管理 StorageGRID

StorageGRID 11.7

NetApp
April 12, 2024

目录

管理 StorageGRID

管理 StorageGRID： 概述

按照以下说明配置和管理 StorageGRID 系统。

关于这些说明

以下说明介绍如何使用网格管理器设置组和用户，创建租户帐户以允许 S3 和 Swift 客户端应用程序存储和检索对象，配置和管理 StorageGRID 网络，配置 AutoSupport ，管理节点设置等。

本说明适用于在安装 StorageGRID 系统后配置，管理和支持该系统的技术人员。

开始之前

- 您已大致了解 StorageGRID 系统。
- 您对 Linux 命令 Shell ，网络连接以及服务器硬件设置和配置有相当详细的了解。

开始使用Grid Manager

Web 浏览器要求

您必须使用受支持的 Web 浏览器。

Web 浏览器	支持的最低版本
Google Chrome	107.
Microsoft Edge	107.
Mozilla Firefox	106.

您应将浏览器窗口设置为建议的宽度。

浏览器宽度	像素
最小值	1024
最佳	1280

登录到网格管理器

您可以通过在支持的 Web 浏览器的地址栏中输入管理节点的完全限定域名（ FQDN ）或 IP 地址来访问网格管理器登录页面。

概述

每个 StorageGRID 系统都包括一个主管理节点和任意数量的非主管理节点。您可以登录到任何管理节点上的网格管理器来管理 StorageGRID 系统。但是、管理节点并不完全相同：

- 在一个管理节点上发出的警报鸣响(旧系统)不会复制到其他管理节点。因此，为警报显示的信息在每个管理节点上可能不相同。
- 某些维护过程只能从主管理节点执行。

连接到**HA**组

如果管理节点包含在高可用性（ HA ）组中，则可以使用 HA 组的虚拟 IP 地址或映射到虚拟 IP 地址的完全限定域名进行连接。应选择主管理节点作为组的主接口，以便在访问网格管理器时，您可以在主管理节点上访问它，除非主管理节点不可用。请参见 "管理高可用性组"。

使用**SSO**

如果、则登录步骤略有不同 "已配置单点登录(SSO)"。

在第一个管理节点上登录到网格管理器

开始之前

- 您已拥有登录凭据。
- 您正在使用 "支持的 Web 浏览器"。
- 已在 Web 浏览器中启用 Cookie 。
- 您所属的用户组至少具有一个权限。
- 您有网格管理器的URL：

  `https://FQDN_or_Admin_Node_IP/`

  您可以使用完全限定域名、管理节点的IP地址或管理节点HA组的虚拟IP地址。

  要通过非HTTPS默认端口(443)访问网格管理器、请在URL中包含端口号：

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO在受限的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. 在浏览器的地址栏中、输入网格管理器的URL。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。请参见 "管理安全证书"。
4. 登录到网格管理器。

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

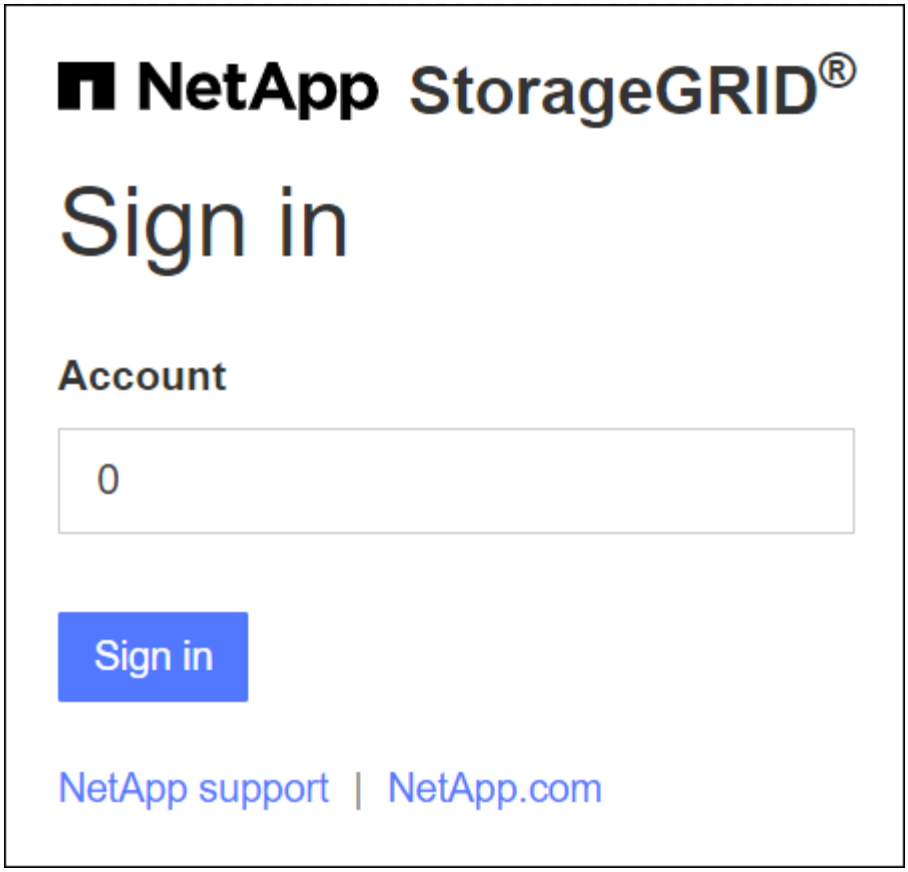
未使用**SSO**

a. 输入网格管理器的用户名和密码。

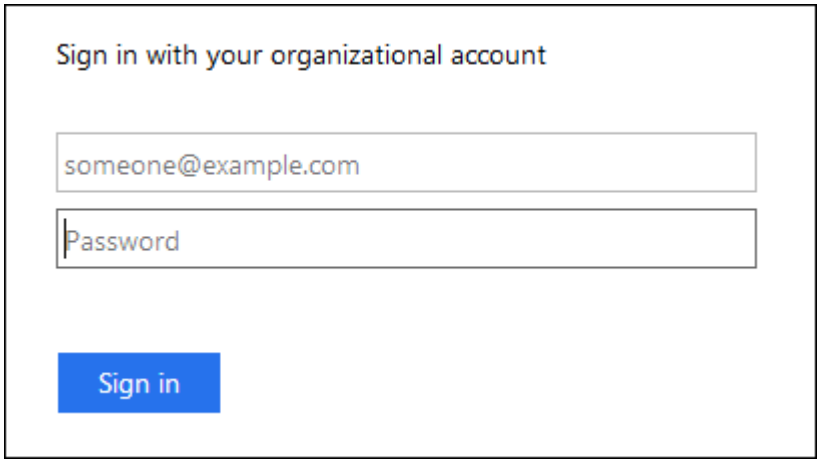
b. 选择 * 登录 * 。

使用**SSO**

- 如果StorageGRID 正在使用SSO、而这是您首次在此浏览器上访问此URL：
  i. 选择 * 登录 * 。您可以在帐户字段中保留0。



ii. 在组织的 SSO 登录页面上输入标准 SSO 凭据。例如：

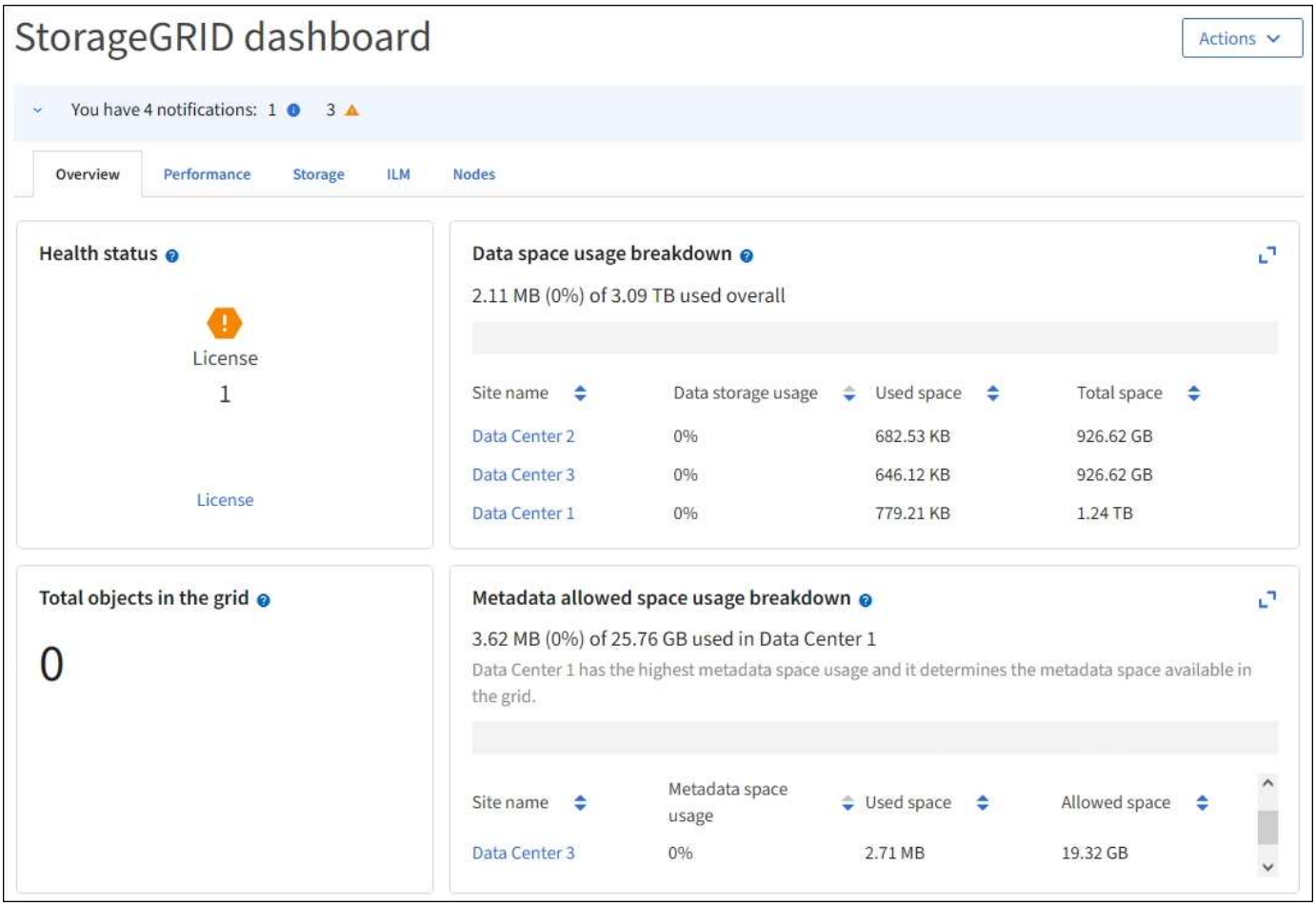


- 如果StorageGRID 正在使用SSO、并且您之前已访问网格管理器或租户帐户：
  i. 输入*0*(网格管理器的帐户ID)或选择*Grid Manager*(如果它出现在最近帐户列表中)。

ii. 选择 * 登录 * 。

iii. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。

登录后、将显示网格管理器的主页、其中包括信息板。要了解所提供的信息，请参见 "查看和管理信息板"。



登录到其他管理节点

按照以下步骤登录到其他管理节点。

未使用**SSO**

步骤

1. 在浏览器的地址栏中，输入另一个管理节点的完全限定域名或 IP 地址。根据需要包括端口号。
2. 输入网格管理器的用户名和密码。
3. 选择 * 登录 * 。

使用**SSO**

如果StorageGRID 正在使用SSO、并且您已登录到一个管理节点、则可以访问其他管理节点、而无需重新登录。

步骤

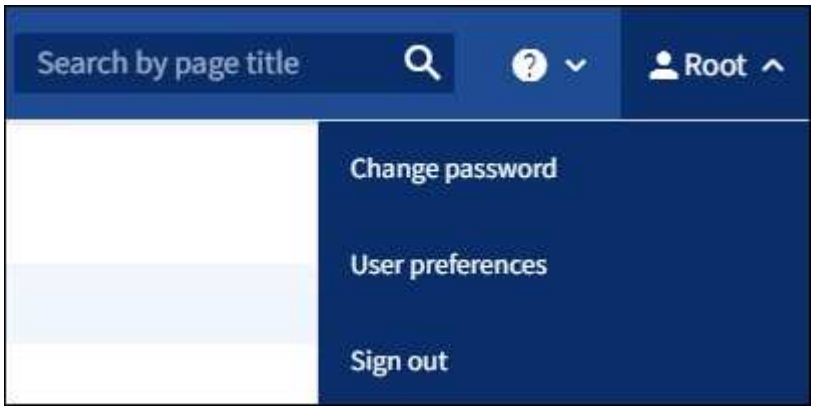
1. 在浏览器的地址栏中输入另一个管理节点的完全限定域名或IP地址。
2. 如果您的SSO会话已过期、请重新输入您的凭据。

注销 Grid Manager

使用网格管理器完成后、您必须注销以确保未经授权的用户无法访问StorageGRID 系统。根据浏览器 Cookie 设置，关闭浏览器可能无法将您从系统中注销。

步骤

1. 在右上角选择您的用户名。



2. 选择*注销*。

选项	Description
SSO 未使用	您已从管理节点注销。 此时将显示网格管理器登录页面。 • 注意： * 如果您已登录到多个管理节点，则必须从每个节点注销。
已启用 SSO	您已从正在访问的所有管理节点中注销。此时将显示 StorageGRID 登录页面。* 网格管理器 * 在 * 近期帐户 * 下拉列表中列为默认值， * 帐户 ID* 字段显示 0 。 *注意：*如果启用了SSO、并且您还登录到租户管理器、则还必须登录 "注销租户帐户" to "注销SSO"。

更改密码

如果您是网格管理器的本地用户，则可以更改自己的密码。

开始之前

您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

如果您以联盟用户身份登录到StorageGRID 、或者启用了单点登录(SSO)、则无法在网格管理器中更改密码。而是必须更改外部身份源中的密码，例如 Active Directory 或 OpenLDAP 。

步骤

1. 从网格管理器标题中，选择 * 。您的姓名 _* > * 更改密码 * 。
2. 输入当前密码。
3. 键入新密码。

   您的密码必须至少包含 8 个字符，并且不能超过 32 个字符。密码区分大小写。

4. 重新输入新密码。
5. 选择 * 保存 * 。

查看 StorageGRID 许可证信息

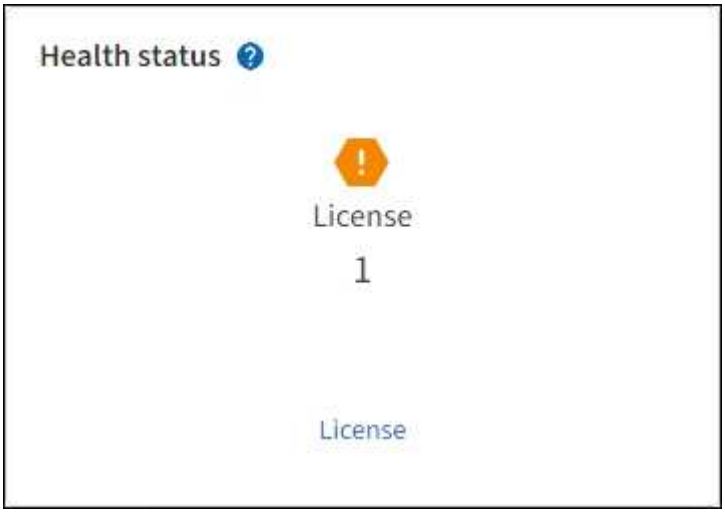
您可以根据需要查看 StorageGRID 系统的许可证信息，例如网格的最大存储容量。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

如果某个问题描述 具有此StorageGRID 系统的软件许可证，信息板上的运行状况卡将包含一个许可证状态图标和一个*License*链接。此数字表示与许可证相关的问题数量。



步骤

1. 通过执行以下操作之一访问许可证页面：
   - 从信息板上的运行状况卡中，选择许可证状态图标或*License*链接。只有当具有许可证的问题描述 时，才会显示此链接。
   - 选择 * 维护 * > * 系统 * > * 许可证 * 。
2. 查看当前许可证的只读详细信息：
   - StorageGRID 系统 ID ，此 ID 是此 StorageGRID 安装的唯一标识号
   - 许可证序列号
   - 许可证类型，永久*或*订阅
   - 网格的许可存储容量

- 支持的存储容量
- 许可证结束日期。*不适用*表示永久许可证。
- 支持服务合同结束日期

  此日期是从当前许可证文件中读取的、如果您在获取许可证文件后延长或续订了支持服务合同、则此日期可能已过时。要更新此值、请参见 "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

> 对于在 StorageGRID 10.3 之前发布的许可证，许可的存储容量不会包含在许可证文件中，并且会显示 " 请参见许可协议 " 消息而不是值。

更新 StorageGRID 许可证信息

您必须在许可证条款发生更改时随时更新 StorageGRID 系统的许可证信息。例如，如果为网格购买了额外的存储容量，则必须更新许可证信息。

开始之前

- 您有一个新的许可证文件可应用于 StorageGRID 系统。
- 您具有特定的访问权限。
- 您具有配置密码短语。

步骤

1. 选择 * 维护 * > * 系统 * > * 许可证 * 。
2. 在*配置密码短语*文本框中输入StorageGRID 系统的配置密码短语，然后选择*浏览*。
3. 在打开对话框中、找到并选择新的许可证文件 (`.txt`)，然后选择*Open*。

   此时将验证并显示新许可证文件。

4. 选择 * 保存 * 。

使用 API

使用网格管理 API

您可以使用网格管理 REST API 执行系统管理任务，而不是使用网格管理器用户界面。例如，您可能希望使用 API 来自动执行操作或更快地创建多个实体，例如用户。

顶级资源

网格管理 API 可提供以下顶级资源：

- `/grid`：访问权限仅限于Grid Manager用户、并且取决于配置的组权限。
- `/org`：只有属于租户帐户的本地或联合LDAP组的用户才能访问。有关详细信息，请参见 "使用租户帐户"。

- `/private`：访问权限仅限于Grid Manager用户、并且取决于配置的组权限。专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

问题描述 **API** 请求

网格管理 API 使用 Swagger 开源 API 平台。Swagger 提供了一个直观的用户界面，使开发人员和非开发人员能够使用 API 在 StorageGRID 中执行实时操作。

Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。

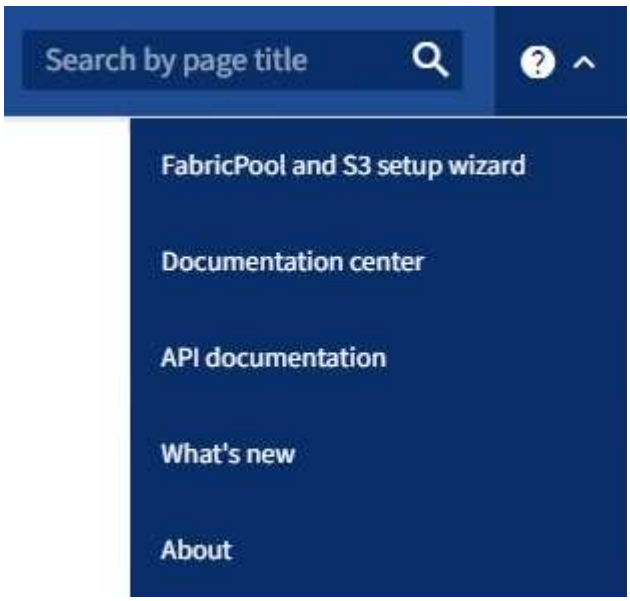
开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

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

步骤

1. 从Grid Manager标题中，选择帮助图标，然后选择*API documents*。



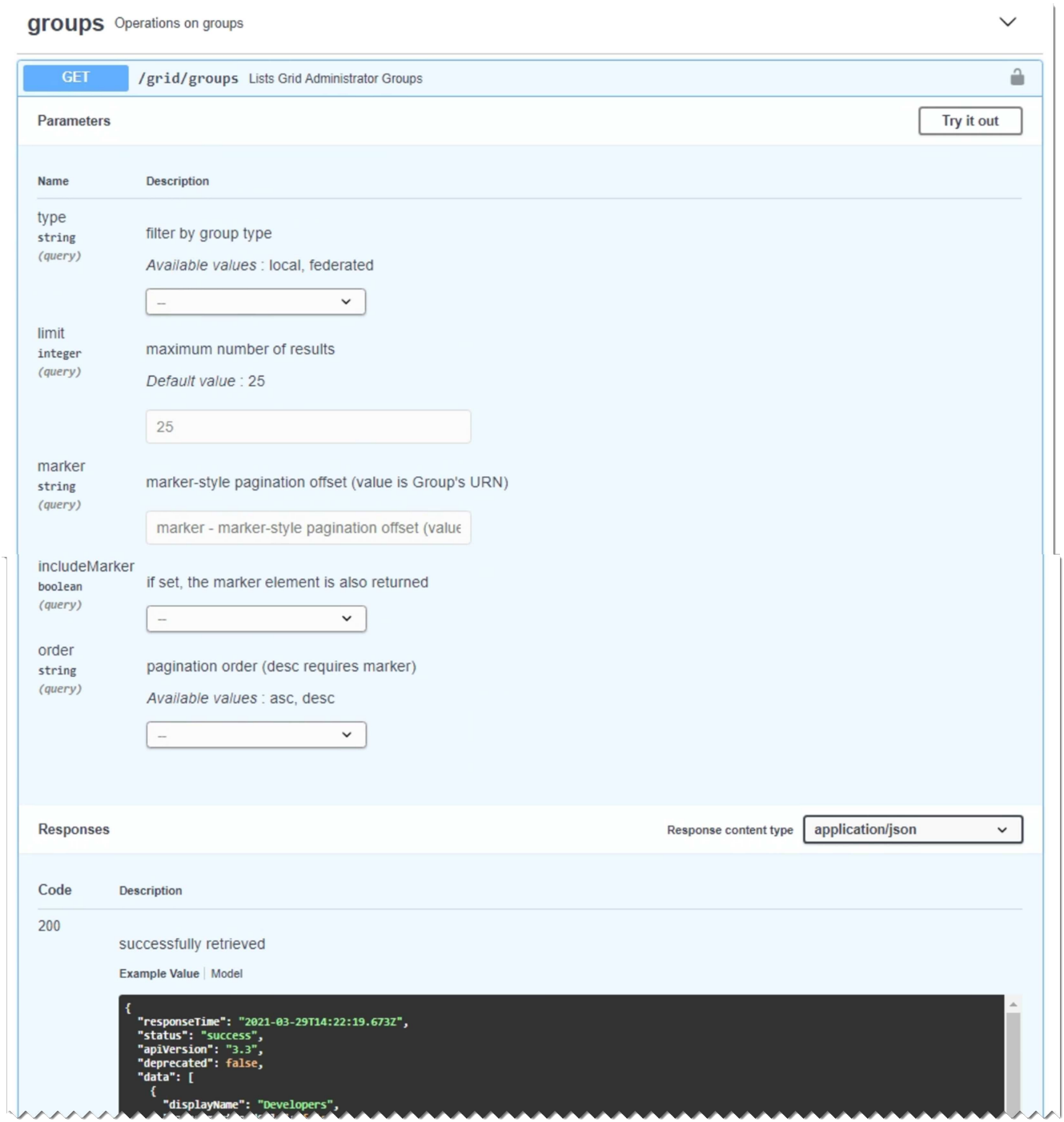
2. 要使用专用 API 执行操作，请在 StorageGRID 管理 API 页面上选择 * 转至专用 API 文档 * 。

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

3. 选择所需的操作。

   展开 API 操作时，您可以看到可用的 HTTP 操作，例如 GET ， PUT ， UPDATE 和 DELETE 。

4. 选择 HTTP 操作可查看请求详细信息，包括端点 URL ，任何必需或可选参数的列表，请求正文示例（如果需要）以及可能的响应。



5. 确定此请求是否需要其他参数，例如组或用户 ID 。然后，获取这些值。您可能需要先对其他 API 请求进行问题描述 处理，以获取所需的信息。
6. 确定是否需要修改示例请求正文。如果是，您可以选择 * 型号 * 来了解每个字段的要求。
7. 选择 * 试用 * 。
8. 提供所需的任何参数，或根据需要修改请求正文。
9. 选择 * 执行 * 。
10. 查看响应代码以确定请求是否成功。

网格管理 API 将可用操作组织到以下部分中。

> 此列表仅包含公有 API 中可用的操作。

- 帐户：用于管理存储租户帐户的操作、包括创建新帐户和检索给定帐户的存储使用量。
- 警报：用于列出当前警报(传统系统)并返回有关网格运行状况的信息(包括当前警报和节点连接状态摘要)的操作。
- **alerts**历史记录：对已解决的警报执行操作。
- 警报接收者：警报通知接收者操作(电子邮件)。
- 警报规则：对警报规则执行操作。
- 警报静音：警报静音操作。
- 警报：对警报执行操作。
- **audi**：列出和更新审核配置的操作。
- **auth**：执行用户会话身份验证的操作。

  网格管理 API 支持不可承载令牌身份验证方案。要登录、请在身份验证请求的JSON正文中提供用户名和密码(即、 `POST /api/v3/authorize`）。如果用户已成功通过身份验证，则会返回一个安全令牌。此令牌必须在后续 API 请求的标题中提供（ "Authorization： bearer *token*" ）。

  > 如果为 StorageGRID 系统启用了单点登录，则必须执行不同的步骤进行身份验证。请参见 "` 在启用单点登录后对 API 进行身份验证。` "

  有关提高身份验证安全性的信息，请参阅“防止跨站点请求伪造”。

- **client-certificates**：用于配置客户端证书的操作，以便使用外部监控工具安全地访问StorageGRID。
- **config**：与网格管理API的产品发行版和版本相关的操作。您可以列出该版本支持的网格管理 API 的产品版本和主要版本，并且可以禁用已弃用的 API 版本。
- *DEactive-Features *：用于查看可能已停用的功能的操作。
- **DNS-SERVERS**：列出和更改已配置的外部DNS服务器的操作。
- **endpoint-domain-names**：列出和更改S3端点域名的操作。
- 纠删编码：对纠删编码配置文件的操作。
- 扩展：扩展操作(程序级)。
- 扩展节点：扩展操作(节点级)。
- 扩展站点：扩展操作(站点级)。
- *GRE-NETWORKS：列出和更改Grid Network List的操作。
- **GRID**密码：网格密码管理操作。
- 组：用于管理本地网格管理员组以及从外部LDAP服务器检索联合网格管理员组的操作。
- 身份源：用于配置外部身份源以及手动同步联盟组和用户信息的操作。

- *ILM：有关信息生命周期管理(ILM)的操作。
- **license**：用于检索和更新StorageGRID 许可证的操作。
- **logs**：用于收集和下载日志文件的操作。
- **metrics**：对StorageGRID 指标的操作，包括在某一时间点的即时指标查询和在一段时间内的范围指标查询。网格管理 API 使用 Prometheus 系统监控工具作为后端数据源。有关构建 Prometheus 查询的信息，请参见 Prometheus 网站。

> 包括的指标 *private* 其名称仅供内部使用。这些指标可能会在 StorageGRID 版本之间发生更改，恕不另行通知。

- 节点详细信息：对节点详细信息执行的操作。
- 节点运行状况：对节点运行状况执行的操作。
- **NONE-storage-state**：对节点存储状态执行的操作。
- **ntp-server**：列出或更新外部网络时间协议(NTP)服务器的操作。
- 对象：对对象和对象元数据执行的操作。
- 恢复：恢复操作步骤 的操作。
- 恢复包：用于下载恢复软件包的操作。
- 区域：用于查看和创建区域的操作。
- **s3-object-lock**：对全局S3对象锁定设置执行操作。
- **server-certificates**：用于查看和更新Grid Manager服务器证书的操作。
- **SNMP**：对当前SNMP配置执行的操作。
- **Traffic Classes**：流量分类策略的操作。
- 不可信客户端网络：对不可信客户端网络配置执行的操作。
- 用户：用于查看和管理Grid Manager用户的操作。

网格管理 **API** 版本控制

网格管理 API 使用版本控制来支持无中断升级。

例如，此请求 URL 指定 API 版本 3 。

```
https://hostname_or_ip_address/api/v3/authorize
```

如果对旧版本进行了 * 不兼容 _* 的更改，则租户管理 API 的主要版本将发生递增。如果对 * 与旧版本兼容 _* 进行了更改，则租户管理 API 的次要版本将发生递增。兼容的更改包括添加新端点或新属性。以下示例说明了如何根据所做更改的类型对 API 版本进行递增。

API 的更改类型	旧版本	新版本
与旧版本兼容	2.1	2.2
与旧版本不兼容	2.1	3.0

首次安装 StorageGRID 软件时，仅会启用最新版本的网格管理 API 。但是，在升级到 StorageGRID 的新功能版本时，您仍可以访问至少一个 StorageGRID 功能版本的旧版 API 。

> 您可以使用网格管理 API 配置受支持的版本。有关详细信息，请参见 Swagger API 文档中的 "`config` " 一节。在更新所有网格管理 API 客户端以使用较新版本后，您应停用对较旧版本的支持。

已过时的请求将通过以下方式标记为已弃用：

- 响应标头为 "depression: true"
- JSON 响应正文包含 "depressioned" ： true
- NMS.log 中会添加一个已弃用的警告。例如：

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

确定当前版本支持哪些 API 版本

请使用以下 API 请求返回受支持的 API 主要版本列表：

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

指定请求的 API 版本

您可以使用path参数指定API版本 (`/api/v3`)或标题 (`Api-Version: 3`）。如果同时提供这两个值，则标头值将覆盖路径值。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

防止跨站点请求伪造（ CSRF ）

您可以通过使用 CSRF 令牌增强使用 Cookie 的身份验证，帮助防止 StorageGRID 受到跨站点请求伪造（ CSRF ）攻击。网格管理器和租户管理器会自动启用此安全功能；其他

API 客户端可以选择在登录时是否启用此功能。

如果攻击者可能触发对其他站点的请求（例如使用 HTTP 表单发布），则可以对使用已登录用户的 cookie 发出的某些请求进行发生原因 处理。

StorageGRID 可通过使用 CSRF 令牌帮助防止 CSRF 攻击。启用后，特定 Cookie 的内容必须与特定标题或特定后处理正文参数的内容匹配。

要启用此功能、请设置 `csrfToken` 参数设置为 `true` 身份验证期间。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、则为A `GridCsrfToken` Cookie会使用随机值设置为网格管理器和登录 `AccountCsrfToken` Cookie会使用随机值设置为登录到租户管理器。

如果存在 Cookie ，则可以修改系统状态的所有请求（ POST ， PUT ， patch ， delete ）都必须包括以下项之一：

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

有关其他示例和详细信息，请参见联机 API 文档。

> 设置了CSRF令牌Cookie的请求也将强制实施 `"Content-Type: application/json"` 任何请求的标头、如果希望JSON请求正文作为对CSRF攻击的额外保护、

如果启用了单点登录，请使用 **API**

如果启用了单点登录，请使用 **API** （ **Active Directory** ）

如果您有 "已配置并启用单点登录（ SSO ）" 如果您使用 Active Directory 作为 SSO 提供程序，则必须对一系列 API 请求进行问题描述 处理，以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了单点登录，请登录到 **API**

如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用。

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- 。 `storagegrid-ssoauth.py` Python脚本、位于StorageGRID 安装文件目录中 (`./rpms` 对于Red Hat Enterprise Linux或CentOS、 `./debs` 适用于Ubuntu或Debian、和 `./vsphere` 适用于VMware)。
- cURL 请求的示例工作流。

  如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误： `A valid SubjectConfirmation was not found on this Response`。

  > 示例 cURL 工作流不会保护密码不会被其他用户看到。

如果您使用的是URL编码问题描述 、则可能会看到以下错误： `Unsupported SAML version`。

步骤

1. 选择以下方法之一以获取身份验证令牌：
   - 使用 `storagegrid-ssoauth.py` Python脚本。转至步骤 2 。
   - 使用 curl 请求。转至步骤 3 。
2. 如果要使用 `storagegrid-ssoauth.py` 脚本、将脚本传递给Python解释器并运行脚本。

   出现提示时，输入以下参数的值：

   - SSO 方法。输入 ADFS 或 ADFS 。
   - SSO 用户名
   - 安装 StorageGRID 的域
   - StorageGRID 的地址
   - 要访问租户管理 API 的租户帐户 ID 。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下操作步骤 。

   a. 声明登录所需的变量。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

> 要访问网格管理API、请使用0作为 `TENANTACCOUNTID`。

b. 要接收签名身份验证URL、问题描述 请将POST请求发送到 `/api/v3/authorize-saml`、并从响应中删除其他JSON编码。

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

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

此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

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

c. 保存 `SAMLRequest` 从响应中获取、以便在后续命令中使用。

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

d. 从 AD FS 获取包含客户端请求 ID 的完整 URL 。

一种方法是使用上一响应中的 URL 请求登录表单。

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

此响应包括客户端请求 ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 保存响应中的客户端请求 ID 。

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

f. 将您的凭据发送到上一响应中的表单操作。

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS 返回 302 重定向，并在标题中显示追加信息 。

> 如果为 SSO 系统启用了多因素身份验证（ MFA ），则此表单发布还将包含第二个密码或其他凭据。

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

g. 保存 `MSISAuth` 响应中的cookie。

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

h. 使用身份验证 POST 中的 Cookie 将 GET 请求发送到指定位置。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

