管理 StorageGRID

StorageGRID software

NetApp
July 23, 2026

目录

管理 StorageGRID . . . 1
管理 StorageGRID . . . 1
${post_edited_translations.segment} . . . 1
开始之前 . . . 1
开始使用 Grid Manager . . . 1
StorageGRID 的 Web 浏览器要求 . . . 1
登录到 StorageGRID Grid Manager . . . 2
从 StorageGRID Grid Manager 中注销 . . . 3
更改您的 StorageGRID Grid Manager 密码 . . . 4
查看 StorageGRID 许可证信息 . . . 5
更新 StorageGRID 许可证信息 . . . 6
使用 API . . . 6
控制对 StorageGRID 的访问 . . . 26
控制 StorageGRID 访问 . . . 26
更改 StorageGRID 配置密码 . . . 27
在 StorageGRID 中更改节点控制台密码 . . . 28
更改 StorageGRID 管理节点的 SSH 访问密码 . . . 30
在 StorageGRID 中使用身份联合 . . . 32
管理 StorageGRID 中的管理员组 . . . 37
StorageGRID 中的管理组权限 . . . 40
在 StorageGRID 中管理用户 . . . 42
使用单点登录 (SSO) . . . 45
使用网格联盟 . . . 68
了解 StorageGRID 网格联合 . . . 68
了解 StorageGRID 中的帐户克隆 . . . 71
了解 StorageGRID 中的跨网格复制 . . . 73
比较 StorageGRID 中的跨网格复制和 CloudMirror 复制 . . . 79
创建 StorageGRID 网格联合连接 . . . 81
管理 StorageGRID 网格联合连接 . . . 84
管理 StorageGRID 网格联盟的允许租户 . . . 88
对 StorageGRID 中的网格联合错误进行故障排除 . . . 94
识别并重试失败的 StorageGRID 复制操作 . . . 99
管理安全 . . . 102
管理 StorageGRID 中的安全性 . . . 102
查看 StorageGRID 加密方法 . . . 103
管理证书 . . . 105
配置安全设置 . . . 133
配置密钥管理服务器 . . . 139
管理代理服务器设置 . . . 156

控制防火墙 157
管理租户 163
StorageGRID 中的租户帐户 163
创建 StorageGRID 租户帐户 164
编辑 StorageGRID 租户帐户 169
更改 StorageGRID 租户的本地 root 用户密码 170
删除 StorageGRID 租户帐户 171
管理平台服务 172
管理 StorageGRID 中租户帐户的 S3 Select 179
配置客户端连接 180
配置 S3 客户端到 StorageGRID 的连接 180
StorageGRID 中 S3 客户端的安全性 182
${post_edited_translations.segment} 184
管理 HA 组 192
管理负载平衡 202
在 StorageGRID 中配置 S3 端点域名 215
StorageGRID 客户端连接的 IP 地址和端口 216
管理网络和连接 218
配置 StorageGRID 网络设置 218
StorageGRID 网络指南 218
在 StorageGRID 中查看 IP 地址 220
在 StorageGRID 中配置 VLAN 接口 221
${post_edited_translations.segment} 225
${post_edited_translations.segment} 225
StorageGRID 中传出 TLS 连接支持的密码 232
StorageGRID 中活动、空闲和并发 HTTP 连接的优势 232
在 StorageGRID 中管理链路成本 234
使用 AutoSupport 236
了解 StorageGRID 中的 AutoSupport 236
在 StorageGRID 中配置 AutoSupport 240
手动触发 StorageGRID 中的 AutoSupport 包 243
对 StorageGRID AutoSupport 包进行故障排除 244
通过 StorageGRID 发送 E-Series AutoSupport 包 245
管理存储节点 249
使用存储选项 249
管理 StorageGRID 中的对象元数据存储 252
增加 StorageGRID 中的 Metadata Reserved Space 设置 258
压缩 StorageGRID 中存储的对象 260
在 StorageGRID 中管理完整存储节点 260
管理管理节点 261
在 StorageGRID 中使用多个管理节点 261

识别 StorageGRID 中的主管理节点 262

管理 StorageGRID

管理 StorageGRID

使用以下说明配置和管理 StorageGRID 系统。

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 创建租户帐户以允许 S3 客户端应用程序存储和检索对象
- ${post_edited_translations.segment}
- 配置 AutoSupport
- ${post_edited_translations.segment}

开始之前

- 您对 StorageGRID 系统有一个大致的了解。
- 您对 Linux 命令 shell、网络以及服务器硬件设置和配置有相当详细的了解。

开始使用 Grid Manager

StorageGRID 的 Web 浏览器要求

您必须使用受支持的网络浏览器。

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
最低	1024
最优	1280

登录到 StorageGRID Grid Manager

您可以通过在受支持的 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 系统包括一个主 Admin 节点和任意数量的非主 Admin 节点。您可以登录任何 Admin 节点上的 Grid Manager 来管理 StorageGRID 系统。但是，某些维护操作只能从主 Admin 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界面，以便在访问 Grid Manager 时，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 "${post_edited_translations.segment}"，登录步骤会略有不同。

在第一个管理节点上登录到 Grid Manager

开始之前

- 您拥有登录凭据。
- 您正在使用 "支持的 Web 浏览器"。
- Cookie 已在您的 Web 浏览器中启用。
- ${post_edited_translations.segment}
- 您有 Grid Manager 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。

  ${post_edited_translations.segment}

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO 在受限 Grid Manager 端口上不可用。必须使用端口 443。

步骤

1. 启动受支持的 Web 浏览器。
2. ${post_edited_translations.segment}
3. 如果系统提示您收到安全警报，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. ${post_edited_translations.segment}

   显示的登录屏幕取决于是否已为 StorageGRID 配置单点登录 (SSO)。

未使用**SSO**

a. ${post_edited_translations.segment}

b. 选择*登录*。

${post_edited_translations.segment}

- ${post_edited_translations.segment}

  i. 选择*登录*。您可以在"帐户"字段中保留 0。

  ii. 在组织的 SSO 登录页面上输入标准 SSO 凭据。

  例如，如果 StorageGRID 正在使用 SSO，并且您以前曾访问过网格管理器或租户帐户：

  A. 输入 **0**（Grid Manager 的帐户 ID），如果 **Grid Manager** 显示在最近帐户列表中，则选择 **Grid Manager**。

  B. 选择*登录*。

  C. ${post_edited_translations.segment}

登录后，系统将显示 Grid Manager 的主页，其中包含仪表板。要了解提供了哪些信息，请参见 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

${post_edited_translations.segment}

未使用**SSO**

步骤

1. 在浏览器的地址栏中，输入其他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. ${post_edited_translations.segment}
3. 选择*登录*。

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤

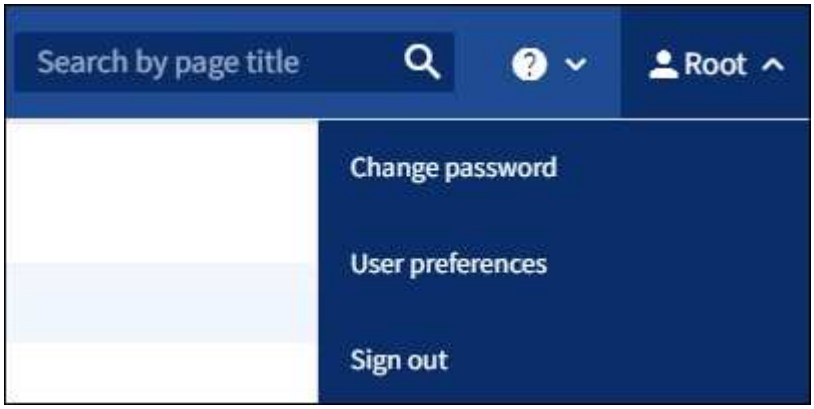
1. ${post_edited_translations.segment}
2. 如果您的SSO会话已过期，请重新输入您的凭据。

从 **StorageGRID Grid Manager** 中注销

使用完 Grid Manager 后，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，关闭浏览器可能不会使您退出系统。

步骤

1. ${post_edited_translations.segment}



2. 选择*退出*。

选项	问题描述
${post_edited_translations.segment}	${post_edited_translations.segment} 此时将显示网格管理器登录页面。 注意： 如果您登录了多个管理节点，则必须注销每个节点。
已启用 SSO	您已从正在访问的所有管理节点中登出。此时将显示 StorageGRID 登录页面。**Grid Manager** 已作为默认值列在 **Recent Accounts** 下拉列表中，且 **Account ID** 字段显示为 0。 注意： 如果启用了 SSO，并且您也登录到租户管理器，则还必须 "从租户帐户中注销" 到 "${post_edited_translations.segment}"。

更改您的 StorageGRID Grid Manager 密码

如果您是 Grid Manager 的本地用户，则可以更改自己的密码。

开始之前

您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

如果您以联合用户身份登录 StorageGRID，或者启用了单点登录 (SSO)，则无法在 Grid Manager 中更改密码。您必须在外部身份源中更改密码，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. ${post_edited_translations.segment}
3. 输入新密码。

   您的密码必须至少包含 8 个字符，最多不超过 32 个字符。密码区分大小写。

4. 重新输入新密码。
5. 选择 **Save**。

查看 StorageGRID 许可证信息

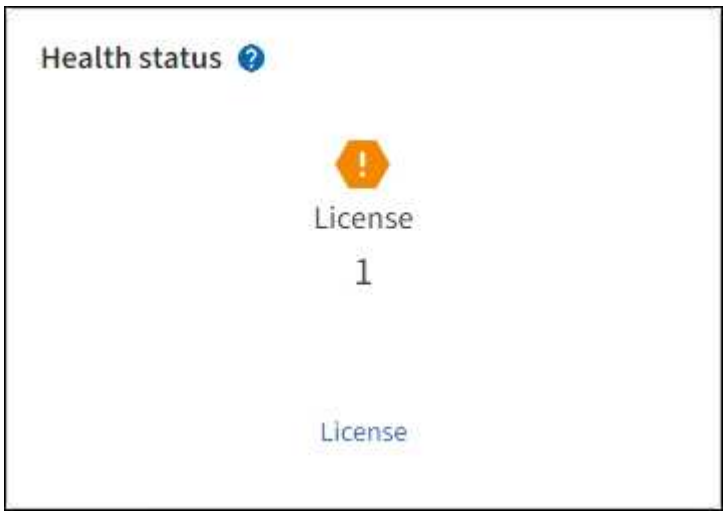
您可以随时查看 StorageGRID 系统的许可证信息，例如网格的最大存储容量。

开始之前

您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

如果此 StorageGRID 系统的软件许可证出现问题，仪表板上的运行状况状态卡包含许可证状态图标和*许可证*链接。数字表示许可证相关问题的数量。



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。
   - 在控制面板的健康状态卡中，选择"许可证状态"图标或 许可证 链接。

     只有在许可证出现问题时，此链接才会显示。
2. 查看当前许可证的只读详细信息：
   - StorageGRID 系统 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。永久许可证显示 **N/A**。
   - 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 Active IQ 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变化时随时更新 StorageGRID 系统的许可证信息。例如，如果您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要应用到 StorageGRID 系统。
- 您有 "特定访问权限"。
- 您有配置密码短语。

步骤

1. 选择*维护* > 系统 > 许可证。
2. 在"更新许可证"部分，选择 **Browse**。
3. 找到并选择新的许可证文件(`.txt`）。

   新许可证文件已验证并显示。
4. 输入配置密码。
5. 选择 **Save**。

使用 API

使用 StorageGRID 网格管理 API

您可以使用网格管理 REST API 而不是 Grid Manager 用户界面来执行系统管理任务。例如，您可能希望使用 API 来自动化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，并基于配置的组权限。
- `/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，并基于配置的组权限。私有 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略请求的 API 版本。

发出 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，允许开发人员和非开发人员使用 API 在 StorageGRID 中执行实时操作。

Swagger 用户界面为每个 API 操作提供完整的详细信息和文档。

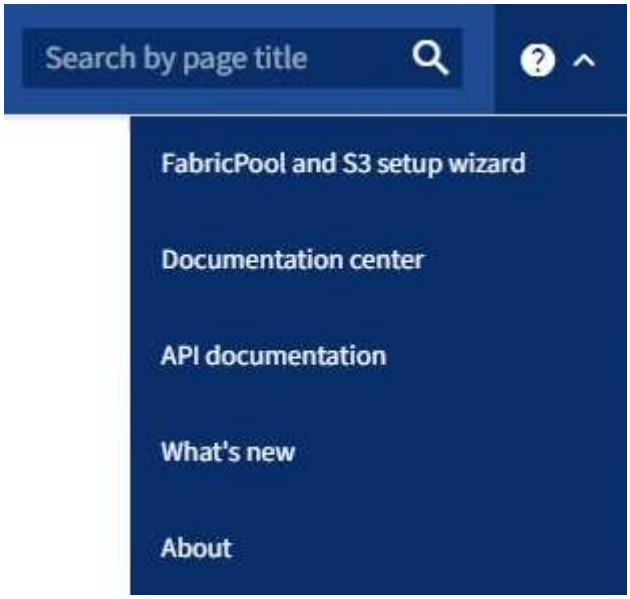
开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

> 使用 API 文档网页执行的任何 API 操作都是实时操作。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 Grid Manager 标题中，选择帮助图标，然后选择 **API documentation**。



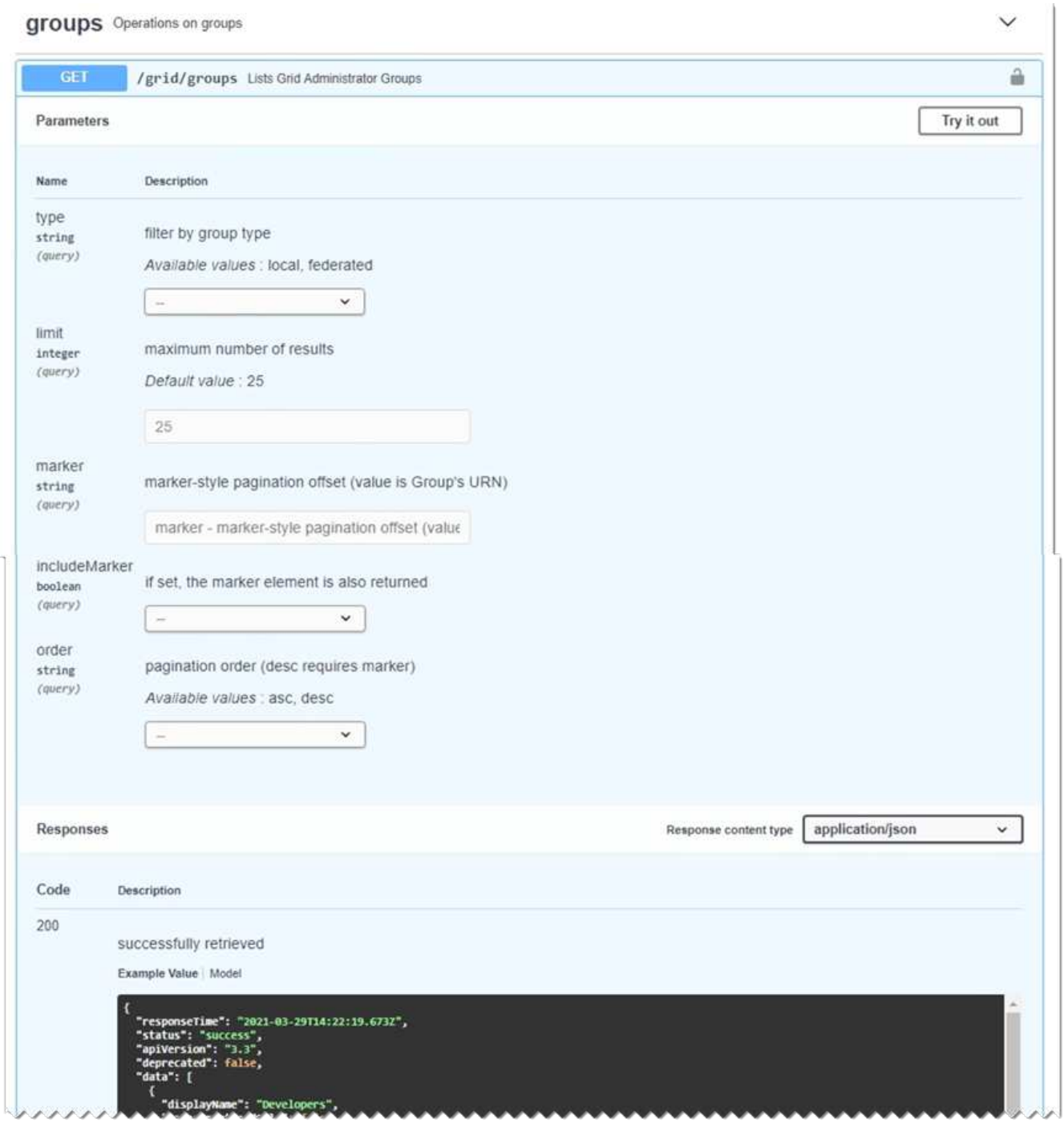
2. 要使用私有 API 执行操作，请在 StorageGRID Management API 页面上选择 转到私有 **API** 文档。

   私有 API 如有更改，恕不另行通知。StorageGRID 专用端点也会忽略请求的 API 版本。

3. 选择所需的操作。

   展开 API 操作时，可以查看可用的 HTTP 操作，例如 GET、PUT、UPDATE 和 DELETE。

4. 选择 HTTP 操作以查看请求详细信息，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。您可能需要先发出其他 API 请求，才能获取所需信息。
6. 确定是否需要修改示例请求正文。如果是，您可以选择 **Model** 以了解每个字段的要求。
7. 选择*试用*。
8. 请提供任何所需的参数，或根据需要修改请求正文。
9. ${post_edited_translations.segment}
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。

此列表仅包括公共 API 中可用的操作。

- **accounts**：管理存储租户帐户的操作，包括创建新帐户和检索给定帐户的存储使用情况。
- **alert-history**：对已解决的警报进行操作。
- **alert-receivers**：对警报通知接收器（电子邮件）的操作。
- **alert-rules**：对警报规则的操作。
- **alert-silences**：对警报静默的操作。
- **alerts**：对警报的操作。
- **audit**：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支持承载令牌身份验证方案。若要登录，请在身份验证请求的JSON正文中提供用户名和密码（即 `POST /api/v3/authorize`）。如果用户成功通过身份验证，则返回安全令牌。此令牌必须在后续API请求的标头中提供（"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来进行身份验证。请参阅"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，请参阅"防止跨站点请求伪造"。

- **client-certificates**：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**：与产品发布和 Grid Management API 版本相关的操作。您可以列出产品发布版本以及该版本支持的 Grid Management API 的主要版本，也可以禁用 API 的已弃用版本。
- **deactivated-features**：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。
- **drive-details**：针对特定存储设备型号的驱动器上的操作。
- **endpoint-domain-names**：用于列出和更改 S3 端点域名的操作。
- **erasure-coding**：对纠删码配置文件的操作。
- **expansion**：扩展操作（过程级）。
- **expansion-nodes**：扩展上的操作（节点级）。
- **expansion-sites**：扩展操作（站点级）。
- **grid-networks**：列出和更改网格网络列表的操作。
- **grid-passwords**：网格密码管理的操作。
- **groups**：用于管理本地网格管理员组以及从外部 LDAP 服务器检索联合网格管理员组的操作。
- **identity-source**：配置外部身份源并手动同步联合组和用户信息的操作。
- **ilm**：对信息生命周期管理 (ILM) 的操作。

- **in-progress-procedures**：检索当前正在进行的维护程序。
- **license**：检索和更新 StorageGRID 许可证的操作。
- **logs**：收集和下载日志文件的操作。v
- 指标：对 StorageGRID 指标的操作，包括在单个时间点的即时指标查询和在一定时间范围内的范围指标查询。网格管理 API 使用 Prometheus 系统监控工具作为后端数据源。有关构造 Prometheus 查询的信息，请参阅 Prometheus 网站。

> 名称中包含 *private* 的指标仅供内部使用。这些指标可能在不同 StorageGRID 版本之间发生变化，恕不另行通知。

- **node-details**：节点详细信息上的操作。
- **node-health**：对节点健康状态的操作。
- **node-storage-state**：对节点存储状态的操作。
- **ntp-servers**：用于列出或更新外部网络时间协议 (NTP) 服务器的操作。
- **objects**：对象和对象元数据的操作。
- **recovery**：恢复过程的操作。
- **recovery-package**：下载恢复包的操作。
- **regions**：用于查看和创建区域的操作。
- **s3-object-lock**：对全局 S3 Object Lock 设置执行的操作。
- **server-certificate**：用于查看和更新 Grid Manager 服务器证书的操作。
- **snmp**：当前 SNMP 配置上的操作。
- **storage-watermarks**：存储节点水印。
- **traffic-classes**：流量分类策略的操作。
- **untrusted-client-network**：对不受信任的客户端网络配置的操作。
- 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 的版本 4。

`https://hostname_or_ip_address/api/v4/authorize`

当进行与旧版本_不兼容_的更改时，API 的主版本号将递增。当进行与旧版本_兼容_的更改时，API 的次版本号将递增。兼容的更改包括添加新端点或新属性。

以下示例说明了如何根据所做的更改类型提升 API 版本。

API 变更类型	旧版本	新版本
与旧版本兼容	2.1	2.2

API 变更类型	旧版本	新版本
与旧版本不兼容	2.1	3.0

首次安装 StorageGRID 软件时，仅启用最新版本的 API。但是，当您升级到 StorageGRID 的新功能版本时，您仍然可以访问至少一个 StorageGRID 功能版本的旧 API 版本。

> 您可以配置支持的版本。有关详细信息，请参见 Swagger API 文档的 "网格管理 API" 的 **config** 部分。将所有 API 客户端更新为使用较新版本后，应停用对较旧版本的支持。

过期的请求通过以下方式标记为已弃用：

- 响应标头为"Deprecated: true"
- JSON 响应正文包括 "deprecated": true
- 已将弃用警告添加到 nms.log。例如：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

确定当前版本支持的API版本

使用 `GET /versions` API 请求可返回支持的 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
  ]
}
```

为请求指定 API 版本

您可以使用路径参数(`/api/v4`）或标头(`Api-Version: 4`）指定 API 版本。如果同时提供这两个值，则标头值会覆盖路径值。

```
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 令牌来增强使用 Cookie 的身份验证，从而帮助防止针对 StorageGRID 的跨站点请求伪造 (CSRF) 攻击。Grid Manager 和 Tenant Manager 会自动启用此安全功能；其他 API 客户端可以选择是否在登录时启用此功能。

可以触发对其他站点（例如使用 HTTP 表单 POST）的请求的攻击者，可以使用已登录用户的 Cookie 发出某些请求。

StorageGRID 通过使用 CSRF 令牌来帮助抵御 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标头或特定 POST 正文参数的内容匹配。

要启用此功能，请在身份验证期间将 `csrfToken`参数设置为 `true`。默认值为 `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

如果为 true，则使用随机值设置 `GridCsrfToken` cookie 以登录到 Grid Manager，并使用随机值设置 `AccountCsrfToken` cookie 以登录到 Tenant Manager。

如果存在 Cookie，则可以修改系统状态（POST、PUT、PATCH、DELETE）的所有请求都必须包括以下内容之一：

- The `X-Csrf-Token` 标头，标头的值设置为 CSRF 令牌 cookie 的值。
- 对于接受表单编码正文的端点：一个 `csrfToken`表单编码的请求正文参数。

有关其他示例和详细信息，请参见在线 API 文档。

设置了 CSRF 令牌 cookie 的请求还将对任何期望 JSON 请求正文的请求强制执行"Content-Type: application/json"标头，作为针对 CSRF 攻击的额外保护。

如果启用了单一登录，请使用 **API**

如果已启用单一登录，请使用 **StorageGRID API**（**Active Directory**）

如果已启用 "已配置并启用单点登录(SSO)" 并将 Active Directory 用作 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，则适用以下说明。

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，则需要知道租户帐户 ID。

关于此任务

可以使用以下示例之一获取身份验证令牌：

- 该 `storagegrid-ssoauth.py` Python 脚本位于 StorageGRID 安装文件目录中（RHEL 为(`./rpms`，`./debs` 适用于 Ubuntu 或 Debian，VMware 为 `./vsphere`）。
- curl 请求的示例工作流。

  如果执行太慢，curl 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 工作流程不会保护密码免遭其他用户查看。

如果您遇到 URL 编码问题，则可能会看到错误： `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。转至第 2 步。
   - 使用 curl 请求。转到步骤 3。
2. 如果要使用 `storagegrid-ssoauth.py`脚本，请将脚本传递给 Python 解释器并运行脚本。

   出现提示时，请输入以下参数的值：
   - SSO 方法。输入 ADFS 或 adfs。
   - SSO 用户名
   - 安装 StorageGRID 的域
   - StorageGRID 的地址
   - 租户帐户 ID（如果要访问租户管理 API）。

```
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
```

   StorageGRID 授权令牌在输出中提供。您现在可以将令牌用于其他请求，类似于在未使用 SSO 的情况下使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下过程。

   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 Grid Management API，请使用 0 作为 `TENANTACCOUNTID`。

   b. 若要接收已签名的身份验证 URL，请向 `/api/v3/authorize-saml`发出 POST 请求，并从响应中删除其他 JSON 编码。

   此示例显示了针对 `TENANTACCOUNTID`的已签名身份验证 URL 的 POST 请求。结果将传递给 `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
```

   此示例的响应包括经过 URL 编码的签名 URL，但不包括附加的 JSON 编码层。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

   c. 从响应中保存 `SAMLRequest`，以便在后续命令中使用。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

   d. 从 AD FS 获取包含客户端请求 ID 的完整 URL。

   一种选择是使用上一个响应中的 URL 请求登录表单。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

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. 从响应中保存客户端请求 ID。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 将您的凭据发送到上一个响应的表单操作。

```
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，标头中包含其他信息。

> 如果您的 SSO 系统启用了多因素身份验证 (MFA)，表单提交内容中也会包含第二个密码或其他凭据。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 从响应中保存 `MSISAuth` Cookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 使用来自身份验证 POST 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，以供以后注销使用，响应正文在隐藏表单字段中包含 SAMLResponse。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 从隐藏字段中保存 `SAMLResponse`：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用保存的 `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，或者如果要登录到 Grid Management 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，您可以将 `MYTOKEN`用于其他请求，类似于在未使用 SSO 的情况下使用 API 的方式。

如果已启用单一登录，则注销 API

如果已启用单点登录 (SSO)，则必须发出一系列 API 请求以注销网格管理 API 或租户管理 API。如果您将 Active Directory 用作 SSO 身份提供程序，则适用以下说明

关于此任务

如果需要，您可以通过从组织的单点注销页面注销来退出 StorageGRID API。或者，您可以从 StorageGRID 触发单点注销 (SLO)，这需要有效的 StorageGRID 承载令牌。

步骤

1. 要生成已签名的注销请求，请将 `cookie "sso=true"` 传递给 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。重定向位置不适用于仅限 API 的注销。

```
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没有 SSO 的工作方式相同。如果未提供 `cookie "sso=true"，则用户将从 StorageGRID 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
```

A `204 No Content` 响应表示用户现已注销。

```
HTTP/1.1 204 No Content
```

如果已启用单点登录，请使用 **StorageGRID API**（**Entra ID**）

如果有"已配置并启用单点登录(SSO)"并将 Entra ID 用作 SSO 提供程序，则可以使用两个示例脚本获取对网格管理 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，请登录到 **API**

如果您使用 Entra ID 作为 SSO 身份提供商，则适用以下说明

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，则需要知道租户帐户 ID。

关于此任务

可以使用以下示例脚本获取身份验证令牌：

- The `storagegrid-ssoauth-azure.py` Python 脚本
- The `storagegrid-ssoauth-azure.js` Node.js 脚本

这两个脚本都位于 StorageGRID 安装文件目录中（RHEL 为 (`./rpms`，Ubuntu 或 Debian 为 `./debs`，VMware 为 `./vsphere`）。

要使用 Entra ID 编写自己的 API 集成，请参见 `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），并调用 Node.js 脚本与 Entra ID 交互以执行 SSO 操作。

SSO 操作可以使用一系列 API 请求执行，但这样做并不简单。Puppeteer Node.js 模块用于抓取 Entra ID SSO 接口。

如果您遇到 URL 编码问题，则可能会看到错误： `Unsupported SAML version`。

步骤

1. 安装所需的依赖项，如下：
   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（或使用参数传入）：
   ◦ 用于登录到 Entra ID 的 SSO 电子邮件地址

- StorageGRID 的地址
- 租户帐户 ID（如果要访问租户管理 API）

4. 出现提示时，请输入密码，并准备好在收到请求时向 Entra ID 提供 MFA 授权。

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> 该脚本假设 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（例如输入在短信中收到的代码）。

StorageGRID 授权令牌在输出中提供。您现在可以将令牌用于其他请求，类似于在未使用 SSO 的情况下使用 API 的方式。

如果已启用单一登录，请使用 **StorageGRID API (PingFederate)**

如果具有"已配置并启用单点登录(SSO)"并使用 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 身份提供商，则适用以下说明

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，则需要知道租户帐户 ID。

关于此任务

可以使用以下示例之一获取身份验证令牌：

- 该 `storagegrid-ssoauth.py` Python 脚本位于 StorageGRID 安装文件目录中（RHEL 为(`./rpms`，`./debs` 适用于 Ubuntu 或 Debian，VMware 为 `./vsphere`）。
- curl 请求的示例工作流。

  如果执行太慢，curl 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 工作流程不会保护密码免遭其他用户查看。

  如果您遇到 URL 编码问题，则可能会看到错误： `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。转至第 2 步。
- 使用 curl 请求。转到步骤 3。

2. 如果要使用 `storagegrid-ssoauth.py`脚本，请将脚本传递给 Python 解释器并运行脚本。

   出现提示时，请输入以下参数的值：

   - SSO 方法。您可以输入"pingfederate"的任何变体（PINGFEDERATE、pingfederate 等）。
   - SSO 用户名
   - 安装 StorageGRID 的域。此字段不用于 PingFederate。您可以将其留空或输入任何值。
   - StorageGRID 的地址
   - 租户帐户 ID（如果要访问租户管理 API）。

   ```
   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
   ```

   StorageGRID 授权令牌在输出中提供。您现在可以将令牌用于其他请求，类似于在未使用 SSO 的情况下使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下过程。

   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 Grid Management API，请使用 0 作为 `TENANTACCOUNTID`。

   b. 若要接收已签名的身份验证 URL，请向 `/api/v3/authorize-saml`发出 POST 请求，并从响应中删除其他 JSON 编码。

   此示例显示了对 TENANTACCOUNTID 的签名身份验证 URL 的 POST 请求。结果将传递到 python -m json.tool 以删除 JSON 编码。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

此示例的响应包括经过 URL 编码的签名 URL，但不包括附加的 JSON 编码层。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 从响应中保存 `SAMLRequest`，以便在后续命令中使用。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 导出响应和 cookie，并回显响应：

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 导出"pf.adapterId"值，并回显响应：

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 导出"href"值（删除尾部斜杠 /），并回显响应：

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 导出"action"值：

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. 将Cookie与凭据一起发送：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 从隐藏字段中保存 `SAMLResponse`：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 使用保存的 `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，或者如果要登录到 Grid Management 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，您可以将 `MYTOKEN`用于其他请求，类似于在未使用 SSO 的情况下使用 API 的方式。

如果已启用单一登录，则注销 API

如果已启用单点登录 (SSO)，则必须发出一系列 API 请求以注销网格管理 API 或租户管理 API。如果您使用 PingFederate 作为 SSO 身份提供商，则适用以下说明

关于此任务

如果需要，您可以通过从组织的单点注销页面注销来退出 StorageGRID API。或者，您可以从 StorageGRID 触发单点注销 (SLO)，这需要有效的 StorageGRID 承载令牌。

步骤

1. 要生成已签名的注销请求，请将 `cookie "sso=true"` 传递给 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。重定向位置不适用于仅限 API 的注销。

```
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没有 SSO 的工作方式相同。如果未提供 `cookie "sso=true"，则用户将从 StorageGRID 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
```

   A `204 No Content` 响应表示用户现已注销。

```
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。停用某项功能后，无法向任何人分配执行与该功能相关的任务的权限。

关于此任务

通过停用功能系统，您可以阻止访问 StorageGRID 系统中的某些功能。停用功能是阻止 root 用户或属于具有 **Root access** 权限的管理员组的用户使用该功能的唯一方法。

要了解此功能的实用性，请考虑以下情形：

A 公司是一家服务提供商，通过创建租户帐户来租赁其 *StorageGRID* 系统的存储容量。为了保护租户对象的安全，*A* 公司希望确保其员工在部署帐户后永远无法访问任何租户帐户。

A 公司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，*A* 公司确保管理员用户（包括 *root* 用户和属于具有*根访问权限*的组的用户）无法更改任何租户帐户的 *root* 用户密码。

步骤

1. 访问网格管理 API 的 Swagger 文档。请参阅 "使用 Grid Management API"。
2. 找到"停用功能"端点。
3. 要停用某项功能（例如 Change tenant root password），请按如下所示向 API 发送正文：

```
{ "grid": {"changeTenantRootPassword": true} }
```

请求完成后，将禁用更改租户根密码功能。用户界面中不再显示 **Change tenant root password** 管理权限，任何尝试更改租户 root 用户密码的 API 请求都将失败并显示"403 Forbidden"。

重新激活已停用的功能

默认情况下，您可以使用 Grid Management API 重新激活已停用的功能。但是，如果您想防止已停用的功能被重新激活，您可以停用 **activateFeatures** 功能本身。

activateFeatures 功能无法重新激活。如果您决定停用此功能，请注意，您将永久失去重新激活任何其他已停用功能的能力。您必须联系技术支持以恢复任何丢失的功能。

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，请将正文发送到 API，如下所示：

```
{ "grid": null }
```

此请求完成后，将重新激活所有功能，包括更改租户 root 密码功能。*更改租户 root 密码*管理权限现在显示在用户界面中，任何尝试更改租户 root 密码的 API 请求都将成功，前提是用户具有 *Root 访问权限*或*更改租户 root 密码*管理权限。

前面的示例会导致_all_已停用的功能重新激活。如果其他应保持停用状态的功能已被停用，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 用户密码"功能并继续停用 storageAdmin 管理权限，请发送此 PUT 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)、创建客户端证书和更改网格密码。

控制对 **Grid Manager** 的访问

您可以通过从身份联合服务导入组和用户，或通过设置本地组和本地用户来确定谁可以访问 Grid Manager 和网格管理 API。

使用"身份联合"可以加快设置"groups"和"用户"的速度，并允许用户使用熟悉的凭据登录 StorageGRID。如果使用 Active Directory、OpenLDAP 或 Oracle Directory Server，则可以配置身份联合。

如果要使用其他 LDAP v3 服务，请联系技术支持。

您可以通过为每个组分配不同的"权限"权限来确定每个用户可以执行哪些任务。例如，您可能希望一个组中的用

户能够管理 ILM 规则，而另一个组中的用户能够执行维护任务。用户必须至少属于一个组才能访问系统。

或者，您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 Grid Manager 或 Grid Management API 中进行任何更改或执行任何操作。

启用单点登录

StorageGRID 系统支持使用安全断言标记语言 2.0 (SAML 2.0) 标准的单点登录 (SSO)。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。您可以根据需要"更改密码短语"。

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"admin"身份登录到节点，或通过 VM/物理控制台连接登录到 root 用户。根据需要，您可以"更改节点控制台密码"针对每个节点。

更改 StorageGRID 配置密码

使用此过程更改 StorageGRID 配置密码。恢复、扩展和维护过程均需要此密码短语。下载恢复包备份时也需要此密码短语，恢复包备份中包含 StorageGRID 系统的网格拓扑信息、网格节点控制台密码和加密密钥。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- ${post_edited_translations.segment}
- 您有当前的设置密码短语。

关于此任务

许多安装和维护程序以及 "${post_edited_translations.segment}" 都需要配置密码。配置密码未在 `Passwords.txt` 文件中列出。请务必记录配置密码并将其保存在安全的位置。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 输入新的密码短语。密码短语必须包含至少 8 个且不超过 32 个字符。密码短语区分大小写。

   将配置密码短语存储在安全位置。这是安装、扩展和维护程序所必需的。

5. 重新输入新密码，然后选择*Save*。

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. 输入新的配置密码短语以下载新的恢复包。

> 更改配置密码后，必须立即下载新的恢复包。恢复包文件允许您在发生故障时还原系统。

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，用于登录到该节点。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 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 您有当前的设置密码短语。

关于此任务

您可以使用节点控制台密码通过 SSH 以"admin"身份登录到节点，或通过 VM/物理控制台连接登录到 root 用户。您可以使用以下选项之一更改节点控制台密码：

- 自动将随机密码应用到每个节点
- 指定一个全局密码并将其应用于所有节点
- 指定唯一密码并将其应用于一个或多个节点

密码存储在恢复包的更新 `Passwords.txt`文件中。密码列在文件的"Password"列中。

> 用于节点之间通信的 SSH 密钥的 "SSH 访问密码" 与节点控制台密码分开。此过程不会更改 SSH 访问密码。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 网格密码。
2. 在*更改节点控制台密码*下，选择*进行更改*。

下载当前恢复包

在更改节点控制台密码之前，请下载当前恢复包。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*下载恢复软件包*。
3. 将恢复包文件 (`.zip`) 复制到两个安全、可靠且分开的位置。

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

4. 选择 **Continue**。

提供新密码

1. 请选择要使用的密码更改方法。
   - 自动：StorageGRID 会自动为所有节点分配新的随机控制台密码。
   - **Custom**：您提供控制台密码。

自动

1. 选择 **Continue**。

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。
   - 唯一控制台密码：在一个或多个节点上应用不同的密码。
2. 如果选择*全局控制台密码*，请输入要用于所有节点的密码。
3. 如果您选择了*Unique console passwords*，请输入一个或多个节点的唯一密码。
4. 选择 **Continue**。

完成密码更改

1. 出现确认对话框时，如果您已准备好让 StorageGRID 开始更改节点控制台密码，请选择 **Yes**。

   此流程开始后，您无法取消。

   StorageGRID 生成包含新密码的新恢复包。

2. 当新的恢复包准备就绪时，选择 **Download new recovery package** 并保存恢复包。
3. 打开 `.zip`文件。
4. 确认您可以访问内容，包括 `Passwords.txt`文件，该文件包含新节点控制台密码。
5. 将新的恢复包文件 (`.zip` 复制到两个安全、可靠且独立的位置。

   不要覆盖旧的恢复软件包。

   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. 选中复选框以指示您已下载新的恢复包并验证了内容。

7. 选择 **Continue**。

   StorageGRID 更新每个节点的密码。

   如果在更新过程中出现错误，进度条会列出未能更改密码的节点数量。系统将自动在无法更改密码的任何节点上重试该过程。如果过程结束时某些节点仍未更改密码，则会出现 **Retry** 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*。

   > 重试仅更改之前密码更改尝试失败的节点上的节点控制台密码。

9. 当进度条指示没有剩余更新时，选择 **Finish**。

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 密钥通过安全的无密码身份验证访问节点。

使用 SSH 密钥以 `admin`身份登录节点，或以 root 用户身份登录虚拟机或物理控制台连接。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 您有当前的设置密码短语。

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恢复包中的 `Passwords.txt`文件中。密钥列在该文件的"密码"列中。

用于节点之间通信的 SSH 密钥有单独的 SSH 访问密码。这些密码不会通过此程序进行更改。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 网格密码。
2. 在 **Change SSH keys** 下，选择 **Make a change**。

下载当前恢复包

在更改 SSH 访问密钥之前，请下载当前恢复包。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*下载恢复软件包*。
3. 将恢复包文件 (`.zip`) 复制到两个安全、可靠且分开的位置。

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

4. 选择 **Continue**。
5. 出现确认对话框时，如果您已准备好开始更改 SSH 访问密钥，请选择 是。

   此流程开始后，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. 等待生成新的恢复包，这可能需要几分钟时间。
2. 启用下载新恢复包按钮后，选择*下载新恢复包*并将新恢复包文件(`.zip`保存到两个安全、可靠且分开的位置。
3. 下载完成后：

   a. 打开 `.zip`文件。

   b. 确认您可以访问内容，包括包含新 SSH 访问密钥的 `Passwords.txt`文件。

   c. 将新的恢复包文件 (`.zip` 复制到两个安全、可靠且独立的位置。

      不要覆盖旧的恢复软件包。

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

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，横幅消息将列出未能更改其密钥的节点数量。系统将自动在任何未能更改其密钥的节点上重试该过程。如果过程结束时某些节点仍然没有更改密钥，则会出现 **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*。

      重试仅更改在先前密钥更改尝试期间失败的节点上的 SSH 访问密钥。

5. 更改所有节点的 SSH 访问密钥后，请删除 您下载的第一个恢复包。
6. （可选）选择 **Maintenance** > **System** > **Recovery package** 以下载新恢复包的其他副本。

在 StorageGRID 中使用身份联合

使用身份联合可以更快地设置组和用户，并允许用户使用熟悉的凭据登录 StorageGRID。

为 Grid Manager 配置身份联合

如果您希望在 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 等其他系统中管理管理组和用户，则可以在 Grid Manager 中配置身份联合。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您已完成 "特定访问权限"。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  如果希望使用未列出的 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 服务器的指南。
- 如果您计划启用单一登录 (SSO)，则已阅读 "单点登录的要求和注意事项"。
- 如果您计划使用传输层安全 (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 "传出 TLS 连接支持的密码"。

关于此任务

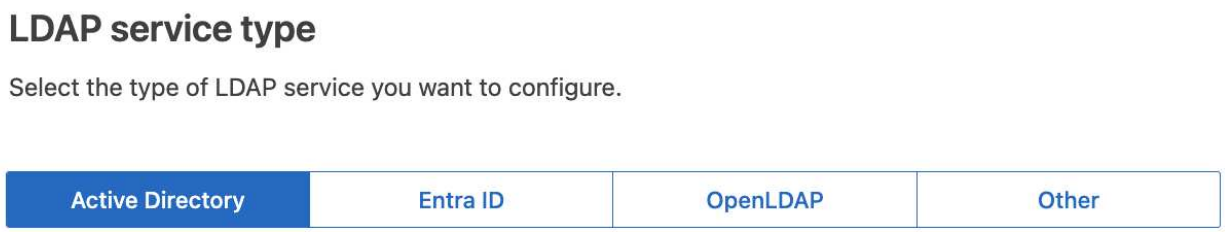
如果要从其他系统（如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）导入组，则可以为网格管理器配置身份源。您可以导入以下类型的组：

- 管理员组。管理员组中的用户可以根据分配给该组的管理权限登录到 Grid Manager 并执行任务。
- 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根据在租户管理器中分配给该组的权限登录到租户管理器并执行任务。请参阅"创建租户帐户"和"使用租户帐户"了解详情。

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，选择要配置的 LDAP 服务类型。



选择*其他*以配置使用 Oracle Directory Server 的 LDAP 服务器的值。

4. 如果您选择了*其他*，请填写 LDAP 属性部分中的字段。否则，请转至下一步。
   - 用户唯一名称：包含 LDAP 用户唯一标识符的属性名称。此属性等效于 Active Directory 的 `sAMAccountName`和 OpenLDAP 的 `uid。如果要配置 Oracle Directory Server，请输入 `uid。
   - 用户 **UUID**：包含 LDAP 用户永久唯一标识符的属性名称。此属性等效于 Active Directory 的 `objectGUID`和 OpenLDAP 的 `entryUUID。如果要配置 Oracle Directory Server，请输入 `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 位十六进制数字，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名称。此属性等效于 Active Directory 的 `sAMAccountName`和 OpenLDAP 的 `cn。如果要配置 Oracle Directory Server，请输入 `cn。
   - 组 **UUID**：包含 LDAP 组的永久唯一标识符的属性名称。此属性等效于 Active Directory 的 `objectGUID`和 OpenLDAP 的 `entryUUID。如果要配置 Oracle Directory Server，请输入 `nsuniqueid。每个组的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数字，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：将连接到 LDAP 服务器的用户的可分辨名称 (DN) 的完整路径。

     对于 Active Directory，还可以指定下层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`
     - **Entra ID**： `accountEnabled`和 `userPrincipalName`

- 密码：与用户名关联的密码。

  > 如果以后更改密码，则必须在此页面上进行更新。

- **Group Base 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，其可分辨名称相对于基本 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。

- 用户群 **DN**：要搜索用户的 LDAP 子树的标识名 (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 应使用的默认用户名模式。

  建议提供*绑定用户名格式*，因为如果 StorageGRID 无法与服务帐户绑定，它仍可允许用户登录。

  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]`
  - 辨识名模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    请按原样填写 **[USERNAME]**。

6. 在传输层安全性 (TLS) 部分，选择一个安全设置。
   - 使用 **STARTTLS**：使用 STARTTLS 保护与 LDAP 服务器的通信。这是 Active Directory、OpenLDAP 或其他选项的推荐选项，但 Microsoft Entra ID 不支持此选项。
   - 使用 **LDAPS**：LDAPS（LDAP over SSL）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。
   - 不使用 **TLS**：StorageGRID 系统与 LDAP 服务器之间的网络流量将不受保护。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. 如果选择了 STARTTLS 或 LDAPS，请选择用于保护连接的证书。
   - **Use operating system CA certificate**：使用操作系统上安装的默认网格 CA 证书来保护连接。
   - 使用自定义 **CA** 证书：使用自定义安全证书。

     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

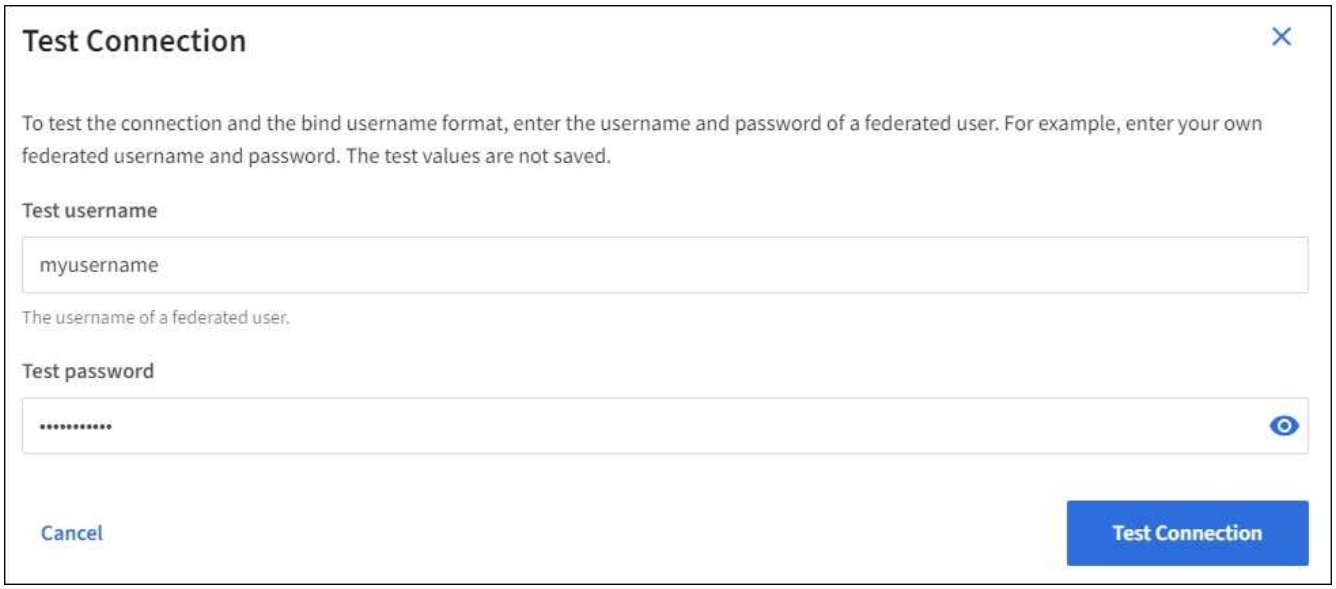
输入所有值后，必须先测试连接，然后才能保存配置。StorageGRID 验证 LDAP 服务器的连接设置以及绑定用

户名格式（如果已提供）。

步骤

1. 选择*测试连接*。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效，则会显示"Test connection successful"（测试连接成功）消息。选择 **Save** 保存配置。
   - 如果连接设置无效，将显示"无法建立测试连接"消息。选择*Close*。然后，解决任何问题并再次测试连接。
3. 如果您提供了绑定用户名格式，请输入有效的联合用户的用户名和密码。

   例如，请输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符，例如@或/。



   - 如果连接设置有效，则会显示"Test connection successful"（测试连接成功）消息。选择 **Save** 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，则会显示错误消息。请解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统定期从身份源同步联合组和用户。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. 选择页面顶端的*同步服务器*。

   同步过程可能需要一段时间，具体取决于您的环境。

   如果从身份源同步联合组和用户时出现问题，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组和用户的身份联合。禁用身份联合后，StorageGRID 与身份源之间将不再进行通信。但是，您已配置的所有设置将被保留，以便将来可以轻松重新启用身份联合。

关于此任务

在禁用身份联合之前，应注意以下事项：

- 联合用户将无法登录。
- 当前登录的联合用户将在其会话过期之前保留对 StorageGRID 系统的访问权限，但在其会话过期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，也不会针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。必须先将单点登录页面上的 SSO 状态设置为*已禁用*，然后才能禁用身份联合。请参阅 "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** 服务器的指南

如果要将 OpenLDAP 服务器用于身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于不是 Active Directory 或 Microsoft Entra ID 的身份源，StorageGRID 不会自动阻止对外部禁用的用户进行 S3 访问。要阻止 S3 访问，请删除该用户的任何 S3 密钥或从所有组中删除该用户。

Memberof和**refint**叠加层

应启用 memberof 和 refint 叠加层。有关详细信息，请参见 "OpenLDAP 文档：Version 2.4 Administrator's Guide" 中的反向组成员资格维护说明。

索引

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，请确保用户名帮助中提到的字段已编入索引，以实现最佳性能。

请参见 "OpenLDAP 文档：Version 2.4 Administrator's Guide" 中有关反向组成员资格维护的信息。

管理 StorageGRID 中的管理员组

您可以创建管理员组来管理一个或多个管理员用户的安全权限。用户必须属于某个组，才能获得对 StorageGRID 系统的访问权限。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 如果您计划导入联合组，则表示您已配置身份联合，并且该联合组已存在于配置的身份源中。

创建管理员组

管理员组允许您确定哪些用户可以访问 Grid Manager 和 Grid Management API 中的哪些功能和操作。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 管理员组。
2. 选择*创建群组*。

选择组类型

您可以创建本地组或导入联合组。

- 如果要将权限分配给本地用户，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进行更新。例如，"Maintenance Users"或"ILM Administrators"。
3. 请输入该组的唯一名称，您以后无法更新该名称。
4. 选择 **Continue**。

联合组

步骤

1. 选择*联合组*。
2. 输入要导入的组的名称，与配置的身份源中显示的名称完全相同。
   - 对于 Active Directory 和 Microsoft Entra ID，请使用 sAMAccountName。
   - 对于 OpenLDAP，请使用 CN（通用名称）。
   - 对于其他 LDAP，请使用 LDAP 服务器的适当唯一名称。
3. 选择 **Continue**。

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 Grid Manager 和 Grid Management API 中更改设置和执行操作，或者他们是否只能查看设置和功能。
   - 读写（默认）：用户可以更改设置并执行其管理权限允许的操作。
   - 只读：用户只能查看设置和功能。他们无法在 Grid Manager 或 Grid Management 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，且任何组设置为*只读*，则该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"。

   您必须为每个组分配至少一个权限；否则，属于该组的用户将无法登录 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*并*完成*。

添加用户（仅限本地组）

步骤

1. 可选地，为此组选择一个或多个本地用户。

   如果您尚未创建本地用户，则可以在不添加用户的情况下保存组。您可以在"用户"页面上将此组添加到用户。有关详细信息，请参阅 "管理用户"。

2. 选择*创建群组*并*完成*。

查看和编辑管理员组

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"页面上的表格。
- 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	${post_edited_translations.segment}	详细信息页面
查看群组详细信息	a. 选中该组的复选框。 b. 选择*操作* > 查看群组详细信息。	在表中选择组名称。
编辑显示名称（仅限本地组）	a. 选中该组的复选框。 b. 选择*操作* > 编辑组名称。 c. 输入新名称。 d. 选择 **Save changes**。	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 **Save changes**。
编辑访问模式或权限	a. 选中该组的复选框。 b. 选择*操作* > 查看群组详细信息。 c. （可选）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 **Save changes**。	a. 选择组名称以显示详细信息。 b. （可选）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 **Save changes**。

复制组

步骤

1. 选中该组的复选框。
2. 选择*操作* > 复制组。
3. 完成复制组向导。

删除组

当要从系统中删除该组时，可以删除管理组，并删除与该组关联的所有权限。删除管理组会从组中删除任何用户，但不会删除用户。

步骤

1. 在"组"页面中，选中要删除的每个组的复选框。
2. 选择*操作* > 删除组。
3. 选择*删除组*。

StorageGRID 中的管理组权限

在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 Grid Manager 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此类管理员组，以确定该用户可以执行的任务。

必须为每个组分配至少一个权限；否则，属于该组的用户将无法登录到 Grid Manager 或 Grid Management API。

默认情况下，属于至少具有一个权限的组的任何用户都可以执行以下任务：

- 登录到网格管理器
- 查看控制面板
- 查看节点页面
- ${post_edited_translations.segment}
- 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

${post_edited_translations.segment}

对于所有权限，组的“访问模式”设置决定了用户是可以更改设置并执行操作，还是只能查看相关设置和功能。如果一个用户属于多个组，且其中任何一个组被设置为“只读”，则该用户对所有选定的设置和功能将具有只读访问权限。

以下各节介绍了创建或编辑管理员组时可以分配的权限。任何未明确提及的功能都需要 **Root access** 权限。

Root 访问

此权限提供对所有网格管理功能的访问。

更改租户 **root** 密码

此权限提供对租户页面上的*更改根密码*选项的访问权限，允许您控制谁可以更改租户的本地 root 用户的密码。启用 S3 密钥导入功能时，此权限也用于迁移 S3 密钥。没有此权限的用户无法看到*更改根密码*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，还应分配*租户帐户*权限。

ILM

此权限提供对以下 **ILM** 菜单选项的访问权限：

- 规则
- 策略
- 策略标签
- 存储池
- 存储级别

- 地区
- 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这些选项：

- 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
  - 对象存在性检查
  - 恢复
- 维护 > 系统：
  - 恢复包
  - 软件更新
- 支持 > 工具：
  - 日志

${post_edited_translations.segment}

- 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 syslog 服务器

${post_edited_translations.segment}

此权限允许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默、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：

- ${post_edited_translations.segment}
- 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 仪表板卡片

对象元数据查找

此权限提供对 **ILM** > 对象元数据查找 页面的访问权限。

其他网格配置

此权限提供对以下附加网格配置选项的访问权限：

- **ILM**：
  - 存储级别
- 配置 > 系统：
- 支持 > 其他：
  - 链路成本

存储设备管理员

此权限提供：

- 通过 Grid Manager 访问存储设备上的 E 系列 SANtricity System Manager。
- 能够在支持这些操作的设备的"管理驱动器"选项卡上执行故障排除和维护任务。

租户帐户

此权限允许：

- 访问租户页面，您可以在其中创建、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网格管理器仪表板卡片

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 Grid Manager 功能。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

创建本地用户

您可以创建一个或多个本地用户，并将每个用户分配到一个或多个本地组。组的权限控制用户可以访问的 Grid Manager 和 Grid Management 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。

如果启用了单一登录 (SSO)，则本地用户无法登录到 StorageGRID。

访问此向导

步骤

1. 选择*配置* > 访问控制 > 管理员用户。
2. 选择*创建用户*。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. （可选）如果此用户无权访问 Grid Manager 或 Grid Management API，请选择 **Yes**。
3. 选择 **Continue**。

分配到组

步骤

1. ${post_edited_translations.segment}

   如果您尚未创建组，则可以在不选择组的情况下保存该用户。您可以在“组”页面上将此用户添加到组中。

   如果用户属于多个组，则权限是累积的。请参见 "管理管理员组" 了解详细信息。

2. 选择*创建用户*并选择*完成*。

${post_edited_translations.segment}

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，以更改该用户的全名、密码或组群成员身份。您还可以临时阻止用户访问 Grid Manager 和 Grid Management API。

您只能编辑本地用户。请使用外部身份源来管理联合用户。

- 若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。
- ${post_edited_translations.segment}

  ${post_edited_translations.segment}

${post_edited_translations.segment}

任务	**${post_edited_translations.segment}**	详细信息页面
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment}	在表中选择用户的名称。
编辑全名（仅限本地用户）	a. ${post_edited_translations.segment} b. 选择*操作* > 编辑全名。 c. 输入新名称。 d. 选择 **Save changes**。	a. 选择用户名以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 **Save changes**。
拒绝或允许 StorageGRID 访问	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. 选择 Access 选项卡。 d. ${post_edited_translations.segment} e. 选择 **Save changes**。	a. 选择用户名以显示详细信息。 b. 选择 Access 选项卡。 c. ${post_edited_translations.segment} d. 选择 **Save changes**。
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. 选择"密码"选项卡。 d. ${post_edited_translations.segment} e. 选择*更改密码*。	a. 选择用户名以显示详细信息。 b. 选择"密码"选项卡。 c. ${post_edited_translations.segment} d. 选择*更改密码*。
${post_edited_translations.segment}	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. ${post_edited_translations.segment} e. 选择*Edit groups*以选择不同的群组。 f. 选择 **Save changes**。	a. 选择用户名以显示详细信息。 b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. 选择*Edit groups*以选择不同的群组。 e. 选择 **Save changes**。

导入联合用户

${post_edited_translations.segment}

步骤

1. 选择*配置* > 访问控制 > 管理员用户。
2. ${post_edited_translations.segment}
3. 输入一个或多个联合用户的 UUID 或用户名。

对于多个条目，请在新行中添加每个 UUID 或用户名。

4. 选择*导入*。

如果一个或多个用户的"用户"字段导入失败，请执行以下步骤：

a. ${post_edited_translations.segment}
b. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 完成复制用户向导。

删除用户

${post_edited_translations.segment}

您无法删除 root 用户。

步骤

1. ${post_edited_translations.segment}
2. 选择*操作* > 删除用户。
3. ${post_edited_translations.segment}

使用单点登录 **(SSO)**

了解 **StorageGRID SSO**

启用单点登录(SSO)后，只有在使用组织实施的SSO登录过程对其凭据进行授权的情况下，用户才能访问网格管理器、租户管理器、网格管理API或租户管理API。本地用户无法登录StorageGRID。

StorageGRID 系统支持使用安全断言标记语言 2.0 (SAML 2.0) 标准的单点登录 (SSO)。

在启用单点登录 (SSO) 之前，请查看启用 SSO 时 StorageGRID 登录和注销流程如何受到影响。

启用 **SSO** 时登录

启用 SSO 并登录 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。

   - 如果这是您第一次在此浏览器上访问该 URL，系统会提示您输入帐户 ID。
   - 如果您以前访问过 Grid Manager 或 Tenant Manager，系统会提示您选择最近的帐户或输入帐户 ID。

   > 当您输入租户帐户的完整 URL（即，完全限定的域名或 IP 地址，后跟 `/?accountId=20-digit-account-id`）时，不会显示 StorageGRID 登录页面。相反，系统会立即将您重定向到组织的 SSO 登录页面，您可以在此处 使用 SSO 凭据登录。

2. 指示是要访问网格管理器还是租户管理器：
   - 要访问 Grid Manager，请将 **Account ID** 字段留空，输入 **0** 作为帐户 ID，或者在最近的帐户列表中显示时选择 **Grid Manager**。
   - 要访问租户管理器，请输入 20 位租户帐户 ID，或者按名称选择一个租户（如果它显示在最近的帐户列表中）。
3. 选择*登录*

   StorageGRID 将您重定向到组织的 SSO 登录页面。例如：

4. 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) 向 StorageGRID 提供身份验证响应。
   b. StorageGRID 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 Grid Manager 或 Tenant Manager，具体取决于您选择的帐户。

   > 如果无法访问服务帐户，只要您是属于具有 StorageGRID 访问权限的联合组的现有用户，您仍然可以登录。

5. 如果您有足够的权限，也可以选择访问其他管理节点，或访问 Grid Manager 或 Tenant Manager。

   您无需重新输入 SSO 凭据。

启用 SSO 时注销

为 StorageGRID 启用 SSO 后，注销时会发生什么情况取决于您登录的内容和注销位置。

步骤

1. 在用户界面的右上角找到*注销*链接。
2. 选择*退出*。

   此时将显示 StorageGRID 登录页面。最近的帐户*下拉列表已更新，包括 ***Grid Manager** 或租户的名称，以便将来可以更快地访问这些用户界面。

下表汇总了使用单个浏览器会话时注销会发生的情况。如果您已跨多个浏览器会话登录 StorageGRID，则必须分别从所有浏览器会话中注销。

如果您已登录到.....	然后您退出.....	您已退出.....
一个或多个管理节点上的 Grid Manager	任何管理节点上的 Grid Manager	所有管理节点上的 Grid Manager 注意： 如果您将 Entra ID 用于 SSO，则可能需要几分钟时间才能从所有管理节点中注销。
一个或多个管理节点上的租户管理器	任何管理节点上的租户管理器	所有管理节点上的租户管理器
网格管理器和租户管理器	Grid Manager	仅网格管理器。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 (SSO) 之前，请查看要求和注意事项。

${post_edited_translations.segment}

${post_edited_translations.segment}

- Active Directory 联合身份验证服务 (AD FS)
- ${post_edited_translations.segment}
- 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 服务类型决定了您可以实施的 SSO 类型。

已配置的**LDAP**服务类型	**SSO** 身份提供程序的选项
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

AD FS 要求

您可以使用以下任一版本的 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 (TLS) 1.2 或 1.3
- Microsoft .NET Framework，版本 3.5.1 或更高版本

Entra ID 注意事项

如果使用 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 服务器断开连接时，可能会出现登录问题。若要允许用户登录，必须还原与 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。当您为 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，将使用服务器证书作为 StorageGRID 请求的签名证书。

如果您还没有"已为管理界面配置自定义证书"，现在应该执行此操作。安装自定义服务器证书时，它将用于所有管理节点，并且可以在所有 StorageGRID 依赖方信任、企业应用程序或 SP 连接中使用。

> 不建议在依赖方信任、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。如果节点出现故障并恢复，则会生成一个新的默认服务器证书。在登录到恢复的节点之前，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。

您可以通过登录到节点的命令 shell 并转到 `/var/local/mgmt-api`目录来访问管理节点的服务器证书。自定义服务器证书名为 `custom-server.crt`。节点的默认服务器证书名为 `server.crt`。

端口要求

单点登录 (SSO) 在受限 Grid Manager 或 Tenant Manager 端口上不可用。如果希望用户使用单点登录进行身份验证，则必须使用默认 HTTPS 端口 (443)。请参阅 "控制外部防火墙的访问"。

确认联合用户可以登录到 **StorageGRID**

在启用单点登录 (SSO) 之前，必须确认至少有一个联合用户可以登录到 Grid Manager 以及任何现有租户帐户的 Tenant Manager。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 您已配置身份联盟。

步骤

1. 如果存在现有租户帐户，请确认没有任何租户正在使用自己的身份源。

启用 SSO 时，租户管理器中配置的身份源将被 Grid Manager 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 Grid Manager 身份源的帐户。

a. 登录到每个租户帐户的 Tenant Manager。
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，请确认不再需要用于此租户帐户的任何联合组，清除复选框，然后选择 **Save**。

2. 确认联合用户可以访问 Grid Manager：
   a. 在 Grid Manager 中，选择 **Configuration** > **Access control** > **Admin groups**。
   b. 请确保已从 Active Directory 身份源导入至少一个联合组，并且已为其分配了 Root 访问权限。
   c. 注销。
   d. 确认您可以作为联合组中的用户重新登录到 Grid Manager。
3. 如果存在现有租户帐户，请确认具有 Root 访问权限的联合用户可以登录：
   a. 在网格管理器中，选择*租户*。
   b. 选择租户帐户，然后选择*操作* > 编辑。
   c. 在"输入详细信息"选项卡上，选择 **Continue**。
   d. 如果选中*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. 在租户管理器中，选择*访问管理* > 组。
   g. 请确保来自 Grid Manager 的至少一个联合组已为此租户分配了 Root 访问权限。
   h. 注销。
   i. 确认可以作为联合组中的用户重新登录到租户。

相关信息

- "单点登录的要求和注意事项"
- "管理管理员组"
- "使用租户帐户"

在 **StorageGRID** 中配置 **SSO**

您可以按照配置 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 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "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，已根据计划使用的 SSO 身份提供程序选择 Active Directory 或 Entra ID。

已配置的**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 • Entra ID • PingFederate
Entra ID	Entra ID

关于此任务

启用 SSO 并且用户尝试登录管理节点时，StorageGRID 将向 SSO 身份提供程序发送身份验证请求。反过来，SSO 身份提供程序将向 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 的响应中包含该用户的通用唯一标识符 (UUID)。
- 来自 Entra ID 的响应包括用户主体名称 (UPN)。

${post_edited_translations.segment}

1. 在 StorageGRID 中配置设置。
2. 使用 SSO 身份提供程序的软件为每个管理节点创建信赖方信任 (AD FS)、企业应用程序 (Entra ID) 或服务提供商 (PingFederate)。
3. 返回 StorageGRID 以启用 SSO。

沙箱模式便于您进行这种反复配置，并在启用 SSO 之前测试所有设置。在使用沙箱模式时，用户无法使用 SSO 登录。

访问此向导

步骤

1. 选择 配置 > 访问控制 > 单点登录。此时将显示“单点登录”页面。

> 如果禁用了"配置 SSO 设置"按钮，请确认已将身份提供程序配置为联合身份源。请参阅 "单点登录的要求和注意事项"。

2. 选择*配置 SSO 设置*。此时将显示提供标识提供程序详细信息页面。

提供标识提供程序详细信息

步骤

1. 从下拉列表中选择 **SSO** 类型。
2. 如果选择 Active Directory 作为 SSO 类型，请输入身份提供程序的*联合身份验证服务名称*，与 Active Directory 联合身份验证服务 (AD FS) 中显示的完全相同。

要查找联合身份验证服务名称，请转到 Windows Server Manager。选择 **Tools** > **AD FS Management**。从操作菜单中，选择 **Edit Federation Service Properties**。联合身份验证服务名称显示在第二个字段中。

3. 指定当身份提供商响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接。
   - **Use operating system CA certificate**：使用操作系统上安装的默认 CA 证书来保护连接。
   - 使用自定义 **CA** 证书：使用自定义 CA 证书来保护连接。

     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 Certificate** 文本框中。
   - 不使用 **TLS**：不使用 TLS 证书来保护连接。

     如果更改 CA 证书，请立即 "在 Admin Nodes 上重新启动 mgmt-api 服务" 并测试是否能成功登录 Grid Manager。

4. 选择*继续*。此时将显示"提供信赖方标识符"页面。

提供依赖方标识符

1. 根据您选择的 SSO 类型，填写"提供信赖方标识符"页面上的字段。

Active Directory

a. 指定 StorageGRID 的*依赖方标识符*。此值控制您在 AD FS 中为每个依赖方信任使用的名称。

   - 例如，如果您的网格只有一个管理节点，并且您预计将来不会添加更多管理节点，请输入 `SG` 或 `StorageGRID`。
   - 如果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，系统将生成一个表，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一个依赖方信任。为每个管理节点创建依赖方信任可确保用户能够安全地登录和退出任何管理节点。

b. 选择*保存并进入沙盒模式*。

Entra ID

a. 在企业应用程序部分，为 StorageGRID 指定*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，并且您预计将来不会添加更多管理节点，请输入 `SG` 或 `StorageGRID`。
   - 如果网格包含多个管理节点，请在标识符中包含字符串 `[HOSTNAME]`。例如， `SG-[HOSTNAME]`。包含此字符串后，系统将生成一个表，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应用程序。为每个管理节点提供企业应用程序可确保用户可以安全地登录和退出任何管理节点。

b. 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。

c. 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 中对应的*联合元数据 URL* 字段中。

d. 复制并粘贴所有管理节点的联合元数据 URL 后，请选择*保存并进入沙盒模式*。

PingFederate

a. 在服务提供商 (SP) 部分，指定 StorageGRID 的 **SP** 连接 **ID**。此值控制您在 PingFederate 中为每个 SP 连接使用的名称。

   - 例如，如果您的网格只有一个管理节点，并且您预计将来不会添加更多管理节点，请输入 `SG` 或 `StorageGRID`。
   - 如果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，系统将生成一个表，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 SP 连接。为每个管理节点建立 SP 连接可确保用户能够安全地登录和退出任何管理节点。

b. 在*联合元数据 URL* 字段中为每个管理节点指定联合元数据 URL。

   使用以下格式：

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

c. 选择*保存并进入沙盒模式*。

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才能登录。

Active Directory

步骤

1. 转至 Active Directory Federation Services (AD FS)。
2. 使用"配置 SSO"页面上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。

   必须为表中显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"。

Entra ID

步骤

1. 从当前登录的管理节点的单一登录页面中，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. 登录到该节点。
   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. 从当前登录的管理节点的单一登录页面中，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. 登录到该节点。
   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. 转至 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。

   您必须为表中显示的每个管理节点创建一个 SP 连接。

测试配置

在对整个 StorageGRID 系统强制使用单点登录之前，请确认已为每个管理节点正确配置了单点登录和单点注销。

Active Directory

步骤

1. 在 Configure SSO 页面中，找到向导 Test configuration 步骤中的链接。

   URL 派生自您在 **Federation service name** 字段中输入的值。

2. 选择链接，或将 URL 复制并粘贴到浏览器中，以访问身份提供商的登录页面。
3. 要确认您可以使用 SSO 登录 StorageGRID，请选择 登录以下站点之一，为主管理节点选择依赖方标识符，然后选择 登录。
4. 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，则会显示一条成功消息。
   - 如果 SSO 操作不成功，系统将显示一条错误消息。请修复该问题，清除浏览器的 Cookie，然后重试。
5. 重复这些步骤以验证网格中每个管理节点的 SSO 连接。

Entra ID

步骤

1. 转到 Azure 门户中的"单一登录"页面。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   - 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 操作不成功，系统将显示一条错误消息。请修复该问题，清除浏览器的 Cookie，然后重试。
4. 重复这些步骤以验证网格中每个管理节点的 SSO 连接。

PingFederate

步骤

1. ${post_edited_translations.segment}

   一次选择并测试一个链接。

2. ${post_edited_translations.segment}
   - 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 操作不成功，系统将显示一条错误消息。请修复该问题，清除浏览器的 Cookie，然后重试。
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

启用单点登录

确认可以使用 SSO 登录每个管理节点后，就可以为整个 StorageGRID 系统启用 SSO。

启用 SSO 后，所有用户都必须使用 SSO 访问网格管理器、租户管理器、网格管理 API 和租户管理 API。本地用户无法再访问 StorageGRID。

步骤

1. 从配置 SSO 向导的测试配置步骤中，选择 **Enable SSO**。
2. 查看警告消息，然后选择*启用 SSO*。

   单点登录现已启用。此时将显示单一登录页面，其中包含刚刚配置的 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 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 门户用户也是已授权的 StorageGRID 用户（已导入到 StorageGRID 的联合组中的用户），或者在尝试登录 StorageGRID 之前先退出 Azure 门户。

在 **AD FS** 中为 **StorageGRID** 创建信赖方信任

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 **AD FS** 作为 SSO 类型。
- 您已在 Grid Manager 中拥有"已进入沙盒模式"。
- 您知道系统中每个管理节点的完全限定域名（或 IP 地址）和依赖方标识符。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一个依赖方信任。为每个管理节点创建依赖方信任可确保用户能够安全地登录和退出任何管理节点。

- 您具有在 AD FS 中创建依赖方信任的经验，或者您具有 Microsoft AD FS 文档的访问权限。
- 您正在使用 AD FS Management 管理单元，并且您属于 Administrators 组。
- 如果要手动创建依赖方信任，则具有为 StorageGRID 管理界面上传的自定义证书，或者您知道如何从命令 Shell 登录到管理节点。

关于此任务

这些说明适用于 Windows Server 2016 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。

使用 **Windows PowerShell** 创建信赖方信任

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*，请输入管理节点的信赖方标识符，与单一登录页面上显示的完全相同。例如， `SG-DC1-ADM1`。
   - 对于 *Admin_Node_FQDN*，请为同一个管理节点输入完全限定的域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

3. 从 Windows Server Manager 中，选择 **Tools** > **AD FS Management**。

   此时将显示AD FS管理工具。

4. 选择 **AD FS** > **Relying Party Trusts**。

   此时将显示依赖方信任列表。

5. 将访问控制策略添加到新创建的依赖方信任：
   a. 找到您刚刚创建的信赖方信任。
   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 **Apply**，然后选择 **OK**
6. 将声明颁发策略添加到新创建的信赖方信任：
   a. 找到您刚刚创建的信赖方信任。
   b. 右键单击信任，然后选择 **Edit claim issuance policy**。
   c. 选择*添加规则*。
   d. 在"选择规则模板"页面上，从列表中选择*Send LDAP Attributes as Claims*，然后选择*Next*。
   e. 在"配置规则"页面上，输入此规则的显示名称。

      例如，**ObjectGUID to Name ID** 或 **UPN to Name ID**。

   f. 对于属性存储，选择 **Active Directory**。
   g. 在 Mapping 表的 LDAP Attribute 列中，键入 **objectGUID** 或选择 **User-Principal-Name**。
   h. 在 Mapping 表的 Outgoing Claim Type 列中，从下拉列表中选择 **Name ID**。
   i. 选择*完成*，然后选择*确定*。
7. 确认已成功导入元数据。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认*端点*、*标识符*和*签名*选项卡上的字段已填充。

      如果缺少元数据，请确认联合元数据地址正确，或手动输入值。

8. 重复这些步骤，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 Management**。
2. 在操作下方，选择*添加信赖方信任*。
3. 在欢迎页面上，选择 **Claims aware**，然后选择 **Start**。
4. 选择*导入有关在线或本地网络上发布的依赖方的数据*。
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*，请为同一个管理节点输入完全限定的域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

6. 完成信赖方信任向导，保存信赖方信任，然后关闭此向导。

   输入显示名称时，请使用管理节点的信赖方标识符，与 Grid Manager 中单点登录页面上显示的完全相同。例如， `SG-DC1-ADM1`。

7. 添加声明规则：
   a. 右键单击信任，然后选择 **Edit claim issuance policy**。
   b. 选择*添加规则*：
   c. 在"选择规则模板"页面上，从列表中选择*Send LDAP Attributes as Claims*，然后选择*Next*。
   d. 在"配置规则"页面上，输入此规则的显示名称。

      例如，**ObjectGUID to Name ID** 或 **UPN to Name ID**。

   e. 对于属性存储，选择 **Active Directory**。
   f. 在 Mapping 表的 LDAP Attribute 列中，键入 **objectGUID** 或选择 **User-Principal-Name**。
   g. 在 Mapping 表的 Outgoing Claim Type 列中，从下拉列表中选择 **Name ID**。
   h. 选择*完成*，然后选择*确定*。
8. 确认已成功导入元数据。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认*端点*、*标识符*和*签名*选项卡上的字段已填充。

      如果缺少元数据，请确认联合元数据地址正确，或手动输入值。

9. 重复这些步骤，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 Management**。
2. 在操作下方，选择*添加信赖方信任*。
3. 在欢迎页面上，选择 **Claims aware**，然后选择 **Start**。
4. 选择*手动输入有关依赖方的数据*，然后选择*下一步*。
5. 完成信赖方信任向导：

   a. 输入此管理节点的显示名称。

      为了保持一致性，请使用管理节点的信赖方标识符，与 Grid Manager 中"单点登录"页面上的标识符完全相同。例如， `SG-DC1-ADM1`。

   b. 跳过此步骤以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`*，请输入管理节点的完全限定域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

   e. 在"配置标识符"页面上，为同一管理节点指定信赖方标识符：

      `Admin_Node_Identifier`

      对于 *`Admin_Node_Identifier`*，请输入管理节点的信赖方标识符，与单一登录页面上显示的完全相同。例如， `SG-DC1-ADM1`。

   f. 检查设置，保存依赖方信任，然后关闭此向导。

      ${post_edited_translations.segment}

      如果未显示此对话框，请右键单击信任，然后选择*Edit claim issuance policy*。

6. 要启动声明规则向导，请选择*添加规则*：

   a. 在"选择规则模板"页面上，从列表中选择*Send LDAP Attributes as Claims*，然后选择*Next*。

   b. 在"配置规则"页面上，输入此规则的显示名称。

      例如，**ObjectGUID to Name ID** 或 **UPN to Name ID**。

c. 对于属性存储，选择 **Active Directory**。

d. 在 Mapping 表的 LDAP Attribute 列中，键入 **objectGUID** 或选择 **User-Principal-Name**。

e. 在 Mapping 表的 Outgoing Claim Type 列中，从下拉列表中选择 **Name 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 **Endpoints** 选项卡上，为单次注销 (SLO) 配置端点：

a. 选择 **Add SAML**。

b. 选择*端点类型* > **SAML** 注销。

c. 选择*绑定* > 重定向。

d. 在 **Trusted URL** 字段中，输入用于从此管理节点单次注销 (SLO) 的 URL：

