个已定义严重性的 Prometheus 表达式。

   b. 要关闭弹出窗口，请选择弹出窗口之外的任何位置。
10. (可选)选择*编辑规则*以编辑导致触发此警报的警报规则。

    您必须具有"管理警报或root访问权限"才能编辑警报规则。

    决定编辑警报规则时请务必小心。如果更改了触发值，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

11. 要关闭警报详细信息，请选择*关闭*。

监控 **StorageGRID** 中的存储容量

监控可用总空间，以确保 StorageGRID 系统不会用尽对象或对象元数据的存储空间。

StorageGRID 会分别存储对象数据和对象元数据，并为包含对象元数据的分布式 Cassandra 数据库预留特定空间量。监控对象和对象元数据的已用空间总量，以及每个对象的已用空间量趋势。这样，您可以提前计划添加节点，并避免任何服务中断。

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

监控网格的整体存储容量、以确保为对象数据和对象元数据保留足够的可用空间。了解存储容量如何随时间变化有助于您计划在占用网格的可用存储容量之前添加存储节点或存储卷。

通过Grid Manager信息板、您可以快速评估整个网格和每个数据中心的可用存储容量。节点页面提供了对象数据和对象元数据的更详细值。

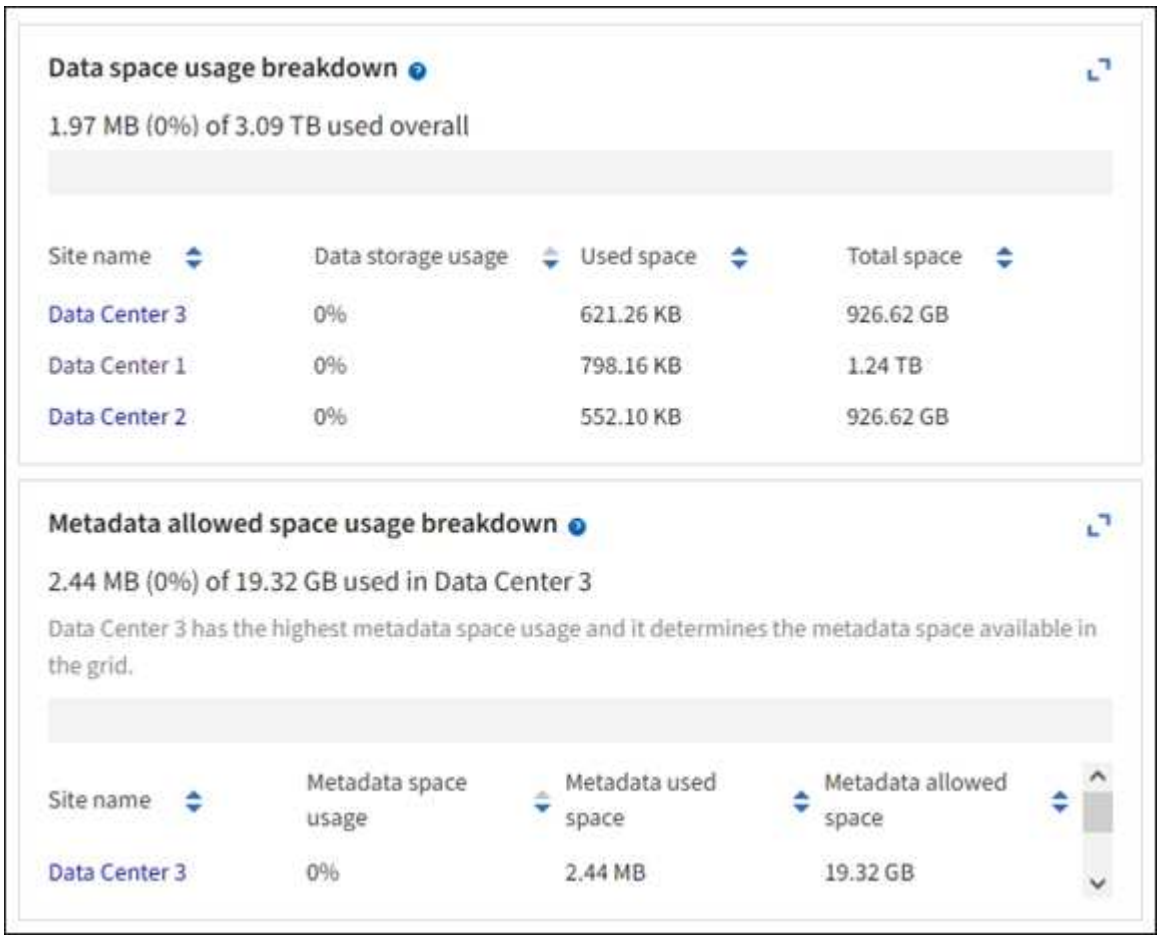
步骤

1. 评估可用于整个网格和每个数据中心的存储量。

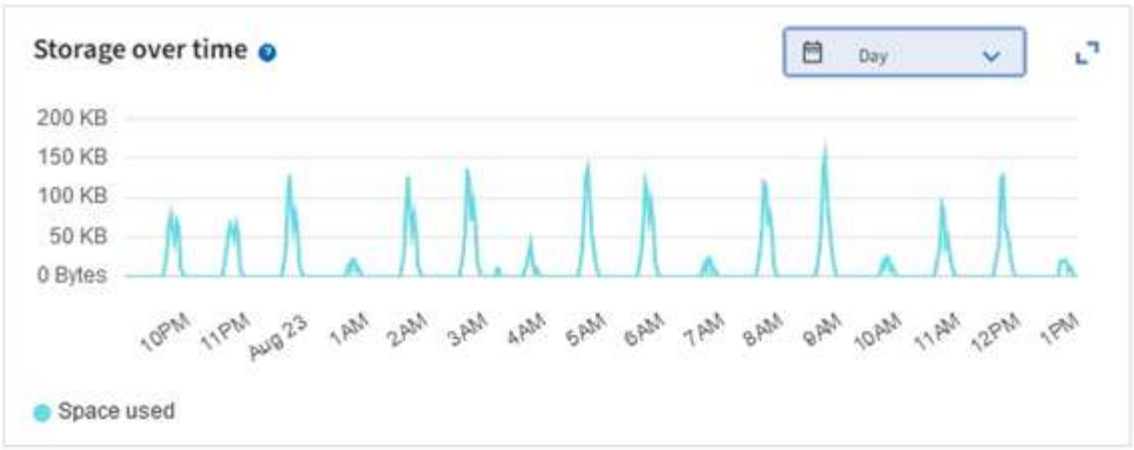
   a. 选择*信息板>概述*。

   b. 记下数据空间使用量细分卡和元数据允许的空间使用量细分卡上的值。每个卡都会列出存储使用量的百分比、已用空间容量以及站点可用或允许的总空间。

      此摘要不包括归档介质。



   a. 记下随时间变化的存储卡上的图表。使用时间段下拉列表帮助您确定存储的使用速度。



2. 有关已使用的存储容量以及网格中可用于存储对象数据和对象元数据的存储容量的其他详细信息、请使用节点页面。

   a. 选择*节点*。

   b. 选择 * ； grid_* > * 存储 * 。



   c. 将光标置于*已用存储-对象数据*和*已用存储-对象元数据*图表上方、可查看整个网格可用的对象存储和对象元数据存储量以及一段时间内已使用的容量。

   站点或网格的总值不包括至少五分钟未报告指标的节点、例如脱机节点。

3. 计划执行扩展，以便在占用网格的可用存储容量之前添加存储节点或存储卷。

   在规划扩展时间时，请考虑购买和安装额外存储需要多长时间。

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

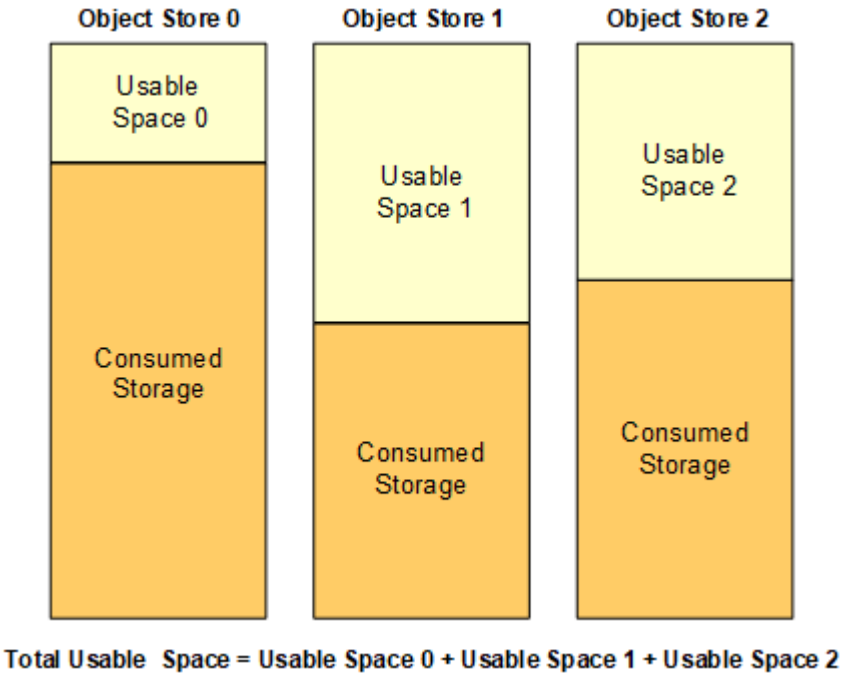
有关规划存储扩展的详细信息，请参见"扩展 StorageGRID 的说明"。

监控每个存储节点的存储容量

监控每个存储节点的总可用空间，以确保该节点具有足够的空间来容纳新对象数据。

关于此任务

可用空间是指可用于存储对象的存储空间量。存储节点的总可用空间是通过将节点中所有对象存储上的可用空间相加来计算得出的。



步骤

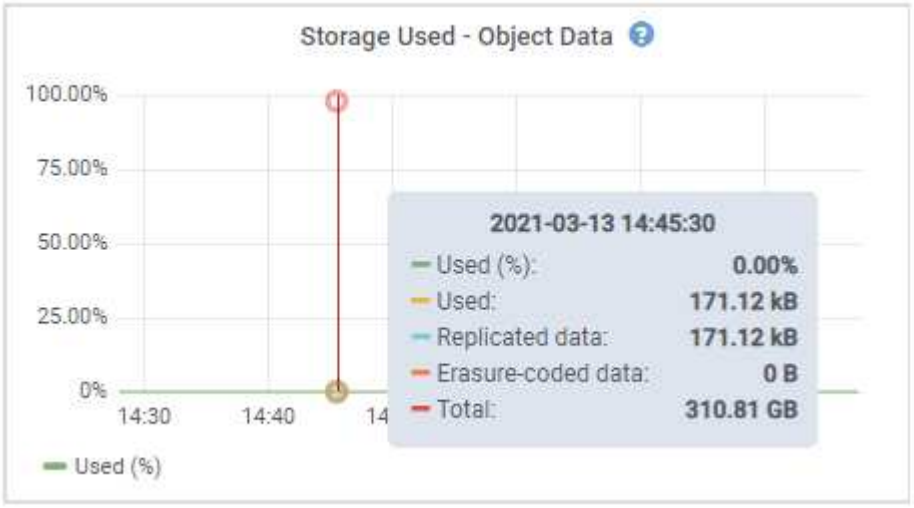
1. 选择*节点* > 存储节点 > 存储。

   此时将显示节点的图形和表。

2. 将光标置于已用存储-对象数据图上。

   此时将显示以下值：

   - * 已用（ % ） * ： 已用于对象数据的总可用空间的百分比。
   - * 已用 * ： 已用于对象数据的总可用空间量。
   - * 复制数据 * ： 此节点，站点或网格上复制的对象数据量的估计值。
   - * 擦除编码数据 * ： 此节点，站点或网格上经过擦除编码的对象数据量的估计值。
   - * 总计 * ： 此节点，站点或网格上的可用空间总量。已用值为 `storagegrid_storage_utilization_data_bytes`度量。



3. 查看图形下方的卷和对象存储表中的可用值。

   要查看这些值的图形，请在"可用"列中选择图表图标。

4. 监控值随时间变化，以估计可用存储空间的消耗速率。
5. 要保持系统正常运行，请在使用可用空间之前添加存储节点，添加存储卷或归档对象数据。

   在规划扩展时间时，请考虑购买和安装额外存储需要多长时间。

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

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

   "对象数据存储不足"如果存储节点上没有足够的空间来存储对象数据、则会触发警报。

监控每个存储节点的对象元数据容量

监控每个存储节点的元数据使用情况，以确保为基本数据库操作保留足够的可用空间。在对象元数据超过允许的元数据空间的 100% 之前，您必须在每个站点添加新的存储节点。

关于此任务

StorageGRID 在每个站点维护三个对象元数据副本，以提供冗余并防止对象元数据丢失。这三个副本会使用每个存储节点的存储卷 0 上为元数据预留的空间均匀分布在每个站点的所有存储节点上。

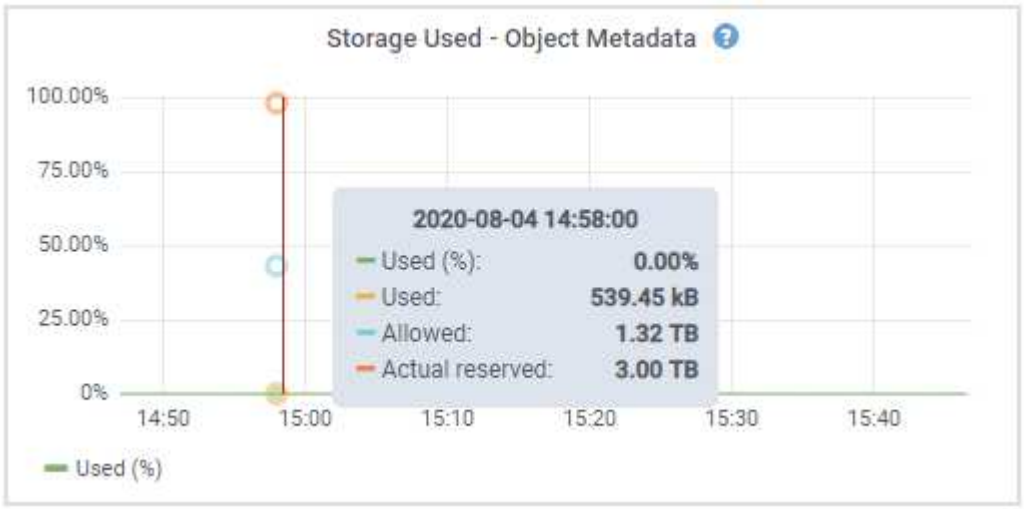
在某些情况下，网格的对象元数据容量消耗速度可能比其对象存储容量更快。例如，如果您通常要载入大量小对象，则可能需要添加存储节点以增加元数据容量，即使仍有足够的对象存储容量。

可能增加元数据使用量的一些因素包括用户元数据和标记的大小和数量，多部分上传中的部件总数以及 ILM 存储位置的更改频率。

步骤

1. 选择*节点* > 存储节点 > 存储。

2. 将光标置于已用存储-对象元数据图上方、可查看特定时间的值。



已用（ **%** ）

此存储节点上已使用的允许元数据空间的百分比。

Prometheus指标： `storagegrid_storage_utilization_metadata_bytes`和 `storagegrid_storage_utilization_metadata_allowed_bytes`

已用

此存储节点上已使用的允许元数据空间的字节数。

Prometheus指标： `storagegrid_storage_utilization_metadata_bytes`

允许

此存储节点上的对象元数据允许的空间。要了解如何确定每个存储节点的此值，请参见"允许的元数据空间的完整问题描述"。

Prometheus指标： `storagegrid_storage_utilization_metadata_allowed_bytes`

实际预留

为此存储节点上的元数据预留的实际空间。包括基本元数据操作所需的允许空间和空间。要了解如何为每个存储节点计算此值，请参见"元数据的实际预留空间的完整问题描述"。

*Prometheus*指标将在未来版本中添加。

站点或网格的总值不包括至少五分钟未报告指标的节点、例如脱机节点。

3. 如果 * 已用（ % ） * 值为 70% 或更高，请通过向每个站点添加存储节点来扩展 StorageGRID 系统。

当 * 已用（ % ） * 值达到特定阈值时，将触发 * 元数据存储不足 * 警报。如果对象元数据使用的空间超过允许的 100% ，则可能会出现不希望出现的结果。

添加新节点时，系统会自动在站点内的所有存储节点之间重新平衡对象元数据。请参见"有关扩展 StorageGRID 系统的说明"。

监控空间使用量预测

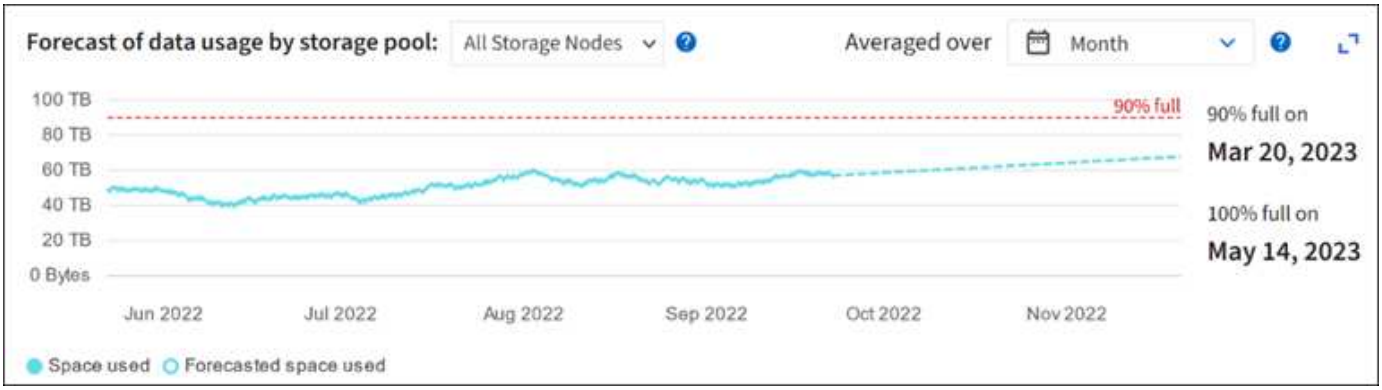
监控用户数据和元数据的空间使用情况预测，以估算何时需要"扩展网格"。

如果您注意到消耗率随时间的变化、请从*平均值超过*下拉列表中选择一个较短的范围、以仅反映最新的接收模式。如果您注意到季节性模式、请选择更长的范围。

如果您安装了新的StorageGRID 、请在评估空间使用量预测之前、先累积数据和元数据。

步骤

1. 在信息板上，选择*Storage*。
2. 查看信息板卡、按存储池显示的数据使用情况预测以及按站点显示的元数据使用情况预测。
3. 使用这些值可估算何时需要为数据和元数据存储添加新存储节点。



监控 **StorageGRID** 中的信息生命周期管理

信息生命周期管理（ ILM ）系统可为网格中存储的所有对象提供数据管理。您必须监控ILM操作、以了解网格是否可以处理当前负载、或者是否需要更多资源。

关于此任务

StorageGRID系统通过应用活动ILM策略来管理对象。ILM策略和关联的ILM规则可确定创建的副本数、创建的副本类型、副本放置位置以及每个副本的保留时间长度。

对象加载和其他与对象相关的活动可能会超过StorageGRID 评估ILM的速率、从而导致系统对无法近乎实时地执行ILM放置指令的对象进行排队。您应监控StorageGRID是否与客户端操作保持一致。

使用**Grid Manager**信息板选项卡

步骤

使用网格管理器信息板上的ILM选项卡监控ILM操作：

1. 登录到网格管理器。
2. 从信息板中、选择ILM选项卡、并记下ILM队列(对象)卡和ILM评估速率卡上的值。

   信息板上的ILM队列(对象)卡可能会出现临时峰值。但是、如果队列持续增加而从未减少、网格需要更多资源才能高效运行：要么增加存储节点、要么增加ILM策略将对象放置在远程位置的网络带宽。

步骤

此外，使用“节点”页面调查 ILM 队列：

> 在未来的StorageGRID版本中，*节点*页面上的图表将被相应的仪表板卡取代。

1. 选择*节点*。
2. 选择 * 网格名称 _* > * ILM * 。
3. 将光标置于ILM队列图上方、可查看在给定时间点的以下属性值：
   - * 已排队的对象（来自客户端操作） *： 由于客户端操作（例如载入）而等待 ILM 评估的对象总数。
   - * 已排队的对象（从所有操作） *： 等待 ILM 评估的对象总数。
   - * 扫描速率（对象 / 秒） *： 为 ILM 扫描网格中的对象并使其排队的速率。
   - * 评估速率（对象 / 秒） *： 根据网格中的 ILM 策略评估对象的当前速率。

   > ILM队列部分仅适用于网格。此信息不会显示在站点或存储节点的 "ILM " 选项卡上。
4. 在 "ILM Queue" 部分中，查看以下属性。
   - 扫描期限-估计：完成对所有对象的完整ILM扫描的估计时间。

     > 完全扫描并不能保证 ILM 已应用于所有对象。
   - 已尝试修复：已尝试对复制数据执行的对象修复操作的总数。每当存储节点尝试修复高风险对象时，此计数都会递增。如果网格繁忙，高风险 ILM 修复会优先处理。

     如果修复后复制失败，则同一对象修复可能会再次增加。 + 当您监控存储节点卷恢复的进度时，这些属性非常有用。如果尝试修复的次数停止增加并且完整扫描已完成，则修复可能已完成。
5. 或者，提交 Prometheus 查询 `storagegrid_ilm_scan_period_estimated_minutes`和 `storagegrid_ilm_repairs_attempted`。

监控 **StorageGRID** 中的网络和系统资源

节点和站点之间网络的完整性和带宽以及各个网格节点的资源使用情况对于高效运营至关重要。

监控网络连接和性能

如果您的信息生命周期管理（ ILM ）策略使用提供站点丢失保护的方案在站点之间复制复制复制的对象或存储经过纠删编码的对象，则网络连接和带宽尤其重要。如果站点之间的网络不可用，网络延迟过高或网络带宽不足，则某些 ILM 规则可能无法将对象放置在预期位置。如果为ILM规则选择了严格的写入选项、则可能会导致写入失败、或者导致写入性能不佳和ILM积压。

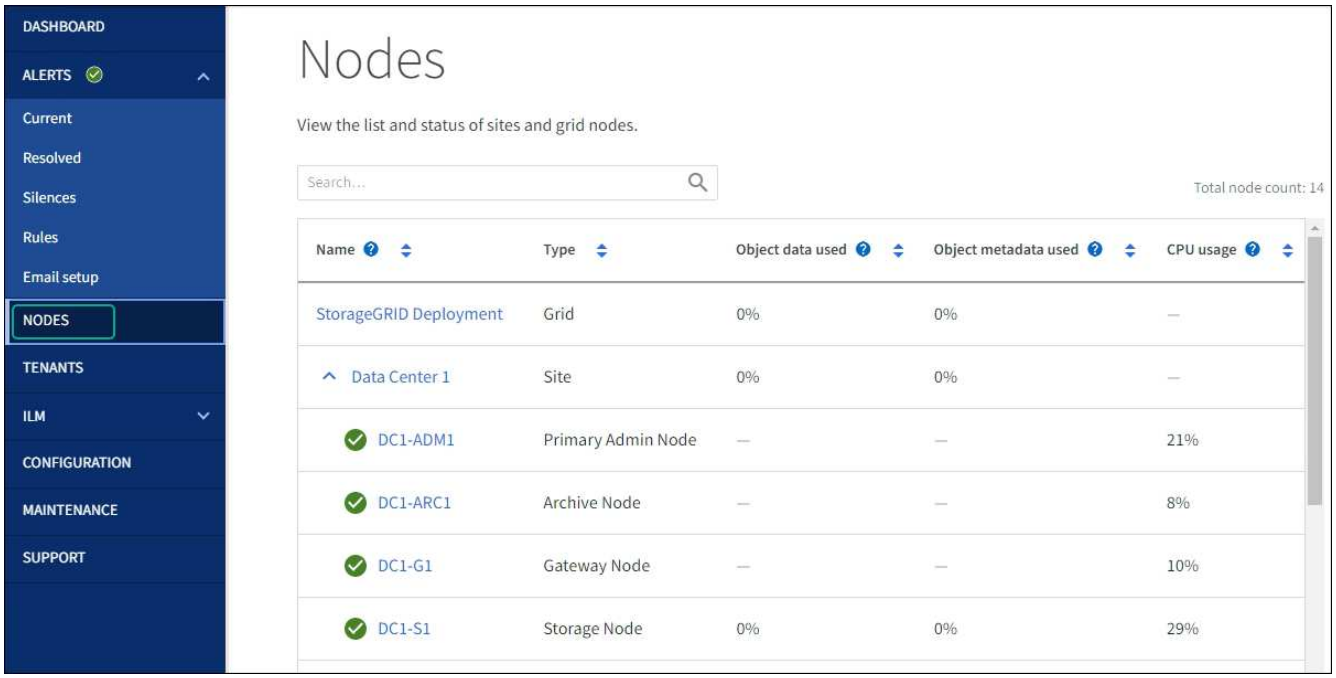
使用网格管理器监控连接和网络性能、以便及时解决任何问题。

此外、请考虑"创建网络流量分类策略"监控与特定租户、分段、子网或负载平衡器端点相关的流量。您可以根据需要设置流量限制策略。

步骤

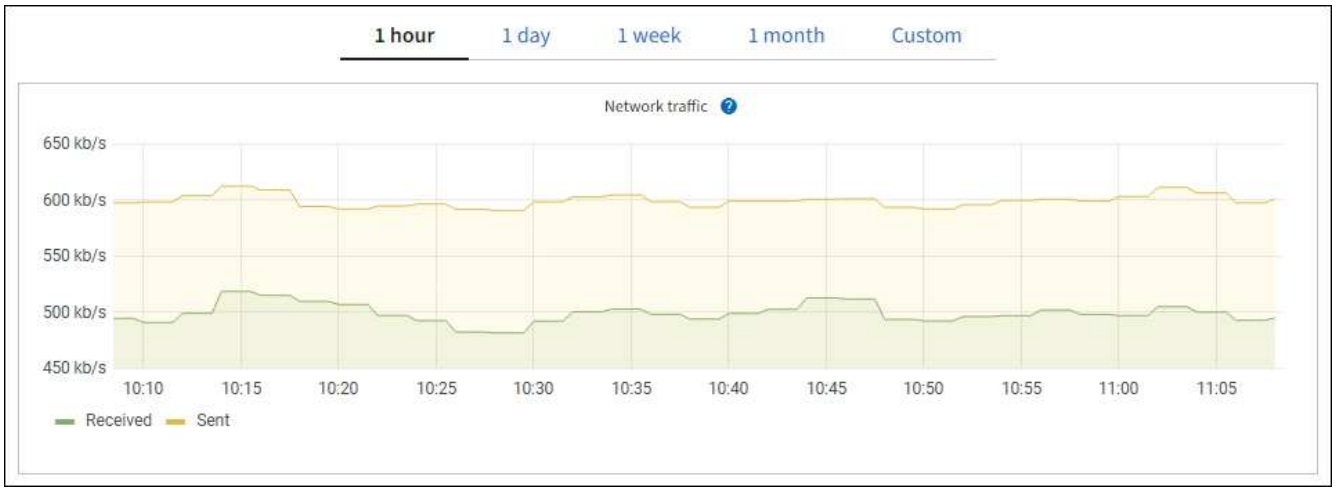
1. 选择*节点*。

   此时将显示节点页面。网格中的每个节点均以表格式列出。

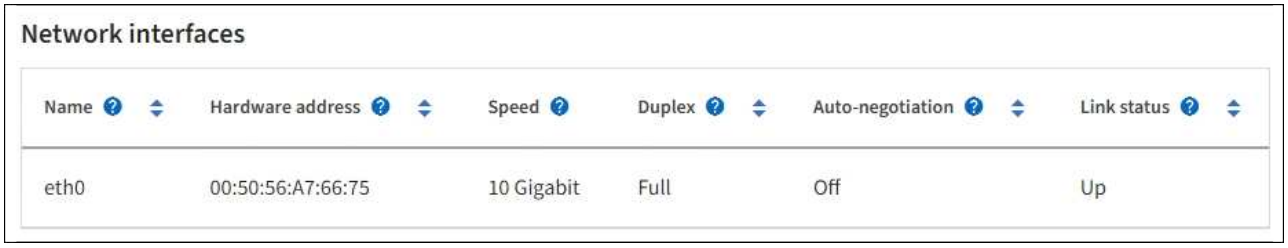


2. 选择网格名称，特定数据中心站点或网格节点，然后选择 * 网络 * 选项卡。

   网络流量图提供了整个网格，数据中心站点或节点的整体网络流量摘要。



   a. 如果选择了网格节点，请向下滚动以查看页面的 * 网络接口 * 部分。



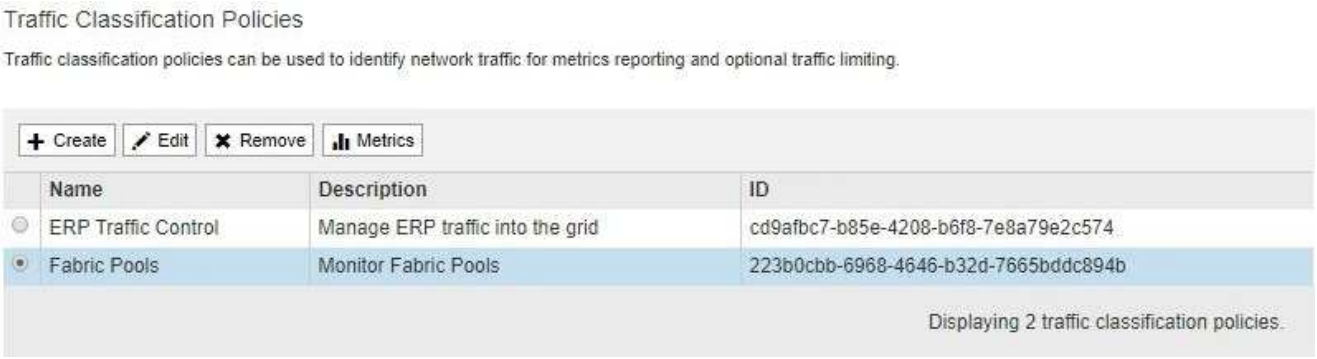
b. 对于网格节点，向下滚动以查看页面的 * 网络通信 * 部分。

接收和传输表显示了通过每个网络接收和发送的字节数和数据包数，以及其他接收和传输指标。

3. 使用与流量分类策略关联的指标监控网络流量。

a. 选择*配置* > 网络 > 流量分类。

此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



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

b. 查看图形以了解与策略关联的网络流量。

如果流量分类策略旨在限制网络流量，请分析流量限制的频率，并确定该策略是否仍能满足您的需求。不时地，"根据需要调整每个流量分类策略".

相关信息

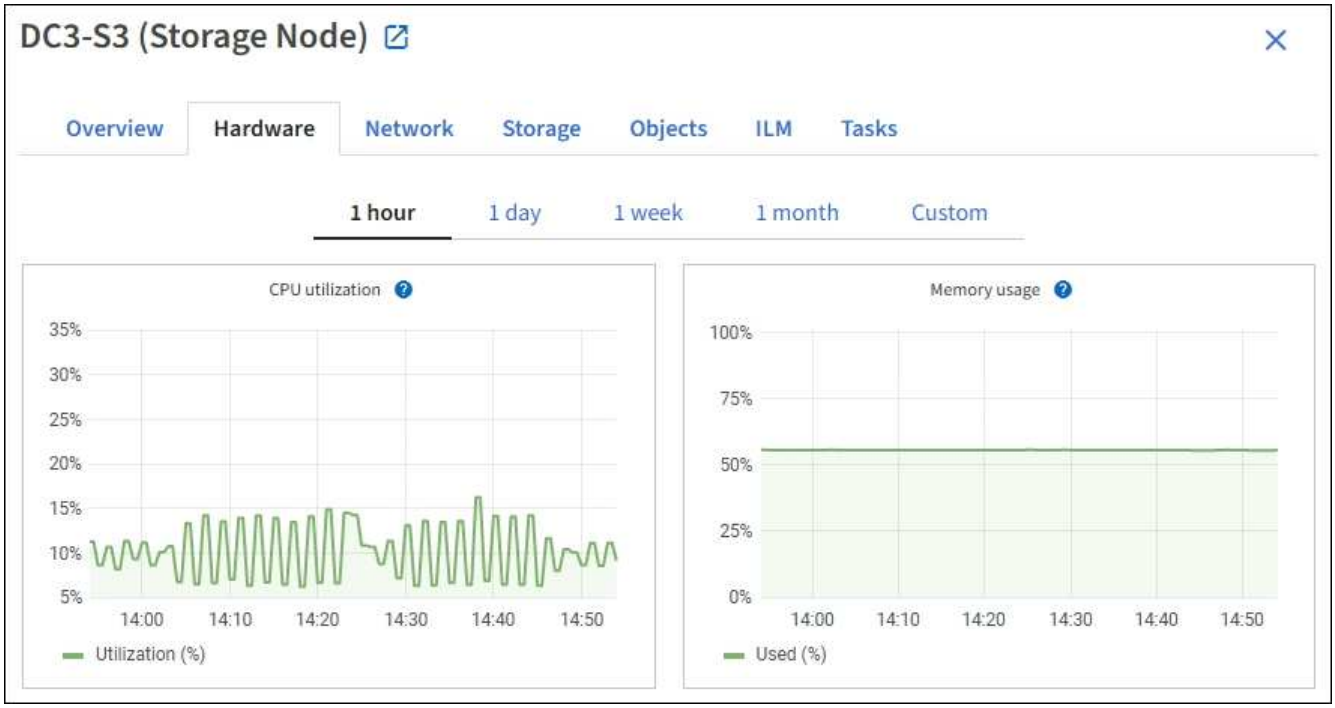
- "查看网络选项卡"
- "监控节点连接状态"

监控节点级资源

监控各个网格节点以检查其资源使用情况。如果节点始终过载，则可能需要更多节点才能高效运行。

步骤

1. 从*节点*页面中选择节点。
2. 选择 * 硬件 * 选项卡以显示 CPU 利用率和内存使用情况的图形。



3. 要显示不同的时间间隔，请选择图表或图形上方的控件之一。您可以显示间隔为 1 小时， 1 天， 1 周或 1 个月的可用信息。您还可以设置自定义间隔，以便指定日期和时间范围。
4. 如果节点托管在存储设备或服务设备上，请向下滚动以查看组件表。所有组件的状态均应为"标称"。调查具有任何其他状态的组件。

相关信息

- "查看有关设备存储节点的信息"
- "查看有关设备管理节点和网关节点的信息"

监控 **StorageGRID** 中的租户活动

所有S3客户端活动都与StorageGRID租户帐户相关联。您可以使用网格管理器监控所有租户或特定租户的存储使用情况或网络流量。您可以使用审核日志或Grafana信息板收集有关租户如何使用StorageGRID 的更多详细信息。

开始之前

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

查看所有租户

租户页面显示所有当前租户帐户的基本信息。

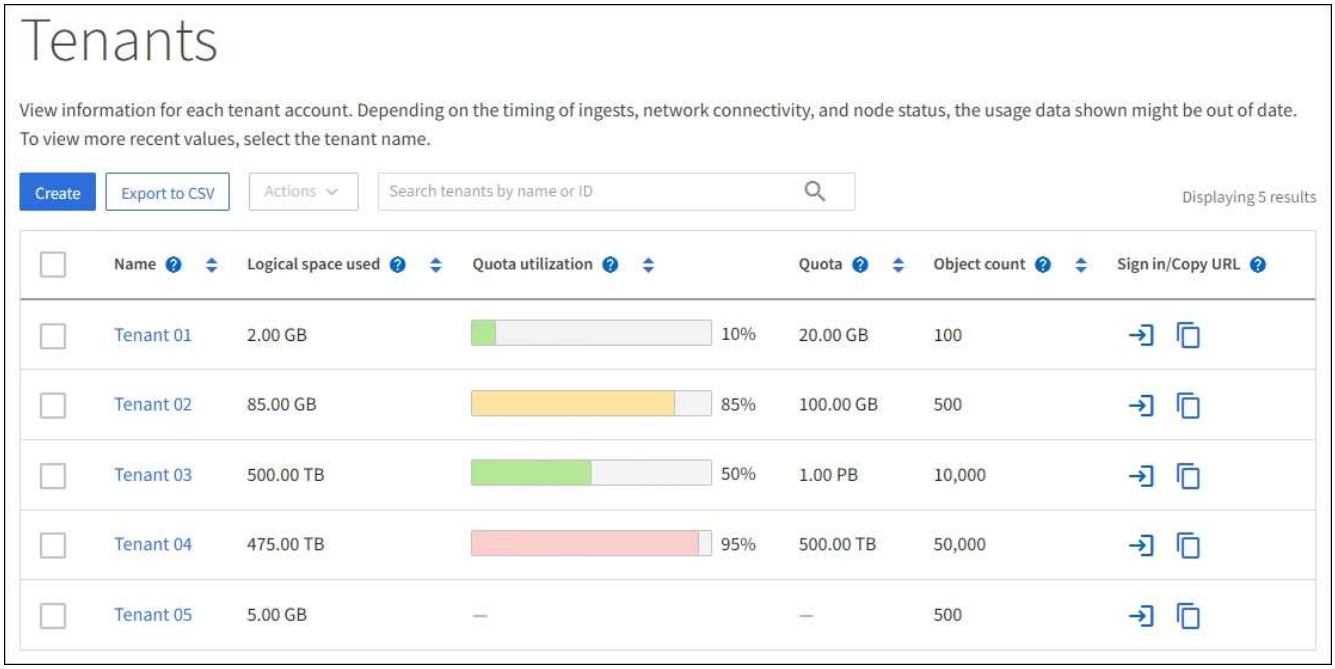
步骤

1. 选择*租户*。
2. 查看租户页面上显示的信息。

   此时将列出每个租户的已用逻辑空间、配额使用量、配额和对象计数。如果未为租户设置配额、则配额使用

量和配额字段包含短划线(&&#8212；)。

> 属于该租户的所有对象的逻辑大小包括未完成和正在进行的分段上传。该大小不包括用于 ILM 策略的额外物理空间。已用空间值是估计值。这些估计受到摄取时间、网络连接和节点状态的影响。



3. （可选）通过选择 **Sign in/Copy URL** 列中的 Sign in 链接 登录租户帐户。
4. 或者，通过选择 **Sign in/Copy URL** 列中的复制 URL 链接，复制租户的登录页面 URL。
5. (可选)选择*导出至CSV-*以查看和导出 `.csv`包含所有租户的使用量值的文件。

   系统将提示您打开或保存 `.csv`文件。

   此文件的内容 `.csv`类似于以下示例：

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

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

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

   如果租户帐户包含任何分段或容器、则不能删除该帐户。

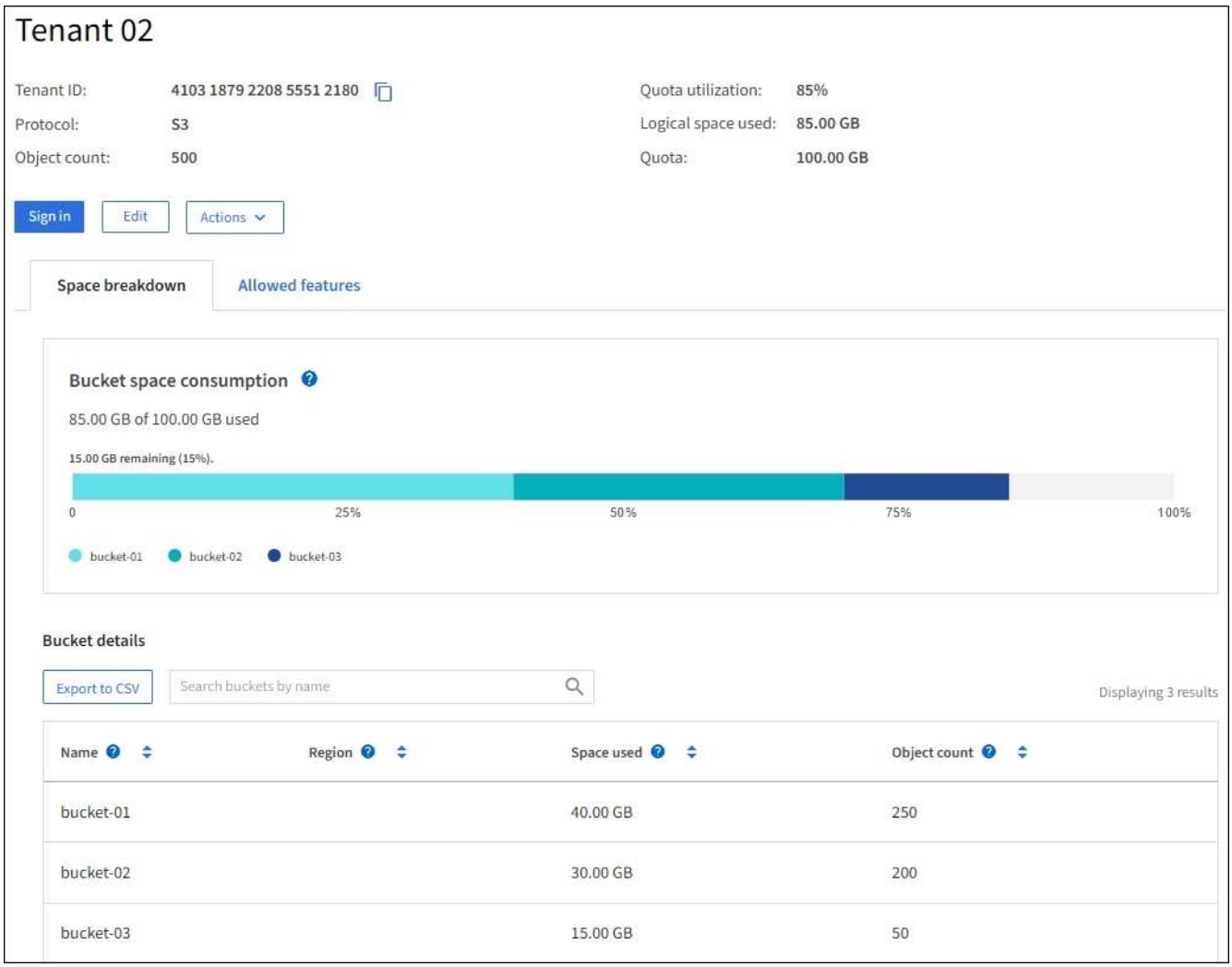
查看特定租户

您可以查看特定租户的详细信息。

步骤

1. 从租户页面中选择租户名称。

   此时将显示租户详细信息页面。



2. 查看页面顶部的租户概述。

   此部分详细信息页面提供了租户的摘要信息、包括租户的对象计数、配额使用量、已用逻辑空间和配额设置。

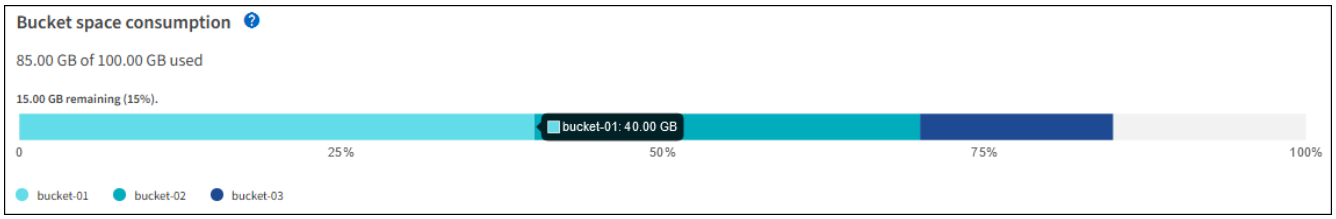
   > 属于该租户的所有对象的逻辑大小包括未完成和正在进行的分段上传。该大小不包括用于 ILM 策略的额外物理空间。已用空间值是估计值。这些估计受到摄取时间、网络连接和节点状态的影响。

3. 在*空间细分*选项卡中，查看*空间消耗*图表。

   此图表显示租户的所有S3存储分段的总空间消耗。

   如果为此租户设置了配额，则已用配额量和剩余配额量将以文本形式显示(例如 `85.00 GB of 100 GB used`)。如果未设置任何配额，则租户具有无限配额，并且文本仅包含已用空间量(例如 `85.00 GB used`)。条形图显示每个分段或容器中的配额百分比。如果租户超过存储配额 1% 以上且至少超过 1 GB ，则此图表将显示总配额和超额量。

您可以将光标置于条形图上方，以查看每个分段或容器使用的存储。您可以将光标置于可用空间段上方以查看剩余存储配额量。



配额使用量基于内部估计值、在某些情况下可能会超过此值。例如，当租户开始上传对象时， StorageGRID 会检查配额，如果租户超过配额，则会拒绝新的载入。但是，在确定是否超过配额时， StorageGRID 不会考虑当前上传的大小。如果删除了对象、则可能会暂时阻止租户上传新对象、直到重新计算配额使用量为止。计算配额使用量可能需要10分钟或更长时间。

租户的配额使用量指示租户上传到StorageGRID的对象数据量(逻辑大小)。配额使用量并不表示用于存储这些对象及其元数据副本的空间(物理大小)。

您可以启用*租户配额使用量高*警报规则来确定租户是否正在使用其配额。如果启用，则在租户已使用其配额的 90% 时触发此警报。有关说明，请参阅"编辑警报规则"。

4. 在*空间细分*选项卡中、查看*存储分段详细信息*。

   此表列出了租户的S3存储分段。已用空间是指存储分段或容器中的对象数据总量。此值不表示 ILM 副本和对象元数据所需的存储空间。

5. 或者，也可以选择 * 导出到 CSV* 以查看和导出包含每个分段或容器的使用量值的 .csv 文件。

   单个S3租户文件的内容 `.csv`类似于以下示例：

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

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

6. (可选)选择*允许的功能*选项卡以查看为租户启用的权限和功能列表。如果需要更改其中任何设置、请参见"编辑租户帐户"。
7. 如果租户具有*使用网格联合连接*权限，则可以选择*网格联合*选项卡以了解有关连接的更多信息。

   请参阅"什么是网格联合？"和"管理网格联盟允许的租户"。

查看网络流量

如果某个租户已设置流量分类策略，请查看该租户的网络流量。

步骤

1. 选择*配置* > 网络 > 流量分类。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。

2. 查看策略列表以确定适用于特定租户的策略。
3. 要查看与策略关联的指标，请选择策略左侧的单选按钮，然后选择*Metrics*。
4. 分析图形以确定策略限制流量的频率以及是否需要调整策略。

有关详细信息、请参见 "管理流量分类策略" 。

使用审核日志

您也可以使用审核日志更精细地监控租户的活动。

例如，您可以监控以下类型的信息：

- 特定客户端操作，例如 PUT ， GET 或 DELETE
- 对象大小
- 应用于对象的 ILM 规则
- 客户端请求的源 IP

审核日志会写入文本文件，您可以使用所选的日志分析工具进行分析。这样，您可以更好地了解客户活动，或者实施复杂的成本分摊和计费模式。

有关详细信息、请参见 "查看审核日志" 。

使用**Prometheus**指标

(可选)使用Prometheus指标报告租户活动。

- 在网格管理器中，选择*支持* > 工具 > 指标。您可以使用现有的仪表板（例如 S3 概览）来查看客户活动。

  > 指标页面上提供的工具主要供技术支持使用。这些工具中的某些功能和菜单项会有意失效。

- 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。您可以使用网格管理 API 的 " 指标 " 部分中的指标为租户活动创建自定义警报规则和信息板。

有关详细信息、请参见 "查看支持指标" 。

监控 **StorageGRID** 中的 **S3** 客户端操作

您可以监控对象载入和检索速率，以及对象计数，查询和验证的指标。您可以查看客户端应用程序在 StorageGRID 系统中成功尝试读取，写入和修改对象的次数和失败的尝试次数。

开始之前

您已使用登录到网格管理器"支持的 Web 浏览器"。

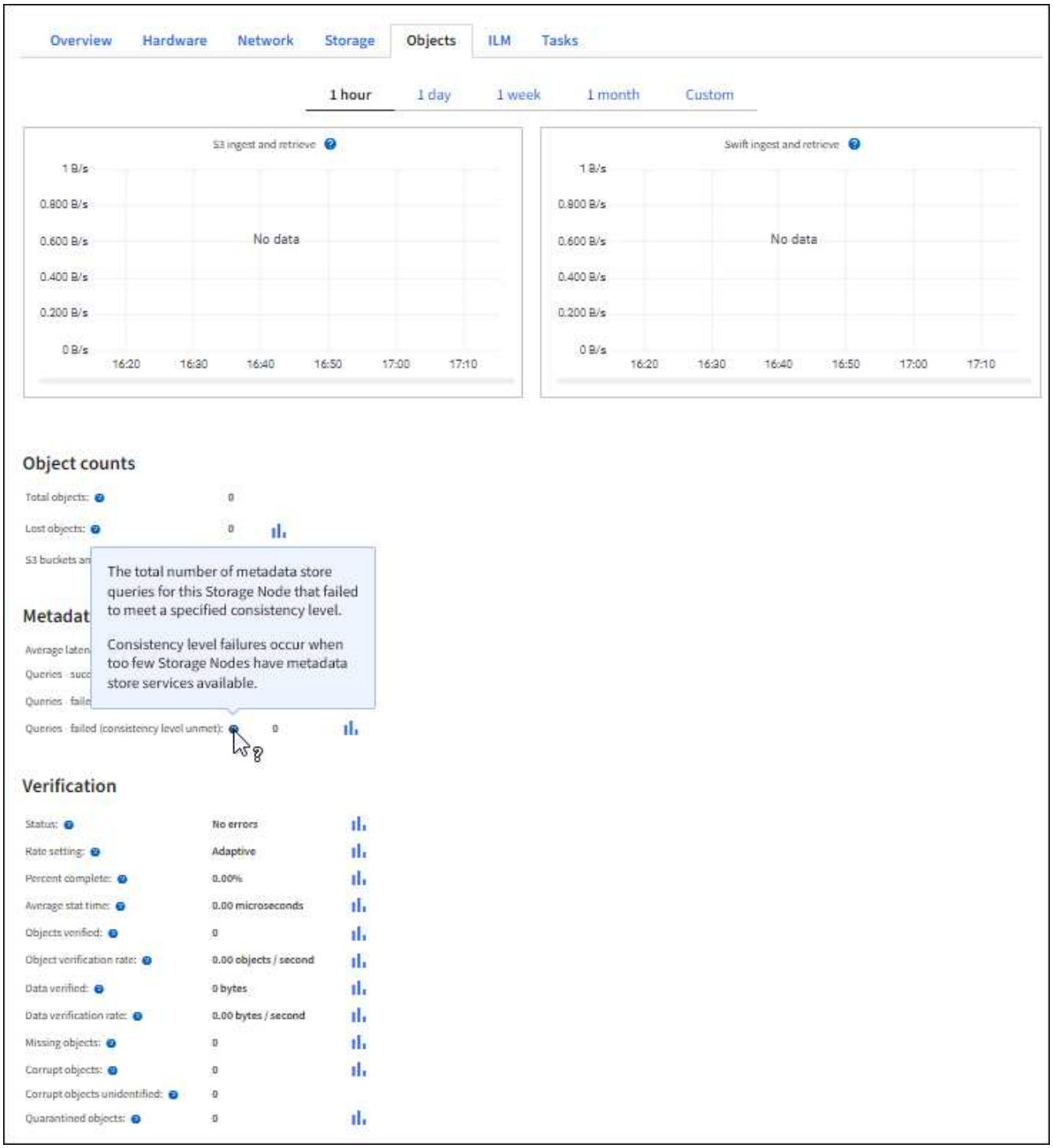
步骤

1. 从信息板中，选择*Performance*选项卡。
2. 请参见S3图表、其中汇总了存储节点在选定时间范围内执行的客户端操作数以及存储节点收到的API请求数。
3. 选择“节点”以访问“节点”页面。
4. 从节点主页(网格级)中，选择*Objects*选项卡。

   此图表显示整个StorageGRID系统的S3加载和检索速率(以字节/秒为单位)以及所加载或检索的数据量。您可以选择时间间隔或应用自定义间隔。

5. 要查看特定存储节点的信息，请从左侧列表中选择节点，然后选择*Objects*选项卡。

   此图表将显示节点的加热和检索速率。该选项卡还包括对象计数、元数据查询和验证操作的指标。



监控 **StorageGRID** 中的负载平衡操作

如果您使用负载平衡器管理客户端与 StorageGRID 的连接，则应在最初配置系统之后以及在进行任何配置更改或执行扩展之后监控负载平衡操作。

关于此任务

您可以在管理节点、网关节点或外部第三方负载平衡器上使用负载平衡器服务在多个存储节点之间分布客户端请求。

配置负载平衡后，您应确认对象载入和检索操作在存储节点之间均匀分布。均匀分布的请求可确保

StorageGRID 始终响应负载下的客户端请求，并有助于保持客户端性能。

如果您在主动备份模式下为网关节点或管理节点配置了一个高可用性（ HA ）组，则该组中只有一个节点会主动分发客户端请求。

有关详细信息，请参见 "配置S3客户端连接"。

步骤

1. 如果S3客户端使用负载平衡器服务进行连接、请检查管理节点或网关节点是否按预期主动分布流量：
   a. 选择*节点*。
   b. 选择网关节点或管理节点。
   c. 在*Overview*选项卡上，检查节点接口是否位于HA组中，以及节点接口是否具有Primary角色。

      角色为Primary的节点以及不属于HA组的节点应主动向客户端分发请求。

   d. 对于应主动分发客户端请求的每个节点，请选择"负载平衡器选项卡"。
   e. 查看上一周的负载平衡器请求流量图表，以确保节点一直在主动分发请求。

      主动备份 HA 组中的节点可能会不时承担备份角色。在此期间、节点不会分发客户端请求。

   f. 查看上周的负载平衡器传入请求速率图表，查看节点的对象吞吐量。
   g. 对 StorageGRID 系统中的每个管理节点或网关节点重复上述步骤。
   h. (可选)使用流量分类策略查看负载平衡器服务提供的流量的更详细分析。
2. 验证这些请求是否均匀分布到存储节点。
   a. 选择 * 存储节点 _* > * LDR* > * HTTP * 。
   b. 查看 * 当前已建立的传入会话 * 的数量。
   c. 对网格中的每个存储节点重复上述步骤。

      所有存储节点的会话数应大致相等。

监控 **StorageGRID** 网格联合连接

您可以监控有关所有的基本信息"网格联合连接"、有关特定连接的详细信息或有关跨网格复制操作的Prometheus指标。您可以从任一网格监控连接。

开始之前

- 您已使用登录到任一网格上的网格管理器"支持的 Web 浏览器"。
- 您拥有已登录到的网格的"root访问权限"。

查看所有连接

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

步骤

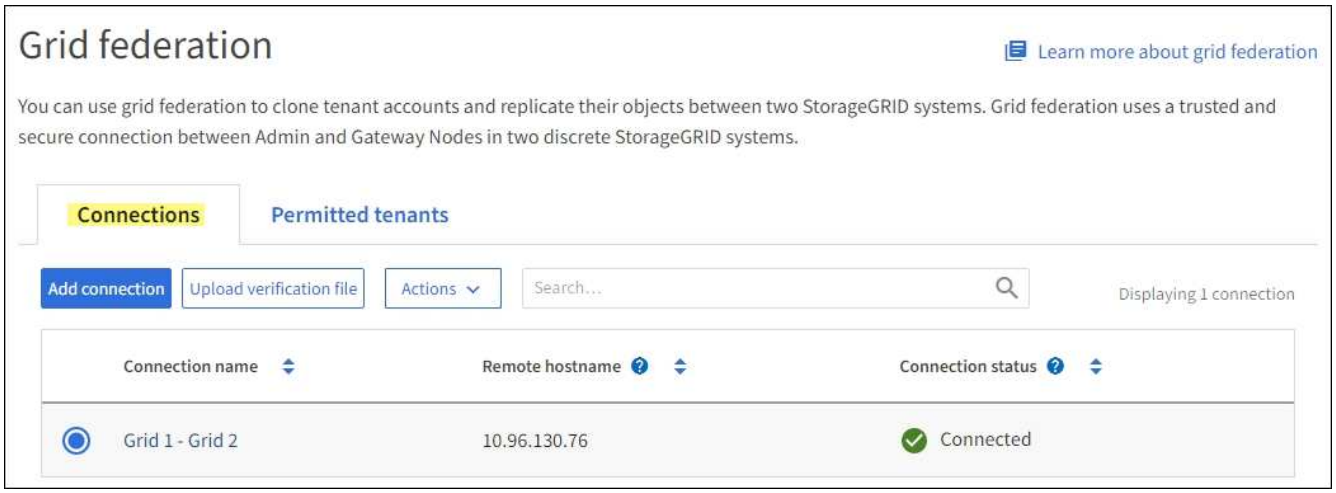
1. 选择*配置* > 系统 > 网格联合。

此时将显示Grid Federation页面。

2. 要查看此网格上所有连接的基本信息，请选择*Connections*选项卡。

   在此选项卡中、您可以：

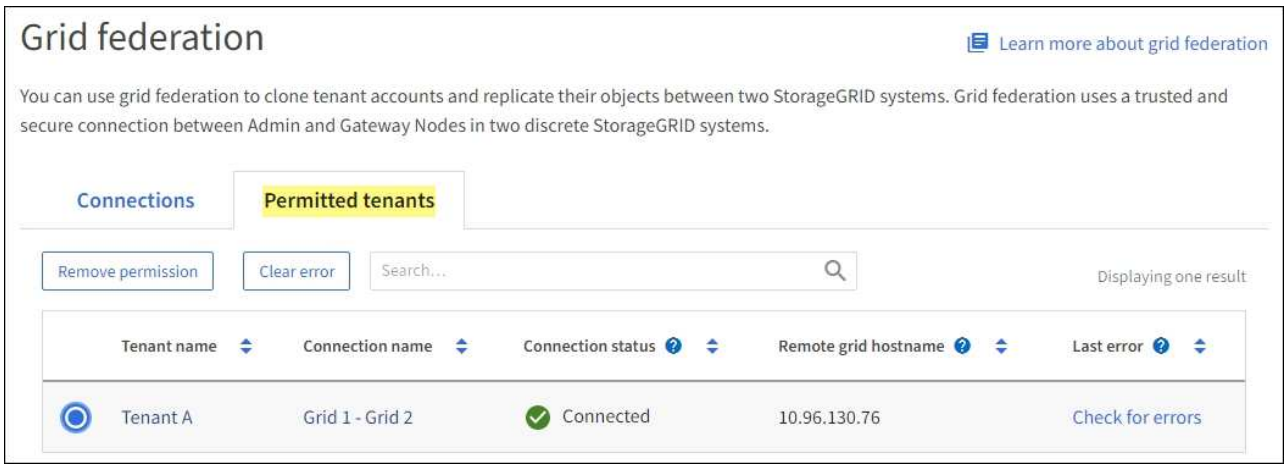
   - "创建新连接"(英文)
   - 选择与的现有连接"编辑或测试"。



3. 要查看此网格上具有*使用网格联合连接*权限的所有租户帐户的基本信息、请选择*允许的租户*选项卡。

   在此选项卡中、您可以：

   - "查看每个允许租户的详细信息页面"(英文)
   - 查看每个连接的详细信息页面。请参阅。 查看特定连接
   - 选择允许的租户，然后选择"删除权限"。
   - 检查是否存在跨网格复制错误、如果有、请清除最后一个错误。请参阅。 "对网格联合错误进行故障排除"



查看特定连接

您可以查看特定网格联合连接的详细信息。

步骤

1. 从"网格联合"页面中选择任一选项卡、然后从表中选择连接名称。

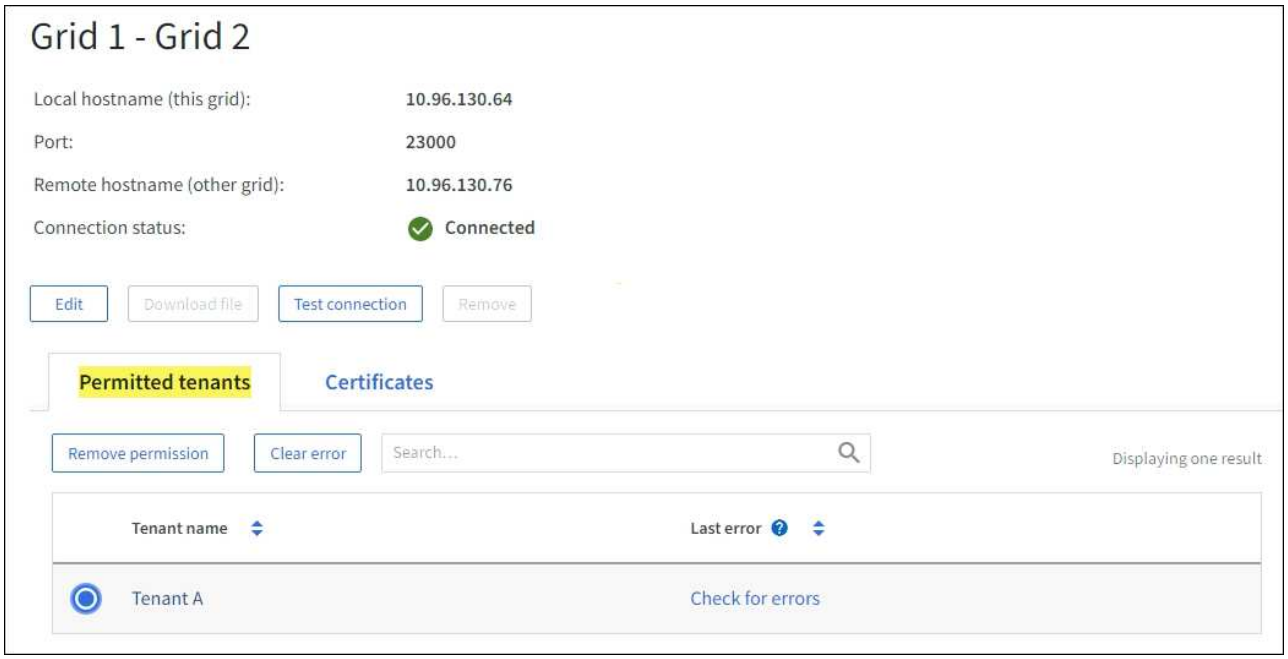
   在连接的详细信息页面中、您可以：

   - 查看有关连接的基本状态信息、包括本地和远程主机名、端口和连接状态。
   - 选择与的连接"编辑、测试或删除"。

2. 查看特定连接时，请选择*允许的租户*选项卡以查看有关该连接允许的租户的详细信息。

   在此选项卡中、您可以：

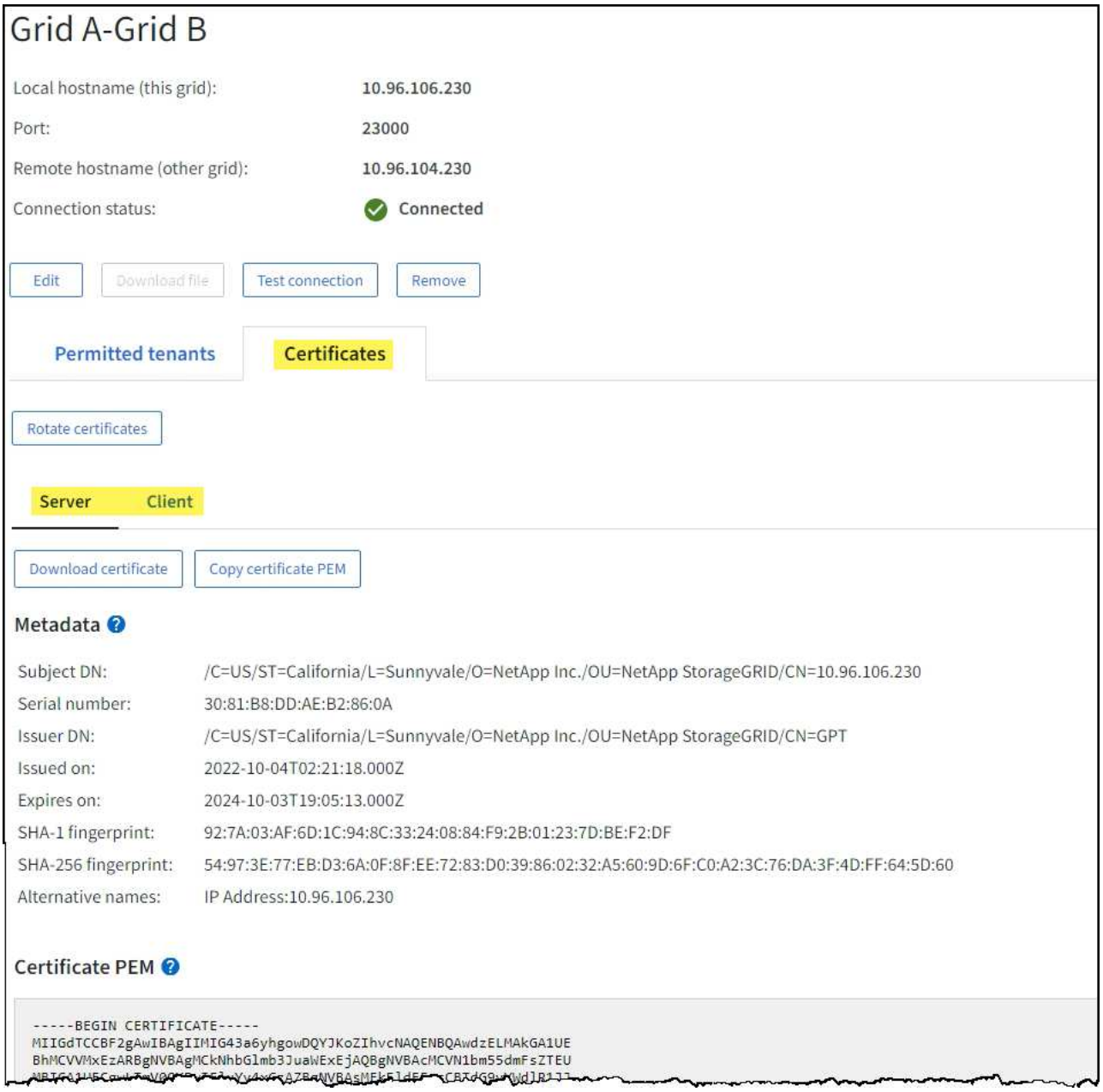
   - "查看每个允许租户的详细信息页面"(英文)
   - "删除租户的权限"可使用连接。
   - 检查是否存在跨网格复制错误、并清除最后一个错误。请参阅。 "对网格联合错误进行故障排除"



3. 查看特定连接时，选择*Certificates*选项卡以查看系统为此连接生成的服务器和客户机证书。

   在此选项卡中、您可以：

   - "轮换连接证书"(英文)
   - 选择*服务器*或*客户端*以查看或下载关联的证书或复制证书PEM。



查看跨网格复制指标

您可以使用Grafana中的跨网格复制信息板查看有关网格上跨网格复制操作的Prometheus指标。

步骤

1. 从网格管理器中，选择*支持* > 工具 > 指标。

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

2. 在页面的Grafana部分中，选择*跨网格复制*。

   有关详细说明，请参见"查看支持指标"。

3. 要重试复制失败的对象，请参见"确定并重试失败的复制操作"。

管理警报

在 StorageGRID 中管理警报

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

当警报规则条件评估为 true 时，系统将在特定严重性级别触发警报。触发警报后，将执行以下操作：

- 在网格管理器的信息板上会显示警报严重性图标、当前警报的计数将递增。
- 警报显示在 **Nodes** 摘要页面和 **Nodes** > ***node*** > **Overview** 选项卡上。
- 假定您已配置 SMTP 服务器并为收件人提供了电子邮件地址，则会发送电子邮件通知。
- 假定您已配置 StorageGRID SNMP 代理，则会发送简单网络管理协议（ SNMP ）通知。

您可以创建自定义警报、编辑或禁用警报以及管理警报通知。

了解更多信息：

- 回顾视频：

  警报概述

  自定义警报

- 请参阅"警报参考"。

查看 StorageGRID 警报规则

警报规则定义触发条件"特定警报"。StorageGRID 包含一组默认警报规则，您可以按原定义使用或修改这些规则，也可以创建自定义警报规则。

您可以查看所有默认和自定义警报规则的列表，以了解将触发每个警报的条件以及是否已禁用任何警报。

开始之前

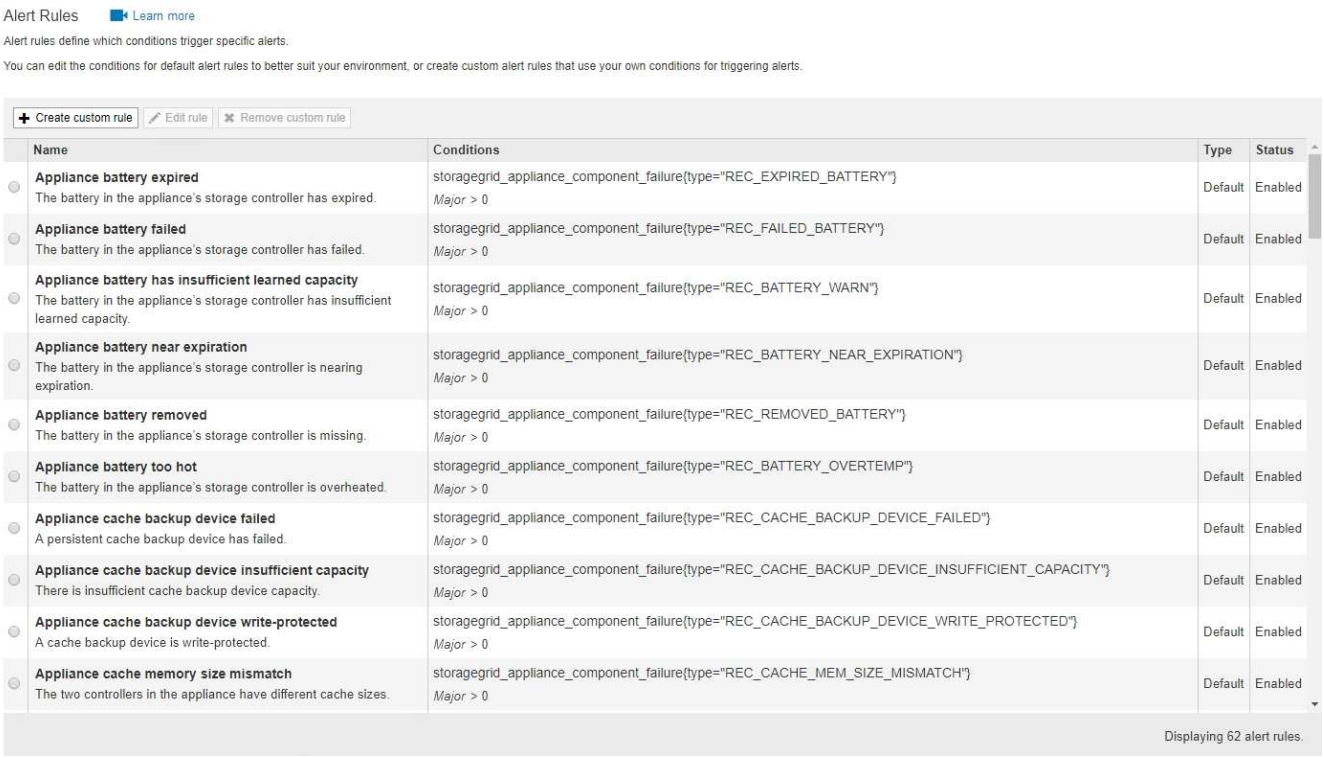
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"管理警报或root访问权限"。
- 或者，您已经观看了视频：

  警报概述

步骤

1. 选择*警报* > 规则。

   此时将显示 "Alert Rules" 页面。



2. 查看警报规则表中的信息：

列标题	说明
名称	警报规则的唯一名称和问题描述 。首先列出自定义警报规则，然后列出默认警报规则。警报规则名称是电子邮件通知的主题。
条件	用于确定何时触发此警报的 Prometheus 表达式。可以在以下一个或多个严重性级别触发警报，但不需要为每个严重性设置一个条件。 • 严重 ：存在已停止 StorageGRID 节点或服务正常操作的异常情况。您必须立即解决根本问题。如果问题未得到解决，可能会导致服务中断和数据丢失。 • 重大 ：存在影响当前操作或接近严重警报阈值的异常情况。您应该调查重大警报并解决任何潜在问题，以确保异常情况不会阻止 StorageGRID 节点或服务的正常运行。 • 轻微 ：系统正常运行，但存在异常情况，如果继续运行，可能会影响系统的运行能力。您应该监控并解决未自行清除的轻微警报，以确保它们不会导致更严重的问题。

列标题	说明
键入	警报规则的类型： • * 默认 * ：随系统提供的警报规则。您可以禁用默认警报规则或编辑默认警报规则的条件和持续时间。您无法删除默认警报规则。 • * 默认值 * ：包含已编辑条件或持续时间的默认警报规则。根据需要，您可以轻松地将修改后的条件还原回原始默认值。 • * 自定义 * ：创建的警报规则。您可以禁用，编辑和删除自定义警报规则。
状态	当前是否已启用此警报规则。系统不会评估已禁用警报规则的条件、因此不会触发警报。

在 **StorageGRID** 中创建自定义警报规则

您可以创建自定义警报规则来定义自己触发警报的条件。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"管理警报或root访问权限"。
- 您熟悉"常用的 Prometheus 指标"。
- 您已了解 "Prometheus 查询的语法"。
- 或者，您已经观看了视频：

  自定义警报

关于此任务

StorageGRID 不会验证自定义警报。如果您决定创建自定义警报规则，请遵循以下一般准则：

- 查看默认警报规则的条件，并将其用作自定义警报规则的示例。
- 如果为警报规则定义了多个条件，请对所有条件使用相同的表达式。然后，更改每个条件的阈值。
- 仔细检查每个条件是否存在拼写错误和逻辑错误。
- 请仅使用网格管理 API 中列出的指标。
- 使用网格管理API测试表达式时、请注意、"成功"响应可能是空响应正文(未触发警报)。要查看警报是否实际触发，您可以临时将阈值设置为您希望当前为 true 的值。

  例如，要测试表达式 `node_memory_MemTotal_bytes < 24000000000`，请首先执行 `node_memory_MemTotal_bytes >= 0`并确保获得预期结果(所有节点返回一个值)。然后，将运算符和阈值改回预期值并重新执行。无结果表明此表达式当前没有警报。

- 除非您已验证自定义警报是按预期触发的、否则不要假定该警报正常工作。

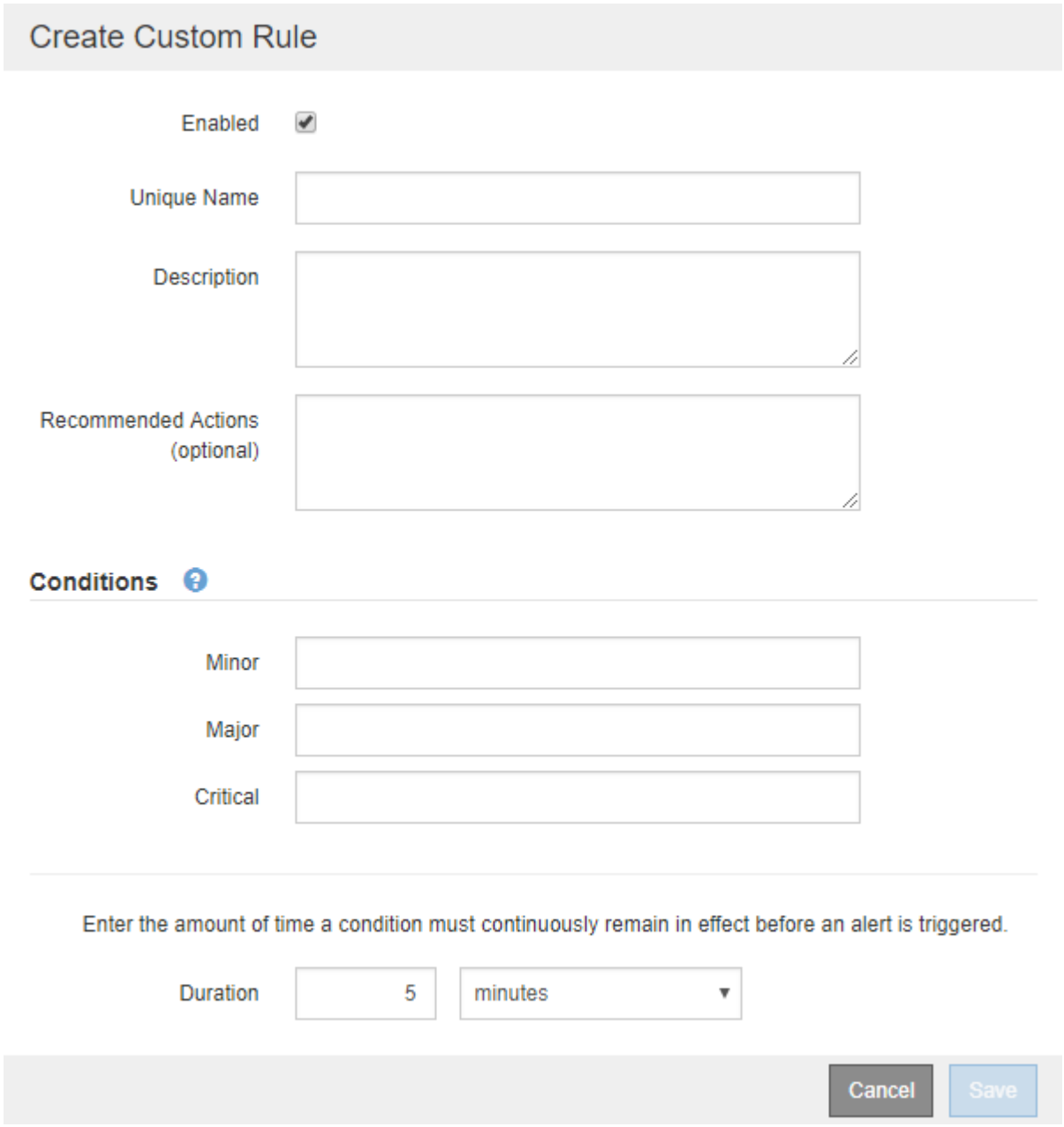
步骤

1. 选择*警报* > 规则。

此时将显示 "Alert Rules" 页面。

2. 选择 * 创建自定义规则 * 。

   此时将显示创建自定义规则对话框。



3. 选中或清除*已启用*复选框以确定当前是否已启用此警报规则。

   如果禁用了警报规则、则不会对其表达式进行评估、也不会触发任何警报。

4. 输入以下信息：

字段	说明
唯一名称	此规则的唯一名称。警报规则名称显示在警报页面上，也是电子邮件通知的主题。警报规则的名称可以介于 1 到 64 个字符之间。
说明	所发生问题的问题描述 。问题描述 是警报页面和电子邮件通知中显示的警报消息。警报规则的说明可以介于 1 到 128 个字符之间。
建议的操作	也可以选择触发此警报时建议采取的操作。以纯文本格式输入建议的操作（无格式化代码）。警报规则的建议操作可以介于 0 到 1 ， 024 个字符之间。

5. 在条件部分中，为一个或多个警报严重性级别输入一个 Prometheus 表达式。

   基本表达式通常采用以下形式：

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

   表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

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

6. 在 * 持续时间 * 字段中，输入在触发警报之前条件必须持续保持有效的时间量，然后选择一个时间单位。

   要在条件变为 true 时立即触发警报，请输入 * 。增加此值可防止临时条件触发警报。

   默认值为 5 分钟。

7. 选择 * 保存 * 。

   此时，对话框将关闭，新的自定义警报规则将显示在 "Alert Rules" 表中。

在 **StorageGRID** 中编辑警报规则

您可以编辑警报规则以更改触发条件，对于自定义警报规则，您还可以更新规则名称，问题描述 和建议的操作。

开始之前

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

关于此任务

编辑默认警报规则时，您可以更改次要警报，主要警报和严重警报的条件以及持续时间。编辑自定义警报规则时，您还可以编辑规则的名称，问题描述 和建议的操作。

决定编辑警报规则时请务必小心。如果更改了触发值，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

步骤

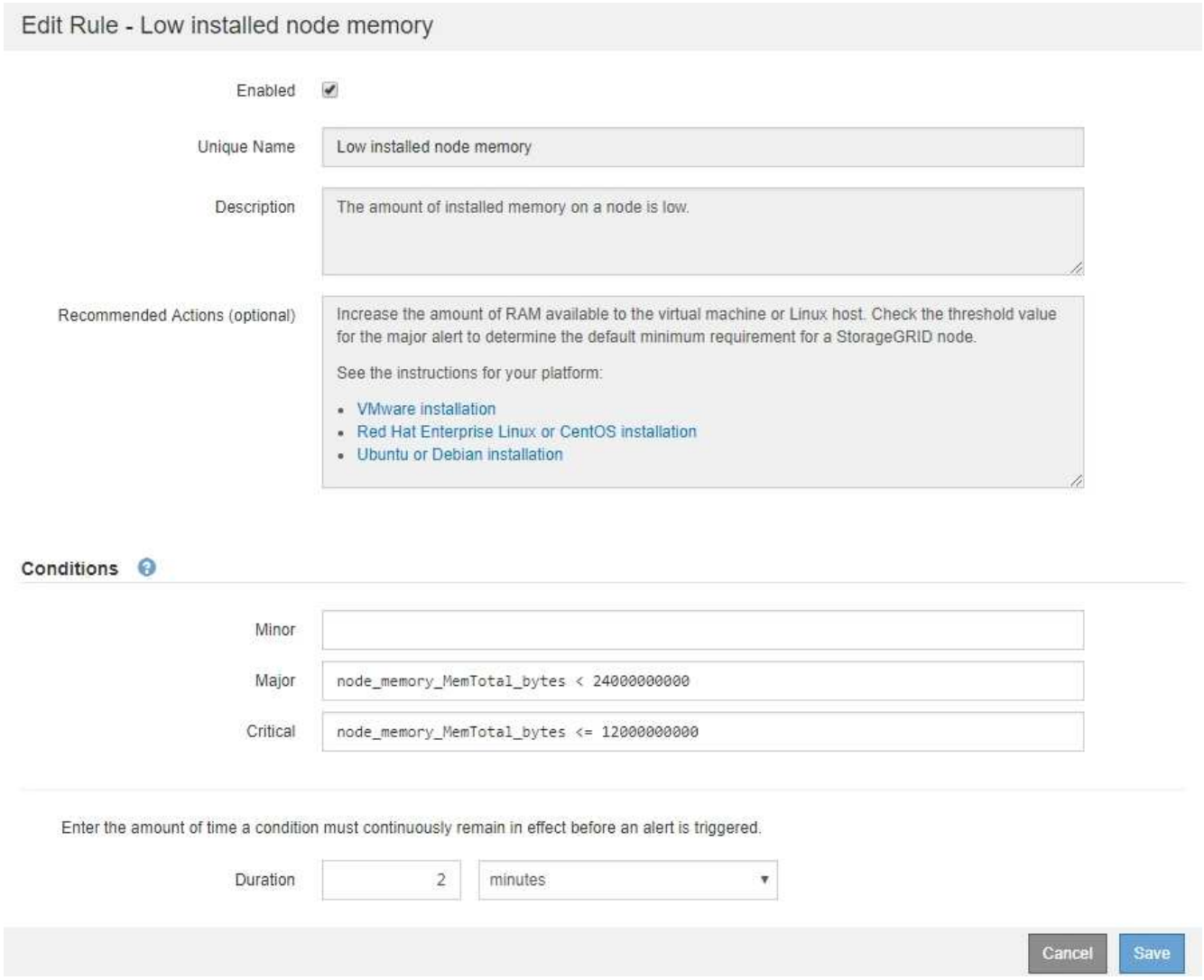
1. 选择*警报* > 规则。

   此时将显示 "Alert Rules" 页面。

2. 选择要编辑的警报规则对应的单选按钮。

3. 选择 * 编辑规则 * 。

   此时将显示编辑规则对话框。此示例显示了一个默认警报规则：“唯一名称”、“问题描述 ”和“建议操作”字段已禁用，无法编辑。



4. 选中或清除*已启用*复选框以确定当前是否已启用此警报规则。

   如果禁用了警报规则、则不会对其表达式进行评估、也不会触发任何警报。

   如果您对当前警报禁用警报规则，则必须等待几分钟，使警报不再显示为活动警报。

通常，不建议禁用默认警报规则。如果禁用了警报规则，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

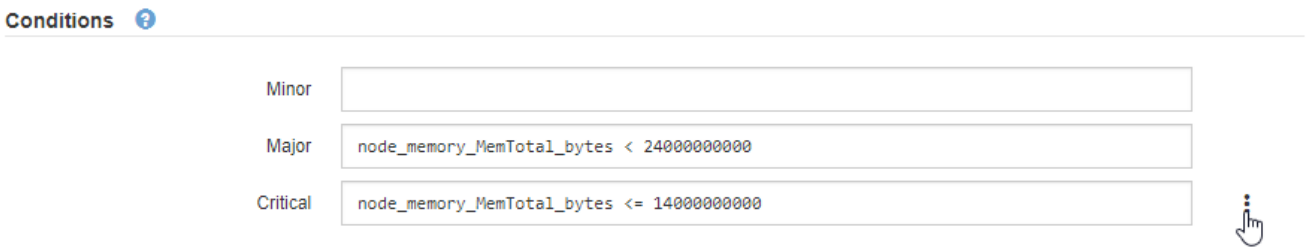
5. 对于自定义警报规则，请根据需要更新以下信息。

您无法编辑默认警报规则的此信息。

字段	说明
唯一名称	此规则的唯一名称。警报规则名称显示在警报页面上，也是电子邮件通知的主题。警报规则的名称可以介于 1 到 64 个字符之间。
说明	所发生问题的问题描述 。问题描述 是警报页面和电子邮件通知中显示的警报消息。警报规则的说明可以介于 1 到 128 个字符之间。
建议的操作	也可以选择触发此警报时建议采取的操作。以纯文本格式输入建议的操作（无格式化代码）。警报规则的建议操作可以介于 0 到 1 ， 024 个字符之间。

6. 在条件部分中，输入或更新一个或多个警报严重性级别的 Prometheus 表达式。

如果要将已编辑默认警报规则的条件还原为其原始值，请选择已修改条件右侧的三个点。



如果您更新了当前警报的条件，则在解决上一条件之前，可能无法实施您所做的更改。下次满足规则的其中一个条件时，警报将反映更新后的值。

基本表达式通常采用以下形式：

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

表达式可以是任意长度，但会显示在用户界面的单行上。至少需要一个表达式。

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

```
node_memory_MemTotal_bytes < 24000000000
```

7. 在 * 持续时间 * 字段中，输入在触发警报之前条件必须持续保持有效的时间量，然后选择时间单位。

要在条件变为 true 时立即触发警报，请输入 * 。增加此值可防止临时条件触发警报。

默认值为 5 分钟。

8. 选择 * 保存 * 。

   如果您编辑了默认警报规则，则 "Type" 列中将显示 "* 默认值 " 。如果禁用了默认或自定义警报规则， * 状态 * 列中将显示 * 已禁用 * 。

在 StorageGRID 中禁用警报规则

您可以更改默认或自定义警报规则的启用 / 禁用状态。

开始之前

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

关于此任务

禁用警报规则后、不会对其表达式进行评估、也不会触发警报。

> 通常，不建议禁用默认警报规则。如果禁用了警报规则，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

步骤

1. 选择*警报* > 规则。

   此时将显示 "Alert Rules" 页面。

2. 选择要禁用或启用的警报规则对应的单选按钮。
3. 选择 * 编辑规则 * 。

   此时将显示编辑规则对话框。

4. 选中或清除*已启用*复选框以确定当前是否已启用此警报规则。

   如果禁用了警报规则、则不会对其表达式进行评估、也不会触发任何警报。

   > 如果您对当前警报禁用警报规则，则必须等待几分钟，以使警报不再显示为活动警报。

5. 选择 * 保存 * 。
   - 已禁用 * 显示在 * 状态 * 列中。

删除 StorageGRID 中的自定义警报规则

如果您不想再使用自定义警报规则，可以将其删除。

开始之前

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

步骤

1. 选择*警报* > 规则。

   此时将显示 "Alert Rules" 页面。

2. 选择要删除的自定义警报规则对应的单选按钮。

   您无法删除默认警报规则。

3. 选择 * 删除自定义规则 * 。

   此时将显示确认对话框。

4. 选择 * 确定 * 以删除警报规则。

   任何处于活动状态的警报实例将在 10 分钟内得到解决。

管理警报通知

为 **StorageGRID** 警报设置 **SNMP** 通知

如果您希望 StorageGRID 在发生警报时发送 SNMP 通知，则必须启用 StorageGRID SNMP 代理并配置一个或多个陷阱目标。

您可以使用网格管理器中的 配置 > 监控 > **SNMP** 代理 选项或网格管理 API 的 SNMP 端点来启用和配置StorageGRID SNMP 代理。 SNMP 代理支持 SNMP 协议的所有三个版本。

要了解如何配置SNMP代理，请参见"使用 SNMP 监控"。

配置 StorageGRID SNMP 代理后，可以发送两种类型的事件驱动型通知：

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

在任何严重性级别触发默认或自定义警报时，系统都会发送陷阱和通知通知通知。要禁止警报的 SNMP 通知，您必须为此警报配置静默。请参阅。 "静默警报通知"

如果您的StorageGRID部署包含多个管理节点、则主管理节点是警报通知、AutoSupport软件包以及SNMP陷阱和通知的首选发送方。如果主管理节点不可用、则其他管理节点会临时发送通知。请参阅。 "什么是管理节点？"

为 **StorageGRID** 警报设置电子邮件通知

如果您希望在出现警报时发送电子邮件通知，则必须提供有关 SMTP 服务器的信息。您还必须输入警报通知收件人的电子邮件地址。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。

- 您拥有"管理警报或root访问权限"。
- 您有 "已配置电子邮件服务器"。

关于此任务

如果您的StorageGRID部署包含多个管理节点、则主管理节点是警报通知、AutoSupport软件包以及SNMP陷阱和通知的首选发送方。如果主管理节点不可用、则其他管理节点会临时发送通知。请参阅。 "什么是管理节点？"

步骤

1. 选择*Alerts* > **Alerts email**。

   此时将显示提醒电子邮件页面。

2. 选中*为警报启用电子邮件*复选框，以指示您希望在警报达到配置的阈值时发送通知电子邮件。
3. 在*按严重程度接收电子邮件*部分，选择要接收通知的警报类型对应的单选按钮。
4. 在发件人部分，指定有效的电子邮件地址用作警报通知的发件人地址。

   例如： `storagegrid-alerts@example.com`

   a. 在收件人部分中，为每个电子邮件列表或发生警报时应接收电子邮件的人员输入电子邮件地址。

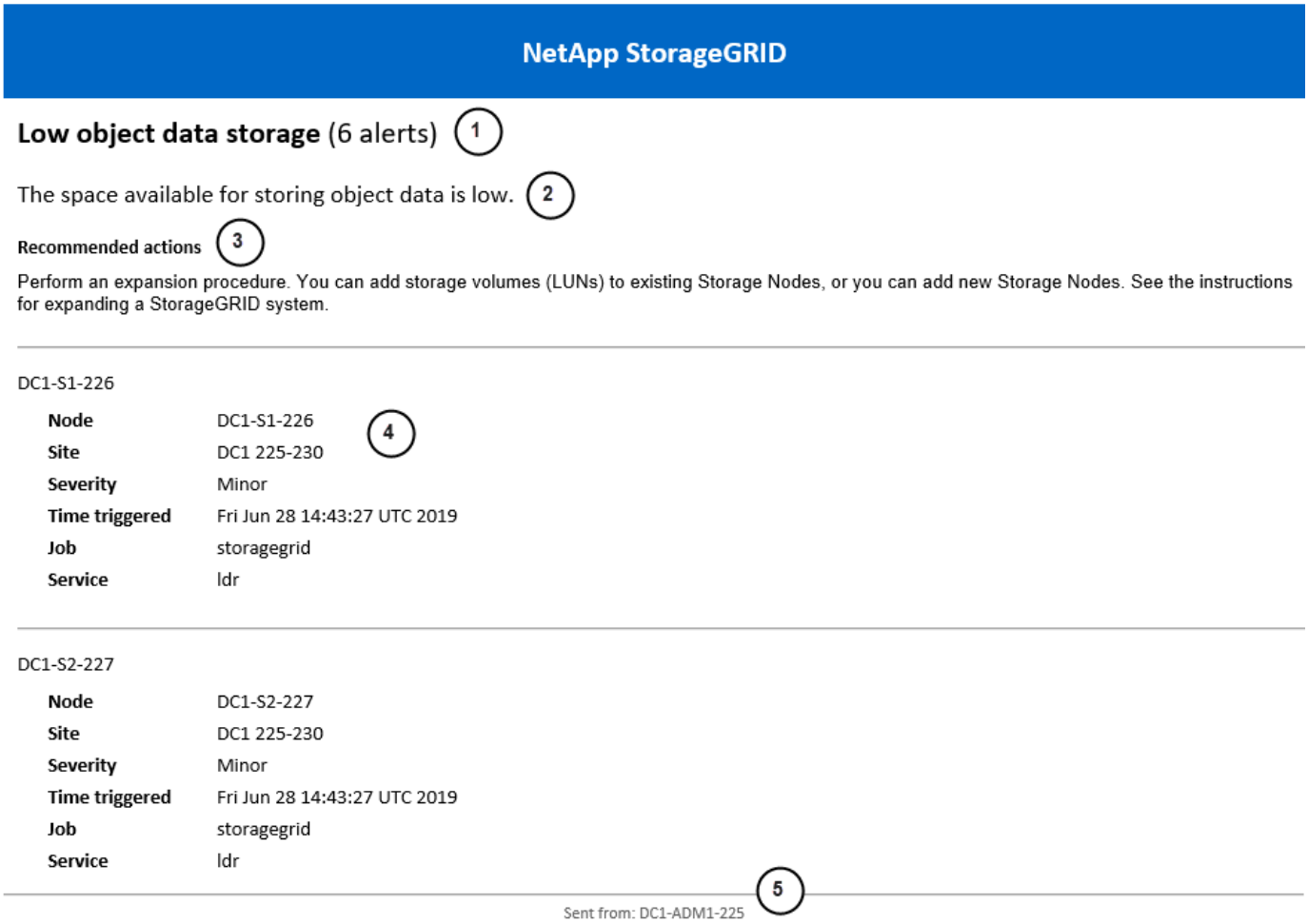
      选择*添加收件人*以添加收件人。

5. 选择 * 保存 * 。

警报电子邮件通知中包含的信息

配置电子邮件服务器并启用电子邮件警报后，在触发警报时，将向指定的收件人发送电子邮件通知，除非警报规则被静默抑制。请参阅"静默警报通知"。

电子邮件通知包括以下信息：



Callout	说明
1	警报名称，后跟此警报的活动实例数。
2	警报的问题描述 。
3	此警报的建议操作。
4	有关警报的每个活动实例的详细信息，包括受影响的节点和站点，警报严重性，触发警报规则的 UTC 时间以及受影响作业和服务的名称。
5	发送通知的管理节点的主机名。

如何对警报进行分组

为了防止在触发警报时发送过多的电子邮件通知， StorageGRID 会尝试在同一通知中对多个警报进行分组。

有关 StorageGRID 如何在电子邮件通知中对多个警报进行分组的示例，请参见下表。

行为	示例
每个警报通知仅适用于同名警报。如果同时触发两个名称不同的警报，则会发送两封电子邮件通知。	• 警报 A 会同时在两个节点上触发。仅发送一个通知。 • 节点 1 上触发警报 A ，节点 2 上同时触发警报 B 。系统会发送两个通知—每个警报一个。
对于特定节点上的特定警报，如果达到阈值的严重性超过一个，则仅针对最严重警报发送通知。	• 此时将触发警报 A ，并达到次要，主要和严重警报阈值。系统会为严重警报发送一条通知。
首次触发警报时， StorageGRID 会等待 2 分钟，然后再发送通知。如果在此期间触发了其他同名警报，则 StorageGRID 会在初始通知中对所有警报进行分组。	1. 警报A在08：00在节点1上触发。不会发送任何通知。 2. 警报A在节点2上于08：01触发。不会发送任何通知。 3. 在08：02时、系统会发送通知以报告这两个警报实例。
如果触发另一个同名警报， StorageGRID 将等待 10 分钟，然后再发送新通知。新通知会报告所有活动警报（当前未静音的警报），即使先前已报告这些警报也是如此。	1. 警报A在08：00在节点1上触发。通知将在08：02发送。 2. 警报A于08：05在节点2上触发。第二个通知将在08：15 (10分钟后)发送。此时将报告这两个节点。
如果当前存在多个同名警报且其中一个警报已解决，则在已解决警报的节点上重新出现此警报时，不会发送新通知。	1. 已针对节点 1 触发警报 A 。此时将发送通知。 2. 已针对节点 2 触发警报 A 。此时将发送第二个通知。 3. 已解决节点 2 的警报 A ，但此警报对于节点 1 仍处于活动状态。 4. 此时将再次触发节点 2 的警报 A 。不会发送任何新通知，因为此警报对于节点 1 仍处于活动状态。
StorageGRID 会继续每 7 天发送一次电子邮件通知，直到所有警报实例均已解决或警报规则已静音为止。	1. 3 月 8 日为节点 1 触发警报 A 。此时将发送通知。 2. 警报 A 未解决或静音。其他通知将于 3 月 15 日， 3 月 22 日， 3 月 29 日等时间发送。

对警报电子邮件通知进行故障排除

如果触发了电子邮件通知失败警报，但您没有收到，请按照以下步骤调查并解决问题：

- 测试电子邮件服务器通知
- StorageGRID 警报电子邮件
- 多管理员验证（MAV）电子邮件

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您有"root访问权限"。如果您具有"管理警报"权限，则可以查看但不能编辑电子邮件服务器配置。

步骤

1. 验证您的警报电子邮件设置。
   a. 验证您是否为收件人指定了有效的电子邮件地址。
   b. 选择 配置 > 电子邮件服务器，并验证电子邮件 (SMTP) 服务器设置是否正确。
2. 检查垃圾邮件筛选器，确保电子邮件未发送到垃圾文件夹。
3. 请您的电子邮件管理员确认来自发件人地址的电子邮件未被阻止。
4. 请检查以下与电子邮件传输相关的项目：
   a. 电子邮件服务器日志监控：查看 StorageGRID 使用的电子邮件服务器的日志（ 配置 > 电子邮件服务器 ）。搜索与 StorageGRID 尝试发送电子邮件时间匹配的中继错误、身份验证错误和其他故障。
   b. 未送达报告（退回邮件）：如果未收到电子邮件，且 StorageGRID 未报告故障，则问题可能是退回邮件。将"发件人"地址配置为使用有效的电子邮件地址，将使这些退回回复电子邮件对您可见。
5. 收集发送电子邮件的管理节点的日志文件。查看 /var/local/log/prometheus.log 和 /var/local/log/nms.log 文件，找出您可能能够纠正的明显问题。如果您无法解决此问题，请联系技术支持。