响应标头将包含 AD FS 会话信息，以便日后注销时使用，而响应正文将 SAMLResponse 隐藏在一个格式的字段中。

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

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

i. 保存 `SAMLResponse` 在隐藏字段中：

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

j. 使用已保存的 `SAMLResponse`、创建StorageGRID`/api/saml-response` 生成StorageGRID 身份验

证令牌的请求。

适用于 `RelayState`、请使用租户帐户ID或如果要登录到网格管理API、请使用0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

响应包括身份验证令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 将响应中的身份验证令牌另存为 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

您现在可以使用 `MYTOKEN` 对于其他请求、类似于未使用SSO时使用API的方式。

如果启用了单点登录，请注销 API

如果已启用单点登录（ Single Sign-On ， SSO ），则必须对一系列 API 请求进行问题描述，才能注销网格管理 API 或租户管理 API 。如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要、您可以从组织的单点注销页面注销、以注销StorageGRID API。或者，您也可以从 StorageGRID 触发单点注销（ SLO ），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求、请传递 `cookie "sso=true"` 至SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

返回注销 URL：

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. 保存注销 URL 。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。条件 `cookie "sso=true"` 如果未提供、则用户将从StorageGRID 中注销、而不会影响SSO状态。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

答 `204 No Content` 响应指示用户现在已注销。

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

如果启用了单点登录，请使用 **API** （ **Azure** ）

如果您有 "已配置并启用单点登录（ SSO ）" 使用 Azure 作为 SSO 提供程序时，您可以使用两个示例脚本来获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了 **Azure** 单点登录，请登录到 **API**

如果您使用 Azure 作为 SSO 身份提供程序，则以下说明适用

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 电子邮件地址和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例脚本：

- 。 `storagegrid-ssoauth-azure.py` Python 脚本
- 。 `storagegrid-ssoauth-azure.js` 节点.js脚本

这两个脚本都位于StorageGRID 安装文件目录中 (`./rpms` 对于Red Hat Enterprise Linux或CentOS、 `./debs` 适用于Ubuntu或Debian、和 `./vsphere` 适用于VMware)。

要编写您自己的与Azure的API集成、请参见 `storagegrid-ssoauth-azure.py` 脚本。Python 脚本会直接向 StorageGRID 发出两个请求（首先获取 SAMLRequest ，然后再获取授权令牌），同时还会调用 Node.js 脚本与 Azure 交互以执行 SSO 操作。

可以使用一系列 API 请求执行 SSO 操作，但这样做并不简单。puppeteer Node.js 模块用于擦除 Azure SSO 接口。

如果您使用的是URL编码问题描述 、则可能会看到以下错误： `Unsupported SAML version`。

步骤

1. 安装所需的依赖关系，如下所示：
   a. 安装 Node.js （请参见 "https://nodejs.org/en/download/"）。
   b. 安装所需的 Node.js 模块（ puppeteer 和 jsdom ）：

      ```
      npm install -g <module>
      ```

2. 将 Python 脚本传递给 Python 解释器以运行此脚本。

   然后， Python 脚本将调用相应的 Node.js 脚本以执行 Azure SSO 交互。

3. 出现提示时，输入以下参数的值（或使用参数传递这些值）：
   - 用于登录到 Azure 的 SSO 电子邮件地址

- StorageGRID 的地址
- 要访问租户管理 API 的租户帐户 ID

4. 出现提示时，输入密码，并在收到请求时准备向 Azure 提供 MFA 授权。

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

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

> 此脚本假定 MFA 是使用 Microsoft Authenticator 完成的。您可能需要修改脚本以支持其他形式的MFA (例如、输入在文本消息中收到的代码)。

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

如果启用了单点登录，请使用 **API** （ **PingFederate** ）

如果您有 "已配置并启用单点登录（SSO）" 如果使用 PingFederate 作为 SSO 提供程序，则必须对一系列 API 请求进行问题描述 处理，以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了单点登录，请登录到 **API**

如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- 。 `storagegrid-ssoauth.py` Python脚本、位于StorageGRID 安装文件目录中 (`./rpms` 对于Red Hat Enterprise Linux或CentOS、 `./debs` 适用于Ubuntu或Debian、和 `./vsphere` 适用于VMware)。
- cURL 请求的示例工作流。

  如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误： `A valid SubjectConfirmation was not found on this Response`。

  > 示例 cURL 工作流不会保护密码不会被其他用户看到。

  如果您使用的是URL编码问题描述 、则可能会看到以下错误： `Unsupported SAML version`。

步骤

1. 选择以下方法之一以获取身份验证令牌：
   - 使用 `storagegrid-ssoauth.py` Python脚本。转至步骤 2 。
   - 使用 curl 请求。转至步骤 3 。
2. 如果要使用 `storagegrid-ssoauth.py` 脚本、将脚本传递给Python解释器并运行脚本。

   出现提示时，输入以下参数的值：

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

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*********************************************************************************

*********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

   输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下操作步骤 。

   a. 声明登录所需的变量。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

   > 要访问网格管理API、请使用0作为 `TENANTACCOUNTID`。

   b. 要接收签名身份验证URL、问题描述 请将POST请求发送到 `/api/v3/authorize-saml`、并从响应中删除其他JSON编码。

   此示例显示了一个 POST 请求，用于为 TENANTACCOBTID 提供签名身份验证 URL 。结果将传递到 python -m json.tool 以删除 JSON 编码。

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

此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

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

c. 保存 `SAMLRequest` 从响应中获取、以便在后续命令中使用。

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

d. 导出响应和 cookie ，并对响应执行回显：

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

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

e. 导出 "pf.adapterId" 值，并对响应执行回显：

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

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

f. 导出 "href" 值（删除后斜杠 / ），并对响应执行回显：

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

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

g. 导出 "act" 值：

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

h. 发送 Cookie 以及凭据：

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

i. 保存 `SAMLResponse` 在隐藏字段中：

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

j. 使用已保存的 `SAMLResponse`、创建StorageGRID`/api/saml-response` 生成StorageGRID 身份验证令牌的请求。

适用于 `RelayState`、请使用租户帐户ID或如果要登录到网格管理API、请使用0。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

响应包括身份验证令牌。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 将响应中的身份验证令牌另存为 `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

您现在可以使用 `MYTOKEN` 对于其他请求、类似于未使用SSO时使用API的方式。

如果启用了单点登录，请注销 API

如果已启用单点登录（ Single Sign-On ， SSO ），则必须对一系列 API 请求进行问题描述 ，才能注销网格管理 API 或租户管理 API 。如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要、您可以从组织的单点注销页面注销、以注销StorageGRID API。或者，您也可以从 StorageGRID 触发单点注销（ SLO ），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求、请传递 `cookie "sso=true"` 至SLO API：

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

   返回注销 URL ：

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. 保存注销 URL 。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

```
curl --include "$LOGOUT_REQUEST"
```

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. 删除 StorageGRID 承载令牌。

   删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。条件 `cookie "sso=true"` 如果未提供、则用户将从StorageGRID 中注销、而不会影响SSO状态。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

   答 `204 No Content` 响应指示用户现在已注销。

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

使用 **API** 停用功能

您可以使用网格管理 API 完全停用 StorageGRID 系统中的某些功能。停用某个功能后，不能为任何人分配执行与该功能相关的任务的权限。

关于此任务

停用的功能系统允许您阻止访问 StorageGRID 系统中的某些功能。停用某个功能是防止 root 用户或具有 * root 访问权限 * 的管理组中的用户能够使用该功能的唯一方法。

要了解此功能的有用程度，请考虑以下情形：

_Company A 是一家服务提供商，通过创建租户帐户租用其 StorageGRID 系统的存储容量。为了保护租户对象的安全， A 公司希望确保自己的员工在部署帐户后永远不能访问任何租户帐户。 _

_Company A 可以通过使用网格管理 API 中的停用功能系统来实现此目标。通过完全停用网格管理器中的 * 更改租户根密码 * 功能（ UI 和 API ），公司 A 可以确保任何管理员用户（包括 root 用户和属于具有 * root 访问权限 * 组的用户）都不能更改任何租户帐户的 root 用户的密码

步骤

1. 访问网格管理 API 的 Swagger 文档。请参见 "使用网格管理 API"。
2. 找到停用功能端点。
3. 要停用更改租户 root 密码等功能，请按如下所示向 API 发送正文：

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

请求完成后，更改租户根密码功能将被禁用。用户界面中不再显示 * 更改租户根密码 * 管理权限，尝试更改租户根密码的任何 API 请求将失败，并显示 "`403 For禁用 。`

重新激活已停用的功能

默认情况下，您可以使用网格管理 API 重新激活已停用的功能。但是，如果要防止重新激活已停用的功能，则可以停用 * 激活功能 * 功能本身。

> 无法重新激活*activateFeature*功能。如果您决定停用此功能，请注意，您将永远无法重新激活任何其他已停用的功能。要还原任何丢失的功能，您必须联系技术支持。

步骤

1. 访问网格管理 API 的 Swagger 文档。
2. 找到停用功能端点。
3. 要重新激活所有功能，请按如下所示将正文发送到 API：

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

此请求完成后，包括更改租户 root 密码功能在内的所有功能都将重新激活。现在， " 更改租户根密码 " 管理权限将显示在用户界面中，如果用户具有 * 根访问权限 * 或 * 更改租户根密码 * 管理权限，则尝试更改租户根密码的任何 API 请求都将成功。

> 上一示例将重新激活 *all* 已停用的功能。如果其他功能已停用，而这些功能应保持停用状态，则必须在 PUT 请求中明确指定它们。例如，要重新激活更改租户 root 密码功能并继续停用警报确认功能，请发送此 PUT 请求：
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

控制对 StorageGRID 的访问

控制StorageGRID 访问：概述

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

控制对网格管理器的访问

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

使用 "身份联合" 进行设置 "组" 和 "users" 速度更快、并且允许用户使用熟悉的凭据登录到StorageGRID。如果使用 Active Directory， OpenLDAP 或 Oracle Directory Server，则可以配置身份联合。

> 如果要使用其他 LDAP v3 服务，请联系技术支持。

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

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

启用单点登录

StorageGRID 系统支持使用安全断言标记语言 2.0 （ SAML 2.0 ）标准的单点登录（ SSO ）。你先请 "配置并启用SSO"，所有用户都必须先通过外部身份提供程序进行身份验证，然后才能访问网格管理器、租户管理器、网格管理API或租户管理API。本地用户无法登录到StorageGRID。

更改配置密码短语

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

更改节点控制台密码

网格中的每个节点都有一个唯一的节点控制台密码、您需要使用SSH以"admin"身份登录到此节点、或者通过VM/物理控制台连接登录到root用户。您可以根据需要执行此操作 "更改节点控制台密码" 对于每个节点。

更改配置密码短语

使用此操作步骤 更改 StorageGRID 配置密码短语。恢复，扩展和维护过程需要密码短语。下载恢复软件包备份时也需要使用密码短语，其中包括网格拓扑信息，网格节点控制台密码以及 StorageGRID 系统的加密密钥。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有维护或 root 访问权限。
- 您具有当前配置密码短语。

关于此任务

许多安装和维护过程以及都需要配置密码短语 "正在下载恢复包"。配置密码短语未在中列出 `Passwords.txt` 文件请务必记录配置密码短语并将其保存在安全的位置。

步骤

1. 选择 * 配置 * > * 访问控制 * > * 网格密码 * 。
2. 在*更改配置密码短语*下，选择*进行更改*
3. 输入当前配置密码短语。
4. 输入新密码短语。密码短语必须至少包含 8 个字符，并且不能超过 32 个字符。密码短语区分大小写。
5. 将新配置密码短语存储在安全位置。安装，扩展和维护过程需要使用它。
6. 重新输入新密码短语，然后选择 * 保存 * 。

   配置密码短语更改完成后，系统将显示一个绿色的成功横幅。

7. 选择 * 恢复包 * 。
8. 输入新的配置密码短语以下载新的恢复软件包。

> 更改配置密码短语后，您必须立即下载新的恢复软件包。通过恢复包文件，您可以在发生故障时还原系统。

更改节点控制台密码

网格中的每个节点都有一个唯一的节点控制台密码，您需要使用该密码登录到该节点。按照以下步骤更改网格中每个节点的每个唯一节点控制台密码。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有维护或 root 访问权限。
- 您具有当前配置密码短语。

关于此任务

使用节点控制台密码通过SSH以"admin"身份登录到节点、或者通过VM/物理控制台连接登录到root用户。更改节点控制台密码过程会为网格中的每个节点创建新密码、并将这些密码存储在更新的中 `Passwords.txt` 文件。密码将在 Passwords.txt 文件的 Password 列中列出。

> 用于节点间通信的 SSH 密钥具有单独的 SSH 访问密码。此操作步骤 不会更改SSH访问密码。

访问向导

步骤

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

输入配置密码短语

步骤

1. 输入网格的配置密码短语。
2. 选择 * 继续 * 。

[[download-current]]下载当前恢复软件包

在更改节点控制台密码之前、请下载当前恢复软件包。如果任何节点的密码更改过程失败、您可以使用此文件中的密码。

步骤

1. 选择 * 下载恢复包 * 。

2. 复制恢复软件包文件 (`.zip`)连接到两个安全、安全和独立的位置。

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

3. 选择 * 继续 * 。
4. 出现确认对话框时、如果您已准备好开始更改节点控制台密码、请选择*是*。

   此过程启动后、您无法取消。

更改节点控制台密码

当节点控制台密码过程启动时、将生成一个包含新密码的新恢复软件包。然后、在每个节点上更新密码。

步骤

1. 等待生成新的恢复软件包、这可能需要几分钟时间。
2. 选择 * 下载新恢复包 * 。
3. 下载完成后：

   a. 打开 `.zip` 文件

   b. 确认您可以访问内容、包括 `Passwords.txt` 文件、其中包含新的节点控制台密码。

   c. 复制新的恢复软件包文件 (`.zip`)连接到两个安全、安全和独立的位置。

   > 请勿覆盖旧恢复软件包。

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

4. 选中此复选框以指示您已下载新的恢复软件包并验证其内容。
5. 选择*更改节点控制台密码*、然后等待所有节点使用新密码进行更新。这可能需要几分钟时间。

   如果所有节点的密码均已更改，则会显示一个绿色的成功横幅。继续执行下一步。

   如果更新过程中出现错误，则会显示一条横幅消息，列出无法更改密码的节点数。系统将在任何无法更改密码的节点上自动重试此过程。如果此过程结束时某些节点仍没有更改密码，则会显示 * 重试 * 按钮。

   如果一个或多个节点的密码更新失败：

   a. 查看表中列出的错误消息。

   b. 解决问题。

   c. 选择 * 重试 * 。

   > 重试仅会更改先前尝试更改密码期间失败的节点上的节点控制台密码。

6. 更改所有节点的节点控制台密码后、请删除 您下载的第一个恢复软件包。
7. (可选)使用*恢复包*链接下载新恢复包的附加副本。

使用身份联合

使用身份联合可以加快设置组和用户的速度，并允许用户使用熟悉的凭据登录到 StorageGRID 。

为 **Grid Manager** 配置身份联合

如果您希望在 Active Directory ， Azure Active Directory （Azure AD ）， OpenLDAP 或 Oracle Directory Server 等其他系统中管理管理管理组和用户，则可以在网格管理器中配置身份联合。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。
- 您正在使用 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

> 如果要使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP ，则必须配置 OpenLDAP 服务器。请参见 配置 OpenLDAP 服务器的准则。
- 如果您计划启用单点登录（SSO），则已查看 "单点登录的要求和注意事项"。
- 如果您计划使用传输层安全（Transport Layer Security， TLS）与 LDAP 服务器进行通信，则身份提供程序正在使用 TLS 1.2 或 1.3 。请参见 "支持传出 TLS 连接的密码"。

关于此任务

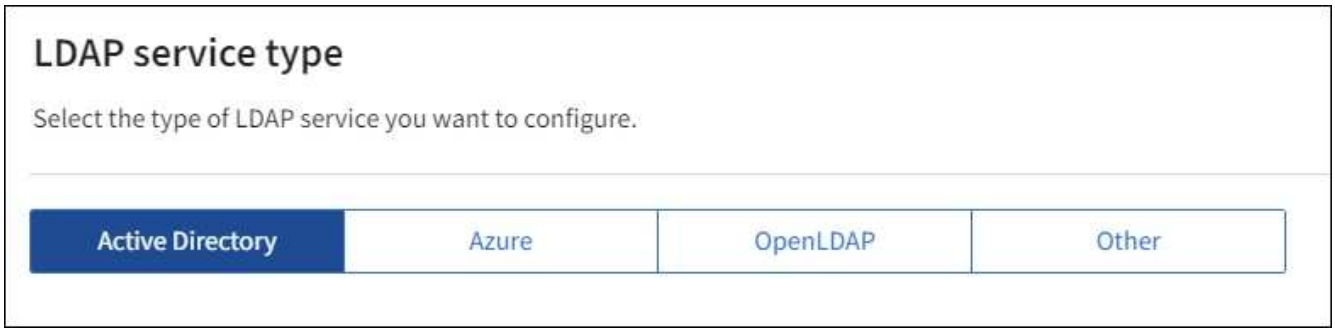
如果要从 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 等其他系统导入组，则可以为网格管理器配置身份源。您可以导入以下类型的组：

- 管理组。管理组中的用户可以登录到网格管理器并根据分配给该组的管理权限执行任务。
- 不使用自己的身份源的租户的租户用户组。租户组中的用户可以登录到租户管理器，并根据在租户管理器中为该组分配的权限执行任务。请参见 "创建租户帐户" 和 "使用租户帐户" 了解详细信息。

输入配置

步骤

1. 选择 * 配置 * > * 访问控制 * > * 身份联合 * 。
2. 选择 * 启用身份联合 * 。
3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - * 用户唯一名称 * ： 包含 LDAP 用户唯一标识符的属性的名称。此属性等效于 `sAMAccountName` 适用于Active Directory和 `uid` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `uid`。
   - * 用户 UID* ： 包含 LDAP 用户的永久唯一标识符的属性的名称。此属性等效于 `objectGUID` 适用于Active Directory和 `entryUUID` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `nsuniqueid`。每个用户在指定属性中的值都必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
   - * 组唯一名称 * ： 包含 LDAP 组唯一标识符的属性的名称。此属性等效于 `sAMAccountName` 适用于Active Directory和 `cn` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `cn`。
   - * 组 UID* ： 包含 LDAP 组的永久唯一标识符的属性的名称。此属性等效于 `objectGUID` 适用于Active Directory和 `entryUUID` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `nsuniqueid`。每个组在指定属性中的值必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
5. 对于所有 LDAP 服务类型，请在配置 LDAP 服务器部分中输入所需的 LDAP 服务器和网络连接信息。
   - * 主机名 * ： LDAP 服务器的完全限定域名 （ FQDN ）或 IP 地址。
   - * 端口 * ： 用于连接到 LDAP 服务器的端口。

     > STARTTLS 的默认端口为 389 ， LDAPS 的默认端口为 636 。但是，只要防火墙配置正确，您就可以使用任何端口。

   - * 用户名 * ： 要连接到 LDAP 服务器的用户的可分辨名称 （ DN ）的完整路径。

     对于 Active Directory ，您还可以指定低级别的登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

     - `sAMAccountName` 或 `uid`
     - `objectGUID`， `entryUUID``或 `nsuniqueid`
     - `cn`
     - `memberOf` 或 `isMemberOf`
     - **Active Directory**： `objectSid`， `primaryGroupID`， `userAccountControl`，和 `userPrincipalName`
     - * Azure *： `accountEnabled` 和 `userPrincipalName`
   - * 密码 * ： 与用户名关联的密码。
   - * 组基本 DN* ： 要搜索组的 LDAP 子树的可分辨名称 （ DN ）的完整路径。在 Active Directory 示例 （如下）中，可分辨名称相对于基础 DN （ DC=storagegrid ， DC=example ， DC=com ）的所有组均可用作联合组。

     > * 组唯一名称 * 值在其所属的 * 组基本 DN* 中必须是唯一的。

   - * 用户基础 DN* ： 要搜索用户的 LDAP 子树的可分辨名称 （ DN ）的完整路径。

> 用户唯一名称 * 值在其所属的 * 用户基础 DN* 中必须是唯一的。

- 绑定用户名格式(可选)：如果无法自动确定模式，StorageGRID 应使用默认用户名模式。

  建议提供 * 绑定用户名格式 * ，因为如果 StorageGRID 无法绑定到服务帐户，它可以允许用户登录。

  输入以下模式之一：

  - **UserPrincipalName模式(Active Directory和Azure)**： `[USERNAME]@example.com`
  - 低级登录名称模式**(Active Directory和Azure)**： `example\[USERNAME]`
  - 可分辨名称模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   - * 使用 STARTTLS * ： 使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是建议的 Active Directory ， OpenLDAP 或其他选项，但 Azure 不支持此选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。您必须为 Azure 选择此选项。
   - * 请勿使用 TLS* ： StorageGRID 系统与 LDAP 服务器之间的网络流量将不会受到保护。Azure 不支持此选项。

   > 如果 Active Directory 服务器强制实施 LDAP 签名，则不支持使用 * 不使用 TLS* 选项。您必须使用 STARTTLS 或 LDAPS 。

7. 如果选择 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认网格 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义安全证书。

     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

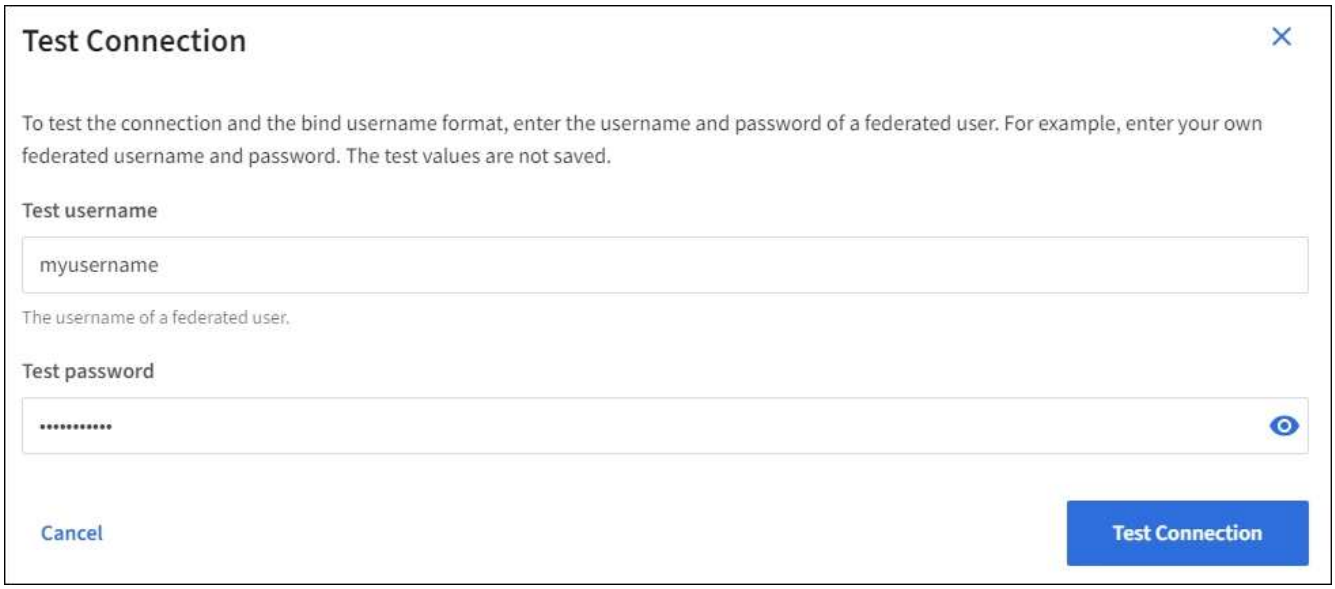
测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

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` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效，则会显示 "`test connection could not be established` " 消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

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



- 如果连接设置有效，则会显示 "`Test connection successful` " 消息。选择 * 保存 * 以保存配置。
- 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到身份联合页面。
2. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   > 如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以临时或永久禁用组和用户的身份联合。禁用身份联合后， StorageGRID 与身份源之间不会进行通信。但是，您配置的任何设置都将保留下来，以便将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，并且不会为尚未同步的帐户发出警报或警报。
- 如果单点登录(SSO)设置为*Enabled"或*Sandbox Mode*，则*启用身份联合*复选框将被禁用。在禁用身份

联合之前，单点登录页面上的 SSO 状态必须为 * 已禁用 * 。请参见 "禁用单点登录"。

步骤

1. 转到身份联合页面。
2. 取消选中*启用身份联合*复选框。

配置 **OpenLDAP** 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于非ActiveDirectory或Azure身份源、StorageGRID 不会自动阻止外部禁用的用户进行S3访问。要阻止S3访问、请删除此用户的任何S3密钥或从所有组中删除此用户。

memberOf 和 **fint** 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

管理管理组

您可以创建管理组来管理一个或多个管理员用户的安全权限。用户必须属于要授予对 StorageGRID 系统访问权限的组。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

创建管理组

通过管理组，您可以确定哪些用户可以访问网格管理器和网格管理 API 中的哪些功能和操作。

访问向导

步骤

1. 选择 * 配置 * > * 访问控制 * > * 管理组 * 。
2. 选择 * 创建组 * 。

选择组类型

您可以创建本地组或导入联合组。

- 如果要为本地用户分配权限，请创建本地组。
- 创建联合组以从身份源导入用户。

本地组

步骤

1. 选择 * 本地组 * 。
2. 输入组的显示名称，您可以稍后根据需要更新该名称。例如， " M维护用户 " 或 "`ILM 管理员。`
3. 输入组的唯一名称、此名称以后无法更新。
4. 选择 * 继续 * 。

联合组

步骤

1. 选择 * 联合组 * 。
2. 输入要导入的组的名称，与此名称在配置的身份源中显示的名称完全相同。
   - 对于 Active Directory 和 Azure ，请使用 sAMAccountName 。
   - 对于 OpenLDAP ，请使用 CN （公用名）。
   - 对于另一个 LDAP ，请为 LDAP 服务器使用适当的唯一名称。
3. 选择 * 继续 * 。

管理组权限

步骤

1. 对于 * 访问模式 * ，选择组中的用户是否可以在网格管理器和网格管理 API 中更改设置并执行操作，或者选择他们是否只能查看设置和功能。
   - * 读写 * （默认）： 用户可以更改其管理权限允许的设置并执行这些操作。
   - * 只读 * ： 用户只能查看设置和功能。他们无法在网格管理器或网格管理API中进行任何更改或执行任何操作。本地只读用户可以更改自己的密码。

     如果用户属于多个组，并且任何组设置为 * 只读 * ，则用户将对所有选定设置和功能具有只读访问权限。

2. 选择一个或多个 "管理员组权限"。

您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到 StorageGRID 。

3. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

步骤

1. 或者，为此组选择一个或多个本地用户。

   如果尚未创建本地用户，则可以保存此组，而无需添加用户。您可以在用户页面上将此组添加到用户。请参见"管理用户" 了解详细信息。

2. 选择 * 创建组 * 和 * 完成 * 。

查看和编辑管理组

您可以查看现有组的详细信息，修改组或复制组。

- 要查看所有组的基本信息，请查看组页面上的表。
- 要查看特定组的所有详细信息或编辑组，请使用 * 操作 * 菜单或详细信息页面。

任务	操作菜单	详细信息页面
查看组详细信息	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。	在表中选择组名称。
编辑显示名称（仅限本地组）	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 编辑组名称 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存更改 * 。
编辑访问模式或权限	a. 选中组对应的复选框。 b. 选择 * 操作 * > * 查看组详细信息 * 。 c. 也可以更改组的访问模式。 d. (可选)选择或清除 "管理员组权限"。 e. 选择 * 保存更改 * 。	a. 选择组名称以显示详细信息。 b. 也可以更改组的访问模式。 c. (可选)选择或清除 "管理员组权限"。 d. 选择 * 保存更改 * 。

复制组

步骤

1. 选中组对应的复选框。
2. 选择 * 操作 * > * 复制组 * 。
3. 完成复制组向导。

删除组

如果要从系统中删除某个管理组，则可以删除该组，并删除与该组关联的所有权限。删除管理员组会从组中删除任何用户，但不会删除这些用户。

步骤

1. 在组页面中、选中要删除的每个组对应的复选框。
2. 选择 * 操作 * > * 删除组 * 。
3. 选择 * 删除组 * 。

管理组权限

创建管理员用户组时，您可以选择一个或多个权限来控制对网格管理器特定功能的访问。然后，您可以将每个用户分配给一个或多个管理组，以确定用户可以执行的任务。

您必须为每个组至少分配一个权限；否则，属于该组的用户将无法登录到网格管理器或网格管理 API 。

默认情况下，属于至少具有一个权限的组的任何用户均可执行以下任务：

- 登录到网格管理器
- 查看信息板
- 查看节点页面
- 监控网格拓扑
- 查看当前警报和已解决警报
- 查看当前和历史警报（旧系统）
- 更改自己的密码（仅限本地用户）
- 查看配置和维护页面上提供的某些信息

权限与访问模式之间的交互

对于所有权限，组的 * 访问模式 * 设置将确定用户是否可以更改设置并执行操作，或者是否只能查看相关设置和功能。如果用户属于多个组，并且任何组设置为 * 只读 * ，则用户将对所有选定设置和功能具有只读访问权限。

以下各节介绍了在创建或编辑管理组时可以分配的权限。未明确提及的任何功能都需要具有 * 根访问权限 * 。

root 访问权限

通过此权限，可以访问所有网格管理功能。

确认警报（传统）

此权限可用于确认和响应警报（旧系统）。所有已登录用户均可查看当前和历史警报。

如果您希望用户仅监控网格拓扑并确认警报，则应分配此权限。

更改租户 **root** 密码

通过此权限，您可以访问租户页面上的 * 更改 root 密码 * 选项，从而可以控制谁可以更改租户的本地 root 用户的密码。启用 S3 密钥导入功能后，此权限也用于迁移 S3 密钥。没有此权限的用户看不到*更改root密码*选项。

> 要授予对包含 * 更改 root 密码 * 选项的租户页面的访问权限，还需要分配 * 租户帐户 * 权限。

网格拓扑页面配置

通过此权限，您可以访问 * 支持 * > * 工具 * > * 网格拓扑 * 页面上的配置选项卡。

ILM

通过此权限，您可以访问以下 * ILM * 菜单选项：

- rules
- 策略
- 纠删编码
- regions
- 存储池

> 用户必须具有 * 其他网格配置 * 和 * 网格拓扑页面配置 * 权限才能管理存储级别。

维护

用户必须具有维护权限才能使用以下选项：

- * 配置 * > * 访问控制 * ：
  - 网格密码
- * 配置 * > * 网络 * ：
  - S3端点域名
- * 维护 * > * 任务 * ：
  - 停用
  - 扩展
  - 对象存在检查
  - 恢复
- * 维护 * > * 系统 * ：
  - 恢复包
  - 软件更新
- * 支持 * > * 工具 * ：
  - 日志

没有维护权限的用户可以查看但不能编辑以下页面：

- * 维护 * > * 网络 * ：
  - DNS 服务器
  - 网格网络
  - NTP 服务器
- * 维护 * > * 系统 * ：
  - 许可证
- * 配置 * > * 网络 * ：
  - S3端点域名
- * 配置 * > * 安全性 * ：
  - 证书
- * 配置 * > * 监控 * ：
  - 审核和系统日志服务器

管理警报

通过此权限，您可以访问用于管理警报的选项。用户必须具有此权限才能管理静音，警报通知和警报规则。

指标查询

此权限提供对以下内容的访问权限：

- **support**>*Tools*>*Metrics *页面
- 使用网格管理API的*Metrics*部分自定义Prometheus指标查询
- 包含指标的Grid Manager信息板卡

对象元数据查找

通过此权限，您可以访问 * ILM * > * 对象元数据查找 * 页面。

其他网格配置

通过此权限可以访问其他网格配置选项。

> 要查看这些附加选项，用户还必须具有 * 网格拓扑页面配置 * 权限。

- * ILM ：
  - 存储等级
- * 配置 * > * 系统 * ：
  - 存储选项
- * 支持 * > * 警报（传统） * ：

    - 自定义事件
    - 全局警报
    - 传统电子邮件设置
- 支持>*其他*：
    - 链路成本

存储设备管理员

通过此权限，您可以通过网格管理器访问存储设备上的 E 系列 SANtricity 系统管理器。

租户帐户

此权限可用于：

- 访问租户页面、在此可以创建、编辑和删除租户帐户
- 查看现有流量分类策略
- 查看包含租户详细信息的Grid Manager信息板卡

管理用户

您可以查看本地用户和联合用户。您还可以创建本地用户并将其分配给本地管理组，以确定这些用户可以访问哪些网格管理器功能。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

创建本地用户

您可以创建一个或多个本地用户，并将每个用户分配给一个或多个本地组。组的权限控制用户可以访问的网格管理器和网格管理 API 功能。

您只能创建本地用户。使用外部身份源管理联合用户和组。

网格管理器包括一个预定义的本地用户、名为"`root.`" 您无法删除root用户。

> 如果启用了单点登录(SSO)、则本地用户无法登录到StorageGRID。

访问向导

步骤

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

输入用户凭据

步骤

1. 输入用户的全名，唯一用户名和密码。
2. 或者，如果此用户不应访问网格管理器或网格管理 API ，请选择 * 是 * 。
3. 选择 * 继续 * 。

分配给组

步骤

1. （可选）将用户分配给一个或多个组以确定用户的权限。

   如果尚未创建组，则可以保存用户而不选择组。您可以在组页面上将此用户添加到组中。

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

2. 选择 * 创建用户 * 并选择 * 完成 * 。

查看和编辑本地用户

您可以查看现有本地用户和联合用户的详细信息。您可以修改本地用户以更改用户的全名，密码或组成员资格。您还可以暂时阻止用户访问网格管理器和网格管理 API 。

您只能编辑本地用户。使用外部身份源管理联合用户。

- 要查看所有本地和联合用户的基本信息，请查看用户页面上的表。
- 要查看特定用户的所有详细信息，编辑本地用户或更改本地用户的密码，请使用 * 操作 * 菜单或详细信息页面。