```
https://Admin_Node_FQDN/api/saml-logout
```

对于 *Admin_Node_FQDN*，请输入管理节点的完全限定域名。（如有必要，您可以使用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果该 IP 地址发生变化，您必须更新或重新创建此依赖方信任。）

a. 选择 **OK**。

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：

- 如果您有已上传到 StorageGRID 的自定义管理证书，请选择该证书。
- 如果没有自定义证书，请登录到管理节点，转到管理节点的 `/var/local/mgmt-api`目录，然后添加 `custom-server.crt`证书文件。

> 不建议使用管理节点的默认证书 (`server.crt`）。如果管理节点发生故障，则在恢复该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*。

已保存并关闭信赖方属性。

10. 重复这些步骤，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 **Entra ID** 中为 **StorageGRID** 创建企业应用程序

您可以使用 Entra ID 为系统中的每个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 "已进入沙盒模式"。
- 您拥有系统中每个管理节点的 **Enterprise application name**。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应用程序。为每个管理节点提供企业应用程序可确保用户可以安全地登录和退出任何管理节点。

- 您有在 Entra ID 中创建企业应用程序的经验。
- 您拥有一个具有有效订阅的 Entra ID 帐户。
- 您在 Entra ID 帐户中具有以下角色之一：Global Administrator、Cloud Application Administrator 、Application Administrator 或服务主体的所有者。

访问 **Entra ID**

步骤

1. 登录到 "Azure Portal"。
2. 导航到 "Entra ID"。
3. 选择 "企业应用程序"。

创建企业应用程序并保存 **StorageGRID SSO** 配置

要将 Entra ID 的 SSO 配置保存在 StorageGRID 中，您必须使用 Entra ID 为每个管理节点创建企业应用程序。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 **New application**。
   b. 选择*创建自己的应用程序*。
   c. 对于名称，请输入您从"配置 SSO"页面上的"管理节点详细信息"表中复制的*企业应用程序名称*。
   d. 保持选中*集成库中未找到的任何其他应用程序（非库）*单选按钮。
   e. 选择 **Create**。
   f. 选择 *2. 中的*开始*链接设置单点登录*框，或选择左边距中的*单点登录*链接。
   g. 选择 **SAML** 框。
   h. 复制*应用联合元数据网址*，您可以在*步骤 3 SAML 签名证书*下找到该网址。
   i. 转到"配置 SSO"页面，然后将 URL 粘贴到与您使用的*企业应用程序名称*对应的*联合元数据 URL* 字段中。
2. 为每个管理节点粘贴联合元数据 URL 并对 SSO 配置进行所有其他必要更改后，请在配置 SSO 页面上选择*保存*。

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这些步骤。
   a. 从管理节点登录到 StorageGRID。

b. 选择*配置* > 访问控制 > 单点登录。

c. 选择该按钮以下载该管理节点的 SAML 元数据。

d. 保存文件，并将其上传到 Entra ID。

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 Azure 门户。
2. 对每个企业应用程序重复以下步骤：

> 您可能需要刷新"企业应用程序"页面才能查看以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*（除非您想单独配置分配）。

c. 转到"单一登录"页面。

d. 完成 SAML 配置。

e. 选择*上传元数据文件*按钮，然后选择您为相应管理节点下载的 SAML 元数据文件。

f. 文件加载后，选择 **Save**，然后选择 **X** 关闭窗格。您将返回到"使用 SAML 设置单点登录"页面。

3. "测试每个应用程序"。

在 **PingFederate** 中为 **StorageGRID** 创建服务提供商连接

使用 PingFederate 为系统中的每个管理节点创建服务提供商 (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 **Ping Federate** 作为 SSO 类型。
- 您在 Grid Manager 中拥有 "已进入沙盒模式"。
- 您拥有系统内每个管理节点的 **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。
- ${post_edited_translations.segment}
- 您有在 PingFederate 服务器中创建 SP 连接的经验。
- 您有 "${post_edited_translations.segment}" for PingFederate Server。PingFederate 文档提供了详细的分步说明和解释。
- 您有 "${post_edited_translations.segment}" for PingFederate Server。

关于此任务

这些说明概述了如何将 PingFederate Server 10.3 版本配置为 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 these 说明。有关您所用版本的详细说明，请参阅 PingFederate Server 文档。

在 **PingFederate** 中完成先决条件

在创建用于 StorageGRID 的 SP 连接之前，您必须完成 PingFederate 中的先决条件任务。在配置 SP 连接时，您将使用这些先决条件中的信息。

${post_edited_translations.segment}

如果尚未创建，请创建一个数据存储以将 PingFederate 连接到 AD FS LDAP 服务器。使用您在 StorageGRID 中 "${post_edited_translations.segment}" 时使用的值。

- 类型：目录 (LDAP)
- **LDAP Type**：Active Directory
- ${post_edited_translations.segment}

创建密码凭据验证器

如果尚未创建，请创建密码凭据验证器。

- 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。
- ${post_edited_translations.segment}
- 搜索过滤器: sAMAccountName=${username}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

如果尚未创建，请创建一个 IdP 适配器实例。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. 选择您创建的 密码凭据验证器。
6. ${post_edited_translations.segment}
7. 选择 **Save**。

创建或导入签名证书

如果尚未创建或导入签名证书，请先执行此操作。

步骤

1. 转到 **Security** > **Signing & Decryption Keys & Certificates**。
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，您需要导入从 StorageGRID 为管理节点下载的 SAML 元数据。元数据文件包含许多您需要的特定值。

> 必须为 StorageGRID 系统中的每个管理节点创建 SP 连接，以便用户可以安全地登录和退出任何节点。使用以下说明创建第一个 SP 连接。然后，转到<<${post_edited_translations.segment}>>以创建您需要的任何其他连接。

选择 **SP** 连接类型

步骤

1. 转到*应用程序* > 集成 > **SP Connections**。
2. 选择*创建连接*。
3. 选择*不要为此连接使用模板*。
4. 选择 **Browser SSO Profiles** 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. 选择您从管理节点的"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 **Next**。

配置 **IdP** 浏览器 **SSO**

步骤

1. 在浏览器 SSO 选项卡中，选择 **Configure Browser SSO**。
2. 在 SAML 配置文件选项卡上，选择 **SP-initiated SSO**、**SP-initial SLO**、**IdP-initiated SSO** 和 **IdP-initiated SLO** 选项。
3. 选择 **Next**。
4. 在 Assertion Lifetime 选项卡上，不做任何更改。
5. 在断言创建选项卡上，选择*Configure Assertion Creation*。
   a. 在身份映射选项卡上，选择*Standard*。
   b. 在 Attribute Contract 选项卡上，使用 **SAML_SUBJECT** 作为 Attribute Contract 和导入的未指定名称格式。
6. 对于 Extend the Contract，选择 **Delete** 以删除未使用的 `urn:oid`。

映射适配器实例

步骤

1. ${post_edited_translations.segment}
2. 在适配器实例选项卡上，选择您创建的 适配器实例。
3. 在"映射方法"选项卡上，选择*从数据存储中检索其他属性*。
4. 在"属性源和用户查找"选项卡上，选择*添加属性源*。
5. 在"数据存储"选项卡上，提供说明并选择您添加的 数据存储。
6. 在"LDAP 目录搜索"选项卡上：
   - 输入 **Base DN**，它应与您在 StorageGRID 中为 LDAP 服务器输入的值完全匹配。
   - 对于搜索范围，选择*Subtree*。
   - 对于根对象类，搜索并添加以下任一属性：**objectGUID** 或 **userPrincipalName**。
7. 在 LDAP 二进制属性编码类型选项卡上，为 **objectGUID** 属性选择 **Base64**。
8. 在 LDAP 筛选器选项卡上，输入 **sAMAccountName=${username}**。
9. 在 Attribute Contract Fulfillment（属性合同履行）选项卡上，从 Source（来源）下拉菜单中选择 **LDAP**（属性），然后从 Value（值）下拉菜单中选择 **objectGUID** 或 **userPrincipalName**。
10. 查看并保存属性源。
11. 在 Failsave Attribute Source 选项卡上，选择 **Abort the SSO Transaction**。
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** > **Browser SSO** > **Protocol Settings** 选项卡上，选择 **Configure Protocol Settings**。
2. 在 Assertion Consumer Service URL 选项卡上，接受从 StorageGRID SAML 元数据导入的默认值（绑定为 **POST**，端点 URL 为 `/api/saml-response`）。
3. 在 SLO Service URLs 选项卡上，接受从 StorageGRID SAML 元数据导入的默认值（绑定为 **REDIRECT**，端点 URL 为 `/api/saml-logout`。
4. 在 Allowable SAML Bindings 选项卡上，清除 **ARTIFACT** 和 **SOAP**。只需要 **POST** 和 **REDIRECT**。
5. 在 Signature Policy（签名策略）选项卡上，保留 **Require Authn Requests to be Signed**（要求对身份验证请求进行签名）和 **Always Sign Assertion**（始终对断言进行签名）复选框处于选中状态。
6. 在加密策略选项卡上，选择*None*。
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. 在 SP Connection 选项卡中，选择 **Credentials**。

2. 在凭据选项卡中，选择 配置凭据。
3. 选择您创建或导入的 签名证书。
4. 选择*下一步*转到*管理签名验证设置*。
    a. 在信任模型选项卡上，选择*Unanchored*。
    b. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以复制第一个 SP 连接，以为网格中的每个管理节点创建所需的 SP 连接。您需要为每个副本上传新的元数据。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. 选择与管理节点对应的元数据文件：
    a. ${post_edited_translations.segment}
    b. ${post_edited_translations.segment}
    c. 选择 **Next**。
    d. 选择 **Save**。
4. 解决由于未使用的属性导致的错误：
    a. 选择新连接。
    b. 选择 **Configure Browser SSO > Configure Assertion Creation > Attribute Contract**。
    c. 删除 **urn:oid** 的条目。
    d. 选择 **Save**。

在 **StorageGRID** 中禁用 **SSO**

如果您不再需要使用单点登录 (SSO) 功能，可以将其禁用。您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 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

步骤

1. 选择*配置* > 访问控制 > 单点登录。

    此时将显示单一登录页面。

2. 选择*禁用 SSO*。
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

${post_edited_translations.segment}

暂时禁用和重新启用 **StorageGRID** 管理节点的 **SSO**

如果单点登录 (SSO) 系统发生故障，您可能无法登录 Grid Manager。在这种情况下，您可以临时禁用并重新启用一个管理节点的 SSO。要禁用并重新启用 SSO，您必须访问该节点的命令 shell。

开始之前

- 您有 "特定访问权限"。
- 您拥有 `Passwords.txt` 文件。
- ${post_edited_translations.segment}

关于此任务

在为一个管理节点禁用 SSO 后，您可以作为本地 root 用户登录到 Grid Manager。为了确保 StorageGRID 系统的安全，您必须在退出登录后立即使用该节点的命令 shell 在该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。Grid Manager 中“单点登录”页面上的 * 启用 SSO* 复选框仍保持选中状态，并且所有现有 SSO 设置都将保留，除非您对其进行更新。

步骤

1. 登录到管理节点：
   a. 输入以下命令： `ssh admin@Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。
2. 运行以下命令：`disable-saml`

   ${post_edited_translations.segment}
3. 确认您要禁用 SSO。

   ${post_edited_translations.segment}
4. 在 Web 浏览器中，访问同一管理节点上的 Grid Manager。

   ${post_edited_translations.segment}

5. 使用用户名 root 和本地 root 用户的密码登录。
6. 如果因需要更正 SSO 配置而暂时禁用 SSO：
   a. 选择*配置* > 访问控制 > 单点登录。
   b. 更改不正确或过期的 SSO 设置。
   c. 选择 **Save**。

      ${post_edited_translations.segment}
7. 如果由于其他原因需要访问 Grid Manager 而暂时禁用了 SSO：
   a. ${post_edited_translations.segment}
   b. 选择*注销*，然后关闭 Grid Manager。
   c. 在管理节点上重新启用 SSO。您可以执行以下步骤之一：

      - 运行以下命令： `enable-saml`

        ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   ◦ 重新启动网格节点： `reboot`
8. ${post_edited_translations.segment}
9. ${post_edited_translations.segment}

使用网格联盟

了解 **StorageGRID** 网格联合

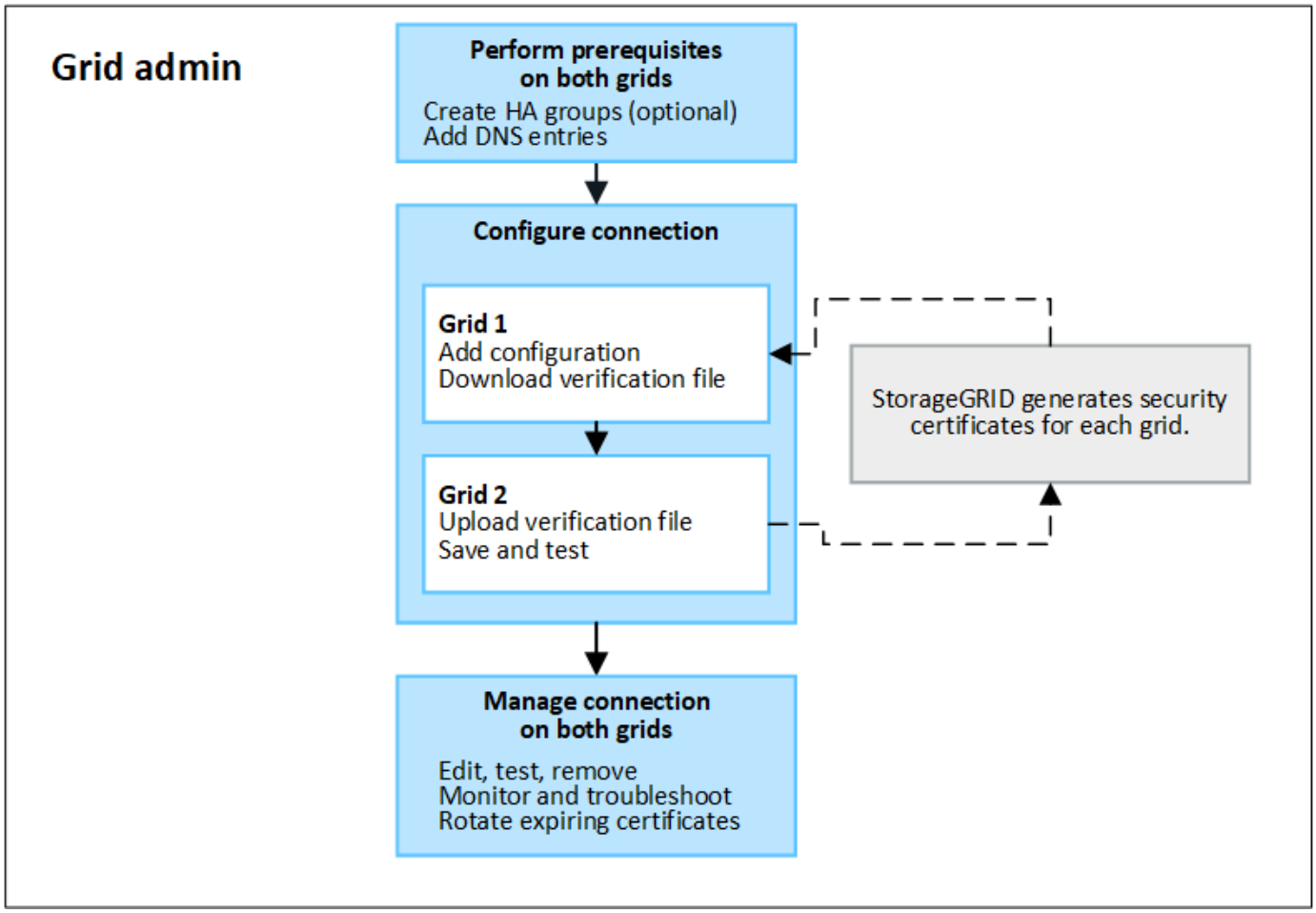
${post_edited_translations.segment}

什么是网格联盟连接?

${post_edited_translations.segment}

${post_edited_translations.segment}

工作流程图总结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或主要版本差异不超过一个的 StorageGRID 版本。

  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。

- 网格可以有一个或多个与其他网格的网格联合连接。每个网格联合连接都独立于任何其他连接。例如，如果 Grid 1 与 Grid 2 有一个连接，与 Grid 3 有第二个连接，则 Grid 2 和 Grid 3 之间没有隐含的连接。
- 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 "帐户克隆" 或 "跨网格复制"。

网络和 **IP** 地址要求

- 网格联合连接可以发生在网格网络、管理网络或客户端网络上。
- 网格联盟连接可将一个网格连接到另一个网格。每个网格的配置都指定了另一个网格上的网格联盟端点，该端点由管理节点、网关节点或两者组成。
- 最佳实践是连接每个网格上网关和 Admin Node 的 "${post_edited_translations.segment}"。使用 HA 组有助于确保在节点不可用时，网格联合连接仍将保持在线状态。如果任一 HA 组中的活动接口发生故障，则连接可以使用备份接口。
- 不建议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" 对象要求每个网格上的存储节点能够访问另一个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通往用于连接的管理节点或网关节点的高带宽路由。

使用 **FQDN** 对连接进行负载平衡

对于生产环境，使用完全限定域名 (FQDN) 来标识连接中的每个网格。然后，按如下所示创建相应的 DNS 条目：

- ${post_edited_translations.segment}
- 网格 2 的 FQDN 映射到网格 2 的一个或多个 VIP 地址，或网格 2 中的一个或多个管理节点或网关节点的 IP 地址。

当您使用多个 DNS 条目时，使用连接的请求将进行负载平衡，如下所示：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

端口要求

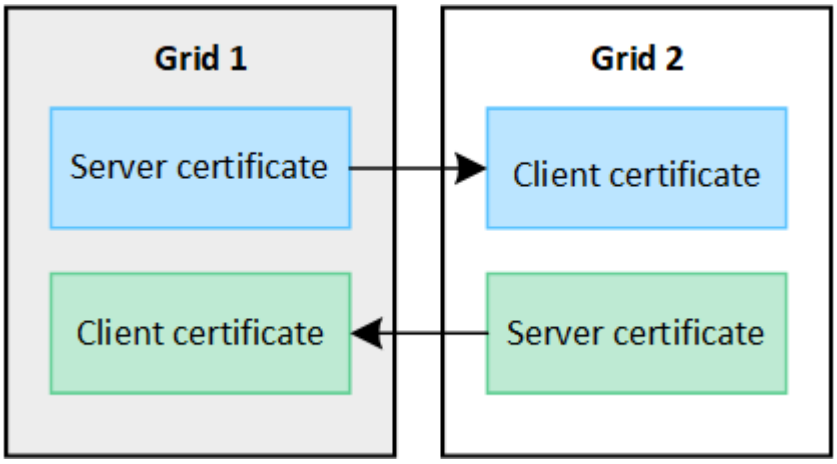
创建网格联合连接时，可以指定 23000 到 23999 之间的任何未使用的端口号。此连接中的两个网格将使用相同的端口。

${post_edited_translations.segment}

证书要求

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- 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）。当这些证书接近其过期日期时，*网格联合证书过期*警报将提醒您轮换证书，您可以使用 Grid Manager 执行此操作。

如果连接任一端的证书过期，连接将停止工作。在更新证书之前，数据复制将处于挂起状态。

了解更多

- "创建网格联盟连接"
- "管理网格联盟连接"
- "对网格联合错误进行故障排除"

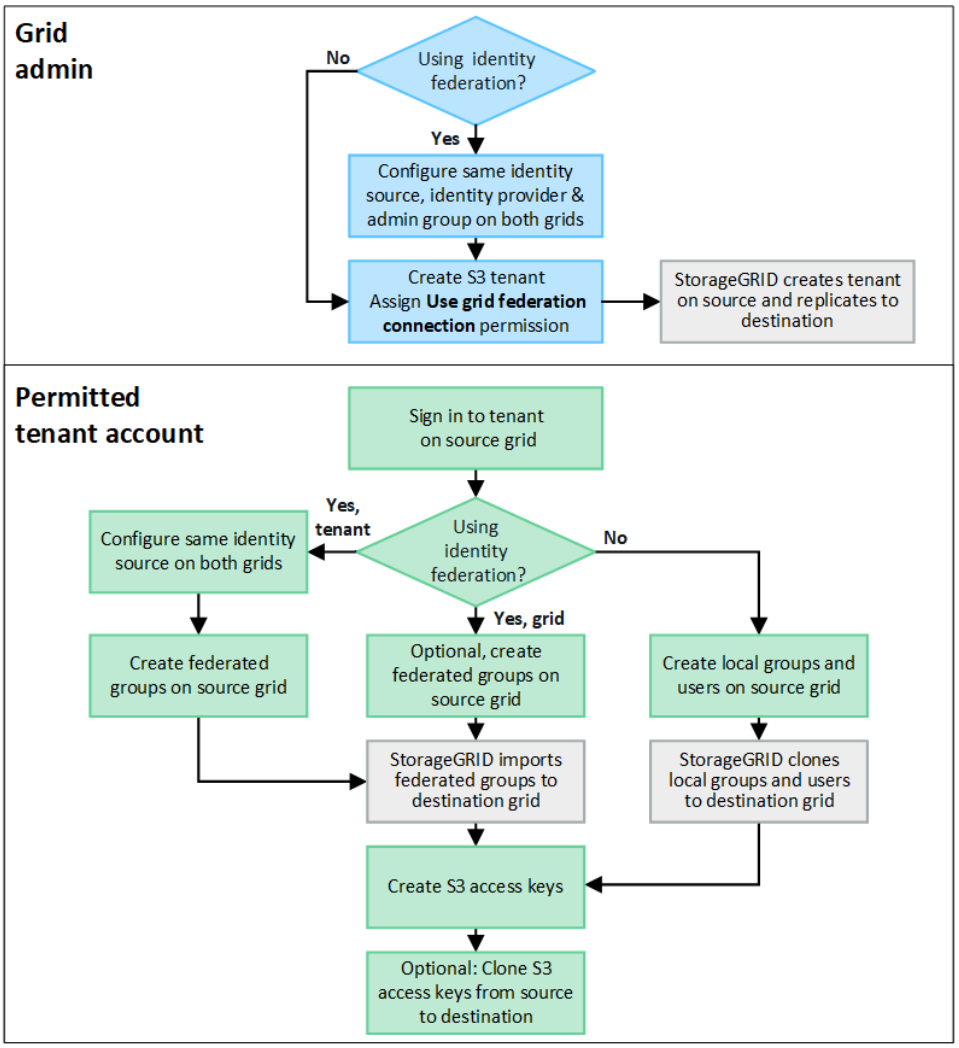
了解 StorageGRID 中的帐户克隆

帐户克隆是指在 "${post_edited_translations.segment}" 中的 StorageGRID 系统之间自动复制租户帐户、租户组、租户用户以及（可选）S3 访问密钥。

"跨网格复制" 需要进行帐户克隆。将帐户信息从源 StorageGRID 系统克隆到目标 StorageGRID 系统可确保租户用户和组可以访问任一 Grid 上的相应存储桶和对象。

${post_edited_translations.segment}

工作流程图显示网格管理员和允许的租户将执行的步骤，以设置帐户克隆。这些步骤在 "${post_edited_translations.segment}" 之后执行。



网格管理员工作流

网格管理员执行的步骤取决于 "${post_edited_translations.segment}" 中的 StorageGRID 系统是使用单点登录

(SSO) 还是身份联盟。

${post_edited_translations.segment}

如果网格联盟连接中的任一 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身份源。请参阅"${post_edited_translations.segment}"。
2. 为两个网格配置相同的 SSO 身份提供程序 (IdP)。请参见 "${post_edited_translations.segment}"。
3. 通过导入相同的联合组在两个网格上 "${post_edited_translations.segment}"。

   创建租户时，您将选择此组以获得源和目标租户帐户的初始 Root 访问权限。

   > 如果在创建租户之前两个网格上都不存在此管理组，则租户不会被复制到目标。

为帐户克隆配置网格级身份联合（可选）

如果任一 StorageGRID 系统使用不带 SSO 的身份联合，则两个网格都必须使用身份联合。在为网格联合创建租户帐户之前，租户的源和目标网格的网格管理员必须执行这些步骤。

步骤

1. 为两个网格配置相同的身份源。请参阅"${post_edited_translations.segment}"。
2. 可选地，如果联合组将对源和目标租户帐户都具有初始 Root 访问权限，请通过在两个网格上导入相同的联合组来实现 "创建相同的管理员组"。

   > 如果将 Root 访问权限分配给两个网格上都不存在的联合组，则租户不会复制到目标网格。

3. 如果不希望联合组具有两个帐户的初始 Root 访问权限，请为本地 root 用户指定密码。

创建允许的 **S3** 租户帐户

在可选配置 SSO 或身份联合之后，网格管理员执行这些步骤来确定哪些租户可以将存储桶对象复制到其他 StorageGRID 系统。

步骤

1. 确定要作为帐户克隆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_源网格_。复制租户的网格称为租户的_目标网格_。

2. 在该网格上，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. 如果租户帐户将管理其自己的联合用户，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克隆到目标租户，除非两个网格使用相同的身份源。

5. 选择特定的网格联盟连接。

6. 保存新租户或修改后的租户。

   当具有*使用网格联合连接*权限的新租户保存后，StorageGRID 会自动在其他网格上创建该租户的副本，如下所示：

   - 两个租户帐户具有相同的帐户 ID、名称、存储配额和分配的权限。
   - 如果选择了具有租户根访问权限的联合组，则会将该组克隆到目标租户。
   - 如果选择了具有租户根访问权限的本地用户，则会将该用户克隆到目标租户。但是，不会克隆此用户的密码。

有关详细信息，请参见 "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克隆租户组、用户和 S3 访问密钥。

步骤

1. 在租户的源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标识联盟。
3. 在源租户上创建组和用户。

   ${post_edited_translations.segment}

4. 创建 S3 访问密钥。
5. （可选）将 S3 访问密钥从源租户克隆到目标租户。

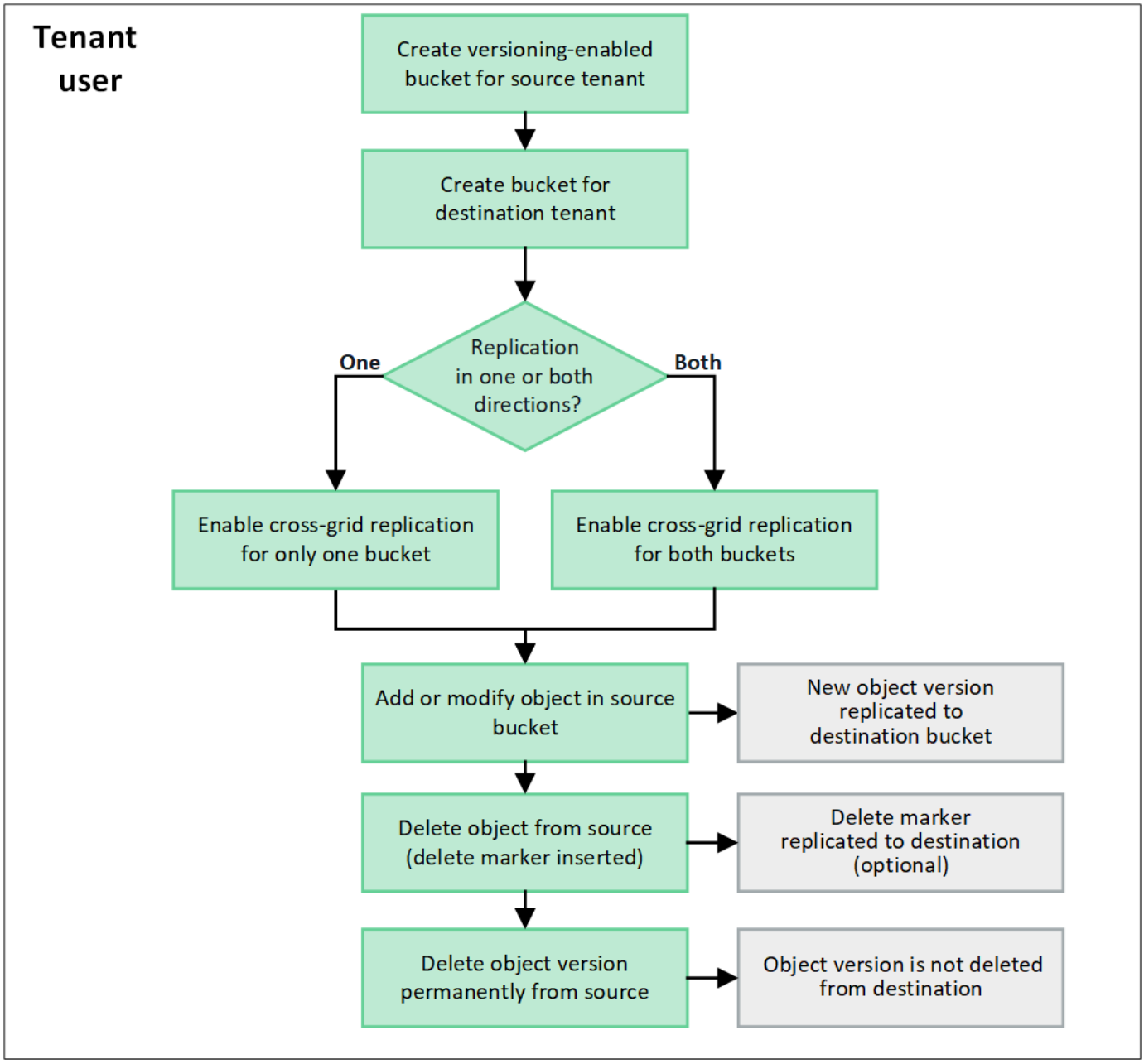
有关允许的租户帐户工作流的详细信息，以及有关如何克隆组、用户和 S3 访问密钥的信息，请参见"克隆租户组和用户"和"使用 API 克隆 S3 访问密钥"。

了解 StorageGRID 中的跨网格复制

跨网格复制是在通过"${post_edited_translations.segment}"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。"帐户克隆"是跨网格复制所必需的。

跨网格复制的工作流

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。这些存储桶：

- 可以有彼此不同的名字
- 可以有不同的区域
- 必须启用版本控制
- 必须为空

创建两个存储桶后，可以为其中一个或两个存储桶配置跨网格复制。

了解更多

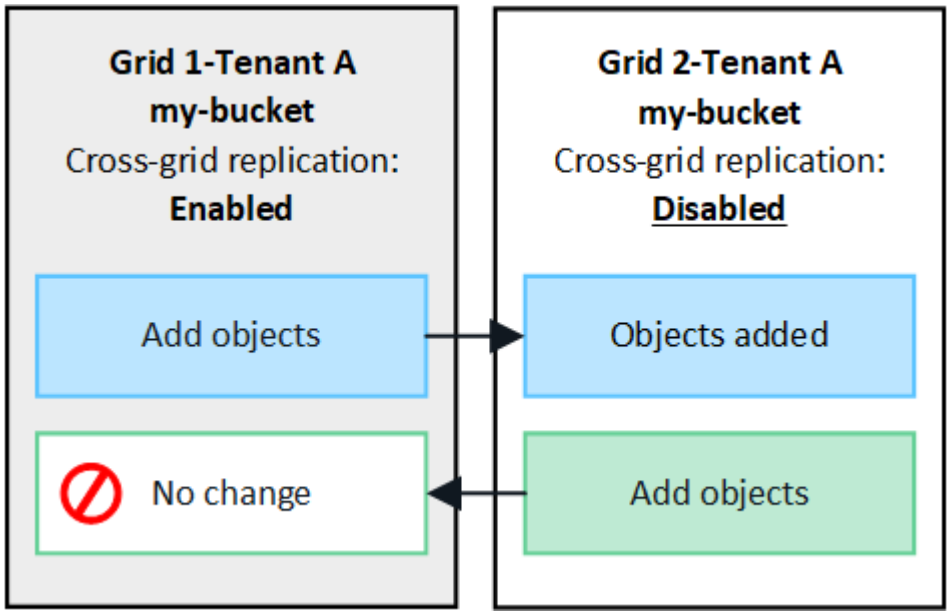
"管理跨网格复制"

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。

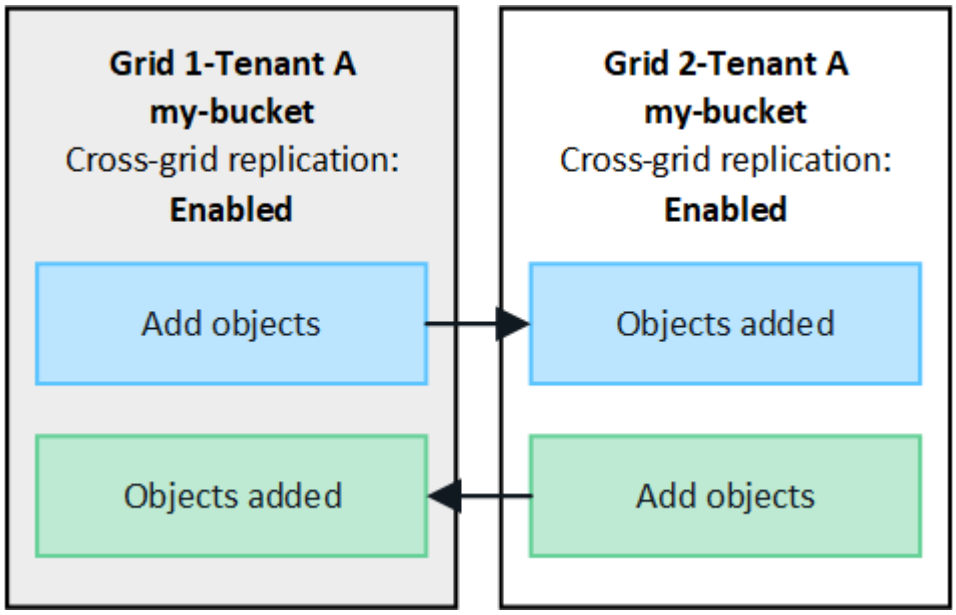
${post_edited_translations.segment}

如果仅在一个网格上为存储桶启用跨网格复制，则添加到该存储桶（源存储桶）的对象将复制到另一个网格（目标存储桶）上的相应存储桶。但是，添加到目标存储桶的对象不会复制回源存储桶。在图中，已为 `my-bucket` 启用从 Grid 1 到 Grid 2 的跨网格复制，但未在另一个方向启用。



双向复制

如果您在两个网格上为同一个存储桶启用跨网格复制，则添加到任一存储桶的对象都会复制到另一个网格。在图中，已为 `my-bucket` 双向启用跨网格复制。



${post_edited_translations.segment}

当 S3 客户端将对象添加到启用了跨网格复制的存储桶时，将出现以下情况：

1. StorageGRID 自动将对象从源存储桶复制到目标存储桶。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。响应包含特定于 StorageGRID 的 `x-ntap-sg-cgr-replication-status`响应标头，该标头具有以下值之一：

Grid	复制状态
源	• **COMPLETED**：所有网格连接的复制成功。 • **PENDING**：对象尚未复制到至少一个网格连接。 • **FAILURE**：任何网格连接的复制均未挂起，且至少有一个因永久故障而失败。用户必须解决此错误。
目标	**REPLICA**：该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 的副本可能使用 2+1 纠删码存储，并在三年后删除。

删除对象后会发生什么？

如"删除数据流"中所述，StorageGRID 可以出于以下任意原因删除对象：

- S3 客户端发出删除请求。
- 租户管理器用户选择 "删除存储桶中的对象" 选项以从存储桶中删除所有对象。
- 存储区具有生命周期配置，该配置已过期。
- 对象的 ILM 规则中的最后一个时间段已结束，且未指定更多放置位置。

当 StorageGRID 因删除存储桶中的对象操作、存储桶生命周期过期或 ILM 放置过期而删除对象时，复制的对象永远不会从网格联合连接中的其他网格中删除。但是，S3 客户端删除操作添加到源存储桶的删除标记可以选择性地复制到目标存储桶。

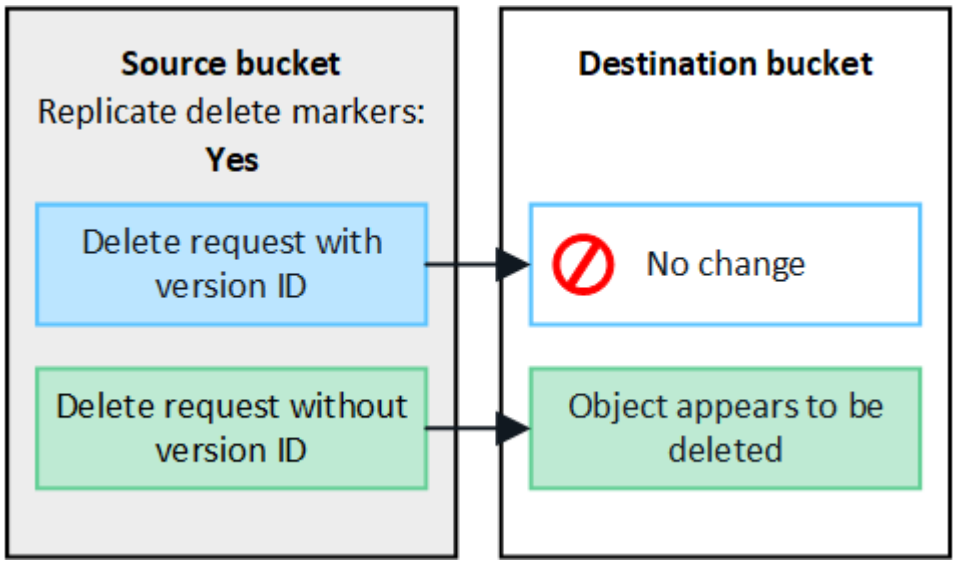
要了解当 S3 客户端从启用了跨网格复制的存储桶中删除对象时会发生什么，请查看 S3 客户端如何从启用了版本控制的存储桶中删除对象，如下所示：

- 如果 S3 客户端发出包含版本 ID 的删除请求，则会永久删除该版本的对象。不会向存储桶添加删除标记。
- 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，它将删除标记添加到存储桶。删除标记会导致 StorageGRID 表现得好像对象已被删除一样：
  - 不带版本 ID 的 GetObject 请求失败，并显示 `404 No Object Found`
  - 带有有效版本 ID 的 GetObject 请求将成功执行并返回请求的对象版本。

${post_edited_translations.segment}

- 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，因此不会从目标中删除相同的对象版本。
- 如果删除请求不包括版本 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桶，并将其复制到目标存储桶。实际上，该对象在两个网格上都显示为已删除。
  - 如果选择不复制删除标记，则会将删除标记添加到源存储桶，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，**Replicate delete markers** 被设置为 **Yes**（当 "${post_edited_translations.segment}" 时）。包含版本 ID 的源存储桶删除请求不会从目标存储桶中删除对象。不包含版本 ID 的源存储桶删除请求将显示为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，请为两个网格上的存储桶创建对应的"${post_edited_translations.segment}"。

如何复制加密对象

当您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、使用默认存储桶加密或配置网格范围加密。您可以在为存储桶启用跨网格复制之前或之后，添加、修改或删除默认存储桶或网格范围加密设置。

要对单个对象进行加密，您可以在将对象添加到源存储桶时使用 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`。请参见 "${post_edited_translations.segment}"。

跨网格复制不支持使用 SSE-C（使用客户提供密钥的服务器端加密）。引入操作将失败。

要对存储桶使用默认加密，请使用 PutBucketEncryption 请求并将 `SSEAlgorithm`参数设置为 `AES256`。存储桶级别加密适用于任何不含 `x-amz-server-side-encryption`请求标头的接收对象。请参阅"${post_edited_translations.segment}"。

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桶级别加密或在没

有 `x-amz-server-side-encryption`请求标头的情况下接收的任何对象。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*存储对象加密*选项，则不会将AES-128算法的使用传播到复制对象。相反，复制对象使用目标的默认存储桶或网格级加密设置（如果可用）。

在确定如何加密源对象时，StorageGRID 应用以下规则：

1. 使用 `x-amz-server-side-encryption`导入标头（如果存在）。
2. 如果不存在接收标头，请使用存储区默认加密设置（如果已配置）。
3. 如果未配置存储区设置，请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，请勿加密源对象。

在确定如何加密复制对象时，StorageGRID 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，请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，请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，请勿加密目标对象。

使用 **S3 Object Lock** 的跨网格复制

在以下情况下，您可以在启用了 S3 Object Lock 的 StorageGRID 存储桶之间配置跨网格复制。

当源存储桶上的 **S3** 对象锁定为……	目标存储桶上的 **S3** 对象锁定是……
已启用	已启用
已禁用	已启用

启用源存储桶上的 S3 Object Lock 时：

- 对象使用目标的保留设置按以下顺序锁定：
  a. 源对象的保留标头值：

     ```
     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。
- 您可以在上传对象时使用 `x-amz-object-lock-legal-hold`设置目标对象的法律保留状态。
- 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 Object Lock 被禁用时：

- 您可以配置目标存储桶上的默认保留，以将 S3 Object Lock 保留设置应用于目标对象。
- 目标对象无法设置法律保留状态。

PutObjectTagging 和 DeleteObjectTagging 不受支持

PutObjectTagging 和 DeleteObjectTagging 请求不支持已启用跨网格复制的存储桶中的对象。

如果 S3 客户端发出 PutObjectTagging 或 DeleteObjectTagging 请求，则返回 `501 Not Implemented`。消息为 `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured`。

PutObjectRetention 和 PutObjectLegalHold 不受支持

PutObjectRetention 和 PutObjectLegalHold 请求不完全支持已启用跨网格复制的存储桶中的对象。

如果 S3 客户端发出 PutObjectRetention 或 PutObjectLegalHold 请求，则会修改源对象的设置，但不会将更改应用于目标。

如何复制分段对象

源网格的最大段大小适用于复制到目标网格的对象。当对象复制到另一个网格时，源网格的 最大段大小 设置（配置 > 系统 > 存储选项 ）将在两个网格上使用。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。如果在源网格上接收 2 GB 的对象，则该对象将保存为两个 1 GB 的段。它也将作为两个 1 GB 的段复制到目标网格，即使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 "跨网格复制" 和 "StorageGRID CloudMirror 复制服务" 之间的异同。

> 您不能在通过跨网格复制所复制的存储桶上使用 CloudMirror，反之亦然。

	跨网格复制	**CloudMirror** 复制服务
${post_edited_translations.segment}	一个 StorageGRID 系统充当灾难恢复系统。存储桶中的对象可以在网格之间进行单向或双向复制。	使租户能够自动将对象从 StorageGRID （源）中的存储桶复制到外部 S3 存储桶（目标）。 CloudMirror 复制会在独立的 S3 基础设施中创建对象的独立副本。此独立副本不作为备份使用，但通常会在云中进行进一步处理。

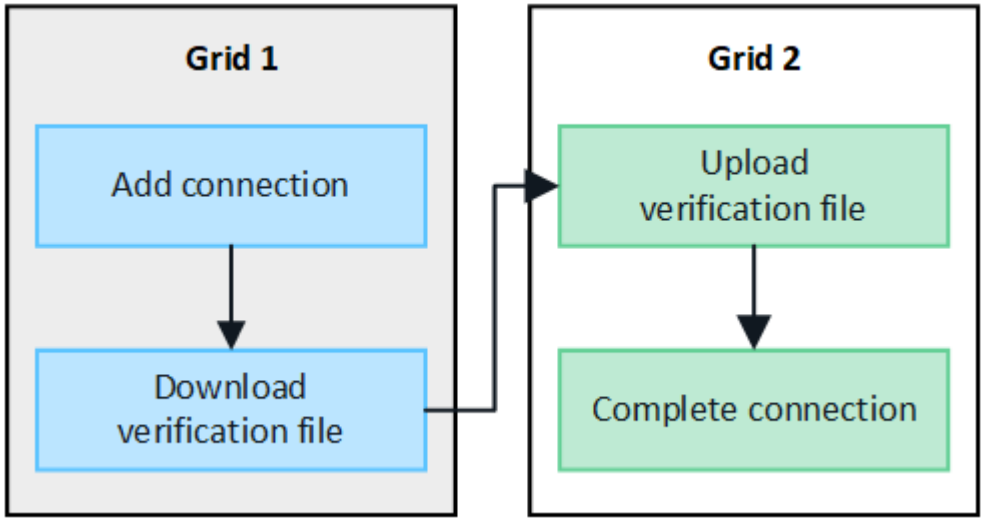
	跨网格复制	**CloudMirror** 复制服务
它是如何设置的?	1. ${post_edited_translations.segment} 2. ${post_edited_translations.segment} 3. ${post_edited_translations.segment} 4. ${post_edited_translations.segment}	1. 租户用户通过使用租户管理器或 S3 API 定义 CloudMirror 端点（IP 地址、凭据等）来配置 CloudMirror 复制。 2. 该租户帐户拥有的任何存储桶均可配置为指向 CloudMirror 端点。
${post_edited_translations.segment}	• ${post_edited_translations.segment} • 租户用户配置组、用户、密钥和存储区。	通常是租户用户。
${post_edited_translations.segment}	${post_edited_translations.segment}	• ${post_edited_translations.segment} • Google Cloud Platform (GCP)
是否需要对象版本控制?	是的，源和目标存储桶都必须启用对象版本控制。	否，CloudMirror 复制支持源和目标上未版本化和版本化存储桶的任何组合。
是什么原因导致对象移动到目标位置?	将对象添加到启用了跨网格复制的存储桶时，将自动复制这些对象。	将对象添加到已使用 CloudMirror 端点配置的存储桶时，将自动复制这些对象。在使用 CloudMirror 端点配置存储桶之前存在于源存储桶中的对象不会被复制，除非对其进行了修改。
如何复制对象?	跨网格复制创建版本控制对象，并将版本 ID 从源存储桶复制到目标存储桶。这样可以在两个网格中保持版本顺序一致。	CloudMirror 复制不需要启用了版本控制的存储桶，因此 CloudMirror 只能维护一个站点内某个键的顺序。无法保证对不同站点上的对象的请求能维持顺序。
如果无法复制对象，该怎么办?	对象已排入复制队列，但受元数据存储限制的限制。	对象已排入复制队列，但受平台服务限制（请参阅"使用平台服务的建议"）。
对象的系统元数据是否已复制?	是的，当对象被复制到另一个网格时，其系统元数据也会被复制。两个网格上的元数据完全相同。	否，当对象复制到外部存储桶时，其系统元数据将被更新。元数据因位置而异，具体取决于摄取时间和独立 S3 基础设施的行为。
如何检索对象?	应用程序可以通过向任一网格上的存储桶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，假设使用 CloudMirror 复制将对象镜像到合作伙伴组织。合作伙伴可以使用自己的应用程序直接从 S3 目标读取或更新对象。无需使用 StorageGRID。

	跨网格复制	**CloudMirror** 复制服务
删除对象后会发生什么？	• 包含版本 ID 的删除请求永远不会复制到目标网格。 • 不包含版本 ID 的删除请求会向源存储桶添加删除标记，该标记可以选择性地复制到目标网格。 • 如果跨网格复制仅配置为一个方向，则可以删除目标存储桶中的对象，而不会影响源。	结果将根据源和目标存储桶的版本控制状态而有所不同（不需要相同）： • 如果两个存储桶都进行了版本控制，则删除请求将在两个位置添加删除标记。 • 如果仅对源存储桶进行版本控制，则删除请求将向源添加删除标记，但不向目标添加删除标记。 • 如果两个存储区均未进行版本控制，则删除请求将从源中删除对象，但不会从目标中删除对象。 同样，可以删除目标存储桶中的对象，而不会影响源。

创建 **StorageGRID** 网格联合连接

如果要克隆租户详细信息并复制对象数据，可以在两个 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。



开始之前

- 您已查看配置网格联合连接的 "注意事项和要求"。
- 如果您计划为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 服务器具有适当的条目。
- 您正在使用 "支持的 Web 浏览器"。
- 您具有根访问权限和两个网格的配置密码短语。

添加连接

在两个 StorageGRID 系统中的任意一个系统上执行这些步骤。

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. 输入连接的详细信息。

字段	问题描述
连接名称	有助于识别此连接的唯一名称，例如"Grid 1-Grid 2"。
此网格的 FQDN 或 IP	以下项之一： • 您当前登录的网格的FQDN • 此网格上HA组的VIP地址 • 此网格上的管理节点或网关节点的 IP 地址。该 IP 可以位于目标网格可以访问的任何网络上。
端口	要用于此连接的端口。您可以输入从 23000 到 23999 的任何未使用的端口号。 此连接中的两个网格将使用相同的端口。您必须确保两个网格中没有任何节点使用此端口进行其他连接。
此网格的证书有效天数	您希望连接中此网格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。 当您保存连接时，StorageGRID 会自动为每个网格生成客户端和服务器证书。
此网格的配置密码短语	您登录到的网格的配置密码短语。
另一个网格的 FQDN 或 IP	以下项之一： • 要连接到的网格的 FQDN • 另一个网格上 HA 组的 VIP 地址 • 另一个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到达的任何网络上。

5. 选择 **Save and continue**。
6. 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。

7. 找到下载的文件(*connection-name*.grid-federation），并将其保存到安全位置。

   此文件包含机密（掩蔽为 *）和其他敏感详细信息，必须安全地存储和传输。

8. 选择*关闭*返回网格联合页面。
9. 确认新连接已显示，并且其*连接状态*为*等待连接*。
10. 将 `*connection-name*.grid-federation`文件提供给另一个网格的网格管理员。

完成连接

在您要连接的 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*Upload verification file*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）。

   此时将显示连接的详细信息。

5. （可选）为此网格的安全证书输入不同的有效天数。*证书有效天数*条目默认为您在第一个网格上输入的值，但每个网格可以使用不同的到期日期。

   一般来说，连接双方的证书使用相同的天数。

   如果连接任一端的证书过期，则连接将停止工作，并且在更新证书之前，复制将处于挂起状态。

6. 输入您当前登录的网格的配置密码短语。
7. 选择 **Save and test**。

   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，并在网格联盟页面上列出新连接。连接状态*将为*已连接。

   如果出现错误消息，请解决任何问题。请参阅 "对网格联合错误进行故障排除"。

8. 转到第一个网格的 Grid federation 页面，然后刷新浏览器。确认*连接状态*现已*已连接*。
9. 建立连接后，请安全地删除验证文件的所有副本。

   如果您编辑此连接，将创建一个新的验证文件。无法重复使用原始文件。

完成后

- 请查看 "管理允许的租户" 的注意事项。

- "创建一个或多个新租户帐户"，分配 **Use grid federation connection** 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" 作为正常 StorageGRID 监控活动的一部分。
- "排查连接问题"，包括解决与帐户克隆和跨网格复制相关的任何警报和错误。

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、删除租户权限和删除未使用的连接。

开始之前

- 您使用 "支持的 Web 浏览器" 登录到任一网格上的 Grid Manager。
- 您拥有您登录的网格的 "root 访问权限"。

编辑网格联盟连接

您可以通过登录到连接中任一网格的主管理节点来编辑网格联合连接。对第一个网格进行更改后，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，帐户克隆或跨网格复制请求将继续使用现有连接设置。对第一个网格所做的任何编辑都将保存在本地，但在上传到第二个网格、保存和测试之前不会使用。

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处于联机状态。

> 当您编辑网格联合连接时，StorageGRID 尝试在第一个网格的所有管理节点上保存"候选配置"文件。如果此文件无法保存到所有管理节点，当您选择 **Save and test** 时，将显示警告消息。

3. 选择*配置* > 系统 > 网格联合。
4. 使用网格联盟页面上的*操作*菜单或特定连接的详细信息页面编辑连接详细信息。查看"创建网格联盟连接"要输入的内容。

${post_edited_translations.segment}

a. 选择连接的单选按钮。

b. ${post_edited_translations.segment}

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. 输入您登录到的网格的配置密码短语。
6. 选择 **Save and continue**。

   新值已保存，但在您在另一个网格上上传新的验证文件之前，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），并将其保存到安全位置。

   验证文件包含机密，必须安全存储和传输。

9. 选择*关闭*返回网格联合页面。
10. 确认*连接状态*为*待编辑*。

    如果您开始编辑连接时，连接状态不是*已连接*，则不会更改为*待编辑*。

11. 将 `*connection-name*.grid-federation`文件提供给另一个网格的网格管理员。

完成连接编辑

通过在另一个网格上上传验证文件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. 输入您当前登录的网格的配置密码短语。
6. 选择 **Save and test**。

   如果可以使用编辑的值建立连接，则会显示成功消息。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. 转到第一个网格的 Grid federation 页面，然后刷新浏览器。确认*连接状态*现已*已连接*。
10. 建立连接后，请安全地删除验证文件的所有副本。

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. 使用网格联盟页面上的*操作*菜单或特定连接的详细信息页面测试连接。

${post_edited_translations.segment}

a. 选择连接的单选按钮。
b. 选择*操作* > 测试。

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. 请查看连接状态：

连接状态	问题描述
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，但该连接仍在使用现有配置。要完成编辑，请将新的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了连接，但尚未在另一个网格上完成连接。从此网格下载验证文件并将其上传到另一个网格。
未知	连接处于未知状态，可能是由于网络问题或离线节点。

5. 如果连接状态为*错误*，请解决任何问题。然后，再次选择*Test connection*以确认问题已修复。

轮换连接证书

每个网格联合连接使用四个自动生成的 SSL 证书来保护连接。当每个网格的两个证书接近其到期日期时，**Expiration of grid federation certificate** 警报会提醒您轮换证书。

如果连接任一端的证书过期，则连接将停止工作，并且在更新证书之前，复制将处于挂起状态。

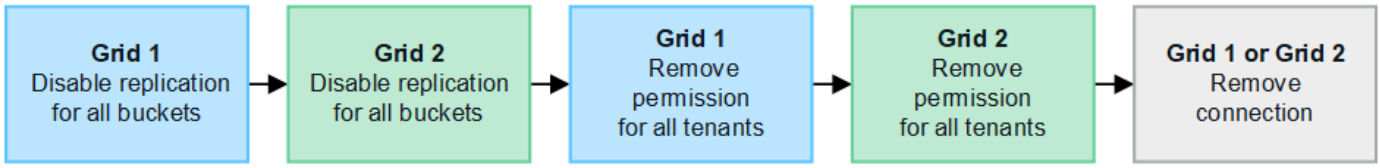
步骤

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 **Certificates** 选项卡。
5. 选择*轮换证书*。
6. 指定新证书应有效的天数。
7. 输入您登录到的网格的配置密码短语。
8. 选择*轮换证书*。
9. 根据需要，对连接中的另一个网格重复这些步骤。

   一般来说，连接双方的证书使用相同的天数。

删除网格联盟连接

您可以从连接中的任何一个网格中删除网格联合连接。如图所示，必须在两个网格上执行先决条件步骤，以确认两个网格上的任何租户都没有使用该连接。



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，当删除租户的权限时，两个网格上都存在的租户用户、组和对象不会从任一网格中删除。如果要删除这些项目，则必须从两个网格中手动删除它们。
- 删除连接时，任何挂起的复制（已接收但尚未复制到另一个网格）对象的复制都将永久失败。

禁用所有租户存储区的复制

步骤

1. 从任一网格开始，从主管理节点登录到 Grid Manager。
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，请指示所有租户对连接中两个网格上的所有存储桶"禁用跨网格复制"。

如果任何租户存储桶已启用跨网格复制，则无法删除*使用网格联合连接*权限。每个租户帐户必须在两个网格上禁用其存储桶的跨网格复制。

删除每个租户的权限

对所有租户存储桶禁用跨网格复制后，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，删除每个租户的*使用网格联合连接*权限。请参阅 "管理允许的租户"。
4. 对另一个网格上允许的租户重复这些步骤。

删除连接

步骤

1. 当两个网格上都没有租户使用连接时，请选择*Remove*。
2. 查看确认消息，然后选择*移除*。
   - 如果可以删除连接，则会显示一条成功消息。现在已从两个网格中删除网格联合连接。
   - 如果无法删除连接（例如，连接仍在使用或存在连接错误），则会显示一条错误消息。您可以执行以下任一操作：
     - 解决错误（推荐）。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，您可以强制删除不具有*Connected*状态的连接。

强制删除仅从本地网格中删除连接。要完全删除连接，请在两个网格上执行相同的步骤。

步骤

1. 在确认对话框中，选择*强制删除*。

   此时会显示一条成功消息。此网格联盟连接将无法再使用。但是，租户存储桶可能仍然启用了跨网格复制，并且某些对象副本可能已在连接中的网格之间复制。

2. 从连接中的另一个网格，从主管理节点登录到 Grid Manager。
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*移除*和*是*。
6. 选择*强制删除*以从此网格中删除连接。

管理 StorageGRID 网格联盟的允许租户

您可以允许 S3 租户帐户在两个 StorageGRID 系统之间使用网格联合连接。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

- 您使用 "支持的 Web 浏览器" 登录到任一网格上的 Grid Manager。
- 您拥有您登录的网格的 "root 访问权限"。
- 您有"已创建网格联合连接"在两个网格之间。
- 您已查看 "帐户克隆" 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) 或标识联合。请参阅 "什么是帐户克隆"。

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克隆和跨网格复制，请按照"创建一个新 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*。
- 当租户被创建或编辑以启用*使用网格联合连接*权限，然后保存在第一个网格上时，相同的租户将自动复制到另一个网格。租户复制到的网格是_租户的目标网格_。
- 两个网格上的租户将拥有相同的 20 位帐户 ID、名称、描述、配额和权限。您可以选择使用 **Description** 字段帮助识别哪个是源租户，哪个是目标租户。例如，在 Grid 1 上创建的租户的此描述也将显示在复制到 Grid 2 的租户中："This tenant was created on Grid 1."
- 出于安全原因，本地 root 用户的密码不会复制到目标网格。

> 在本地 root 用户可以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的或已编辑的租户后，租户用户可以执行以下操作：
  - 从租户的源网格创建组和本地用户，这些组和本地用户会自动克隆到租户的目标网格。请参阅 "克隆租户组和用户"。
  - 创建新的 S3 访问密钥，可选择将其克隆到租户的目标网格。请参阅 "使用 API 克隆 S3 访问密钥"。
  - 在连接中的两个网格上创建相同的存储桶，并启用单向或双向跨网格复制。请参见 "管理跨网格复制"。

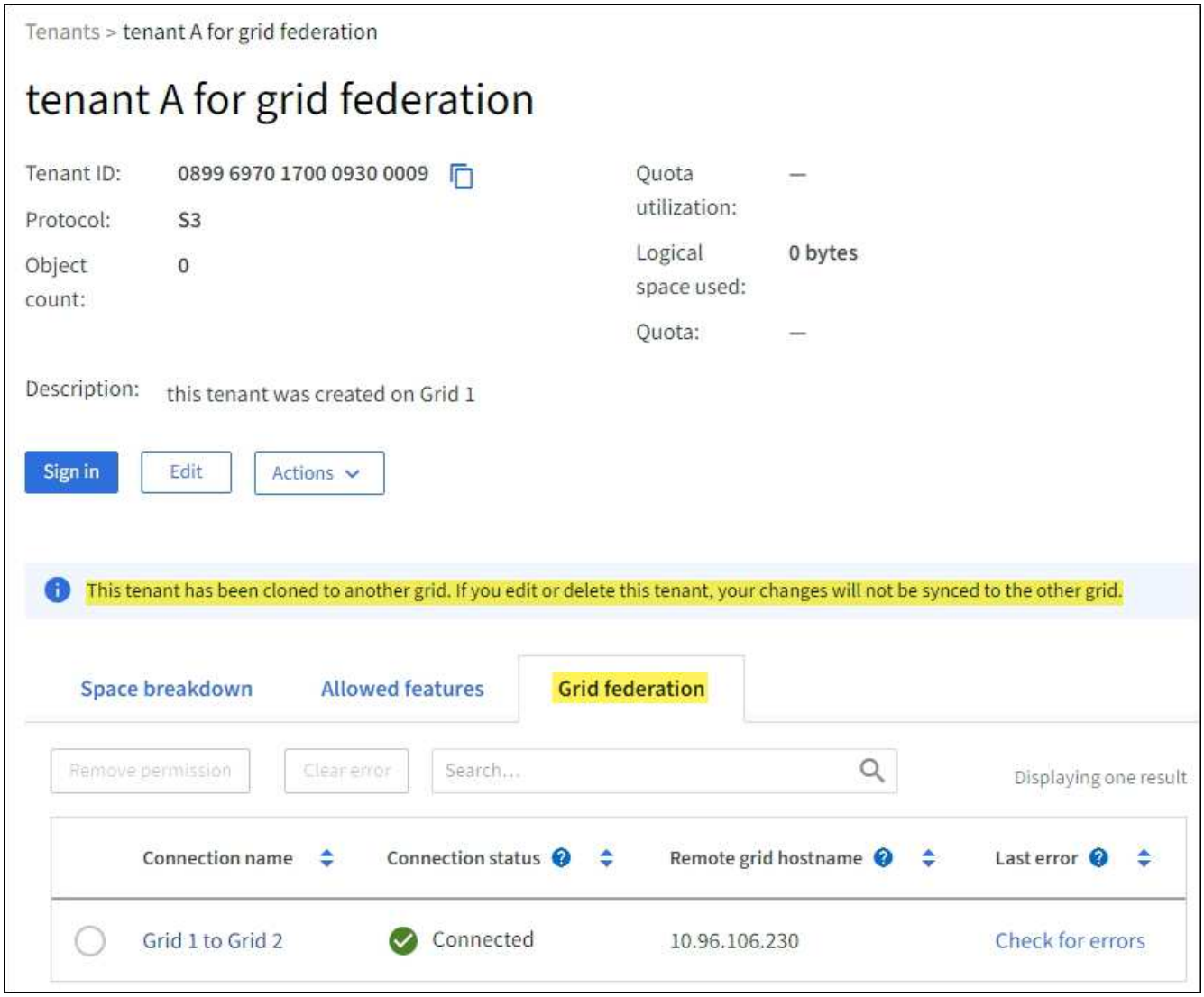
查看允许的租户

您可以查看允许使用网格联合连接的租户的详细信息。

步骤

1. ${post_edited_translations.segment}
2. 从租户页面中，选择租户名称以查看租户详细信息页面。

   如果这是租户的源网格（即，如果租户是在此网格上创建的），则会出现一个横幅，提醒您租户已克隆到另一个网格。如果编辑或删除此租户，则您所做的更改将不会同步到其他网格。



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

如果需要编辑具有*使用网格联合连接*权限的租户，请按照"编辑租户帐户"的一般说明进行操作，并注意以下事项：

- 如果租户具有*使用网格联合连接*权限，则可以从连接中的任一网格编辑租户详细信息。但是，您所做的任何更改都不会复制到其他网格。如果要使租户详细信息在网格之间保持同步，则必须在两个网格上进行相同的编辑。
- 编辑租户时，无法清除*使用网格联合连接*权限。
- ${post_edited_translations.segment}

${post_edited_translations.segment}

如果您需要删除具有 **Use grid federation connection** 权限的租户，请遵循 "${post_edited_translations.segment}" 的常规说明并注意以下事项：

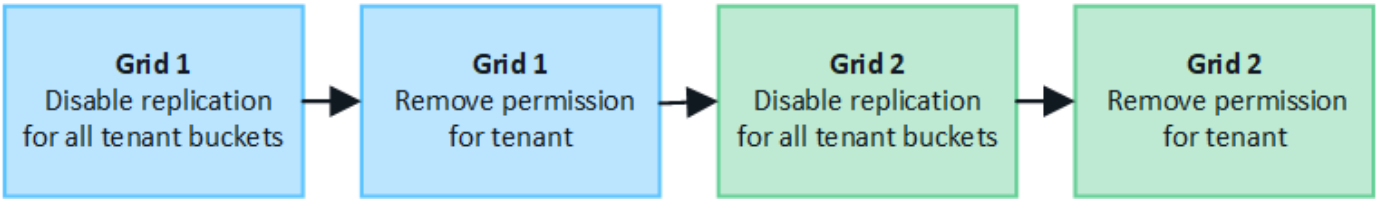
- ${post_edited_translations.segment}

- 在目标网格上删除克隆的租户之前，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克隆的租户，则无法再将帐户用于跨网格复制。
- 如果要删除源网格上的原始租户，则克隆到目标网格的任何租户组、用户或密钥都不会受到影响。您可以删除克隆的租户，也可以允许其管理自己的组、用户、访问密钥和存储区。
- ${post_edited_translations.segment}

  为避免这些错误，请先删除租户使用网格联合连接的权限，然后再从此网格中删除租户。

${post_edited_translations.segment}

${post_edited_translations.segment}



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：

- 如果租户的任何存储桶启用了跨网格复制，则无法删除 使用网格联盟连接 权限。租户帐户必须先为其所有存储桶禁用跨网格复制。
- 删除 使用网格联盟连接 权限不会删除已在网格之间复制的任何项目。例如，在删除租户权限时，两个网格上存在的任何租户用户、组和对象都不会从任何一个网格中删除。如果要删除这些项目，您必须手动从两个网格中将其删除。
- 如果要使用相同的网格联合连接重新启用此权限，请先在目标网格上删除此租户；否则，重新启用此权限将导致错误。

> 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，并触发克隆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，则克隆将导致冲突错误。

开始之前

- 您正在使用 "支持的 Web 浏览器"。
- 您拥有两个网格的 "root 访问权限"。

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤

1. 从任一网格开始，从主管理节点登录到 Grid Manager。
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. ${post_edited_translations.segment}
5. 如果列出了该租户，请指示其针对连接中两个网格上的所有存储桶 "禁用跨网格复制"。

如果任何租户存储桶启用了跨网格复制，则无法删除 使用网格联盟连接 权限。租户必须在两个网格上为其存储桶禁用跨网格复制。

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤

1. 从主管理节点登录到网格管理器。
2. 从网格联合页面或租户页面中删除权限。

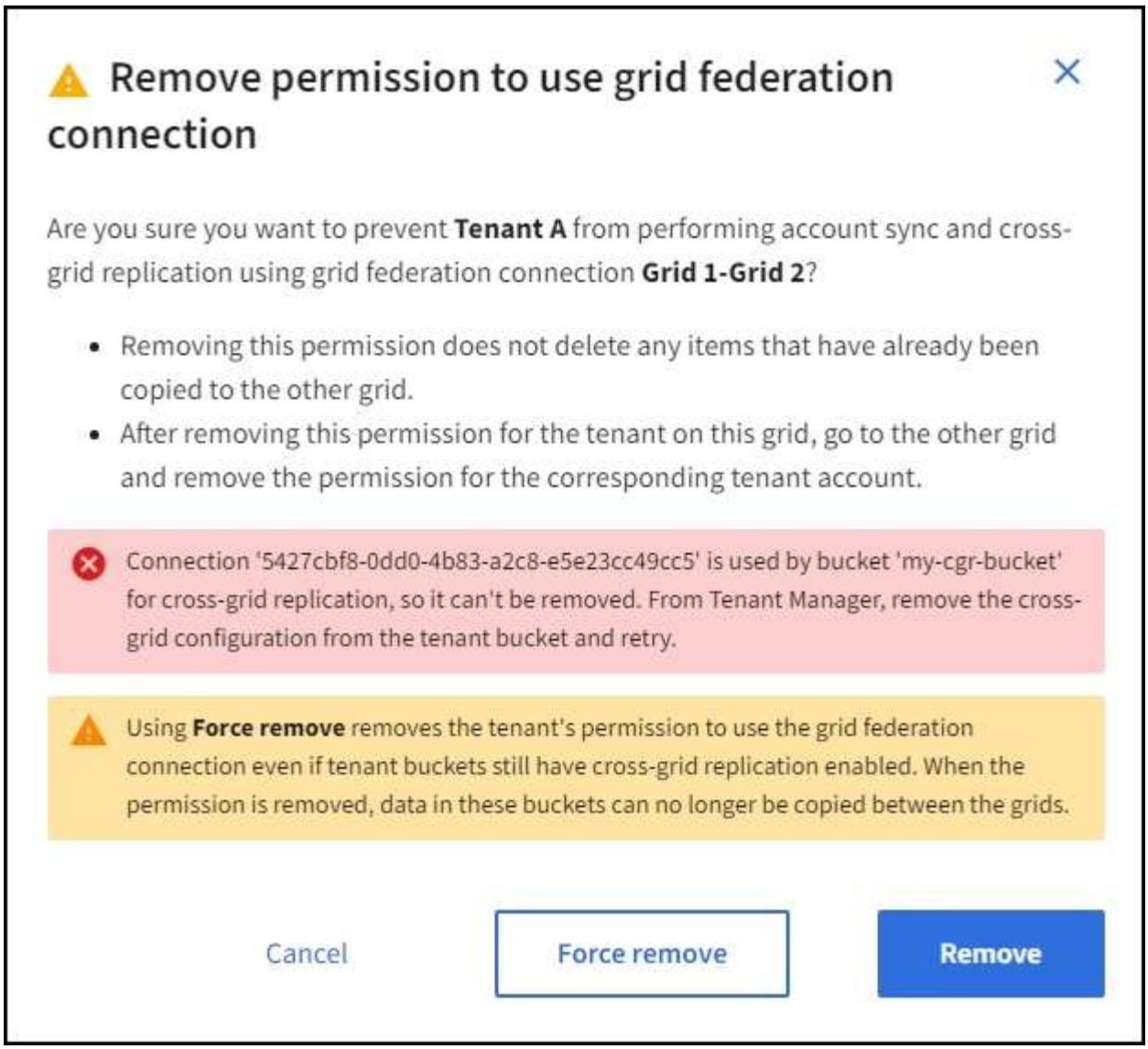
   ${post_edited_translations.segment}

   a. 选择*配置* > 系统 > 网格联合。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
   - 如果可以删除该权限，您将返回到详情页面，并显示成功消息。此租户将无法再使用网格联盟连接。
   - 如果一个或多个租户存储桶仍启用了跨网格复制，则会显示错误。



您可以执行以下操作之一：

- （推荐。）登录到租户管理器并禁用每个租户存储桶的复制。请参阅"管理跨网格复制"。然后，重复这些步骤以删除 **Use grid connection** 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

如果需要，即使租户存储桶已启用跨网格复制，也可以强制删除租户使用网格联合连接的权限。

在强制删除租户的权限之前，请注意 删除权限 的一般注意事项以及以下其他注意事项：

- 如果强制删除*使用网格联合连接*权限，则任何挂起复制到另一个网格（已摄取但尚未复制）的对象都将继续被复制。要防止这些进程中的对象到达目标存储桶，还必须删除租户在另一个网格上的权限。
- ${post_edited_translations.segment}

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. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
6. 查看确认对话框中的警告，并选择*Force remove*。

   系统将显示成功消息。此租户将无法再使用网格联盟连接。

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相同租户帐户的权限。例如，您应该在另一个网格上重复这些步骤，以防止正在处理的对象到达目标存储桶。

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、帐户克隆和跨网格复制相关的警报和错误。

网格联盟连接警报和错误

您可能会收到网格联盟连接的警报或遇到错误。

进行任何更改以解决连接问题后，请测试连接，以确保连接状态返回到 **Connected**。有关说明，请参见"管理网格联盟连接"。

网格联合连接失败警报

问题描述

${post_edited_translations.segment}

详细信息

${post_edited_translations.segment}

建议的操作

1. 检查两个网格的“网格联盟”页面上的设置。确认所有值均正确。参见 "管理网格联盟连接"。
2. 检查用于连接的证书。确保没有关于网格联盟证书过期的警报，且每个证书的详细信息均有效。请参见 "管理网格联盟连接" 中关于轮换连接证书的说明。
3. 确认两个网格中的所有管理节点和网关节点均在线且可用。解决可能影响这些节点的任何警报，然后重试。
4. 如果您为本地或远程 grid 提供了完全限定域名 (FQDN)，请确认 DNS 服务器已联机且可用。有关网络、IP 地址和 DNS 要求，请参见 "什么是网格联盟？"。

${post_edited_translations.segment}

问题描述

已触发*网格联合证书到期*警报。

详细信息

此警报表示一个或多个网格联合证书即将过期。

建议的操作

请参见 "管理网格联盟连接" 中关于轮换连接证书的说明。

编辑网格联盟连接时出错

问题描述

在编辑网格联合连接时，您在选择*保存并测试*时会看到以下警告消息："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 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，因为管理节点处于脱机状态），则会显示警告消息。

建议的操作

1. 从用于编辑连接的网格中，选择*Nodes*。
2. 确认该网格的所有管理节点都处于联机状态。
3. 如果任何节点处于脱机状态，请将其重新联机并尝试再次编辑连接。

帐户克隆错误

无法登录到克隆的租户帐户

问题描述

无法登录克隆的租户帐户。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

出于安全原因，将租户帐户从租户的源网格克隆到租户的目标网格时，不会克隆您为租户的本地 root 用户设置的密码。同样，当租户在其源网格上创建本地用户时，本地用户密码不会克隆到目标网格。

建议的操作

在 root 用户登录到租户的目标网格之前，网格管理员必须先在目标网格上"更改本地 root 用户的密码"。

在克隆的本地用户登录到租户的目标网格之前，克隆租户的 root 用户必须在目标网格上为该用户添加密码。有关说明，请参阅使用 Tenant Manager 的说明中的 "管理用户"。

在没有克隆的情况下创建的租户

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"Tenant created without a clone"消息。

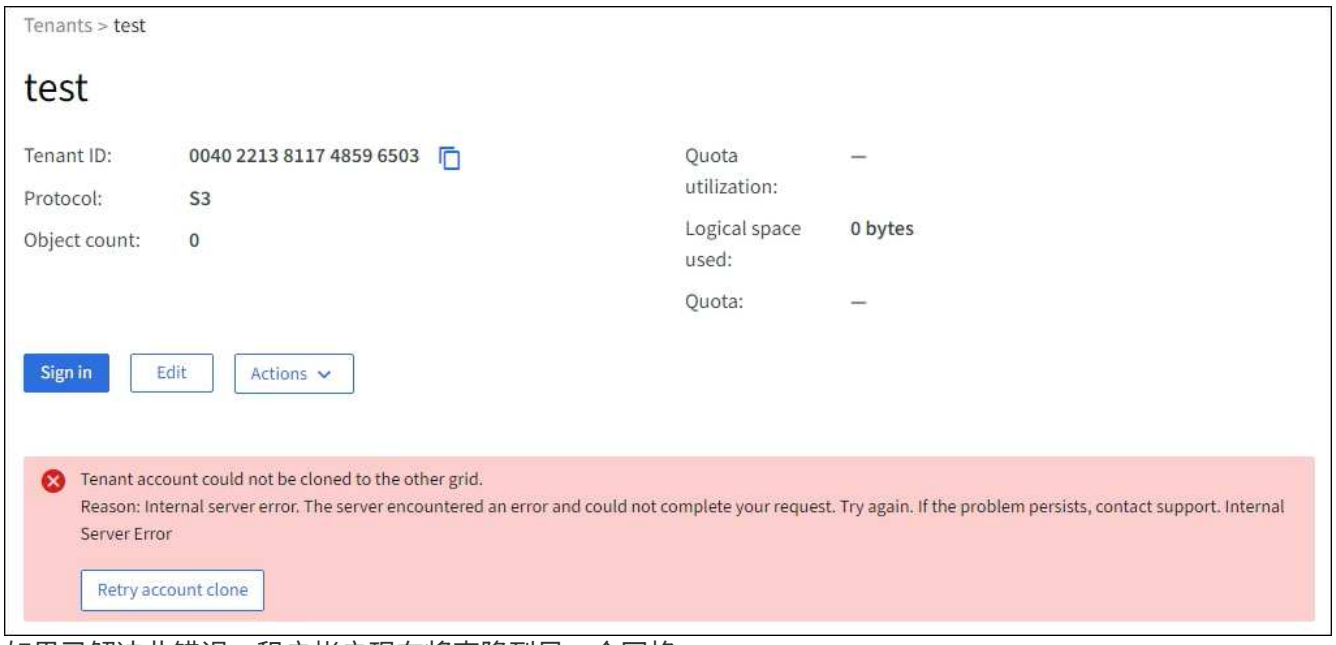
详细信息

如果连接状态的更新出现延迟，则可能会发生此问题，这可能导致不正常的连接被列为*已连接*。

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"管理网格联盟连接"中的说明测试网格联合连接，以确认此问题已修复。

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
6. 选择*重试帐户克隆*。



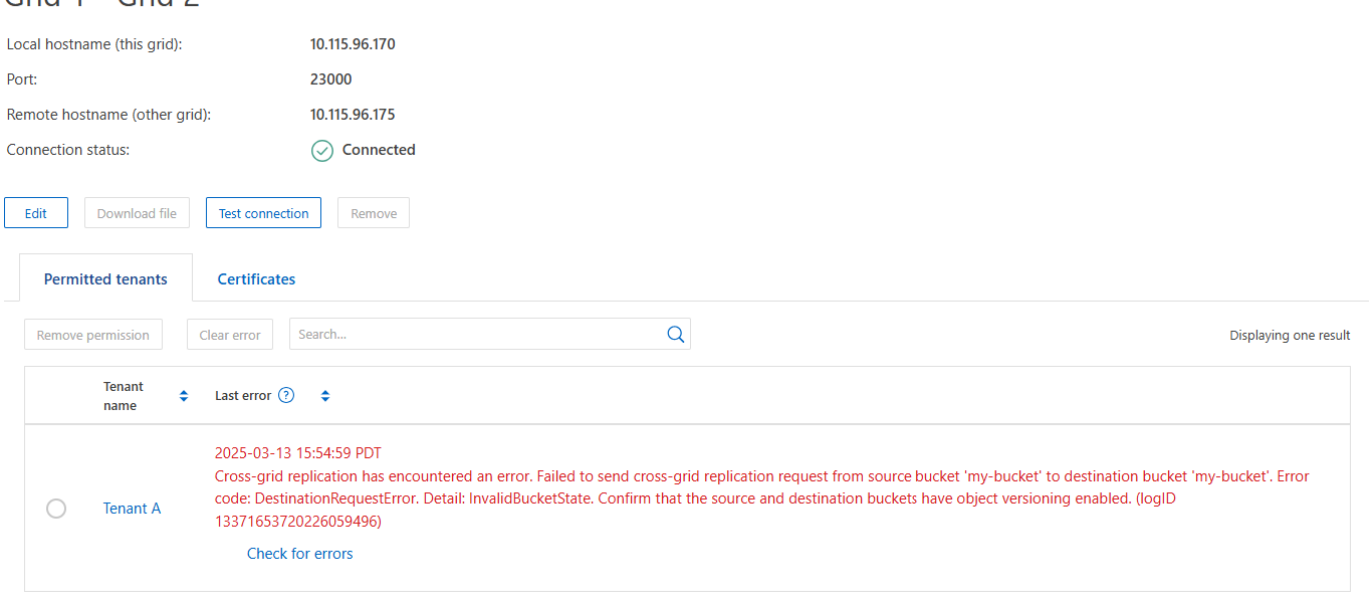
如果已解决此错误，租户帐户现在将克隆到另一个网格。

${post_edited_translations.segment}

${post_edited_translations.segment}

问题描述

当 "查看网格联合连接"（或当 "${post_edited_translations.segment}" 进行连接时），您会在连接详细信息页面的*上一个错误*列中发现错误。例如：



详细信息

对于每个网格联盟连接，“上一次错误”列会显示在将租户数据复制到另一个网格时发生的最新的错误（如果有）。此列仅显示上一次发生的跨网格复制错误；可能发生的先前错误不会显示。此列中出现错误可能是由于以下原因之一：

- 未找到源对象版本。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

建议的操作

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. 执行任何推荐的操作。例如，如果针对跨网格复制暂停了目标存储桶的版本控制，请重新启用该存储桶的版本控制。
3. ${post_edited_translations.segment}
4. 选择*清除错误*。
5. ${post_edited_translations.segment}
6. 等待 5-6 分钟，然后向存储桶中摄入一个新对象。确认未再次出现该错误消息。

   为确保清除错误消息，请在消息中的时间戳后至少等待 5 分钟，然后再摄取新对象。

   ${post_edited_translations.segment}

7. 要确定是否因存储区错误而无法复制任何对象，请参阅 "${post_edited_translations.segment}"。

跨网格复制永久故障警报

问题描述

${post_edited_translations.segment}

详细信息

此警报表示，由于需要用户干预才能解决的原因，无法在两个网格的存储桶之间复制租户对象。此警报通常是由于源存储桶或目标存储桶发生更改而引起的。

建议的操作

1. ${post_edited_translations.segment}
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*上一个错误*列，以确定哪些租户帐户出错。

4. 要了解有关故障的详细信息，请参见 "${post_edited_translations.segment}" 中的说明，以查看跨网格复制指标。
5. ${post_edited_translations.segment}
   a. 请参见 "监控租户活动" 中的说明，以确认租户在目标网格上未超出其跨网格复制配额。
   b. 根据需要，增加租户在目标网格上的配额，以允许保存新对象。
6. ${post_edited_translations.segment}
7. ${post_edited_translations.segment}
   - 另一个网格上有相同租户的相应存储桶（必须使用确切的名称）。
   - 两个存储桶都启用了对象版本控制（不能在任何网格上暂停版本控制）。
   - ${post_edited_translations.segment}
8. 要确认问题已解决，请参见 "${post_edited_translations.segment}" 中的说明以查看跨网格复制指标，或执行以下步骤：
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. 等待 5-6 分钟，然后向存储桶中摄入一个新对象。确认未再次出现该错误消息。

      为确保清除错误消息，请在消息中的时间戳后至少等待 5 分钟，然后再摄取新对象。

   ${post_edited_translations.segment}

   a. 转到 "${post_edited_translations.segment}" 以识别任何未能复制到另一个网格的对象或删除标记，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挂起状态，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，查看问题是否自行解决。
2. 如果问题仍然存在，请确定任一网格是否针对同一连接显示 **Grid federation connection failure**（网格联合连接失败）警报，或者针对某个节点显示 **Unable to communicate with node**（无法与节点通信）警报。当您解决这些警报时，此警报可能会随之解决。
3. 要了解有关故障的详细信息，请参见 "${post_edited_translations.segment}" 中的说明，以查看跨网格复制指标。
4. ${post_edited_translations.segment}

${post_edited_translations.segment}

识别并重试失败的 StorageGRID 复制操作

在解决“跨网格复制永久故障”警报后，您应该确定是否有任何对象或删除标记未能复制到另一个网格。然后，您可以重新摄入这些对象，或使用 Grid Management API 重试复制。

跨网格复制永久故障 警报指示，由于需要用户干预才能解决的原因，无法在两个网格上的存储桶之间复制租户对象。此警报通常是由于对源存储桶或目标存储桶进行更改而导致的。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未能复制

要确定是否有任何对象或删除标记未复制到其他网格，可以在审核日志中搜索 "CGRR（跨网格复制请求）" 消息。当 StorageGRID 无法将对象、多部分对象或删除标记复制到目标存储桶时，此消息将添加到日志中。

您可以使用 "audit-explain 工具" 将结果转换为更易于阅读的格式。

开始之前

- ${post_edited_translations.segment}
- 您拥有 `Passwords.txt` 文件。
- 您知道主管理节点的 IP 地址。

步骤

1. ${post_edited_translations.segment}
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 身份登录时，提示符将从 `$`更改为 `#`。

2. ${post_edited_translations.segment}

   例如，此命令对过去 30 分钟内的所有 CGRR 消息执行 grep 操作，并使用 audit-explain 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
   ```