   技术支持可以使用日志中的信息帮助确定出现问题的原因。例如， prometheus.log 文件在连接到您指定的服务器时可能会显示错误。

   请参阅 "收集日志文件和系统数据"。

在 **StorageGRID** 中静音警报通知

或者，您也可以配置静音以临时禁止警报通知。

开始之前

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

关于此任务

您可以对整个网格，单个站点或单个节点以及一个或多个严重性静默警报规则。每次静默都将禁止针对单个警报规则或所有警报规则发出所有通知。

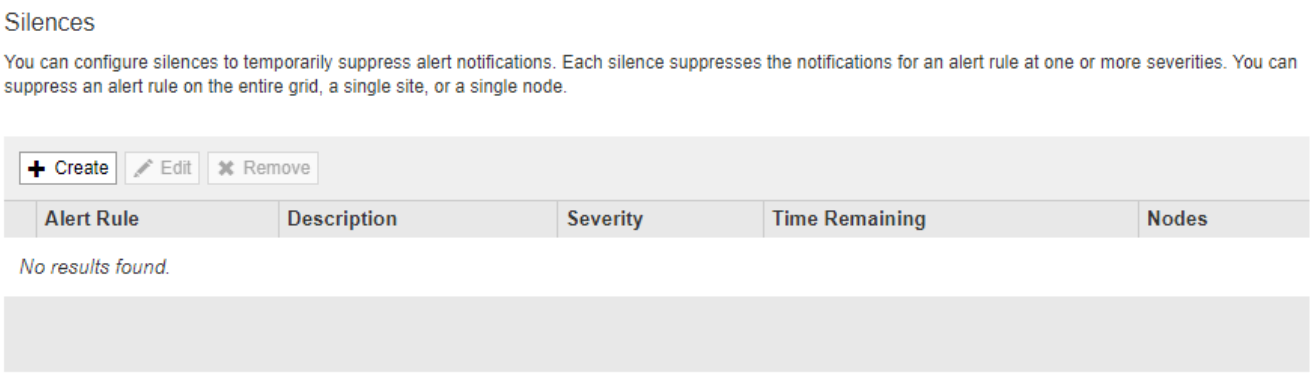
如果已启用 SNMP 代理，则 Silences 还会禁止 SNMP 陷阱并通知。

> 在决定静默警报规则时，请务必小心。如果您静默警报，则可能无法检测到潜在问题，直到它阻止完成关键操作为止。

步骤

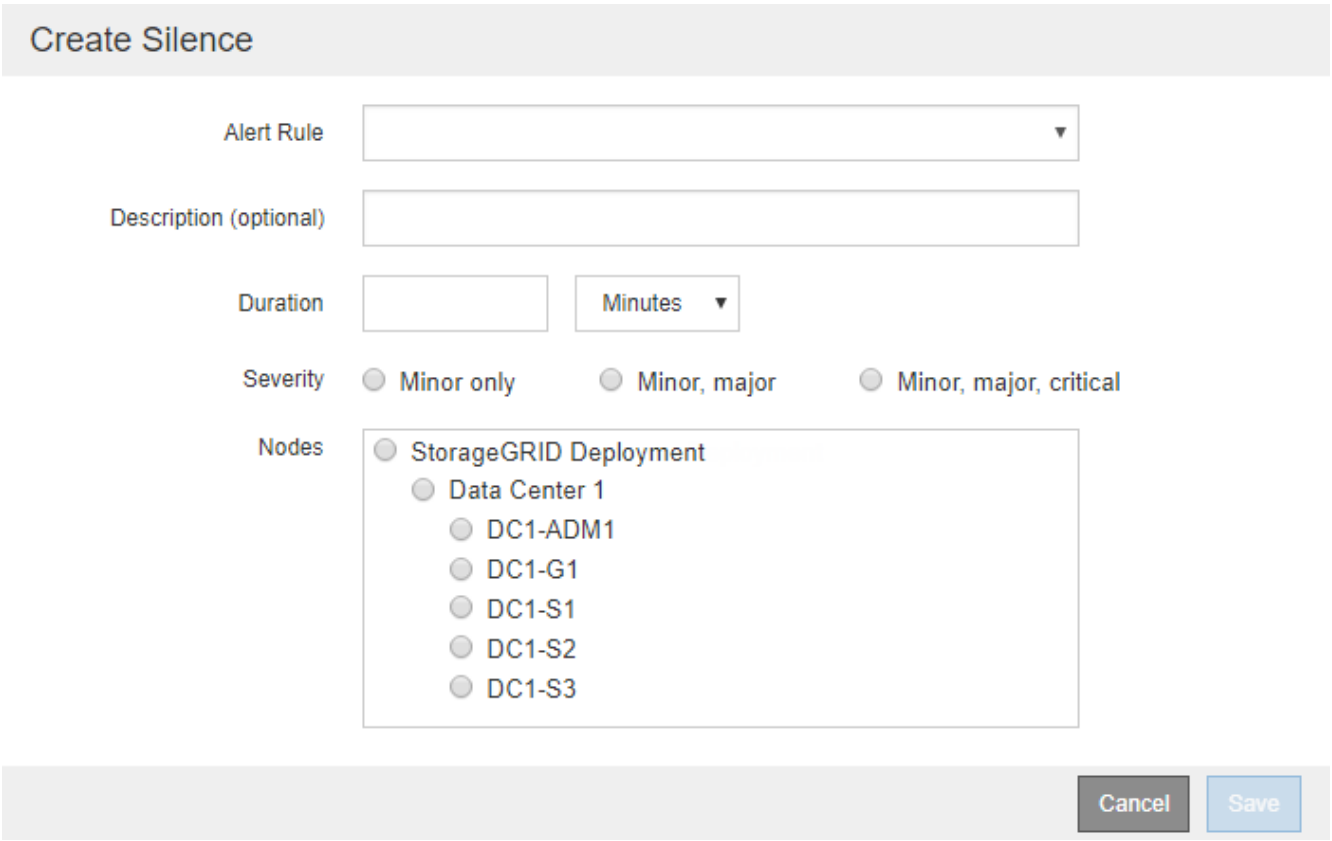
1. 选择*警报* > 静音。

   此时将显示 Silences 页面。



2. 选择 * 创建 * 。

   此时将显示创建静默对话框。



3. 选择或输入以下信息：

字段	说明
警报规则	要静默的警报规则的名称。您可以选择任何默认或自定义警报规则，即使警报规则已禁用也是如此。 • 注： * 如果要使用此对话框中指定的标准将所有警报规则静默，请选择 * 所有规则 * 。
说明	也可以选择静默问题描述 。例如，请描述此静默的目的。

字段	说明
持续时间	希望此静默保持有效的时间，以分钟，小时或天为单位。静默时间为 5 分钟到 1 ， 825 天（ 5 年）。 • 注意： * 不应将警报规则静默较长时间。如果某个警报规则已静音，则在阻止完成关键操作之前，您可能无法检测到潜在问题。但是，如果警报是由特定的有意配置触发的，则可能需要使用长时间静默，例如， "* 服务设备链路已关闭 " 警报和 "* 存储设备链路已关闭 " 警报可能会出现这种情况。
严重性	应将哪个警报严重性或严重性静音。如果在选定严重性之一触发警报，则不会发送任何通知。
节点	您希望此静默应用于哪个或哪些节点。您可以禁止整个网格，单个站点或单个节点上的警报规则或所有规则。如果选择整个网格，则会将适用场景 静默所有站点和所有节点。如果选择站点，则此静默状态仅适用于该站点上的节点。 *注意：*每次静默不能选择多个节点或多个站点。如果要同时在多个节点或多个站点上禁止相同的警报规则，则必须创建其他静音。

4. 选择 * 保存 * 。
5. 如果要在静默过期之前修改或结束静默，可以对其进行编辑或删除。

选项	说明
编辑静默	a. 选择*警报* > 静音。 b. 从表中，选择要编辑的静默设置对应的单选按钮。 c. 选择 * 编辑 * 。 d. 更改问题描述 ，剩余时间，选定严重性或受影响的节点。 e. 选择 * 保存 * 。
取消静默	a. 选择*警报* > 静音。 b. 从表中，选择要删除的静默设置对应的单选按钮。 c. 选择 * 删除 * 。 d. 选择 * 确定 * 确认要删除此静默状态。 ◦ 注意 * ：现在，在触发此警报时，系统将发送通知（除非被另一个静默禁止）。如果当前触发此警报，则发送电子邮件或 SNMP 通知以及更新警报页面可能需要几分钟的时间。

相关信息

"配置 SNMP 代理"

StorageGRID 中的警报

此参考列出了网格管理器中显示的默认警报。建议的操作会显示在您收到的警报消息中。

您可以根据需要创建自定义警报规则，以适合您的系统管理方法。

某些默认警报使用"Prometheus 指标"。

设备警报

警报名称	说明
设备电池已过期	设备存储控制器中的电池已过期。
设备电池出现故障	设备存储控制器中的电池出现故障。
设备电池的已学习容量不足	设备存储控制器中的电池已获取容量不足。
设备电池即将过期	设备存储控制器中的电池即将过期。
已取出设备电池	设备存储控制器中的电池缺失。
设备电池过热	设备存储控制器中的电池过热。
设备 BMC 通信错误	与基板管理控制器（ BMC ）的通信已丢失。
检测到设备启动设备故障	检测到设备中的启动设备有问题。
设备缓存备份设备失败	永久性缓存备份设备出现故障。
设备缓存备份设备容量不足	缓存备份设备容量不足。
设备缓存备份设备已写保护	缓存备份设备受写保护。
设备缓存内存大小不匹配	设备中的两个控制器具有不同的缓存大小。
设备CMOS电池故障	检测到设备中的 CMOS 电池存在问题。
设备计算控制器机箱温度过高	StorageGRID 设备中计算控制器的温度已超过额定阈值。
设备计算控制器 CPU 温度过高	StorageGRID 设备中计算控制器的 CPU 温度已超过额定阈值。
设备计算控制器需要引起注意	在 StorageGRID 设备的计算控制器中检测到硬件故障。
设备计算控制器电源 A 出现问题	计算控制器中的电源A出现问题。

警报名称	说明
设备计算控制器电源 B 出现问题	计算控制器中的电源 B 出现问题。
设备计算硬件监控服务已停止	监控存储硬件状态的服务已停止。
设备DAS驱动器超过每天写入数据的限制	每天向驱动器写入的数据量过多、这可能会使其保修失效。
检测到设备DAS驱动器故障	检测到设备中的直连存储(DAS)驱动器存在问题。
设备 DAS 驱动器位于错误的插槽或节点	直接连接存储 (DAS) 驱动器位于错误的插槽或节点
设备DAS驱动器定位灯亮起	设备存储节点中的一个或多个直连存储(DAS)驱动器的驱动器定位灯亮起。
设备DAS驱动器正在重建	正在重建直连存储(DAS)驱动器。如果最近更换或移除/重新插入、则这是预期的。
检测到设备风扇故障	检测到产品中的风扇装置有问题。
检测到设备光纤通道故障	检测到设备存储控制器与计算控制器之间存在光纤通道链路问题
设备光纤通道 HBA 端口故障	光纤通道 HBA 端口出现故障或出现故障。
设备闪存缓存驱动器非最佳	用于 SSD 缓存的驱动器并非最佳驱动器。
已卸下设备互连 / 电池箱	互连 / 电池箱缺失。
缺少设备 LACP 端口	StorageGRID 设备上的端口不参与 LACP 绑定。
检测到设备NIC故障	检测到设备中的网络接口卡(NIC)有问题。
设备整体电源性能下降	StorageGRID 设备的电源已偏离建议的工作电压。
需要设备SANtricity OS 软件更新	SANtricity软件版本低于此StorageGRID版本的建议最低版本。
检测到设备 SFP 故障	在 StorageGRID 设备的计算控制器中检测到 SFP 故障。
设备SSD严重警告	设备SSD报告严重警告。
设备存储控制器 A 出现故障	StorageGRID 设备中的存储控制器 A 出现故障。

警报名称	说明
设备存储控制器 B 故障	StorageGRID 设备中的存储控制器 B 出现故障。
设备存储控制器驱动器故障	StorageGRID 设备中的一个或多个驱动器出现故障或不是最佳驱动器。
设备存储控制器硬件问题描述	SANtricity 软件报告 StorageGRID 设备中的某个组件 " 需要关注 " 。
设备存储控制器电源 A 出现故障	StorageGRID 设备中的电源 A 与建议的工作电压不同。
设备存储控制器电源 B 故障	StorageGRID 设备中的电源 B 与建议的工作电压不同。
设备存储硬件监控服务已停止	监控存储硬件状态的服务已停止。
设备存储架降级	存储设备存储架中某个组件的状态为已降级。
已超过设备温度	已超过设备存储控制器的额定或最大温度。
已卸下设备温度传感器	已卸下温度传感器。
设备UEFI安全启动错误	设备未安全启动。
磁盘 I/O 速度非常慢	磁盘I/O非常慢可能会影响网格性能。
检测到存储设备风扇故障	检测到设备存储控制器中的风扇单元出现问题。
存储设备存储连接已降级	计算控制器和存储控制器之间的一个或多个连接出现问题。
无法访问存储设备	无法访问存储设备。

审核和系统日志警报

警报名称	说明
正在将审核日志添加到内存队列中	节点无法将日志发送到本地系统日志服务器，并且内存队列正在填满。
外部系统日志服务器转发错误	节点无法将日志转发到外部系统日志服务器。
审核队列较大	审计消息的磁盘队列已满。如果不解决此问题，S3 操作可能会失败。
正在将日志添加到磁盘队列中	节点无法将日志转发到外部系统日志服务器，并且磁盘队列正在填满。

存储分段警报

警报名称	说明
FabricPool 存储分段具有不受支持的存储分段一致性设置	FabricPool分段使用可用或强站点一致性级别、这种级别不受支持。
FabricPool存储分段具有不受支持的版本控制设置	FabricPool分段已启用版本控制或S3对象锁定、但不支持此功能。
ListBucket 对 Get/Head 对象的权限检查已禁用	ListBucket 对不存在的密钥执行 GetObject/HeadObject 的权限检查已禁用。

Cassandia警报

警报名称	说明
Cassandra auto-compactor 错误	Cassandra 自动 compactor 出现错误。
Cassandra 自动数据压缩器指标已过期	描述 Cassandra 自动数据压缩器的指标已过时。
Cassandra 通信错误	运行 Cassandra 服务的节点无法彼此通信。
Cassandra compActions 已过载	Cassandra 数据缩减过程过载。
Cassand拉 特写错误	内部StorageGRID 进程向Cassanda发送了一个过大的写入请求。
Cassandra 修复指标已过期	描述 Cassandra 修复作业的指标已过时。
Cassandra 修复进度缓慢	Cassandra 数据库修复进度缓慢。
Cassandra 修复服务不可用	Cassandra 修复服务不可用。
Cassandra 表损坏	Cassandra 检测到表损坏。如果 Cassandra 检测到表损坏，则它会自动重新启动。

云存储池警报

警报名称	说明
云存储池连接错误	云存储池的运行状况检查检测到一个或多个新错误。
IAM角色无处不在最终实体认证到期	IAM角色Anywhere最终实体证书即将过期。

跨网格复制警报

警报名称	说明
跨网格复制永久失败	发生跨网格复制错误、需要用户干预才能解决。
跨网格复制资源不可用	由于资源不可用、跨网格复制请求处于待处理状态。

DHCP警报

警报名称	说明
DHCP 租约已过期	网络接口上的 DHCP 租约已过期。
DHCP 租约即将到期	网络接口上的 DHCP 租约即将到期。
DHCP 服务器不可用	DHCP 服务器不可用。

调试和跟踪警报

警报名称	说明
调试性能影响	启用调试模式后、系统性能可能会受到负面影响。
已启用跟踪配置	启用跟踪配置后、系统性能可能会受到负面影响。

电子邮件和**AutoSupport** 警报

警报名称	说明
无法发送AutoSupport 消息	无法发送最新的AutoSupport 消息。
域名解析失败	StorageGRID节点无法解析域名。
电子邮件通知失败	无法发送警报电子邮件通知。
未找到日志归档目标存储桶	缺少日志归档目标存储桶，导致日志无法归档到目标存储桶。
SNMP通知错误	向陷阱目标发送SNMP通知时出错。
已启用 SSH 外部访问	SSH 外部访问已启用超过 24 小时。
检测到SSH或控制台登录	在过去24小时内、用户已使用Web控制台或SSH登录。

纠删编码**(EC)**警报

警报名称	说明
区块服务高 goroutine 计数	区块服务的 goroutine 数量异常高，这可能表示死锁或资源泄漏。
EC 重新平衡失败	EC重新平衡操作步骤 失败或已停止。
EC 修复失败	EC数据的修复作业失败或已停止。
EC 修复已停止	EC数据的修复作业已停止。
已对片段验证进行了审核编码错误	无法再验证经过删除编码的片段。损坏的碎片可能无法修复。
处于需要修复状态的擦除编码组	当没有正在进行的擦除编码数据修复时，一个或多个擦除编码组处于需要修复状态。

证书到期警报

警报名称	说明
管理代理CA证书到期	管理代理服务器CA包中的一个或多个证书即将过期。
客户端证书到期	一个或多个客户端证书即将过期。
S3 的全局服务器证书到期	S3 的全球服务器证书即将过期。
负载平衡器端点证书到期	一个或多个负载平衡器端点证书即将过期。
管理接口的服务器证书到期	用于管理接口的服务器证书即将过期。
外部系统日志 CA 证书到期	用于签署外部系统日志服务器证书的证书颁发机构（ CA ）证书即将过期。
外部系统日志客户端证书到期	外部系统日志服务器的客户端证书即将过期。
外部系统日志服务器证书到期	外部系统日志服务器提供的服务器证书即将过期。

网格网络警报

警报名称	说明
网格网络 MTU 不匹配	网格网络接口(eth0)的MTU设置在网格中的各个节点之间差别很大。

网格联盟警报

警报名称	说明
网格联合证书到期	一个或多个网格联合证书即将过期。
网格联合连接失败	本地网格与远程网格之间的网格联合连接不起作用。

高使用量或高延迟警报

警报名称	说明
元数据查询延迟较长	Cassandra 元数据查询的平均时间过长。

身份联合警报

警报名称	说明
身份联合同步失败	无法从身份源同步联合组和用户。
租户的身份联合同步失败	无法从租户配置的身份源同步联合组和用户。

信息生命周期管理**(ILM)**警报

警报名称	说明
无法实现 ILM 放置	无法为某些对象实现 ILM 规则中的放置指令。
ILM 扫描速率低	ILM 扫描速率设置为每秒不到 100 个对象。

密钥管理服务器**(KMS)**警报

警报名称	说明
Kms CA 证书到期	用于对密钥管理服务器（ KMS ）证书进行签名的证书颁发机构（ CA ）证书即将过期。
Kms 客户端证书到期	密钥管理服务器的客户端证书即将过期
无法加载 Kms 配置	密钥管理服务器的配置存在，但无法加载。
Kms 连接错误	设备节点无法连接到其站点的密钥管理服务器。
未找到 Kms 加密密钥名称	配置的密钥管理服务器没有与提供的名称匹配的加密密钥。

警报名称	说明
Kms 加密密钥轮换失败	所有设备卷均已成功解密、但一个或多个卷无法转换为最新密钥。
未配置公里	此站点不存在密钥管理服务器。
Kms 密钥无法对设备卷进行解密	无法使用当前 KMS 密钥对启用了节点加密的设备上的一个或多个卷进行解密。
Kms 服务器证书到期	密钥管理服务器（ KMS ）使用的服务器证书即将过期。
Kms服务器连接失败	设备节点无法连接到其站点的密钥管理服务器集群中的一个或多个服务器。

负载平衡器警报

警报名称	说明
提升了零请求负载平衡器连接	与负载平衡器端点的连接在未执行请求的情况下断开的百分比增加。

本地时钟偏移警报

警报名称	说明
本地时钟大时间偏移	本地时钟和网络时间协议(NTP)时间之间的偏移过大。

内存不足或空间不足警报

警报名称	说明
审核日志磁盘容量低	审计日志的可用空间不足。如果不解决此问题，S3 操作可能会失败。
可用节点内存不足	节点上的可用 RAM 量较低。
存储池可用空间不足	存储节点中可用于存储对象数据的空间不足。
节点内存不足	节点上安装的内存量不足。
元数据存储不足	可用于存储对象元数据的空间不足。
低指标磁盘容量	可用于指标数据库的空间不足。
对象数据存储不足	可用于存储对象数据的空间不足。
低只读水印覆盖	存储卷软只读水印覆盖小于存储节点的最小优化水印。

警报名称	说明
根磁盘容量低	根磁盘上的可用空间不足。
系统数据容量低	/var/local 的可用空间不足。如果不解决此问题，S3 操作可能会失败。
tmp 目录可用空间不足	/tmp 目录中的可用空间不足。

节点或节点网络警报

警报名称	说明
ADC 法定人数未达到	具有 ADC 服务的存储节点处于离线状态。在 ADC 仲裁恢复之前，扩展和退役操作将被阻止。
管理网络接收使用量	管理网络上的接收使用率较高。
管理网络传输使用量	管理网络上的传输使用率较高。
防火墙配置失败	无法应用防火墙配置。
回退模式下的管理接口端点	所有管理接口端点回退到默认端口的时间过长。
节点网络连接错误	在节点之间传输数据时出错。
节点网络接收帧错误	节点收到的网络帧中有很高比例出现错误。
节点与 NTP 服务器不同步	此节点与网络时间协议(NTP)服务器不同步。
节点未使用 NTP 服务器锁定	节点未锁定到网络时间协议（ NTP ）服务器。
非设备节点网络已关闭	一个或多个网络设备已关闭或断开连接。
管理网络上的服务设备链接已关闭	管理网络(eth1)的设备接口已关闭或断开连接。
管理网络端口 1 上的服务设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。
客户端网络上的服务设备链路关闭	客户端网络(eth2)的设备接口已关闭或断开连接。
网络端口1上的服务设备链路关闭	设备上的网络端口1已关闭或断开连接。
网络端口2上的服务设备链路关闭	设备上的网络端口2已关闭或断开连接。

警报名称	说明
网络端口3上的服务设备链路关闭	设备上的网络端口3已关闭或断开连接。
网络端口4上的服务设备链路关闭	设备上的网络端口4已关闭或断开连接。
管理网络上的存储设备链路关闭	管理网络(eth1)的设备接口已关闭或断开连接。
管理网络端口 1 上的存储设备链路已关闭	设备上的管理网络端口 1 已关闭或断开连接。
客户端网络上的存储设备链路关闭	客户端网络(eth2)的设备接口已关闭或断开连接。
网络端口1上的存储设备链路关闭	设备上的网络端口1已关闭或断开连接。
网络端口2上的存储设备链路关闭	设备上的网络端口2已关闭或断开连接。
网络端口3上的存储设备链路关闭	设备上的网络端口3已关闭或断开连接。
网络端口4上的存储设备链路关闭	设备上的网络端口4已关闭或断开连接。
存储节点未处于所需的存储状态	由于内部错误或与卷相关的问题描述、存储节点上的LDR服务无法过渡到所需状态
TCP连接使用情况	此节点上的TCP连接数即将达到可跟踪的最大数量。
无法与节点通信	一个或多个服务无响应，或者无法访问节点。
节点意外重新启动	节点在过去 24 小时内意外重新启动。

对象警报

警报名称	说明
对象存在检查失败	对象存在检查作业失败。
对象存在检查已停止	对象存在检查作业已停止。
可能丢失的物品	网格中可能丢失一个或多个对象。
检测到孤立对象	已检测到孤立对象。
S3 分段上传的分段大小过大	客户端正在尝试执行超出分段大小限制的分段上传操作。

警报名称	说明
S3放置对象大小太大	客户端尝试的Put Object操作超出S3大小限制。
使用不受支持的条件标头的 S3 请求	S3 客户端正在对某些操作使用不受支持的条件标头（If-Match 或 If-None-Match）。
S3 请求使用了错误区域，且已启用全局命名空间	S3 客户端正在使用错误的签名区域来访问此网格的存储桶。
检测到未标识的损坏对象	在复制的对象存储中找到无法标识为复制对象的文件。

对象损坏警报

警报名称	说明
物体尺寸不匹配	在对象存在性检查过程中检测到意外的对象大小。

平台服务警报

警报名称	说明
平台服务待处理请求容量低	平台服务待处理请求的数量即将达到容量。
平台服务不可用	具有 RSM 服务的存储节点在站点上运行或可用的数量太少。

存储卷警报

警报名称	说明
存储卷需要引起注意	存储卷已脱机、需要引起注意。
需要还原存储卷	存储卷已恢复、需要还原。
存储卷脱机	存储卷已脱机5分钟以上。
已尝试重新挂载存储卷	存储卷已脱机并触发自动重新挂载。这可能表示驱动器问题或文件系统错误。
卷还原无法启动复制的数据修复	无法自动启动已修复卷的复制数据修复。

StorageGRID 服务警报

警报名称	说明
使用备份配置的NGinx服务	Nginx服务的配置无效。现在正在使用先前的配置。
使用备份配置的Ngins-GW服务	Ngins-GW服务的配置无效。现在正在使用先前的配置。
要禁用FIPS、需要重新启动	安全策略不需要 FIPS 模式，但正在使用 FIPS 模块。
要启用FIPS、需要重新启动	安全策略需要 FIPS 模式，但未使用 FIPS 模块。
使用备份配置的SSH服务	SSH服务的配置无效。现在正在使用先前的配置。

租户警报

警报名称	说明
租户配额使用量高	正在使用的配额空间百分比较高。默认情况下、此规则处于禁用状态、因为它可能发生原因 会发送过多通知。

StorageGRID 中常用的 **Prometheus** 指标

请参阅此常用Prometheus指标列表、以更好地了解默认警报规则中的条件或构建自定义警报规则的条件。

您也可以获取所有指标的完整列表。

有关 Prometheus 查询语法的详细信息，请参见 "查询基础知识"。

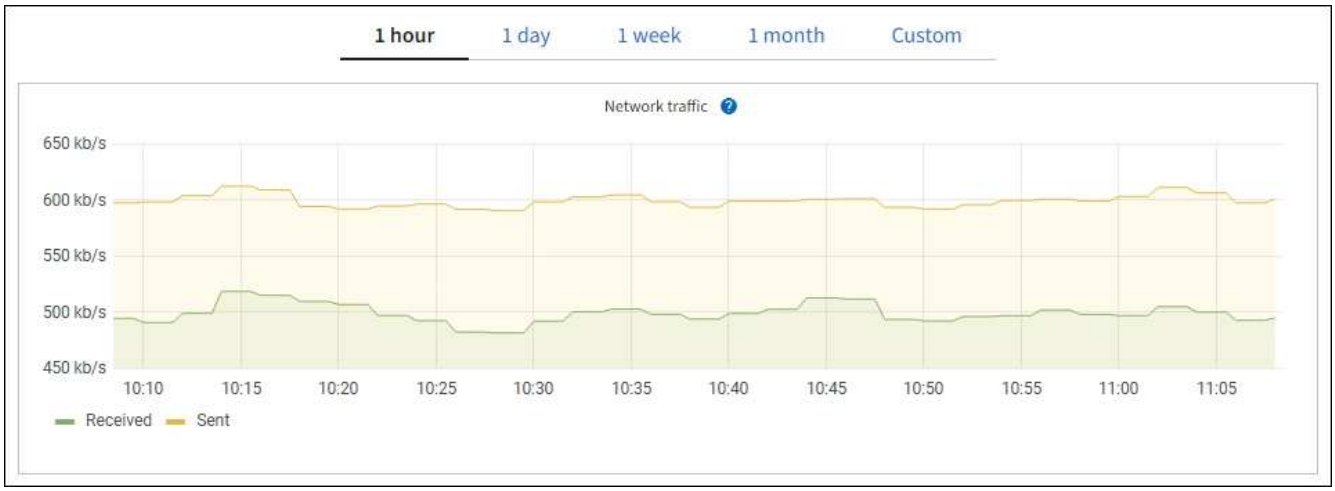
什么是**Prometheus**指标?

Prometheus指标是时间序列测量值。管理节点上的Prometheus服务会从所有节点上的服务收集这些指标。指标会存储在每个管理节点上，直到为 Prometheus 数据预留的空间已满为止。当卷达到容量时 `/var/local/mysql_ibdata/`、将首先删除最早的指标。

Prometheus指标在哪里使用?

Prometheus收集的指标在网格管理器的多个位置使用：

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



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

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

- 支持 > 工具 > 诊断*页面和*支持 > 工具 > *指标*页面：这些页面主要供技术支持使用，提供了使用 Prometheus 指标值的多种工具和图表。

> 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。

列出最常见的指标

以下列表包含最常用的Prometheus指标。

> 名称中包含_privly_的指标仅供内部使用、可能会在不同StorageGRID 版本之间进行更改、恕不另行通知。

alertmanager_notifications _failed_total

失败警报通知的总数。

node_filesystem_avail_bytes

可供非root用户使用的文件系统空间量(以字节为单位)。

node_memory_MemAvailable_bytes

内存信息字段 MemAvailable_bytes 。

node_network_Carrier

托架值 `/sys/class/net/iface`。

node_network_receive； errs_total

网络设备统计信息 `receive_errs`。

node_network_transmit_errs_total

网络设备统计信息 `transmit_errs`。

storaggrid_administratively 关闭

由于预期原因，节点未连接到网格。例如，节点或节点上的服务已正常关闭，节点正在重新启动或软件正在升级。

storagegrid_appliage_compute_controller_hardware_status

设备中计算控制器硬件的状态。

storagegrid_appliation_failed_disks

对于设备中的存储控制器、不是最佳驱动器的数量。

storagegrid_appliage_storage_controller_hardware_status

设备中存储控制器硬件的整体状态。

storagegrid_content_bages_and_containers

此存储节点已知的 S3 存储桶总数。

storaggrid_content_objects

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

storaggrid_content_objects_lost

此服务在 StorageGRID 系统中检测到缺失的对象总数。应采取措施确定丢失的发生原因 以及是否可以恢复。

"对丢失和丢失的对象数据进行故障排除"

storagegRid_http_sessions_incoming_attempted

尝试访问存储节点的 HTTP 会话总数。

storaggrid_http_sessions_incoming_currently 已建立

存储节点上当前处于活动状态（已打开）的 HTTP 会话数。

storagegRid_http_sessions_incoming_failed

由于 HTTP 请求格式错误或在处理操作时失败而无法成功完成的 HTTP 会话总数。

storagegRid_http_sessions_incoming_successful

已成功完成的 HTTP 会话总数。

storaggrid_ilm_awaiting 背景对象

此节点上等待通过扫描进行 ILM 评估的对象总数。

storaggrid_ilm_awaiting 客户端评估对象每秒对象数

根据此节点上的 ILM 策略评估对象的当前速率。

storaggrid_ilm_awaiting 客户端对象

此节点上等待通过客户端操作进行 ILM 评估的对象总数（例如，载入）。

storaggrid_ilm_awaing_total_objects

等待 ILM 评估的对象总数。

storagegrid_ilm_scanne_objects_per_second

此节点拥有的对象在 ILM 中进行扫描和排队的速率。

storaggrid_ilm_scann_period_estimated_minutes

在此节点上完成完整 ILM 扫描的估计时间。

- 注： * 完全扫描并不能保证 ILM 已应用于此节点拥有的所有对象。

storagegRid_load_Balancer_endpoint_ct_expiry_time

负载平衡器端点证书自 Epoch 以来的到期时间（以秒为单位）。

storaggrid_metadata_queries_average ； **latency** ；毫秒

通过此服务对元数据存储运行查询所需的平均时间。

storaggrid_network_received_bytes

自安装以来接收的总数据量。

storaggrid_network_transmated_bytes

自安装以来发送的总数据量。

storagegrid_node_cpu_utilization 百分比

此服务当前正在使用的可用 CPU 时间的百分比。指示服务的繁忙程度。可用 CPU 时间量取决于服务器的 CPU 数量。

storaggrid_ntp_chosed_time_source_offset_mms

选定时间源提供的系统时间偏移。如果到达某个时间源的延迟与该时间源到达 NTP 客户端所需的时间不相等，则会引入偏移。

storaggrid_ntp_locked

此节点未锁定到网络时间协议(NTP)服务器。

storagegrid_s3_data_transfers_bytes_ingested

自上次重置属性以来从 S3 客户端载入到此存储节点的总数据量。

storagegrid_s3_data_transfers_bytes_retrieved

自上次重置属性以来 S3 客户端从此存储节点检索的总数据量。

storagegrid_s3_operations_failed

S3 操作失败的总数（ HTTP 状态代码 4xx 和 5xx ），不包括因 S3 授权失败而导致的操作。

storagegrid_s3_operations_successful

成功执行 S3 操作的总数（ HTTP 状态代码 2xx ）。

storagegrid_s3_operations_unauthorized

授权失败导致的 S3 操作失败的总数。

storagegRid_servercertificate_management_interface_cert_expiry_days

管理接口证书到期前的天数。

storagegRid_servercertificate_storage_api_Endpoints" 证书到期日 **"**

对象存储 API 证书到期前的天数。

storaggrid_service_cpu_seconds

自安装以来此服务使用 CPU 的累积时间。

storagegrid_service_memory_usage_bytes

此服务当前正在使用的内存量（ RAM ）。此值与 Linux 顶部实用程序显示的值相同，即 Res 。

storaggrid_service_network_received_bytes

自安装以来此服务收到的总数据量。

storaggrid_service_network_transmated_bytes

此服务发送的总数据量。

storagegrid_service_Restart

重新启动服务的总次数。

storaggrid_service_runtime_seconds

自安装以来服务一直运行的总时间量。

storaggrid_service_uptime_seconds

服务自上次重新启动以来的总运行时间。

storaggrid_storage_state_current

存储服务的当前状态。属性值为：

- 10 = 脱机
- 15 = 维护
- 20 = 只读
- 30 = 联机

storagegrid_storage_status

存储服务的当前状态。属性值为：

- 0 = 无错误
- 10 = 正在过渡
- 20 = 可用空间不足
- 30 = 卷不可用
- 40 = 错误

storagegrid存储利用率数据字节

存储节点上已复制和已进行过彻底编码的对象数据的估计总大小。

storaggrid_storage_utilization metadata_allowed_bytes

每个存储节点的卷 0 上允许用于对象元数据的总空间。此值始终小于为节点上的元数据预留的实际空间，因为必要的数据库操作（如数据缩减和修复）以及未来的硬件和软件升级都需要预留部分空间。对象元数据允许的空间控制整体对象容量。

storaggrid_storage_utilization metadata_bytes

存储卷 0 上的对象元数据量，以字节为单位。

storaggrid_storage_utilization 总空间字节

分配给所有对象存储的存储空间总量。

storagegRid_storage_utilization_usable_space_bytes

剩余的对象存储空间总量。计算方法是将存储节点上所有对象存储的可用空间量相加。

storagegrid_tenant_usage_data_bytes

租户的所有对象的逻辑大小。

storagegrid_tenant_usage_object_count

租户的对象数。

storagegRid_tenant_usage_quota_bytes

可用于租户对象的最大逻辑空间量。如果未提供配额指标，则可用空间量不受限制。

获取所有指标的列表

[[obtain all-metrics]]要获取完整的指标列表、请使用网格管理API。

步骤

1. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
2. 找到 * 指标 * 操作。
3. 执行此 `GET /grid/metric-names`操作。
4. 下载结果。

日志文件参考

StorageGRID 日志文件

StorageGRID 提供了用于捕获事件，诊断消息和错误情况的日志。系统可能会要求您收集日志文件并将其转发给技术支持以协助进行故障排除。

这些日志分为以下几类：

- "StorageGRID 软件日志"
- "部署和维护日志"

- "关于 bycast.log"

> 为每种日志类型提供的详细信息仅供参考。这些日志可供技术支持进行高级故障排除。使用审核日志和应用程序日志文件重建问题历史记录的高级技术不在本说明的范围之内。

访问日志

要访问日志，您可以"收集日志文件和系统数据"来自一个或多个节点作为单个日志文件存档。或者，您可以按如下方式访问每个网格节点的单独日志文件：

步骤

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

将日志导出到系统日志服务器

将日志导出到系统日志服务器可提供以下功能：

- 除了 S3 请求之外，还接收所有网格管理器和租户管理器请求的列表。
- 更好地了解返回错误的S3请求、而不会因审核日志记录方法而影响性能。
- 访问易于解析的HTTP层请求和错误代码。
- 更好地了解负载平衡器上的流量划分器阻止的请求。

要导出日志，请参阅"配置日志管理和外部系统日志服务器"。

日志文件类别

StorageGRID 日志文件归档包含为每个类别描述的日志以及包含指标和调试命令输出的其他文件。

归档位置	说明
acct-tunnel.log	与负载均衡器配合使用的帐户隧道助手的日志。
审核	在正常系统操作期间生成的审核消息。
基础操作系统日志	基本操作系统信息，包括 StorageGRID 映像版本。
捆绑包	全局配置信息（捆绑包）。
缓存服务	缓存服务日志（仅在网关节点上）。
Cassandra	Cassandra 数据库信息和 Reaper 修复日志。

归档位置	说明
EC	按配置文件ID列出的有关当前节点和EC组信息的vCS信息。
网格	常规网格日志，包括调试(`bycast.log`)和 `servermanager`日志。
grid．json	网格配置文件在所有节点之间共享。此外、 `node.json`特定于当前节点。
hagroup	高可用性组指标和日志。
安装	`Gdu-server`并安装日志。
internal-access.log	内部 HTTP 代理流量日志。
lambda-arbitrator	与 S3 Select 代理请求相关的日志。
泄漏	来自 leakd 服务的日志。
lumberjack.log	与日志收集相关的调试消息。
manage-audit.log	`mgmt-api` 访问审核日志。
指标	Grafana ， Jaeger ，节点导出程序和 Prometheus 的服务日志。
错误	其他访问和错误日志。
MySQL	MariaDB 数据库配置和相关日志。
网络	网络相关脚本和动态 IP 服务生成的日志。
nginx	负载平衡器和网格联合配置文件和日志。还包括 Grid Manager 和租户管理器流量日志。

归档位置	说明
nginx 网关	• `access.log`：网格管理器和租户管理器请求日志消息。 ◦ 使用系统日志导出时、这些消息会以作为前处理 `mgmt:`。 ◦ 这些日志消息的格式为 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`：入站跨网格复制请求。 ◦ 使用系统日志导出时、这些消息会以作为前处理 `cgr:`。 ◦ 这些日志消息的格式为 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`：S3 请求负载均衡器端点。 ◦ 使用系统日志导出时、这些消息会以作为前处理 `endpoint:`。 ◦ 这些日志消息的格式为 `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`：与新DNS检查警报相关。 • stream-access.log：流块的 TCP/TLS 流（第 4 层）代理会话。 注意：这不是 HTTP 请求日志。
NTP	NTP 配置文件和日志。
孤立对象	与孤立对象相关的日志。
os	节点和网格状态文件，包括服务 `pid`。
其他	下的日志文件 `/var/local/log`不会收集到其他文件夹中。
性能	CPU ，网络和磁盘 I/O 的性能信息
Prometheus-data	当前 Prometheus 指标（如果日志收集包含 Prometheus 数据）。
配置	与网格配置过程相关的日志。
草稿	来自平台服务中使用的 raft 集群的日志。
revision_history.json	修订历史记录。

归档位置	说明
routed-s3-access.log.gz	路由的网格联合流量的访问日志，类似于 S3（全局命名空间/联合 URL）。
SSH	与SSH配置和服务相关的日志。
SNMP	用于发送SNMP通知的SNMP代理配置。
套接字数据	用于网络调试的套接字数据。
system-bucket.log	`update-system-bucket-configuration.log`：系统存储桶日志。
system-commands.txt	StorageGRID 容器命令的输出。包含系统信息，例如网络连接和磁盘使用情况。
synchron-recovery—软件包	与维护托管 ADC 服务的所有管理节点和存储节点上最新恢复包的一致性有关。
update-cipher-configurations.log	`update-cors-configurations.log`：跟踪与 TLS/cipher 和 CORS 更改相关的日志。
update-leakd-configurations.log	孤立检测配置日志。

StorageGRID 软件日志

您可以使用 StorageGRID 日志对问题进行故障排除。

如果您想要将日志发送到外部系统日志服务器或更改审计信息的目的地，例如 `bycast.log`和 `nms.log`， 看"配置日志管理"。

常规 **StorageGRID** 日志

文件名	备注	在上找到
/var/local/log/bycast.log	主要的StorageGRID故障排除文件。	所有节点
/var/local/log/bycast-err.log	包含一个子集 `bycast.log`（严重性为 ERROR 和 CRITICAL 的消息）。系统中也会显示严重消息。	所有节点

文件名	备注	在上找到
/var/local/core/	包含在程序异常终止时创建的任何核心转储文件。可能的原因包括断言失败，违规或线程超时。 注意：文件 ``/var/local/core/kexec_cmd` 通常位于设备节点上，并不表示出现错误。	所有节点

与密码相关的日志

文件名	备注	在上找到
/var/local/log/ssh-config-generation.log	包含与生成SSH配置和重新加载SSH服务相关的日志。	所有节点
/var/local/log/ginx/config-generation.log	包含与生成Nginx配置和重新加载Nginx服务相关的日志。	所有节点
/var/local/log/Ngins-gw/ config-generation.log	包含与生成Ngins-GW配置(以及重新加载Ngins-GW服务)相关的日志。	管理节点和网关节点
/var/local/log/update-cipher-configurations.log	包含与配置TLS和SSH策略相关的日志。	所有节点

网格联合日志

文件名	备注	在上找到
/var/local/log/update_grid_federation_config.log	包含与为网格联盟连接生成Nginx和Ngins-GW配置相关的日志。	所有节点

NMS 日志

文件名	备注	在上找到
/var/local/log/nms.log	• 从网格管理器和租户管理器捕获通知。 • 捕获与NMS服务操作相关的事件。例如、电子邮件通知和配置更改。 • 包含因系统中的配置更改而导致的 XML 包更新。 • 包含与每天执行一次的属性缩减采样相关的错误消息。 • 包含 Java Web 服务器错误消息，例如页面生成错误和 HTTP 状态 500 错误。 • 包含与 AutoSupport 相关的日志。	管理节点
/var/local/log/nms.errlog	包含与 MySQL 数据库升级相关的错误消息。 包含相应服务的标准错误（ stderr ）流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	管理节点
/var/local/log/nms.requestlog	包含有关从管理 API 到内部 StorageGRID 服务的传出连接的信息。	管理节点

Server Manager 日志

文件名	备注	在上找到
/var/local/log/servermanager.log	服务器上运行的 Server Manager 应用程序的日志文件。	所有节点
/var/local/log/GridstatBackend.errlog	Server Manager GUI 后端应用程序的日志文件。	所有节点
/var/local/log/gridstat.errlog	Server Manager 图形用户界面的日志文件。	所有节点

StorageGRID 服务日志

文件名	备注	在上找到
/var/local/log/acct.errlog		运行此 ADC 服务的存储节点

文件名	备注	在上找到
/var/local/log/adc.errlog	包含相应服务的标准错误（ stderr ）流。每个服务有一个日志文件。除非服务出现问题，否则这些文件通常为空。	运行此 ADC 服务的存储节点
/var/local/log/ams.errlog		管理节点
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	缓存服务日志。	网关节点
/var/local/log/Cassanda/system.log	元数据存储（ Cassandra 数据库）的信息，如果添加新存储节点时出现问题或节点池修复任务停止，则可以使用这些信息。	存储节点
/var/local/log/cassandra-reaper.log	Cassandra Reaper 服务的信息，用于修复 Cassandra 数据库中的数据。	存储节点
/var/local/log/cassandra-reaper.errlog	Cassandra Reaper 服务的错误信息。	存储节点
/var/local/log/chunk．errlog		存储节点
/var/local/log/CMN.errlog		管理节点
/var/local/log/cms．errlog	此日志文件可能存在于已从旧版 StorageGRID 升级的系统上。它包含旧信息。	存储节点
/var/local/log/ds.errlog		存储节点
/var/local/log/dmv.errlog		存储节点
/var/local/log/dynip*	包含与 dynip 服务相关的日志，该日志可监控网格中的动态 IP 更改并更新本地配置。	所有节点
/var/local/log/grafana.log	与 Grafana 服务关联的日志，用于在网格管理器中显示指标。	管理节点
/var/local/log/hagroups.log	与高可用性组关联的日志。	管理节点和网关节点
/var/local/log/hagroups_events.log	跟踪状态更改，例如从备份过渡到主节点或故障。	管理节点和网关节点

文件名	备注	在上找到
/var/local/log/idnt.errlog		运行此 ADC 服务的存储节点
/var/local/log/jaeger.log	与 jaeger 服务关联的日志，用于收集跟踪。	所有节点
/var/local/log/kstn.errlog		运行此 ADC 服务的存储节点
/var/local/log/兰 百德*	包含 S3 Select 服务的日志。	管理节点和网关节点 只有某些管理节点和网关节点才包含此日志。请参见"S3 Select 管理节点和网关节点的要求和限制"。
/var/local/log/ldr.errlog		存储节点
/var/local/log/m3cd /*。log	包含 MISCd 服务（信息服务控制守护进程）的日志，此服务提供一个界面，用于查询和管理其他节点上的服务以及管理节点上的环境配置，例如查询其他节点上运行的服务的状态。	所有节点
/var/local/log/ginx/*.log	包含 nginx 服务的日志，此服务可充当各种网格服务（例如 Prometheus 和动态 IP ）的身份验证和安全通信机制，以便能够通过 HTTPS API 与其他节点上的服务进行通信。	所有节点
/var/local/log/Ngins-gw/*.log	包含与Ngins-GW服务相关的常规日志、包括错误日志以及管理节点上受限管理端口的日志。	管理节点和网关节点
/var/local/log/Ngins-gw/ cgr-access.log.gz	包含与跨网格复制流量相关的访问日志。	管理节点、网关节点或两者、具体取决于网格联合配置。仅在用于跨网格复制的目标网格上找到。
/var/local/log/Ngins-gw/ endpoint-access.log.gz	包含负载平衡器服务的访问日志、该服务可为从客户端到存储节点的S3流量提供负载平衡。	管理节点和网关节点
/var/local/log/perency*	包含永久性服务的日志，该服务用于管理根磁盘上需要在重新启动后持续存在的文件。	所有节点

文件名	备注	在上找到
/var/local/log/prometheus.log	对于所有节点，包含节点导出程序服务日志和 ade-exporter指标 服务日志。 对于管理节点，还包含 Prometheus 和警报管理器服务的日志。	所有节点
/var/local/log/raft.log	包含用于 raft 协议的 RSM 服务所使用的库的输出。	具有 RSM 服务的存储节点
/var/local/log/rms.errlog	包含用于 S3 平台服务的复制状态机服务（ RSM ）服务的日志。	具有 RSM 服务的存储节点
/var/local/log/ssm.errlog		所有节点
/var/local/log/update-s3vs-domains.log	包含与处理 S3 虚拟托管域名配置的更新相关的日志。请参见实施 S3 客户端应用程序的说明。	管理节点和网关节点
/var/local/log/update-SNMP-Firewall.*	包含与为 SNMP 管理的防火墙端口相关的日志。	所有节点
/var/local/log/update-sysl.log	包含与对系统系统系统日志配置所做更改相关的日志。	所有节点
/var/local/log/update-traffic-classes.log	包含与流量分类器配置更改相关的日志。	管理节点和网关节点
/var/local/log/update-utcn.log	包含与此节点上的不可信客户端网络模式相关的日志。	所有节点

相关信息

- "关于 bycast.log"
- "使用S3 REST API"

StorageGRID 中的部署和维护日志

您可以使用部署和维护日志对问题进行故障排除。

文件名	备注	在上找到
/var/local/log/install.log	在软件安装期间创建。包含安装事件的记录。	所有节点

文件名	备注	在上找到
/var/local/log/expansion-progress.log	在扩展操作期间创建。包含扩展事件的记录。	存储节点
/var/local/log/pa-move.log	在运行脚本时创建 `pa-move.sh`。	主管理节点
/var/local/log/pa-move-new_pa.log	在运行脚本时创建 `pa-move.sh`。	主管理节点
/var/local/log/pa-move-old_pa.log	在运行脚本时创建 `pa-move.sh`。	主管理节点
/var/local/log/gdu-server.log	由 GDU 服务创建。包含与主管理节点管理的配置和维护过程相关的事件。	管理节点
/var/local/log/send_admin_hw.log	在安装期间创建。包含与节点与主管理节点的通信相关的调试信息。	所有节点
/var/local/log/upgrade.log	在软件升级期间创建。包含软件更新事件的记录。	所有节点

了解 StorageGRID bycast.log

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

该文件 `/var/local/log/bycast-err.log`是的子集 `bycast.log`。它包含严重性错误和严重的消息。

或者，您可以更改审计日志的目标并将审计信息发送到外部系统日志服务器。当配置外部系统日志服务器时，将继续生成和存储审计记录的本地日志。看"配置日志管理和外部系统日志服务器" 。

bycast.log 的文件轮换

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

保存的文件将重命名 `bycast.log.1`，新文件名为 `bycast.log`。当新的达到1 GB时 `bycast.log`，`bycast.log.1`将重命名并压缩为，并 `bycast.log`重命名 `bycast.log.1`为 `bycast.log.2.gz`。

的旋转限制 `bycast.log`为21个文件。创建文件的第22个版本时 `bycast.log`、最旧的文件将被删除。

的旋转限制 `bycast-err.log`为七个文件。

> 如果日志文件已被压缩，则不能将其解压缩到写入该文件的同一位置。将文件解压缩到同一位置可能会干扰日志轮换脚本。

或者，您可以更改审计日志的目标并将审计信息发送到外部系统日志服务器。当配置外部系统日志服务器时，将

继续生成和存储审计记录的本地日志。看"配置日志管理和外部系统日志服务器" 。

相关信息

"收集日志文件和系统数据"

bycast.log 中的消息

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

ADE 消息示例：

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

ADE 消息包含以下信息：

消息段	示例中的值
节点ID	12455685
ADE 进程 ID	0357819531
模块名称	SVMR
消息标识符	EVHR
UTC 系统时间	2019-05-05T27T17：10：29.784677 (YYYY-MM-DDTHH：MM：SS.uuuuuuu)
严重性级别	错误
内部跟踪编号	0906
消息	SVMR ： 卷 3 的运行状况检查失败，原因为 "Tut"

bycast.log 中的消息严重性

中的消息 `bycast.log`已分配严重性级别。

例如：

- * 通知 * —发生了应记录的事件。大多数日志消息都处于此级别。
- * 警告 * - 发生意外情况。

- * 错误 * —发生了一个会影响操作的重大错误。
- * 严重 * —发生异常情况，导致正常操作停止。您应立即解决基本情况。

中的错误代码 `bycast.log`

中的大多数错误消息 `bycast.log`都包含错误代码。

下表列出了中常见的非数字代码 `bycast.log`。非数字代码的确切含义取决于报告上下文。

错误代码	含义
SUC	无错误
GERR	未知
已完成	已取消
异常	已中止
输出	超时
调用	无效
NFND	未找到
服务器	版本
配置	配置
失败	失败
ICPL	未完成
完成	完成
SUNV	服务不可用

下表列出了中的数字错误代码 `bycast.log`。

错误编号	错误代码	含义
001	EPERM	不允许执行此操作
002	已执行	没有此类文件或目录

错误编号	错误代码	含义
003	ESRCH	无此过程
004	EINTR	系统调用中断
005	EIO	I/O 错误
006	ENXIO	没有此类设备或地址
007	E2BIG	参数列表太长
008	ENOExec	Exec 格式错误
009	EBADF	文件编号错误
010	ECHILD	无子进程
011	EAGAIN	请重试
012	ENOMEM	内存不足
013	EACCE	权限被拒绝
014	默认	地址错误
015	ENOTBLK	需要块设备
016	EBUSY	设备或资源繁忙
017	EEXIST	文件已存在
018	EXDEV	跨设备链路
019	ENODEV	没有此类设备
020	ENOTDIR	不是目录
021	EISDIR	是一个目录
022	EINVAL	参数无效
023	ENFILE	文件表溢出

错误编号	错误代码	含义
024	EMFILE	打开的文件过多
025	ENOTTY	不是一种打字机
026	ETXTBSY	文本文件繁忙
027	EFBIG	文件太大
028	ENOSPC	设备上没有剩余空间
029	ESPIPE	非法寻道
030	EROFS	只读文件系统
031	EMLINK	链路太多
032	EPIPE	管道已断开
033	以登	数学参数不在功能域中
034	电子书	数学结果不可代表
035	EDEADLK	可能会发生资源死锁
036	ENAMETOOLONG	文件名太长
037	ENOLCK	没有可用的记录锁定
038	ENOSYS	未实施功能
039	ENOTEMPTY	目录不为空
040	ELOOP	遇到的符号链接太多
041		
042	ENOMSG	没有所需类型的消息
043	EIDRM	已删除标识符
044	ECHRNG	通道编号超出范围

错误编号	错误代码	含义
045	EL2NSYNC	2 级未同步
046	EL3HLT	级别 3 已暂停
047	EL3RST	3 级重置
048	ELNRNG	链路编号超出范围
049	EUNATCH	未连接协议驱动程序
050	ENOCSI	没有可用的 CSI 结构
051	EL2HLT	级别 2 已暂停
052	EBADE	交换无效
053	EBADR	请求描述符无效
054	EXFULL	Exchange 已满
055	ENOANO	无阳极
056	EBADRQC	请求代码无效
057	EBADLT	插槽无效
058		
059	EBFNT	字体文件格式错误
060	ENOSTR	设备不是流
061	ENODATA	无可用数据
062	时间	计时器已过期
063	ENOSR	流资源不足
064	ENONET	计算机不在网络上
065	ENOPK	未安装软件包

错误编号	错误代码	含义
066	EREMOTE	对象为远程对象
067	ENOLINK	链路已切断
068	EADV	公布错误
069	ESRMNT	Srmount 错误
070	eComm	发送时出现通信错误
071	EPROTO	协议错误
072	EMULTIHOP	已尝试多跃点
073	EDOTDOT	RFS 专用错误
074	EBADMSG	不是数据消息
075	超越	对于定义的数据类型，值太大
076	ENOTUNIQ	名称在网络上不唯一
077	EBADFD	文件描述符处于错误状态
078	错误	已更改远程地址
079	EIBAcc	无法访问所需的共享库
080	EIBBAD	访问损坏的共享库
081	ELIBSCN	
082	ELIBMAX	正在尝试链接过多的共享库
083	ELIBExec	无法直接执行共享库
084	EILSEQ	字节序列非法
085	错误	应重新启动中断的系统调用
086	ESTRPIPE	流管道错误

错误编号	错误代码	含义
087	EUSERs.	用户过多
088	ENOTSOCK	在非套接字上执行套接字操作
089	EDESTADDRREQ	目标地址为必填项
090	EMSSIZE	消息太长
091	EPROTOTYPE	套接字的协议类型错误
092	ENOPROTOOPT	协议不可用
093	产品说明	不支持协议
094	ESOCKTNOSUPPORT	不支持套接字类型
095	EOPNOTSUPP	传输端点上不支持此操作
096	EPFNOSUPPORT	不支持协议系列
097	EAFNOSUPPORT	协议不支持地址系列
098	EADDRINUSE	地址已在使用中
099	EADDRNOTAVAIL	无法分配请求的地址
100	ENETDOWN	网络已关闭
101	ENETUNREACH	无法访问网络
102	ENETRESET	由于重置，网络已断开连接
103	已完成	软件导致连接终止
104	ECONNRESET	对等方重置连接
105	ENOBUFS	无可用缓冲区空间
106	EISCONN	传输端点已连接
107	ENOTCONN	传输端点未连接

错误编号	错误代码	含义
108	ESHUTDOWN	传输端点关闭后无法发送
109	ETOOMANYREFS	参考太多：无法拼接
110	ETIMEDOUT	连接超时
111	ECONNREFUSED	连接被拒绝
112	EHOSTDOWN	主机已关闭
113	EHOSTUNREACH	没有到主机的路由
114	EALREADY	操作已在进行中
115	EINPROGRESS	操作正在进行中
116		
117	EUC	结构需要清理
118	ENOTCAM	不是名为 type 的 Xenix 文件
119	ENAVAIL	没有可用的 Xenix 信号
120	EISNAM	是一个命名类型的文件
121	EREMOTEIO	远程 I/O 错误
122	EDQUOT	已超过配额
123	ENOMINDIUM	未找到介质
124	EMeduMTYPE	介质类型错误
125	ECANCELED	操作已取消
126	ENOKEY	所需密钥不可用
127	EKEYEXPIRED	密钥已过期
128	EKBREVOKED	密钥已撤销

错误编号	错误代码	含义
129	已完成	密钥已被服务拒绝
130	终止	对于稳定可靠的 mMutexes： owner died
131	ENOTRECOVERABLE	对于强大的 mutexes：状态不可恢复

配置日志管理和外部系统日志服务器

StorageGRID 中的外部系统日志服务器

外部系统日志服务器是 StorageGRID 外部的服务器，您可以使用它在一个位置收集系统审核信息。通过使用外部系统日志服务器、您可以减少管理节点上的网络流量、并更高效地管理信息。对于StorageGRID、出站系统日志消息数据包格式符合RFC 3164。

可以发送到外部系统日志服务器的审核信息类型包括：

- 包含在正常系统操作期间生成的审核消息的审核日志
- 与安全相关的事件，例如登录和上报给 root
- 如果需要创建支持案例以对遇到的问题描述 进行故障排除，则可能需要请求的应用程序日志

何时使用外部系统日志服务器

如果您的网格较大、使用多种类型的S3应用程序或希望保留所有审核数据、则外部系统日志服务器尤其有用。通过将审核信息发送到外部系统日志服务器，您可以：

- 更高效地收集和管理审核信息、例如审核消息、应用程序日志和安全事件。
- 减少管理节点上的网络流量、因为审核信息直接从各种存储节点传输到外部系统日志服务器、而无需通过管理节点。

> 将日志发送到外部系统日志服务器时、超过8、192字节的单个日志会在消息末尾被截断、以符合外部系统日志服务器实施中的常见限制。

> 为了在外部系统日志服务器发生故障时最大限度地恢复数据，(`localaudit.log`每个节点上最多保留20 GB的本地审核记录日志。

如何配置外部系统日志服务器

要了解如何配置外部 syslog 服务器，请参阅"配置日志管理和外部系统日志服务器"。

如果您计划配置使用TLS或RELP/TLS协议、则必须具有以下证书：

- 服务器**CA**证书：一个或多个可信CA证书，用于验证采用PEM编码的外部系统日志服务器。如果省略此参数，则会使用默认网格 CA 证书。
- 客户端证书：以PEM编码向外部系统日志服务器进行身份验证的客户端证书。

- 客户端专用密钥：PEM编码的客户端证书专用密钥。

> 如果使用客户端证书，则还必须使用客户端专用密钥。如果您提供加密的私钥，则还必须提供密码短语。使用加密的私钥不会带来显著的安全优势，因为必须存储密钥和密码短语；为了简化操作，建议使用未加密的私钥（如果可用）。

如何估算外部系统日志服务器的大小

通常，您的网格会进行规模估算，以达到所需的吞吐量，该吞吐量是按每秒 S3 操作数或每秒字节数定义的。例如，您可能要求网格每秒处理 1 ， 000 次 S3 操作，或者每秒处理 2 ， 000 MB 的对象载入和检索。您应根据网格的数据要求调整外部系统日志服务器的大小。

本节提供了一些启发式公式，可帮助您估算外部系统日志服务器需要能够处理的各种类型的日志消息的速率和平均大小，这些消息以网格的已知或所需性能特征（每秒 S3 操作数）表示。

在估计公式中使用每秒 **S3** 操作数

如果网格的大小以每秒字节为单位表示，则必须将此规模估算转换为每秒 S3 操作，才能使用估算公式。要转换网格吞吐量，您必须先确定平均对象大小，您可以使用现有审核日志和指标（如果有）中的信息或根据您对将使用 StorageGRID 的应用程序的了解来确定平均对象大小。例如，如果您的网格大小调整为可实现 2 ， 000 MB/秒的吞吐量，而您的平均对象大小为 2 MB ，则您的网格大小将调整为能够每秒处理 1 ， 000 次 S3 操作（ 2 ， 000 MB/ 2 MB ）。

> 以下各节中用于估算外部系统日志服务器规模的公式提供了常见案例估算（而不是最坏案例估算）。根据您的配置和工作负载，您可能会发现系统日志消息或系统日志数据卷的速率高于或低于公式的预测。这些公式仅供参考。

审核日志的估计公式

如果除了网格应支持的每秒 S3 操作数之外，您没有其他有关 S3 工作负载的信息，则可以使用以下公式估算外部系统日志服务器需要处理的审核日志卷， 假设您将审核级别设置为默认值（所有类别均设置为正常，但存储设置为错误除外）：

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，则外部系统日志服务器的大小应为每秒支持 2 ， 000 条系统日志消息，并且应能够以每秒 1.6 MB 的速率接收（并且通常存储）审核日志数据。

如果您对工作负载有更多了解，可以进行更准确的估计。对于审核日志、最重要的其他变量是S3操作的放置(与获取)百分比、以及以下S3字段的平均大小(表中使用的4个字符缩写为审核日志字段名称)(以字节为单位)：

代码	字段	说明
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。

代码	字段	说明
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3存储分段	S3 存储分段名称。
S3KY	S3密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。

让我们使用 P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

让我们使用K来表示S3帐户名称、S3存储分段和S3密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。然后， K 值为 90 （ 13+13+28+36 ）。

如果您可以确定 P 和 K 的值，则可以使用以下公式估算外部系统日志服务器需要处理的审核日志卷，前提是您将审核级别设置为默认值（除存储外的所有类别均设置为正常）。 设置为 Error ）：

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

例如，如果您的网格大小为每秒 1 ， 000 次 S3 操作，则工作负载将占 50% ， S3 帐户名称，存储分段名称，对象名称平均为 90 字节，您的外部系统日志服务器应调整大小以支持每秒 1 ， 500 条系统日志消息，并且应能够以大约每秒 1 MB 的速率接收（并且通常存储）审核日志数据。

非默认审核级别的估计公式

为审核日志提供的公式假定使用默认审核级别设置（所有类别均设置为 " 正常 " ，但存储设置为 " 错误 " 除外）。未提供用于估计非默认审核级别设置的审核消息速率和平均大小的详细公式。不过，下表可用于粗略估计费率； 您可以使用为审核日志提供的平均大小公式、但请注意、它可能会导致高估、因为"额外"审核消息平均小于默认审核消息。

条件	公式
Replication： Audit Levels all set to Debug or Normal	审核日志速率= 8 x S3操作速率
纠删编码：审核级别均设置为 " 调试 " 或 " 正常 "	使用与默认设置相同的公式

安全事件的估计公式

安全事件与S3操作无关、通常会生成极少的日志和数据。出于这些原因，不提供任何估计公式。

应用程序日志的估计公式

如果除了网格预期支持的每秒 S3 操作数之外，您没有其他有关 S3 工作负载的信息，则可以使用以下公式估算

外部系统日志服务器需要处理的应用程序日志卷：

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

因此，例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，则外部系统日志服务器的大小应为每秒支持 3 ， 300 个应用程序日志，并且能够以大约每秒 1.2 MB 的速率接收（和存储）应用程序日志数据。

如果您对工作负载有更多了解，可以进行更准确的估计。对于应用程序日志、最重要的其他变量是数据保护策略(复制与纠删编码)、S3操作的放置百分比(与Gets/Other)以及以下S3字段的平均大小(以字节为单位)(表中使用的4个字符缩写为审核日志字段名称)：

代码	字段	说明
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
S3BK	S3存储分段	S3 存储分段名称。
S3KY	S3密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。

规模估算示例

本节介绍了如何使用网格估算公式和以下数据保护方法的示例案例：

- 复制
- 纠删编码

如果使用复制来保护数据

Let P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

让K表示S3帐户名称、S3存储分段和S3密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。K 的值为 90 （ 13+13+28+36 ）。

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

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

因此，例如，如果网格的大小为每秒 1 ， 000 次 S3 操作，工作负载占用率为 50% ， S3 帐户名称，存储分段名称和对象名称平均为 90 字节，则外部系统日志服务器的大小应为每秒支持 1800 个应用程序日志。 并且将以每秒 0.5 MB 的速率接收（并通常存储）应用程序数据。

如果您使用纠删编码进行数据保护

Let P 表示所放置的 S3 操作的百分比，其中 0 ≤ P ≤ 1 （因此，对于 100% PUT 工作负载， P = 1 ，对于 100% GET 工作负载， P = 0 ）。

让K表示S3帐户名称、S3存储分段和S3密钥之和的平均大小。假设 S3 帐户名始终为 my-s3-account （ 13 字节），存储分段的名称长度固定，例如 /my/application/bucket-12345 （ 28 字节），而对象的密钥长度固定，例如 5733a5d7-f069-41ef-8fbd-13247494c69c （ 36 字节）。K 的值为 90 （ 13+13+28+36 ）。

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

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

例如、如果您的网格的规模为每秒1、000次S3操作、则您的工作负载为50%的"放置"、而您的S3帐户名称、存储分段名称、 对象名称平均为90字节、您的外部系统日志服务器应调整为每秒支持2、250个应用程序日志、并且应能够以每秒0.6 MB的速率接收(并通常存储)应用程序数据。

在 **StorageGRID** 中配置日志管理

根据需要，配置审核级别、协议标头、审核消息和日志的位置以及日志保留。

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

您也可以"配置外部系统日志服务器"选择远程保存审核信息。通过使用外部服务器，您可以最大限度地减少审核消息日志记录对性能的影响，同时不会降低审核数据的完整性。如果您拥有大型网格、使用多种类型的 S3 应用程序或希望保留所有审核数据，则外部 syslog 服务器特别有用。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 如果您计划配置外部系统日志服务器，则您已阅读并遵循"使用外部系统日志服务器的注意事项"。
- 如果您计划使用TLS或RELP/TLS协议配置外部系统日志服务器、则您具有所需的服务器CA和客户端证书以及客户端专用密钥。

更改审核消息级别

您可以为审核日志中的以下每种消息设置不同的审核级别：

审核类别	默认设置	更多信息
系统	正常	"系统审核消息"

审核类别	默认设置	更多信息
存储	错误	"对象存储审核消息"
管理	正常	"管理审核消息"
客户端读取	正常	"客户端读取审核消息"
客户端写入	正常	"客户端写入审核消息"
ILM	正常	"ILM审核消息"
跨网格复制	错误	"CGRR：跨网格复制请求"

升级期间，审计级别配置不会立即生效。

步骤

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

审核级别	说明
关闭	不会记录此类别中的任何审核消息。
错误	仅记录错误消息——结果代码不“成功”（SUCS）的审计消息。
正常	系统会记录标准事务处理消息，即这些说明中针对此类别列出的消息。
调试	已弃用。此级别的行为与正常审核级别相同。

对于任何特定级别，包含的消息都包括那些将在较高级别记录的消息。例如，正常级别包括所有错误消息。

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

3. 选择 * 保存 * 。

定义HTTP请求标头

您可以选择定义要包含在客户端读写审计消息中的任何 HTTP 请求标头。

步骤

1. 在*Audit protocol headers*部分中，定义要包含在客户端读写审核消息中的HTTP请求标头。

   使用星号（*）作为通配符，以匹配零个或多个字符。使用转义序列（*）匹配文字星号。

2. 如果需要，选择 * 添加另一个标题 * 以创建其他标题。

   当 StorageGRID 在请求中找到 HTTP 标头时，它会将其包含在 HTRH 字段下的审核消息中。

   仅当“客户端读取”或“客户端写入”的审计级别不是“关闭*”时，才会记录审计协议请求标头。

3. 选择 * 保存 *

配置日志位置

默认情况下，审核消息和日志保存在生成它们的节点上。StorageGRID 定期轮换并最终删除审核消息和日志，以防止它们占用过多的磁盘空间。要在外部保存审核消息和一部分日志， 使用外部系统日志服务器。

如果要在内部保存日志文件，请选择用于日志存储的租户和存储桶并启用日志存档。

使用外部系统日志服务器

您可以选择配置外部系统日志服务器、将审核日志、应用程序日志和安全事件日志保存到网格外部的某个位置。

如果您不想使用外部系统日志服务器，请跳过此步骤并转到选择日志位置。

如果此过程中提供的配置选项不够灵活，无法满足您的要求，则可以使用端点应用其他配置选项 `audit-destinations`，这些端点位于的私有API部分"网格管理 API"。例如、如果要对不同的节点组使用不同的系统日志服务器、则可以使用API。

输入系统日志信息

访问配置外部系统日志服务器向导、并提供StorageGRID访问外部系统日志服务器所需的信息。

步骤

1. 从本地节点和外部服务器选项卡中，选择*配置外部系统日志服务器*。或者，如果您之前配置了外部系统日志服务器，请选择*编辑外部系统日志服务器*。

   此时将显示配置外部系统日志服务器向导。

2. 对于向导的*Enter syslog info*步骤，在*Host*字段中输入外部系统日志服务器的有效完全限定域名或IPv4或IPv6地址。
3. 输入外部系统日志服务器上的目标端口（必须是介于 1 到 65535 之间的整数）。默认端口为514。
4. 选择用于向外部系统日志服务器发送审核信息的协议。

   建议使用*TLS*或*RELP/TLS*。您必须上传服务器证书才能使用其中任一选项。使用证书有助于确保网格与外部系统日志服务器之间的连接安全。有关详细信息，请参见 "管理安全证书"。

   所有协议选项都需要外部系统日志服务器的支持和配置。您必须选择与外部系统日志服务器兼容的选项。

   可靠事件日志记录协议（ Relp ）扩展了系统日志协议的功能，可提供可靠的事件消息传送。如果外部系统日志服务器必须重新启动，则使用 RELP 有助于防止审核信息丢失。

5. 选择 * 继续 * 。

6. [[attache-certificate]如果选择了*tls*或*RELP/tls*，请上传服务器CA证书、客户端证书和客户端专用密钥。
   a. 为要使用的证书或密钥选择 * 浏览 * 。
   b. 选择证书或密钥文件。
   c. 选择 * 打开 * 上传文件。

      证书或密钥文件名称旁边会显示一个绿色复选框，通知您已成功上传此证书或密钥文件。
7. 选择 * 继续 * 。

管理系统日志内容

您可以选择要发送到外部系统日志服务器的信息。

步骤

1. 对于向导的*管理系统日志内容*步骤，选择要发送到外部系统日志服务器的每种审核信息类型。
   - 发送审核日志：发送StorageGRID 事件和系统活动
   - 发送安全事件：发送安全事件，例如未授权用户尝试登录或用户以root身份登录时
   - 发送应用程序日志：发送"StorageGRID软件日志文件"对故障排除很有用的信息，包括：
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`(仅限管理节点)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - 发送访问日志：将外部请求的HTTP访问日志发送到网格管理器、租户管理器、已配置的负载平衡器端点以及来自远程系统的网格联合请求。
2. 使用下拉菜单为您要发送的每类审核信息选择严重性和设施(消息类型)。

   设置严重性和设施值可帮助您以可自定义的方式聚合日志、以便于分析。

   a. 对于*严重性*，请选择*直通*，或选择介于0到7之间的严重性值。

      如果选择一个值，StorageGRID 会将所选值应用于此类型的所有消息。如果使用固定值覆盖严重性，则会丢失有关不同严重性的详细信息。

严重性	说明
直通	发送到外部系统日志的每条消息的严重性值与在本地记录到节点时的严重性值相同： • 对于审核日志、严重性为"info"。 • 对于安全事件、严重性值由节点上的Linux分发版生成。 • 对于应用程序日志、"info"和"noty"之间的严重级别因问题描述的定义而异。例如、添加NTP服务器并配置HA组时、值为"info"、而故意停止SSM或RSM服务时、值为"note"。 • 对于访问日志、严重性为"info"。
0	紧急：系统不可用
1	alert ： 必须立即执行操作
2	严重：严重情况
3	错误：错误情况
4	警告：警告条件
5	注意：正常但重要的情况
6	Informational ： 信息性消息
7	debug ： 调试级别的消息

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

如果您选择一个值，它将应用于此类型的所有消息。如果您使用固定值覆盖医院、则有关不同医院的信息将丢失。

设施	说明
直通	发送到外部系统日志的每条消息都具有与在本地记录到节点上时相同的工具值： • 对于审核日志、发送到外部系统日志服务器的工具为"local7"。 • 对于安全事件、工具值由节点上的Linux分发版生成。 • 对于应用程序日志、发送到外部系统日志服务器的应用程序日志具有以下工具值： ◦ `bycast.log`：用户或守护进程 ◦ `bycast-err.log`：用户、守护进程、local3或local4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3. ◦ `prometheus.log`：本地4 ◦ `raft.log`：local5. ◦ `hagroups.log`：local6 • 对于访问日志、发送到外部系统日志服务器的工具为"local0"。
0	KERN （内核消息）
1	用户（用户级消息）
2	邮件
3	守护进程（系统守护进程）
4	auth （安全 / 授权消息）
5	系统日志（由 syslogd 在内部生成的消息）
6	LPR （行式打印机子系统）
7	新闻（网络新闻子系统）
8	uucp
9	cron （时钟守护进程）
10	安全性（安全性 / 授权消息）
11	FTP

设施	说明
12	NTP
13	日志审核（日志审核）
14	日志警报（日志警报）
15	时钟（时钟守护进程）
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. 选择 * 继续 * 。

发送测试消息

在使用外部 syslog 服务器之前，请要求网格中的所有节点向外部 syslog 服务器发送测试消息。这些测试消息可帮助您在将数据发送到外部 syslog 服务器之前验证整个日志收集基础架构。

在确认外部系统日志服务器收到来自网格中每个节点的测试消息且该消息已按预期处理之前、请勿使用外部系统日志服务器配置。

步骤

1. 如果由于您确定外部系统日志服务器配置正确并且可以从网格中的所有节点接收审核信息而不想发送测试消息，请选择*跳过并完成*。

   绿色横幅表示配置已保存。

2. 否则，请选择*发送测试消息*(建议)。

   测试结果会持续显示在页面上，直到您停止测试为止。测试期间，审核消息会继续发送到先前配置的目标。

3. 如果您在 syslog 服务器配置期间或运行时收到任何错误，请更正它们并再次选择*发送测试消息*。

请参见"对外部系统日志服务器进行故障排除"以帮助您解决任何错误。

4. 请等待，直到看到一个绿色横幅，指示所有节点均已通过测试。
5. 检查系统日志服务器以确定是否按预期接收和处理了测试消息。

> 如果您使用 UDP，请检查整个日志收集基础设施。 UDP 协议不像其他协议那样允许严格的错误检测。

6. 选择 * 停止并完成 * 。

此时将返回到 * 审核和系统日志服务器 * 页面。绿色横幅表示系统日志服务器配置已保存。

> 直到您选择包含外部系统日志服务器的目标时， StorageGRID审计信息才会发送到外部系统日志服务器。

选择日志位置

您可以指定审计日志、安全事件日志、"StorageGRID应用程序日志" ，并发送访问日志。

> StorageGRID默认使用本地节点审核目标，并将审核信息存储在中 `/var/local/log/localaudit.log`。
>
> 使用时 `/var/local/log/localaudit.log`，Grid Manager和租户管理器审核日志条目可能会发送到存储节点。您可以使用命令查找哪个节点具有最新的条目 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`。
>
> 只有在配置了外部系统日志服务器后、某些目标才可用。

步骤

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

> *仅限本地节点*和*外部系统日志服务器*通常可提供更好的性能。

选项	说明
仅本地节点(默认)	审计消息、安全事件日志和应用程序日志不会发送到管理节点。相反，它们仅保存在生成它们的节点（“本地节点”）上。每个本地节点生成的审计信息存储在 `/var/local/log/localaudit.log`。 注意： StorageGRID会定期删除本地日志以释放空间。当节点的日志文件达到 1 GB 时，将保存现有文件并启动新的日志文件。日志的轮换限制为 21 个文件。当创建第 22 个版本的日志文件时，最旧的日志文件将被删除。每个节点平均存储约 20 GB 的日志数据。为了长期保存日志，使用租户和存储桶进行日志存储 。

选项	说明
管理节点/本地节点	审核消息会发送到管理节点上的审核日志、安全事件日志和应用程序日志会存储在生成这些消息的节点上。审核信息存储在以下文件中： • 管理节点（主要和非主要）：`/var/local/audit/export/audit.log` • 所有节点：`/var/local/log/localaudit.log`文件通常为空或缺失。它可能包含辅助信息、例如某些消息的附加副本。
外部系统日志服务器	审计信息被发送到外部系统日志服务器并保存在本地节点上（`/var/local/log/localaudit.log`）。发送的信息类型取决于您如何配置外部系统日志服务器。此选项仅在您配置外部系统日志服务器。
管理节点和外部系统日志服务器	审计消息被发送到审计日志（`/var/local/audit/export/audit.log`），并将审计信息发送到外部系统日志服务器并保存在本地节点上（`/var/local/log/localaudit.log`）。发送的信息类型取决于您如何配置外部系统日志服务器。此选项仅在您配置外部系统日志服务器。

3. 选择 * 保存 * 。

   此时将显示一条警告消息。

4. 选择*OK*确认要更改审核信息的目标。

   新日志将发送到选定的目标。现有日志将保留在其当前位置。

使用存储桶

日志会定期轮换。使用同一网格中的 S3 存储桶来长期存储日志。

1. 选择*日志位置* > 使用存储桶。
2. 选中“启用存档日志”复选框。
3. 如果列出的租户和存储桶不是您想要使用的，请选择*更改租户和存储桶*，然后选择*创建租户和存储桶*或*选择租户和存储桶*。

创建租户和存储桶

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

选择租户和存储分段

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

4. 选择 * 保存 * 。

日志将存储在您指定的租户和存储桶中。日志的对象键名称采用以下格式：

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

例如：

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

管理日志保留

您可以通过创建 ILM 规则或配置 S3 存储桶生命周期策略来管理 StorageGRID 保留日志的时长。

ILM规则

为存储桶创建 ILM 规则，并将此规则添加到活动 ILM 策略。

步骤

1. 选择 * ILM * > * 规则 * 。
2. 选择 **Create**。"第1步(输入详细信息)" 此时将显示 Create an ILM rule wizard（创建 ILM 规则向导）：
   a. 请输入规则的唯一名称。例如：归档日志的 ILM 规则。
   b. 选择日志存档 S3 租户帐户。
   c. 指定日志存档 S3 存储桶。
3. 继续"第2步(定义放置位置)"并定义存档日志规则的放置位置。例如，ILM 规则在第一年内在站点 1 中存储一个复制副本，在站点 2 中存储一个复制副本。一年后，仅在一个站点上创建并保存 2+1 纠删码副本。
4. 创建规则后，将其添加到活动的 ILM 策略。

S3 bucket 生命周期

在日志存档 S3 存储桶上配置 S3 存储桶生命周期策略：

```
{
      "Rules": [
        {
           "ID": "Retain logs forever",
           "Filter": {},
           "Status": "Enabled",
           "Expiration": {}
        }
      ]
}
```

在日志存档 S3 存储桶上配置 S3 存储桶生命周期策略时，生命周期到期操作将覆盖与存储桶生命周期筛选器匹配的对象的 ILM 策略。与存储桶生命周期筛选器不匹配的对象使用 ILM 策略的保留设置。如果对象与存储桶生命周期筛选器匹配，且未明确指定过期操作，则不会使用 ILM 策略的保留设置，这意味着对象版本将被永久保留。

配置电子邮件服务器

作为 StorageGRID 管理员，您需要配置电子邮件服务器，以便从 StorageGRID 警报和监控系统发送通知，通知您、其他管理员和技术支持有关系统事件和问题的信息。

使用电子邮件服务器进行通知的 StorageGRID 功能包括警报、AutoSupport 和多管理员验证 (MAV)。您可以对所有通知使用相同的电子邮件服务器。

开始之前

- 您拥有"root访问权限"。

- 您已使用登录到网格管理器"支持的 Web 浏览器"。

步骤

1. 选择*配置* > 监控 > 电子邮件服务器。

   此时将显示电子邮件服务器页面。

2. 选择下拉菜单，查看可能需要电子邮件服务器的功能。如果要查看配置功能的电子邮件通知的详细信息和所需信息，请选择 查看。

   您将转到网格管理器中功能的配置页面。每个功能的配置页面都包含需要电子邮件服务器才能发送电子邮件通知的通知。

3. 要从电子邮件服务器页面配置电子邮件服务器，请执行以下操作：

   a. 输入电子邮件服务器的 IP 地址或 FQDN。

   b. 选择电子邮件服务器使用的端口号。默认值为 25。

   c. 要启用身份验证，请选择*Use authentication*并输入用户名和密码。

   d. 要求验证 SMTP 服务器的身份，请选择 **Use Transport Layer Security (TLS)**。然后：

      i. 提供 CA 捆绑包。

      ii. 如果 SMTP 电子邮件服务器要求电子邮件发件人提供客户端证书进行身份验证，请选择 **Send client certificate**。然后提供客户端证书和私钥。

   e. 为确保您的电子邮件设置正确，请通过输入发件人和收件人来发送测试电子邮件。选择 **Send**。

      此时将显示一条确认消息，指示已发送测试电子邮件。

   f. 检查所有电子邮件收件人的收件箱，确认已收到测试电子邮件。

      如果在几分钟内未收到电子邮件，或者触发了 * 电子邮件通知失败 * 警报，请检查您的设置并重试。

   g. 登录到任何其他管理节点并发送测试电子邮件以验证所有站点的连接。

      在测试警报通知时，您必须登录到每个管理节点以验证连接。这与测试AutoSupport软件包不同、在测试软件包中、所有管理节点都会发送测试电子邮件。

4. 选择 * 保存 * 。

   发送测试电子邮件不会保存您的设置。必须选择 **Save**。

   此时将保存电子邮件设置。

5. 转到使用电子邮件服务器的功能的配置页面并完成电子邮件通知设置。

   - "警报"。对于警报，您也可以 "设置 SNMP 通知"。
   - "AutoSupport"。您可以通过电子邮件、HTTPS 或 HTTP（不建议使用 HTTP）发送 AutoSupport 包。
   - "多管理员验证（MAV）"。

使用 SNMP 监控

在 StorageGRID 中使用 SNMP 监控

如果要使用简单网络管理协议（ Simple Network Management Protocol ， SNMP ）监控 StorageGRID ，则必须配置 StorageGRID 附带的 SNMP 代理。

- "配置 SNMP 代理"
- "更新 SNMP 代理"

功能

每个StorageGRID 节点都运行一个SNMP代理或守护进程、用于提供MIB。StorageGRID MIB包含警报的表和通知定义。MIB 还包含系统问题描述 信息，例如每个节点的平台和型号。每个 StorageGRID 节点还支持一组 MIB-II 对象。

> 查看"访问MIB文件"是否要在网格节点上下载MIB文件。

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

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

陷阱
: 陷阱是由SNMP代理发送的通知、不需要管理系统进行确认。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
: 通知与陷阱类似，但需要管理系统确认。如果SNMP代理未在一定时间内收到确认、则会重新发送通知、直到收到确认或已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、您必须禁止"配置静音"警报。警报通知由发送"首选发件人管理节点"。

  每个警报都会根据警报的严重性级别映射到以下三种陷阱类型之一： activeMinorAlert ， activeMajorAlert 和 activeCriticalAlert 。有关可触发这些陷阱的警报列表，请参见"警报参考"。

SNMP 版本支持

下表简要总结了每个 SNMP 版本支持的功能。

	SNMPv1	SNMPv2c	SNMPv3
查询 (GET 和GETNEXT)	只读 MIB 查询	只读 MIB 查询	只读 MIB 查询
查询身份验证	社区字符串	社区字符串	基于用户的安全模型（ USM ）用户
通知 (陷阱和通知)	仅陷阱	陷阱和通知	陷阱和通知
通知身份验证	每个陷阱目标的默认陷阱社区或自定义社区字符串	每个陷阱目标的默认陷阱社区或自定义社区字符串	每个陷阱目标的 USM 用户

限制

- StorageGRID 支持只读 MIB 访问。不支持读写访问。
- 网格中的所有节点都接收相同的配置。
- SNMPv3： StorageGRID 不支持传输支持模式（ TSM ）。
- SNMPv3： 支持的唯一身份验证协议是 SHA （ HMAC-SHA-96 ）。
- SNMPv3： 支持的唯一隐私协议是 AES 。

在 **StorageGRID** 中配置 **SNMP** 代理

您可以将StorageGRID SNMP代理配置为使用第三方SNMP管理系统进行只读MIB访问和通知。

开始之前

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

关于此任务

StorageGRID SNMP代理支持SNMPv1、SNMPv2c和SNMPv3。您可以为代理配置一个或多个版本。对于SNMPv3、仅支持用户安全模型(User Security Model、USM)身份验证。

网格中的所有节点都使用相同的SNMP配置。

指定基本配置

首先、启用StorageGRID SMNP代理并提供基本信息。

步骤

1. 选择*配置* > 监控 > **SNMP** 代理。

此时将显示SNMP代理页面。

2. 要在所有网格节点上启用SNMP代理，请选中*Enable SNMP*复选框。
3. 在Basic configuration部分中输入以下信息。

字段	说明
系统联系人	可选。StorageGRID系统的主要联系人、在SNMP消息中以sysContact的形式返回。 系统联系人通常是一个电子邮件地址。此值用于适用场景StorageGRID系统中的所有节点。*系统联系人*最多可以包含255个字符。
系统位置	可选。StorageGRID系统的位置、在SNMP消息中以sysLocation的形式返回。 系统位置可以是任何有助于确定StorageGRID系统所在位置的信息。例如，您可以使用设施的街道地址。此值用于适用场景StorageGRID系统中的所有节点。*系统位置*最多可以是255个字符。
启用SNMP代理通知	• 如果选中此选项、StorageGRID SNMP代理将发送陷阱和通知通知。 • 如果未选中、则SNMP代理支持只读MIB访问、但不会发送任何SNMP通知。
启用身份验证陷阱	如果选中此选项、则StorageGRID SNMP代理会在收到未经正确身份验证的协议消息时发送身份验证陷阱。

输入社区字符串

如果使用SNMPv1或SNMPv2c、请完成社区字符串部分。

当管理系统查询 StorageGRID MIB 时，它会发送一个社区字符串。如果社区字符串与此处指定的值之一匹配，则 SNMP 代理会向管理系统发送响应。

步骤

1. 对于*只读社区*，可选择输入社区字符串，以允许对IPv4和IPv6代理地址进行只读MIB访问。

   为确保StorageGRID系统的安全性、请勿使用"public"作为社区字符串。如果将此字段留空、SNMP代理将使用StorageGRID系统的网格ID作为社区字符串。

   每个社区字符串最多可以包含32个字符、并且不能包含空格字符。

2. 选择*添加其他社区字符串*以添加其他字符串。

   最多允许五个字符串。

使用其他配置部分中的陷阱目标选项卡为StorageGRID陷阱或通知定义一个或多个目标。如果启用SNMP代理并选择*保存*，则在触发警报时，StorageGRID会向每个定义的目标发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

步骤

1. 对于*默认陷阱社区*字段、可选择输入要用于SNMPv1或SNMPv2陷阱目标的默认社区字符串。

   定义特定陷阱目标时、您可以根据需要提供不同的("自定义")社区字符串。

   *默认陷阱社区*最多可包含32个字符、不能包含空格字符。

2. 要添加陷阱目标，请选择*Cree*。
3. 选择要用于此陷阱目标的SNMP版本。
4. 完成所选版本的创建陷阱目标表单。

SNMPv1

如果选择SNMPv1作为版本、请填写这些字段。

字段	说明
键入	必须为SNMPv1陷阱。
主机	用于接收陷阱的IPv4或IPv6地址或完全限定域名(FQDN)。
端口	使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
社区字符串	使用默认陷阱团体(如果已指定)、或者为此陷阱目标输入自定义社区字符串。 自定义社区字符串最多可以包含32个字符、并且不能包含空格。

SNMPv2c

如果选择SNMPv2c作为版本、请填写这些字段。

字段	说明
键入	目标将用于陷阱还是通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。
端口	请使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
社区字符串	使用默认陷阱团体(如果已指定)、或者为此陷阱目标输入自定义社区字符串。 自定义社区字符串最多可以包含32个字符、并且不能包含空格。

SNMPv3

如果选择SNMPv3作为版本、请填写这些字段。

字段	说明
键入	目标将用于陷阱还是通知。
主机	用于接收陷阱的IPv4或IPv6地址或FQDN。

字段	说明
端口	请使用162、这是SNMP陷阱的标准端口、除非您必须使用其他值。
协议	使用UDP、这是标准SNMP陷阱协议、除非您需要使用TCP。
USM用户	要用于身份验证的USM用户。 • 如果选择了 * 陷阱 * ，则仅显示不具有权威引擎 ID 的 USM 用户。 • 如果选择 * 通知 * ，则仅显示具有权威引擎 ID 的 USM 用户。 • 如果未显示任何用户： i. 创建并保存陷阱目标。 ii. 转到创建USM用户并创建用户。 iii. 返回到陷阱目标选项卡，从表中选择保存的目标，然后选择*Edit*。 iv. 选择用户。

5. 选择 * 创建 * 。

   此时将创建陷阱目标并将其添加到表中。

创建代理地址

(可选)使用“其他配置”部分中的“业务代表地址”选项卡指定一个或多个“侦听地址”。这些地址是SNMP代理可以接收查询的StorageGRID地址。

如果不配置代理地址、则所有StorageGRID 网络上的默认侦听地址均为UDP端口161。

步骤

1. 选择 * 创建 * 。
2. 输入以下信息。

字段	说明
互联网协议	此地址将使用IPv4还是IPv6。 默认情况下， SNMP 使用 IPv4 。
传输协议	此地址将使用UDP还是TCP。 默认情况下， SNMP 使用 UDP 。

字段	说明
StorageGRID网络	代理将侦听哪个StorageGRID网络。 • 网格、管理和客户端网络：SNMP代理将侦听所有三个网络上的查询。 • 网格网络 • 管理网络 • 客户端网络 注意：如果使用客户端网络处理不安全的数据，并为客户端网络创建代理地址，请注意SNMP流量也不安全。
端口	(可选) SNMP代理应侦听的端口号。 SNMP 代理的默认 UDP 端口为 161 ，但您可以输入任何未使用的端口号。 注意：保存SNMP代理时，StorageGRID会自动打开内部防火墙上的代理地址端口。您必须确保任何外部防火墙允许访问这些端口。

3. 选择 * 创建 * 。

   此时将创建代理地址并将其添加到表中。

创建**USM**用户

如果使用SNMPv3、请使用其他配置部分中的USM用户选项卡定义有权查询MIB或接收陷阱和通知的USM用户。

> 对于 SNMPv3 *trap* 目的地，建议为每个管理节点创建一个 USM 用户。如果每个管理节点都没有 USM 用户，则当主管理节点发生故障时，您的管理系统可能会停止接收通知。

> SNMPv3 _INFORM _目标必须具有具有引擎ID的用户。SNMPv3 _陷阱_目标不能包含具有引擎ID的用户。

如果您仅使用SNMPv1或SNMPv2c、则这些步骤不适用。

步骤

1. 选择 * 创建 * 。
2. 输入以下信息。

字段	说明
用户名	此USM用户的唯一名称。 用户名最多可以包含32个字符、且不能包含空格字符。创建用户后、无法更改此用户名。
只读MIB访问	如果选中、则此用户应对MIB具有只读访问权限。
权威引擎ID	如果要在通知目标中使用此用户、则为该用户的权威引擎ID。 输入10到64个十六进制字符(5到32字节)、不含空格。要在陷阱目标中选择用于通知的USM用户需要此值。要在陷阱目标中为陷阱选择的USM用户不允许使用此值。 注意：如果您选择了*只读MIB访问*，则不会显示此字段，因为具有只读MIB访问权限的USM用户不能具有引擎ID。
安全级别	USM用户的安全级别： • * authPriv* ： 此用户与身份验证和隐私（加密）通信。您必须指定身份验证协议和密码以及隐私协议和密码。 • * authNoPriv* ： 此用户使用身份验证进行通信，并且没有隐私（无加密）。您必须指定身份验证协议和密码。
身份验证协议	始终设置为SHA、这是唯一支持的协议(HMAC-SHA-96)。
密码	此用户将用于身份验证的密码。
隐私协议	仅当您选择了*authPriv*并始终设置为AES时显示，AES是唯一支持的隐私协议。
密码	仅在选择了*authSv*时显示。此用户用于保护隐私的密码。

3. 选择 * 创建 * 。

   此时将创建 USM 用户并将其添加到表中。

4. 完成SNMP代理配置后，选择*Save*。

   新的 SNMP 代理配置将变为活动状态。

相关信息

"用于外部通信的端口"

更新 **StorageGRID SNMP** 代理

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

开始之前

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

关于此任务

有关SNMP代理页面上每个字段的详细信息、请参见"配置 SNMP 代理"。您必须选择页面底部的*保存*以提交您在每个选项卡上所做的任何更改。

步骤

1. 选择*配置* > 监控 > **SNMP** 代理。

   此时将显示SNMP代理页面。

2. 要在所有网格节点上禁用SNMP代理，请清除*Enable SNMP*复选框，然后选择*Save*。

   如果重新启用SNMP代理、则会保留先前的任何SNMP配置设置。

3. (可选)更新Basic configuration部分中的信息：

   a. 根据需要更新*系统联系人*和*系统位置*。

   b. (可选)选中或清除*启用SNMP代理通知*复选框以控制StorageGRID SNMP代理是否发送陷阱和通知通知。

      清除此复选框后、SNMP代理支持只读MIB访问、但不会发送SNMP通知。

   c. (可选)选中或清除*启用身份验证陷阱*复选框，以控制StorageGRID SNMP代理在收到未经正确身份验证的协议消息时是否发送身份验证陷阱。

4. 如果使用SNMPv1或SNMPv2c，则可以选择在“团体字符串”部分中更新或添加*只读社区*。

5. 要更新陷阱目标、请选择其他配置部分中的陷阱目标选项卡。

   使用此选项卡可以定义StorageGRID陷阱或通知通知的一个或多个目标。如果启用SNMP代理并选择*保存*，则在触发警报时，StorageGRID会向每个定义的目标发送通知。此外，还会为受支持的 MIB-II 实体（例如 ifdown 和 coldstart ）发送标准通知。

   有关输入内容的详细信息，请参见"创建陷阱目标"。

   - (可选)更新或删除默认陷阱社区。

     如果删除默认陷阱团体、则必须先确保任何现有陷阱目标使用自定义社区字符串。

   - 要添加陷阱目标，请选择*Cree*。
   - 要编辑陷阱目标，请选择单选按钮，然后选择*Edit*。
   - 要删除陷阱目标，请选择单选按钮，然后选择*Remove*。

- 要提交更改，请选择页面底部的*保存*。

6. 要更新业务代表地址，请选择其他配置部分中的业务代表地址选项卡。

   使用此选项卡指定一个或多个"侦听地址"。这些地址是SNMP代理可以接收查询的StorageGRID地址。

   有关输入内容的详细信息，请参见"创建代理地址"。

   - 要增加业务代表地址，请选择*Cree*。
   - 要编辑业务代表地址，请选择单选按钮，然后选择*Edit*。
   - 要删除业务代表地址，请选择单选按钮，然后选择*Remove*。
   - 要提交更改，请选择页面底部的*保存*。

7. 要更新USM用户、请选择其他配置部分中的USM用户选项卡。

   使用此选项卡可定义有权查询 MIB 或接收陷阱并通知的 USM 用户。

   有关输入内容的详细信息，请参见"创建USM用户"。

   - 要添加USM用户，请选择*Cree*。
   - 要编辑USM用户，请选择单选按钮，然后选择*Edit*。

     无法更改现有USM用户的用户名。如果需要更改用户名，必须删除此用户并创建新用户名。

     > 如果添加或删除用户的权威引擎ID、并且当前已为目标选择该用户、则必须编辑或删除目标。否则，在保存 SNMP 代理配置时会发生验证错误。

   - 要删除USM用户，请选择单选按钮，然后选择*Remove*。

     > 如果您删除的用户当前已被选定为陷阱目标、则必须编辑或删除该目标。否则，在保存 SNMP 代理配置时会发生验证错误。

   - 要提交更改，请选择页面底部的*保存*。

8. 更新SNMP代理配置后，选择*Save*。

访问 **StorageGRID MIB** 文件

MIB文件包含有关网格中节点的受管资源和服务属性的定义和信息。您可以访问用于定义StorageGRID 对象和通知的MIB文件。这些文件可用于监控网格。

有关SNMP和MIB文件的详细信息、请参见"使用 SNMP 监控"。

访问**MIB**文件

按照以下步骤访问MIB文件。

步骤

1. 选择*配置* > 监控 > **SNMP** 代理。

2. 在SNMP代理页面上、选择要下载的文件：
   - **NetApp-STORAGEGRID-MIB.TXT**：定义可在所有管理节点上访问的警报表和通知(陷阱)。
   - **ES-NetApp-06-MIB.MIB**：为基于E系列的设备定义对象和通知。
   - **mib_1_10.zip**：使用BMC接口为设备定义对象和通知。

   您还可以在任何StorageGRID节点上访问以下位置的MIB文件：`/usr/share/snmp/mibs`

3. 要从MIB文件中提取StorageGRID OID、请执行以下操作：
   a. 获取StorageGRID MIB根目录的OID：

      ```
      root@user-adm1:~ # snmptranslate -On -IR storagegrid
      ```

      结果： `.1.3.6.1.4.1.789.28669` (`28669`始终为StorageGRID的OID)

   b. 整个树中StorageGRID OID的gep (用于 `paste`连接行)：

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

      `snmptranslate`命令提供了许多可用于浏览MIB的选项。此命令可在任何StorageGRID 节点上使用。

MIB文件内容

所有对象都位于StorageGRID OID下。

对象名称	对象**ID (OID)**	说明
		NetApp StorageGRID实体的MIB模块。

MIB对象

对象名称	对象**ID (OID)**	键入	使用权	**MIB** 模块	说明
活动的计数	1.3.6.1.4.1。+ 789.28669.1.3	Integer32	只读	NETAPP-STORAGEGRID-MIB	activeAlert表中活动警报的数量。
活动的活动的表	1.3.6.1.4.1。+ 789.28669.1.4	ActiveAlertEntry 的序列	不可访问	NETAPP-STORAGEGRID-MIB	StorageGRID 中活动警报的表。
活动警报条目		顺序	不可访问	NETAPP-STORAGEGRID-MIB	单个StorageGRID警报，按警报 ID 索引。