  用户下次注销后重新登录到网格管理器时，系统将应用任何编辑。

  本地用户可以使用网格管理器横幅中的*更改密码*选项更改自己的密码。

任务	操作菜单	详细信息页面
查看用户详细信息	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。	在表中选择用户名。
编辑全名（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 编辑全名 * 。 c. 输入新名称。 d. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存更改 * 。

任务	操作菜单	详细信息页面
拒绝或允许 StorageGRID 访问	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择访问选项卡。 d. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 e. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择访问选项卡。 c. 选择 * 是 * 以防止用户登录到网格管理器或网格管理 API ，或者选择 * 否 * 以允许用户登录。 d. 选择 * 保存更改 * 。
更改密码（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择密码选项卡。 d. 输入新密码。 e. 选择 * 更改密码 * 。	a. 选择用户的名称以显示详细信息。 b. 选择密码选项卡。 c. 输入新密码。 d. 选择 * 更改密码 * 。
更改组（仅限本地用户）	a. 选中用户对应的复选框。 b. 选择 * 操作 * > * 查看用户详细信息 * 。 c. 选择组选项卡。 d. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 e. 选择 * 编辑组 * 以选择不同的组。 f. 选择 * 保存更改 * 。	a. 选择用户的名称以显示详细信息。 b. 选择组选项卡。 c. 也可以选择组名称后面的链接，以便在新的浏览器选项卡中查看组的详细信息。 d. 选择 * 编辑组 * 以选择不同的组。 e. 选择 * 保存更改 * 。

复制用户

您可以复制现有用户以创建具有相同权限的新用户。

步骤

1. 选中用户对应的复选框。
2. 选择 * 操作 * > * 复制用户 * 。
3. 完成复制用户向导。

删除用户

您可以删除本地用户，以便从系统中永久删除该用户。

> 您不能删除root用户。

步骤

1. 在用户页面中、选中要删除的每个用户对应的复选框。
2. 选择 * 操作 * > * 删除用户 * 。
3. 选择 * 删除用户 * 。

使用单点登录（ **SSO** ）

配置单点登录

启用单点登录（ SSO ）后，只有在用户凭据通过贵组织实施的 SSO 登录过程获得授权的情况下，用户才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用户无法登录到StorageGRID。

单点登录的工作原理

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

在启用单点登录（ SSO ）之前，请查看启用 SSO 后 StorageGRID 登录和注销过程会受到什么影响。

启用 **SSO** 后登录

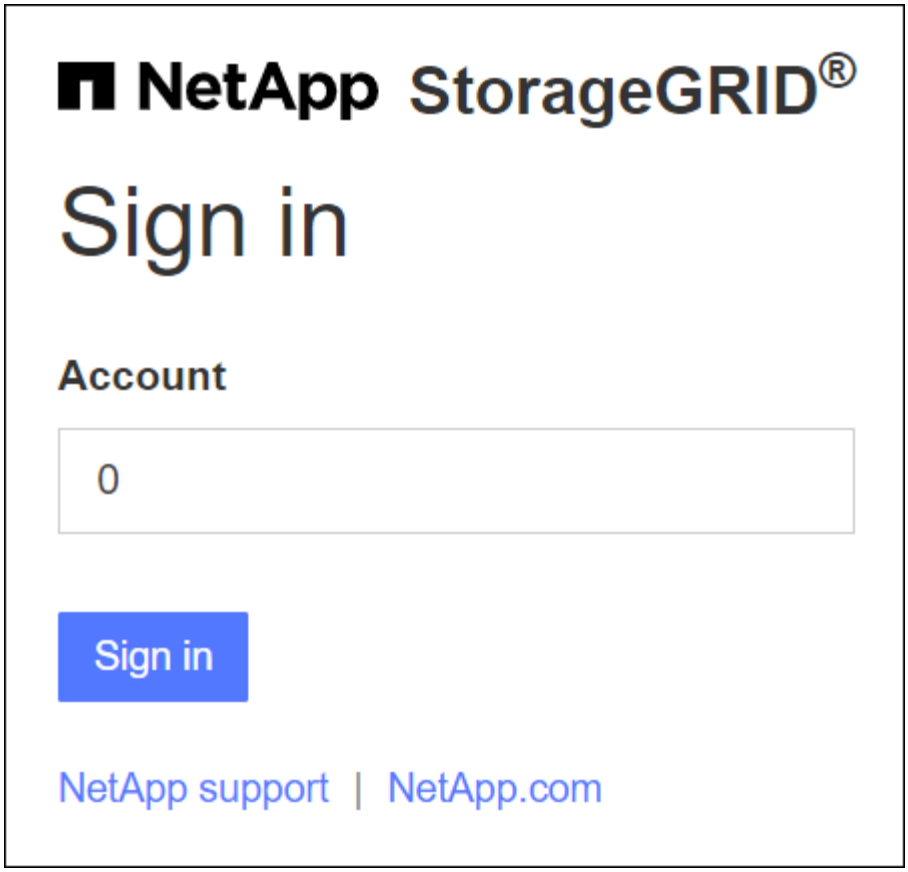
启用 SSO 并登录到 StorageGRID 后，系统会将您重定向到组织的 SSO 页面以验证您的凭据。

步骤

1. 在 Web 浏览器中输入任何 StorageGRID 管理节点的完全限定域名或 IP 地址。

   此时将显示 StorageGRID 登录页面。

   - 如果这是您首次在此浏览器上访问此 URL ，系统将提示您输入帐户 ID ：

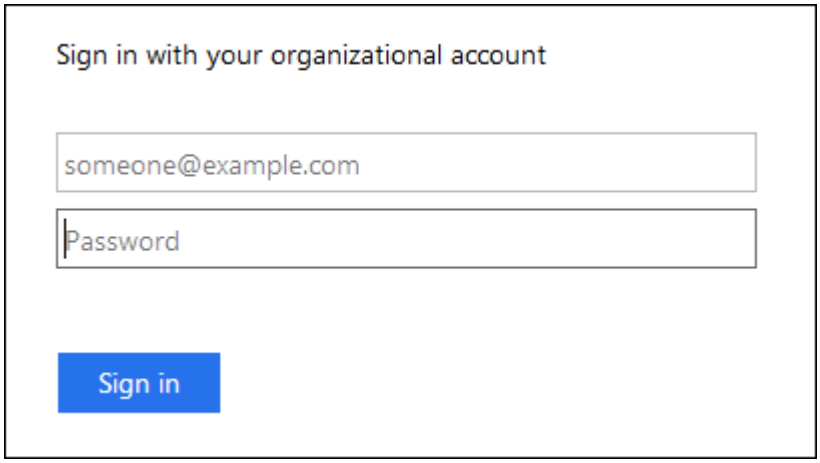


- 如果您之前访问过网格管理器或租户管理器，系统将提示您选择最近的帐户或输入帐户 ID：

> 输入租户帐户的完整URL (即、完全限定域名或IP地址后跟)时、不会显示StorageGRID 登录页面 `/?accountId=20-digit-account-id`）。而是会立即重定向到您所在组织的 SSO 登录页面，您可以在该页面上进行登录 使用您的 SSO 凭据登录。

2. 指示您是要访问网格管理器还是租户管理器：
   - 要访问网格管理器，请将 * 帐户 ID* 字段留空，输入 * 0 * 作为帐户 ID ，或者选择 * 网格管理器 * （如果它显示在近期帐户列表中）。
   - 要访问租户管理器，请输入 20 位租户帐户 ID ，或者如果某个租户显示在近期帐户列表中，则按名称选择此租户。
3. 选择 * 登录 *

   StorageGRID 会将您重定向到贵组织的 SSO 登录页面。例如：



4. 【签名 _sso]] 使用您的 SSO 凭据登录。

   如果您的 SSO 凭据正确：

   a. 身份提供程序（ IdP ）为 StorageGRID 提供身份验证响应。
   b. StorageGRID 将验证身份验证响应。
   c. 如果响应有效，并且您属于具有 StorageGRID 访问权限的联合组，则您将登录到网格管理器或租户管理器，具体取决于您选择的帐户。

   > ⓘ 如果此服务帐户不可访问，则只要您是具有 StorageGRID 访问权限的联合组的现有用户，您仍可登录。

5. 或者，如果您拥有足够的权限，也可以访问其他管理节点，或者访问网格管理器或租户管理器。

   您无需重新输入SSO凭据。

启用 **SSO** 后注销

为 StorageGRID 启用 SSO 后，注销时会发生什么情况取决于您登录到的内容以及注销的位置。

步骤

1. 在用户界面右上角找到*Sign Out (注销)*链接。
2. 选择*注销*。

   此时将显示 StorageGRID 登录页面。更新了 * 近期帐户 * 下拉列表，其中包含 * 网格管理器 * 或租户名称，

以便您将来可以更快地访问这些用户界面。

如果您已登录到 ...	您可以从以下位置注销 ...	您已注销 ...
一个或多个管理节点上的网格管理器	任何管理节点上的网格管理器	所有管理节点上的网格管理器 • 注意： * 如果您使用 Azure 进行 SSO ，则从所有管理节点中注销可能需要几分钟的时间。
一个或多个管理节点上的租户管理器	任何管理节点上的租户管理器	所有管理节点上的租户管理器
网格管理器和租户管理器	网格管理器	仅限网格管理器。您还必须注销租户管理器才能注销 SSO 。

下表总结了在使用单个浏览器会话时注销时会发生的情况。如果您通过多个浏览器会话登录到 StorageGRID ，则必须单独注销所有浏览器会话。

单点登录的要求和注意事项

在为StorageGRID 系统启用单点登录(Single Sign On、SSO)之前、请查看相关要求和注意事项。

身份提供程序要求

StorageGRID 支持以下 SSO 身份提供程序（ IdP ）：

- Active Directory 联合身份验证服务（ AD FS ）
- Azure Active Directory （ Azure AD ）
- PingFederate

您必须先为 StorageGRID 系统配置身份联合，然后才能配置 SSO 身份提供程序。用于身份联合的 LDAP 服务类型控制您可以实施的 SSO 类型。

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

AD FS 要求

您可以使用以下任意版本的 AD FS：

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 应使用 "KB3201845 更新"或更高版本。

- AD FS 3.0 ，随 Windows Server 2012 R2 更新或更高版本提供。

其他要求

- 传输层安全（ Transport Layer Security ， TLS ） 1.2 或 1.3
- Microsoft .NET Framework 3.5.1 或更高版本

Azure注意事项

如果您使用Azure作为SSO类型、并且用户的用户主体名称未使用sAMAccountName作为前缀、则在StorageGRID 与LDAP服务器断开连接时可能会出现登录问题。要允许用户登录、您必须还原与LDAP服务器的连接。

服务器证书要求

默认情况下， StorageGRID 会在每个管理节点上使用管理接口证书来保护对网格管理器，租户管理器，网格管理 API 和租户管理 API 的访问。在为 StorageGRID 配置依赖方信任（ AD FS ），企业应用程序（ Azure ）或服务提供商连接（ PingFederate ）时，您可以使用服务器证书作为 StorageGRID 请求的签名证书。

如果您尚未执行此操作 "已为管理接口配置自定义证书"，您现在应执行此操作。安装自定义服务器证书时，该证书将用于所有管理节点，您可以在所有 StorageGRID 依赖方信任关系，企业应用程序或 SP 连接中使用该证书。

> 建议不要在依赖方信任，企业应用程序或 SP 连接中使用管理节点的默认服务器证书。如果节点发生故障而您恢复了该节点，则会生成一个新的默认服务器证书。在登录到已恢复的节点之前，您必须使用新证书更新依赖方信任，企业应用程序或 SP 连接。

您可以通过登录到管理节点的命令Shell并转到来访问管理节点的服务器证书 `/var/local/mgmt-api` 目录。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

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。请参见 "在外部防火墙处控制访问"。

确认联合用户可以登录

在启用单点登录（ SSO ）之前，您必须确认至少有一个联合用户可以登录到网格管理器以及任何现有租户帐户的租户管理器。

开始之前

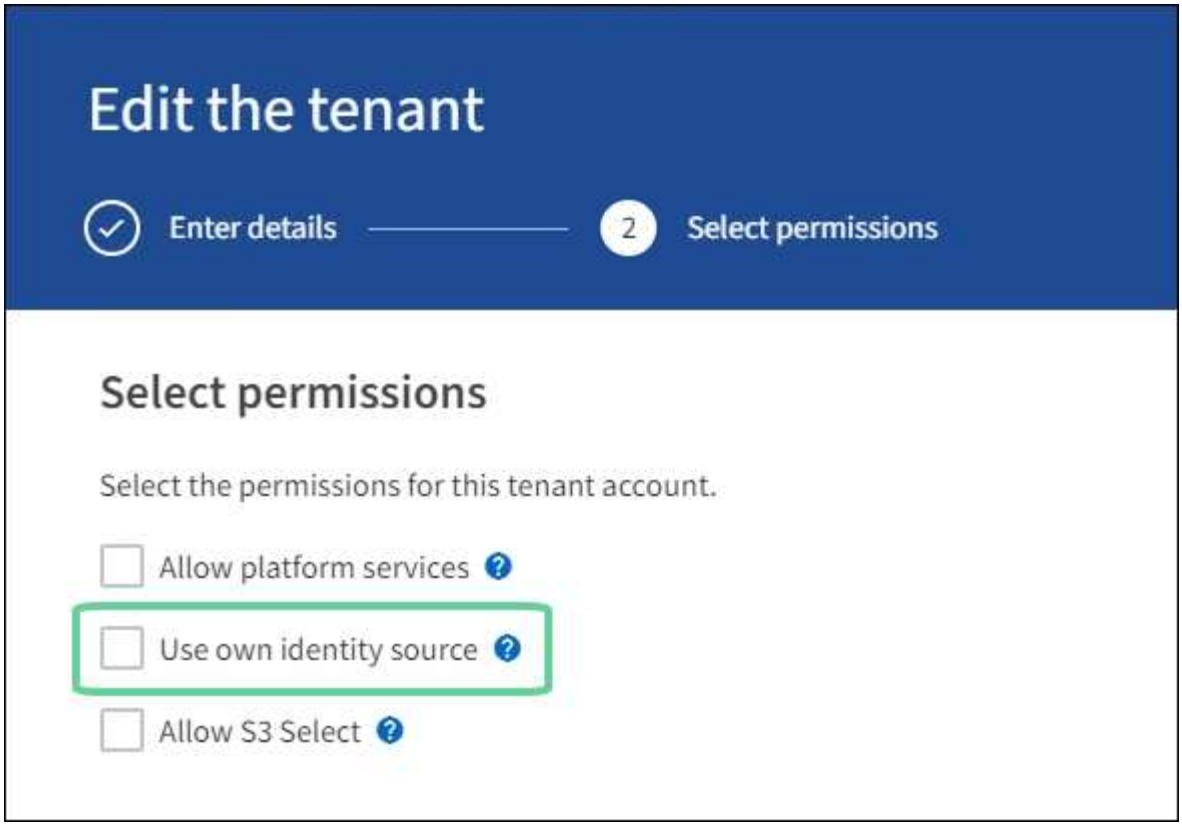
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。
- 您已配置身份联合。

步骤

1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

> 启用 SSO 后，在租户管理器中配置的身份源将被网格管理器中配置的身份源覆盖。属于租户身份源的用户将无法再登录，除非他们拥有网格管理器身份源帐户。

   a. 登录到每个租户帐户的租户管理器。
   b. 选择 * 访问管理 * > * 身份联合 * 。
   c. 确认未选中*启用身份联合*复选框。
   d. 如果是、请确认不再需要此租户帐户可能正在使用的任何联盟组、清除此复选框、然后选择*保存*。
2. 确认联合用户可以访问网格管理器：
   a. 在网格管理器中，选择 * 配置 * > * 访问控制 * > * 管理组 * 。
   b. 确保已从 Active Directory 身份源导入至少一个联合组，并已为其分配 root 访问权限。
   c. 注销。
   d. 确认您可以以联合组中的用户身份重新登录到网格管理器。
3. 如果存在现有租户帐户，请确认具有 root 访问权限的联合用户可以登录：
   a. 在网格管理器中，选择 * 租户 * 。
   b. 选择租户帐户，然后选择 * 操作 * > * 编辑 * 。
   c. 在输入详细信息选项卡上，选择 * 继续 * 。
   d. 如果选中了*使用自己的身份源*复选框，请取消选中该复选框并选择*保存*。



此时将显示租户页面。

a. 选择租户帐户，选择 * 登录 * ，然后以本地 root 用户身份登录到租户帐户。
b. 在租户管理器中，选择 * 访问管理 * > * 组 * 。
c. 确保至少已为此租户为网格管理器中的一个联合组分配 root 访问权限。
d. 注销。
e. 确认您可以以联盟组中的用户身份重新登录到租户。

相关信息

- "单点登录的要求和注意事项"
- "管理管理组"
- "使用租户帐户"

使用沙盒模式

在为所有 StorageGRID 用户启用单点登录（SSO）之前，您可以使用沙盒模式配置和测试单点登录（SSO）。启用 SSO 后，您可以在需要更改或重新测试配置时返回到沙盒模式。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。
- 您已为 StorageGRID 系统配置身份联合。

- 对于身份联合 * LDAP 服务类型 * ，您根据计划使用的 SSO 身份提供程序选择了 Active Directory 或 Azure 。

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

关于此任务

启用 SSO 后，如果用户尝试登录到管理节点，则 StorageGRID 会向 SSO 身份提供程序发送身份验证请求。然后， SSO 身份提供程序会向 StorageGRID 发回身份验证响应，指示身份验证请求是否成功。对于成功的请求：

- Active Directory 或 PingFederate 的响应包括用户的通用唯一标识符（ UUID ）。
- Azure 的响应包括用户主体名称（ UPN ）。

要允许 StorageGRID （服务提供商）和 SSO 身份提供程序就用户身份验证请求进行安全通信，您必须在 StorageGRID 中配置某些设置。接下来，您必须使用 SSO 身份提供程序的软件为每个管理节点创建依赖方信任（ AD FS ），企业应用程序（ Azure ）或服务提供商（ PingFederate ）。最后，您必须返回到 StorageGRID 以启用 SSO 。

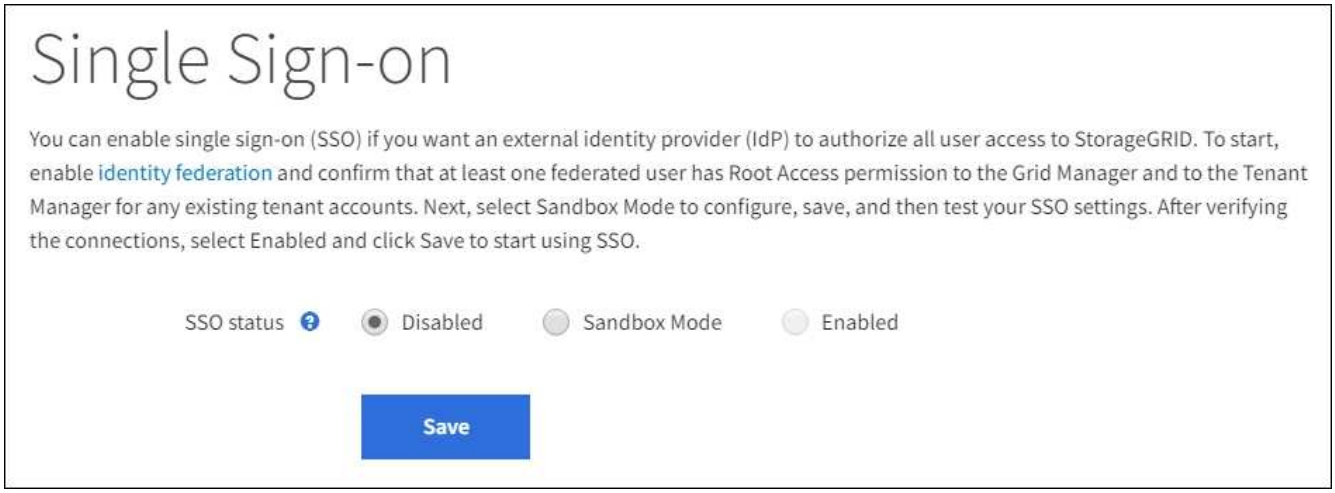
使用沙盒模式，可以轻松执行此背面配置，并在启用 SSO 之前测试所有设置。使用沙盒模式时、用户无法使用SSO登录。

访问沙盒模式

步骤

1. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。

   此时将显示 Single Sign-On 页面，并选择 * 已禁用 * 选项。



> 如果未显示SSO状态选项、请确认已将身份提供程序配置为联合身份源。请参见 "单点登录的要求和注意事项"。

2. 选择 * 沙盒模式 * 。

   此时将显示 "Identity Provider" 部分。

输入身份提供程序详细信息

步骤

1. 从下拉列表中选择 * SSO 类型 * 。
2. 根据您选择的 SSO 类型填写身份提供程序部分中的字段。

Active Directory

1. 输入身份提供程序的 * 联合服务名称 * ，与 Active Directory 联合身份验证服务（AD FS）中显示的名称完全相同。

> 要查找联合服务名称，请转到 Windows Server Manager 。选择 * 工具 * > * AD FS 管理 * 。从操作菜单中，选择 * 编辑联合身份验证服务属性 * 。联合服务名称显示在第二个字段中。

2. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。
3. 在依赖方部分中，指定 StorageGRID 的 * 依赖方标识符 * 。此值控制 AD FS 中每个依赖方信任所使用的名称。
   - 例如、如果您的网格只有一个管理节点、并且您不希望将来添加更多管理节点、请输入 `SG` 或 `StorageGRID`。
   - 如果网格包含多个管理节点、请包含字符串 `[HOSTNAME]` 在标识符中。例如： `SG-[HOSTNAME]`。此时将生成一个表，其中根据节点的主机名显示系统中每个管理节点的依赖方标识符。

> 您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

4. 选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

Azure 酒店

1. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 * ： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。
2. 在企业应用程序部分中，为 StorageGRID 指定 * 企业应用程序名称 * 。此值控制 Azure AD 中每个企业应用程序使用的名称。

- 例如、如果您的网格只有一个管理节点、并且您不希望将来添加更多管理节点、请输入 `SG` 或 `StorageGRID`。
- 如果网格包含多个管理节点、请包含字符串 `[HOSTNAME]` 在标识符中。例如： `SG-[HOSTNAME]`。此时将生成一个表，其中根据节点的主机名显示系统中每个管理节点的企业应用程序名称。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

3. 按照中的步骤进行操作 "在 Azure AD 中创建企业级应用程序" 为表中列出的每个管理节点创建企业级应用程序。
4. 从 Azure AD 中，复制每个企业应用程序的联合元数据 URL 。然后，将此 URL 粘贴到 StorageGRID 中相应的 * 联合元数据 URL* 字段中。
5. 复制并粘贴所有管理节点的联合元数据 URL 后，选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

PingFederate

1. 指定当身份提供程序响应 StorageGRID 请求发送 SSO 配置信息时，将使用哪个 TLS 证书来保护连接安全。
   - * 使用操作系统 CA 证书 *： 使用操作系统上安装的默认 CA 证书确保连接安全。
   - * 使用自定义 CA 证书 *： 使用自定义 CA 证书确保连接安全。

     如果选择此设置，请复制自定义证书的文本并将其粘贴到 * CA 证书 * 文本框中。

   - * 请勿使用 TLS*： 请勿使用 TLS 证书来保护连接。
2. 在服务提供商（ SP ）部分中，为 StorageGRID 指定 * SP 连接 ID* 。此值控制 PingFederate 中每个 SP 连接使用的名称。
   - 例如、如果您的网格只有一个管理节点、并且您不希望将来添加更多管理节点、请输入 `SG` 或 `StorageGRID`。
   - 如果网格包含多个管理节点、请包含字符串 `[HOSTNAME]` 在标识符中。例如： `SG-[HOSTNAME]`。此时将生成一个表，其中根据节点的主机名显示系统中每个管理节点的 SP 连接 ID 。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接。为每个管理节点建立 SP 连接可确保用户可以安全地登录和注销任何管理节点。

3. 在 * 联合元数据 URL* 字段中指定每个管理节点的联合元数据 URL 。

   请使用以下格式：

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

4. 选择 * 保存 * 。

   绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

配置依赖方信任，企业应用程序或 **SP** 连接

保存配置后，将显示沙盒模式确认通知。此通知用于确认沙盒模式现已启用，并提供了概述说明。

只要需要， StorageGRID 就可以保持沙盒模式。但是，如果在 Single Sign-On 页面上选择了 * 沙盒模式 * ，则所有 StorageGRID 用户都将禁用 SSO 。只有本地用户才能登录。

按照以下步骤配置依赖方信任（ Active Directory ），完整的企业应用程序（ Azure ）或配置 SP 连接（ PingFederate ）。

Active Directory

步骤

1. 转至 Active Directory 联合身份验证服务（AD FS）。
2. 使用 StorageGRID 单点登录页面上的表中所示的每个依赖方标识符为 StorageGRID 创建一个或多个依赖方信任。

   您必须为表中所示的每个管理节点创建一个信任。

   有关说明，请转至 "在 AD FS 中创建依赖方信任"。

Azure 酒店

步骤

1. 从当前登录到的管理节点的单点登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到节点。
   b. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 Azure 门户。
4. 按照中的步骤进行操作 "在 Azure AD 中创建企业级应用程序" 将每个管理节点的 SAML 元数据文件上传到其对应的 Azure 企业应用程序中。

PingFederate

步骤

1. 从当前登录到的管理节点的单点登录页面中，选择按钮以下载并保存 SAML 元数据。
2. 然后，对于网格中的任何其他管理节点，重复以下步骤：
   a. 登录到节点。
   b. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   c. 下载并保存该节点的 SAML 元数据。
3. 转到 PingFederate 。
4. "为 StorageGRID 创建一个或多个服务提供商（SP）连接"。使用每个管理节点的 SP 连接 ID （如 StorageGRID 单点登录页面上的表所示）以及为该管理节点下载的 SAML 元数据。

   您必须为表中所示的每个管理节点创建一个 SP 连接。

测试 **SSO** 连接

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

Active Directory

步骤

1. 在 StorageGRID 单点登录页面中，找到沙盒模式消息中的链接。

   此 URL 是从您在 * 联合服务名称 * 字段中输入的值派生的。

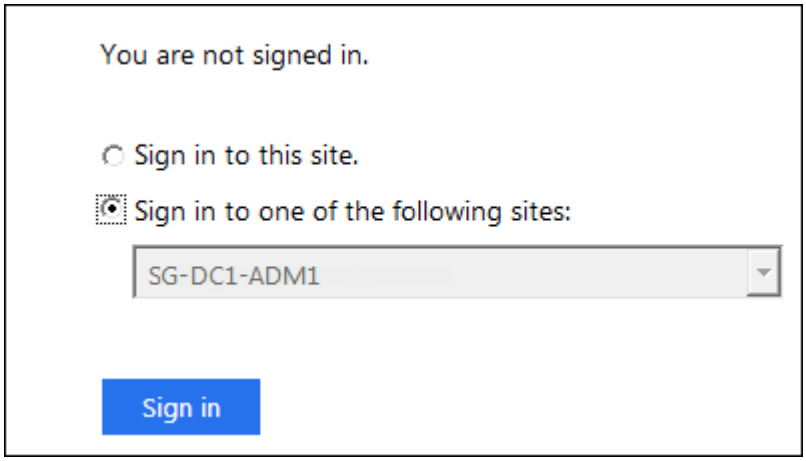
   Sandbox mode

   Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

   1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
   2. Go to your identity provider's sign-on page: https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm
   3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

   When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. 选择此链接，或者将此 URL 复制并粘贴到浏览器中，以访问身份提供程序的登录页面。
3. 要确认您可以使用 SSO 登录到 StorageGRID ，请选择 * 登录到以下站点之一 * ，选择主管理节点的依赖方标识符，然后选择 * 登录 * 。

4. 输入您的联合用户名和密码。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
5. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

Azure 酒店

步骤

1. 转到 Azure 门户中的单点登录页面。
2. 选择 * 测试此应用程序 * 。
3. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

     ✔ Single sign-on authentication and logout test completed successfully.

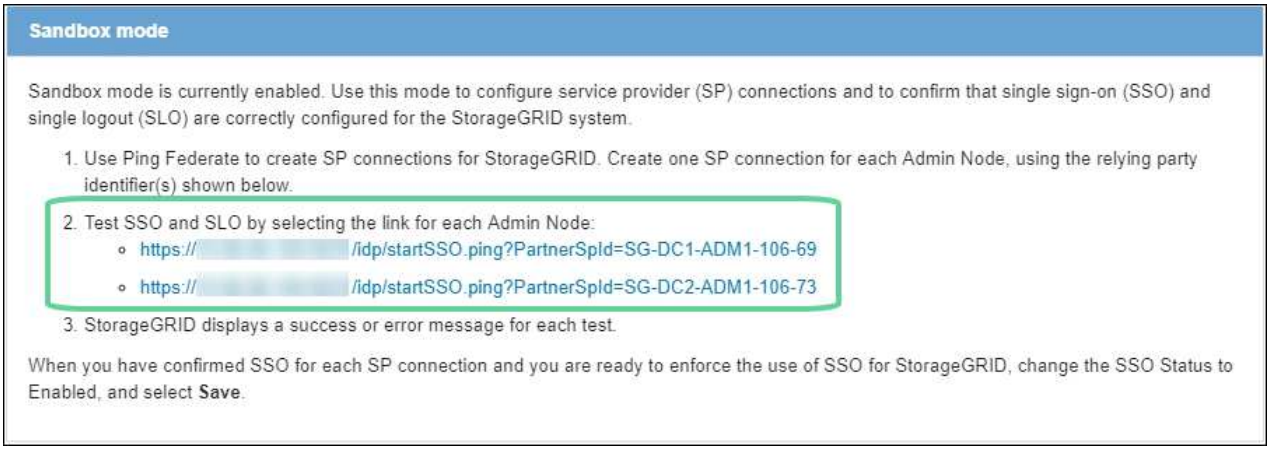
   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
4. 重复上述步骤，验证网格中每个管理节点的 SSO 连接。

PingFederate

步骤

1. 从 StorageGRID 单点登录页面中，选择沙盒模式消息中的第一个链接。

   一次选择并测试一个链路。

2. 输入联合用户的凭据。
   - 如果 SSO 登录和注销操作成功，则会显示一条成功消息。

     ✔ Single sign-on authentication and logout test completed successfully.