   此命令的结果将类似于此示例，其中包含六个 CGRR 消息的条目。在该示例中，由于无法复制对象，因此所有跨网格复制请求都返回了一般错误。前三个错误为 "replicate object" 操作，后三个错误为 "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	问题描述
CGRR 跨网格复制请求	请求的名称
租户	租户的账号 ID
连接	网格联合连接的 ID
operation	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	存储桶名称
对象	${post_edited_translations.segment}
version	${post_edited_translations.segment}

字段	问题描述
错误	错误类型。如果跨网格复制失败，则错误为 "General error"。

${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

> 标记为"私有"的 StorageGRID API 端点如有更改，恕不另行通知。StorageGRID 私有端点也会忽略请求的 API 版本。

3. 在 **cross-grid-replication-advanced** 部分，选择以下端点：

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. 选择*试用*。
5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. ${post_edited_translations.segment}

> 挂起表示已将跨网格复制请求添加到内部队列中进行处理。

监控复制重试

应监视复制重试操作，以确保它们已完成。

> 将对象或删除标记复制到另一个网格可能需要几个小时或更长时间。

可以通过以下两种方式之一监视重试操作：

- 使用 S3 "HeadObject" 或 "获取对象" 请求。响应包括 StorageGRID 特定的 `x-ntap-sg-cgr-replication-status`响应标头，该标头将具有以下其中一个值：

Grid	复制状态
源	• **COMPLETED**：复制成功。 • **PENDING**：对象尚未复制。 • **FAILURE**：复制失败，出现永久性故障。用户必须解决此错误。
目标	**REPLICA**：该对象已从源网格复制。

- ${post_edited_translations.segment}

步骤

1. 在私有 API 文档的 **cross-grid-replication-advanced** 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 `cross-grid-replication-retry-failed`请求中使用的版本 ID。
4. ${post_edited_translations.segment}
5. 确认服务器响应代码为 **200**。
6. 查看复制状态，复制状态将为以下选项之一：
   - **PENDING**：对象尚未复制。
   - **COMPLETED**：复制成功。
   - **FAILED**：复制失败，出现永久性故障。用户必须解决此错误。

管理安全

管理 StorageGRID 中的安全性

您可以从 Grid Manager 配置各种安全设置，以帮助保护您的 StorageGRID 系统。

管理加密

StorageGRID 提供多种加密数据的选项。您应该 "查看可用的加密方法" 以确定哪些选项符合您的数据保护要求。

管理证书

您可以 "配置和管理服务器证书" 用于 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移除。设备卷加密后，除非节点可以与 KMS 通信，否则您无法访问设备上的任何数据。

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

管理代理服务器设置

如果使用的是 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 "管理员代理服务器"。

控制防火墙

为了提高系统的安全性，您可以通过在 "外部防火墙" 上打开或关闭特定端口来控制对 StorageGRID 管理节点的访问。您还可以通过配置其 "内部防火墙" 来控制对每个节点的网络访问。您可以阻止对所有端口的访问，部署所需的端口除外。

查看 **StorageGRID** 加密方法

StorageGRID 提供多种加密数据的选项。您应查看可用的方法，以确定哪些方法符合您的数据保护要求。

下表提供了 StorageGRID 中可用加密方法的概要摘要。

加密选项	工作原理	适用于
Grid Manager 中的密钥管理服务器 (KMS)	您"配置密钥管理服务器"用于 StorageGRID 站点和 "为设备启用节点加密"。然后，设备节点连接到 KMS 以请求密钥加密密钥 (KEK)。此密钥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。设备上的所有数据都会受到保护，以防止物理丢失或从数据中心移除。 注意：仅存储节点和服务设备支持使用 KMS 管理加密密钥。
StorageGRID 设备安装程序中的驱动器加密页面	如果设备包含支持硬件加密的驱动器，您可以在安装过程中设置驱动器密码。当您设置驱动器密码时，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。在开始安装之前，请转到 **Configure Hardware** > **Drive Encryption** ，以设置适用于节点中所有 StorageGRID 管理的自加密驱动器的驱动器密码。	包含自加密驱动器的设备。安全驱动器上的所有数据都会受到保护，以防止物理丢失或从数据中心移除。 驱动器加密不适用于 SANtricity 管理的驱动器。如果您有带有自加密驱动器和 SANtricity 控制器的存储设备，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	如果您的 StorageGRID 设备启用了驱动器安全功能，您可以使用 "SANtricity System Manager"来创建和管理安全密钥。访问安全驱动器上的数据需要此密钥。	具有全磁盘加密 (FDE) 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都受到保护，以防止物理丢失或从数据中心中移除。不能与某些存储设备或任何服务设备一起使用。

加密选项	工作原理	适用于
存储对象加密	您在 Grid Manager 中启用 "存储对象加密" 选项。启用后，任何未在存储桶级别或对象级别进行加密的新对象都将在摄入期间进行加密。	${post_edited_translations.segment} 现有的已存储对象不会被加密。对象元数据和其他敏感数据不会被加密。
${post_edited_translations.segment}	您发出 PutBucketEncryption 请求以启用存储桶加密。任何未在对象级进行加密的新对象都会在摄入期间进行加密。	${post_edited_translations.segment} 必须为存储桶指定加密。现有的存储桶对象不会被加密。对象元数据和其他敏感数据不会被加密。 "${post_edited_translations.segment}"
S3 对象服务器端加密 (SSE)	您发出 S3 请求以存储对象并包含 `x-amz-server-side-encryption`请求标头。	${post_edited_translations.segment} 必须为对象指定加密。对象元数据和其他敏感数据未加密。 StorageGRID 管理密钥。 "${post_edited_translations.segment}"
使用客户提供的密钥（SSE-C）对 S3 对象进行服务器端加密	${post_edited_translations.segment} • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	${post_edited_translations.segment} 必须为对象指定加密。对象元数据和其他敏感数据未加密。 ${post_edited_translations.segment} "${post_edited_translations.segment}"
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment} 外部加密方法可对加密算法和密钥进行更严格的控制。可以与列出的其他方法相结合。

加密选项	工作原理	适用于
StorageGRID 外部的对象加密	在将对象数据和元数据摄入 StorageGRID 之前，您可以使用 StorageGRID 外部的加密方法对其进行加密。	仅对象数据和元数据（系统配置数据未加密）。 外部加密方法可对加密算法和密钥进行更严格的控制。可以与列出的其他方法相结合。 "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，一次可以使用多个加密方法。例如：

- 您可以使用 KMS 保护设备节点，也可以使用 SANtricity System Manager 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 来保护设备节点上的数据，也可以使用存储对象加密选项在接收所有对象时对其进行加密。

如果只有一小部分对象需要加密，请考虑在存储桶或单个对象级别控制加密。启用多级加密会带来额外的性能成本。

相关信息

"了解 FIPS 认证加密选项"

管理证书

管理 **StorageGRID** 中的安全证书

安全证书是用于在 StorageGRID 组件之间以及 StorageGRID 组件和外部系统之间创建安全、可信连接的小型数据文件。

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，向其客户端验证服务器的身份并为数据提供安全通信路径。服务器和客户端各有一个证书副本。
- *客户端证书*向服务器验证客户端或用户身份，提供比仅使用密码更安全的身份验证。客户端证书不加密数据。

当客户端使用 HTTPS 连接到服务器时，服务器将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，则客户端使用相同的公钥启动与服务器的会话。

StorageGRID 用作某些连接（如负载平衡器端点）的服务器，或用作其他连接（如 CloudMirror 复制服务）的客户端。

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网格 CA 证书。默认情况下，网格 CA 证书用于保护内部 StorageGRID 流量。外部证书颁发机构 (CA) 可以颁发完全符合组织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。对于生产环境，请使用由外部证书颁发机构签名的自定义证书。支持无证书的非安全连接，但不推荐使用。

- ${post_edited_translations.segment}
- 所有自定义证书都必须符合 "${post_edited_translations.segment}"。
- ${post_edited_translations.segment}

> StorageGRID 还包含在所有网格上均相同的操作系统 CA 证书。在生产环境中，请确保指定由外部证书颁发机构签名的自定义证书，以代替操作系统 CA 证书。