对象名称	对象ID (OID)	键入	使用权	MIB 模块	说明
活动的标识号	1.3.6.1.4.1。+ 789.28669.1.4 .1.1	八位字节串	只读	NETAPP-STORAGEGRID-MIB	警报的ID。仅在当前一组活动警报中是唯一的。
活动报告名称	1.3.6.1.4.1。+ 789.28669.1.4 .1.2	八位字节串	只读	NETAPP-STORAGEGRID-MIB	警报的名称。
已执行的活动的活动的实例	1.3.6.1.4.1。+ 789.28669.1.4 .1.3	八位字节串	只读	NETAPP-STORAGEGRID-MIB	生成警报的实体的名称、通常为节点名称。
活动告警严重性	1.3.6.1.4.1。+ 789.28669.1.4 .1.4	八位字节串	只读	NETAPP-STORAGEGRID-MIB	警报的严重性。
活动的起始时间	1.3.6.1.4.1。+ 789.28669.1.4 .1.5	日期和时间	只读	NETAPP-STORAGEGRID-MIB	触发警报的时间。

收集其他 StorageGRID 数据

监控 StorageGRID 中的 PUT 和 GET 性能

您可以监控某些操作的性能，例如对象存储和检索，以帮助确定可能需要进一步调查的更改。

关于此任务

要监控Put和GET性能、您可以直接从工作站或使用开源S3TESTOR应用程序运行S3命令。使用这些方法可以独立于 StorageGRID 外部因素（例如客户端应用程序问题或外部网络问题）评估性能。

对 PUT 和 GET 操作执行测试时，请遵循以下准则：

- 使用与通常载入到网格中的对象相当的对象大小。
- 对本地站点和远程站点执行操作。

中的消息"审核日志"指示运行某些操作所需的总时间。例如，要确定 S3 GET 请求的总处理时间，您可以查看 SGET 审核消息中的时间属性值。您还可以在以下S3操作的审核消息中找到时间属性：删除、获取、机头、元数据已更新、发布、放置

在分析结果时，请查看满足请求所需的平均时间以及可以实现的总吞吐量。定期重复相同的测试并记录结果、以便确定可能需要调查的趋势。

- 您可以 "从 GitHub 下载 S3tester"。

StorageGRID 系统可以验证存储节点上对象数据的完整性，并检查是否存在损坏和缺失的对象。

开始之前

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

关于此任务

这两种方法"验证过程"协同工作、以确保数据完整性：

- * 后台验证 * 会自动运行，并持续检查对象数据的正确性。

  后台验证会自动持续检查所有存储节点，以确定复制的和经过纠删编码的对象数据是否存在损坏的副本。如果发现问题， StorageGRID 系统会自动尝试替换存储在系统其他位置的副本中损坏的对象数据。后台验证不会对云存储池中的对象运行。

  > 如果系统检测到无法自动更正的损坏对象，则会触发*检测到未识别的损坏对象*警报。

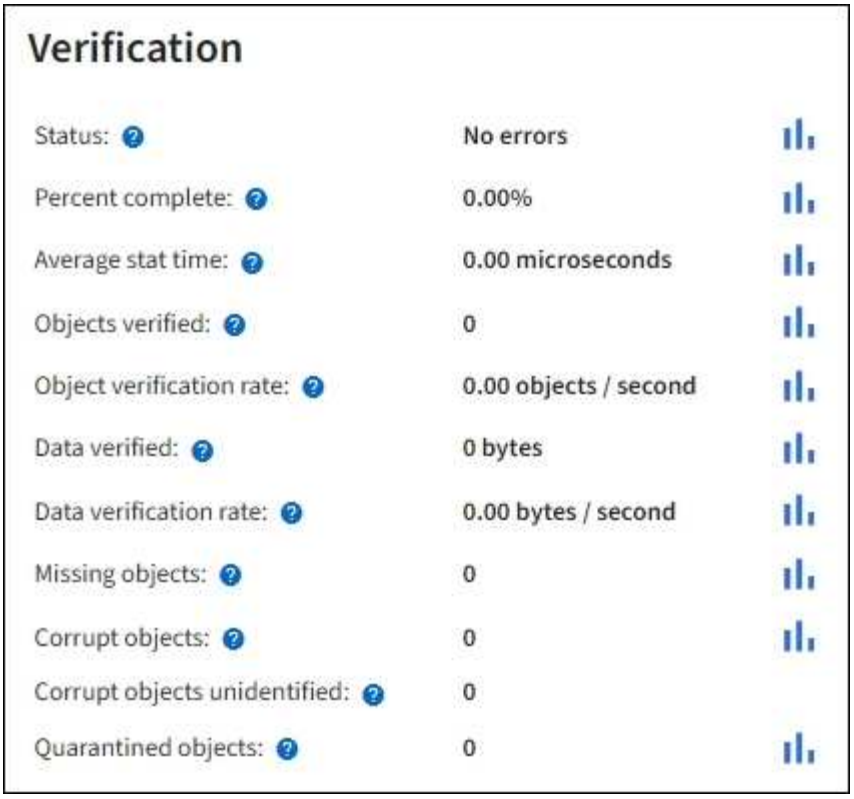
- 用户可以触发 * 对象存在检查 * ，以便更快速地验证对象数据是否存在（尽管不是正确）。

  对象存在检查可验证存储节点上是否存在所有预期复制的对象副本以及经过纠删编码的片段。对象存在检查提供了一种验证存储设备完整性的方法，尤其是在最新的硬件问题描述 可能会影响数据完整性的情况下。

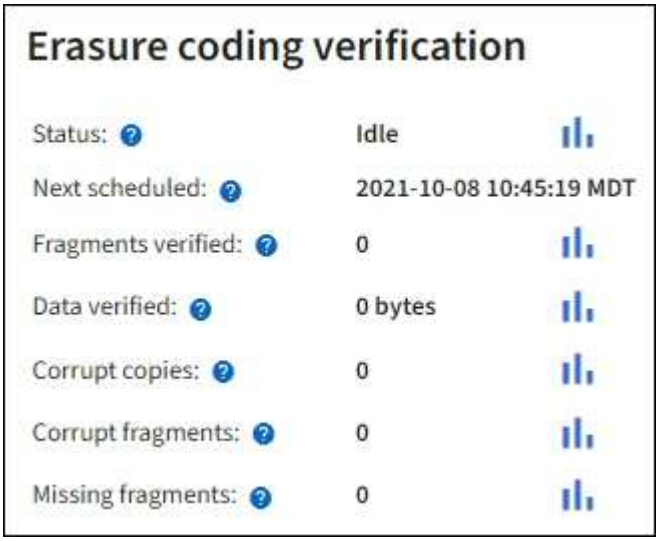
您应定期查看后台验证和对象存在检查的结果。立即调查任何对象数据损坏或丢失的实例，以确定根发生原因。

步骤

1. 查看后台验证的结果：
   a. 选择*节点* > 存储节点 > 对象。
   b. 检查验证结果：
      - 要检查复制的对象数据验证，请查看验证部分中的属性。

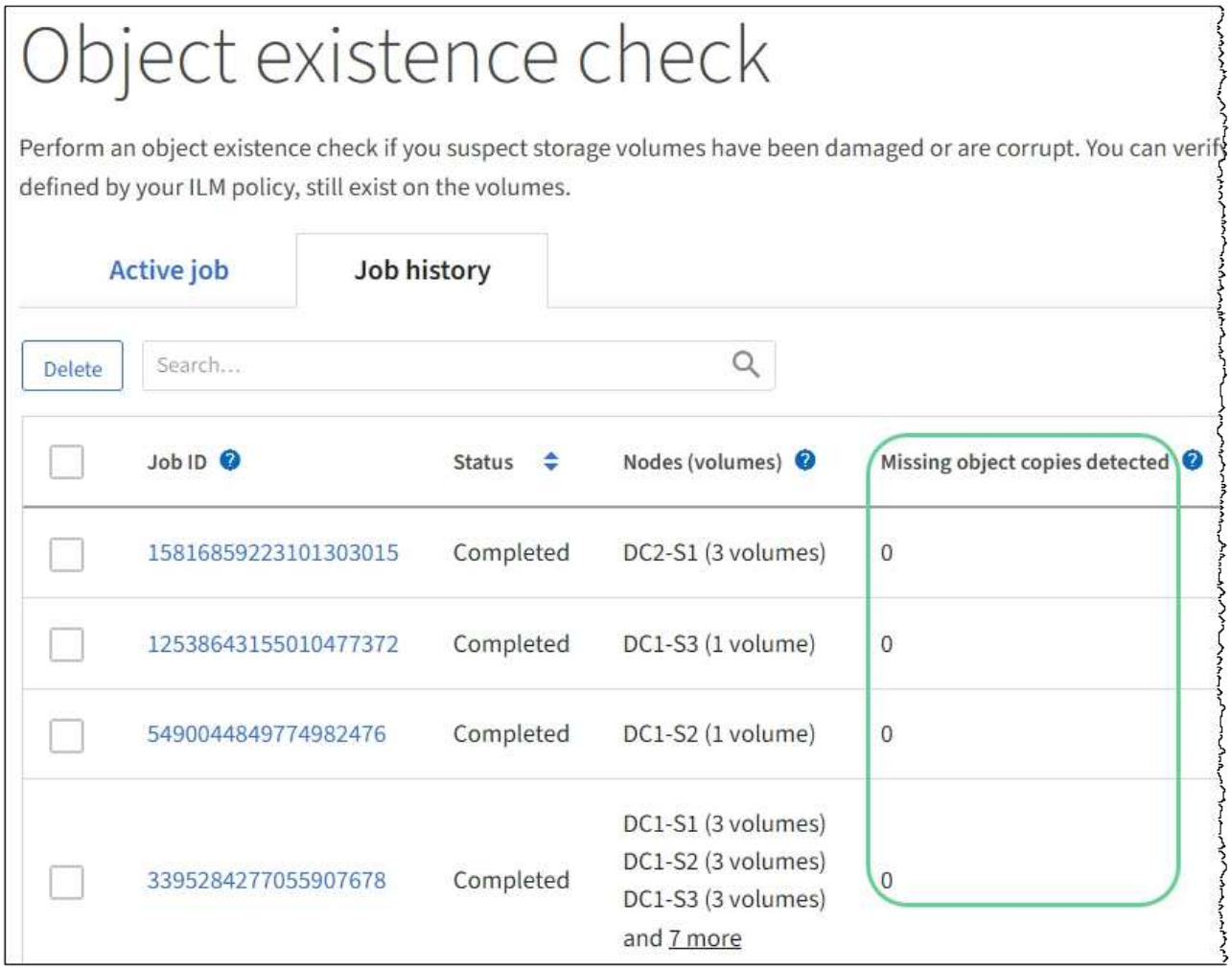


- 要检查擦除编码的片段验证，请选择 * 存储节点 _* > * ILM * ，然后查看擦除编码验证部分中的属性。



选择属性名称旁边的问号 ? 以显示帮助文本。

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



查看 **StorageGRID** 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客户端应用程序请求创建、修改或检索对象时、系统会记录客户端读写审核消息。
- 管理审核消息会将用户请求记录到管理 API 。

每个管理节点都会将审核消息存储在文本文件中。审核共享包含活动文件（ audit.log ）以及前几天压缩的审核日志。网格中的每个节点还会存储在该节点上生成的审核信息的副本。

您可以直接从管理节点的命令行访问审核日志文件。

默认情况下、StorageGRID可以发送审核信息、也可以更改目标：

- StorageGRID默认为本地节点审核目标。

- 可能会将网格管理器和租户管理器审核日志条目发送到存储节点。
- 您也可以更改审核日志的目标并将审核信息发送到外部系统日志服务器。配置外部系统日志服务器后，仍会生成并存储审核记录的本地日志。
- "了解有关配置日志管理的信息" 。

有关审核日志文件、审核消息格式、审核消息类型以及可用于分析审核消息的工具的详细信息，请参见"查看审核日志"。

收集 **StorageGRID** 日志文件和系统数据

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

开始之前

- 您已使用任意管理节点登录到网格管理器"支持的 Web 浏览器"。
- 您拥有 "特定访问权限"。

关于此任务

使用网格管理器来收集"日志文件"、系统数据和来自任何网格节点的您选择的时间段的配置数据。数据被收集并归档在 `.tar.gz`然后您可以将其下载到本地计算机或发送给技术支持。

或者，您可以更改审计日志的目标并将审计信息发送到外部系统日志服务器。当配置外部系统日志服务器时，将继续生成和存储审计记录的本地日志。看"配置日志管理和外部系统日志服务器" 。

如果用于启动日志收集的管理节点在日志收集期间脱机，StorageGRID 不会保留结果。您需要重新启动节点，并在重新启动完成后重新启动日志收集。

步骤

1. 选择*支持* > 工具 > 日志收集。显示节点表。
2. 选择要收集日志文件的网格节点。

   您可以按节点名称、站点和节点类型进行排序。站点和节点类型列包含按单个站点和节点类型选择的过滤器。

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

   如果您选择很长的时间段或从大型网格中的所有节点收集日志，则日志存档可能会变得太大而无法存储在节点上，或者太大而无法由管理节点收集进行下载。如果发生任何一种情况，请使用较小的数据集重新开始日志收集。

5. 选择要收集的日志类型。
   - 应用程序日志：技术支持最常用于故障排除的应用程序特定日志。收集的日志是可用应用程序日志的子集。
   - 审计日志：包含系统正常运行期间生成的审计消息的日志。
   - 网络跟踪：用于网络调试的日志。
   - **Prometheus** 数据库：来自所有节点上的服务的时间序列指标。

6. 或者，使用 **Notes** 文本框输入有关您正在收集的日志文件的注释。

   您可以使用这些注释提供有关提示您收集日志文件的问题的技术支持信息。您的注释将与有关日志文件收集的其他信息一起添加到名为的文件中 `info.txt`。该 `info.txt`文件将保存在日志文件归档包中。

7. 选择*收集日志*。

   您可以使用日志收集页面来监控每个网格节点的日志文件收集进度。

   如果您收到有关日志大小的错误消息，请尝试收集较短时间段或较少节点的日志。

8. 如果日志收集失败：

   - 如果出现“日志收集失败”消息，您可以重试日志收集或完成会话而无需重试。
   - 如果出现“日志收集部分失败”消息，您可以重试日志收集、完成会话、下载部分日志文件或将部分日志文件发送到AutoSupport。

   > 您可以选择将配置密码短语字段留空进行标准重试，也可以输入密码短语以使用 SSH 重试。

9. 当日志文件收集完成时：

   - 选择*下载*下载 `.tar.gz`文件。
   - 选择“发送至AutoSupport”以发送 `.tar.gz`文件发送给技术支持。

     这 `.tar.gz`文件包含所有成功收集日志的网格节点的所有日志文件。合并后的 `.tar.gz`文件包含每个网格节点的一个日志文件存档。

   AutoSupport软件包的主题是 `USER_TRIGGERED_SUPPORT_BUNDLE`。

10. 选择 * 完成 * 。

    > 这 `.tar.gz`当您选择*完成*时，文件将被删除。请确保您先下载或发送该文件。

查看 **StorageGRID** 支持指标

对问题描述 进行故障排除时，您可以与技术支持人员一起查看 StorageGRID 系统的详细指标和图表。

开始之前

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

关于此任务

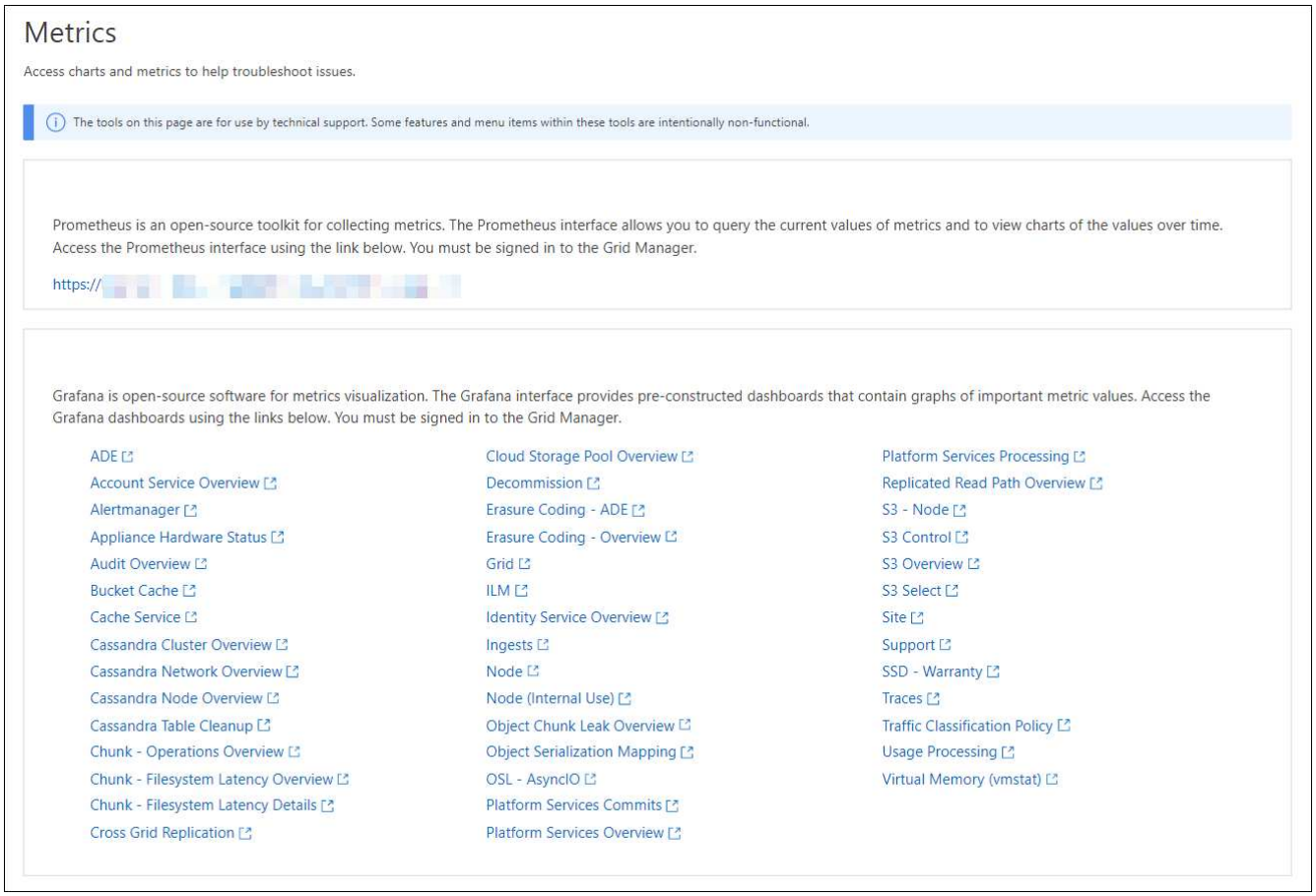
您可以通过指标页面访问 Prometheus 和 Grafana 用户界面。Prometheus 是用于收集指标的开源软件。Grafana 是用于可视化指标的开源软件。

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

步骤

1. 按照技术支持的指示，选择 支持 > 工具 > 指标。

   下面显示了 " 指标 " 页面的一个示例：



2. 要查询 StorageGRID 指标的当前值并查看随时间变化的值图形，请选择 Prometheus 部分中的链接。

   此时将显示 Prometheus 界面。您可以使用此界面对可用的 StorageGRID 指标执行查询，并绘制一段时间内的 StorageGRID 指标图。

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

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

   此时将显示选定链接的 Grafana 界面。



更改 **StorageGRID** 中的 **I/O** 优先级

输入/输出 (I/O) 优先级允许您更改网格上 I/O 操作的相对优先级。

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

开始之前

- 查看 I/O 优先级页面，确定哪些选项可能会影响您的网格。
- 评估正在进行的客户端流量是否可以安全地处理更长的等待时间或客户端超时。
- 准备好监控优先级变化的影响并根据需要进行调整。这些变化实施得很快，但其效果可能需要几个小时才能显现。

步骤

1. 选择*支持* > **I/O** 优先级。

2. （可选）将清除 EC 数据的后台操作的 EC 清除和修复优先级从其默认值更改。

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

3. 选择 * 保存 * 。
4. 监控"指标"评估优先级变化的影响。

在 **StorageGRID** 中运行诊断

在对问题描述 进行故障排除时，您可以与技术支持一起在 StorageGRID 系统上运行诊断并查看结果。

- "查看支持指标"
- "常用的 Prometheus 指标"

开始之前

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

关于此任务

" 诊断 " 页面会对网格的当前状态执行一组诊断检查。每个诊断检查可以具有以下三种状态之一：

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

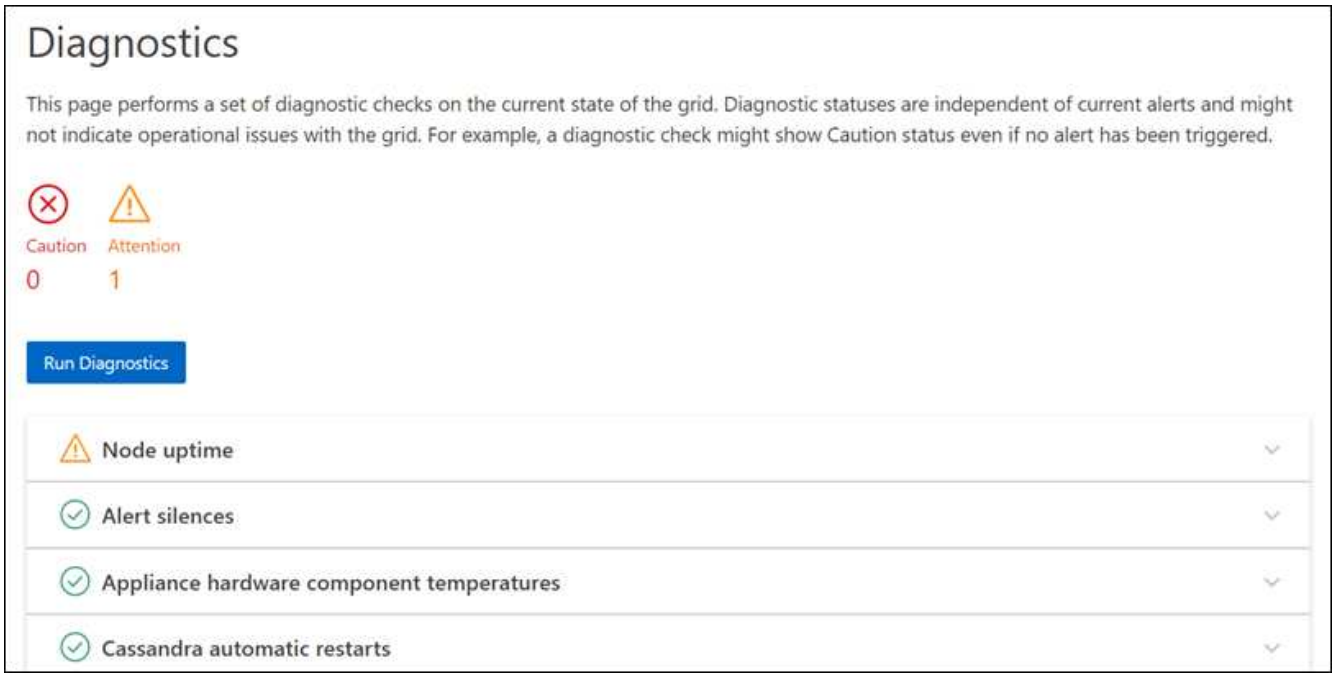
诊断状态与当前警报无关，可能并不表示网格存在操作问题。例如，即使未触发任何警报，诊断检查也可能会显示 " 小心 " 状态。

步骤

1. 选择*支持* > 工具 > 诊断。

   此时将显示 "Diagnostics " 页面，其中列出了每个诊断检查的结果。结果将按严重性（ " 小心 " ， " 注意 " 和 " 正常 " ）进行排序。在每个严重性范围内，结果按字母顺序排序。

   在此示例中，一个诊断具有“注意”状态，三个诊断具有“正常”状态。



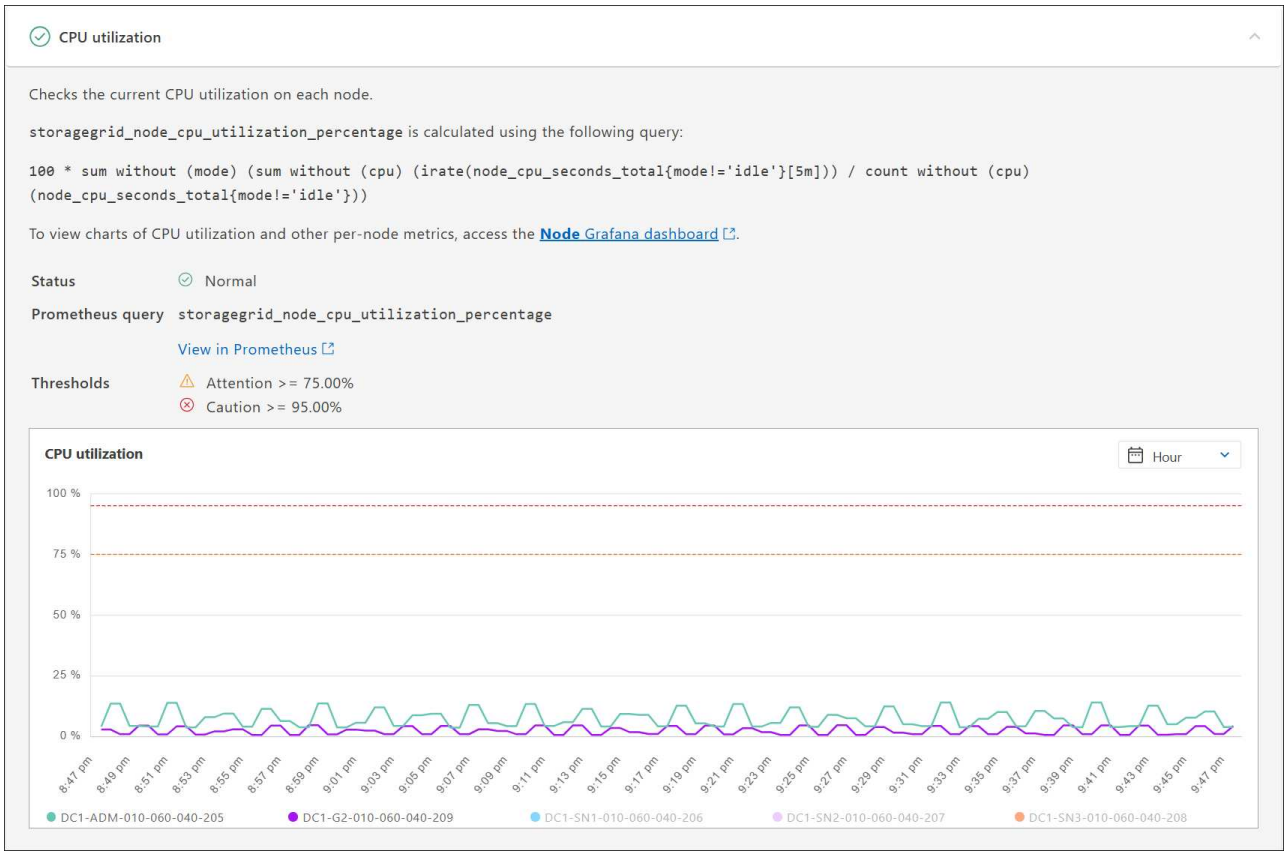
2. 要了解有关特定诊断的更多信息，请选择该行。

   此时将显示有关此诊断及其当前结果的详细信息。此时将列出以下详细信息：

   - * 状态 * ：此诊断的当前状态：正常，注意或小心。
   - * 项目查询 * ：如果用于诊断，则为用于生成状态值的 Prometheus 表达式。（并非所有诊断都使用 Prometheus 表达式。）
   - * 阈值 * ：如果可用于诊断，则为每个异常诊断状态提供系统定义的阈值。(阈值并不用于所有诊断。)

     您不能更改这些阈值。

   - 状态值：图形和表格（屏幕截图中未显示表格）显示整个StorageGRID系统的诊断状态和值。在此示例中，显示了StorageGRID系统中每个节点的当前 CPU 利用率。所有节点值均低于注意和警告阈值，因此诊断的总体状态为正常。



3. 可选：要查看与此诊断相关的 Grafana 图表，请选择 **Grafana** 仪表板。

   并非所有诊断都显示此链接。

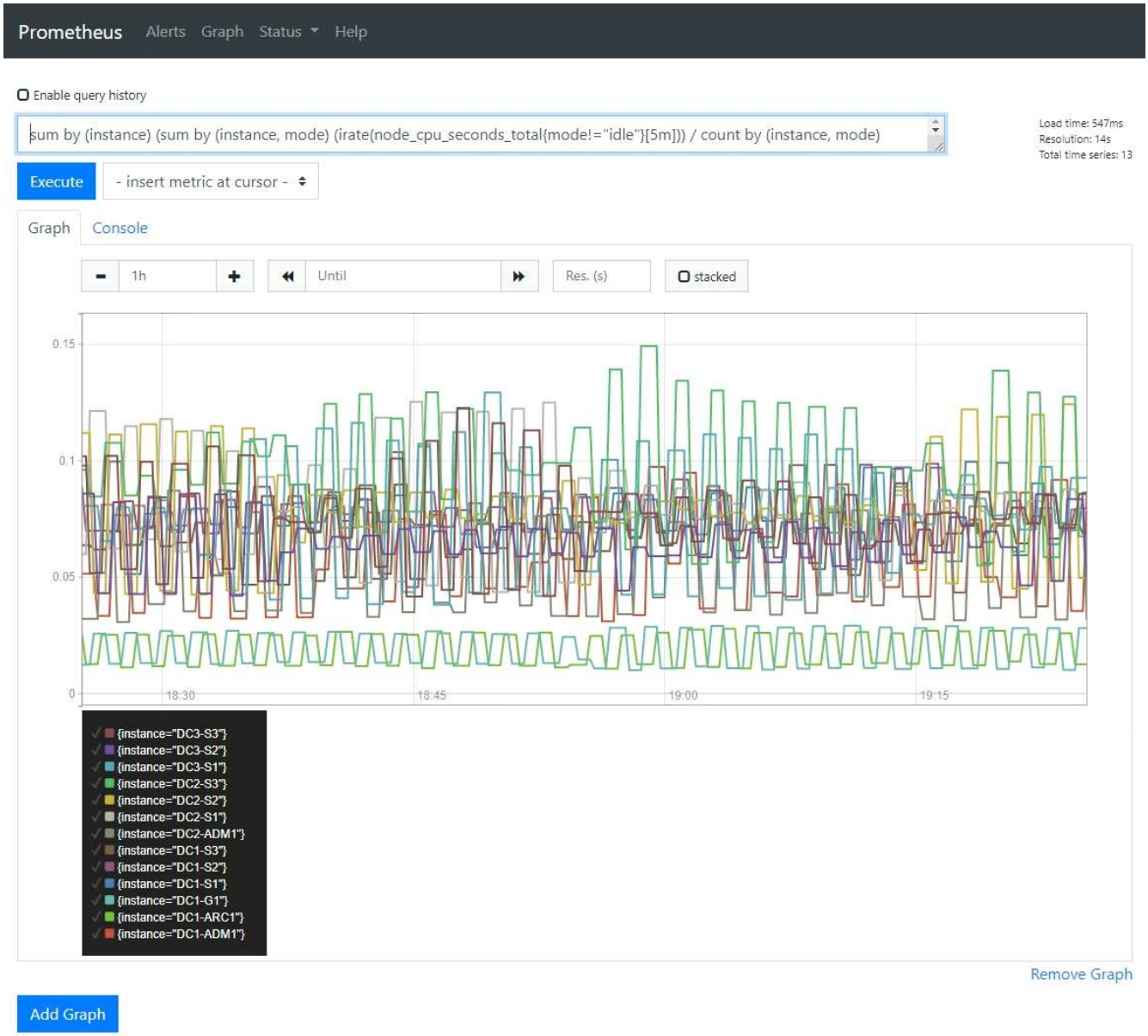
   出现相关的 Grafana 仪表板。在此示例中，节点仪表板显示该节点随时间变化的 CPU 利用率以及该节点的其他 Grafana 图表。

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



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

   此时将显示诊断中使用的表达式的 Prometheus 图形。



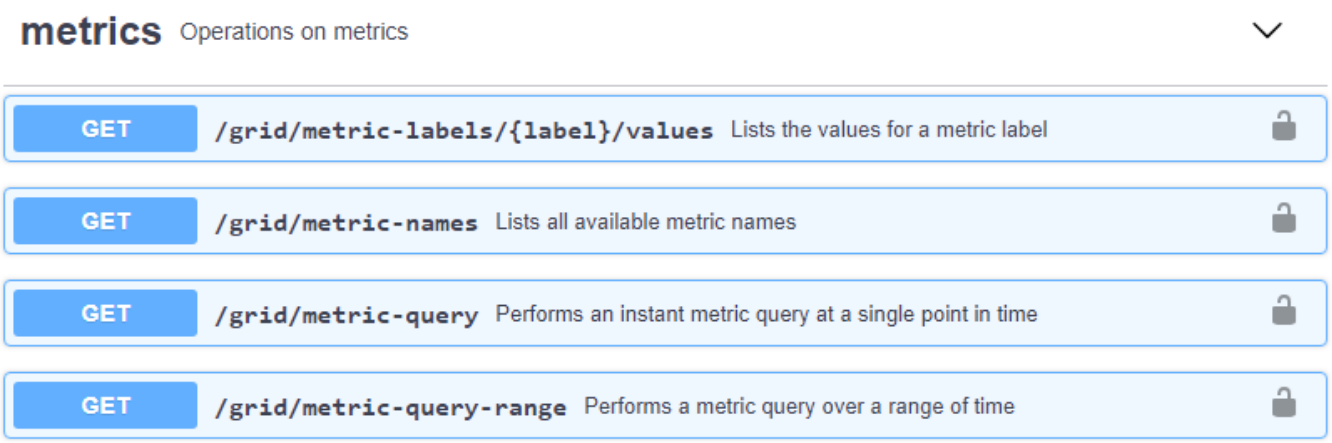
为 **StorageGRID** 创建自定义监控应用程序

您可以使用网格管理 API 提供的 StorageGRID 指标构建自定义监控应用程序和信息板。

如果要监控网格管理器现有页面上未显示的指标、或者要为StorageGRID 创建自定义信息板、则可以使用网格管理API查询StorageGRID 指标。

您还可以直接使用外部监控工具（例如 Grafana ）访问 Prometheus 指标。使用外部工具时，您需要上传或生成管理客户端证书，以使 StorageGRID 能够对该工具进行身份验证以确保安全性。请参见"有关管理 StorageGRID 的说明"。

要查看指标 API 操作，包括可用指标的完整列表，请转到 Grid Manager。在页面顶端，选择帮助图标，然后选择 **API documentation** > **metrics**。



本文档不会详细介绍如何实施自定义监控应用程序。

排除StorageGRID 系统故障

对 StorageGRID 系统进行故障排除

如果在使用 StorageGRID 系统时遇到问题，请参阅本节中的提示和准则，以帮助确定和解决问题描述 。

通常、您可以自行解决问题；但是、您可能需要将某些问题上报给技术支持。

定义问题

解决问题的第一步是明确定义问题。

下表提供了定义问题时可能收集的信息类型示例：

问题	响应示例
StorageGRID 系统正在执行什么操作或不执行什么操作？其症状是什么？	客户端应用程序报告无法将对象插入StorageGRID。
问题是从何时开始的？	2020年1月8日14：50左右、对象首次被拒绝。
您是如何首次注意到该问题的？	客户端应用程序已通知。同时还收到警报电子邮件通知。
问题是持续发生还是仅偶尔发生？	问题仍在继续。
如果此问题经常发生，则说明发生发生原因 的步骤是什么	每次客户端尝试载入对象时都会发生问题。
如果此问题间歇性发生，何时发生？记录您所知的每个意外事件的时间。	问题不是间歇性的。

问题	响应示例
您以前是否遇到过此问题？您过去遇到此问题的频率如何？	这是我第一次看到此问题描述 。

评估风险和对系统的影响

定义问题后，请评估其对 StorageGRID 系统的风险和影响。例如，存在严重警报并不一定意味着系统不提供核心服务。

下表总结了示例问题对系统操作的影响：

问题	响应示例
StorageGRID 系统是否可以载入内容？	否
客户端应用程序是否可以检索内容？	某些对象可以检索、而其他对象则无法检索。
数据是否存在风险？	否
开展业务的能力是否受到严重影响？	是、因为客户端应用程序无法将对象存储到StorageGRID 系统、并且无法一致地检索数据。

收集数据

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

要收集的数据类型	为什么要收集此数据	说明
创建最近更改的时间线	对 StorageGRID 系统，其配置或环境进行更改可以发生原因 新行为。	• 创建最近更改的时间线
查看警报	警报可以通过提供有关可能导致问题的根本问题的重要线索、帮助您快速确定问题的根本原因。 查看当前警报列表、查看StorageGRID是否已确定问题的根本原因。 查看过去触发的警报、了解更多信息。	• "查看当前警报和已解决警报"
建立基线	收集有关各种运行值的正常级别的信息。这些基线值以及与这些基线的偏差可以提供有价值的线索。	• 建立基线
执行载入和检索测试	要解决载入和检索的性能问题，请使用工作站存储和检索对象。将结果与使用客户端应用程序时看到的结果进行比较。	• "监控 PUT 和 GET 性能"

要收集的数据类型	为什么要收集此数据	说明
查看审核消息	查看审核消息以详细了解 StorageGRID 操作。审核消息中的详细信息对于排除包括性能问题在内的多种类型的问题非常有用。	• "查看审核消息"
检查对象位置和存储完整性	如果存在存储问题，请验证对象是否已放置在预期位置。检查存储节点上对象数据的完整性。	• "监控对象验证操作" • "确认对象数据位置" • "验证对象完整性"
为技术支持收集数据	技术支持可能会要求您收集数据或查看特定信息，以帮助您解决问题。	• "收集日志文件和系统数据" • "手动触发AutoSupport软件包" • "查看支持指标"

【create_timeline】创建最近更改的时间线

出现问题时，您应考虑最近发生了哪些更改以及何时发生了这些更改。

- 对 StorageGRID 系统，其配置或环境进行更改可以发生原因 新行为。
- 更改时间线可以帮助您确定哪些更改可能会对问题描述 造成影响，以及每个更改可能会对其开发产生何种影响。

创建一个系统近期更改的表，其中包含有关每次更改发生时间的信息以及有关更改的任何相关详细信息，以及有关更改进行期间发生的其他情况的信息：

更改时间	更改类型	详细信息
例如： • 您何时开始节点恢复？ • 软件升级何时完成？ • 您是否中断了此过程？	发生什么事了？您做了什么？	记录有关变更的任何相关详细信息。例如： • 网络更改的详细信息。 • 安装了哪个修补程序。 • 客户端工作负载如何更改。 请务必注意，如果同时发生多个更改。例如，是否在升级过程中进行了此更改？

近期重大变更的示例

以下是一些可能会发生重大变化的示例：

- StorageGRID 系统是最近安装，扩展还是恢复的？
- 系统近期是否已升级？是否应用了修补程序？
- 最近是否修复或更改过任何硬件？

- 是否已更新 ILM 策略?
- 客户端工作负载是否已更改?
- 客户端应用程序或其行为是否发生变化?
- 您是否更改了负载平衡器，添加或删除了管理节点或网关节点的高可用性组?
- 是否已启动可能需要很长时间才能完成的任务？示例包括：
  - 恢复发生故障的存储节点
  - 存储节点停用
- 是否对用户身份验证进行了任何更改，例如添加租户或更改 LDAP 配置?
- 是否正在进行数据迁移?
- 最近是否启用或更改了平台服务?
- 最近是否启用了合规性?
- 是否已添加或删除云存储池?
- 是否对存储压缩或加密进行了任何更改?
- 网络基础架构是否有任何变化？例如， VLAN ，路由器或 DNS 。
- 是否对 NTP 源进行了任何更改?
- 是否对网格，管理员或客户端网络接口进行了任何更改?
- 是否对 StorageGRID 系统或其环境进行了任何其他更改?

建立基线

您可以通过记录各种运行值的正常级别来为系统建立基线。将来，您可以将当前值与这些基线进行比较，以帮助检测和解决异常值。

属性	价值	如何获取
平均存储消耗	GB 已用 / 天 每日消耗百分比	转到网格管理器。在节点页面上，选择整个网格或站点，然后转到存储选项卡。 在 " 已用存储 - 对象数据 " 图表上，找到一个线相当稳定的句点。将光标置于图表上方、以估计每天占用的存储容量 您可以收集整个系统或特定数据中心的此信息。
平均元数据消耗	GB 已用 / 天 每日消耗百分比	转到网格管理器。在节点页面上，选择整个网格或站点，然后转到存储选项卡。 在 " 已用存储 - 对象元数据 " 图表上，找到一个线相当稳定的句点。将光标置于图表上方、以估计每天占用的元数据存储容量 您可以收集整个系统或特定数据中心的此信息。

属性	价值	如何获取
S3 操作速率	操作数 / 秒	在网格管理器仪表板上，选择*性能*>*存储节点的 S3 操作*。 要查看特定站点或节点的提取和检索速率和计数，请选择 **Nodes** > ***site*** 或 ***Storage Node*** > **Objects**。将光标放在 S3 摄取和检索图表上。
ILM 评估率	对象 / 秒	从节点页面中，选择 * ； grid_* > * 。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标置于图表上方以估算系统的*评估率*基线值。
ILM 扫描速率	对象 / 秒	选择 **Nodes** > ***grid*** > **ILM**。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标置于图表上方，估算系统的*Scan Rate (扫描速率)*基线值。
从客户端操作排队的对象	对象 / 秒	选择 **Nodes** > ***grid*** > **ILM**。 在 ILM 队列图表中，找到线条相当稳定的句点。将光标置于图表上方可估算系统*已排队(来自客户端操作)的对象*的基线值。
平均查询延迟	毫秒	选择*节点* > 存储节点 > 对象。在查询表中，查看平均延迟的值。

分析数据

使用您收集的信息确定问题的发生原因 以及可能的解决方案。

分析与问题 - 相关，但一般而言：

- 使用警报查找故障点和瓶颈。
- 使用警报历史记录和图表重建问题历史记录。
- 使用图表查找异常并将问题情况与正常运行进行比较。

上报信息检查清单

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

✔	项目	备注
	问题陈述	问题症状是什么？问题是从何时开始的？是否持续或间歇性发生？如果间歇性发生，发生过什么时间？ 定义问题
	影响评估	问题的严重性是什么？对客户端应用程序有何影响？ • 客户端以前是否已成功连接？ • 客户端是否可以载入，检索和删除数据？
	StorageGRID 系统 ID	选择*维护* > 系统 > 许可证。 StorageGRID系统 ID 显示为当前许可证的一部分。
	软件版本	从网格管理器顶部，选择帮助图标并选择 * 关于 * 以查看 StorageGRID 版本。
	自定义	总结 StorageGRID 系统的配置方式。例如，列出以下内容： • 网格是否使用存储压缩，存储加密或合规性？ • ILM是否创建复制的或经过重复编码的对象？ILM 是否可确保站点冗余？ILM规则是否使用平衡、严格或双重提交加网行为？
	日志文件和系统数据	收集系统的日志文件和系统数据。选择*支持* > 工具 > 日志收集。 您可以收集整个网格或选定节点的日志。 如果您仅收集选定节点的日志，请确保至少包含一个具有 ADC 服务的存储节点。站点安装的前三个存储节点包括 ADC 服务。
	基线信息	收集有关载入操作，检索操作和存储消耗的基线信息。 建立基线
	最近更改的时间线	创建一个时间线，用于汇总系统或其环境的所有近期更改。 创建最近更改的时间线
	诊断问题描述 的工作历史记录	如果您已自行采取步骤对问题描述 进行诊断或故障排除，请务必记录所采取的步骤和结果。

对对象和存储问题进行故障排除

确认 StorageGRID 中的对象数据位置

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

开始之前

- 您必须具有一个对象标识符，该标识符可以是以下项之一：
  - * UUID * ： 对象的通用唯一标识符。输入全部大写的 UUID 。
  - * CBID* ： StorageGRID 中对象的唯一标识符。您可以从审核日志中获取对象的 CBID 。输入全部大写的 CBID 。
  - **S3**"S3接口"存储分段和对象密钥:通过插入对象时，客户端应用程序使用存储分段和对象密钥组合来存储和标识对象。

步骤

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

   您可以输入 UUID、CBID 或 S3 bucket/object-key。

3. 如果要查找对象的特定版本，请输入版本 ID （可选）。



4. 选择 * 查找 * 。

   "对象元数据查找结果"此时将显示。此页面列出了以下类型的信息：

   - 系统元数据，包括对象 ID （ UUID ），版本 ID （可选），对象名称，容器名称，租户帐户名称或 ID ，对象的逻辑大小，首次创建对象的日期和时间以及上次修改对象的日期和时间。
   - 与对象关联的任何自定义用户元数据键值对。
   - 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
   - 对于复制的对象副本，为每个副本提供当前存储位置。
   - 对于经过擦除编码的对象副本，为每个片段的当前存储位置。
   - 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。

- 对于分段对象和多部分对象，包含分段标识符和数据大小的对象分段列表。对于包含 100 个以上区块的对象，仅显示前 100 个区块。
- 所有对象元数据均采用未处理的内部存储格式。此原始元数据包括内部系统元数据，不能保证这些元数据在版本之间持续存在。

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

System Metadata

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

Replicated Copies

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

Raw Metadata


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


了解 **StorageGRID** 中存储卷的对象存储故障

存储节点上的底层存储分为多个对象存储。对象存储也称为存储卷。

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

Disk devices

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

Volumes

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

Object stores

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

根据故障的性质，存储卷的故障可能会反映在中"存储卷警报"。如果存储卷发生故障，您应尽快修复故障存储卷，以将存储节点还原到完整功能。如有必要，您可以转到*Configuration*选项卡，以便StorageGRID系统可以使用该选项卡"将存储节点置于只读 - 状态"进行数据检索，同时为服务器的完全恢复做准备。

验证 **StorageGRID** 中对象数据的完整性

StorageGRID 系统会验证存储节点上对象数据的完整性，并检查是否存在损坏和缺失的对象。

验证过程有两个：后台验证和对象存在检查（以前称为前台验证）。它们协同工作，确保数据完整性。后台验证会自动运行，并持续检查对象数据的正确性。用户可以触发对象存在检查，以便更快速地验证对象是否存在（尽管不是正确）。

什么是后台验证?

后台验证过程会自动持续检查存储节点中是否存在损坏的对象数据副本，并自动尝试修复发现的任何问题。

后台验证将检查复制对象和经过纠删编码的对象的完整性，如下所示：

- * 复制对象 * ：如果后台验证过程发现复制的对象已损坏，则损坏的副本将从其位置中删除，并隔离到存储节点上的其他位置。然后、系统将生成并放置一个未损坏的新副本、以满足活动ILM策略的要求。新副本可能不会放置在用于原始副本的存储节点上。

  > 损坏的对象数据将被隔离而不是从系统中删除，以便仍可访问。有关访问已拒绝的对象数据的详细信息、请与技术支持联系。

- * 擦除编码对象 * ：如果后台验证过程检测到擦除编码对象的片段已损坏，则 StorageGRID 会自动尝试使用剩余的数据和奇偶校验片段在同一个存储节点上原位重建缺失的片段。如果无法重建损坏的片段、则会尝试检索对象的另一个副本。如果检索成功，则会执行 ILM 评估以创建经过纠删编码的对象的替代副本。

  后台验证过程仅检查存储节点上的对象。它不会检查云存储池中的对象。对象必须超过四天，才能进行后台验证。

后台验证以连续速率运行，不会干扰普通系统活动。无法停止后台验证。但是，如果您怀疑存在问题，则可以提高后台验证率，以便更快地验证存储节点的内容。

与后台验证相关的警报

如果系统检测到无法自动更正的损坏对象(因为损坏导致无法识别该对象)，将触发*检测到未识别的损坏对象*警报。

如果后台验证无法替换损坏的对象，因为它无法找到另一个副本，则会触发*对象可能丢失*警报。

什么是对象存在检查?

对象存在检查可验证存储节点上是否存在所有预期复制的对象副本以及经过纠删编码的片段。对象存在检查不会验证对象数据本身（后台验证会验证）；相反，它可以提供一种验证存储设备完整性的方法，尤其是在最新的硬件问题描述 可能会影响数据完整性的情况下。

与自动执行的后台验证不同，您必须手动启动对象存在检查作业。

对象存在检查会读取存储在 StorageGRID 中的每个对象的元数据，并验证是否存在复制的对象副本和经过纠删

编码的对象片段。任何缺失的数据将按以下方式处理：

- * 复制的副本 * ： 如果缺少已复制对象数据的副本， StorageGRID 会自动尝试替换存储在系统其他位置的副本中的副本。存储节点通过 ILM 评估运行现有副本，该评估将确定此对象不再符合当前 ILM 策略，因为缺少另一个副本。此时将生成并放置一个新副本、以满足系统的活动ILM策略。此新副本可能不会放置在存储缺失副本的同一位置。
- * 擦除编码片段 * ： 如果缺少擦除编码对象的片段， StorageGRID 会自动尝试使用剩余片段在同一存储节点上原位重建缺失的片段。如果无法重建缺少的片段(因为丢失的片段太多)、ILM将尝试查找对象的另一个副本、它可以使用该副本生成新的经过删除编码的片段。

运行对象存在检查

一次创建并运行一个对象存在检查作业。创建作业时，您可以选择要验证的存储节点和卷。您还可以选择作业的一致性。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您已确保要检查的存储节点处于在线状态。选择*节点*来查看节点表。确保要检查的节点的节点名称旁边没有出现警报图标。
- 您已确保要检查的节点上 * 未 * 运行以下过程：
  - 网格扩展以添加存储节点
  - 存储节点停用
  - 恢复发生故障的存储卷
  - 恢复系统驱动器出现故障的存储节点
  - EC 重新平衡
  - 设备节点克隆

在这些过程中，对象存在检查不会提供有用的信息。

关于此任务

对象存在性检查作业可能需要数天或数周才能完成、具体取决于网格中的对象数量、选定存储节点和卷以及选定一致性。一次只能运行一个作业，但可以同时选择多个存储节点和卷。

步骤

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

   您可以按节点名称或站点进行搜索。

   您不能选择未连接到网格的节点。

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

要为选定的每个节点选择所有卷、请选中列标题中的*存储卷*复选框。

6. 选择 * 继续 * 。
7. 选择作业的一致性。

   一致性决定了用于对象存在性检查的对象元数据副本数。

   - * 强站点 * ： 在一个站点上创建两个元数据副本。
   - * 强 - 全局 * ： 每个站点上有两个元数据副本。
   - * 全部 * （默认）： 每个站点上的所有三个元数据副本。

     有关一致性的详细信息、请参见向导中的说明。

8. 选择 * 继续 * 。
9. 查看并验证您的选择。您可以选择 * 上一步 * 以转到向导中的上一步以更新所做的选择。

   此时将生成并运行对象存在检查作业，直到出现以下情况之一：

   - 作业完成。
   - 暂停或取消作业。您可以恢复已暂停的作业、但不能恢复已取消的作业。
   - 作业停止。此时将触发 * 对象存在检查已停止 * 警报。按照为警报指定的更正操作进行操作。
   - 作业失败。触发 * 对象存在检查失败 * 警报。按照为警报指定的更正操作进行操作。
   - 出现“Service不可用”或“内部服务器错误”消息。一分钟后，刷新页面以继续监控作业。

     您可以根据需要离开对象存在检查页面并返回以继续监控作业。

10. 在作业运行时，查看 * 活动作业 * 选项卡，并记下检测到的缺少对象副本的值。

    此值表示缺少一个或多个片段的复制对象和经过纠删编码的对象的副本总数。

    如果检测到的丢失对象副本数量大于 100，则存储节点的存储可能存在问题。

11. 作业完成后，执行任何其他所需操作：
    - 如果检测到缺少对象副本为零，则未发现任何问题。无需执行任何操作。
    - 如果检测到的丢失对象副本大于零并且未触发*对象可能丢失*警报，则系统已修复所有丢失的副本。验证所有硬件问题是否都已得到纠正，以防止将来对对象副本造成损坏。
    - 如果检测到的丢失对象副本数大于零，并且触发了*对象可能丢失*警报，则数据完整性可能会受到影响。请联系技术支持。
    - 您可以使用 grep 提取 LLST 审计消息来调查可能丢失的对象副本： `grep LLST audit_file_name` 。

      此过程类似于"调查可能丢失的物品"，尽管你搜索的是对象副本 `LLST`而不是 `OLST`。

12. 如果为此作业选择了强站点或强全局一致性、请等待大约三周、以确保元数据一致性、然后在相同的卷上重新运行此作业。

如果 StorageGRID 有时间为作业中包含的节点和卷实现元数据一致发生原因 性，则重新运行作业可能会错误地清除报告的缺失对象副本，或者如果未选中其他对象副本，则重新运行作业可能会清除这些副本。

a. 选择*维护* > 对象存在检查 > 作业历史记录。
b. 确定哪些作业已准备好重新运行：
   i. 查看 * 结束时间 * 列，确定三周前运行的作业。
   ii. 对于这些作业，请扫描一致性控制列中的强站点或强全局。
c. 选中要重新运行的每个作业对应的复选框，然后选择*Rerun*。
d. 在重新运行作业向导中、查看选定节点和卷以及一致性。
e. 准备好重新运行作业后，请选择 * 重新运行 * 。

此时将显示活动作业选项卡。您选择的所有作业将以一个作业的形式重新运行、并保持Strong站点一致性。详细信息部分中的 * 相关作业 * 字段列出了原始作业的作业 ID 。

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

如果租户尝试执行的非多部分PutObject操作超过S3大小限制5 GiB、则会触发"S3 Put Object Size Too Lize"警报。

开始之前

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

确定哪些租户使用大于5 GiB的对象、以便您可以向其发出通知。

步骤

1. 转到*配置*>*监控*>*审计和系统日志服务器*。
2. 如果客户端写入正常、请访问审核日志：
   a. 输入 `ssh admin@primary_Admin_Node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$` 改为 `#`。

   e. 更改为审核日志所在的目录。

      审核日志目录和适用节点取决于您的审核目标设置。

选项	目标
本地节点(默认)	`/var/local/log/localaudit.log`

选项	目标
管理节点/本地节点	• 管理节点（主要和非主要）：`/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log`在此模式下、文件通常为空或缺失。
外部系统日志服务器	`/var/local/log/localaudit.log`

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

要了解更多信息，请参阅"选择日志位置"。

f. 确定哪些租户正在使用大于5 GiB的对象。

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

ii. 对于结果中的每个审核消息、请查看 `S3AI`字段以确定租户帐户ID。使用消息中的其他字段确定客户端、存储分段和对象使用的IP地址：

代码	说明
SAIP	源IP
S3AI	租户ID
S3BK	存储分段
S3KY	对象
CSIZ	大小(字节)

审核日志结果示例

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CSTR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:identity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][SBAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. 如果客户端写入不正常、请使用警报中的租户ID来标识租户：

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

   b. 提取文件并转到 `bycast.log`：

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

   c. 在日志中搜索 `method=PUT`并在字段中标识客户端 `clientIP`。

      示例**bycast**。**log**

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

4. 通知租户PutObject的最大大小为5 GiB、并对大于5 GiB的对象使用多部分上传。
5. 如果应用程序已更改、请忽略警报一周。

对丢失和丢失的对象数据进行故障排除

了解 **StorageGRID** 中丢失和缺失的对象数据

可以出于多种原因检索对象，包括从客户端应用程序读取请求，对复制的对象数据进行后台验证， ILM 重新评估以及在存储节点恢复期间还原对象数据。

StorageGRID系统使用对象元数据中的位置信息来确定从哪个位置检索对象。如果在预期位置未找到该对象的副本，系统将尝试从系统的其他位置检索该对象的另一个副本，假设 ILM 策略包含制作该对象的两个或更多个副本的规则。

如果检索成功， StorageGRID系统将替换该对象的丢失副本。否则，将触发*对象可能丢失*警报，如下所示：

- 对于复制的副本、如果无法检索到另一个副本、则会将对象视为丢失、并触发警报。
- 对于经过删除编码的副本、如果无法从预期位置检索副本、则在尝试从其他位置检索副本之前、已检测到损坏的副本(ECO)属性会增加一个。如果未找到其他副本，则会触发警报。

您应该立即调查所有*对象可能丢失*警报，以确定丢失的根本原因，并确定对象是否仍存在于离线或当前不可用的存储节点中。看"调查可能丢失的物品" 。丢失物品警报可能会因谨慎而被错误触发。

如果没有副本的对象数据丢失，则没有恢复解决方案。但是，你必须"重置可能丢失的对象计数器"以防止已知丢失的物品掩盖任何新的丢失物品。

解决 **StorageGRID** 中可能丢失对象的警报

当触发“物体可能丢失”警报时，您必须立即进行调查。收集受影响对象的信息并联系技术支持。

开始之前

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

关于此任务

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

立即调查丢失的对象警报。您可能需要采取措施以防止进一步数据丢失。在某些情况下，如果您立即采取措施，则可能能够还原丢失的对象。

如果报告丢失的物品超过 10 件，请联系技术支持。请勿自行遵循此程序。

步骤

1. 选择*节点*。
2. 选择 * 存储节点 _* > * 对象 * 。
3. 查看对象计数表中显示的丢失对象的数量。

   此数字表示此网格节点在整个 StorageGRID 系统中检测到缺少的对象总数。该值是 LDR 和 DDS 服务中数据存储组件的丢失对象计数器之和。

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

      审核日志目录和适用节点取决于您的审核目标设置。

选项	目标
本地节点(默认)	`/var/local/log/localaudit.log`
管理节点/本地节点	• 管理节点（主要和非主要）： `/var/local/audit/export/audit.log` • 所有节点： `/var/local/log/localaudit.log`在此模式下、文件通常为空或缺失。
外部系统日志服务器	`/var/local/log/localaudit.log`

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

要了解更多信息，请参阅"选择日志位置"。

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

d. 记下消息中包含的 UUID 值。

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

5. 使用UUID查找丢失对象的元数据：

a. 选择 * ILM * > * 对象元数据查找 * 。

b. 输入UUID并选择*查找*。

c. 查看元数据中的位置、并采取适当的措施：

元数据	结论
未找到对象<object_identifier>	如果未找到该对象，则返回消息“ERROR”：“”。 如果未找到该对象，重置可能丢失的对象计数器清除警报。缺少某个对象表明该对象被故意删除。
位置 > 0	如果输出中列出了位置，则“物体可能丢失”警报可能是误报。 确认对象存在。使用输出中列出的节点 ID 和文件路径确认对象文件位于列出的位置。 如果物体存在，重置可能丢失的对象计数器清除警报。
位置 = 0	如果输出中没有列出位置，则该对象可能丢失。请联系技术支持。 技术支持可能会要求您确定是否存在正在进行的存储恢复过程。请参阅： • "将对象数据还原到设备的存储卷" • "将对象数据还原到系统驱动器完好无损的存储卷" • "将对象数据还原到存储卷(系统驱动器故障)"

6. 解决丢失对象问题后，请重置可能丢失的对象计数器，以确保警报不是误报：

a. 选择*节点*。

b. 选择*_Storage Node_* > **Tasks**。

c. 在重置对象可能丢失计数器部分，选择*重置*。

解决 **StorageGRID** 中的低对象数据存储警报

对象数据存储空间 * 不足警报可监控每个存储节点上可用于存储对象数据的空间量。

开始之前

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

关于此任务

当存储节点上复制和经过数据线程的对象数据总量满足警报规则中配置的条件之一时，将触发“对象数据存储不足”警报。

默认情况下，如果此情况评估为 true ，则会触发重大警报：

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

在这种情况下：

- `storagegrid_storage_utilization_data_bytes`是对存储节点中已复制和已进行过彻底编码的对象数据总大小的估计值。
- `storagegrid_storage_utilization_usable_space_bytes`是存储节点的剩余对象存储空间总量。

如果触发主要或次要的 * 对象数据存储空间不足 * 警报，则应尽快执行扩展操作步骤 。

步骤

1. 选择*警报* > 当前。

   此时将显示警报页面。

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

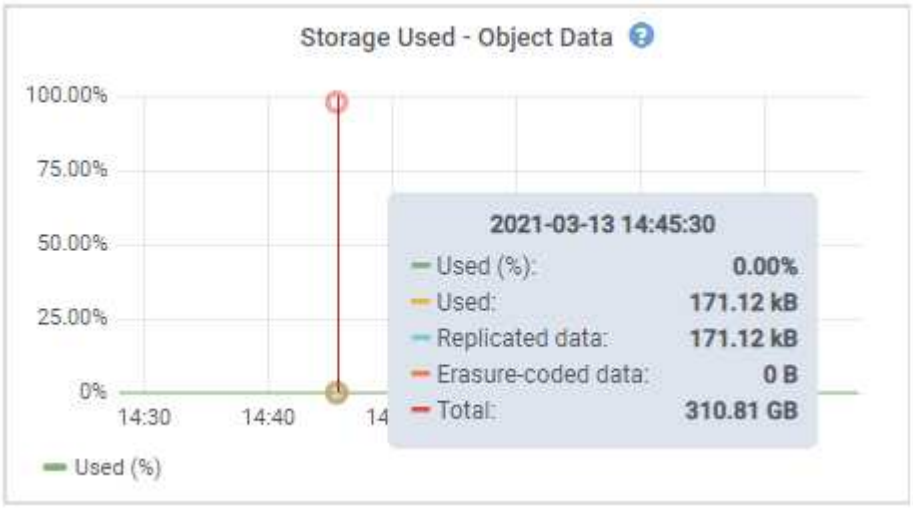
   选择警报，而不是一组警报的标题。

3. 查看对话框中的详细信息，并注意以下事项：
   - 时间已触发
   - 站点和节点的名称
   - 此警报的指标的当前值
4. 选择 **Nodes** > ***Storage Node*** 或 ***Site*** > **Storage**。

5. 将光标置于"Storage Used - Object Data"(已用存储-对象数据)图上。

   此时将显示以下值：

   - * 已用（ % ） * ： 已用于对象数据的总可用空间的百分比。
   - * 已用 * ： 已用于对象数据的总可用空间量。
   - * 复制数据 * ： 此节点，站点或网格上复制的对象数据量的估计值。
   - * 擦除编码数据 * ： 此节点，站点或网格上经过擦除编码的对象数据量的估计值。
   - * 总计 * ： 此节点，站点或网格上的可用空间总量。已用值为 `storagegrid_storage_utilization_data_bytes`度量。



6. 选择图形上方的时间控件可查看不同时间段的存储使用情况。

   查看一段时间内的存储使用量有助于您了解触发警报前后的存储使用量，并有助于您估计节点的剩余空间可能需要多长时间才能达到全满状态。

7. 请尽快"添加存储容量"连接到您的网格。

   您可以向现有存储节点添加存储卷（ LUN ），也可以添加新的存储节点。

   有关详细信息，请参见 "管理完整存储节点"。

解决 **StorageGRID** 中的水印覆盖警报

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

在先前版本中、这三个"存储卷水印"值分别为全局设置&#8212；每个存储节点上的每个存储卷都应用了相同的值。从 StorageGRID 11.6 开始，软件可以根据存储节点的大小和卷的相对容量为每个存储卷优化这些水印。

升级到StorageGRID 11.6或更高版本时、优化的只读和读写水印会自动应用于所有存储卷、除非满足以下任一条件：

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

了解警报

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

每个警报实例均指示存储卷软只读水印的自定义值小于该存储节点的最小优化值。如果您继续使用自定义设置，则存储节点可能会在空间严重不足的情况下运行，然后才能安全地过渡到只读状态。当节点达到容量时，某些存储卷可能无法访问（自动卸载）。

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

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

为存储节点 A 触发 * 低只读水印覆盖 * 警报，因为您的自定义水印（ 5 GB ）小于该节点中所有卷的最小优化值（ 11 GB ）。如果继续使用自定义设置，则节点可能会在空间严重不足的情况下运行，然后才能安全过渡到只读状态。

解决警报

如果触发了一个或多个 * 低只读水印覆盖 * 警报，请执行以下步骤。如果您当前正在使用自定义水印设置，并且希望开始使用优化设置，即使未触发任何警报，也可以使用这些说明。

开始之前

- 您已完成StorageGRID 11.6或更高版本的升级。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限"。

关于此任务

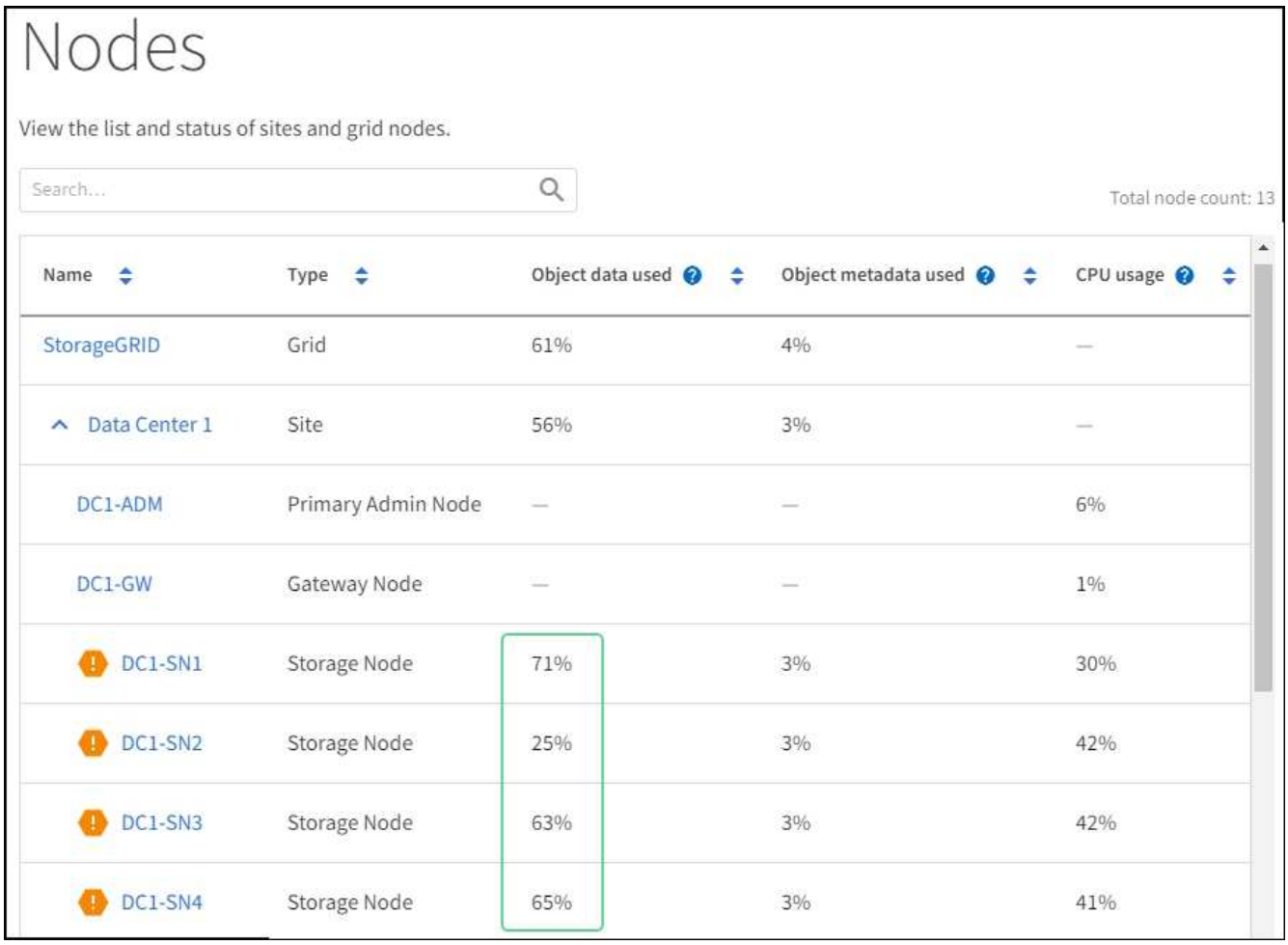
您可以通过将自定义水印设置更新为新的水印覆盖来解决 * 低只读水印覆盖 * 警报。但是，如果一个或多个存储节点接近全满或您有特殊的 ILM 要求，则应首先查看优化的存储水印并确定使用它们是否安全。

评估整个网格的对象数据使用情况

步骤

1. 选择*节点*。
2. 对于网格中的每个站点，展开节点列表。

3. 查看每个站点的每个存储节点的 * 对象数据已用 * 列中显示的百分比值。



4. 按照相应步骤操作：

   a. 如果所有存储节点均未接近全满（例如，所有 * 已使用的对象数据 * 值均小于 80% ），则可以开始使用覆盖设置。转到。 使用优化的水印

   b. 如果ILM规则使用严格的加载行为，或者特定存储池接近全满，请执行和中的步骤。查看优化的存储水印 确定是否可以使用优化的水印

[[view-优化 的水印**]]**查看优化的存储水印

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

步骤

1. 选择*支持* > 工具 > 指标。
2. 在 Prometheus 部分中，选择用于访问 Prometheus 用户界面的链接。
3. 要查看建议的最小软只读水印，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

5. 【最大优化值】记下每个存储节点的最大优化值。

确定是否可以使用优化的水印

步骤

1. 选择*节点*。
2. 对每个联机存储节点重复上述步骤：
   a. 选择 * 存储节点 _* > * 存储 * 。
   b. 向下滚动到对象存储表。
   c. 将每个对象存储（卷）的 * 可用 * 值与您为该存储节点记下的最大优化水印进行比较。
3. 如果每个联机存储节点上至少有一个卷的可用空间超过该节点的最大优化水印、请转到开始使用优化水印。使用优化的水印

   否则、请尽快扩展网格。"添加存储卷"到现有节点或"添加新存储节点"。然后、转到使用优化的水印以更新水印设置。

4. 如果您需要继续对存储卷水印使用自定义值，"静默"或者"禁用"“低只读水印覆盖”警报。

   相同的自定义水印值将应用于每个存储节点上的每个存储卷。对存储卷水印使用小于建议值可能发生原因 会导致某些存储卷在节点达到容量时无法访问（自动卸载）。

[[use-优化 水印]]使用优化水印

步骤

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

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

对 StorageGRID 中的元数据问题进行故障排除

如果发生元数据问题、警报将通知您问题的根源以及建议采取的措施。尤其是、如果触发了"元数据存储不足"警报、则必须添加新的存储节点。

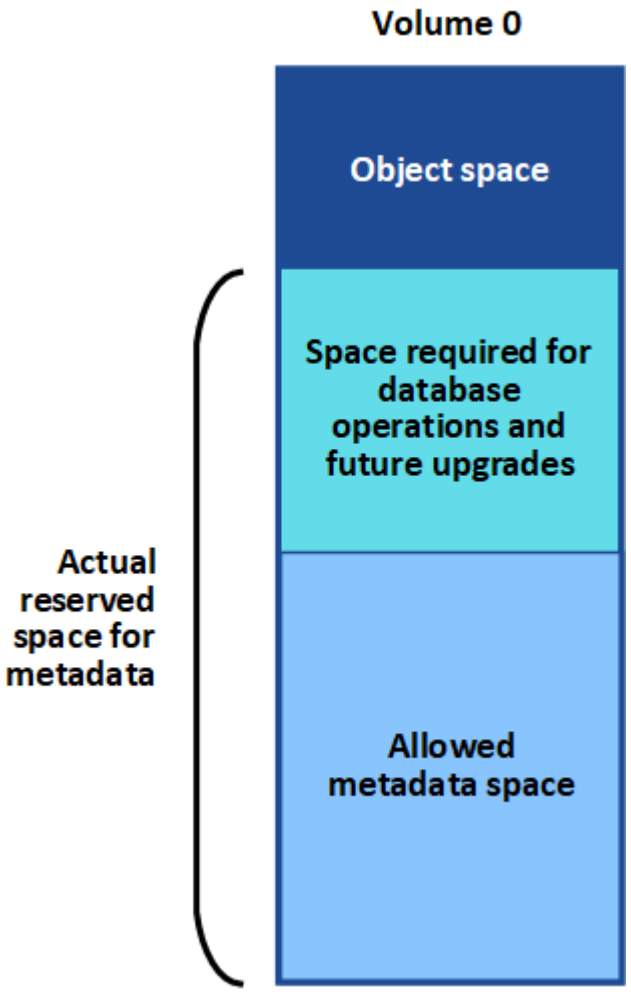
开始之前

您已使用登录到网格管理器"支持的 Web 浏览器"。

关于此任务

对于触发的每个元数据相关警报、请遵循建议的操作。如果触发 * 低元数据存储 * 警报，则必须添加新的存储节点。

StorageGRID 会在每个存储节点的卷 0 上为对象元数据预留一定数量的空间。此空间称为_쪵 뵆 Reserved space_、它细分为允许对象元数据使用的空间(允许的元数据空间)以及执行数据缩减和修复等基本数据库操作所需的空间。允许的元数据空间用于控制整体对象容量。



如果对象元数据占用的空间超过元数据所允许的全部空间、则数据库操作将无法高效运行、并会发生错误。

您可以"监控每个存储节点的对象元数据容量"帮助您预测错误并在错误发生之前予以更正。

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

- * 次要 *： 对象元数据正在使用允许的元数据空间的 70% 或更多。您应尽快添加新的存储节点。
- * 主要 *： 对象元数据正在使用允许的元数据空间的 90% 或更多。您必须立即添加新的存储节点。

当对象元数据使用90%或更多允许的元数据空间时、信息板上会显示一条警告。如果显示此警告，则必须立即添加新的存储节点。绝不能允许对象元数据使用超过允许空间的 100% 。

- * 严重 * ： 对象元数据正在使用 100% 或更多的允许元数据空间，并且开始占用基本数据库操作所需的空间。您必须停止载入新对象，并且必须立即添加新的存储节点。

如果卷 0 的大小小于元数据预留空间存储选项（例如，在非生产环境中），则计算 * 低元数据存储 * 警报可能不准确。

步骤

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

由于 StorageGRID 会在每个站点保留所有对象元数据的完整副本，因此整个网格的元数据容量受最小站点的元数据容量限制。如果您需要向一个站点添加元数据容量、则存储节点的数量也应"扩展任何其他站点"相同。

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

对 StorageGRID 中的证书错误进行故障排除

如果在尝试使用Web浏览器、S3客户端或外部监控工具连接到StorageGRID时发现安全或证书问题、则应检查此证书。

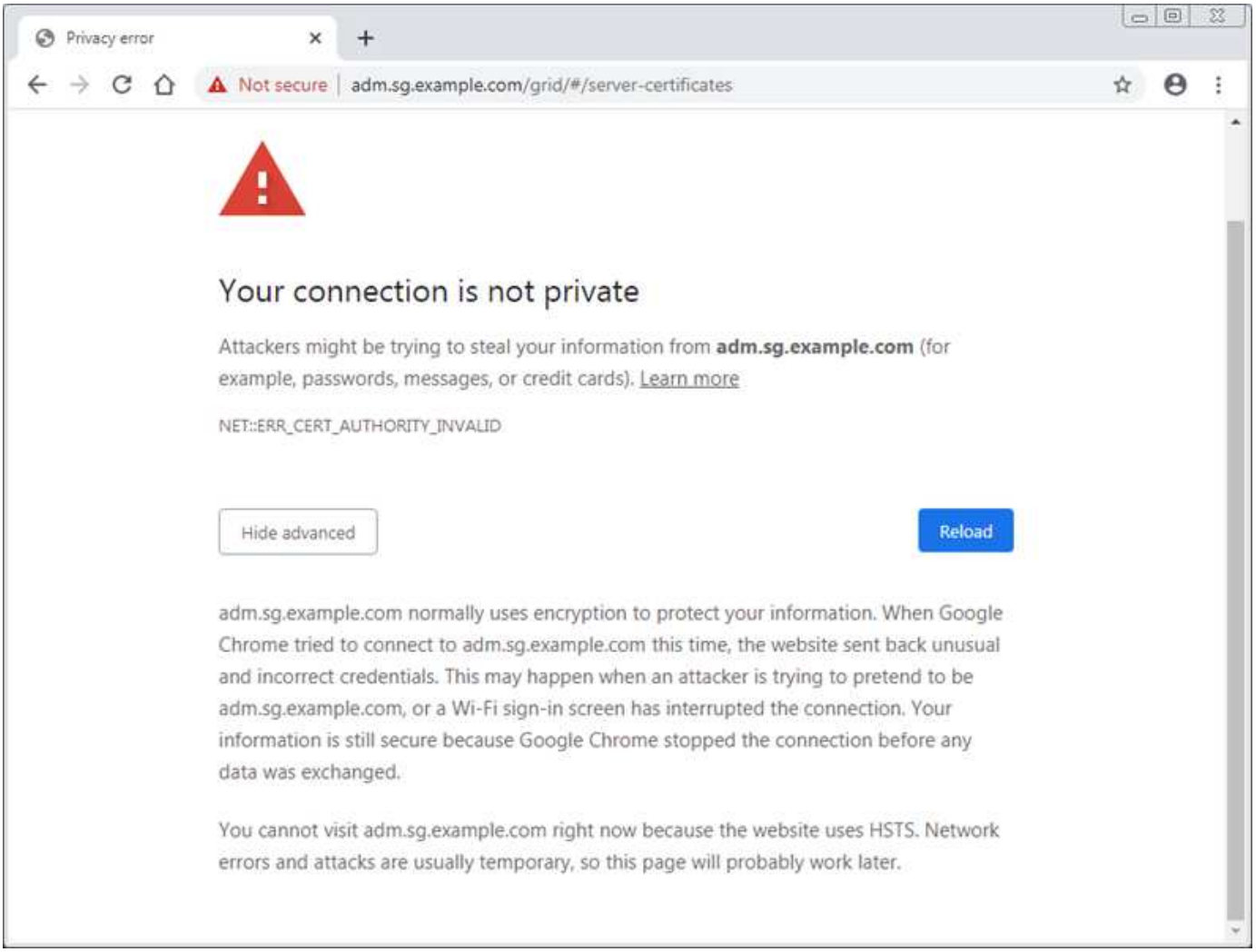
关于此任务

尝试使用网格管理器，网格管理 API ，租户管理器或租户管理 API 连接到 StorageGRID 时，证书错误可能会出现发生原因 问题。在尝试连接到S3客户端或外部监控工具时、也可能发生证书错误。

如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：

- 您的自定义管理接口证书将过期。
- 您可以从自定义管理接口证书还原到默认服务器证书。

以下示例显示了自定义管理接口证书过期时的证书错误：



为确保操作不会因服务器证书失败而中断，当服务器证书即将到期时，将触发*管理接口的服务器证书到期*警报。

在使用客户端证书进行外部 Prometheus 集成时，证书错误可能是由 StorageGRID 管理接口证书或客户端证书引起的。当客户端证书即将过期时，将触发 " 证书 " 页面上配置的 * 客户端证书到期 * 警报。

步骤

如果您收到有关证书过期的警报通知，请访问证书详细信息：。选择 配置 > 安全 > 证书，然后"选择相应的证书选项卡"。

1. 检查证书的有效期。+一些Web浏览器和S3客户端不接受有效期超过398天的证书。
2. 如果证书已过期或即将过期，请上传或生成新证书。
   - 有关服务器证书，请参见的步骤"为网格管理器和租户管理器配置自定义服务器证书"。
   - 有关客户端证书，请参见的步骤"配置客户端证书"。
3. 对于服务器证书错误，请尝试以下任一或两个选项：
   - 确保已填充证书的使用者备用名称（ SAN ），并且 SAN 与要连接到的节点的 IP 地址或主机名匹配。
   - 如果您尝试使用域名连接到 StorageGRID ：
     i. 输入管理节点的 IP 地址，而不是域名，以绕过连接错误并访问网格管理器。

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

iii. 在管理StorageGRID的说明中，请参见的步骤"为网格管理器和租户管理器配置自定义服务器证书"。

对 StorageGRID 中的管理节点和用户界面问题进行故障排除

您可以执行多项任务来帮助确定与管理节点和StorageGRID用户界面相关的问题的根源。

管理节点登录错误

如果您在登录到StorageGRID管理节点时遇到错误，则系统可能会遇到"网络连接"或 "硬件"问题、"管理节点服务"或"使用Cassand拉 数据库的问题描述"已连接存储节点上的问题。

开始之前

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

关于此任务

如果在尝试登录到管理节点时看到以下任何错误消息，请遵循以下故障排除准则：

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

步骤

1. 等待 10 分钟，然后重新尝试登录。

   如果此错误未自动解决，请转至下一步。

2. 如果您的StorageGRID系统具有多个管理节点、请尝试从另一个管理节点登录到网格管理器、以检查不可用管理节点的状态。

   - 如果您能够登录，您可以使用*仪表板*、节点、*警报*和*支持*选项来帮助确定错误的原因。
   - 如果您只有一个管理节点或仍无法登录、请转到下一步。

3. 确定节点的硬件是否脱机。

4. 如果为您的 StorageGRID 系统启用了单点登录 (SSO)，请参阅使用 "OIDC" 或 "SAML" 设置 SSO。

   要解决任何问题，您可能需要暂时禁用并重新启用单个管理节点的 SSO 。

5. 确定您正在使用的帐户是否属于联合用户。

   如果此联合用户帐户不起作用，请尝试以本地用户（例如 root ）身份登录到网格管理器。

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

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

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

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

   确保 NMS ， Mi ， nginx 和 mgmt API 服务均已运行。

   如果服务状态发生变化，输出将立即更新。

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

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

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

   终端的输出指示日志归档的复制位置。

10. 【 review_logs ， start=10]] 查看以下日志：
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`

11. 如果您无法确定管理节点存在任何问题问题描述 ，请执行以下任一命令来确定在您的站点上运行此 ADA 服务的三个存储节点的 IP 地址。通常，这些存储节点是站点上安装的前三个存储节点。

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

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

管理节点会在身份验证过程中使用此 ADC 服务。

12. 在管理节点中、使用ssh使用您标识的IP地址登录到每个ADC存储节点。
13. 查看网格节点上正在运行的所有服务的状态： `storagegrid-status`

确保 idnt ， Acct ， nginx 和 Cassandra 服务均已运行。

14. 重复步骤使用 Lumberjack 收集日志和查看日志以查看存储节点上的日志。
15. If you are unable to resolve the issue, contact technical support.

将收集的日志提供给技术支持。另请参见"日志文件参考"。

用户界面问题

升级StorageGRID 软件后、网格管理器或租户管理器的用户界面可能无法按预期响应。

步骤

1. 确保您使用的是"支持的 Web 浏览器"。
2. 清除 Web 浏览器缓存。

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

对 **StorageGRID** 中的网络、硬件和平台问题进行故障排除

您可以执行多项任务来帮助确定与 StorageGRID 网络，硬件和平台问题相关的问题的根源。

[[422-unprocessable-entity-errors]]
== "422：Unprocessable Entry"(422：无法处理的实体)错误

错误422：Unprocessable实体可能会因不同原因而出现。检查错误消息以确定导致问题描述 的原因。

如果您看到列出的错误消息之一，请采取建议的操作。

错误消息	根发生原因 和更正操作

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

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

[[INROTY_MTU/警报]]网格网络**MTU**不匹配警报

如果网格网络接口（ eth0 ）的最大传输单元（ MTU ）设置在网格中的各个节点之间差别很大，则会触发 * 网格网络 MTU 不匹配 * 警报。

关于此任务

MTU 设置的差异可能表明，某些（但并非所有） eth0 网络配置了巨型帧。如果 MTU 大小不匹配大于 1000 ，则可能会出现发生原因 网络性能问题。

步骤

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

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

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

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

定位参数	说明
`mtu`	要设置的 MTU 。必须介于 1280 到 9216 之间。
`network`	要应用 MTU 的网络。包括以下一种或多种网络类型： • 网格 • 管理员 • 客户端

+

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

4. 如果您允许外部 SSH 访问，"阻止访问"当你完成任务时。

节点网络接收帧错误警报

*节点网络接收帧错误*警报可能是由StorageGRID与网络硬件之间的连接问题引起的。解决基本问题后、此警报将自行清除。

关于此任务

*节点网络接收帧错误*警报可能是由连接到StorageGRID的网络硬件出现以下问题引起的：

- 需要正向错误更正（ FEC ），但不在使用中
- 交换机端口和 NIC MTU 不匹配
- 链路错误率较高
- NIC 环缓冲区溢出

步骤

1. 根据您的网络配置、针对此警报的所有潜在原因、请按照故障排除步骤进行操作。
2. 根据错误的发生原因 执行以下步骤：

FEC不匹配

这些步骤仅适用于StorageGRID设备上FEC不匹配导致的*节点网络接收帧错误*警报。

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

b. 检查从设备到交换机的缆线的物理完整性。

c. 如果要更改FEC设置以尝试解决警报，请首先确保在StorageGRID设备安装程序的“链接配置”页面上将设备配置为*Auto*模式(请参阅设备说明：

- "SG6160"
- "SGF6112"
- "SG6000"
- "SGs了"
- "SG5700"
- "SG110和SG1100"
- "SG100和SG1000"

d. 更改交换机端口上的FEC设置。如果可能， StorageGRID 设备端口会调整其 FEC 设置以匹配。

您无法在StorageGRID 设备上配置FEC设置。相反，设备会尝试发现并镜像其所连接的交换机端口上的 FEC 设置。如果强制链路达到 25 GbE 或 100 GbE 网络速度，则交换机和 NIC 可能无法协商通用 FEC 设置。如果没有通用FEC设置、网络将回退到"无FEC"模式。如果未启用FEC、则连接更容易受到电噪声引起的错误的影响。

StorageGRID 设备支持光纤编码(FC)和Reed Solomon (RS) FEC、但不支持FEC。

交换机端口和 **NIC MTU** 不匹配

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

节点上配置的 MTU 大小可能小于节点所连接的交换机端口上的设置。如果StorageGRID节点接收到大于其MTU的以太网帧(这在这种配置下是可能的)，则可能会报告*Node network receeps接收 帧error*警报。如果您认为发生了这种情况，请根据端到端 MTU 目标或要求更改交换机端口的 MTU 以匹配 StorageGRID 网络接口 MTU ，或者更改 StorageGRID 网络接口的 MTU 以匹配交换机端口。

为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的MTU值都必须相同。有关详细信息、请参见 对网格网络 MTU 不匹配警报进行故障排除 。

另请参见 "更改 MTU 设置"。

链路错误率较高

a. 启用 FEC （如果尚未启用）。

b. 确认网络布线质量良好，并且未损坏或连接不正确。

c. 如果缆线没有问题、请联系技术支持。

> 在具有高电噪声的环境中，您可能会发现错误率较高。

NIC 环缓冲区溢出

如果错误是 NIC 环缓冲区溢出，请联系技术支持。

如果 StorageGRID 系统过载且无法及时处理网络事件，则环缓冲区可能会溢出。

3. 监控问题、如果警报未解决、请联系技术支持。

时间同步错误

您可能会在网格中看到时间同步问题。

如果遇到时间同步问题，请确认您至少指定了四个外部 NTP 源，每个源均提供 Stratum 3 或更好的参考，并且所有外部 NTP 源均正常运行且可由 StorageGRID 节点访问。

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

Linux：网络连接问题

您可能会发现Linux主机上托管的StorageGRID节点的网络连接出现问题。

MAC 地址克隆

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

> 创建单独的虚拟网络接口供 Linux 主机操作系统使用。为 Linux 主机操作系统和 StorageGRID 容器使用相同的网络接口可能会导致主机操作系统无法访问。

欲了解更多信息，请参阅"启用 MAC 克隆"。

Linux：节点状态为**"孤立"**

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

关于此任务

如果 Linux 节点报告其处于孤立状态，您应：

- 检查日志中的错误和消息。
- 尝试重新启动节点。
- 如有必要，请使用 container engine 命令停止现有节点容器。

- 重新启动节点。

步骤

1. 检查服务守护进程和孤立节点的日志，查看是否存在明显的错误或有关意外退出的消息。
2. 以 root 身份或使用具有 sudo 权限的帐户登录到主机。
3. 运行以下命令、尝试重新启动节点： `$ sudo storagegrid node start node-name`

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

   如果节点已孤立，则响应为

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

4. 在 Linux 中，停止容器引擎以及任何控制存储节点进程。例如：`sudo docker stop --time secondscontainer-name`

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

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

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

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

Linux： 对 **IPv6** 支持进行故障排除

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

关于此任务

要查看已分配给网格节点的IPv6地址、请执行以下操作：

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

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

步骤

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

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

结果应为 0 。

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

如果结果不是0，请参阅操作系统的说明文件以更改 `sysctl`设置。然后，将此值更改为 0 ，然后再继续。

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

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

结果应为 1 。

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

如果结果不是 1 ，则此操作步骤 不适用。请联系技术支持。

5. 退出容器： `exit`

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

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

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

7. 找到以下两行并删除注释标记。然后，保存并关闭该文件。

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

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

8. 运行以下命令重新启动 StorageGRID 容器：

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

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

对 StorageGRID 外部系统日志服务器错误消息进行故障排除

下表介绍了可能与外部系统日志服务器相关的错误消息、并列出了更正操作。

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

运行时问题可能会由"外部系统日志服务器转发错误"警报。如果您收到此警报，请按照警报中的说明重新发送测试消息，以便您可以获得详细的错误消息。

有关将审核信息发送到外部系统日志服务器的详细信息、请参见：

- "使用外部系统日志服务器的注意事项"
- "配置日志管理和外部系统日志服务器"

错误消息	问题描述 和建议的操作
无法解析主机名	您为系统日志服务器输入的 FQDN 无法解析为 IP 地址。 1. 检查输入的主机名。如果输入了IP地址、请确保该地址是有效的IP地址、采用w.x.y.z ("点分十进制")表示法。 2. 检查 DNS 服务器是否配置正确。 3. 确认每个节点均可访问 DNS 服务器的 IP 地址。
连接被拒绝	拒绝与系统日志服务器建立 TCP 或 TLS 连接。可能没有服务在侦听主机的 TCP 或 TLS 端口，或者防火墙可能正在阻止访问。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 2. 确认系统日志服务的主机正在运行侦听指定端口的系统日志守护进程。 3. 确认防火墙不会阻止从节点到系统日志服务器的 IP 和端口的 TCP/TLS 连接访问。
无法访问网络	系统日志服务器不在直连子网上。路由器返回 ICMP 失败消息，指示它无法将测试消息从列出的节点转发到系统日志服务器。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 对于列出的每个节点，请检查网格网络子网列表，管理网络子网列表和客户端网络网关。确认这些配置已通过预期网络接口和网关（网格，管理员或客户端）将流量路由到系统日志服务器。

错误消息	问题描述 和建议的操作
无法访问主机	系统日志服务器位于直连子网上（列出的节点用于其网格，管理员或客户端 IP 地址的子网）。节点尝试发送测试消息，但未收到对系统日志服务器 MAC 地址的 ARP 请求的响应。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 检查运行系统日志服务的主机是否已启动。
连接超时	已尝试进行 TCP/TLS 连接，但系统日志服务器长时间未收到任何响应。可能存在路由配置不当或防火墙在未发送任何响应的情况下丢弃流量（通用配置）。 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址是否正确。 2. 对于列出的每个节点，请检查网格网络子网列表，管理网络子网列表和客户端网络网关。确认已将这些端口配置为使用网络接口和网关(网格、管理或客户端)将流量路由到系统日志服务器、系统日志服务器将通过这些接口和网关访问。 3. 确认防火墙未阻止从列出的节点到系统日志服务器的 IP 和端口访问 TCP/TLS 连接。
配对节点已关闭连接	已成功建立与系统日志服务器的 TCP 连接，但稍后关闭。原因可能包括： • 系统日志服务器可能已重新启动或重新启动。 • 节点和系统日志服务器可能具有不同的 TCP/TLS 设置。 • 中间防火墙可能正在关闭闲置的 TCP 连接。 • 侦听系统日志服务器端口的非系统日志服务器可能已关闭连接。 要解决此问题描述，请执行以下操作： 1. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 2. 如果您使用的是 TLS ，请确认系统日志服务器也使用 TLS 。如果您使用的是 TCP ，请确认系统日志服务器也使用 TCP 。 3. 检查中间防火墙是否未配置为关闭空闲 TCP 连接。
TLS 证书错误	从系统日志服务器收到的服务器证书与您提供的 CA 证书包和客户端证书不兼容。 1. 确认 CA 证书包和客户端证书（如果有）与系统日志服务器上的服务器证书兼容。 2. 确认系统日志服务器的服务器证书中的身份包含预期的 IP 或 FQDN 值。
转发已暂停	系统日志记录不再转发到系统日志服务器， StorageGRID 无法检测到原因。 查看随此错误提供的调试日志，尝试确定根发生原因 。

错误消息	问题描述 和建议的操作
TLS 会话已终止	系统日志服务器已终止 TLS 会话， StorageGRID 无法检测到原因。 1. 查看随此错误提供的调试日志，尝试确定根发生原因 。 2. 检查您为系统日志服务器输入的 FQDN 或 IP 地址，端口和协议是否正确。 3. 如果您使用的是 TLS ，请确认系统日志服务器也使用 TLS 。如果您使用的是 TCP ，请确认系统日志服务器也使用 TCP 。 4. 确认 CA 证书包和客户端证书（如果有）与系统日志服务器的服务器证书兼容。 5. 确认系统日志服务器的服务器证书中的身份包含预期的 IP 或 FQDN 值。
结果查询失败	用于系统日志服务器配置和测试的管理节点无法从列出的节点请求测试结果。一个或多个节点可能已关闭。 1. 按照标准故障排除步骤操作，确保节点联机且所有预期服务均正在运行。 2. 在列出的节点上重新启动 miscd 服务。

了解 StorageGRID 中的负载均衡器缓存问题

了解负载均衡器缓存可能存在的问题以及如何解决这些问题。

确定请求是否是缓存命中

- X-Cache 标头是在缓存服务处理的请求的响应中设置的。可能的代码：
  - `HIT`：该对象由缓存提供
  - `PARTIAL-HIT`：存储桶/键在缓存中有记录，但并非所有请求的范围都能够从缓存中得到服务
  - `STALE`：存储桶/键在缓存中有一个记录，但自上次从缓存中提供该对象后，该对象已被更新。
  - `MISS`：该对象不在缓存中
- 这 `nginx-gw/endpoint-access.log.gz`请求的记录包括“unix:/run/cache-svc/cache-svc.sock”，用于缓存处理的请求。
- 这 `cache-svc/cache-svc.log`报告诸如“请求 320390：成功完成（缓存命中）”或“请求 320375：成功完成（缓存未命中）”之类的消息。通过搜索具有相同“Request <*number*>”字符串的其他记录来查找请求的路径。

缓存命中率低

- 当添加新的工作负载或工作负载访问的工作集发生变化时，可能会出现较低的缓存命中率。在这些情况下，命中率预计会随着时间的推移而增加。
- 如果多个工作负载正在使用缓存，请考虑添加流量分类策略来隔离由缓存服务的工作负载部分。每个流量分类策略都有缓存命中率指标。如果某些工作负载的缓存命中率不高，请考虑将这些工作负载移动到未启用缓存的其他端点。
- 评估缓存驱逐率。如果缓存太小而无法容纳工作集，它将经历高驱逐率并可能导致命中率降低。
- FPVR 下可能提供用于提高某些工作负载命中率的选项。

性能低下

- 评估缓存命中率。低缓存命中率会导致整体性能低下。
- 评估缓存驱逐率。在驱逐期间，一些存储资源用于从磁盘中删除现有对象。如果驱逐过程跟不上新对象的访问，系统可能会达到硬水印阈值并开始绕过缓存。
- 使用“网络接口接收使用情况”和“网络接口传输使用情况”诊断检查网络限制。

查看审核日志

审核消息和日志

这些说明包含有关 StorageGRID 审核消息和审核日志的结构和内容的信息。您可以使用此信息读取和分析系统活动的审核跟踪。

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

要使用文本日志文件，您必须有权访问管理节点上配置的审核共享。

有关配置审计消息级别和使用外部系统日志服务器的信息，请参阅"配置日志管理和外部系统日志服务器"。

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

所有 StorageGRID 服务都会在系统正常运行期间生成审核消息。您应了解这些审核消息如何在StorageGRID系统中移动到 `audit.log`文件。

仅当为 管理节点/本地节点 或 管理节点和外部系统日志服务器 配置StorageGRID时，以下审计消息和审计消息保留工作流程才适用。如果StorageGRID配置为“仅本地节点”（默认）或“外部系统日志服务器”，则审计消息将保存在本地的每个节点上 `/var/local/log/localaudit.log`文件并且无法由管理节点或存储节点处理。