   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
3. 选择下一个链接以验证网格中每个管理节点的 SSO 连接。

   如果您看到页面已过期消息，请在浏览器中选择 * 返回 * 按钮，然后重新提交您的凭据。

启用单点登录

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

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

步骤

1. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
2. 将 SSO 状态更改为 * 已启用 * 。
3. 选择 * 保存 * 。
4. 查看警告消息，然后选择 * 确定 * 。

   现在，已启用单点登录。

如果您使用的是 Azure 门户，并且从用于访问 Azure 的同一计算机访问 StorageGRID ，请确保 Azure 门户用户也是授权的 StorageGRID 用户（已导入到 StorageGRID 的联合组中的用户） 或者，在尝试登录到 StorageGRID 之前，请先从 Azure 门户中注销。

在 **AD FS** 中创建依赖方信任

您必须使用 Active Directory 联合身份验证服务（ AD FS ）为系统中的每个管理节点创建依赖方信任。您可以使用 PowerShell 命令，从 StorageGRID 导入 SAML 元数据或手动输入数据来创建依赖方信任。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择了 * AD FS* 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 "使用沙盒模式"。
- 您知道系统中每个管理节点的完全限定域名（或 IP 地址）和依赖方标识符。您可以在 StorageGRID 单点登录页面上的管理节点详细信息表中找到这些值。

  您必须为 StorageGRID 系统中的每个管理节点创建依赖方信任。对每个管理节点拥有依赖方信任，可确保用户可以安全地登录和注销任何管理节点。

- 您有在 AD FS 中创建依赖方信任的经验，也可以访问 Microsoft AD FS 文档。
- 您正在使用 AD FS 管理单元，并且属于管理员组。
- 如果您要手动创建依赖方信任，则可以获得为 StorageGRID 管理界面上传的自定义证书，或者知道如何从命令 Shell 登录到管理节点。

关于此任务

以下说明适用于 Windows Server 2016 AD FS 。如果您使用的是其他版本的 AD FS ，则会注意到操作步骤 略有不同。如果您有任何疑问，请参见 Microsoft AD FS 文档。