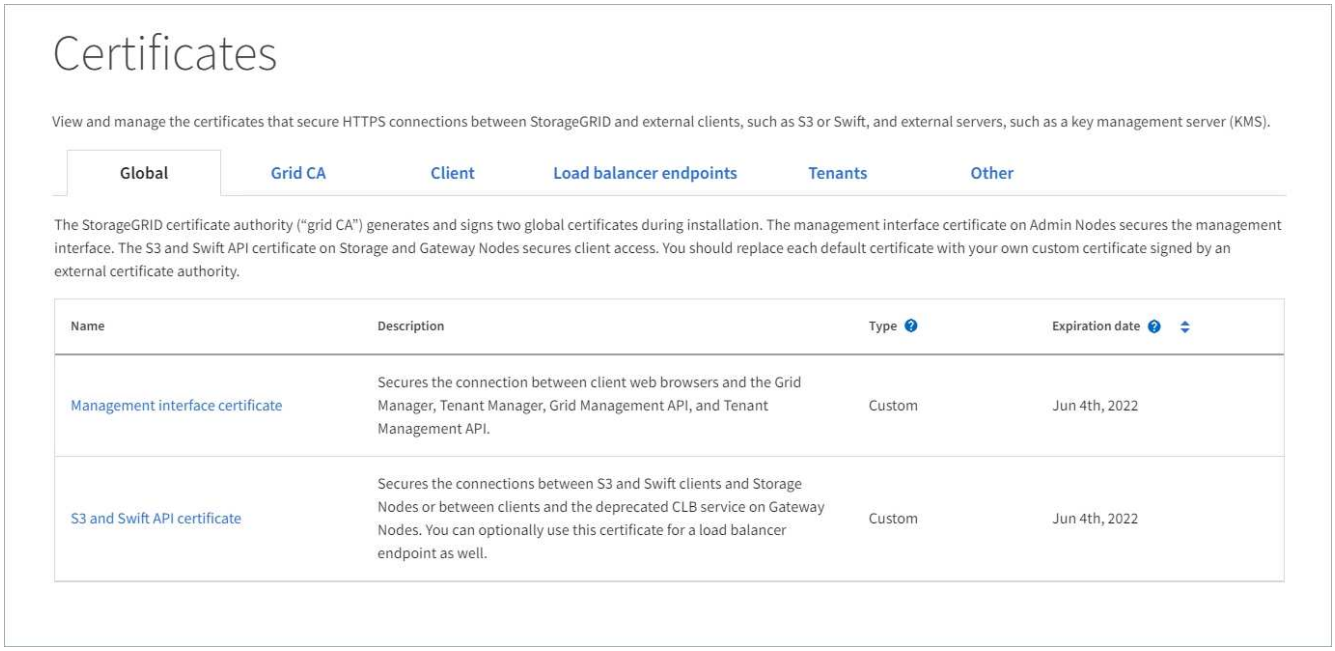
服务器和客户端证书类型的变体以多种方式实现。在配置系统之前，您应该准备好特定 StorageGRID 配置所需的所有证书。

${post_edited_translations.segment}

您可以在单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 Grid Manager 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。如果您拥有 "适当的权限"，则可以访问该选项卡。
   - 全局：保护网络浏览器和外部 API 客户端对 StorageGRID 的访问。
   - **Grid CA**：保护内部 StorageGRID 流量。
   - 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 客户端和 StorageGRID 负载平衡器之间的连接。
- 租户：保护到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。

  下面将介绍每个选项卡，并链接到其他证书详细信息。

全局

全局证书可确保从 Web 浏览器和外部 S3 API 客户端安全地访问 StorageGRID。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]：保护客户端 Web 浏览器与 StorageGRID 管理界面的连接。
- <<${post_edited_translations.segment}>>：保护客户端 API 与存储节点、管理节点和网关节点的连接，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：

- ${post_edited_translations.segment}
- 说明
- 类型：自定义或默认。+ 您应始终使用自定义证书来提高网格安全性。
- **Expiration date**：如果使用默认证书，则不会显示到期日期。

您可以轻松实现以下目标：

- 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：
  - "替换默认 StorageGRID 生成的管理接口证书" 用于 Grid Manager 和 Tenant Manager 连接。
  - "${post_edited_translations.segment}" 用于 Storage Node 和负载均衡器端点（可选）连接。
- "还原默认管理接口证书"。
- "还原默认 S3 API 证书"。
- "${post_edited_translations.segment}"。
- 复制或下载 "${post_edited_translations.segment}" 或 "${post_edited_translations.segment}"。

${post_edited_translations.segment}

网格CA证书由 StorageGRID 证书颁发机构在 StorageGRID 安装期间生成，用于保护所有内部 StorageGRID 流量。

证书信息包括证书过期日期和证书内容。

您可以 "复制或下载网格 CA 证书"，但无法进行修改。

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。

${post_edited_translations.segment}

您可以轻松实现以下目标：

- "${post_edited_translations.segment}"
- ${post_edited_translations.segment}
  - "${post_edited_translations.segment}"

- "设置 Prometheus 访问权限。"
- "上传并替换客户端证书。"
- "复制或下载客户端证书。"
- "删除客户端证书。"

- 选择*操作*以快速"${post_edited_translations.segment}"、"挂载"或"删除"客户端证书。您最多可以选择 10 个客户端证书，并使用*操作* > *删除*一次删除它们。

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 负载均衡器服务之间的连接安全。

负载均衡器端点表为每个配置的负载均衡器端点包含一行，并指示该端点使用的是全局 S3 API 证书还是自定义负载均衡器端点证书。还会显示每个证书的过期日期。

对端点证书的更改可能需要长达 15 分钟才能应用于所有节点。

您可以轻松实现以下目标：

- "${post_edited_translations.segment}"，包括其证书详细信息。
- "为 FabricPool 指定负载均衡器端点证书。"
- "${post_edited_translations.segment}" 而不是生成新的负载均衡器端点证书。

租户

租户可以使用${post_edited_translations.segment}或平台服务端点证书来保护其与 StorageGRID 的连接。

${post_edited_translations.segment}

您可以轻松实现以下目标：

- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"

其他

StorageGRID 使用其他安全证书来满足特定用途。这些证书按其功能名称列出。其他安全证书包括：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 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到期日期（如适用）。选择函数名称将打开一个浏览器选项卡，您可以在其中查看和编辑证书详细信息。

只有在具有 "适当的权限" 的情况下，才能查看和访问其他证书的信息。

您可以轻松实现以下目标：

- "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"
- "为外部 syslog 服务器使用证书"
- "轮换网格联合连接证书"
- "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

下面将介绍每种类型的安全证书，并提供指向实现说明的链接。

管理接口证书

证书类型	问题描述	导航位置	详细信息
服务器	验证客户端 Web 浏览器与 StorageGRID 管理界面之间的连接，允许用户在不出现安全警告的情况下访问 Grid Manager 和 Tenant Manager。 此证书还验证 Grid Management API 和 Tenant Management API 连接。 您可以使用在安装过程中创建的默认证书，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"

${post_edited_translations.segment}

证书类型	问题描述	导航位置	详细信息
服务器	验证到存储节点和负载均衡器端点的安全 S3 客户端连接（可选）。	配置 > 安全 > 证书，选择*全局*选项卡，然后选择 **S3 API certificate**	"配置 S3 API 证书"

网格**CA**证书

请参阅默认网格 CA 证书说明。

管理员客户端证书

证书类型	问题描述	导航位置	详细信息
客户端	安装在每个客户端上，允许 StorageGRID 对外部客户端访问进行身份验证。 • 允许授权外部客户端访问 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	问题描述	导航位置	详细信息
服务器	验证 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。配置负载平衡器端点时，可以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。 您还可以使用全局 <<${post_edited_translations.segment}>> 证书的自定义版本来验证与负载平衡器服务的连接。如果全局证书用于验证负载平衡器连接，则无需为每个负载平衡器端点上传或生成单独的证书。 注意： 用于负载均衡器身份验证的证书是正常 StorageGRID 操作期间最常用的证书。	配置 > 网络 > 负载平衡器端点	• "配置负载平衡器端点" • "为 FabricPool 创建负载平衡器端点"

云存储池端点证书

证书类型	问题描述	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"

电子邮件警报通知证书

证书类型	问题描述	导航位置	详细信息
服务器和客户端	验证 SMTP 电子邮件服务器与用于警报通知的 StorageGRID 之间的连接。 • 如果与 SMTP 服务器的通信需要传输层安全性 (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。	告警 > 电子邮件设置	"为警报设置电子邮件通知"

外部 **syslog** 服务器证书

证书类型	问题描述	导航位置	详细信息
服务器	验证外部 syslog 服务器与 StorageGRID 之间的 TLS 或 RELP/TLS 连接，该服务器用于记录 StorageGRID 中的事件。 注意： TCP、RELP/TCP 和 UDP 连接到外部 syslog 服务器不需要外部 syslog 服务器证书。	配置 > 监控 > 审核和 **syslog** 服务器	"使用外部 syslog 服务器"

网格联盟连接证书

证书类型	问题描述	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 > 网格联合	• "创建网格联盟连接" • "轮换连接证书"

身份联合证书

证书类型	问题描述	导航位置	详细信息
服务器	验证 StorageGRID 与外部身份提供程序（如 Active Directory、OpenLDAP 或 Oracle Directory Server）之间的连接。用于身份联合，允许管理员组和用户由外部系统管理。	配置 > 访问控制 > 身份联合	"${post_edited_translations.segment}"

密钥管理服务器**(KMS)**证书

证书类型	问题描述	导航位置	详细信息
服务器和客户端	验证 StorageGRID 与外部密钥管理服务器 (KMS) 之间的连接，该服务器为 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	问题描述	导航位置	详细信息
服务器	验证从 StorageGRID 平台服务到 S3 存储资源的连接。	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	问题描述	导航位置	详细信息
服务器	验证身份联合服务（如 Active Directory Federation Services (AD FS)）与用于单点登录 (SSO) 请求的 StorageGRID 之间的连接。	配置 > 访问控制 > 单点登录	"${post_edited_translations.segment}"

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. 您可以配置负载平衡器端点，并在 StorageGRID 中上传或生成服务器证书。
2. 您可以配置与负载均衡器端点的 S3 客户端连接，并将相同的证书上传到客户端。

3. 当客户端想要保存或检索数据时，它使用 HTTPS 连接到负载均衡器端点。
4. StorageGRID 使用包含公钥的服务器证书以及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，则客户端使用相同的公钥启动会话。
6. 客户端将对象数据发送至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. 使用外部密钥管理服务器软件，可以将 StorageGRID 配置为 KMS 客户端，并获取 CA 签名的服务器证书、公共客户端证书和客户端证书的私钥。
2. 使用 Grid Manager，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私钥。
3. 当 StorageGRID 节点需要加密密钥时，它会向 KMS 服务器发出请求，其中包括来自证书的数据和基于私钥的签名。
4. KMS 服务器验证证书签名并决定它可以信任 StorageGRID。
5. ${post_edited_translations.segment}

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 密码需要 RSA 证书，而 ECDSA 密码需要 ECDSA 证书。请参阅"管理安全证书"。如果配置与服务器证书不兼容的自定义安全策略，则可以"暂时还原为默认安全策略"。

有关 StorageGRID 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单个自定义证书，该证书允许用户访问 Grid Manager 和 Tenant Manager，而不会遇到安全警告。您还可以还原为默认管理接口证书或生成新证书。

关于此任务

默认情况下，每个管理节点都会颁发由网格 CA 签名的证书。这些 CA 签名的证书可以替换为单个通用自定义管理接口证书和相应的私钥。

由于所有管理节点都使用单个自定义管理接口证书，因此如果客户端在连接到 Grid Manager 和 Tenant Manager 时需要验证主机名，则必须将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。

${post_edited_translations.segment}

为确保操作不会因服务器证书失效而中断，当此服务器证书即将过期时会触发*管理接口的服务器证书过期*警报。根据需要，您可以通过选择*配置* > 安全 > *证书*并在 Global 选项卡上查看管理接口证书的到期日期来查看当前证书的到期时间。

如果使用域名而不是 IP 地址访问 Grid Manager 或 Tenant Manager，则浏览器将显示证书错误，如果发生以下任一情况，则无法选择绕过：

- 您的自定义管理界面证书已过期。
- 你 从自定义管理接口证书还原为默认服务器证书。

添加自定义管理接口证书

要添加自定义管理界面证书，您可以提供自己的证书或使用 Grid Manager 生成证书。

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*管理界面证书*。
3. ${post_edited_translations.segment}
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：

   - ${post_edited_translations.segment}
   - 证书私钥：自定义服务器证书私钥文件 (`.key`）。

     EC 私钥必须为 224 位或更大。RSA 私钥必须为 2048 位或更大。

   - **CA bundle**：包含来自每个中间颁发证书颁发机构 (CA) 的证书的单个可选文件。该文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。

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 捆绑包，则每个证书都会显示在自己的选项卡上。

   - 选择*下载证书*保存证书文件，或选择*下载 CA 捆绑包*保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. 选择 * 保存 *。+ 自定义管理接口证书将用于随后与 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的所有新连接。

生成证书

${post_edited_translations.segment}

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	问题描述
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 主题或标识名 (DN)。 如果在此字段中未输入任何值，则生成的证书将使用第一个域名或 IP 地址作为使用者通用名称 (CN)。

字段	问题描述
有效天数	创建后证书过期的天数。
添加密钥使用扩展	${post_edited_translations.segment} ${post_edited_translations.segment} ${post_edited_translations.segment}

c. 选择 **Generate**。

d. 选择*证书详细信息*可查看生成的证书的元数据。

- 选择*下载证书*以保存证书文件。

  指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

e. 选择 * 保存 *。+ 自定义管理接口证书将用于随后与 Grid Manager、Tenant Manager、Grid Manager API 或 Tenant Manager API 的所有新连接。

5. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

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

${post_edited_translations.segment}

步骤

1. 选择*配置* > 安全 > 证书。
2. 在*全局*选项卡上，选择*管理界面证书*。
3. 选择*使用默认证书*。

   还原默认管理接口证书时，您配置的自定义服务器证书文件将被删除，无法从系统中恢复。默认管理接口证书用于所有后续新客户端连接。

4. ${post_edited_translations.segment}

${post_edited_translations.segment}

如果需要严格的主机名验证，您可以使用脚本生成管理接口证书。

开始之前

- 您有 "特定访问权限"。
- 您拥有 `Passwords.txt` 文件。

关于此任务

生产环境的最佳实践是使用由外部证书颁发机构签名的证书。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 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`，请使用通配符来表示所有 Admin Node 的完全限定域名。例如，`*.ui.storagegrid.example.com` 使用 * 通配符来表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 将 以配置管理接口证书，该证书由 Grid Manager 和 Tenant Manager 使用。 `--type` 设置为 `management`
   - 默认情况下，生成的证书有效期为一年（365 天），并且必须在到期前重新创建。您可以使用 `--days`参数覆盖默认有效期。

     > 证书的有效期从运行 `make-certificate`时开始。您必须确保管理客户端与 StorageGRID 同步到相同的时间源；否则，客户端可能会拒绝证书。

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
     ```

     ${post_edited_translations.segment}
4. 选择并复制证书。

   在您的选择中包括 BEGIN 和 END 标记。
5. 从命令外壳中注销。 `$ exit`
6. 确认证书已配置：
   a. 访问 Grid Manager。

b. 选择*配置* > 安全 > 证书

c. 在*全局*选项卡上，选择*管理界面证书*。

7. 将管理客户端配置为使用您复制的公共证书。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*管理界面证书*。
3. 选择 **Server** 或 **CA bundle** 选项卡，然后下载或复制证书。

${post_edited_translations.segment}

下载证书或 CA 捆绑包 `.pem`文件。如果您使用的是可选的 CA 捆绑包，则该捆绑包中的每个证书都会显示在各自的子选项卡上。

a. 选择*下载证书*或*下载 CA 捆绑包*。

如果要下载 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书都将作为单个文件下载。

b. 指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果使用可选的 CA 捆绑包，则捆绑包中的每个证书都显示在其自己的子选项卡上。

a. 选择 **Copy certificate PEM** 或 **Copy CA bundle PEM**。

如果要复制 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书将一起复制。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存带有扩展名 `.pem`的文本文件。

例如： `storagegrid_certificate.pem`

在 **StorageGRID** 中配置 **S3 API** 证书

您可以替换或恢复用于 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贵组织。

Swift 详细信息已从此版本的文档网站中删除。请参阅 "StorageGRID 11.8：配置 S3 和 Swift API 证书"。

关于此任务

默认情况下，每个存储节点都会颁发由网格 CA 签名的 X.509 服务器证书。这些 CA 签名的证书可以替换为单个通用自定义服务器证书和相应的私钥。

所有存储节点都使用单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，则必须将该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，您可能还需要在将用于访问系统的 S3 API 客户端中安装网格 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效而中断，当根服务器证书即将过期时，将触发 **S3 API** 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，并在全局选项卡上查看 S3 API 证书的到期日期，来了解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** 证书。
3. ${post_edited_translations.segment}
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：

   - ${post_edited_translations.segment}
   - 证书私钥：自定义服务器证书私钥文件 (`.key`）。

     EC 私钥必须为 224 位或更大。RSA 私钥必须为 2048 位或更大。

   - **CA bundle**：包含来自每个中间颁发证书颁发机构的证书的单个可选文件。文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。

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 捆绑包，则每个证书都会显示在自己的选项卡上。

   - 选择*下载证书*保存证书文件，或选择*下载 CA 捆绑包*保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. 选择 **Save**。

   自定义服务器证书用于后续新的 S3 客户端连接。

生成证书

${post_edited_translations.segment}

a. 选择*生成证书*。

b. 指定证书信息：

字段	问题描述
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 主题或标识名 (DN)。 如果在此字段中未输入任何值，则生成的证书将使用第一个域名或 IP 地址作为使用者通用名称 (CN)。
有效天数	创建后证书过期的天数。

字段	问题描述
添加密钥使用扩展	${post_edited_translations.segment} ${post_edited_translations.segment} ${post_edited_translations.segment}

c. 选择 **Generate**。

d. 选择*证书详细信息*以显示已生成的自定义 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 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

e. 选择 **Save**。

自定义服务器证书用于后续新的 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、上传的 CA 签名证书或生成的自定义证书的元数据。

${post_edited_translations.segment}

6. ${post_edited_translations.segment}
7. 添加自定义 S3 API 证书后，S3 API 证书页面会显示正在使用的自定义 S3 API 证书的详细信息。+ 您可以根据需要下载或复制证书 PEM。

还原默认 **S3 API** 证书

对于到存储节点的 S3 客户端连接，您可以还原为使用默认的 S3 API 证书。但是，不能对负载平衡器端点使用默认的 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** 证书。
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，无法从系统中恢复。默认 S3 API 证书将用于后续到存储节点的新 S3 客户端连接。

4. 选择 **OK** 确认警告并恢复默认 S3 API 证书。

   如果您具有根访问权限，并且自定义 S3 API 证书用于负载平衡器端点连接，则会显示无法再使用默认 S3 API 证书访问的负载平衡器端点列表。转到 "配置负载平衡器端点" 以编辑或删除受影响的端点。

5. ${post_edited_translations.segment}

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** 证书。
3. 选择 **Server** 或 **CA bundle** 选项卡，然后下载或复制证书。

${post_edited_translations.segment}

下载证书或 CA 捆绑包 `.pem`文件。如果您使用的是可选的 CA 捆绑包，则该捆绑包中的每个证书都会显示在各自的子选项卡上。

a. 选择*下载证书*或*下载 CA 捆绑包*。

   如果要下载 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书都将作为单个文件下载。

b. 指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果使用可选的 CA 捆绑包，则捆绑包中的每个证书都显示在其自己的子选项卡上。

a. 选择 **Copy certificate PEM** 或 **Copy CA bundle PEM**。

   如果要复制 CA 捆绑包，CA 捆绑包辅助选项卡中的所有证书将一起复制。

b. 将复制的证书粘贴到文本编辑器中。

c. 保存带有扩展名 `.pem`的文本文件。

   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，此证书不会更改。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

关于此任务

如果已配置自定义服务器证书，则客户端应用程序应使用自定义服务器证书验证服务器。它们不应从 StorageGRID 系统中复制 CA 证书。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，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 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

复制证书 **PEM**

复制证书文本以粘贴到其他位置。

a. 选择 **Copy certificate PEM**。
b. 将复制的证书粘贴到文本编辑器中。
c. 保存带有扩展名 `.pem`的文本文件。

例如： `storagegrid_certificate.pem`

为 **FabricPool** 配置 **StorageGRID** 证书

对于执行严格主机名验证且不支持禁用严格主机名验证的 S3 客户端，例如使用 FabricPool 的 ONTAP 客户端，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

- 您有 "特定访问权限"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

创建负载平衡器端点时，可以生成自签名服务器证书或上载由已知证书颁发机构 (CA) 签名的证书。在生产环境中，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，因为它们能够更好地防御中间人攻击。

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程序，请参见 "为 FabricPool 配置 StorageGRID"。

步骤

1. 可选操作：配置供 FabricPool 使用的高可用性 (HA) 组。
2. 创建供 FabricPool 使用的 S3 负载平衡器端点。

   当您创建 HTTPS 负载均衡器端点时，系统会提示您上传服务器证书、证书私钥和可选的 CA 捆绑包。

3. 在 ONTAP 中将 StorageGRID 附加为云层。

   指定上传的 CA 证书中使用的负载均衡器端点端口和完全限定域名。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 证书由根 CA 直接颁发，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，为外部工具监控 StorageGRID 提供了一种安全的方式。

如果需要使用外部监控工具访问 StorageGRID，您必须使用 Grid Manager 上传或生成客户端证书，并将证书信息复制到外部工具。

请参见 "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效而中断，当此服务器证书即将过期时，会触发*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*并在客户端选项卡上查看客户端证书的到期日期来了解当前证书的过期时间。

> 如果使用密钥管理服务器 (KMS) 保护特殊配置的设备节点上的数据，请参阅有关 "上传 KMS 客户端证书" 的具体信息。

开始之前

- ${post_edited_translations.segment}
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 要配置客户端证书：
  - 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，则具有用于配置管理接口证书的 CA、客户端证书和私钥。
  - 要上传自己的证书，证书的私钥需在本地计算机上可用。
  - 私钥必须在创建时保存或记录。如果您没有原始私钥，则必须创建一个新私钥。
- 要编辑客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 要上传自己的证书或新证书，私钥、客户端证书和 CA（如果使用）需在本地计算机上可用。

添加客户端证书

要添加客户端证书，请使用以下过程之一：

- [管理接口证书已配置]
- CA 颁发的客户端证书
- 从 Grid Manager 生成的证书

管理接口证书已配置

如果已使用客户提供的 CA、客户端证书和私钥配置管理接口证书，请使用此过程添加客户端证书。

步骤

1. 在 Grid Manager 中，选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. 选择 **Add**。
3. 请输入证书名称。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
5. 选择 **Continue**。
6. 对于*附加证书*步骤，上传管理接口证书。
   a. 选择*上传证书*。
   b. 选择*Browse*，然后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 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。
   c. 选择 **Create** 将证书保存到 Grid Manager 中。

      新证书将显示在"客户端"选项卡上。
7. 配置外部监控工具，例如 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私钥的 Prometheus 添加客户端证书，请使用此过程添加管理员客户端证书。

步骤

1. 执行"配置管理接口证书"中的步骤。
2. 在 Grid Manager 中，选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
3. 选择 **Add**。
4. 请输入证书名称。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
6. 选择 **Continue**。
7. 对于*附加证书*步骤，上传客户端证书、私钥和 CA 捆绑包文件：

a. 选择*上传证书*。

b. 选择*Browse*，然后选择客户端证书、私钥和 CA 捆绑包文件(`.pem`）。

- 选择*客户端证书详细信息*以显示证书元数据和证书 PEM。
- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

c. 选择 **Create** 将证书保存到 Grid Manager 中。

新证书显示在"客户端"选项卡上。

8. 配置外部监控工具，例如 Grafana。

从 **Grid Manager** 生成的证书

如果未配置管理接口证书，并且您计划为使用 Grid Manager 中生成证书功能的 Prometheus 添加客户端证书，请使用此过程添加管理员客户端证书。

步骤

1. 在 Grid Manager 中，选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. 选择 **Add**。
3. 请输入证书名称。
4. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
5. 选择 **Continue**。
6. 对于*附加证书*步骤，选择*生成证书*。
7. 指定证书信息：

- 主题（可选）：证书所有者的 X.509 主题或标识名（DN）。
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

8. 选择 **Generate**。
9. ${post_edited_translations.segment}

关闭对话框后，您将无法查看证书私钥。请将密钥复制或下载到安全位置。

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。
- 选择*下载证书*以保存证书文件。

指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择*复制私钥*以复制证书私钥，以便粘贴到其他位置。
- 选择*下载专用密钥*将专用密钥另存为文件。

  ${post_edited_translations.segment}

10. 选择 **Create** 将证书保存到 Grid Manager 中。

    新证书将显示在"客户端"选项卡上。

11. ${post_edited_translations.segment}
12. ${post_edited_translations.segment}
13. ${post_edited_translations.segment}
14. 从 ${post_edited_translations.segment} 步骤中上传 certificate.pem 和 private_key.pem 文件。无需上传 CA 捆绑包。
    a. ${post_edited_translations.segment}
    b. 上传每个证书文件 (`.pem`)。
    c. 选择*保存*将证书保存到 Grid Manager 中。

       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，例如 Grafana。

配置外部监控工具

步骤

1. ${post_edited_translations.segment}
   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. ${post_edited_translations.segment}
   d. 在 TLS/SSL 身份验证详细信息下，复制并粘贴：
      - 管理接口 CA 证书至 **CA Cert**
      - ${post_edited_translations.segment}
      - ${post_edited_translations.segment}
   e. **ServerName**：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 "监控 StorageGRID 的说明"。

${post_edited_translations.segment}

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 访问权限，或者在当前证书过期时上传新证书。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。

   证书过期日期和 Prometheus 访问权限列在表中。如果证书即将过期或已过期，表中会显示一条消息，并触发警报。

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 请输入证书名称。
5. 要使用外部监控工具访问 Prometheus 指标，请选择 **Allow prometheus**。
6. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

附加新客户端证书

您可以在当前证书过期时上传新证书。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。

   证书过期日期和 Prometheus 访问权限列在表中。如果证书即将过期或已过期，表中会显示一条消息，并触发警报。

2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

上传证书

复制证书文本以粘贴到其他位置。

a. ${post_edited_translations.segment}

b. 上传客户端证书名称(`.pem`）。

   选择*客户端证书详细信息*以显示证书元数据和证书 PEM。

   - 选择*下载证书*以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

c. 选择 **Create** 将证书保存到 Grid Manager 中。

   ${post_edited_translations.segment}

生成证书

生成证书文本以粘贴到其他位置。

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 主题或标识名（DN）。
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

     ${post_edited_translations.segment}

c. 选择 **Generate**。

d. 选择*客户端证书详细信息*以显示证书元数据和证书 PEM。

   关闭对话框后，您将无法查看证书私钥。请将密钥复制或下载到安全位置。

   - 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。
   - 选择*下载证书*以保存证书文件。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - 选择*复制私钥*以复制证书私钥，以便粘贴到其他位置。

- 选择*下载专用密钥*将专用密钥另存为文件。

  ${post_edited_translations.segment}

e. 选择 **Create** 将证书保存到 Grid Manager 中。

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地方使用。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. 选择要复制或下载的证书。
3. 下载或复制证书。

下载证书文件

下载证书 `.pem`文件。

a. 选择*下载证书*。
b. 指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

复制证书

复制证书文本以粘贴到其他位置。

a. 选择 **Copy certificate PEM**。
b. 将复制的证书粘贴到文本编辑器中。
c. 保存带有扩展名 `.pem`的文本文件。

例如： `storagegrid_certificate.pem`

删除客户端证书

如果您不再需要管理员客户端证书，则可以将其删除。

步骤

1. 选择 **Configuration** > **Security** > **Certificates**，然后选择 **Client** 选项卡。
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

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 策略确定使用哪些协议和密码与客户端应用程序建立安全的 TLS 连接，以及与内部 StorageGRID 服务建立安全的 SSH 连接。

安全策略控制 TLS 和 SSH 如何加密传输中的数据。通常，使用 Modern compatibility（默认）策略，除非您的系统需要符合 Common Criteria 标准，或者您需要使用其他密码。

某些 StorageGRID 服务尚未更新为使用这些策略中的密码。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

选择安全策略

步骤

1. 选择*配置* > 安全 > 安全设置。

   TLS and SSH policies 选项卡显示可用策略。当前有效的策略在策略图块上以绿色复选标记标注。

2. 查看选项卡以了解可用的策略。

现代兼容性（默认）

如果您需要强加密且没有特殊要求，请使用默认策略。此策略与大多数 TLS 和 SSH 客户端兼容。

旧版兼容性

如果您需要旧版客户端的其他兼容性选项，请使用旧版兼容性策略。此策略中的其他选项可能会使其安全性低于新式兼容性策略。

通用标准

如果您需要Common Criteria认证，请使用Common Criteria策略。

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) 3.0.8 或 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模块进行与负载均衡器端点、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 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模块用于以下操作：

- NCSM
  - 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
  - 客户端与 nginx-gw 服务（负载均衡器端点）之间的 TLS 连接
  - 客户端与 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 #4838"。
- NetApp StorageGRID 内核加密 API 模块

  NetApp StorageGRID 内核加密 API 模块仅存在于 VM 和 StorageGRID 设备平台上。
  - 熵收集
  - 节点加密

  有关详细信息，请参见 NIST Cryptographic Algorithm Validation Program "证书 #A6242 至 #A6257"和 "熵证书 #E223"。

注意：选择此策略后，"执行滚动重启"所有节点都要激活 NCSM。使用 维护 > 滚动重启 来启动和监控重启。

自定义

如果需要应用自己的密码，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 3.0.8 和 NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 模块：

a. 将 `fipsMode`参数设置为 `true`。

b. 出现提示时，"执行滚动重启"让所有节点激活加密模块。使用 **Maintenance** > **Rolling reboot** 启动和监控重启。

c. 选择 **Support** > **Diagnostics** 以查看活动的 FIPS 模块版本。

3. 要查看每个策略的密码、协议和算法的详细信息，请选择 **View details**。
4. 要更改当前策略，请选择 **Use policy**。

   策略磁贴上的*当前策略*旁边会显示一个绿色复选标记。

创建自定义安全策略

如果需要应用自己的密码，则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图块中，选择*查看详细信息*。
2. 选择*复制到剪贴板*，然后选择*取消*。

3. 在*自定义策略*图块中，选择*配置和使用*。
4. 粘贴您复制的 JSON 并进行所需的更改。
5. 选择*使用策略*。

   自定义策略磁贴上的*当前策略*旁边会显示一个绿色复选标记。

6. （可选）选择*编辑配置*以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，且配置的 TLS 策略与 "已配置的服务器证书" 不兼容，则可能无法登录到 Grid Manager。

您可以暂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 `Passwords.txt`文件中列出的密码。
   c. 输入以下命令切换到 root： `su -`
   d. 输入 `Passwords.txt`文件中列出的密码。

      以 root 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. 在 Web 浏览器中，访问同一管理节点上的 Grid Manager。
4. 请按照 选择安全策略 中的步骤重新配置策略。

配置 **StorageGRID** 网络和对象安全性

您可以配置网络和对象安全性，以加密存储的对象，防止某些 S3 请求，或允许客户端连接到 Storage Nodes 时使用 HTTP 而不是 HTTPS。

存储对象加密

存储对象加密可对通过 S3 摄取的所有对象数据进行加密。默认情况下，存储的对象不会加密，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，所有新摄取的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密，当前已加密的对象将保持加密状态，但新摄取的对象将不会被加密。

存储对象加密设置仅适用于未通过存储桶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"。

防止客户端修改

防止客户端修改是系统范围内的设置。当选择*防止客户端修改*选项时，以下请求将被拒绝。

S3 REST API

- DeleteBucket 请求
- 任何修改现有对象数据、用户定义元数据或 S3 对象标记的请求

为存储节点连接启用 **HTTP**

默认情况下，客户端应用程序使用 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，才对存储节点连接使用 HTTP。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，不需要使用此选项（因为您可以"配置每个负载均衡器端点"使用 HTTP 或 HTTPS）。

请参阅"摘要：客户端连接的 IP 地址和端口"以了解 S3 客户端在使用 HTTP 或 HTTPS 连接到 Storage Nodes 时使用的端口。

选择选项

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- ${post_edited_translations.segment}

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. 对于存储对象加密，如果您不希望对存储对象进行加密，请使用 **None**（默认）设置，或选择 **AES-128** 或 **AES-256** 对存储对象进行加密。
4. 如果要阻止 S3 客户端发出特定请求，可以选择*防止客户端修改*。

   如果更改此设置，应用新设置大约需要一分钟。配置的值将被缓存以提升性能和扩展能力。

5. 如果客户端直接连接到存储节点并且要使用 HTTP 连接，则可选择*为存储节点连接启用 HTTP*。

   ${post_edited_translations.segment}

6. 选择 **Save**。

更改 **StorageGRID** 接口安全设置

通过界面安全设置，可以控制用户在超过指定时间内处于非活动状态时是否自动注销，以及 API 错误响应中是否包含堆栈跟踪。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

*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

指示在用户注销之前，用户的浏览器可以处于非活动状态的时间长度。默认时间为 15 分钟。

浏览器非活动超时也受以下因素控制：

- 一个单独的、不可配置的 StorageGRID 计时器，用于系统安全。每个用户的身份验证令牌在用户登录后 16 小时过期。当用户的身份验证过期时，即使浏览器非活动超时已禁用或尚未达到浏览器超时的值，该用户也会自动注销。要续订令牌，用户必须重新登录。
- 身份提供程序的超时设置，假设已为 StorageGRID 启用单点登录 (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。请参阅 "SSO 的工作原理"。

管理 **API** 堆栈跟踪

控制是否在 Grid Manager 和 Tenant Manager API 错误响应中返回堆栈跟踪。

此选项默认处于禁用状态，但您可能希望为测试环境启用此功能。一般来说，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*界面*选项卡。
3. 要更改浏览器非活动超时的设置，请执行以下操作：
   a. 展开折叠面板。
   b. 要更改超时时间段，请指定一个介于 60 秒和 7 天之间的值。默认超时时间为 15 分钟。
   c. 要禁用此功能，请取消选中该复选框。
   d. 选择 **Save**。

   此新设置不会影响当前登录的用户。要使新的超时设置生效，用户必须重新登录或刷新浏览器。
4. 要更改 Management API 堆栈跟踪的设置，请执行以下操作：
   a. 展开折叠面板。
   b. 选中复选框以在 Grid Manager 和 Tenant Manager 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 **Save**。

在 **StorageGRID** 中管理外部 **SSH** 访问

通过阻止或允许外部访问，管理进入网格的入站流量的 SSH 访问。管理 SSH 外部访问不会对网格中节点之间的流量产生影响。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

为增强系统安全性，默认情况下会阻止外部 SSH 访问。如果需要执行需要入站 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，请阻止外部访问。

步骤

1. 选择*配置* > 安全 > 安全设置。
2. 选择 **Block 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. 取消选中该复选框以允许访问。

> 需要访问服务笔记本电脑和所有其他网格节点之间的端口 22。完成维护任务后，请删除端口 22 的访问权限。

4. 选择 **Save**。

配置密钥管理服务器

了解 **StorageGRID** 中的密钥管理服务器

${post_edited_translations.segment}

StorageGRID 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 互操作性矩阵工具 (IMT)"。

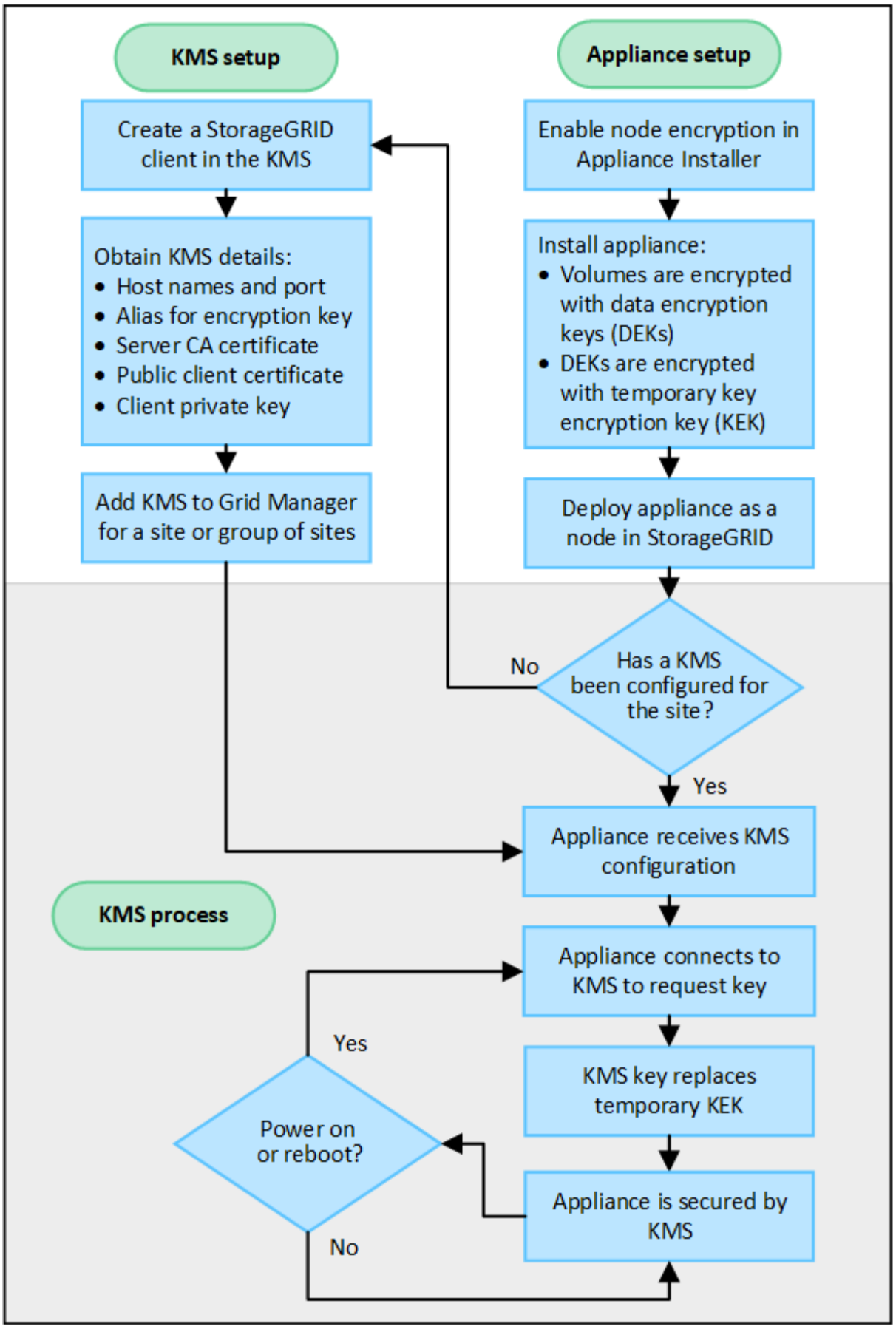
您可以使用一个或多个密钥管理服务器来管理在安装期间启用了 节点加密 设置的任何 StorageGRID 设备节点的节点加密密钥。将密钥管理服务器与这些设备节点结合使用，即使设备从数据中心移出，也可以保护您的数据。在对设备卷进行加密后，除非节点可以与 KMS 进行通信，否则您将无法访问该设备上的任何数据。

> StorageGRID 不创建或管理用于对应用装置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，您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。执行密钥管理任务超出了这些说明的范围。如果您需要帮助，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，您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。

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。



流程图显示并行进行的 KMS 设置和设备设置；但是，您可以根据需求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。

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤	请参阅
${post_edited_translations.segment}	"${post_edited_translations.segment}"
在 KMS 上获取 StorageGRID 客户端所需的信息。	"${post_edited_translations.segment}"
将 KMS 添加到网格管理器，将其分配给单个站点或默认站点组，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

设置用于 KMS 的设备节点包括以下高级步骤。

1. ${post_edited_translations.segment}

   > 将设备添加到网格后，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 装置安装程序。在安装过程中，系统会为每个装置卷分配一个随机数据加密密钥 (DEK)，如下所示：
   - DEK 用于加密每个卷上的数据。这些密钥是使用设备 OS 中的 Linux Unified Key Setup (LUKS) 磁盘加密生成的，且无法更改。
   - 每个 DEK 都由主密钥加密密钥（KEK）加密。初始 KEK 是一个临时密钥，用于加密 DEK，直到设备可以连接到 KMS。
3. ${post_edited_translations.segment}

有关详细信息，请参见 "启用节点加密"。

${post_edited_translations.segment}

${post_edited_translations.segment}

1. 当您将启用了节点加密的设备安装到网格中时，StorageGRID 会确定包含新节点的站点是否存在 KMS 配置。
   - ${post_edited_translations.segment}
   - 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 并且设备收到 KMS 配置。
2. 设备使用 KMS 配置连接到 KMS 并请求加密密钥。
3. KMS 向设备发送加密密钥。来自 KMS 的新密钥取代了临时 KEK，现在用于加密和解密设备卷的 DEK。

在加密设备节点连接到配置的 KMS 之前存在的任何数据都会使用临时密钥进行加密。但是，在临时密钥被 KMS 加密密钥替换之前，不应认为设备卷已受到保护，可防止从数据中心中被移除。

4. 如果设备已通电或重新启动，则会重新连接到 KMS 以请求密钥。密钥保存在易失性内存中，无法在断电或重新启动后保留。

StorageGRID 密钥管理服务器要求和注意事项

${post_edited_translations.segment}

${post_edited_translations.segment}

StorageGRID 支持 KMIP 版本 1.4。

"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(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具有对您为该站点配置的 KMS 或 KMS 集群的网络访问权限。

支持哪些版本的 **TLS**?

设备节点与配置的 KMS 之间的通信使用安全的 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 支持的协议以及您正在使用的 "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，请查看网格的活动 TLS 和 SSH 策略的 `tlsOutbound`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(KMS)管理网格中已启用*节点加密*设置的任何 StorageGRID 设备的加密密钥。此设置只能在使用 StorageGRID Appliance Installer 安装设备的硬件配置阶段启用。

将设备添加到网格后，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。

您可以将配置的 KMS 用于 StorageGRID 设备和设备节点。

您不能将配置的 KMS 用于基于软件的（非设备）节点，其中包括：

- 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

部署在这些其他平台上的节点可以在数据存储库或磁盘级别使用 StorageGRID 外部的加密。

何时应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 Grid Manager 中设置一个或多个密钥管理服务器。此顺序可确保在节点上存储任何对象数据之前对其进行保护。

您可以在安装设备节点之前或之后在 Grid Manager 中配置密钥管理服务器。

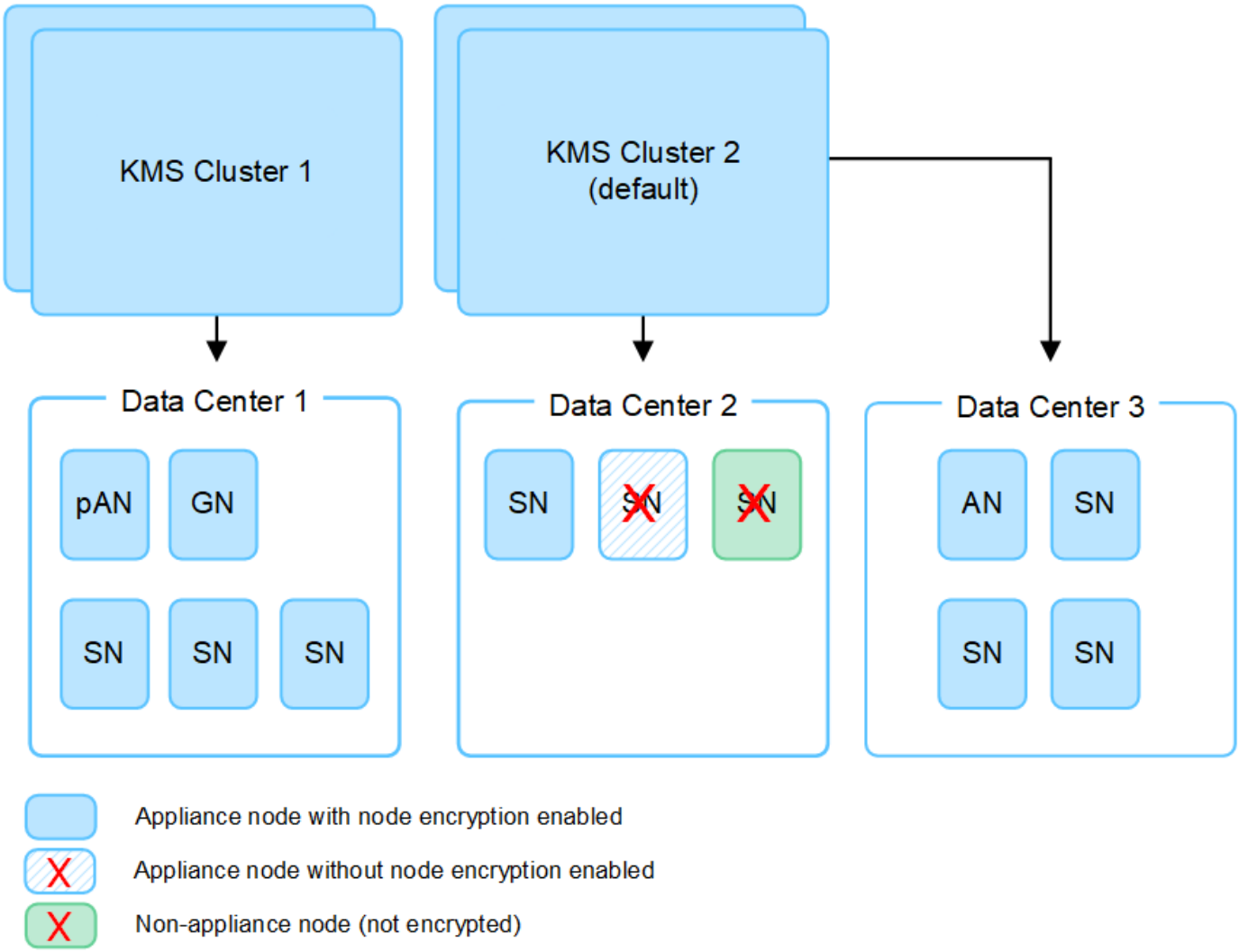
我需要多少密钥管理服务器?

您可以配置一个或多个外部密钥管理服务器，为 StorageGRID 系统中的设备节点提供加密密钥。每个 KMS 为单个站点或一组站点的 StorageGRID 设备节点提供单个加密密钥。

StorageGRID 支持使用 KMS 集群。每个 KMS 集群包含多个共享配置设置和加密密钥的复制密钥管理服务器。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能力。

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 集群配置为向数据中心 1 的所有设备节点提供密钥，并将另一个 KMS 集群配置为向所有其他站点的所有设备节点提供密钥。添加第二个 KMS 集群时，可以为数据中心 2 和数据中心 3 配置默认 KMS。

请注意，您不能将 KMS 用于非设备节点或安装期间未启用*节点加密*设置的任何设备节点。



作为安全最佳做法，您应定期"轮换加密密钥"每个已配置的 KMS 所使用的内容。

当新的密钥版本可用时：

- 它会自动分发到与 KMS 关联的一个或多个站点上的加密设备节点。分发应在密钥轮换后的一小时内完成。
- 如果在分发新密钥版本时加密的设备节点处于离线状态，则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应用装置卷进行加密，则会针对该应用装置节点触发 **KMS** 加密密钥轮换失败 警报。您可能需要联系技术支持以协助解决此警报。

${post_edited_translations.segment}

如果需要将加密设备安装到另一个 StorageGRID 系统中，则必须首先停用网格节点以将对象数据移动到另一个节点。然后，您可以使用 StorageGRID Appliance Installer "清除 KMS 配置"。清除 KMS 配置将禁用 **Node Encryption** 设置，并删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。

由于无法访问 KMS 加密密钥，设备上的任何剩余数据将无法再被访问，并被永久锁定。

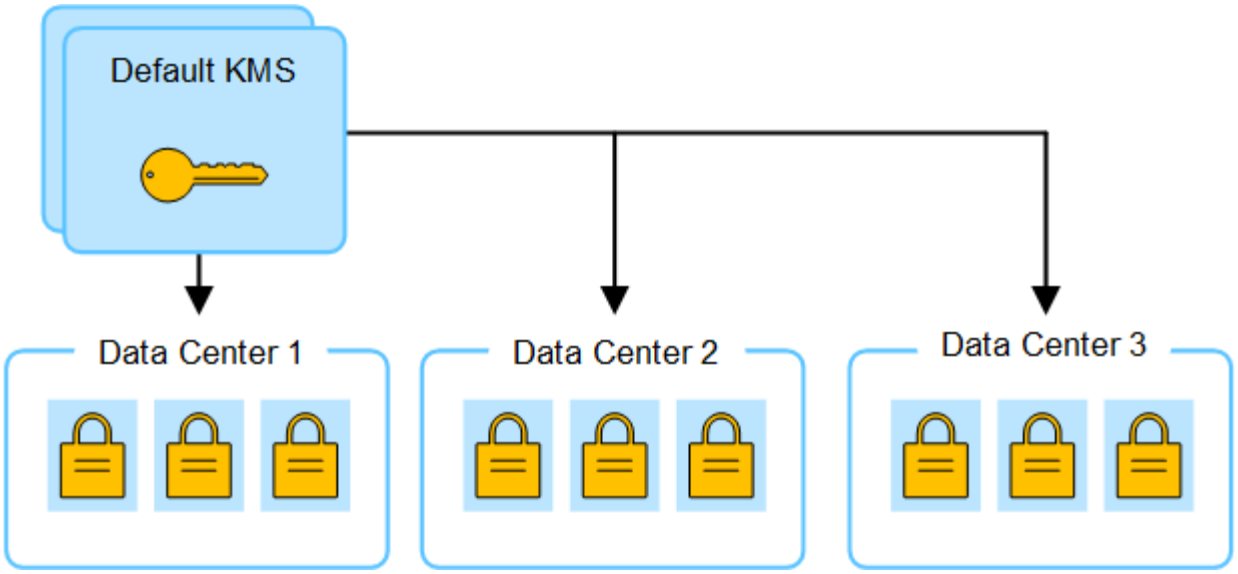
更改 **StorageGRID** 站点 **KMS** 的注意事项

每个密钥管理服务器(KMS)或 KMS 集群为单个站点或一组站点的所有设备节点提供加密密钥。如果您需要更改用于站点的 KMS，则可能需要将加密密钥从一个 KMS 复制到另一个 KMS。

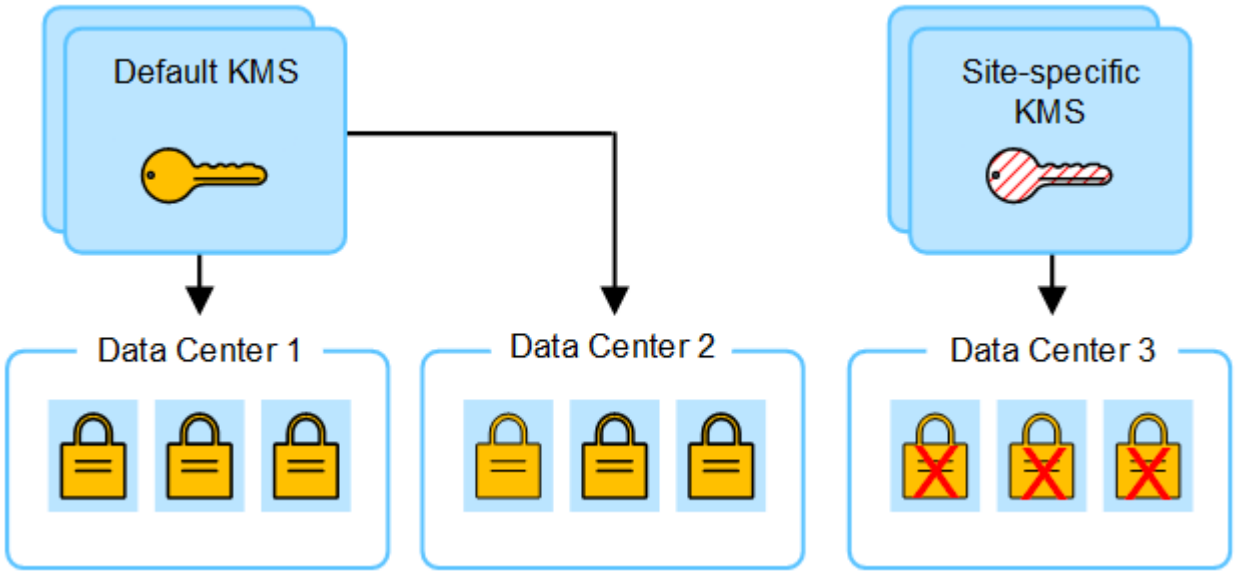
如果您更改了用于某个站点的 KMS，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS。您必须确保 KMS 具有正确的密钥，以便对该站点上加密的设备节点进行解密。

例如：

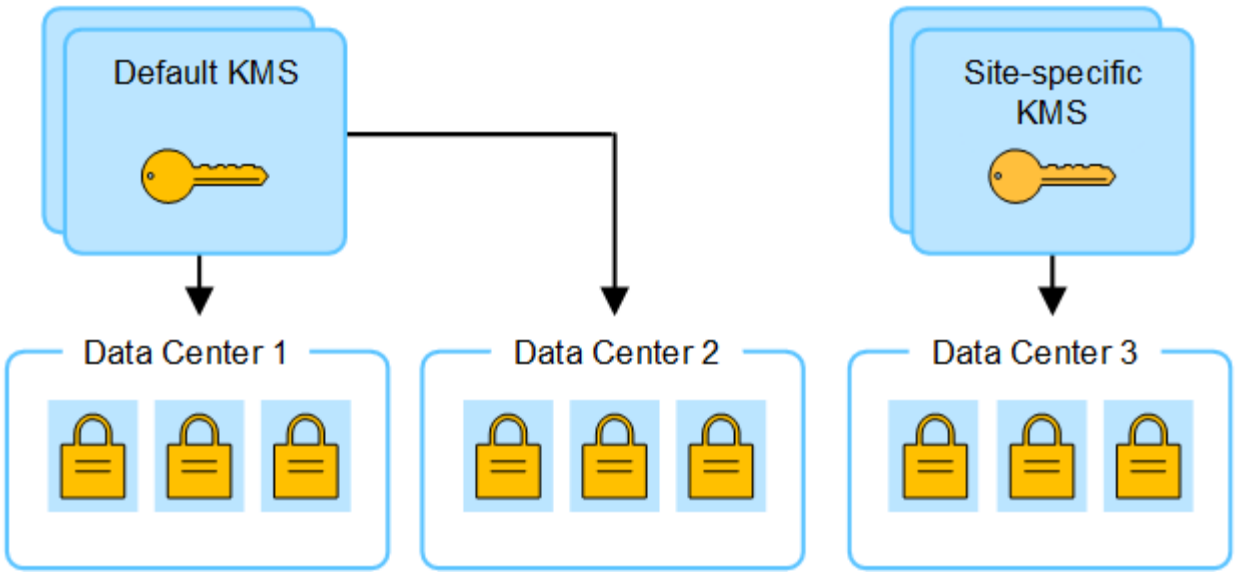
1. ${post_edited_translations.segment}
2. 保存 KMS 时，所有启用了 节点加密 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于加密所有站点上的设备节点。必须使用同一密钥对这些设备进行解密。



3. 您决定为一个站点添加特定于站点的 KMS（图中的数据中心 3）。但是，由于设备节点已加密，因此在尝试保存站点特定 KMS 的配置时会出现验证错误。此错误的原因是站点特定的 KMS 没有正确的密钥来解密该站点上的节点。



4. 要解决此问题，请将当前版本的加密密钥从默认 KMS 复制到新 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。）站点特定的 KMS 现在具有正确的密钥来解密 Data Center 3 的设备节点，因此可以将其保存在 StorageGRID 中。