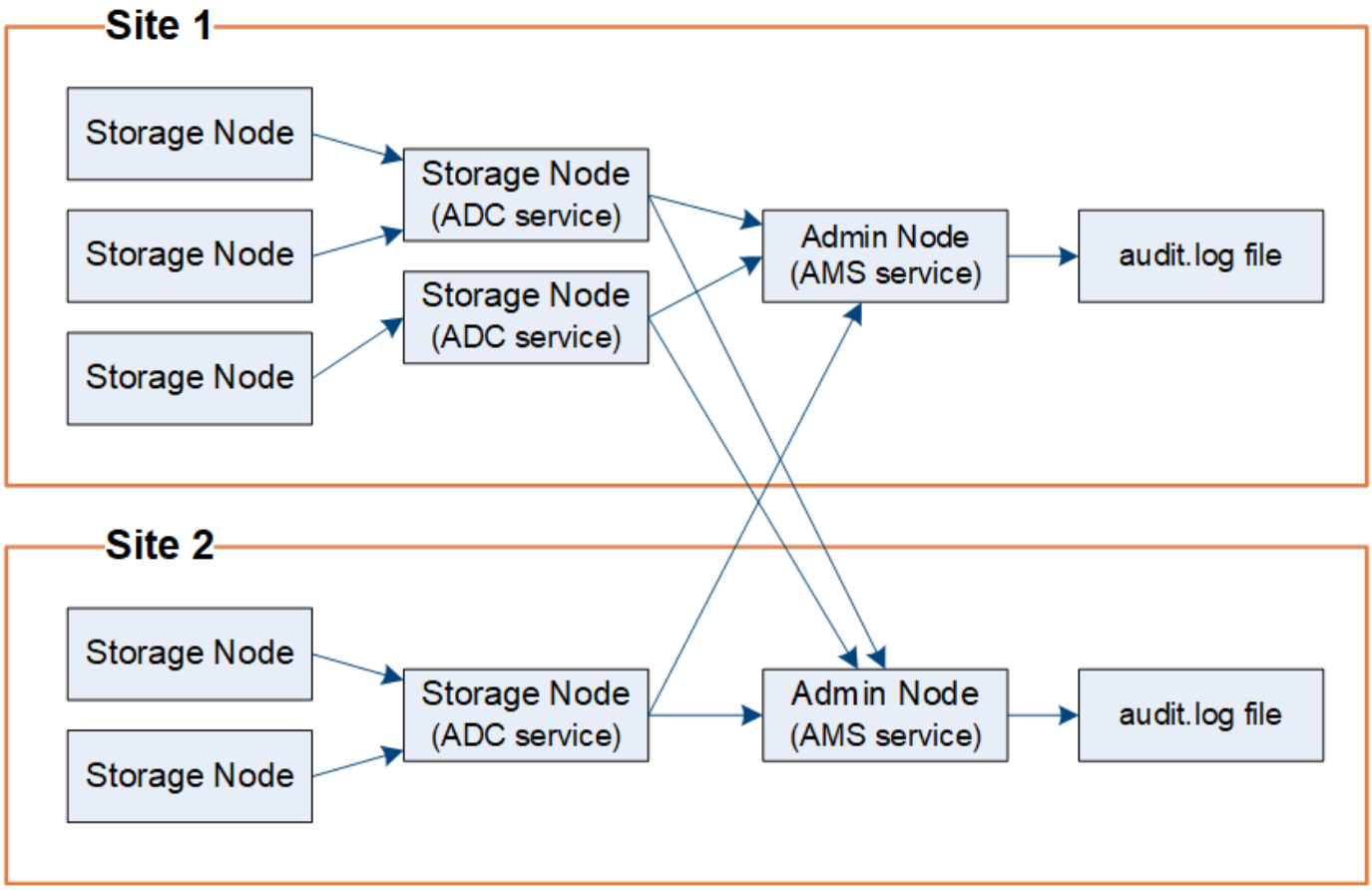
审核消息流

当StorageGRID配置为 管理节点/本地节点 或 管理节点和外部系统日志服务器 时，审计消息由管理节点处理，并且由具有管理域控制器 (ADC) 服务的存储节点处理。

如审核消息流程图所示，每个 StorageGRID 节点都会将其审核消息发送到数据中心站点的一个模板服务。每个站点上安装的前三个存储节点会自动启用此 ADC-Service 。

反过来，每个 ADC 服务都充当中继，并将其审核消息集合发送到 StorageGRID 系统中的每个管理节点，从而为每个管理节点提供完整的系统活动记录。

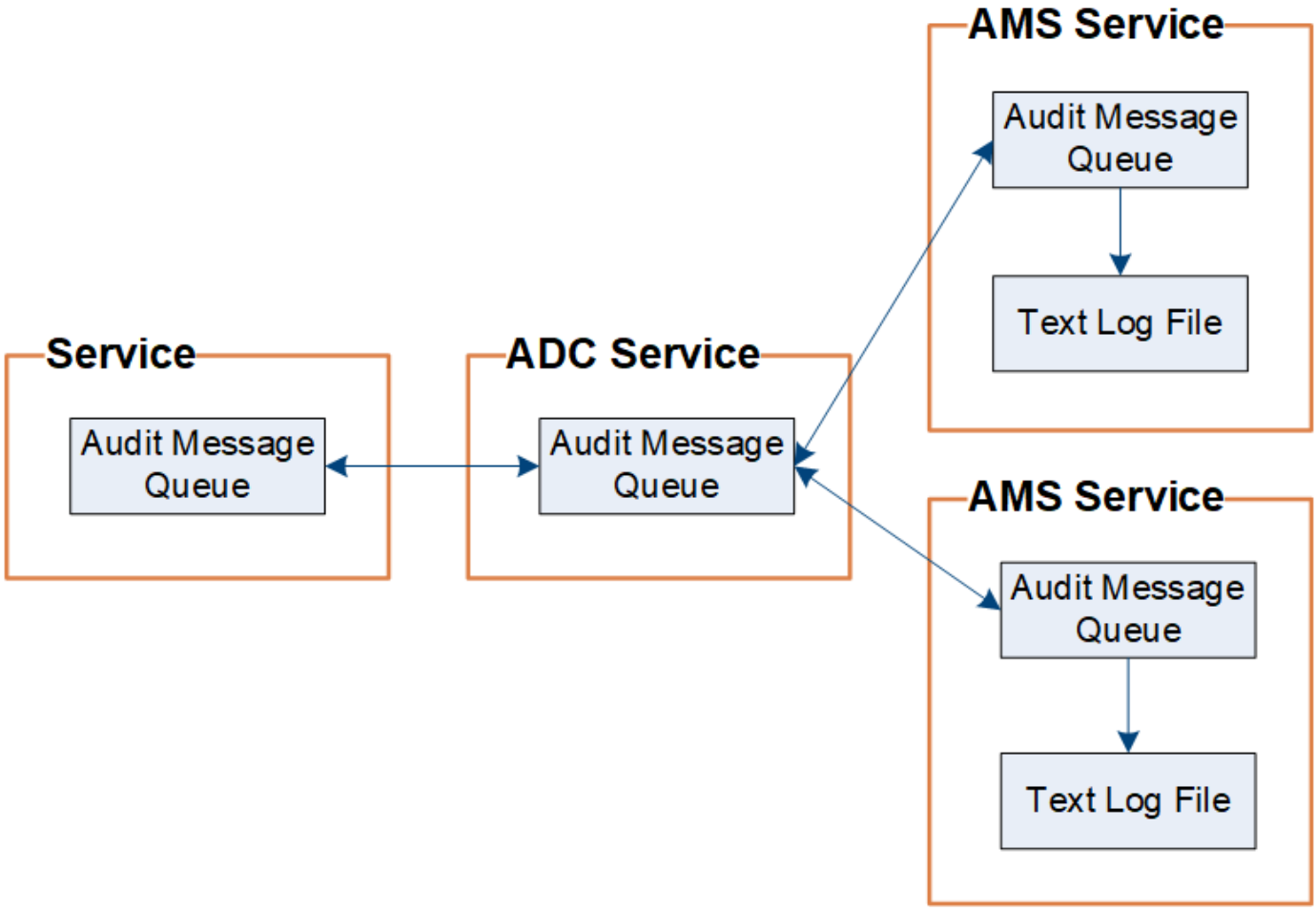
每个管理节点都会将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log`。



审核消息保留

StorageGRID 使用复制和删除过程来确保在将审核消息写入审核日志之前不会丢失任何审核消息。

当节点生成或中继审计消息时，该消息将存储在网格节点系统磁盘上的审计消息队列中。消息的副本始终保存在审计消息队列中，直到该消息被写入管理节点的审计日志文件为止 `/var/local/audit/export`目录。这有助于防止审计消息在传输过程中丢失。



由于网络连接问题或审计容量不足，审计消息队列可能会暂时增加。随着队列的增加，它们会消耗每个节点的更多可用空间 `/var/local/`目录。如果问题仍然存在，并且节点的审计消息目录变得太满，则各个节点将优先处理其积压消息，并暂时无法接收新消息。

具体来说，您可能会看到以下行为：

- 如果 `/var/local/audit/export`管理节点使用的目录已满，管理节点将被标记为无法接收新的审计消息，直到目录不再满为止。 S3 客户端请求不受影响。当审计存储库无法访问时，会触发 XAMS（无法访问的审计存储库）警报。
- 如果 `/var/local/`当具有 ADC 服务的存储节点使用的目录已满 92% 时，该节点将被标记为不可用于审核消息，直到目录仅已满 87% 为止。 S3 客户端对其他节点的请求不受影响。当审计中继无法访问时，会触发 NRLY（可用审计中继）警报。

> 如果没有具有ADC服务的可用存储节点、则存储节点会将审核消息存储在本地文件中 `/var/local/log/localaudit.log`。

- 如果 `/var/local/`当存储节点使用的目录已满 `85%` 时，该节点开始拒绝 `S3` 客户端请求 `503 Service Unavailable`。

以下类型的问题可能会使发生原因 审核消息队列变得非常庞大：

- 管理节点或存储节点使用 ADC-Service 中断的情况。如果系统的一个节点已关闭，则其余节点可能会回记录。

- 超过系统审核容量的持续活动率。
- `/var/local/`ADC存储节点上的空间因与审核消息无关的原因而变满。发生这种情况时，节点将停止接受新的审核消息，并优先处理当前的积压工作，而这可能会使发生原因 回退到其他节点上。

大型审核队列警报和审核消息已排队（**Audit Messages Queued** ， **AMQS** ）警报

为了帮助您监控一段时间内审核消息队列的大小，当存储节点队列或管理节点队列中的消息数量达到特定阈值时，将触发 * 大型审核队列 * 警报和原有 AMQS 警报。

如果触发了 * 大型审核队列 * 警报或原有 AMQS 警报，请首先检查系统上的负载—如果最近发生了大量事务，则警报和警报应随着时间的推移而解决，并且可以忽略。

如果警报或警告持续存在且严重程度增加，请查看队列大小图表。如果该数字在数小时或数天内稳步增加，则审计负载可能已经超出了系统的审计容量。通过将客户端写入和客户端读取的审计级别更改为错误或关闭，降低客户端操作率或减少记录的审计消息数量。看"配置日志管理和外部系统日志服务器" 。

重复的消息

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

从 StorageGRID 管理节点命令行访问审核日志文件

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

这 `audit.log`除非您为 管理节点/本地节点 或 管理节点和外部系统日志服务器 配置StorageGRID ，否则文件保持为空。有关详细信息，请参阅"选择日志位置" 。

开始之前

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

步骤

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

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 转到包含审核日志文件的目录：

   ```
   cd /var/local/audit/export/
   ```
3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

了解 StorageGRID 中的审核日志文件轮换

如果StorageGRID配置为 管理节点/本地节点 或 管理节点和外部系统日志服务器，则审计日志文件将保存到管理节点的 `/var/local/audit/export/`目录。活动审计日志文件被命名为 `audit.log`。

> 或者，您可以更改审计日志的目标并将审计信息发送到外部系统日志服务器。当配置外部系统日志服务器时，将继续生成和存储审计记录的本地日志。请参阅"配置审核消息和外部系统日志服务器"。

每天保存一次活动 `audit.log`文件、并启动一个新 `audit.log`文件。保存文件的名称以格式指示保存时间 `_yyyy-mm-dd.txt_`。如果一天内创建了多个审核日志，则文件名将使用文件的保存日期，并附加一个数字，格式为 `_yyyy-mm-dd.txt.n_`。例如、 `2018-04-15.txt`和 `2018-04-15.txt.1`是在2018年4月15日创建和保存的第一个和第二个日志文件。

一天后，保存的文件被压缩并重命名，格式为 `_yyyy-mm-dd.txt.gz_`，保留原始日期。随着时间的推移，分配给审计日志的管理节点存储空间将被消耗。脚本监控审计日志空间消耗，并根据需要删除日志文件以释放空间 `/var/local/audit/export/`目录。审计日志将根据其创建日期删除。最旧的日志将首先被删除。您可以在以下文件中监视脚本的操作： `/var/local/log/manage-audit.log`。

此示例显示活动 `audit.log`文件、前一天的文件 (`2018-04-15.txt`和前一天的压缩文件 (`2018-04-14.txt.gz`。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

审核日志文件格式

了解 StorageGRID 中审计日志文件的格式

审核日志文件位于每个管理节点上，其中包含一组单独的审核消息。

每个审核消息都包含以下内容：

- 触发审核消息（ATIM ）的事件的协调世界时（ UTC ），格式为 ISO 8601 ，后跟一个空格：

  `_YYYY-MM-DDTHH:MM:SS.UUUUUU_`，其中 `_UUUUUU_` 是微秒。

- 审计消息本身，括在方括号内，以开头 `AUDT`。

以下示例显示了一个审核日志文件中的三条审核消息（为便于阅读，添加了换行符）。这些消息是在租户创建 S3 存储分段并向该存储分段添加两个对象时生成的。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

在默认格式下、审核日志文件中的审核消息不易阅读或解释。您可以使用"Audy-讲解 工具"获取审核日志中审核消息的简化摘要。您可以使用"audy-sum工具"汇总记录了多少写入、读取和删除操作以及这些操作所用时间。

使用 **audit-explain** 工具翻译 **StorageGRID** 审核消息

您可以使用 `audit-explain`工具将审核日志中的审核消息转换为易于阅读的格式。

开始之前

- 您拥有 "特定访问权限"。
- 您必须拥有该 `Passwords.txt`文件。
- 您必须知道主管理节点的 IP 地址。

关于此任务

`audit-explain`主管理节点上提供的工具可在审核日志中提供审核消息的简化摘要。

该 `audit-explain`工具主要供技术支持在故障排除操作期间使用。处理 `audit-explain`查询可能会消耗大量CPU功率、从而可能影响StorageGRID操作。

此示例显示了该工具的典型输出 `audit-explain`。如果帐户ID为92484777680322627870的S3租户使用S3 Put请求创建名为bucket1的分段并向该分段添加三个对象、则会生成这四"SPUT"条审核消息。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

该 `audit-explain`工具可执行以下操作：

- 处理普通或压缩的审核日志。例如：

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- 同时处理多个文件。例如：

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- 接受来自管道的输入、这样您可以使用命令或其他方式筛选和预处理输入 `grep`。例如：

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

由于审核日志可能非常大且解析速度较慢、因此、您可以筛选要查看并运行的部分(而不是整个文件)来节省时间 `audit-explain`。

该 `audit-explain`工具不接受压缩文件作为管道输入。要处理压缩文件、请以命令行参数的形式提供其文件名、或者先使用 `zcat`工具解压缩这些文件。例如：

```
zcat audit.log.gz | audit-explain
```

使用 `help (-h)`选项可查看可用选项。例如：

```
$ audit-explain -h
```

步骤

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

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 输入以下命令，其中 `/var/local/audit/export/audit.log`代表您要分析的文件的名称和位置：

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   该 `audit-explain`工具可打印指定文件中所有消息的可读解释。

   为了缩短线长并提高可读性、默认情况下不会显示时间戳。如果要查看时间戳，请使用timestamp (`-t`(时间戳)选项。

使用 **audit-sum** 工具汇总 **StorageGRID** 审核消息

您可以使用 `audit-sum`工具统计写入、读取、机头和删除审核消息的数量、并查看每种操作类型的最小、最大和平均时间(或大小)。

开始之前

- 您拥有 "特定访问权限"。
- 您已获得 `Passwords.txt`文件。
- 您知道主管理节点的IP地址。

关于此任务

`audit-sum`主管理节点上提供的工具汇总了记录的写入、读取和删除操作的数量以及这些操作所用的时间。

该 `audit-sum`工具主要供技术支持在故障排除操作期间使用。处理 `audit-sum`查询可能会消耗大量CPU功率、从而可能影响StorageGRID操作。

此示例显示了该工具的典型输出 `audit-sum`。此示例显示了协议操作所需的时间。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

这 `audit-sum`该工具为审计日志中的以下 S3 和 ILM 审计消息提供计数和时间。

> 由于功能已被弃用，审计代码已从产品和文档中删除。如果您遇到此处未列出的审计代码，请检查此主题的先前版本以了解较旧的StorageGRID版本。例如， "StorageGRID 11.8 使用审计总和工具" 。

代码	说明	请参见
标识	ILM Initiated Delete ： 记录 ILM 开始删除对象的过程。	"idel ： ILM 已启动删除"
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。	"SDEL ： S3 delete"
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。	"SGET ： S3 GET"
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	"Shea ： S3 机头"
SPUT	S3 PUT ： 记录成功的事务以创建新对象或存储分段。	"SPUT ： S3 PUT"

该 `audit-sum`工具可执行以下操作：

- 处理普通或压缩的审核日志。例如：

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- 同时处理多个文件。例如：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

- 接受来自管道的输入、这样您可以使用命令或其他方式筛选和预处理输入 `grep`。例如：

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> 此工具不接受压缩文件作为管道输入。要处理压缩文件，请将其文件名作为命令行参数提供，或使用 `zcat`工具先解压缩文件。例如：
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

您可以使用命令行选项将存储分段上的操作与对象上的操作分开进行汇总，或者按存储分段名称，时间段或目标类型对消息摘要进行分组。默认情况下、摘要会显示最小、最大和平均操作时间、但您可以改用 `size (-s)`选项查看对象大小。

使用 `help (-h)`选项可查看可用选项。例如：

```
$ audit-sum -h
```

步骤

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

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 如果要分析与写入，读取，磁头和删除操作相关的所有消息，请执行以下步骤：
   a. 输入以下命令，其中 `/var/local/audit/export/audit.log`代表您要分析的文件的名称和位置：

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      此示例显示了该工具的典型输出 `audit-sum`。此示例显示了协议操作所需的时间。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

在此示例中， SGET （ S3 GET ）操作的平均速度最慢，为 1.13 秒，但 SGET 和 SPUT （ S3 PUT ）操作的最坏情况时间都较长，约为 1 ， 770 秒。

b. 要显示最慢的10个检索操作，请使用grep命令仅选择SGET消息并添加长输出选项(`-l`()以包括对象路径：

```
grep SGET audit.log | audit-sum -l
```

结果包括类型（对象或分段）和路径，您可以通过此类结果在审核日志中添加与这些特定对象相关的其他消息。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
在此示例输出中，您可以看到，三个最慢的 S3 GET 请求针对的是大小约为 5 GB 的对象，该大小远远大于其他对象。大容量导致最差情况检索时间较慢。

3. 如果要确定要从网格中插入和检索的对象的大小，请使用size选项(`-s`)：

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

在此示例中， SPUT 的平均对象大小小于 2.5 MB ，但 SGET 的平均大小要大得多。SPUT 消息的数量远远高于 SGET 消息的数量，这表明大多数对象永远不会被检索到。

4. 如果要确定昨天的检索速度是否较慢：

   a. 在相应的审核日志上发出命令，并使用group-by－time选项(`-gt`，然后是时间段(例如，15M、1H、10S)：

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

这些结果表明，S3 GET 流量在 06:00 至 07:00 之间出现峰值。在此时间跨度内，最大时间和平均时间都相当高，并且它们并没有随着计数的增加而逐渐增加。这些指标表明容量可能超出了范围，可能是网络或电网处理请求的能力超出了范围。

b. 要确定昨天每小时检索到的对象大小，请将size选项(`-s`()添加到命令中：

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group            count       min(B)          max(B)
average(B)
  =============            =====     ========        ========
============
  2019-09-05T00             7591        0.040        1481.867
1.976
  2019-09-05T01             4173        0.043        1740.290
2.062
  2019-09-05T02            20142        0.083        1274.961
2.303
  2019-09-05T03            57591        0.912        1383.867
1.182
  2019-09-05T04           124171        0.730        1740.290
1.528
  2019-09-05T05           420182        0.875        4274.511
2.398
  2019-09-05T06          1220371        0.691  5663711385.961
51.328
  2019-09-05T07           527142        0.130        1974.228
2.147
  2019-09-05T08           384173        0.625        1740.290
1.878
  2019-09-05T09            27591        0.689        1481.867
1.354
```

这些结果表明，当整体检索流量达到最大值时，会发生一些非常大的检索。

c. 要查看更多详细信息、请使用查看该时段的"Audy-讲解 工具"所有SGET操作：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

如果grep命令的输出应包含多行、请添加该 `less`命令以一次显示一页(一屏)审核日志文件的内容。

5. 如果要确定存储分段上的 SPUT 操作是否比对象的 SPUT 操作慢：

a. 首先使用 `-go`选项、该选项将对象操作和存储分段操作的消息分开分组：

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

结果显示，存储分段的 SPUT 操作与对象的 SPUT 操作具有不同的性能特征。

b. 要确定哪些分段的SPUT操作速度最慢、请使用 `-gb`选项、该选项会按分段对消息进行分组：

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. 要确定哪些分段具有最大的SPUT对象大小、请同时使用 `-gb`和 `-s`选项：

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

审核消息格式

了解 **StorageGRID** 审核消息的结构

在 StorageGRID 系统中交换的审核消息包括所有消息通用的标准信息以及描述所报告事件或活动的特定内容。

如果和"审计和"工具提供的摘要信息"审核说明"不足、请参阅本节了解所有审核消息的常规格式。

下面是可能显示在审核日志文件中的审核消息示例：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

每个审核消息都包含一个属性元素字符串。整个字符串用方括号括起来(`[ ]`)，字符串中的每个属性元素都具有以下特征：

- 括在方括号中 `[ ]`
- 由字符串引入 `AUDT`，表示审核消息
- 前后不带分隔符（无逗号或空格）
- 由换行符终止 `\n`

每个元素都包含一个属性代码，一个数据类型以及一个以以下格式报告的值：

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

消息中的属性元素数量取决于消息的事件类型。属性元素不会按任何特定顺序列出。

以下列表介绍了这些属性元素：

- `ATTR`是所报告属性的四字符代码。某些属性对于所有审核消息都是通用的，而其他属性则针对事件。
- `type`是值的编程数据类型（例如UI64、FC32等）的四字符标识符。类型用圆括号括起 `( )`。
- `value`是属性的内容、通常是数字或文本值。值始终跟在冒号后面（:`）。数据类型CStr的值由双引号""括起来。

StorageGRID 审核消息中的数据类型

使用不同的数据类型将信息存储在审核消息中。

键入	说明
UI32	无符号长整数（ 32 位）；它可以存储 0 到 4 ， 294 ， 967 ， 295 之间的数字。
UI64	无符号双长整数（ 64 位）；它可以存储 0 到 18 ， 446 ， 744 ， 073 ， 709 ， 551 ， 615 之间的数字。
FC32	四字符常量；32位无符号整数值、表示为四个ASCII字符、例如"ABCD"。
iPad	用于 IP 地址。
CStr	长度可变的UTF-8字符数组。可以按照以下约定对字符进行转义： • 反斜杠为 \\ 。 • 回车符为 • 双引号为 " 。 • 换行符（新行）为 • 字符可以替换为其十六进制等效项（格式为 \xHH ，其中 HH 是表示该字符的十六进制值）。

StorageGRID 审核消息中的事件特定数据

审核日志中的每个审核消息都会记录特定于系统事件的数据。

在标识消息本身的打开容器之后 `[AUDT:`、下一组属性将提供有关审核消息所述事件或操作的信息。以下示例突出显示了这些属性：

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

`ATYP`元素(在示例中带下划线)用于标识生成消息的事件。此示例消息包括link:shea-s3-head.html["Shea"]消息代码([ATYP (FC32)： Shea])、表示它是由成功的S3机头请求生成的。

StorageGRID 审核消息中的常见元素

所有审核消息都包含通用要素。

代码	键入	说明
在中	FC32	模块ID：生成消息的模块ID的四字符标识符。这表示生成审核消息的代码段。
ANID	UI32	Node ID ： 分配给生成消息的服务的网格节点 ID 。在配置和安装 StorageGRID 系统时，系统会为每个服务分配一个唯一的标识符。无法更改此ID。
ASE	UI64	审核会话标识符：在先前版本中，此元素表示在服务启动后初始化审核系统的时间。此时间值是自操作系统时代(1970年1月1日00：00：00 UTC)以来以微秒为单位测量的。 • 注： * 此元素已废弃，不再显示在审核消息中。
ASQN	UI64	序列计数：在先前版本中，对于网格节点（ ANID ）上生成的每个审核消息，此计数器会递增，并在服务重新启动时重置为零。 • 注： * 此元素已废弃，不再显示在审核消息中。
Atid	UI64	跟踪 ID ： 由单个事件触发的一组消息共享的标识符。

代码	键入	说明
Atim	UI64	时间戳：生成触发审核消息的事件的时间、以操作系统发生后(1970年1月1日00：00：00 UTC)微秒为单位。请注意，用于将时间戳转换为本地日期和时间的大多数可用工具均以毫秒为基础。 可能需要对记录的时间戳进行舍入或截断。文件中审核消息开头显示的可供用户读取的时间 `audit.log`是ISO 8601格式的ATIM属性。日期和时间表示为，其中是表示 `*YYYY-MMDDTHH:MM:SS.UUUUUU*`日期时间段开始的 `T`文字字符串字符。 `*UUUUUU*`微秒。
ATYP	FC32	Event Type：要记录的事件的四字符标识符。这将控制消息的 " 有效负载 " 内容：包含的属性。
保护程序	UI32	version ： 审核消息的版本。随着 StorageGRID 软件的发展，新版本的服务可能会在审核报告中加入新功能。通过此字段，可以在 AMS 服务中实现向后兼容性，以处理来自旧版本服务的消息。
RSLT	FC32	result ： 事件，进程或事务的结果。如果与消息无关，则不会使用 none 而不是 SUC ，这样就不会意外筛选该消息。

StorageGRID 审核消息格式和示例

您可以在每个审核消息中找到详细信息。所有审核消息都使用相同的格式。

以下是可能显示在文件中的审核消息示例 `audit.log`：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

审核消息包含有关所记录事件的信息以及有关审核消息本身的信息。

要确定审核消息记录的事件，请查找 ATYP 属性（突出显示在下方）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性的值为 SPUT 。"SPUT"表示S3 Put事务、该事务会将对象的写入记录到存储分段中。

以下审核消息还会显示与对象关联的存储分段：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

要发现 PUT 事件发生的时间，请注意审核消息开头的通用协调时间（ UTC ）时间戳。此值是审核消息本身的ATIM属性的可读版本：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

Atim 会以微秒为单位记录自 UNIX Epoch 开始以来的时间。在此示例中、此值 `1405631878959669`转换为2014年7月17日星期四21：17：59 UTC。

审核消息和对象生命周期

在 **StorageGRID** 中生成审核消息时

每次载入，检索或删除对象时都会生成审核消息。您可以通过查找S3 API专用的审核消息在审核日志中确定这些事务。

审核消息通过每个协议专用的标识符进行链接。

协议	代码
链接 S3 操作	S3BK (铲斗)、S3KY (钥匙)或两者
链接内部操作	CBID (对象的内部标识符)

审核消息的时间

由于网格节点之间的时间差异，对象大小和网络延迟等因素，不同服务生成的审核消息的顺序可能与本节示例中所示的顺序不同。

StorageGRID 中对象摄取事务的审核消息

您可以通过查找S3 API专用的审核消息来在审核日志中确定客户端加载事务。

下表并未列出摄取事务期间生成的所有审计消息。仅包含跟踪摄取事务所需的消息。

S3 载入审核消息

代码	名称	说明	跟踪	请参见
SPUT	S3 PUT 事务	S3 PUT 载入事务已成功完成。	CBID ，S3BK ，S3KY	"SPUT： S3 PUT"
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	"ORLM： 符合对象规则"

示例： **S3** 对象载入

下面的一系列审核消息是在 S3 客户端将对象载入存储节点（ LDR 服务）时生成并保存到审核日志中的审核消息的示例。

在此示例中、活动ILM策略包括"创建2个副本"ILM规则。

> 在以下示例中并未列出事务期间生成的所有审核消息。仅列出与 S3 载入事务（ SPUT ）相关的那些。

此示例假设先前已创建 S3 存储分段。

SPUT： S3 PUT

此时将生成 SPUT 消息，以指示已发出 S3 PUT 事务，以便在特定存储分段中创建对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM： 符合对象规则

ORLM 消息指示已对此对象满足 ILM 策略要求。此消息包含对象的 CBID 以及应用的 ILM 规则的名称。

对于复制的对象， " LOC" 字段包含对象位置的 LDR 节点 ID 和卷 ID 。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

对于纠删编码对象、LOCS字段包括纠删编码配置文件ID和纠删编码组ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

PATH 字段包含 S3 存储桶和密钥信息。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

StorageGRID 中对象删除事务的审核消息

您可以通过查找S3 API专用的审核消息来确定审核日志中的对象删除事务。

下表列出了在删除事务期间生成的并非所有审核消息。仅包含跟踪删除事务所需的消息。

S3 删除审核消息

代码	名称	说明	跟踪	请参见
SDEL	S3 删除	请求从存储分段中删除对象。	CBID ，S3KY	"SDEL： S3 delete"

示例： **S3** 对象删除

当 S3 客户端从存储节点（ LDR 服务）中删除对象时，系统会生成一条审核消息并将其保存到审核日志中。

> 在删除事务期间生成的审核消息并非都在以下示例中列出。仅列出与 S3 删除事务（ SDEL ）相关的那些。

SDEL： S3 删除

当客户端向LDR服务发送DeleteObject请求时、对象删除开始。此消息包含用于删除对象的存储分段以及用于标识对象的 S3 密钥。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

StorageGRID 中对象检索事务的审核消息

您可以通过查找S3 API专用的审核消息来确定审核日志中的对象检索事务。

下表并未列出检索事务期间生成的所有审计消息。仅包含跟踪检索事务所需的消息。

S3 检索审核消息

代码	名称	说明	跟踪	请参见
SGET	S3 GET	请求从存储分段中检索对象。	CBID ， S3BK ， S3KY	"SGET： S3 GET"

示例： **S3** 对象检索

当 S3 客户端从存储节点（ LDR 服务）检索对象时，系统会生成一条审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 检索事务（ SGET ）相关的那些。

SGET： S3 GET

当客户端向LDR服务发送GetObject请求时、对象检索开始。此消息包含用于检索对象的存储分段以及用于标识对象的 S3 密钥。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

如果存储分段策略允许，客户端可以匿名检索对象，或者从其他租户帐户拥有的存储分段中检索对象。审核消息包含有关存储分段所有者的租户帐户的信息，以便您可以跟踪这些匿名请求和跨帐户请求。

在以下示例消息中、客户端针对存储在非其所有存储分段中的对象发送GetObject请求。SBAI 和 SBAC 的值会记录存储分段所有者的租户帐户 ID 和名称，这与 S3AI 和 SACC 中记录的租户帐户 ID 和客户端名称不同。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

示例：对象上的 **S3 Select**

当 S3 客户端对某个对象发出 S3 Select 查询时，系统会生成审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 Select 事务（ SelectObjectContent ）相关的那些内容。

每个查询都会生成两条审核消息：一条用于授权S3 Select请求(S3SR字段设置为"Select")、另一条用于在处理期间从存储中检索数据的后续标准GET操作。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

StorageGRID 中 **S3** 对象元数据更新的审核消息

当 S3 客户端更新对象的元数据时，系统会生成审核消息。

S3 元数据更新审核消息

代码	名称	说明	跟踪	请参见
SUPD	已更新 S3 元数据	当 S3 客户端更新已载入对象的元数据时生成。	CBID，S3KY，HTRH	"SUPD： 已更新 S3 元数据"

示例： **S3** 元数据更新

此示例显示了更新现有 S3 对象的元数据的成功事务。

SUPD： S3 元数据更新

S3 客户端发出请求 (SUPD)，以更新 S3 对象 (S3KY) 的指定元数据(`x-amz-meta-*`。

在此示例中，请求标头包含在 HTRH 字段中，因为它已配置为审核协议标头（**Configuration** > **Monitoring** > **Audit and syslog server**）。请参阅 "配置日志管理和外部系统日志服务器"。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

审核消息

了解 **StorageGRID** 中的审计消息类型和代码

以下各节列出了系统返回的审核消息的详细说明。每个审核消息首先列在一个表中，该表按相关消息所代表的活动类别对相关消息进行分组。这些分组对于了解要审核的活动类型以及选择所需的审核消息筛选类型都很有用。

审核消息也会按其四个字符的代码的字母顺序列出。通过此字母列表、您可以查找有关特定消息的信息。

本章中使用的四字符代码是在审核消息中找到的ATYP值，如以下示例消息所示：

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

有关设置审计消息级别、更改日志目标以及使用外部系统日志服务器存储审计信息的信息，请参阅"配置日志管理和外部系统日志服务器"

审核消息类别

属于系统审核类别的审核消息用于与审核系统本身、网格节点状态、系统范围任务活动(网格任务)和服务备份操作相关的事件。

代码	消息标题和问题描述	请参见
ECMC	缺失经过删除编码的数据片段：表示检测到缺失经过删除编码的数据片段。	"ECMC：缺少经过Erasure编码的数据片段"
ECOC	经删除编码的数据片段已损坏：表示检测到经删除编码的数据片段已损坏。	"EECO：经过Erasure编码的数据片段已损坏"
ETAF	安全身份验证失败：尝试使用传输层安全（ Transport Layer Security ， TLS ）进行连接失败。	"ETAF ： 安全身份验证失败"
GNRG	GNDS 注册：服务在 StorageGRID 系统中更新或注册了有关自身的信息。	"GNRG ： GNDS 注册"
GNUR	GNDS 注销：服务已从 StorageGRID 系统中注销自身。	"GN-R ： GNDS 注销"
GTED	网格任务已结束： CMN 服务已完成网格任务的处理。	"GTed ： 网格任务已结束"
GTSt	网格任务已启动： CMN 服务已开始处理网格任务。	"GTST ： 已启动网格任务"
GTSU	已提交网格任务：已将网格任务提交到 CMN 服务。	"GTSU ： 已提交网格任务"
LLST	Location Lost ： 当某个位置丢失时，会生成此审核消息。	"LLST ： 位置丢失"
OLST	对象丢失：无法在 StorageGRID 系统中找到请求的对象。	"OLST ： 系统检测到丢失对象"
Sadd	禁用安全审核：已关闭审核消息日志记录。	"Sadd ： 禁用安全审核"
Sade	启用安全审核：审核消息日志记录已还原。	"Sade ： 启用安全审核"
SVRF	对象存储验证失败：内容块验证检查失败。	"SVRF ： 对象存储验证失败"
SVRU	对象存储验证未知：在对象存储中检测到意外的对象数据。	"SVRU ： 对象存储验证未知"

代码	消息标题和问题描述	请参见
系统	节点停止：已请求关闭。	"SYSD ： 节点停止"
系统	节点停止：服务已正常停止。	"Syst ： 节点正在停止"
系统	节点启动：服务已启动；消息中显示了上次关闭的性质。	"SYSU ： 节点启动"

StorageGRID 中对象存储事件的审核消息

属于对象存储审核类别的审核消息用于与StorageGRID 系统中的对象存储和管理相关的事件。其中包括对象存储和检索，网格节点到网格节点的传输以及验证。

由于功能已弃用、因此从产品和文档中删除了审核代码。如果遇到此处未列出的审核代码、请查看此主题的先前版本以了解早期SG版本。例如， "StorageGRID 11.8.对象存储审核消息"。

代码	说明	请参见
运动内衣	存储分段只读请求：存储分段已进入或退出只读模式。	"BROR：存储分段只读请求"
CBSE	对象发送结束：源实体完成了网格节点到网格节点的数据传输操作。	"CBSE ： 对象发送结束"
CBRE	对象接收结束：目标实体完成了网格节点到网格节点的数据传输操作。	"CBRE ： 对象接收结束"
CRR	跨网格复制请求：StorageGRID 尝试执行跨网格复制操作、以便在网格联合连接中的分段之间复制对象。	"CGRR：跨网格复制请求"
EBDL	清空存储分段删除：ILM扫描程序删除存储分段中正在删除所有对象的对象(执行空存储分段操作)。	"EBDL：清空存储分段删除"
EBKR	空分段请求：用户发送了打开或关闭空分段的请求(即删除分段对象或停止删除对象)。	"EBKR：空分段请求"
SCMT	对象存储提交：内容块已完全存储和验证，现在可以请求。	"SCMT：对象存储提交请求"
Srem	对象存储删除：已从网格节点中删除内容块，无法再直接请求。	"Srem ： 对象存储删除"

StorageGRID 中客户端读取操作的审核消息

当S3客户端应用程序请求检索对象时、系统会记录客户端读取审核消息。

代码	说明	使用人	请参见
S3SL	S3 Select请求：在S3 Select请求返回到客户端后记录完成。S3SL消息可以包括错误消息和错误代码详细信息。此请求可能未成功。	S3 客户端	"S3SL：S3选择请求"
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	"SGET ： S3 GET"
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	S3 客户端	"Shea ： S3 机头"

StorageGRID 中客户端写入操作的审核消息

当S3客户端应用程序请求创建或修改对象时、系统会记录客户端写入审核消息。

代码	说明	使用人	请参见
OVWR	对象覆盖：记录一个事务，以便使用另一个对象覆盖一个对象。	S3 客户端	"OVWR ： 对象覆盖"
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	"SDEL ： S3 delete"
SPOS	S3 POST ： 记录将对象从 AWS Glacier 存储还原到云存储池的成功事务。	S3 客户端	"SPOS ： S3 POST"
SPUT	S3 PUT ： 记录成功的事务以创建新对象或存储分段。 • 注： * 如果事务对子资源执行操作，则审核消息将包含字段 S3SR 。	S3 客户端	"SPUT ： S3 PUT"
SUPD	S3 元数据已更新：记录成功的事务以更新现有对象或存储分段的元数据。	S3 客户端	"SUPD ： 已更新 S3 元数据"

StorageGRID 管理审核消息

" 管理 " 类别可将用户请求记录到管理 API 。

代码	消息标题和问题描述	请参见
MGAU	Management API 审核消息：用户请求日志。	"MGAU ： 管理审核消息"

StorageGRID ILM 审核消息

属于ILM审核类别的审核消息用于与信息生命周期管理(ILM)操作相关的事件。

代码	消息标题和问题描述	请参见
标识	ILM Initiated Delete ： 当 ILM 开始删除对象的过程时，会生成此审核消息。	"idel ： ILM 已启动删除"
LKCU	已覆盖对象清理。自动删除已覆盖的对象以释放存储空间时会生成此审核消息。	"LKCU ： 覆盖对象清理"
ORLM	满足对象规则：在按照ILM规则指定的方式存储对象数据时、将生成此审核消息。	"ORLM ： 符合对象规则"

审核消息参考

StorageGRID 中存储桶只读请求的 BROR 审核消息

当存储分段进入或退出只读模式时、LDR服务会生成此审核消息。例如、删除所有对象时、存储分段将进入只读模式。

代码	字段	说明
BKHD	存储分段UUID	分段标识。
BROV	存储分段只读请求值	存储分段是设置为只读状态还是保持只读状态(1 =只读、0 =非只读)。
Bros.	存储分段只读原因	将存储分段设为只读或保持只读状态的原因。例如、emptyBucket.
S3AI	S3租户帐户ID	发送请求的租户帐户的ID。空值表示匿名访问。
S3BK	S3存储分段	S3 存储分段名称。

StorageGRID 中对象接收开始的 CBRB 审核消息

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，目标实体会发出此消息。

代码	字段	说明
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。
CTES	预期结束序列计数	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS ： 已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从 " 开始序列计数 " 到 " 预期结束序列计数 " 请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

StorageGRID 中对象接收结束的 **CBRE** 审核消息

内容块从一个节点传输到另一个节点完成后，此消息将由目标实体发出。

代码	字段	说明
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。

代码	字段	说明
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。
RSLT	传输结果	传输操作的结果（从发送实体的角度来看）： SUC ： 传输成功完成；已发送请求的所有序列计数。 CONL ： 传输期间连接丢失 CTMO： 建立或传输期间连接超时 UNDE ： 无法访问目标节点 ID CRPT：由于接收到损坏或无效数据、传输已结束

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 " 。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

StorageGRID 中对象发送开始的 **CBSB** 审核消息

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，源实体会发出此消息。

代码	字段	说明
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。

代码	字段	说明
CTES	预期结束序列计数	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS ： 已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从 " 开始序列计数 " 到 " 预期结束序列计数 " 请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

StorageGRID 中对象发送结束的 **CBSE** 审核消息

在将内容块从一个节点传输到另一个节点后，源实体会发出此消息。

代码	字段	说明
CNID	连接标识符	节点到节点会话 / 连接的唯一标识符。
CBID	内容块标识符	要传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉启动： push ： 发送实体请求传输操作。 Pull ： 接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID 。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID 。
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。

代码	字段	说明
RSLT	传输结果	传输操作的结果（从发送实体的角度来看）： SUC ： 传输成功完成；已发送请求的所有序列计数。 CONL ： 传输期间连接丢失 CTMO： 建立或传输期间连接超时 UNDE ： 无法访问目标节点 ID CRPT：由于接收到损坏或无效数据、传输已结束

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 " 。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

StorageGRID 中跨网格复制请求的 **CGRR** 审核消息

当StorageGRID 尝试跨网格复制操作在网格联盟连接中的分段之间复制对象时、将生成此消息。

代码	字段	说明
CSIZ	对象大小	对象的大小（以字节为单位）。 StorageGRID 11.8.因此、跨网格复制请求(从StorageGRID 11.7升级到11.8)可能具有不准确的总对象大小。
S3AI	S3租户帐户ID	拥有从中复制对象的存储分段的租户帐户的ID。
GFID	网格联合连接ID	用于跨网格复制的网格联合连接的ID。
工序	CGR操作	尝试的跨网格复制操作的类型： • 0 = Replicate对象 • 1 =重复多部分对象 • 2= Replicate delete标记
S3BK	S3存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。
VSID	版本ID	正在复制的对象的特定版本的版本ID。

代码	字段	说明
RSLT	结果代码	返回成功(SUC)或一般错误(ERR)。

StorageGRID 中空存储桶对象删除的 **EBDL** 审核消息

ILM扫描程序删除了存储分段中正在删除所有对象的对象(执行空存储分段操作)。

代码	字段	说明
CSIZ	对象大小	对象的大小（以字节为单位）。
路径	S3存储分段/密钥	S3存储分段名称和S3密钥名称。
SEGC	容器UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
RSLT	删除操作的结果	事件、流程或事务的结果。如果与消息无关，则不会使用 none 而不是 SUC ，这样就不会意外筛选该消息。

StorageGRID 中空存储桶请求的 **EBKR** 审核消息

此消息指示用户发送了打开或关闭空存储分段的请求(即删除存储分段对象或停止删除对象)。

代码	字段	说明
BUID	存储分段UUID	分段标识。
EBJS	空存储分段JSON配置	包含表示当前空分段配置的JSON。
S3AI	S3租户帐户ID	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。

StorageGRID 中缺失纠删码数据的 **ECMC** 审计消息

此审核消息指示系统检测到缺少经过纠删编码的数据片段。

代码	字段	说明
VCMC	VCS ID	包含缺少的块的 VCS 的名称。

代码	字段	说明
MCID	区块 ID	缺少纠删编码片段的标识符。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

StorageGRID 中损坏的纠删编码数据的 **ECOC** 审核消息

此审核消息指示系统检测到经过纠删编码的数据片段已损坏。

代码	字段	说明
VCCO	VCS ID	包含损坏区块的 VCS 的名称。
VLID	Volume ID	包含损坏的纠删编码片段的 RangeDB 卷。
CCID	区块 ID	已损坏的纠删编码片段的标识符。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

StorageGRID 中安全身份验证失败的 **ETAF** 审核消息

如果尝试使用传输层安全（ Transport Layer Security ， TLS ）进行连接失败，则会生成此消息。

代码	字段	说明
CNID	连接标识符	身份验证失败的 TCP/IP 连接的唯一系统标识符。
RID	用户身份	表示远程用户身份的服务相关标识符。

代码	字段	说明
RSLT	原因代码	失败的原因： SCNI ： 安全连接建立失败。 CERM ： 证书缺失。 证书：证书无效。 cere ： 证书已过期。 CERR ： 证书已撤销。 CSGN ： 证书签名无效。 CSGU ： 证书签名者未知。 UCRM ： 缺少用户凭据。 UCRI ： 用户凭据无效。 UCRU ： 不允许使用用户凭据。 tout ： 身份验证超时。

在与使用 TLS 的安全服务建立连接后，系统会使用 TLS 配置文件和服务中内置的其他逻辑来验证远程实体的凭据。如果此身份验证因证书或凭据无效，意外或不允许而失败，则会记录审核消息。这样可以查询未经授权的访问尝试以及其他与安全相关的连接问题。

此消息可能是由于远程实体的配置不正确或尝试向系统提供无效或不允许的凭据而导致的。应监控此审核消息，以检测未经授权访问系统的尝试。

StorageGRID 中 GNDS 注册的 GNRG 审核消息

如果某个服务在 StorageGRID 系统中更新或注册了有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	说明
RSLT	结果	更新请求的结果： • SUC ： 成功 • SUNV ： 服务不可用 • GERR ： 其他故障
GNID	节点ID	启动更新请求的服务的节点 ID 。
GNTP	设备类型	网格节点的设备类型（例如 LDR 服务的 BLDR ）。

代码	字段	说明
GNDV	设备型号版本	标识 DMDL 捆绑包中网格节点设备型号版本的字符串。
GNGP	组	网格节点所属的组（在链路成本和服务查询排名环境中）。
GNIA	IP 地址	网格节点的 IP 地址。

每当网格节点更新其在网格节点包中的条目时，都会生成此消息。

StorageGRID 中 GNDS 注销的 GNUR 审核消息

如果某个服务已从 StorageGRID 系统中取消注册有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	说明
RSLT	结果	更新请求的结果： • SUC ： 成功 • SUNV ： 服务不可用 • GERR ： 其他故障
GNID	节点ID	启动更新请求的服务的节点 ID 。

StorageGRID 中已结束网格任务的 GTED 审核消息

此审核消息表示 CMN 服务已完成指定网格任务的处理，并已将此任务移至历史表。如果结果为 SUC ， ABRT 或 Rolf ，则会显示相应的 Grid Task Started 审核消息。其他结果表明，此网格任务的处理从未开始。

代码	字段	说明
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在整个生命周期内对网格任务进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。

代码	字段	说明
RSLT	结果	网格任务的最终状态结果： • SUC ： 已成功完成网格任务。 • ABRT：网格任务已终止、但未发生回滚错误。 • Rolf：网格任务已终止、无法完成回滚过程。 • 取消：用户在启动网格任务之前已取消此任务。 • expr ： 网格任务在启动之前已过期。 • IVLD ： 网格任务无效。 • auth ： 未授权网格任务。 • DUPL ： 网格任务被拒绝为重复项。

StorageGRID 中已启动网格任务的 **GTST** 审核消息

此审核消息指示 CMN 服务已开始处理指定的网格任务。对于由内部网格任务提交服务启动并选择自动激活的网格任务，审核消息会紧跟在网格任务提交消息之后。对于提交到 "Pending" 表中的网格任务，用户启动网格任务时会生成此消息。

代码	字段	说明
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在任务的整个生命周期内对其进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	结果。此字段只有一个值： • SUC ： 已成功启动网格任务。

StorageGRID 中已提交网格任务的 **GTSU** 审核消息

此审核消息表示已将网格任务提交到 CMN 服务。

代码	字段	说明
SID	任务 ID	唯一标识生成的网格任务，并允许在整个生命周期内对该任务进行管理。 • 注意： * 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下， " 任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
TTYP	任务类型	网格任务的类型。

代码	字段	说明
版本	任务版本	指示网格任务版本的数字。
TDSC	任务问题描述	网格任务的用户可读问题描述 。
VAT	在时间戳之后有效	网格任务最早有效的时间（从 1970 年 1 月 1 日开始的 UINT64 微秒 - UNIX 时间）。
Vbts	在时间戳之前有效	网格任务有效的最新时间（从 1970 年 1 月 1 日开始的 UINT64 微秒 - UNIX 时间）。
TRC	源	任务源： • TXTB ： 网格任务是以签名文本块的形式通过 StorageGRID 系统提交的。 • 网格：网格任务是通过内部网格任务提交服务提交的。
ACTV	激活类型	激活类型： • Auto ： 已提交网格任务以自动激活。 • PEND ： 网格任务已提交到待定表中。这是 TXTB 源的唯一可能性。
RSLT	结果	提交结果： • SUC ： 已成功提交网格任务。 • fail ： 任务已直接移至历史表。

StorageGRID 中 **ILM** 启动删除的 **IDEL** 审核消息

ILM 开始删除对象时会生成此消息。

在以下任一情况下都会生成 idel 消息：

- * 对于合规 S3 存储分段中的对象 * ： 当 ILM 开始自动删除对象的过程时，系统会生成此消息，因为该对象的保留期限已过期（假设已启用自动删除设置且已关闭合法保留）。
- 适用于不合规**S3**存储分段中的对象。当ILM开始删除对象时、会生成此消息、因为活动ILM策略中当前没有应用于对象的放置指令。

代码	字段	说明
CBID	内容块标识符	对象的 CBID 。
CMPA	合规性：自动删除	仅适用于合规 S3 存储分段中的对象。0 （ false ）或 1 （ true ），指示合规对象在保留期限结束时是否应自动删除，除非分段处于合法保留状态。

代码	字段	说明
Cmpl	合规性：法律保留	仅适用于合规 S3 存储分段中的对象。0 （ false ）或 1 （ true ），指示存储分段当前是否处于合法保留状态。
CMPR	合规性：保留期限	仅适用于合规 S3 存储分段中的对象。对象保留期限的长度，以分钟为单位。
CTME	合规性：载入时间	仅适用于合规 S3 存储分段中的对象。对象的载入时间。您可以将保留期限（以分钟为单位）添加到此值，以确定何时可以从存储分段中删除对象。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID 。存储分段上的操作不包括此字段。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOC	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 "" 。 CEC：对于纠删编码对象、应用于对象数据的纠删编码配置文件ID和纠删编码组ID。 CLDI ： 对于复制的对象， LDR 节点 ID 和对象位置的卷 ID 。 CLNL ： 归档对象数据时对象位置的弧节点 ID 。
路径	S3存储分段/密钥	S3存储分段名称和S3密钥名称。
RSLT	结果	ILM 操作的结果。 SUC ： ILM 操作成功。
规则	规则标签	• 如果合规 S3 存储分段中的某个对象因其保留期限已过期而被自动删除，则此字段为空。 • 如果由于当前没有其他应用于对象的放置指令而删除对象，则此字段将显示应用于对象的最后一个 ILM 规则的可读标签。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	已删除对象的特定版本的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

StorageGRID 中覆盖对象清理的 **LKCU** 审核消息

如果 StorageGRID 删除了先前需要清理以释放存储空间的已覆盖对象，则会生成此消息。当S3客户端将对象写入已包含对象的路径时、对象将被覆盖。删除过程会自动在后台进行。

代码	字段	说明
CSIZ	内容大小	对象的大小（以字节为单位）。
LTYP	清理类型	_ 仅供内部使用。 _
LUID	已删除对象 UUID	已删除的对象的标识符。
路径	S3存储分段/密钥	S3存储分段名称和S3密钥名称。
SEGC	容器UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
UUID	通用唯一标识符	仍存在的对象的标识符。只有在尚未删除对象时，此值才可用。

StorageGRID 中泄漏对象清理的 **LKDM** 审计消息

清除或删除泄漏的区块后会生成此消息。区块可以是复制的对象的一部分、也可以是经过erasure编码的对象的一部分。

代码	字段	说明
Cloc	区块位置	已删除的泄漏区块的文件路径。

CTYP	区块类型	区块类型：
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

代码	字段	说明

LTYP	泄漏类型	可以检测到的五种泄漏类型：
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

Ctim	区块创建时间	创建泄漏块的时间。
UUID	通用唯一标识符	区块所属对象的标识符。
CBID	内容块标识符	泄漏块所属对象的CBID。
CSIZ	内容大小	区块的大小(以字节为单位)。

StorageGRID 中丢失对象副本位置的 **LLST** 审核消息

每当找不到对象副本(已复制或经过删除编码)的位置时、都会生成此消息。

代码	字段	说明
CBIL	CBID	受影响的 CBID 。
ECPR	纠删编码配置文件	用于经过擦除编码的对象数据。所用纠删编码配置文件的ID。
LTYP	位置类型	CLDI （联机）：用于复制的对象数据 CLEC （联机）：用于经过纠删编码的对象数据 CLNL （近线）：用于归档复制的对象数据
NOID	源节点 ID	丢失位置的节点 ID 。

代码	字段	说明
PCLD	复制对象的路径	丢失对象数据的磁盘位置的完整路径。仅当 LTYP 的值为 CLDI （即，对于复制的对象）时才返回。 采取形式 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	结果	始终为无。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。
TRC	触发源	User ： 用户触发 Syst ： 系统已触发
UUID	通用唯一 ID	StorageGRID 系统中受影响对象的标识符。

StorageGRID 中管理 **API** 请求的 **MGAU** 审核消息

" 管理 " 类别可将用户请求记录到管理 API 。对于并非对有效API URI的GET或HEAD请求的每个HTTP请求、都会记录一个响应、其中包含对此API的用户名、IP和请求类型。不会记录无效的API URL (例如/API/v3-Authorize)以及对有效API URL的无效请求。

代码	字段	说明
MDIP	目标 IP 地址	服务器（目标） IP 地址。
MDNA	域名	主机域名。
MPAT	请求路径	请求路径。
MPQP	请求查询参数	请求的查询参数。
MRBD	请求正文	请求正文的内容。虽然默认情况下会记录响应正文，但在某些情况下，如果响应正文为空，则会记录请求正文。由于响应正文中不提供以下信息，因此会从以下 POST 方法的请求正文中获取这些信息： • * POST Authorize * 中的用户名和帐户 ID • * POST /grid/grid-networks/update* 中的新子网配置 • * POST /grid/ntp-servers/update* 中的新 NTP 服务器 • 已停用的服务器 ID 位于 * POST /grid/servers/decommission* 中 • 注： * 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。

代码	字段	说明
MRmd	请求方法	HTTP 请求方法： • 发布 • PUT • 删除 • patch
MRSC	响应代码	响应代码。
MRSP	响应正文	默认情况下，系统会记录响应的内容（响应正文）。 • 注： * 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。
MSIP	源 IP 地址	客户端（源） IP 地址。
MUN	用户URN	发送请求的用户的 URN （统一资源名称）。
RSLT	结果	返回成功（ SUC ）或后端报告的错误。

StorageGRID 中系统检测到丢失对象的 **OLST** 审核消息

如果DDS服务在StorageGRID 系统中找不到对象的任何副本、则会生成此消息。

代码	字段	说明
CBID	内容块标识符	丢失对象的 CBID 。
NOID	节点ID	丢失对象的最后一个已知直接或近线位置(如果可用)。如果卷信息不可用，则只能使用节点 ID 而不使用卷 ID 。
路径	S3存储分段/密钥	S3存储分段名称和S3密钥名称(如果可用)。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。
UUID	通用唯一 ID	StorageGRID 系统中丢失对象的标识符。
卷	Volume ID	丢失对象的最后一个已知位置的存储节点的卷ID (如果可用)。

StorageGRID 中满足 **ILM** 规则的 **ORLM** 审核消息

如果对象已按照 ILM 规则的指定成功存储和复制，则会生成此消息。

如果策略中的另一条规则使用对象大小高级筛选器，则使用默认的 Make 2 Copies 规则成功存储对象时不会生成 ORLM 消息。

代码	字段	说明
BUID	存储分段标题	存储分段 ID 字段。用于内部操作。仅当统计数据为 PRGD 时才显示。
CBID	内容块标识符	对象的 CBID 。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOC	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 "" 。 CEC：对于纠删编码对象、应用于对象数据的纠删编码配置文件ID和纠删编码组ID。 CLDI ： 对于复制的对象， LDR 节点 ID 和对象位置的卷 ID 。 CLNL ： 归档对象数据时对象位置的弧节点 ID 。
路径	S3存储分段/密钥	S3存储分段名称和S3密钥名称。
RSLT	结果	ILM 操作的结果。 SUC ： ILM 操作成功。
规则	规则标签	为应用于此对象的 ILM 规则提供的可读标签。
SEGC	容器UUID	已分段对象的容器的 UUID 。只有当对象已分段时，此值才可用。
SGCB	容器CBID	已分段对象的容器的 CBID 。此值仅适用于已分段和多部分对象。
临时	状态	ILM 操作的状态。 Done ： 已完成对对象的 ILM 操作。 DDER ： 对象已标记为待未来 ILM 重新评估。 PRGD ： 此对象已从 StorageGRID 系统中删除。 NLOC ： 在 StorageGRID 系统中找不到对象数据。此状态可能表示对象数据的所有副本均缺失或已损坏。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

代码	字段	说明
VSID	版本ID	在受版本控制的存储分段中创建的新对象的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

对于单个对象、可以多次发出ORLM审核消息。例如、每当发生以下事件之一时、都会发出此命令：

- 对象的 ILM 规则将永久满足。
- 此 Epoch 已满足对象的 ILM 规则。
- ILM 规则已删除此对象。
- 后台验证过程检测到复制的对象数据的副本已损坏。StorageGRID 系统会执行 ILM 评估以替换损坏的对象。

相关信息

- "对象载入事务"
- "对象删除事务"

StorageGRID 中对象覆写的 OVWR 审核消息

如果外部（客户端请求的）操作导致一个对象被另一个对象覆盖，则会生成此消息。

代码	字段	说明
CBID	内容块标识符（新增）	新对象的 CBID 。
CSIZ	先前对象大小	要覆盖的对象的大小（以字节为单位）。
OCBD	内容块标识符（上一个）	上一个对象的 CBID 。
UUID	通用唯一 ID （新）	StorageGRID 系统中新对象的标识符。
OUID	通用唯一 ID （以前的）	StorageGRID 系统中上一个对象的标识符。
路径	S3对象路径	用于上一个对象和新对象的S3对象路径
RSLT	结果代码	对象覆盖事务的结果。结果始终为： SUC ： 成功
SGRP	站点（组）	如果存在此参数，则会在指定的站点上删除此覆盖对象，而不是在其中载入此覆盖对象的站点。

此消息会在S3 Select请求返回给客户端后记录完成。S3SL消息可以包括错误消息和错误代码详细信息。此请求可能未成功。

代码	字段	说明
BYSC	已扫描字节数	从存储节点扫描(接收)的字节数。 如果对对象进行压缩、BYSC和BYPR可能会有所不同。如果对象已压缩、则BYSC将具有经过压缩的字节计数、而BYPR将是解压缩后的字节。
BYPR	已处理的字节数	已处理的字节数。指示S3 Select作业实际处理或处理了多少字节的"已扫描字节数"。
BYRT	返回的字节数	S3 Select作业返回到客户端的字节数。
重新	记录已处理	S3 Select作业从存储节点收到的记录或行数。
RERT	返回的记录	S3 Select作业返回到客户端的记录或行数。
JOFI	作业已完成	指示S3 Select作业是否已完成处理。如果此值为false、则作业无法完成、并且错误字段中可能包含数据。客户端可能已收到部分结果、或者根本没有结果。
Reid	请求ID	S3 Select请求的标识符。
EXTM	执行时间	S3选择作业完成所需的时间(以秒为单位)。
ERMG	错误消息	S3 Select作业生成的错误消息。
很差	错误类型	S3 Select作业生成的错误类型。
错误	Stacktrace错误	S3 Select作业生成的Stacktrace出错。
S3BK	S3存储分段	S3 存储分段名称。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的S3访问密钥ID。
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID 。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。

StorageGRID 中安全审核禁用的 SADD 审核消息

此消息指示原始服务（节点 ID）已关闭审核消息日志记录。StorageGRID 不再收集或传递审核消息。

代码	字段	说明
AETM	启用方法	用于禁用审核的方法。
AEUN	用户名	执行命令以禁用审核日志记录的用户名。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。

此消息表示先前已启用日志记录，但现在已禁用。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，将还原审核（ SAade ），并永久阻止禁用审核的功能。

StorageGRID 中启用安全审核的 SADE 审核消息

此消息指示发起服务（节点 ID）已恢复审核消息日志记录。StorageGRID 再次收集和传递审核消息。

代码	字段	说明
AETM	启用方法	用于启用审核的方法。
AEUN	用户名	执行命令以启用审核日志记录的用户名。
RSLT	结果	此字段的值为 none 。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC ，因此不会筛选此消息。

此消息表示先前已禁用日志记录（ Sadd ），但现在已还原。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，审核将恢复，而禁用审核的功能将被永久阻止。

StorageGRID 中对象存储提交的 SCMT 审核消息

网格内容在提交之前不可用或无法识别为已存储（这意味着它已持久存储）。持久存储的内容已完全写入磁盘，并已通过相关的完整性检查。将内容块提交到存储时会发出此消息。

代码	字段	说明
CBID	内容块标识符	提交到永久存储的内容块的唯一标识符。
RSLT	结果代码	将对象存储到磁盘时的状态： SUCS ： 对象已成功存储。

此消息表示给定内容块已完全存储和验证，现在可以请求。它可用于跟踪系统内的数据流。

StorageGRID 中 **S3 DELETE** 事务的 **SDEL** 审核消息

当S3客户端发出删除事务时、系统会请求删除指定的对象或存储分段、或者删除存储分段/对象子资源。如果事务成功，服务器将发出此消息。

代码	字段	说明
ASRS	已假定角色会话 URN	假设角色会话的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
ASRU	假定角色 URN	所承担角色的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID 。存储分段上的操作不包括此字段。
GFID	网格联合连接ID	与跨网格复制删除请求关联的网格联合连接的连接ID。仅包含在目标网格的审核日志中。
GFSA	网格联合源帐户ID	源网格上用于跨网格复制删除请求的租户帐户ID。仅包含在目标网格的审核日志中。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 `X-Forwarded-For`如果请求中存在此地址、并且此值与请求发送者IP地址不同(SAIP审核字段)、则会自动包含此 `X-Forwarded-For`地址。 `x-amz-bypass-governance-retention`如果请求中存在、则会自动包含。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。

代码	字段	说明
RSLT	结果代码	删除事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SGRP	站点（组）	如果存在此对象，则会在指定的站点上删除此对象，而不是在其中载入此对象的站点。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。

代码	字段	说明
UUDM	删除标记的通用唯一标识符	删除标记的标识符。审核日志消息指定UUDM或UUID、其中UDM表示因对象删除请求而创建的删除标记、UUID表示对象。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	已删除对象的特定版本的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

StorageGRID 中 **S3 GET** 事务的 **SGET** 审核消息

当S3客户端发出GET事务时、系统会请求检索对象或列出存储分段中的对象、或者删除存储分段/对象子资源。如果事务成功，服务器将发出此消息。

代码	字段	说明
ASRS	已假定角色会话URN	假设角色会话的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
ASRU	假定角色 URN	所承担角色的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 `X-Forwarded-For`如果请求中存在此地址、并且此值与请求发送者IP地址不同(SAIP审核字段)、则会自动包含此 `X-Forwarded-For`地址。
。	ListObjectsV2	请求了_v2 format_响应。有关详细信息，请参见 "AWS List对象V2"。仅适用于GET分段操作。

代码	字段	说明
NCHD	儿童人数	包括密钥和通用前缀。仅适用于GET分段操作。
已振铃	范围读取	仅适用于范围读取操作。指示此请求读取的字节数范围。斜杠（ / ）后面的值显示整个对象的大小。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。

代码	字段	说明
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
常闭	已截断或未截断	如果返回所有结果、请设置为false。如果可返回更多结果、请设置为true。仅适用于GET分段操作。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	所请求对象的特定版本的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

StorageGRID 中 **S3 HEAD** 操作的 **SHEA** 审核消息

当 S3 客户端发出 HEAD 操作时，会发出请求来检查对象或存储桶是否存在并检索有关对象的元数据。如果操作成功，服务器将发出此消息。

代码	字段	说明
ASRS	已假定角色会话 URN	假设角色会话的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
ASRU	假定角色 URN	所承担角色的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检查对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 `X-Forwarded-For`如果请求中存在此地址、并且此值与请求发送者IP地址不同(SAIP审核字段)、则会自动包含此 `X-Forwarded-For`地址。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功

代码	字段	说明
S3AI	S3 租户帐户 ID （请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID （请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	所请求对象的特定版本的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

StorageGRID 中 **S3 POST** 事务的 **SPOS** 审计消息

当 S3 客户端发出 POST 对象请求时，如果事务成功，服务器将发出此消息。

代码	字段	说明
ASRS	已假定角色会话 URN	假设角色会话的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
ASRU	假定角色 URN	所承担角色的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 `X-Forwarded-For`如果请求中存在此地址、并且此值与请求发送者IP地址不同(SAIP审核字段)、则会自动包含此 `X-Forwarded-For`地址。 (SPOS不需要)。
RSLT	结果代码	RestorEObject请求的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。 对于S3 Select操作、设置为"Select"。

代码	字段	说明
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID （存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SRCF	子资源配置	还原信息。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	所请求对象的特定版本的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

StorageGRID 中 **S3 PUT** 事务的 **SPUT** 审核消息

当S3客户端发出Put事务时、系统会请求创建新对象或存储分段、或者删除存储分段/对象子资源。如果事务成功，服务器将发出此消息。

代码	字段	说明
ASRS	已假定角色会话 URN	假设角色会话的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。

代码	字段	说明
ASRU	假定角色 URN	所承担角色的唯一标识符。 仅当 S3 请求使用来自 AssumeRole 请求的临时安全凭据时才显示。
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CMPS	合规性设置	创建存储分段时使用的合规性设置(如果请求中存在)(截断为前1024个字符)。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。
GFID	网格联合连接ID	与跨网格复制放置请求关联的网格联合连接的连接ID。仅包含在目标网格的审核日志中。
GFSA	网格联合源帐户ID	源网格上用于跨网格复制放置请求的租户帐户ID。仅包含在目标网格的审核日志中。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 `X-Forwarded-For`如果请求中存在此地址、并且此值与请求发送者IP地址不同(SAIP审核字段)、则会自动包含此 `X-Forwarded-For`地址。 `x-amz-bypass-governance-retention`如果请求中存在、则会自动包含。
LKEN	对象锁定已启用	请求标头的值 `x-amz-bucket-object-lock-enabled`(如果在请求中存在)。
LKLH	对象锁定合法保留	请求标头的值 `x-amz-object-lock-legal-hold`(如果在PutObject请求中存在)。
LKMD	对象锁定保留模式	请求标头的值 `x-amz-object-lock-mode`(如果在PutObject请求中存在)。
LKRU	对象锁定保留至日期	请求标头的值 `x-amz-object-lock-retain-until-date`(如果在PutObject请求中存在)。值限制为自对象被纳入之日起100年内。

代码	字段	说明
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID（存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SRCF	子资源配置	新的子资源配置（截断为前 1024 个字符）。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。

代码	字段	说明
ULID	上传 ID	仅包含在CompleteMultipartUpload操作的SPUT消息中。表示所有部件均已上传和组装。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	在受版本控制的存储分段中创建的新对象的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。
VSST	版本控制状态	存储分段的新版本控制状态。使用两种状态："已启用"或"已暂停"。对象操作不包括此字段。

StorageGRID 中对象存储删除的 **SREM** 审核消息

从永久性存储中删除内容后会发出此消息，并且无法再通过常规 API 进行访问。

代码	字段	说明
CBID	内容块标识符	从永久存储中删除的内容块的唯一标识符。
RSLT	结果代码	指示内容删除操作的结果。唯一定义的值为： SUC ： 从永久性存储中删除的内容

此审核消息表示已从节点中删除给定内容块，无法再直接请求。此消息可用于跟踪系统中已删除内容的流。

StorageGRID 中 **S3** 元数据更新的 **SUPD** 审核消息

当 S3 客户端更新所载入对象的元数据时， S3 API 会生成此消息。如果元数据更新成功，则服务器会发出此消息。

代码	字段	说明
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0 。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	更新存储分段的合规性设置时，如果请求中存在一致性控制 HTTP 请求标头的值。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储分段上的操作不包括此字段。

代码	字段	说明
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 `X-Forwarded-For`如果请求中存在此地址、并且此值与请求发送者IP地址不同(SAIP审核字段)、则会自动包含此 `X-Forwarded-For`地址。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC ： 成功
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID 。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发件人）	发送请求的用户的哈希 S3 访问密钥 ID 。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID（存储分段所有者）	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN （请求发件人）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户，也可以是 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间，以微秒为单位。

代码	字段	说明
TLSIP	可信负载平衡器 IP 地址	如果请求是由受信任的第 7 层负载平衡器路由的，则为负载平衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本ID	已更新其元数据的对象的特定版本的版本 ID 。对未受版本管理的分段中的分段和对象执行的操作不包括此字段。

StorageGRID 中对象存储验证失败的 **SVRF** 审核消息

每当内容块验证过程失败时，都会发出此消息。每次从磁盘读取或写入复制的对象数据时，都会执行多项验证和完整性检查，以确保发送给请求用户的数据与最初载入系统的数据完全相同。如果其中任何一项检查失败，系统会自动隔离损坏的复制对象数据，以防止再次检索该数据。

代码	字段	说明
CBID	内容块标识符	验证失败的内容块的唯一标识符。
RSLT	结果代码	验证失败类型： CRCF ： 循环冗余检查（ CRC ）失败。 HMAC ： 基于哈希的消息身份验证代码（ HMAC ）检查失败。 EHSH ： 意外的加密内容哈希。 PHSH ： 意外的原始内容哈希。 SEQC ： 磁盘上的数据顺序不正确。 PERR ： 磁盘文件的结构无效。 DERR ： 磁盘错误。 fnam ： 文件名错误。

应密切监视此消息。内容验证失败可能表示即将发生硬件故障。

要确定哪个操作触发了消息，请参见 amid （模块 ID ）字段的值。例如， SV财年 值表示消息是由存储验证程序模块生成的，即后台验证， STor 表示消息是通过内容检索触发的。

StorageGRID 中未知对象存储内容的 **SVRU** 审核消息

LDR 服务的存储组件会持续扫描对象存储中复制的对象数据的所有副本。如果在对象存储中检测到复制的对象数据的未知或意外副本并将其移动到隔离目录，则会发出此消息。

代码	字段	说明
FPTH	文件路径	意外对象副本的文件路径。
RSLT	结果	此字段的值为 " 无 " 。RSLT- 是一个必填消息字段，但与此消息无关。使用 " 无 " 而不是 "CSU" ，因此不会筛选此消息。

应密切监控SVRU：对象存储验证未知审核消息。这意味着在对象存储中检测到意外的对象数据副本。应立即调查这种情况、以确定这些副本是如何创建的、因为它可能表示即将发生硬件故障。

StorageGRID 中正常节点停止的 SYSD 审核消息

如果服务正常停止，则会生成此消息以指示已请求关闭。通常、只有在后续重新启动后才会发送此消息、因为在关闭前不会清除审核消息队列。如果服务未重新启动，请查找在关闭序列开始时发送的 SYST 消息。

代码	字段	说明
RSLT	完全关闭	关闭的性质： SUC ： 系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYSD的RSLT无法指示"异常"关机、因为该消息仅由"干净"关机生成。

StorageGRID 中节点停止的 SYST 审核消息

当服务正常停止时，将生成此消息以指示已请求关闭，并且该服务已启动其关闭序列。SYST 可用于在服务重新启动之前确定是否已请求关闭（与 SYSD 不同，SYSD 通常在服务重新启动后发送）。

代码	字段	说明
RSLT	完全关闭	关闭的性质： SUC ： 系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYST消息的RSLT代码不能指示"异常"关机、因为该消息仅由"干净"关机生成。

节点的 SYSU 审核消息在 StorageGRID 中开始

重新启动服务时，系统会生成此消息，以指示上次关闭是正常关闭（已发出命令）还是无序关闭（意外关闭）。

代码	字段	说明
RSLT	完全关闭	关闭的性质： SUC ： 系统已完全关闭。 DSDN ： 系统未完全关闭。 VRGN ： 在安装（或重新安装）服务器后首次启动系统。

此消息不会指示是否已启动主机服务器，仅会指示报告服务。此消息可用于：

- 检测审核跟踪中的不连续性。
- 确定服务在运行期间是否出现故障（因为 StorageGRID 系统的分布式特征可能会掩盖这些故障）。Server Manager 会自动重新启动失败的服务。

扩展StorageGRID系统的容量或功能

了解如何扩展您的StorageGRID系统

了解如何扩展StorageGRID系统，以在不中断运行的情况下增加容量或功能。您可以向现有存储节点添加存储卷，向现有站点添加新的网格节点，或者添加新站点。

在扩展网格节点之前，您必须确认没有处于活动状态的数据修复作业。如果任何修复失败，则必须重新启动它们并让它们完成，然后再执行退役或扩展程序。请参阅"检查数据修复作业" 。

StorageGRID扩展允许您添加：

- 存储卷到存储节点
- 新网格节点到现有站点
- 整个新站点

执行扩展的原因决定了您必须添加的每种类型的新节点数以及这些新节点的位置。例如，如果要执行扩展以增加存储容量，添加元数据容量或添加冗余或新功能，则节点要求会有所不同。

按照适用于您所执行扩展类型的步骤进行操作：

添加网格节点

1. 按照的步骤进行操作"将网格节点添加到现有站点"。
2. "更新子网"(英文)
3. 部署网格节点：
   - "设备"
   - "VMware"
   - "Linux"

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

1. "执行扩展"(英文)
2. "配置扩展的系统"(英文)

添加存储卷

按照的步骤进行操作"将存储卷添加到存储节点"。

添加新站点

1. 按照的步骤进行操作"添加新站点"。
2. "更新子网"(英文)
3. 部署网格节点：
   - "设备"
   - "VMware"
   - "Linux"

> “Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

1. "执行扩展"(英文)
2. "配置扩展的系统"(英文)

扩张计划

StorageGRID中复制数据的扩展规划

如果您的部署的信息生命周期管理（ ILM ）策略包含一条规则，用于创建对象的复制副本，则必须考虑要添加的存储容量以及要添加新存储卷或存储节点的位置。

有关在何处添加额外存储的指导，请查看创建复制副本的 ILM 规则。如果 ILM 规则创建两个或更多对象副本，请计划在创建对象副本的每个位置添加存储。例如、如果您有一个双站点网格、并且有一个ILM规则在每个站点创建一个对象副本、则必须对每个站点执行此操作、"添加存储"才能增加网格的整体对象容量。有关对象复制的

信息，请参见"什么是复制"。

出于性能原因，您应尝试在各个站点之间保持存储容量和计算能力的平衡。因此，在此示例中，您应向每个站点添加相同数量的存储节点或在每个站点添加更多存储卷。

如果您的 ILM 策略更加复杂，其中包括根据存储分段名称等标准将对象放置在不同位置的规则，或者随着时间的推移更改对象位置的规则，则您对扩展所需存储位置的分析将类似，但更为复杂。

绘制整体存储容量的消耗速度图表有助于您了解要在扩展中添加多少存储以及何时需要额外存储空间。您可以使用网格管理器"监控存储容量并绘制图表"。

在规划扩展时间时，请记住考虑采购和安装额外存储可能需要多长时间。为了简化扩展规划，当现有存储节点达到 70% 容量时，请考虑添加存储节点。

StorageGRID中纠删码（EC）数据的扩展规划

如果 ILM 策略包含创建纠删编码副本的规则，则必须计划在何处添加新存储以及何时添加新存储。您添加的存储量和添加的时间可能会影响网格的可用存储容量。

规划存储扩展的第一步是，检查 ILM 策略中用于创建纠删编码对象的规则。由于 StorageGRID 会为每个纠删编码对象创建 *k+m_fragments* ，并将每个片段存储在不同的存储节点上，因此您必须确保在扩展后至少 *_k+m* 存储节点具有用于存储新纠删编码数据的空间。如果纠删编码配置文件提供站点丢失保护，则必须向每个站点添加存储。有关纠删编码配置文件的信息、请参见"什么是纠删编码方案"。

您需要添加的节点数还取决于执行扩展时现有节点的容量。

有关为经过纠删编码的对象添加存储容量的一般建议

如果要避免详细计算，可以在现有存储节点容量达到 70% 时为每个站点添加两个存储节点。

对于单站点网格和纠删编码可提供站点丢失保护的网格，此一般建议可在多种纠删编码方案中提供合理的结果。

要更好地了解导致此建议的因素或为您的站点制定更精确的计划，请参见"重新平衡经过纠删编码的数据的注意事项"。有关针对您的情况进行优化的自定义建议、请联系您的NetApp专业服务顾问。

了解StorageGRID扩展后的 EC 重新平衡

如果要执行扩展以添加存储节点、并且要使用ILM规则来纠删代码数据、则如果无法为所使用的纠删编码方案添加足够的存储节点、则可能需要执行纠删编码(EC)重新平衡过程。

查看这些注意事项后、请执行扩展、然后转到"添加存储节点后重新平衡经过纠删编码的数据"运行此过程。

什么是 **EC** 重新平衡?

EC 重新平衡是扩展存储节点后可能需要的 StorageGRID 操作步骤 。操作步骤 将作为主管理节点上的命令行脚本运行。运行EC重新平衡操作步骤 时、StorageGRID 会在站点的现有存储节点和新添加的存储节点之间重新分布纠删编码的片段。

EC 重新平衡操作步骤：

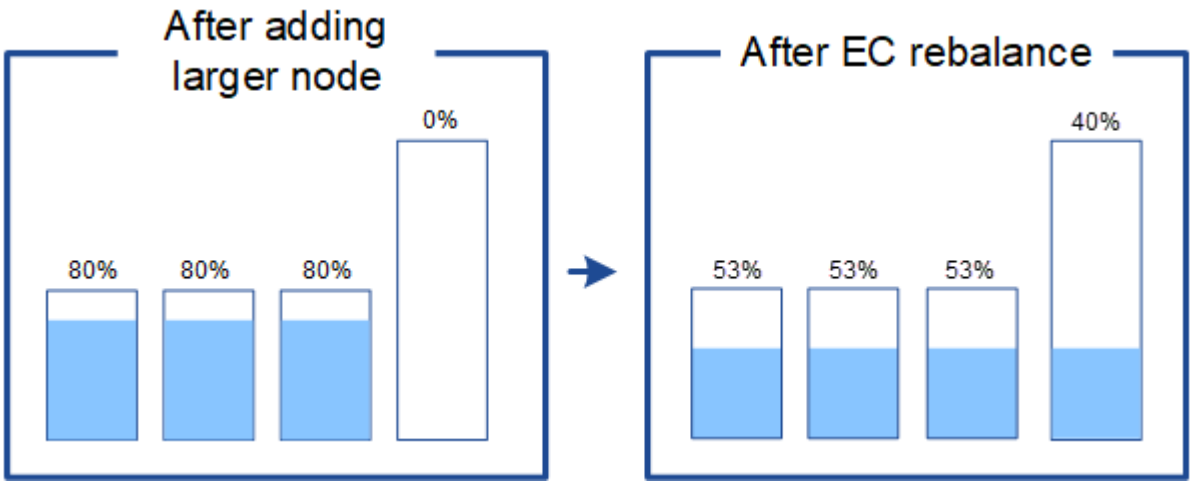
- 仅移动经过纠删编码的对象数据。它不会移动复制的对象数据。

- 在站点内重新分布数据。它不会在站点之间移动数据。
- 在站点的所有存储节点之间重新分布数据。它不会在存储卷中重新分配数据。
- 尝试分配数据字节，以便每个节点具有相同的可用空间。在重新平衡完成后，包含更多复制数据的节点可能存储较少的纠删编码数据。
- 在不考虑每个节点的相对容量的情况下，在存储节点之间均匀地重新分配可用空间。复制的数据包含在计算中。
- 如果重新平衡过程无法再移动任何纠删码数据，即使可用空间仍未均匀分布，也视为该过程已完成。
- 不会将纠删码数据分发到已满 80% 以上的存储节点或仅元数据的存储节点。
- 可能会在运行ILM操作和S3客户端操作时降低性能&#8212；重新分布纠删编码片段需要额外的资源。

完成 EC 重新平衡操作步骤 后：

- 经过删除编码的数据将从可用空间较少的存储节点移至可用空间较多的存储节点。
- 擦除编码对象的数据保护将保持不变。
- 不同存储节点的已用(%)值可能不同、原因有两个：
  - 复制的对象副本将继续占用现有节点上的空间##8212;EC重新平衡操作步骤 不会移动复制的数据。
  - 容量较大的节点可能比容量较小的节点相对较少填充，即使所有节点最终的可用空间量大致相同。

    例如，使用 2+1 擦除编码方案，假设三个 200 TB 节点各自填充到 80%（每个节点 200 × 0.8 = 160 TB ，或站点 480 TB）。如果添加 400 TB 节点并运行重新平衡过程，则所有较旧节点现在将具有大致相同的擦除编码数据量（106.66 TB 或已用 53%）。新节点将具有（160 TB 数据或已用 40%）。在这种情况下，较大节点的已用 (%) 将小于较小节点的已用 (%)。重新平衡过程在可用空间平衡之前完成，因为在不破坏擦除编码方案约束的情况下，无法移动更多擦除编码数据。



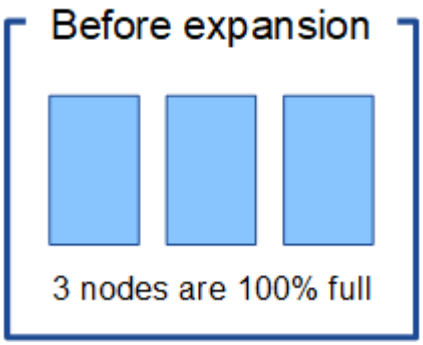
何时重新平衡已通过数据进行了数据迁移

EC 重新平衡程序重新分配现有的擦除编码数据，以确保节点不会变满或保持满状态。该程序有助于确保 EC 编码能够在网站上继续进行。

当站点上的数据分布存在令人担忧的偏差并且站点存储大部分 EC 数据时（因为复制的数据无法通过重新平衡来移动），运行重新平衡程序。

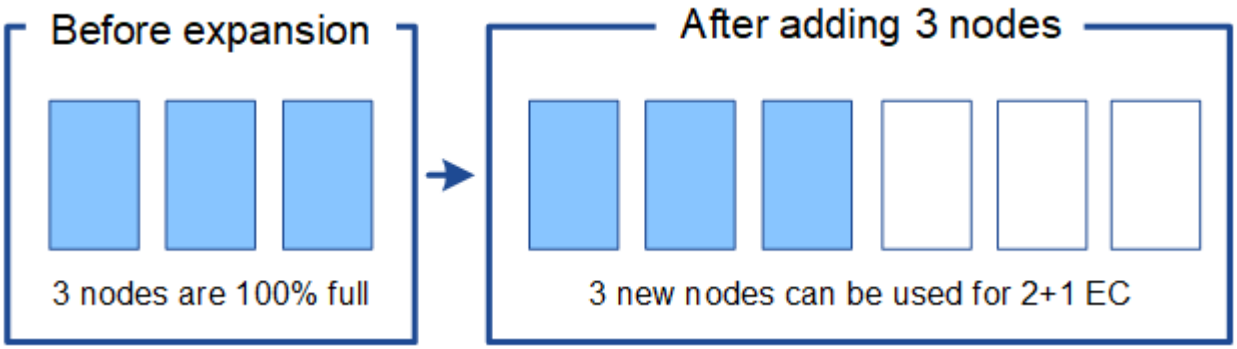
请考虑以下情形：

- StorageGRID 正在一个站点上运行，该站点包含三个存储节点。
- ILM策略对大于1.0 MB的所有对象使用2+1擦除编码规则、对较小的对象使用双副本复制规则。
- 所有存储节点均已全满。已在主要严重性级别触发“对象存储不足”警报。



如果添加足够的节点，则不需要重新平衡

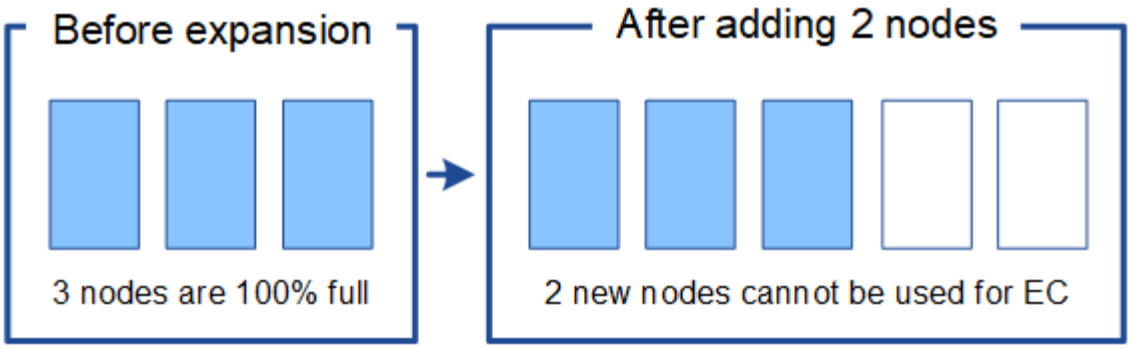
要了解何时不需要EC重新平衡、假设您添加了三个(或更多)新存储节点。在这种情况下、您不需要执行EC重新平衡。原始存储节点将保持已满、但新对象现在将使用这三个新节点进行2+1纠删编码##8212；两个数据片段和一个奇偶校验片段可以分别存储在不同的节点上。



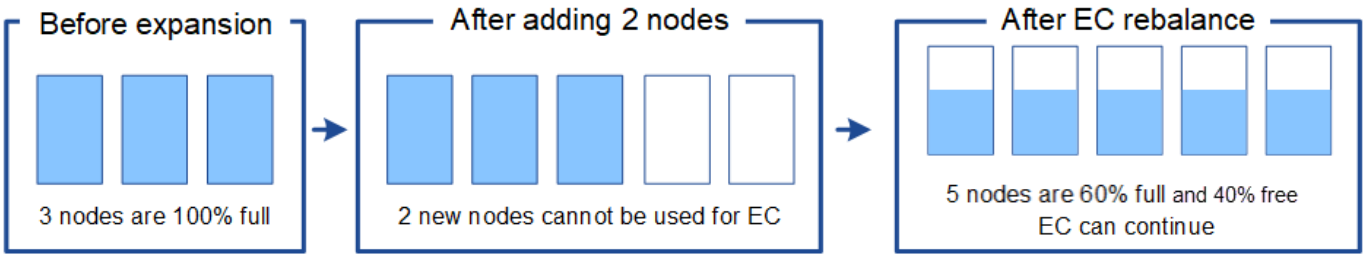
在这种情况下、虽然您可以运行EC重新平衡操作步骤 、但移动现有纠删编码的数据会暂时降低网格的性能、从而可能影响客户端操作。

如果无法添加足够多的节点、则需要重新平衡

要了解何时需要EC重新平衡、假设您只能添加两个存储节点、而不能添加三个存储节点。由于2+1方案至少需要三个存储节点具有可用空间、因此、这些空节点不能用于新的已通过erasure编码的数据。



要使用新的存储节点，您应该运行 EC 重新平衡程序。运行此过程时，StorageGRID 重新分配现有的纠删码数据和奇偶校验片段，以便在站点的所有存储节点之间均匀分配可用空间。在此示例中，当 EC 重新平衡过程完成时，所有五个节点现在都已满 60%，可用空间为 40%，并且可以继续将对象摄入所有存储节点上的 2+1 纠删码方案。



EC重新平衡的建议

如果以下陈述中的_all_为真、则NetApp需要EC重新平衡：

- 您可以对对象数据使用纠删编码。
- 已针对站点上的一个或多个存储节点触发 * 对象存储空间不足 * 警报，表示这些节点已满 80% 或以上。
- 您无法为正在使用的纠删编码方案添加足够多的新存储节点。请参阅。 "为经过纠删编码的对象添加存储容量"
- 在运行EC重新平衡过程时、S3客户端的写入和读取操作性能可能会降低。

如果您希望将存储节点填充到类似级别、并且在运行EC重新平衡过程期间、S3客户端的写入和读取操作性能可以降低、则可以选择运行EC重新平衡过程。

EC 重新平衡操作步骤 如何与其他维护任务进行交互

您不能在运行EC重新平衡操作步骤 的同时执行某些维护过程。

操作步骤	在 **EC** 重新平衡操作步骤 期间是否允许？
其他 EC 重新平衡过程	否 一次只能运行一个 EC 重新平衡操作步骤 。

操作步骤	在 **EC** 重新平衡操作步骤 期间是否允许?
停用操作步骤 EC 数据修复作业	否 • 在 EC 重新平衡操作步骤 运行期间，系统会阻止您启动停用操作步骤或 EC 数据修复。 • 在存储节点停用操作步骤 操作步骤 或 EC 数据修复正在运行时，系统会阻止您启动 EC 重新平衡。
扩展操作步骤	否 如果您需要在扩展中添加新存储节点、请在添加所有新节点后运行EC重新平衡操作步骤。
升级操作步骤	否 如果您需要升级StorageGRID 软件、请在运行EC重新平衡操作步骤 之前或之后执行升级操作步骤。您可以根据需要终止 EC 重新平衡操作步骤以执行软件升级。
设备节点克隆操作步骤	否 如果您需要克隆设备存储节点、请在添加新节点后运行EC重新平衡操作步骤。
修补程序操作步骤	是。 您可以在 EC 重新平衡操作步骤 运行期间应用 StorageGRID 修补程序。
其他维护过程	否 在运行其他维护过程之前，您必须终止 EC 重新平衡操作步骤 。

EC 重新平衡操作步骤 如何与 **ILM** 交互

在运行 EC 重新平衡操作步骤 时，请避免进行可能会更改现有纠删编码对象位置的 ILM 更改。例如、不要开始使用具有不同纠删编码配置文件的ILM规则。如果需要进行此类ILM更改、则应终止EC重新平衡操作步骤。

扩展指南

StorageGRID中添加对象容量的指南

您可以通过向现有存储节点添加存储卷或向现有站点添加新存储节点来扩展 StorageGRID 系统的对象存储容量。添加存储容量时，必须满足信息生命周期管理（ ILM ）策略的要求。

添加存储卷的准则

在将存储卷添加到现有存储节点之前，请查看以下准则和限制：

- 您必须检查当前的ILM规则，以确定在何处以及何时"添加存储卷"增加或"经过编程的对象"的可用存储"复制的对象"。
- 您不能通过添加存储卷来增加系统的元数据容量、因为对象元数据仅存储在卷0上。
- 每个基于软件的存储节点最多可支持 48 个存储卷。如果您需要添加的容量超出此范围，则必须添加新的存储节点。
- 您可以向每个SG6060设备添加一个或两个扩展架。每个扩展架可添加16个存储卷。如果安装了这两个扩展架、SG6060总共可支持48个存储卷。
- 您可以向每个SG6160设备添加一个或两个扩展架。每个扩展架可添加60个存储卷。如果安装了这两个扩展架、SG6160总共可支持180个存储卷。
- 您不能将存储卷添加到任何其他存储设备。
- 您不能增加现有存储卷的大小。
- 您不能在执行系统升级、恢复操作或其他扩展时向存储节点添加存储卷。

在决定添加存储卷并确定必须扩展哪些存储节点以满足 ILM 策略后，请按照适用于您的存储节点类型的说明进行操作：

- 要向SG6060存储设备添加一个或两个扩展架，请转至 "将扩展架添加到已部署的SG6060"。
- 要向SG6160存储设备添加一个或两个扩展架、请转至 "将扩展架添加到已部署的SG6160"
- 对于基于软件的节点，请按照的说明"将存储卷添加到存储节点"进行操作。

添加存储节点的准则

在将存储节点添加到现有站点之前，请查看以下准则和限制：

- 您必须检查当前的ILM规则，以确定在何处以及何时添加存储节点以增加或"经过编程的对象"的可用存储"复制的对象"。
- 在一个扩展操作步骤 中添加的存储节点不应超过 10 个。
- 您可以在一个扩展操作步骤 中将存储节点添加到多个站点。
- 您可以在一个扩展操作步骤 中添加存储节点和其他类型的节点。
- 在启动扩展操作步骤 之前，您必须确认在恢复过程中执行的所有数据修复操作均已完成。请参阅。 "检查数据修复作业"
- 如果在执行扩展之前或之后需要删除存储节点，则在一个 " 停用节点 " 操作步骤 中停用的存储节点不应超过 10 个。
- 添加足够的存储节点以维持底层存储 I/O 性能。写入操作将根据可用存储容量在存储节点之间分配。如果扩展的存储节点具有更多可用存储容量，则这些节点将接收更多的写入。特别是，当现有的存储节点几乎已满时，新的写入将仅依赖于扩展的存储节点。读取和删除操作将根据您的具体工作负载来处理。

存储节点上的模块转换服务准则

配置扩展时，必须选择是否在每个新存储节点上包含管理域控制器（ ADA ）服务。此 ADA 服务可跟踪网格服务的位置和可用性。

- 您可以"将 ADC 服务从一个存储节点移动到同一站点上的另一个存储节点" 。
- StorageGRID系统要求"ADC 服务的仲裁"每个站点随时都有可用的。
- 每个站点至少有三个存储节点必须包含此 ADC-Service 。
- 不建议将此 ADA 服务添加到每个存储节点。包含过多的 ADC 服务可能会因节点间通信量增加而导致发生原因 速度变慢。
- 一个网格中包含的存储节点不应超过 48 个，而是使用了此 ADA 服务。这相当于 16 个站点，每个站点有三个模块转换服务。
- 一般来说，当您为新节点选择*ADC 服务*设置时，您应该选择*自动*。仅当新节点将替换包含 ADC 服务的另一个存储节点时才选择*是*。由于如果剩余的 ADC 服务太少，您就无法停用存储节点，因此选择“是”可确保在删除旧服务之前有新的 ADC 服务可用。

StorageGRID元数据容量添加指南

要确保为对象元数据提供足够的可用空间，您可能需要执行扩展操作步骤 以在每个站点添加新的存储节点。

StorageGRID 会为每个存储节点的卷 0 上的对象元数据预留空间。每个站点维护三个所有对象元数据副本，这些副本均匀分布在所有存储节点上。

您可以使用网格管理器监控存储节点的元数据容量，并估计元数据容量的使用速度。此外，当已用元数据空间达到特定阈值时，系统会为存储节点触发 * 低元数据存储 * 警报。

请注意，根据网格的使用方式，网格的对象元数据容量消耗速度可能比其对象存储容量更快。例如，如果您通常要载入大量小对象或向对象添加大量用户元数据或标记，则即使仍有足够的对象存储容量，您可能需要添加存储节点以增加元数据容量。

有关详细信息，请参见以下内容：

- "管理对象元数据存储"
- "监控每个存储节点的对象元数据容量"

增加元数据容量的准则

在添加存储节点以增加元数据容量之前，请查看以下准则和限制：

- 假设有足够的对象存储容量可用，则为对象元数据提供更多的可用空间将增加可存储在 StorageGRID 系统中的对象数量。
- 您可以通过向每个站点添加一个或多个存储节点来增加网格的元数据容量。
- 在任何给定存储节点上为对象元数据预留的实际空间取决于元数据预留空间存储选项（系统范围设置），分配给节点的 RAM 量以及节点卷 0 的大小。
- 您不能通过向现有存储节点添加存储卷来增加元数据容量、因为元数据仅存储在卷0上。
- 您不能通过添加新站点来增加元数据容量。
- StorageGRID 会为每个站点上的所有对象元数据保留三个副本。因此，系统的元数据容量受最小站点的元数据容量限制。
- 在添加元数据容量时，应向每个站点添加相同数量的存储节点。

纯元数据存储节点具有特定的硬件要求：

- 使用StorageGRID设备时、只能在具有12个1.9 TB或12个3.8 TB驱动器的GF6112设备上配置纯元数据节点。
- 使用基于软件的节点时、纯元数据节点资源必须与现有存储节点资源匹配。例如：
  - 如果现有StorageGRID站点使用SG6000或SG6100设备、则基于软件的纯元数据节点必须满足以下最低要求：
    - 128 GB RAM
    - 8核CPU
    - 用于cassandr数据库的8 TB SSD或等效存储(rangedb/0)
  - 如果现有的StorageGRID站点使用具有 24 GB RAM、8 核 CPU 和 3 TB 或 4TB 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 4TB 元数据存储（rangedb/0））。
- 添加新StorageGRID站点时、新站点的元数据总容量至少应与现有StorageGRID站点匹配、新站点资源应与现有StorageGRID站点的存储节点匹配。

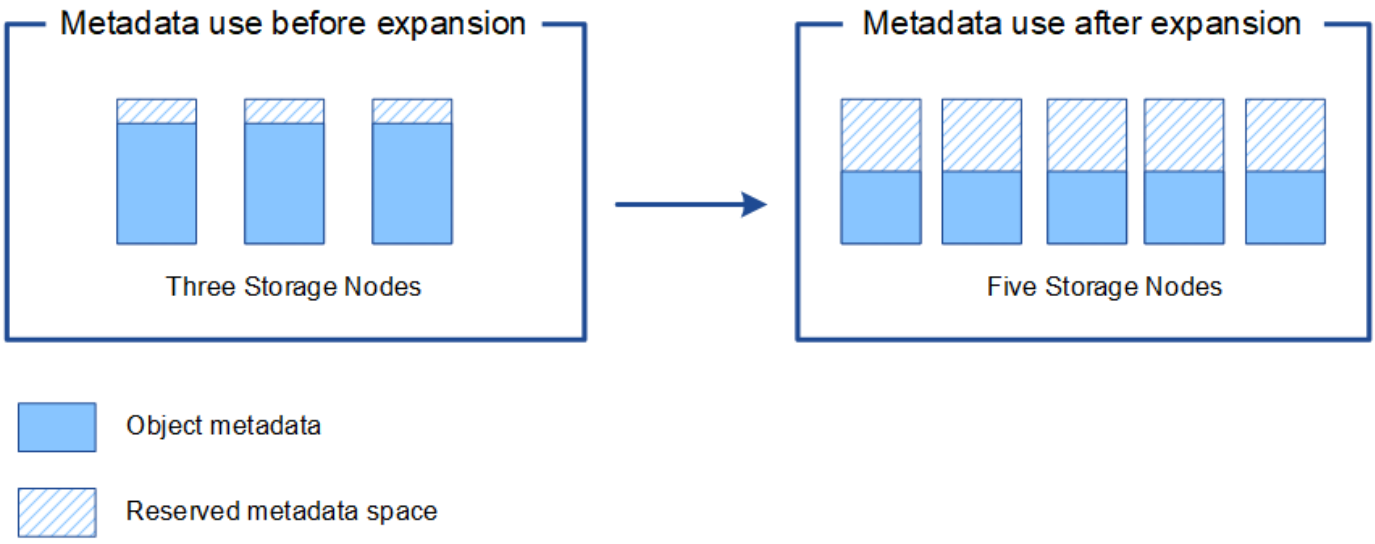
请参见"什么是元数据预留空间的问题描述"。

添加存储节点时如何重新分配元数据

在扩展中添加存储节点时， StorageGRID 会将现有对象元数据重新分发到每个站点的新节点，从而增加网格的整体元数据容量。无需用户操作。

下图显示了在扩展中添加存储节点时 StorageGRID 如何重新分发对象元数据。图的左侧表示扩展之前三个存储节点的卷 0 。元数据占用了每个节点可用元数据空间的相对较大部分，并且已触发 "* 低元数据存储 * " 警报。

图的右侧显示了在向站点添加两个存储节点后如何重新分配现有元数据。每个节点上的元数据数量已减少，不再触发 * 元数据存储不足 * 警报，并且可用于元数据的空间已增加。



StorageGRID中添加网格节点的指南

您可以通过向现有站点添加新的网格节点来为 StorageGRID 系统添加冗余或其他功能。

例如、您可以选择添加要在高可用性(HA)组中使用的网关节点、也可以在远程站点添加管理节点以允许使用本地节点进行监控。

您可以通过单个扩展操作向一个或多个现有站点添加以下一种或多种类型的节点：

- 非主管理节点
- 存储节点
- 网关节点

准备添加网格节点时，请注意以下限制：

- 主管理节点会在初始安装期间部署。您无法在扩展期间添加主管理节点。
- 您可以在同一扩展中添加存储节点和其他类型的节点。
- 添加存储节点时，必须仔细规划新节点的数量和位置。请参阅。 "添加对象容量的准则"
- 如果防火墙控制页面上不受信任的客户端网络选项卡上的 设置新节点默认值 选项为 不受信任，则使用客户端网络连接到扩展节点的客户端应用程序必须使用负载平衡器端点端口进行连接（配置 > 安全 > 防火墙控制）。请参阅说明"更改新节点的安全设置"以及"配置负载平衡器端点"。

StorageGRID添加新站点的指南

您可以通过添加新站点来扩展 StorageGRID 系统。

添加站点的准则

在添加站点之前，请查看以下要求和限制：

- 每个扩展操作只能添加一个站点。
- 您不能在同一扩展中向现有站点添加网格节点。
- 所有站点必须包含至少三个存储节点。它们可以是组合存储节点和仅元数据存储节点的任意组合。如果有三个以上的存储节点，只要有三个可用的 ADC 服务，它们可以是组合、仅元数据和仅数据存储节点的任意组合。有关详细信息，请参阅 "每个网格和每个站点所需的存储节点"。
- 添加新站点时，不会自动增加可以存储的对象数。网格的总对象容量取决于每个站点的可用存储量、ILM 策略和元数据容量。
- 在估算新站点的规模时，您必须确保其包含足够的元数据容量。

  StorageGRID 在每个站点保留所有对象元数据的副本。添加新站点时，请确保其包含足够的元数据容量以存储现有对象元数据，以及足够的元数据容量以支持增长。

  有关详细信息，请参阅以下内容：

  - "管理对象元数据存储"
  - "监控每个存储节点的对象元数据容量"
- 您必须考虑站点之间的可用网络带宽以及网络延迟级别。元数据更新会在站点之间持续复制，即使所有对象都仅存储在要载入的站点上也是如此。

  要避免因延迟而导致性能不佳，请执行以下操作：

- 不建议在延迟大于 100 毫秒的站点之间使用纠删码。
- StorageGRID 系统中的站点不应跨越很远的地理距离，例如，跨越多个大陆。

- 由于 StorageGRID 系统在扩展期间仍可正常运行，因此您必须在启动扩展操作步骤 之前查看 ILM 规则。您必须确保在扩展操作步骤 完成之前不会将对象副本存储到新站点。

  例如，在开始扩展之前，请检查是否有任何规则使用默认存储池（所有存储节点）。如果是这样，请使用现有存储节点创建一个新的存储池，并更新您的 ILM 规则以使用新的存储池。否则，一旦该站点的第一个节点处于活动状态，就会将对象复制到新站点。

  有关添加新站点时更改 ILM 策略的详细信息，请参见 "更改ILM策略的示例"。

准备扩展您的StorageGRID系统

在执行扩展操作之前，请收集相关材料并安装和配置任何新的硬件和网络。

项目	备注
StorageGRID 安装归档	如果要添加新的网格节点或新站点，则必须下载并提取 StorageGRID 安装归档。您必须使用网格上当前运行的相同版本。 有关详细信息，请参见的说明下载并提取 StorageGRID 安装文件。 *注意：*如果要向现有存储节点添加新存储卷或安装新的StorageGRID 设备、则无需下载文件。
服务笔记本电脑	服务笔记本电脑具有以下功能： • 网络端口 • SSH 客户端（例如 PuTTY ） • "支持的 Web 浏览器"
`Passwords.txt`文件	包含在命令行上访问网格节点所需的密码。包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在此文件中 `Passwords.txt`。
StorageGRID 文档	• "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。 • "适用于您的平台的安装说明"
适用于您的平台的最新文档	有关支持的版本，请参见 "互操作性表工具(IMT)"。

下载并提取 StorageGRID 安装文件

【下载并提取安装文件】

在添加新网格节点或新站点之前，必须下载相应的 StorageGRID 安装归档并提取文件。

关于此任务

您必须使用网格上当前运行的 StorageGRID 版本执行扩展操作。

步骤

1. 转到。 "NetApp 下载： StorageGRID"
2. 选择网格上当前运行的 StorageGRID 版本。
3. 使用您的 NetApp 帐户的用户名和密码登录。
4. 阅读最终用户许可协议，选中复选框，然后选择*接受并继续*。
5. 在下载页面的*安装StorageGRID *列中，选择 `.tgz`适用于您的平台的或 `.zip`文件。

   安装归档文件中显示的版本必须与当前安装的软件版本匹配。

   如果您在服务笔记本电脑上运行Windows、请使用此 `.zip`文件。

平台	安装归档
RHEL	`StorageGRID-Webscale-version-RPM-uniqueID.zip` `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
Ubuntu ， Debian 或设备	`StorageGRID-Webscale-version-DEB-uniqueID.zip` `StorageGRID-Webscale-version-DEB-uniqueID.tgz`
VMware	`StorageGRID-Webscale-version-VMware-uniqueID.zip` `StorageGRID-Webscale-version-VMware-uniqueID.tgz`
OpenStack/ 其他虚拟机管理程序	要在 OpenStack 上扩展现有部署，您必须部署一个运行上述受支持 Linux 分发版本之一的虚拟机，并按照适用于 Linux 的相应说明进行操作。

6. 下载并提取归档文件。
7. 按照适用于您的平台的步骤，根据您的平台，计划的网格拓扑以及您将如何扩展 StorageGRID 系统来选择所需的文件。

   步骤中为每个平台列出的路径与归档文件安装的顶级目录相对。

8. 如果您正在扩展 RHEL 系统，请选择适当的文件。

路径和文件名	说明
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。

路径和文件名	说明
	一种免费许可证，不提供产品的任何支持授权。
	RPM软件包、用于在RHEL主机上安装StorageGRID节点映像。
	RPM软件包、用于在RHEL主机上安装StorageGRID主机服务。
部署脚本工具	说明
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	用于为StorageGRID容器部署配置RHEL主机的AndsableRole和操作手册示例。您可以根据需要自定义角色或攻略手册。
	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

1. 如果要扩展 Ubuntu 或 Debian 系统，请选择相应的文件。

路径和文件名	说明
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。
	文件的MD5校验和 `/debs/storagegrid-webscale-images-version-SHA.deb`。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	说明
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
storagegrid-ssoauth-azure.py	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。

路径和文件名	说明
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

1. 如果要扩展 VMware 系统，请选择相应的文件。

路径和文件名	说明
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。
	(`.mf`用于部署主管理节点(`.ovf`的开放式虚拟化格式模板文件()和清单文件()。
	(`.mf`用于部署非主管理节点(`.ovf`的模板文件()和清单文件()。
	(`.mf`用于部署网关节点(`.ovf`的模板文件()和清单文件()。
	(`.mf`用于部署基于虚拟机的存储节点的模板(`.ovf`文件()和清单文件()。
部署脚本工具	说明
	Bash shell 脚本，用于自动部署虚拟网格节点。
	用于脚本的示例配置文件 `deploy-vsphere-ovftool.sh`。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。

路径和文件名	说明
	一个Python脚本示例、在启用单点登录(Single Sign On、SSO)后、您可以使用该脚本登录到网格管理API。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

1. 如果要扩展基于 StorageGRID 设备的系统，请选择相应的文件。

> 对于设备安装，仅当您需要避免网络流量时才需要这些文件。设备可以从您执行恢复过程的管理节点下载所需的文件。

路径和文件名	说明
	用于在设备上安装 StorageGRID 节点映像的 Deb 软件包。
	文件的MD5校验和 `/debs/storagegridwebscale-images-version-SHA.deb`。

验证硬件和网络连接

开始扩展 StorageGRID 系统之前，请确保满足以下要求：

- 已安装并配置支持新网格节点或新站点所需的硬件。
- 所有新节点都具有指向所有现有节点和新节点的双向通信路径（网格网络的一项要求）。具体而言、请确认要添加到扩展中的新节点与主管理节点之间的以下TCP端口已打开：

- 1055
- 7443
- 8011
- 10342

请参阅。 "内部网格节点通信"

- 主管理节点可以与用于托管 StorageGRID 系统的所有扩展服务器进行通信。
- 如果任何新节点在先前未使用的子网上具有网格网络IP地址、则表示您已"已添加新子网"访问网格网络子网列表。否则，您必须取消扩展，添加新子网并重新启动操作步骤 。
- 您没有在网格网络中的网格节点之间或StorageGRID 站点之间使用网络地址转换(Network Address Translation、NAT)。如果您对网格网络使用专用 IPv4 地址，则这些地址必须可从每个站点的每个网格节点直接路由。只有在使用对网格中的所有节点都透明的通道应用程序时，才支持使用 NAT 在公有 网段中桥接网格网络，这意味着网格节点不需要了解公有 IP 地址。

  此 NAT 限制特定于网格节点和网格网络。您可以根据需要在外部客户端和网格节点之间使用 NAT ，例如为网关节点提供公有 IP 地址。

添加网格节点或站点

向StorageGRID添加网格节点或新站点的工作流程概述

按照此操作步骤向现有站点添加网格节点或添加新站点。一次只能执行一种类型的扩展。

开始之前

- 您拥有"root访问权限或维护权限"。
- 网格中的所有现有节点在所有站点上均已启动且正在运行。
- 先前的任何扩展，升级，停用或恢复过程均已完成。

> 如果正在进行另一个扩展，升级，恢复或活动的停用操作步骤 ，则系统将阻止您启动扩展。但是，如有必要，您可以暂停已停用的操作步骤 以启动扩展。

步骤

1. "更新网格网络的子网"。
2. "部署新的网格节点"。
3. "执行扩展"(英文)

在StorageGRID中添加或更新网格网络子网以进行扩展

在扩展中添加网格节点或新站点时，您可能需要更新子网或向网格网络添加子网。

StorageGRID 会维护一个网络子网列表，用于在网格网络（ eth0 ）上的网格节点之间进行通信。这些条目包括 StorageGRID 系统中每个站点用于网格网络的子网，以及通过网格网络网关访问的 NTP ， DNS ， LDAP 或其他外部服务器所使用的任何子网。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您已获得要配置的子网的网络地址，以 CIDR 表示法表示。

关于此任务

如果任何新节点的子网上有一个以前未使用的网格网络 IP 地址，则必须在开始扩展之前将此新子网添加到网格网络子网列表中。否则，您必须取消扩展，添加新子网并重新启动操作步骤 。

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，请勿使用以下子网范围：

- 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
- 198.51.100.0/24，因为此子网范围包含 IP 地址 198.51.100.2 和 198.51.100.4

步骤

1. 选择*维护* > 网络 > 电网。
2. 选择*添加其他子网*以使用CIDR表示法添加新子网。

   例如，输入 `10.96.104.0/22`。

3. 输入配置密码短语，然后选择 * 保存 * 。
4. 等待更改应用完毕，然后下载新的恢复包。
   a. 选择*维护* > 系统 > 恢复包。
   b. 输入 **Provisioning passphrase**。

恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。它还用于恢复主管理节点。

您指定的子网将自动为 StorageGRID 系统配置。

在StorageGRID中部署新的网格节点

在扩展中部署新网格节点的步骤与首次安装网格时使用的步骤相同。您必须先部署所有新的网格节点，然后才能执行扩展。

扩展网格时、添加的节点不必与现有节点类型匹配。您可以添加 VMware 节点，基于 Linux 容器的节点或设备节点。

VMware： 部署网格节点

您必须在 VMware vSphere 中为要添加到扩展中的每个 VMware 节点部署一个虚拟机。

步骤

1. "将新节点部署为虚拟机"并将其连接到一个或多个StorageGRID网络。

   部署节点时，您可以选择重新映射节点端口或增加 CPU 或内存设置。

2. 部署完所有新的VMware节点后，"执行扩展操作步骤"。

Linux： 部署网格节点

您可以在新的 Linux 主机或现有的 Linux 主机上部署网格节点。如果您需要更多的 Linux 主机来满足要添加到网格中的 StorageGRID 节点的 CPU ， RAM 和存储要求，请按照首次安装主机时准备主机的方式对其进行准备。然后，按照安装期间部署网格节点的方式部署扩展节点。

开始之前

- 您已获得针对您的 Linux 版本安装StorageGRID 的说明，并且您已查看"硬件和存储要求"。
- 如果您计划在现有主机上部署新的网格节点，则已确认现有主机具有足够的 CPU ， RAM 和存储容量来容纳其他节点。
- 您计划最大限度地减少故障域。例如，不应将所有网关节点部署在一个物理主机上。

  > 在生产部署中、不要在一个物理或虚拟主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

- 如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

步骤

1. 如果要添加新主机，请访问有关部署 StorageGRID 节点的安装说明。
2. 要部署新主机，请按照说明准备主机。
3. 要创建节点配置文件并验证 StorageGRID 配置，请按照有关部署网格节点的说明进行操作。
4. 如果要向新的 Linux 主机添加节点，请启动 StorageGRID 主机服务。
5. 如果要向现有Linux主机添加节点、请使用StorageGRID主机服务命令行界面启动新节点： `sudo storagegrid node start [<node name\>]`

完成后

部署所有新网格节点后，您可以"执行扩展"。

设备：部署存储，网关或非主管理节点

要在设备节点上安装 StorageGRID 软件，请使用设备中提供的 StorageGRID 设备安装程序。在扩展中，每个存储设备都充当一个存储节点，而每个服务设备则充当一个网关节点或非主管理节点。任何设备都可以连接到网格网络，管理网络和客户端网络。

开始之前

- 此设备已安装在机架或机柜中，并已连接到您的网络并已启动。
- 您已完成这些 "设置硬件"步骤。

  设置设备硬件包括配置StorageGRID 连接(网络链路和IP地址)所需的步骤、以及启用节点加密、更改RAID模式和重新映射网络端口的可选步骤。

- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。
- 替代设备上的 StorageGRID 设备安装程序固件与网格上当前运行的 StorageGRID 软件版本兼容。如果这些版本不兼容、则必须升级StorageGRID 设备安装程序固件。
- 您有一台带的服务笔记本电脑"支持的 Web 浏览器"。
- 您知道分配给设备计算控制器的一个 IP 地址。您可以对任何已连接的 StorageGRID 网络使用此 IP 地址。

关于此任务

在设备节点上安装 StorageGRID 的过程分为以下阶段：

- 您可以指定或确认主管理节点的 IP 地址以及设备节点的名称。
- 您开始安装，并等待卷配置完毕并安装软件。

  在执行设备安装任务时，安装将暂停。要恢复安装，请登录到网格管理器，批准所有网格节点并完成 StorageGRID 安装过程。

  > 如果您需要一次部署多个设备节点、可以使用设备安装脚本自动执行安装过程 `configure-sga.py`。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

   `https://Controller_IP:8443`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在 * 主管理节点 * 连接部分中，确定是否需要指定主管理节点的 IP 地址。

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

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

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

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

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

5. 在*Installation*部分中，确认当前状态为“Ready to start installation of *node name* into GRID with Primary Admin Node *admin_IP*”，并且已启用*Start Installation*按钮。

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

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

   当前状态更改为"正在安装"，并显示监控安装页面。

7. 如果扩展包含多个设备节点，请对每个设备重复上述步骤。

   > 如果您需要一次部署多个设备存储节点，则可以使用 configure-sga.py 设备安装脚本自动执行安装过程。

8. 如果需要手动访问监视器安装页面，请从菜单栏中选择*Monitor Installation*。

   监视器安装页面显示安装进度。

   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保先前安装中完成的任务不会重新运行。如果要重新运行安装、则不需要重新运行的任何任务都会显示绿色状态栏和状态"已跳过"。

9. 查看前两个安装阶段的进度。

   *1.配置设备 *

   在此阶段，将执行以下过程之一：

- 对于存储设备、安装程序将连接到存储控制器、清除任何现有配置、与SANtricity 操作系统通信以配置卷以及配置主机设置。
- 对于服务设备，安装程序将从计算控制器中的驱动器中清除任何现有配置，并配置主机设置。

2.安装 **OS**

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

10. 继续监控安装进度，直到控制台窗口显示一条消息，提示您使用网格管理器批准节点。

> 等待您在此扩展中添加的所有节点都准备好进行批准，然后再转到网格管理器来批准这些节点。

执行**StorageGRID**扩展

执行扩展时，新的网格节点将添加到现有 StorageGRID 部署中。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您具有配置密码短语。
- 您已部署要在此扩展中添加的所有网格节点。
- 您拥有"维护或root访问权限"。
- 如果您要添加存储节点，则已确认在恢复过程中执行的所有数据修复操作均已完成。请参阅。 "检查数据修复作业"
- 如果您要添加存储节点，并且要为这些节点分配自定义存储级别，则您已经拥有"已创建自定义存储级别"。此外、您还具有root访问权限、或者同时具有维护和ILM权限。
- 如果要添加新站点、则已查看并更新ILM规则。您必须确保在扩展完成之前不会将对象副本存储到新站点。例如，如果某个规则使用默认存储池(所有存储节点)，则必须"创建新存储池"仅包含现有存储节点和"更新ILM规则"ILM策略才能使用该新存储池。否则，一旦新站点上的第一个节点变为活动状态，对象就会复制到该站点。

关于此任务

执行扩展包括以下主要用户任务：

1. 配置扩展。
2. 开始扩展。
3. 下载新的恢复包文件。
4. 监控扩展步骤和阶段、直到安装和配置所有新节点并启动所有服务为止。

> 在大型网格上运行某些扩展步骤和阶段可能需要很长时间。例如，如果 Cassandra 数据库为空，则将 Cassandra 流式传输到新存储节点可能只需要几分钟的时间。但是，如果 Cassandra 数据库包含大量对象元数据，则此阶段可能需要数小时或更长时间。在"扩展Cassandr集群"或"启动Cassandr并流式传输数据"阶段、请勿重新启动任何存储节点。

步骤

1. 选择*维护* > 任务 > 网格扩展。

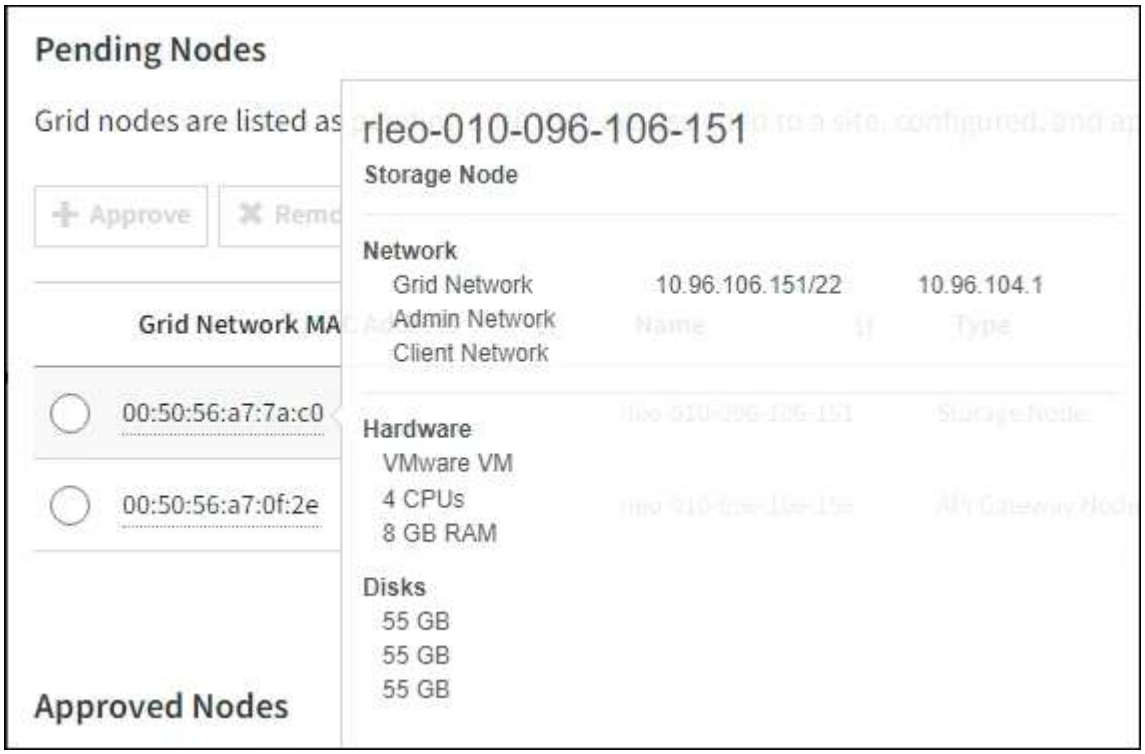
   此时将显示网格展开页面。"挂起节点"部分列出了已准备好添加的节点。

2. 选择 * 配置扩展 * 。

   此时将显示站点选择对话框。

3. 选择要启动的扩展类型：
   - 如果要添加新站点，请选择 * 新建 * ，然后输入新站点的名称。
   - 如果要向现有站点添加一个或多个节点，请选择*exist*。
4. 选择 * 保存 * 。
5. 查看 * 待定节点 * 列表，并确认它显示了您部署的所有网格节点。

   您可以根据需要将光标置于节点的*网格网络MAC地址*上，以查看有关该节点的详细信息。



   如果缺少节点、请确认已成功部署该节点。

6. 从待定节点列表中、批准要添加到此扩展中的节点。
   a. 选择要批准的第一个待定网格节点旁边的单选按钮。
   b. 选择 * 批准 * 。

      此时将显示网格节点配置表单。

   c. 根据需要修改常规设置：

字段	说明
站点	网格节点要关联的站点的名称。如果要添加多个节点，请确保为每个节点选择正确的站点。如果要添加新站点，则所有节点都将添加到新站点。
名称	节点的系统名称。内部StorageGRID 操作需要系统名称、并且无法更改。
存储类型(仅限存储节点)	• 数据和元数据("组合")：对象-数据和元数据存储节点 • 仅数据：存储节点仅包含对象数据(无元数据) • 仅元数据：仅包含元数据(无对象数据)的存储节点
NTP角色	网格节点的网络时间协议(NTP)角色： • 选择*Automatic (自动)*(默认)以自动将NTP角色分配给节点。主要角色将分配给管理节点、具有ADC服务的存储节点、网关节点以及具有非静态IP地址的任何网格节点。客户端角色将分配给所有其他网格节点。 • 选择*主*以手动将主NTP角色分配给节点。每个站点至少应有两个节点具有Primary角色、以便为外部计时源提供冗余系统访问。 • 选择*Client*以手动将客户端NTP角色分配给节点。
ADC服务(组合存储节点或纯元数据存储节点)	此存储节点是否将运行管理域控制器 (ADC) 服务。 ADC 服务跟踪电网服务的位置和可用性。每个站点至少有三个存储节点必须包含 ADC 服务。 • 如果您要更换的存储节点包括 ADC 服务，请选择*是*。由于如果剩余的 ADC 服务太少，您就无法停用存储节点，因此此设置可确保在删除旧服务之前有新的 ADC 服务可用。 • 你可以"将 ADC 服务移至同一站点上的另一个存储节点"以确保满足 ADC 服务法定人数。 • 选择*自动*让系统确定此节点是否需要ADC服务。 了解"ADC仲裁"。
存储级别(组合存储节点或纯数据存储节点)	使用*Default*存储级别，或选择要分配给此新节点的自定义存储级别。 存储级别由ILM存储池使用、因此您的选择可能会影响要放置在存储节点上的对象。

d. 根据需要修改网格网络，管理网络和客户端网络的设置。

   - * IPv4 地址（ CIDR ） *：网络接口的 CIDR 网络地址。例如： 172.16.10.100/24

如果在批准节点时发现节点在网格网络上具有重复的IP地址、则必须取消扩展、使用非重复IP重新部署虚拟机或设备、然后重新启动扩展。

- * 网关 * ： 网格节点的默认网关。例如： 172.16.10.1
- * 子网（ CIDR ） * ： 管理网络的一个或多个子网。

e. 选择 * 保存 * 。

批准的网格节点将移至批准的节点列表。

- 要修改已批准的网格节点的属性，请选择其单选按钮，然后选择 * 编辑 * 。
- 要将已批准的网格节点移回 "Pending Nodes" 列表，请选择其单选按钮，然后选择 * 重置 * 。
- 要永久删除已批准的网格节点，请关闭此节点。然后，选择其单选按钮并选择 * 删除 * 。

f. 对要批准的每个待定网格节点重复上述步骤。

如果可能，您应批准所有待定网格注释并执行一次扩展。如果执行多个小型扩展，则需要更多时间。

7. 批准所有网格节点后，输入*配置密码*，然后选择*扩展*。

几分钟后，此页面将更新以显示扩展操作步骤 的状态。如果正在执行影响各个网格节点的任务、则"Grid Node Status"部分将列出每个网格节点的当前状态。

在新设备的"安装网格节点"步骤中、StorageGRID设备安装程序会显示安装从第3阶段移至第4阶段"完成安装"。阶段 4 完成后，控制器将重新启动。

站点扩展包括一项额外任务，用于为新站点配置 Cassandra 。

8. 一旦出现*下载恢复包*链接，请下载恢复包文件。

对StorageGRID系统进行网格拓扑更改后，您必须尽快下载恢复包文件的更新副本。如果发生故障，恢复包文件可让您恢复系统。

a. 选择下载链接。
b. 输入配置密码短语，然后选择 * 开始下载 * 。
c. 下载完成后、打开 `.zip`文件并确认您可以访问其中的内容、包括 `Passwords.txt`文件。
d. 复制下载的恢复包文件(`.zip`）到两个安全、可靠且独立的位置。

恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

9. 如果要向现有站点添加存储节点或添加站点、请监控Cassandr阶段、这些阶段会在新网格节点上启动服务时发生。

在"扩展Cassandr集群"或"启动Cassandr并流式传输数据"阶段、请勿重新启动任何存储节点。对于每个新存储节点，这些阶段可能需要花费数小时才能完成，尤其是在现有存储节点包含大量对象元数据的情况下。

正在添加存储节点

如果要向现有站点添加存储节点、请查看"正在启动cassand拉 并流式传输数据"状态消息中显示的百分比。

此百分比根据可用的 Cassandra 数据总量以及已写入新节点的数据量估计 Cassandra 流操作的完成程度。

正在添加站点

如果要添加新站点、请使用 `nodetool status`监控cassanda流式传输的进度、并查看在"扩展cassanda集群"阶段向新站点复制了多少元数据。新站点上的总数据负载应介于当前站点总负载的 20% 左右。

10. 继续监控扩展，直到所有任务均完成，并且 * 配置扩展 * 按钮再次出现。

完成后

根据您添加的网格节点类型、执行其他集成和配置步骤。请参阅。 "扩展后的配置步骤"

添加存储卷

向StorageGRID系统添加存储卷

您可以扩展低于最大支持卷数的存储节点的存储容量。您可能需要将存储卷添加到多个存储节点以满足复制或擦除编码副本的 ILM 要求。

开始之前

在添加存储卷之前、请查看"添加对象容量的准则"以确保您知道要将卷添加到何处以满足ILM策略的要求。

这些说明仅适用于基于软件的存储节点。请参见 "将扩展架添加到已部署的SG6060"或 "将扩展架添加到已部署的SG6160"、了解如何通过安装扩展架向SG6060或SG6160添加存储卷。无法扩展其他设备存储节点。

关于此任务

存储节点的底层存储分为多个存储卷。存储卷是基于块的存储设备，由 StorageGRID 系统格式化并挂载以存储对象。每个存储节点最多可支持 48 个存储卷，在网格管理器中称为 *object stores* 。

对象元数据始终存储在对象存储 0 中。

每个对象存储都挂载在与其 ID 对应的卷上。例如、ID为0000的对象存储对应于 `/var/local/rangedb/0`挂载点。

在添加新存储卷之前，请使用网格管理器查看每个存储节点的当前对象存储以及相应的挂载点。您可以在添加存储卷时使用此信息。

步骤

1. 选择 节点 > 站点 > 存储节点 > 存储。
2. 向下滚动以查看每个卷和对象存储的可用存储容量。

   对于设备存储节点、每个磁盘的全球通用名称与在SANtricity OS (连接到设备存储控制器的管理软件)中查看标准卷属性时显示的卷全球通用标识符(WWID)匹配。

   为了帮助您解释与卷挂载点相关的磁盘读取和写入统计信息，磁盘设备表的 * 名称 * 列（即 *sdc* ， *sdd* ， *sde* 等）中显示的名称的第一部分与卷表的 * 设备 * 列中显示的值匹配。

Disk devices

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

Volumes

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

Object stores

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

3. 按照适用于您的平台的说明向存储节点添加新存储卷。
   - "VMware： 将存储卷添加到存储节点"
   - "Linux： 将直连卷或 SAN 卷添加到存储节点"

在StorageGRID中向 VMware 存储节点添加存储卷

如果存储节点包含的存储卷少于 16 个，则可以使用 VMware vSphere 添加卷来增加其容量。

开始之前

- 您可以访问"为 VMware 部署安装StorageGRID的说明"。
- 您已获得 `Passwords.txt`文件。
- 您拥有 "特定访问权限"。

> 在软件升级、恢复操作步骤 或其他扩展操作步骤 处于活动状态时、请勿尝试向存储节点添加存储卷。

关于此任务

添加存储卷时，此存储节点将暂时不可用。您应一次在一个存储节点上执行此操作步骤 ，以避免影响面向客户端的网格服务。

步骤

1. 如有必要，请安装新的存储硬件并创建新的 VMware 数据存储库。
2. 向虚拟机添加一个或多个硬盘以用作存储（对象存储）。
   a. 打开 VMware vSphere Client 。
   b. 编辑虚拟机设置以添加一个或多个附加硬盘。

   硬盘通常配置为虚拟机磁盘（ Virtual Machine Disk ， VMDK ）。VMDK更常用且更易于管理、而对于使用较大对象(例如大于100 MB)的工作负载、RDM可能会提供更好的性能。有关向虚拟机添加硬盘的详细信息，请参见 VMware vSphere 文档。
3. 使用VMware vSphere Client中的*Restart Guest OS*选项或在与虚拟机的ssh会话中输入以下命令，重新启动虚拟机：`sudo reboot`

   > 请勿使用*Power Off*或*Reset *重新启动虚拟机。
4. 配置新存储以供存储节点使用：
   a. 登录到网格节点：
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入文件中列出的密码 `Passwords.txt`。
      iii. 输入以下命令切换到root： `su -`
      iv. 输入文件中列出的密码 `Passwords.txt`。当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

b. 配置新存储卷：