使用 **Windows PowerShell** 创建依赖方信任

您可以使用 Windows PowerShell 快速创建一个或多个依赖方信任。

步骤

1. 从 Windows 开始菜单中，右键选择 PowerShell 图标，然后选择 * 以管理员身份运行 * 。

2. 在 PowerShell 命令提示符处，输入以下命令：

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
"https://Admin_Node_FQDN/api/saml-metadata"
```

   - 适用于 *Admin_Node_Identifier*`下、输入管理节点的依赖方标识符、与单点登录页面上显示的完全相同。例如： `SG-DC1-ADM1。
   - 适用于 `*Admin_Node_FQDN*`下、输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

3. 在 Windows Server Manager 中，选择 * 工具 * > * AD FS 管理 * 。

   此时将显示 AD FS 管理工具。

4. 选择 * AD FS* > * 依赖方信任 * 。

   此时将显示依赖方信任列表。

5. 向新创建的依赖方信任添加访问控制策略：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击信任，然后选择 * 编辑访问控制策略 * 。
   c. 选择访问控制策略。
   d. 选择 * 应用 * ，然后选择 * 确定 *
6. 将款项申请发放策略添加到新创建的相关方信任：
   a. 找到您刚刚创建的依赖方信任。
   b. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   c. 选择 * 添加规则 * 。
   d. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。
   e. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。

   f. 对于属性存储，选择 * Active Directory* 。
   g. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。
   h. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。
   i. 选择 * 完成 * ，然后选择 * 确定 * 。
7. 确认元数据已成功导入。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

      如果缺少元数据、请确认联盟元数据地址是否正确、或者手动输入值。

8. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

9. 完成后，返回到 StorageGRID 并测试所有相关方信任，以确认其配置正确。请参见 "使用沙盒模式" 有关说明，请参见。

通过导入联合元数据创建依赖方信任

您可以通过访问每个管理节点的 SAML 元数据来导入每个依赖方信任的值。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。
2. 在操作下，选择 * 添加依赖方信任 * 。
3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。
4. 选择 * 导入有关依赖方的在线或本地网络上发布的数据 * 。
5. 在 * 联合元数据地址（主机名或 URL ） * 中，键入此管理节点的 SAML 元数据的位置：

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

   适用于 `*Admin_Node_FQDN*` 下、输入同一管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

6. 完成依赖方信任向导，保存依赖方信任并关闭该向导。

   > 输入显示名称时，请使用管理节点的相关方标识符，与网格管理器的 Single Sign-On 页面上显示的完全相同。例如： `SG-DC1-ADM1`。

7. 添加声明规则：
   a. 右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。
   b. 选择 * 添加规则 * ：
   c. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。
   d. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。

   e. 对于属性存储，选择 * Active Directory* 。
   f. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。
   g. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。
   h. 选择 * 完成 * ，然后选择 * 确定 * 。
8. 确认元数据已成功导入。
   a. 右键单击依赖方信任以打开其属性。
   b. 确认已填充 * 端点 * ， * 标识符 * 和 * 签名 * 选项卡上的字段。

      如果缺少元数据、请确认联盟元数据地址是否正确、或者手动输入值。

9. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

10. 完成后，返回到 StorageGRID 并测试所有相关方信任，以确认其配置正确。请参见 "使用沙盒模式" 有关说明，请参见。

手动创建依赖方信任

如果您选择不导入依赖部件信任的数据，则可以手动输入值。

步骤

1. 在 Windows Server Manager 中，选择 * 工具 * ，然后选择 * AD FS 管理 * 。
2. 在操作下，选择 * 添加依赖方信任 * 。
3. 在 Welcome 页面上，选择 * 声明感知 * ，然后选择 * 开始 * 。
4. 选择 * 手动输入有关依赖方的数据 * ，然后选择 * 下一步 * 。
5. 完成依赖方信任向导：

   a. 输入此管理节点的显示名称。

      为了确保一致性，请使用管理节点的依赖方标识符，与网格管理器的单点登录页面上显示的一致。例如： `SG-DC1-ADM1`。

   b. 跳过此步骤可配置可选令牌加密证书。

   c. 在配置URL页面上，选中*启用对SAML 2.0 WebSSO协议的支持*复选框。

   d. 键入管理节点的 SAML 服务端点 URL：

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

      适用于 `*Admin_Node_FQDN*` 下、输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

   e. 在配置标识符页面上，指定同一管理节点的依赖方标识符：

      `Admin_Node_Identifier`

      适用于 `Admin_Node_Identifier` 下、输入管理节点的依赖方标识符、与单点登录页面上显示的完全相同。例如： `SG-DC1-ADM1`。

   f. 查看设置，保存依赖方信任并关闭向导。

      此时将显示编辑款项申请发放策略对话框。

      > 如果未显示此对话框，请右键单击此信任，然后选择 * 编辑款项申请发放策略 * 。

6. 要启动 Claim Rule 向导，请选择 * 添加规则 * ：

   a. 在选择规则模板页面上，从列表中选择 * 将 LDAP 属性作为声明发送 * ，然后选择 * 下一步 * 。

   b. 在配置规则页面上，输入此规则的显示名称。

      例如，将 * 对象 GUID 更改为名称 ID* 。

c. 对于属性存储，选择 * Active Directory* 。

d. 在映射表的 LDAP 属性列中，键入 * 对象 GUID* 。

e. 在映射表的传出款项申请类型列中，从下拉列表中选择 * 名称 ID* 。

f. 选择 * 完成 * ，然后选择 * 确定 * 。

7. 右键单击依赖方信任以打开其属性。

8. 在 * 端点 * 选项卡上，为单点注销（ SLO ）配置端点：

   a. 选择 * 添加 SAML * 。

   b. 选择 * 端点类型 * > * SAML 注销 * 。

   c. 选择 * 绑定 * > * 重定向 * 。

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

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

   适用于 `*Admin_Node_FQDN*` 下、输入管理节点的完全限定域名。（如有必要，您可以改用节点的 IP 地址。但是，如果您在此处输入 IP 地址，请注意，如果此依赖方信任的 IP 地址发生更改，您必须更新或重新创建此信任。）

   a. 选择 * 确定 * 。

9. 在 * 签名 * 选项卡上，指定此依赖方信任的签名证书：

   a. 添加自定义证书：

      - 如果您已将自定义管理证书上传到 StorageGRID ，请选择此证书。
      - 如果您没有自定义证书、请登录到管理节点、然后转到 `/var/local/mgmt-api` 管理节点的目录、然后添加 `custom-server.crt` 证书文件。

        *注：*使用管理节点的默认证书 (`server.crt`)。如果管理节点出现故障，则在恢复节点时将重新生成默认证书，您需要更新依赖方信任。

   b. 选择 * 应用 * ，然后选择 * 确定 * 。

      依赖方属性将被保存并关闭。

10. 重复上述步骤，为 StorageGRID 系统中的所有管理节点配置依赖方信任。

11. 完成后，返回到 StorageGRID 并测试所有相关方信任，以确认其配置正确。请参见 "使用沙盒模式" 有关说明，请参见。

在 **Azure AD** 中创建企业级应用程序

您可以使用 Azure AD 为系统中的每个管理节点创建企业级应用程序。

开始之前

- 您已开始为 StorageGRID 配置单点登录，并选择了 * Azure * 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 "使用沙盒模式"。
- 系统中每个管理节点都有 * 企业级应用程序名称 * 。您可以从 StorageGRID 单点登录页面上的管理节点详

细信息表复制这些值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个企业级应用程序。为每个管理节点配备一个企业级应用程序可确保用户可以安全地登录和注销任何管理节点。

- 您有在 Azure Active Directory 中创建企业级应用程序的经验。
- 您有一个 Azure 帐户且订阅有效。
- 您在 Azure 帐户中具有以下角色之一：全局管理员，云应用程序管理员，应用程序管理员或服务主体的所有者。

访问 **Azure AD**

步骤

1. 登录到 "Azure 门户"。
2. 导航到 "Azure Active Directory"。
3. 选择 … "企业级应用程序"。

创建企业级应用程序并保存 **StorageGRID SSO** 配置

要在StorageGRID 中保存Azure的SSO配置、您必须使用Azure为每个管理节点创建一个企业应用程序。您将从 Azure 复制联合元数据 URL ，并将其粘贴到 StorageGRID Single Sign-On 页面上对应的 * 联合元数据 URL* 字段中。

步骤

1. 对每个管理节点重复以下步骤。
   a. 在 Azure Enterprise 应用程序窗格中，选择 * 新建应用程序 * 。
   b. 选择 * 创建您自己的应用程序 * 。
   c. 对于此名称，请输入您从 StorageGRID Single Sign-On 页面上的管理节点详细信息表中复制的 * 企业应用程序名称 * 。
   d. 保持选中 * 集成在库（非库）中找不到的任何其他应用程序 * 单选按钮。
   e. 选择 * 创建 * 。
   f. 选择 * 。 2.设置单点登录 * 框，或者选择左侧边距中的 * 单点登录 * 链接。
   g. 选择 * SAML * 框。
   h. 复制 * 应用程序联合元数据 URL* ，该 URL 可在 * 步骤 3 SAML 签名证书 * 下找到。
   i. 转到 StorageGRID 单点登录页面，然后将 URL 粘贴到与您使用的 * 企业应用程序名称 * 对应的 * 联合元数据 URL* 字段中。
2. 为每个管理节点粘贴联合元数据 URL 并对 SSO 配置进行所有其他所需更改后，请在 StorageGRID Single Sign-On 页面上选择 * 保存 * 。

下载每个管理节点的 **SAML** 元数据

保存 SSO 配置后，您可以为 StorageGRID 系统中的每个管理节点下载 SAML 元数据文件。

步骤

1. 对每个管理节点重复上述步骤。
   a. 从管理节点登录到 StorageGRID 。
   b. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   c. 选择按钮以下载此管理节点的 SAML 元数据。
   d. 保存要上传到 Azure AD 的文件。

将 **SAML** 元数据上传到每个企业级应用程序

为每个 StorageGRID 管理节点下载 SAML 元数据文件后，在 Azure AD 中执行以下步骤：

步骤

1. 返回到 Azure 门户。
2. 对每个企业级应用程序重复以下步骤：

   > 您可能需要刷新 " 企业应用程序 " 页面才能查看先前在列表中添加的应用程序。

   a. 转到企业应用程序的属性页面。
   b. 将 * 需要分配 * 设置为 * 否 * （除非您要单独配置分配）。
   c. 转到单点登录页面。
   d. 完成 SAML 配置。
   e. 选择 * 上传元数据文件 * 按钮，然后选择为相应管理节点下载的 SAML 元数据文件。
   f. 加载文件后，选择 * 保存 * ，然后选择 * X * 以关闭窗格。此时将返回到使用 SAML 设置单点登录页面。
3. 按照中的步骤进行操作 "使用沙盒模式" 测试每个应用程序。

在 **PingFederate** 中创建服务提供商（ **SP** ）连接

您可以使用 PingFederate 为系统中的每个管理节点创建服务提供商（ SP ）连接。要加快此过程，您需要从 StorageGRID 导入 SAML 元数据。

开始之前

- 您已为 StorageGRID 配置单点登录，并选择了 * Ping 联邦 * 作为 SSO 类型。
- 在网格管理器的单点登录页面上选择了 * 沙盒模式 * 。请参见 "使用沙盒模式"。
- 您拥有系统中每个管理节点的 * SP 连接 ID* 。您可以在 StorageGRID 单点登录页面上的管理节点详细信息表中找到这些值。
- 您已为系统中的每个管理节点下载 * SAML 元数据 * 。
- 您在 PingFederate 服务器中创建 SP 连接的经验。
- 您拥有https://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["《管理员参考指南》"^] PingFederate 服务器。PingFederate 文档提供了详细的分步说明和说明。
- 您具有 PingFederate 服务器的管理员权限。

关于此任务

以下说明总结了如何将 PingFederate 服务器 10.3 版配置为 StorageGRID 的 SSO 提供程序。如果您使用的是其他版本的 PingFederate ，则可能需要调整这些说明。有关您的版本的详细说明，请参见 PingFederate 服务器文档。

完成 **PingFederate** 中的前提条件

在创建要用于 StorageGRID 的 SP 连接之前，必须先在 PingFederate 中完成前提条件任务。配置 SP 连接时，您将使用这些前提条件中的信息。

创建数据存储库**[Data -store]]**

如果尚未创建数据存储库，请将 PingFederate 连接到 AD FS LDAP 服务器。使用您在使用时使用的值 "配置身份联合" 在 StorageGRID 中。

- * 类型 *： 目录（ LDAP ）
- * LDAP 类型 *： Active Directory
- * 二进制属性名称 *： 在 "LDAP 二进制属性 " 选项卡上输入 * 对象 GUID* ，具体如图所示。

创建密码凭据验证器**[password-validator]]**

如果尚未创建密码凭据验证程序，请创建一个。

- * 类型 *： LDAP 用户名密码凭据验证器
- * 数据存储 *： 选择您创建的数据存储。
- * 搜索基础 *： 输入 LDAP 中的信息（例如， DC=SAML ， DC=sgws ）。
- * 搜索筛选器 *： sAMAccountName=$ ｛ username ｝
- * 范围 *： 子树

创建**IdP**适配器实例**[adapter-instance]]**

如果尚未创建 IdP 适配器实例，请创建此实例。

步骤

1. 转至 * 身份验证 * > * 集成 * > * IdP 适配器 * 。
2. 选择 * 创建新实例 * 。
3. 在类型选项卡上，选择 * HTML 表单 IdP 适配器 * 。
4. 在 IdP 适配器选项卡上，选择 * 向 " 凭据验证器 "* 添加新行。
5. 选择 密码凭据验证程序 您已创建。
6. 在适配器属性选项卡上，为 * 伪名称 * 选择 * 用户名 * 属性。
7. 选择 * 保存 * 。

创建或导入签名证书

如果尚未创建，请创建或导入签名证书。

步骤

1. 转至 * 安全性 * > * 签名和解密密钥和证书 * 。
2. 创建或导入签名证书。

在 **PingFederate** 中创建 **SP** 连接

在 PingFederate 中创建 SP 连接时，您可以导入从 StorageGRID 为管理节点下载的 SAML 元数据。元数据文件包含您需要的许多特定值。

> 您必须为 StorageGRID 系统中的每个管理节点创建一个 SP 连接，以便用户可以安全地登录和注销任何节点。按照以下说明创建第一个 SP 连接。然后，转到 创建其他 SP 连接 创建所需的任何其他连接。

选择 **SP** 连接类型

步骤

1. 转至 * 应用程序 * > * 集成 * > * SP 连接 * 。
2. 选择 * 创建连接 * 。
3. 选择 * 不对此连接使用模板 * 。
4. 选择 * 浏览器 SSO 配置文件 * 和 * SAML 2.0* 作为协议。

导入 **SP** 元数据

步骤

1. 在导入元数据选项卡上，选择 * 文件 * 。
2. 选择从管理节点的 StorageGRID 单点登录页面下载的 SAML 元数据文件。
3. 查看"元数据摘要"以及"常规信息"选项卡上提供的信息。

   合作伙伴的实体 ID 和连接名称设置为 StorageGRID SP 连接 ID 。（例如 10.96.105.200-DC1-ADM1-105-200 ）。基本 URL 是 StorageGRID 管理节点的 IP 。

4. 选择 * 下一步 * 。

配置 **IdP** 浏览器 **SSO**

步骤

1. 从浏览器 SSO 选项卡中，选择 * 配置浏览器 SSO* 。
2. 在 SAML 配置文件选项卡上，选择 * SP 启动的 SSO* ， * SP 初始 SLO* ， * IdP-Initiated SSO* 和 * IdP-Initiated SLO* 选项。
3. 选择 * 下一步 * 。
4. 在 Assertion Lifetime 选项卡上，不进行任何更改。
5. 在断言创建选项卡上，选择 * 配置断言创建 * 。
   a. 在身份映射选项卡上，选择 * 标准 * 。
   b. 在属性合同选项卡上，使用 * SAML 主题 * 作为属性合同以及导入的未指定名称格式。
6. 要延长合同，请选择*Delete*以删除 `urn:oid`，未使用。

映射适配器实例

步骤

1. 在身份验证源映射选项卡上，选择 * 映射新适配器实例 * 。
2. 在适配器实例选项卡上，选择 适配器实例 您已创建。
3. 在映射方法选项卡上，选择 * 从数据存储中检索其他属性 * 。
4. 在属性源和用户查找选项卡上，选择 * 添加属性源 * 。
5. 在数据存储选项卡上，提供问题描述 并选择 数据存储 您已添加。
6. 在 LDAP 目录搜索选项卡上：
   - 输入 * 基本 DN* ，该 DN 应与您在 StorageGRID 中为 LDAP 服务器输入的值完全匹配。
   - 对于搜索范围，请选择 * 子树 * 。
   - 对于根对象类，搜索 * 对象 GUID* 属性并添加它。
7. 在 LDAP 二进制属性编码类型选项卡上，为 * 对象 GUID* 属性选择 * Base64* 。
8. 在 LDAP 筛选器选项卡上，输入 * 。 sAMAccountName=$ ｛ username ｝ * 。
9. 在属性合同履行选项卡上，从源下拉列表中选择 * LDAP （ attribute ） * ，然后从值下拉列表中选择 * 对象 GUID* 。
10. 查看并保存属性源。
11. 在故障保存属性源选项卡上，选择 * 中止 SSO 事务 * 。
12. 查看摘要并选择 * 完成 * 。
13. 选择 * 完成 * 。

配置协议设置

步骤

1. 在 * SP Connection* > * 浏览器 SSO* > * 协议设置 * 选项卡上，选择 * 配置协议设置 * 。
2. 在断言使用方服务URL选项卡上、接受从StorageGRID SAML元数据导入的默认值(* post*用于绑定和 `/api/saml-response` 表示端点URL)。
3. 在SLO服务URL选项卡上、接受从StorageGRID SAML元数据导入的默认值(*重定向*用于绑定和) `/api/saml-logout` 端点URL。
4. 在允许的SAML绑定选项卡上、清除*项目*和* SOAP *。仅需要 * 发布 * 和 * 重定向 * 。
5. 在“签名策略”选项卡上，保持选中“要求对authn请求进行签名”和“始终签名断言”复选框。
6. 在加密策略选项卡上，选择 * 无 * 。
7. 查看摘要并选择 * 完成 * 以保存协议设置。
8. 查看摘要并选择 * 完成 * 以保存浏览器 SSO 设置。

配置凭据

步骤

1. 从 SP 连接选项卡中，选择 * 凭据 * 。

2. 从凭据选项卡中，选择 * 配置凭据 * 。
3. 选择 正在签名证书 您已创建或导入。
4. 选择 * 下一步 * 转到 * 管理签名验证设置 * 。
   a. 在信任模式选项卡上，选择 * 已取消锁定 * 。
   b. 在签名验证证书选项卡上，查看从 StorageGRID SAML 元数据导入的签名证书信息。
5. 查看摘要屏幕并选择 * 保存 * 以保存 SP 连接。

创建其他 **SP** 连接

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

> 不同管理节点的 SP 连接使用相同的设置，但合作伙伴的实体 ID ，基本 URL ，连接 ID ，连接名称，签名验证除外。 和 SLO 响应 URL 。

步骤

1. 选择 * 操作 * > * 复制 * 为每个附加管理节点创建初始 SP 连接的副本。
2. 输入副本的连接 ID 和连接名称，然后选择 * 保存 * 。
3. 选择与管理节点对应的元数据文件：
   a. 选择 * 操作 * > * 使用元数据更新 * 。
   b. 选择 * 选择文件 * 并上传元数据。
   c. 选择 * 下一步 * 。
   d. 选择 * 保存 * 。
4. 解决由于属性未使用而导致的错误：
   a. 选择新连接。
   b. 选择 * 配置浏览器 SSO > 配置断言创建 > 属性合同 * 。
   c. 删除 * urn ： oid* 的条目。
   d. 选择 * 保存 * 。

禁用单点登录

如果您不再希望使用单点登录（ SSO ）功能，则可以禁用此功能。必须先禁用单点登录，然后才能禁用身份联合。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

步骤

1. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。

此时将显示 Single Sign-On 页面。

2. 选择 * 已禁用 * 选项。
3. 选择 * 保存 * 。

   此时将显示一条警告消息，指示本地用户现在可以登录。

4. 选择 * 确定 * 。

   下次登录到 StorageGRID 时，将显示 StorageGRID 登录页面，您必须输入本地或联合 StorageGRID 用户的用户名和密码。

临时禁用并重新启用一个管理节点的单点登录

如果单点登录（ Single Sign-On ， SSO ）系统发生故障，您可能无法登录到网格管理器。在这种情况下，您可以为一个管理节点临时禁用并重新启用 SSO 。要禁用并重新启用 SSO ，必须访问节点的命令 Shell 。

开始之前

- 您具有特定的访问权限。
- 您拥有 `Passwords.txt` 文件
- 您知道本地 root 用户的密码。

关于此任务

为一个管理节点禁用 SSO 后，您可以以本地 root 用户身份登录到网格管理器。要保护 StorageGRID 系统的安全，您必须在注销后立即使用节点的命令 Shell 在管理节点上重新启用 SSO 。

> 为一个管理节点禁用 SSO 不会影响网格中任何其他管理节点的 SSO 设置。网格管理器中单点登录页面上的*Enable SSO*复选框保持选中状态，所有现有SSO设置都将保持不变，除非您对其进行更新。

步骤

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

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 运行以下命令：`disable-saml`

   此时将显示一条消息，指出命令适用场景 this Admin Node only 。

3. 确认要禁用 SSO 。

显示一条消息，指示节点上已禁用单点登录。

4. 从 Web 浏览器访问同一管理节点上的网格管理器。

   现在，由于已禁用 SSO ，将显示网格管理器登录页面。

5. 使用用户名 root 和本地 root 用户的密码登录。
6. 如果您因需要更正 SSO 配置而临时禁用 SSO：
   a. 选择 * 配置 * > * 访问控制 * > * 单点登录 * 。
   b. 更改不正确或过时的 SSO 设置。
   c. 选择 * 保存 * 。

      从 Single Sign-On 页面选择 * 保存 * 会自动为整个网格重新启用 SSO 。

7. 如果您因某些其他原因需要访问网格管理器而临时禁用 SSO：

   a. 执行需要执行的任何任务。
   b. 选择*注销*，然后关闭网格管理器。
   c. 在管理节点上重新启用 SSO 。您可以执行以下任一步骤：

      - 运行以下命令： `enable-saml`

        此时将显示一条消息，指出命令适用场景 this Admin Node only 。

      确认要启用 SSO 。

   显示一条消息，指示节点上已启用单点登录。

   - 重新启动网格节点： `reboot`

8. 从 Web 浏览器中，从同一管理节点访问网格管理器。
9. 确认此时将显示 StorageGRID 登录页面，并且您必须输入 SSO 凭据才能访问网格管理器。

使用网格联盟

什么是网格联合?

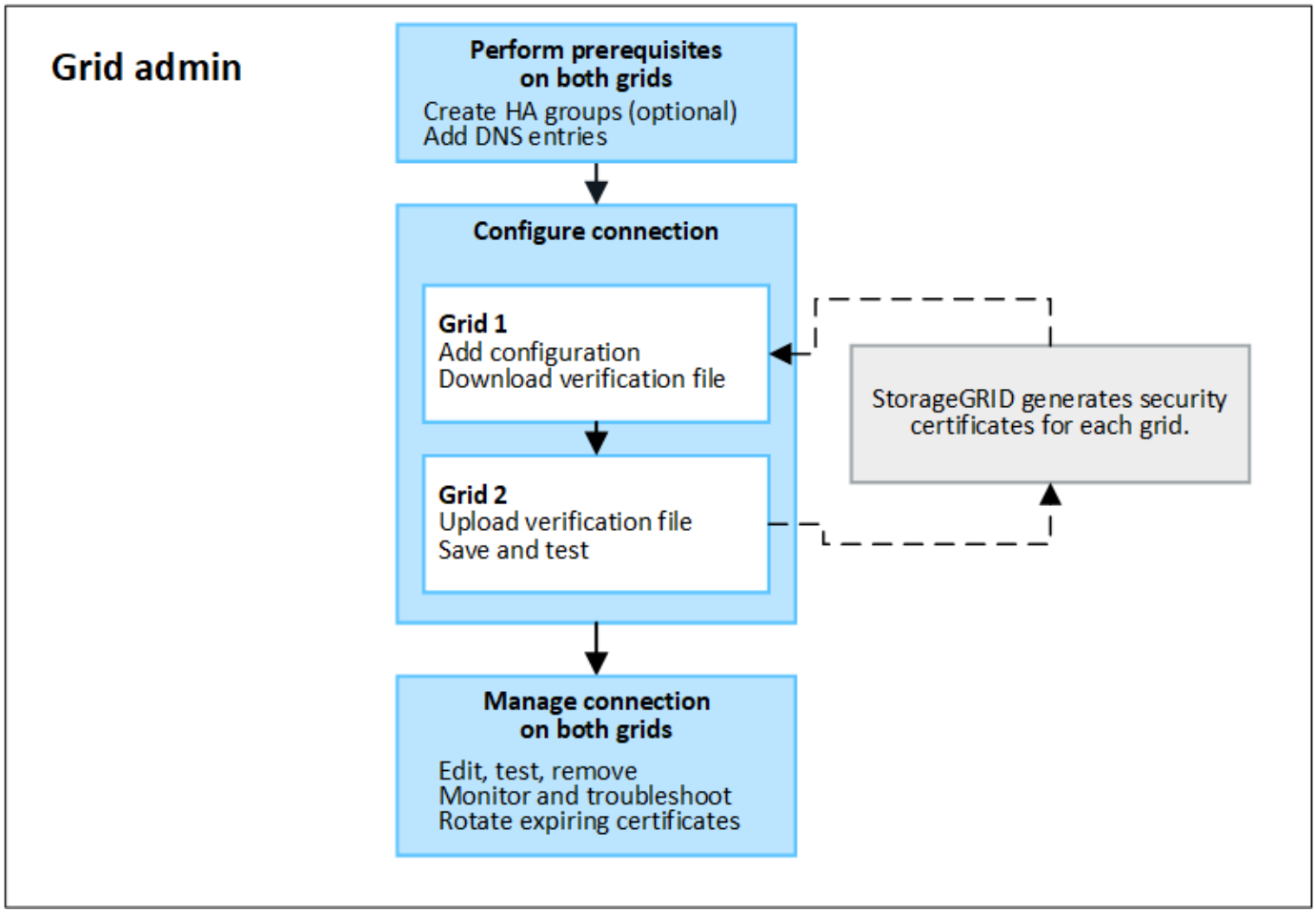
您可以使用网格联盟在两个StorageGRID 系统之间克隆租户并复制其对象、以实现灾难恢复。

什么是网格联合连接?

网格联合连接是两个StorageGRID 系统中的管理节点和网关节点之间的双向、可信且安全的连接。

网格联合工作流

此工作流图汇总了在两个网格之间配置网格联合连接的步骤。



网格联合连接的注意事项和要求

- 用于网格联盟的两个网格都必须运行StorageGRID 11.7。
- 一个网格可以与其他网格建立一个或多个网格联合连接。每个网格联合连接都与任何其他连接无关。例如、如果网格1与网格2有一个连接、而与网格3有另一个连接、则网格2与网格3之间不存在隐含连接。
- 网格联合连接是双向的。建立连接后、您可以从任一网格监控和管理连接。
- 要使用、必须至少存在一个网格联合连接 "帐户克隆" 或 "跨网格复制"。

网络和**IP**地址要求

- 网格联合连接可以在网格网络、管理网络或客户端网络上进行。
- 网格联合连接将一个网格连接到另一个网格。每个网格的配置用于在另一个网格上指定一个网格联合端点、此联合端点由管理节点、网关节点或这两者组成。
- 最佳做法是进行连接 "高可用性(HA)组" 每个网格上的网关和管理节点数。使用HA组有助于确保网格联合连接在节点不可用时保持联机。如果任一HA组中的活动接口发生故障、则此连接可以使用备份接口。
- 建议不要创建使用单个管理节点或网关节点的IP地址的网格联合连接。如果节点不可用、网格联合连接也将不可用。
- "跨网格复制" 的对象要求每个网格上的存储节点能够访问另一网格上配置的管理节点和网关节点。对于每个网格、确认所有存储节点都具有一个高带宽路由、作为用于连接的管理节点或网关节点。

使用FQDN对连接进行负载平衡

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

- 网格1的FQDN映射到网格1中HA组的一个或多个虚拟IP (VIP)地址、或者映射到网格1中一个或多个管理节点或网关节点的IP地址。
- 网格2的FQDN映射到网格2的一个或多个VIP地址、或者映射到网格2中一个或多个管理节点或网关节点的IP地址。

如果使用多个DNS条目、则会对使用此连接的请求进行负载平衡、如下所示：

- 映射到多个HA组的VIP地址的DNS条目会在HA组中的活动节点之间进行负载平衡。
- 映射到多个管理节点或网关节点的IP地址的DNS条目会在映射的节点之间进行负载平衡。

端口要求

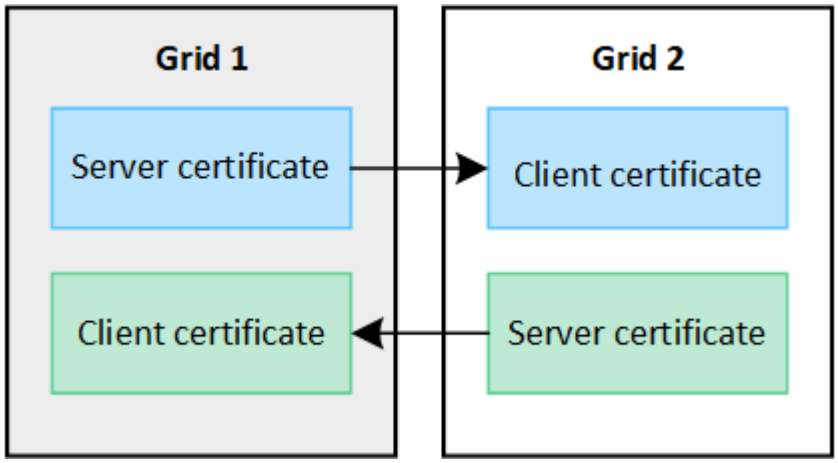
创建网格联合连接时、您可以指定介于23000到23999之间的任何未使用端口号。此连接中的两个网格将使用同一端口。

您必须确保任一网格中的任何节点都不会将此端口用于其他连接。

证书要求

配置网格联合连接时、StorageGRID 会自动生成四个SSL证书：

- 用于对从网格1发送到网格2的信息进行身份验证和加密的服务器和客户端证书
- 用于对从网格2发送到网格1的信息进行身份验证和加密的服务器和客户端证书



默认情况下、证书的有效期为730天(2年)。当这些证书接近到期日期时，“网格联合证书到期”警报会提醒您轮换证书，您可以使用网格管理器执行此操作。

> 如果连接任一端的证书过期、则连接将停止工作。数据复制将处于待定状态、直到证书更新为止。

了解更多信息。

- "创建网格联合连接"

- "管理网格联合连接"
- "对网格联合错误进行故障排除"

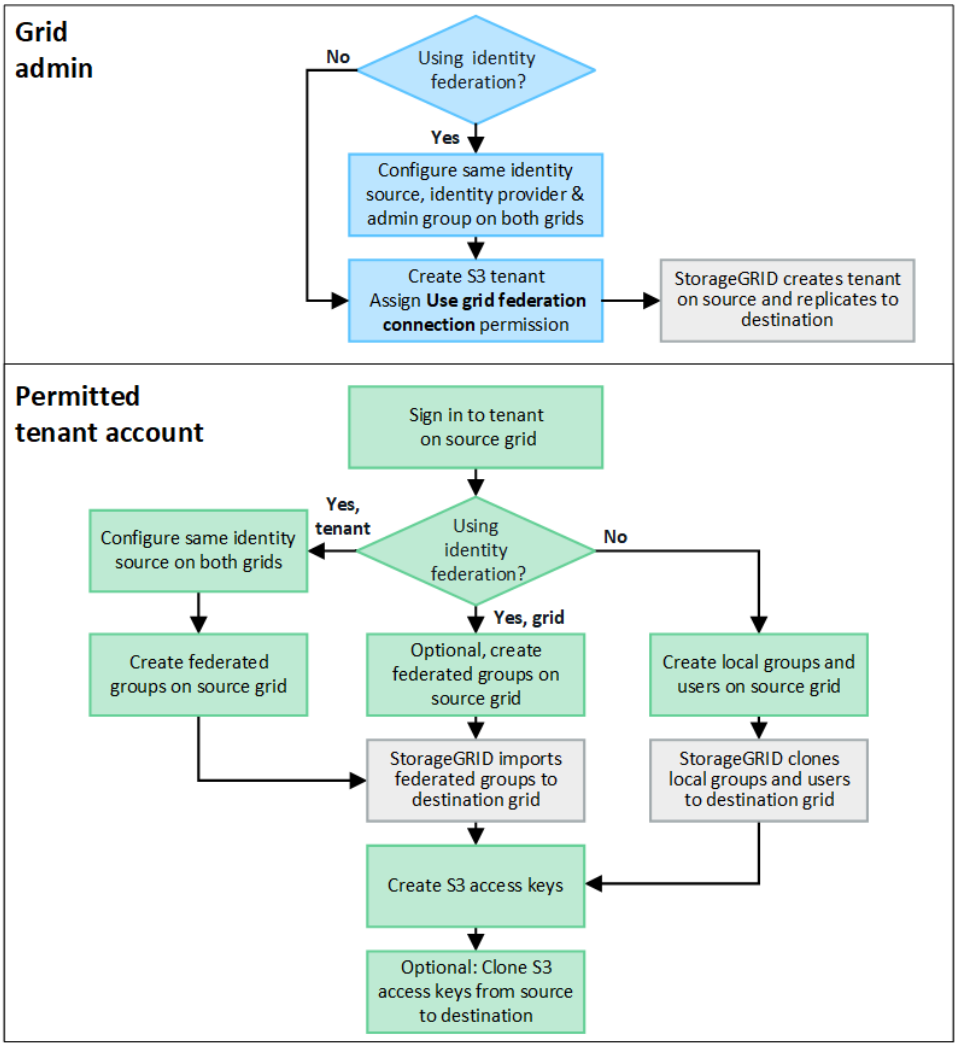
什么是帐户克隆?

帐户克隆是指自动复制租户帐户、租户组、租户用户以及(可选) 中StorageGRID 系统之间的S3访问密钥 "网格联合连接"。

需要使用帐户克隆 "跨网格复制"。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网格上的相应分段和对象。

帐户克隆工作流

此工作流图显示了网格管理员和允许的租户设置帐户克隆时要执行的步骤。这些步骤将在之后执行 "已配置网格联合连接"。



网格管理工作流

网格管理员执行的步骤取决于中的StorageGRID 系统 "网格联合连接" 使用单点登录(SSO)或身份联合。

[[account-Clone SSO]]为帐户克隆配置SSO (可选)

如果网格联合连接中的任一StorageGRID 系统使用SSO、则两个网格都必须使用SSO。在为网格联盟创建租户帐户之前、租户的源网格和目标网格的网格管理员必须执行以下步骤。

步骤

1. 为两个网格配置相同的标识源。请参见 "使用身份联合"。
2. 为两个网格配置相同的SSO身份提供程序(Idp)。请参见 "配置单点登录"。
3. "创建同一个管理员组" 通过导入同一联盟组在两个网格上。

   创建租户时、您需要选择此组、以获得源租户帐户和目标租户帐户的初始root访问权限。

   > 如果在创建租户之前此管理员组不在两个网格上、则不会将租户复制到目标。

为帐户克隆配置网格级身份联合(可选)

如果任一StorageGRID 系统使用无SSO的身份联合、则两个网格都必须使用身份联合。在为网格联盟创建租户帐户之前、租户的源网格和目标网格的网格管理员必须执行以下步骤。

步骤

1. 为两个网格配置相同的标识源。请参见 "使用身份联合"。
2. (可选)如果联盟组对源租户帐户和目标租户帐户都具有初始root访问权限、 "创建同一个管理员组" 通过导入同一联盟组在两个网格上。

   > 如果为两个网格上都不存在的联盟组分配root访问权限、则租户不会复制到目标网格。

3. 如果您不希望联盟组对这两个帐户都具有初始root访问权限、请指定本地root用户的密码。

创建允许的S3租户帐户

根据需要配置SSO或身份联合之后、网格管理员可以执行以下步骤来确定哪些租户可以将存储分段对象复制到其他StorageGRID 系统。

步骤

1. 确定要用作租户的源网格以执行帐户克隆操作的网格。

   最初创建租户的网格称为租户的_ssource grid _。用于复制租户的网格称为租户的_Destination grid _。

2. 在该网格上创建新的S3租户帐户。
3. 分配*使用网格联合连接*权限。
4. 如果租户帐户要管理自己的联盟用户，请分配“使用自己的身份源”权限。

   如果分配了此权限、则源租户帐户和目标租户帐户必须先配置相同的身份源、然后才能创建联盟组。添加到源租户的联盟组无法克隆到目标租户、除非两个网格使用同一身份源。

5. 选择特定的网格联合连接。
6. 保存租户。

保存具有*使用网格联合连接*权限的新租户时、StorageGRID 会自动在另一个网格上创建该租户的副本、如下所示：

- 这两个租户帐户具有相同的帐户ID、名称、存储配额和已分配权限。
- 如果您选择的联盟组对租户具有root访问权限、则该组将克隆到目标租户。
- 如果您选择的本地用户对租户具有root访问权限、则该用户将克隆到目标租户。但是、不会克隆该用户的密码。

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以下步骤来克隆租户组、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、请在源租户帐户和目标租户帐户上配置"标识联合"。
3. 在源租户上创建组和用户。

   在源租户上创建新组或用户时、StorageGRID 会自动将其克隆到目标租户、但不会从目标克隆回源。

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。

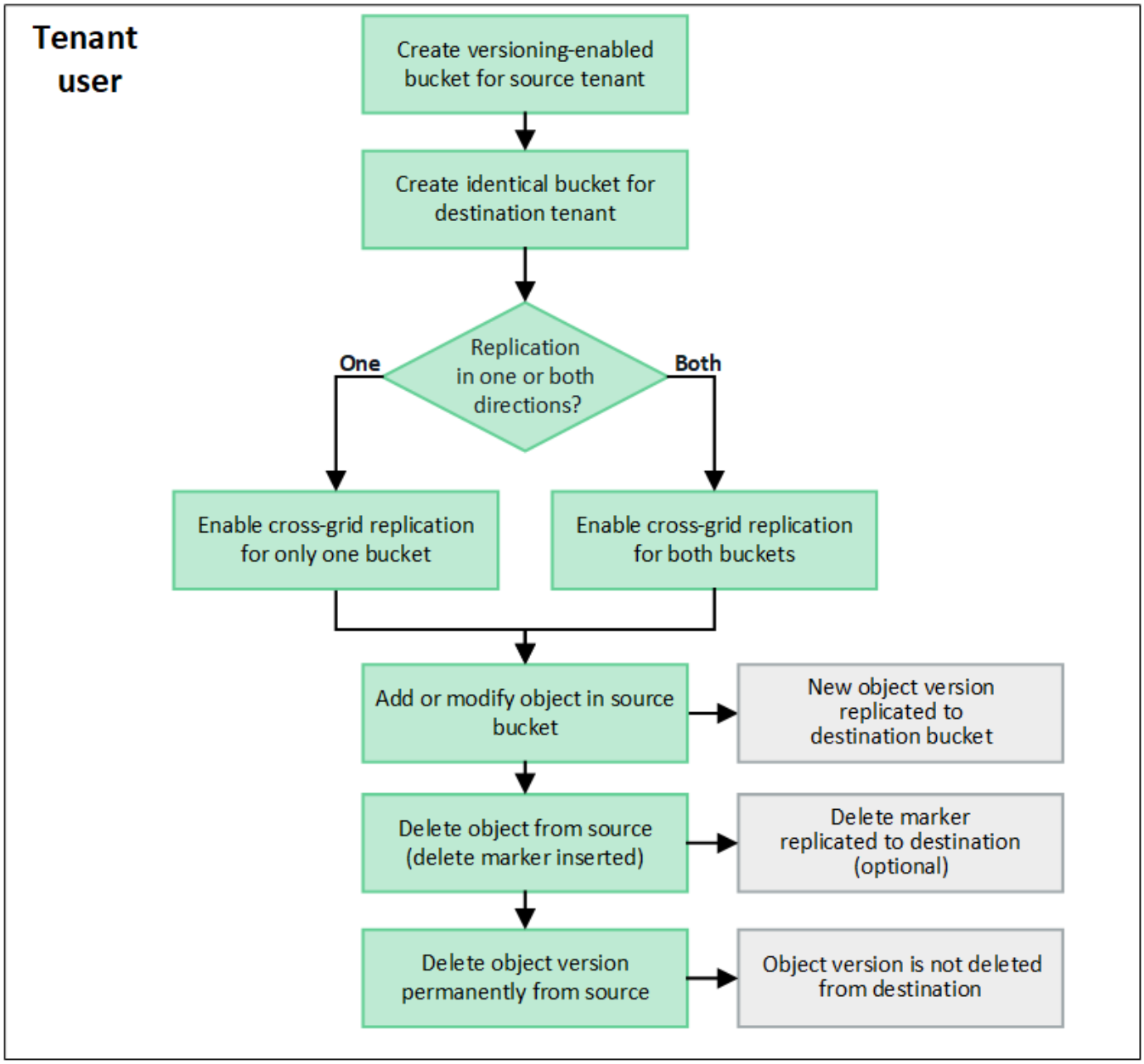
有关允许的租户帐户工作流的详细信息以及如何克隆组、用户和S3访问密钥、请参阅 "克隆租户组和用户" 和 "使用API克隆S3访问密钥"。

什么是跨网格复制?

跨网格复制是指在中连接的两个StorageGRID 系统中的选定S3分段之间自动复制对象 "网格联合连接"。 "帐户克隆" 跨网格复制需要。

跨网格复制工作流

此工作流图汇总了在两个网格上的分段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"，具有root访问权限的租户用户可以在每个网格的相应租户帐户中创建相同的分段。这些存储分段：

- 必须具有相同的名称和区域
- 必须启用版本控制
- 必须已禁用S3对象锁定
- 必须为空

创建这两个分段后、可以为其中一个分段或这两个分段配置跨网格复制。

了解更多信息。

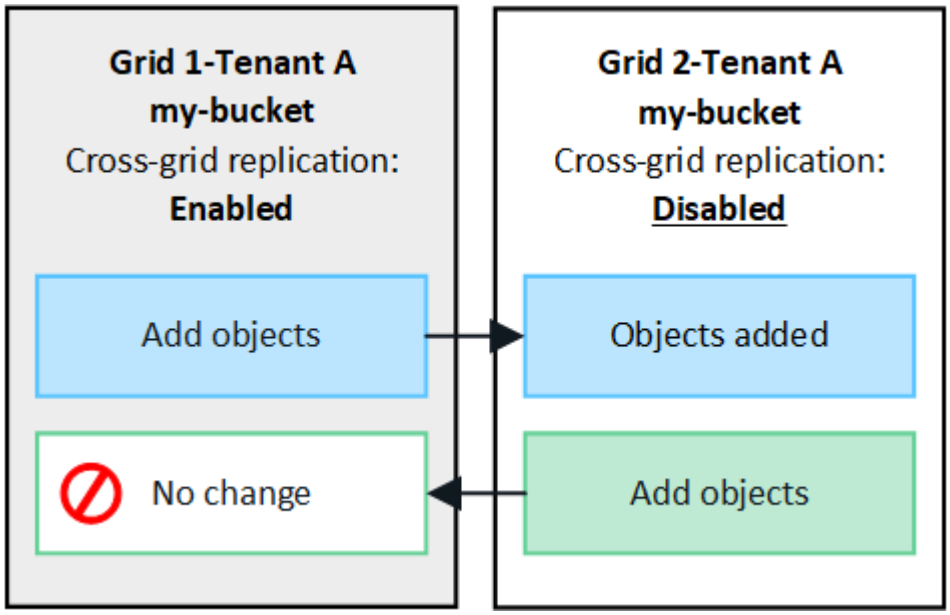
"管理跨网格复制"

跨网格复制的工作原理

可以将跨网格复制配置为单向或双向进行。

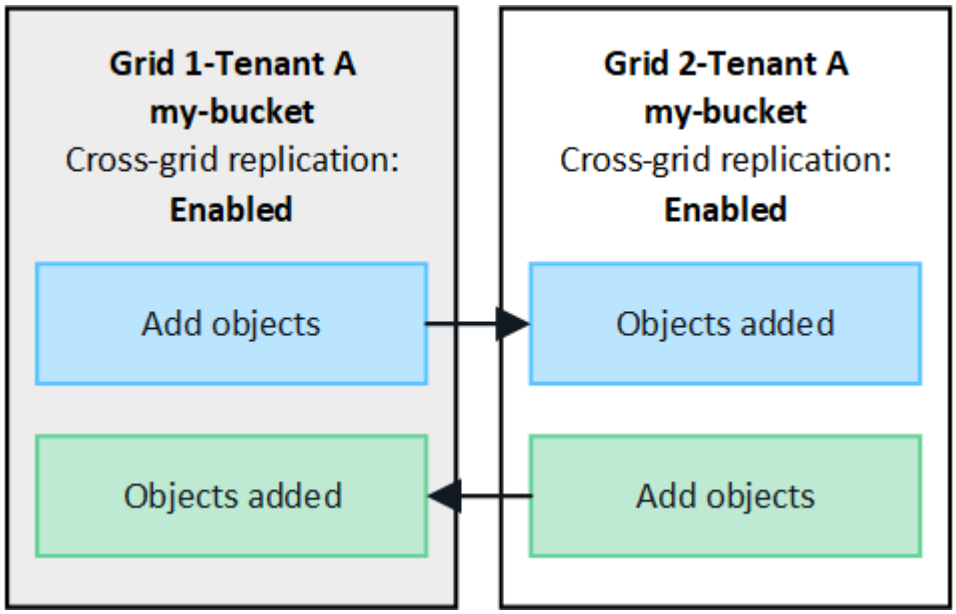
单向复制

如果仅对一个网格上的某个分段启用跨网格复制、则添加到该分段(源分段)的对象将复制到另一网格上的相应分段(目标分段)。但是、添加到目标存储分段的对象不会复制回源存储分段。在图中、为启用了跨网格复制 `my-bucket` 从网格1到网格2、但不会在另一个方向启用。



双向复制

如果为两个网格上的同一存储分段启用跨网格复制、则添加到任一存储分段的对象将复制到另一个网格。在图中、为启用了跨网格复制 `my-bucket` 双向。



当对象被加热时会发生什么情况?

当S3客户端向启用了跨网格复制的存储分段添加对象时、会发生以下情况：

1. StorageGRID 会自动将对象从源存储分段复制到目标存储分段。执行此后台复制操作所需的时间取决于多个因素、包括待处理的其他复制操作的数量。

   S3客户端可以通过发出GET对象或HEAD对象请求来验证对象的复制状态。响应包括特定于StorageGRID的响应 `x-ntap-sg-cgr-replication-status` 响应标头、具有以下值之一：S3客户端可以通过发出GET对象或HEAD对象请求来验证对象的复制状态。响应包括特定于StorageGRID的响应 `x-ntap-sg-cgr-replication-status` 响应标头、它将具有以下值之一：

网格	复制状态
源	• *SUCCESS *：所有网格连接的复制均成功。 • *pending *：对象尚未复制到至少一个网格连接。 • 失败：任何网格连接都未等待复制、至少一个网格出现故障并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

   > StorageGRID 不支持 `x-amz-replication-status` 标题。

2. StorageGRID 使用每个网格的活动ILM策略来管理对象、就像管理任何其他对象一样。例如、网格1上的对象A可能会存储为两个复制副本并永久保留、而复制到网格2的对象A的副本可能会使用2+1纠删编码进行存储、并在三年后删除。

删除对象时会发生什么情况?

如中所述 "删除数据流"，StorageGRID 可以出于以下任一原因删除对象：

- S3客户端发出删除请求。
- 租户管理器用户选择 "删除存储分段中的对象" 用于从存储分段中删除所有对象的选项。
- 此存储分段具有生命周期配置、此配置将过期。
- 对象的ILM规则中的最后一个时间段结束、并且未指定其他放置位置。

如果StorageGRID 因"删除存储分段"操作中的对象、存储分段生命周期到期或ILM放置到期而删除对象、则不会从网格联合连接中的其他网格中删除复制的对象。但是、S3客户端删除操作添加到源存储分段的删除标记可以选择复制到目标存储分段。

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

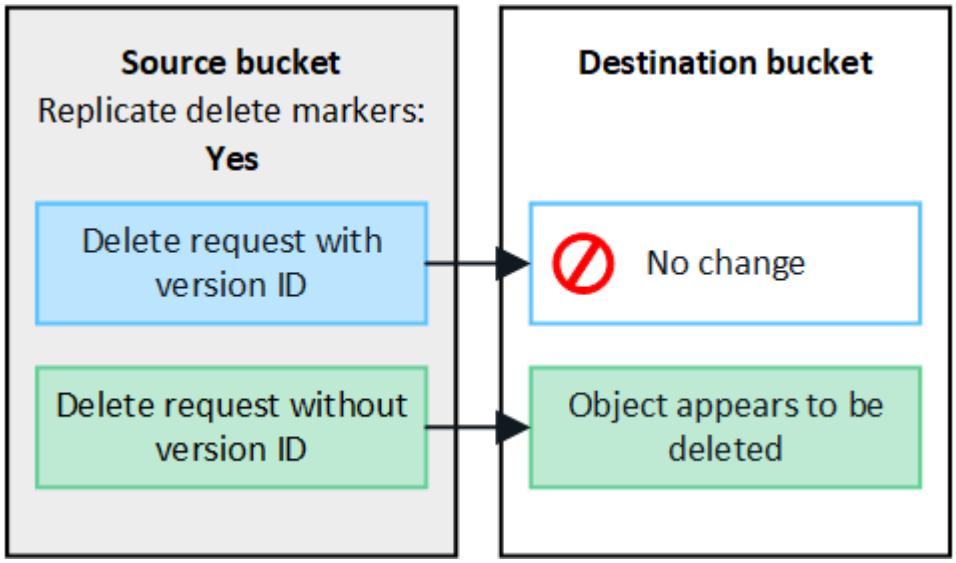
- 如果S3客户端发出包含版本ID的删除请求、则该对象的版本将被永久删除。不会向存储分段添加任何删除标记。
- 如果S3客户端发出的删除请求不包含版本ID、则StorageGRID 不会删除任何对象版本。而是向存储分段添加删除标记。删除标记会使StorageGRID 如同对象已被删除一样：
  - 没有版本ID的获取请求将失败 `404 No Object Found`

- 具有有效版本ID的GET请求将成功并返回请求的对象版本。

当S3客户端从启用了跨网格复制的存储分段中删除对象时、StorageGRID 将确定是否将删除请求复制到目标、如下所示：

- 如果删除请求包含版本ID、则该对象版本将从源网格中永久删除。但是、StorageGRID 不会复制包含版本ID的删除请求、因此不会从目标中删除同一对象版本。
- 如果删除请求不包含版本ID、则StorageGRID 可以根据为存储分段配置跨网格复制的方式选择复制删除标记：
  - 如果选择复制删除标记(默认)、则会将删除标记添加到源存储分段并复制到目标存储分段。实际上，该对象在两个网格上似乎都被删除。
  - 如果选择不复制删除标记、则删除标记将添加到源存储分段、但不会复制到目标存储分段。实际上、在源网格上删除的对象不会在目标网格上删除。

在该图中，当时，“已将删除标记”设置为“是” "已启用跨网格复制"。包含版本ID的源存储分段的删除请求不会从目标存储分段中删除对象。对不包含版本ID的源存储分段的删除请求将显示为删除目标存储分段中的对象。



> 如果要使对象删除在网格之间保持同步、请创建相应的 "S3生命周期配置" 用于两个网格上的存储分段。

如何复制加密对象

使用跨网格复制在网格之间复制对象时、您可以对单个对象进行加密、使用默认分段加密或配置网格范围的加密。在为存储分段启用跨网格复制之前或之后、您可以添加、修改或删除默认存储分段或网格范围的加密设置。

要对单个对象进行加密、可以在向源存储分段添加对象时使用SSE (使用StorageGRID托管密钥的服务器端加密)。使用 `x-amz-server-side-encryption` 请求标头并指定 `AES256`。请参见 "使用服务器端加密"。

> 跨网格复制不支持使用SSE-C (使用客户提供的密钥进行服务器端加密)。载入操作将失败。

要对存储分段使用默认加密、请使用放置存储分段加密请求并设置 `SSEAlgorithm` 参数设置为 `AES256`。存储分段级加密适用场景 任何未使用的已加载对象 `x-amz-server-side-encryption` 请求标题。请参见 "对存储分段执行的操作"。

要使用网格级加密，请将*存储对象加密*选项设置为*AES-256*。网格级加密适用场景 未在存储分段级别加密的任何对象或未使用进行加密的任何对象 `x-amz-server-side-encryption` 请求标题。请参见 "配置网络和对象选项"。

> SSE不支持AES-128。如果使用*AES-128*选项为源网格启用了*存储对象加密*选项，则AES-128算法的使用不会传播到复制的对象。相反、复制的对象将使用目标的默认分段或网格级加密设置(如果可用)。

在确定如何对源对象进行加密时、StorageGRID 会应用以下规则：

1. 使用 `x-amz-server-side-encryption` 如果存在、则为"加载"标题。
2. 如果不存在加载标头、请使用存储分段默认加密设置(如果已配置)。
3. 如果未配置存储分段设置、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设置、请勿对源对象进行加密。

在确定如何对复制的对象进行加密时、StorageGRID 会按以下顺序应用这些规则：

1. 使用与源对象相同的加密、除非该对象使用AES-128加密。
2. 如果源对象未加密或使用AES-128、请使用目标存储分段的默认加密设置(如果已配置)。
3. 如果目标存储分段没有加密设置、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设置、请勿对目标对象进行加密。

不支持放置对象标记和删除对象标记

启用了跨网格复制的分段中的对象不支持放置对象标记和删除对象标记请求。

如果S3客户端发出Put Object标记或Delete Object标记请求、 `501 Not Implemented` 返回。消息为 `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`。

分段对象的复制方式

复制到目标网格的源网格的最大区块大小适用场景 对象。将对象复制到另一个网格时，源网格的*最大区块大小*设置(**configuration**>*System*>*Storage options *)将同时在两个网格上使用。例如、假设源网格的最大区块大小为1 GB、而目标网格的最大区块大小为50 MB。如果在源网格上加载2 GB对象、则该对象将另存为两个1 GB区块。它还会作为两个1 GB区块复制到目标网格、即使该网格的最大区块大小为50 MB也是如此。

请比较跨网格复制和**CloudMirror**复制

开始使用网格联盟时、请查看之间的相似之处和不同之处 "跨网格复制" 和 "StorageGRID CloudMirror 复制服务"。

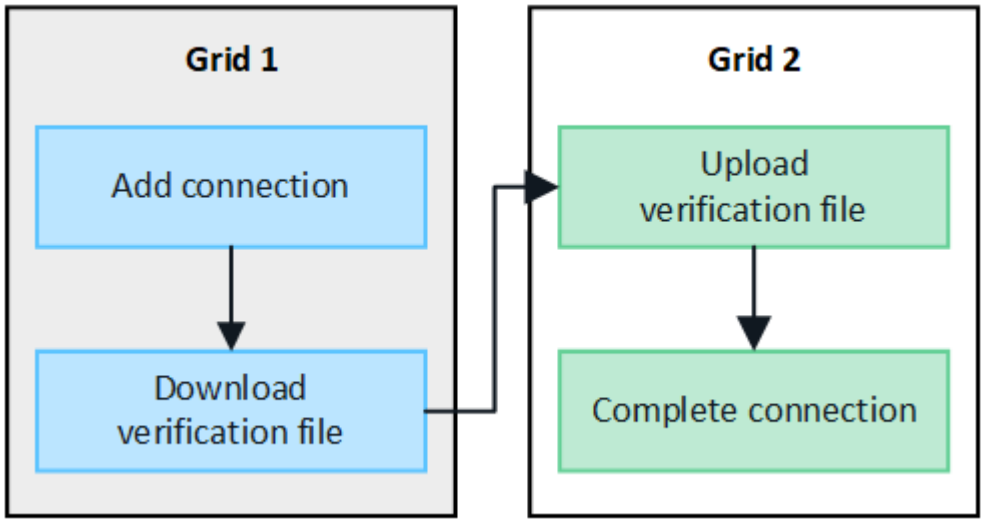
	跨网格复制	**CloudMirror** 复制服务
主要目的是什么?	一个StorageGRID 系统充当灾难恢复系统。分段中的对象可以在网格之间进行一个或两个方向的复制。	允许租户自动将对象从StorageGRID (源)中的存储分段复制到外部S3存储分段(目标)。 CloudMirror 复制会在独立的 S3 基础架构中为对象创建一个独立副本。此独立副本不会用作备份、但通常会在云中进行进一步处理。