用于更改站点使用的 **KMS** 的用例

该表总结了更改站点 KMS 的最常见情况所需的步骤。

更改站点 **KMS** 的用例	所需步骤
${post_edited_translations.segment}	编辑站点特定的 KMS。在 **Manages keys for** 字段中，选择 **Sites not managed by another KMS (default KMS)**。站点特定的 KMS 现在将用作默认 KMS。它将适用于任何没有专用 KMS 的站点。 "编辑密钥管理服务器（KMS）"
您拥有默认 KMS，并在扩容中添加了新站点。您不想对新站点使用默认 KMS。	1. ${post_edited_translations.segment} 2. ${post_edited_translations.segment} "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 Grid Manager，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)"

${post_edited_translations.segment}

在将 KMS 添加到 StorageGRID 之前，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。

这些说明适用于 Thales CipherTrust Manager 和 Hashicorp Vault。有关受支持产品和版本的列表，请使用 "NetApp 互操作性矩阵工具 (IMT)"。

步骤

1. 从 KMS 软件中，为您计划使用的每个 KMS 或 KMS 集群创建一个 StorageGRID 客户端。

   ${post_edited_translations.segment}

2. 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。在 "上传客户端证书" 之后进行测试并保存时，系统将提示您。

3. 记录每个KMS或KMS集群的以下信息。

   将 KMS 添加到 StorageGRID 时，您需要以下信息：

   - 每台服务器的主机名或 IP 地址。
   - KMS 使用的 KMIP 端口。
   - ${post_edited_translations.segment}

4. 对于每个 KMS 或 KMS 集群，获取由证书颁发机构 (CA) 签名的服务器证书，或包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件的证书包。

   ${post_edited_translations.segment}

   - 证书必须使用隐私增强邮件 (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将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 **Hostname** 字段中输入相同的 FQDN 或 IP 地址。

   - ${post_edited_translations.segment}

5. 获取外部 KMS 颁发给 StorageGRID 的公共客户端证书和客户端证书的私钥。

   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

${post_edited_translations.segment}

开始之前

- 您已审阅 "使用密钥管理服务器的注意事项和要求"。
- 您拥有"在 KMS 中将 StorageGRID 配置为客户端"，并且您拥有每个KMS或KMS集群所需的信息。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

如果可能，在配置适用于不由其他 KMS 管理的所有站点的默认 KMS 之前，请配置任何特定于站点的密钥管理服务器。如果首先创建默认 KMS，则网格中的所有节点加密设备都将使用默认 KMS 进行加密。如果要在以后创建站点特定的 KMS，则必须首先将当前版本的加密密钥从默认 KMS 复制到新 KMS。有关详细信息，请参阅 "更改站点 KMS 的注意事项"。

步骤 1：KMS 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，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 **Create**。

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

字段	问题描述
KMS 名称	用于帮助您识别此 KMS 的描述性名称。必须介于 1 到 64 个字符之间。
密钥名称	KMS 中 StorageGRID 客户端的确切密钥别名。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。
${post_edited_translations.segment}	将与此 KMS 关联的 StorageGRID 站点。如果可能，应先配置特定站点的密钥管理服务器，再配置适用于所有非其他 KMS 管理站点的默认 KMS。 • 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 **Sites not managed by another KMS (default KMS)** 以配置默认 KMS，该默认 KMS 将应用于没有专用 KMS 的任何站点以及您在后续扩展中添加的任何站点。 ${post_edited_translations.segment}
端口	KMS 服务器用于密钥管理互操作性协议 (KMIP) 通信的端口。默认为 5696，即 KMIP 标准端口。

字段	问题描述
主机名称	${post_edited_translations.segment} 注意： 服务器证书的“主题备用名称 (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 集群，请选择 添加另一个主机名 为集群中的每个服务器添加主机名。
5. 选择 **Continue**。

${post_edited_translations.segment}

在“添加密钥管理服务器”向导的第 2 步（上传服务器证书）中，您需要上传 KMS 的服务器证书（或证书包）。服务器证书允许外部 KMS 向 StorageGRID 进行自身身份验证。

步骤

1. ${post_edited_translations.segment}
2. 上传证书文件。

   此时将显示服务器证书元数据。

   ${post_edited_translations.segment}

3. 选择 **Continue**。

${post_edited_translations.segment}

在添加密钥管理服务器向导的步骤 3（上载客户端证书）中，上载客户端证书和客户端证书私钥。客户端证书允许 StorageGRID 向 KMS 进行身份验证。

步骤

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

3. 浏览到客户端证书专用密钥的位置。
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

   如果密钥不存在，系统会提示您让 StorageGRID 创建一个密钥。

   测试密钥管理服务器和设备节点之间的连接。如果所有连接都有效，并且在 KMS 上找到了正确的密钥，则会将新的密钥管理服务器添加到"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. ${post_edited_translations.segment}

   例如，如果连接测试失败，您可能会收到 422: Unprocessable Entity 错误。

7. ${post_edited_translations.segment}

   > 选择*强制保存*将保存 KMS 配置，但不会测试每个设备到该 KMS 的外部连接。如果配置出现问题，则可能无法重新启动在受影响站点上启用了节点加密的设备节点。在问题得到解决之前，您可能会失去对数据的访问权限。

8. 查看确认警告，如果确定要强制保存配置，请选择*OK*。

   ${post_edited_translations.segment}

在 **StorageGRID** 中管理密钥管理服务器

管理密钥管理服务器 (KMS) 涉及查看或编辑详细信息、管理证书、查看加密节点以及在不再需要时删除 KMS。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "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。
   - 已加密节点选项卡列出已启用节点加密的任何节点。

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	问题描述
${post_edited_translations.segment}	与 KMS 关联的 StorageGRID 站点。 此字段显示特定 StorageGRID 站点或*不由其他 KMS 管理的站点的名称（默认 KMS）。*

字段	问题描述
主机名称	KMS 的完全限定域名或 IP 地址。 如果有两个密钥管理服务器的集群，则列出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 并选择*编辑*或*操作* > 编辑。

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	问题描述
关键详细信息	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. 根据组织安全实践的要求，选择*Rotate key*，或使用 KMS 软件创建新版本的密钥。

密钥轮换成功后，将更新密钥 UID 和上次修改字段。

> 如果您使用 KMS 软件轮换加密密钥，请将其从该密钥上次使用的版本轮换为同一密钥的新版本。请勿轮换为完全不同的密钥。
>
> 切勿尝试通过更改 KMS 的密钥名称（别名）来轮换密钥。StorageGRID 要求所有以前使用的密钥版本（以及任何未来的密钥版本）都可以使用相同的密钥别名从 KMS 访问。如果更改已配置的 KMS 的密钥别名，StorageGRID 可能无法解密您的数据。

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，请在证书过期前更换。

> 您必须尽快解决任何证书问题，以保持数据访问权限。

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 的证书过期值。
3. 如果任何 KMS 的证书过期时间为未知，请等待最多 30 分钟，然后刷新您的 Web 浏览器。
4. ${post_edited_translations.segment}
   a. 选择 **Server certificate** 并验证"Expires on"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，选择*客户端证书*而不是服务器证书。
5. 当 **KMS CA** 证书过期、*KMS 客户端证书过期*和 *KMS 服务器证书过期*警报触发时，请注意每个警报的描述并执行建议的操作。

   StorageGRID 可能需要长达 30 分钟才能获取证书过期的更新。刷新 Web 浏览器以查看当前值。

${post_edited_translations.segment}

查看加密节点

您可以查看有关在您的 StorageGRID 系统中启用了 **Node Encryption** 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. ${post_edited_translations.segment}

   加密节点选项卡列出了 StorageGRID 系统中已启用*节点加密*设置的设备节点。

3. 查看表格中每个设备节点的信息。

列	问题描述
节点名称	${post_edited_translations.segment}
节点类型	节点的类型：Storage、Admin 或 Gateway。
站点	安装节点的 StorageGRID 站点的名称。
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)"

列	问题描述
密钥 UID	用于对应用装置节点上的数据进行加密和解密的加密密钥的唯一 ID。要查看完整的密钥 UID，请选择该文本。 破折号(--)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。
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，连接状态可能需要几分钟才能更新。 *注意：*刷新您的网络浏览器以查看新值。

4. ${post_edited_translations.segment}

   在正常的 KMS 操作期间，状态将为 **Connected to 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：

   - ${post_edited_translations.segment}
   - KMS 连接错误
   - 未找到 KMS 加密密钥名称
   - KMS加密密钥轮换失败
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   您必须立即解决任何问题，以确保您的数据得到充分保护。

编辑 KMS

您可能需要编辑密钥管理服务器的配置，例如，如果证书即将过期。

开始之前

- 如果您计划更新为 KMS 选择的站点，则表示您已阅读 "${post_edited_translations.segment}"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

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. ${post_edited_translations.segment}

您还可以通过在表中选择KMS名称并在KMS详细信息页面上选择*编辑*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	问题描述
KMS 名称	用于帮助您识别此 KMS 的描述性名称。必须介于 1 到 64 个字符之间。
密钥名称	KMS 中 StorageGRID 客户端的确切密钥别名。必须介于 1 到 255 个字符之间。 您只需要在极少数情况下编辑密钥名称。例如，如果别名在 KMS 中重命名，或者如果上一个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。
${post_edited_translations.segment}	如果您正在编辑特定于站点的 KMS，并且尚无默认 KMS，则可以选择 未由其他 **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，该 KMS 将适用于所有没有专用 KMS 的站点以及在扩容中添加的任何站点。 *注意：*如果您正在编辑特定于站点的 KMS，则无法选择其他站点。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 (KMIP) 通信的端口。默认为 5696，即 KMIP 标准端口。
主机名称	${post_edited_translations.segment} 注意： 服务器证书的“主题备用名称 (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 集群，请选择 添加另一个主机名 为集群中的每个服务器添加主机名。
5. 选择 **Continue**。

   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. 如果需要更换服务器证书，请选择*浏览*并上传新文件。
7. 选择 **Continue**。

   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. ${post_edited_translations.segment}
9. ${post_edited_translations.segment}

   对受影响站点的密钥管理服务器和所有节点加密设备节点之间的连接进行了测试。如果所有节点连接都有效，并且在 KMS 上找到了正确的密钥，则会将密钥管理服务器添加到"密钥管理服务器"页面上的表中。

10. 如果出现错误消息，请查看消息详情，然后选择*OK*。

${post_edited_translations.segment}

11. 如果需要在解决连接错误之前保存当前配置，请选择*强制保存*。

> 选择*强制保存*将保存 KMS 配置，但不会测试每个设备到该 KMS 的外部连接。如果配置出现问题，则可能无法重新启动在受影响站点上启用了节点加密的设备节点。在问题得到解决之前，您可能会失去对数据的访问权限。

KMS 配置已保存。

12. 查看确认警告，如果确定要强制保存配置，请选择*OK*。

已保存 KMS 配置，但未测试与 KMS 的连接。

${post_edited_translations.segment}

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，则可能需要删除特定于站点的 KMS。

开始之前

- 您已审阅 "使用密钥管理服务器的注意事项和要求"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

关于此任务

在以下情况下，您可以删除 KMS：

- 如果站点已停用或站点不包括启用了节点加密的设备节点，则可以删除站点特定的KMS。
- ${post_edited_translations.segment}

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*操作* > 删除。

${post_edited_translations.segment}

3. 确认是否满足以下条件：
   - ${post_edited_translations.segment}
   - 您正在删除默认的 KMS，但每个具有节点加密的站点已经存在特定于站点的 KMS。
4. ${post_edited_translations.segment}

已删除 KMS 配置。

管理代理服务器设置

配置 StorageGRID 存储代理

如果使用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，以允许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

- 您有 "特定访问权限"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

您可以配置单个存储代理的设置。

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：HTTP 为 80，SOCKS5 为 1080。

6. 选择 **Save**。

   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。

   > 代理服务器更改最多可能需要 10 分钟才能生效。

7. 请检查代理服务器的设置，以确保来自 StorageGRID 的平台服务相关消息不会被阻止。
8. 如果需要禁用存储代理，请清除复选框，然后选择*保存*。

在 StorageGRID 中配置管理代理设置

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之间配置非透明代理服务器（AutoSupport）。

有关 AutoSupport 的详细信息，请参见 "配置 AutoSupport"。

开始之前

- 您有 "特定访问权限"。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

关于此任务

您可以配置单个管理代理的设置。

步骤

1. 选择*配置* > 安全 > 代理设置。

   此时将显示"代理服务器设置"页面。默认情况下，在选项卡菜单中选择"存储"。

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. 请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。

   如果您的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：

   - 如果要保护与管理代理的连接，请选择*验证代理证书*。上传 CA 捆绑包以验证管理代理服务器提供的 SSL 证书的真实性。

     AutoSupport on Demand、通过 StorageGRID 的 E-Series AutoSupport 以及 StorageGRID 升级页面上的更新路径确定，在验证代理证书后将无法正常工作。

   上传 CA 捆绑包后，将显示其元数据。

   - 如果在与管理员代理服务器通信时不想验证证书，请选择*Do not verify proxy certificate*。

8. 选择 **Save**。

   保存管理员代理后，将配置管理节点与技术支持之间的代理服务器。

   代理服务器更改最多可能需要 10 分钟才能生效。

9. 如果您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*。

控制防火墙

在外部防火墙处控制 **StorageGRID** 访问

您可以在外部防火墙上打开或关闭特定端口。

您可以通过在外部防火墙上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，除了使用其他方法来控制系统访问之外，您可能还希望阻止租户在防火墙处连接到 Grid Manager。

如果要配置 StorageGRID 内部防火墙，请参见 "配置内部防火墙"。

端口	问题描述	如果端口打开.....
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 Grid Manager、Grid Management API、Tenant Manager 和 Tenant Management API。 注意： 端口 443 也用于一些内部流量。
8443	管理节点上的受限 Grid Manager 端口	• 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 Tenant Manager 或 Tenant Management API。 • 对内部内容的请求将被拒绝。
9443	管理节点上的受限租户管理器端口	• 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 Grid Manager 或网格管理 API。 • 对内部内容的请求将被拒绝。

单点登录 (SSO) 在受限 Grid Manager 或 Tenant Manager 端口上不可用。如果希望用户使用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 在每个节点上包含一个内部防火墙，通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止所有端口上的网络访问，特定网格部署所必需的端口除外。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可自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡可允许选定访问已关闭的端口。您可以添加 CIDR 表示法的 IP 地址或子网，这些地址或子网可以访问使用"管理外部访问"选项卡关闭的端口。
- 管理外部访问：使用此选项卡可关闭默认打开的端口，或重新打开先前已关闭的端口。
- 不受信任的客户端网络：使用此选项卡可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。

  - 具有不受信任客户端网络的节点将仅接受在该节点上配置的负载均衡器端点端口上的连接（全局、节点接口和节点类型绑定端点）。

- 无论 Manage external networks 选项卡上的设置如何，在不受信任的客户端网络上，负载均衡器端点端口_是唯一开放的端口_。
- 受信任时，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。

> 您在一个选项卡上进行的设置可能会影响您在另一个选项卡上进行的访问更改。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，请参见 "控制外部防火墙的访问"。

${post_edited_translations.segment}

“特权地址列表”选项卡使您能够注册一个或多个被授予访问已关闭网格端口权限的 IP 地址。“管理外部访问”选项卡使您能够关闭对选定外部端口或所有打开的外部端口的外部访问（外部端口是默认情况下非网格节点可访问的端口）。这两个选项卡通常可以结合使用，以自定义允许网格访问的精确网络访问权限。

> ${post_edited_translations.segment}

示例 **1**：使用跳板机执行维护任务

假设您要使用跳板机（经过安全加固的主机）进行网络管理。您可以使用以下常规步骤：

1. ${post_edited_translations.segment}
2. 使用"管理外部访问"选项卡可阻止所有端口。

> 在阻止端口 443 和 8443 之前，请先添加特权 IP 地址。当前连接到被阻止端口的任何用户（包括您）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。

保存配置后，网格中管理节点上的所有外部端口将对除跳转主机之外的所有主机被阻止。然后，您可以使用跳转主机更安全地对网格执行维护任务。

示例 **2**：锁定敏感端口

假设您要锁定敏感端口以及该端口上的服务。您可以使用以下常规步骤：

1. 使用"特权地址列表"选项卡，仅向需要访问该服务的主机授予访问权限。
2. 使用"管理外部访问"选项卡可阻止所有端口。

> 在阻止访问分配给 Grid Manager 和 Tenant Manager 的任何端口（预设端口为 443 和 8443）之前，请先添加特权 IP 地址。当前连接到被阻止端口的任何用户（包括您）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。

保存配置后，特权地址列表中的主机可以使用该敏感端口及其上的服务。无论请求来自哪个接口，所有其他主机均被拒绝访问该服务。

示例 **3**：禁用对未使用服务的访问

在网络级别，您可以禁用某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。

不受信任的客户端网络选项卡

如果使用客户端网络，则可以通过仅接受显式配置的端点上的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为_trusted_。也就是说，默认情况下，StorageGRID 信任所有 "可用外部端口" 上每个网格节点的入站连接。

您可以通过指定每个节点上的客户端网络_不可信_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受信任，则该节点仅接受明确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 请求之外的所有入站流量。您将执行以下一般步骤：

1. 在"负载平衡器端点"页面中，通过端口 443 上的 HTTPS 为 S3 配置负载平衡器端点。
2. 在防火墙控制页面中，选择"不受信任"以指定网关节点上的客户端网络不受信任。

保存配置后，除端口 443 上的 HTTPS S3 请求和 ICMP echo (ping) 请求外，网关节点客户端网络上的所有入站流量都将被丢弃。

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该存储节点的任何入站连接。您将执行以下常规步骤：

- 在防火墙控制页面的"不受信任的客户端网络"选项卡中，指示存储节点上的客户端网络不受信任。

保存配置后，存储节点不再接受客户端网络上的任何传入流量，但它继续允许向已配置的平台服务目标发出出站请求。

示例 **3**：将对 **Grid Manager** 的访问限制为子网

假设您只想允许 Grid Manager 访问特定子网。您将执行以下步骤：

1. 将管理节点的客户端网络附加到子网。
2. 使用"不受信任的客户端网络"选项卡将客户端网络配置为不受信任。
3. 在创建管理接口负载均衡器端点时，输入端口并选择该端口将访问的管理接口。
4. 对于不受信任的客户端网络，选择*是*。
5. 使用管理外部访问选项卡可阻止所有外部端口（为该子网外的主机设置或不设置特权 IP 地址）。

保存配置后，只有您指定的子网上的主机才能访问 Grid Manager。所有其他主机均被屏蔽。

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 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 您已查看 "管理防火墙控件" 和 "网络连接准则" 中的信息。
- 如果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，如果未配置负载均衡器端点，则现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上包含一个内部防火墙，使您能够打开或关闭网格节点上的某些端口。您可以使用防火墙控制选项卡打开或关闭默认情况下在网格网络、管理网络和客户端网络上打开的端口。您还可以创建可访问已关闭网格端口的特权 IP 地址列表。如果使用客户端网络，则可以指定节点是否信任来自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权限。

将对网格外部 IP 地址开放的端口数量限制为仅绝对必要的端口，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，以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，请参见 "管理防火墙控件"。

有关外部防火墙和网络安全的详细信息，请参见 "控制外部防火墙的访问"。

访问防火墙控件

步骤

1. 选择*配置* > 安全 > 防火墙控制。

   本页上的三个选项卡如 "管理防火墙控件" 中所述。

2. 选择任意选项卡以配置防火墙控件。

   您可以按任何顺序使用这些选项卡。您在一个选项卡上设置的配置不限制您可以在其他选项卡上执行的操作；但是，您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，特权 IP 地址和子网没有内部网格访问权限。此外，即使在"管理外部访问"选项卡中被阻止，也可以访问在"特权地址列表"选项卡中打开的负载均衡器端点和其他端口。

> "特权地址列表"选项卡上的设置无法覆盖"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 address or subnet in CIDR notation** 以添加其他特权客户端。

   将尽可能少的地址添加到特权列表。

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"。

   此选项将删除对内部服务的一些保护。如有可能，请将其停用。

4. 选择 **Save**。

管理外部访问

在"管理外部访问"选项卡中关闭端口时，除非您将 IP 地址添加到特权地址列表，否则任何非网格 IP 地址都无法访问该端口。您只能关闭默认情况下处于打开状态的端口，也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"不受信任的客户端网络"选项卡上的设置。例如，如果节点不受信任，端口 SSH/22 在客户端网络上被阻止，即使它在"管理外部访问"选项卡上已打开。"不受信任的客户端网络"选项卡上的设置将覆盖客户端网络上的封闭端口（如 443、8443、9443）。

步骤

1. 选择*管理外部访问权限*。该选项卡显示一个表格，其中包含网格中节点的所有外部端口（默认情况下非网格节点可访问的端口）。
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开关打开或关闭选定端口。
   - 选择*Open all displayed ports*以打开表格中列出的所有端口。
   - 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，则当前连接到受阻端口的任何用户（包括您）都将失去对 Grid Manager 的访问权限，除非其 IP 地址已添加到特权地址列表中。

   使用表格右侧的滚动条，确保您已查看所有可用端口。使用搜索字段通过输入端口号来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 **Save**

不受信任的客户端网络

如果节点的客户端网络不受信任，则该节点仅接受配置为负载平衡器端点的端口上的入站流量，以及您在此选项卡上选择的其他端口（可选）。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。

如果未配置负载均衡器端点，则现有客户端连接可能会失败。

您在*不受信任的客户端网络*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*不受信任的客户端网络*。
2. 在设置新节点默认值部分，指定在扩展过程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。
   - 不受信任：在扩展中添加节点时，其客户端网络不受信任。

   根据需要，您可以返回此选项卡以更改特定新节点的设置。

   此设置不会影响 StorageGRID 系统中的现有节点。

3. 使用以下选项选择应仅在显式配置的负载平衡器端点或其他选定端口上允许客户端连接的节点：

   - 选择*显示的节点不受信任*，将表中显示的所有节点添加到不受信任的客户端网络列表中。
   - 选择*Trust on displayed nodes*，从不受信任的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开关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*对显示的节点不信任*将所有节点添加到不受信任的客户端网络列表中，然后使用单个节点旁边的切换开关将该单个节点添加到受信任的客户端网络列表中。

   使用表格右侧的滚动条，确保您已查看所有可用节点。使用搜索字段通过输入节点名称来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 **Save**。

   新的防火墙设置将立即应用和实施。如果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

借助租户帐户，可以使用 Simple Storage Service (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网站中删除。请参阅 "StorageGRID 11.8：管理租户"。

作为网格管理员，您可以创建并管理 S3 客户端用于存储和检索对象的租户帐户。

每个租户帐户都有联合或本地组、用户、S3 存储桶和对象。

租户帐户可用于按不同实体隔离存储的对象。例如，可以将多个租户帐户用于以下任一用例：

- 企业用例： 如果您在企业应用程序中管理 StorageGRID 系统，则可能需要按组织中的不同部门隔离网格的对象存储。在这种情况下，您可以为营销部门、客户支持部门、人力资源部门等创建租户帐户。

如果使用 S3 客户端协议，则可以使用 S3 存储桶和存储桶策略在企业中的部门之间隔离对象。您无需使用租户帐户。有关详细信息，请参见实施 "S3 存储桶和存储桶策略" 的说明。

- *服务提供商用例：*如果您以服务提供商身份管理 StorageGRID 系统，则可以按将在网格上租用存储的不同实体隔离网格的对象存储。在这种情况下，您可以为 Company A、Company B、Company 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 Grid Manager 创建租户帐户。创建租户帐户时，请指定以下信息：

- 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 或使用网格联合连接。
- 租户的初始 root 访问权限，基于 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 租户帐户需要遵守监管要求，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 租户帐户都可以创建和管理合规存储桶。

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 Tenant Manager 以执行以下任务：

- 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克隆和跨网格复制
- 管理 S3 访问密钥
- 创建和管理 S3 存储桶
- 使用 S3 平台服务
- 使用 S3 Select
- 监控存储空间使用情况

虽然 S3 租户用户可以使用 Tenant Manager 创建和管理 S3 访问密钥和存储桶，但他们必须使用 S3 客户端应用程序来接收和管理对象。有关详细信息，请参见 "使用 S3 REST API"。

创建 StorageGRID 租户帐户

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。

根据是否配置了"身份联合"和"单点登录"，以及用于创建租户帐户的 Grid Manager 帐户是否属于具有 Root access 权限的管理员组，创建租户帐户的步骤会有所不同。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。

- 您有 "Root 访问权限或租户帐户权限"。
- 如果租户帐户将使用为 Grid Manager 配置的身份源，并且要将租户帐户的 Root 访问权限授予联合组，则已将该联合组导入 Grid Manager。您无需为此管理组分配任何 Grid Manager 权限。请参阅 "管理管理员组"。
- 如果要允许 S3 租户使用网格联合连接克隆帐户数据并将存储桶对象复制到另一个网格：
  - 您有 "已配置网格联盟连接"。
  - 连接状态为*已连接*。
  - ${post_edited_translations.segment}
  - 您已查看 "管理网格联合的允许租户" 的注意事项。
  - 如果租户帐户将使用为 Grid Manager 配置的身份源，则已将同一联合组导入两个网格上的 Grid Manager。

    创建租户时，您将选择此组以获得源和目标租户帐户的初始 Root 访问权限。

    如果在创建租户之前两个网格上都不存在此管理组，则租户不会被复制到目标。

访问此向导

步骤

1. ${post_edited_translations.segment}
2. 选择 **Create**。

输入详细信息

步骤

1. 输入租户的详细信息。

字段	问题描述
名称	租户帐户的名称。租户名称不需要是唯一的。创建租户帐户后，它将收到一个唯一的 20 位帐户 ID。
${post_edited_translations.segment}	${post_edited_translations.segment} 如果您正在创建将使用网格联盟连接的租户，则可以根据需要使用此字段来帮助识别哪个是源租户，哪个是目标租户。例如，在网格 1 上创建的租户的以下描述也将显示在复制到网格 2 的租户中：“此租户是在网格 1 上创建的。”
客户端类型	必须是 **S3**。
${post_edited_translations.segment}	如果希望此租户具有存储配额，则为配额和单位的数值。

2. 选择 **Continue**。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}

   其中部分权限具有其他要求。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 S3 平台服务，例如 CloudMirror。请参阅 "管理 S3 租户帐户的平台服务"。
使用自己的身份源	租户可以为其联合组和用户配置和管理自己的身份源。如果您为 StorageGRID 系统"已配置 SSO"，则此选项将被禁用。
允许 S3 Select	租户可以发出 S3 SelectObjectContent API 请求以筛选和检索对象数据。请参阅 "管理租户帐户的 S3 Select"。 重要提示：SelectObjectContent 请求可能会降低所有 S3 客户端和所有租户的负载均衡器性能。仅在需要时且仅对受信任的租户启用此功能。

2. ${post_edited_translations.segment}

权限	如果选择.....
网格联盟连接	租户可以使用网格联合连接，其中： • 使此租户以及添加到帐户的所有租户组和用户从此网格（源网格）克隆到选定连接中的另一个网格（目标网格）。 • 允许此租户在每个网格上的相应存储桶之间配置跨网格复制。 请参阅 "管理网格联盟的允许租户"。
S3 对象锁定	允许租户使用 S3 对象锁定的特定功能： • **Set maximum retention period** 定义从摄取时间开始，添加到此存储桶的新对象应保留多长时间。 • **Allow compliance mode** 可防止用户在保留期间覆盖或删除受保护对象版本。

3. 选择 **Continue**。

定义根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使用的密码。
如果启用了身份联合	a. 选择现有联合组以获得租户的 root 访问权限。 b. （可选）指定以本地 root 用户身份登录租户时使用的密码。
如果已启用身份联合和单一登录(SSO)	选择现有联合组以具有租户的 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，并在"租户"页面上列出新租户。要了解如何查看租户详细信息和监视租户活动，请参阅"监控租户活动"。

   ${post_edited_translations.segment}

3. 如果为租户选择了*使用网格联合连接*权限：

   a. 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。

      如果您看到错误消息"Tenant created without a clone"，请参阅 "对网格联合错误进行故障排除" 中的说明。

   b. 如果在定义 root 访问权限时提供了本地 root 用户密码，"更改本地 root 用户的密码" 用于复制的租户。

      ${post_edited_translations.segment}

登录租户（可选）

根据需要，您可以立即登录到新租户以完成配置，也可以稍后登录到该租户。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 Grid Manager。请参阅 "控制外部防火墙的访问"。

立即登录

条件	操作
端口 443，您为本地 root 用户设置了密码	1. 选择 **Sign in as root**。 登录时，将显示用于配置存储桶、身份联合、组和用户的链接。 2. 选择链接以配置租户帐户。 每个链接都会在租户管理器中打开相应的页面。要完成页面，请参见 "租户帐户的使用说明"。

条件	操作
端口 443，您未为本地 root 用户设置密码	选择 **Sign in**，然后输入 Root access 联盟组中用户的凭据。
受限端口	1. 选择*完成* 2. 在租户表中选择*受限*以了解有关访问此租户帐户的更多信息。 租户管理器的 URL 具有以下格式： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的 IP 地址 ◦ *port* 是仅限租户的端口 ◦ *20-digit-account-id* 是租户的唯一帐户 ID

稍后登录

条件	执行以下操作之一.....
端口 443	• 在网格管理器中，选择 **Tenants**，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* 是完全限定域名或管理节点的 IP 地址 ◦ *20-digit-account-id* 是租户的唯一帐户 ID
受限端口	• 在网格管理器中，选择 **Tenants**，然后选择 **Restricted**。 • 在 Web 浏览器中输入租户的 URL： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的 IP 地址 ◦ *port* 为仅限租户的受限端口 ◦ *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、平台服务以及帐户克隆和跨网格复制。

编辑 StorageGRID 租户帐户

${post_edited_translations.segment}

如果租户具有*使用网格联合连接*权限，则可以从连接中的任一网格编辑租户详细信息。但是，您在连接中的一个网格上所做的任何更改都不会复制到另一个网格。如果要使租户详细信息在网格之间完全同步，请在两个网格上进行相同的编辑。请参阅 "管理网格联合连接的允许租户"。

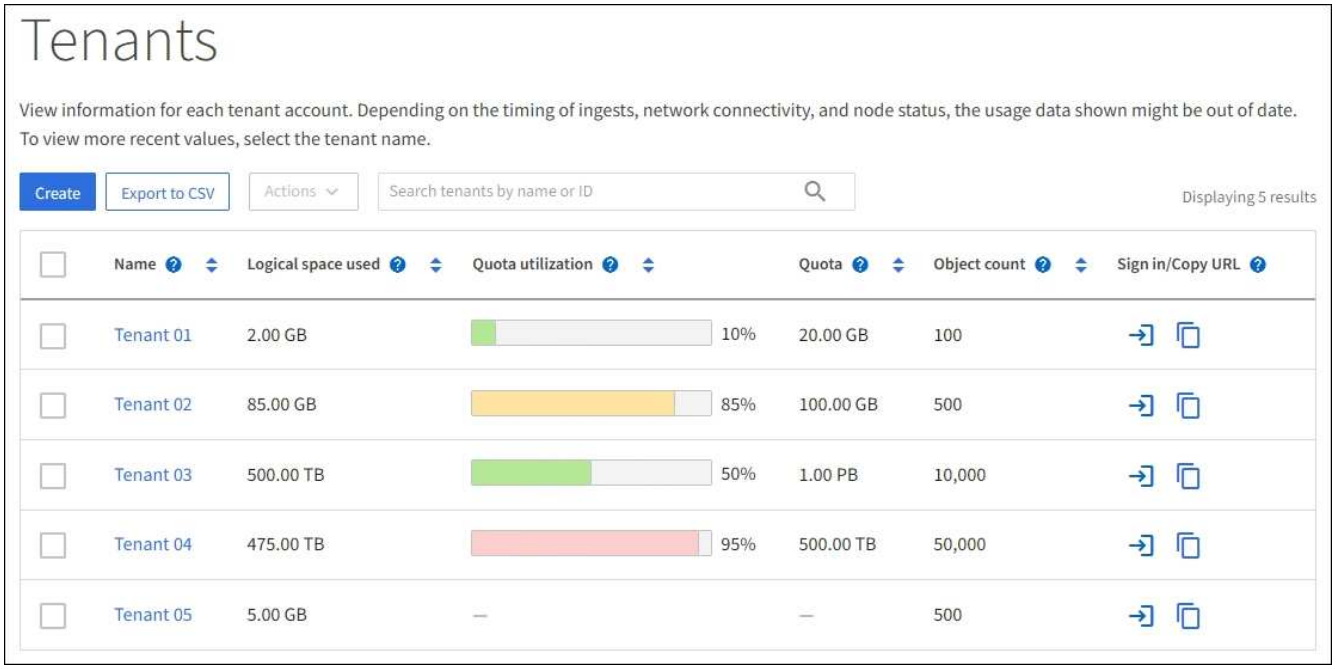
开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "Root 访问权限或租户帐户权限"。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}



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。您可以执行以下操作之一：
   - ${post_edited_translations.segment}
   - 选择租户名称以显示详细信息页面，然后选择*编辑*。
4. ${post_edited_translations.segment}
   - 名称
   - 说明
   - 存储配额

5. 选择 **Continue**。
6. ${post_edited_translations.segment}
   - 如果您为已在使用平台服务的租户禁用 平台服务，则他们为其 S3 存储桶配置的服务将停止工作。系统不会向该租户发送任何错误消息。例如，如果租户为 S3 存储桶配置了 CloudMirror 复制，他们仍可以在该存储桶中存储对象，但这些对象的副本将不再创建在他们配置为端点的外部 S3 存储桶中。请参见 "管理 S3 租户帐户的平台服务"。
   - 更改*使用自己的身份源*的设置，以确定租户帐户是使用自己的身份源还是为 Grid Manager 配置的身份源。

     如果*使用自己的身份源*为：

     - 已禁用并选中，表示租户已启用其自己的身份源。租户必须先禁用其身份源，然后才能使用为 Grid Manager 配置的身份源。
     - 禁用且未选中，StorageGRID 系统已启用 SSO。租户必须使用为 Grid Manager 配置的身份源。
   - 根据需要选择或清除 **Allow S3 Select** 权限。请参阅 "管理租户帐户的 S3 Select"。
   - ${post_edited_translations.segment}
     i. 选择 **Grid federation** 选项卡。
     ii. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
     i. 选择 **Grid federation** 选项卡。
     ii. ${post_edited_translations.segment}
     iii. （可选）选择*克隆现有本地用户和组*以将其克隆到远程网格。如果需要，可以停止正在进行的克隆，或者在上次克隆操作完成后无法克隆某些本地用户或组时重试克隆。
   - 要设置最长保留期限或允许符合性模式：

     在使用这些设置之前，必须先在网格上启用 S3 Object Lock。

     i. ${post_edited_translations.segment}
     ii. ${post_edited_translations.segment}
     iii. 对于*允许合规模式*，请选中复选框。

更改 **StorageGRID** 租户的本地 **root** 用户密码

${post_edited_translations.segment}

开始之前

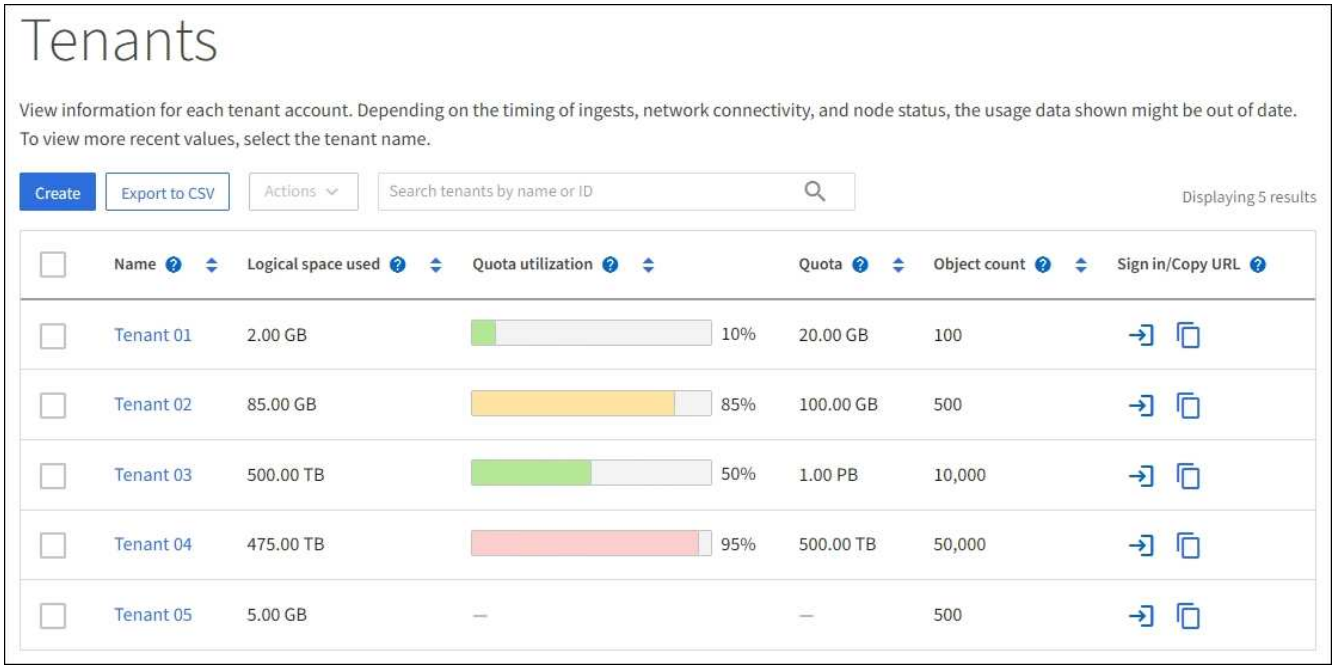
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

关于此任务

如果您的 StorageGRID 系统启用了单点登录 (SSO)，则本地 root 用户将无法登录到租户帐户。要执行 root 用户任务，用户必须属于对该租户具有 Root 访问权限的联合组。

步骤

1. ${post_edited_translations.segment}



2. 选择租户账户。您可以执行以下任一操作：
   - 选中租户的复选框，然后选择*操作* > 更改 **root** 密码。
   - ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. 选择 **Save**。

删除 StorageGRID 租户帐户

如果要永久删除租户对系统的访问权限，则可以删除租户帐户。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 已删除与租户帐户关联的所有 S3 存储区和对象。
- 如果允许租户使用网格联合连接，您已查看 "删除具有使用网格联合连接权限的租户" 的注意事项。

步骤

1. ${post_edited_translations.segment}
2. 找到要删除的一个或多个租户帐户。

   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*操作* > 删除。
4. 要删除单个租户，请执行以下操作之一：
   - 选中复选框，然后选择*操作* > 删除。

- 选择租户名称以显示详细信息页面，然后选择*操作* > 删除。

5. ${post_edited_translations.segment}

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。

${post_edited_translations.segment}

平台服务不支持 "${post_edited_translations.segment}"。

CloudMirror 复制

StorageGRID CloudMirror 复制服务用于将特定对象从 StorageGRID 存储桶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 服务对您的数据执行分析。

CloudMirror 复制与跨网格复制功能有一些重要的异同。要了解更多信息，请参见 "比较跨网格复制和 CloudMirror 复制"。

> 如果源存储桶启用了 S3 Object Lock，则不支持 CloudMirror 复制。

通知

${post_edited_translations.segment}

例如，您可以配置向管理员发送有关添加到存储桶的每个对象的警报，其中对象表示与关键系统事件关联的日志文件。

> ${post_edited_translations.segment}

${post_edited_translations.segment}

搜索集成服务用于将 S3 对象元数据发送到指定的 Elasticsearch 索引，其中可以使用外部服务搜索或分析元数据。

例如，您可以将存储桶配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 对存储桶执行搜索，并对对象元数据中存在的模式进行复杂的分析。

> 虽然可以在启用 S3 Object Lock 的存储桶上配置 Elasticsearch 集成，但通知消息中不会包含对象的 S3 Object Lock 元数据（包括 Retain Until Date 和 Legal Hold 状态）。

平台服务使租户能够使用外部存储资源、通知服务以及搜索或分析服务来处理其数据。由于平台服务的目标位置通常位于 StorageGRID 部署的外部，因此必须决定是否要允许租户使用这些服务。如果是这样，则必须在创建或编辑租户帐户时启用平台服务的使用。您还必须配置网络，以便租户生成的平台服务消息可以到达其目的地。

在使用平台服务之前，请注意以下建议：

- 如果 StorageGRID 系统中的 S3 存储桶同时启用了版本控制和 CloudMirror 复制，则还应为目标端点启用 S3 存储桶版本控制。这样，CloudMirror 复制便可在端点上生成类似的对象版本。
- 对于需要 CloudMirror 复制、通知和搜索集成的 S3 请求，不应使用超过 100 个活动租户。拥有 100 个以上的活动租户可能会导致 S3 客户端性能降低。
- 无法完成的端点请求将排队，最多可排队 500,000 个请求。此限制在活跃租户之间平均分配。新租户可以暂时超过此 500,000 的限制，以避免对新创建的租户造成不公平的影响。

相关信息

- "管理平台服务"
- "配置存储代理服务器设置"
- "监控 StorageGRID"

StorageGRID 平台服务的网络和端口

${post_edited_translations.segment}

创建或更新租户帐户时，可以为 S3 租户帐户启用平台服务。如果启用了平台服务，租户可以创建端点，作为 CloudMirror 复制、事件通知或从其 S3 存储桶搜索集成消息的目标。这些平台服务消息从运行 ADC 服务的存储节点发送到目标端点。

${post_edited_translations.segment}

- 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
- ${post_edited_translations.segment}

  此端点可以托管在各种 Web 服务器、框架或 Fluentd 等数据处理工具上。

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

为了确保平台服务消息可以传递，您必须配置包含 ADC 存储节点的网络。必须确保可以使用以下端口将平台服务消息发送到目标端点。

${post_edited_translations.segment}

- **80**：对于以 http 开头的端点 URI（大多数端点）
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

租户可以在创建或编辑端点时指定其他端口。

如果将 StorageGRID 部署用作 CloudMirror 复制的目标，则可能会在 80 或 443 以外的端口上接收复制消息。请确保在端点中指定了目标 StorageGRID 部署用于 S3 的端口。

如果使用不透明的代理服务器，则还必须"配置存储代理设置"以允许将消息发送到外部端点，例如 Internet 上的端点。

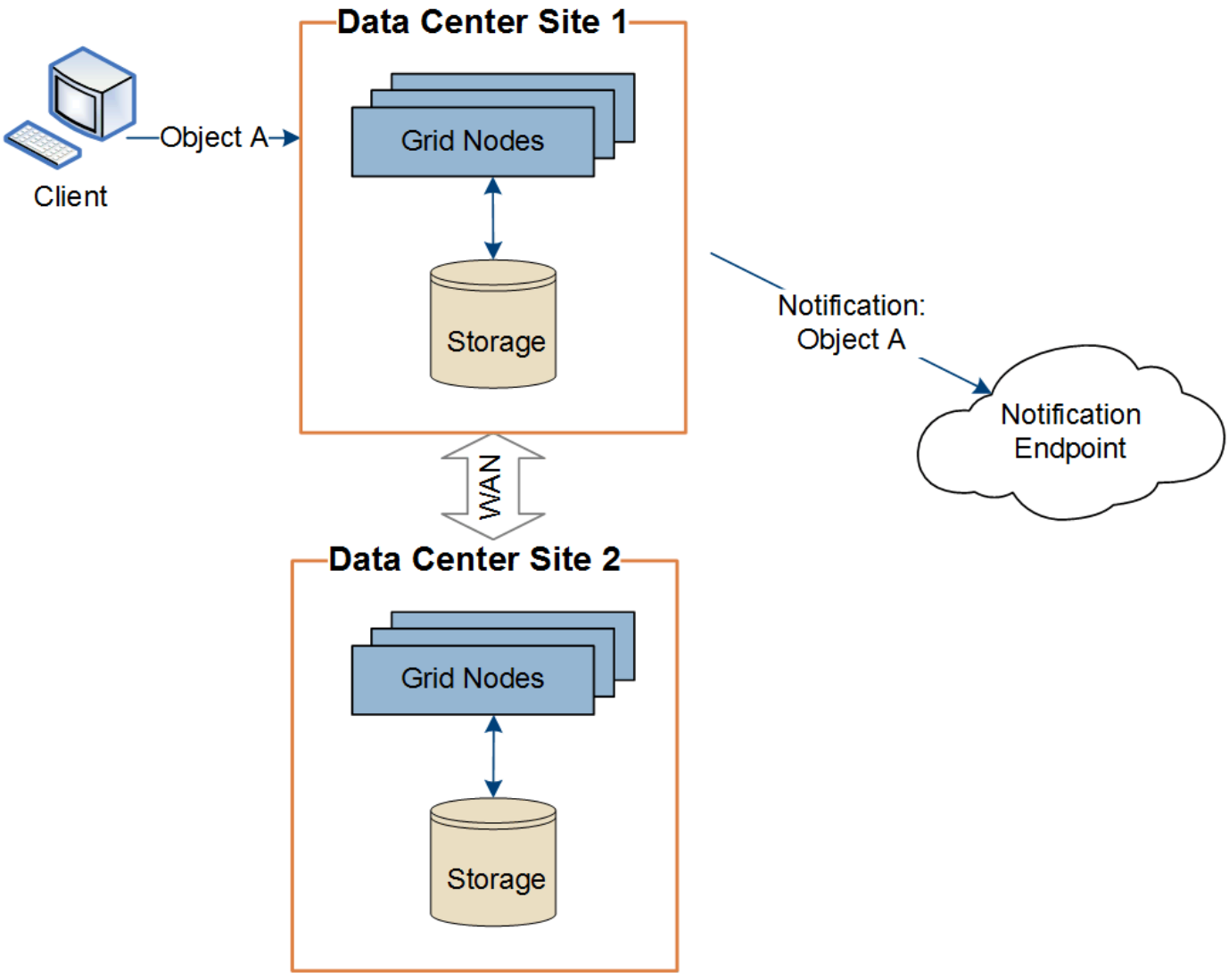
相关信息

"使用租户帐户"

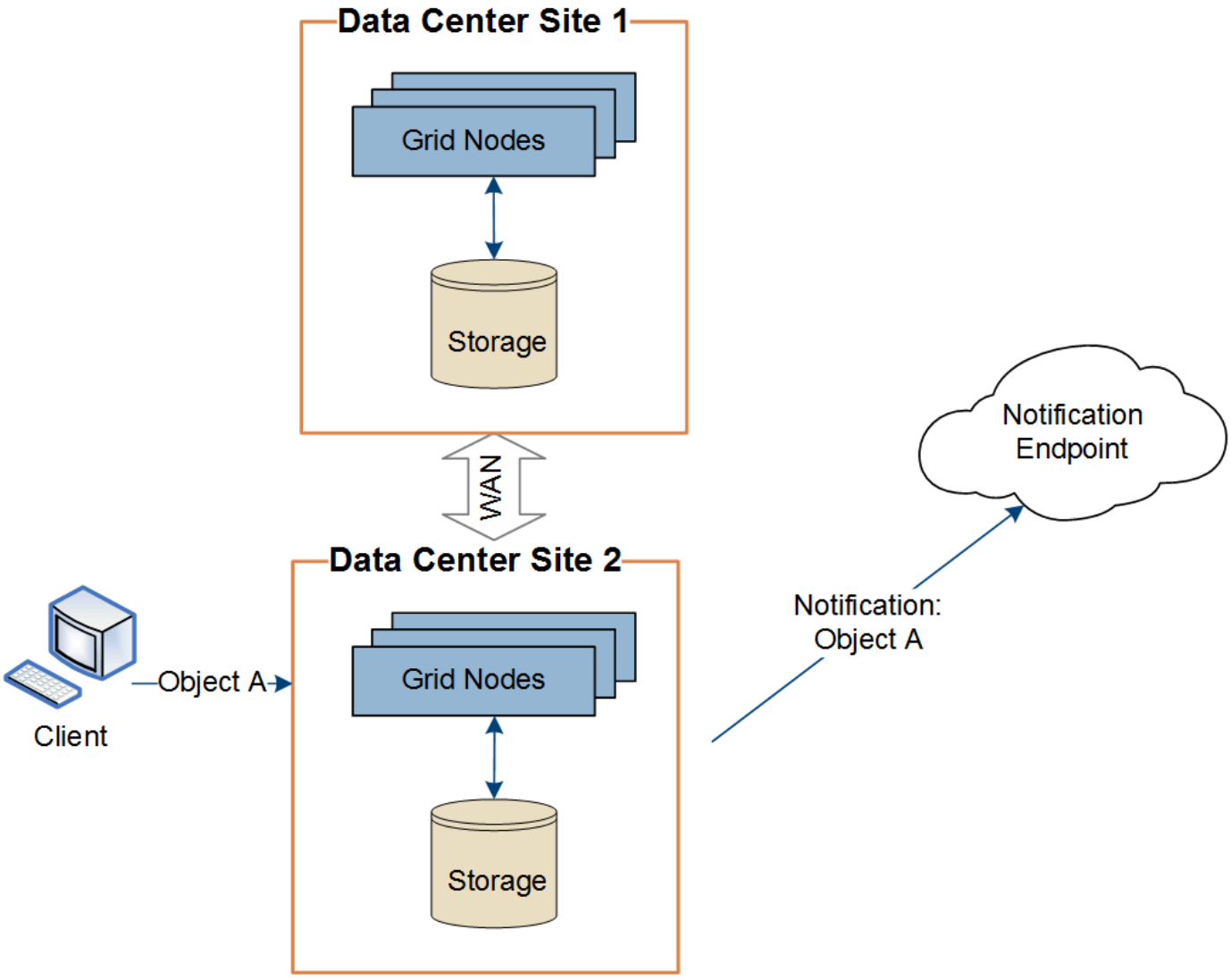
按站点交付 **StorageGRID** 平台服务消息

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，则会触发有关该操作的通知并从数据中心站点 1 发送。



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，则会触发有关删除操作的通知，并从数据中心站点 2 发送。



确保每个站点的网络配置正确，以便平台服务消息可以传递到其目标位置。

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。

${post_edited_translations.segment}

租户必须先使用租户管理器创建一个或多个端点，然后才能使用平台服务。每个端点代表一个平台服务的外部目标，例如 StorageGRID S3 存储桶、Amazon Web Services 存储桶、Amazon Simple Notification Service 主题、Kafka 主题或在本地或 AWS 上托管的 Elasticsearch 集群。每个端点都包含外部资源的位置以及访问该资源所需的凭据。

当租户创建端点时，StorageGRID 系统会验证该端点是否存在，以及是否可以使用指定的凭据访问该端点。从每个站点的一个节点验证到端点的连接。

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。租户用户应解决此问题，然后尝试重新创建端点。

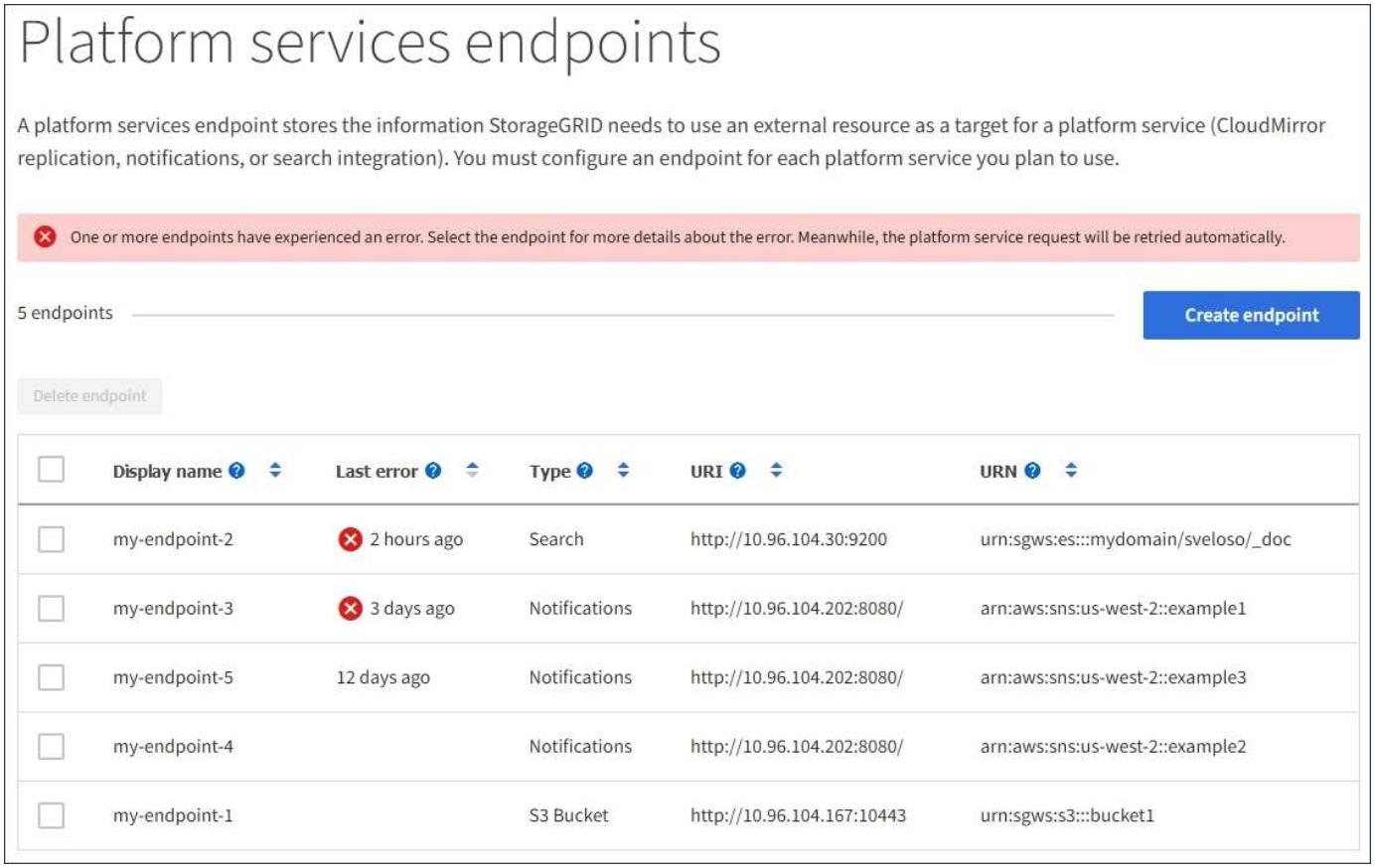
${post_edited_translations.segment}

${post_edited_translations.segment}

如果 StorageGRID 尝试访问现有端点时发生错误，租户管理器中的仪表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。



“**Last error**”（上一个错误）列中的某些错误消息可能会在括号中包含 logID。Grid 管理员或技术支持人员可以使用此 ID 在 bycast.log 中查找有关该错误的更详细信息。

${post_edited_translations.segment}

如果您在存储节点和平台服务端点之间配置了 "存储代理"，则当您的代理服务不允许来自 StorageGRID 的消息时，可能会发生错误。要解决这些问题，请检查代理服务器的设置，以确保不会阻止与平台服务相关的消息。

${post_edited_translations.segment}

如果过去 7 天内发生过任何端点错误，Tenant Manager 中的仪表板将显示一条警报消息。您可以转到 Endpoints 页面查看有关该错误的更多详细信息。

${post_edited_translations.segment}

某些平台服务问题可能会导致 S3 存储桶上的客户端操作失败。例如，如果内部复制状态机 (RSM) 服务停止，或者有太多平台服务消息排队等待传送，则 S3 客户端操作将失败。

要检查服务的状态：

1. 选择*节点* > 站点 > 存储节点 > 概述。
2. ${post_edited_translations.segment}
3. 解决所有活动警报。根据需要，联系技术支持。

可恢复和不可恢复的端点错误

创建端点后，可能会由于各种原因导致平台服务请求错误。某些错误可以通过用户干预进行恢复。例如，由于以下原因，可能会发生可恢复的错误：

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 无法发送通知。

${post_edited_translations.segment}

其他错误无法恢复。例如，可能出现不可恢复的错误，原因如下：

- 端点已删除。
- Webhook 端点目标响应通知请求时出现 `400 Bad Request`错误。

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- 检查 `/var/local/log/bycast-err.log` 以获取相关错误。运行 ADC 服务的存储节点包含此日志文件。

${post_edited_translations.segment}

如果目标遇到阻止其接受平台服务消息的问题，则存储桶上的客户端操作将成功，但平台服务消息不会送达。例如，如果目标上的凭据已更新，导致 StorageGRID 无法再向目标服务进行身份验证，则可能会发生此错误。

${post_edited_translations.segment}

平台服务请求的性能较低

如果发送 S3 请求的速率超过了目标端点接收请求的速率，StorageGRID 软件可能会限制该存储桶的传入请求。只有当存在等待发送到目标端点的积压请求时，才会发生限制。

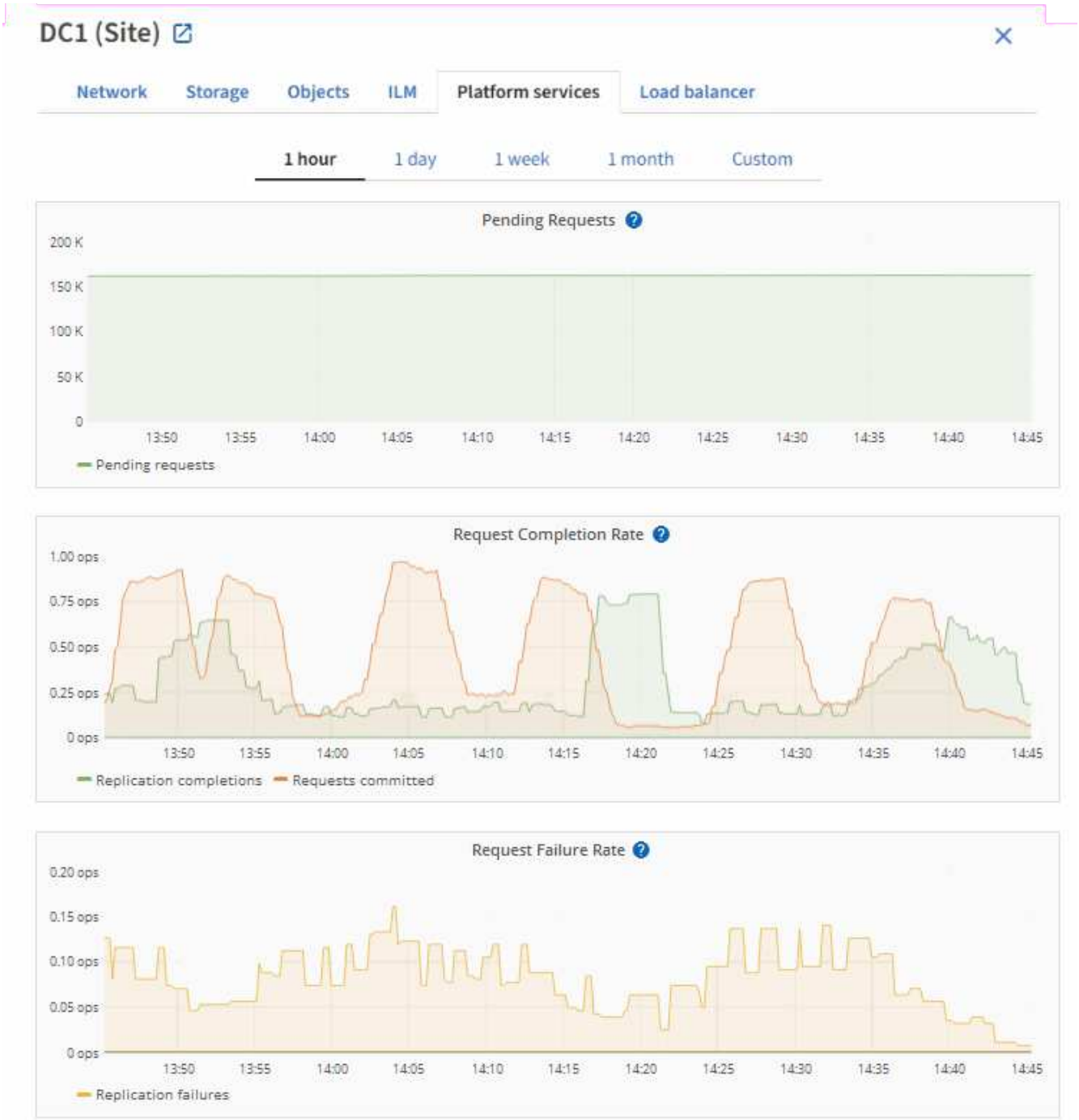
唯一可见的影响是传入的 S3 请求需要更长的时间才能执行。如果您开始检测到性能明显变慢，则应降低摄入速率或使用容量更高的端点。如果积压的请求继续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。

CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求通常涉及比搜索集成或事件通知请求更多的数据传输。

${post_edited_translations.segment}

要查看平台服务的请求失败率：

1. 选择 **Nodes**。
2. 选择 ***site*** > **Platform Services**。
3. ${post_edited_translations.segment}



平台服务不可用警报

${post_edited_translations.segment}

${post_edited_translations.segment}

要解决此警报，请确定该站点上的哪些 Storage Node 包含 RSM 服务。（RSM 服务存在于同样包含 ADC 服务的 Storage Node 上。）然后，确保这些 Storage Node 中的绝大多数正在运行且可用。

${post_edited_translations.segment}

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>排查平台服务端点故障"。

相关信息

"StorageGRID 系统故障排除"

管理 StorageGRID 中租户帐户的 S3 Select

您可以允许某些 S3 租户使用 S3 Select 对单个对象发出 SelectObjectContent 请求。

S3 Select 提供了一种有效的方法来搜索大量数据，而无需部署数据库和相关资源来启用搜索。它还降低了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 请求来过滤和检索对象中所需的数据。StorageGRID 的 S3 Select 实现包括 S3 Select 命令和功能的子集。

使用 S3 Select 的注意事项和要求

Grid 管理要求

网格管理员必须授予租户 S3 Select 能力。在 "创建租户" 或 "编辑租户" 时，选择 **Allow S3 Select**。

对象格式要求

要查询的对象必须采用以下格式之一：

- **CSV**。可以按原样使用或压缩到 GZIP 或 BZIP2 存档中。
- **Parquet**。Parquet 对象的其他要求：
  - S3 Select 仅支持使用 GZIP 或 Snappy 的列压缩。S3 Select 不支持 Parquet 对象的全对象压缩。
  - S3 Select 不支持 Parquet 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。
  - 您必须使用在对象架构中指定的数据类型。
  - 不能使用 INTERVAL、JSON、LIST、TIME 或 UUID 逻辑类型。

终结点要求

必须将 SelectObjectContent 请求发送至 "StorageGRID 负载平衡器端点"。

端点使用的管理节点和网关节点必须是以下选项之一：

- 服务设备节点
- 基于VMware的软件节点
- 运行启用了 cgroup v2 的内核的裸机节点

一般注意事项

无法将查询直接发送到存储节点。

SelectObjectContent 请求可能会降低所有 S3 客户端和所有租户的负载均衡器性能。仅在需要时启用此功能，并且仅适用于受信任的租户。

请参阅"使用 S3 Select 的说明"。

要查看 S3 Select 操作随时间变化的"Grafana 图表"，请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的配置选项。

此版本的文档网站中已删除 Swift 详细信息。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 中执行前提任务。

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。+

${post_edited_translations.segment}

按照 S3 设置向导中的步骤操作。

手动配置

1. 创建高可用性组
2. 创建负载均衡器端点
3. 创建租户帐户
4. 创建存储桶和访问密钥
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，将 IP 地址与您计划使用的任何域名相关联。

   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，以便随时间推移管理和监控对象存储。

将 **StorageGRID** 附加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，必须在 StorageGRID 中执行配置步骤并获取特定值。

我需要哪些值?