```
sudo add_rangedbs.rb
```

此脚本将查找任何新存储卷并提示您对其进行格式化。

c. 输入 * 。 * 接受格式化。

d. 如果先前已对任何卷进行格式化，请确定是否要重新格式化这些卷。

- 输入 * y * 重新格式化。
- 输入 * 。 n* 可跳过重新格式化。

该 `setup_rangedbs.sh`脚本将自动运行。

5. 检查服务是否正确启动：

a. 查看服务器上所有服务的状态列表：

```
sudo storagegrid-status
```

状态将自动更新。

a. 请等待所有服务均已运行或已验证。

b. 退出状态屏幕：

```
Ctrl+C
```

6. 验证存储节点是否联机：

a. 使用登录到网格管理器"支持的 Web 浏览器"。

b. 选择“节点”>“存储节点”>“任务”。

c. 如果“存储状态”下拉列表设置为“只读”或“离线”，请选择“在线”。

d. 选择 * 保存 * 。

7. 要查看新的对象存储，请选择*存储*。

8. 查看*Volumes*表中的详细信息。

结果

您可以使用存储节点的扩展容量来保存对象数据。

在StorageGRID中向 Linux 存储节点添加直连卷或 SAN 卷

如果某个存储节点包含的存储卷少于 48 个，则可以通过添加新的块存储设备，使其对 Linux 主机可见，并将新的块设备映射添加到用于该存储节点的 StorageGRID 配置文件来增加其容量。

开始之前

- 您可以访问"StorageGRID安装说明"适用于您的 Linux 平台。

- 您已获得 `Passwords.txt`文件。
- 您拥有 "特定访问权限"。

> 在软件升级、恢复操作步骤 或其他扩展操作步骤 处于活动状态时、请勿尝试向存储节点添加存储卷。

关于此任务

添加存储卷时，此存储节点将暂时不可用。您应一次在一个存储节点上执行此操作步骤 ，以避免影响面向客户端的网格服务。

步骤

1. 安装新的存储硬件。

   有关详细信息，请参见硬件供应商提供的文档。

2. 创建所需大小的新块存储卷。
   - 连接新驱动器并根据需要更新RAID控制器配置、或者在共享存储阵列上分配新的SAN LUN并允许Linux主机访问这些LUN。
   - 请使用与现有存储节点上的存储卷相同的永久性命名方案。
   - 如果使用 StorageGRID 节点迁移功能，请使作为此存储节点迁移目标的其他 Linux 主机可以看到新卷。有关详细信息，请参见有关为 Linux 平台安装 StorageGRID 的说明。
3. 以root用户或具有sudo权限的帐户登录到支持此存储节点的Linux主机。
4. 确认新存储卷在 Linux 主机上可见。

   您可能需要重新扫描设备。

5. 运行以下命令以临时禁用存储节点：

   ```
   sudo storagegrid node stop <node-name>
   ```

6. 使用vio或pica等文本编辑器编辑存储节点的节点配置文件，该文件位于 `/etc/storagegrid/nodes/<node-name>.conf`。
7. 找到节点配置文件中包含现有对象存储块设备映射的部分。

   在此示例中、 `BLOCK_DEVICE_RANGEDB_00`到 `BLOCK_DEVICE_RANGEDB_03`是现有对象存储块设备映射。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. 添加与为此存储节点添加的块存储卷对应的新对象存储块设备映射。

   确保从下一个开始 `BLOCK_DEVICE_RANGEDB_nn`。不要留下差距。

   - 根据上面的示例，从开始 `BLOCK_DEVICE_RANGEDB_04`。
   - 在以下示例中，节点中添加了四个新的块存储卷： `BLOCK_DEVICE_RANGEDB_04`至 `BLOCK_DEVICE_RANGEDB_07`。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. 运行以下命令以验证对存储节点的节点配置文件所做的更改：

   ```
   sudo storagegrid node validate <node-name>
   ```

   解决所有错误或警告，然后再继续下一步。

如果您发现类似以下内容的错误、则表示节点配置文件正在尝试将用于的 `<PURPOSE>`块设备映射 `<node-name>`到Linux文件系统中提供的、 `<path-name>`但该位置没有有效的块设备专用文件(或指向块设备专用文件的软链接)。

```
Checking configuration file for node <node-name>…
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device
```

验证您输入的是否正确 `<path-name>`。

10. 运行以下命令以重新启动具有新块设备映射的节点：

```
sudo storagegrid node start <node-name>
```

11. 使用文件中列出的密码以管理员身份登录到存储节点 `Passwords.txt`。
12. 检查服务是否正确启动：
    a. 查看服务器上所有服务的状态列表：+
    ```
    sudo storagegrid-status
    ```
    状态将自动更新。
    b. 请等待所有服务均已运行或已验证。
    c. 退出状态屏幕：
    ```
    Ctrl+C
    ```
13. 配置新存储以供存储节点使用：
    a. 配置新存储卷：
    ```
    sudo add_rangedbs.rb
    ```
    此脚本将查找任何新存储卷并提示您对其进行格式化。
    b. 输入 * 。 * 格式化存储卷。
    c. 如果先前已对任何卷进行格式化，请确定是否要重新格式化这些卷。
       - 输入 * y * 重新格式化。
       - 输入 * 。 n* 可跳过重新格式化。

    该 `setup_rangedbs.sh`脚本将自动运行。
14. 验证存储节点的存储状态是否为联机：
    a. 使用登录到网格管理器"支持的 Web 浏览器"。
    b. 选择“节点”>“存储节点”>“任务”。
    c. 如果“存储状态”下拉列表设置为“只读”或“离线”，请选择“在线”。

d. 选择 * 保存 * 。

15. 要查看新的对象存储，请选择*存储*。
16. 查看*Volumes*表中的详细信息。

结果

现在，您可以使用存储节点的扩展容量来保存对象数据。

配置扩展系统

在StorageGRID中配置新添加的节点和站点

完成扩展后，您必须执行其他集成和配置步骤。

关于此任务

您必须为要添加到扩展中的网格节点或站点完成下面列出的配置任务。某些任务可能是可选的、具体取决于在安装和管理系统时选择的选项、以及您希望如何配置扩展期间添加的节点和站点。

步骤

1. 如果您添加了站点：
   - "创建存储池"对于站点以及为新存储节点选择的每个存储级别。
   - 确认ILM策略满足新要求。如果需要更改规则，请执行、"创建新规则"和"更新ILM策略"。如果规则已正确、则不会更改任何规则、"激活新策略"以确保StorageGRID使用新节点。
   - 确认可从该站点访问网络时间协议(Network Time Protocol、NTP)服务器。请参阅。 "管理NTP服务器"

     确保每个站点至少有两个节点可以访问至少四个外部 NTP 源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。

2. 如果向现有站点添加了一个或多个存储节点：
   - "查看存储池详细信息"确认添加的每个节点都包含在预期存储池中并在预期ILM规则中使用。
   - 确认ILM策略满足新要求。如果需要更改规则，请执行、"创建新规则"和"更新ILM策略"。如果规则已正确、则不会更改任何规则、"激活新策略"以确保StorageGRID使用新节点。
   - "验证存储节点是否处于活动状态"并且能够加热对象。
   - 如果您无法添加建议数量的存储节点、请重新平衡已进行过重复数据检索的数据。请参阅。 "添加存储节点后重新平衡经过纠删编码的数据"
3. 如果添加了网关节点：
   - 如果客户端连接使用高可用性 (HA) 组，则可以选择将网关节点添加到 HA 组。选择“配置”>“网络”>“高可用性组”来查看现有 HA 组的列表并添加新节点。看"配置高可用性组" 。
4. 如果添加了管理节点：
   a. 如果您的 StorageGRID 系统启用了单点登录 (SSO)，请为新的管理节点创建一个依赖方信任。在创建此依赖方信任之前，无法登录到该节点。请参阅使用 "OIDC" 或 "SAML" 设置 SSO。
   b. 如果您计划在管理节点上使用负载均衡器服务，则可以选择将新的管理节点添加到 HA 组。选择“配置”>“

网络”>“高可用性组”来查看现有 HA 组的列表并添加新节点。看"配置高可用性组" 。

c. 如果要使每个管理节点上的历史指标保持一致，也可以将 Prometheus 数据库从主管理节点复制到扩展管理节点。请参阅。 "复制 Prometheus 指标"

d. 如果要使每个管理节点上的历史日志信息保持一致，也可以将现有审核日志从主管理节点复制到扩展管理节点。请参阅。 "复制审核日志"

5. 要检查扩展节点是否添加了不受信任的客户端网络，或者要更改节点的客户端网络是否不受信任或受信任，请转到*配置*>*安全*>*防火墙控制*。

   如果扩展节点上的客户端网络不可信，则必须使用负载平衡器端点与客户端网络上的节点建立连接。请参阅"配置负载平衡器端点"和"管理防火墙控制"。

6. 配置DNS。

   如果您一直在为每个网格节点单独指定 DNS 设置，则必须为新节点添加自定义的每节点 DNS 设置。请参阅。 "修改单网格节点的 DNS 配置"

要确保正常运行、请指定两个或三个DNS服务器。如果指定的值超过三个、则可能仅使用三个、因为某些平台上存在已知的操作系统限制。如果您的环境存在路由限制、则各个节点(通常是站点上的所有节点)可以"自定义DNS服务器列表"使用一组不同的DNS服务器、最多可使用三个。

如果可能、请使用每个站点可以在本地访问的DNS服务器、以确保受支持的站点可以解析外部目标的FQDN。

在StorageGRID扩展后，验证存储节点是否处于活动状态。

添加新存储节点的扩展操作完成后， StorageGRID 系统应自动开始使用新存储节点。您必须使用 StorageGRID 系统验证新存储节点是否处于活动状态。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 选择“节点”>“扩展存储节点”>“存储”。
3. 将光标置于*已用存储-对象数据*图形上方可查看*已用*的值，即已用于对象数据的总可用空间量。
4. 将光标移至图形右侧时，请验证 * 已用 * 的值是否正在增加。

将 Prometheus 指标复制到StorageGRID中的新管理节点

添加新的管理节点后，您可以选择将 Prometheus 维护的历史指标从主管理节点复制到新的管理节点。复制指标可确保管理节点之间的历史指标一致。

开始之前

- 新管理节点已安装并正在运行。
- 您已获得 `Passwords.txt`文件。
- 您具有配置密码短语。

关于此任务

添加管理节点时，软件安装过程会创建一个新的 Prometheus 数据库。您可以通过将 Prometheus 数据库从主管理节点（ _source 管理节点 _ ）复制到新管理节点来保持节点之间的历史指标一致。

复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。
2. 从源管理节点中、停止Prometheus服务： `service prometheus stop`
3. 在新管理节点上完成以下步骤：
   a. 登录到新的管理节点：
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入文件中列出的密码 `Passwords.txt`。
      iii. 输入以下命令切换到root： `su -`
      iv. 输入文件中列出的密码 `Passwords.txt`。
   b. 停止Prometheus服务： `service prometheus stop`
   c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   d. 输入文件中列出的SSH访问密码 `Passwords.txt`。
   e. 将Prometheus数据库从源管理节点复制到新管理节点：
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出现提示时，按 * 输入 * 确认要销毁新管理节点上的新 Prometheus 数据库。

      原始 Prometheus 数据库及其历史数据将复制到新的管理节点。完成复制操作后，此脚本将启动新的管理节点。此时将显示以下状态：

```
Database cloned, starting services
```

   a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入 …

```
ssh-add -D
```

4. 在源管理节点上重新启动 Prometheus 服务。

```
service prometheus start
```

将审计日志复制到StorageGRID中的新管理节点

当您通过扩展程序添加新的管理节点时，其 AMS 服务仅记录其加入系统后发生的事件和操作。根据需要，您可以将审计日志从先前安装的管理节点复制到新的扩展管理节点，以

便它与StorageGRID系统的其余部分同步。

开始之前

- 您已完成添加管理节点所需的扩展步骤。
- 您已获得 `Passwords.txt`文件。

关于此任务

要使历史审核消息在新管理节点上可用，必须手动将审核日志文件从现有管理节点复制到扩展管理节点。

> 默认情况下，审计信息将发送到 `localaudit`登录每个节点。要使用此过程，您必须将管理节点配置为审计目标，如下所示：
>
> - 您将 管理节点/本地节点 配置为日志目标。
> - 您已将*管理节点和外部系统日志服务器*配置为日志目标。
>
> 参考"配置审核消息和外部系统日志服务器"了解详情。

步骤

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

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 停止AMS服务以防止其创建新文件： `service ams stop`
3. 导航到审核导出目录：

   ```
   cd /var/local/audit/export/
   ```

4. 重命名源 `audit.log`文件以确保它不会覆盖您要将其复制到的扩展管理节点上的文件：

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```

5. 将所有审核日志文件复制到扩展管理节点上的目标位置：

   ```
   scp -p * IP_address:/var/local/audit/export/
   ```

6. 如果系统提示您输入的密码短语 `/root/.ssh/id_rsa`，请输入文件中列出的主管理节点的SSH访问密码 `Passwords.txt`。
7. 还原原始 `audit.log`文件：

```
mv new_name.txt audit.log
```

8. 启动 AMS 服务：

```
service ams start
```

9. 从服务器注销：

```
exit
```

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

    当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

11. 更新审核日志文件的用户和组设置：