如何设置?	1. 配置两个网格之间的网格联合连接。 2. 添加新租户帐户、这些帐户将自动克隆到其他网格。 3. 添加新的租户组和用户、这些组和用户也会进行克隆。 4. 在每个网格上创建相应的存储分段、并允许跨网格复制在一个或两个方向进行。	1. 租户用户可通过使用租户管理器或S3 API定义CloudMirror端点(IP地址、凭据等)来配置CloudMirror复制。 2. 可以将该租户帐户拥有的任何存储分段配置为指向CloudMirror端点。
谁负责设置?	• 网格管理员配置连接和租户。 • 租户用户配置组、用户、密钥和分段。	通常指租户用户。
目标是什么?	网格联盟连接中另一个StorageGRID 系统上的相应且相同的S3存储分段。	• 任何兼容的S3基础架构(包括Amazon S3)。 • Google Cloud Platform （ GCP ）
是否需要对象版本控制?	是的、源分段和目标分段都必须启用对象版本控制。	不可以、CloudMirror复制支持源和目标上的任何未受版本控制的分段和受版本控制的分段组合。
将对象移动到目标的原因是什么?	将对象添加到启用了跨网格复制的存储分段时、系统会自动复制这些对象。	将对象添加到配置了CloudMirror端点的存储分段时、系统会自动复制这些对象。在为源存储分段配置CloudMirror端点之前、源存储分段中存在的对象不会进行复制、除非对其进行了修改。
如何复制对象?	跨网格复制可创建版本控制对象、并将版本ID从源存储分段复制到目标存储分段。这样可以在两个网格之间保持版本顺序。	CloudMirror复制不需要启用了版本控制的分段、因此CloudMirror只能保持站点内密钥的顺序。对于向不同站点的对象发出的请求、不保证会保持排序。
如果无法复制对象、该怎么办?	对象将排队等待复制、但要遵守元数据存储限制。	对象将排队等待复制、但受平台服务限制的约束(请参见 "使用平台服务的建议"）。
是否复制了对象的系统元数据?	可以、当将对象复制到另一个网格时、也会复制其系统元数据。两个网格上的元数据将相同。	不可以、将对象复制到外部存储分段时、系统将更新其系统元数据。元数据因位置而异、具体取决于加数据时间以及独立S3基础架构的行为。

	跨网格复制	**CloudMirror** 复制服务
如何检索对象？	应用程序可以通过向任一网格上的存储分段发出请求来检索或读取对象。	应用程序可以通过向StorageGRID 或S3目标发出请求来检索或读取对象。例如，假设您使用 CloudMirror 复制将对象镜像到合作伙伴组织。配对节点可以使用自己的应用程序直接从 S3 目标读取或更新对象。不需要使用 StorageGRID 。
删除对象会发生什么情况?	• 包含版本ID的删除请求不会复制到目标网格。 • 如果删除请求不包含版本ID、请向源存储分段添加一个删除标记、此标记可以选择复制到目标网格。 • 如果只为一个方向配置了跨网格复制、则可以删除目标存储分段中的对象、而不会影响源。	根据源分段和目标分段的版本控制状态、结果会有所不同(不必相同)： • 如果这两个存储分段都已分版本、则删除请求将在这两个位置添加一个删除标记。 • 如果仅对源存储分段进行了版本控制、则删除请求会向源添加一个删除标记、但不会向目标添加此标记。 • 如果两个存储分段均未进行版本控制、则删除请求将从源中删除对象、而不是从目标中删除对象。 同样，可以删除目标分段中的对象而不影响源。

创建网格联合连接

如果要克隆租户详细信息和复制对象数据、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。您可以在一个网格上添加连接、并在另一个网格上完成连接。您可以从任一网格开始。



开始之前

- 您已查看 "注意事项和要求" 用于配置网格联合连接。

- 如果您计划对每个网格使用完全限定域名(FQDN)、而不是IP或VIP地址、则您知道要使用哪些名称、并且已确认每个网格的DNS服务器具有相应的条目。
- 您正在使用 "支持的 Web 浏览器"。
- 您必须具有两个网格的root访问权限和配置密码短语。

添加连接

在两个StorageGRID 系统中的任一系统上执行以下步骤。

步骤

1. 从任一网格上的主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 选择*添加连接*。
4. 输入连接的详细信息。

字段	**Description**
连接名称	帮助您识别此连接的唯一名称、例如"`Grid 1-Grid 2.`"
此网格的FQDN或IP	以下选项之一： • 当前已登录到的网格的FQDN • 此网格上HA组的VIP地址 • 此网格上管理节点或网关节点的IP地址。IP可以位于目标网格可以访问的任何网络上。
Port	要用于此连接的端口。您可以输入介于23000到23999之间的任何未使用端口号。 此连接中的两个网格将使用同一端口。您必须确保任一网格中的任何节点都不会将此端口用于其他连接。
此网格的证书有效天数	希望此网格在连接中的安全证书有效的天数。默认值为730天(2年)、但您可以输入1到762天之间的任何值。 保存连接时、StorageGRID 会自动为每个网格生成客户端和服务器证书。
为此网格配置密码短语	要登录到的网格的配置密码短语。

字段	Description
其他网格的FQDN或IP	以下选项之一： • 要连接到的网格的FQDN • 另一个网格上HA组的VIP地址 • 另一网格上的管理节点或网关节点的IP地址。IP可以位于源网格可以访问的任何网络上。

5. 选择*保存并继续*。
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。

   > 此文件包含密码(屏蔽为 *)和其他敏感详细信息、必须安全地存储和传输。

8. 选择*Close*(关闭*)返回到Grid Federation (网格联合)页面。
9. 确认新连接已显示且其*Connection statues*为*waits to connect *。
10. 提供 `connection-name.grid-federation` 文件分配给另一个网格的网格管理员。

完成连接

在要连接的StorageGRID 系统(另一个网格)上执行这些步骤。

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 选择*上传验证文件*以访问上传页面。
4. 选择*上传验证文件*。然后、浏览并选择从第一个网格下载的文件 (`connection-name.grid-federation`) 。

   此时将显示此连接的详细信息。

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

   通常、对连接两端的证书使用相同天数。

   > 如果连接任一端的证书过期、则连接将停止工作、复制将处于待定状态、直到证书更新为止。

6. 输入当前已登录的网格的配置密码短语。
7. 选择*保存并测试*。

此时将生成证书并测试连接。如果连接有效、则会显示一条成功消息、新连接将列在Grid Federation页面上。连接状态*将为*已连接。

如果出现错误消息、请解决所有问题。请参见 "对网格联合错误进行故障排除"。

8. 转到第一个网格上的"网格联合"页面并刷新浏览器。确认*连接状态*现在为*已连接*。
9. 建立连接后、安全地删除验证文件的所有副本。

   如果编辑此连接、则会创建一个新的验证文件。无法重复使用原始文件。

完成后

- 查看的注意事项 "管理允许的租户"。
- "创建一个或多个新租户帐户"，分配*使用网格联合连接*权限，然后选择新连接。
- "管理连接" 根据需要。您可以编辑连接值、测试连接、轮换连接证书或删除连接。
- "监控连接" 作为常规StorageGRID 监控活动的一部分。
- "排除连接故障"，包括解决与帐户克隆和跨网格复制相关的任何警报和错误。

管理网格联合连接

管理StorageGRID 系统之间的网格联合连接包括编辑连接详细信息、轮换证书、删除租户权限以及删除未使用的连接。

开始之前

- 您已使用登录到任一网格上的网格管理器 "支持的 Web 浏览器"。
- 您拥有所登录网格的root访问权限。

[[Edit_GRID_FED_CONNECTION]]编辑网格联合连接

您可以通过登录到连接中任一网格上的主管理节点来编辑网格联合连接。更改第一个网格后、必须下载新的验证文件并将其上传到另一个网格。

> 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、但只有在上传到第二个网格并进行保存和测试后、才会使用。

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均已联机。

   > 编辑网格联合连接时、StorageGRID 会尝试在第一个网格的所有管理节点上保存"`候选配置`"文件。如果无法将此文件保存到所有管理节点，则在选择*保存并测试*时会显示一条警告消息。

3. 选择*configuration*>*System*>*Grid Federation。

4. 使用“网格联合”页面或特定连接的详细信息页面上的*Actions*菜单编辑连接详细信息。请参见 "创建网格联合连接" 输入内容。

   操作菜单

   a. 选择连接的单选按钮。
   b. 选择*Actions*>*Edit*。
   c. 输入新信息。

   详细信息页面

   a. 选择连接名称以显示其详细信息。
   b. 选择 * 编辑 * 。
   c. 输入新信息。

5. 输入要登录到的网格的配置密码短语。
6. 选择*保存并继续*。

   新值将被保存、但在将新验证文件上传到另一个网格之前、这些值不会应用于连接。

7. 选择*下载验证文件*。

   要稍后下载此文件、请转到连接的详细信息页面。

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

   验证文件包含机密信息、必须安全地存储和传输。

9. 选择*Close*(关闭*)返回到Grid Federation (网格联合)页面。
10. 确认*连接状态*为*待定编辑*。

    如果在开始编辑连接时连接状态不是*conned*，则不会更改为*Pending edit*。

11. 提供 `connection-name.grid-federation` 文件分配给另一个网格的网格管理员。

完成对连接的编辑

通过将验证文件上传到其他网格来完成对连接的编辑。

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 选择*上传验证文件*以访问上传页面。
4. 选择*上传验证文件*。然后、浏览并选择从第一个网格下载的文件。
5. 输入当前已登录的网格的配置密码短语。

6. 选择*保存并测试*。

   如果可以使用编辑的值建立连接、则会显示一条成功消息。否则、将显示错误消息。查看消息并解决任何问题。

7. 关闭向导以返回到"网格联盟"页面。
8. 确认*连接状态*为*已连接*。
9. 转到第一个网格上的"网格联合"页面并刷新浏览器。确认*连接状态*现在为*已连接*。
10. 建立连接后、安全地删除验证文件的所有副本。

[[test_grid _ FED_CONNECTION]]测试网格联合连接

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 使用“网格联合”页面或详细信息页面上的*Actions*菜单测试特定连接。

   操作菜单

   a. 选择连接的单选按钮。
   b. 选择*Actions*>*Test*。

   详细信息页面

   a. 选择连接名称以显示其详细信息。
   b. 选择 * 测试连接 * 。

4. 查看连接状态：

连接状态	**Description**
已连接	两个网格均已连接并正常通信。
error	连接处于错误状态。例如、证书已过期或配置值不再有效。
待编辑	您已编辑此网格上的连接、但此连接仍在使用现有配置。要完成编辑、请将新验证文件上传到另一个网格。
正在等待连接	您已在此网格上配置连接、但在另一网格上连接尚未完成。从此网格下载验证文件并将其上传到另一个网格。
未知	连接处于未知状态、可能是由于网络问题描述 或脱机节点。

5. 如果连接状态为*Error*，请解决所有问题。然后，再次选择*测试连接*以确认问题描述 已修复。

[[rotate_grid _ FED_certificates]]旋转连接证书

每个网格联合连接都使用四个自动生成的SSL证书来保护此连接的安全。当每个网格的两个证书接近其到期日期时，“网格联合证书到期”警报将提醒您轮换证书。

> 如果连接任一端的证书过期、则连接将停止工作、复制将处于待定状态、直到证书更新为止。

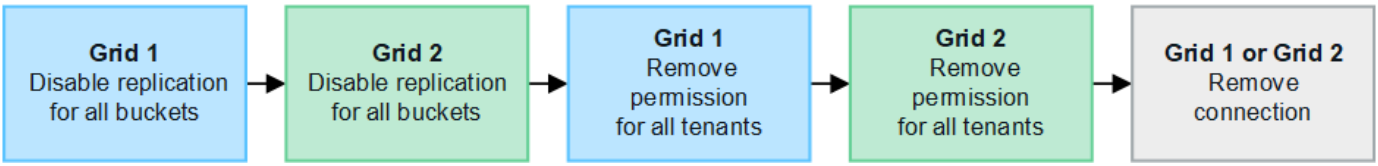
步骤

1. 从任一网格上的主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 从网格联盟页面上的任一选项卡中、选择连接名称以显示其详细信息。
4. 选择*证书*选项卡。
5. 选择*旋转证书*。
6. 指定新证书的有效天数。
7. 输入要登录到的网格的配置密码短语。
8. 选择*旋转证书*。
9. 根据需要、对连接中的另一个网格重复上述步骤。

   通常、对连接两端的证书使用相同天数。

[[remove_grid _ FED_CONNECTION]]删除网格联合连接

您可以从连接中的任一网格删除网格联合连接。如图所示、您必须在两个网格上执行前提条件步骤、以确认任一网格上的任何租户均未使用此连接。



删除连接之前、请注意以下事项：

- 删除连接不会删除已在网格之间复制的任何项目。例如、删除租户的权限后、不会从任一网格中删除存在于两个网格上的租户用户、组和对象。如果要删除这些项目、则必须手动将其从两个网格中删除。
- 删除连接后、任何正在等待复制的对象(已装载但尚未复制到另一个网格)的复制将永久失败。

对所有租户分段禁用复制

步骤

1. 从任一网格开始、从主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
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、请指示所有租户执行此操作 "禁用跨网格复制" 连接中两个网格上的所有存储分段。

> 如果任何租户分段已启用跨网格复制、则无法删除*使用网格联合连接*权限。每个租户帐户都必须在两个网格上为其分段禁用跨网格复制。

删除每个租户的权限

对所有租户分段禁用跨网格复制后、从两个网格上的所有租户中删除*使用网格联合权限*。

步骤

1. 选择*configuration*>*System*>*Grid Federation。
2. 选择连接名称以显示其详细信息。
3. 对于*允许的租户*选项卡上的每个租户、从每个租户中删除*使用网格联合连接*权限。请参见 "管理允许的租户"。
4. 对其他网格上允许的租户重复上述步骤。

断开连接

步骤

1. 如果任一网格上没有租户正在使用此连接，请选择*Remove*。
2. 查看确认消息，然后选择*Remove*。
   - 如果可以删除连接、则会显示一条成功消息。现在、两个网格中的网格联合连接均已删除。
   - 如果无法删除连接(例如、连接仍在使用中或出现连接错误)、则会显示一条错误消息。您可以执行以下任一操作：
     - 解决此错误(建议)。请参见 "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。

[[FORCE-Remove_GRY_FED_CONNECTION]]强制删除网格联合连接

如有必要，您可以强制删除未处于*已连接*状态的连接。

强制删除仅会从本地网格中删除此连接。要完全断开连接、请在两个滤线栅上执行相同的步骤。

步骤

1. 从确认对话框中，选择*Force remove*。

   此时将显示一条成功消息。无法再使用此网格联合连接。但是、租户分段可能仍会启用跨网格复制、并且某些对象副本可能已在连接中的网格之间进行复制。

2. 从连接中的另一个网格、从主管理节点登录到网格管理器。
3. 选择*configuration*>*System*>*Grid Federation。
4. 选择连接名称以显示其详细信息。
5. 选择*Remove*和*Yes*。
6. 选择*Force remove*以从该网格中删除连接。

管理网格联盟允许的租户

您可以允许新的S3租户帐户在两个StorageGRID 系统之间使用网格联合连接。如果允许租户使用连接、则需要执行特殊步骤来编辑租户详细信息或永久删除租户使用连接的权限。

开始之前

- 您已使用登录到任一网格上的网格管理器 "支持的 Web 浏览器"。
- 您拥有所登录网格的root访问权限。
- 您已拥有 "已创建网格联合连接" 两个网格之间。
- 您已查看的工作流 "帐户克隆" 和 "跨网格复制"。
- 根据需要、您已为连接中的两个网格配置单点登录(SSO)或标识联合。请参见 "什么是帐户克隆"。

创建允许的租户

如果要允许租户帐户使用网格联合连接进行帐户克隆和跨网格复制、请按照的常规说明进行操作 "创建新的S3租户" 并注意以下事项：

- 您可以从连接中的任一网格创建租户。创建租户的网格是_租 户的源网格_。
- 连接状态必须为*已连接*。
- 在创建新S3租户时只能选择*使用网格联合连接*权限；在编辑现有租户时不能启用此权限。
- 将新租户保存在第一个网格上后、相同的租户将自动复制到另一个网格。复制租户的网格是_租 户的目标网格_。
- 两个网格上的租户将具有相同的20位数帐户ID、名称、问题描述 、配额和权限。您也可以使用*问题描述 * 字段帮助确定哪个是源租户、哪个是目标租户。例如、在网格1上创建的租户的此问题描述 也会在复制到网格2的租户中显示：“此租户是在网格1上创建的。”
- 出于安全原因、本地root用户的密码不会复制到目标网格。

> 本地root用户登录到目标网格上的复制租户之前、该网格的网格管理员必须先登录 "更改本地root用户的密码"。

- 在两个网格上都有新租户可用后、租户用户可以执行以下操作：
  - 从租户的源网格中、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。请参见 "克隆租户组和用户"。
  - 创建新的S3访问密钥、可以选择将这些密钥克隆到租户的目标网格。请参见 "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分段、并在一个方向或两个方向上启用跨网格复制。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盟连接的租户的详细信息。

步骤

1. 选择 * 租户 * 。

2. 从租户页面中、选择租户名称以查看租户详细信息页面。

   如果这是租户的源网格(即、如果租户是在此网格上创建的)、则会显示一个横幅、提醒您租户已克隆到另一个网格。如果编辑或删除此租户、您所做的更改不会同步到其他网格。

3. (可选)选择*网格联合*选项卡 "监控网格联合连接"。

编辑允许的租户

如果您需要编辑具有*使用网格联合连接*权限的租户、请按照的常规说明进行操作 "编辑租户帐户" 并注意以下事项：

- 如果租户具有*使用网格联合连接*权限、您可以从连接中的任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另一个网格。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。
- 编辑租户时、不能选择其他网格联合连接。

删除允许的租户

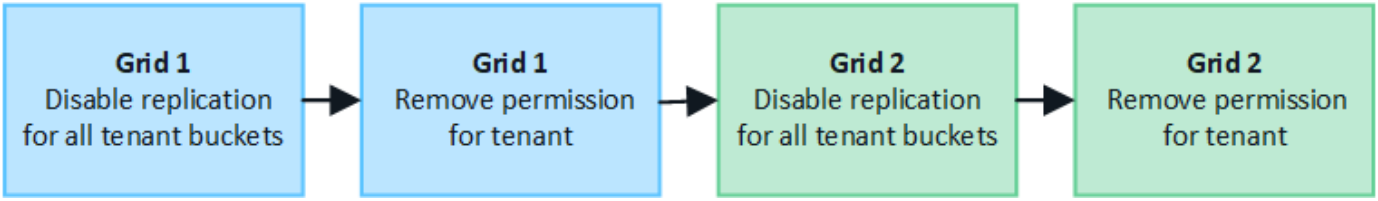
如果您需要删除具有*使用网格联合连接*权限的租户、请按照的常规说明进行操作 "删除租户帐户" 并注意以下事项：

- 在删除源网格上的原始租户之前、必须先删除源网格上帐户的所有分段。
- 在删除目标网格上的克隆租户之前、必须先删除目标网格上帐户的所有分段。
- 如果删除原始租户或克隆的租户、则帐户将无法再用于跨网格复制。
- 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、访问密钥和分段。
- 如果要删除目标网格上的克隆租户、则在向原始租户添加新组或用户时将发生克隆错误。

  要避免这些错误、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。

删除使用网格联合连接权限

要防止租户使用网格联合连接、您必须删除*使用网格联合连接*权限。



在删除租户使用网格联合连接的权限之前、请注意以下事项：

- 从租户中删除*使用网格联合连接*权限是一项永久性操作。您不能为此租户重新启用权限。
- 如果租户的任何分段已启用跨网格复制、则无法删除*使用网格联合连接*权限。租户帐户必须先为其所有分段禁用跨网格复制。

- 删除*使用网格联合连接*权限不会删除已在网格之间复制的任何项目。例如、删除租户的权限后、不会从任一网格中删除存在于两个网格上的任何租户用户、组和对象。如果要删除这些项目、则必须手动将其从两个网格中删除。

开始之前

- 您正在使用 "支持的 Web 浏览器"。
- 您对这两个网格都具有root访问权限。

禁用租户分段复制

首先、对所有租户分段禁用跨网格复制。

步骤

1. 从任一网格开始、从主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 选择连接名称以显示其详细信息。
4. 在*允许的租户*选项卡上、确定租户是否正在使用此连接。
5. 如果列出了租户、请指示他们这样做 "禁用跨网格复制" 连接中两个网格上的所有存储分段。

> 如果任何租户分段已启用跨网格复制、则无法删除*使用网格联合连接*权限。租户必须在两个网格上为其分段禁用跨网格复制。

删除租户的权限

为租户分段禁用跨网格复制后、您可以删除租户使用网格联合连接的权限。

步骤

1. 从主管理节点登录到网格管理器。
2. 从"网格联盟"页面或"租户"页面中删除此权限。

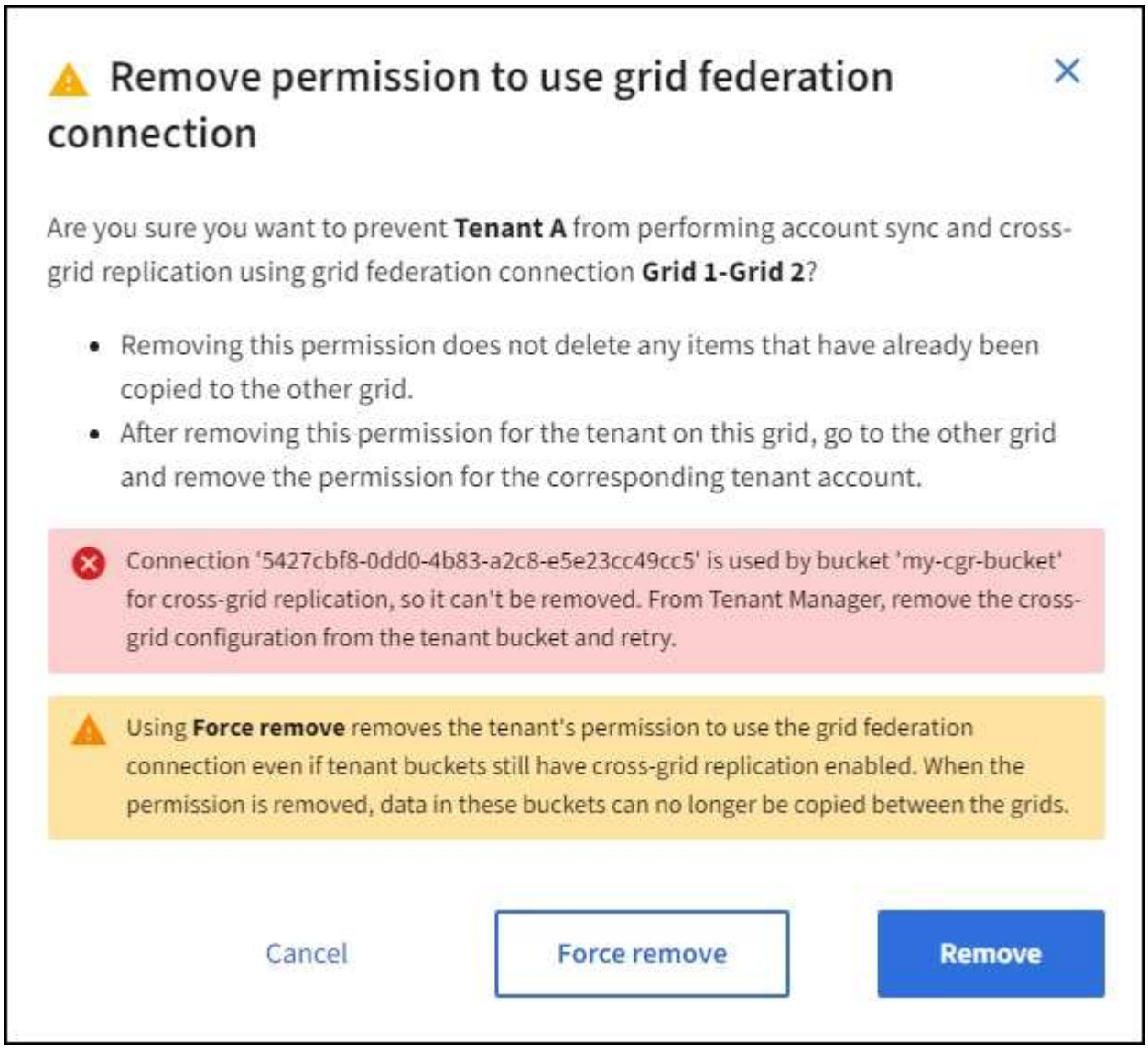
   网格联合页面

   a. 选择*configuration*>*System*>*Grid Federation。
   b. 选择连接名称以显示其详细信息页面。
   c. 在*允许的租户*选项卡上、选择租户的单选按钮。
   d. 选择*删除权限*。

   租户页面

   a. 选择 * 租户 * 。
   b. 选择租户的名称以显示详细信息页面。
   c. 在*网格联盟*选项卡上，选择连接的单选按钮。
   d. 选择*删除权限*。

3. 查看确认对话框中的警告，然后选择*Remove*。
   - 如果可以删除此权限、则会返回到详细信息页面、并显示一条成功消息。此租户无法再使用网格联合连接。
   - 如果一个或多个租户分段仍启用了跨网格复制、则会显示错误。



   您可以执行以下任一操作：

   - (建议。) 登录到租户管理器并为租户的每个分段禁用复制。请参见 "管理跨网格复制"。然后，重复这些步骤以删除*使用网格连接*权限。
   - 强制删除权限。请参见下一节。

4. 转到另一个网格并重复这些步骤、以删除另一个网格上同一租户的权限。

[[FORCE-Remove_Permission]]强制删除权限

如有必要、您可以强制删除租户使用网格联合连接的权限、即使租户分段已启用跨网格复制也是如此。

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

- 如果您强制删除*使用网格联合连接*权限，则所有正在等待复制到另一网格的对象(已加载但尚未复制)将继续被复制。为了防止这些进程中对象到达目标存储分段、您还必须删除租户对其他网格的权限。
- 删除*使用网格联合连接*权限后、插入到源存储分段中的任何对象都不会复制到目标存储分段。

步骤

1. 从主管理节点登录到网格管理器。
2. 选择*configuration*>*System*>*Grid Federation。
3. 选择连接名称以显示其详细信息页面。
4. 在*允许的租户*选项卡上、选择租户的单选按钮。
5. 选择*删除权限*。
6. 查看确认对话框中的警告，然后选择*Force remove*。

   此时将显示一条成功消息。此租户无法再使用网格联合连接。

7. 根据需要、转到另一个网格并重复这些步骤、以强制删除另一个网格上同一租户帐户的权限。例如、您应在其他网格上重复这些步骤、以防止进程中对象到达目标分段。

对网格联合错误进行故障排除

您可能需要对与网格联合连接、帐户克隆和跨网格复制相关的警报和错误进行故障排除。

网格联合连接警报和错误

您可能会收到有关网格联盟连接的警报或遇到错误。

在进行任何更改以解析连接问题描述 后，请测试该连接以确保连接状态返回到*conn岗位*。有关说明，请参见 "管理网格联合连接"。

Grid Federation connection failure警报

问题描述

已触发*网格联合连接失败*警报。

详细信息

此警报表示网格之间的网格联合连接不起作用。

建议的操作

1. 查看两个网格的网格联合页面上的设置。确认所有值均正确无误。请参见 "管理网格联合连接"。
2. 查看用于连接的证书。确保没有针对已过期的网格联合证书的警报、并且每个证书的详细信息有效。请参见中有关轮换连接证书的说明 "管理网格联合连接"。
3. 确认两个网格中的所有管理节点和网关节点均已联机且可用。解决可能影响这些节点的所有警报、然后重试。
4. 如果您为本地或远程网格提供了完全限定域名(FQDN)、请确认DNS服务器联机且可用。请参见 "什么是网格联合？" 了解网络连接、IP地址和DNS要求。

网格联合证书到期警报

问题描述

已触发*网格联合证书到期*警报。

详细信息

此警报指示一个或多个网格联合证书即将过期。

建议的操作

请参见中有关轮换连接证书的说明 "管理网格联合连接"。

编辑网格联合连接时出错

问题描述

编辑网格联合连接时，如果选择*保存并测试*，则会看到以下警告消息："Ffailed to create a candidate configuration file on one or more Nides"(无法在一个或多个节点上创建候选配置文件)。

详细信息

编辑网格联合连接时、StorageGRID 会尝试在第一个网格的所有管理节点上保存"候选配置"文件。如果无法将此文件保存到所有管理节点(例如、由于某个管理节点脱机)、则会显示一条警告消息。

建议的操作

1. 从用于编辑连接的网格中，选择*N节点*。
2. 确认该网格的所有管理节点均已联机。
3. 如果任何节点处于脱机状态、请将其恢复联机、然后重新尝试编辑连接。

帐户克隆错误

无法登录到克隆的租户帐户

问题描述

您无法登录到克隆的租户帐户。租户管理器登录页面上的错误消息为"`您的此帐户凭据无效。请重试。`"

详细信息

出于安全原因、在将租户帐户从租户的源网格克隆到租户的目标网格时、您为租户的本地root用户设置的密码不会克隆。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、网格管理员必须首先登录 "更改本地root用户的密码" 在目标网格上。

克隆的本地用户必须在目标网格上为该用户添加密码、才能登录到租户的目标网格。有关说明，请参见 "管理本地用户" 在使用租户管理器的说明中。

租户在不使用克隆的情况下创建

问题描述

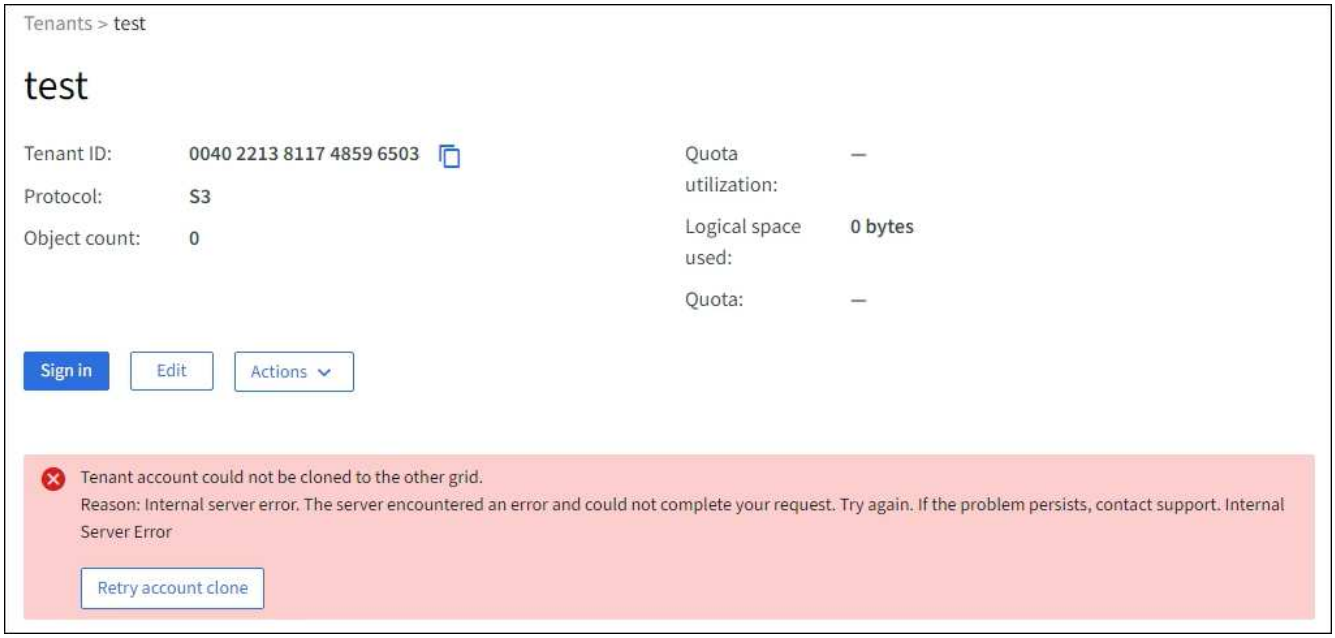
在使用*使用网格联合连接*权限创建新租户后、您会看到消息"`租户已创建但无克隆`"。

详细信息

如果连接状态更新延迟，发生原因 则可能会出现此问题描述 ，这可能会使运行状况不正常的连接显示为*conn 象*。

建议的操作

1. 查看错误消息中列出的原因、并解决可能导致连接无法正常工作的任何网络或其他问题。请参见 网格联合连接警报和错误。
2. 按照说明在中测试网格联合连接 "管理网格联合连接" 以确认问题描述 已修复。
3. 从租户的源网格中、选择*租户*。
4. 找到无法克隆的租户帐户。
5. 选择租户名称以显示详细信息页面。
6. 选择*重试帐户克隆*。



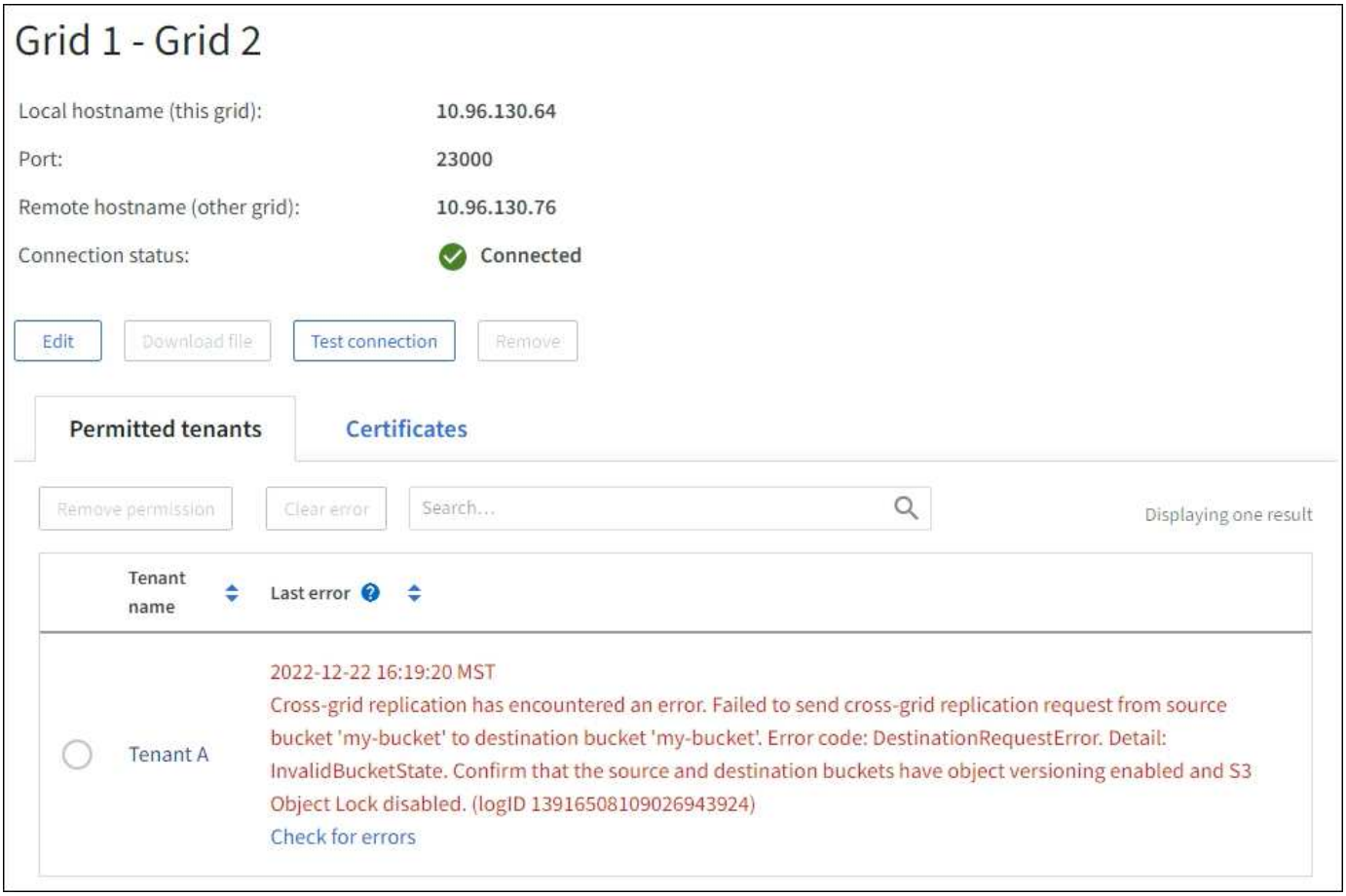
如果错误已解决、则租户帐户现在将克隆到另一个网格。

跨网格复制警报和错误

为连接或租户显示的最后一个错误

问题描述

时间 "查看网格联合连接" (或何时 "管理允许的租户" 对于连接)，您注意到连接详细信息页面上的“上次错误”列中出现错误。例如：



详细信息

对于每个网格联合连接、*最后一个错误*列显示租户的数据复制到另一个网格时发生的最新错误(如果有)。此列仅显示上次发生的跨网格复制错误；不会显示先前可能发生的错误。此列中可能会出现错误、原因如下：

- 未找到源对象版本。
- 未找到源存储分段。
- 已删除此目标存储分段。
- 目标存储分段已由其他帐户重新创建。
- 目标存储分段已暂停版本控制。
- 目标存储分段已由同一帐户重新创建、但现在已取消版本控制。

建议的操作

如果“上次错误”列中出现错误消息，请按照以下步骤操作：

1. 查看消息文本。
2. 执行任何建议的操作。例如、如果在目标存储分段上暂停版本控制以进行跨网格复制、请为此存储分段重新启用版本控制。
3. 从表中选择连接或租户帐户。
4. 选择*清除错误*。
5. 选择*是*以清除消息并更新系统状态。

6. 等待5-6分钟、然后将新对象插入存储分段。确认错误信息不会再次出现。

> 要确保清除错误消息、请在消息中的时间戳后至少等待5分钟、然后再输入新对象。

> 清除错误后，如果在另一个存储分段中载入对象，并且该存储分段也存在错误，则可能会出现一个新的*last error*。

7. 要确定是否有任何对象因存储分段错误而无法复制、请参见 "确定并重试失败的复制操作"。

跨网格复制永久故障警报

问题描述

已触发*跨网格复制永久失败*警报。

详细信息

此警报指示无法在两个网格上的分段之间复制租户对象、原因是需要用户干预才能解决。此警报通常是由源存储分段或目标存储分段的更改引起的。

建议的操作

1. 登录到触发警报的网格。
2. 进入*configuration*>*System*>*Grid Federation，找到警报中列出的连接名称。
3. 在允许的租户选项卡上、查看*上次错误*列以确定哪些租户帐户存在错误。
4. 要了解有关故障的更多信息、请参见中的说明 "监控网格联合连接" 以查看跨网格复制指标。
5. 对于每个受影响的租户帐户：
   a. 请参见中的说明 "监控租户活动" 确认租户未超过其在目标网格上用于跨网格复制的配额。
   b. 根据需要、增加目标网格上的租户配额、以允许保存新对象。
6. 对于每个受影响的租户、在两个网格上登录到租户管理器、以便比较存储分段列表。
7. 对于已启用跨网格复制的每个存储分段、请确认以下内容：
   - 同一租户在另一个网格上有对应的存储分段(必须使用确切名称)。
   - 这两个分段均已启用对象版本控制(不能在任一网格上暂停版本控制)。
   - 这两个分段均已禁用S3对象锁定。
   - 两个存储分段均未处于*删除对象：只读*状态。
8. 要确认问题描述 已解决、请参见中的说明 "监控网格联合连接" 要查看跨网格复制指标、或执行以下步骤：
   a. 返回到"网格联盟"页面。
   b. 选择受影响的租户、然后在*上次错误*列中选择*清除错误*。
   c. 选择*是*以清除消息并更新系统状态。
   d. 等待5-6分钟、然后将新对象插入存储分段。确认错误信息不会再次出现。

   > 要确保清除错误消息、请在消息中的时间戳后至少等待5分钟、然后再输入新对象。

解决警报后、可能需要长达一天时间才能清除警报。

a. 转至 "确定并重试失败的复制操作" 标识未能复制到其他网格的任何对象或删除标记、并根据需要重试复制。

跨网格复制资源不可用警报

问题描述

已触发*跨网格复制资源不可用*警报。

详细信息

此警报表示跨网格复制请求处于待处理状态、因为资源不可用。例如、可能存在网络错误。

建议的操作

1. 监控警报以查看问题描述 是否自行解决。
2. 如果问题描述 仍然存在，请确定其中一个网格对于同一连接是否具有*Grid Federation connection failure*警报，或者对于某个节点是否具有*Unable to与节点*通信警报。当您解决这些警报时、可能会解决此警报。
3. 要了解有关故障的更多信息、请参见中的说明 "监控网格联合连接" 以查看跨网格复制指标。
4. 如果无法解决此警报、请联系技术支持。

解决问题描述 后、跨网格复制将正常进行。

确定并重试失败的复制操作

解决*跨网格复制永久失败*警报后，您应确定是否有任何对象或删除标记无法复制到另一网格。然后、您可以重新创建这些对象或使用网格管理API重试复制。

*跨网格复制永久失败*警报指示无法在两个网格上的分段之间复制租户对象、原因是需要用户干预才能解决。此警报通常是由源存储分段或目标存储分段的更改引起的。有关详细信息，请参见 "对网格联合错误进行故障排除"。

确定是否有任何对象无法复制

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

您可以使用 "Audy-讲解 工具" 将结果转换为易于阅读的格式。

开始之前

- 您具有 root 访问权限。
- 您拥有 `Passwords.txt` 文件
- 您知道主管理节点的IP地址。

步骤

1. 登录到主管理节点：

a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`

b. 输入中列出的密码 `Passwords.txt` 文件

c. 输入以下命令切换到root： `su -`

d. 输入中列出的密码 `Passwords.txt` 文件

以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 在audit.log中搜索CGRR消息、并使用audy-expand工具对结果进行格式化。

例如、此命令将对过去30分钟内的所有CGRR消息进行greps、并使用audy-explast工具。

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

此命令的结果类似于此示例、其中包含六条CGRR消息的条目。在此示例中、所有跨网格复制请求均返回一个一般错误、因为无法复制对象。前三个错误用于"replicate object"操作、后三个错误用于"replicate delete marker"操作。

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

每个条目都包含以下信息：

字段	**Description**
CGRR跨网格复制请求	请求的名称

字段	Description
租户	租户的帐户ID
连接	网格联合连接的ID
操作	正在尝试的复制操作类型： • 复制对象 • 复制删除标记 • 复制多部分对象
存储分段	分段名称
对象	对象名称
version	对象的版本标识
error	错误的类型。如果跨网格复制失败、则错误为"General error"。

重试失败的复制

生成对象列表并删除未复制到目标存储分段的标记并解决底层问题后、您可以通过以下两种方式之一重试复制：

- 将每个对象重新装入源存储分段。
- 使用网格管理专用API、如所述。

步骤

1. 在网格管理器的顶部，选择帮助图标，然后选择*API documents*。
2. 选择*转至专用API文档*。

> 标记为"`private`"的StorageGRID API端点如有更改、恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

3. 在*cross-grid复制-高级*部分中，选择以下端点：

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

4. 选择 * 试用 * 。
5. 在*body文本框中，将*versionID*的示例条目替换为audit.log中与失败的跨网格复制请求对应的版本ID。

   请务必在字符串周围保留双引号。

6. 选择 * 执行 * 。
7. 确认服务器响应代码为*204*，表示对象或删除标记已标记为等待跨网格复制到另一网格。

Pending表示跨网格复制请求已添加到内部队列进行处理。

监控复制重试次数

您应监控复制重试操作以确保其完成。

将对象或删除标记复制到另一个网格可能需要数小时甚至更长时间。

您可以通过以下两种方式之一监控重试操作：

- 使用S3 "HEAD 对象" 或 "获取对象" 请求。响应包括特定于StorageGRID的 `x-ntap-sg-cgr-replication-status` 响应标头、它将具有以下值之一：

网格	复制状态
源	• *SUCCESS *：复制成功。 • *pending *：对象尚未复制。 • 失败：复制失败并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

- 使用网格管理专用API、如所述。

步骤

1. 在专用API文档的*跨网格复制-高级*部分中，选择以下端点：

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. 选择 * 试用 * 。
3. 在参数部分中、输入您在中使用的版本ID `cross-grid-replication-retry-failed` 请求。
4. 选择 * 执行 * 。
5. 确认服务器响应代码为*200*。
6. 查看复制状态、该状态为以下状态之一：
   - *pending *：对象尚未复制。
   - 已完成：复制成功。
   - **failer**：复制失败并出现永久故障。用户必须解决此错误。

管理安全性

管理安全性：概述

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

管理加密

StorageGRID 提供了多种数据加密选项。您应该 "查看可用的加密方法" 以确定哪些解决方案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" 即使从数据中心删除设备、您也可以保护StorageGRID 数据。对设备卷进行加密后、您将无法访问设备上的任何数据、除非此节点可以与KMS进行通信。

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

管理代理设置

如果您使用的是S3平台服务或云存储池、则可以配置 "存储代理服务器" 存储节点和外部S3端点之间。如果使用HTTPS或HTTP发送AutoSupport 消息、则可以配置 "管理代理服务器" 在管理节点和技术支持之间。

控制防火墙

为了增强系统的安全性、您可以通过在中打开或关闭特定端口来控制对StorageGRID 管理节点的访问 "外部防火墙"。您还可以通过配置每个节点来控制对其的网络访问 "内部防火墙"。您可以阻止对除部署所需端口以外的所有端口进行访问。

查看 **StorageGRID** 加密方法

StorageGRID 提供了多种数据加密选项。您应查看可用的方法，以确定哪些方法符合数据保护要求。

下表简要总结了 StorageGRID 中可用的加密方法。

加密选项	工作原理	适用场景
网格管理器中的密钥管理服务器（KMS）	您 "配置密钥管理服务器" 对于StorageGRID 站点、请执行以下操作：和 "为此设备启用节点加密"。然后，设备节点将连接到 KMS 以请求密钥加密密钥（Key Encryption Key， KEK）。此密钥用于对每个卷上的数据加密密钥（DEK）进行加密和解密。	安装期间启用了 * 节点加密 * 的设备节点。设备上的所有数据均可防止物理丢失或从数据中心删除。 只有存储节点和服务设备才支持使用KMS管理加密密钥。

加密选项	工作原理	适用场景
SANtricity System Manager 中的驱动器安全性	如果为SG5700或SG6000存储设备启用了驱动器安全性功能、则可以使用 "SANtricity 系统管理器" 以创建和管理安全密钥。要访问受保护驱动器上的数据，需要使用此密钥。	具有全磁盘加密(Full Disk Encryption、FD)驱动器或FIPS驱动器的存储设备。安全驱动器上的所有数据均可防止物理丢失或从数据中心中删除。不能用于某些存储设备或任何服务设备。
存储对象加密	您可以启用 "存储对象加密" 选项。启用后、在存储分段级别或对象级别未加密的任何新对象都会在数据导入期间进行加密。	新载入的 S3 和 Swift 对象数据。 现有存储对象未加密。对象元数据和其他敏感数据不会加密。
S3 存储分段加密	问题描述 PUT 分段加密请求以对分段启用加密。在对象级别未加密的任何新对象都会在导入期间进行加密。	仅新载入的 S3 对象数据。 必须为存储分段指定加密。现有存储分段对象未加密。对象元数据和其他敏感数据不会加密。 "对存储分段执行的操作"
S3 对象服务器端加密（SS3）	您可以问题描述 S3请求以存储对象并包括 `x-amz-server-side-encryption` 请求标题。	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据不会加密。 StorageGRID 负责管理密钥。 "使用服务器端加密"
使用客户提供的密钥（SSI-C）进行 S3 对象服务器端加密	您可以问题描述 S3 请求以存储一个对象并包含三个请求标头。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	仅新载入的 S3 对象数据。 必须为对象指定加密。对象元数据和其他敏感数据不会加密。 密钥在 StorageGRID 之外进行管理。 "使用服务器端加密"

加密选项	工作原理	适用场景
外部卷或数据存储库加密	如果您的部署平台支持，则可以在 StorageGRID 外部使用加密方法对整个卷或数据存储库进行加密。	所有对象数据，元数据和系统配置数据，假设每个卷或数据存储库都已加密。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。
StorageGRID 外部的对象加密	在将对象数据和元数据载入 StorageGRID 之前，您可以在 StorageGRID 外部使用加密方法对这些数据和元数据进行加密。	仅限对象数据和元数据（系统配置数据不加密）。 外部加密方法可以更严格地控制加密算法和密钥。可以与列出的其他方法结合使用。 "Amazon Simple Storage Service—开发人员指南：使用客户端加密保护数据"

使用多种加密方法

根据您的要求，您一次可以使用多种加密方法。例如：

- 您可以使用 KMS 来保护设备节点，也可以使用 SANtricity 系统管理器中的驱动器安全功能在同一设备中的自加密驱动器上 " d 进行灵活加密 " 数据。
- 您可以使用KMS保护设备节点上的数据、也可以使用存储对象加密选项对所有对象进行加密。

如果只有一小部分对象需要加密，请考虑在存储分段或单个对象级别控制加密。启用多个级别的加密会产生额外的性能成本。

管理证书

管理安全证书：概述

安全证书是一个小型数据文件，用于在 StorageGRID 组件之间以及 StorageGRID 组件与外部系统之间创建安全可信的连接。

StorageGRID 使用两种类型的安全证书：

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

当客户端使用 HTTPS 连接到服务器时，服务器会使用包含公有 密钥的服务器证书进行响应。客户端通过将服务器签名与其证书副本上的签名进行比较来验证此证书。如果签名匹配，则客户端将使用相同的公有 密钥启动与服务器的会话。

StorageGRID 用作某些连接的服务器（例如负载平衡器端点）或其他连接的客户端（例如 CloudMirror 复制服务）。

- 默认网格 CA 证书 *

StorageGRID 包含一个内置证书颁发机构（ Certificate Authority ， CA ），可在系统安装期间生成内部网格 CA 证书。默认情况下，使用网格 CA 证书保护内部 StorageGRID 流量。外部证书颁发机构（ CA ）可以对完全符合组织信息安全策略的自定义证书进行问题描述 。虽然您可以在非生产环境中使用网格 CA 证书，但在生产环境中，最佳做法是使用由外部证书颁发机构签名的自定义证书。也支持不带证书的不安全连接、但不建议这样做。

- 自定义CA证书不会删除内部证书；但是、自定义证书应是为验证服务器连接而指定的证书。
- 所有自定义证书都必须满足 "服务器证书的系统强化准则"。
- StorageGRID 支持将 CA 中的证书捆绑到一个文件中（称为 CA 证书包）。

> StorageGRID 还包括在所有网格上相同的操作系统 CA 证书。在生产环境中，请确保指定一个由外部证书颁发机构签名的自定义证书，以替代操作系统 CA 证书。

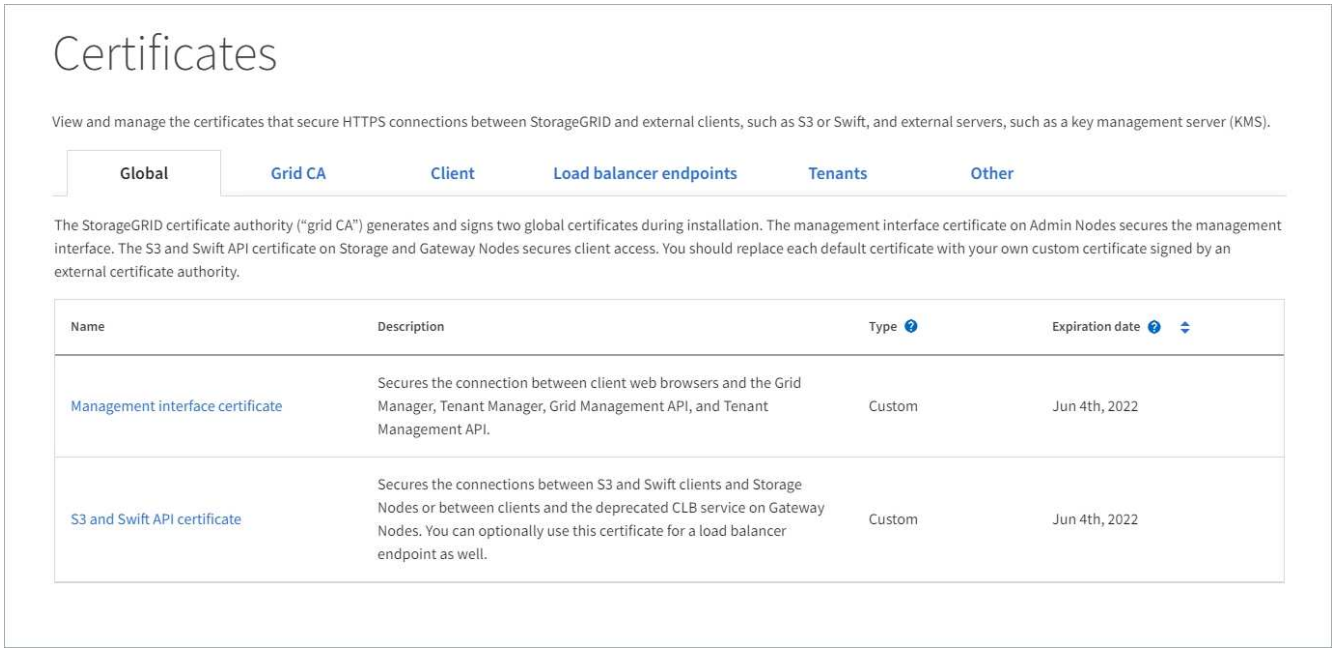
服务器和客户端证书类型的变体通过多种方式实现。在配置系统之前，您应准备好特定 StorageGRID 配置所需的所有证书。

访问安全证书

您可以在一个位置访问有关所有 StorageGRID 证书的信息，以及指向每个证书的配置工作流的链接。

步骤

1. 在网格管理器中，选择*configuration*>*Security*>*Certificates*。