${post_edited_translations.segment}

值	配置值的位置	使用值的位置
虚拟 IP (VIP) 地址	StorageGRID > HA 组	DNS条目
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
${post_edited_translations.segment}	${post_edited_translations.segment}	客户端应用程序
${post_edited_translations.segment}	${post_edited_translations.segment}	客户端应用程序

如何获得这些值?

根据您的要求，您可以执行以下操作之一来获取所需的信息：

- 使用 **"S3 设置向导"**。S3 设置向导可帮助您快速配置 StorageGRID 中所需的值，并输出一个或两个可在配置 S3 应用程序时使用的文件。该向导将引导您完成所需的步骤，并帮助确保您的设置符合 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，或者您的实现需要大量自定义。

- 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的值，并输出一个文件，您可以在 ONTAP 中配置 FabricPool 云层时使用该文件。

  如果您计划将 StorageGRID 用作 FabricPool 云分层的对象存储系统，除非您确定自己有特殊需求或您的实施需要进行大量自定义，否则建议使用 FabricPool 设置向导。

- 手动配置项目。如果您正在连接到 S3 应用程序，并且不希望使用 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 应用程序将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 应用程序将使用的租户账户。参见 "创建租户帐户"。

  d. 对于 S3 租户，请登录该租户账户，并为每个将访问该应用程序的用户生成一个访问密钥 ID 和机密访问密钥。请参见 "${post_edited_translations.segment}"。

  e. 在租户帐户中创建一个或多个 S3 存储桶。有关 S3，请参见"创建 S3 存储桶"。

  f. 要为属于新租户或存储区/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至 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 实现安全性：

连接安全
: TLS

服务器身份验证
: 由系统 CA 签名的 X.509 服务器证书或由管理员提供的自定义服务器证书

客户端身份验证
: S3 账号访问密钥 ID 和密钥

客户端授权

存储桶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。

- 连接到负载均衡器服务的客户端可以使用 HTTPS 或 HTTP，具体取决于您如何"配置负载均衡器端点"。

  HTTPS 提供安全的 TLS 加密通信，建议使用。您必须将安全证书附加到端点。

  HTTP 提供安全性较低的未加密通信，应仅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 提供安全性较低的未加密通信，但可以选择"启用"用于非生产或测试网格。

- StorageGRID 和客户端之间的通信使用 TLS 进行加密。
- 无论负载均衡器端点配置为接受 HTTP 还是 HTTPS 连接，网格中负载均衡器服务与存储节点之间的通信均会加密。
- 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—由网格管理员上传的自定义服务器证书或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，它们使用安装 StorageGRID 系统时为存储节点生成的系统生成的服务器证书（由系统证书颁发机构签名），或者使用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其用于建立 TLS 连接的任何证书进行签名的证书颁发机构。

TLS 库支持的哈希和加密算法

StorageGRID 系统支持一组密码套件，客户端应用程序可以在建立 TLS 会话时使用这些密码套件。要配置密码，请转到 配置 > 安全 > 安全设置，然后选择 **TLS** 和 **SSH** 策略。

支持的 TLS 版本

StorageGRID 支持 TLS 1.2 和 TLS 1.3。

SSLv3 和 TLS 1.1（或更早版本）不再受支持。

${post_edited_translations.segment}

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。作为完成向导的一部分，您可以下载可用于在 S3 应用程序中输入值的文件。使用向导可以更快地配置您的系统，并确保您的设置符合 StorageGRID 最佳实践。

如果具有"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，也可以在以后的任何时候访问并完成该向导。根据您的要求，您还可以手动配置某些或所有必需项目，然后使用向导汇编 S3 应用程序所需的值。

使用向导之前

在使用向导之前，请确认您已完成这些先决条件。

获取 **IP** 地址并设置 **VLAN** 接口

如果您将配置高可用性 (HA) 组，您将知道 S3 应用程序将连接到哪些节点以及将使用哪个 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 来隔离来自 S3 应用程序的流量，则表示您已经配置了 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)，则已启用这些功能。您还知道哪个联合组应具有 S3 应用程序将使用的租户帐户的根访问权限。请参阅 "${post_edited_translations.segment}" 和 "${post_edited_translations.segment}"。

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 "配置的 S3 端点域名"。建议使用虚拟主机式请求。

查看负载均衡器和安全证书要求

如果您计划使用 StorageGRID 负载均衡器，则已查看负载均衡的一般注意事项。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）负载均衡器端点，则您具有该负载均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克隆帐户数据并将存储桶对象复制到另一个网格，请在启动向导之前确认以下内容：

- 您有 "已配置网格联盟连接"。
- 连接状态为*已连接*。

- ${post_edited_translations.segment}

访问并完成 **StorageGRID** 中的 **S3** 设置向导

您可以使用 S3 设置向导将 StorageGRID 配置为与 S3 应用程序一起使用。设置向导提供应用程序访问 StorageGRID 存储桶和保存对象所需的值。

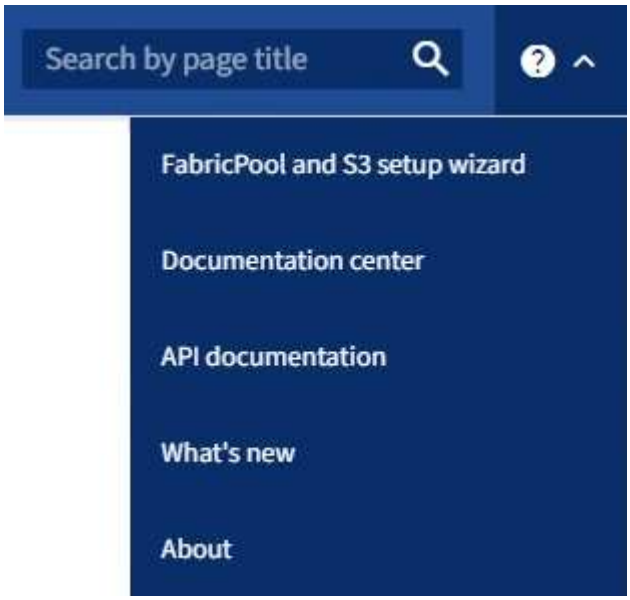
开始之前

- 您有 "root 访问权限"。
- 您已查阅"注意事项和要求"以使用向导。

访问此向导

步骤

1. 使用 "支持的 Web 浏览器" 登录到网格管理器。
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 中的标题栏中选择帮助图标，然后选择 **FabricPool and S3 setup wizard**。



3. 在 FabricPool 和 S3 设置向导页面的 S3 应用程序部分，选择*立即配置*。

步骤 **1/6**：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、管理节点或两者。

您可以使用 HA 组来帮助保持 S3 数据连接可用。如果 HA 组中的活动接口出现故障，备份接口可以管理工作负载，对 S3 操作的影响很小。

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均衡器，则无需创建 HA 组。选择 跳过此步骤 并转到 步骤 2/6：配置负载均衡器端点。

2. 要使用 StorageGRID 负载均衡器，您可以创建新的 HA 组或使用现有的 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	问题描述
HA 组名称	此 HA 组的唯一显示名称。
${post_edited_translations.segment}	此 HA 组的描述。

c. 对于*添加接口*步骤，请选择要在此 HA 组中使用的节点接口。

${post_edited_translations.segment}

您可以选择一个或多个节点，但每个节点只能选择一个接口。

d. 对于*Prioritize interfaces*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 Primary 接口。除非发生故障，否则 Primary 接口为活动接口。

如果 HA 组包含多个接口，并且活动接口发生故障，则虚拟 IP（VIP）地址按优先级顺序移动到第一个备份接口。如果该接口出现故障，VIP 地址将移动到下一个备份接口，依此类推。故障解决后，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	问题描述
子网 CIDR	CIDR 表示法中 VIP 子网的地址 — IPv4 地址后跟斜杠和子网长度（0-32）。 网络地址不得设置任何主机位。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 地址不在同一子网中，请输入 StorageGRID VIP 本地网关 IP 地址。本地网关 IP 地址必须在 VIP 子网内。
虚拟 IP 地址	为 HA 组中的活动接口输入至少一个且不超过十个 VIP 地址。所有 VIP 地址必须在 VIP 子网内。 必须至少有一个地址为 IPv4。或者，您可以指定其他 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*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*转到负载平衡器步骤。

步骤 **2/6**：配置负载均衡器端点

StorageGRID 使用负载均衡器管理来自客户端应用程序的工作负载。负载均衡可最大限度地提高跨多个存储节点的速度和连接容量。

您可以使用 StorageGRID 负载平衡器服务，该服务存在于所有网关和管理节点上，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 负载均衡器服务，请选择 **StorageGRID load balancer** 选项卡，然后创建或选择要使用的负载均衡器端点。要使用外部负载均衡器，请选择 **External load balancer** 选项卡，并提供有关已配置系统的详细信息。

创建端点

步骤

1. 要创建负载均衡器端点，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	问题描述
名称	终结点的描述性名称。
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，因为这些端口在管理节点上保留。 注意： 不允许使用其他网格服务使用的端口。请参阅 "StorageGRID 内部端口"。
客户端类型	必须是 **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。绑定模式控制使用任何 IP 地址或使用特定 IP 地址和网络接口访问端点的方式。

模式	问题描述
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、任何网络上的任何 HA 组的虚拟 IP (VIP) 地址或相应的 FQDN 来访问端点。 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）来访问此端点。 具有此绑定模式的端点都可以使用相同的端口号，只要您为端点选择的 HA 组不重叠即可。
节点接口	${post_edited_translations.segment}
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，请选择以下选项之一：

字段	问题描述
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存储区。
允许选定的租户	只有选定租户帐户可以使用此端点访问其存储桶。
阻止选定租户	选定的租户帐户无法使用此端点来访问其存储桶。所有其他租户都可以使用此端点。

5. 对于*附加证书*步骤，请选择以下选项之一：

字段	问题描述
上传证书（推荐）	使用此选项可上传 CA 签名的服务器证书、证书私钥和可选的 CA 捆绑包。
生成证书	使用此选项可生成自签名证书。有关要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	仅当已上传或生成 StorageGRID 全局证书的自定义版本时，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*返回 S3 设置向导。
7. 选择*继续*转到租户和存储桶步骤。

对端点证书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*选择负载均衡器端点*中选择其名称。
2. 选择*继续*转到租户和存储桶步骤。

使用外部负载均衡器

步骤

1. 要使用外部负载平衡器，请完成以下字段。

字段	问题描述
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均衡器的端口号。
证书	复制外部负载均衡器的服务器证书并将其粘贴到此字段中。

2. 选择*继续*转到租户和存储桶步骤。

步骤 **3/6**：创建租户和存储区

租户是可以使用 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、存储桶、对象和一组特定的功能。

存储区是用于存储租户的对象和对象元数据的容器。虽然租户可能有很多存储区，但此向导可帮助您以最快捷、最简单的方式创建租户和存储区。如果稍后需要添加存储区或设置选项，可以使用 Tenant Manager。

有关此任务的详细信息，请参见 "创建租户帐户" 和 "创建 S3 存储桶"。

步骤

1. 输入租户帐户的名称。

   租户名称不必是唯一的。创建租户帐户时，它将收到一个唯一的数字帐户 ID。

2. 根据您的 StorageGRID 系统使用 "身份联合"、"单点登录 (SSO)" 还是同时使用两者，定义租户帐户的根访问权限。

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使用的密码。
如果启用了身份联合	a. 选择现有联合组，以便为租户提供 "root 访问权限"。 b. （可选）指定以本地 root 用户身份登录租户时使用的密码。
如果已启用身份联合和单一登录(SSO)	选择现有联合组，使其拥有 "root 访问权限" 租户权限。没有本地用户可以登录。

3. 如果要向导为 root 用户创建访问密钥 ID 和秘密访问密钥，请选择 **Create root user S3 access key automatically**。

   如果租户的唯一用户是 root 用户，请选择此选项。如果其他用户将使用此租户，"使用租户管理器"以配置密钥和权限。

4. 如果要立即为此租户创建存储桶，请选择*Create bucket for this tenant*。

   如果为网格启用了 S3 对象锁定，则此步骤中创建的存储桶未启用 S3 对象锁定。如果需要为此 S3 应用程序使用 S3 对象锁定存储桶，请不要选择立即创建存储桶。请改用 Tenant Manager "创建存储桶" 稍后执行此操作。

   a. 输入 S3 应用程序将使用的存储桶的名称。例如， `s3-bucket`。

      创建存储桶后，您无法更改存储桶名称。

   b. 选择此存储桶的*区域*。

      使用默认区域(`us-east-1`），除非您希望将来使用 ILM 根据存储桶的区域筛选对象。

5. 选择*创建并继续*。

步骤 **4/6**：下载数据

在下载数据步骤中，您可以下载一个或两个文件来保存刚刚配置的详细信息。

步骤

1. 如果您选择了*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*以下载包含租户帐户名称、访问密钥 ID 和机密访问密钥的 `.csv`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*以下载包含负载平衡器端点、租户、存储桶和 root 用户设置的 `.txt`文件。
3. 请将此信息保存到安全位置。

   在复制两个访问密钥之前，请不要关闭此页面。关闭此页面后，密钥将不可用。请务必将此信息保存在安全的位置，因为它可用于从 StorageGRID 系统获取数据。

4. 如果出现提示，请选中复选框以确认已下载或复制密钥。
5. 选择 **Continue** 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、持续时间和接收行为。StorageGRID 附带的 ILM 策略会生成所有对象的两个复制副本。在您激活至少一项新策略之前，此策略有效。

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区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需要执行的操作*。
4. 选中复选框表示您了解下一步该怎么做。
5. 选择*继续*前往*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，其中描述了连接到 S3 客户端之前可能需要的其他配置。例如，选择 **Sign in as root** 会将您转至租户管理器，您可以在其中添加租户用户、创建其他存储桶并更新存储桶设置。
3. 选择 **Finish**。
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

了解 **StorageGRID** 高可用性组

高可用性(HA)组为S3客户端提供高可用性数据连接，并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高可用性 (HA) 组中。如果 HA 组中的活动接口出现故障，备份接口可以管理工作负载。

每个HA组都提供对选定节点上共享服务的访问权限。

- 包括网关节点、管理节点或两者的 HA 组为 S3 客户端提供高可用数据连接。
- 仅包含管理节点的 HA 组提供到 Grid Manager 和 Tenant Manager 的高可用性连接。
- 仅包括服务设备和基于 VMware 的软件节点的 HA 组可以为 "使用 S3 Select 的 S3 租户" 提供高可用性连接。使用 S3 Select 时建议使用 HA 组，但不是必需的。

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。

   如果接口具有 DHCP 分配的 IP 地址，则无法将其添加到 HA 组。

2. 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这些 VIP 地址中的任何一个连接到 StorageGRID。

有关说明，请参阅 "配置高可用性组"。

什么是活动接口?

在正常运行过程中，HA 组的所有 VIP 地址都会添加到主接口中，这是优先级顺序中的第一个接口。只要主接口保持可用，当客户端连接到组的任何 VIP 地址时，就会使用该接口。也就是说，在正常运行期间，主接口是组的"活动"接口。

同样，在正常操作期间，HA 组的任何优先级较低的接口都充当"备份"接口。除非主（当前活动）接口不可用，否则不会使用这些备份接口。

查看节点的当前**HA**组状态

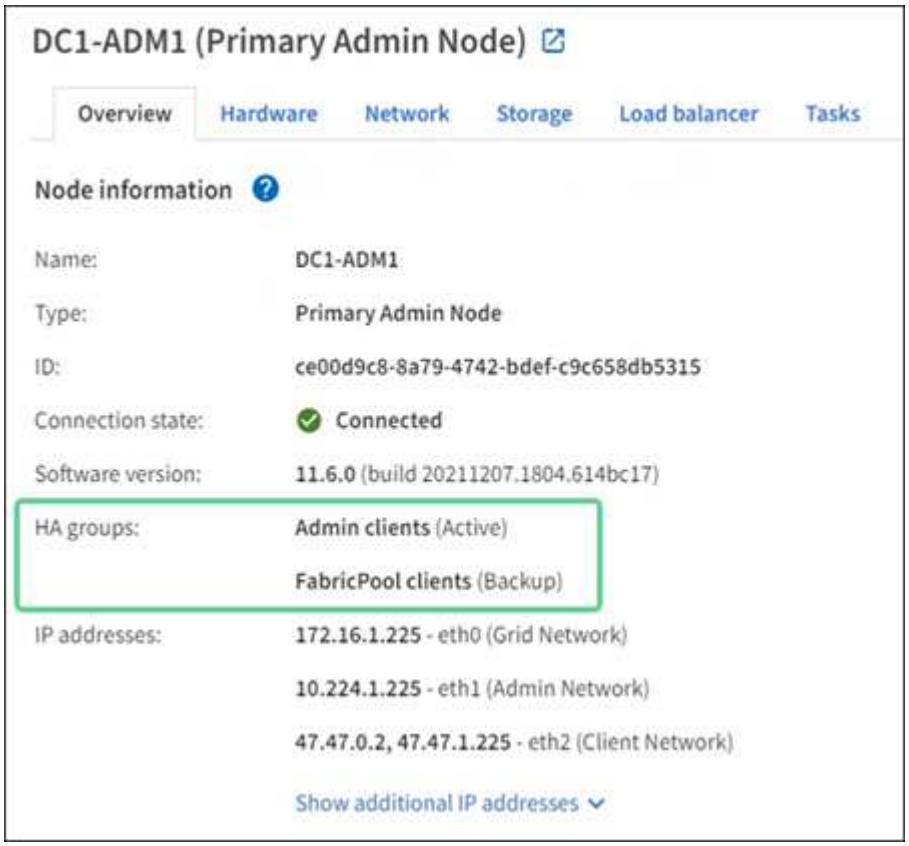
要查看是否将节点分配给 HA 组并确定其当前状态，请选择 节点 > ***node***。

如果*概述*选项卡包含 *HA 组*的条目，则该节点将被分配到列出的 HA 组。组名后面的值是该节点在 HA 组中的当前状态：

- **Active**：HA 组当前托管在此节点上。
- **Backup**：HA 组当前未使用此节点；此为备份接口。
- 已停止：HA 组无法在此节点上托管，因为高可用性（keepalived）服务已手动停止。
- **Fault**：由于以下一个或多个原因，HA 组无法在此节点上托管：
  - 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。此节点当前是 Admin 客户端组的活动接口和 FabricPool 客户端组的备份接口。



活动接口出现故障时会发生什么?

当前承载 VIP 地址的接口是活动接口。如果 HA 组包含多个接口，并且活动接口发生故障，则 VIP 地址将按优先级顺序移动到第一个可用的备份接口。如果该接口出现故障，VIP 地址将移动到下一个可用的备份接口，依此类推。

可以出于以下任意原因触发故障转移：

- 配置此接口的节点已关闭。
- 配置该接口的节点将与所有其他节点断开连接至少 2 分钟。
- 活动接口关闭。
- 负载平衡器服务停止。
- 高可用性服务停止。

> 故障转移可能不会由托管活动接口的节点外部的网络故障触发。同样，故障转移不会由 Grid Manager 或 Tenant Manager 的服务触发。

故障转移过程通常只需几秒钟，速度足够快，客户端应用程序受到的影响极小，可以依靠正常的重试行为继续运行。

当故障得到解决且更高优先级的接口再次可用时，VIP 地址将自动移动到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 (HA) 组为对象数据和管理用途提供到 StorageGRID 的高可用性连接。

- 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。
- 仅包含一个接口的 HA 组允许您提供多个 VIP 地址并显式设置 IPv6 地址。

只有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，并启用对 Grid Manager 或 Tenant Manager 的访问。
- 网关节点：包括负载平衡器服务。

HA 组的目的	将此类型的节点添加到**HA**组
访问 Grid Manager	• 主管理节点（ **Primary** ） • 非主管理节点 注意： 主管理节点必须是主界面。某些维护程序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
S3 客户端访问 "S3 Select"	• 服务设备 • 基于VMware的软件节点 注意：建议在使用 S3 Select 时使用 HA 组，但不是必需的。

对网格管理器或租户管理器使用**HA**组的限制

如果 Grid Manager 或 Tenant Manager 服务失败，则不会触发 HA 组故障转移。

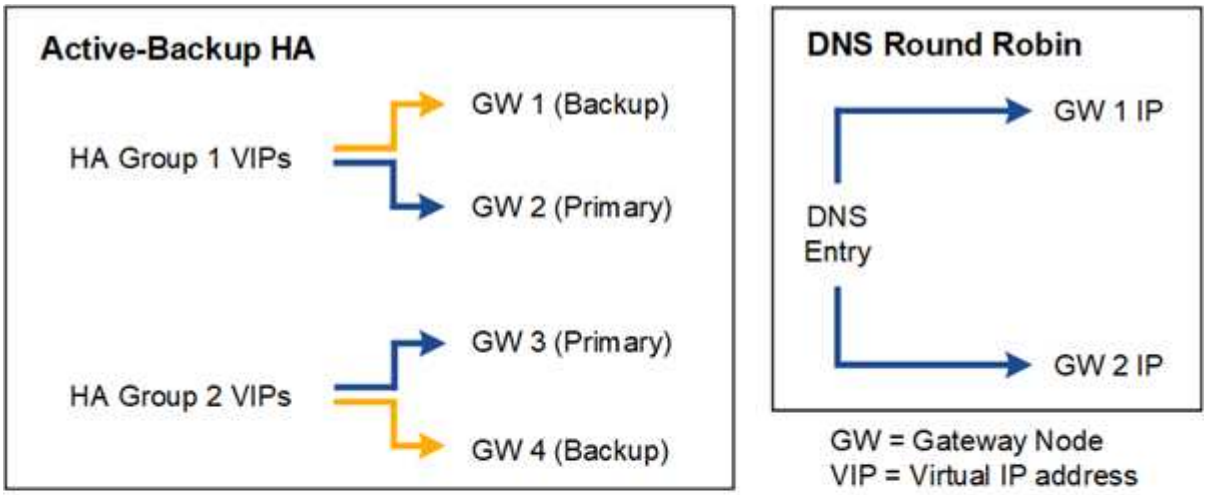
如果在发生故障转移时已登录到 Grid Manager 或 Tenant Manager，则您将被注销，必须重新登录才能继续执行任务。

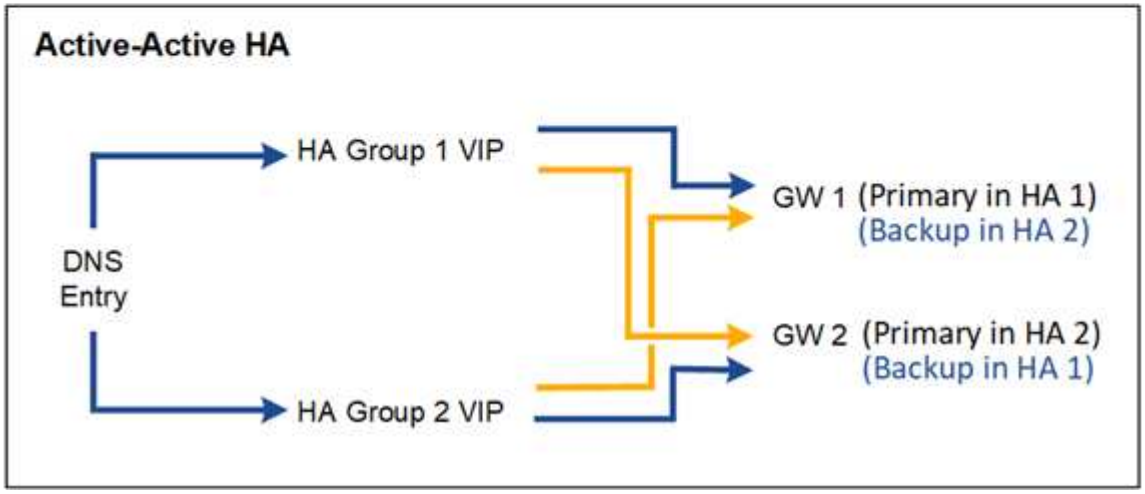
当主管理节点不可用时，无法执行某些维护程序。在故障转移期间，您可以使用 Grid Manager 监控您的 StorageGRID 系统。

StorageGRID 高可用性组的配置选项

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的每个 HA 配置的优点。

配置	优势	劣势
活动-备份 HA	• 由 StorageGRID 管理，无外部依赖关系。 • 快速故障转移。	• HA 组中只有一个节点处于活动状态。每个 HA 组至少有一个节点将处于空闲状态。
DNS 轮询	• 提高聚合吞吐量。 • 无空闲主机。	• 故障转移速度较慢，这可能取决于客户端行为。 • 需要在 StorageGRID 外部配置硬件。 • 需要客户实施的运行状况检查。

配置	优势	劣势
主动-主动 HA	• ${post_edited_translations.segment} • ${post_edited_translations.segment} • 快速故障转移。	• 配置更复杂。 • 需要在 StorageGRID 外部配置硬件。 • 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(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。

${post_edited_translations.segment}

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。
- 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"。
- ${post_edited_translations.segment}
  - **Linux**（安装节点之前）： "创建节点配置文件"
  - **Linux**（安装节点后）： "将中继或接入接口添加到节点"
  - **VMware (**安装节点后): "将中继或接入接口添加到节点"

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

创建高可用性组

创建高可用性组时，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，将一个或多个 VIP 地址分配给该组。

接口必须是网关节点或管理节点的接口，才能包含在 HA 组中。HA 组只能为任何给定节点使用一个接口；但是，同一节点的其他接口可以在其他 HA 组中使用。

访问此向导

步骤

1. 选择*配置* > 网络 > 高可用性组。
2. 选择 **Create**。

输入**HA**组的详细信息

步骤

1. 为 HA 组提供唯一名称。
2. （可选）输入HA组的说明。

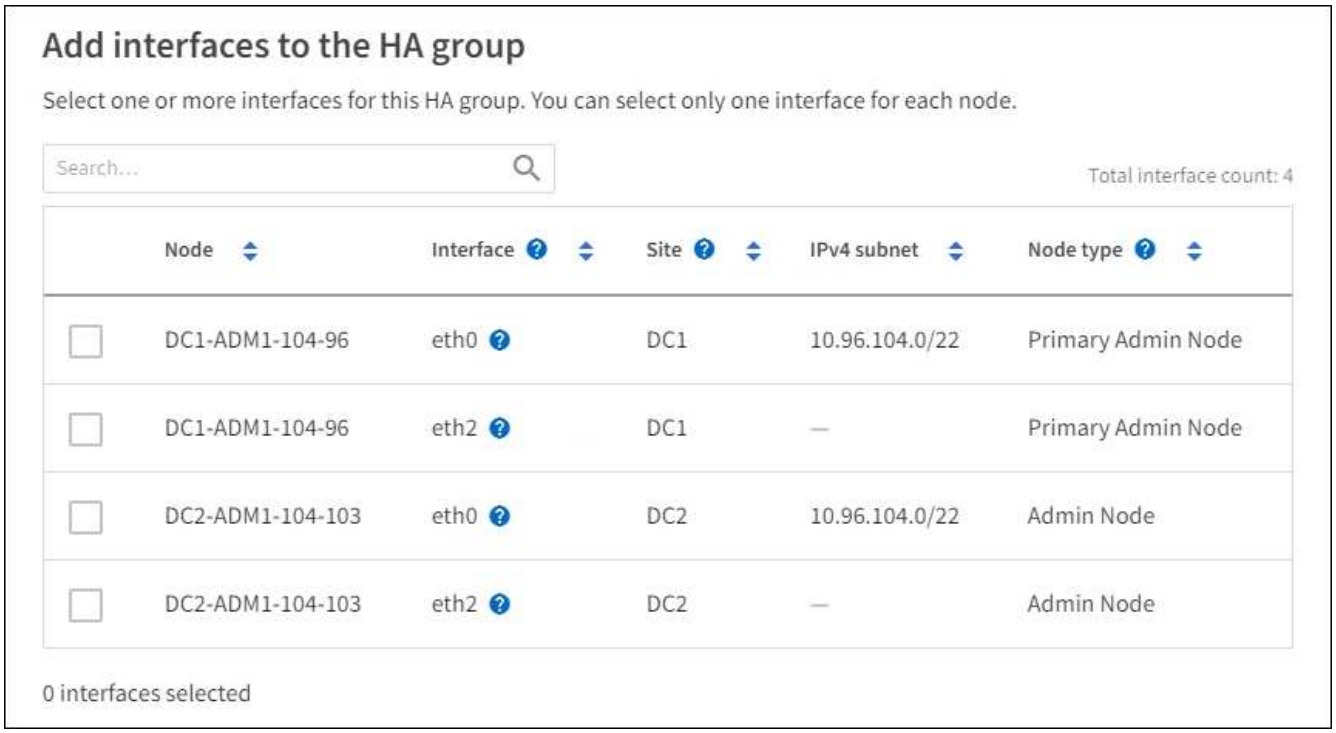
3. 选择 **Continue**。

向 **HA** 组添加接口

步骤

1. ${post_edited_translations.segment}

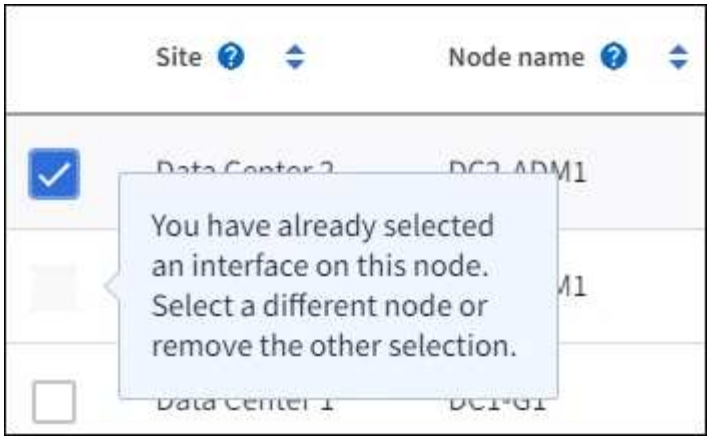
   ${post_edited_translations.segment}



   ${post_edited_translations.segment}

   接口选择指南

   - ${post_edited_translations.segment}
   - 您只能为节点选择一个接口。
   - 如果 HA 组用于管理节点服务（包括 Grid Manager 和 Tenant Manager）的 HA 保护，请仅选择管理节点上的接口。
   - ${post_edited_translations.segment}
   - 如果选择不同类型的节点上的接口，则会显示信息说明。系统会提醒您，如果发生故障转移，以前活动节点提供的服务可能在新活动节点上不可用。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，其复选框将被禁用。工具提示提供了更多信息。



- 如果接口的子网值或网关与另一个选定的接口冲突，则无法选择该接口。
- 如果配置的接口没有静态 IP 地址，则无法选择该接口。

2. 选择 **Continue**。

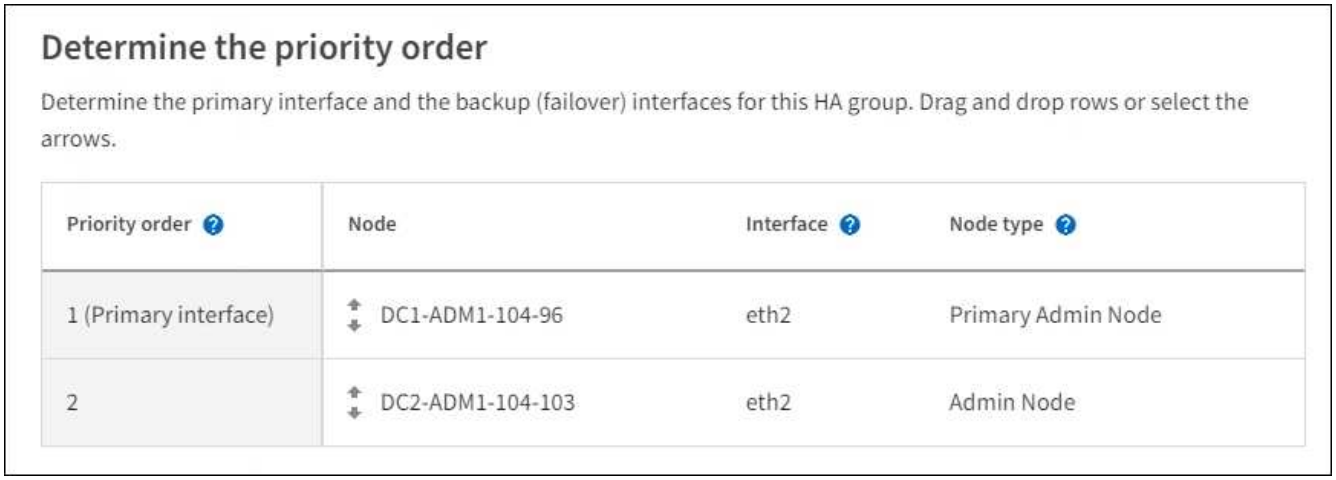
确定优先级顺序

如果 HA 组包括多个接口，则可以确定哪个是主接口，哪个是备份（故障转移）接口。如果主接口出现故障，VIP 地址将移动到可用的最高优先级接口。如果该接口出现故障，VIP 地址将移动到下一个可用的最高优先级接口，依此类推。

步骤

1. 在*优先级顺序*列中拖动行以确定主接口和任何备份接口。

   列表中的第一个接口是 Primary 接口。除非发生故障，否则 Primary 接口为活动接口。



如果 HA 组提供对 Grid Manager 的访问权限，则必须在主管理节点上选择一个接口作为主接口。某些维护程序只能从主管理节点执行。

2. 选择 **Continue**。

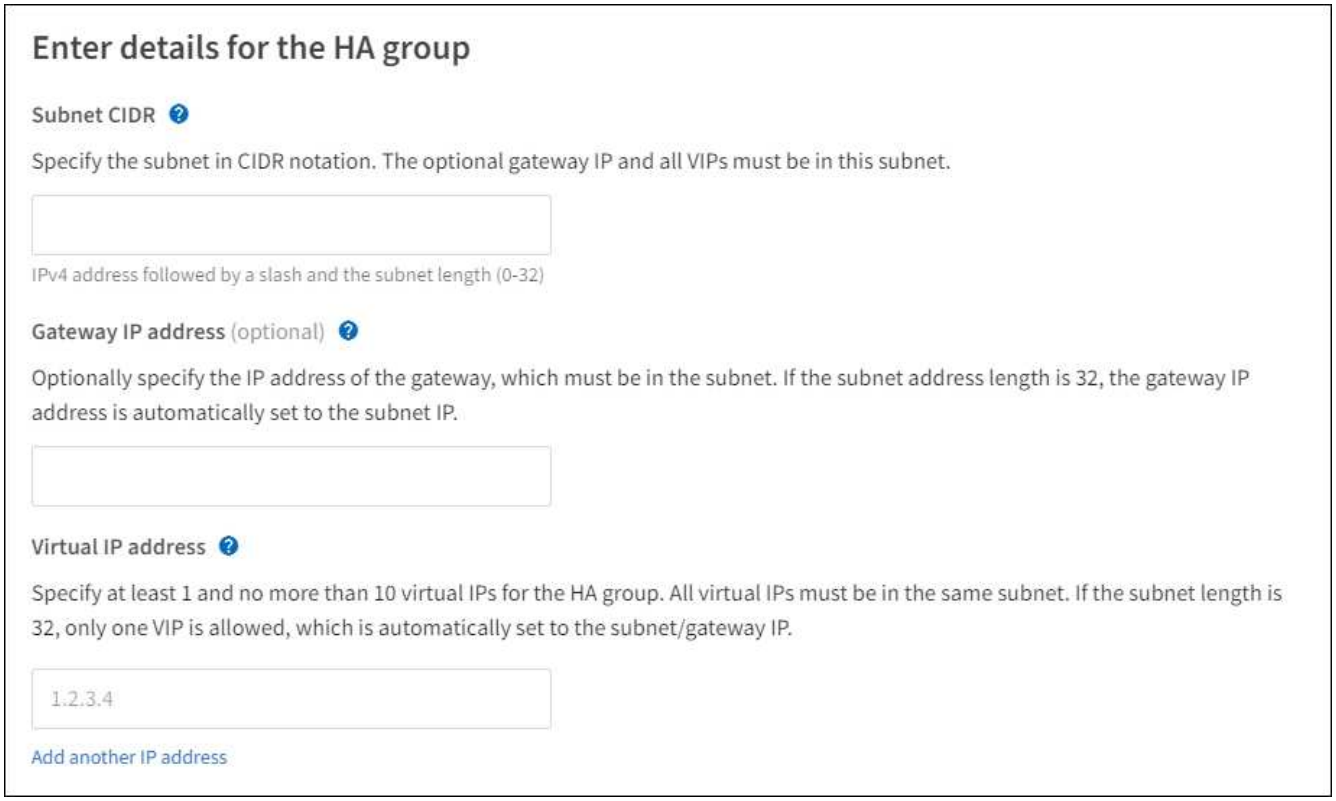
输入 **IP** 地址

步骤

1. 在 **Subnet CIDR** 字段中，以 CIDR 表示法指定 VIP 子网——一个 IPv4 地址，后跟斜杠和子网长度（0-32）。

   网络地址不得设置任何主机位。例如， `192.16.0.0/22`。

   ${post_edited_translations.segment}



2. 可选地，如果任何 S3 管理或租户客户端将从不同的子网访问这些 VIP 地址，请输入*网关 IP 地址*。网关地址必须在 VIP 子网内。

   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 组中的活动接口输入至少一个且不超过十个 VIP 地址。所有 VIP 地址必须位于 VIP 子网内，并且所有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*。

   已创建 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(HA)组以更改其名称和描述、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过程中的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 HA 组。

2. 选中要编辑的 HA 组的复选框。
3. 根据您要更新的内容，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*以更新组的名称或描述、添加或删除接口、更改优先级顺序或添加或删除 VIP 地址。
4. 如果您选择了*编辑虚拟 IP 地址*：
   a. 更新HA组的虚拟IP地址。
   b. 选择 **Save**。
   c. 选择 **Finish**。
5. 如果选择 **Edit HA group**：
   a. （可选）更新组的名称或描述。
   b. （可选）选中或清除复选框以添加或删除接口。

      如果 HA 组提供对 Grid Manager 的访问权限，则必须在主管理节点上选择一个接口作为主接口。某些维护程序只能从主管理节点执行

   c. 可选操作：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. （可选）更新虚拟 IP 地址。
   e. 选择 **Save**，然后选择 **Finish**。

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。

如果高可用性 (HA) 组已绑定到负载均衡器端点，则无法将其删除。要删除 HA 组，必须将其从使用该组的任何负载均衡器端点中移除。

为了防止客户端中断，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另一个 IP 地址进行连接，例如，其他 HA 组的虚拟 IP 地址或在安装期间为接口配置的 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. ${post_edited_translations.segment}
   b. 选中端点的复选框。
   c. 选择*操作* > 编辑端点绑定模式。
   d. ${post_edited_translations.segment}
   e. 选择 **Save changes**。
3. 如果未列出负载平衡器端点，请选中要删除的每个 HA 组的复选框。
4. 选择*操作* > 删除 **HA** 组。
5. 查看消息并选择 **Delete HA group** 以确认您的选择。

   您选择的所有 HA 组均已删除。"高可用性组"页面上将显示绿色成功横幅。

管理负载平衡

了解 StorageGRID 负载平衡

您可以使用负载均衡来处理来自 S3 客户端的接收和检索工作负载。

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 使用负载均衡器来管理摄取和检索工作负载。负载均衡通过将工作负载分布在多个存储节点上，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。它执行客户端请求的传输层安全性 (TLS) 终止，检查请求，并建立到存储节点的新安全连接。

在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独立运行。通过加权过程，负载平衡器服务将更多请求路由到 CPU 可用性更高的存储节点。

> 虽然 StorageGRID 负载均衡器服务是推荐的负载均衡机制，但您可能需要集成第三方负载均衡器。有关信息，请联系您的 NetApp 客户代表或参阅 "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？

作为一般最佳做法，StorageGRID 系统中的每个站点都应包含具有负载平衡器服务的两个或多个节点。例如，站点可能包括两个网关节点，或者同时包括管理节点和网关节点。确保每个负载平衡节点都有足够的网络、硬件或虚拟化基础架构，无论您是使用服务设备、裸机节点还是基于虚拟机 (VM) 的节点。

什么是负载平衡器端点？

负载平衡器端点定义传入和传出客户端应用程序请求将用于访问包含负载平衡器服务的那些节点的端口和网络协议（HTTPS 或 HTTP）。端点还定义了客户端类型（S3）、绑定模式，以及可选的允许或阻止的租户列表。

要创建负载平衡器端点，请使用 Grid Manager 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"

负载平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，缓存会显著提高性能。此外，缓存提供对对象存储的远程访问，而无需完整的网格部署。负载平衡器缓存仅适用于网关节点。

创建负载平衡器端点时：

- 仅对可缓存的工作负载启用缓存。与未缓存数据相比，访问缓存数据频率更低的工作负载，其性能将比未使用缓存服务时更差。在某些情况下，覆盖率和逐出率较高的工作负载也可能超过保修的驱动器写入耐久性。
- 考虑添加额外的端点或节点，以缓存适合缓存的各个工作负载。
- 对可缓存和不可缓存的工作负载使用不同的端点。这种分离可确保适当应用缓存机制，并且不会干扰不可缓存的数据处理。
- 通过将其定向到启用缓存的端点来评估潜在的可缓存工作负载。监控并验证缓存命中率，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高效使用缓存资源。
- "查看审核日志" 以确定现有工作负载是否适合缓存。在给定的时间段内，确定唯一对象的 GET 百分比。要适合缓存，此值应低于 50%。

可能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

如果要由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。

不会缓存的对象和请求的类型

- The `response-content-encoding` 查询参数

- The `partNumber` 查询参数
- 条件标头
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- 使用以下任何内容进行静态加密的请求：
  - SSE（使用 StorageGRID 管理的密钥的服务器端加密）
  - SSE-C（使用客户提供的密钥的服务器端加密）
  - 存储对象加密

未缓存的任何请求都将转发到上游 LDR，就像未启用缓存一样。

相关信息

- "对负载平衡器缓存进行故障排除"
- 有关负载平衡器缓存的详细信息，请与技术支持联系。

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。如果您使用端口 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保留。如果您对多个端点使用相同的端口，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所用的端口。请参阅"StorageGRID 内部端口"。

网络协议的注意事项

在大多数情况下，客户端应用程序与 StorageGRID 之间的连接应使用传输层安全性 (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 负载均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** 作为负载均衡器端点的网络协议，则必须提供安全证书。创建负载均衡器端点时，可以使用以下三个选项中的任何一个：

- 上传已签名的证书（推荐）。此证书可以由公用信任的证书颁发机构或专用证书颁发机构 (CA) 签名。使用公开可信的 CA 服务器证书来保护连接是最佳做法。与生成的证书不同，由 CA 签名的证书可以无中断地轮换，这有助于避免过期问题。

  在创建负载平衡器端点之前，必须获取以下文件：

  - 自定义服务器证书文件。
  - 自定义服务器证书私钥文件。
  - 可选，来自每个中间颁发证书颁发机构的证书的 CA 捆绑包。

- 生成自签名证书。
- 使用全局 **StorageGRID S3** 证书。必须上传或生成此证书的自定义版本，然后才能将其选择用于负载平衡器端点。请参阅 "配置 S3 API 证书"。

我需要哪些值?

要创建证书，您必须知道 S3 客户端应用程序将用于访问端点的所有域名和 IP 地址。

证书的 使用者 **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，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*备用名称*条目，包括任何通配符名称。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

如果对域名使用通配符，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 DNS 条目。

如何管理过期的证书?