```
cd /var/local/audit/export/

chown ams-user:bycast *
```

12. 从服务器注销：

```
exit
```

在向StorageGRID系统添加节点后，重新平衡纠删码数据。

添加存储节点后、您可以使用纠删编码(EC)重新平衡过程在现有存储节点和新存储节点之间重新分布经过纠删编码的片段。

开始之前

- 您已完成添加新存储节点的扩展步骤。
- 您已查看"重新平衡经过纠删编码的数据的注意事项"。
- 您了解复制的对象数据不会被此过程移动，并且 EC 重新平衡过程不会移动复制的数据。但是，在确定将 EC 数据移动到何处时，会考虑复制数据。
- 您已获得 `Passwords.txt`文件。

此操作步骤 运行时会发生什么情况

启动操作步骤 之前、请注意以下事项：

- 如果一个或多个卷脱机(卸载)或联机(挂载)但处于错误状态、EC重新平衡操作步骤 将不会启动。
- EC 重新平衡操作步骤 会临时预留大量存储。可能会触发存储警报，但会在重新平衡完成后解决。如果没有足够的存储空间用于预留， EC 重新平衡操作步骤 将失败。无论操作步骤 出现故障还是成功， EC 重新平

衡操作步骤 完成后都会释放存储预留。

- 如果在EC重新平衡操作步骤正在进行时卷脱机、重新平衡操作步骤将终止。已移动的任何数据片段将保留在其新位置、不会丢失任何数据。

  您可以在所有卷恢复联机后重新运行操作步骤。

- 运行EC重新平衡过程时、ILM操作和S3客户端操作的性能可能会受到影响。

  > 如果要上传对象(或对象部件)的S3 API操作需要24小时以上才能完成、则在EC重新平衡过程中这些操作可能会失败。如果适用的ILM规则在加载时使用平衡放置或严格放置、则长时间放置操作将失败。将报告以下错误： `500 Internal Server Error`。

- 工作完成条件。当满足以下任一条件时、EC重新平衡过程被视为已完成：
  - 它无法再移动任何经过了经过数据经过了数据迁移的数据。
  - 所有节点中的数据与目标可用空间分区的偏差均在 5% 以内。
  - 操作步骤已运行30天。

步骤

1. 【 Review object_storage]] 查看计划重新平衡的站点的当前对象存储详细信息。
   a. 选择*节点*。
   b. 选择站点上的第一个存储节点。
   c. 选择 * 存储 * 选项卡。
   d. 将光标置于"已用存储-对象数据"图表上方、可查看存储节点上当前复制的数据量和经过重复数据操作的数据。
   e. 重复上述步骤以查看站点上的其他存储节点。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
3. 启动操作步骤 ：

   `re平衡数据启动—site "*ssite-name*"

   对于"*site-name*"、指定添加新存储节点的第一个站点。用引号括起来。 `site-name`

   此时将启动 EC 重新平衡操作步骤 ，并返回作业 ID 。
4. 复制作业 ID 。
5. 监控EC重新平衡操作步骤的状态。

- 要查看单个 EC 重新平衡操作步骤 的状态，请执行以下操作：

  `rebalance-data status --job-id job-id`

  对于 *job-id*，指定在开始过程时返回的ID。

- 要查看当前 EC 重新平衡操作步骤 的状态以及先前完成的任何过程：

  `rebalance-data status`

> 要获取有关 rebalance-data 命令的帮助，请执行以下操作：
>
> `rebalance-data --help`

6. 根据返回的状态执行其他步骤：

   - 如果 `State`为 `In progress`，则EC重新平衡操作仍在运行。您应定期监控操作步骤 ，直到其完成。

     转到节点页面来评估站点中存储节点的数据分布。

   当所有节点中的可用空间与目标可用空间分区的偏差在 5% 以内时，EC 再平衡作业将被视为完成并停止。

   - 如果 `State`是 `Success`，则可以选择查看对象存储查看站点的更新详细信息。

     现在，站点上的存储节点之间的可用空间应该更加平衡。

   - 如果 `State`为 `Failure`：

     i. 确认站点上的所有存储节点均已连接到网格。

     ii. 检查并解决可能影响这些存储节点的任何警报。

     iii. 重新启动EC重新平衡操作步骤 ：

     `rebalance-data start --job-id job-id`

     iv. 查看状态新程序的执行情况。如果 `State`仍然存在 `Failure`，请联系技术支持。

7. 如果 EC 重新平衡操作步骤 生成的负载过多（例如，载入操作受到影响），请暂停操作步骤 。

   `rebalance-data pause --job-id job-id`

8. 如果您需要终止 EC 重新平衡操作步骤 （例如，以便执行 StorageGRID 软件升级），请输入以下内容：

   `rebalance-data terminate --job-id job-id`

> 终止EC重新平衡操作步骤后、已移动的所有数据片段仍会保留在其新位置。数据不会移回原始位置。

9. 如果要在多个站点上使用纠删编码，请对所有其他受影响站点运行此操作步骤 。

排查StorageGRID中的扩展错误

如果在网格扩展过程中遇到无法解决的错误、或者网格任务失败、请收集日志文件并联系技术支持。

在联系技术支持之前、请收集所需的日志文件以帮助进行故障排除。

步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 连接到发生故障的扩展节点：

   a. 输入以下命令： `ssh -p 8022 admin@grid_node_IP`

      端口 8022 是基础操作系统的 SSH 端口，而端口 22 是运行 StorageGRID 的容器引擎的 SSH 端口。

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   以root用户身份登录后，提示符将从更 `$` 改为 `#`。

3. 根据安装达到的阶段，检索网格节点上提供的以下任何日志：

平台	日志
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf`(对于每个故障节点) • `/var/log/storagegrid/nodes/<node-name>.log`(对于每个故障节点；可能不存在)

4. 如果您允许外部 SSH 访问，"阻止访问"当你完成任务时。

维护StorageGRID系统

StorageGRID 网格维护

网格维护任务包括停用节点或站点、重命名网格、节点或站点以及维护网络。您还可以执行主机和中间件过程以及网格节点过程。

> 在这些说明中，“Linux”指的是 Red Hat® Enterprise Linux® (RHEL)、Ubuntu® 或 Debian® 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具"。

开始之前

- 您对 StorageGRID 系统有着广泛的了解。
- 您已查看 StorageGRID 系统的拓扑并了解网格配置。
- 您知道必须严格按照所有说明进行操作，并注意所有警告。
- 您了解、未介绍的维护过程不受支持或不需要服务项目。

设备的维护过程

有关硬件过程，请参见 "StorageGRID设备的维护说明"。

下载 StorageGRID 恢复包

如果发生故障，恢复包文件允许您恢复StorageGRID系统。

开始之前

- 从任何管理节点，您都可以使用"支持的 Web 浏览器"。
- 您具有配置密码短语。
- 您拥有 "特定访问权限"。

在对StorageGRID系统进行网格拓扑更改或升级软件之前，请下载当前的恢复包文件。然后，在更改电网拓扑或升级软件后下载恢复包的新副本。

步骤

1. 选择*维护* > 系统 > 恢复包。
2. 输入配置密码短语，然后选择*Start download*。

   下载将立即开始。
3. 下载完成后、打开 `.zip`文件并确认您可以访问其中的内容、包括 `Passwords.txt`文件。
4. 复制下载的恢复包文件(`.zip`）到两个安全、可靠且独立的位置。

恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

停用节点或站点

停用 StorageGRID 节点或站点

您可以执行停用操作步骤 ，以便从 StorageGRID 系统中永久删除网格节点或整个站点。

要删除网格节点或站点，请执行以下停用过程之一：

- 执行"网格节点停用"以删除一个或多个节点、这些节点可以位于一个或多个站点上。您删除的节点可以联机并连接到 StorageGRID 系统，也可以脱机并断开连接。
- 执行"站点停用"以删除站点。如果所有节点都连接到StorageGRID ，则执行*已连接站点停用*。如果所有节点都与StorageGRID 断开连接，则执行*断开连接的站点停用*。如果站点中既有已连接节点、也有已断开连接的节点、则必须将所有脱机节点恢复联机。

在执行断开连接的站点停用之前、请联系您的NetApp客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。如果您认为可以恢复站点或从站点恢复对象数据，则不应尝试执行已断开连接的站点停用。

在退役网格节点之前，您必须确认没有处于活动状态的数据修复作业。如果任何修复失败，则必须重新启动它们并让它们完成，然后再执行退役程序。请参阅"检查数据修复作业" 。

停用节点

StorageGRID 网格节点停用

您可以使用节点停用操作步骤删除一个或多个站点上的一个或多个网格节点。您不能停用主管理节点。

何时停用节点

如果满足以下任一条件，请使用节点停用操作步骤 ：

- 您在扩展中添加了一个较大的存储节点、并且希望删除一个或多个较小的存储节点、同时保留对象。

如果要将旧设备更换为新设备、请考虑 "正在克隆设备节点"不要在扩展中添加新设备、然后停用旧设备。

- 您所需的总存储较少。
- 您不再需要网关节点。
- 您不再需要非主管理节点。
- 您的网格包含一个无法恢复或恢复联机的已断开节点。
- 网格包含一个归档节点。

如何停用节点

您可以停用已连接的网格节点或已断开连接的网格节点。

停用已连接节点

一般来说，只有当网格节点连接到StorageGRID系统并且所有节点都处于正常状态（在 节点 页面和 退役节点 页面上有绿色图标）时，才应该退役网格节点。

有关说明，请参阅"停用已连接的网格节点"。

停用已断开连接的节点

在某些情况下、您可能需要停用当前未连接到网格的网格节点(运行状况未知或已被管理员关闭的节点)。

有关说明，请参阅"停用已断开连接的网格节点"。

停用节点前应考虑的事项

在执行任一操作步骤之前、请查看每种类型节点的注意事项：

- "停用管理节点或网关节点的注意事项"
- "存储节点停用注意事项"

StorageGRID 管理或网关节点停用注意事项

查看停用管理节点或网关节点的注意事项。

管理节点注意事项

- 您不能停用主管理节点。
- 如果某个管理节点的某个网络接口属于高可用性(HA)组、则无法停用该节点。您必须先从 HA 组中删除网络接口。请参阅的说明"管理HA组"。
- 在停用管理节点时、您可以根据需要安全地更改ILM策略。
- 如果停用管理节点并为 StorageGRID 系统启用了单点登录（ SSO ），则必须记住从 Active Directory 联合身份验证服务（ AD FS ）中删除该节点的依赖方信任。
- 如果使用"网格联盟"，请确保没有为网格联合连接指定要停用的节点的IP地址。
- 停用已断开连接的管理节点时，该节点上的审核日志将丢失；但是，这些日志也应存在于主管理节点上。

网关节点的注意事项

- 如果某个网关节点的某个网络接口属于高可用性(HA)组、则无法停用该节点。您必须先从 HA 组中删除网络接口。请参阅的说明"管理HA组"。
- 在停用网关节点时、您可以根据需要安全地更改ILM策略。
- 如果使用"网格联盟"，请确保没有为网格联合连接指定要停用的节点的IP地址。
- 您可以在网关节点断开连接时安全地停用它。

StorageGRID 中的存储节点停用注意事项

在停用存储节点之前、请考虑是否可以克隆此节点。然后、如果您决定停用此节点、请查看StorageGRID在停用操作步骤期间如何管理对象和元数据。

何时克隆节点而不是停用节点

如果要将旧设备存储节点更换为新设备或更大的设备、请考虑克隆设备节点、而不是在扩展中添加新设备、然后停用旧设备。

通过设备节点克隆、您可以轻松地将现有设备节点更换为同一StorageGRID站点上的兼容设备。克隆过程会将所有数据传输到新设备、将新设备置于运行状态、并使旧设备处于预安装状态。

如果需要，您可以克隆设备节点：

- 更换即将达到使用寿命的产品。
- 升级现有节点以利用改进的设备技术。
- 增加网格存储容量，而不更改 StorageGRID 系统中的存储节点数。
- 提高存储效率、例如通过更改RAID模式。

有关详细信息、请参见。 "设备节点克隆"

已连接存储节点的注意事项

查看停用已连接存储节点的注意事项。

- 在一个 " 停用节点 " 操作步骤 中停用的存储节点不应超过 10 个。
- 系统必须始终包括足够的存储节点，以满足操作要求，包括"ADC仲裁"和活动的"ILM策略"。如果停用会使站点的 ADC 计数低于法定数量，StorageGRID 会自动将 ADC 服务移动到同一站点上的可用非 ADC 存储节点，从而保持 ADC 法定数量。如果无法自动移动 ADC 服务，则可能需要先"在扩展操作中添加新 Storage Node"，然后才能停用现有存储节点。

  在包含基于软件的纯元数据节点的网格中停用存储节点时、请务必小心谨慎。如果停用配置为存储_Both _对象和元数据的所有节点、则会从网格中删除存储对象的功能。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

- 删除存储节点后、将通过网络传输大量对象数据。尽管这些传输不会影响正常系统操作、但它们会影响StorageGRID系统占用的网络带宽总量。
- 与正常系统操作相关的任务相比，与存储节点停用相关的任务的优先级更低。这意味着停用不会干扰 StorageGRID 系统的正常运行，也不需要计划系统在一段时间内处于非活动状态。由于停用是在后台执行的，因此很难估计完成此过程需要多长时间。通常，在系统处于静默状态或一次仅删除一个存储节点时，停用速度会更快。
- 停用存储节点可能需要数天或数周时间。相应地规划此操作步骤 。尽管停用过程不会影响系统运行，但它会限制其他过程。通常，在删除网格节点之前，您应执行任何计划内的系统升级或扩展。
- 如果您需要在删除存储节点期间执行另一个维护过程、则可以在另一过程完成后继续执行"暂停停用操作步骤"。

只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。

- 正在运行停用任务时、无法在任何网格节点上运行数据修复操作。
- 在停用存储节点期间、不应对ILM策略进行任何更改。
- 要永久安全地删除数据、您必须在停用操作步骤完成后擦除存储节点的驱动器。

断开连接的存储节点的注意事项

查看停用已断开连接的存储节点的注意事项。

- 切勿停用已断开连接的节点、除非您确定该节点无法联机或恢复。

如果您认为可以从节点中恢复对象数据、请勿执行此操作步骤。请联系技术支持以确定是否可以进行节点恢复。

- 停用已断开连接的存储节点时、StorageGRID会使用其他存储节点中的数据重建已断开连接的节点上的对象数据和元数据。
- 如果停用多个断开连接的存储节点、可能会发生数据丢失。如果没有足够的对象副本，纠删编码片段或对象元数据保持可用，则系统可能无法重建数据。在使用基于软件的纯元数据节点的网格中停用存储节点时、停用配置为同时存储对象和元数据的所有节点会从网格中删除所有对象存储。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

如果您有多个无法恢复的已断开连接的存储节点、请联系技术支持以确定最佳操作方案。

- 停用已断开连接的存储节点时， StorageGRID 会在停用过程结束时启动数据修复作业。这些作业会尝试重建已断开连接的节点上存储的对象数据和元数据。
- 停用已断开连接的存储节点时，停用操作步骤 的完成速度相对较快。但是、数据修复作业可能需要数天或数周才能运行、并且不受停用操作步骤 的监控。您必须手动监控这些作业并根据需要重新启动它们。请参阅。"检查数据修复作业"
- 如果停用的存储节点已断开连接，而该存储节点包含某个对象的唯一副本，则该对象将丢失。只有当当前连接的存储节点上至少存在一个复制副本或足够多的纠删编码片段时，数据修复作业才能重建和恢复对象。

什么是 **StorageGRID ADC** 仲裁?

ADC 仲裁可确保每个站点保持最低数量的管理域控制器 (ADC) 服务可用。StorageGRID 在需要时会在停用期间自动移动 ADC 服务。

某些存储节点上的ADC服务负责维护网格拓扑信息并为网格提供配置服务。StorageGRID 系统要求每个站点始终提供一定的数字转换服务仲裁。

如果删除存储节点会发生原因 使不再满足ADC仲裁、则无法停用该节点。要在停用期间满足ADC仲裁要求、每个站点上至少必须有三个存储节点具有ADC服务。如果站点中有三个以上的存储节点使用ADC服务、则停用后、这些节点中的简单多数必须保持可用： `((0.5 * Storage Nodes with ADC) + 1)`

在包含基于软件的纯元数据节点的网格中停用存储节点时、请务必小心谨慎。如果停用配置为存储_Both _对象和元数据的所有节点、则会从网格中删除存储对象的功能。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

例如、假设某个站点当前包含六个具有ADC服务的存储节点、而您要停用三个存储节点。由于需要使用 ADC 仲裁，您必须完成两个停用过程，如下所示：

- 在第一次停用过程中，必须确保具有ADC服务的四个存储节点保持可用： `((0.5 * 6) + 1)`。这意味着最初只能停用两个存储节点。
- 在第二个退役过程中，您可以删除第三个存储节点，因为 ADC 仲裁现在只需要三个 ADC 服务保持可用： `((0.5 * 4) + 1)`。

当您停用具有 ADC 服务的存储节点时，如果停用会使站点的 ADC 计数低于法定数量，StorageGRID 会自动将 ADC 服务移动到同一站点上的另一个存储节点。自动移动要求网格中的所有节点都已连接，并且同一站点上有可用的非 ADC 存储节点来接收该服务。停用程序为每个站点至少维护三个 ADC 存储节点。例如，如果您停用站点上的四个或六个 ADC 节点，则假设同一站点上存在可用的非 ADC 节点，此过程完成后将保留三个 ADC 存储节点。

如果无法自动移动 ADC 服务，您可以"手动移动 ADC 服务"到同一站点上的另一个存储节点，或者"在扩展中添加新的 Storage Node"并指定它应具有 ADC 服务。然后，您可以在不影响仲裁的情况下停用现有存储节点。

查看 StorageGRID ILM 策略和存储配置

如果您计划停用存储节点，则应在开始停用过程之前查看 StorageGRID 系统的 ILM 策略。

在停用期间，所有对象数据都会从停用的存储节点迁移到其他存储节点。

停用期间使用的 ILM 策略将是停用后使用的策略。在开始停用之前和停用完成后，您必须确保此策略满足您的数据要求。

您应查看每个规则中的规则"活动ILM策略"、以确保StorageGRID系统将继续具有正确类型和正确位置的足够容量、以便停用存储节点。

请考虑以下几点：

- ILM 评估服务是否可以复制对象数据以满足 ILM 规则？
- 如果在停用过程中某个站点暂时不可用，会发生什么情况？是否可以在备用位置创建其他副本？
- 停用过程将如何影响内容的最终分发？如中所述"整合存储节点"，您应"添加新存储节点"在停用旧系统之前执行此操作。如果在停用较小的存储节点后添加较大的替代存储节点，则旧存储节点可能接近容量，新存储节点可能几乎没有任何内容。然后，新对象数据的大多数写入操作将定向到新存储节点，从而降低系统操作的整体效率。
- 系统是否会始终包含足够的存储节点来满足活动ILM策略？

如果ILM策略不能满足要求、则会导致积压和警报、并可能导致StorageGRID系统停止运行。

通过评估表中列出的区域、验证停用过程所产生的建议拓扑是否满足ILM策略。

要评估的区域	考虑事项
Available capacity	是否有足够的存储容量来容纳StorageGRID系统中存储的所有对象数据、包括要停用的存储节点上当前存储的对象数据的永久副本? 在停用完成后、是否有足够的容量在合理的时间间隔内处理存储对象数据的预期增长?
存储位置	如果整个 StorageGRID 系统中仍有足够的容量，则容量是否位于合适的位置以满足 StorageGRID 系统的业务规则?
Storage type	停用完成后，是否有足够的相应类型存储? 例如、ILM规则可能会在内容过期时将内容从一种存储类型移动到另一种存储类型。在这种情况下、您必须确保在StorageGRID系统的最终配置中具有足够的适当类型的存储。

整合 **StorageGRID** 存储节点

您可以整合存储节点以减少站点或部署的存储节点数，同时增加存储容量。

整合存储节点时、您可以"展开StorageGRID系统"添加容量更大的新存储节点、然后停用容量较小的旧存储节点。在停用操作步骤 期间，对象会从旧存储节点迁移到新存储节点。

> 如果要将较旧和较小的设备与新型号或较大容量的设备整合、请考虑 "正在克隆设备节点"使用(或者、如果不进行一对一更换、请使用设备节点克隆和停用过程)。

例如，您可以添加两个容量更大的新存储节点来替换三个旧存储节点。您应首先使用扩展操作步骤 添加两个更大的新存储节点，然后使用停用操作步骤 删除三个容量较小的旧存储节点。

通过在删除现有存储节点之前添加新容量，您可以确保在 StorageGRID 系统中更平衡地分布数据。此外，还可以减少现有存储节点可能被推送到存储水印级别以外的可能性。

停用多个 **StorageGRID** 存储节点

如果需要删除多个存储节点，可以按顺序或并行停用它们。

> 在包含基于软件的纯元数据节点的网格中停用存储节点时、请务必小心谨慎。如果停用配置为存储_Both _对象和元数据的所有节点、则会从网格中删除存储对象的功能。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

- 如果您按顺序停用存储节点，则必须等待第一个存储节点完成停用，然后再开始停用下一个存储节点。
- 如果您并行停用存储节点，则存储节点会同时处理要停用的所有存储节点的停用任务。这可能会导致文件的所有永久副本都标记为"只读 - "、从而在启用了此功能的网格中临时禁用删除。

检查 **StorageGRID** 中的数据修复作业

在退役或扩展网格节点之前，您必须确认没有处于活动状态的数据修复作业。如果任何修复失败，则必须重新启动它们并让它们完成，然后再执行退役程序。

- 参考"扩展类型"有关如何扩展网格节点的详细信息。
- 使用 Grid Manager 监控正在进行的恢复过程并显示恢复历史记录。请参阅以下步骤：
  - "将对象数据还原到设备的存储卷"
  - "将对象数据还原到系统驱动器完好无损的存储卷"
  - "将对象数据还原到存储卷(系统驱动器故障)"

收集 **StorageGRID** 节点停用所需的材料

在执行网格节点停用之前，您必须获取以下信息。

项目	备注
恢复包 `.zip`文件	你必须"下载最新的恢复包" `.zip`文件（`sgws-recovery-package-id-revision.zip`）。如果发生故障，您可以使用恢复包文件来恢复系统。
`Passwords.txt`文件	该文件包含在命令行上访问网格节点所需的密码，并包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在此文件中 `Passwords.txt`。
停用前 StorageGRID 系统拓扑的问题描述	如果有，请获取描述系统当前拓扑的任何文档。

相关信息

"Web 浏览器要求"

访问 **StorageGRID** 中的停用节点页面

访问网格管理器中的 " 停用节点 " 页面时，您可以一目了然地看到哪些节点可以停用。

开始之前

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

> 在包含基于软件的纯元数据节点的网格中停用存储节点时、请务必小心谨慎。如果停用配置为存储_Both _对象和元数据的所有节点、则会从网格中删除存储对象的功能。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

步骤

1. 选择*维护* > 任务 > 退役。
2. 选择 * 取消配置节点 * 。

   此时将显示 Decommission Nodes 页面。在此页面中，您可以：

- 确定当前可以停用的网格节点。
- 查看所有网格节点的运行状况
- 按 * 名称 * ， * 站点 * ， * 类型 * 或 * 具有 ADC* 按升序或降序对列表进行排序。
- 输入搜索词可快速查找特定节点。

  在此示例中，"可能停用"列中的绿色复选标记表示可以停用 API Gateway Node 和纯数据 Storage Node。由于各种原因，其他节点无法停用。例如，无法停用主 Admin Node，因为不支持停用此节点类型。仅元数据 Storage Node 无法停用，因为该站点将不再满足 "ADC仲裁"。

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-G1	Data Center 1	API Gateway Node	-		✔
DC1-S1	Data Center 1	Storage Node (Metadata-only)	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S4	Data Center 1	Storage Node (Data-only)	No		✔
DC2-ADM1	Data Center 2	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC2-S1	Data Center 2	Storage Node	Yes		No, site Data Center 2 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.

3. 查看要停用的每个节点的 * 可能停用 * 列。

如果可以停用网格节点、则此列会显示一个绿色复选标记、而左列会显示一个复选框。如果无法停用某个节点、则此列会说明问题描述。如果节点无法停用的原因不止一个、则会显示最严重的原因。

停用可能的原因	说明	解决步骤
不支持、不支持停用_node type_.	您不能停用主管理节点。	无。
否，至少有一个网格节点已断开连接。 注意：此消息仅针对连接的网格节点显示。	如果任何网格节点已断开连接、则无法停用已连接的网格节点。 对于已断开连接的网格节点， * 运行状况 * 列包含以下图标之一： • （灰色）：管理性关闭 • （蓝色）：未知	您必须先使所有断开连接的节点恢复联机、或者"停用所有已断开连接的节点"才能删除已连接的节点。 注意：如果您的网格包含多个断开连接的节点，则该软件要求您同时停用这些节点，这会增加出现意外结果的可能性。

停用可能的原因	说明	解决步骤
否，一个或多个所需节点当前已断开连接，必须进行恢复。 注意：此消息仅针对断开连接的网格节点显示。	如果一个或多个所需节点也已断开连接、则无法停用已断开连接的网格节点(例如、ADC仲裁所需的存储节点)。	a. 查看所有已断开连接的节点的 " 取消配置 " 可能消息。 b. 确定哪些节点因需要而无法停用。 ◦ 如果所需节点的运行状况已被管理员关闭，请使此节点重新联机。 ◦ 如果所需节点的运行状况未知，请执行节点恢复操作步骤 以恢复所需节点。
否，HA 组的成员：组名称。在停用此节点之前，您必须将其从所有 HA 组中删除。	如果某个节点接口属于高可用性(HA)组、则无法停用管理节点或网关节点。	编辑 HA 组以删除节点的接口或删除整个 HA 组。请参阅。 "配置高可用性组"
否，站点 *x* 需要至少 3 个具有 ADC 服务的存储节点或可用的非 ADC 节点，才能将 ADC 服务移至其中。如果任何节点处于脱机状态，则 ADC 节点停用不可用。	仅存储节点（组合或仅元数据存储节点）。如果站点中没有足够的节点来支持 ADC 仲裁要求，并且无法自动移动 ADC 服务，则无法停用存储节点。自动移动需要跨网格的两个以上 ADC 存储节点联机，以及同一站点上可用的非 ADC 存储节点。	确保满足自动 ADC 服务移动的条件（请参阅"ADC仲裁"），或将其"手动移动 ADC 服务"移动到同一站点的其他存储节点。您也可以通过向站点添加新的存储节点并指定其应具有 ADC 服务来执行扩展。请参阅"向 StorageGRID 添加网格节点的工作流摘要"。
不需要、一个或多个纠删编码配置文件至少需要_n_个存储节点。如果在 ILM 规则中未使用此配置文件，您可以将其停用。	仅限存储节点。除非为现有的擦除编码配置文件保留足够的节点，否则您不能停用存储节点。 例如、如果4+2纠删编码存在纠删编码配置文件、则必须至少保留6个存储节点。	对于每个受影响的纠删编码配置文件、根据该配置文件的使用方式执行以下步骤之一： • 用于活动**ILM**策略：执行扩展。添加足够多的新存储节点，以便继续进行纠删编码。请参阅的说明"扩展网格"。 • 用于**ILM**规则，但不用于活动**ILM**策略：编辑或删除规则，然后停用纠删编码配置文件。 • 不用于任何**ILM**规则：停用纠删编码配置文件。 *注意：*如果您尝试停用纠删编码配置文件，而对象数据仍与该配置文件关联，则会显示一条错误消息。您可能需要等待几周才能再次尝试停用过程。 了解 "停用纠删编码配置文件"。

停用可能的原因	说明	解决步骤
不能、除非已断开归档节点连接、否则无法停用该节点。	如果归档节点仍处于连接状态、则无法将其删除。	注意：已删除对归档节点的支持。如果需要停用归档节点、请参见 "网格节点停用(StorageGRID 11.8 文档站点)"

停用已断开连接的 **StorageGRID** 节点

您可能需要停用当前未连接到网格的节点（运行状况为未知或管理员关闭的节点）。

开始之前

- 您了解停用的注意事项和停用的注意事项""管理节点和网关节点""存储节点"。
- 您已获取所有前提条件项。
- 您已确保没有处于活动状态的数据修复作业。请参阅。 "检查数据修复作业"
- 您已确认网格中的任何位置均未进行存储节点恢复。如果是，则必须等待在恢复过程中执行的任何 Cassandra 重建完成。然后，您可以继续停用。
- 您已确保在节点停用操作步骤 运行期间不会运行其他维护过程，除非节点停用操作步骤 已暂停。
- 要停用的已断开连接节点的 * 可停用 * 列包含一个绿色复选标记。
- 您具有配置密码短语。

关于此任务

您可以通过在*健康*列中查找蓝色未知图标或灰色管理关闭图标来识别断开连接的节点。

停用任何已断开连接的节点之前，请注意以下事项：

- 此操作步骤 主要用于删除一个断开连接的节点。如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。

  如果一次停用多个断开连接的存储节点、可能会发生数据丢失。请参阅。 "断开连接的存储节点的注意事项"

  在包含基于软件的纯元数据节点的网格中停用存储节点时、请务必小心谨慎。如果停用配置为存储_Both _对象和元数据的所有节点、则会从网格中删除存储对象的功能。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

- 如果无法删除已断开连接的节点(例如、ADC仲裁所需的存储节点)、则无法删除任何其他已断开连接的节点。

步骤

1. 除非要停用归档节点(必须断开连接)、否则请尝试使所有断开连接的网格节点恢复联机或恢复它们。

   有关说明、请参见。 "网格节点恢复过程"

2. 如果无法恢复已断开连接的网格节点、而您希望在其断开连接时将其停用、请选中该节点对应的复选框。

如果您的网格包含多个断开连接的节点，则软件要求您同时停用所有节点，从而增加意外结果的可能性。

如果选择一次停用多个断开连接的网格节点、请务必小心、尤其是在选择多个断开连接的存储节点时。如果您有多个无法恢复的已断开连接的存储节点、请联系技术支持以确定最佳操作方案。

3. 输入配置密码短语。

   已启用 * 开始取消配置 * 按钮。

4. 选择*Start decommission*。

   此时将显示一条警告，指示您已选择断开连接的节点，如果此节点具有唯一的对象副本，则此对象数据将丢失。

5. 查看节点列表，然后选择*OK*。

   退役程序开始，并显示每个节点的进度。在此过程中，将生成一个包含电网配置更改的新恢复包。

6. 一旦新的恢复包可用，请选择链接或选择*维护* > 系统 > *恢复包*以访问恢复包页面。然后，下载 `.zip`文件。

   请参阅说明"下载恢复包"。

   尽快下载恢复包，以确保在退役过程中出现问题时可以恢复电网。

   恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

7. 定期监控 " 停用 " 页面，以确保所有选定节点均已成功停用。

   存储节点停用可能需要数天或数周时间。完成所有任务后，系统将重新显示节点选择列表，并显示成功消息。如果停用了已断开连接的存储节点，则会显示一条信息消息，指出修复作业已启动。

8. 在停用操作步骤 期间自动关闭节点后，请删除与已停用节点关联的任何剩余虚拟机或其他资源。

   在节点自动关闭之前、请勿执行此步骤。

9. 如果要停用存储节点，请监控在停用过程中自动启动的*已复制数据*和*纠删编码 (EC) 数据*修复作业的状态。

复制的数据

- 要确定修复是否已完成，请执行以下操作：
  i. 选择 节点 > 正在修复的存储节点 > **ILM**。
  ii. 查看 " 评估 " 部分中的属性。修复完成后， * 正在等待 - 全部 * 属性指示 0 个对象。
- 要更详细地监控修复，请执行以下操作：
  i. 选择*节点*。
  ii. 选择 * 网格名称 _* > * ILM * 。
  iii. 将光标放在 ILM 队列图上，查看 扫描速率（对象/秒） 属性的值，该值是网格中对象被扫描并排队等待 ILM 的速率。
  iv. 在 ILM 队列部分中，查看以下属性：
    - 扫描期限-估计：完成对所有对象的完整ILM扫描的估计时间。

      全面扫描并不能保证 ILM 已应用于所有对象。

    - 尝试修复：针对被视为高风险的复制数据尝试的对象修复操作的总数。高风险对象是任何仅剩一个副本的对象，无论是由 ILM 策略指定的还是由于副本丢失造成的。每次存储节点尝试修复高风险对象时，此计数都会增加。如果电网变得繁忙，则优先进行高风险的 ILM 修复。

      如果修复后复制失败，则同一对象修复可能会再次增加。 + 当您监控存储节点卷恢复的进度时，这些属性非常有用。如果尝试修复的次数停止增加并且完整扫描已完成，则修复可能已完成。

  v. 或者，提交 Prometheus 查询 `storagegrid_ilm_scan_period_estimated_minutes` 和 `storagegrid_ilm_repairs_attempted`。

纠删编码**(EC)**数据

要监控擦除编码数据的修复并重试可能失败的任何请求，请选择 **Support** > **Tools** > **Metrics** 以查看当前作业的估计完成时间和完成百分比。然后，在 Grafana 部分选择 **EC Overview**。查看 **Grid EC Job Estimated Time to Completion** 和 **Grid EC Job Percentage Completed** 仪表板。

完成后

一旦断开连接的节点停用并完成所有数据修复作业，您就可以根据需要停用任何已连接的网格节点。

然后，在完成停用操作步骤 后完成以下步骤：

- 确保已停用网格节点的驱动器已擦除干净。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果您停用了某个设备节点，并且该设备上的数据已使用节点加密进行保护，请使用 StorageGRID 设备安装程序清除密钥管理服务器配置（清除 KMS ）。如果要将设备添加到另一个网格，则必须清除 KMS 配置。有关说明，请参阅 "监控维护模式下的节点加密"。

停用连接的 **StorageGRID** 节点

您可以停用并永久删除连接到网格的节点。

开始之前

- 您了解停用的注意事项和停用的注意事项"管理节点和网关节点""存储节点"。
- 您已收集所有必需的材料。
- 您已确保没有处于活动状态的数据修复作业。
- 您已确认网格中的任何位置均未进行存储节点恢复。如果是、请等待、直到在恢复过程中执行的任何Cassandrebuild完成为止。然后，您可以继续停用。
- 您已确保在节点停用操作步骤 运行期间不会运行其他维护过程，除非节点停用操作步骤 已暂停。
- 您具有配置密码短语。
- 已连接网格节点。
- 要取消配置的一个或多个节点的*取消配置可能*列包含一个绿色复选标记。

  如果一个或多个卷脱机(已卸载)、或者它们联机(已挂载)但处于错误状态、则不会开始取消配置。

  如果在停用过程中一个或多个卷脱机、则停用过程将在这些卷恢复联机后完成。

- 所有网格节点均处于正常（绿色）运行状况。如果您在 **Health** 列中看到以下图标之一，则必须尝试解决此问题：

图标	颜色	严重性
	黄色	通知
	浅橙色	次要
	深橙色	主要
	红色	关键

- 如果您先前停用了已断开连接的存储节点，则数据修复作业均已成功完成。请参阅。 "检查数据修复作业"

在此操作步骤 中指示删除网格节点的虚拟机或其他资源之前、请勿删除此网格节点。

在包含基于软件的纯元数据节点的网格中停用存储节点时、请务必小心谨慎。如果停用配置为存储_Both _对象和元数据的所有节点、则会从网格中删除存储对象的功能。有关纯元数据存储节点的详细信息、请参见"存储节点的类型"。

关于此任务

停用某个节点后、该节点的服务将被禁用、并且该节点会自动关闭。

步骤

1. 在停用节点页面中、选中要停用的每个网格节点对应的复选框。
2. 输入配置密码短语。

   已启用 * 开始取消配置 * 按钮。

3. 选择*开始取消配置*。
4. 在确认对话框中查看节点列表，然后选择*OK*。

   此时将启动节点停用操作步骤 ，并显示每个节点的进度。

   > 请勿在停用操作步骤 启动后使存储节点脱机。更改状态可能会导致某些内容未复制到其他位置。

5. 一旦新的恢复包可用，请选择横幅中的恢复包链接或选择*维护*>*系统*>*恢复包*以访问恢复包页面。然后，下载 `.zip`文件。

   看"下载恢复包" 。

   > 尽快下载恢复包，以确保在退役过程中出现问题时可以恢复电网。

6. 定期监控 " 停用节点 " 页面，以确保所有选定节点均已成功停用。

   > 存储节点停用可能需要数天或数周时间。

   完成所有任务后，系统将重新显示节点选择列表，并显示成功消息。

完成后

完成节点停用操作步骤 后，请完成以下步骤：

1. 按照适用于您的平台的步骤进行操作。例如：
   - **Linux**：您可能想要分离卷并删除在安装期间创建的节点配置文件。看"在基于软件的节点上安装StorageGRID" 。
   - **VMware**：您可能希望使用vCenter的"从磁盘删除"选项来删除虚拟机。您可能还需要删除独立于虚拟机的任何数据磁盘。
   - * StorageGRID 设备 * ：设备节点会自动恢复为未部署状态，您可以在此状态下访问 StorageGRID 设备安装程序。您可以关闭设备电源或将其添加到另一个 StorageGRID 系统。
2. 确保已停用网格节点的驱动器已擦除干净。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
3. 如果您停用了某个设备节点，并且该设备上的数据已使用节点加密进行保护，请使用 StorageGRID 设备安装程序清除密钥管理服务器配置（清除 KMS ）。如果要将设备添加到另一个网格，则必须清除 KMS 配置。有关说明，请参阅 "监控维护模式下的节点加密"。

暂停和恢复 **StorageGRID** 存储节点的停用过程

如果需要执行第二个维护操作步骤 ，可以在某些阶段暂停存储节点的停用操作步骤 。另一个操作步骤 完成后，您可以恢复停用。

只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。

开始之前

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

步骤

1. 选择*维护* > 任务 > 退役。

   此时将显示 Decommission 页面。

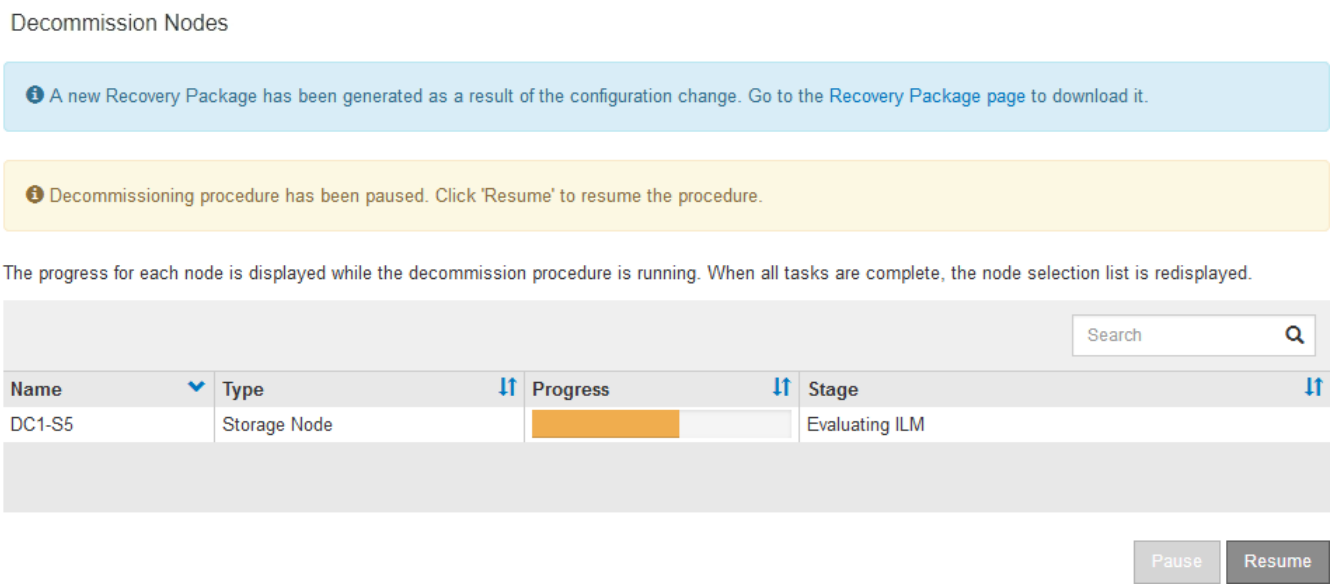
2. 选择 * 取消配置节点 * 。

   此时将显示 Decommission Nodes 页面。当停用操作步骤 达到以下任一阶段时， * 暂停 * 按钮将处于启用状态。

   - 评估 ILM
   - 停用经过Erasure编码的数据

3. 选择 * 暂停 * 以暂停操作步骤 。

   当前阶段已暂停，并且 * 恢复 * 按钮已启用。



4. 另一个维护操作步骤 完成后，选择 * 恢复 * 继续执行停用。

停用站点

StorageGRID 中的站点停用注意事项

在使用站点停用操作步骤 删除站点之前，您必须查看注意事项。

停用站点时会发生什么情况

停用站点时， StorageGRID 会从 StorageGRID 系统中永久删除站点上的所有节点以及站点本身。

站点停用操作步骤 完成后：

- 您不能再使用 StorageGRID 查看或访问站点或站点上的任何节点。
- 您无法再使用引用该站点的任何存储池或纠删编码配置文件。StorageGRID停用站点时、会自动删除这些存储池并停用这些纠删编码配置文件。

已连接站点与已断开站点停用过程之间的差异

您可以使用站点停用操作步骤 删除所有节点均已连接到 StorageGRID 的站点（称为已连接站点停用），或者删除所有节点均已与 StorageGRID 断开连接的站点（称为已断开连接的站点停用）。开始之前，您必须了解这些过程之间的差异。

如果站点包含已连接()和已断开连接的节点( 或 )的混合，则必须使所有脱机节点重新联机。

- 通过已连接站点停用，您可以从 StorageGRID 系统中删除操作站点。例如，您可以执行已连接站点停用以删除正常运行但不再需要的站点。
- 当 StorageGRID 删除已连接站点时，它会使用 ILM 管理该站点上的对象数据。在开始停用已连接站点之前，必须先从所有 ILM 规则中删除此站点并激活新的 ILM 策略。迁移对象数据的 ILM 过程和删除站点的内部过程可以同时进行，但最佳实践是，在开始实际停用操作步骤 之前，允许完成 ILM 步骤。
- 断开连接的站点停用允许您从 StorageGRID 系统中删除故障站点。例如，您可以执行已断开连接的站点停用，以删除已被火灾或洪水破坏的站点。

  当 StorageGRID 删除已断开连接的站点时，它会将所有节点视为不可恢复的，并且不会尝试保留数据。但是，在开始执行已断开连接的站点停用之前，必须先从所有 ILM 规则中删除此站点并激活新的 ILM 策略。

在执行已断开连接的站点停用操作步骤 之前，您必须联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。如果您认为可以恢复站点或从站点恢复对象数据，则不应尝试执行已断开连接的站点停用。

删除已连接或已断开连接的站点的一般要求

在删除已连接或已断开连接的站点之前，您必须了解以下要求：

- 您不能停用包含主管理节点的站点。
- 如果任何节点的接口属于高可用性(HA)组、则无法停用站点。您必须编辑 HA 组以删除节点的接口或删除整个 HA 组。
- 如果站点包含已连接（  ）和已断开连接（  或  ）节点的混合，则无法停用该站点。
- 如果任何其他站点上的任何节点已断开连接（  或  ），则无法停用站点。
- 如果正在执行EC节点修复操作、则无法启动站点停用操作步骤。请参见"检查数据修复作业"以跟踪经过过整编码的数据的修复。
- 站点停用操作步骤 运行时：

- 您不能创建引用要停用的站点的ILM规则。您也无法编辑现有ILM规则以引用此站点。
- 您无法执行其他维护过程、例如扩展或升级。

> 如果您需要在已连接站点停用期间执行另一个维护过程，您可以"在删除存储节点时暂停操作步骤"。只有在达到 ILM 评估或纠删编码的数据停用阶段时， * 暂停 * 按钮才会启用；但是， ILM 评估（数据迁移）将继续在后台运行。第二个维护操作步骤 完成后，您可以恢复停用。

- 如果您需要在启动站点停用操作步骤 后恢复任何节点，必须联系支持部门。

- 一次不能停用多个站点。
- 如果站点包含一个或多个管理节点，并且为 StorageGRID 系统启用了单点登录（ Single Sign-On ， SSO ），则必须从 Active Directory 联合身份验证服务（ Active Directory Federation Services ， AD FS ）中删除此站点的所有依赖方信任。

信息生命周期管理（ **ILM** ）的要求

在删除站点时，您必须更新 ILM 配置。" 取消配置站点 " 向导将指导您完成许多前提条件步骤，以确保满足以下要求：

- 此站点不受任何ILM策略的引用。如果是、则必须编辑策略、或者创建策略并使用新的ILM规则激活策略。
- 任何ILM规则都不会引用此站点、即使这些规则未在任何策略中使用也是如此。您必须删除或编辑引用此站点的所有规则。

在StorageGRID停用站点时、它会自动停用引用该站点的任何未使用的纠删编码配置文件、并自动删除引用该站点的任何未使用的存储池。如果存在所有存储节点存储池(StorageGRID 11.6及更早版本)、则会将其删除、因为它会使用所有站点。

> 在删除站点之前，您可能需要创建新的 ILM 规则并激活新的 ILM 策略。以下说明假定您已充分了解ILM的工作原理、并熟悉创建存储池、纠删编码配置文件、ILM规则以及模拟和激活ILM策略。请参阅。 "使用 ILM 管理对象"

已连接站点上的对象数据注意事项

如果要执行已连接站点停用，则必须在创建新的 ILM 规则和新的 ILM 策略时确定如何处理站点上的现有对象数据。您可以执行以下任一操作，也可以同时执行这两项操作：

- 将对象数据从选定站点移动到网格中的一个或多个其他站点。
- 移动数据的示例 * ： 假设您要停用罗利的某个站点，因为您在森尼韦尔添加了一个新站点。在此示例中，您希望将所有对象数据从旧站点移动到新站点。在更新ILM规则和ILM策略之前、您必须查看这两个站点的容量。您必须确保森尼韦尔站点具有足够的容量来容纳来自罗利站点的对象数据，并且森尼韦尔将保留足够的容量以满足未来增长的需要。

> 要确保有足够的可用容量、您可能需要"扩展网格"在执行此过程之前向现有站点添加存储卷或存储节点、或者添加新站点。

- 从选定站点删除对象副本。
- 删除数据的示例 * ： 假设您当前使用 3 个副本 ILM 规则在三个站点之间复制对象数据。在停用站点之前，您可以创建等效的双副本 ILM 规则，以便仅将数据存储在两个站点上。激活使用双副本规则的新 ILM 策略时

， StorageGRID 会从第三个站点删除这些副本，因为它们不再满足 ILM 要求。但是，对象数据仍会受到保护，其余两个站点的容量将保持不变。

> 切勿创建单个副本 ILM 规则来容纳站点的删除。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

已连接站点停用的其他要求

在 StorageGRID 删除已连接站点之前，您必须确保满足以下条件：

- StorageGRID 系统中的所有节点的连接状态必须为 **Connected**（）；但是，节点可以有活动警报。

> 如果一个或多个节点断开连接，您可以完成 " 取消配置站点 " 向导的步骤 1-4 。但是、除非所有节点均已连接、否则无法完成向导中启动停用过程的步骤5。

- 如果您计划删除的站点包含用于负载平衡的网关节点或管理节点、则可能需要"扩展网格"在另一站点添加等效的新节点。在启动站点停用操作步骤 之前，请确保客户端可以连接到替代节点。
- 如果要删除的站点包含高可用性（ HA ）组中的任何网关节点或管理节点，则可以完成 " 取消配置站点 " 向导的步骤 1-4 。但是、在从所有HA组中删除这些节点之前、您无法完成向导中启动停用过程的步骤5。如果现有客户端连接到包含站点中节点的 HA 组，则必须确保它们可以在删除站点后继续连接到 StorageGRID 。
- 如果客户端直接连接到您要删除的站点上的存储节点，则必须确保它们可以连接到其他站点上的存储节点，然后再启动站点停用操作步骤 。
- 您必须在其余站点上提供足够的空间、以容纳因任何活动ILM策略发生更改而要移动的任何对象数据。在某些情况下、您可能需要"扩展网格"先添加存储节点、存储卷或新站点、然后才能完成已连接站点的停用。
- 您必须留出足够的时间来完成停用操作步骤 。StorageGRID ILM 过程可能需要数天，数周甚至数月才能从站点中移动或删除对象数据，然后才能停用此站点。

> 从站点移动或删除对象数据可能需要数天，数周甚至数月的时间，具体取决于站点上的数据量，系统上的负载，网络延迟以及所需 ILM 更改的性质。

- 您应尽可能早地完成 " 弃用站点 " 向导的步骤 1-4 。如果您允许在启动实际停用操作步骤 之前从站点移动数据，则停用操作步骤 将更快地完成，并且中断和性能影响更少（方法是在向导的步骤 5 中选择 * 启动停用 * ）。

断开连接的站点停用的其他要求

在 StorageGRID 删除已断开连接的站点之前，您必须确保满足以下条件：

- 您已联系您的 NetApp 客户代表。在取消配置站点向导中启用所有步骤之前， NetApp 将查看您的要求。

> 如果您认为可以恢复站点或从站点恢复任何对象数据，则不应尝试执行已断开连接的站点停用。请参阅。 "技术支持如何恢复站点"

- 站点上的所有节点的连接状态必须为以下之一：

- 未知 ( )：由于未知原因，节点断开连接或节点上的服务意外关闭。例如，节点上的服务可能已停止，或者节点可能因电源故障或意外中断而失去网络连接。
- **Administratively Down** ( )：由于预期的原因，节点未连接到网格。例如，节点上的节点或服务已正常关闭。

- 所有其他站点的所有节点都必须具有*已连接* ( ) 的连接状态；但是，这些其他节点可以具有活动警报。
- 您必须了解，您将无法再使用 StorageGRID 查看或检索站点上存储的任何对象数据。当 StorageGRID 执行此操作步骤 时，它不会尝试保留已断开连接的站点中的任何数据。

  如果您的 ILM 规则和策略旨在防止单个站点丢失，则其余站点上仍存在对象的副本。

- 您必须了解、如果站点包含对象的唯一副本、则对象将丢失、并且无法检索。

删除站点时的一致性注意事项

S3存储分段的一致性决定了StorageGRID是否在通知客户端对象已成功执行对象加热之前将对象元数据完全复制到所有节点和站点。一致性可在不同存储节点和站点之间的对象可用性与这些对象的一致性之间实现平衡。

StorageGRID 删除站点时，需要确保不会向要删除的站点写入任何数据。因此、它会临时覆盖每个存储分段或容器的一致性。启动站点停用过程后， StorageGRID 会暂时使用强站点一致性来防止将对象元数据写入要删除的站点。

由于这种临时覆盖，请注意，如果其他站点上的多个节点不可用，则站点停用期间发生的任何客户端写入，更新和删除操作都可能失败。

收集 **StorageGRID** 站点停用所需的材料

停用站点之前，您必须获取以下材料。

项目	备注
恢复包 `.zip`文件	您必须下载最新的恢复包 `.zip`文件（`sgws-recovery-package-id-revision.zip`）。如果发生故障，您可以使用恢复包文件来恢复系统。 "下载恢复包"
`Passwords.txt`文件	该文件包含在命令行上访问网格节点所需的密码，并包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在此文件中 `Passwords.txt`。
停用前 StorageGRID 系统拓扑的问题描述	如果有，请获取描述系统当前拓扑的任何文档。

相关信息

"Web 浏览器要求"

在 **StorageGRID** 中选择要停用的站点

要确定是否可以停用某个站点，请首先访问 " 停用站点 " 向导。

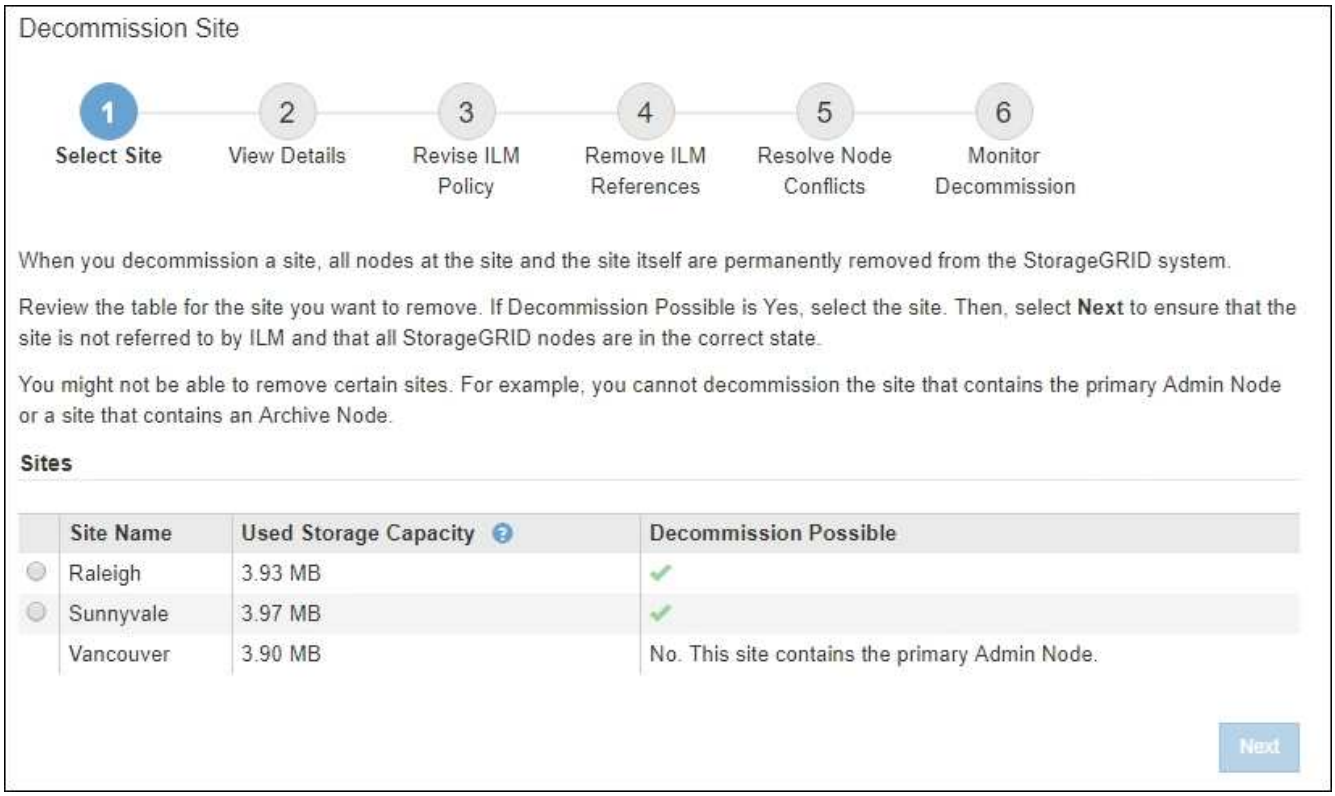
开始之前

- 您已获得所有必需的材料。
- 您已查看删除站点的注意事项。
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"root访问权限或维护和ILM权限"。

步骤

1. 选择*维护* > 任务 > 退役。
2. 选择 * 取消配置站点 * 。

   此时将显示取消配置站点向导的第 1 步（选择站点）。此步骤包含 StorageGRID 系统中站点的字母列表。



3. 查看 * 已用存储容量 * 列中的值，确定每个站点上的对象数据当前使用的存储容量。

   已用存储容量是一个估计值。如果节点处于脱机状态，则已用存储容量是站点的最后一个已知值。

   - 对于已连接站点停用，此值表示在安全停用此站点之前需要将多少对象数据移动到其他站点或由 ILM 删除。
   - 对于已断开连接的站点停用，此值表示停用此站点后系统的数据存储容量将变得不可访问。

   如果您的 ILM 策略旨在防止单个站点丢失，则其余站点上仍应存在对象数据的副本。

4. 查看 * 可能停用 * 列中的原因，确定哪些站点当前可以停用。

   如果站点无法停用的原因不止一个、则会显示最严重的原因。

停用可能的原因	说明	下一步
绿色复选标记（）	您可以停用此站点。	转到。 下一步
否。此站点包含主管理节点。	您不能停用包含主管理节点的站点。	无。您无法执行此操作步骤。
否。此站点包含一个或多个归档节点。	您不能停用包含归档节点的站点。	无。您无法执行此操作步骤。
不会。此站点上的所有节点均已断开连接。请联系您的 NetApp 客户代表。	除非站点中的每个节点都已连接（），否则无法执行连接的站点停用。	如果您要执行已断开连接的站点停用，必须联系您的 NetApp 客户代表，客户代表将查看您的要求并启用停用站点向导的其余部分。 • 重要信息 * ：切勿使联机节点脱机，以便可以删除站点。您将丢失数据。

   示例显示了具有三个站点的 StorageGRID 系统。Raleigh 和 Sunnyvale 站点的绿色复选标记（）表示您可以停用这些站点。但是，您无法停用 Vancouver 站点，因为它包含主管理节点。

1. 如果可以停用，请选择站点的单选按钮。

   此时将启用 * 下一步 * 按钮。

2. 选择 * 下一步 * 。

   此时将显示第 2 步（查看详细信息）。

在 **StorageGRID** 中停用前查看站点详细信息

从 " 弃用站点 " 向导的第 2 步（查看详细信息）中，您可以查看站点中包含的节点，查看每个存储节点上已使用的空间量，并评估网格中其他站点上的可用空间量。

开始之前

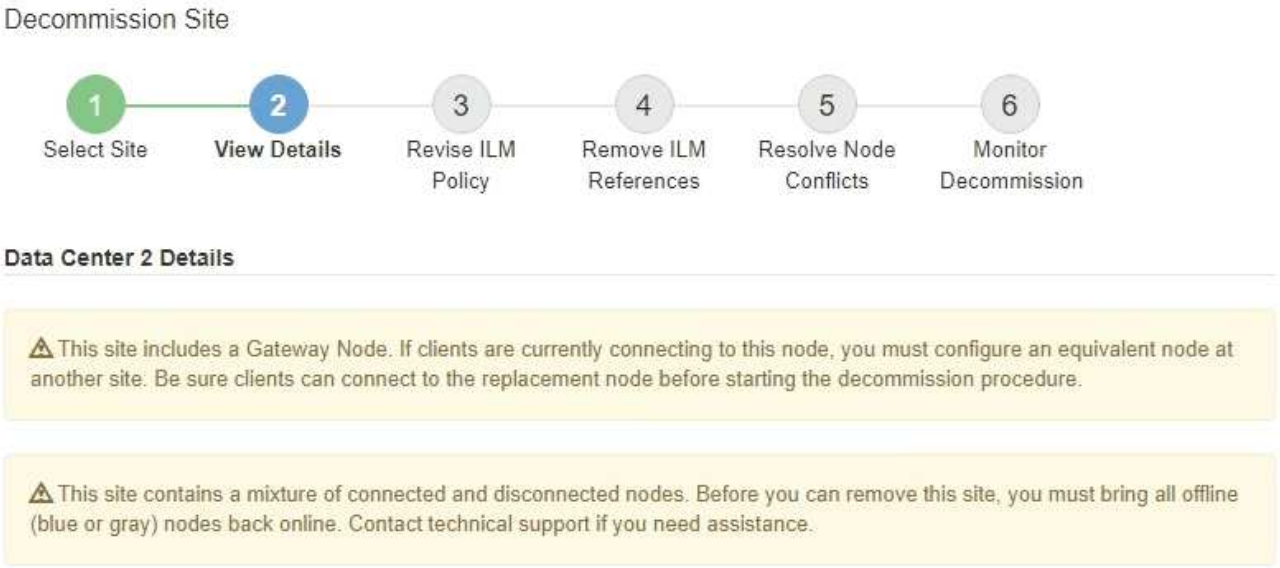
停用站点之前，您必须查看站点上存在的对象数据量。

- 如果您要执行已连接站点停用，则必须先了解站点上当前存在的对象数据量，然后再更新 ILM 。根据站点容量和数据保护需求，您可以创建新的 ILM 规则，将数据移动到其他站点或从站点中删除对象数据。
- 如果可能，请在启动停用操作步骤 之前执行任何所需的存储节点扩展。
- 如果您要执行断开连接的站点停用，则必须了解删除此站点后将永久无法访问多少对象数据。

如果您正在执行断开连接的站点停用、ILM将无法移动或删除对象数据。站点上保留的所有数据都将丢失。但是，如果您的 ILM 策略旨在防止单个站点丢失，则其余站点上仍存在对象数据的副本。请参阅。 "启用站点丢失保护"

步骤

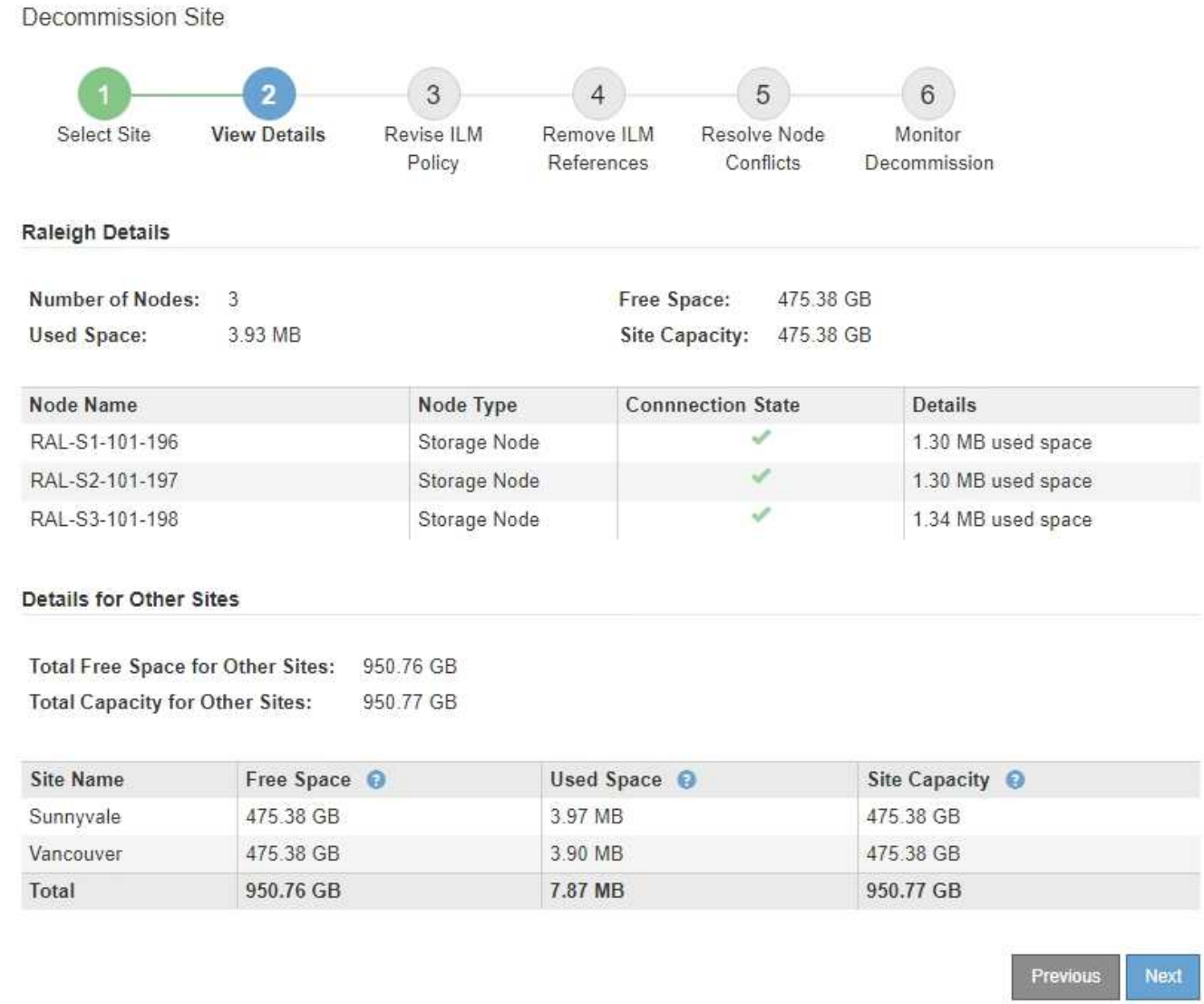
1. 从第 2 步（查看详细信息）中，查看与您选择删除的站点相关的任何警告。



在以下情况下会显示警告：

- 此站点包含一个网关节点。如果S3客户端当前正在连接到此节点、则必须在另一站点配置等效节点。在继续执行停用操作步骤 之前，请确保客户端可以连接到替代节点。
- 该站点包含已连接（）和已断开连接的节点（或）的混合。在删除此站点之前，必须使所有脱机节点恢复联机。

2. 查看有关选定要删除的站点的详细信息。



选定站点包含以下信息：

- 节点数
- 站点中所有存储节点的已用总空间，可用空间和容量。
  - 对于已连接站点停用， * 已用空间 * 值表示必须将多少对象数据移动到其他站点或使用 ILM 删除。
  - 对于已断开连接的站点停用， * 已用空间 * 值表示删除此站点后将无法访问多少对象数据。
- 节点名称，类型和连接状态：
  - （已连接）
  - (管理性关闭)
  - (未知)
- 有关每个节点的详细信息：
  - 对于每个存储节点，为对象数据使用的空间量。
  - 对于管理节点和网关节点，表示此节点当前是否在高可用性（ HA ）组中使用。您不能停用HA组中

使用的管理节点或网关节点。开始停用之前、请编辑HA组以删除站点上的所有节点、或者删除仅包含此站点中节点的HA组。有关说明，请参阅"管理高可用性(HA)组"。

3. 在页面的其他站点的详细信息部分中，评估网格中其他站点的可用空间量。

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	**950.76 GB**	**7.87 MB**	**950.77 GB**

如果您正在执行已连接站点停用，并且计划使用 ILM 从选定站点移动对象数据（而不是仅删除该数据），则必须确保其他站点具有足够的容量来容纳移动的数据，并且为未来的增长保留足够的容量。

如果要删除的站点的 * 已用空间 * 大于 * 其他站点的总可用空间 * ，则会显示警告。要确保删除站点后有足够的存储容量可用，您可能需要在执行此操作步骤 之前执行扩展。

4. 选择 * 下一步 * 。

此时将显示第 3 步（修订 ILM 策略）。

在 **StorageGRID** 中修订站点停用的 **ILM** 策略

从停用站点向导的第3步(修订ILM策略)中、您可以确定站点是否由任何ILM策略引用。

开始之前

您已很好地了解如何"使用ILM管理对象"。您熟悉创建存储池和ILM规则以及模拟和激活ILM策略。

关于此任务

如果任何策略(活动或非活动)中的任何ILM规则引用某个站点、则StorageGRID无法停用该站点。

如果任何ILM策略引用要停用的站点、则必须删除或编辑这些策略、以使其满足以下要求：

- 全面保护所有对象数据。
- 请勿参考要停用的站点。
- 请勿使用引用该站点的存储池或使用"所有站点"选项。
- 请勿使用引用站点的纠删编码配置文件。
- 请勿使用StorageGRID 11.5或更早版本安装中的创建2个副本规则。

切勿创建单个副本 ILM 规则来容纳站点的删除。如果 ILM 规则在任何时间段内仅创建一个复制副本，则会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

如果您正在执行_connec地点 停用_、则必须考虑StorageGRID应如何管理要删除的地点当前的对象数据。根据您的数据保护要求、新规则可以将现有对象数据移动到不同站点、也可以删除不再需要的任何额外对象副本。

如果您在设计新策略时需要帮助、请联系技术支持。

步骤

1. 从第3步(修订ILM策略)开始、确定是否有任何ILM策略引用您选择停用的站点。
2. 如果未列出任何策略，请选择*下一步*转到"第 4 步：删除 ILM 引用"。
3. 如果列出了一个或多个_active_ ILM策略、请克隆每个现有策略或创建不引用要停用的站点的新策略：

   a. 在策略名称列中选择策略的链接。

      此策略的ILM策略详细信息页面将显示在新的浏览器选项卡中。" 取消配置站点 " 页面将在 " 其他 " 选项卡上保持打开状态。

   b. 根据需要遵循以下准则和说明：

      - 使用ILM规则：
        - "创建一个或多个存储池"不是指站点。
        - "编辑或替换规则"引用站点的。

          请勿选择*创建2个副本*规则、因为该规则使用*所有存储节点*存储池、这是不允许的。

      - 使用ILM策略：
        - "克隆现有ILM策略" 或 "创建新的ILM策略"。
        - 确保默认规则和其他规则不引用站点。

          您必须确认 ILM 规则的顺序正确。激活策略后，新对象和现有对象将按列出的顺序从顶部开始进行评估。

   c. 请加热测试对象并模拟策略、以确保应用正确的规则。

      ILM 策略中的错误可能会导致发生原因 丢失不可恢复的数据。在激活策略之前，请仔细查看并模拟策略，以确认策略将按预期运行。

      激活新的 ILM 策略时， StorageGRID 会使用它来管理所有对象，包括现有对象和新载入的对象。在激活新的 ILM 策略之前，请查看对现有复制对象和纠删编码对象的放置方式所做的任何更改。在评估和实施新放置时，更改现有对象的位置可能会导致临时资源问题。

   d. 激活新策略并确保旧策略现在处于非活动状态。

      如果要激活多个策略，请"按照以下步骤创建ILM策略标记"。

如果您要执行已连接站点停用，则一旦激活新的 ILM 策略， StorageGRID 就会开始从选定站点删除对象数

据。移动或删除所有对象副本可能需要数周时间。尽管在站点上仍存在对象数据的情况下，您可以安全地开始站点停用，但如果您允许在实际停用操作步骤 之前从站点移动数据，则停用操作步骤 将更快地完成，并减少中断和性能影响 （通过在向导的步骤 5 中选择 * 启动取消配置 * ）。

4. 对于每个_INEVIOUS_策略、请先按照前面的步骤所述选择每个策略的链接来编辑或删除该策略。
   - "编辑策略"因此、它并不是指要停用的站点。
   - "删除策略"(英文)
5. 完成对ILM规则和策略的更改后、第3步(修订ILM策略)中不应再列出任何策略。选择 * 下一步 * 。

   此时将显示第 4 步（删除 ILM 参考）。

删除 **StorageGRID** 中对站点的 **ILM** 引用

从停用站点向导的第4步(删除ILM引用)开始、您必须删除或编辑引用该站点的任何未使用的ILM规则、即使这些规则未在任何ILM策略中使用也是如此。

步骤

1. 确定任何未使用的 ILM 规则是否引用站点。

   如果列出了任何ILM规则、则这些规则仍会引用此站点、但不会在任何策略中使用。

   > 在StorageGRID停用站点时、它会自动停用引用该站点的任何未使用的纠删编码配置文件、并自动删除引用该站点的任何未使用的存储池。删除所有存储节点存储池(StorageGRID 11.6及更早版本)、因为它使用所有站点站点。

2. 编辑或删除每个未使用的规则：
   - 要编辑规则、请转到ILM规则页面并更新使用引用站点的纠删编码配置文件或存储池的所有放置位置。然后，返回到 * 步骤 4 （删除 ILM 参考） * 。
   - 要删除规则，请选择垃圾桶图标 并选择 **OK**。

     > 您必须先删除*创建2个副本*规则，然后才能停用站点。

3. 确认没有未使用的ILM规则引用该站点，并且已启用*Next*按钮。
4. 选择 * 下一步 * 。

   > 删除此站点后、引用此站点的任何其余存储池和纠删编码配置文件将无效。在StorageGRID停用站点时、它会自动停用引用该站点的任何未使用的纠删编码配置文件、并自动删除引用该站点的任何未使用的存储池。删除所有存储节点存储池(StorageGRID 11.6及更早版本)、因为它使用所有站点站点。

   此时将显示第 5 步（解决节点冲突）。

解决节点冲突并在 **StorageGRID** 中启动站点停用

从 " 弃用站点 " 向导的第 5 步（解决节点冲突）中，您可以确定 StorageGRID 系统中的任何节点是否已断开连接，或者选定站点中的任何节点是否属于高可用性（ HA ）组。解决

任何节点冲突后，您可以从此页面启动停用操作步骤 。

开始之前

您必须确保 StorageGRID 系统中的所有节点均处于正确状态，如下所示：

- StorageGRID 系统中的所有节点都必须已连接（）。

> 如果要执行已断开连接的站点停用，则必须断开要删除站点上的所有节点，并且必须连接所有其他站点上的所有节点。

> 如果一个或多个卷脱机(已卸载)、或者它们联机(已挂载)但处于错误状态、则不会开始取消配置。

> 如果在停用过程中一个或多个卷脱机、则停用过程将在这些卷恢复联机后完成。

- 要删除的站点上的任何节点都不能具有属于高可用性（ HA ）组的接口。

关于此任务

如果步骤 5 （解决节点冲突）中列出了任何节点，则必须更正问题描述 ，然后才能开始停用。

在此页面中启动站点停用操作步骤 之前，请查看以下注意事项：

- 您必须留出足够的时间来完成停用操作步骤 。

> 从站点移动或删除对象数据可能需要数天，数周甚至数月的时间，具体取决于站点上的数据量，系统上的负载，网络延迟以及所需 ILM 更改的性质。

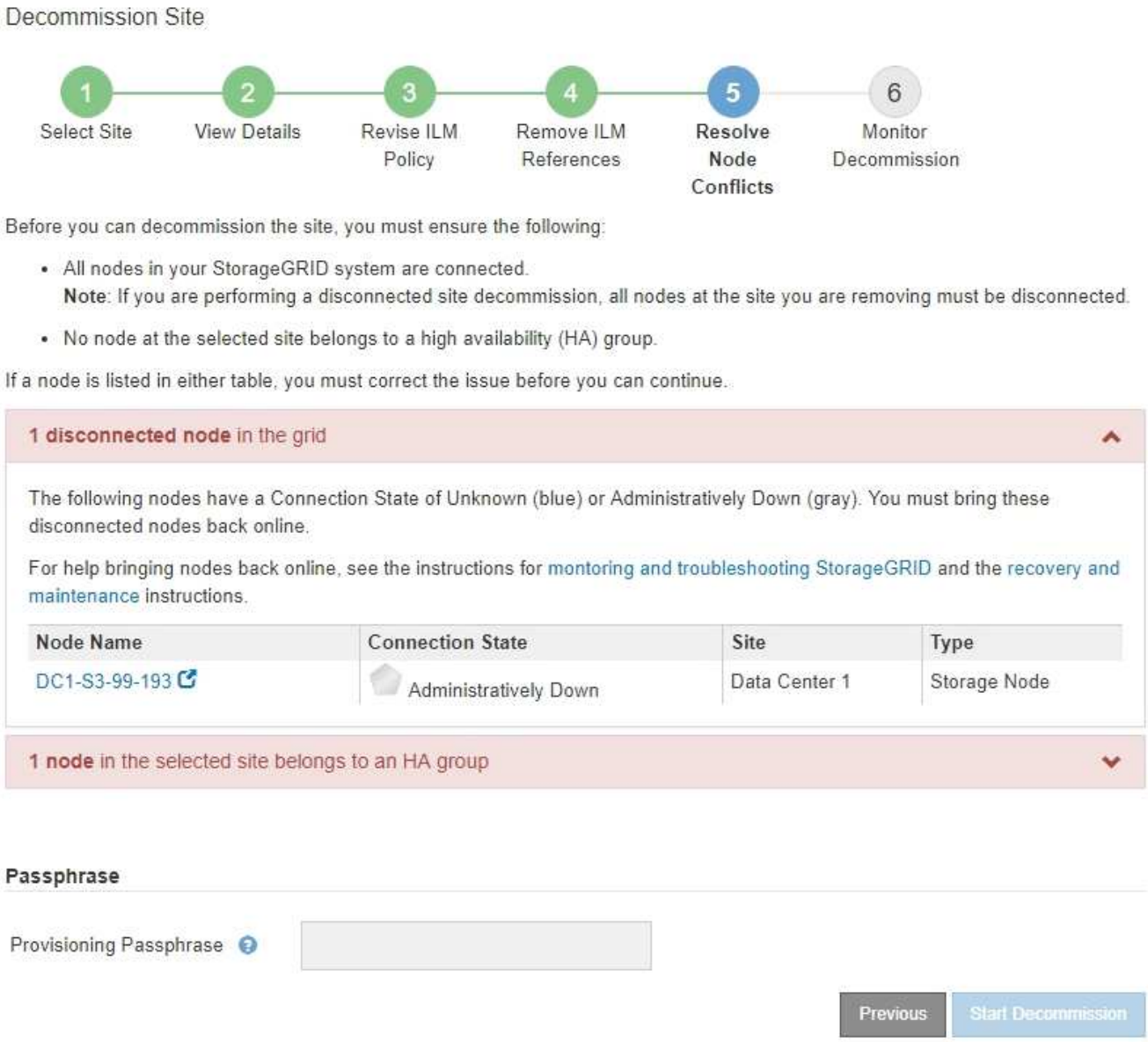
- 站点停用操作步骤 运行时：
  - 您不能创建引用要停用的站点的ILM规则。您也无法编辑现有ILM规则以引用此站点。
  - 您无法执行其他维护过程、例如扩展或升级。

> 如果在已连接站点停用期间需要执行另一个维护操作步骤 ，则可以在删除存储节点时暂停操作步骤 。“停用复制的和经过删除编码的数据”阶段会启用*Pause*按钮。

  - 如果您需要在启动站点停用操作步骤 后恢复任何节点，必须联系支持部门。

步骤

1. 查看步骤 5（解决节点冲突）的断开的节点部分，以确定 StorageGRID 系统中是否有任何节点的连接状态为未知（）或管理性关闭（）。

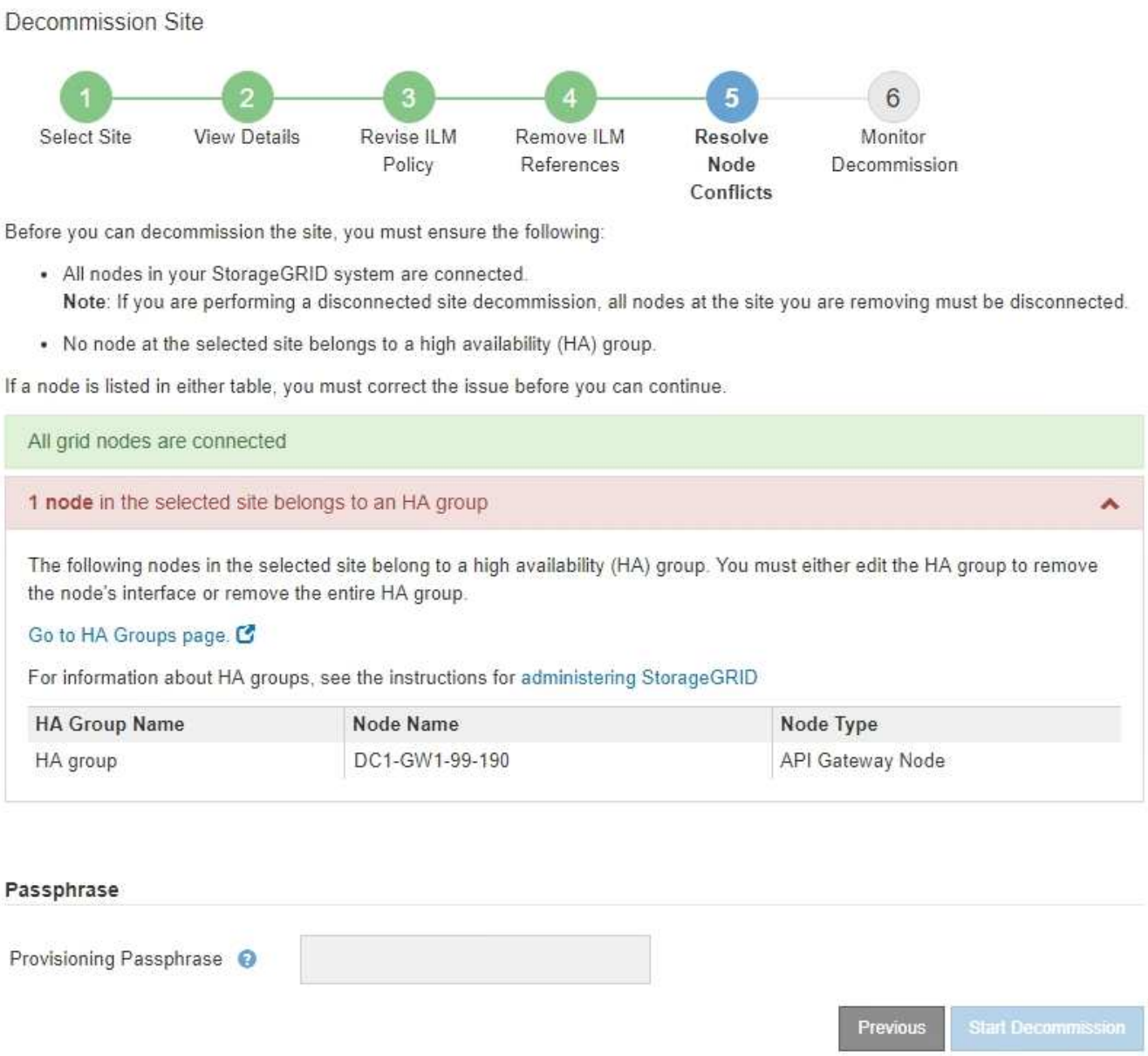


2. 如果任何节点已断开连接，请将其恢复联机。

   请参见"节点过程"。如需帮助，请联系技术支持。

3. 当所有已断开连接的节点恢复联机后，请查看步骤 5 （解决节点冲突）中的 HA 组部分。

   此表列出了选定站点中属于高可用性（ HA ）组的任何节点。



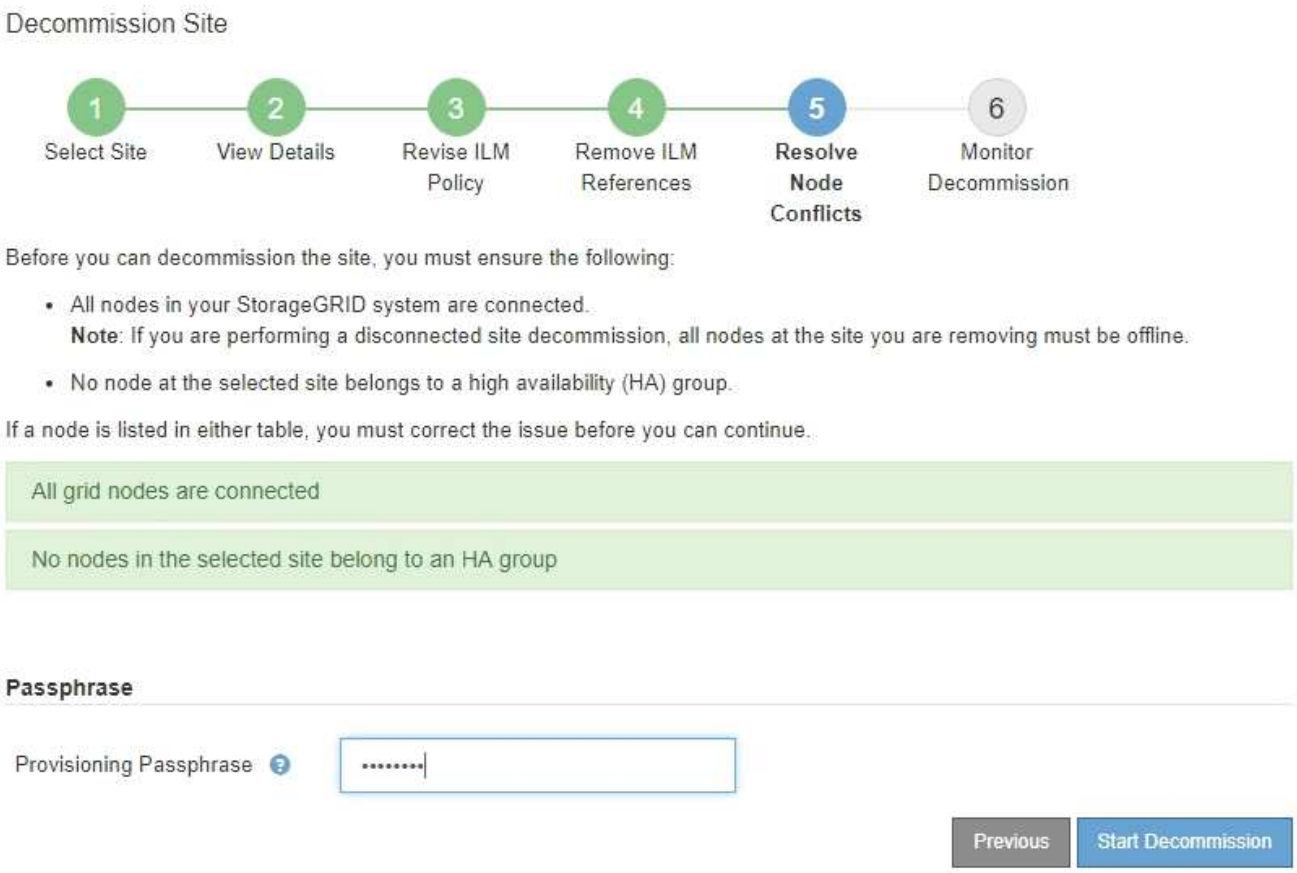
4. 如果列出了任何节点，请执行以下操作之一：

   - 编辑每个受影响的 HA 组以删除节点接口。
   - 从此站点中删除仅包含节点的 HA 组。请参见有关管理 StorageGRID 的说明。

   如果所有节点都已连接，并且所选站点中的节点未用于 HA 组，则启用 **Provisioning passphrase** 字段。

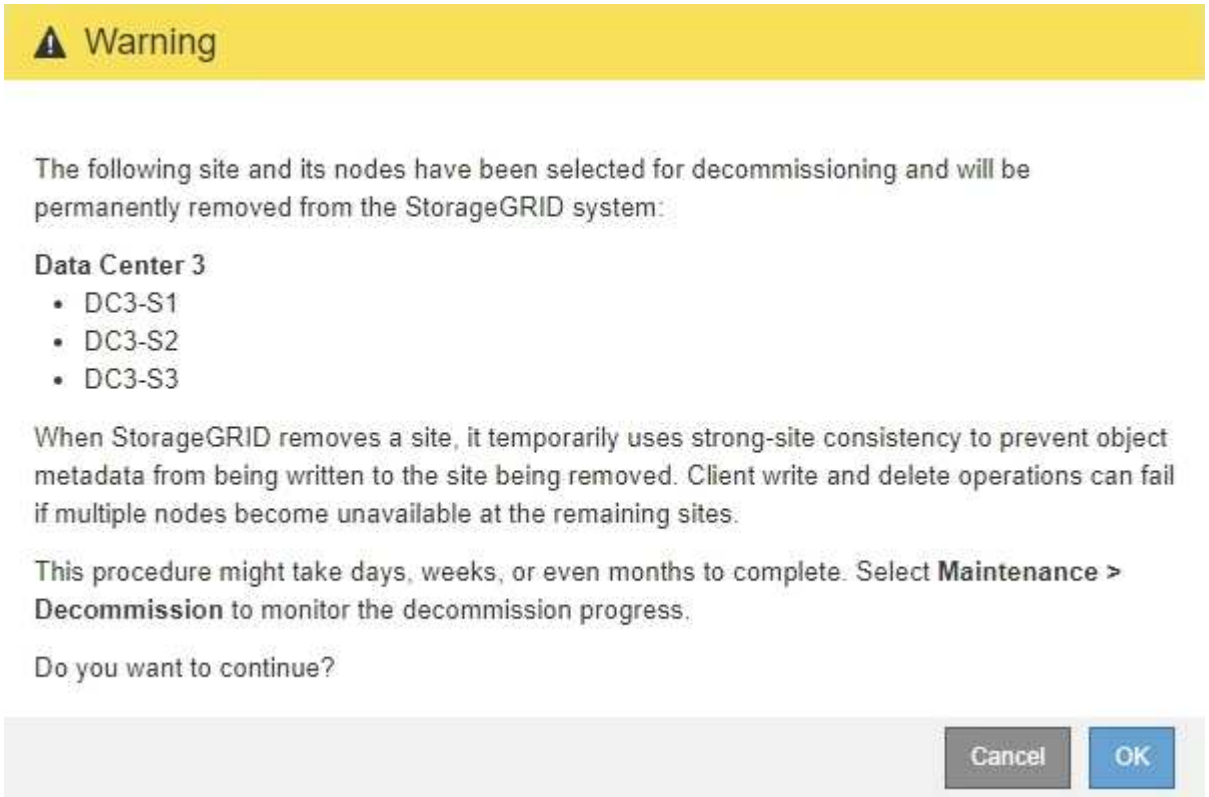
5. 输入配置密码短语。

   此时， * 开始取消配置 * 按钮将变为启用状态。



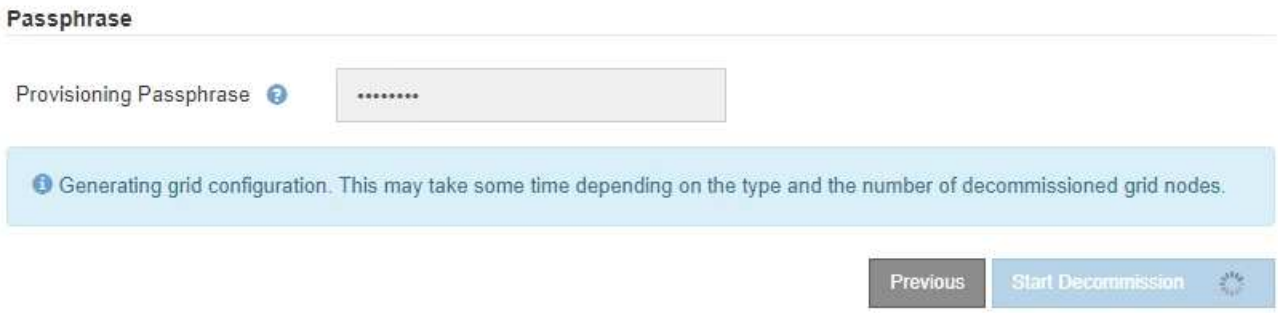
6. 如果您已准备好启动站点停用操作步骤，请选择 * 启动停用 * 。

警告将列出要删除的站点和节点。系统会提醒您，完全删除此站点可能需要数天，数周甚至数月的时间。



7. 查看警告。如果您已准备好开始，请选择 * 确定 * 。

   生成新网格配置时，将显示一条消息。此过程可能需要一些时间，具体取决于停用的网格节点的类型和数量。



   生成新网格配置后，将显示步骤 6 （监控取消配置）。

   在停用完成之前， * 上一步 * 按钮将保持禁用状态。

在 **StorageGRID** 中监控站点停用进度

从 " 取消配置站点 " 页面向导的第 6 步（监控取消配置）中，您可以在删除站点时监控进度。

关于此任务

当 StorageGRID 删除已连接站点时，它将按以下顺序删除节点：

1. 网关节点
2. 管理节点
3. 存储节点

当 StorageGRID 删除已断开连接的站点时，它会按以下顺序删除节点：

1. 网关节点
2. 存储节点
3. 管理节点

每个网关节点或管理节点可能只需要几分钟或一小时即可删除；但是，存储节点可能需要数天或数周的时间。

步骤

1. 一旦生成新的恢复包，请下载该文件。



尽快下载恢复包，以确保在退役过程中出现问题时可以恢复电网。

a. 选择消息中的链接，或选择*维护* > 系统 > 恢复包。

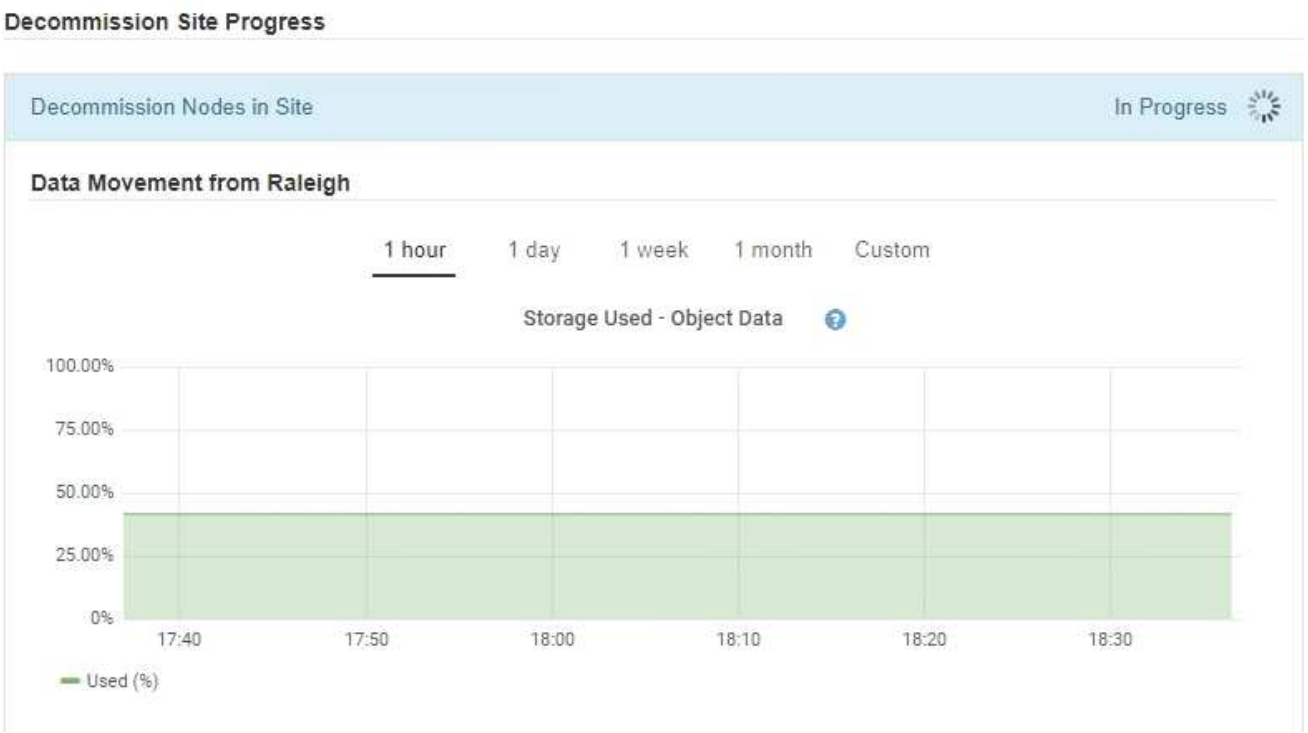
b. 下载 `.zip`文件。

请参阅说明"下载恢复包"。

恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

2. 使用 " 数据移动 " 图表监控对象数据从该站点到其他站点的移动情况。

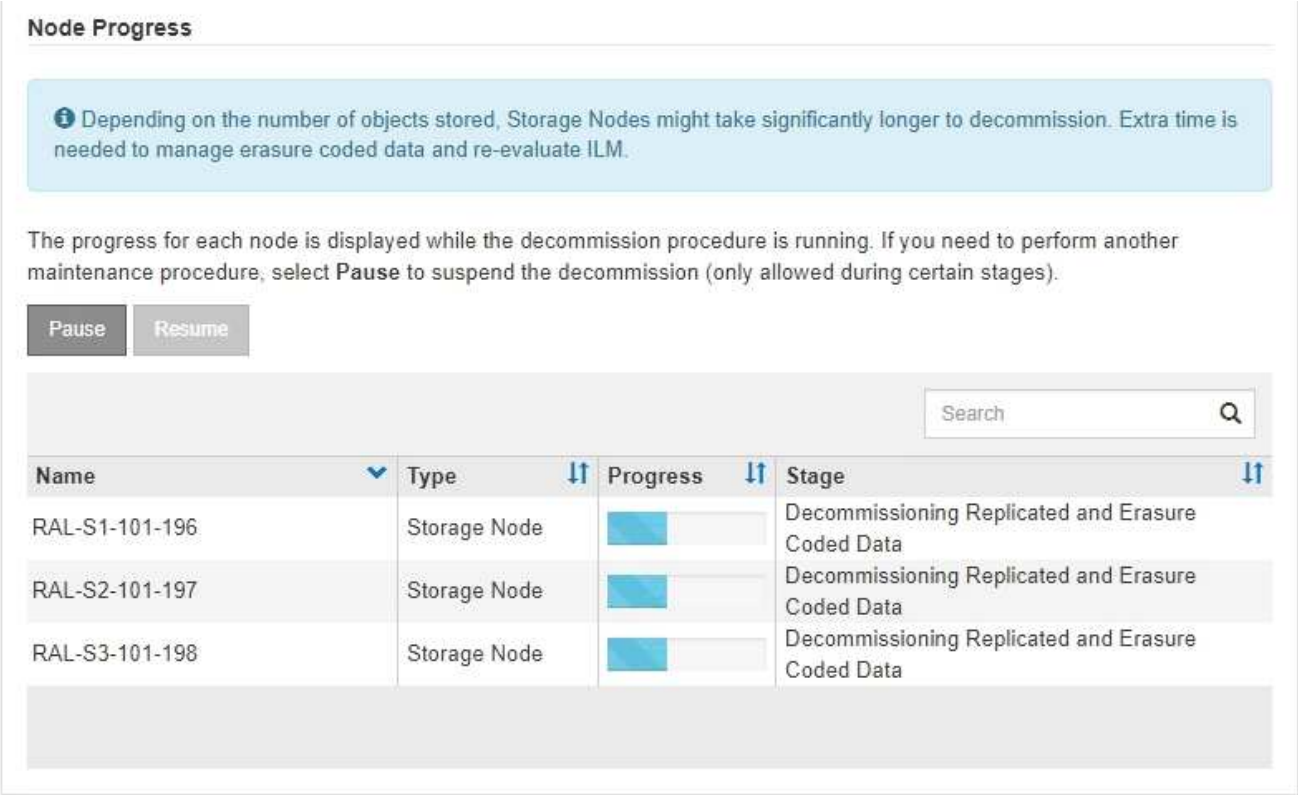
在步骤 3 （修订 ILM 策略）中激活新的 ILM 策略后，数据移动开始。数据移动将在整个停用操作步骤 中进行。



3. 在页面的节点进度部分中，在删除节点时监控停用操作步骤 的进度。

删除存储节点后，每个节点将经历一系列阶段。尽管其中大多数阶段发生得很快甚至不可能发生，但根据需

要移动的数据量，您可能需要等待几天甚至几周才能完成其他阶段。需要更多时间来管理经过纠删编码的数据并重新评估 ILM 。



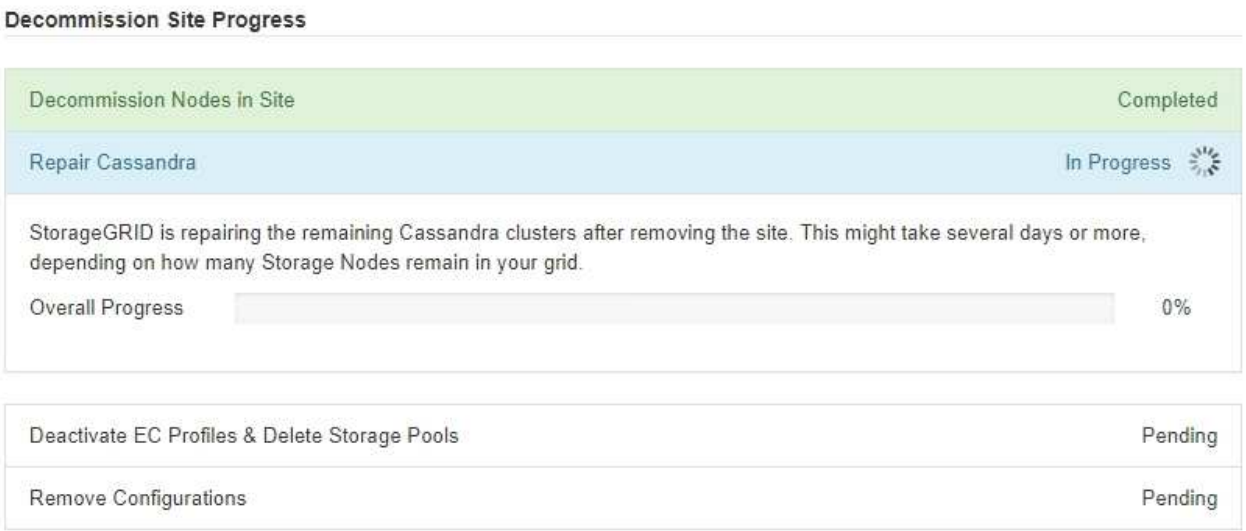
如果您正在监控已连接站点停用的进度，请参阅此表以了解存储节点的停用阶段：

阶段	估计持续时间
待定	分钟或更短
等待锁定	分钟
准备任务	分钟或更短
将 LDR 标记为已停用	分钟
停用复制的和经过Erasure编码的数据	小时，天或周，具体取决于数据量 • 注意 *： 如果您需要执行其他维护活动，可以在此阶段暂停站点停用。
LDR 设置状态	分钟
刷新审核队列	分钟到小时，具体取决于消息数量和网络延迟。
完成	分钟

如果您要监控已断开连接的站点停用的进度，请参见下表以了解存储节点的停用阶段：

阶段	估计持续时间
待定	分钟或更短
等待锁定	分钟
准备任务	分钟或更短
禁用外部服务	分钟
证书撤消	分钟
节点取消注册	分钟
存储级别取消注册	分钟
删除存储组	分钟
实体删除	分钟
完成	分钟

4. 在所有节点均已达到完成阶段后，请等待其余站点停用操作完成。
   - 在 * 修复 Cassandra* 步骤中， StorageGRID 会对网格中保留的 Cassandra 集群进行任何必要的修复。这些修复可能需要几天或更长时间，具体取决于网格中剩余的存储节点数。



   - 在 * 停用 EC 配置文件并删除存储池 * 步骤中，将进行以下 ILM 更改：
     - 任何引用站点的纠删编码配置文件都将被停用。

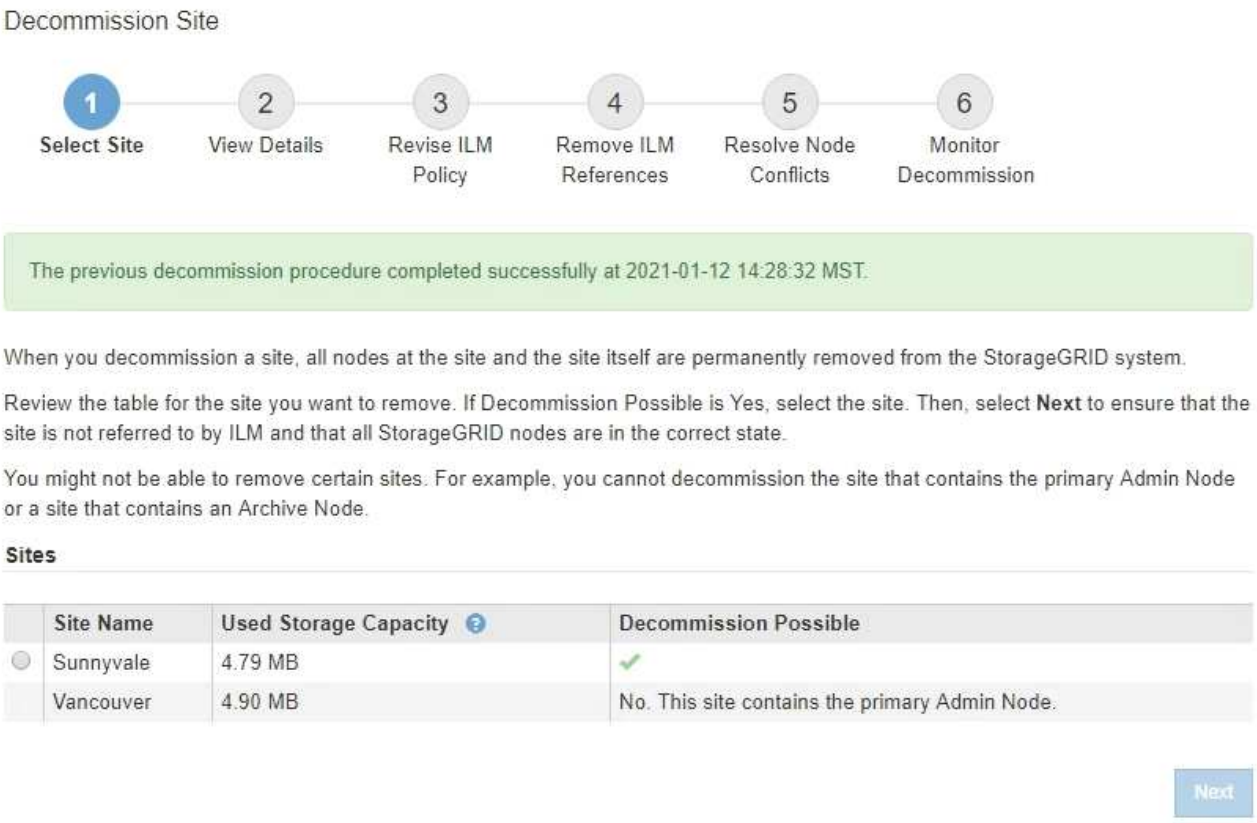
- 系统将删除引用此站点的任何存储池。

> 所有存储节点存储池(StorageGRID 11.6及更早版本)也会被删除、因为它会使用所有站点站点。

- 最后，在 * 删除配置 * 步骤中，对站点及其节点的任何剩余引用都将从网格的其余部分中删除。



5. 停用操作步骤 完成后， " 停用站点 " 页面将显示一条成功消息，并且不再显示已删除的站点。



完成后

完成站点停用操作步骤 后，完成以下任务：

- 确保已擦除已停用站点中所有存储节点的驱动器。使用商用数据擦除工具或服务永久安全地从驱动器中删除数据。
- 如果此站点包含一个或多个管理节点，并且已为您的 StorageGRID 系统启用单点登录（ SSO ），请从 Active Directory 联合身份验证服务（ AD FS ）中删除此站点的所有依赖方信任。
- 在已连接站点停用操作步骤 期间正常关闭节点后，请删除关联的虚拟机。

重命名网格、站点或节点

使用 **StorageGRID** 重命名过程

您可以根据需要更改整个网格、每个站点和每个节点在网格管理器中显示的显示名称。您可以根据需要随时安全地更新显示名称。

什么是重命名操作步骤？

首次安装StorageGRID 时、您需要为网格、每个站点和每个节点指定一个名称。这些初始名称称为_system names"、它们是最初在整个StorageGRID 中显示的名称。

内部StorageGRID 操作需要系统名称、并且无法更改。但是、您可以使用重命名操作步骤 为网格、每个站点和每个节点定义新的_display names"。这些显示名称显示在不同的StorageGRID 位置、而不是(在某些情况下、除了显示)底层系统名称。

使用重命名操作步骤 可更正错误、实施不同的命名约定或指示某个站点及其所有节点均已重新定位。与系统名称不同、显示名称可以根据需要随时更新、而不会影响StorageGRID 操作。

系统名称和显示名称显示在何处?

下表总结了系统名称和显示名称在StorageGRID 用户界面和StorageGRID 文件中的显示位置。

位置	系统名称	显示名称
网格管理器页面	除非重命名项目、否则显示	如果重命名某个项目、则会在以下位置显示、而不是显示系统名称： • 信息板 • 节点页面 • 高可用性组、负载平衡器端点、VLAN接口、密钥管理服务器、网格密码的配置页面 和防火墙控制 • 警报 • 存储池定义 • 对象元数据查找页面 • 与维护过程相关的页面、包括升级、修补程序、SANtricity OS 升级、停用、 扩展、恢复和对象存在性检查 • 支持页面(日志和诊断) • 单点登录页面、位于管理节点详细信息表中管理节点主机名旁边
节点 > 节点的 概览选项卡	始终显示	仅在重命名项目时显示
节点健康 API	总是返回	仅当重命名项目时返回

使用SSH访问节点时的提示	显示为主名称、除非该项目已重命名：
	`admin@SYSTEM-NAME: ~ $`
	重命名项目时包含在圆括号中：
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		重命名项目时显示为主名称：
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt`恢复包中的文件	显示为 `Server Name`	显示为 `Display Name`

位置	系统名称	显示名称
`/etc/hosts`文件 例如： `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	始终显示在第二列中	重命名项目时、显示在第四列中
`topology-display-names.json`，随AutoSupport数据提供	不包括	为空、除非已重命名项；否则、会将网格、站点和节点ID映射到其显示名称。

显示名称要求

在使用此操作步骤 之前、请查看显示名称的要求。

显示节点的名称

节点的显示名称必须遵循以下规则：

- 必须在整个StorageGRID 系统中是唯一的。
- 不能与StorageGRID 系统中任何其他项目的系统名称相同。
- 必须包含至少1个且不超过32个字符。
- 可以包含数字、连字符(-)以及大小写字母。
- 可以以字母或数字开头或结尾、但不能以连字符开头或结尾。
- 不能全部为数字。
- 不区分大小写。例如、 `DC1-ADM`和 `dc1-adm`被视为重复项。

您可以使用先前由其他节点使用的显示名称重命名节点、只要重命名不会导致显示名称或系统名称重复即可。

网格和站点的显示名称

网格和站点的显示名称遵循相同的规则、但以下情况除外：

- 可以包含空格。
- 可以包含以下特殊字符： `= - _ : , . @ !`
- 可以以特殊字符开头和结尾、包括连字符。

- 可以是所有数字或特殊字符。

显示名称最佳实践

如果您计划重命名多个项目、请在使用此操作步骤 之前记录您的常规命名方案。设计一个系统、确保名称唯一、一致且易于理解。

您可以使用符合组织要求的任何命名约定。请考虑以下基本建议、了解应包含哪些内容：

- 站点指示符：如果有多个站点、请为每个节点名称添加一个站点代码。
- 节点类型：节点名称通常表示节点的类型。您可以使用、 `adm`和 `gw`(存储节点、管理节点和网关节点)等缩写 `s`。
- 节点编号：如果站点包含多个特定类型的节点、请在每个节点的名称中添加一个唯一编号。

在为名称添加可能随时间推移而变化的特定详细信息之前、请三思。例如、不要在节点名称中包含IP地址、因为这些地址可以更改。同样、如果您移动设备或升级硬件、机架位置或设备型号也可能会发生变化。

示例显示名称

假设您的StorageGRID 系统有三个数据中心、每个数据中心都有不同类型的节点。您的显示名称可能很简单、如下所示：

- 网格： `StorageGRID Deployment`
- 第一个站点： `Data Center 1`
  - `dc1-adm1`
  - `dc1-s1`
  - `dc1-s2`
  - `dc1-s3`
  - `dc1-gw1`
- 第二个站点： `Data Center 2`
  - `dc2-adm2`
  - `dc2-s1`
  - `dc2-s2`
  - `dc2-s3`
- 第三站点： `Data Center 3`
  - `dc3-s1`
  - `dc3-s2`
  - `dc3-s3`

添加或更新 **StorageGRID** 显示名称

您可以使用此操作步骤 添加或更新网格、站点和节点所使用的显示名称。您可以同时重命

名单个项目、多个项目甚至所有项目。定义或更新显示名称不会以任何方式影响StorageGRID 操作。

开始之前

- 从任何管理节点，您都可以使用"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您了解显示名称的要求和最佳实践。请参阅。 "重命名网格、站点和节点"

如何重命名网格、站点或节点

您可以重命名StorageGRID 系统、一个或多个站点或一个或多个节点。

您可以使用其他节点先前使用的显示名称、只要重命名不会导致显示名称或系统名称重复即可。

选择要重命名的项目

要开始、请选择要重命名的项目。

步骤

1. 选择*维护* > 任务 > 重命名网格、站点和节点。
2. 在*选择名称*步骤中，选择要重命名的项目。

要更改的项目	说明
系统中所有内容(或几乎所有内容)的名称	a. 选择*全选*。 b. (可选)清除不想重命名的任何项目。
网格的名称	选中网格对应的复选框。
站点及其部分或全部节点的名称	a. 选中站点的表标题中的复选框。 b. (可选)清除不想重命名的任何节点。
站点名称	选中站点的复选框。
节点名称	选中节点对应的复选框。

3. 选择 * 继续 * 。
4. 查看表格、其中包括您选择的项目。
   - *显示名称*列显示每个项目的当前名称。如果项目从未重命名，则其显示名称与其系统名称相同。
   - “系统名称”列显示您在安装过程中为每个项目输入的名称。系统名称用于内部StorageGRID 操作、无法更改。例如、节点的系统名称可能是其主机名。
   - “类型”列表示项目的类型：网格、站点或特定节点类型。

对于*PROPIN NEW NAMES*步骤，您可以分别为每个项目输入显示名称，也可以批量重命名项目。

单独重命名项目

按照以下步骤为要重命名的每个项目输入显示名称。

步骤

1. 在*显示名称*字段中，为列表中的每个项目输入建议的显示名称。

   请参见"重命名网格、站点和节点"了解命名要求。

2. 要删除任何不想重命名的项目，请在*从列表中删除*列中选择 ✕。

   如果您不会为项目建议新名称、则必须将其从表中删除。

3. 为表中的所有项目建议新名称后，选择*Rename*。

   此时将显示一条成功消息。现在，网格管理器中将使用新的显示名称。

批量重命名项目

如果项目名称共享要替换为其他字符串的通用字符串、请使用批量重命名工具。

步骤

1. 对于“建议新名称”步骤，选择“使用批量重命名工具”。

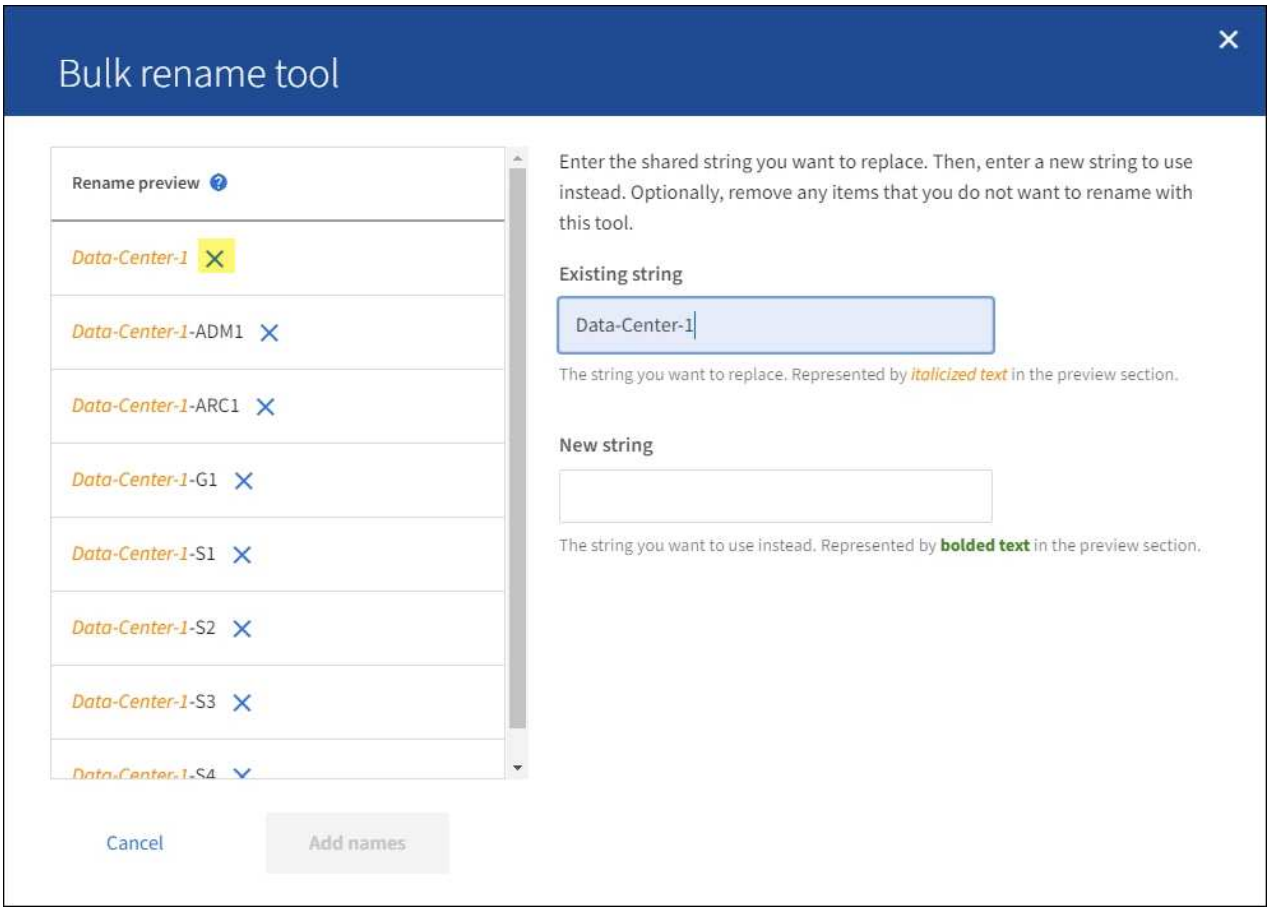
   重命名预览*包括在*PROPURE NEW NAMES*步骤中显示的所有项目。您可以使用预览查看替换共享字符串后显示名称的外观。

2. 在*existing string*字段中，输入要替换的共享字符串。例如，如果要替换的字符串为 `Data-Center-1` ，请输入*Data-Center-1*。

   键入时、无论左侧名称中的任何位置、文本都会突出显示。

3. 选择 ✕ 可删除不希望使用此工具重命名的任何项目。

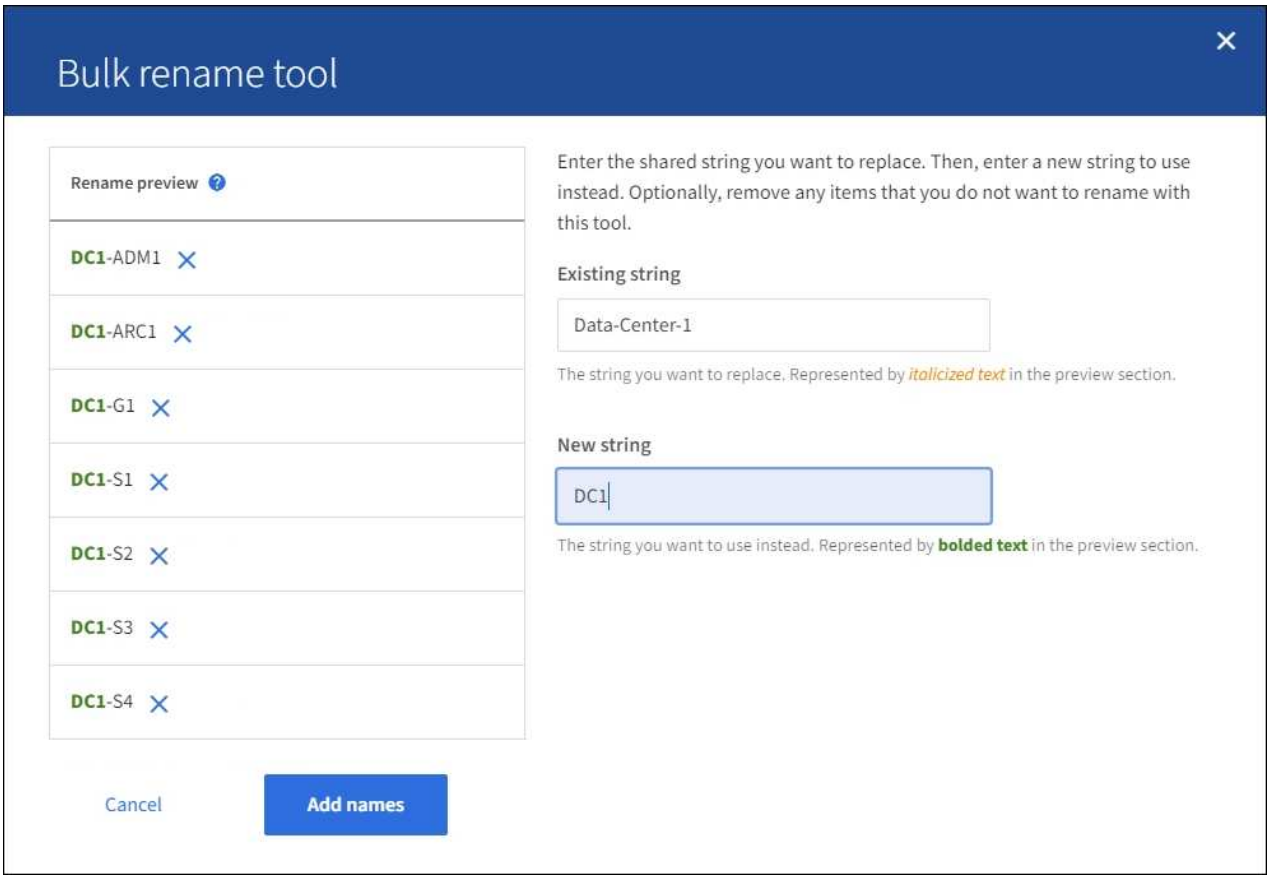
   例如，假设要重命名包含字符串 `Data-Center-1` 的所有节点，但不要重命名 `Data-Center-1` 站点本身。选择 ✕ 以从重命名预览中删除该站点。



4. 在*New string*字段中，输入要使用的替换字符串。例如，输入*DC1*。

   请参见"重命名网格、站点和节点"了解命名要求。

   输入替换字符串时、左侧的名称将更新、以便您可以验证新名称是否正确。



5. 对预览中显示的名称感到满意后，选择*添加名称*将名称添加到表中，以执行*建议新名称*步骤。
6. 进行所需的任何其他更改，或选择 ✕ 以删除不想重命名的任何项目。
7. 当您准备好重命名表中的所有项目时，选择*Rename*。

   此时将显示一条成功消息。现在，网格管理器中将使用新的显示名称。

下载恢复包

完成重命名项目后，下载并保存新的恢复包。您重命名的项目的新显示名称包含在 `Passwords.txt`文件。

步骤

1. 输入配置密码短语。
2. 选择 * 下载恢复包 * 。

   下载将立即开始。

3. 下载完成后、打开 `Passwords.txt`文件以查看所有节点的服务器名称以及任何已重命名节点的显示名称。
4. 将文件复制 `sgws-recovery-package-*id-revision*.zip`到两个安全、独立的位置。

   恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

5. 选择*完成*以返回到第一步。

将显示名称还原为系统名称

您可以将重命名的网格、站点或节点还原回其原始系统名称。将项目还原回其系统名称后，网格管理器页面和其他StorageGRID 位置将不再显示该项目的*Display name*。仅显示项目的系统名称。

步骤

1. 选择*维护* > 任务 > 重命名网格、站点和节点。
2. 在*选择名称*步骤中，选择要恢复为系统名称的任何项目。
3. 选择 * 继续 * 。
4. 对于*PROPIN NEW NAMES*步骤，将显示名称分别或批量还原回系统名称。

   分别还原为系统名称

   a. 复制每个项目的原始系统名称并将其粘贴到*显示名称*字段中，或选择 ✕ 以删除任何您不想还原的项目。

      要还原显示名称，系统名称必须显示在*Display name*字段中，但名称不区分大小写。

   b. 选择 * 重命名 * 。

      此时将显示一条成功消息。不再使用这些项目的显示名称。

   批量还原为系统名称

   a. 对于“建议新名称”步骤，选择“使用批量重命名工具”。
   b. 在*existing string*字段中，输入要替换的显示名称字符串。
   c. 在*New string*字段中，输入要使用的系统名称字符串。
   d. 选择*Add Names*，将名字添加到表中，以执行*PROPIMINGNEW NAMES*步骤。
   e. 确认*显示名称*字段中的每个条目与*系统名称*字段中的名称匹配。进行任何更改或选择 ✕ 以删除您不想还原的任何项目。

      要还原显示名称，系统名称必须显示在*Display name*字段中，但名称不区分大小写。

   f. 选择 * 重命名 * 。

      此时将显示一条成功消息。不再使用这些项目的显示名称。

5. 下载并保存新的恢复包 。

   您还原的项目的显示名称不再包含在文件中 `Passwords.txt`。

节点过程

StorageGRID 节点维护程序

您可能需要执行与特定网格节点或节点服务相关的维护过程。

移动 ADC

这"ADC 服务"位于一些存储节点上。在某些退役和节点转换情况下，您需要将 ADC 服务移动到同一站点上的另一个存储节点。

将存储节点转换为仅数据节点

您可以将不包含 ADC 服务的存储节点转换为仅数据的存储节点。

节点重启、关闭和电源

您可以使用以下过程重新启动一个或多个节点、关闭并重新启动节点、或者关闭节点并重新启动它们。

端口重映射

您可以使用端口重新映射过程从节点中删除端口重新映射、例如、如果要使用先前重新映射的端口配置负载平衡器端点、则可以使用此过程。

服务器管理器

服务器管理器在每个网格节点上运行，用于监控服务的启动和停止，并确保服务正常加入和退出 StorageGRID 系统。Server Manager 还会监控每个网格节点上的服务，并自动尝试重新启动报告故障的任何服务。

要执行服务器管理器程序，通常需要访问节点的命令行。

只有在技术支持指示您访问 Server Manager 时，才应访问此服务器管理器。

在 StorageGRID 中移动 ADC 服务

您可以将 ADC 服务移动到同一站点上的另一个存储节点。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 你有"维护或root访问权限"。
- 源节点包含 ADC 服务。
- 目标节点不包含 ADC 服务。
- 目标节点是仅元数据节点或组合（元数据和对象数据）节点。
- 源节点和目标节点位于同一站点。

关于此任务

使用移动 ADC 过程在存储节点之间手动移动 ADC 服务。例如，您可能希望跨节点重新分配 ADC 服务或将 ADC 服务移动到性能更高的节点。

此过程将 ADC、IDNT、ACCT 和 RSM 服务从一个存储节点移动到同一站点上的另一个存储节点。 RSM 、IDNT 和 ACCT 服务依赖于 ADC 服务，因此当 ADC 服务移动时，它们也会自动移动。

- 在"将存储节点转换为仅数据节点"或停用存储节点之前，您无需手动移动 ADC 服务。这些程序会在需要时自动移动 ADC 服务。有关要求的详细信息，请参阅"什么是 ADC 仲裁？"。
- StorageGRID 将 ADC 服务移动到满足托管服务要求的最新 Storage Node。

步骤

1. 记录源节点和目标节点的节点ID。

   在网格管理 API 中，源节点 ID 被称为 `sourceNodeId`。目标节点 ID 称为 `targetNodeId`。

2. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
3. 选择*转至专用API文档*。
4. 选择 `POST /private/move-adc/start`手术。请参阅"问题描述 API 请求"了解更多信息。

   在此过程中，两个节点将依次重新启动。源节点首先重新启动，然后是目标节点。

5. 您可以使用 `GET /private/move-adc`监控该过程。如果出现错误，请选择 `POST /private/move-adc/retry`重试该过程。
6. "下载恢复包"完成此过程后。

将 StorageGRID 存储节点转换为仅数据节点

为了提高性能，您可以将较慢的非 ADC 存储节点转换为仅数据的存储节点。

如果存储节点具有不同的性能特征、则将存储节点专用于数据可能会很有意义。例如、为了可能提高性能、您可以将纯数据、大容量旋转磁盘存储节点与纯元数据高性能存储节点结合使用。

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" 。

转换仅数据节点时，每个站点的网格必须至少包含三个组合或仅元数据的存储节点。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 存储节点不是仅元数据节点或仅数据节点。
- 如果存储节点包含 ADC 服务，则网格中有两个以上的 ADC 存储节点联机，并且同一站点上有可用于托管 ADC 服务的非 ADC 存储节点。
- 站点上其他节点上有足够的元数据空间（或者您已经"扩大你的网格") 来容纳将从您正在转换的存储节点迁移的元数据。

  - 如果迁移到同一站点上其他节点的元数据超出了"元数据保留空间"，电网就会变得不稳定。
  - 开始转换后，您将无法扩展网格。

关于此任务

使用此过程可将一个或多个组合的存储节点转换为仅限数据的节点。如果存储节点包含 ADC 服务，则在转换过程中，该服务将自动移动到同一站点上的另一个存储节点。

除了转换存储节点之外，此过程还会从节点中退役 Cassandra。所有元数据将迁移到组合或仅元数据的存储节点。根据需要迁移的元数据的数量，每个节点可能需要几天的时间才能完成此过程。

通常，如果每个节点的元数据使用量小于 1 TB，则一次最多可以转换 10 个节点。如果每个节点的元数据使用量超过 1 TB，则每个过程最多转换 5 个节点。

StorageGRID 将 ADC 服务移动到满足托管服务要求的最新 Storage Node。

步骤

1. 记录要转换的非 ADC 存储节点的节点 ID。
2. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
3. 选择*转至专用API文档*。
4. 选择 `POST /private/convert-to-data-only-node/start`手术。请参阅"问题描述 API 请求"了解更多信息。

   在此过程中，每个节点都会重新启动。
5. 您可以使用 `GET /private/convert-to-data-only-node`监控该过程。如果出现错误，请选择 `POST /private/convert-to-data-only-node/retry`重试该过程。
6. "下载恢复包"完成此过程后。

重新启动、关闭和电源过程

执行 **StorageGRID** 滚动重启

您可以执行滚动重新启动以重新启动多个网格节点、而不会造成服务中断。

开始之前

- 您已登录到主管理节点上的网格管理器，并且正在使用"支持的 Web 浏览器"。

  要执行此操作步骤、您必须登录到主管理节点。

- 您拥有"维护或root访问权限"。

关于此任务

如果需要同时重新启动多个节点、请使用此操作步骤。例如，在更改网格的FIPS模式后，可以使用此过程"TLS和SSH安全策略"。FIPS模式发生更改时、必须重新启动所有节点才能使更改生效。

如果只需要重新启动一个节点，则可以"从任务选项卡重新启动节点"。

当StorageGRID重新启动网格节点时、它会对每个节点发出 `reboot`命令、从而导致节点关闭并重新启动。所有服务都会自动重新启动。

- 重新启动VMware节点将重新启动虚拟机。

- 重新启动Linux节点将重新启动容器。
- 重新启动StorageGRID设备节点将重新启动计算控制器。

滚动重新启动操作步骤可以同时重新启动多个节点、但以下情况除外：

- 同一类型的两个节点不会同时重新启动。
- 网关节点和管理节点不会同时重新启动。

而是按顺序重新启动这些节点、以确保HA组、对象数据和关键节点服务始终可用。

重新启动主管理节点后、浏览器会暂时失去对网格管理器的访问权限、因此无法再监控操作步骤。因此、主管理节点将最后重新启动。

执行滚动重新启动

您可以选择要重新启动的节点、查看所做的选择、启动重新启动操作步骤并监控进度。

选择节点

首先、访问滚动重新启动页面并选择要重新启动的节点。

步骤

1. 选择*维护* > 任务 > 滚动重启。
2. 查看*节点名称*列中的连接状态和警报图标。

   如果节点与网格断开连接，则无法重新启动该节点。具有以下图标的节点，其复选框将被禁用： 或 。

3. 如果任何节点具有活动警报，请查看*Alert摘要*列中的警报列表。

   要查看节点的所有当前警报，您也可以选择"节点管理；概述选项卡"。

4. (可选)执行建议的操作以解决任何当前警报。
5. (可选)如果所有节点均已连接，并且您要重新启动所有节点，请选中表标题中的复选框，然后选择*Select All*。否则、请选择要重新启动的每个节点。

   您可以使用表的筛选器选项查看节点的子集。例如、您可以仅查看和选择某个站点上的存储节点或所有节点。

6. 选择*查看选择*。

查看选择

在此步骤中、您可以确定重新启动操作步骤所需的总时间、并确认您选择的节点正确无误。

1. 在Review Selection页面上、查看Summary、其中会指示要重新启动的节点数以及所有节点的估计总重新启动时间。
2. (可选)要从重新启动列表中删除特定节点，请选择*Remove*。

3. (可选)要添加更多节点，请选择*上一步*，选择其他节点，然后选择*查看选择*。
4. 准备好为所有选定节点启动滚动重新启动操作步骤后，请选择*Reboot N节点*。
5. 如果选择重新引导主管理节点，请阅读信息消息，然后选择*Yes*。

> 主管理节点将是最后一个重新启动的节点。此节点重新启动时、浏览器的连接将断开。当主管理节点再次可用时、您必须重新加载滚动重新启动页面。

监控滚动重新启动

在滚动重新启动操作步骤运行时、您可以从主管理节点监控它。

步骤

1. 查看操作的整体进度、其中包括以下信息：
   - 重新启动的节点数
   - 正在重新启动的节点数
   - 仍需重新启动的节点数
2. 查看每种节点类型的表。

   这些表提供了每个节点上的操作进度条、并显示了该节点的重新启动阶段、可以是以下阶段之一：

   - 正在等待重新启动
   - 正在停止服务
   - 正在重新启动系统
   - 正在启动服务
   - 重新启动已完成

停止滚动重新启动操作步骤

您可以从主管理节点停止滚动重新启动操作步骤。停止操作步骤后、状态为"正在停止服务"、"正在重新启动系统"或"正在启动服务"的所有节点都将完成重新启动操作。但是、这些节点将不再作为操作步骤的一部分进行跟踪。

步骤

1. 选择*维护* > 任务 > 滚动重启。
2. 从*监视器重新引导*步骤中，选择*停止重新引导过程*。

从任务选项卡重新启动 **StorageGRID** 节点

您可以从节点页面上的任务选项卡重新启动单个网格节点。

开始之前

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

- 您具有配置密码短语。
- 如果要重新启动主管理节点或任何存储节点、请查看以下注意事项：
  - 重新启动主管理节点后、浏览器将暂时失去对网格管理器的访问权限。
  - 如果重新启动给定站点上的两个或更多存储节点、则在重新启动期间可能无法访问某些对象。如果任何ILM规则使用*双提交*加注选项(或规则指定了*平衡*并且无法立即创建所有所需副本)、则可能会发生此问题描述。在这种情况下、StorageGRID会将新加载的对象提交到同一站点上的两个存储节点、并在稍后评估ILM。
  - 为了确保您可以在存储节点重新启动时访问所有对象，请在重新启动节点之前，停止在站点上载入对象大约一小时。

关于此任务

当StorageGRID重新启动网格节点时、它会对该节点发出 `reboot`命令、从而导致该节点关闭并重新启动。所有服务都会自动重新启动。

- 重新启动VMware节点将重新启动虚拟机。
- 重新启动Linux节点将重新启动容器。
- 重新启动StorageGRID设备节点将重新启动计算控制器。



如果需要重新启动多个节点，可以使用"滚动重新启动操作步骤"。

步骤

1. 选择*节点*。
2. 选择要重新启动的网格节点。
3. 选择 * 任务 * 选项卡。
4. 选择 * 重新启动 * 。

   此时将显示确认对话框。如果要重新启动主管理节点，则确认对话框会提醒您，服务停止后，浏览器与网格管理器的连接将暂时断开。

5. 输入配置密码短语，然后选择 * 确定 * 。
6. 等待节点重新启动。

   关闭服务可能需要一些时间。

   重新启动节点时、节点页面上会显示此节点的灰色(管理员关闭)图标。当所有服务重新启动且节点成功连接到网格后、节点页面应显示正常状态(节点名称左侧无图标)、表示没有处于活动状态的警报、并且节点已连接到网格。

从命令外壳重新启动 **StorageGRID** 节点

如果需要更密切地监控重新启动操作、或者无法访问Grid Manager、则可以登录到Grid节点并从命令Shell运行Server Manager reboot命令。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. (可选)停止服务： `service servermanager stop`

   停止服务是一个可选步骤，但建议执行此步骤。服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程，然后再在下一步中重新启动节点。

3. 重新启动网格节点： `reboot`

4. 从命令Shell中注销： `exit`

关闭 **StorageGRID** 节点

您可以使用节点的命令 Shell 关闭网格节点。

开始之前

- 您已获得 `Passwords.txt`文件。

关于此任务

在执行此操作步骤 之前，请查看以下注意事项：

- 通常，一次关闭的节点不应超过一个，以避免中断。
- 除非文档或技术支持明确指示、否则请勿在维护操作步骤 期间关闭节点。
- 关闭过程取决于节点的安装位置，如下所示：
  - 关闭 VMware 节点将关闭虚拟机。
  - 关闭 Linux 节点将关闭容器。
  - 关闭 StorageGRID 设备节点将关闭计算控制器。
- 如果您计划关闭一个站点上的多个存储节点、请在关闭这些节点之前停止在该站点上载入对象大约一小时。

  如果任何ILM规则使用*双提交*写入选项(或者如果某个规则使用*平衡*选项且无法立即创建所有所需副本)、则StorageGRID 会立即将所有新加热的对象提交到同一站点上的两个存储节点、并在稍后评估ILM。如果某个站点上的多个存储节点关闭、则在关闭期间、您可能无法访问新载入的对象。如果站点上的可用存储节点太少、写入操作也可能失败。请参阅。 "使用 ILM 管理对象"

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 停止所有服务： `service servermanager stop`

服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。

3. 如果此节点正在VMware虚拟机上运行、或者它是设备节点、请发出shutdown命令： `shutdown -h now`

无论命令的结果如何、均可执行此步骤 `service servermanager stop`。

> 在设备节点上发出命令后 `shutdown -h now`、必须重新启动设备以重新启动节点。

对于设备，此命令将关闭控制器，但设备仍处于打开状态。您必须完成下一步。

4. 如果要关闭设备节点、请按照适用于您的设备的步骤进行操作。

SG6160

a. 关闭SG6100-CN存储控制器的电源。

b. 等待SG6100-CN存储控制器上的蓝色电源LED熄灭。

SGF6112

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

SG6000

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 关闭设备电源，然后等待蓝色电源 LED 熄灭。

SGs了

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 从 SANtricity 系统管理器的主页中，选择 * 查看正在执行的操作 * 。

c. 确认所有操作均已完成，然后再继续下一步。

d. 关闭控制器架上的两个电源开关、然后等待控制器架上的所有LED熄灭。

SG5700

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 关闭设备电源，等待所有 LED 和七段显示活动停止。

SG100或SG1000

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

关闭 **StorageGRID** 主机电源

在关闭主机电源之前，必须停止该主机上所有网格节点上的服务。

步骤

1. 登录到网格节点：

a. 输入以下命令： `ssh admin@grid_node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 停止节点上运行的所有服务： `service servermanager stop`

服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。

3. 对主机上的每个节点重复步骤 1 和 2 。
4. 如果您使用的是 Linux 主机：
   a. 登录到主机操作系统。
   b. 停止节点： `storagegrid node stop`
   c. 关闭主机操作系统。
5. 如果此节点正在VMware虚拟机上运行、或者它是设备节点、请发出shutdown命令： `shutdown -h now`

无论命令的结果如何、均可执行此步骤 `service servermanager stop`。

> 在设备节点上发出命令后 `shutdown -h now`、必须重新启动设备以重新启动节点。

对于设备，此命令将关闭控制器，但设备仍处于打开状态。您必须完成下一步。

6. 如果要关闭设备节点、请按照适用于您的设备的步骤进行操作。

SG6160

a. 关闭SG6100-CN存储控制器的电源。

b. 等待SG6100-CN存储控制器上的蓝色电源LED熄灭。

SGF6112

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

SG6000

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 关闭设备电源，然后等待蓝色电源 LED 熄灭。

SGs了

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 从 SANtricity 系统管理器的主页中，选择 * 查看正在执行的操作 * 。

c. 确认所有操作均已完成，然后再继续下一步。

d. 关闭控制器架上的两个电源开关、然后等待控制器架上的所有LED熄灭。

SG5700

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 关闭设备电源，等待所有 LED 和七段显示活动停止。

SG110或SG1100

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

SG100或SG1000

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

7. 从命令Shell中注销： `exit`

相关信息

- "SGF6112和SG6160存储设备"
- "SG6000存储设备"

- "SG5700存储设备"
- "SG工具"
- "SG110和SG1100服务设备"
- "SG100和SG1000服务设备"

关闭和打开所有 **StorageGRID** 节点

例如，如果要移动数据中心，您可能需要关闭整个 StorageGRID 系统。以下步骤简要概述了执行受控关闭和启动的建议顺序。

当您关闭站点或网格中的所有节点时，存储节点脱机期间将无法访问已载入的对象。

停止服务并关闭网格节点

在关闭 StorageGRID 系统之前，必须先停止每个网格节点上运行的所有服务，然后关闭所有 VMware 虚拟机，容器引擎和 StorageGRID 设备。

关于此任务

首先停止管理节点和网关节点上的服务，然后停止存储节点上的服务。

通过此方法，您可以使用主管理节点尽可能长时间地监控其他网格节点的状态。

> 如果一台主机包含多个网格节点、则在停止该主机上的所有节点之前、不要关闭该主机。如果主机包含主管理节点，请最后关闭该主机。

> 如果需要、您可以"将节点从一台 Linux 主机迁移到另一台 Linux 主机"在不影响网格功能或可用性的情况下执行主机维护。

步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 停止所有客户端应用程序访问网格。
3. 【登录到每个网关节点】登录到每个网关节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
4. [[STOP_ALL_SERIS]停止节点上运行的所有服务： `service servermanager stop`

   服务可能需要长达 15 分钟才能关闭，您可能需要远程登录到系统以监控关闭过程。
5. 重复上述两个步骤、以停止所有存储节点和非主管理节点上的服务。

您可以按任何顺序停止这些节点上的服务。

> 如果您发出 `service servermanager stop`命令以停止设备存储节点上的服务、则必须重新启动设备以重新启动节点。

6. 对于主管理节点，重复和停止节点上的所有服务的步骤登录到节点。
7. 对于在 Linux 主机上运行的节点：
   a. 登录到主机操作系统。
   b. 停止节点： `storagegrid node stop`
   c. 关闭主机操作系统。
8. 对于VMware虚拟机上运行的节点以及设备存储节点、发出shutdown命令： `shutdown -h now`

   无论命令的结果如何、均可执行此步骤 `service servermanager stop`。

   对于设备，此命令将关闭计算控制器，但设备仍处于打开状态。您必须完成下一步。
9. 如果您有设备节点、请按照适用于您的设备的步骤进行操作。

SG110或SG1100

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

SG100或SG1000

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

SG6160

a. 关闭SG6100-CN存储控制器的电源。

b. 等待SG6100-CN存储控制器上的蓝色电源LED熄灭。

SGF6112

a. 关闭设备电源。

b. 等待蓝色电源 LED 熄灭。

SG6000

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 关闭设备电源，然后等待蓝色电源 LED 熄灭。

SGs了

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 从 SANtricity 系统管理器的主页中，选择 * 查看正在执行的操作 * 。

c. 确认所有操作均已完成，然后再继续下一步。

d. 关闭控制器架上的两个电源开关、然后等待控制器架上的所有LED熄灭。

SG5700

a. 等待存储控制器背面的绿色缓存活动 LED 熄灭。

当需要将缓存的数据写入驱动器时，此 LED 亮起。您必须等待此 LED 关闭，然后再关闭电源。

b. 关闭设备电源，等待所有 LED 和七段显示活动停止。

10. 如果需要、从命令Shell中注销： `exit`

此时， StorageGRID 网格已关闭。

11. 如果您允许外部 SSH 访问，"阻止访问"当您关闭完节点后。

启动网格节点

如果可能、请按以下顺序打开网格节点的电源：

- 首先为管理节点接通电源。
- 请最后为网关节点通电。

如果主机包含多个网格节点，则当您打开主机时，这些节点会自动恢复联机状态。

步骤

1. 打开主管理节点和任何非主管理节点的主机的电源。

   在重新启动存储节点之前，您无法登录到管理节点。

2. 启动所有存储节点的主机。

   您可以按任意顺序打开这些节点的电源。

3. 启动所有网关节点的主机。
4. 登录到网格管理器。
5. 选择*节点*并监控网格节点的状态。验证节点名称旁边没有警报图标。

相关信息

- "SGF6112和SG6160存储设备"
- "SG110和SG1100服务设备"
- "SG100和SG1000服务设备"
- "SG6000存储设备"
- "SG工具"
- "SG5700存储设备"

端口重新映射过程

删除**StorageGRID**设备上的端口重新映射

如果要为负载平衡器服务配置端点，并且要使用已配置为端口重新映射的映射到端口的端口，则必须先删除现有端口重新映射，否则此端点将无效。您必须在每个管理节点和网关节点上运行一个脚本，该节点具有冲突的重新映射端口，以删除该节点的所有端口重新映射。

关于此任务

此操作步骤 将删除所有端口重新映射。如果需要保留部分重新映射，请联系技术支持。

有关配置负载平衡器端点的信息，请参见"配置负载平衡器端点"。

如果端口重新映射提供了客户端访问、请重新配置客户端、使其使用其他端口作为负载平衡器端点、以避免服务丢失。否则、删除端口映射将导致客户端访问丢失、因此应相应地进行计划。

对于在裸机主机上部署为容器的 StorageGRID 系统，此操作步骤 不起作用。请参阅的说明"删除裸机主机上的端口重新映射"。

步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 登录到此节点。
   a. 输入以下命令： `ssh -p 8022 admin@node_IP`

      端口 8022 是基础操作系统的 SSH 端口，而端口 22 是运行 StorageGRID 的容器引擎的 SSH 端口。

   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
3. 运行以下脚本： `remove-port-remap.sh`
4. 重新启动节点： `reboot`
5. 从命令Shell中注销： `exit`
6. 对具有冲突重新映射端口的每个管理节点和网关节点重复上述步骤。
7. 如果您允许外部 SSH 访问，"阻止访问"当您完成删除端口重新映射后。

相关信息

- "用于外部通信的端口"

删除裸机主机上的 **StorageGRID** 端口重映射

如果要为负载平衡器服务配置端点，并且要使用已配置为端口重新映射的映射到端口的端口，则必须先删除现有端口重新映射，否则此端点将无效。

关于此任务

如果您在裸机主机上运行 StorageGRID ，请按照此操作步骤 而不是常规操作步骤 删除端口重新映射。您必须为每个管理节点和网关节点编辑节点配置文件，该节点的重新映射端口相互冲突，以删除该节点的所有端口重新映射并重新启动该节点。

此操作步骤 将删除所有端口重新映射。如果需要保留部分重新映射，请联系技术支持。

有关配置负载平衡器端点的信息，请参见有关管理 StorageGRID 的说明。

此操作步骤 可能会在节点重新启动时暂时丢失服务。

步骤

1. 登录到支持此节点的主机。以 root 用户身份或使用具有 sudo 权限的帐户登录。
2. 运行以下命令以临时禁用此节点： `sudo storagegrid node stop node-name`
3. 使用 vim 或 pico 等文本编辑器编辑节点的节点配置文件。

   节点配置文件位于 `/etc/storagegrid/nodes/node-name.conf`。

4. 找到节点配置文件中包含端口重新映射的部分。

   请参见以下示例中的最后两行。

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = DedicatedInterface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = DedicatedInterface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = DedicatedInterface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. 编辑 port_remap 和 port_remap_inbound 条目以删除端口重新映射。

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 运行以下命令以验证对节点的节点配置文件所做的更改：`sudo storagegrid node validate node-`

name

解决所有错误或警告，然后再继续下一步。

7. 运行以下命令重新启动节点而不重新映射端口： `sudo storagegrid node start node-name`
8. 使用文件中列出的密码以管理员身份登录到此节点 `Passwords.txt`。
9. 验证服务是否正确启动。
   a. 查看服务器上所有服务的状态列表：`sudo storagegrid-status`

      状态将自动更新。

   b. 请等待，直到所有服务的状态均为 " 正在运行 " 或 " 已验证 " 。
   c. 退出状态屏幕：`Ctrl+C`
10. 对具有冲突重新映射端口的每个管理节点和网关节点重复上述步骤。

服务器管理器过程

查看 StorageGRID Server Manager 状态和版本

对于每个网格节点，您可以查看该网格节点上运行的 Server Manager 的当前状态和版本。您还可以获取该网格节点上运行的所有服务的当前状态。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 查看在网格节点上运行的Server Manager的当前状态： **`service servermanager status`**

   报告网格节点上运行的 Server Manager 的当前状态（无论是否正在运行）。如果服务器管理器的状态为 `running`，则会列出自上次启动以来的运行时间。例如：

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. 查看在网格节点上运行的Server Manager的当前版本： **`service servermanager version`**

   此时将列出当前版本。例如：

```
11.1.0-20180425.1905.39c9493
```

4. 从命令Shell中注销： **`exit`**

查看所有 **StorageGRID** 服务的当前状态

您可以随时查看网格节点上运行的所有服务的当前状态。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 查看网格节点上正在运行的所有服务的状态： `storagegrid-status`

   例如，主管理节点的输出将 AMS ， CMN 和 NMS 服务的当前状态显示为正在运行。如果服务状态发生变化，此输出将立即更新。

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. (可选)查看网格节点上运行的所有服务的静态报告： `/usr/local/servermanager/reader.rb`

   此报告包含与持续更新报告相同的信息，但如果服务状态发生变化，则不会更新此报告。

5. 从命令Shell中注销： `exit`

启动 StorageGRID Server Manager 和所有服务

您可能需要启动 Server Manager ，该操作也会启动网格节点上的所有服务。

开始之前

您已获得 `Passwords.txt`文件。

关于此任务

如果在已运行 Server Manager 的网格节点上启动 Server Manager ，则会重新启动 Server Manager 以及网格节点上的所有服务。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 启动服务器管理器： `service servermanager start`
3. 从命令Shell中注销： `exit`

重新启动 StorageGRID Server Manager 和所有服务

您可能需要重新启动 Server Manager 和在网格节点上运行的所有服务。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 重新启动服务器管理器以及网格节点上的所有服务： `service servermanager restart`

   Server Manager 以及网格节点上的所有服务将停止并重新启动。

   使用 `restart`命令与依次使用命令 `start`和命令相同 `stop`。

3. 从命令Shell中注销： `exit`

停止 **StorageGRID Server Manager** 和所有服务

Server Manager 可始终运行，但您可能需要停止 Server Manager 以及网格节点上运行的所有服务。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 停止服务器管理器以及在网格节点上运行的所有服务： `service servermanager stop`

   服务器管理器以及网格节点上运行的所有服务均正常终止。服务可能需要长达 15 分钟才能关闭。

3. 从命令Shell中注销： `exit`

查看 **StorageGRID** 服务的当前状态

您可以随时查看在网格节点上运行的服务的当前状态。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 查看在网格节点上运行的服务的当前状态：`* service *servicename* status* 报告在网格节点上运行的请求服务的当前状态（无论是否正在运行）。例如：

```
cmn running for 1d, 14h, 21m, 2s
```

3. 从命令Shell中注销： **`exit`**

停止 **StorageGRID** 服务

某些维护过程要求您停止一项服务，同时保持网格节点上的其他服务正常运行。只有在维护操作步骤 指示停止单个服务时，才停止这些服务。

开始之前

您已获得 `Passwords.txt`文件。

关于此任务

当您使用这些步骤"以管理方式停止"服务时、服务器管理器不会自动重新启动该服务。您必须手动启动单个服务或重新启动 Server Manager 。

如果需要停止存储节点上的 LDR 服务，请注意，如果存在活动连接，则停止此服务可能需要一段时间。

步骤

1. 登录到网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 停止单个服务： `service servicename stop`

   例如：

```
service ldr stop
```

   服务可能需要长达 11 分钟才能停止。

3. 从命令Shell中注销： `exit`

相关信息

"强制终止服务"

强制终止 **StorageGRID** 服务

如果需要立即停止服务、可以使用命令。 `force-stop`

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 手动强制终止服务： `service servicename force-stop`

   例如：

   ```
   service ldr force-stop
   ```

   系统将等待 30 秒，然后再终止此服务。
3. 从命令Shell中注销： `exit`

启动或重新启动 **StorageGRID** 服务

您可能需要启动已停止的服务，或者可能需要停止并重新启动服务。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 根据服务当前是正在运行还是已停止，确定向问题描述 发出的命令。

   - 如果此服务当前已停止、请使用 `start`命令手动启动此服务： `service servicename start`

     例如：

     ```
     service ldr start
     ```

   - 如果此服务当前正在运行、请使用 `restart`命令停止此服务、然后重新启动它： `service servicename restart`

     例如：

```
service ldr restart
```

+

> 使用 `restart`命令与依次使用命令 `start`和命令相同 `stop`。即使服务当前已停止、您也可以发出 `restart`此问题。

3. 从命令Shell中注销： `exit`

使用 **StorageGRID DoNotStart** 文件

如果您在技术支持的指导下执行各种维护或配置过程，则可能会要求您使用 DoNotStart 文件来防止在启动或重新启动 Server Manager 时启动服务。

> 只有在技术支持要求您添加或删除 DoNotStart 文件时，才应添加或删除此文件。

要阻止服务启动，请将 DoNotStart 文件置于要阻止启动的服务的目录中。启动时， Server Manager 将查找 DoNotStart 文件。如果文件存在，则会阻止服务（以及与之相关的任何服务）启动。删除 DoNotStart 文件后，先前停止的服务将在下次启动或重新启动 Server Manager 时启动。删除DoNotStart文件后、服务不会自动启动。

阻止所有服务重新启动的最有效方法是阻止 NTP 服务启动。所有服务都依赖于NTP服务、如果NTP服务未运行、则无法运行。

为服务添加 **DoNotStart** 文件

通过将 DoNotStart 文件添加到网格节点上某个服务的目录中，您可以阻止单个服务启动。

开始之前

您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

a. 输入以下命令： `ssh admin@grid_node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 添加DoNotStart文件： `touch /etc/sv/service/DoNotStart`

其中 `service`是要阻止启动的服务的名称。例如、