2. 在证书页面上选择一个选项卡，以获取有关每个证书类别的信息并访问证书设置。只有在拥有相应权限的情况下，才能访问选项卡。
   - * 全局 *： 确保从 Web 浏览器和外部 API 客户端访问 StorageGRID 的安全。

- * 网格 CA*： 保护内部 StorageGRID 流量的安全。
- * 客户端 *： 保护外部客户端与 StorageGRID Prometheus 数据库之间的连接。
- * 负载平衡器端点 *： 确保 S3 和 Swift 客户端与 StorageGRID 负载平衡器之间的连接安全。
- * 租户 *： 保护与身份联合服务器或从平台服务端点到 S3 存储资源的连接。
- * 其他 *： 保护需要特定证书的 StorageGRID 连接。

下面介绍了每个选项卡，并提供了指向其他证书详细信息的链接。

全局

这些全局证书可确保从 Web 浏览器以及外部 S3 和 Swift API 客户端访问 StorageGRID 的安全。在安装期间， StorageGRID 证书颁发机构最初会生成两个全局证书。生产环境的最佳实践是使用由外部证书颁发机构签名的自定义证书。

- [管理接口证书]：确保客户端 Web 浏览器与 StorageGRID 管理界面的连接安全。
- S3 和 Swift API 证书：保护与存储节点，管理节点和网关节点的客户端 API 连接的安全， S3 和 Swift 客户端应用程序使用这些连接上传和下载对象数据。

有关已安装的全局证书的信息包括：

- * 名称 * ： 证书名称，其中包含用于管理证书的链接。
- * 问题描述 *
- * 类型 * ： 自定义或默认。+ 为了提高网格安全性，您应始终使用自定义证书。
- * 到期日期 * ： 如果使用默认证书，则不会显示到期日期。

您可以

- 将默认证书替换为由外部证书颁发机构签名的自定义证书，以提高网格安全性：
  - "替换由 StorageGRID 生成的默认管理接口证书" 用于网格管理器和租户管理器连接。
  - "替换 S3 和 Swift API 证书" 用于存储节点和负载平衡器端点(可选)连接。
- "还原默认管理接口证书。"
- "还原默认 S3 和 Swift API 证书。"
- "使用脚本生成新的自签名管理接口证书。"
- 复制或下载 "管理接口证书" 或 "S3 和 Swift API 证书"。

网格 **CA**

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

证书信息包括证书到期日期和证书内容。

您可以 "复制或下载网格CA证书"，但您无法更改它。

客户端

客户端证书由外部证书颁发机构生成，用于保护外部监控工具与 StorageGRID Prometheus 数据库之间的连接。

证书表中的每个已配置客户端证书都有一行，用于指示此证书是否可用于 Prometheus 数据库访问以及证书到期日期。

您可以

- "上传或生成新的客户端证书。"
- 选择一个证书名称以显示证书详细信息，您可以在其中执行以下操作：

    - "更改客户端证书名称。"
    - "设置 Prometheus 访问权限。"
    - "上传并替换客户端证书。"
    - "复制或下载客户端证书。"
    - "删除客户端证书。"
- 选择 * 操作 * 以快速执行 "编辑"， "附加"或 "删除" 客户端证书。您最多可以选择 10 个客户端证书，并使用 * 操作 * > * 删除 * 一次删除这些证书。

负载平衡器端点

负载平衡器端点证书 保护S3和Swift客户端之间的连接以及网关节点和管理节点上的StorageGRID 负载平衡器服务。

负载平衡器端点表对每个已配置的负载平衡器端点都有一行，用于指示此端点是否使用全局 S3 和 Swift API 证书或自定义负载平衡器端点证书。此外，还会显示每个证书的到期日期。

> 对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

您可以

- "查看负载平衡器端点"，包括其证书详细信息。
- "为 FabricPool 指定负载平衡器端点证书。"
- "使用全局 S3 和 Swift API 证书" 而不是生成新的负载平衡器端点证书。

Tenants

租户可以使用 身份联合服务器证书 或 平台服务端点证书 以确保其与 StorageGRID 的连接安全。

租户表中的每个租户都有一行，用于指示每个租户是否有权使用自己的身份源或平台服务。

您可以

- "选择一个租户名称以登录到租户管理器"
- "选择租户名称以查看租户身份联合详细信息"
- "选择租户名称以查看租户平台服务详细信息"
- "在创建端点期间指定平台服务端点证书"

其他

StorageGRID 会将其他安全证书用于特定目的。这些证书按其功能名称列出。其他安全证书包括：

- 云存储池证书
- 通过电子邮件发送警报通知证书
- 外部系统日志服务器证书
- 网格联合连接证书
- 身份联合证书

- 密钥管理服务器（KMS）证书
- 单点登录证书

信息指示函数使用的证书类型及其服务器和客户端证书的到期日期（如果适用）。选择功能名称将打开一个浏览器选项卡，您可以在此查看和编辑证书详细信息。

> 只有在拥有相应权限的情况下，才能查看和访问其他证书的信息。

您可以

- "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"
- "指定外部系统日志服务器证书"
- "旋转网格联合连接证书"
- "查看和编辑身份联合证书"
- "上传密钥管理服务器（KMS）服务器和客户端证书"
- "手动为依赖方信任指定SSO证书"

安全证书详细信息

下面介绍了每种类型的安全证书、并提供了指向实施说明的链接。

管理接口证书

证书类型	**Description**	导航位置	详细信息
服务器	对客户端 Web 浏览器和 StorageGRID 管理界面之间的连接进行身份验证，使用户能够访问网格管理器和租户管理器，而不会出现安全警告。 此证书还会对网格管理 API 和租户管理 API 连接进行身份验证。 您可以使用安装期间创建的默认证书，也可以上传自定义证书。	• 配置 * > * 安全性 * > * 证书 *，选择 * 全局 * 选项卡，然后选择 * 管理接口证书 *	"配置管理接口证书"

S3 和 Swift API 证书

证书类型	**Description**	导航位置	详细信息
服务器	对存储节点和负载平衡器端点的安全S3或Swift客户端连接进行身份验证(可选)。	• 配置 * > * 安全性 * > * 证书 *，选择 * 全局 * 选项卡，然后选择 * S3 和 Swift API 证书 *	"配置 S3 和 Swift API 证书"

网格 **CA** 证书

请参见 默认网格 CA 证书问题描述。

管理员客户端证书

证书类型	**Description**	导航位置	详细信息
客户端	安装在每个客户端上，使 StorageGRID 能够对外部客户端访问进行身份验证。 • 允许授权的外部客户端访问 StorageGRID Prometheus 数据库。 • 允许使用外部工具安全监控 StorageGRID 。	• 配置 * > * 安全性 * > * 证书 *，然后选择 * 客户端 * 选项卡	"配置客户端证书"

负载平衡器端点证书

证书类型	Description	导航位置	详细信息
服务器	对 S3 或 Swift 客户端与网关节点和管理节点上的 StorageGRID 负载平衡器服务之间的连接进行身份验证。您可以在配置负载平衡器端点时上传或生成负载平衡器证书。客户端应用程序在连接到 StorageGRID 时使用负载平衡器证书来保存和检索对象数据。 您也可以使用自定义版本的全局 S3 和 Swift API 证书 用于对与负载平衡器服务的连接进行身份验证的证书。如果使用全局证书对负载平衡器连接进行身份验证、则无需为每个负载平衡器端点上载或生成单独的证书。 • 注意： * 用于负载平衡器身份验证的证书是正常 StorageGRID 操作期间使用量最多的证书。	• 配置 * > * 网络 * > * 负载平衡器端点 *	• "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	Description	导航位置	详细信息
服务器	对从 StorageGRID 云存储池到外部存储位置（例如 S3 Glacier 或 Microsoft Azure Blob 存储）的连接进行身份验证。每种云提供商类型都需要一个不同的证书。	• ILM * > * 存储池 *	"创建云存储池"

通过电子邮件发送警报通知证书

证书类型	Description	导航位置	详细信息
服务器和客户端	对 SMTP 电子邮件服务器与用于警报通知的 StorageGRID 之间的连接进行身份验证。 • 如果与 SMTP 服务器的通信需要传输层安全（Transport Layer Security， TLS），则必须指定电子邮件服务器 CA 证书。 • 仅当 SMTP 电子邮件服务器需要客户端证书进行身份验证时，才指定客户端证书。	• 警报 * > * 电子邮件设置 *	"为警报设置电子邮件通知"

外部系统日志服务器证书

证书类型	Description	导航位置	详细信息
服务器	对在 StorageGRID 中记录事件的外部系统日志服务器之间的 TLS 或 RELP/TLS 连接进行身份验证。 • 注： * 与外部系统日志服务器的 TCP，RELP/TCP 和 UDP 连接不需要外部系统日志服务器证书。	• 配置 * > * 监控 * > * 审核和系统日志服务器 *，然后选择 * 配置外部系统日志服务器 *	"配置外部系统日志服务器"

网格联合连接证书

证书类型	Description	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*	• "创建网格联合连接" • "轮换连接证书"

身份联合证书

证书类型	**Description**	导航位置	详细信息
服务器	对 StorageGRID 与外部身份提供程序（例如 Active Directory ， OpenLDAP 或 Oracle 目录服务器）之间的连接进行身份验证。用于身份联合，允许管理组和用户由外部系统管理。	• 配置 * > * 访问控制 * > * 身份联合 *	"使用身份联合"

密钥管理服务器（ **KMS** ）证书

证书类型	**Description**	导航位置	详细信息
服务器和客户端	对 StorageGRID 与外部密钥管理服务器（ KMS ）之间的连接进行身份验证，该服务器可为 StorageGRID 设备节点提供加密密钥。	• 配置 * > * 安全性 * > * 密钥管理服务器 *	"添加密钥管理服务器（ KMS ）"

平台服务端点证书

证书类型	**Description**	导航位置	详细信息
服务器	对从 StorageGRID 平台服务到 S3 存储资源的连接进行身份验证。	• 租户管理器 * > * 存储（ S3 ） * > * 平台服务端点 *	"创建平台服务端点" "编辑平台服务端点"

单点登录（ **SSO** ）证书

证书类型	**Description**	导航位置	详细信息
服务器	对身份联合服务（例如 Active Directory 联合身份验证服务（ AD FS ））与用于单点登录（ SSO ）请求的 StorageGRID 之间的连接进行身份验证。	• 配置 * > * 访问控制 * > * 单点登录 *	"配置单点登录"

证书示例

示例 **1** ： 负载平衡器服务

在此示例中， StorageGRID 充当服务器。

1. 您可以在 StorageGRID 中配置负载平衡器端点并上传或生成服务器证书。

2. 您可以配置与负载平衡器端点的 S3 或 Swift 客户端连接，并将同一证书上传到客户端。
3. 当客户端要保存或检索数据时，它会使用 HTTPS 连接到负载平衡器端点。
4. StorageGRID 会使用包含公有 密钥的服务器证书进行响应，并使用基于私钥的签名进行响应。
5. 客户端通过将服务器签名与其证书副本上的签名进行比较来验证此证书。如果签名匹配，客户端将使用相同的公有 密钥启动会话。
6. 客户端将对象数据发送到 StorageGRID 。

示例 **2**： 外部密钥管理服务器（ **KMS** ）

在此示例中， StorageGRID 充当客户端。

1. 您可以使用外部密钥管理服务器软件将 StorageGRID 配置为 KMS 客户端，并获取 CA 签名的服务器证书，公有 客户端证书以及客户端证书的专用密钥。
2. 使用网格管理器，您可以配置 KMS 服务器并上传服务器和客户端证书以及客户端专用密钥。
3. 当 StorageGRID 节点需要加密密钥时，它会向 KMS 服务器发出请求，请求包含证书中的数据以及基于私钥的签名。
4. KMS 服务器会验证证书签名，并决定它可以信任 StorageGRID 。
5. KMS 服务器使用经过验证的连接进行响应。

配置服务器证书

支持的服务器证书类型

StorageGRID 系统支持使用 RSA 或 ECDSA （椭圆曲线数字签名算法）加密的自定义证书。

> 安全策略的密码类型必须与服务器证书类型匹配。例如、RSA密钥需要RSA证书、而ECDSA密钥需要ECDSA证书。请参见 "管理安全证书"。如果您配置的自定义安全策略与服务器证书不兼容、则可以执行此操作 "暂时还原为默认安全策略"。

有关StorageGRID 如何保护REST API的客户端连接的详细信息、请参阅 "为S3 REST API配置安全性" 或 "配置Swift REST API的安全性"。

配置管理接口证书

您可以将默认管理接口证书替换为一个自定义证书，使用户可以访问 Grid Manager 和租户管理器，而不会遇到安全警告。您还可以还原到默认管理接口证书或生成新的管理接口证书。

关于此任务

默认情况下，每个管理节点都会获得一个由网格 CA 签名的证书。这些 CA 签名的证书可以替换为一个通用的自定义管理接口证书和相应的专用密钥。

由于所有管理节点都使用一个自定义管理接口证书，因此，如果客户端在连接到网格管理器和租户管理器时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有管理节点匹配。

您需要在服务器上完成配置，根据所使用的根证书颁发机构（CA），用户可能还需要在用于访问网格管理器和租户管理器的 Web 浏览器中安装网格 CA 证书。

> 为确保操作不会因服务器证书失败而中断，当此服务器证书即将到期时，将触发*管理接口的服务器证书到期*警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在全局选项卡上查看管理接口证书的到期日期来查看当前证书的到期时间。

> 如果您要使用域名而非 IP 地址访问网格管理器或租户管理器，则在发生以下任一情况时，浏览器将显示证书错误，并且无法绕过此错误：
>
> - 您的自定义管理接口证书将过期。
> - 您 从自定义管理接口证书还原到默认服务器证书。

添加自定义管理接口证书

要添加自定义管理接口证书，您可以提供自己的证书或使用网格管理器生成一个证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。
b. 上传所需的服务器证书文件：
   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - 证书专用密钥:自定义服务器证书专用密钥文件 (`.key`）。

     EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。
c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。
   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。
d. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

生成证书

生成服务器证书文件。

生产环境的最佳实践是使用由外部证书颁发机构签名的自定义管理接口证书。

a. 选择 * 生成证书 * 。
b. 指定证书信息：

字段	**Description**
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。

字段	Description
有效天数	创建后证书过期的天数。
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。+ 自定义管理接口证书用于此后与网格管理器，租户管理器，网格管理器 API 或租户管理器 API 的所有新连接。

5. 刷新页面以确保 Web 浏览器已更新。

   上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 添加自定义管理接口证书后， " 管理接口证书 " 页面将显示正在使用的证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认管理接口证书

您可以使用网格管理器和租户管理器连接的默认管理接口证书还原到。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 使用默认证书 * 。

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

4. 刷新页面以确保 Web 浏览器已更新。

使用脚本生成新的自签名管理接口证书

如果需要严格验证主机名，可以使用脚本生成管理接口证书。

开始之前

- 您具有特定的访问权限。
- 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. 获取每个管理节点的完全限定域名（FQDN）。
2. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@primary_Admin_Node_IP`
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。

3. 使用新的自签名证书配置 StorageGRID 。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - 适用于 `--domains`下、使用通配符表示所有管理节点的完全限定域名。例如：`*.ui.storagegrid.example.com` 使用*通配符表示 `admin1.ui.storagegrid.example.com` 和 `admin2.ui.storagegrid.example.com`。
   - 设置 `--type` to `management` 配置网格管理器和租户管理器使用的管理接口证书。
   - 默认情况下，生成的证书有效期为一年（365 天），必须在证书过期之前重新创建。您可以使用 `--days` 用于覆盖默认有效期的参数。

     证书的有效期从何时开始 `make-certificate` 已运行。您必须确保管理客户端与 StorageGRID 同步到同一个时间源；否则，客户端可能会拒绝此证书。

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

     生成的输出包含管理 API 客户端所需的公有 证书。

4. 选择并复制证书。

   在您的选择中包括开始和结束标记。

5. 从命令 Shell 中注销。 `$ exit`
6. 确认已配置证书：
   a. 访问网格管理器。
   b. 选择 * 配置 * > * 安全性 * > * 证书 *
   c. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
7. 将管理客户端配置为使用您复制的公有 证书。包括开始和结束标记。

下载或复制管理接口证书

您可以保存或复制管理接口证书内容，以便在其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * 管理接口证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或CA包 `.pem` 文件如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

您可以替换或还原用于将S3或Swift客户端连接到存储节点或负载平衡器端点的服务器证书。替换的自定义服务器证书特定于您的组织。

关于此任务

默认情况下，每个存储节点都会获得一个由网格 CA 签名的 X.509 服务器证书。这些 CA 签名的证书可以替换为一个通用的自定义服务器证书和相应的专用密钥。

所有存储节点都使用一个自定义服务器证书，因此，如果客户端在连接到存储端点时需要验证主机名，则必须将此证书指定为通配符或多域证书。定义自定义证书，使其与网格中的所有存储节点匹配。

在服务器上完成配置后，您可能还需要在用于访问系统的 S3 或 Swift API 客户端中安装网格 CA 证书，具体取决于您正在使用的根证书颁发机构（ CA ）。

> 为确保操作不会因服务器证书失败而中断，根服务器证书即将到期时会触发*S3和Swift API*全局服务器证书到期*警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在全局选项卡上查看 S3 和 Swift API 证书的到期日期来查看当前证书的到期时间。

您可以上传或生成自定义 S3 和 Swift API 证书。

添加自定义 **S3** 和 **Swift API** 证书

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 使用自定义证书 * 。
4. 上传或生成证书。

上传证书

上传所需的服务器证书文件。

a. 选择 * 上传证书 * 。
b. 上传所需的服务器证书文件：
   - * 服务器证书 * ： 自定义服务器证书文件（ PEM 编码）。
   - 证书专用密钥:自定义服务器证书专用密钥文件 (`.key`）。

     EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

   - * CA bundle* ： 一个可选文件，其中包含来自每个中间颁发证书颁发机构的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。
c. 选择证书详细信息以显示上传的每个自定义 S3 和 Swift API 证书的元数据和 PEM 。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。
   - 选择 * 下载证书 * 以保存证书文件，或者选择 * 下载 CA 捆绑包 * 以保存证书捆绑包。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

     例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。
d. 选择 * 保存 * 。

   自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

生成证书

生成服务器证书文件。

a. 选择 * 生成证书 * 。
b. 指定证书信息：

字段	**Description**
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。
有效天数	创建后证书过期的天数。

字段	Description
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可显示生成的自定义 S3 和 Swift API 证书的元数据和 PEM 。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 保存 * 。

   自定义服务器证书用于后续的新 S3 和 Swift 客户端连接。

5. 选择一个选项卡以显示默认 StorageGRID 服务器证书，已上传的 CA 签名证书或已生成的自定义证书的元数据。

   上传或生成新证书后，请留出最多一天的时间来清除任何相关证书到期警报。

6. 刷新页面以确保 Web 浏览器已更新。

7. 添加自定义 S3 和 Swift API 证书后， S3 和 Swift API 证书页面将显示正在使用的自定义 S3 和 Swift API 证书的详细证书信息。+ 您可以根据需要下载或复制证书 PEM 。

还原默认 **S3** 和 **Swift API** 证书

您可以还原为使用默认的S3和Swift API证书进行S3和Swift客户端与存储节点的连接。但是、不能对负载平衡器端点使用默认的S3和Swift API证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。

2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。

3. 选择 * 使用默认证书 * 。

   还原全局S3和Swift API证书的默认版本时、您配置的自定义服务器证书文件将被删除、并且无法从系统中恢复。默认的S3和Swift API证书将用于后续与存储节点的新S3和Swift客户端连接。

4. 选择 * 确定 * 确认警告并还原默认 S3 和 Swift API 证书。

如果您拥有根访问权限，并且自定义 S3 和 Swift API 证书用于负载平衡器端点连接，则会显示一个负载平衡器端点列表，这些端点将无法再使用默认 S3 和 Swift API 证书进行访问。转至 "配置负载平衡器端点" 编辑或删除受影响的端点。

5. 刷新页面以确保 Web 浏览器已更新。

下载或复制 **S3** 和 **Swift API** 证书

您可以保存或复制 S3 和 Swift API 证书内容，以便在其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * 。
2. 在 * 全局 * 选项卡上，选择 * S3 和 Swift API 证书 * 。
3. 选择 * 服务器 * 或 * CA 捆绑包 * 选项卡，然后下载或复制证书。

下载证书文件或 **CA** 包

下载证书或CA包 `.pem` 文件如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 下载证书 * 或 * 下载 CA 捆绑包 * 。

   如果要下载 CA 包，则 CA 包二级选项卡中的所有证书将作为一个文件下载。

b. 指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

复制证书或 **CA** 捆绑包 **PEM**

复制证书文本以粘贴到其他位置。如果您使用的是可选的 CA 包，则该包中的每个证书都会显示在其自己的子选项卡上。

a. 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* 。

   如果要复制 CA 包，则 CA 包二级选项卡中的所有证书会同时复制在一起。

b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

相关信息

- "使用S3 REST API"
- "使用Swift REST API"
- "配置S3端点域名"

复制网格 **CA** 证书

StorageGRID 使用内部证书颁发机构（CA）来保护内部流量。如果您上传自己的证书，则此证书不会更改。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

如果配置了自定义服务器证书，则客户端应用程序应使用自定义服务器证书验证服务器。他们不应从 StorageGRID 系统复制 CA 证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 网格 CA* 选项卡。
2. 在*Certificate PEM*部分，下载或复制证书。

下载证书文件

下载证书 `.pem` 文件

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

   例如： `storagegrid_certificate.pem`

复制证书 **PEM**

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

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

对于执行严格主机名验证但不支持禁用严格主机名验证的S3客户端(例如使用FabricPool的ONTAP 客户端)、您可以在配置负载平衡器端点时生成或上传服务器证书。

开始之前

- 您具有特定的访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

创建负载平衡器端点时，您可以生成自签名服务器证书或上传由已知证书颁发机构（ CA ）签名的证书。在生产环境中，您应使用由已知 CA 签名的证书。由 CA 签名的证书可以无中断地轮换。它们也更安全，因为它们可以更好地防止中间人攻击。

以下步骤为使用 FabricPool 的 S3 客户端提供了一般准则。有关更多详细信息和过程，请参见 "为 FabricPool 配置 StorageGRID"。

步骤

1. （可选）配置一个高可用性（ High Availability ， HA ）组以供 FabricPool 使用。
2. 创建 S3 负载平衡器端点以供 FabricPool 使用。

   创建 HTTPS 负载平衡器端点时，系统会提示您上传服务器证书，证书专用密钥和可选的 CA 捆绑包。

3. 在 ONTAP 中将 StorageGRID 附加为云层。

   指定负载平衡器端点端口以及上载的 CA 证书中使用的完全限定域名。然后，提供 CA 证书。

   > 如果中间 CA 颁发了 StorageGRID 证书，则必须提供中间 CA 证书。如果 StorageGRID 证书是直接由根 CA 颁发的，则必须提供根 CA 证书。

配置客户端证书

客户端证书允许授权的外部客户端访问 StorageGRID Prometheus 数据库，从而为外部工具监控 StorageGRID 提供了一种安全的方式。

如果您需要使用外部监控工具访问StorageGRID 、则必须使用网格管理器上传或生成客户端证书、并将证书信息复制到外部工具。

请参见 "管理安全证书" 和 "配置自定义服务器证书"。

> 为确保操作不会因服务器证书失败而中断，当此服务器证书即将到期时，将触发“证书页上配置的客户端证书*到期”警报。根据需要，您可以通过选择 * 配置 * > * 安全性 * > * 证书 * 并在客户端选项卡上查看客户端证书的到期日期来查看当前证书的到期时间。

> 如果您使用密钥管理服务器（ KMS ）保护专门配置的设备节点上的数据，请参见有关的特定信息 "上传 KMS 客户端证书"。

开始之前

- 您具有 root 访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 配置客户端证书：
  - 您拥有管理节点的 IP 地址或域名。
  - 如果已配置StorageGRID 管理接口证书、则可以使用CA、客户端证书和专用密钥来配置管理接口证书。
  - 要上传您自己的证书、您的本地计算机上提供了证书的专用密钥。

    - 私钥必须在创建时已保存或记录。如果您没有原始私钥、则必须创建一个新的私钥。
- 编辑客户端证书：
    - 您拥有管理节点的 IP 地址或域名。
    - 要上传您自己的证书或新证书、您的本地计算机上提供了私钥、客户端证书和CA (如果使用)。

添加客户端证书

要添加客户端证书、请使用以下过程之一：

- [已配置管理接口证书]
- CA颁发的客户端证书
- [从网格管理器生成的证书]

已配置管理接口证书

如果已使用客户提供的CA、客户端证书和专用密钥配置管理接口证书、请使用此操作步骤 添加客户端证书。

步骤

1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择 * 添加 * 。
3. 输入证书名称。
4. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
5. 选择 * 继续 * 。
6. 对于*attach certificates*步骤，请上传管理接口证书。
    a. 选择 * 上传证书 * 。
    b. 选择*浏览*并选择管理接口证书文件 (`.pem`) 。
        - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
        - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
    c. 选择 * 创建 * 以在网格管理器中保存证书。

    新证书将显示在客户端选项卡上。
7. 配置外部监控工具，如Grafana。

CA颁发的客户端证书

如果未配置管理接口证书、并且您计划为使用CA颁发的客户端证书和专用密钥的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 执行步骤至 "配置管理接口证书"。
2. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

3. 选择 * 添加 * 。
4. 输入证书名称。
5. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
6. 选择 * 继续 * 。
7. 对于*attach certificates*步骤，上传客户端证书、私钥和CA包文件：
   a. 选择 * 上传证书 * 。
   b. 选择*浏览*并选择客户证书、私钥和CA包文件（`.pem`）。
      - 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。
      - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   c. 选择 * 创建 * 以在网格管理器中保存证书。

      新证书将显示在客户端选项卡上。
8. 配置外部监控工具，如Grafana。

从网格管理器生成的证书

如果未配置管理接口证书、并且您计划为使用网格管理器中的生成证书功能的Prometheus添加客户端证书、请使用此操作步骤 添加管理员客户端证书。

步骤

1. 在网格管理器中，选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择 * 添加 * 。
3. 输入证书名称。
4. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
5. 选择 * 继续 * 。
6. 对于*attach certificates*步骤，选择*Generate certificates*。
7. 指定证书信息：
   - 主题(可选)：证书所有者的X.509主题或可分辨名称(DN)。
   - 有效天数：生成的证书自生成之日起生效的天数。
   - 添加密钥用法扩展：如果选择(默认值和建议值)，则会将密钥用法扩展和扩展密钥用法扩展添加到生成的证书中。

     这些扩展定义了证书中所含密钥的用途。

     除非在证书包含这些扩展时遇到与旧客户端的连接问题、否则保持选中此复选框。
8. 选择 * 生成 * 。
9. 【客户端证书详细信息】选择*客户端证书详细信息*可显示证书元数据和证书PEM。

关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

- 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
- 选择 * 下载证书 * 以保存证书文件。

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
- 选择 * 下载私钥 * 将私钥另存为文件。

  指定私钥文件名和下载位置。

10. 选择 * 创建 * 以在网格管理器中保存证书。

    新证书将显示在客户端选项卡上。

11. 在网格管理器中、选择*配置*>*安全性*>*证书*、然后选择*全局*选项卡。
12. 选择*管理接口证书*。
13. 选择 * 使用自定义证书 * 。
14. 从上传certificate.pem和private_key.pem文件 客户端证书详细信息 步骤。无需上传CA捆绑包。
    a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
    b. 上传每个证书文件（`.pem`）。
    c. 选择 * 创建 * 以在网格管理器中保存证书。

       新证书将显示在客户端选项卡上。

15. 配置外部监控工具，如Grafana。

[[configure-External monitoring-tool]]配置外部监控工具

步骤

1. 在外部监控工具上配置以下设置，例如 Grafana 。
   a. * 名称 * ： 输入连接的名称。

      StorageGRID 不需要此信息，但您必须提供一个名称来测试连接。

   b. * URL * ： 输入管理节点的域名或 IP 地址。指定 HTTPS 和端口 9091 。

      例如： `https://admin-node.example.com:9091`

   c. 启用 * TLS 客户端身份验证 * 和 * 使用 CA 证书 * 。
   d. 在TLS/SSL身份验证详细信息下、复制并粘贴：+
      - 管理接口CA证书到"** CA证书"

    - 到"Client Cert"的客户端证书
    - "**客户端密钥"的专用密钥

  e. * 服务器名称 *： 输入管理节点的域名。

     servername 必须与管理接口证书中显示的域名匹配。

2. 保存并测试从 StorageGRID 或本地文件复制的证书和私钥。

   现在，您可以使用外部监控工具从 StorageGRID 访问 Prometheus 指标。

   有关指标的信息，请参见 "有关监控 StorageGRID 的说明"。

编辑客户端证书

您可以编辑管理员客户端证书以更改其名称，启用或禁用 Prometheus 访问，或者在当前证书已过期时上传新证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

   表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择 * 编辑名称和权限 *
4. 输入证书名称。
5. 要使用外部监控工具访问Prometheus指标，请选择*Allow Prometheus*(允许Prometheus*)。
6. 选择 * 继续 * 以在网格管理器中保存证书。

   更新后的证书将显示在客户端选项卡上。

附加新的客户端证书

您可以在当前证书过期后上传新证书。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。

   表中列出了证书到期日期和 Prometheus 访问权限。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。

2. 选择要编辑的证书。
3. 选择 * 编辑 * ，然后选择编辑选项。

上传证书

复制证书文本以粘贴到其他位置。

a. 选择 * 上传证书 * ，然后选择 * 继续 * 。
b. 上传客户端证书名称 (`.pem`) 。

   选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
c. 选择 * 创建 * 以在网格管理器中保存证书。

   更新后的证书将显示在客户端选项卡上。

生成证书

生成要粘贴到其他位置的证书文本。

a. 选择 * 生成证书 * 。
b. 指定证书信息：

   - 主题(可选)：证书所有者的X.509主题或可分辨名称(DN)。
   - 有效天数：生成的证书自生成之日起生效的天数。
   - 添加密钥用法扩展：如果选择(默认值和建议值)，则会将密钥用法扩展和扩展密钥用法扩展添加到生成的证书中。

     这些扩展定义了证书中所含密钥的用途。

     除非在证书包含这些扩展时遇到与旧客户端的连接问题、否则保持选中此复选框。
c. 选择 * 生成 * 。
d. 选择 * 客户端证书详细信息 * 以显示证书元数据和证书 PEM 。

   关闭此对话框后，您将无法查看此证书专用密钥。将密钥复制或下载到安全位置。

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。
   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

- 选择 * 复制私钥 * 可复制证书私钥以粘贴到其他位置。
- 选择 * 下载私钥 * 将私钥另存为文件。

  指定私钥文件名和下载位置。

e. 选择 * 创建 * 以在网格管理器中保存证书。

   新证书将显示在客户端选项卡上。

下载或复制客户端证书

您可以下载或复制客户端证书以供其他位置使用。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择要复制或下载的证书。
3. 下载或复制证书。

下载证书文件

下载证书 `.pem` 文件

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

   例如： `storagegrid_certificate.pem`

复制证书

复制证书文本以粘贴到其他位置。

a. 选择 * 复制证书 PEM* 。
b. 将复制的证书粘贴到文本编辑器中。
c. 使用扩展名保存文本文件 `.pem`。

   例如： `storagegrid_certificate.pem`

删除客户端证书

如果您不再需要管理员客户端证书，可以将其删除。

步骤

1. 选择 * 配置 * > * 安全性 * > * 证书 * ，然后选择 * 客户端 * 选项卡。
2. 选择要删除的证书。

3. 选择 * 删除 * ，然后确认。

> 要删除最多 10 个证书，请在客户端选项卡上选择要删除的每个证书，然后选择 * 操作 * > * 删除 * 。

删除证书后，使用该证书的客户端必须指定一个新的客户端证书，才能访问 StorageGRID Prometheus 数据库。

配置安全设置

管理TLS和SSH策略

TLS和SSH策略用于确定使用哪些协议和加密方法与客户端应用程序建立安全TLS连接、以及与内部StorageGRID 服务建立安全SSH连接。

此安全策略控制TLS和SSH如何对移动数据进行加密。通常、请使用现代兼容性(默认)策略、除非您的系统需要符合通用标准或您需要使用其他密钥。

> 某些StorageGRID 服务尚未更新、无法在这些策略中使用这些加密方法。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "root访问权限"。

选择一个安全策略

步骤

1. 选择*configuration*>*Security*>*Security settings。

   TLS和SSH策略*选项卡显示可用策略。当前活动的策略会在策略磁贴上标记为绿色复选标记。

2. 查看图块、了解可用策略。

策略	Description
现代兼容性(默认)	如果需要强加密、则使用默认策略、除非您有特殊要求。此策略与大多数TLS和SSH客户端兼容。

策略	Description
传统兼容性	如果需要为旧客户端提供其他兼容性选项、请使用此策略。此策略中的其他选项可能会使其不如现代兼容性策略安全。
通用标准	如果您需要通用标准认证、请使用此策略。
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3.0.0进行外部客户端连接以连接到负载平衡器端点、租户管理器和网格管理器、请使用此策略。使用此策略可能会降低性能。
自定义	如果需要应用您自己的用户名或用户名、请创建自定义策略。

3. 要查看有关每个策略的加密、协议和算法的详细信息，请选择*查看详细信息*。
4. 要更改当前策略，请选择*使用策略*。

   策略磁贴上的*current policy*旁边会出现一个绿色复选标记。

创建自定义安全策略

如果需要应用自己的用户名、可以创建自定义策略。

步骤

1. 从与要创建的自定义策略最相似的策略的磁贴中，选择*查看详细信息*。
2. 选择*复制到剪贴板*，然后选择*取消*。

3. 从“自定义策略”磁贴中，选择“配置和使用”。
4. 粘贴您复制的JSON并进行所需的任何更改。
5. 选择*使用策略*。

   自定义策略磁贴上的*当前策略*旁边会出现一个绿色复选标记。

6. (可选)选择*Edit configuration*对新的自定义策略进行更多更改。

暂时还原为默认安全策略

如果配置了自定义安全策略、并且配置的TLS策略与不兼容、则可能无法登录到网格管理器 "已配置服务器证书"。

您可以临时还原为默认安全策略。

步骤

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

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 运行以下命令：