如果用于保护 S3 应用程序和 StorageGRID 之间连接的证书过期，则应用程序可能会暂时失去对 StorageGRID 的访问权限。

要避免证书过期问题，请遵循以下最佳实践：

- 仔细监控任何警告证书过期日期即将到来的警报，例如*负载平衡器端点证书过期*和*S3 API 全局服务器证书过期*警报。
- 始终保持 StorageGRID 和 S3 应用程序的证书版本同步。如果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。
- 使用公开签名的 CA 证书。如果使用由 CA 签名的证书，则可以无中断地替换即将过期的证书。
- 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

绑定模式可让您控制哪些 IP 地址可用于访问负载平衡器端点。如果端点使用绑定模式，则客户端应用程序只有在使用允许的 IP 地址或其相应的完全限定域名 (FQDN) 时才能访问端点。使用任何其他 IP 地址或 FQDN 的客户端应用程序无法访问端点。

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、任何网络上的任何 HA 组的虚拟 IP (VIP) 地址或相应的 FQDN 来访问端点。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。客户端必须使用所选节点接口的 IP 地址（或相应的 FQDN）。
- 节点类型。根据您选择的节点类型，客户端必须使用任意管理节点的 IP 地址（或相应的 FQDN）或任意网关节点的 IP 地址（或相应的 FQDN）。

租户访问的注意事项

租户访问是一项可选安全功能，允许您控制哪些 StorageGRID 租户帐户可以使用负载平衡器端点来访问其存储桶。您可以允许所有租户访问端点（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拥有的绝密或高度机密的材料对其他租户完全不可访问。

> 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确定的，如果请求中未提供访问密钥（例如匿名访问），则使用存储桶所有者来确定租户。

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，并允许访问所有租户。
   - **Top secret** 端点：使用端口 10444，仅允许访问 **Top secret** 租户。所有其他租户均无法访问此端点。
2. The `top-secret.pdf` 位于*绝密*租户拥有的存储桶中。

要访问 `top-secret.pdf`，*绝密*租户中的用户可以向 `\https://w.x.y.z:10444/top-secret.pdf` 发出 GET 请求。由于允许此租户使用 10444 端点，因此用户可以访问该对象。但是，如果属于任何其他租户的用户向相同的 URL 发出相同的请求，则会立即收到"拒绝访问"消息。即使凭据和签名有效，也会拒绝访问。

CPU可用性

每个管理节点和网关节点上的负载平衡器服务在将 S3 流量转发到存储节点时独立运行。通过加权过程，负载平衡器服务将更多请求路由到具有更高 CPU 可用性的存储节点。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 100% 的利用率或未能报告其利用率，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均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 Grid Manager、Tenant Manager 或两者。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。
- 您已审阅 "负载平衡的注意事项"。
- 如果您之前重新映射了要用于负载平衡器端点的端口，则您有 "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，但不是必需的。请参阅 "管理高可用性组"。
- 如果负载均衡器端点将由 "S3 Select 的 S3 租户" 使用，则不得使用任何裸机节点的 IP 地址或 FQDN。用于 S3 Select 的负载均衡器端点仅允许使用服务设备和基于 VMware 的软件节点。
- 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（推荐），则需要具备服务器证书的相关信息。

  对端点证书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，需要服务器证书、证书私钥以及 CA 捆绑包（可选）。
  - 要生成证书，您需要 S3 客户端用于访问端点的所有域名和 IP 地址。您还必须了解主题（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"。

创建负载均衡器端点

每个 S3 客户端负载平衡器端点都指定端口、客户端类型 (S3) 和网络协议（HTTP 或 HTTPS）。管理接口负载平衡器端点指定端口、接口类型和不受信任的客户端网络。

访问此向导

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 client** 选项卡。
3. 要创建用于访问 Grid Manager、Tenant Manager 或两者的端点，请选择*管理界面*选项卡。
4. 选择 **Create**。

输入端点详细信息

步骤

1. 选择适当的说明以输入要创建的端点类型的详细信息。

S3客户端

字段	问题描述
名称	端点的描述性名称，将显示在负载均衡器端点页面的表格中。
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 1 到 65535 之间的任何未使用的外部端口。 如果您输入 **80** 或 **8443**，则仅在网关节点上配置端点，除非您已释放端口 8443。然后，您可以使用端口 8443 作为 S3 端点，该端口将在网关节点和管理节点上进行配置。
客户端类型	必须是 **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** 进行安全的 TLS 加密通信（推荐）。必须先附加安全证书，然后才能保存端点。 • 选择 **HTTP** 进行不太安全的未加密通信。仅对非生产网格使用 HTTP。
启用缓存	为此负载均衡器端点启用或禁用 "网关节点上的缓存"。 如果缓存出现问题，请参阅 "对负载平衡器缓存进行故障排除"。

管理界面

字段	问题描述
名称	端点的描述性名称，将显示在负载均衡器端点页面的表格中。
端口	要用于访问 Grid Manager、Tenant Manager 或两者的 StorageGRID 端口。 • 网格管理器：**8443** • 租户管理器：**9443** • Grid Manager 和 Tenant Manager：**443** 注意：您可以使用这些预设端口或其他可用端口。
接口类型	选择您将使用此端点访问的 StorageGRID 接口的单选按钮。

字段	问题描述
不受信任的客户端网络	如果此端点应可供不受信任的客户端网络访问，请选择*是*。否则，请选择*否*。 当您选择*是*时，该端口将在所有不受信任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受信任的客户端网络开放或关闭。

1. 选择 **Continue**。

选择绑定模式

步骤

1. 选择端点的绑定模式，以控制使用任何 IP 地址或使用特定 IP 地址和网络接口访问端点的方式。

   某些绑定模式可用于客户端端点或管理接口端点。此处列出了两种端点类型的所有模式。

模式	问题描述
全局(客户端端点的默认值)	客户端可以使用任何网关节点或管理节点的 IP 地址、任何网络上的任何 HA 组的虚拟 IP (VIP) 地址或相应的 FQDN 来访问端点。 除非需要限制此端点的可访问性，否则请使用*全局*设置。
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）来访问此端点。 具有此绑定模式的端点都可以使用相同的端口号，只要您为端点选择的 HA 组不重叠即可。
节点接口	${post_edited_translations.segment}
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（管理接口端点的默认值）	客户端必须使用任何管理节点的 IP 地址（或相应的 FQDN）来访问此端点。

   如果多个端点使用相同的端口，StorageGRID 使用此优先级顺序来决定使用哪个端点：**HA** 组的虚拟 **IP** > 节点接口 > 节点类型 > 全局。

   如果要创建管理接口端点，则仅允许使用管理节点。

2. 如果您选择了 **Virtual IPs of HA groups**，请选择一个或多个 HA 组。

   如果要创建管理界面端点，请选择仅与管理节点关联的 VIP。

3. 如果选择*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. 如果您选择了*节点类型*，请选择管理节点（其中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

只有当终结点具有 Tenant Manager 的接口类型 时，管理接口终结点才能控制租户访问。

步骤

1. 对于*租户访问*步骤，请选择以下选项之一：

字段	问题描述
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存储区。 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，可以编辑负载平衡器端点以允许或阻止特定帐户。
允许选定的租户	只有选定租户帐户可以使用此端点访问其存储桶。
阻止选定租户	选定的租户帐户无法使用此端点来访问其存储桶。所有其他租户都可以使用此端点。

2. 如果您正在创建 **HTTP** 端点，则无需附加证书。选择 创建 以添加新的负载均衡器端点。然后，转到 完成后。否则，选择 继续 以附加证书。

${post_edited_translations.segment}

步骤

1. ${post_edited_translations.segment}

   该证书保护 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。

   - 上传证书。如果要上传自定义证书，请选择此选项。
   - 生成证书。如果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。如果您要使用全局 S3 API 证书，请选择此选项，该证书也可用于直接连接到存储节点。

     除非您已将由网格 CA 签名的默认 S3 API 证书替换为由外部证书颁发机构签名的自定义证书，否则无法选择此选项。请参见 "配置 S3 API 证书"。

   - 使用管理接口证书。如果您要使用全局管理接口证书，请选择此选项，该证书也可用于直接连接到 Admin Nodes。

2. ${post_edited_translations.segment}

上传证书

a. 选择*上传证书*。

b. 上传所需的服务器证书文件：

   - ${post_edited_translations.segment}
   - 证书私钥：自定义服务器证书私钥文件 (`.key`）。

     EC 私钥必须为 224 位或更大。RSA 私钥必须为 2048 位或更大。

   - **CA bundle**：包含来自每个中间颁发证书颁发机构 (CA) 的证书的单个可选文件。该文件应包含以证书链顺序连接的每个 PEM 编码的 CA 证书文件。

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 捆绑包，则每个证书都会显示在自己的选项卡上。

   - 选择*下载证书*保存证书文件，或选择*下载 CA 捆绑包*保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

   例如： `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. 选择 **Create**。+ 此时将创建负载均衡器端点。自定义证书将用于 S3 客户端或管理界面与该端点之间后续的所有新连接。

生成证书

a. 选择*生成证书*。

b. 指定证书信息：

字段	问题描述
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 主题或标识名 (DN)。 如果在此字段中未输入任何值，则生成的证书将使用第一个域名或 IP 地址作为使用者通用名称 (CN)。
有效天数	创建后证书过期的天数。

字段	问题描述
添加密钥使用扩展	${post_edited_translations.segment} ${post_edited_translations.segment} ${post_edited_translations.segment}

c. 选择 **Generate**。

d. 选择*证书详细信息*可查看生成的证书的元数据。

- 选择*下载证书*以保存证书文件。

  指定证书文件名和下载位置。使用扩展名 `.pem` 保存文件。

例如： `storagegrid_certificate.pem`

- 选择 **Copy certificate PEM** 以复制证书内容并粘贴到其他位置。

e. 选择 **Create**。

已创建负载均衡器端点。自定义证书用于 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. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

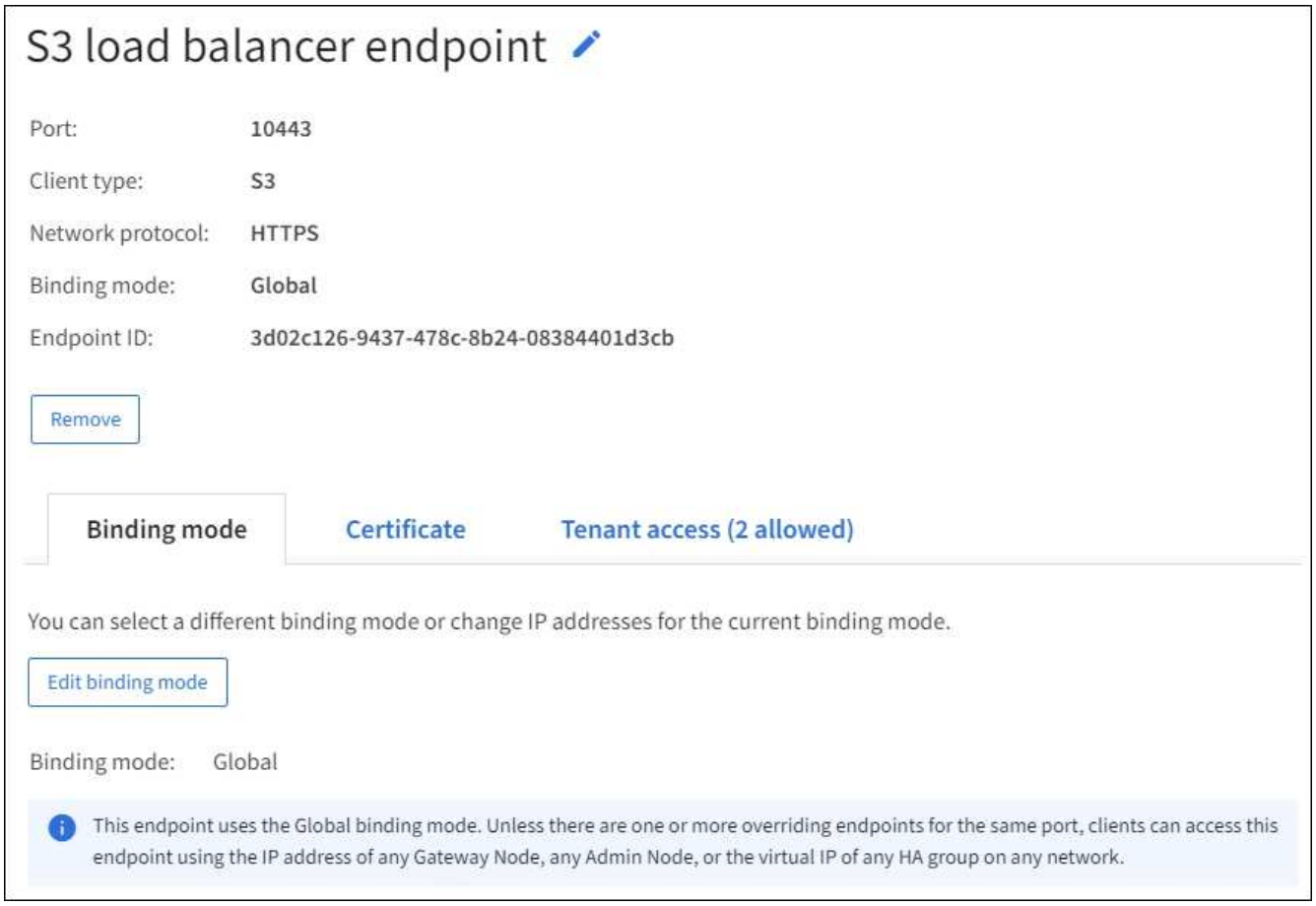
     ${post_edited_translations.segment}

2. 请向 S3 客户端提供连接到端点所需的信息：
   - ${post_edited_translations.segment}
   - 完全限定的域名或 IP 地址
   - ${post_edited_translations.segment}

${post_edited_translations.segment}

您可以查看现有负载均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。

- ${post_edited_translations.segment}
- 要查看有关特定端点的所有详细信息（包括证书元数据），请在表中选择该端点的名称。显示的信息因端点类型及其配置方式而异。



- ${post_edited_translations.segment}

如果在编辑管理接口端点端口时无法访问 Grid Manager，请更新 URL 和端口以重新获得访问权限。

${post_edited_translations.segment}

任务	**${post_edited_translations.segment}**	详细信息页面
编辑端点名称	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点名称。 c. 输入新名称。 d. 选择 **Save**。	a. ${post_edited_translations.segment} b. 选择编辑图标 。 c. 输入新名称。 d. 选择 **Save**。
${post_edited_translations.segment}	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点端口 c. ${post_edited_translations.segment} d. 选择 **Save**。	不适用

任务	**${post_edited_translations.segment}**	详细信息页面
编辑端点绑定模式	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点绑定模式。 c. ${post_edited_translations.segment} d. 选择 **Save changes**。	a. ${post_edited_translations.segment} b. 选择*编辑绑定模式*。 c. ${post_edited_translations.segment} d. 选择 **Save changes**。
编辑端点证书	a. 选中端点的复选框。 b. 选择*操作* > 编辑端点证书。 c. 根据需要上传或生成新的自定义证书，或开始使用全局 S3 证书。 d. 选择 **Save changes**。	a. ${post_edited_translations.segment} b. 选择 **Certificate** 选项卡。 c. ${post_edited_translations.segment} d. 根据需要上传或生成新的自定义证书，或开始使用全局 S3 证书。 e. 选择 **Save changes**。
${post_edited_translations.segment}	a. 选中端点的复选框。 b. ${post_edited_translations.segment} c. 选择其他访问选项，从列表中选择或删除租户，或同时执行这两项操作。 d. 选择 **Save changes**。	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. 选择*编辑租户访问权限*。 d. 选择其他访问选项，从列表中选择或删除租户，或同时执行这两项操作。 e. 选择 **Save changes**。

删除负载平衡器端点

${post_edited_translations.segment}

为防止客户端中断，请在删除负载均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，使其使用分配给另一个负载均衡器端点的端口进行连接。请务必同时更新任何所需的证书信息。

${post_edited_translations.segment}

- 要删除一个或多个端点：
  a. 从"负载平衡器"页面中，选中要删除的每个端点的复选框。
  b. 选择*操作* > 删除。
  c. 选择 **OK**。
- 从详细信息页面中删除一个端点：
  a. 从负载均衡器页面，选择端点名称。
  b. 在详细信息页面上选择*移除*。
  c. 选择 **OK**。

在 StorageGRID 中配置 S3 端点域名

要支持 S3 虚拟托管样式的请求，必须使用 Grid Manager 配置 S3 客户端连接到的 S3 端点域名列表。

不支持为端点域名使用 IP 地址。未来的版本将阻止此配置。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。
- 您已确认未进行网格升级。

正在进行网格升级时，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，必须执行以下所有操作：

- ${post_edited_translations.segment}
- 确保已针对客户端所需的所有域名对 "客户端用于与 StorageGRID 建立 HTTPS 连接的证书" 进行了签名。

  例如，如果端点为 `s3.company.com`，则必须确保用于 HTTPS 连接的证书包含 `s3.company.com` 端点以及该端点的通配符主题备用名称 (SAN)： `*.s3.company.com`。

- 配置客户端使用的 DNS 服务器。包含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 地址连接到 StorageGRID，也可以通过连接到高可用性组的虚拟 IP 地址进行连接。您应该了解客户端应用程序如何连接 to 网格，以便在 DNS 记录中包含正确的 IP 地址。

${post_edited_translations.segment}

- 连接到负载均衡器端点的客户端可以使用该端点的自定义证书。每个负载均衡器端点都可以配置为识别不同的 S3 端点域名。
- ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

步骤

1. 选择*配置* > 网络 > **S3** 端点域名。
2. 在 **Domain name 1** 字段中输入域名。选择 **Add another domain name** 以添加更多域名。
3. 选择 **Save**。

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其自己的证书的负载平衡器端点，"更新与端点关联的证书"。
   - 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，则 "更新全局 S3 API 证书"。
5. 添加确保可以解析端点域名请求所需的 DNS 记录。

结果

现在，当客户端使用端点 `*bucket.s3.company.com*`时，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，则虚拟托管样式的请求将失败。

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 **Save**。
4. 选择*是*以确认更改。

删除 **S3** 端点域名

如果删除 S3 应用程序使用的名称，则虚拟托管风格的请求将失败。

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

${post_edited_translations.segment}

客户端应用程序可以使用网格节点的 IP 地址和该节点上的服务端口号连接到 StorageGRID。也可以创建负载平衡节点的高可用性 (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，可以配置 DNS 条目。

下表总结了客户端连接到 StorageGRID 的不同方式，以及每种连接类型所使用的 IP 地址和端口。如果您已创建负载均衡器端点和高可用性 (HA) 组，请参见 <<${post_edited_translations.segment}>> 以在 Grid Manager 中找到这些值。

在何处进行连接	**${post_edited_translations.segment}**	**IP** 地址	端口
HA 组	负载平衡器	HA 组的虚拟 IP 地址	${post_edited_translations.segment}
管理节点	负载平衡器	管理节点的 IP 地址	${post_edited_translations.segment}
网关节点	负载平衡器	网关节点的 IP 地址	${post_edited_translations.segment}
存储节点	LDR	${post_edited_translations.segment}	${post_edited_translations.segment} • HTTPS：18082 • HTTP：18084

示例 **URL**

要将客户端应用程序连接到网关节点的 HA 组的负载均衡器端点，请使用如下所示的 URL 结构：

`https://VIP-of-HA-group:LB-endpoint-port`

${post_edited_translations.segment}

`https://192.0.2.5:10443`

${post_edited_translations.segment}

1. 使用 "支持的 Web 浏览器" 登录到网格管理器。
2. 要查找网格节点的 IP 地址：
   a. 选择 **Nodes**。
   b. ${post_edited_translations.segment}
   c. 选择 **Overview** 选项卡。
   d. 在节点信息部分，记下节点的 IP 地址。
   e. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

      - ${post_edited_translations.segment}
      - **eth1:** 管理网络（可选）
      - **eth2:** 客户端网络（可选）

      ${post_edited_translations.segment}

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. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   a. 选择*配置* > 网络 > 负载均衡器端点。
   b. 请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，因为这些端口在管理节点上保留。所有其他端口都配置在网关节点和管理节点上。

   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

管理网络和连接

配置 StorageGRID 网络设置

您可以从 Grid Manager 配置各种网络设置，以微调 StorageGRID 系统的操作。

配置 VLAN 接口

您可以"${post_edited_translations.segment}"隔离和分区流量，以实现安全性、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关联。您可以在 HA 组和负载平衡器端点中使用 VLAN 接口，以按应用程序或租户隔离客户端或管理员流量。

${post_edited_translations.segment}

您可以使用"${post_edited_translations.segment}"来识别和处理不同类型的网络流量，包括与特定存储桶、租户、客户端子网或负载均衡器端点相关的流量。这些策略可以帮助限制和监控流量。

StorageGRID 网络指南

您可以使用 Grid Manager 配置和管理 StorageGRID 网络和连接。

请参见"配置 S3 客户端连接"以了解如何连接 S3 客户端。

默认 StorageGRID 网络

默认情况下，StorageGRID 支持每个网格节点三个网络接口，允许您为每个单独的网格节点配置网络，以满足您的安全和访问要求。

有关网络拓扑的详细信息，请参见 "网络连接准则"。

网格网络

必需。网格网络用于所有内部 StorageGRID 流量。它提供网格中所有节点之间、所有站点和子网之间的连接。

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。管理网络通常是专用网络，不需要在站点之间路由。

客户端网络

可选。客户端网络是一个开放网络，通常用于提供对 S3 客户端应用程序的访问，因此可以隔离和保护网格网络。客户端网络可以与通过本地网关可访问的任何子网通信。

实施准则

- 每个 StorageGRID 节点都需要为其分配的每个网络提供专用网络接口、IP 地址、子网掩码和网关。
- 一个网格节点在网络上不能有多个接口。
- 每个网络、每个网格节点支持一个网关，且该网关必须与节点位于同一子网。如果需要，您可以在网关中实现更复杂的路由。
- 在每个节点上，每个网络都映射到特定的网络接口。

网络	接口名称
Grid	eth0
管理员（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，请参见设备的安装说明。
- 默认路由是按节点自动生成的。如果启用了 eth2，则 0.0.0.0/0 使用 eth2 上的客户端网络。如果未启用 eth2，则 0.0.0.0/0 使用 eth0 上的网格网络。
- 在网格节点加入网格之前，客户端网络不会开始运行
- 可以在网格节点部署期间配置管理网络，以允许在网格完全安装之前访问安装用户界面。

可选接口

您也可以选择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，您可能需要添加一个访问接口，以便在 "高可用性(HA)组" 中使用。

要添加中继或接入接口，请参见以下内容：

- **VMware** （安装节点后）：“VMware：将中继或访问接口添加到节点”
  - **Linux**（安装节点之前）：“创建节点配置文件”
  - **Linux**（安装节点后）：“将中继或接入接口添加到节点”

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

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 地址在命令行登录到该网格节点并执行各种维护程序。

开始之前

您已使用 "支持的 Web 浏览器" 登录到网格管理器。

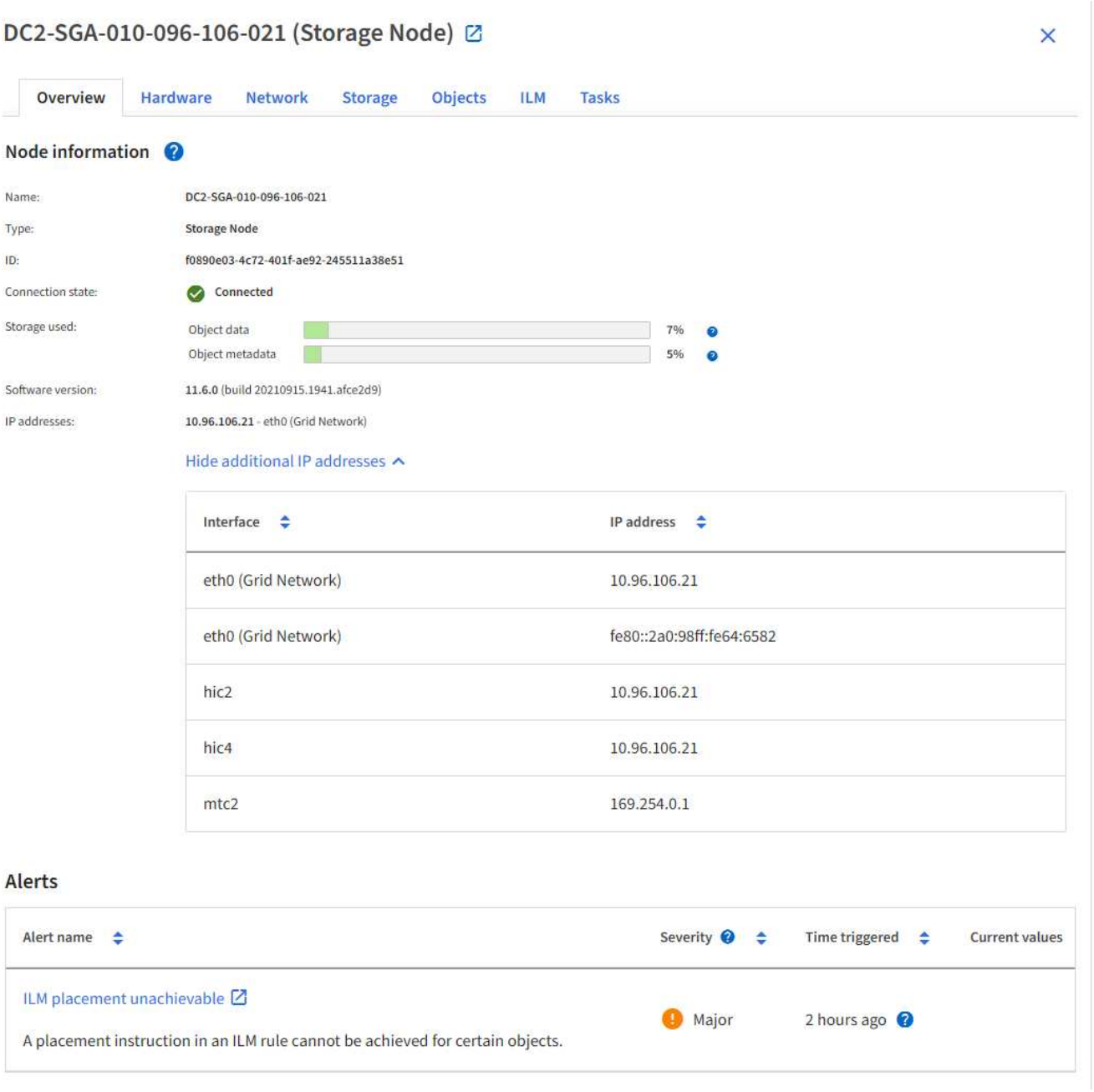
关于此任务

有关更改 IP 地址的信息，请参见 "配置 IP 地址"。

步骤

1. ${post_edited_translations.segment}
2. 选择 IP Addresses 标题右侧的*显示更多*。

   ${post_edited_translations.segment}



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这些接口来隔离和分区流量，以实现安全性、灵活性和性能。HA 组中的选定节点可以使用 VLAN 接口共享多达 10 个虚拟 IP 地址，因此如果某个节点发生故障，另一个节点将接管与虚拟 IP 地址之间的流量。

VLAN 接口注意事项

- 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，您不能在同一 Gateway Node 上同时使用网格网络接口和客户端网络接口作为同一 VLAN 的父接口。
- 如果 VLAN 接口用于管理节点流量（包括与 Grid Manager 和 Tenant Manager 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，请参见以下详细信息：
  - **VMware** （安装节点后）：“VMware：将中继或访问接口添加到节点”
  - **Linux**（安装节点之前）：“创建节点配置文件”
  - **Linux**（安装节点后）：“将中继或接入接口添加到节点”

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

创建 **VLAN** 接口

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。
- 中继接口已在网络中配置并连接到 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和一个或多个 VLAN，以隔离属于不同应用程序或租户的客户端或管理员流量。每个 VLAN 都由数字 ID 或标记标识。例如，您的网络可能使用 VLAN 100 作为 FabricPool 流量，使用 VLAN 200 作为存档应用程序。

您可以使用 Grid Manager 创建 VLAN 接口，允许客户端访问特定 VLAN 上的 StorageGRID。创建 VLAN 接口时，您需要指定 VLAN ID 并在一个或多个节点上选择父（中继）接口。

访问此向导

步骤

1. 选择*配置* > 网络 > **VLAN**接口。
2. 选择 **Create**。

输入 **VLAN** 接口的详细信息

步骤

1. 指定网络中的 VLAN 的 ID。您可以输入介于 1 到 4094 之间的任何值。

   VLAN ID 不必是唯一的。例如，您可以将 VLAN ID 200 用于一个站点的管理员流量，将相同的 VLAN ID 用于另一个站点的客户端流量。您可以在每个站点上创建具有不同父接口集的单独 VLAN 接口。但是，具有相同 ID 的两个 VLAN 接口不能在节点上共享相同的接口。如果指定已使用的 ID，则会显示一条消息。

2. （可选）输入 VLAN 接口的简短说明。
3. 选择 **Continue**。

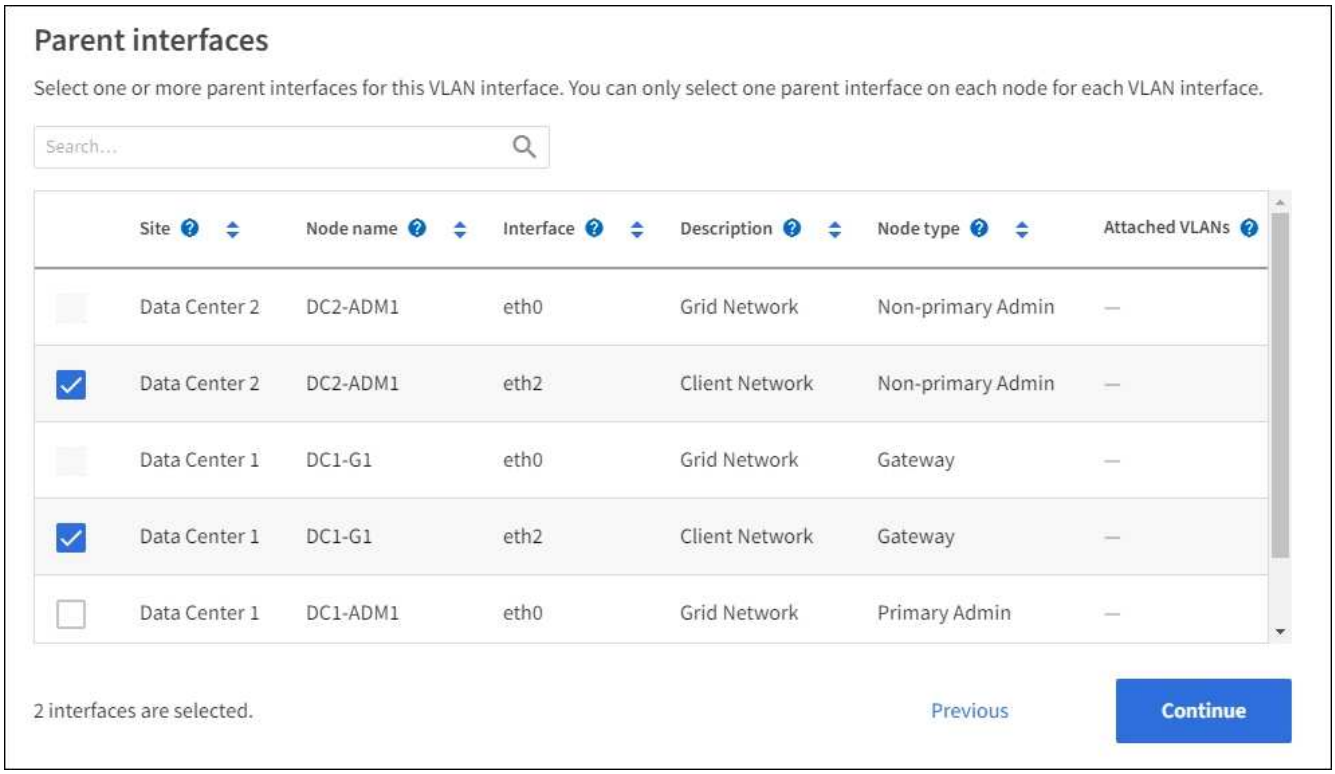
选择父接口

该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。

步骤

1. 选择一个或多个要附加此 VLAN 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 **Continue**。

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 或描述，请在页面顶部选择 输入 **VLAN** 详细信息。
   - 如果需要更改父接口，请在页面顶部选择 **Choose parent interfaces**，或选择 **Previous**。
   - 如果需要删除父接口，请选择垃圾桶 。
2. 选择 **Save**。
3. 等待最多 5 分钟，新接口将作为选项显示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

当您编辑 VLAN 接口时，您可以进行以下类型的更改：

- 更改 VLAN ID 或说明。
- 添加或删除父接口。

例如，如果您计划停用关联的节点，您可能希望从 VLAN 接口中删除父接口。

请注意以下事项：

- 如果 VLAN 接口用于 HA 组，则无法更改 VLAN ID。
- 如果父接口用于 HA 组，则无法删除该父接口。

  例如，假设 VLAN 200 连接到节点 A 和 B 上的父接口。如果 HA 组使用节点 A 的 VLAN 200 接口和节点 B 的 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 正在使用的父接口。

步骤

1. 选择*配置* > 网络 > **VLAN**接口。
2. 选中要编辑的 VLAN 接口的复选框。然后，选择 操作 > 编辑。
3. （可选）更新 VLAN ID 或说明。然后，选择*继续*。

   如果 VLAN 用于 HA 组，则无法更新 VLAN ID。

4. （可选）选中或清除复选框以添加父接口或删除未使用的接口。然后，选择 **Continue**。
5. 查看配置并进行任何更改。
6. 选择 **Save**。

删除 **VLAN** 接口

您可以删除一个或多个 VLAN 接口。

如果 VLAN 接口当前在 HA 组中使用，则无法删除该接口。必须先从 HA 组中删除 VLAN 接口，然后才能将其删除。

为避免客户流量中断，请考虑采取以下措施之一：

- 请先在 HA 组中添加一个新 VLAN 接口，然后再删除此 VLAN 接口。
- 创建不使用此 VLAN 接口的新 HA 组。
- 如果要删除的 VLAN 接口当前是活动接口，请编辑 HA 组。将要删除的 VLAN 接口移动到优先级列表的底部。等待在新的主接口上建立通信，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 接口的复选框。然后，选择 **Actions** > **Delete**。
3. 选择*是*以确认您的选择。

您选择的所有 VLAN 接口均已删除。VLAN 接口页面上将显示绿色成功横幅。

${post_edited_translations.segment}

作为网格管理员，如果您希望使用管理 API 从其他域访问 StorageGRID 中的数据，则可以为向 StorageGRID 发出的管理 API 请求启用跨源资源共享 (CORS)。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- "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 应用程序访问另一个不同域中的资源。例如，假设您要在域 `http://www.example.com` 中为 StorageGRID 构建一个监控仪表板。通过在 StorageGRID 中为 `http://www.example.com` 和 "Grid Manager" 启用 CORS，StorageGRID 域将响应来自 `http://www.example.com` 的 Grid Management API 请求。

带有 `application/json`的管理 API (mgmt-api) 请求或针对 `Content-Type`的 `multipart/formdata`请求支持 CORS。

步骤

1. 在 Grid Manager 中，转到 **CONFIGURATION** > **Network** > **Management interface CORS settings**。
2. 选择 **Grid Manager**、**Tenant Manager** 或这两个选项。
   - **Grid Manager**：为跨域 Grid Management API 请求启用 CORS。
   - ${post_edited_translations.segment}
3. 在 **Domains** 字段中输入其他域的 URL。

   如果要在 StorageGRID 中为多个域启用 CORS，请选择*添加其他域*。
4. 选择 **Save**。

相关信息

"${post_edited_translations.segment}"

${post_edited_translations.segment}

StorageGRID 中的流量分类策略

流量分类策略允许您识别和监控不同类型的网络流量。这些策略可以帮助限制和监控流量，以提高服务质量 (QoS)。

流量分类策略将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,以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
- Tenant（租户）
- 负载平衡器端点

StorageGRID 根据规则的目标监控与策略内任何规则匹配的流量。与策略的任何规则匹配的任何流量都由该策略处理。相反，您可以设置规则以匹配除指定实体之外的所有流量。

流量限制

您可以选择将以下限制类型添加到策略中：

- 聚合带宽
- 按请求带宽
- 并发请求
- 请求速率

限制值按每个负载均衡器强制执行。如果流量同时分布在多个负载均衡器上，则最大总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 不能同时限制两种类型的带宽。聚合带宽限制可能会对非限制流量造成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 减速响应。

在 Grid Manager 中，您可以查看流量图表并验证策略是否正在执行您预期的流量限制。

将流量分类策略与 **SLA** 结合使用

您可以将流量分类策略与容量限制和数据保护结合使用，以强制执行提供容量、数据保护和性能细节的服务级别协议 (SLA)。

以下示例显示了 SLA 的三个层次。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	允许的最大性能	成本
黄金	允许 1 PB 存储空间	3 副本 ILM 规则	25 K 次请求/秒 5 GB/sec（40 Gbps）带宽	每月 $$$ 元
银牌	允许使用 250 TB 存储空间	2 副本 ILM 规则	10 K 次请求/秒 1.25 GB/秒（10 Gbps）带宽	每月 $$ 元

服务级别层	容量	数据保护	允许的最大性能	成本
青铜	允许 100 TB 的存储空间	2 副本 ILM 规则	5 K 次请求/秒 1 GB/sec（8 Gbps）带宽	每月 $

创建 **StorageGRID** 流量分类策略

如果要监视，并可选择按存储桶、存储桶正则表达式、CIDR、负载平衡器端点或租户限制网络流量，可以创建流量分类策略。也可以根据带宽、并发请求数或请求速率为策略设置限制。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。
- 您已创建要匹配的任何负载均衡器端点。
- 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 **Create**。
3. 输入策略的名称和说明（可选），然后选择*继续*。

   例如，请说明此流量分类策略的适用范围和限制范围。

4. 选择*添加规则*并指定下列详细信息以创建策略的一个或多个匹配规则。您创建的任何策略都应至少有一个匹配规则。选择*继续*。

字段	问题描述
类型	选择匹配规则适用的流量类型。流量类型为存储桶、存储桶正则表达式、CIDR、负载平衡器端点和租户。

字段	问题描述
匹配值	输入与选定类型匹配的值。 • 存储桶：输入一个或多个存储桶名称。 • 存储桶正则表达式：输入一个或多个用于匹配一组存储桶名称的正则表达式。 正则表达式未锚定。使用 ^ 锚点来匹配存储桶名称的开头，并使用 $ 锚点来匹配名称的结尾。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：选择一个端点名称。这些是您在 "配置负载平衡器端点" 上定义的负载平衡器端点。 • 租户：租户匹配使用访问密钥 ID。如果请求不包含访问密钥 ID（例如，匿名访问），则访问的存储桶的所有权将用于确定租户。
反向匹配	如果要匹配除与刚才定义的类型和匹配值一致的流量之外的所有网络流量，请选中*反向匹配*复选框。否则，请将复选框留空。 例如，如果希望此策略应用于除一个以外的所有负载平衡器端点，请指定要排除的负载平衡器端点，然后选择*Inverse match*。 对于包含多个匹配程序的策略，其中至少有一个是反向匹配程序，请注意不要创建匹配所有请求的策略。

5. （可选）选择 **Add a limit** 并选择以下详细信息，以添加一个或多个限制来控制与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，以便了解流量趋势。

字段	问题描述
类型	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，当使用每个请求带宽时，聚合带宽不可用。聚合带宽限制可能会对非限制流量造成额外的轻微性能影响。 对于带宽限制，StorageGRID 应用与限制集类型最匹配的策略。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不受限制，即使存在与具有带宽限制的其他策略匹配的流量。StorageGRID 按以下顺序实现带宽限制的"最佳"匹配： • 确切的 IP 地址（/32 掩码） • 确切的存储桶名称 • 存储桶正则表达式 • Tenant（租户） • 端点 • 非精确 CIDR 匹配（not /32） • 反向匹配
适用于	此限制是否适用于客户端读取请求（GET 或 HEAD）或写入请求（PUT、POST 或 DELETE）。
值	将根据您选择的单位限制网络流量的值。例如，输入 10 并选择 MiB/s，以防止此规则匹配的网络流量超过 10 MiB/s。 注意：根据单位设置，可用单位将为二进制（例如 GiB）或十进制（例如 GB）。要更改单位设置，请选择 Grid Manager 右上角的用户下拉菜单，然后选择*用户首选项*。
单位	描述您输入的值的单位。

例如，如果要为 SLA 层创建 4 GB/s 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 **Continue**。
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。对该策略感到满意后，选择*保存并继续*。

   S3 客户端流量现在根据流量分类策略进行处理。

完成后

"查看网络流量指标" 以验证这些策略是否正在执行您预期的流量限制。

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描述，或者为策略创建、编辑或删除任何规则或限制。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

步骤

1. 选择*配置* > 网络 > 流量分类。

   ${post_edited_translations.segment}

2. 使用“操作”菜单或详情页面编辑策略。有关要输入的内容，请参见 "${post_edited_translations.segment}"。

   ${post_edited_translations.segment}

   a. 选中此策略的复选框。

   b. ${post_edited_translations.segment}

   详细信息页面

   a. ${post_edited_translations.segment}

   b. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

   您对策略所做的更改已保存，现在将根据流量分类策略处理网络流量。您可以查看流量图表，并验证策略是否正在执行您预期的流量限制。

删除 StorageGRID 流量分类策略

如果您不再需要流量分类策略，可以将其删除。请确保删除了正确的策略，因为策略一旦删除便无法恢复。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

步骤

1. 选择*配置* > 网络 > 流量分类。

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}

${post_edited_translations.segment}

a. 选中此策略的复选框。

b. 选择*操作* > 删除。

策略详情页面

a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

${post_edited_translations.segment}

在 **StorageGRID** 中查看网络流量指标

您可以通过查看"流量分类策略"页面中提供的图表来监控网络流量。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "Root 访问权限或租户帐户权限"。

关于此任务

对于任何现有的流量分类策略，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了网络上的流量。图表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，这些图表可提供有用的信息，帮助您了解流量趋势。

步骤

1. 选择*配置* > 网络 > 流量分类。

${post_edited_translations.segment}

2. ${post_edited_translations.segment}
3. 选择*Metrics*选项卡。

此时将显示流量分类策略图形。图表仅显示与选定策略匹配的流量的指标。

以下图表包含在页面上。

- 请求速率：此图表提供所有负载均衡器处理的与此策略匹配的带宽量。接收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。已发送包括所有请求的响应标头，以及在响应中包含正文数据的请求的响应正文数据大小。

> 当请求完成时，此图表仅显示带宽使用情况。对于慢速或大型对象请求，实际瞬时带宽可能与此图表中报告的值有所不同。

- 错误响应率：此图表提供了匹配此策略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（非错误）：此图表提供了与此策略匹配的成功请求的平均持续时间。
- 策略带宽使用情况：此图表提供了所有负载均衡器处理的与此策略匹配的带宽量。接收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。已发送包括所有请求的响应标头，以及在响应中包含正文数据的请求的响应正文数据大小。

4. ${post_edited_translations.segment}
5. 选择指标标题正下方的 **Grafana dashboard** 以查看策略的所有图表。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：
   - 按对象大小的写入请求率：与此策略匹配的 PUT/POST/DELETE 请求的速率。定位在单个单元格上可显示每秒速率。悬停视图中显示的速率被截断为整数计数，当存储桶中存在非零请求时，可能会报告 0。
   - 按对象大小的读取请求率：与此策略匹配的 GET/HEAD 请求的速率。定位在单个单元格上可显示每秒速率。悬停视图中显示的速率被截断为整数计数，当存储桶中存在非零请求时，可能会报告 0。
6. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. 从页面左上角的菜单中选择策略。
   d. 将光标放在图形上可看到弹出窗口，其中显示样本的日期和时间、聚合到计数中的对象大小以及该时间段内每秒的请求数。

      流量分类策略通过其 ID 进行标识。策略 ID 列在流量分类策略页面上。

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

${post_edited_translations.segment}

支持的 **TLS** 版本

${post_edited_translations.segment}

已选择支持与外部系统配合使用的 TLS 密码，以确保与各种外部系统的兼容性。该列表大于支持与 S3 客户端应用程序配合使用的密码列表。要配置密码，请转至 **Configuration** > **Security** > **Security settings**，然后选择 **TLS and SSH policies**。

> 在 StorageGRID 中，TLS 配置选项（例如协议版本、密码、密钥交换算法和 MAC 算法）是不可配置的。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。配置因 HTTP 连接是活动还是空闲，或者有多个并发连接而异。

您可以确定以下类型的 HTTP 连接的性能优势：

- 空闲的 HTTP 连接
- 活动的HTTP连接
- 并发 HTTP 连接

保持空闲 **HTTP** 连接打开的优势

当客户端应用程序空闲时，保持 HTTP 连接打开，以允许后续事务处理。保持空闲 HTTP 连接最长打开 10 分钟。StorageGRID 可能会自动关闭已打开且空闲超过 10 分钟的 HTTP 连接。

开放和空闲的HTTP连接具有以下优势：

- 从 StorageGRID 系统确定必须执行 HTTP 事务的时间到 StorageGRID 系统可以执行事务的时间，减少了延迟

  减少延迟是主要优势，特别是在建立 TCP/IP 和 TLS 连接所需的时间方面。

- 通过使用先前执行的传输来启动 TCP/IP 慢启动算法，从而提高数据传输速率
- 中断客户端应用程序和 StorageGRID 系统之间连接的几类故障情况的即时通知

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长。

活动 **HTTP** 连接的优势

对于直接到存储节点的连接，即使 HTTP 连接连续执行事务，也应将活动 HTTP 连接的持续时间限制为最多 10 分钟。

确定连接应保持开放的最长持续时间，是连接持久性的优势与内部系统资源的理想分配之间的权衡。

对于到存储节点的客户端连接，限制活动 HTTP 连接具有以下优点：

- 实现整个 StorageGRID 系统的最佳负载平衡。

  随着时间的推移，随着负载平衡要求的变化，HTTP 连接可能不再是最佳连接。当客户端应用程序为每个事务建立单独的 HTTP 连接时，系统会执行最佳负载平衡，但此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。
- 允许启动维护程序。

  某些维护过程仅在所有正在进行的 HTTP 连接完成后才开始。

对于与负载平衡器服务的客户端连接，限制打开连接的持续时间对于允许某些维护过程及时启动非常有用。如果客户端连接的持续时间不受限制，则活动连接可能需要几分钟才能自动终止。

并发 **HTTP** 连接的优势

您应该保持与 StorageGRID 系统的多个 TCP/IP 连接处于打开状态，以实现并行性，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：

- 减少延迟

  事务可以立即开始，而无需等待其他事务完成。

- 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的连接。

每个 StorageGRID 系统的拓扑对于并发事务和连接具有不同的峰值吞吐量。峰值吞吐量取决于计算、网络、存储资源、WAN 链路以及 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，每个软件实体都建立到 StorageGRID 系统的连接，则将所有实体之间的连接数相加。在以下情况下，您可能需要调整最大并发连接数：

- StorageGRID 系统的拓扑结构影响系统可以支持的并发事务和连接的最大数量。
- 通过带宽有限的网络与 StorageGRID 系统交互的客户端应用程序可能必须降低并发程度，以确保在合理的时间内完成单个事务。
- 当许多客户端应用程序共享 StorageGRID 系统时，您可能必须降低并发程度，以避免超出系统的限制。

用于读取和写入操作的 **HTTP** 连接池分离

您可以使用单独的 HTTP 连接池进行读取和写入操作，并控制每个连接池的使用量。单独的 HTTP 连接池可让您更好地控制事务和平衡负载。

客户端应用程序可以创建检索主导（读取）或存储主导（写入）的负载。通过为读取和写入事务使用单独的 HTTP 连接池，您可以调整每个池专用于读取或写入事务的比例。

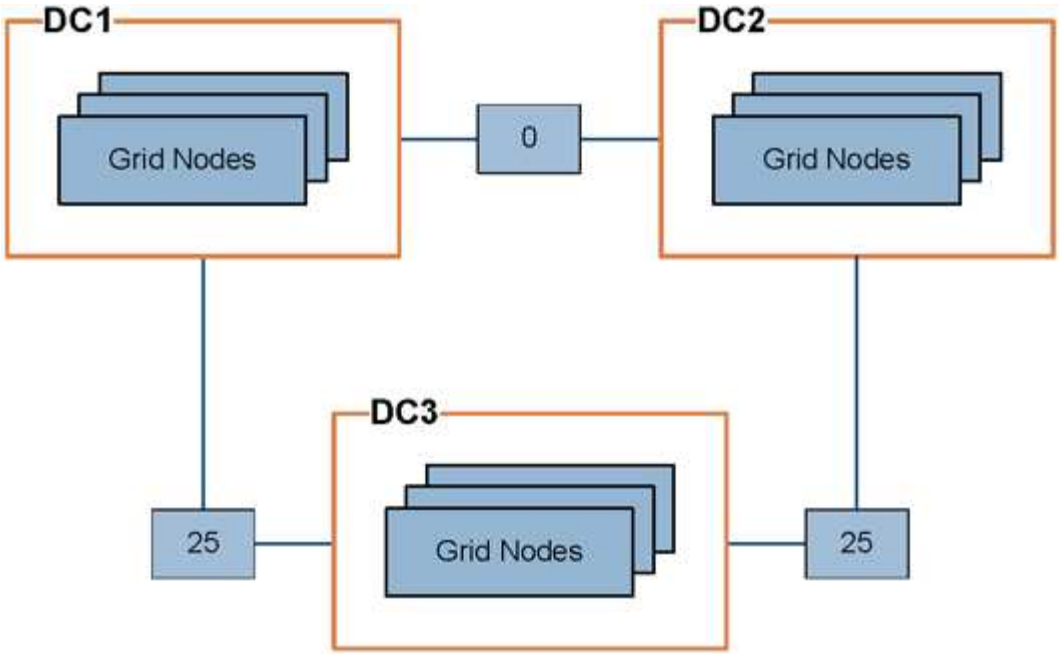
在 StorageGRID 中管理链路成本

链接成本允许您在存在两个或多个数据中心站点时优先考虑哪个数据中心站点提供所请求的服务。您可以调整链接成本以反映站点之间的延迟。

什么是链路开销？

- 链接成本用于优先考虑使用哪个对象副本来完成对象检索。
- 链接成本由 Grid Management API 和 Tenant Management API 用于确定要使用的内部 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"。

该图显示了在站点之间配置链接成本的三个站点网格：



- 管理节点和网关节点上的负载平衡器服务将客户端连接均匀分布到同一数据中心站点上的所有存储节点以及链路开销为 0 的任何数据中心站点。

  在本示例中，数据中心站点 1 (DC1) 的网关节点将客户端连接均匀分布到 DC1 的存储节点和 DC2 的存储节点。DC3 的网关节点仅将客户端连接发送到 DC3 的存储节点。

- 当检索作为多个复制副本存在的对象时，StorageGRID 会检索链路成本最低的数据中心的副本。

  在该示例中，如果 DC2 处的客户端应用程序检索存储在 DC1 和 DC3 处的对象，则将从 DC1 检索该对象，因为从 DC1 到 DC2 的链路开销为 0，低于从 DC3 到 DC2 的链路开销 (25)。

链路成本是任意相对数，没有特定的计量单位。例如，链路成本 50 不如链路成本 25 优先使用。下表显示了常用的链路成本。

链路	链路成本	说明
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	位于同一物理建筑物或园区内、通过 LAN 连接的逻辑数据中心。

更新链接费用

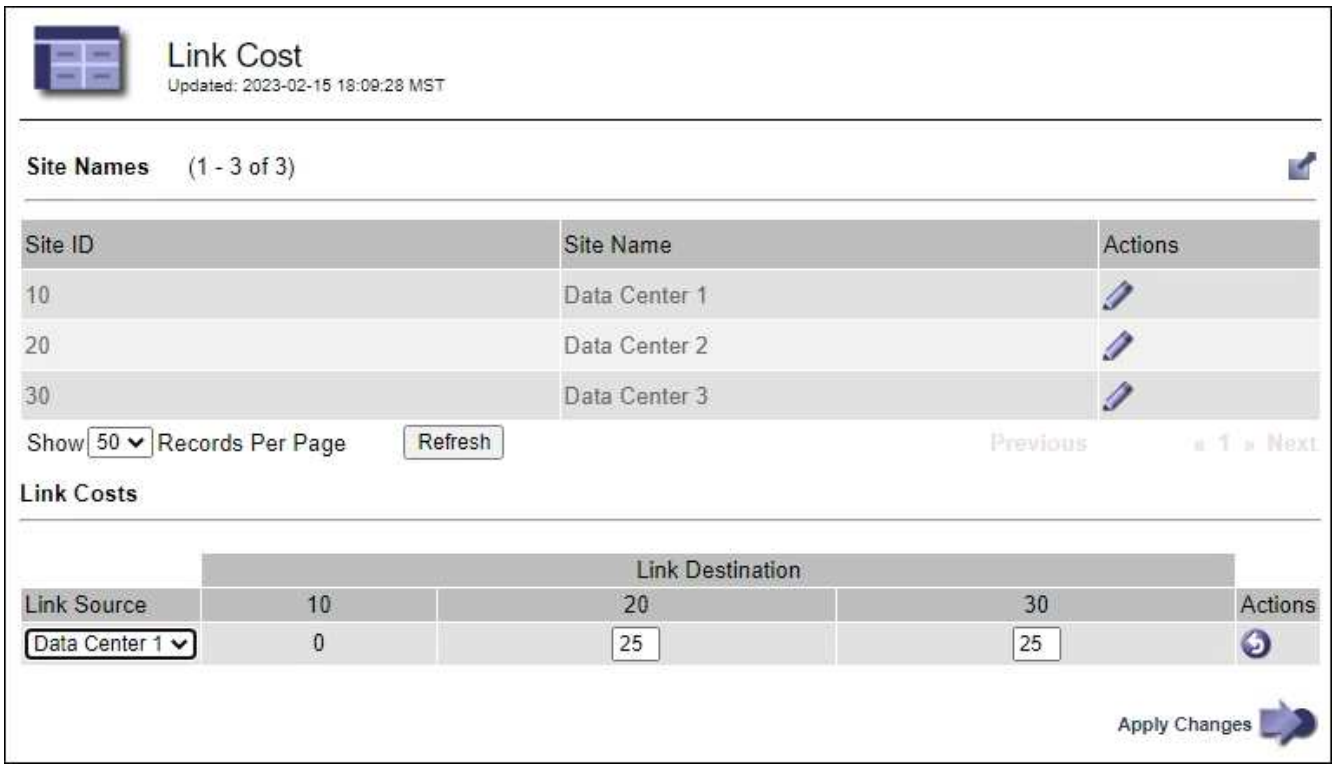
您可以更新数据中心站点之间的链接成本，以反映站点之间的延迟。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "其他网格配置权限"。

步骤

1. 选择*支持* > 其他 > 链接费用。



2. 在*链接源*下选择一个站点，并在*链接目的地*下输入一个介于 0 到 100 之间的成本值。

   如果来源与目的地相同，则无法更改链接成本。

   要取消更改，请选择 **Revert**。

3. 选择*应用更改*。

使用 AutoSupport

了解 StorageGRID 中的 AutoSupport

AutoSupport 功能使 StorageGRID 能够将运行状况和状态包发送给 NetApp 技术支持。

使用 AutoSupport 有助于更快地解决问题。技术支持可以监控系统的存储需求，并帮助确定是否需要添加新节点或站点。（可选）AutoSupport 可以将软件包发送到一个额外的目标位置。

StorageGRID 有两种类型的 AutoSupport：

- **StorageGRID AutoSupport** 报告 StorageGRID 软件问题。首次安装 StorageGRID 时默认启用。如有需要，您可以 "更改默认 AutoSupport 配置"。

> 如果未启用 StorageGRID AutoSupport，Grid Manager 仪表板上将显示一条消息。该消息包含指向 AutoSupport 配置页面的链接。如果关闭此消息，则在浏览器缓存被清除之前，它不会再次显示，即使 AutoSupport 仍处于禁用状态。

- 设备硬件 **AutoSupport** 报告 StorageGRID 设备问题。您必须 "在每台设备上配置硬件 AutoSupport"。

什么是 **Active IQ**?