```
touch /etc/sv/ldr/DoNotStart
```

此时将创建 DoNotStart 文件。不需要文件内容。

重新启动 Server Manager 或网格节点后， Server Manager 将重新启动，但服务不会重新启动。

3. 从命令Shell中注销： `exit`

删除 DoNotStart 文件以进行维护

删除阻止服务启动的 DoNotStart 文件时，必须启动该服务。

开始之前
您已获得 `Passwords.txt`文件。

步骤

1. 登录到网格节点：

a. 输入以下命令： `ssh admin@grid_node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 从服务目录中删除DoNotStart文件： `rm /etc/sv/service/DoNotStart`

其中 `service`是服务的名称。例如、

```
rm /etc/sv/ldr/DoNotStart
```

3. 启动服务： `service servicename start`
4. 从命令Shell中注销： `exit`

如果使用 Server Manager 时出现问题，请检查其日志文件。

与服务器管理器相关的错误消息会捕获到服务器管理器日志文件中、该文件位于：
`/var/local/log/servermanager.log`

检查此文件中有关故障的错误消息。如果需要，请将问题描述 升级到技术支持。系统可能会要求您将日志文件转发给技术支持。

存在错误状态的服务

如果您检测到某个服务已进入错误状态，请尝试重新启动此服务。

开始之前

您已获得 `Passwords.txt`文件。

关于此任务

Server Manager 可监控服务并重新启动任何意外停止的服务。如果服务失败， Server Manager 将尝试重新启动它。如果在五分钟内启动服务的尝试失败三次，则该服务将进入错误状态。Server Manager 不会尝试再次重新启动。

步骤

1. 登录到网格节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 确认服务的错误状态： `service servicename status`

   例如：

   ```
   service ldr status
   ```

   如果服务处于错误状态，则返回以下消息： `servicename in error state`。例如：

   ```
   ldr in error state
   ```

   如果服务状态为 `disabled`，请参阅的说明"删除服务的 DoNotStart 文件"。

3. 尝试通过重新启动服务来删除此错误状态： `service servicename restart`

如果服务无法重新启动，请联系技术支持。

4. 从命令Shell中注销： `exit`

网络过程

更新 **StorageGRID** 网格网络的子网

StorageGRID 会维护一个网络子网列表，用于在网格网络（ eth0 ）上的网格节点之间进行通信。这些条目包括 StorageGRID 系统中每个站点用于网格网络的子网，以及通过网格网络网关访问的 NTP ， DNS ， LDAP 或其他外部服务器所使用的任何子网。在扩展中添加网格节点或新站点时，您可能需要更新子网或向网格网络添加子网。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您已获得要配置的子网的网络地址，以 CIDR 表示法表示。

关于此任务

如果您要执行的扩展活动包括添加新子网、则必须在启动扩展操作步骤 之前将新子网添加到网格网络子网列表中。否则、您必须取消扩展、添加新子网、然后重新开始扩展。

请勿对任何节点的网格网络、管理网络或客户端网络使用包含以下 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，不要对任何节点的网格网络、管理网络或客户端网络使用以下子网范围：

- 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
- 198.51.100.0/24，因为此子网范围包含 IP 地址 198.51.100.2 和 198.51.100.4

添加子网

步骤

1. 选择*维护* > 网络 > 电网。
2. 选择*添加其他子网*以使用CIDR表示法添加新子网。

   例如，输入 `10.96.104.0/22`。

3. 输入配置密码短语，然后选择 * 保存 * 。
4. 等待更改应用完毕，然后下载新的恢复包。
   a. 选择*维护* > 系统 > 恢复包。
   b. 输入 **Provisioning passphrase**。

> 恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。它还用于恢复主管理节点。

您指定的子网将自动为 StorageGRID 系统配置。

编辑子网

步骤

1. 选择*维护* > 网络 > 电网。
2. 选择要编辑的子网并进行必要的更改。
3. 输入配置密码短语，然后选择 * 保存 * 。
4. 在确认对话框中选择 * 是 * 。
5. 等待更改应用完毕，然后下载新的恢复包。
   a. 选择*维护* > 系统 > 恢复包。
   b. 输入 **Provisioning passphrase**。

删除子网

步骤

1. 选择*维护* > 网络 > 电网。
2. 选择子网旁边的删除图标 ✕。
3. 输入配置密码短语，然后选择*Save*。
4. 在确认对话框中选择 * 是 * 。
5. 等待更改应用完毕，然后下载新的恢复包。
   a. 选择*维护* > 系统 > 恢复包。
   b. 输入 **Provisioning passphrase**。

配置 IP 地址

StorageGRID IP 地址指南

您可以使用更改 IP 工具为网格节点配置 IP 地址来执行网络配置。

您必须使用更改 IP 工具对网格部署期间最初设置的网络配置进行大部分更改。使用标准 Linux 网络命令和文件进行的手动更改可能不会传播到所有 StorageGRID 服务，并且可能不会在升级，重新启动或节点恢复过程中持续存在。

IP 更改操作步骤 可以是中断操作步骤 。在应用新配置之前，网格的某些部分可能不可用。

如果仅更改网格网络子网列表，请使用网格管理器添加或更改网络配置。否则，如果网格管理器因网络配置问题描述 而无法访问，或者您同时执行网格网络路由更改和其他网络更改，请使用更改 IP 工具。

如果要更改网格中所有节点的网格网络IP地址，请使用"适用于网格范围更改的特殊操作步骤"。

以太网接口

分配给 eth0 的 IP 地址始终是网格节点的网格网络 IP 地址。分配给 eth1 的 IP 地址始终是网格节点的管理网络 IP 地址。分配给 eth2 的 IP 地址始终是网格节点的客户端网络 IP 地址。

请注意，在某些平台上，例如 StorageGRID 设备， eth0 ， eth1 和 eth2 可能是由物理或 VLAN 接口的从属网桥或绑定组成的聚合接口。在这些平台上， * SSM* > * 资源 * 选项卡可能会显示除 eth0 ， eth1 或 eth2 之外分配给其他接口的网格，管理员和客户端网络 IP 地址。

DHCP

您只能在部署阶段设置 DHCP 。配置期间无法设置DHCP。如果要更改网格节点的 IP 地址，子网掩码和默认网关，则必须使用 IP 地址更改过程。使用更改 IP 工具将使发生原因 DHCP 地址变为静态地址。

高可用性(HA)组

- 如果客户端网络接口包含在HA组中、则不能将该接口的客户端网络IP地址更改为为HA组配置的子网之外的地址。
- 您不能将客户端网络IP地址更改为分配给在客户端网络接口上配置的HA组的现有虚拟IP地址的值。
- 如果某个网格网络接口包含在HA组中、则不能将该接口的网格网络IP地址更改为为HA组配置的子网之外的地址。
- 您不能将网格网络IP地址更改为分配给在网格网络接口上配置的HA组的现有虚拟IP地址的值。

更改 StorageGRID 中的节点网络配置

您可以使用更改 IP 工具更改一个或多个节点的网络配置。您可以更改网格网络的配置，也可以添加、更改或删除管理员或客户端网络。您还可以更改设备节点 BMC 的 LAN IP 设置。

开始之前

您已获得 `Passwords.txt`文件。

关于此任务

*Linux：*如果您是第一次将网格节点添加到管理网络或客户端网络，并且之前没有在节点配置文件中配置 ADMIN_NETWORK_TARGET 或 CLIENT_NETWORK_TARGET，则必须现在这样做。查看StorageGRID"安装说明"适用于您的 Linux 操作系统。

*设备：*在StorageGRID 设备上，如果在初始安装期间未在StorageGRID 设备安装程序中配置客户端或管理网络，则无法仅使用更改IP工具来添加网络。首先，您必须 "将设备置于维护模式"配置链路，将设备恢复到正常运行模式，然后使用更改IP工具修改网络配置。请参见 "用于配置网络链路的操作步骤"。

您可以更改任何网络上一个或多个节点的 IP 地址，子网掩码，网关或 MTU 值。

您还可以从客户端网络或管理网络添加或删除节点：

- 您可以通过向客户端网络或管理网络添加节点上的 IP 地址 / 子网掩码来将该节点添加到该节点。
- 您可以通过删除客户端网络或管理网络中某个节点的 IP 地址 / 子网掩码来从该网络中删除该节点。

  无法从网格网络中删除节点。

> 不允许IP地址交换。如果必须在网格节点之间交换 IP 地址，则必须使用临时中间 IP 地址。

> 如果您的 StorageGRID 系统启用了单点登录 (SSO)，并且您正在更改管理节点的 IP 地址，请注意，使用管理节点的 IP 地址（而不是建议的完全限定域名）配置的任何依赖方信任都将失效。您将无法再登录到节点。更改 IP 地址后，必须立即使用新 IP 地址更新或重新配置节点在 Active Directory 联合身份验证服务 (AD FS) 中的依赖方信任。请参阅使用 "OIDC" 或 "SAML" 设置 SSO 的说明。

> 使用更改 IP 工具对网络所做的任何更改都会传播到 StorageGRID 设备的安装程序固件。这样，如果在设备上重新安装 StorageGRID 软件，或者将设备置于维护模式，则网络配置将正确无误。

步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 登录到主管理节点：

   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

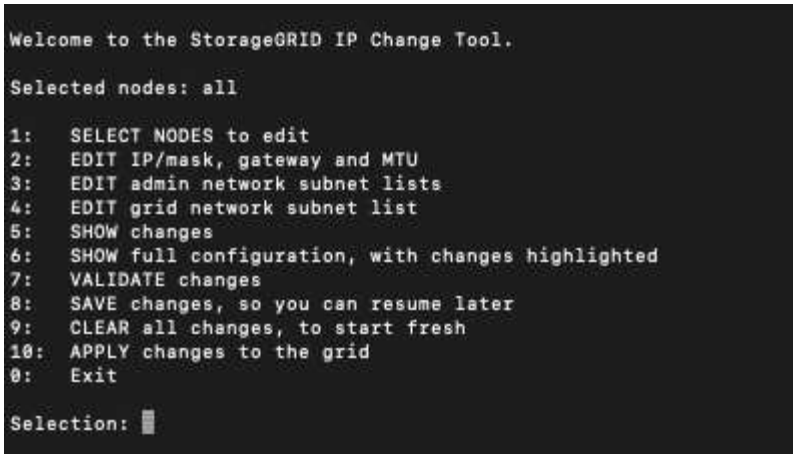
   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

3. 输入以下命令、启动更改IP工具： `change-ip`
4. 在提示符处输入配置密码短语。

   此时将显示主菜单。



5. 也可以选择 * 1 * 来选择要更新的节点。然后选择以下选项之一：

   - * 1 * ： 单节点—按名称选择
   - * 2 * ： 单节点—按站点选择，然后按名称选择
   - **3** ： 单节点—按当前 IP 选择
   - **4** ： 站点上的所有节点
   - **5** ： 网格中的所有节点
     - 注： * 如果要更新所有节点，请允许 " 全部 " 保持选中状态。

   选择后，将显示主菜单，并更新 * 选定节点 * 字段以反映您的选择。所有后续操作仅在显示的节点上执行。

6. 在主菜单上，选择选项 * 2 * 以编辑选定节点的 IP/ 掩码，网关和 MTU 信息。

   a. 选择要更改的网络：

      - * 1 * ： 网格网络
      - * 2 * ： 管理网络
      - * 3 * ： 客户端网络
      - **4**:所有网络

      选择后、提示符将显示节点名称、网络名称(网格、管理或客户端)、数据类型(IP/掩码、 网关或MTU)和当前值。

      编辑 DHCP 配置接口的 IP 地址，前缀长度，网关或 MTU 将使接口更改为静态。如果选择更改由 DHCP 配置的接口，则会显示一条警告，通知您该接口将更改为静态。

      无法编辑配置为的接口 `fixed`。

   b. 要设置新值，请按当前值所示格式输入该值。

   c. 要保持当前值不变，请按 * 输入 * 。

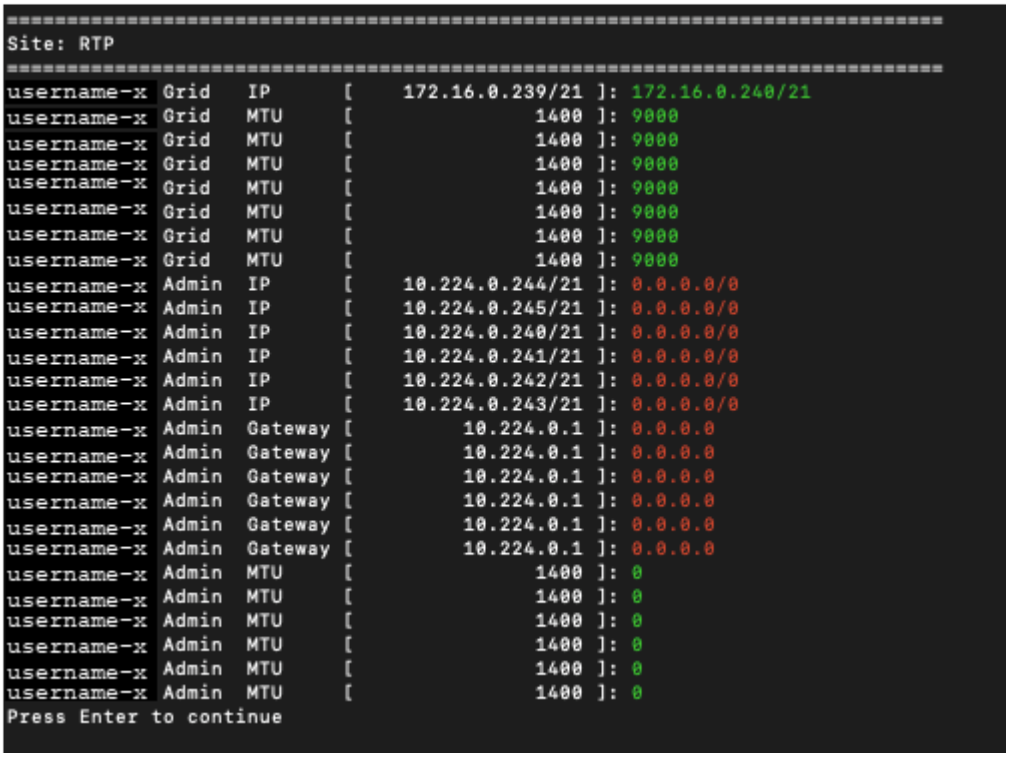
   d. 如果数据类型为 `IP/mask`，则可以输入*d*或*0.0.0.0/0*从节点中删除管理或客户端网络。

   e. 编辑要更改的所有节点后，输入 * 。 q* 返回主菜单。

      您所做的更改将一直保留，直到清除或应用为止。

7. 选择以下选项之一，查看您所做的更改：

   - * 5* ：显示输出中的编辑内容，这些编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如示例输出所示：



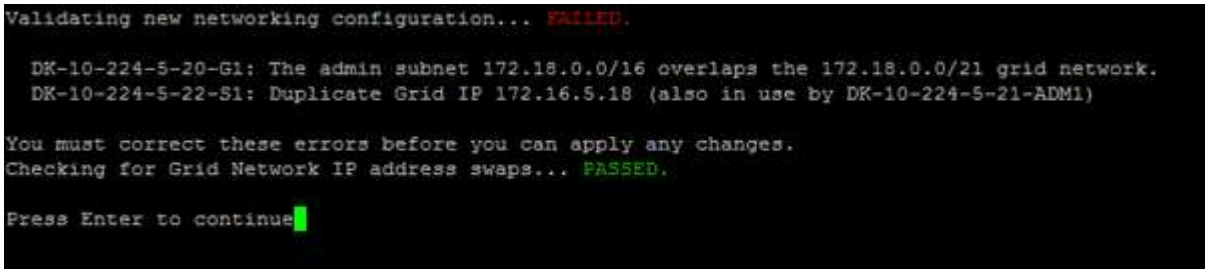
   - * 6 * ：显示输出中显示的编辑内容，其中显示了完整配置。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。正确显示取决于您的终端客户端是否支持必要的 VT100 转义序列。

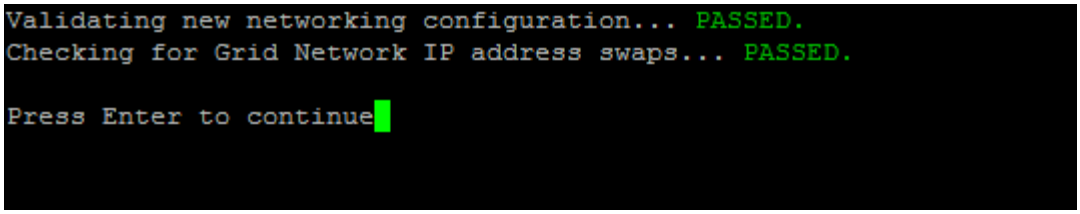
8. 选择选项 * 7* 以验证所有更改。

   此验证可确保不违反网格、管理和客户端网络的规则、例如不使用重叠子网。

   在此示例中，验证返回错误。



   在此示例中，验证已通过。



9. 验证通过后、选择以下选项之一：

   - **8**：保存未应用的更改。

     使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

   - * 。 10*：应用新网络配置。

10. 如果选择了选项 * 。 10* ，请选择以下选项之一：

    - * 应用 *：立即应用更改，并在必要时自动重新启动每个节点。

      如果新网络配置不需要更改任何物理网络连接，您可以选择 * 应用 * 以立即应用更改。如果需要，节点将自动重新启动。此时将显示需要重新启动的节点。

    - * 阶段 *：下次手动重新启动节点时应用更改。

      如果要使新网络配置正常运行，需要更改物理或虚拟网络配置，则必须使用 * 阶段 * 选项，关闭受影响的节点，进行必要的物理网络更改并重新启动受影响的节点。如果选择 * 应用 * 而未先进行这些网络更改，则更改通常会失败。

      如果使用 * 阶段 * 选项，则必须在暂存后尽快重新启动节点，以最大程度地减少中断。

    - **CANCEL**：目前请勿更改任何网络。

      如果您不知道建议的更改需要重新启动节点，则可以推迟更改以最大限度地减少对用户的影响。选择 * 取消 * 将返回到主菜单并保留所做的更改，以便稍后应用。

      如果选择 * 应用 * 或 * 阶段 * ，则会生成一个新的网络配置文件，并执行配置，同时会使用新的工作信息更新节点。

      在配置期间，输出将在应用更新时显示状态。

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

    应用或阶段更改后，将根据网格配置更改生成新的恢复包。

11. 如果选择了 * 阶段 * ，请在配置完成后按照以下步骤进行操作：

    a. 根据需要进行物理或虚拟网络更改。

- 物理网络更改 * ：进行必要的物理网络更改，必要时安全关闭节点。

Linux：如果您是首次将节点添加到管理网络或客户端网络，请确保已按中所述添加接口"Linux ： 向现有节点添加接口"。

a. 重新启动受影响的节点。

12. 完成更改后，选择 * 。 0* 退出更改 IP 工具。
13. 从网格管理器下载新的恢复包。
    a. 选择*维护* > 系统 > 恢复包。
    b. 输入配置密码短语。
14. 如果您允许外部 SSH 访问，"阻止访问"当您完成更改节点网络配置后。

暂时更改 **LACP PDU** 速率

要对设备中安装的网络组件执行维护操作（例如升级 NIC 固件），您可以检查当前 LACP PDU 速率设置是否满足 NIC 通信时序要求。如果需要，您可以非持续地在快速（等待 1 秒）和慢速（等待 30 秒）之间切换 LACP PDU 速率。

要永久更改 LACP PDU 速率，请参阅 "配置网络链路"。

开始之前

- 管理节点已安装并正在运行。
- 您已获得 `Passwords.txt`文件。

步骤

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

    当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 要检查当前 LACP PDU 速率设置，请输入以下命令：

    ```
    run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh'
    ```

3. 要临时更改 LACP PDU 速率，请输入以下命令：

    ```
    run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh <speed>'
    ```

    在哪里 `<speed>`是 `fast`或者 `slow`。

下次设备重启时，LACP PDU 速率将恢复到之前的设置。

更改设备节点 **BMC LAN IP** 设置

您可以更改设备节点 BMC 的 LAN IP 设置。

1. 在 Grid Manager 中，转到 节点 > 网格节点 > **BMC** 设置。
2. 在 LAN IP 设置部分，选择 静态 或 **DHCP** 的 IP 分配类型。
3. 输入 BMC 的 MAC 地址、IPv4 地址 (CIDR) 和默认网关。
4. 选择 * 保存 * 。

您还可以使用 `PUT /bmc-configuration/root-password`或 `GET /bmc-configuration/root-password` API 更改或查看 BMC LAN IP 设置。

在 **StorageGRID** 中添加或更改管理网络上的子网列表

您可以在管理网络子网列表中添加，删除或更改一个或多个节点的子网。

开始之前

- 您已获得 `Passwords.txt`文件。

您可以为管理网络子网列表中的所有节点添加，删除或更改子网。

请勿对任何节点的网格网络、管理网络或客户端网络使用包含以下 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，不要对任何节点的网格网络、管理网络或客户端网络使用以下子网范围：

- 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
- 198.51.100.0/24，因为此子网范围包含 IP 地址 198.51.100.2 和 198.51.100.4

步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 登录到主管理节点：

a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

3. 输入以下命令、启动更改IP工具： `change-ip`
4. 在提示符处输入配置密码短语。

此时将显示主菜单。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

5. 或者，也可以限制执行操作的网络 / 节点。选择以下选项之一：
   - 如果要筛选要执行操作的特定节点，请选择 * 1 * 以选择要编辑的节点。选择以下选项之一：
     - * 1 * ： 单个节点（按名称选择）
     - * 2 * ： 单个节点（按站点选择，然后按名称选择）
     - * 3 * ： 单个节点（由当前 IP 选择）
     - **4** ： 站点上的所有节点
     - **5** ： 网格中的所有节点
     - **0** ： 返回
   - 允许"全部"保持选中状态。进行选择后，将显示主菜单屏幕。选定节点字段反映了您的新选择，现在，选定的所有操作将仅对此项执行。
6. 在主菜单上，选择用于编辑管理网络子网的选项（选项 * 3 * ）。
7. 选择以下选项之一：
   - 输入以下命令以添加子网： `add CIDR`
   - 输入以下命令以删除子网： `del CIDR`
   - 输入以下命令以设置子网列表： `set CIDR`

对于所有命令、可以使用以下格式输入多个地址： `add CIDR, CIDR`

示例： `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

您可以使用"向上箭头"将先前键入的值重新调用到当前输入提示符中、然后根据需要对其进行编辑、从而减少所需的键入量。

以下示例输入显示了如何向管理网络子网列表添加子网：

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

8. 准备好后，输入 * 。 q* 可返回主菜单屏幕。您所做的更改将一直保留，直到清除或应用为止。

如果您在步骤 3 中选择了任何“全部”节点选择模式，请按 **Enter**（不带 **q**）转到列表中的下一个节点。

9. 选择以下选项之一：

   - 选择选项 * 5* 可显示输出中的编辑内容，而输出中的编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如以下示例输出所示：

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - 选择选项 **6** 可在显示完整配置的输出中显示编辑内容。更改将以绿色（添加项）或红色（删除项）突出显示。* 注： * 某些终端模拟器可能会使用删除线格式显示添加和删除内容。

     尝试更改子网列表时，将显示以下消息：

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

如果您未明确将 NTP 和 DNS 服务器子网分配给网络，则 StorageGRID 会自动为此连接创建一个主机路由（ /32 ）。例如，如果您希望使用 /16 或 /24 路由与 DNS 或 NTP 服务器建立出站连接，则应删除自动创建的 /32 路由并添加所需的路由。如果不删除自动创建的主机路由、则在对子网列表应用任何更改后、此路由将保持不变。

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

10. 选择选项 * 7* 以验证所有暂存更改。

    此验证可确保遵循网格网络，管理网络和客户端网络的规则，例如使用重叠的子网。

11. （可选）选择选项 * 8* 保存所有分阶段更改，稍后返回以继续进行更改。

    使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

12. 执行以下操作之一：
    - 如果要在不保存或应用新网络配置的情况下清除所有更改，请选择选项 * 。
    - 如果您已准备好应用更改并配置新的网络配置，请选择选项 * 。配置期间、输出将显示已应用更新的状态、如以下示例输出所示：

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

13. 从网格管理器下载新的恢复包。
    a. 选择*维护* > 系统 > 恢复包。
    b. 输入配置密码短语。
14. 如果您允许外部 SSH 访问，"阻止访问"当您完成添加或更改子网列表后。

在 **StorageGRID** 中添加或更改网格网络上的子网列表

您可以使用更改 IP 工具在网格网络上添加或更改子网。

开始之前

- 您已获得 `Passwords.txt`文件。

您可以在网格网络子网列表中添加，删除或更改子网。更改将影响网格中所有节点上的路由。

如果仅更改网格网络子网列表，请使用网格管理器添加或更改网络配置。否则，如果网格管理器因网络配置问题描述 而无法访问，或者您同时执行网格网络路由更改和其他网络更改，请使用更改 IP 工具。

请勿对任何节点的网格网络、管理网络或客户端网络使用包含以下 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，不要对任何节点的网格网络、管理网络或客户端网络使用以下子网范围：

- 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
- 198.51.100.0/24，因为此子网范围包含 IP 地址 198.51.100.2 和 198.51.100.4

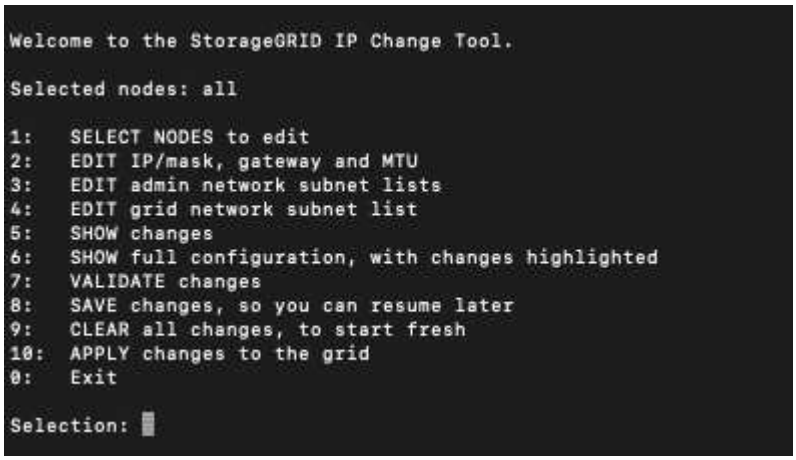
步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
3. 输入以下命令、启动更改IP工具： `change-ip`

4. 在提示符处输入配置密码短语。

   此时将显示主菜单。



5. 在主菜单上，选择用于编辑网格网络子网的选项（选项 * 4* ）。

   对网格网络子网列表所做的更改在网格范围内进行。

6. 选择以下选项之一：

   - 输入以下命令以添加子网： `add CIDR`
   - 输入以下命令以删除子网： `del CIDR`
   - 输入以下命令以设置子网列表： `set CIDR`

   对于所有命令、可以使用以下格式输入多个地址： `add CIDR, CIDR`

   示例： `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   您可以使用"向上箭头"将先前键入的值重新调用到当前输入提示符中、然后根据需要对其进行编辑、从而减少所需的键入量。

   以下示例输入显示了为网格网络子网列表设置子网：

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

7. 准备好后，输入 * 。 q* 可返回主菜单屏幕。您所做的更改将一直保留，直到清除或应用为止。
8. 选择以下选项之一：
   - 选择选项 * 5* 可显示输出中的编辑内容，而输出中的编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如以下示例输出所示：

```
================================================================================
Grid Network Subnet List (GNSL)
================================================================================
                                                    add 172.30.0.0/21
                                                    add 172.31.0.0/21
                                                    del 172.16.0.0/21
                                                    del 172.17.0.0/21
                                                    del 172.18.0.0/21
                                [      172.30.0.0/21 ]
                                [      172.31.0.0/21 ]
                                [    192.168.0.0/21 ]
Press Enter to continue
```

   - 选择选项 **6** 可在显示完整配置的输出中显示编辑内容。更改将以绿色（添加项）或红色（删除项）突出显示。

     某些命令行界面可能会使用删除线格式显示添加和删除。

9. 选择选项 * 7* 以验证所有暂存更改。

   此验证可确保遵循网格网络，管理网络和客户端网络的规则，例如使用重叠的子网。

10. （可选）选择选项 * 8* 保存所有分阶段更改，稍后返回以继续进行更改。

    使用此选项，您可以退出更改 IP 工具并稍后重新启动它，而不会丢失任何未应用的更改。

11. 执行以下操作之一：
    - 如果要在不保存或应用新网络配置的情况下清除所有更改，请选择选项 * 。
    - 如果您已准备好应用更改并配置新的网络配置，请选择选项 * 。配置期间、输出将显示已应用更新的状态、如以下示例输出所示：

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. 如果在更改网格网络时选择了选项 * 。 10 ，请选择以下选项之一：

    - * 应用 * ： 立即应用更改，并在必要时自动重新启动每个节点。

      如果新网络配置将与旧网络配置同时运行而不进行任何外部更改，则可以使用 * 应用 * 选项进行完全自动化的配置更改。

    - * 阶段 * ： 下次重新启动节点时应用更改。

      如果要使新网络配置正常运行，需要更改物理或虚拟网络配置，则必须使用 * 阶段 * 选项，关闭受影响的节点，进行必要的物理网络更改并重新启动受影响的节点。

      如果使用*stag*选项，请在暂存后尽快重新启动节点，以最大限度地减少中断。

    - **CANCEL**：目前请勿更改任何网络。

      如果您不知道建议的更改需要重新启动节点，则可以推迟更改以最大限度地减少对用户的影响。选择 * 取消 * 将返回到主菜单并保留所做的更改，以便稍后应用。

    应用或阶段更改后，将根据网格配置更改生成新的恢复包。

13. 如果配置因错误而停止，则可以使用以下选项：

    - 要终止IP更改操作步骤 并返回主菜单，请输入*A*。
    - 要重试失败的操作，请输入 * 。
    - 要继续执行下一个操作，请输入 * c* 。

      稍后可以从主菜单中选择选项 * 10 * （应用更改）重试失败的操作。只有成功完成所有操作后， IP 更改操作步骤 才会完成。

    - 如果您必须手动干预（例如重新启动节点），并确信工具认为失败的操作已实际成功完成，请输入 * f* 将其标记为成功并移至下一操作。

14. 从网格管理器下载新的恢复包。

    a. 选择*维护* > 系统 > 恢复包。

    b. 输入配置密码短语。

    恢复包文件必须是安全的，因为它包含可用于从StorageGRID系统获取数据的加密密钥和密码。

15. 如果您允许外部 SSH 访问，"阻止访问"当您完成添加或更改子网列表后。

更改 **StorageGRID** 网格中所有节点的 **IP** 地址

如果需要更改网格中所有节点的网格网络 IP 地址，则必须遵循此专用操作步骤 。您不能使用操作步骤 更改网格范围的网格网络IP以更改各个节点。

开始之前

- 您已获得 `Passwords.txt`文件。

要确保网格成功启动、必须同时进行所有更改。

> 此 操作步骤 适用场景 仅适用于网格网络。您不能使用此操作步骤 更改管理或客户端网络上的IP地址。

如果您只想更改一个站点上节点的IP地址和MTU、请按照说明进行操作"更改节点网络配置"。

步骤

1. 提前规划需要在更改 IP 工具之外进行的更改，例如更改 DNS 或 NTP 以及更改单点登录（ Single Sign-On ， SSO ）配置（如果使用）。

   > 如果现有 NTP 服务器无法通过新 IP 地址访问网格，请在执行 change-IP 操作步骤 之前添加新的 NTP 服务器。

   > 如果现有 DNS 服务器无法通过新 IP 地址访问网格，请在执行 change-IP 操作步骤 之前添加新的 DNS 服务器。

   > 如果您的 StorageGRID 系统启用了 SSO，并且使用管理节点 IP 地址（而不是建议的完全限定域名）配置了任何依赖方信任，请准备好在更改 IP 地址后立即更新或重新配置 Active Directory Federation Services (AD FS) 中的这些依赖方信任。请参阅使用 "OIDC" 或 "SAML" 设置 SSO。

   > 如有必要，请为新 IP 地址添加新子网。

2. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
3. 登录到主管理节点：

   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

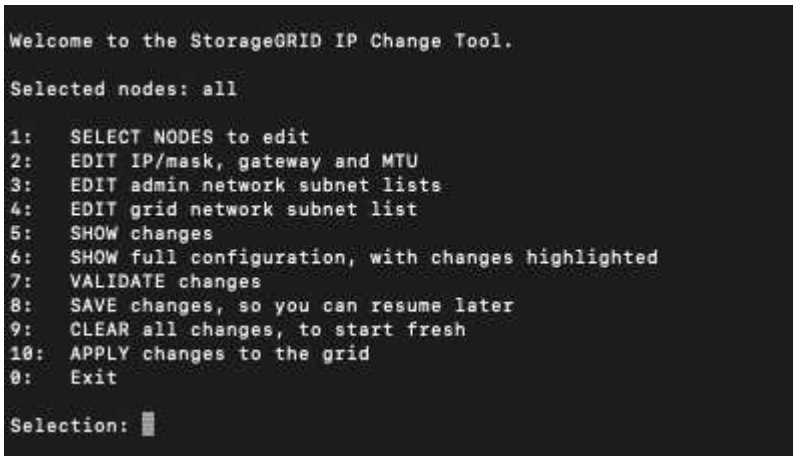
   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

4. 输入以下命令、启动更改IP工具： `change-ip`
5. 在提示符处输入配置密码短语。

   此时将显示主菜单。默认情况下，该 `Selected nodes`字段设置为 `all`。



6. 在主菜单上，选择 * 。 2* 以编辑所有节点的 IP/ 子网掩码，网关和 MTU 信息。

   a. 选择 * 1 * 以更改网格网络。

      选择后，提示符将显示节点名称，网格网络名称，数据类型（ IP/ 掩码，网关或 MTU ）， 和当前值。

      编辑 DHCP 配置接口的 IP 地址，前缀长度，网关或 MTU 将使接口更改为静态。在 DHCP 配置每个接口之前，系统会显示一条警告。

   无法编辑配置为的接口 `fixed`。

   a. 要设置新值，请按当前值所示格式输入该值。

   b. 编辑要更改的所有节点后，输入 * 。 q* 返回主菜单。

      您所做的更改将一直保留，直到清除或应用为止。

7. 选择以下选项之一，查看您所做的更改：

   ◦ * 5* ：显示输出中的编辑内容，这些编辑内容是孤立的，仅显示更改后的项。所做的更改以绿色（添加项）或红色（删除项）突出显示，如示例输出所示：

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

- * 6 *： 显示输出中显示的编辑内容，其中显示了完整配置。更改将以绿色（添加项）或红色（删除项）突出显示。

> 某些命令行界面可能会使用删除线格式显示添加和删除。正确显示取决于您的终端客户端是否支持必要的 VT100 转义序列。

8. 选择选项 * 7* 以验证所有更改。

   此验证可确保不违反网格网络的规则、例如不使用重叠子网。

   在此示例中，验证返回错误。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   在此示例中，验证已通过。

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

9. 验证通过后，选择*10*以应用新的网络配置。
10. 选择 * 阶段 * ，以便在下次重新启动节点时应用更改。

    必须选择 * 阶段 * 。请勿手动或通过选择*Apply*而不是*stage *来执行滚动重新启动；网格将无法成功启动。

11. 完成更改后，选择 * 。 0* 退出更改 IP 工具。
12. 同时关闭所有节点。

    必须关闭整个网格、以使所有节点同时关闭。

13. 根据需要进行物理或虚拟网络更改。
14. 验证所有网格节点是否均已关闭。
15. 打开所有节点的电源。
16. 网格成功启动后：
    a. 如果添加了新的 NTP 服务器，请删除旧的 NTP 服务器值。
    b. 如果添加了新的 DNS 服务器，请删除旧的 DNS 服务器值。
17. 从网格管理器下载新的恢复包。
    a. 选择*维护* > 系统 > 恢复包。
    b. 输入配置密码短语。
18. 如果您允许外部 SSH 访问，"阻止访问"当您完成更改 IP 地址后。

相关信息

- "在网格网络上添加或更改子网列表"
- "关闭网格节点"

向现有节点添加接口

向 **StorageGRID** 中的 **Linux** 节点添加管理员或客户端接口

按照以下步骤将管理网络或客户端网络上的接口添加到安装后的 Linux 节点中。

如果在安装期间未在 Linux 主机上的节点配置文件中配置 ADMIN_NETWORK_TARGET 或 CLIENT_NETWORK_TARGET，请使用此过程添加接口。有关节点配置文件的更多信息，请参阅"在基于软件的节点上安装StorageGRID"。

您可以在托管需要新网络分配的节点的 Linux 服务器上执行此操作步骤 ，而不是在节点内部执行。此操作步骤仅会将接口添加到节点；如果您尝试指定任何其他网络参数，则会发生验证错误。

要提供地址信息，必须使用更改 IP 工具。请参阅。 "更改节点网络配置"

步骤

1. 登录到托管此节点的 Linux 服务器。

2. 编辑节点配置文件： `/etc/storagegrid/nodes/node-name.conf`。

   请勿指定任何其他网络参数、否则会出现验证错误。

   a. 为新网络目标添加一个条目。例如：

      ```
      CLIENT_NETWORK_TARGET = bond0.3206
      ```

   b. 可选：为 MAC 地址添加一个条目。例如：

      ```
      CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
      ```

3. 运行 node validate 命令：

   ```
   sudo storagegrid node validate node-name
   ```

4. 解决所有验证错误。
5. 运行 node reload 命令：

   ```
   sudo storagegrid node reload node-name
   ```

向 **StorageGRID** 中的 **Linux** 节点添加中继或访问接口

安装 Linux 节点后，您可以向该节点添加额外的中继或访问接口。添加的接口将显示在 VLAN 接口页面和 HA 组页面上。

开始之前

- 您可以访问"StorageGRID安装说明"在您的 Linux 平台上。
- 您已获得 `Passwords.txt`文件。
- 您拥有 "特定访问权限"。

在软件升级、恢复操作步骤 或扩展操作步骤 处于活动状态时、请勿尝试向节点添加接口。

关于此任务

安装完 Linux 节点后，请按照以下步骤向该节点添加一个或多个额外的接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口、则可以将该接口直接添加到HA组；无需配置VLAN接口。

添加接口时，节点暂时不可用。您应一次在一个节点上执行此操作步骤 。

步骤

1. 登录到托管此节点的 Linux 服务器。
2. 使用 vim 或 pico 等文本编辑器编辑节点配置文件：

```
/etc/storagegrid/nodes/node-name.conf
```

3. 向文件中添加一个条目，以指定要添加到节点的每个额外接口的名称以及问题描述 （可选）。请使用此格式。

   ```
   INTERFACE_TARGET_nnnn=value
   ```

   对于_nnnn_、请为要添加的每个条目指定一个唯一编号 `INTERFACE_TARGET`。

   对于 *value* ，指定裸机主机上物理接口的名称。然后，也可以添加一个逗号并提供接口的问题描述 ，该接口将显示在 "VLAN interfaces" 页面和 "HA Groups" 页面上。

   例如：

   ```
   INTERFACE_TARGET_0001=ens256, Trunk
   ```

   > 请勿指定任何其他网络参数、否则会出现验证错误。

4. 运行以下命令以验证对节点配置文件所做的更改：

   ```
   sudo storagegrid node validate node-name
   ```

   解决所有错误或警告，然后再继续下一步。

5. 运行以下命令以更新节点的配置：

   ```
   sudo storagegrid node reload node-name
   ```

完成后

- 如果添加了一个或多个中继接口、请转到"配置 VLAN 接口"为每个新的父接口配置一个或多个VLAN接口。
- 如果添加了一个或多个访问接口、请转到"配置高可用性组"、将新接口直接添加到HA组。

向 **StorageGRID** 中的 **VMware** 节点添加中继或访问接口

您可以在安装 VM 节点后向该节点添加中继或访问接口。添加的接口将显示在 VLAN 接口页面和 HA 组页面上。

开始之前

- 您可以访问以下说明"在VMware平台上安装StorageGRID"。
- 您拥有管理节点和网关节点 VMware 虚拟机。
- 您的网络子网未用作网格、管理员或客户端网络。
- 您已获得 `Passwords.txt`文件。
- 您拥有 "特定访问权限"。

> 在软件升级、恢复操作步骤 或扩展操作步骤 处于活动状态时、请勿尝试向节点添加接口。

关于此任务

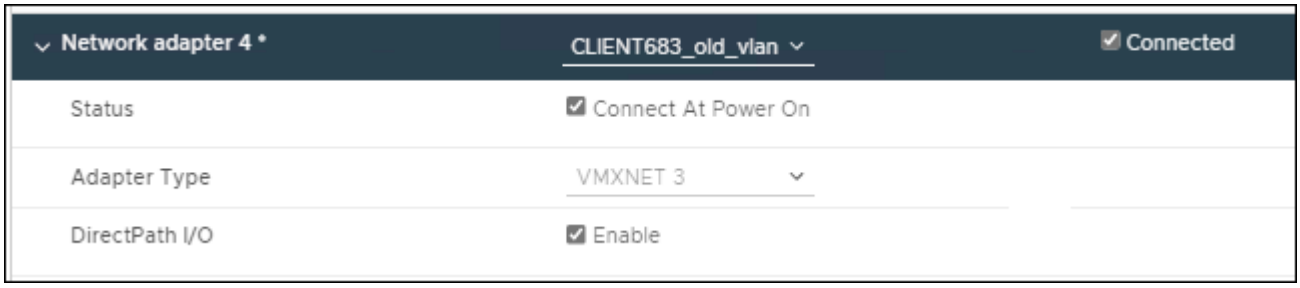
安装 VMware 节点后，请按照以下步骤向该节点添加一个或多个额外接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 VLAN 接口隔离属于不同应用程序或租户的流量。或者，您可能希望添加一个访问接口以在高可用性（ HA ）组中使用。

如果添加中继接口，则必须在 StorageGRID 中配置 VLAN 接口。如果添加访问接口、则可以将该接口直接添加到HA组；无需配置VLAN接口。

添加接口时，节点可能会暂时不可用。

步骤

1. 在 vCenter 中，向管理节点和网关节点虚拟机添加新的网络适配器（类型为 VMXNET3 ）。选中*已连接*和*开机时连接*复选框。



2. 使用 SSH 登录到管理节点或网关节点。
3. `ip link show`用于确认检测到新的网络接口ens256。

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

完成后

- 如果添加了一个或多个中继接口、请转到"配置 VLAN 接口"为每个新的父接口配置一个或多个VLAN接口。
- 如果添加了一个或多个访问接口、请转到"配置高可用性组"、将新接口直接添加到HA组。

在 StorageGRID 中配置 DNS 服务器

您可以添加、更新和删除DNS服务器、以便可以使用完全限定域名(FQDN)主机名、而不是IP地址。

要在为外部目标指定主机名时使用完全限定域名(FQDN)而不是IP地址、请指定要使用的每个DNS服务器的IP地址。这些条目用于AutoSupport 、警报电子邮件、SNMP通知、平台服务端点、云存储池、 等等。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您有要配置的DNS服务器的IP地址。

关于此任务

要确保正常运行、请指定两个或三个DNS服务器。如果指定的值超过三个、则可能仅使用三个、因为某些平台上存在已知的操作系统限制。如果您的环境存在路由限制、则各个节点(通常是站点上的所有节点)可以"自定义DNS服务器列表"使用一组不同的DNS服务器、最多可使用三个。

如果可能、请使用每个站点可以在本地访问的DNS服务器、以确保受支持的站点可以解析外部目标的FQDN。

添加**DNS**服务器

按照以下步骤添加DNS服务器。

步骤

1. 选择*维护* > 网络 > **DNS** 服务器。
2. 选择*添加另一台服务器*以添加DNS服务器。
3. 选择 * 保存 * 。

修改**DNS**服务器

按照以下步骤修改DNS服务器。

步骤

1. 选择*维护* > 网络 > **DNS** 服务器。
2. 选择要编辑的服务器名称的IP地址并进行必要的更改。
3. 选择 * 保存 * 。

删除**DNS**服务器

按照以下步骤删除DNS服务器的IP地址。

步骤

1. 选择*维护* > 网络 > **DNS** 服务器。
2. 选择 IP 地址旁边的删除图标 ✕。
3. 选择 * 保存 * 。

修改单个 **StorageGRID** 节点的 **DNS** 配置

您可以运行一个脚本来为每个网格节点配置不同的DNS、而不是为整个部署全局配置DNS。

一般来说，您应该使用网格管理器上的 维护 > 网络 > **DNS** 服务器 选项来配置 DNS 服务器。仅当您需要为不同的网格节点使用不同的 DNS 服务器时才使用以下脚本。

步骤

1. 默认情况下，外部 SSH 访问是被阻止的。如果需要，"暂时允许访问" 。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

   e. 将 SSH 专用密钥添加到 SSH 代理。输入： `ssh-add`
   f. 输入文件中列出的SSH访问密码 `Passwords.txt`。
3. 登录到要使用自定义DNS配置更新的节点： `ssh node_IP_address`
4. 运行DNS设置脚本： `setup_resolv.rb`.

   此脚本将以支持的命令列表进行响应。

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

5. 添加为您的网络提供域名服务的服务器的IPv4地址： `add <nameserver IP_address>`
6. 重复此 `add nameserver`命令以添加名称服务器。
7. 按照提示输入其他命令时的说明进行操作。
8. 保存更改并退出应用程序： `save`
9. 关闭服务器上的命令shell： `exit`
10. 对于每个网格节点，重复执行到中的步骤登录到节点关闭命令 Shell。
11. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入： `ssh-add -D`

12. 如果您允许外部 SSH 访问，"阻止访问"当您完成修改 DNS 配置后。

管理 StorageGRID 中的 NTP 服务器

您可以添加、更新或删除网络时间协议(NTP)服务器、以确保StorageGRID 系统中网格节点之间的数据准确同步。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您有要配置的NTP服务器的IPv4地址。

StorageGRID 如何使用NTP

StorageGRID 系统使用网络时间协议(NTP)同步网格中所有网格节点之间的时间。

在每个站点上，至少会为 StorageGRID 系统中的两个节点分配主 NTP 角色。它们会同步到建议的至少四个外部时间源，最多六个外部时间源以及彼此之间。StorageGRID 系统中不是主 NTP 节点的每个节点都充当 NTP 客户端，并与这些主 NTP 节点同步。

外部NTP服务器会连接到先前已分配主要NTP角色的节点。因此、建议至少指定两个具有主NTP角色的节点。

NTP服务器准则

请遵循以下准则以防止出现计时问题：

- 外部NTP服务器会连接到先前已分配主要NTP角色的节点。因此、建议至少指定两个具有主NTP角色的节点。
- 确保每个站点上至少有两个节点可以访问至少四个外部NTP源。如果一个站点上只有一个节点可以访问 NTP 源，则在该节点关闭时会发生计时问题。此外，指定每个站点两个节点作为主要 NTP 源可确保在站点与网格其余部分隔离时的时间准确无误。
- 指定的外部 NTP 服务器必须使用 NTP 协议。您必须指定 Stratum 3 或更高的 NTP 服务器引用，以防止出现时间偏差问题。

> 为生产级 StorageGRID 安装指定外部 NTP 源时，请勿在 Windows Server 2016 之前的 Windows 版本上使用 Windows Time (W32Time) 服务。早期版本的 Windows 上的时间服务不够准确，Microsoft 不支持在高精度环境中使用，包括 StorageGRID。有关详细信息，请参见 "高精度时间的支持边界"。

配置 NTP 服务器

按照以下步骤添加、更新或删除NTP服务器。

步骤

1. 选择*维护* > 网络 > NTP 服务器。
2. 在服务器部分中、根据需要添加、更新或删除NTP服务器条目。

应至少包含四个NTP服务器、并且最多可以指定六个服务器。

3. 输入StorageGRID 系统的配置密码短语，然后选择*Save*。

   在配置更新完成之前，此页面将处于禁用状态。

   如果在保存新NTP服务器后所有NTP服务器的连接测试均失败、请勿继续。请联系技术支持。

解决**NTP**服务器问题

如果您遇到安装期间最初指定的 NTP 服务器的稳定性或可用性问题，可以通过添加其他服务器或更新或删除现有服务器来更新 StorageGRID 系统使用的外部 NTP 源列表。

为隔离的 **StorageGRID** 节点恢复网络连接

在某些情况下、一组或多组节点可能无法访问网格的其余部分。例如、站点范围或网格范围的IP地址更改可能导致节点彼此隔离。

关于此任务

节点隔离通过以下方式表示：

- 警报，例如*无法与节点*通信(警报>*当前*)
- 与连接相关的诊断（支持 > 工具 > 诊断）

隔离节点会产生以下后果：

- 如果隔离了多个节点，您可能无法登录或访问网格管理器。
- 如果隔离多个节点、则租户管理器信息板上显示的存储使用情况和配额值可能已过时。恢复网络连接后，总数将更新。

要解决隔离问题描述 ，您可以在与网格隔离的每个隔离节点或组中的一个节点（子网中不包含主管理节点的所有节点）上运行命令行实用程序。该实用程序可为节点提供网格中非隔离节点的 IP 地址，从而使隔离的节点或节点组能够再次访问整个网格。

如果在网络中禁用了多播域名系统(mDNS)、则可能需要在每个隔离的节点上运行命令行实用程序。

步骤

只有部分服务脱机或报告通信错误时、此过程不适用。

1. 访问节点并检查 `/var/local/log/dynip.log`隔离消息。

   例如：

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action might be required.
```

如果您使用的是 VMware 控制台，则它将包含一条消息，指出此节点可能已隔离。

在Linux部署中、隔离消息会显示在文件中 `/var/log/storagegrid/node/<nodename>.log`。

2. 如果隔离消息重复出现且持久，请运行以下命令：

   `add_node_ip.py <address>`

   其中 `<address>`是连接到网格的远程节点的IP地址。

```
# /usr/sbin/add_node_ip.py  10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. 验证先前隔离的每个节点的以下情况：
   - 节点的服务已启动。
   - 运行命令后、动态IP服务的状态为"正在运行" `storagegrid-status`。
   - 在节点页面上、节点不再显示为与网格的其余部分断开连接。

如果运行 `add_node_ip.py`命令无法解决问题、则可能还需要解决其他网络问题。

主机和中间件过程

将 StorageGRID 节点迁移到新的 Linux 主机

您可以将一个或多个StorageGRID 节点从一个Linux主机(*ssource host*)迁移到另一个Linux主机(*ttarget host*)、以便在不影响网格功能或可用性的情况下执行主机维护。

例如、您可能希望迁移节点以执行操作系统修补和重新启动。

开始之前

- 您计划将StorageGRID部署包括迁移支持。看"节点容器迁移要求" 。
- 目标主机已准备好供StorageGRID 使用。
- 共享存储用于所有每个节点的存储卷
- 网络接口在主机之间具有一致的名称。

在生产部署中、请勿在一个主机上运行多个存储节点。为每个存储节点使用专用主机可提供一个隔离的故障域。

可以在同一主机上部署其他类型的节点，例如管理节点或网关节点。但是、如果有多个类型相同的节点(例如两个网关节点)、请勿在同一主机上安装所有实例。

从源主机导出节点

首先、关闭网格节点并将其从源Linux主机导出。

在_ssource host_上运行以下命令。

步骤

1. 获取源主机上当前正在运行的所有节点的状态。

   ```
   sudo storagegrid node status all
   ```

   示例输出：

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. 确定要迁移的节点的名称、如果其运行状态为running、请将其停止。

   ```
   sudo storagegrid node stop DC1-S3
   ```

   示例输出：

   ```
   Stopping node DC1-S3
   Waiting up to 630 seconds for node shutdown
   ```

3. 从源主机导出节点。

   ```
   sudo storagegrid node export DC1-S3
   ```

   示例输出：

   ```
   Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
   Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
   want to import it again.
   ```

4. 记下 `import`输出中建议的命令。

   您将在下一步的目标主机上运行此命令。

在目标主机上导入节点

从源主机导出节点后、您可以导入目标主机上的节点并对其进行验证。验证可确认节点可以访问与源主机上相同的块存储和网络接口设备。

在_ttarget host_上运行以下命令。

步骤

1. 在目标主机上导入节点。

   ```
   sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
   ```

   示例输出：

   ```
   Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
   You should run 'storagegrid node validate DC1-S3'
   ```

2. 验证新主机上的节点配置。

   ```
   sudo storagegrid node validate DC1-S3
   ```

   示例输出：

   ```
   Confirming existence of node DC1-S3... PASSED
   Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
   DC1-S3... PASSED
   Checking for duplication of unique values... PASSED
   ```

3. 如果发生任何验证错误，请在启动迁移的节点之前解决这些错误。

   有关故障排除信息，请参阅StorageGRID"安装说明"适用于您的 Linux 操作系统。

启动迁移的节点

验证迁移的节点后、您可以通过在_target host_上运行命令来启动该节点。

步骤

1. 在新主机上启动节点。

   ```
   sudo storagegrid node start DC1-S3
   ```

2. 登录到网格管理器并验证节点的状态是否为绿色且无警报。

验证节点的状态是否为绿色可确保已迁移的节点已完全重新启动并重新加入网格。如果此状态不是绿色、请勿迁移任何其他节点、以免有多个节点停止服务。

3. 如果无法访问网格管理器，请等待 10 分钟，然后运行以下命令：

   ```
   sudo storagegrid node status _node-name
   ```

   确认迁移的节点的"运行状态"为"正在运行"。

在 **StorageGRID** 中配置 **VMware** 虚拟机自动重启

如果在重新启动 VMware vSphere 虚拟机管理程序后虚拟机未重新启动，则可能需要对虚拟机进行配置，使其自动重新启动。

如果在恢复网格节点或执行其他维护操作步骤 期间发现虚拟机未重新启动，则应执行此操作步骤 。

步骤

1. 在 VMware vSphere Client 树中，选择未启动的虚拟机。
2. 右键单击虚拟机，然后选择 * 启动 * 。
3. 配置 VMware vSphere 虚拟机管理程序，以便将来自动重新启动虚拟机。

恢复或更换节点

StorageGRID 节点恢复的警告和注意事项

如果网格节点发生故障，您必须尽快恢复。开始之前，您必须查看节点恢复的所有警告和注意事项。

StorageGRID 是一个分布式系统，由多个节点组成，这些节点彼此协同工作。请勿使用磁盘快照还原网格节点。请参阅每种类型节点的恢复和维护过程。

如果整个StorageGRID站点出现故障，请联系技术支持。技术支持将与您合作制定并执行站点恢复计划，以最大限度地恢复数据量并满足您的业务目标。请参阅"技术支持如何恢复站点" 。

尽快恢复出现故障的网格节点的一些原因包括：

- 出现故障的网格节点可以减少系统和对象数据的冗余，因此，如果另一个节点发生故障，您容易受到永久数据丢失的风险。
- 网格节点发生故障可能会影响日常操作的效率。
- 出现故障的网格节点可能会降低您监控系统操作的能力。
- 如果存在严格的 ILM 规则，则出现故障的网格节点可能会发生原因 a 500 internal server error 。
- 如果未及时恢复网格节点，则恢复时间可能会增加。例如，可能会出现需要在恢复完成之前清除的队列。

对于要恢复的特定网格节点类型，请始终遵循恢复操作步骤 。主管理节点、网关节点、设备节点和存储节点的恢复过程因主管理节点或非主管理节点而异。

恢复网格节点的前提条件

恢复网格节点时，系统会假设以下所有条件：

- 已更换并配置发生故障的物理或虚拟硬件。
- 替代设备上的StorageGRID设备安装程序版本与StorageGRID系统的软件版本相匹配，如中所述 "验证并升级 StorageGRID 设备安装程序版本"。
- 如果要恢复主管理节点以外的网格节点，则必须在要恢复的网格节点和管理恢复过程的管理节点之间存在连接。
- 如果要恢复设备存储节点，则必须在设备安装期间指定与原始设备相同的存储类型（组合、仅元数据或仅数据）。如果指定不同的存储类型，恢复将失败，并且需要使用指定的正确存储类型重新安装设备。

托管多个网格节点的服务器发生故障时的节点恢复顺序

如果托管多个网格节点的服务器发生故障，则可以按任何顺序恢复节点。但是，如果发生故障的服务器托管主管理节点，并且不存在非主管理节点，则必须首先恢复主管理节点。

已恢复节点的 IP 地址

请勿尝试使用当前分配给任何其他节点的IP地址恢复节点。部署新节点时，请使用故障节点的当前 IP 地址或未使用的 IP 地址。

如果您使用新 IP 地址部署新节点，然后恢复该节点，则新 IP 地址将继续用于已恢复的节点。如果要还原到原始 IP 地址，请在恢复完成后使用更改 IP 工具。

收集 StorageGRID 网格节点恢复所需的材料

在执行维护过程之前，您必须确保具有必要的材料来恢复出现故障的网格节点。

项目	备注
StorageGRID 安装归档	如果需要恢复网格节点、则需要为您的平台恢复下载 StorageGRID 安装文件。 *注意：*如果要恢复存储节点上发生故障的存储卷、则无需下载文件。
服务笔记本电脑	服务笔记本电脑必须具有以下组件： • 网络端口 • SSH 客户端（例如 PuTTY ） • "支持的 Web 浏览器"
恢复包 `.zip`文件	获取最新恢复包的副本 `.zip`文件： `sgws-recovery-package-*id-revision*.zip` 的内容 `.zip`每次修改系统时都会更新文件。进行此类更改后，您需要将最新版本的恢复包存储在安全的位置。使用最新的副本来恢复电网故障。 登录到任何管理节点后，使用网格管理器下载恢复包。选择*维护* > 系统 > 恢复包。 如果您无法访问网格管理器，您可以在包含 ADC 服务的某些存储节点上找到恢复包的加密副本。在每个存储节点上，检查恢复包的此位置：`/var/local/install/sgws-recovery-package-*grid-id-revision*.zip.gpg`使用修订号最高的恢复包。
`Passwords.txt`文件	包含在命令行上访问网格节点所需的密码。包含在恢复包中。
配置密码短语	首次安装 StorageGRID 系统时，系统会创建并记录密码短语。配置密码短语不在此文件中 `Passwords.txt`。
适用于您的平台的最新文档	请访问平台供应商的网站以获取相关文档。 有关当前支持的平台版本，请参见 "NetApp 互操作性表工具"。

下载并提取 StorageGRID 安装文件

下载软件并解压缩文件，除非您是"恢复存储节点上的故障存储卷"。

您必须使用网格上当前运行的 StorageGRID 版本。

步骤

1. 确定当前安装的软件版本。从网格管理器顶部，选择帮助图标并选择 * 关于 * 。
2. 转到。 "StorageGRID 的 "NetApp 下载 " 页面"
3. 选择网格上当前运行的 StorageGRID 版本。

   StorageGRID软件版本采用以下格式： `11.x.y`。

4. 使用您的 NetApp 帐户的用户名和密码登录。
5. 阅读最终用户许可协议，选中复选框，然后选择*接受并继续*。
6. 在下载页面的*安装StorageGRID *列中，选择 `.tgz`适用于您的平台的或 `.zip`文件。

   安装归档文件中显示的版本必须与当前安装的软件版本匹配。

   如果运行的是Windows、请使用 `.zip`文件。

平台	安装归档
RHEL	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu ， Debian 或设备	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip` `StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

7. 下载并提取归档文件。
8. 根据您的平台和需要恢复的网格节点，跳至适合您平台的部分来选择您需要的文件。

   步骤中为每个平台列出的路径与归档文件安装的顶级目录相对。

9. 如果你正在恢复"基于软件的节点"，选择相应的文件：

RHEL

路径和文件名	说明
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	RPM软件包、用于在RHEL主机上安装StorageGRID节点映像。
	RPM软件包、用于在RHEL主机上安装StorageGRID主机服务。
部署脚本工具	说明
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	用于为StorageGRID容器部署配置RHEL主机的AndsableRole和操作手册示例。您可以根据需要自定义角色或攻略手册。
	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。

路径和文件名	说明
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

Ubuntu 或 Debian

路径和文件名	说明
/debs/README	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	非生产 NetApp 许可证文件，可用于测试和概念验证部署。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 节点映像的 Deb 软件包。
	文件的MD5校验和 `/debs/storagegrid-webscale-images-version-SHA.deb`。
	用于在 Ubuntu 或 Debian 主机上安装 StorageGRID 主机服务的 Deb 软件包。
部署脚本工具	说明
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个示例 Python 脚本，启用单点登录后，您可以使用该脚本登录到网格管理 API 。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	用于脚本的空配置文件 `configure-storagegrid.py`。

路径和文件名	说明
	用于为 StorageGRID 容器部署配置 Ubuntu 或 Debian 主机的 Ansible 角色示例和攻略手册。您可以根据需要自定义角色或攻略手册。
storagegrid-ssoauth-azure.py	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

VMware

路径和文件名	说明
	一个文本文件，用于描述 StorageGRID 下载文件中包含的所有文件。
	一种免费许可证，不提供产品的任何支持授权。
	用作创建网格节点虚拟机的模板的虚拟机磁盘文件。
	(`.mf`用于部署主管理节点(`.ovf`的开放式虚拟化格式模板文件()和清单文件()。
	(`.mf`用于部署非主管理节点(`.ovf`的模板文件()和清单文件()。
	(`.mf`用于部署网关节点(`.ovf`的模板文件()和清单文件()。
	(`.mf`用于部署基于虚拟机的存储节点的模板(`.ovf`文件()和清单文件()。
部署脚本工具	说明

路径和文件名	说明
	Bash shell 脚本，用于自动部署虚拟网格节点。
	用于脚本的示例配置文件 `deploy-vsphere-ovftool.sh`。
	一种用于自动配置 StorageGRID 系统的 Python 脚本。
	一种用于自动配置 StorageGRID 设备的 Python 脚本。
	一个Python脚本示例、在启用单点登录(Single Sign On、SSO)后、您可以使用该脚本登录到网格管理API。您也可以使用此脚本进行Ping联盟集成。
	用于脚本的示例配置文件 `configure-storagegrid.py`。
	用于脚本的空配置文件 `configure-storagegrid.py`。
	一个Python脚本示例、在使用Active Directory或Ping联合启用单点登录(Single Sign On、SSO)时、您可以使用该脚本登录到网格管理API。
	由配套Python脚本调用的帮助程序 `storagegrid-ssoauth-azure.py`脚本、用于与Azure执行SSO交互。
	StorageGRID 的 API 架构。 注意：如果您没有用于升级兼容性测试的非生产StorageGRID 环境，则在执行升级之前，可以使用这些模式来确认为使用StorageGRID 管理API而编写的任何代码是否与新的StorageGRID 版本兼容。

10. 如果要恢复基于 StorageGRID 设备的系统，请选择相应的文件。

> 对于设备安装，仅当您需要避免网络流量时才需要这些文件。设备可以从您执行恢复过程的管理节点下载所需的文件。

路径和文件名	说明
	用于在设备上安装 StorageGRID 节点映像的 Deb 软件包。
	文件的MD5校验和 `/debs/storagegridwebscale-images-version-SHA.deb`。

选择 StorageGRID 节点恢复过程

为出现故障的节点类型选择正确的恢复过程。

网格节点	恢复操作步骤
存储节点	存储节点恢复流程取决于故障类型。 "从存储节点故障中恢复"
管理节点	管理节点操作步骤 取决于您是需要恢复主管理节点还是非主管理节点。 "从管理节点故障中恢复"
网关节点	"从网关节点故障中恢复"
归档节点	"从归档节点故障中恢复(StorageGRID 11.8文档站点)"

如果托管多个网格节点的服务器发生故障，则可以按任何顺序恢复节点。但是，如果发生故障的服务器托管主管理节点，并且不存在非主管理节点，则必须首先恢复主管理节点。首先恢复主管理节点可防止其他节点在尝试联系主管理节点时停止恢复。如果非主管理节点可用，您也可以使用它来恢复其他节点，以便这些恢复可以继续，而无需联系主管理节点。

从存储节点故障中恢复

从 StorageGRID 存储节点故障中恢复

用于恢复故障存储节点的操作步骤 取决于故障类型和故障存储节点的类型。

使用此表为出现故障的存储节点选择恢复操作步骤 。

问题描述	操作	备注
多个存储节点出现故障。	请联系技术支持。	如果多个存储节点发生故障，则技术支持必须协助恢复，以防止可能导致数据丢失的 Cassandra 数据库不一致。可能需要站点恢复程序。 技术支持可以确定何时可以安全地开始恢复第二个 Storage Node。 注意：如果站点上包含 ADC 服务的多个存储节点发生故障，则该站点的任何待处理平台服务请求都将丢失。
一个站点上的多个存储节点出现故障或整个站点出现故障。	请联系技术支持。可能需要执行站点恢复操作步骤。	技术支持将评估您的情况并制定恢复计划。请参阅。 "技术支持如何恢复站点"
设备存储节点出现故障。	"恢复设备存储节点"	对于所有故障，设备存储节点的恢复操作步骤 均相同。
一个或多个存储卷发生故障，但系统驱动器完好无损	"从系统驱动器完好无损的存储卷故障中恢复"	此操作步骤 用于基于软件的存储节点。
系统驱动器出现故障。	"从系统驱动器故障中恢复"	节点更换操作步骤 取决于部署平台以及是否有任何存储卷也出现故障。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到"reaper"或"cassandr修复"。如果您看到指示修复失败的错误消息、请运行错误消息中指示的命令。

恢复设备存储节点

恢复 **StorageGRID** 设备存储节点的警告

无论您是从系统驱动器丢失还是仅从存储卷丢失中恢复，用于恢复出现故障的 StorageGRID 设备存储节点的操作步骤 都是相同的。

如果多个存储节点出现故障（或离线），请联系技术支持。请勿执行以下恢复过程。可能会发生数据丢失。有关详细信息，请参阅"技术支持如何恢复站点" 。

如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

有关硬件维护过程(例如更换控制器或重新安装SANtricity OS的说明)，请参阅 "存储设备的维护说明"。

准备 **StorageGRID** 设备存储节点以重新安装

恢复设备存储节点时，必须先准备设备以重新安装 StorageGRID 软件。

步骤

1. 登录到发生故障的存储节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 准备设备存储节点以安装StorageGRID软件。 `sgareinstall`

3. 当系统提示您继续时、输入： `y`

   设备将重新启动， SSH 会话将结束。StorageGRID 设备安装程序通常需要大约 5 分钟才能投入使用，但在某些情况下，您可能需要等待长达 30 分钟。

   请勿尝试通过重启电源或以其他方式重置设备来加快重新启动速度。您可能会中断BIOS、BMC或其他固件自动升级。

   StorageGRID 设备存储节点已重置，并且无法再访问存储节点上的数据。在初始安装过程中配置的 IP 地址应保持不变；但是，建议您在操作步骤 完成后进行确认。

   执行命令后 `sgareinstall`、所有StorageGRID配置的帐户、密码和SSH密钥都会被删除、并生成新的主机密钥。

开始安装 **StorageGRID** 设备

要在设备存储节点上安装 StorageGRID ，请使用设备中提供的 StorageGRID 设备安装程序。

开始之前

- 此设备已安装在机架中，并已连接到您的网络并已启动。
- 已使用 StorageGRID 设备安装程序为此设备配置网络链路和 IP 地址。
- 您知道以下管理节点之一的IP地址：
  - StorageGRID 网格的主管理节点
  - 非主管理节点（如果有）
- StorageGRID 设备安装程序的 IP 配置页面上列出的所有网格网络子网均已在主管理节点上的网格网络子网列表中定义。

- 您已按照存储设备的安装说明完成这些前提任务。请参阅。 "硬件安装快速入门"
- 您正在使用"支持的 Web 浏览器"。
- 您知道分配给设备中计算控制器的一个 IP 地址。您可以使用管理网络（控制器上的管理端口 1 ），网格网络或客户端网络的 IP 地址。

关于此任务

要在设备存储节点上安装 StorageGRID ，请执行以下操作：

- 您可以指定主管理节点的 IP 地址。如果主管理节点不可用，则指定非主管理节点的 IP 地址（如果可用）。您还可以确认节点的主机名（系统名称）。
- 您开始安装，并等待卷配置完毕并安装软件。

> 恢复设备存储节点时，使用与原始设备相同的存储类型（组合、仅元数据或仅数据）重新安装它。如果指定不同的存储类型，恢复将失败，并且需要使用指定的正确存储类型重新安装设备。

- 在整个过程中，安装将暂停。要恢复安装，您必须登录到网格管理器，并将待定存储节点配置为故障节点的替代节点。
- 配置节点后，设备安装过程将完成，设备将重新启动。

步骤

1. 打开浏览器并输入设备中计算控制器的 IP 地址之一。

   `https://Controller_IP:8443`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

   假设主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上， StorageGRID 设备安装程序可以自动发现此 IP 地址。

3. 如果未显示此 IP 地址或您需要更改此 IP 地址，请指定地址：

选项	步骤
手动输入 IP	a. 清除*启用管理节点发现*复选框。 b. 手动输入 IP 地址。 注意：对于安装，请手动输入要用于安装节点的管理节点的 IP 地址。对于恢复，如果可用，请使用主管理节点的 IP；否则，使用非主管理节点的 IP。 a. 选择 * 保存 * 。 b. 等待新IP地址的连接状态变为"就绪"。

选项	步骤
自动发现所有已连接的主管理节点	a. 选中*启用管理节点发现*复选框。 b. 从发现的 IP 地址列表中，选择将部署此设备存储节点的网格的管理节点。 注意：对于恢复，如果可用，请使用主管理节点的 IP；否则，使用非主管理节点的 IP。 a. 选择 * 保存 * 。 b. 等待新IP地址的连接状态变为"就绪"。

4. 在*节点名称*字段中，输入用于正在恢复的节点的相同主机名（系统名称），然后选择*保存*。
5. 在安装部分，确认当前状态为"准备好开始将 `node name`安装到具有主管理节点 `admin_ip` 的网格中"，并且*开始安装*按钮已启用。

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

6. 从 StorageGRID 设备安装程序主页中，选择 开始安装。

   当前状态更改为"正在安装"，并显示监控安装页面。

   > 如果需要手动访问监视器安装页面，请从菜单栏中选择*监视器安装*。请参阅 "监控设备安装"。

监控 **StorageGRID** 设备安装

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

步骤

1. 要监控安装进度，请从菜单栏中选择*监控安装*。

   监视器安装页面显示安装进度。

   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保先前安装中完成的任务不会重新运行。如果要重新运行安装、则不需要重新运行的任何任务都会显示绿色状态栏和状态"已跳过"。

2. 查看前两个安装阶段的进度。
   - *1.配置存储 *

     在此阶段、安装程序会连接到存储控制器、清除任何现有配置、与SANtricity 操作系统通信以配置卷以及配置主机设置。

   - **2.**安装 **OS**

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

3. 继续监控安装进度，直到 * 安装 StorageGRID 网格管理器 * 阶段暂停，并且嵌入式控制台上显示一条消息，提示您使用网格管理器在管理节点上批准此节点。
4. 转到。 "选择 Start Recovery 以配置设备存储节点"

选择 **Start Recovery** 以配置 **StorageGRID** 设备存储节点

您必须在网格管理器中选择启动恢复，才能将设备存储节点配置为故障节点的替代节点。

开始之前

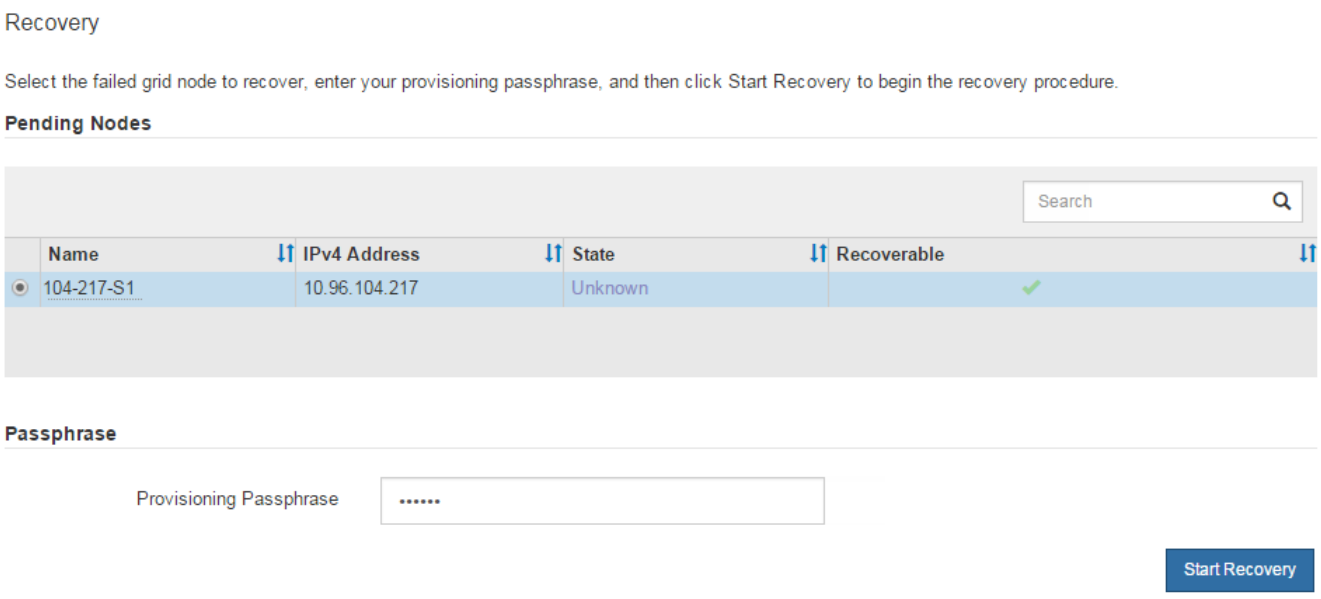
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您已部署恢复设备存储节点。
- 您知道已进行过数据检索的任何修复作业的开始日期。

步骤

1. 在网格管理器中，选择*Maintenance* > **Tasks** > **Node recovery**。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点发生故障后会显示在列表中、但您无法选择某个节点、直到它重新安装并准备好进行恢复为止。

3. 输入 **Provisioning passphrase**。
4. 选择*Start recovery*。



5. 在恢复网格节点表中监控恢复进度。
   - 如果网格节点达到"等待手动步骤"阶段，则必须 "手动重新挂载并重新格式化设备存储卷"。

- 如果未显示"等待手动步骤"消息，则表示存储卷已自动重新装载和重新格式化，您可以 "将对象数据还原至卷"。

> 在恢复过程中的任何时候，您都可以选择*重置*以开始新的恢复。将显示一个对话框，指示如果重置过程，节点将保持不确定状态。
>
> 如果要在重置过程后重试恢复、则必须在设备节点上运行以将该节点还原到预安装状态 `sgareinstall`。

重新挂载并重新格式化 **StorageGRID** 设备存储卷（手动步骤）

如果自动过程无法重新挂载保留的存储卷并重新格式化发生故障的存储卷，则必须手动运行两个脚本来完成这些操作。第一个脚本重新挂载已正确格式化为 StorageGRID 存储卷的卷。第二个脚本重新格式化所有未挂载的卷，如果需要，重建 Cassandra 数据库，然后启动服务。

在存储节点恢复期间，如果 Grid Manager 中出现"等待手动步骤"消息，请按照以下步骤重新挂载并重新格式化存储卷。如果您没有看到此消息，则重新挂载和重新格式化操作已自动完成，您可以跳过本过程并"还原对象数据"。

开始之前

- 您已更换已知需要更换的任何故障存储卷的硬件。

  运行此 `sn-remount-volumes`脚本可能有助于确定其他故障存储卷。

- 您已检查存储节点退役未正在进行，或者您已暂停节点退役过程。 （在网格管理器中，选择*维护* > 任务 > 退役。）
- 您已检查扩展是否尚未进行。 （在网格管理器中，选择*维护* > 任务 > 扩展。）

> 如果多个存储节点离线，请联系技术支持。不要运行 `sn-recovery-postinstall.sh`脚本。

关于此任务

要完成此操作步骤 ，请执行以下高级任务：

- 登录到已恢复的存储节点。
- 运行 `sn-remount-volumes`脚本以重新挂载格式正确的存储卷。运行此脚本时，它将执行以下操作：
  - 挂载和卸载每个存储卷以重放 XFS 日志。
  - 执行 XFS 文件一致性检查。
  - 如果文件系统一致，则确定存储卷是否为格式正确的 StorageGRID 存储卷。
  - 如果存储卷格式正确，请重新挂载该存储卷。卷上的所有现有数据保持不变。
- 查看脚本输出并解决任何问题。
- 运行 `sn-recovery-postinstall.sh`脚本。运行此脚本时，它将执行以下操作。

在运行(步骤4)以重新格式化故障存储卷和还原对象元数据之前、请勿在恢复期间重新启动存储节点 `sn-recovery-postinstall.sh`。在完成之前重新启动存储节点 `sn-recovery-postinstall.sh`会导致尝试启动的服务出现错误、并导致StorageGRID设备节点退出维护模式。

- 重新格式化脚本无法挂载或发现格式不正确的任何存储卷 `sn-remount-volumes`。

  如果重新格式化某个存储卷，则该卷上的所有数据都将丢失。假设已将 ILM 规则配置为存储多个对象副本，则必须执行额外的操作步骤 以从网格中的其他位置还原对象数据。

- 如果需要，在节点上重建 Cassandra 数据库。
- 启动存储节点上的服务。

步骤

1. 登录到已恢复的存储节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 运行第一个脚本重新挂载任何格式正确的存储卷。

   如果所有存储卷都是新的，需要进行格式化，或者所有存储卷都出现故障，您可以跳过此步骤并运行第二个脚本，重新格式化所有已卸载的存储卷。

   a. 运行脚本： `sn-remount-volumes`

      此脚本可能需要数小时才能在包含数据的存储卷上运行。

   b. 在脚本运行期间，查看输出并问题解答 任何提示。

      根据需要，您可以使用 `tail -f`命令监控脚本日志文件的内容 (/var/local/log/sn-remount-volumes.log`)。日志文件包含比命令行输出更详细的信息。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
```

```
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.
```

```
Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

在示例输出中，一个存储卷已成功重新挂载，三个存储卷出现错误。

- `/dev/sdb`已通过XFS文件系统一致性检查并具有有效的卷结构、因此已成功重新挂载。此脚本重新挂载的设备上的数据将保留下来。
- `/dev/sdc`未通过XFS文件系统一致性检查、因为存储卷是新的或已损坏。
- `/dev/sdd`无法挂载、因为磁盘未初始化或磁盘的超块已损坏。当脚本无法挂载存储卷时、它会询问您是否要运行文件系统一致性检查。
  - 如果存储卷已连接到新磁盘，请将 * N * 问题解答 到提示符处。您不需要检查新磁盘上的文件系统。
  - 如果存储卷已连接到现有磁盘，问题解答 请将 * 。 *您可以使用文件系统检查的结果来确定损坏的来源。结果将保存在日志文件中 `/var/local/log/sn-remount-volumes.log`。
- `/dev/sde`已通过XFS文件系统一致性检查并具有有效的卷结构；但是、文件中的LDR节点ID `volID`与此存储节点的ID不匹配(`configured LDR noid`显示在顶部)。此消息表示此卷属于另一个存储节点。

3. 查看脚本输出并解决任何问题。

> 如果存储卷未通过 XFS 文件系统一致性检查或无法挂载，请仔细查看输出中的错误消息。您必须了解在这些卷上运行此脚本的含义 `sn-recovery-postinstall.sh`。

a. 检查以确保结果中包含所需所有卷的条目。如果未列出任何卷、请重新运行此脚本。

b. 查看所有已挂载设备的消息。确保没有指示存储卷不属于此存储节点的错误。

在此示例中， /dev/sde 的输出包含以下错误消息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

如果报告某个存储卷属于另一个存储节点，请联系技术支持。如果运行此 `sn-recovery-postinstall.sh`脚本、则存储卷将被重新格式化、从而可能导致数据丢失。

c. 如果无法挂载任何存储设备，请记下此设备的名称，然后修复或更换此设备。

您必须修复或更换任何无法挂载的存储设备。

d. 修复或更换所有无法挂载的设备后、再次运行 `sn-remount-volumes`脚本、以确认可以重新挂载的所有存储卷均已重新挂载。

如果某个存储卷无法挂载或格式不正确、则在继续下一步后、该卷以及该卷上的任何数据将被删除。如果对象数据有两个副本，则只有一个副本，直到完成下一个操作步骤 （还原对象数据）为止。

如果您认为无法从网格中的其他位置重建故障存储卷上剩余的数据(例如、如果您的ILM策略使用的规则仅创建一个副本、或者卷在多个节点上发生故障)、请勿运行此 `sn-recovery-postinstall.sh`脚本。请联系技术支持以确定如何恢复数据。

4. 运行 `sn-recovery-postinstall.sh`脚本： `sn-recovery-postinstall.sh`

此脚本将重新格式化无法挂载或格式不正确的任何存储卷；根据需要在节点上重建 Cassandra 数据库；并启动存储节点上的服务。

请注意以下事项：

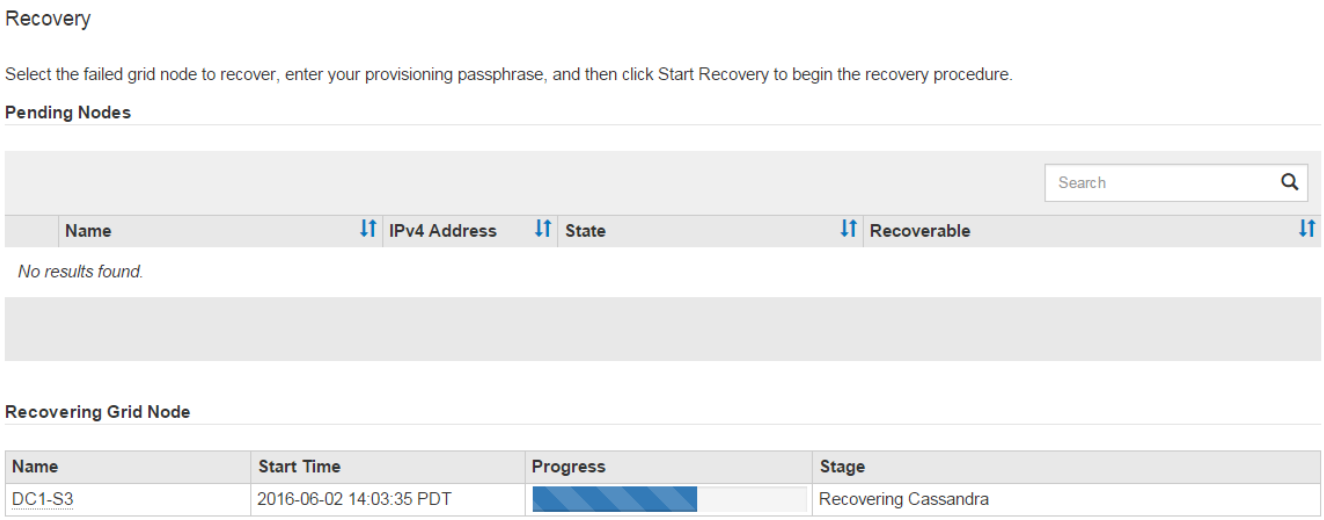
- 此脚本可能需要数小时才能运行。
- 通常，在脚本运行期间，您应单独保留 SSH 会话。
- 在SSH会话处于活动状态时，请勿按*Ctrl+C*。
- 如果发生网络中断并终止 SSH 会话，则此脚本将在后台运行，但您可以从 " 恢复 " 页面查看进度。
- 如果存储节点使用 RSM 服务，则随着节点服务重新启动，脚本可能会暂停 5 分钟。每当 RSM 服务首次启动时，预计会有 5 分钟的延迟。

RSM 服务位于包含此 ADC 服务的存储节点上。

某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到"reaper"或"cassandr修复"。如果您看到指示修复失败的错误消息、请运行错误消息中指示的命令。

5. 运行该脚本时 `sn-recovery-postinstall.sh`、请监控网格管理器中的"Recrecovery (恢复)"页面。

恢复页面上的进度栏和阶段列提供了该脚本的简要状态 `sn-recovery-postinstall.sh`。



6. 脚本在节点上启动服务后 `sn-recovery-postinstall.sh`、您可以将对象数据还原到由脚本格式化的任何存储卷。

   该脚本询问您是否要使用 Grid Manager 卷还原过程来还原对象数据。

   - 在大多数情况下，您应该"使用网格管理器还原对象数据"。答案 `y`以使用 Grid Manager。
   - 在极少数情况下，例如当您知道替换节点可用于对象存储的卷少于原始节点时，请联系技术支持以手动还原对象数据。如果其中一种情况适用，请回答 `n`并按任意键返回命令行。

将对象数据还原至 **StorageGRID** 设备的存储卷

在恢复设备存储节点的存储卷之后、您可以还原在存储节点发生故障时丢失的已复制或已删除编码的对象数据。

开始之前

- 如果自动过程未能重新挂载保留的存储卷并重新格式化发生故障的存储卷，则表示您已执行以下过程之一：
  - "重新挂载并重新格式化设备存储卷(手动步骤)"
  - "重新挂载和重新格式化存储卷(手动步骤)"
- 您已确认要还原对象的存储节点在网格管理器中的*节点* > 概览*选项卡上的连接状态为*已连接 。
- 您已确认以下事项：
  - 未进行网格扩展以添加存储节点。
  - 存储节点停用未在进行中或失败。
  - 故障存储卷的恢复未在进行中。
  - 具有故障系统驱动器的存储节点的恢复未在进行中。
  - EC 重新平衡作业未在进行中。
  - 设备节点克隆未在进行中。

关于此任务

更换驱动器并格式化卷后，Grid Manager 会在*维护* > 卷恢复 > *要恢复的节点*选项卡上将卷显示为要恢复的

候选卷。

请尽可能使用网格管理器中的卷还原页面还原对象数据。您可以在卷准备好进行还原时自动启动卷还原，也可以启用自动还原模式手动执行卷还原。请遵循以下准则：

- 如果卷在 维护 > 卷恢复 > 要恢复的节点 中列出，请按照以下步骤恢复对象数据。如果满足以下条件，则会列出卷：
  - 节点中的部分(而非全部)存储卷发生故障
  - 一个节点中的所有存储卷均发生故障、并正在替换为相同数量或更多卷

  网格管理器中的卷还原页面还可用于监控卷还原过程和查看还原历史记录。

  如果恢复的存储节点包含的卷少于要替换的节点，请联系技术支持以获得帮助。

您可以还原两种类型的对象数据：

- 复制的数据对象会从其他位置还原、前提是已将网格的ILM规则配置为使对象副本可用。
  - 如果将 ILM 规则配置为仅存储一个复制副本，并且该副本存在于出现故障的存储卷上，则无法恢复该对象。
  - 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。
- 纠删编码(纠删编码、EC)数据对象可通过重新组装存储的片段来还原。损坏或丢失的片段会通过纠删编码算法从其余数据和奇偶校验片段中重新创建。

  在某些存储节点脱机时，可以开始修复经过擦除编码的数据。但是、如果无法计算出所有经过数据检索的数据、则无法完成修复。修复将在所有节点均可用后完成。

> 卷还原取决于存储对象副本的资源的可用性。卷还原进度是非线性的、可能需要数天或数周才能完成。

[[enable－auto－restore－mode]]启用自动恢复模式

启用自动还原模式后、卷还原将在卷准备就绪后自动开始。

步骤

1. 在网格管理器中转到*维护*>*卷恢复*。
2. 选择*要还原的节点*选项卡，然后将*自动还原模式*的切换滑至启用位置。
3. 出现确认对话框时、请查看详细信息。

   > - 您将无法在任何节点上手动启动卷还原作业。
   > - 只有在没有执行其他维护过程时、卷还原才会自动开始。
   > - 您可以从进度监控页面监控作业的状态。
   > - StorageGRID会自动重试无法启动的卷还原。

4. 了解启用自动恢复模式的结果后，在确认对话框中选择*Yes*。

您可以随时禁用自动还原模式。

[[manually -restore]]手动还原故障卷或节点

按照以下步骤还原发生故障的卷或节点。

步骤

1. 在网格管理器中转到*维护*>*卷恢复*。
2. 选择*要还原的节点*选项卡，然后将*自动还原模式*的切换滑至禁用位置。

   选项卡上的数字表示卷需要还原的节点数。

3. 展开每个节点以查看其中需要还原的卷及其状态。
4. 更正阻止还原每个卷的所有问题。如果选择*正在等待手动步骤*(如果显示为卷状态)，则会指示出现问题。
5. 选择一个要还原的节点、其中所有卷都指示"Ready to Restore"状态。

   一次只能还原一个节点的卷。

   节点中的每个卷都必须指示其已准备好还原。

6. 选择*开始还原*。
7. 解决可能出现的任何警告，或者选择*Start anyway *以忽略警告并开始恢复。

恢复开始时，节点将从“要还原的节点”选项卡移至“还原进度”选项卡。

如果无法启动卷还原、则节点将返回到*要还原的节点*选项卡。

查看还原进度

"还原进度"选项卡显示卷还原过程的状态以及有关要还原的节点的卷的信息。

所有卷中复制和纠删编码对象的数据修复率是汇总所有正在进行的恢复的平均值。还显示了这些卷中完好无损且不需要还原的对象的百分比。

> 复制的数据还原取决于存储复制副本的资源的可用性。复制的数据还原进度是非线性的、可能需要数天或数周才能完成。

"还原作业"部分显示有关从网格管理器启动的卷还原的信息。

- "Restoration Jobs"部分标题中的数字表示正在还原或排队等待还原的卷的数量。
- 此表显示了有关要还原的节点中每个卷的信息及其进度。
  - 每个节点的进度将显示每个作业的百分比。
  - 展开详细信息列以显示还原开始时间和作业ID。
- 如果卷还原失败：
  - 状态列指示 `failed (attempting retry)`，将自动重试。
  - 如果多个还原作业失败、则会首先自动重试最近的作业。

◦ 如果重试继续失败，将触发*EC修复失败*警报。按照警报中的步骤解决问题描述。

查看还原历史记录

"还原历史记录"选项卡显示有关已成功完成的所有卷还原的信息。

大小不适用于复制的对象、仅适用于包含纠删编码(纠删编码、EC)数据对象的还原。

恢复 **StorageGRID** 设备存储节点后检查存储状态

恢复设备存储节点后，您必须验证设备存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择“节点”>“存储节点”>“任务”。
2. 如果“存储状态”下拉列表设置为“只读”或“离线”，请选择“在线”。
3. 选择 * 保存 * 。

从系统驱动器完好无损的存储卷故障中恢复

StorageGRID 存储卷恢复警告

在为存储节点恢复故障存储卷之前、请查看以下警告。

存储节点中的存储卷（或卷组）由十六进制数标识，该十六进制数称为卷 ID 。例如， 0000 是第一个卷， 000f 是第 16 个卷。每个存储节点上的第一个对象存储（卷 0 ）最多使用 4 TB 的空间来执行对象元数据和 Cassandra 数据库操作；该卷上的任何剩余空间都用于对象数据。所有其他存储卷专用于对象数据。

如果出现以下情况，则 Cassandra 数据库可能会作为卷恢复过程的一部分进行重建：

- 卷 0 发生故障并已恢复。
- 系统驱动器和一个或多个存储卷发生故障并已恢复。

当 Cassandra 重建时，系统使用来自其他存储节点的信息。如果 Cassandra 最近重建，Cassandra 数据可能在整个网格中尚不一致。如果太多存储节点处于离线状态：

- 某些 Cassandra 数据可能不可用。
- 可能会发生数据丢失。

如果多个存储节点出现故障（或离线），请联系技术支持。请勿执行以下恢复过程。可能会发生数据丢失。有关详细信息，请参阅"技术支持如何恢复站点" 。

如果 ILM 规则配置为仅存储一个复制副本，并且该副本存在于发生故障的存储卷上，则您将无法恢复该对象。

相关信息

"有关网格节点恢复的警告和注意事项"

识别并卸载 StorageGRID 中的故障存储卷

在恢复包含故障存储卷的存储节点时，您必须确定并卸载故障卷。您必须验证在恢复操作步骤 中仅重新格式化故障存储卷。

开始之前

您已使用登录到网格管理器"支持的 Web 浏览器"。

关于此任务

您应尽快恢复发生故障的存储卷。

恢复过程的第一步是检测已断开连接，需要卸载或存在 I/O 错误的卷。如果故障卷仍然连接，但文件系统随机损坏，则系统可能无法检测到磁盘中未使用或未分配的部分有任何损坏。

您必须先完成此操作步骤 ，然后再执行手动步骤来恢复卷，例如添加或重新连接磁盘，停止节点 ，启动节点或重新启动。否则、在运行脚本时 `reformat_storage_block_devices.rb`、您可能会遇到文件系统错误、从而导致脚本挂起或失败。

在运行命令之前、请修复硬件并正确连接磁盘 `reboot`。

请仔细识别故障存储卷。您将使用此信息验证哪些卷必须重新格式化。重新格式化卷后、卷上的数据将无法恢复。

要恢复故障存储卷，您需要知道故障存储卷的设备名称及其卷 ID。

在安装时，每个存储设备都分配一个文件系统通用唯一标识符 (UUID)，并使用该分配的文件系统 UUID 安装到存储节点上的 rangedb 目录。文件系统 UUID 和 rangedb 目录列在 `/etc/fstab`文件。网格管理器中显示卷的挂载点、设备名称和大小。

步骤

1. 完成以下步骤以记录故障存储卷及其设备名称：
   a. 选择 节点 > 站点 > 故障存储节点 > 存储。
   b. 向下滚动以找到卷表和对象存储表，并记录每个状态为未知或离线的卷的以下信息。
      - 从卷表中，记录安装点、设备和大小。
      - 从对象存储表中，记录 `object_store_ID`。

        `object_store_ID`是发生故障的存储卷的ID。例如、在命令中为ID为0000的对象存储指定 `0`。

2. 登录到发生故障的存储节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

3. 运行以下脚本以卸载发生故障的存储卷：

   ```
   sn-unmount-volume object_store_ID
   ```

4. 如果出现提示，请按*y*停止Cassand拉 服务，具体取决于存储卷0。

   如果Cassand拉 服务已停止、则不会出现提示。仅对卷 0 停止 Cassandra 服务。

   ```
   root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
   Services depending on storage volume 0 (cassandra) aren't down.
   Services depending on storage volume 0 must be stopped before running
   this script.
   Stop services that require storage volume 0 [y/N]? y
   Shutting down services that require storage volume 0.
   Services requiring storage volume 0 stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   几秒钟后、此卷将被卸载。此时将显示消息，指示此过程的每个步骤。最后一条消息指示卷已卸载。

5. 如果卸载因卷繁忙而失败、您可以使用选项强制卸载 `--use-umountof`：

   使用选项强制卸载 `--use-umountof`可能会导致使用此卷的进程或服务行为异常或崩溃。

   ```
   root@Storage-180:~ # sn-unmount-volume --use-umountof
   /var/local/rangedb/2
   Unmounting /var/local/rangedb/2 using umountof
   /var/local/rangedb/2 is unmounted.
   Informing LDR service of changes to storage volumes
   ```

恢复发生故障的存储卷并在 **StorageGRID** 中重建 **Cassandra** 数据库

您必须运行一个脚本来重新格式化和重新挂载故障存储卷上的存储，并在系统确定有必要时在存储节点上重建 Cassandra 数据库。

开始之前

- 您已获得 `Passwords.txt`文件。
- 服务器上的系统驱动器完好无损。
- 已确定故障的发生原因 、并且已在必要时获取更换存储硬件。
- 替换存储的总大小与原始存储相同。
- 您已检查存储节点退役未正在进行，或者您已暂停节点退役过程。 （在网格管理器中，选择*维护* > 任务 > 退役。）
- 您已检查扩展是否尚未进行。 （在网格管理器中，选择*维护* > 任务 > 扩展。）
- 您拥有 "已查看有关存储卷恢复的警告"。

步骤

1. 根据需要，更换与先前已确定并卸载的故障存储卷关联的故障物理或虚拟存储。

   请勿在此步骤中重新挂载卷。存储将在后续步骤中重新挂载并添加到中 `/etc/fstab`。

2. 在网格管理器中，转到 节点 > **`appliance Storage Node`** > 硬件。在页面的StorageGRID Appliance 部分中，验证存储 RAID 模式是否正常。
3. 登录到发生故障的存储节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

4. 使用文本编辑器(vi或vm)从文件中删除故障卷 `/etc/fstab`、然后保存文件。

   > 注释掉文件中出现故障的卷 `/etc/fstab`是不够的。必须从中删除此卷、因为恢复过程会验证此 `fstab`文件中的所有行是否 `fstab`与挂载的文件系统匹配。

5. 重新格式化任何发生故障的存储卷，并根据需要重建 Cassandra 数据库。输入：
   `reformat_storage_block_devices.rb`
   - 卸载存储卷0后、系统将显示提示和消息、指示Cassand拉 服务正在停止。
   - 如果需要，系统将提示您重建 Cassandra 数据库。
     - 查看警告。如果其中任何一项都不适用，请重建 Cassandra 数据库。输入： *
     - 如果多个存储节点处于离线状态。输入：**n**

       该脚本将退出而不重建 Cassandra 。请联系技术支持。
   - 对于存储节点上的每个rangedb驱动器，当系统询问您：时，输入以下响应之一： `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`

- * y * 重新格式化出现错误的驱动器。此操作将重新格式化存储卷、并将重新格式化的存储卷添加到文件中 `/etc/fstab`。
- **n**(如果驱动器没有错误，并且您不想重新格式化它)。

> 选择 * n * 将退出此脚本。挂载驱动器（如果您认为应保留驱动器上的数据且错误地卸载了驱动器）或删除驱动器。然后、再次运行 `reformat_storage_block_devices.rb` 命令。

> 某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到"reaper"或"cassandr修复"。如果您看到指示修复失败的错误消息、请运行错误消息中指示的命令。

在以下示例输出中、必须重新格式化驱动器 `/dev/sdf`、并且不需要重建cassandreas:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

下一步是什么?

在重新格式化和重新装载存储卷以及必要的 Cassandra 操作完成后，您可以 "使用网格管理器还原对象数据"。

将对象数据还原至系统驱动器完好无损的 **StorageGRID** 存储卷

在系统驱动器完好无损的存储节点上恢复存储卷后、您可以还原在存储卷发生故障时丢失的已复制或经过删除编码的对象数据。

开始之前

- 如果自动过程未能重新挂载保留的存储卷并重新格式化发生故障的存储卷，则表示您已执行以下过程之一：
  - "重新挂载并重新格式化设备存储卷(手动步骤)"
  - "重新挂载和重新格式化存储卷(手动步骤)"

- 您已确认要还原对象的存储节点在网格管理器中的*节点* > 概览*选项卡上的连接状态为*已连接 。
- 您已确认以下事项：
  - 未进行网格扩展以添加存储节点。
  - 存储节点停用未在进行中或失败。
  - 故障存储卷的恢复未在进行中。
  - 具有故障系统驱动器的存储节点的恢复未在进行中。
  - EC 重新平衡作业未在进行中。
  - 设备节点克隆未在进行中。

关于此任务

更换驱动器并格式化卷后，Grid Manager 会在*维护* > 卷恢复 > *要恢复的节点*选项卡上将卷显示为要恢复的候选卷。

请尽可能使用网格管理器中的卷还原页面还原对象数据。您可以在卷准备好进行还原时自动启动卷还原，也可以启用自动还原模式手动执行卷还原。请遵循以下准则：

- 如果卷在 维护 > 卷恢复 > 要恢复的节点 中列出，请按照以下步骤恢复对象数据。如果满足以下条件，则会列出卷：
  - 节点中的部分(而非全部)存储卷发生故障
  - 一个节点中的所有存储卷均发生故障、并正在替换为相同数量或更多卷

    网格管理器中的卷还原页面还可用于监控卷还原过程和查看还原历史记录。

  如果恢复的存储节点包含的卷少于要替换的节点，请联系技术支持以获得帮助。

您可以还原两种类型的对象数据：

- 复制的数据对象会从其他位置还原、前提是已将网格的ILM规则配置为使对象副本可用。
  - 如果将 ILM 规则配置为仅存储一个复制副本，并且该副本存在于出现故障的存储卷上，则无法恢复该对象。
  - 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。
- 纠删编码(纠删编码、EC)数据对象可通过重新组装存储的片段来还原。损坏或丢失的片段会通过纠删编码算法从其余数据和奇偶校验片段中重新创建。

  在某些存储节点脱机时，可以开始修复经过擦除编码的数据。但是、如果无法计算出所有经过数据检索的数据、则无法完成修复。修复将在所有节点均可用后完成。

> 卷还原取决于存储对象副本的资源的可用性。卷还原进度是非线性的、可能需要数天或数周才能完成。

[[enable－auto－restore－mode]]启用自动恢复模式

启用自动还原模式后、卷还原将在卷准备就绪后自动开始。

步骤

1. 在网格管理器中转到*维护*>*卷恢复*。
2. 选择*要还原的节点*选项卡，然后将*自动还原模式*的切换滑至启用位置。
3. 出现确认对话框时、请查看详细信息。

   - 您将无法在任何节点上手动启动卷还原作业。
   - 只有在没有执行其他维护过程时、卷还原才会自动开始。
   - 您可以从进度监控页面监控作业的状态。
   - StorageGRID会自动重试无法启动的卷还原。

4. 了解启用自动恢复模式的结果后，在确认对话框中选择*Yes*。

   您可以随时禁用自动还原模式。

[[manually -restore]]手动还原故障卷或节点

按照以下步骤还原发生故障的卷或节点。

步骤

1. 在网格管理器中转到*维护*>*卷恢复*。
2. 选择*要还原的节点*选项卡，然后将*自动还原模式*的切换滑至禁用位置。

   选项卡上的数字表示卷需要还原的节点数。

3. 展开每个节点以查看其中需要还原的卷及其状态。
4. 更正阻止还原每个卷的所有问题。如果选择*正在等待手动步骤*(如果显示为卷状态)，则会指示出现问题。
5. 选择一个要还原的节点、其中所有卷都指示"Ready to Restore"状态。

   一次只能还原一个节点的卷。

   节点中的每个卷都必须指示其已准备好还原。

6. 选择*开始还原*。
7. 解决可能出现的任何警告，或者选择*Start anyway *以忽略警告并开始恢复。

恢复开始时，节点将从“要还原的节点”选项卡移至“还原进度”选项卡。

如果无法启动卷还原、则节点将返回到*要还原的节点*选项卡。

查看还原进度

"还原进度"选项卡显示卷还原过程的状态以及有关要还原的节点的卷的信息。

所有卷中复制和纠删编码对象的数据修复率是汇总所有正在进行的恢复的平均值。还显示了这些卷中完好无损且不需要还原的对象的百分比。

复制的数据还原取决于存储复制副本的资源的可用性。复制的数据还原进度是非线性的、可能需要数天或数周才能完成。

"还原作业"部分显示有关从网格管理器启动的卷还原的信息。

- "Restoration Jobs"部分标题中的数字表示正在还原或排队等待还原的卷的数量。
- 此表显示了有关要还原的节点中每个卷的信息及其进度。
  - 每个节点的进度将显示每个作业的百分比。
  - 展开详细信息列以显示还原开始时间和作业ID。
- 如果卷还原失败：
  - 状态列指示 `failed (attempting retry)`，将自动重试。
  - 如果多个还原作业失败、则会首先自动重试最近的作业。
  - 如果重试继续失败，将触发*EC修复失败*警报。按照警报中的步骤解决问题描述。

查看还原历史记录

"还原历史记录"选项卡显示有关已成功完成的所有卷还原的信息。

大小不适用于复制的对象、仅适用于包含纠删编码(纠删编码、EC)数据对象的还原。

恢复 **StorageGRID** 存储卷后检查存储状态

恢复存储卷后，您必须验证存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择“节点”>“存储节点”>“任务”。
2. 如果“存储状态”下拉列表设置为“只读”或“离线”，请选择“在线”。
3. 选择 * 保存 * 。

从系统驱动器故障中恢复

StorageGRID 存储节点系统驱动器恢复警告

在恢复存储节点的故障系统驱动器之前、请查看常规"有关网格节点恢复的警告和注意事项"警告和以下特定警告。

存储节点有一个包含对象元数据的 Cassandra 数据库。如果出现以下情况，则可能需要重建 Cassandra 数据库：

- 存储卷发生故障并已恢复。
- 系统驱动器和一个或多个存储卷发生故障并已恢复。

当 Cassandra 重建时，系统使用来自其他存储节点的信息。如果 Cassandra 最近重建，Cassandra 数据可能在整个网格中尚不一致。如果太多存储节点处于离线状态：

- 某些 Cassandra 数据可能不可用。
- 可能会发生数据丢失。

> 如果多个存储节点出现故障（或离线），请联系技术支持。不要执行以下恢复过程。可能会发生数据丢失。有关详细信息，请参阅"技术支持如何恢复站点"。

> 如果此存储节点处于只读维护模式，以允许具有发生故障的存储卷的另一个存储节点检索对象，则在恢复此发生故障的存储节点之前，请恢复具有发生故障的存储卷的存储节点上的卷。请参阅"从系统驱动器完好无损的存储卷故障中恢复"的说明。

> 如果 ILM 规则配置为仅存储一个复制副本，而该副本位于发生故障的存储卷上，则您将无法恢复对象。

替换 **StorageGRID** 存储节点

如果系统驱动器发生故障，您必须先更换存储节点。

您必须为您的平台选择节点替代操作步骤 。对于所有类型的网格节点，更换节点的步骤都相同。

> 仅限此基于 操作步骤 适用场景 软件的存储节点。您必须按照与不同的过程进行"恢复设备存储节点"操作。

*Linux:*如果不确定系统驱动器是否出现故障，请按照说明更换节点以确定需要执行哪些恢复步骤。

平台	操作步骤
VMware	"更换 VMware 节点"
Linux	"更换 Linux 节点"
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照的过程进行操作"更换Linux节点"。

选择 **Start Recovery** 以配置 **StorageGRID** 存储节点

更换存储节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您已部署并配置替代节点。
- 您知道已进行过数据检索的任何修复作业的开始日期。

关于此任务

如果存储节点作为容器安装在 Linux 主机上，则只有在满足以下条件之一时，才必须执行此步骤：

- 您必须使用 `--force`标志导入节点、否则会发出此命令 `storagegrid node force-recovery node-name`
- 您必须执行完整节点重新安装，或者需要还原 /var/local 。

步骤

1. 登录到主管理节点。如果主管理节点不可用，请使用非主管理节点（如果存在）。
2. 在网格管理器中，选择*Maintenance* > **Tasks** > **Node recovery**。
3. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点发生故障后会显示在列表中、但您无法选择某个节点、直到它重新安装并准备好进行恢复为止。

4. 输入 **Provisioning passphrase**。
5. 单击*开始恢复*。
6. 通过选择*维护* > 任务 > *节点恢复*并查看恢复进度来监控恢复进度。
   - 如果网格节点达到"等待手动步骤"阶段，则必须"手动重新挂载并重新格式化存储卷"。完成手动步骤后，请继续"将对象数据还原至卷"。
   - 如果网格节点恢复已从*进行中*过渡到*已恢复*，而无需经过"等待手动步骤"阶段，则无需执行进一步操作。

> 在恢复过程中的任何时候，您都可以选择*重置*以开始新的恢复。将显示一个对话框，指示如果重置过程，节点将保持不确定状态。
>
> 如果要在重置过程后重试恢复，则必须将设备节点恢复到预安装状态，如下所示：
>
> - * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
> - **Linux**：通过在Linux主机上运行以下命令来重新启动节点： `storagegrid node force-recovery node-name`

重新挂载并重新格式化 **StorageGRID** 存储卷（手动步骤）

如果自动过程无法重新挂载保留的存储卷并重新格式化发生故障的存储卷，则必须手动运行两个脚本来完成这些操作。第一个脚本重新挂载已正确格式化为 StorageGRID 存储卷的卷。第二个脚本重新格式化所有未挂载的卷，如果需要，重建 Cassandra 数据库，然后启动服务。

在存储节点恢复期间，如果 Grid Manager 中出现"等待手动步骤"消息，请按照以下步骤重新挂载并重新格式化存储卷。如果您没有看到此消息，则重新挂载和重新格式化操作已自动完成，您可以跳过_this_过程和"还原对象数据"。

开始之前

- 您已更换已知需要更换的任何故障存储卷的硬件。

  运行此 `sn-remount-volumes`脚本可能有助于确定其他故障存储卷。

- 您已检查存储节点退役未正在进行，或者您已暂停节点退役过程。 （在网格管理器中，选择*维护* > 任务 > 退役。）
- 您已检查扩展是否尚未进行。 （在网格管理器中，选择*维护* > 任务 > 扩展。）
- 您拥有 "已查看有关存储节点系统驱动器恢复的警告"。

> 如果多个存储节点离线，请联系技术支持。不要运行 `sn-recovery-postinstall.sh`脚本。

关于此任务

要完成此操作步骤 ，请执行以下高级任务：

- 登录到已恢复的存储节点。
- 运行 `sn-remount-volumes`脚本以重新挂载格式正确的存储卷。运行此脚本时，它将执行以下操作：
  - 挂载和卸载每个存储卷以重放 XFS 日志。
  - 执行 XFS 文件一致性检查。
  - 如果文件系统一致，则确定存储卷是否为格式正确的 StorageGRID 存储卷。
  - 如果存储卷格式正确，请重新挂载该存储卷。卷上的所有现有数据保持不变。
- 查看脚本输出并解决任何问题。
- 运行 `sn-recovery-postinstall.sh`脚本。运行此脚本时，它将执行以下操作。

> 在运行以重新格式化故障存储卷和还原对象元数据之前、请勿在恢复期间重新启动存储节点 `sn-recovery-postinstall.sh`。在完成之前重新启动存储节点 `sn-recovery-postinstall.sh`会导致尝试启动的服务出现错误、并导致StorageGRID设备节点退出维护模式。请参阅的步骤安装后脚本。

  - 重新格式化脚本无法挂载或发现格式不正确的任何存储卷 `sn-remount-volumes`。

> 如果重新格式化某个存储卷，则该卷上的所有数据都将丢失。假设已将 ILM 规则配置为存储多个对象副本，则必须执行额外的操作步骤 以从网格中的其他位置还原对象数据。

  - 如果需要，在节点上重建 Cassandra 数据库。
  - 启动存储节点上的服务。

步骤

1. 登录到已恢复的存储节点：

a. 输入以下命令： `ssh admin@grid_node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 运行第一个脚本重新挂载任何格式正确的存储卷。

> 如果所有存储卷都是新的，需要进行格式化，或者所有存储卷都出现故障，您可以跳过此步骤并运行第二个脚本，重新格式化所有已卸载的存储卷。

a. 运行脚本： `sn-remount-volumes`

此脚本可能需要数小时才能在包含数据的存储卷上运行。

b. 在脚本运行期间，查看输出并问题解答 任何提示。

> 根据需要，您可以使用 `tail -f`命令监控脚本日志文件的内容 (/var/local/log/sn-remount-volumes.log`)。日志文件包含比命令行输出更详细的信息。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
```

```
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
```

```
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
```

```
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

在示例输出中，一个存储卷已成功重新挂载，三个存储卷出现错误。

- `/dev/sdb`已通过XFS文件系统一致性检查并具有有效的卷结构、因此已成功重新挂载。此脚本重新挂载的设备上的数据将保留下来。
- `/dev/sdc`未通过XFS文件系统一致性检查、因为存储卷是新的或已损坏。
- `/dev/sdd`无法挂载、因为磁盘未初始化或磁盘的超块已损坏。当脚本无法挂载存储卷时、它会询问您是否要运行文件系统一致性检查。
  - 如果存储卷已连接到新磁盘，请将 * N * 问题解答 到提示符处。您不需要检查新磁盘上的文件系统。
  - 如果存储卷已连接到现有磁盘，问题解答 请将 * 。 *您可以使用文件系统检查的结果来确定损坏的来源。结果将保存在日志文件中 `/var/local/log/sn-remount-volumes.log`。
- `/dev/sde`已通过XFS文件系统一致性检查并具有有效的卷结构；但是、volID文件中的LDR节点ID与此存储节点的ID不匹配(`configured LDR noid`显示在顶部)。此消息表示此卷属于另一个存储节点。

3. 查看脚本输出并解决任何问题。

> 如果存储卷未通过 XFS 文件系统一致性检查或无法挂载，请仔细查看输出中的错误消息。您必须了解在这些卷上运行此脚本的含义 `sn-recovery-postinstall.sh`。

a. 检查以确保结果中包含所需所有卷的条目。如果未列出任何卷、请重新运行此脚本。

b. 查看所有已挂载设备的消息。确保没有指示存储卷不属于此存储节点的错误。

在此示例中、的输出 `/dev/sde`包括以下错误消息：

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> 如果报告某个存储卷属于另一个存储节点，请联系技术支持。如果运行此 `sn-recovery-postinstall.sh`脚本、则存储卷将被重新格式化、从而可能导致数据丢失。

c. 如果无法挂载任何存储设备，请记下此设备的名称，然后修复或更换此设备。

> 您必须修复或更换任何无法挂载的存储设备。

d. 修复或更换所有无法挂载的设备后、再次运行 `sn-remount-volumes`脚本、以确认可以重新挂载的所有存储卷均已重新挂载。

> 如果某个存储卷无法挂载或格式不正确、则在继续下一步后、该卷以及该卷上的任何数据将被删除。如果对象数据有两个副本，则只有一个副本，直到完成下一个操作步骤 （还原对象数据）为止。

> 如果您认为无法从网格中的其他位置重建故障存储卷上剩余的数据(例如、如果您的ILM策略使用的规则仅创建一个副本、或者卷在多个节点上发生故障)、请勿运行此 `sn-recovery-postinstall.sh`脚本。请联系技术支持以确定如何恢复数据。

4. 运行 `sn-recovery-postinstall.sh`脚本： `sn-recovery-postinstall.sh`

此脚本将重新格式化无法挂载或格式不正确的任何存储卷；根据需要在节点上重建 Cassandra 数据库；并启动存储节点上的服务。

请注意以下事项：

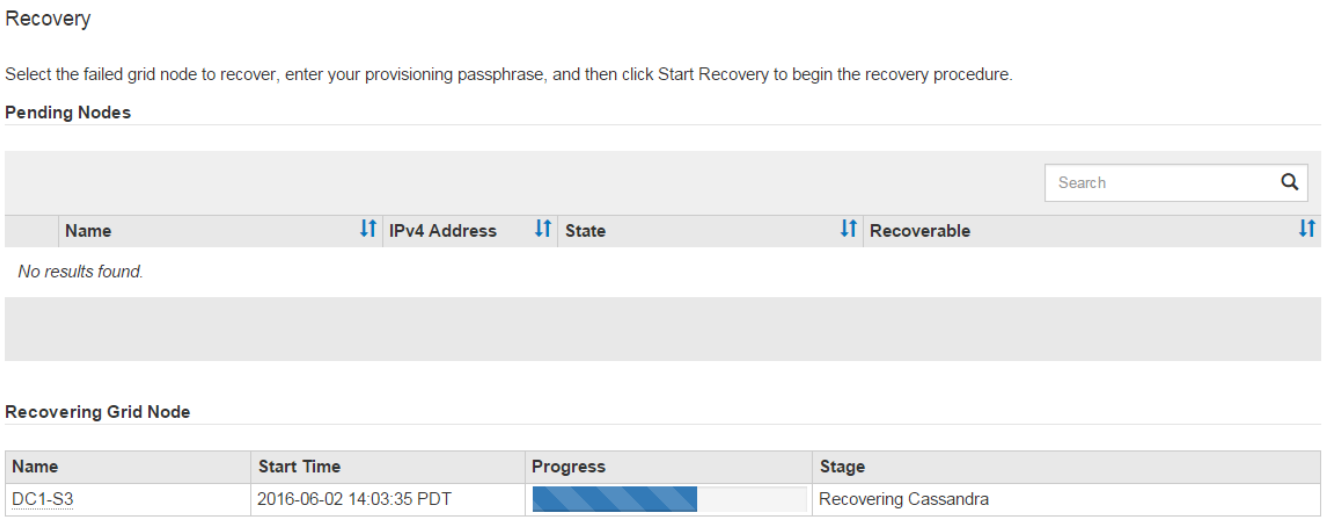
- 此脚本可能需要数小时才能运行。
- 通常，在脚本运行期间，您应单独保留 SSH 会话。
- 在SSH会话处于活动状态时，请勿按*Ctrl+C*。
- 如果发生网络中断并终止 SSH 会话，则此脚本将在后台运行，但您可以从 " 恢复 " 页面查看进度。
- 如果存储节点使用 RSM 服务，则随着节点服务重新启动，脚本可能会暂停 5 分钟。每当 RSM 服务首次启动时，预计会有 5 分钟的延迟。

> RSM 服务位于包含此 ADC 服务的存储节点上。

> 某些 StorageGRID 恢复过程使用 Reaper 处理 Cassandra 修复。一旦相关服务或所需服务开始，便会自动进行修复。您可能会注意到脚本输出中提到"reaper"或"cassandr修复"。如果您看到指示修复失败的错误消息、请运行错误消息中指示的命令。

5. 在脚本运行时 `sn-recovery-postinstall.sh`、监控网格管理器中的"RecRecovery (恢复)"页面。

恢复页面上的进度栏和阶段列提供了该脚本的简要状态 `sn-recovery-postinstall.sh`。



6. 脚本在节点上启动服务后 `sn-recovery-postinstall.sh`、您可以将对象数据还原到由脚本格式化的任何存储卷。

   该脚本会询问您是否要使用Grid Manager卷还原过程。

   - 在大多数情况下，您应该"使用网格管理器还原对象数据"。答案 `y`以使用 Grid Manager。
   - 在极少数情况下，例如当您知道替换节点可用于对象存储的卷少于原始节点时，请联系技术支持以手动还原对象数据。如果其中一种情况适用，请回答 `n`并按任意键返回命令行。

将对象数据还原至 **StorageGRID** 存储卷（系统驱动器故障）

在恢复非设备存储节点的存储卷之后、您可以还原在存储节点发生故障时丢失的复制或经过删除编码的对象数据。

开始之前

- 如果自动过程未能重新挂载保留的存储卷并重新格式化发生故障的存储卷，则表示您已执行以下过程之一：
  - "重新挂载并重新格式化设备存储卷(手动步骤)"
  - "重新挂载和重新格式化存储卷(手动步骤)"
- 您已确认要还原对象的存储节点在网格管理器中的*节点* > 概览*选项卡上的连接状态为*已连接 。
- 您已确认以下事项：
  - 未进行网格扩展以添加存储节点。
  - 存储节点停用未在进行中或失败。
  - 故障存储卷的恢复未在进行中。
  - 具有故障系统驱动器的存储节点的恢复未在进行中。
  - EC 重新平衡作业未在进行中。
  - 设备节点克隆未在进行中。

关于此任务

更换驱动器并格式化卷后，Grid Manager 会在*维护* > 卷恢复 > *要恢复的节点*选项卡上将卷显示为要恢复的

候选卷。

请尽可能使用网格管理器中的卷还原页面还原对象数据。您可以在卷准备好进行还原时自动启动卷还原，也可以启用自动还原模式手动执行卷还原。请遵循以下准则：

- 如果卷在 维护 > 卷恢复 > 要恢复的节点 中列出，请按照以下步骤恢复对象数据。如果满足以下条件，则会列出卷：
  - 节点中的部分(而非全部)存储卷发生故障
  - 一个节点中的所有存储卷均发生故障、并正在替换为相同数量或更多卷

  网格管理器中的卷还原页面还可用于监控卷还原过程和查看还原历史记录。

  如果恢复的存储节点包含的卷少于要替换的节点，请联系技术支持以获得帮助。

您可以还原两种类型的对象数据：

- 复制的数据对象会从其他位置还原、前提是已将网格的ILM规则配置为使对象副本可用。
  - 如果将 ILM 规则配置为仅存储一个复制副本，并且该副本存在于出现故障的存储卷上，则无法恢复该对象。
  - 如果某个对象的唯一剩余副本位于云存储池中，则 StorageGRID 必须将多个请求问题描述 到云存储池端点以还原对象数据。
- 纠删编码(纠删编码、EC)数据对象可通过重新组装存储的片段来还原。损坏或丢失的片段会通过纠删编码算法从其余数据和奇偶校验片段中重新创建。

  在某些存储节点脱机时，可以开始修复经过擦除编码的数据。但是、如果无法计算出所有经过数据检索的数据、则无法完成修复。修复将在所有节点均可用后完成。

> 卷还原取决于存储对象副本的资源的可用性。卷还原进度是非线性的、可能需要数天或数周才能完成。

[[enable－auto－restore－mode]]启用自动恢复模式

启用自动还原模式后、卷还原将在卷准备就绪后自动开始。

步骤

1. 在网格管理器中转到*维护*>*卷恢复*。
2. 选择*要还原的节点*选项卡，然后将*自动还原模式*的切换滑至启用位置。
3. 出现确认对话框时、请查看详细信息。

   > - 您将无法在任何节点上手动启动卷还原作业。
   > - 只有在没有执行其他维护过程时、卷还原才会自动开始。
   > - 您可以从进度监控页面监控作业的状态。
   > - StorageGRID会自动重试无法启动的卷还原。

4. 了解启用自动恢复模式的结果后，在确认对话框中选择*Yes*。

您可以随时禁用自动还原模式。

[[manually -restore]]手动还原故障卷或节点

按照以下步骤还原发生故障的卷或节点。

步骤

1. 在网格管理器中转到*维护*>*卷恢复*。
2. 选择*要还原的节点*选项卡，然后将*自动还原模式*的切换滑至禁用位置。

   选项卡上的数字表示卷需要还原的节点数。

3. 展开每个节点以查看其中需要还原的卷及其状态。
4. 更正阻止还原每个卷的所有问题。如果选择*正在等待手动步骤*(如果显示为卷状态)，则会指示出现问题。
5. 选择一个要还原的节点、其中所有卷都指示"Ready to Restore"状态。

   一次只能还原一个节点的卷。

   节点中的每个卷都必须指示其已准备好还原。

6. 选择*开始还原*。
7. 解决可能出现的任何警告，或者选择*Start anyway *以忽略警告并开始恢复。

恢复开始时，节点将从“要还原的节点”选项卡移至“还原进度”选项卡。

如果无法启动卷还原、则节点将返回到*要还原的节点*选项卡。

查看还原进度

"还原进度"选项卡显示卷还原过程的状态以及有关要还原的节点的卷的信息。

所有卷中复制和纠删编码对象的数据修复率是汇总所有正在进行的恢复的平均值。还显示了这些卷中完好无损且不需要还原的对象的百分比。

> 复制的数据还原取决于存储复制副本的资源的可用性。复制的数据还原进度是非线性的、可能需要数天或数周才能完成。

"还原作业"部分显示有关从网格管理器启动的卷还原的信息。

- "Restoration Jobs"部分标题中的数字表示正在还原或排队等待还原的卷的数量。
- 此表显示了有关要还原的节点中每个卷的信息及其进度。
  - 每个节点的进度将显示每个作业的百分比。
  - 展开详细信息列以显示还原开始时间和作业ID。
- 如果卷还原失败：
  - 状态列指示 `failed (attempting retry)`，将自动重试。
  - 如果多个还原作业失败、则会首先自动重试最近的作业。

◦ 如果重试继续失败，将触发*EC修复失败*警报。按照警报中的步骤解决问题描述。

查看还原历史记录

"还原历史记录"选项卡显示有关已成功完成的所有卷还原的信息。

大小不适用于复制的对象、仅适用于包含纠删编码(纠删编码、EC)数据对象的还原。

恢复 **StorageGRID** 存储节点系统驱动器后检查存储状态

恢复存储节点的系统驱动器后，您必须验证存储节点的所需状态是否设置为联机，并确保每当重新启动存储节点服务器时，此状态默认为联机。

开始之前

- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 存储节点已恢复，数据恢复已完成。

步骤

1. 选择“节点”>“存储节点”>“任务”。
2. 如果“存储状态”下拉列表设置为“只读”或“离线”，请选择“在线”。
3. 选择 * 保存 * 。

从管理节点故障中恢复

StorageGRID 中的主管理节点或非主管理节点恢复

管理节点的恢复过程取决于它是主管理节点还是非主管理节点。

恢复主管理节点或非主管理节点的高级步骤相同，但具体步骤有所不同。

对于要恢复的管理节点，请始终遵循正确的恢复操作步骤 。这些过程从较高的层面来看是相同的，但细节却有所不同。

选项

- "使用相同的主管理节点恢复主管理节点"
- "使用非主管理节点从主管理节点故障中恢复"
- "从非主管理节点故障中恢复"

使用相同的主管理节点从主管理节点故障中恢复

使用相同的主管理节点恢复 **StorageGRID** 主管理节点

要从主管理节点故障中恢复，您必须完成一组特定的任务。主管理节点托管网格的配置管理节点（ CMN ）服务。

必须及时修复或更换出现故障的主管理节点，否则可能无法执行某些维护过程。

按照以下简要步骤恢复主管理节点：

1. "从发生故障的主管理节点复制审核日志"
2. "更换主管理节点"
3. "配置替代主管理节点"
4. "确定已恢复的主管理节点是否需要修补程序"
5. "在已恢复的主管理节点上还原审核日志"
6. "在恢复主管理节点时还原管理节点数据库"
7. "恢复主管理节点时还原Prometheus指标"

从发生故障的 **StorageGRID** 主管理节点复制审核日志

如果您能够从出现故障的主管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的主管理节点启动并运行后将保留的审核日志还原到该节点。

关于此任务

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

如果现在无法在故障管理节点上访问审核日志、您可以稍后访问这些日志、例如、在主机恢复之后。

步骤

1. 如果可能，请登录到发生故障的主管理节点。否则，登录到任何可用的管理节点。
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

      当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 停止AMS服务以防止其创建新日志文件：`service ams stop`
3. 导航到审核导出目录：

   ```
   cd /var/local/audit/export
   ```

   （或者 `cd /var/local/log`在早期系统上）

4. 将源日志文件重命名为唯一编号的文件名。

   - 如果日志文件位于 `/var/local/audit/export`目录，其名称是 `audit.log。
   - 如果日志文件位于 `/var/local/log`目录，其名称是 `localaudit.log。

   例如，重命名 `localaudit.log`文件到 `2025-10-22.txt.1。

   ```
   ls -l
   mv localaudit.log 2025-10-22.txt.1
   ```

5. 重新启动AMS服务： `service ams start`
6. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

7. 将所有审核日志文件复制到临时位置： `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

8. 以root身份注销： `exit`

使用相同的主管理节点替换 **StorageGRID** 主管理节点

要恢复主管理节点，必须先更换物理或虚拟硬件。

要恢复主管理节点，必须先更换物理或虚拟硬件。

- 您可以将发生故障的主管理节点替换为在同一平台上运行的主管理节点。
- 您可以将 VMware 或 Linux 主机上运行的主管理节点替换为 StorageGRID 服务设备上托管的主管理节点。
- 您可以将 VMware 主机上运行的主管理节点替换为 SG1000 或 SG100 服务设备。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将引导您进入主管理节点恢复的下一步。

更换平台	操作步骤
VMware	"用恢复节点替换 VMware 节点" "用 SG1000 或 SG100 替换 VMware 节点"
Linux	"更换 Linux 节点"
服务设备	"更换服务设备"

更换平台	操作步骤
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照的过程进行操作"更换Linux节点"。

在 **StorageGRID** 中配置替换主管理节点

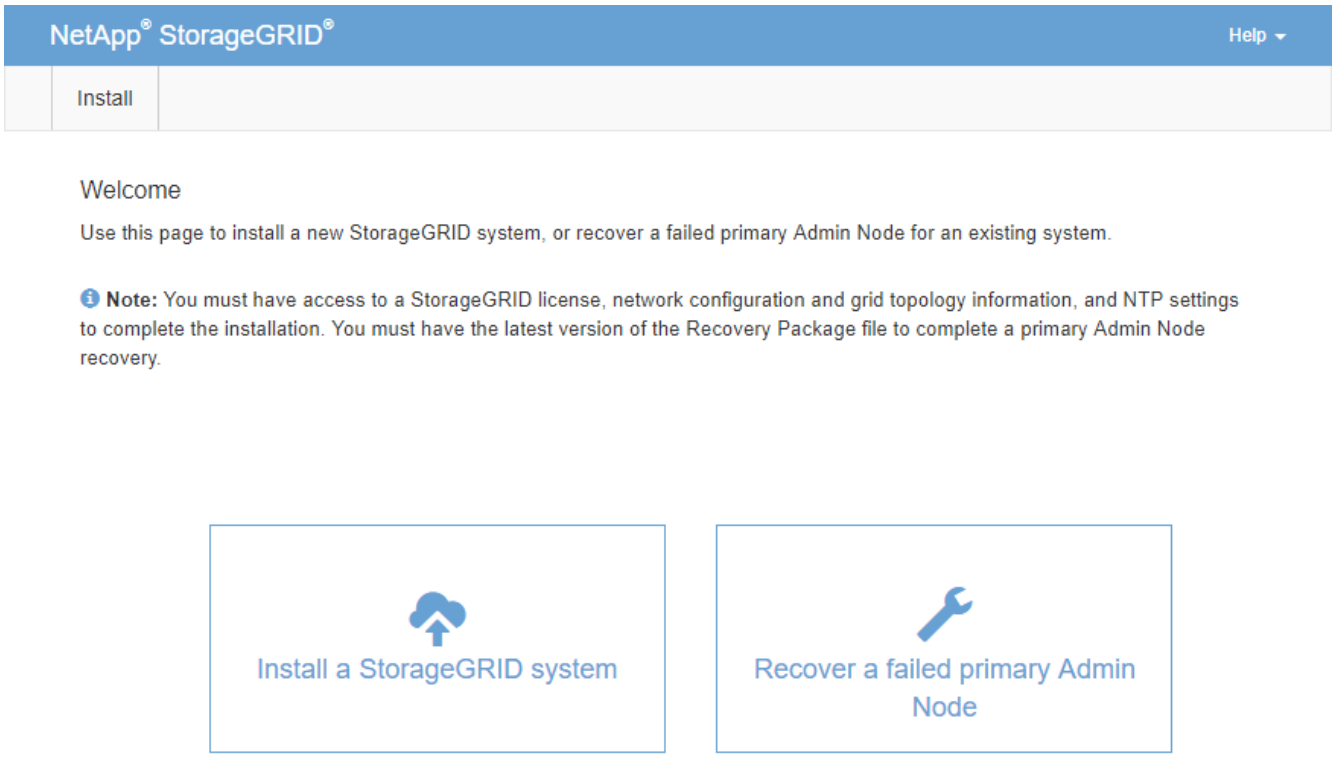
必须将替代节点配置为 StorageGRID 系统的主管理节点。

开始之前

- 对于虚拟机上托管的主管理节点、虚拟机已部署、启动并初始化。
- 对于服务设备上托管的主管理节点，您已更换此设备并安装了软件。请参见 "设备安装说明"。
- 您有恢复包文件的最新备份(`sgws-recovery-package-id-revision.zip`）。
- 您具有配置密码短语。

步骤

1. 打开Web浏览器并导航至 `https://primary_admin_node_ip`。
2. 根据需要管理临时安装程序密码：
   - 如果已使用以下方法之一设置密码、请输入密码以继续。
     - 用户在先前访问安装程序时设置了密码
     - 对于裸机系统、密码会自动从的节点配置文件中导入 `/etc/storagegrid/nodes/<node_name>.conf`
     - 对于VM、SSH/控制台密码会自动从VF属性导入
   - 如果尚未设置密码、则可以选择设置密码以保护StorageGRID安装程序。
3. 选择*恢复发生故障的主管理节点*。



4. 上传恢复包的最新备份：
   a. 选择 * 浏览 * 。
   b. 找到您的 StorageGRID 系统的最新恢复包文件，然后选择*打开*。
5. 输入配置密码短语。
6. 选择*Start recovery*。

   恢复过程开始。随着所需服务的启动，网格管理器可能会在几分钟内不可用。恢复完成后，将显示登录页面。

7. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

   要配置依赖方信任，请参阅使用 "OIDC" 或 "SAML" 设置 SSO。要访问默认服务器证书，请登录到管理节点的命令 shell。转到 `/var/local/mgmt-api` 目录，然后选择 `server.crt` 文件。

恢复主管理节点后，"确定是否需要应用修补程序"。

确定 **StorageGRID** 中主管理节点的修补程序要求

恢复主管理节点后、确定是否需要应用修补程序。

开始之前

主管理节点恢复已完成。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 选择*节点*。
3. 从左侧列表中，选择主管理节点。
4. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。
5. 选择任何其他网格节点。
6. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。
   - 如果“软件版本”字段中显示的版本相同，则不需要应用修补程序。
   - 如果“软件版本”字段中显示的版本不同，则必须"应用修补程序"将已恢复的主管理节点更新为相同的版本。

在恢复的 **StorageGRID** 主管理节点上还原审核日志

如果能够保留故障主管理节点中的审核日志，则可以将其复制到要恢复的主管理节点。

开始之前

- 已恢复的管理节点已安装并正在运行。
- 在原始管理节点出现故障后、您已将审核日志复制到其他位置。

关于此任务

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点、并且无法从故障节点复制审核日志、则恢复的管理节点会开始将事件记录到审核日志中、就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

> 默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：
>
> - 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
> - 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。
>
> 看"配置日志管理和外部系统日志服务器"了解详情。

步骤

1. 登录到已恢复的管理节点：
   a. 输入以下命令： `ssh admin@recovery_Admin_Node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

以root用户身份登录后，提示符将从更 `$`改为 `#`。

2. 检查哪些审计文件已被保存： `cd /var/local/audit/export`
3. 将保留的审核日志文件复制到已恢复的管理节点： `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   出现提示时，输入 admin 的密码。

4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复的管理节点上的审计日志文件的用户和组设置： `chown ams-user:bycast *`
6. 以root身份注销： `exit`

恢复主管理节点时还原 **StorageGRID** 管理节点数据库

如果要保留有关发生故障的主管理节点上的属性和警报的历史信息、您可以还原管理节点数据库。只有当 StorageGRID 系统包含另一个管理节点时，才能还原此数据库。

开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您已获得 `Passwords.txt`文件。
- 您具有配置密码短语。

关于此任务

如果管理节点出现故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 历史属性数据、用于"节点"页面上的原有模式图表

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统一部分或稍后添加的服务器和服务的信息。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将管理节点数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史信息。如果您的系统只有一个主管理节点、则无法还原管理节点数据库。

> 复制管理节点数据库可能需要几小时的时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

2. 从源管理节点中、停止MI服务： `service mi stop`

3. 从源管理节点中、停止管理应用程序接口(mgmt-api)服务： `service mgmt-api stop`

4. 在已恢复的管理节点上完成以下步骤：

a. 登录到已恢复的管理节点：

i. 输入以下命令： `ssh admin@grid_node_IP`

ii. 输入文件中列出的密码 `Passwords.txt`。

iii. 输入以下命令切换到root： `su -`

iv. 输入文件中列出的密码 `Passwords.txt`。

b. 停止MI服务： `service mi stop`

c. 停止mgmt-api服务： `service mgmt-api stop`

d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`

e. 输入文件中列出的SSH访问密码 `Passwords.txt`。

f. 出现提示时，确认要覆盖已恢复的管理节点上的 MI 数据库。

数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。

g. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

5. 重新启动源管理节点上的服务： `service servermanager start`

恢复 **StorageGRID** 主管理节点时还原 **Prometheus** 指标

或者，您也可以在出现故障的主管理节点上保留 Prometheus 维护的历史指标。只有当您的 StorageGRID 系统包含另一个管理节点时，才能还原 Prometheus 指标。

开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您已获得 `Passwords.txt`文件。
- 您具有配置密码短语。

关于此任务

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将 Prometheus 数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史指标。如果您的系统只有一个主管理节点、则无法还原Prometheus数据库。

复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。
2. 从源管理节点中、停止Prometheus服务： `service prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入文件中列出的密码 `Passwords.txt`。
      iii. 输入以下命令切换到root： `su -`
      iv. 输入文件中列出的密码 `Passwords.txt`。
   b. 停止Prometheus服务： `service prometheus stop`
   c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   d. 输入文件中列出的SSH访问密码 `Passwords.txt`。
   e. 将Prometheus数据库从源管理节点复制到已恢复的管理节点：
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

      原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

   已克隆数据库，正在启动服务

   a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`
4. 在源管理节点上重新启动Prometheus服务.`service prometheus start`

使用非主管理节点从主管理节点故障中恢复

使用非主管理节点从 **StorageGRID** 主管理节点故障中恢复

必须完成一组特定任务，才能使用非主管理节点从主管理节点故障恢复。主管理节点托管网格的配置管理节点 (CMN) 服务。

按照以下高级步骤使用非主管理节点恢复主管理节点：

1. "从发生故障的主管理节点复制审核日志"
2. "更换主管理节点"
3. "选择"开始恢复"以配置主管理节点"
4. "确定主管理节点的修补程序要求"
5. "在已恢复的主管理节点上还原审核日志"
6. "恢复主管理节点时还原 Prometheus 指标"

从发生故障的主管理节点复制 **StorageGRID** 审核日志

如果您能够从出现故障的主管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的主管理节点启动并运行后将保留的审核日志还原到该节点。

关于此任务

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

> 如果现在无法在故障管理节点上访问审核日志、您可以稍后访问这些日志、例如、在主机恢复之后。

步骤

1. 如果可能，请登录到发生故障的主管理节点。否则，登录到任何可用的管理节点。
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令以切换到 root 用户帐户： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 停止AMS服务以防止其创建新日志文件：`service ams stop`
3. 导航到审核导出目录：

   ```
   cd /var/local/audit/export
   ```

   （或者 `cd /var/local/log`在早期系统上）
4. 将源日志文件重命名为唯一编号的文件名。

   > ◦ 如果日志文件位于 `/var/local/audit/export`目录，其名称是 `audit.log`。
   > ◦ 如果日志文件位于 `/var/local/log`目录，其名称是 `localaudit.log`。

例如，重命名 `localaudit.log`文件到 `2025-10-22.txt.1`。

```
ls -l
mv localaudit.log 2025-10-22.txt.1
```

5. 重新启动AMS服务： `service ams start`
6. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入管理员用户帐户的密码。

7. 将所有审核日志文件复制到临时位置： `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   出现提示时，输入管理员用户帐户的密码。

8. 以 root 用户身份注销： `exit`。

使用非主管理节点替换 **StorageGRID** 主管理节点

要恢复主管理节点，必须先更换物理或虚拟硬件。

- 您可以将发生故障的主管理节点替换为在同一平台上运行的主管理节点。
- 您可以将 VMware 或 Linux 主机上运行的主管理节点替换为 StorageGRID 服务设备上托管的主管理节点。
- 您可以将 VMware 主机上运行的主管理节点替换为 SG1000 或 SG100 服务设备。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将引导您进入主管理节点恢复的下一步。

更换平台	操作步骤
VMware	"用恢复节点替换 VMware 节点" "将 VMware 节点替换为 SG1000 或 SG100 服务设备"
Linux	"更换 Linux 节点"
服务设备	"更换服务设备"
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照的过程进行操作"更换Linux节点"。

选择"开始恢复"以配置主管理节点

替换主管理节点后，必须在 Grid Manager 中选择 Start Recovery，将新节点配置为故障节

点的替换节点。

开始之前

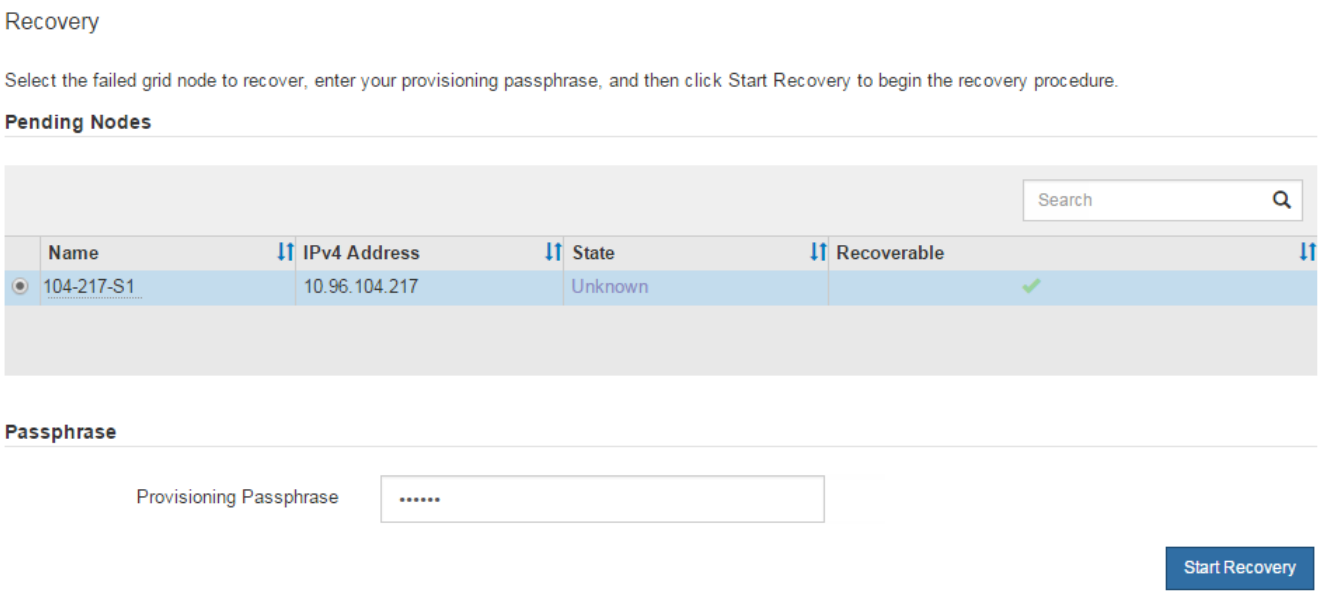
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您已部署并配置替代节点。

步骤

1. 在网格管理器中，选择*Maintenance* > **Tasks** > **Node recovery**。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点发生故障后会显示在列表中、但您无法选择某个节点、直到它重新安装并准备好进行恢复为止。

3. 输入 **Provisioning passphrase**。
4. 选择*Start recovery*。



5. 在恢复网格节点表中监控恢复进度。

   在恢复过程运行时，您可以选择 **Reset** 以开始新的恢复。将显示一个对话框，指示如果重置过程，节点将保持不确定状态。

   如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

   - * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
   - **Linux**：通过在Linux主机上运行以下命令来重新启动节点： `storagegrid node force-recovery node-name`
   - 设备：如果要在重置过程后重试恢复，则必须通过在该节点上运行将该设备节点还原到预安装状态 `sgareinstall`。请参阅。 "准备要重新安装的设备（仅限平台更换）"

6. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

> 要配置信赖方信任，请参阅"配置单点登录"。要访问默认服务器证书，请登录管理节点的命令 shell。前往 `/var/local/mgmt-api`目录，然后选择 `server.crt`文件。

确定主管理节点的 **StorageGRID** 修补程序要求

恢复主管理节点后，确定是否需要应用修补程序。

开始之前

主管理节点恢复完成。

步骤

1. 使用登录到网格管理器"支持的 Web 浏览器"。
2. 选择*节点*。
3. 从左侧列表中，选择主管理节点。
4. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。
5. 选择任何其他网格节点。
6. 在"概述"选项卡上，记录 软件版本 字段中显示的版本。
   - 如果“软件版本”字段中显示的版本相同，则不需要应用修补程序。
   - 如果“软件版本”字段中显示的版本不同，则必须"应用修补程序"将已恢复的主管理节点更新为相同的版本。

在恢复的主管理节点上还原 **StorageGRID** 审核日志

如果能够保留故障主管理节点中的审核日志，则可以将其复制到要恢复的主管理节点。

开始之前

- 已恢复的管理节点已安装并正在运行。
- 在原始管理节点出现故障后、您已将审核日志复制到其他位置。

关于此任务

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点、并且无法从故障节点复制审核日志、则恢复的管理节点会开始将事件记录到审核日志中、就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：

- 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
- 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。

看"配置日志管理和外部系统日志服务器"了解详情。

步骤

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

   以root用户身份登录后，提示符将从更 `$`改为 `#`。
2. 检查哪些审计文件已被保存： `cd /var/local/audit/export`
3. 将保留的审核日志文件复制到已恢复的管理节点： `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   出现提示时，输入 admin 的密码。
4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复的管理节点上的审计日志文件的用户和组设置： `chown ams-user:bycast *`
6. 以root身份注销： `exit`

恢复 **StorageGRID** 主管理节点时还原 **Prometheus** 指标

或者，您也可以在出现故障的主管理节点上保留 Prometheus 维护的历史指标。只有当您的 StorageGRID 系统包含另一个管理节点时，才能还原 Prometheus 指标。

开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您已获得 `Passwords.txt`文件。
- 您具有配置密码短语。

关于此任务

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将 Prometheus 数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史指标。如果您的系统只有一个主管理节点、则无法还原Prometheus数据库。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。
2. 从源管理节点中、停止Prometheus服务： `service prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入文件中列出的密码 `Passwords.txt`。
      iii. 输入以下命令切换到root： `su -`
      iv. 输入文件中列出的密码 `Passwords.txt`。
   b. 停止Prometheus服务： `service prometheus stop`
   c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   d. 输入文件中列出的SSH访问密码 `Passwords.txt`。
   e. 将Prometheus数据库从源管理节点复制到已恢复的管理节点：
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

      原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

   已克隆数据库，正在启动服务

   a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`
4. 在源管理节点上重新启动Prometheus服务.`service prometheus start`

从非主管理节点故障中恢复

从 **StorageGRID** 非主管理节点故障中恢复

要从非主管理节点故障中恢复，您必须完成以下任务。一个管理节点托管配置管理节点（

CMN ）服务，称为主管理节点。尽管可以有多个管理节点，但每个 StorageGRID 系统仅包含一个主管理节点。所有其他管理节点均为非主管理节点。

按照以下简要步骤恢复非主管理节点：

1. "从发生故障的非主管理节点复制审核日志"
2. "更换非主管理节点"
3. "选择Start Recovery (开始恢复)以配置非主管理节点"
4. "在已恢复的非主管理节点上还原审核日志"
5. "在恢复非主管理节点时还原管理节点数据库"
6. "恢复非主管理节点时还原Prometheus指标"

从失败的 **StorageGRID** 非主管理节点复制审核日志

如果您能够从出现故障的管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的非主管理节点启动并运行后将保留的审核日志还原到该节点。

此操作步骤 会将审核日志文件从故障管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。

> 如果现在无法在故障管理节点上访问审核日志、您可以稍后访问这些日志、例如、在主机恢复之后。

1. 如果可能，请登录到出现故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果有）。
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
2. 停止AMS服务以防止其创建新日志文件：`service ams stop`
3. 导航到审核导出目录：

   ```
   cd /var/local/audit/export/
   ```
4. 将源audit.log文件重命名为唯一编号的文件名。例如，将audit.log文件重命名为 `2023-10-25.txt.1`。

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. 重新启动AMS服务： `service ams start`
6. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

7. 将所有审核日志文件复制到临时位置： `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   出现提示时，输入 admin 的密码。

8. 以root身份注销： `exit`

替换 **StorageGRID** 非主管理节点

要恢复非主管理节点，必须首先更换物理或虚拟硬件。

您可以将出现故障的非主管理节点替换为在同一平台上运行的非主管理节点，也可以将 VMware 上运行的非主管理节点或 Linux 主机替换为服务设备上托管的非主管理节点。

使用与您为节点选择的替代平台匹配的操作步骤 。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将指导您执行非主管理节点恢复的下一步。

更换平台	操作步骤
VMware	"更换 VMware 节点"
Linux	"更换 Linux 节点"
服务设备	"更换服务设备"
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照的过程进行操作"更换Linux节点"。

选择"开始恢复"以配置 **StorageGRID** 非主管理节点

更换非主管理节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

开始之前

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

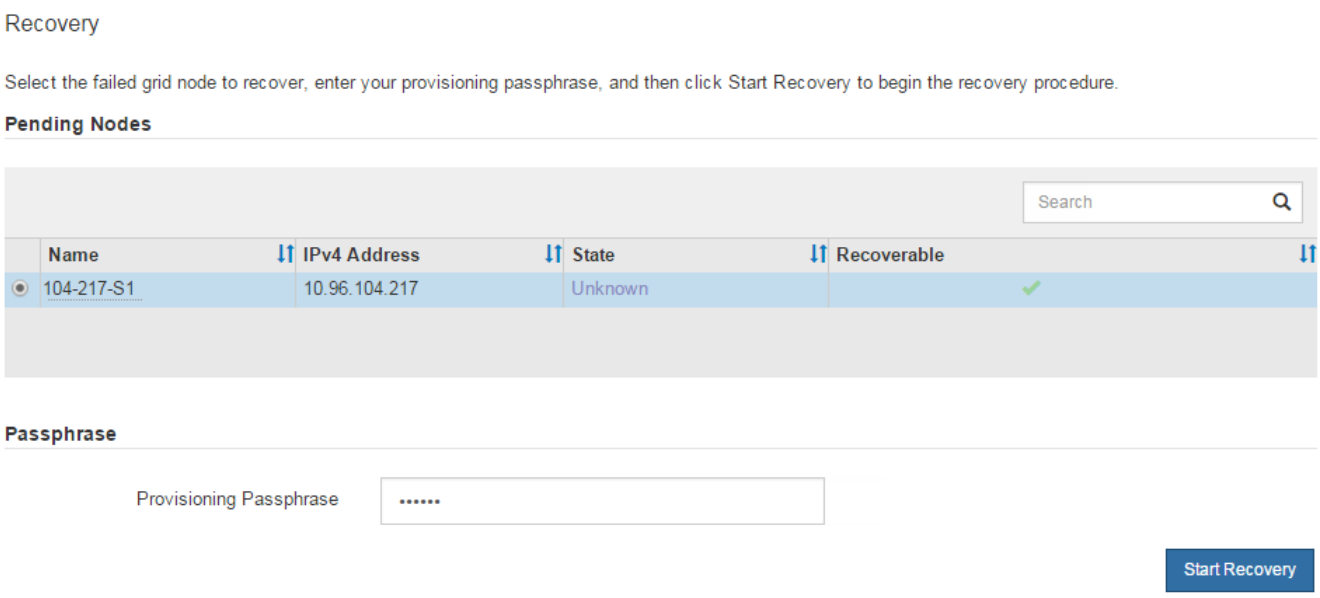
- 您具有配置密码短语。
- 您已部署并配置替代节点。

步骤

1. 在网格管理器中，选择*Maintenance* > **Tasks** > **Node recovery**。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点发生故障后会显示在列表中、但您无法选择某个节点、直到它重新安装并准备好进行恢复为止。

3. 输入 **Provisioning passphrase**。
4. 选择*Start recovery*。



5. 在恢复网格节点表中监控恢复进度。

   在恢复过程运行时，您可以选择 **Reset** 以开始新的恢复。将显示一个对话框，指示如果重置过程，节点将保持不确定状态。

   如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

   - * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
   - **Linux**：通过在Linux主机上运行以下命令来重新启动节点： `storagegrid node force-recovery node-name`
   - 设备：如果要在重置过程后重试恢复，则必须通过在该节点上运行将该设备节点还原到预安装状态 `sgareinstall`。请参阅。 "准备要重新安装的设备（仅限平台更换）"

6. 如果为 StorageGRID 系统启用了单点登录（ SSO ），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（ AD FS ）中更新（或删除并重新创建）该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。

   要配置信赖方信任，请参阅"配置单点登录"。要访问默认服务器证书，请登录管理节点的命令 shell。前往 `/var/local/mgmt-api`目录，然后选择 `server.crt`文件。

在恢复的 **StorageGRID** 非主管理节点上还原审核日志

如果您能够保留故障非主管理节点中的审核日志，以便保留历史审核日志信息，则可以将其复制到要恢复的非主管理节点。

开始之前

- 已恢复的管理节点已安装并正在运行。
- 在原始管理节点出现故障后、您已将审核日志复制到其他位置。

关于此任务

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。可以通过从出现故障的管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点、并且无法从故障节点复制审核日志、则恢复的管理节点会开始将事件记录到审核日志中、就像安装是新的一样。

您必须尽快恢复管理节点，才能还原日志记录功能。

> 默认情况下，审核信息会发送到管理节点上的审核日志。如果符合以下任一条件，则可以跳过这些步骤：
>
> - 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
> - 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。
>
> 看"配置日志管理和外部系统日志服务器"了解详情。

步骤

1. 登录到已恢复的管理节点：

   a. 输入以下命令：+
   `ssh admin@recovery_Admin_Node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   以root用户身份登录后，提示符将从更 `$`改为 `#`。

2. 检查已保留哪些审核文件：

   ```
   cd /var/local/log
   ```

3. 将保留的审核日志文件复制到已恢复的管理节点：

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   出现提示时，输入 admin 的密码。

4. 为了安全起见，请在验证审核日志是否已成功复制到已恢复的管理节点后，从出现故障的网格节点中删除这些审核日志。
5. 更新已恢复管理节点上审核日志文件的用户和组设置：

   ```
   chown ams-user:bycast *
   ```

6. 以root身份注销： `exit`

在恢复非主管理节点时还原 **StorageGRID** 管理节点数据库

如果要保留有关发生故障的非主管理节点上的属性和警报的历史信息、您可以从主管理节点还原管理节点数据库。

开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您已获得 `Passwords.txt`文件。
- 您具有配置密码短语。

关于此任务

如果管理节点出现故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 历史属性数据，用于节点页面上的图表

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统一部分或稍后添加的服务器和服务的信息。

如果还原了非主管理节点，则可以通过将管理节点数据库从主管理节点（ *source Admin Node* ）复制到恢复的节点来还原历史信息。

> 复制管理节点数据库可能需要几小时的时间。在源节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 输入以下命令切换到root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。
2. 从源管理节点运行以下命令。然后、根据提示输入配置密码短语。 `recover-access-points`
3. 从源管理节点中、停止MI服务： `service mi stop`
4. 从源管理节点中、停止管理应用程序接口(mgmt-api)服务： `service mgmt-api stop`

5. 在已恢复的管理节点上完成以下步骤：
   a. 登录到已恢复的管理节点：
      i. 输入以下命令： `ssh admin@grid_node_IP`
      ii. 输入文件中列出的密码 `Passwords.txt`。
      iii. 输入以下命令切换到root： `su -`
      iv. 输入文件中列出的密码 `Passwords.txt`。
   b. 停止MI服务： `service mi stop`
   c. 停止mgmt-api服务： `service mgmt-api stop`
   d. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
   e. 输入文件中列出的SSH访问密码 `Passwords.txt`。
   f. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`
6. 重新启动源管理节点上的服务： `service servermanager start`

恢复 **StorageGRID** 非主管理节点时还原 **Prometheus** 指标

您也可以在出现故障的非主管理节点上保留 Prometheus 维护的历史指标。

开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您已获得 `Passwords.txt`文件。
- 您具有配置密码短语。

关于此任务

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果还原了非主管理节点，则可以通过将 Prometheus 数据库从主管理节点（ *source Admin Node* ）复制到恢复的管理节点来还原历史指标。

> 复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

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

2. 从源管理节点中、停止Prometheus服务： `service prometheus stop`
3. 在已恢复的管理节点上完成以下步骤：
    a. 登录到已恢复的管理节点：
        i. 输入以下命令： `ssh admin@grid_node_IP`
        ii. 输入文件中列出的密码 `Passwords.txt`。
        iii. 输入以下命令切换到root： `su -`
        iv. 输入文件中列出的密码 `Passwords.txt`。
    b. 停止Prometheus服务： `service prometheus stop`
    c. 将 SSH 专用密钥添加到 SSH 代理。输入：`ssh-add`
    d. 输入文件中列出的SSH访问密码 `Passwords.txt`。
    e. 将Prometheus数据库从源管理节点复制到已恢复的管理节点：
    `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
    f. 出现提示时，按 * 输入 * 确认要销毁已恢复管理节点上的新 Prometheus 数据库。

        原始 Prometheus 数据库及其历史数据将复制到已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

    已克隆数据库，正在启动服务

    a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入：`ssh-add -D`
4. 在源管理节点上重新启动Prometheus服务.`service prometheus start`

从网关节点故障中恢复

替换 StorageGRID 网关节点

您可以将出现故障的网关节点更换为运行在同一物理或虚拟硬件上的网关节点，也可以将运行在 VMware 或 Linux 主机上的网关节点更换为托管在服务设备上的网关节点。

您必须遵循的节点更换操作步骤 取决于更换节点将使用的平台。完成节点更换操作步骤 （适用于所有节点类型）后，该操作步骤 将指导您执行网关节点恢复的下一步。

更换平台	操作步骤
VMware	"更换 VMware 节点"
Linux	"更换 Linux 节点"
服务设备	"更换服务设备"

更换平台	操作步骤
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后，按照的过程进行操作"更换Linux节点"。

选择 **Start Recovery** 以配置 **StorageGRID** 网关节点

更换网关节点后，您必须在网格管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

开始之前

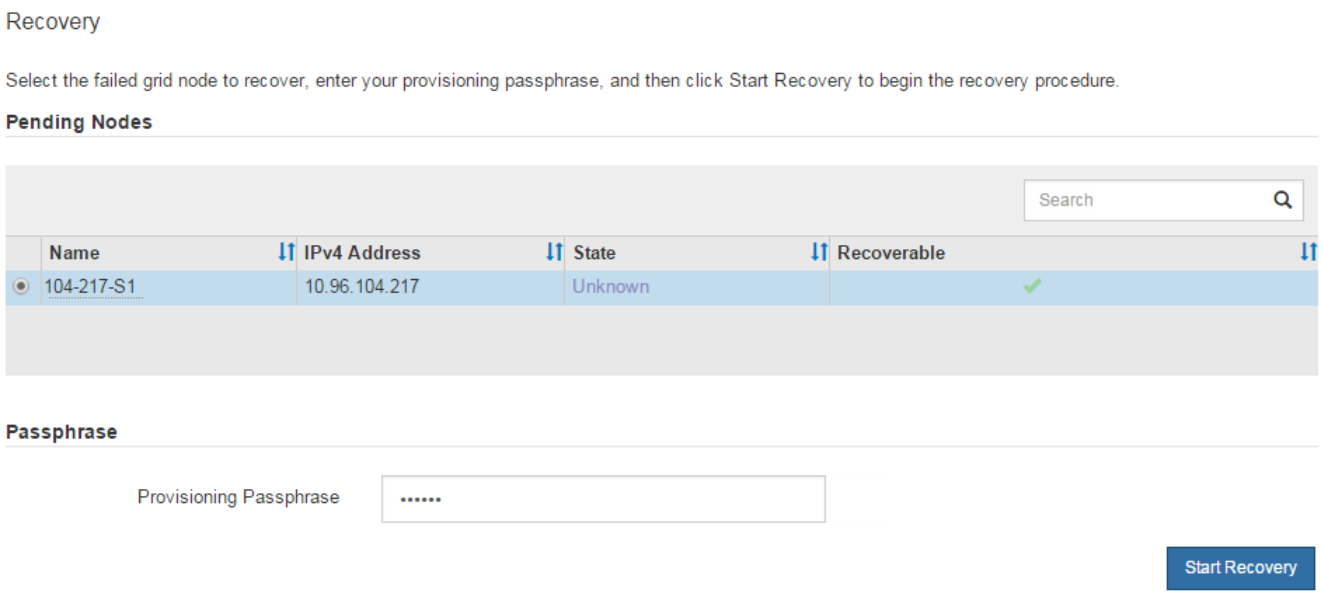
- 您已使用登录到网格管理器"支持的 Web 浏览器"。
- 您拥有"维护或root访问权限"。
- 您具有配置密码短语。
- 您已部署并配置替代节点。

步骤

1. 在网格管理器中，选择*Maintenance* > **Tasks** > **Node recovery**。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

   节点发生故障后会显示在列表中、但您无法选择某个节点、直到它重新安装并准备好进行恢复为止。

3. 输入 **Provisioning passphrase**。
4. 选择*Start recovery*。



5. 在恢复网格节点表中监控恢复进度。

在恢复过程运行时，您可以选择 **Reset** 以开始新的恢复。将显示一个对话框，指示如果重置过程，节点将保持不确定状态。

如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- * VMware * ：删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，重新部署节点。
- **Linux**：通过在Linux主机上运行以下命令来重新启动节点： `storagegrid node force-recovery node-name`
- 设备：如果要在重置过程后重试恢复，则必须通过在该节点上运行将该设备节点还原到预安装状态 `sgareinstall`。请参阅。 "准备要重新安装的设备（仅限平台更换）"

从归档节点故障中恢复

从 StorageGRID 归档节点故障中恢复

已删除对归档节点的支持。

有关恢复归档节点的信息，请参见 "从归档节点故障中恢复(StorageGRID 11.8文档站点)"。

替换Linux节点

替换 StorageGRID 中的 Linux 节点

如果发生故障需要您部署一个或多个新的物理或虚拟主机、或者在现有主机上重新安装Linux、请先部署并配置替代主机、然后才能恢复网格节点。对于所有类型的网格节点，此操作步骤 是网格节点恢复过程的一个步骤。

“Linux”指的是 Red Hat® Enterprise Linux® (RHEL)、Ubuntu® 或 Debian® 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

此过程仅作为恢复基于软件的存储节点、主管理节点或非主管理节点或网关节点过程中的一个步骤来执行。无论您要恢复的网格节点类型如何，这些步骤都是相同的。

如果在物理或虚拟 Linux 主机上托管了多个网格节点，您可以按任何顺序恢复网格节点。但是，如果主管理节点存在，您必须首先恢复它，以防止其他网格节点在尝试联系主管理节点时停止恢复。如果您无法首先恢复主管理节点，并且非主管理节点可用，您可以使用非主管理节点以任何顺序恢复节点。

为 StorageGRID 部署新的 Linux 主机

除了一些例外情况，您可以像在初始安装过程中一样准备新主机。

要部署新的或重新安装的物理或虚拟 Linux 主机，请按照适用于您的 Linux 操作系统的StorageGRID安装说明中准备主机的步骤进行操作。看"安装 Linux" 。

“Linux”指的是 RHEL、Ubuntu 或 Debian 部署。有关受支持版本的列表，请参阅 "NetApp 互操作性表工具（ IMT ）"。

此操作步骤 包含用于完成以下任务的步骤：

1. 安装 Linux 。
2. 配置主机网络。
3. 配置主机存储。
4. 安装容器引擎。
5. 安装 StorageGRID 主机服务。

> 完成安装说明中的"安装StorageGRID主机服务"任务后、请停止。请勿启动"部署网格节点"任务。

执行这些步骤时，请注意以下重要准则：

- 请确保使用与原始主机上使用的主机接口名称相同的主机接口名称。
- 如果您使用共享存储来支持StorageGRID 节点、或者已将部分或全部驱动器或SSD从出现故障的移至替代节点、则必须重新建立与原始主机上的存储映射相同的存储映射。例如、如果您按照安装说明中的建议在中使用了WWID和别名 `/etc/multipath.conf`、请确保在替代主机上的中使用相同的别名/WWID对 `/etc/multipath.conf`。
- 如果StorageGRID 节点使用从NetApp ONTAP 系统分配的存储、请确认此卷未启用FabricPool 分层策略。对 StorageGRID 节点使用的卷禁用 FabricPool 分层可简化故障排除和存储操作。

> 切勿使用 FabricPool 将与 StorageGRID 相关的任何数据分层回 StorageGRID 本身。将 StorageGRID 数据分层回 StorageGRID 会增加故障排除和操作复杂性。

将 StorageGRID 节点还原到主机

要将发生故障的网格节点还原到新的Linux主机、请执行以下步骤来还原节点配置文件。

1. 还原并验证节点还原节点配置文件。对于新安装、您需要为要安装在主机上的每个网格节点创建一个节点配置文件。将网格节点还原到替代主机时，您需要还原或替换任何出现故障的网格节点的节点配置文件。
2. 启动 StorageGRID 主机服务(英文)
3. 根据需要，恢复无法启动的所有节点。

如果从上一主机保留了任何块存储卷，则可能需要执行其他恢复过程。本节中的命令可帮助您确定需要执行的其他过程。

还原和验证网格节点

如果从非主 Admin 节点恢复节点，请将 ADMIN_IP 设置为_非主 Admin 节点_的网格网络 IP 地址，以便恢复的节点向非主 Admin 节点而不是主 Admin 节点注册。要查看管理网络密钥的规则，请参阅 "为 Linux 部署创建 StorageGRID 节点配置文件"。

您必须还原任何出现故障的网格节点的网格配置文件，然后验证网格配置文件并解决任何错误。

关于此任务

您可以导入主机上应存在的任何网格节点、但前提是其 `/var/local`卷不会因上一台主机发生故障而丢失。例如、

如果您对StorageGRID系统数据卷使用共享存储、则该 `/var/local`卷可能仍存在、如适用于Linux操作系统的StorageGRID安装说明中所述。导入节点会将其节点配置文件还原到主机。

如果无法导入缺少的节点、则必须重新创建其网格配置文件。

然后，您必须验证网格配置文件，并解决可能发生的任何网络或存储问题，然后再继续重新启动 StorageGRID 。重新创建节点的配置文件时，必须为要恢复的节点所使用的替代节点使用相同的名称。

查看"Linux 安装说明"欲了解关于 `/var/local`节点的卷。

步骤

1. 在已恢复主机的命令行中、列出当前配置的所有StorageGRID节点：`sudo storagegrid node list`

   如果未配置网格节点，则不会显示任何输出。如果配置了某些网格节点，则输出格式应为：

   ```
   Name                Metadata-Volume
   ============================================================
   dc1-adm1            /dev/mapper/sgws-adm1-var-local
   dc1-gw1             /dev/mapper/sgws-gw1-var-local
   dc1-sn1             /dev/mapper/sgws-sn1-var-local
   dc1-arc1            /dev/mapper/sgws-arc1-var-local
   ```

   如果未列出应在主机上配置的部分或全部网格节点、则需要还原缺少的网格节点。

2. 要导入具有卷的网格节点 `/var/local`、请执行以下操作：

   a. 对要导入的每个节点运行以下命令：`sudo storagegrid node import node-var-local-volume-path`

      只有在目标节点在上次运行该命令的主机上完全关闭后、该 `storagegrid node import`命令才会成功。否则，您将看到类似以下内容的错误：

      ```
      This node (node-name) appears to be owned by another host (UUID host-uuid).

   Use the --force flag if you are sure import is safe.
      ```

   a. 如果您看到有关节点属于其他主机的错误、请使用标志再次运行命令 `--force`以完成导入：`sudo storagegrid --force node import node-var-local-volume-path`

      > 使用标志导入的任何节点都 `--force`需要执行其他恢复步骤，然后才能重新加入网格，如中所述"下一步操作：如果需要，执行其他恢复步骤"。

3. 对于没有 `/var/local`卷，重新创建节点的配置文件以将其恢复到主机。有关说明，请参阅"创建节点配置文件"。

   > 重新创建节点的配置文件时，必须为要恢复的节点所使用的替代节点使用相同的名称。对于 Linux 部署，请确保配置文件名称包含节点名称。应尽可能使用相同的网络接口，块设备映射和 IP 地址。这种做法可以最大限度地减少恢复期间需要复制到节点的数据量，从而可以显著加快恢复速度（在某些情况下，只需几分钟而不是几周）。

如果在为节点重新创建配置文件时使用任何新的块设备(StorageGRID节点以前未使用的设备)作为以开头的任何配置变量的值 `BLOCK_DEVICE_`，请遵循中的指导。修复缺少的块设备错误

4. 在已恢复的主机上运行以下命令以列出所有 StorageGRID 节点。

   ```
   sudo storagegrid node list
   ```

5. 验证名称显示在 StorageGRID 节点列表输出中的每个网格节点的节点配置文件：

   ```
   sudo storagegrid node validate node-name
   ```

   在启动 StorageGRID 主机服务之前，您必须解决任何错误或警告。以下各节详细介绍了在恢复期间可能具有特殊意义的错误。

修复缺少的网络接口错误

如果主机网络配置不正确或名称拼写错误、则在StorageGRID检查文件中指定的映射时会发生错误 `/etc/storagegrid/nodes/node-name.conf`。

您可能会看到与此模式匹配的错误或警告：

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

可能会报告网格网络，管理网络或客户端网络的错误。此错误意味着该 `/etc/storagegrid/nodes/node-name.conf`文件会将指定的StorageGRID网络映射到名为的主机接口 `host-interface-name`，但当前主机上没有与该名称相同的接口。

如果收到此错误，请验证是否已完成中的步骤"部署新的 Linux 主机"。对所有主机接口使用与原始主机相同的名称。

如果您无法为主机接口命名以匹配节点配置文件，则可以编辑节点配置文件，并更改 grid_network_target ，admin_network_target 或 client_network_target 的值以匹配现有主机接口。

确保主机接口提供对相应物理网络端口或 VLAN 的访问，并且该接口不直接引用绑定或网桥设备。您必须在主机上的绑定设备上配置 VLAN （或其他虚拟接口），或者使用网桥和虚拟以太网（ veth ）对。

修复缺少的块设备错误

系统会检查每个已恢复的节点是否映射到有效的块设备专用文件或块设备专用文件的有效软链接。如果StorageGRID在文件中发现无效映射 `/etc/storagegrid/nodes/node-name.conf`、则会显示缺少块设备错误。

如果您发现与此模式匹配的错误：

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

这意味着、会 `/etc/storagegrid/nodes/*node-name*.conf`将_no-name_使用的块设备映射 `PURPOSE`到Linux文件系统中的给定路径名、但在该位置没有有效的块设备专用文件或指向块设备专用文件的软链接。

确认已完成中的步骤"部署新的 Linux 主机"。对所有块设备使用与原始主机相同的永久性设备名称。

如果您无法还原或重新创建缺少的块设备专用文件、则可以分配具有适当大小和存储类别的新块设备、并编辑节点配置文件以将的值更 `BLOCK_DEVICE_PURPOSE`改为指向新的块设备专用文件。

使用 Linux 操作系统的表格确定适当的大小和存储类别。看"存储和性能要求" 。

查看以下建议"配置主机存储"在继续进行块设备替换之前。

> 如果您必须为以开头的任何配置文件变量提供新的块存储 `BLOCK_DEVICE_`设备、因为原始块设备在故障主机上丢失、请确保新块设备未格式化、然后再尝试执行进一步的恢复过程。如果您使用的是共享存储并已创建新卷，则新块设备将取消格式化。如果不确定，请对任何新的块存储设备特殊文件运行以下命令。

> 仅对新块存储设备运行以下命令。如果您认为块存储仍包含要恢复的节点的有效数据、请勿运行此命令、因为设备上的任何数据都将丢失。
>
> ```
> sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
> ```

启动 **StorageGRID** 主机服务

要启动 StorageGRID 节点并确保它们在主机重新启动后重新启动，您必须启用并启动 StorageGRID 主机服务。

步骤

1. 在每个主机上运行以下命令：

   ```
   sudo systemctl enable storagegrid
   sudo systemctl start storagegrid
   ```

2. 运行以下命令以确保部署正在进行：

   ```
   sudo storagegrid node status node-name
   ```

3. 如果任何节点返回状态"Nnot running"(未运行)或"STOPPEed"(已停止)、请运行以下命令：

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

4. 如果您先前已启用并启动 StorageGRID 主机服务（或者不确定此服务是否已启用和启动），请同时运行以下命令：

```
sudo systemctl reload-or-restart storagegrid
```

恢复无法正常启动的节点

如果StorageGRID 节点未正常重新加入网格且未显示为可恢复、则可能已损坏。您可以强制节点进入恢复模式。

步骤

1. 确认节点的网络配置是否正确。

   由于网络接口映射不正确或网格网络IP地址或网关不正确、此节点可能无法重新加入网格。

2. 如果网络配置正确、请发出 `force-recovery`命令：

   `sudo storagegrid node force-recovery node-name`

3. 对节点执行其他恢复步骤。请参阅。 "下一步操作：如果需要，执行其他恢复步骤"

执行其他 StorageGRID 节点恢复步骤

根据您为使 StorageGRID 节点在替代主机上运行而采取的特定操作，您可能需要对每个节点执行其他恢复步骤。

如果在更换 Linux 主机或将故障网格节点还原到新主机时不需要采取任何更正操作，则节点恢复已完成。

更正操作和后续步骤

在更换节点期间、您可能需要执行以下更正操作之一：

- 您必须使用 `--force`标志导入节点。
- 对于任何 `<PURPOSE>`，配置文件变量的值 `BLOCK_DEVICE_<PURPOSE>`是指不包含与主机发生故障前相同的数据的块设备。
- 您为此节点发出的命令 `storagegrid node force-recovery node-name`。
- 您添加了一个新的块设备。

如果您采取了上述 * 任何 * 更正操作，则必须执行其他恢复步骤。

恢复类型	下一步
主管理节点	• "选择"开始恢复"以配置主管理节点" • "使用非主管理节点恢复主管理节点"
非主管理节点	"选择 Start Recovery 以配置非主管理节点"
网关节点	"选择 Start Recovery 以配置网关节点"
存储节点（基于软件）： • 如果必须使用 `--force`标志导入节点、或者您发出了 `storagegrid node force-recovery node-name` • 如果您必须执行完整节点重新安装，或者需要还原 /var/local	"选择启动恢复以配置存储节点"
存储节点（基于软件）： • 添加新块设备时。 • 如果对于任何 <PURPOSE>，配置文件变量的值 `BLOCK_DEVICE_<PURPOSE>`引用的块设备所包含的数据与主机发生故障前的数据不同。	"从系统驱动器完好无损的存储卷故障中恢复"

将 StorageGRID 中的 VMware 节点替换为恢复节点

在恢复VMware上托管的故障StorageGRID 节点时、您需要删除故障节点并部署恢复节点。

开始之前

您已确定虚拟机无法还原、必须进行更换。

关于此任务

您可以使用 VMware vSphere Web Client 首先删除与故障网格节点关联的虚拟机。然后，您可以部署新的虚拟机。

此操作步骤 只是网格节点恢复过程中的一个步骤。所有VMware节点的节点删除和部署过程都相同、包括管理节点、存储节点和网关节点。

步骤

1. 登录到 VMware vSphere Web Client 。
2. 导航到出现故障的网格节点虚拟机。
3. 记下部署恢复节点所需的所有信息。

a. 右键单击虚拟机，选择 * 编辑设置 * 选项卡，并记下正在使用的设置。

b. 选择 * vApp 选项 * 选项卡以查看和记录网格节点网络设置。

4. 如果发生故障的网格节点是存储节点，请确定用于数据存储的任何虚拟硬盘是否完好无损，并保留这些虚拟硬盘以重新连接到已恢复的网格节点。

5. 关闭虚拟机。

6. 选择 * 操作 * > * 所有 vCenter 操作 * > * 从磁盘中删除 * 以删除虚拟机。

7. 部署一个新的虚拟机作为替换节点，并将其连接到一个或多个StorageGRID网络。有关说明，请参阅"将StorageGRID 节点部署为虚拟机"。

   部署节点时，您可以选择重新映射节点端口或增加 CPU 或内存设置。

   部署新节点后，您可以根据存储要求添加新的虚拟磁盘，重新连接从先前删除的故障网格节点中保留的任何虚拟硬盘，或者同时添加这两者。

8. 根据要恢复的节点类型完成节点恢复操作步骤 。

节点类型	转至
管理节点	"StorageGRID 中的主管理节点或非主管理节点恢复"
网关节点	"选择 Start Recovery 以配置网关节点"
存储节点	"选择启动恢复以配置存储节点"

将 StorageGRID 中的 VMware 节点替换为 SG1000 或 SG100

如果主管理节点作为 VMware 节点运行，则可以将其替换为 SG1000 或 SG100 服务设备。

完成并验证节点替换后，必须删除原始 VMware 节点。如果旧节点重新上线，将其保留在原位可能会导致严重的网格中断。

开始之前

- 您已确定虚拟机无法还原、必须进行更换。
- 您已确认没有正在执行的网格维护程序。
- 您已确认 SG1000 或 SG100 服务设备上的 StorageGRID 设备安装程序版本与 StorageGRID 系统的软件版本相匹配。
- 您有关于现有主管理节点的下列信息：

  节点名称：必须使用与现有主管理节点相同的节点名称安装服务设备。节点名称是主机名（系统名称）。

  IP 地址：您可以为服务设备分配与现有主管理节点相同的 IP 地址（推荐），也可以在每个网络上选择一个新的未使用 IP 地址。

- 您具有配置密码短语。

步骤 1：更换 VMware 节点

首先在网格管理器中删除现有的主管理节点。然后，使用 StorageGRID Appliance Installer 将 SG1000 或 SG100 服务设备安装为新的主管理节点，并恢复该节点。如果您使用的是新的 IP 地址，则可以在删除现有主管理节点之前安装服务设备。

使用现有 **IP** 地址

使用现有的主管理节点 IP 地址替换主管理节点。

步骤

1. 从网格管理器下载恢复包：
   a. 选择*维护* > 恢复包。
   b. 输入配置密码并下载包。
2. 登录到现有的主管理节点：
   a. 输入以下命令： `ssh admin@grid_node_IP`
   b. 输入文件中列出的密码 `Passwords.txt`。
   c. 切换到 root： `su -`
   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。
3. "从现有主管理节点复制审核日志"。
4. 停止服务器管理器和网格节点上的所有服务：

   ```
   shutdown -h now
   ```

   最多需要 15 分钟才能停止服务。
5. "安装 SG1000 或 SG100 服务设备"。
6. "部署 SG1000 或 SG100 服务设备"。
7. 选择*开始安装*后，安装大约需要十分钟才能到达*加载 StorageGRID 安装程序*步骤。

   六到七分钟后，浏览器将重定向以开始恢复。
8. 检查设备时钟是否正确。
   a. 使用 SSH 连接到端口 8022：
      i. 输入命令： `ssh -p 8022 admin@grid_node_IP`。
      ii. 切换到 root： `su -`
      iii. 输入 `netapp1!`。
   b. 验证设备时钟是否与当前 UTC 时间相差在几分钟以内。如有需要，请设置正确的日期和时间：

      ```
      date -s "DD Mon YYYY HH:MM:SS"
      ```
9. 返回 Web 浏览器并选择*恢复发生故障的主管理节点*。

10. 上传 您下载的恢复包。
11. 输入配置密码并选择*Start Recovery*。

    此时将显示恢复进度条。等待 6 到 10 分钟，以完成恢复过程并启动服务。

12. 出现提示时，登录到 Grid Manager。

使用新的 **IP** 地址

使用新的 IP 地址替换主管理节点。

步骤

1. "安装 SG1000 或 SG100 服务设备"。
2. 检查设备时钟是否正确，以避免在恢复过程中出现 NTP 错误。
   a. 使用 SSH 连接到端口 8022：
      i. 输入命令： `ssh -p 8022 admin@grid_node_IP`。
      ii. 切换到 root： `su -`
      iii. 输入 `netapp1!`。
   b. 验证设备时钟是否在当前协调世界时 (UTC) 的几分钟内。如果需要，请设置正确的日期和时间：

      ```
      date -s "DD Mon YYYY HH:MM:SS"
      ```

3. 转到 StorageGRID 设备安装程序中的*上传 StorageGRID 软件*，并检查设备上预加载的软件版本是否与网格上运行的 StorageGRID 版本相匹配。如果版本不匹配：
   a. 从 "NetApp 支持站点" 下载正确的 StorageGRID Debian 安装包。
   b. 选择*删除*以删除安装软件。
   c. 上传 `storagegrid-webscale-images-<sg-version>.deb`和 `storagegrid-webscale-images-<sgversion>.deb.md5`文件。
4. 在 StorageGRID 设备安装程序主页选项卡上，选择 **Primary Admin (with Load Balancer)** 作为节点类型。
5. 输入节点名称。节点名称必须与现有的主管理节点名称匹配。

   请勿选择*开始安装*。

6. 检查新 IP 地址的子网是否在网格网络中。如果新 IP 子网不存在，请将其添加到网格网络：
   a. 在网格管理器中，选择*维护* > 网格网络。
   b. 输入配置密码以更新子网列表。
7. 从 GRID Manager 下载恢复包：
   a. 选择*维护* > 恢复包。
   b. 输入配置密码，然后下载软件包。
8. 登录到现有的主管理节点：

a. 输入以下命令： `ssh admin@grid_node_IP`

b. 输入文件中列出的密码 `Passwords.txt`。

c. 输入以下命令切换到root： `su -`

d. 输入文件中列出的密码 `Passwords.txt`。

当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

9. "从现有主管理节点复制审核日志"。

10. 停止服务器管理器和网格节点上的所有服务：

```
service servermanager stop
```

最多需要 15 分钟才能停止服务。

11. 在 StorageGRID Appliance Installer 主页选项卡上：

a. 验证以下设置：

- 节点类型设置为 **Primary Admin (with Load Balancer)**
- 节点名称与现有主管理节点名称匹配

b. 记录新的 IP 地址。

12. 选择*开始安装*。

安装大约需要 10 分钟才能到达 **Load StorageGRID installer** 步骤。

六到七分钟后，浏览器将重定向以开始恢复过程。

13. 检查设备时钟是否正确。

a. 使用 SSH 连接到端口 8022：

i. 输入命令： `ssh -p 8022 admin@grid_node_IP`。

ii. 切换到 root： `su -`

iii. 输入 `netapp1!`。

b. 验证设备时钟是否与当前 UTC 时间相差在几分钟以内。如有需要，请设置正确的日期和时间：

```
date -s "DD Mon YYYY HH:MM:SS"
```

14. 返回 Web 浏览器，然后选择*恢复发生故障的主管理节点*。

15. 上传 您下载的恢复包。

16. 输入配置密码并选择*Start Recovery*。

主管理节点恢复页面消失，然后重新出现。如果再次选择 **Start Recovery**，则会出现 `500: Internal Server Error`，因为恢复已开始，但无法将更新发送到正在使用新 IP 地址的 Grid Manager。通过更新 `/etc/hosts`文件中的主管理节点 IP 地址来解决此问题：

a. 使用 SSH 连接到端口 8022：

   i. 输入命令： `ssh -p 8022 admin@grid_node_IP`。

   ii. 切换到 root： `su -`

   iii. 输入文件中列出的密码 `Passwords.txt`。

b. 访问日志：

```
tail /var/local/log/install.log
```

   您应该会反复看到以下错误： `curl: (7) Failed to connect to <primary_Admin_Node_name> port9999: No route to host`

   这是预期的行为。StorageGRID 正在尝试使用现有的主管理节点 IP 地址将更新发送到主管理节点。

c. 验证容器是否正在运行：

```
storagegrid node status
```

```
storagegrid node enter <primary_Admin_Node_name>
```

a. 在容器内的 `/etc/hosts`文件中，将现有的主管理节点 IP 地址替换为新的 IP 地址。

b. 保存文件。

c. 返回 Web 浏览器。几秒钟后，将显示恢复进度条。

   等待6到10分钟，以完成恢复过程并启动服务。

17. 出现提示时，登录到 Grid Manager。

18. 更新恢复软件包：

a. 登录到主管理节点：

   i. 输入以下命令： `ssh admin@primary_Admin_Node_IP`

   ii. 切换到 root： `su -`

   iii. 输入以下命令： `change-ip`

b. 选择选项 **3 – Edit admin network subnet lists**，然后添加新子网。

StorageGRID 自动生成包含新主管理节点 IP 地址的新恢复包。

19. 从 Grid Manager 下载最新的恢复包。

步骤2：完成节点恢复

将现有非主管理节点用作还原过程（审核日志、管理节点数据库和 Prometheus 指标）的源管理节点。如果网格没有非主管理节点，您可以使用正在被替换的原始 VMware 节点，前提是它运行的 IP 地址与恢复的主管理节点不同。

步骤

1. "还原审核日志"。
2. "还原管理节点数据库"。
3. "还原 Prometheus 指标"。
4. 验证新的主管理节点是否正常工作。然后，立即删除原始 VM 节点或裸机容器。

将故障节点更换为服务设备

将失败的 StorageGRID 节点替换为服务设备

您可以使用服务设备恢复VMware、Linux主机或服务设备上托管的发生故障的网关节点、发生故障的非主管理节点或发生故障的主管理节点。此操作步骤 是网格节点恢复操作步骤的一个步骤。

开始之前

- 您已确定存在以下情况之一：
  - 无法还原托管此节点的虚拟机。
  - 网格节点的物理或虚拟 Linux 主机出现故障，必须更换。
  - 必须更换托管网格节点的服务设备。
- 您已确认服务设备上的StorageGRID 设备安装程序版本与StorageGRID 系统的软件版本匹配。请参阅。 "验证并升级 StorageGRID 设备安装程序版本"

> 请勿在同一站点同时部署SG110和SG1100服务设备、也不要同时部署SG100和SG1000服务设备。可能会导致性能不可预测。

关于此任务

在以下情况下、您可以使用服务设备恢复发生故障的网格节点：

- 故障节点托管在VMware或Linux上"平台变更"()
- 故障节点托管在服务设备上"平台更换"()

安装 StorageGRID 服务设备（仅限平台更改）

在恢复VMware或Linux主机上托管的发生故障的网格节点时、如果要使用服务设备作为替代节点、则必须先使用与故障节点相同的节点名称(系统名称)安装新设备硬件。

开始之前

您具有有关故障节点的以下信息：

- * 节点名称 * ： 必须使用与故障节点相同的节点名称安装服务设备。节点名称是主机名(系统名称)。
- * IP 地址 * ： 您可以为服务设备分配与故障节点相同的 IP 地址，这是首选选项，也可以在每个网络上选择新的未使用的 IP 地址。

关于此任务

只有在恢复 VMware 或 Linux 上托管的故障节点并将其替换为服务设备上托管的节点时，才执行此操作步骤 。

步骤

1. 按照说明安装新服务设备。请参阅。 "硬件安装快速入门"
2. 当系统提示您输入节点名称时，请使用故障节点的节点名称。

准备 StorageGRID 设备以重新安装（仅更换平台）

在恢复服务设备上托管的网格节点时，您必须先准备该设备以重新安装 StorageGRID 软件。

只有在更换服务设备上托管的故障节点时，才执行此操作步骤 。如果故障节点最初托管在VMware或Linux主机上、请勿执行以下步骤。

步骤

1. 登录到出现故障的网格节点：

   a. 输入以下命令： `ssh admin@grid_node_IP`

   b. 输入文件中列出的密码 `Passwords.txt`。

   c. 输入以下命令切换到root： `su -`

   d. 输入文件中列出的密码 `Passwords.txt`。

   当您以root用户身份登录时，提示符将从更 `$`改为 `#`。

2. 准备用于安装 StorageGRID 软件的设备。输入： `sgareinstall`
3. 当系统提示您继续时、输入： `y`

   设备将重新启动， SSH 会话将结束。StorageGRID 设备安装程序通常需要大约 5 分钟才能投入使用，但在某些情况下，您可能需要等待长达 30 分钟。

   服务设备将重置，并且网格节点上的数据将无法再访问。在初始安装过程中配置的 IP 地址应保持不变；但是，建议您在操作步骤 完成后进行确认。

   执行命令后 `sgareinstall`、所有StorageGRID配置的帐户、密码和SSH密钥都会被删除、并生成新的主机密钥。

在服务设备上启动 StorageGRID 软件安装

要在服务设备上安装网关节点或管理节点、请使用该设备中提供的StorageGRID设备安装程序。

开始之前

- 设备安装在机架中、连接到您的网络并打开电源。
- 可以使用StorageGRID 设备安装程序为此设备配置网络链路和IP地址。
- 如果要安装网关节点或非主管理节点，则需要知道以下管理节点之一的 IP 地址：

- StorageGRID 网格的主管理节点
- 非主管理节点（如果可用），以及是否正用于恢复该节点

- 如果要使用非主管理节点恢复节点（包括主管理节点），则可以指定该管理节点的 IP 地址。
- StorageGRID 设备安装程序的"IP Configuration"(IP配置)页面上列出的所有网格网络子网都在主管理节点上的"Grid Network Subnet"(网格网络子网)列表中进行定义。

  请参阅。 "硬件安装快速入门"

- 您正在使用"支持的 Web 浏览器"。
- 您已将其中一个IP地址分配给此设备。您可以使用管理网络，网格网络或客户端网络的 IP 地址。
- 如果您要安装主管理节点，则可以使用此版本 StorageGRID 的 Ubuntu 或 Debian 安装文件。

> 在制造过程中，服务设备会预加载最新版本的 StorageGRID 软件。如果预加载的软件版本与StorageGRID 部署中使用的版本匹配、则不需要安装文件。

关于此任务

要在服务设备上安装StorageGRID软件、请执行以下操作：

- 对于主管理节点，指定节点的名称，然后上传相应的软件包（如果需要）。如果要恢复主管理节点，并且网格中有非主管理节点，则可以选择使用非主管理节点恢复节点并指定该管理节点的 IP，也可以使用当前配置安装或恢复节点。
- 对于非主管理节点或网关节点，您可以指定或确认主管理节点的 IP 地址以及节点的名称。
- 您开始安装，并等待卷配置完毕并安装软件。
- 在整个过程中，安装将暂停。要恢复安装，您必须登录到网格管理器并将待定节点配置为故障节点的替代节点。
- 配置节点后，设备安装过程将完成，设备将重新启动。

步骤

1. 打开浏览器并输入服务设备的IP地址之一。

   `https://Controller_IP:8443`

   此时将显示 StorageGRID 设备安装程序主页页面。

2. 要安装主管理节点：
   a. 在 "This Node" 部分中，对于 "* 节点类型 " ，选择 "* 主管理 * " 。
   b. 在*节点名称*字段中，输入与您正在恢复的节点相同的名称，然后选择*保存*。
   c. 从"安装模式"部分提供的两种模式中选择一种合适的模式。您可以选择 Install a node or recover this node using current configuration 方法，也可以选择 Recover this node using a non-primary Admin Node 方法。

当前配置方法

使用当前配置安装节点或恢复此节点。

i. 在安装部分，检查当前状态下列出的软件版本。如果已准备好安装的软件版本正确，请跳至 安装步骤。

ii. 如果您需要上传不同版本的软件，请在*高级*菜单下选择*上传 StorageGRID 软件*。此时将显示 Upload StorageGRID Software（上传 StorageGRID 软件）页面。

iii. 选择*浏览*以上传 StorageGRID 软件的*软件包*和*校验和文件*。文件在您选择后会自动上传。

iv. 选择*主页*返回 StorageGRID Appliance Installer 主页。

非主管理节点方法

使用非主管理节点恢复此节点。

i. 在非主管理节点IP字段中，输入要用于恢复的非主管理节点的网格网络IP地址，然后选择*保存*。

ii. 如果准备安装的软件版本正确，请跳至安装步骤。

3. 要安装网关节点或非主管理节点：

a. 在 "This Node" 部分中，对于 "* 节点类型 " ，根据要还原的节点类型选择 "* 网关 * " 或 "* 非主管理 * " 。

b. 在*节点名称*字段中，输入与您正在恢复的节点相同的名称，然后选择*保存*。

c. 在主管理节点连接部分中，确定是否需要指定主管理节点的 IP 地址。

假设主管理节点或至少一个配置了 admin_ip 的其他网格节点位于同一子网上， StorageGRID 设备安装程序可以自动发现此 IP 地址。

d. 如果未显示此 IP 地址或者您需要更改它，请指定地址：

选项	说明
手动输入 IP	a. 清除*启用管理节点发现*复选框。 b. 手动输入 IP 地址。 c. 选择 * 保存 * 。 d. 等待新IP地址的连接状态变为"就绪"。
自动发现所有已连接的主管理节点	a. 选中*启用管理节点发现*复选框。 b. 从已发现的 IP 地址列表中，选择要部署此服务设备的网格的主管理节点。 c. 选择 * 保存 * 。 d. 等待新IP地址的连接状态变为"就绪"。

4. 在 "Installation_section_steP]] 中，确认当前状态为 Ready to start installation of node name 且 * Start Installation* 按钮已启用。

   如果未启用“开始安装”按钮，您可能需要更改网络配置或端口设置。请参阅您设备的维护说明。

5. 从 StorageGRID 设备安装程序主页中，选择 开始安装。

   当前状态更改为"正在安装"，并显示监控安装页面。

   > 如果需要手动访问监视器安装页面，请从菜单栏中选择*监视器安装*。

监控 **StorageGRID** 服务设备安装

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

步骤

1. 要监控安装进度，请从菜单栏中选择*监控安装*。

   监视器安装页面显示安装进度。

   蓝色状态栏指示当前正在进行的任务。绿色状态条表示已成功完成的任务。

   > 安装程序可确保先前安装中完成的任务不会重新运行。如果要重新运行安装、则不需要重新运行的任何任务都会显示绿色状态栏和状态"已跳过"。

2. 查看前两个安装阶段的进度。

   - *1.配置存储 *

     在此阶段，安装程序将从驱动器中清除任何现有配置，并配置主机设置。

   - **2.**安装 **OS**

     在此阶段，安装程序会将 StorageGRID 的基本操作系统映像从主管理节点复制到设备，或者从主管理节点的安装包安装基本操作系统。

3. 继续监控安装进度，直到出现以下情况之一：

   - 对于设备网关节点或非主设备管理节点， * 安装 StorageGRID * 阶段将暂停，嵌入式控制台上会显示一条消息，提示您使用网格管理器在管理节点上批准此节点。
   - 对于设备主管理节点，将显示第五阶段（ Load StorageGRID 安装程序）。如果第五阶段的进度超过 10 分钟，请手动刷新页面。

4. 针对要恢复的设备网格节点类型、转到恢复过程的下一步。

恢复类型	参考
网关节点	"选择 Start Recovery 以配置网关节点"

恢复类型	参考
非主管理节点	"选择 Start Recovery 以配置非主管理节点"
主管理节点	"配置替代主管理节点"

技术支持如何恢复 StorageGRID 站点

如果整个 StorageGRID 站点出现故障或多个存储节点出现故障，您必须联系技术支持。技术支持将评估您的情况，制定恢复计划，然后按照符合您业务目标的方式恢复故障节点或站点，优化恢复时间并防止不必要的数据丢失。

站点恢复只能由技术支持执行。

StorageGRID 系统可以对各种故障进行故障恢复，您可以自行成功执行许多恢复和维护过程。但是，创建一个简单的通用站点恢复操作步骤 很困难，因为详细步骤取决于您的具体情况。例如：

- * 您的业务目标 * ：在完全丢失 StorageGRID 站点后，您应评估如何以最佳方式实现您的业务目标。例如，是否要原位重建丢失的站点？是否要在新位置更换丢失的 StorageGRID 站点？每个客户的情况都不同，您的恢复计划必须针对您的优先事项进行设计。
- 故障的确切性质：在开始站点恢复之前、请确定故障站点上的任何节点是否完好无损、或者任何存储节点是否包含可恢复的对象。如果重建包含有效数据的节点或存储卷，可能会发生不必要的数据丢失。
- 活动**ILM**策略：网格中对象副本的数量、类型和位置由活动ILM策略控制。ILM策略的具体内容可能会影响可恢复数据量以及恢复所需的特定技术。

  如果某个站点包含某个对象的唯一副本，而该站点丢失，则该对象将丢失。

- 存储分段(或容器)一致性：应用于存储分段(或容器)的一致性会影响StorageGRID是否在通知客户端对象成功装载之前将对象元数据完全复制到所有节点和站点。如果一致性值允许最终实现一致性、则某些对象元数据可能会在站点故障中丢失。这可能会影响可恢复的数据量以及恢复操作步骤 的详细信息。
- 近期变更历史：恢复操作步骤的详细信息可能会受到发生故障时是否正在执行任何维护过程或最近是否对ILM策略进行了任何更改的影响。在开始站点恢复之前，技术支持必须评估网格的最新历史记录及其当前状况。

站点恢复只能由技术支持执行。

下面概括介绍了技术支持用于恢复故障站点的过程：

1. 技术支持：
   a. 对故障进行详细评估。
   b. 与您一起审核业务目标。
   c. 根据您的具体情况制定恢复计划。
2. 如果主管理节点出现故障、技术支持将对其进行恢复。

3. 技术支持将按照以下概述恢复所有存储节点：

   a. 根据需要更换 Storage Node 硬件或虚拟机。
   b. 将对象元数据还原到故障站点。
   c. 将对象数据还原到已恢复的存储节点。

   如果对单个故障存储节点执行恢复过程，则会发生数据丢失。



当整个站点出现故障时、技术支持将使用专用命令成功还原对象和对象元数据。

4. 技术支持可恢复其他故障节点。

   恢复对象元数据和数据后、技术支持将使用标准过程恢复发生故障的网关节点或非主管理节点。

相关信息

"站点停用"

StorageGRID解决方案和资源

前往 "StorageGRID解决方案和资源"了解如何在StorageGRID环境中测试和启用应用程序。

如何使用NetApp控制台管理StorageGRID

前往 "使用NetApp控制台进行StorageGRID管理"了解如何使用 Grid Manager 从NetApp Console 管理您的StorageGRID系统，以及如何使用NetApp Console 的数据服务进行备份、数据分层等。

- BlueXP现在是NetApp控制台*

NetApp控制台建立在增强和重组的BlueXP基础之上，可在企业级内部和云环境中集中管理NetApp存储和NetApp数据服务，提供实时洞察、更快的工作流程和简化的管理，并且高度安全且合规。

有关具体变更内容，请参阅…… "NetApp控制台发行说明"。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 NetApp 、 Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

"https://www.netapp.com/company/legal/trademarks/"

专利

有关 NetApp 拥有的专利的最新列表，请访问：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

API 许可证

本文档不授予对StorageGRID S3 REST API 的任何许可或其他权利。使用或访问StorageGRID S3 REST API需要与NetApp签订单独的许可协议，并且受该协议约束。

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

https://library.netapp.com/ecm/ecm_download_file/ECMLP3351268

https://library.netapp.com/ecm/ecm_download_file/ECMLP3373066

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。