Active IQ 是一款基于云的数字顾问，利用来自 NetApp 安装基础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预防问题，从而改善系统健康状况并提高系统可用性。

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

"Active IQ Digital Advisor 文档"

AutoSupport 软件包中包含的信息

AutoSupport 包中包含以下文件和详细信息。

文件名	字段	问题描述
AUTOSUPPORT-HISTORY.XML	AutoSupport 序列号 + 此 AutoSupport 的目的地 + 交付状态 + 交付尝试次数 + AutoSupport 主题 + 交付 URI + 上次错误 + AutoSupport PUT 文件名 + 生成时间 + Autosupport 压缩大小 + Autosupport 解密大小 + 总收集时间 (ms)	AutoSupport 历史文件。
AUTOSUPPORT.XML	节点 + 联系支持所使用的协议 + HTTP/HTTPS 的支持 URL + 支持地址 + AutoSupport OnDemand 状态 + AutoSupport OnDemand 服务器 URL + AutoSupport OnDemand 轮询间隔	AutoSupport 状态文件。提供所用协议、技术支持 URL 和地址、轮询间隔以及 OnDemand AutoSupport 是否启用或禁用的详细信息。
BUCKETS.XML	存储桶 ID + 帐户 ID + 生成版本 + 位置约束配置 + 合规性已启用 + 合规性配置 + S3 对象锁定已启用 + S3 对象锁定配置 + 一致性配置 + CORS 已启用 + CORS 配置 + 上次访问时间已启用 + 策略已启用 + 策略配置 + 通知已启用 + 通知配置 + 云镜像已启用 + 云镜像配置 + 搜索已启用 + 搜索配置 + 存储桶标记已启用 + 存储桶标记配置 + 版本控制配置	提供存储桶级别的配置详细信息和统计信息。存储桶配置的示例包括平台服务、合规性和存储桶一致性。

文件名	字段	问题描述
${post_edited_translations.segment}	${post_edited_translations.segment}	网格范围的配置信息文件。包含有关网格证书、元数据保留空间、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）、擦除编码配置文件详细信息、DNS 名称和 "NMS 名称" 的信息。
GRID-SPEC.XML	网格规范，原始 XML	用于配置和部署 StorageGRID。包含网格规格、NTP 服务器 IP、DNS 服务器 IP、网络拓扑和节点的硬件配置文件。
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（维护程序）状态文件。提供网格的活动、终止、完成、失败和挂起任务的详细信息。
GRID.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-CONFIGURATION.XML	${post_edited_translations.segment}	ILM 配置的属性列表。
ILM-STATUS.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 评估率和网格范围的指标。
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、接收行为、筛选器、规则和描述。
${post_edited_translations.segment}	不适用	可下载的日志文件。包含 `bycast-err.log`和 `servermanager.log`来自每个节点。
MANIFEST.XML	收集顺序 + 此数据的 AutoSupport 内容文件名 + 此数据项的描述 + 收集的字节数 + 收集时间 + 此数据项的状态 + 错误描述 + 此数据的 AutoSupport 内容类型	包含 AutoSupport 元数据和所有 AutoSupport 文件的简要说明。
NMS-ENTITIES.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	对 "NMS树" 中的组和服务实体进行分组。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。

文件名	字段	问题描述
OBJECTS-STATUS.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、总传输数、删除速率、损坏的片段、丢失的对象、缺失的对象、尝试修复、扫描速率、估计扫描周期和修复完成状态。
SERVER-STATUS.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、安装的内存、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-STATUS.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。包含已分配的表空间、可用表空间、数据库的 Reaper 指标、段修复持续时间、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-GRADES.XML	存储等级 ID + 存储等级名称 + 存储节点 ID + 存储节点路径	每个存储节点的存储等级定义文件。
SUMMARY-ATTRIBUTES.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 + 静默 + 其他注释 + 其他标签	指示 StorageGRID 系统中潜在问题的当前系统警报。
USERAGENTS.XML	用户代理 + 天数 + HTTP 请求总数 + 摄取的总字节数 + 检索到的总字节数 + PUT 请求 + GET 请求 + DELETE 请求 + HEAD 请求 + POST 请求 + OPTIONS 请求 + 平均请求时间 (ms) + 平均 PUT 请求时间 (ms) + 平均 GET 请求时间 (ms) + 平均 DELETE 请求时间 (ms) + 平均 HEAD 请求时间 (ms) + 平均 POST 请求时间 (ms) + 平均 OPTIONS 请求时间 (ms)	基于应用程序用户代理的统计信息。例如，每个用户代理的 PUT/GET/DELETE/HEAD 操作数和每个操作的总字节数。

文件名	字段	问题描述
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	AutoSupport 标头数据。

在 StorageGRID 中配置 AutoSupport

默认情况下，首次安装 StorageGRID 时会启用 StorageGRID AutoSupport 功能。但是，您必须在每个应用上配置硬件 AutoSupport。您可以根据需要更改 AutoSupport 配置。

如果您要更改 StorageGRID AutoSupport 的配置，请仅在主管理节点上进行更改。您必须在每个应用装置上 配置硬件 AutoSupport。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。
- 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，您需要 "${post_edited_translations.segment}" 将 AutoSupport 包作为 HTTPS 转发。NetApp 的 AutoSupport 服务器将拒绝使用 HTTP 发送的包。
- 如果您要将 SMTP 用作 AutoSupport 包的协议，则您已配置了 SMTP 邮件服务器。

关于此任务

您可以使用以下选项的任意组合向技术支持发送 AutoSupport 包：

- 每周：每周自动发送一次 AutoSupport 包。默认设置：已启用。
- 事件触发：每小时或在发生重大系统事件时自动发送 AutoSupport 包。默认设置：已启用。
- **On Demand**：允许技术支持请求您的 StorageGRID 系统自动发送 AutoSupport 包，这在他们主动解决问题时非常有用（需要 HTTPS AutoSupport 传输协议）。默认设置：已禁用。
- 用户触发：随时手动发送 AutoSupport 包。
- 日志收集："手动收集日志文件和系统数据并发送 AutoSupport 包"。

指定 AutoSupport 包的协议

您可以使用以下任一协议发送 AutoSupport 包：

- **HTTPS**：这是新安装的默认和推荐设置。此协议使用端口 443。如果需要启用 AutoSupport 按需功能，必须使用 HTTPS。
- **HTTP**：如果选择 HTTP，则必须配置代理服务器以将 AutoSupport 包作为 HTTPS 进行转发。NetApp 的 AutoSupport 服务器会拒绝使用 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。

您设置的协议用于发送所有类型的 AutoSupport 包。

步骤

1. 选择 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 选择要用于发送 AutoSupport 软件包的协议。
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 包的传输是安全的。NetApp 支持证书已随 StorageGRID 软件一起安装。
   - 不验证证书：仅当您有充分理由不使用证书验证时（例如证书出现临时问题时），才选择此选项。
4. 选择 * 保存 *。所有每周、用户触发和事件触发的包都会使用所选协议进行发送。

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。

要确定发送每周 AutoSupport 软件包的时间，请转到 **AutoSupport** > 结果 选项卡。在 每周 **AutoSupport** 部分，查看 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 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 清除*启用每周 AutoSupport* 复选框。
3. 选择 **Save**。

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个 AutoSupport 包。

您可以随时禁用事件触发的 AutoSupport。

步骤

1. 选择 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 清除*启用事件触发 AutoSupport* 复选框。
3. 选择 **Save**。

启用按需 **AutoSupport**

AutoSupport on Demand可以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，技术支持人员可以请求您的 StorageGRID 系统自动发送 AutoSupport 软件包。技术支持人员还可以为 AutoSupport on Demand 查询设置轮询时间间隔。

技术支持无法启用或禁用按需 AutoSupport。

步骤

1. 选择 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 为协议选择 **HTTPS**。
3. 选中*启用每周 AutoSupport* 复选框。
4. 选中*启用 AutoSupport 按需*复选框。
5. 选择 **Save**。

   AutoSupport on Demand 已启用，并且技术支持可以向 StorageGRID 发送 AutoSupport on Demand 请求。

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。如果有 StorageGRID 修补程序或新版本可用，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，如果您的系统没有 WAN 访问权限，则应禁用检查以避免下载错误。

步骤

1. 选择 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 清除*检查软件更新*复选框。
3. 选择 **Save**。

添加其他 **AutoSupport** 目的地

启用 AutoSupport 后，健康和状态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 指定 AutoSupport 包的协议 中的说明。

> 您不能使用 SMTP 协议将 AutoSupport 包发送到其他目标。

步骤

1. 选择 **Support** > **Tools** > **AutoSupport** > **Settings**。
2. 选择*启用其他 AutoSupport 目的地*。
3. 指定以下内容：

   主机名称
   : 其他 AutoSupport 目标服务器的服务器主机名或 IP 地址。

     > 您只能输入一个其他目的地。

   端口
   : 用于连接到其他 AutoSupport 目标服务器的端口。默认值为 HTTP 的端口 80 或 HTTPS 的端口 443。

证书验证

是否使用 TLS 证书来保护与附加目标的连接。

- 选择*验证证书*以使用证书验证。
- 选择*不验证证书*以在不进行证书验证的情况下发送您的 AutoSupport 软件包。

  仅当您有充分理由不使用证书验证时，例如证书暂时出现问题时，才选择此选项。

4. 如果您选择了*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 **Save**。

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。

为设备配置 **AutoSupport**

AutoSupport for appliances 报告 StorageGRID 硬件问题，StorageGRID AutoSupport 报告 StorageGRID 软件问题，但有一个例外：对于 SGF6112，StorageGRID AutoSupport 报告硬件和软件问题。您必须在除 SGF6112 之外的每个设备上配置 AutoSupport，SGF6112 无需额外配置。AutoSupport 对于服务设备和存储设备的实现方式不同。

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 System Manager 中配置 AutoSupport"

如果您在 "SANtricity System Manager" 中配置通过代理传输 AutoSupport，则来自 E-Series 设备的 AutoSupport 包可以包含在 StorageGRID AutoSupport 中。

StorageGRID AutoSupport 不报告硬件问题，例如 DIMM 或主机接口卡 (HIC) 故障。但是，某些组件故障可能会触发"硬件警报"。对于带有基板管理控制器 (BMC) 的 StorageGRID 设备，您可以配置电子邮件和 SNMP 陷阱以报告硬件故障：

- "为 BMC 警报设置电子邮件通知"
- "配置 BMC 的 SNMP 设置"

相关信息

"NetApp 支持"

手动触发 **StorageGRID** 中的 **AutoSupport** 包

为了帮助技术支持解决 StorageGRID 系统的问题，您可以手动触发发送 AutoSupport 软件包。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您具有根访问权限或其他网格配置权限。

步骤

1. 选择*支持* > 工具 > **AutoSupport**。
2. 在*操作*选项卡上，选择*发送用户触发的 AutoSupport*。

   StorageGRID 尝试将 AutoSupport 包发送到 NetApp 支持站点。如果尝试成功，**Results** （结果）选项卡上的 **Most Recent Result** （最近结果）和 **Last Successful Time** （上次成功时间）值将更新。如果出现问题，**Most Recent Result** 值将更新为"Failed"，StorageGRID 不会再次尝试发送 AutoSupport 包。

3. 1 分钟后，请在浏览器中刷新 AutoSupport 页面以访问最新结果。

> 此外，您可以"收集更广泛的日志文件和系统数据"并将它们发送到 NetApp 支持站点。

对 StorageGRID AutoSupport 包进行故障排除

如果尝试发送 AutoSupport 软件包失败，StorageGRID 系统会根据 AutoSupport 软件包类型采取不同的操作。您可以通过选择 支持 > 工具 > **AutoSupport** > 结果 来检查 AutoSupport 软件包的状态。

当 AutoSupport 包发送失败时，**AutoSupport** 页面的 **Results** 选项卡上将显示 “Failed”。

> 如果您配置了代理服务器以将 AutoSupport 包转发到 NetApp，则应"验证代理服务器配置设置是否正确"。

每周 **AutoSupport** 软件包故障

如果每周 AutoSupport 软件包发送失败，StorageGRID 系统将采取以下操作：

1. 将"最新结果"属性更新为"重试"。
2. 尝试在一小时内每四分钟重新发送 AutoSupport 软件包 15 次。
3. 发送失败一小时后，将"最近结果"属性更新为"失败"。
4. 尝试在下一个计划时间再次发送 AutoSupport 软件包。
5. 如果由于 NMS 服务不可用而导致包发送失败，且在七天内发送了包，则保持常规 AutoSupport 计划。
6. 当 NMS 服务再次可用时，如果已有七天或更长时间未发送 AutoSupport 包，则会立即发送一个包。

用户触发或事件触发的 **AutoSupport** 包失败

如果用户触发或事件触发的 AutoSupport 包发送失败，StorageGRID 系统将采取以下操作：

1. 如果错误已知，则显示错误消息。例如，如果用户在未提供正确电子邮件配置设置的情况下选择了 SMTP 协议，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. ${post_edited_translations.segment}
3. 将错误记录在 `nms.log` 中。

如果发生故障且选择的协议是 SMTP，请验证 StorageGRID 系统的电子邮件服务器配置是否正确，并且您的电子邮件服务器正在运行（支持 > 警报（旧版） > 旧版电子邮件设置）。以下错误消息可能会显示在 AutoSupport 页面上： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

了解如何 "${post_edited_translations.segment}"。

修复 **AutoSupport** 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.`

通过 StorageGRID 发送 E-Series AutoSupport 包

您可以通过 StorageGRID 管理节点而非存储设备管理端口，将 E 系列 SANtricity System Manager AutoSupport 包发送到技术支持。

有关将 AutoSupport 与 E-Series 设备配合使用的详细信息，请参见 "E 系列硬件 AutoSupport"。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 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 System Manager 中配置 AutoSupport"

> 要使用 Grid Manager 访问 SANtricity System Manager，您必须拥有 SANtricity 固件 8.70 或更高版本。

关于此任务

E-Series 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 System Manager 中配置特殊的代理服务器地址，以通过 StorageGRID 管理节点传输 AutoSupport 包，而无需使用设备的管理端口。以这种方式传输的 AutoSupport 包由 "首选发件人管理节点" 发送，它们使用在 Grid Manager 中配置的任何 "管理员代理设置"。

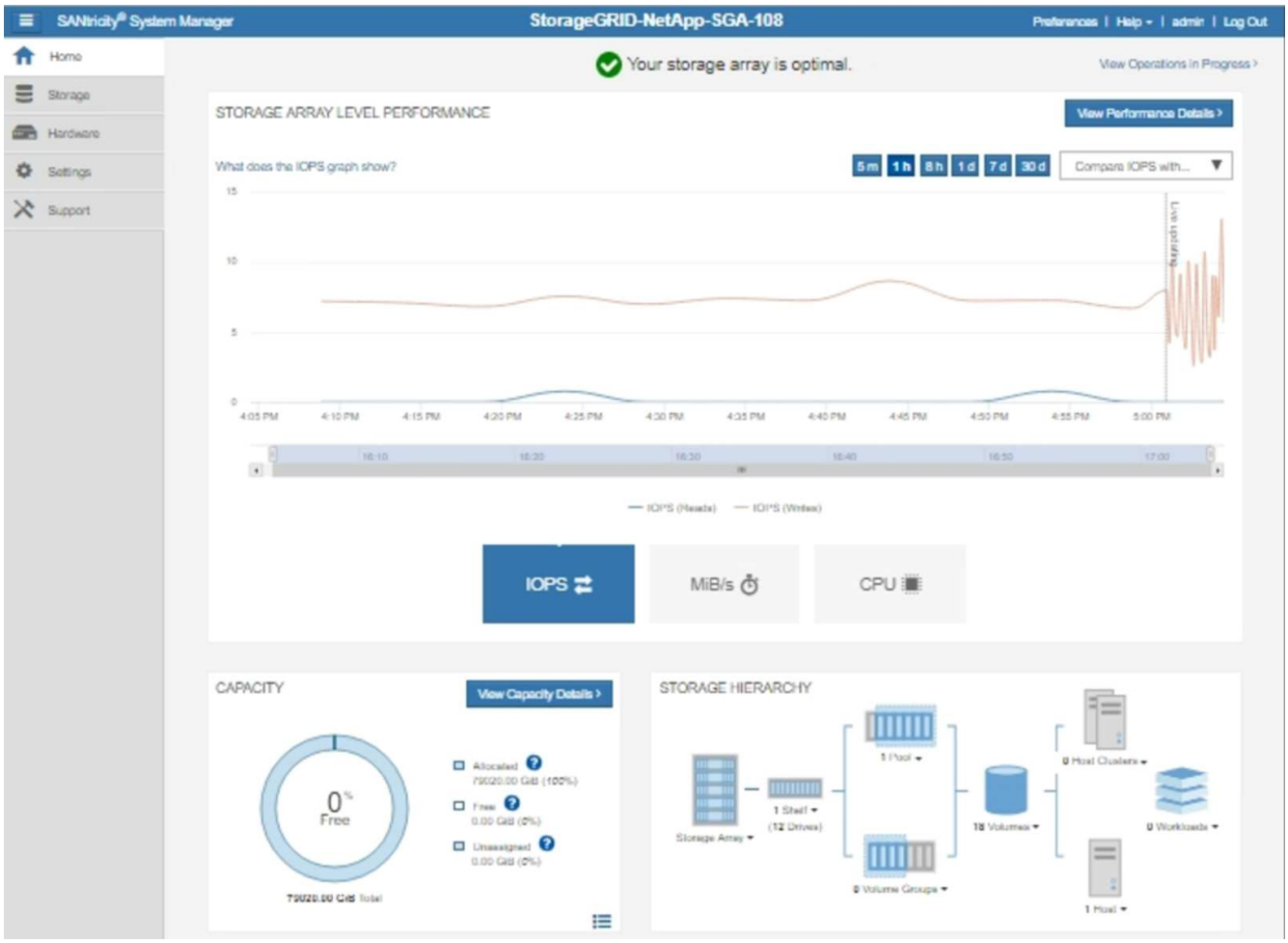
> 此过程仅适用于为 E 系列 AutoSupport 包配置 StorageGRID 代理服务器。有关 E 系列 AutoSupport 配置的其他详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

步骤

1. 在 Grid Manager 中，选择 **Nodes** 。
2. 从左侧的节点列表中，选择要配置的存储设备节点。

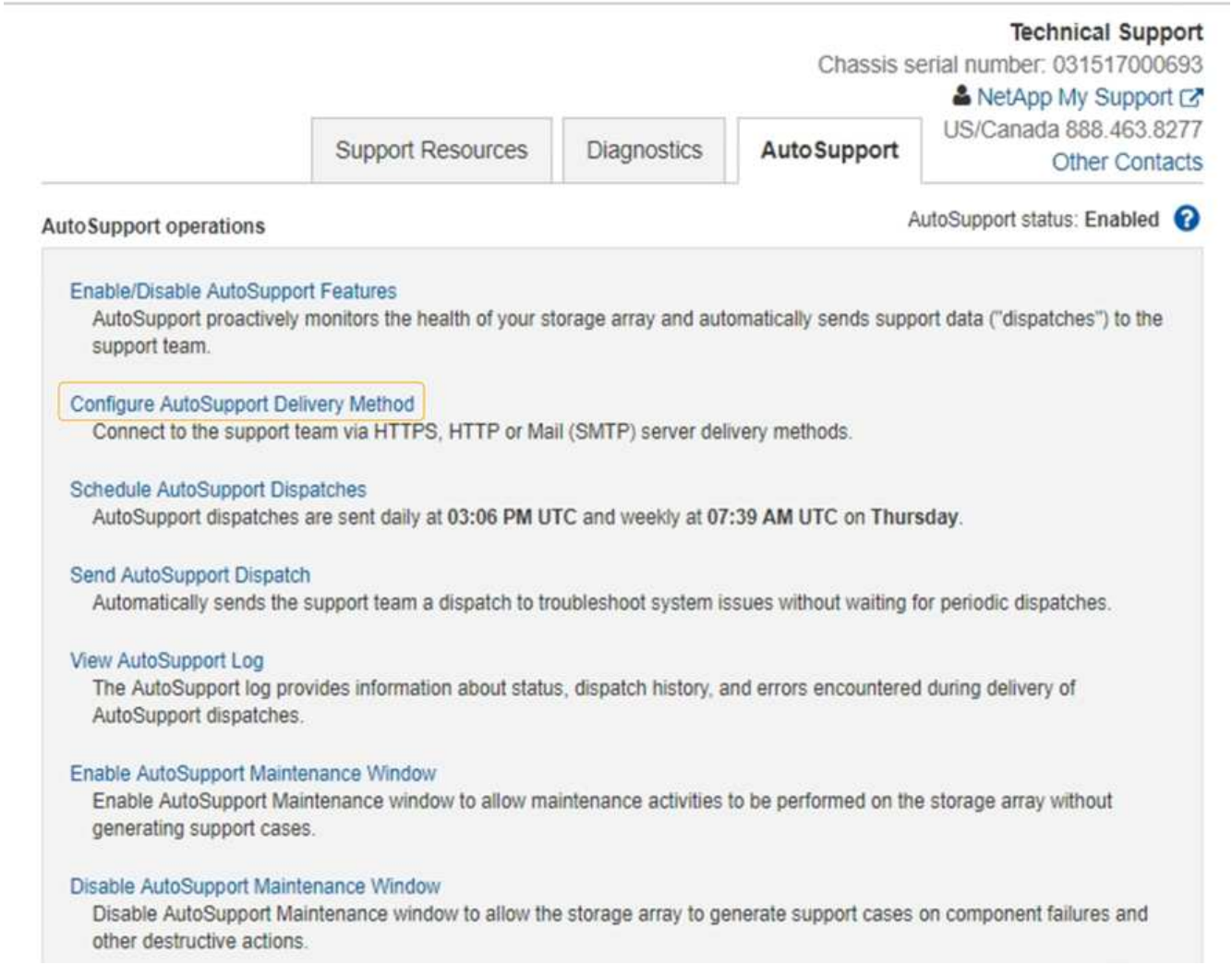
3. 选择 **SANtricity System Manager**。

   此时将显示 SANtricity System Manager 主页。



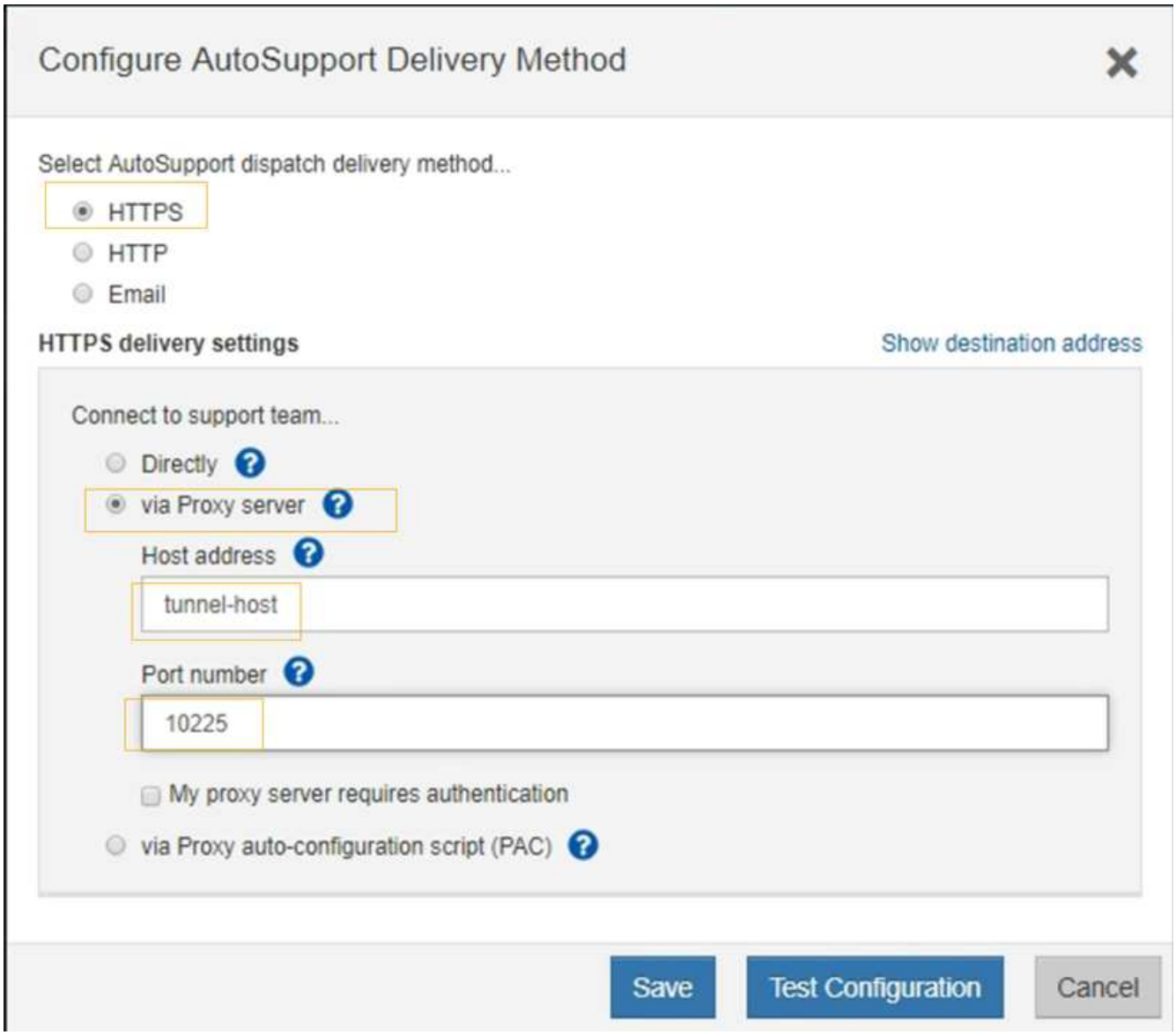
4. 选择*支持* > 支持中心 > **AutoSupport**。

   此时将显示 AutoSupport 操作页面。



5. 选择 配置 **AutoSupport** 交付方式。

   此时将显示 Configure AutoSupport Delivery Method 页面。



6. 选择 **HTTPS** 作为传送方式。

   已预安装启用 HTTPS 的证书。

7. 选择*via Proxy server*。
8. 在 主机地址 中输入 `tunnel-host`。

   `tunnel-host` 是使用管理节点发送 E-Series AutoSupport 包的专用地址。

9. 输入 `10225`作为*端口号*。

   `10225` 是 StorageGRID 代理服务器上的端口号，用于接收来自设备中 E-Series 控制器的 AutoSupport 包。

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，绿色横幅中会显示一条消息："您的 AutoSupport 配置已通过验证。"

    如果测试失败，红色横幅中会显示一条错误消息。请检查您的 StorageGRID DNS 设置和网络，确保 "首选

发件人管理节点" 可以连接到 NetApp 支持站点，然后再次尝试测试。

11. 选择 **Save**。

    此时会保存配置，并且会显示一条确认消息："AutoSupport delivery method has been configured。"

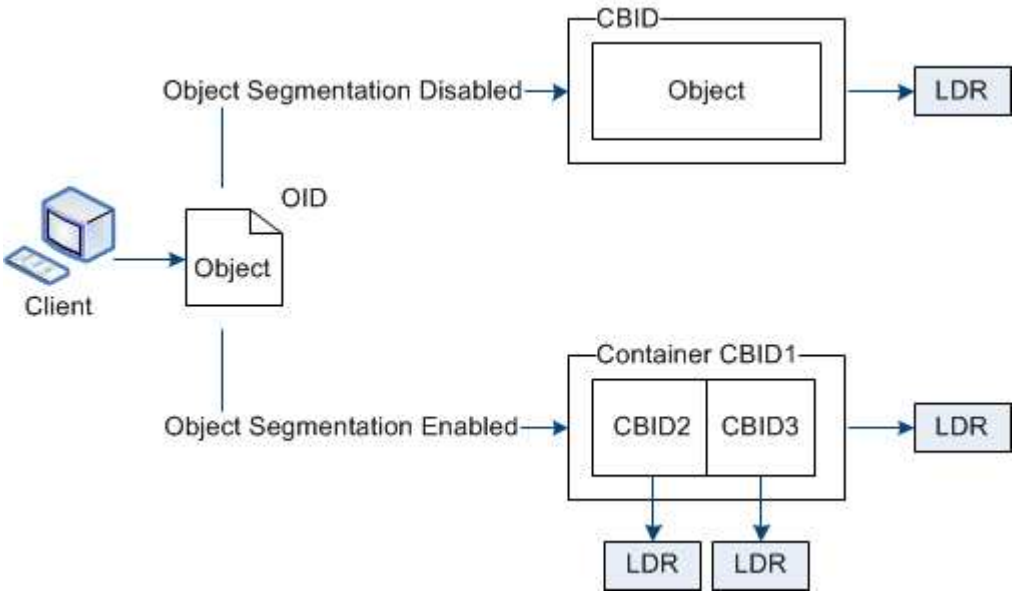
管理存储节点

使用存储选项

了解 StorageGRID 中的对象分段

对象分割是将对象拆分为较小的固定大小对象集合的过程，以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，其中一个对象表示每个部分。

当对象被摄入 StorageGRID 系统时，LDR 服务将对象拆分为段，并创建一个段容器，其中将所有段的标头信息列为内容。



在检索段容器时，LDR 服务从其段组装原始对象，并将此对象返回到客户端。

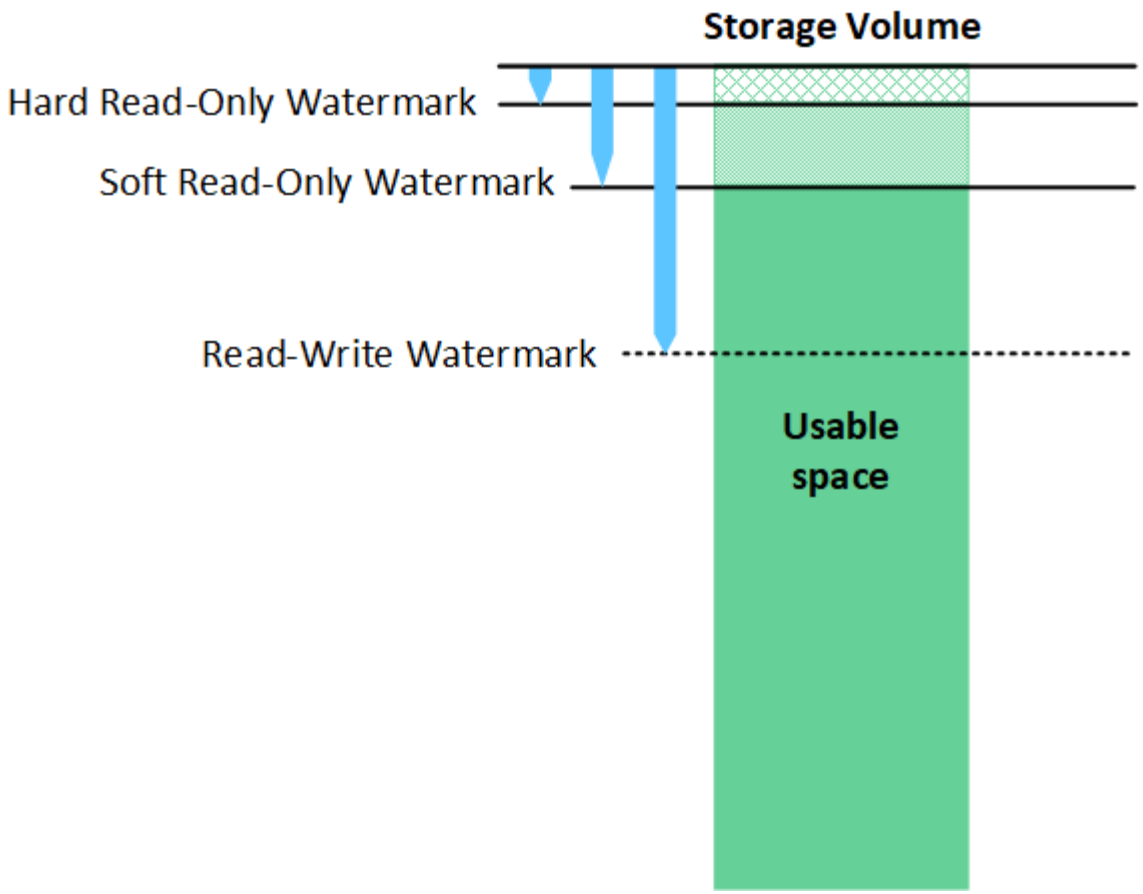
容器和段不一定存储在同一存储节点上。容器和段可以存储在 ILM 规则中指定的存储池内的任何存储节点上。

每个段都由 StorageGRID 系统独立处理，并有助于托管对象和存储对象等属性的计数。例如，如果存储到 StorageGRID 系统的对象被分为两个段，则托管对象的值在导入完成后会增加三个，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，以确保存储节点在空间严重不足之前安全地转换为只读状态，并允许已转换为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纠删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，请转到 "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*是表示存储节点用于对象数据的可用空间正在变满的第一个水印。

如果存储节点中的每个卷的可用空间少于该卷的软只读水印，则存储节点将转换为_只读模式_。只读模式意味着存储节点向 StorageGRID 系统的其余部分通告只读服务，但会完成所有挂起的写入请求。

例如，假设存储节点中的每个卷都有 10 GB 的软只读水印。一旦每个卷的可用空间少于 10 GB，存储节点就会转换为软只读模式。

什么是硬只读水印?

*存储卷硬只读水印*是下一个水印，用于指示节点用于对象数据的可用空间即将耗尽。

如果卷上的可用空间小于该卷的硬只读水印，则对卷的写入将失败。但是，可以继续写入其他卷，直到这些卷上的可用空间小于其硬只读水印。

例如，假设存储节点中的每个卷都有 5 GB 的硬只读水印。一旦每个卷的可用空间少于 5 GB，存储节点就不再接受任何写入请求。

硬只读水印始终小于软只读水印。

什么是读写水印?

*存储卷读写水印*仅适用于已过渡到只读模式的 Storage Nodes。它决定了节点何时可以再次变为读写状态。当 Storage Node 中任意一个存储卷上的可用空间大于该卷的读写水印时，该节点会自动过渡回读写状态。

例如，假设存储节点已转换为只读模式。另外，假设每个卷的读写水印为 30 GB。一旦任何卷的可用空间增加到 30 GB，节点就会再次变为读写模式。

读写水印始终大于软只读水印和硬只读水印。

查看存储卷水位标记

您可以查看当前的水印设置和系统优化的值。如果未使用优化的水印，您可以确定是否可以或应该调整设置。

开始之前

- 您已完成升级到 StorageGRID 11.6 或更高版本。
- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "root 访问权限"。

查看当前水印设置

您可以在网格管理器中查看当前的存储水印设置。

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。

     这是默认和推荐的设置。不要更新这些值。或者，您可以 查看优化的存储水印。
   - 如果未选中"使用优化值"复选框，则将使用自定义（非优化）水印。不建议使用自定义水印设置。请参阅"低只读水印覆盖警报故障排除"的说明，以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。

查看优化的存储水印

StorageGRID 使用两个 Prometheus 指标来显示它为存储卷软只读水印计算的优化值。您可以查看网格中每个存储节点的最小和最大优化值。

1. ${post_edited_translations.segment}
2. 在 Prometheus 部分，选择链接以访问 Prometheus 用户界面。
3. 要查看推荐的最小软只读水印，请输入以下 Prometheus 指标，然后选择 **Execute**：

   ```
   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 **Low read-only watermark override** 警报。

4. 要查看建议的最大软只读水印，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控制可以存储在该系统上的对象的最大数量。为了确保您的 StorageGRID 系统有足够的空间来存储新对象，您必须了解 StorageGRID 存储对象元数据的位置和方式。

什么是对象元数据?

对象元数据是描述对象的任何信息。StorageGRID 使用对象元数据来跟踪网格中所有对象的位置，并随时间管理每个对象的生命周期。

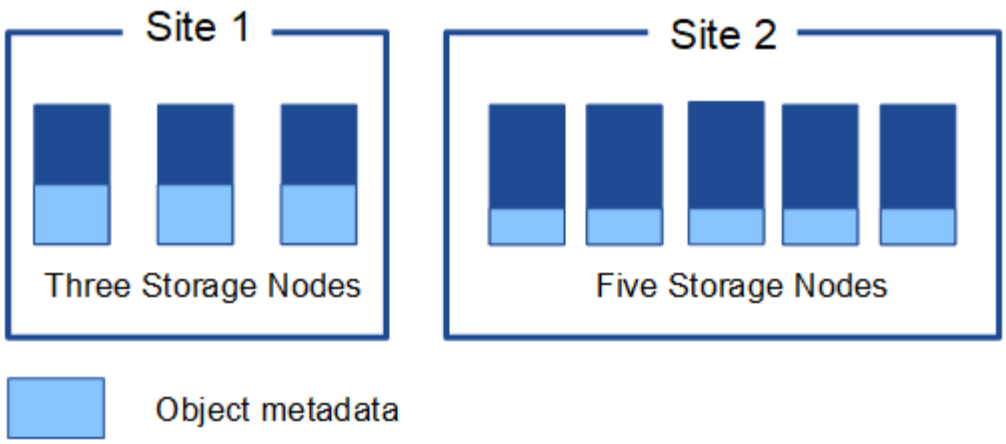
对于 StorageGRID 中的对象，对象元数据包含以下类型的信息：

- 系统元数据，包括每个对象的唯一 ID （UUID）、对象名称、S3 存储桶的名称、租户帐户名称或 ID、对象的逻辑大小、对象首次创建的日期和时间以及对象上次修改的日期和时间。
- 与对象关联的任何自定义用户元数据键值对。
- 对于 S3 对象，与对象关联的任何对象标记键值对。
- 对于复制的对象副本，每个副本的当前存储位置。
- 对于擦除编码的对象副本，每个片段的当前存储位置。
- 对于云存储池中的对象副本，对象的位置，包括外部存储桶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。

对象元数据是如何存储的?

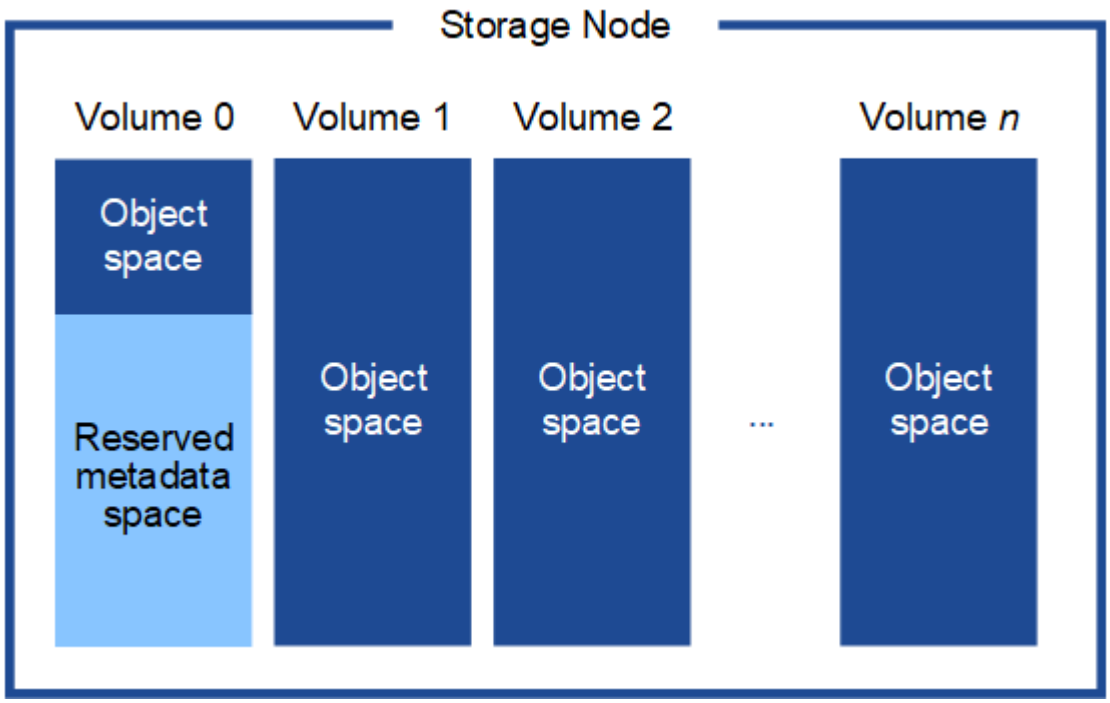
StorageGRID 将对象元数据维护在 Cassandra 数据库中，该数据库独立于对象数据存储。为了提供冗余并保护对象元数据免受丢失，StorageGRID 在每个站点为系统中的所有对象存储三个元数据副本。

此图表示两个站点的存储节点。每个站点具有相同数量的对象元数据，每个站点的元数据在该站点的所有存储节点之间进行细分。



对象元数据存储在哪里?

此图表示单个存储节点的存储卷。



如图所示，StorageGRID 在每个存储节点的存储卷 0 上为对象元数据预留空间。它使用预留空间来存储对象元数据并执行基本的数据库操作。存储卷 0 上的任何剩余空间以及存储节点中的所有其他存储卷均专用于对象数据（复制副本和纠删码片段）。

为特定存储节点上的对象元数据保留的空间量取决于以下几个因素。

元数据预留空间设置

_元数据保留空间_是一个系统范围的设置，表示将为每个存储节点的卷 0 上的元数据保留的空间量。如表所示，此设置的默认值基于：

- 您最初安装 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	默认元数据保留空间设置
11.5 至 12.0	网格中每个存储节点上 128 GB 或更多	8 TB (8,000 GB)
	网格中的任何存储节点上小于 128 GB	3 TB (3,000 GB)
11.1 至 11.4	任意一个站点的每个存储节点上 128 GB 或更多	4 TB (4,000 GB)
	每个站点上任何存储节点上的小于 128 GB	3 TB (3,000 GB)
11.0或更早版本	任意金额	2 TB (2,000 GB)

查看元数据保留空间设置

按照以下步骤查看 StorageGRID 系统的元数据保留空间设置。

步骤

1. 选择*配置* > 系统 > 存储设置。
2. 在存储设置页面上，展开*元数据保留空间*部分。

对于 StorageGRID 11.8 或更高版本，元数据保留空间值必须至少为 100 GB 且不超过 1 PB。

新 StorageGRID 11.6 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 8,000 GB（8 TB）。

元数据的实际预留空间

与系统范围的元数据保留空间设置不同，对象元数据的_实际保留空间_是为每个存储节点单独确定的。对于任何给定的存储节点，元数据的实际保留空间取决于该节点的卷 0 的大小以及系统范围的元数据保留空间设置。

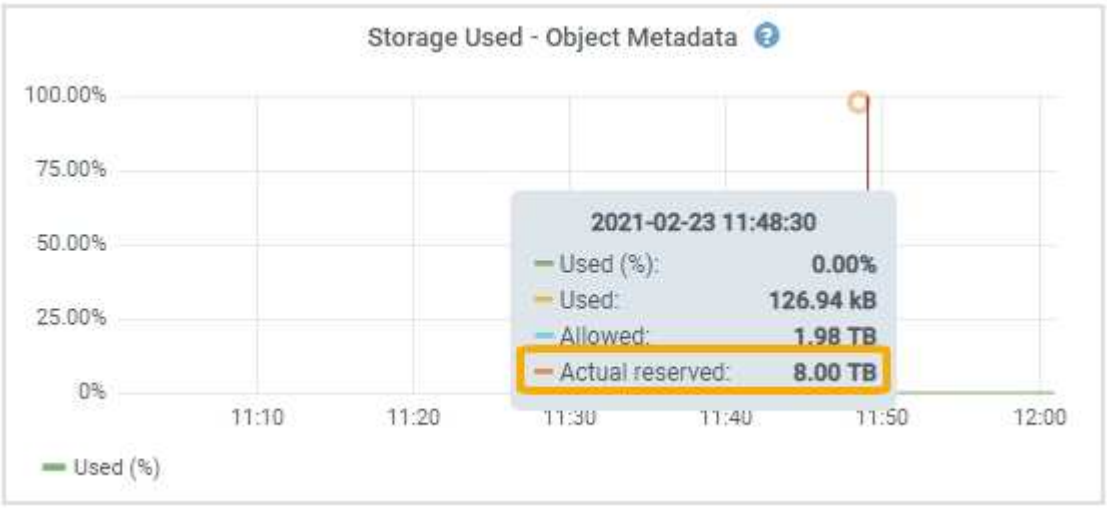
此节点的卷 **0** 的大小	元数据的实际预留空间
不到 500 GB（非生产用）	卷 0 的 10%
500 GB 或更多 + 或 + 仅元数据 Storage Nodes	以下值中较小的值： • 卷 0 • 元数据预留空间设置 注意：仅元数据存储节点仅需要一个 rangedb。

查看元数据的实际预留空间

按照下面的步骤查看特定存储节点上元数据的实际保留空间。

步骤

1. 从网格管理器中，选择*节点* > 存储节点。
2. 选择 **Storage** 选项卡。
3. 将光标放在"已用存储 - 对象元数据"图表上，并找到*实际保留*值。



在屏幕截图中，*实际保留*值为 8 TB。此屏幕截图适用于新 StorageGRID 11.6 安装中的大型存储节点。由于此存储节点的系统范围元数据保留空间设置小于卷 0，因此此节点的实际保留空间等于元数据保留空间设置。

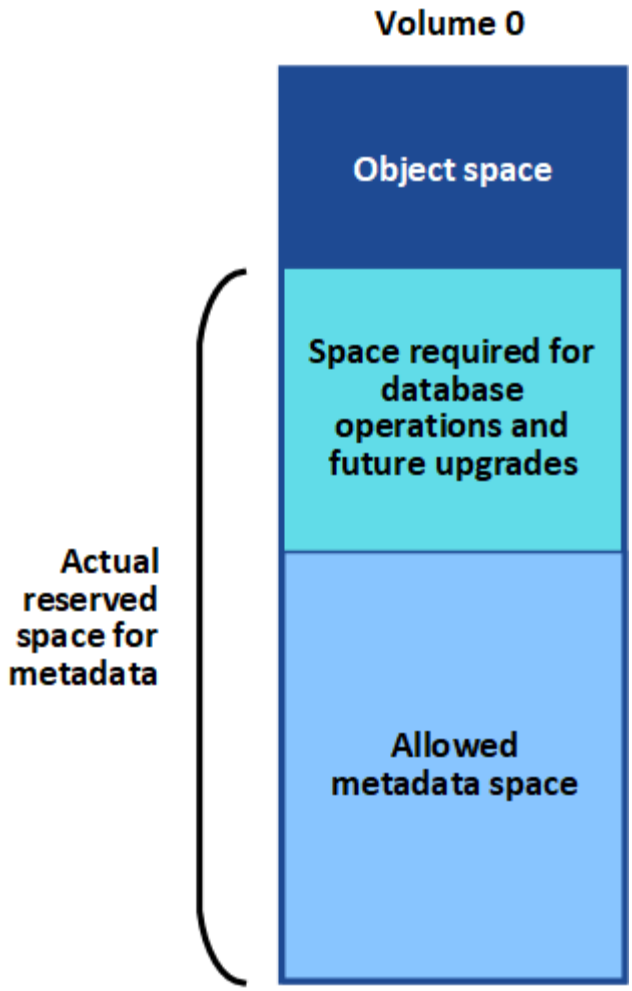
实际保留元数据空间示例

假设您使用 11.7 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 8 TB。（如果每个存储节点的 RAM 超过 128 GB，这是新 StorageGRID 11.6 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。）

允许的元数据空间

每个存储节点的元数据实际保留空间被细分为可用于对象元数据的空间（允许的元数据空间）和基本数据库操作（如压缩和修复）以及未来硬件和软件升级所需的空间。允许的元数据空间控制整体对象容量。



下表显示了 StorageGRID 如何根据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	
	< 128 GB	>= 128 GB	元数据的实际预留空间
⇦ 4 TB	元数据实际保留空间的 60%，最多 1.32 TB	元数据实际保留空间的 60%，最多 1.98 TB	4 TB

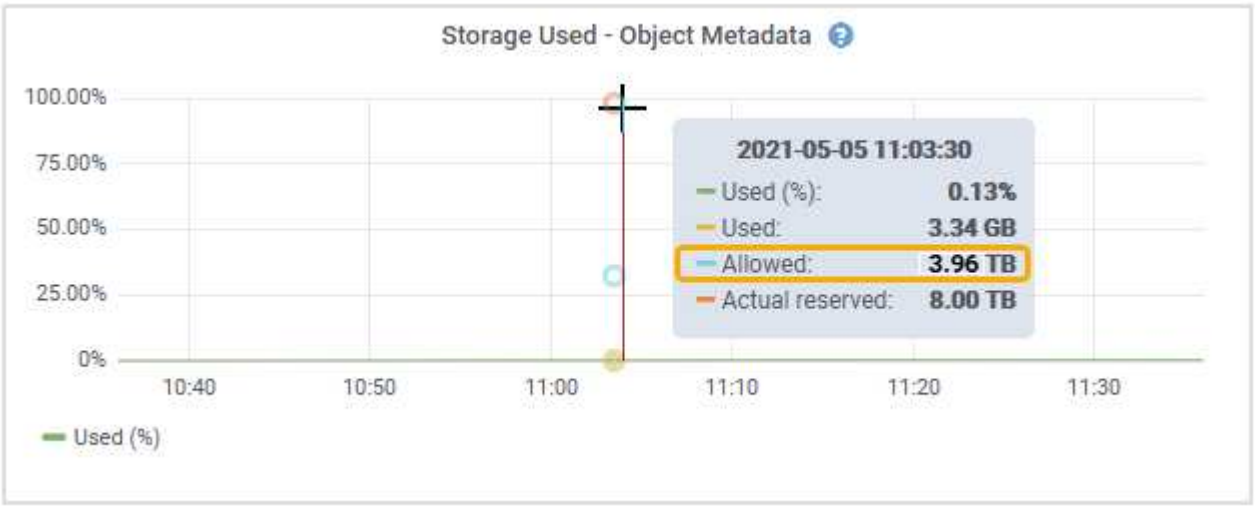
查看允许的元数据空间

按照下面的步骤查看存储节点允许的元数据空间。

步骤

1. 在网格管理器中，选择 节点 。
2. 选择存储节点。
3. 选择 **Storage** 选项卡。

4. 将光标放在"已用存储 - 对象元数据"图表上，并找到 **Allowed** 值。



在屏幕截图中，*允许*值为 3.96 TB，这是元数据实际保留空间超过 4 TB 的 Storage Node 的最大值。

*允许的*值对应于此 Prometheus 指标：

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

允许的元数据空间示例

假设您使用版本 11.6 安装 StorageGRID 系统。对于此示例，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 8 TB。（这是每个 Storage Node 内存超过 128 GB RAM 时，StorageGRID 11.6 或更高版本的默认值。）
- 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 TB，基于元数据允许空间的表中所示的计算：（元数据的实际保留空间 – 1 TB）× 60%，最多 3.96 TB。

不同大小的存储节点如何影响对象容量

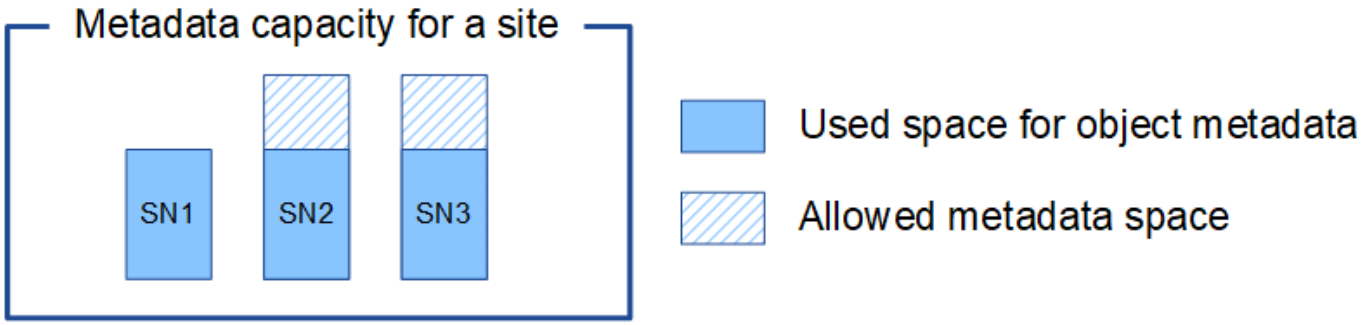
如上所述，StorageGRID 会在每个站点的存储节点之间均匀分布对象元数据。因此，如果站点包含不同大小的存储节点，则该站点上最小的节点决定了站点的元数据容量。

请考虑以下示例：

- 您有一个包含三个不同大小的存储节点的单站点网格。
- *元数据保留空间*设置为 4 TB。
- 对于实际保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	实际保留的元数据空间	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

由于对象元数据均匀分布在站点的存储节点上，因此本示例中的每个节点只能容纳 1.32 TB 的元数据。SN2 和 SN3 允许的额外 0.66 TB 元数据空间无法使用。



同样，由于 StorageGRID 在每个站点维护 StorageGRID 系统的所有对象元数据，因此 StorageGRID 系统的整体元数据容量由最小站点的对象元数据容量决定。

由于对象元数据容量控制最大对象计数，当某个节点的元数据容量耗尽时，网格实际上已满。

相关信息

- 要了解如何监视每个存储节点的对象元数据容量，请参见 "监控 StorageGRID" 的说明。
- 要增加系统的对象元数据容量，请 "展开网格" 通过添加新的存储节点。

增加 StorageGRID 中的 Metadata Reserved Space 设置

如果存储节点满足 RAM 和可用空间的特定要求，或许可以增加元数据保留空间系统设置。

您需要什么

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "Root 访问权限或其他网格配置权限"。

关于此任务

您或许可以手动将系统范围的元数据保留空间设置增加到 8 TB。

仅当以下两个条件均为真时，才能增加系统范围元数据保留空间设置的值：

- 您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，将同时减少所有存储节点存储卷 0 上对象存储的可用空间。为此，您可能希望根据预期的对象元数据要求，将元数据保留空间设置为小于 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"元数据保留空间"设置太大，可以稍后将其减小。相反，如果稍后增加值，系统可能需要移动对象数据以释放空间。

有关元数据保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. 确定当前元数据保留空间设置。
   a. 选择*配置* > 系统 > 存储设置。
   b. 请注意*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 **Nodes**。
   b. 选择网格中的第一个存储节点。
   c. 选择Storage选项卡。
   d. 在卷部分，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保留空间值之间的差值。

      ${post_edited_translations.segment}

   f. ${post_edited_translations.segment}
      - 如果一个或多个 Storage Node 没有足够的可用空间，则无法增加 Metadata Reserved Space 值。请勿继续执行此步骤。
      - ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   a. 选择 **Nodes**。
   b. 选择网格中的第一个存储节点。
   c. ${post_edited_translations.segment}
   d. 将光标悬停在内存使用情况图表上。确保 总内存 至少为 128 GB。
   e. ${post_edited_translations.segment}
      - 如果一个或多个存储节点没有足够的可用总内存，则无法增加元数据保留空间值。请勿继续此过程。
      - ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   a. 选择*配置* > 系统 > 存储设置。
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

d. 选择 **Save**。

压缩 StorageGRID 中存储的对象

您可以启用对象压缩以减少存储在 StorageGRID 中的对象大小，从而使对象占用更少的存储空间。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

关于此任务

默认情况下，禁用对象压缩。如果启用压缩，StorageGRID 会尝试在保存每个对象时使用无损压缩对其进行压缩。

> 如果更改此设置，应用新设置大约需要一分钟。配置的值将被缓存以提升性能和扩展能力。

在启用对象压缩之前，请注意以下几点：

- 除非您知道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 之前已对其进行压缩，则选择此选项不会进一步减小对象的大小。
- 如果您将 NetApp FabricPool 与 StorageGRID 结合使用，请勿选择*压缩存储的对象*。
- 如果选择*压缩存储对象*，S3 客户端应用程序应避免执行指定返回字节范围的 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所请求的字节。从非常大的对象请求小范围字节的 GetObject 操作效率特别低；例如，从 50 GB 压缩对象读取 10 MB 范围是低效的。

  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*压缩存储对象*复选框。
3. 选择 **Save**。

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。有三个可用选项：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少于最大数量，则

可以添加卷以增加其容量。请参阅 "扩展 StorageGRID 系统" 的说明。

添加存储扩展架

某些 StorageGRID 设备存储节点（例如 SG6060 或 SG6160）可以支持其他存储架。如果您的 StorageGRID 设备具有尚未扩展到最大容量的扩展功能，则可以添加存储架以增加容量。请参阅 "扩展 StorageGRID 系统" 的说明。

添加存储节点

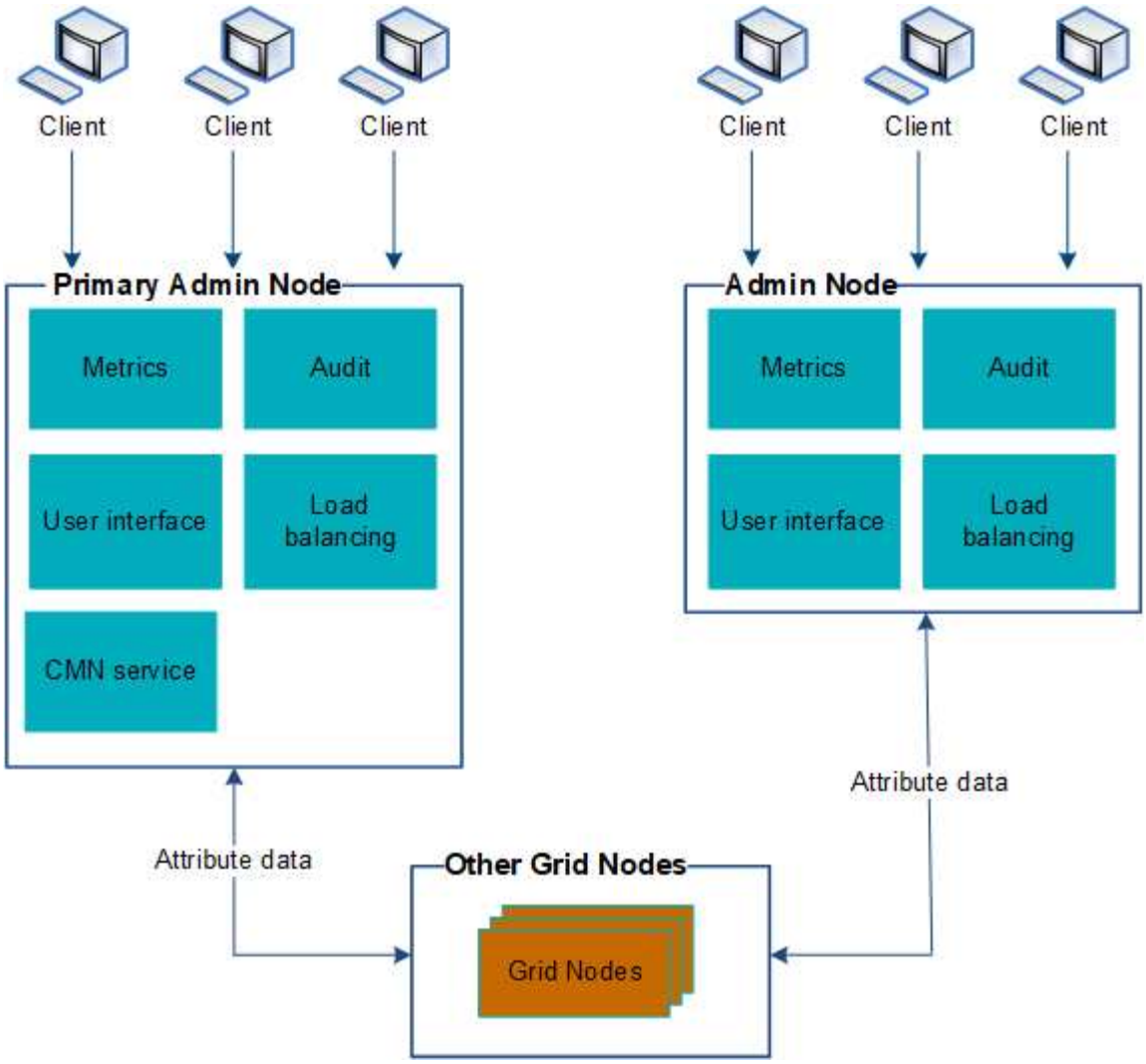
您可以通过添加存储节点来增加存储容量。添加存储时，必须仔细考虑当前活动的 ILM 规则和容量要求。请参阅 "扩展 StorageGRID 系统" 的说明。

管理管理节点

在 **StorageGRID** 中使用多个管理节点

一个 StorageGRID 系统可以包括多个管理节点，使您能够持续监控和配置 StorageGRID 系统，即使某个管理节点发生故障也不例外。

如果管理节点不可用，属性处理将继续，仍然会触发警报，并且仍然会发送电子邮件通知和 AutoSupport 包。但是，拥有多个管理节点并不能提供故障转移保护，通知和 AutoSupport 包除外。



如果管理节点出现故障，可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管理节点的高可用性组，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，如果活动的管理节点出现故障，访问将会中断。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，必须先恢复该节点，StorageGRID 系统才能再次完全正常运行。

识别 StorageGRID 中的主管理节点

主管理节点比非主管理节点提供更多功能。例如，必须使用主管理节点执行某些维护程序。

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 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "特定访问权限"。

步骤

1. 选择 **Nodes**。
2. 在搜索框中输入 **primary**。

   在搜索结果中，找到类型列中显示"Primary Admin Node"的节点。应列出一个主管理节点。