```
restore-default-cipher-configurations
```

3. 从 Web 浏览器访问同一管理节点上的网格管理器。
4. 按照中的步骤进行操作 选择一个安全策略 以重新配置策略。

配置网络和对象安全性

您可以将网络和对象安全性配置为对存储的对象进行加密、防止某些S3和Swift请求、或者允许客户端连接到存储节点时使用HTTP而不是HTTPS。

存储对象加密

通过存储对象加密、可以在通过S3读取所有对象数据时对这些数据进行加密。默认情况下、存储的对象不会进行加密、但您可以选择使用AES‐128或AES‐256加密算法对对象进行加密。启用此设置后，所有新载入的对象都将被加密，但不会对现有存储的对象进行任何更改。如果禁用加密、则当前加密的对象仍会保持加密状态、但不会对新加装的对象进行加密。

存储的对象加密设置仅适用于尚未通过存储分段级或对象级加密进行加密的S3对象。

有关StorageGRID 加密方法的更多详细信息、请参见 "查看 StorageGRID 加密方法"。

防止修改客户端

防止客户端修改是一项系统范围的设置。如果选择了*prevent client修改*选项，则会拒绝以下请求。

S3 REST API

- 删除存储分段请求

- 修改现有对象数据，用户定义的元数据或 S3 对象标记的任何请求

Swift REST API

- 删除容器请求
- 修改任何现有对象的请求。例如，以下操作被拒绝： PUT 覆盖，删除，元数据更新等。

为存储节点连接启用HTTP

默认情况下、客户端应用程序会使用HTTPS网络协议直接连接到存储节点。您可以选择为这些连接启用 HTTP ，例如在测试非生产网格时。

仅当S3和Swift客户端需要直接与存储节点建立HTTP连接时、才使用HTTP进行存储节点连接。对于仅使用HTTPS连接的客户端或连接到负载平衡器服务的客户端、您无需使用此选项(因为您可以 "配置每个负载平衡器端点" 以使用HTTP或HTTPS)。

请参见 "摘要：客户端连接的 IP 地址和端口" 了解S3和Swift客户端在使用HTTP或HTTPS连接到存储节点时使用的端口。

选择选项

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

步骤

1. 选择*configuration*>*Security*>*Security settings。
2. 选择*网络和对象*选项卡。
3. 对于存储的对象加密，如果不希望对存储的对象进行加密，请使用*None*(默认)设置，或者选择*AES-128*或*AES-256*对存储的对象进行加密。
4. 如果要阻止S3和Swift客户端发出特定请求，可选择*prevent client修改*。

   > 如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

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

   > 为生产网格启用 HTTP 时请务必小心，因为请求会以未加密方式发送。

6. 选择 * 保存 * 。

更改浏览器非活动超时

如果 Grid Manager 和租户管理器用户处于非活动状态的时间超过一段时间，您可以控制他们是否已注销。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

关于此任务

浏览器非活动超时默认为15分钟。如果用户的浏览器在此时间段内未处于活动状态、则该用户将被注销。

您可以根据需要通过设置*注销非活动用户*选项来增加或减少超时期限。

浏览器非活动超时还受以下因素控制：

- 一个单独的不可配置 StorageGRID 计时器，其中包括用于系统安全保护的计时器。默认情况下，每个用户的身份验证令牌在用户登录后 16 小时到期。当用户的身份验证过期时、即使禁用了浏览器非活动超时或尚未达到浏览器超时值、该用户也会自动注销。要续订令牌，用户必须重新登录。
- 身份提供程序的超时设置(假设为StorageGRID 启用了单点登录(SSO))。

  如果启用了SSO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。请参见 "配置单点登录"。

步骤

1. 选择*configuration*>*Security*>*Security settings。
2. 选择*浏览器非活动超时*选项卡。
3. 在*注销非活动用户后*字段中，指定浏览器超时期限，介于60秒到7天之间。

   您可以指定浏览器超时期限(以秒、分钟、小时或天为单位)。

4. 选择 * 保存 * 。如果浏览器在指定时间内处于非活动状态、则用户将从网格管理器或租户管理器中注销。

   新设置不会影响当前已登录的用户。用户必须重新登录或刷新浏览器，新的超时设置才能生效。

配置密钥管理服务器

配置密钥管理服务器：概述

您可以配置一个或多个外部密钥管理服务器（ KMS ）来保护专门配置的设备节点上的数据。

什么是密钥管理服务器（ KMS ）？

密钥管理服务器（ Key Management Server ， KMS ）是一种外部第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为关联 StorageGRID 站点上的 StorageGRID 设备节点提供加密密钥。

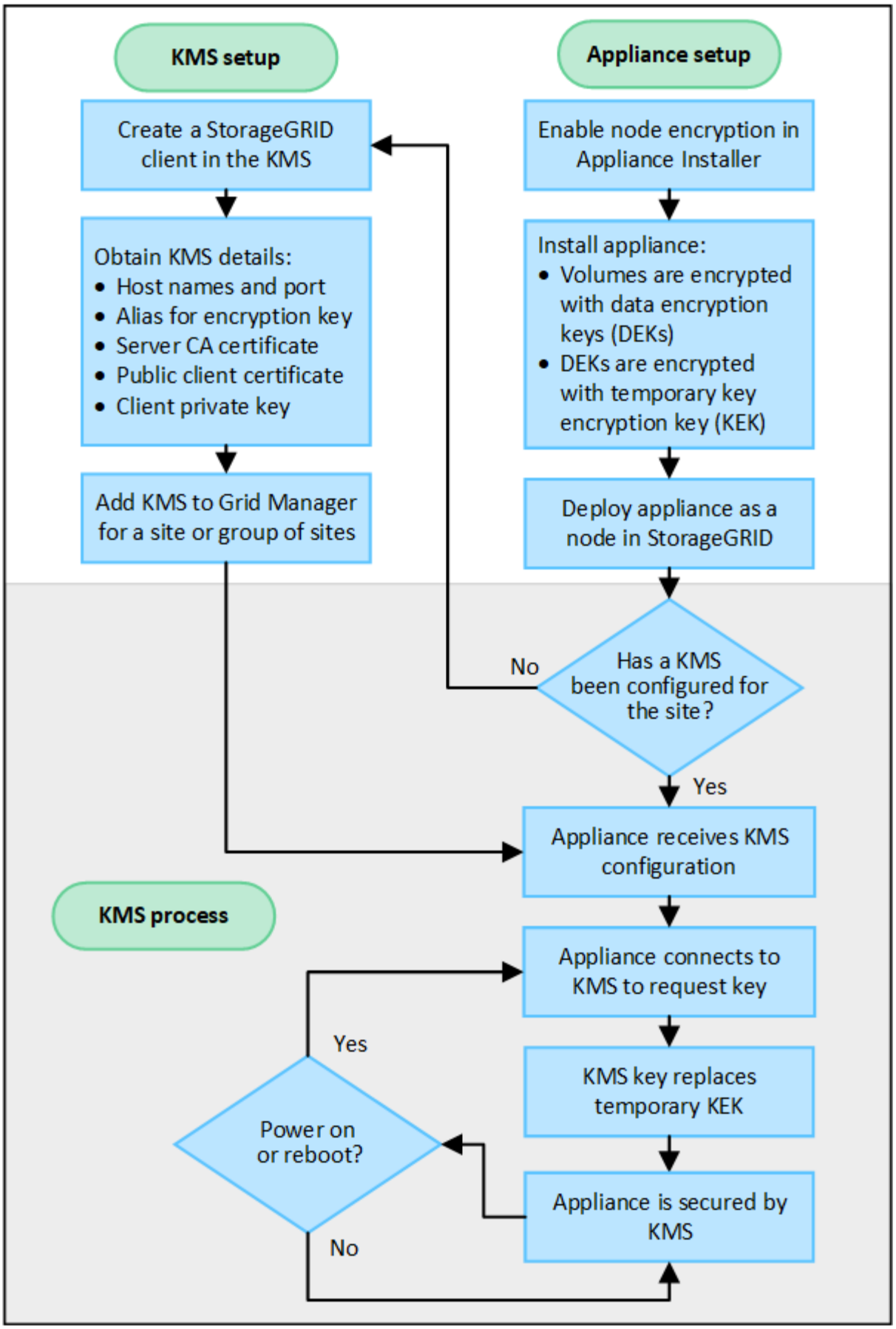
您可以使用一个或多个密钥管理服务器来管理安装期间启用了 * 节点加密 * 设置的任何 StorageGRID 设备节点的节点加密密钥。通过将密钥管理服务器与这些设备节点结合使用，您可以保护数据，即使设备已从数据中心中删除也是如此。对设备卷进行加密后、您将无法访问设备上的任何数据、除非此节点可以与KMS进行通信。

StorageGRID 不会创建或管理用于对设备节点进行加密和解密的外部密钥。如果您计划使用外部密钥管理服务器来保护 StorageGRID 数据，则必须了解如何设置该服务器，并且必须了解如何管理加密密钥。执行密钥管理任务不在本说明的范围之内。如果需要帮助，请参见密钥管理服务器的文档或联系技术支持。

KMS 和设备配置概述

在使用密钥管理服务器（KMS）保护设备节点上的 StorageGRID 数据之前，必须完成两项配置任务：设置一个或多个 KMS 服务器以及为设备节点启用节点加密。完成这两项配置任务后，密钥管理过程将自动进行。

此流程图显示了使用 KMS 在设备节点上保护 StorageGRID 数据的高级步骤。



流程图显示了 KMS 设置和设备设置并行进行；但是，您可以根据需要在为新设备节点启用节点加密之前或之后

设置密钥管理服务器。

设置密钥管理服务器（KMS）

设置密钥管理服务器包括以下高级步骤。

步骤	请参见
访问 KMS 软件，并向每个 KMS 或 KMS 集群添加一个 StorageGRID 客户端。	"在 KMS 中将 StorageGRID 配置为客户端"
在 KMS 上获取 StorageGRID 客户端所需的信息。	"在 KMS 中将 StorageGRID 配置为客户端"
将 KMS 添加到网格管理器中，将其分配到一个站点或一组默认站点，上传所需的证书并保存 KMS 配置。	"添加密钥管理服务器（KMS）"

设置设备

设置要使用 KMS 的设备节点包括以下高级步骤。

1. 在设备安装的硬件配置阶段，使用 StorageGRID 设备安装程序为设备启用 * 节点加密 * 设置。

> 将设备添加到网格后、您无法启用*节点加密*设置、并且无法对未启用节点加密的设备使用外部密钥管理。

2. 运行 StorageGRID 设备安装程序。在安装期间，系统会为每个设备卷分配一个随机数据加密密钥（DEK），如下所示：
   - 这些 DEks 用于对每个卷上的数据进行加密。这些密钥是在设备操作系统中使用Linux统一密钥设置(LUKS)磁盘加密生成的、无法更改。
   - 每个 DEK 都通过主密钥加密密钥（KEK）进行加密。初始 KEK 是一个临时密钥，用于对密钥进行加密，直到设备可以连接到 KMS 为止。
3. 将设备节点添加到 StorageGRID 。

请参见 "启用节点加密" 了解详细信息。

密钥管理加密过程（自动发生）

密钥管理加密包括以下高级步骤，这些步骤会自动执行。

1. 在网格中安装启用了节点加密的设备时， StorageGRID 会确定包含新节点的站点是否存在 KMS 配置。
   - 如果已为站点配置 KMS ，则设备将接收 KMS 配置。
   - 如果尚未为站点配置 KMS ，则设备上的数据将继续由临时 KEK 加密，直到您为站点配置 KMS 且设备收到 KMS 配置为止。
2. 设备使用 KMS 配置连接到 KMS 并请求加密密钥。
3. KMS 会向设备发送加密密钥。KMS 中的新密钥将取代临时的 KEK ，现在用于对设备卷的 DEK 进行加密和解密。

> 加密设备节点连接到配置的 KMS 之前存在的任何数据都将使用临时密钥进行加密。但是，在将临时密钥替换为 KMS 加密密钥之前，不应将设备卷视为不受从数据中心删除的保护。

4. 如果设备已启动或重新启动，它将重新连接到 KMS 以请求密钥。此密钥保存在易失性内存中、无法经受断电或重新启动的影响。

使用密钥管理服务器的注意事项和要求

在配置外部密钥管理服务器（KMS）之前，您必须了解注意事项和要求。

KMIP 要求是什么？

StorageGRID 支持 KMIP 1.4 版。

"密钥管理互操作性协议规范 1.4 版"

设备节点与配置的 KMS 之间的通信使用安全 TLS 连接。StorageGRID 支持 KMIP 使用以下 TLS v1.2 密码：

- tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_ECDSA_WIT_AES_256_GCM_SHA384

您必须确保使用节点加密的每个设备节点都可以通过网络访问为站点配置的 KMS 或 KMS 集群。

网络防火墙设置必须允许每个设备节点通过用于密钥管理互操作性协议（Key Management Interoperability Protocol， KMIP）通信的端口进行通信。默认 KMIP 端口为 5696 。

支持哪些设备？

您可以使用密钥管理服务器（Key Management Server， KMS）管理网格中启用了 * 节点加密 * 设置的任何 StorageGRID 设备的加密密钥。只有在使用 StorageGRID 设备安装程序安装设备的硬件配置阶段，才能启用此设置。

> 将设备添加到网格后、您无法启用节点加密、并且无法对未启用节点加密的设备使用外部密钥管理。

您可以对StorageGRID 设备和设备节点使用已配置的KMS。

您不能对基于软件(非设备)的节点使用已配置的KMS、包括以下节点：

- 部署为虚拟机（VM）的节点
- 在 Linux 主机上的容器引擎中部署的节点

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

应在何时配置密钥管理服务器？

对于新安装，通常应在创建租户之前在网格管理器中设置一个或多个密钥管理服务器。此顺序可确保节点在存储任何对象数据之前受到保护。

您可以在安装设备节点之前或之后在网格管理器中配置密钥管理服务器。

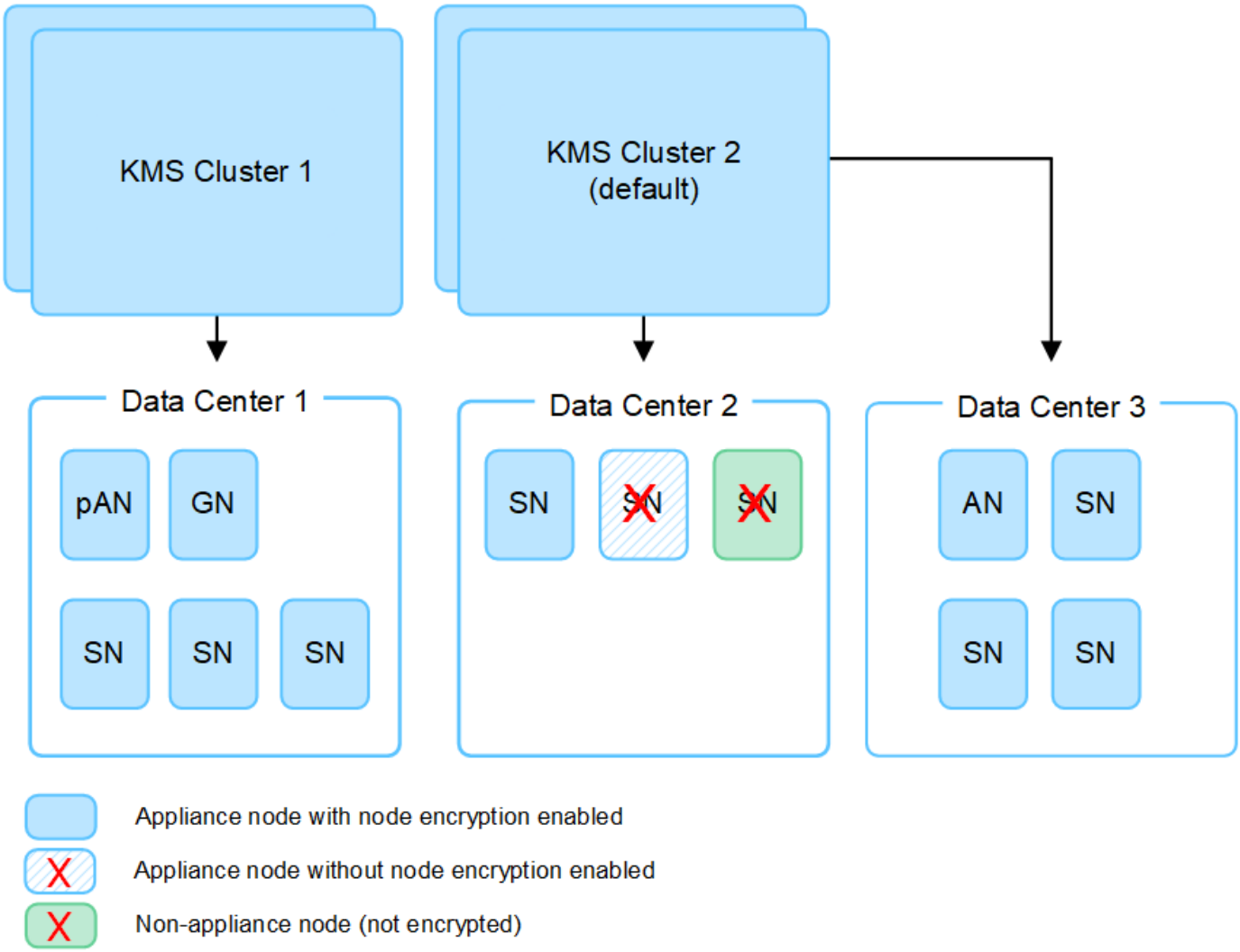
我需要多少个密钥管理服务器？

您可以配置一个或多个外部密钥管理服务器，以便为 StorageGRID 系统中的设备节点提供加密密钥。每个 KMS 都为单个站点或一组站点上的 StorageGRID 设备节点提供一个加密密钥。

StorageGRID 支持使用 KMS 集群。每个 KMS 集群都包含多个复制的密钥管理服务器，这些服务器共享配置设置和加密密钥。建议使用 KMS 集群进行密钥管理，因为它可以提高高可用性配置的故障转移功能。

例如，假设您的 StorageGRID 系统有三个数据中心站点。您可以将一个 KMS 集群配置为为为 Data Center 1 上的所有设备节点提供密钥，而将另一个 KMS 集群配置为为为所有其他站点上的所有设备节点提供密钥。添加第二个 KMS 集群时，您可以为 Data Center 2 和 Data Center 3 配置默认 KMS 。

请注意，不能对非设备节点或安装期间未启用*Node Encryption设置的任何设备节点使用KMS。



轮换密钥时会发生什么情况？

作为安全最佳实践，您应定期轮换每个已配置的 KMS 使用的加密密钥。

在旋转加密密钥时，请使用 KMS 软件将该密钥从上次使用的版本轮换到同一密钥的新版本。不要旋转到完全不同的键。

> 切勿尝试通过在网格管理器中更改 KMS 的密钥名称（别名）来轮换密钥。而是通过更新 KMS 软件中的密钥版本来轮换密钥。对新密钥使用与先前密钥相同的密钥别名。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。

新密钥版本可用时：

- 它会自动分发到与 KMS 关联的站点上的加密设备节点。分发应在轮换密钥后的一小时内完成。
- 如果在分发新密钥版本时加密设备节点脱机，则该节点将在重新启动后立即收到新密钥。
- 如果由于任何原因无法使用新密钥版本对设备卷进行加密、则会为此设备节点触发* KMS加密密钥轮换失败* 警报。您可能需要联系技术支持以帮助解决此警报。

是否可以在设备节点加密后重复使用它?

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

> 如果无法访问 KMS 加密密钥，则设备上保留的任何数据将无法再访问并永久锁定。

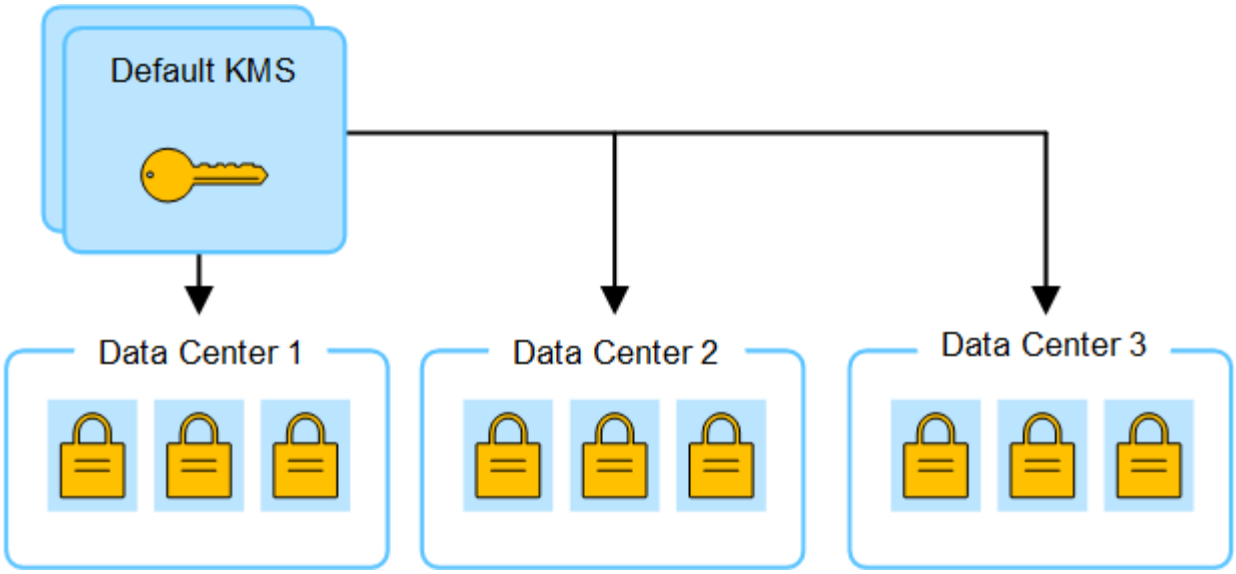
更改站点的 **KMS** 的注意事项

每个密钥管理服务器（ Key Management Server ， KMS ）或 KMS 集群都会为单个站点或一组站点上的所有设备节点提供一个加密密钥。如果需要更改站点使用的 KMS ，则可能需要将加密密钥从一个 KMS 复制到另一个 KMS 。

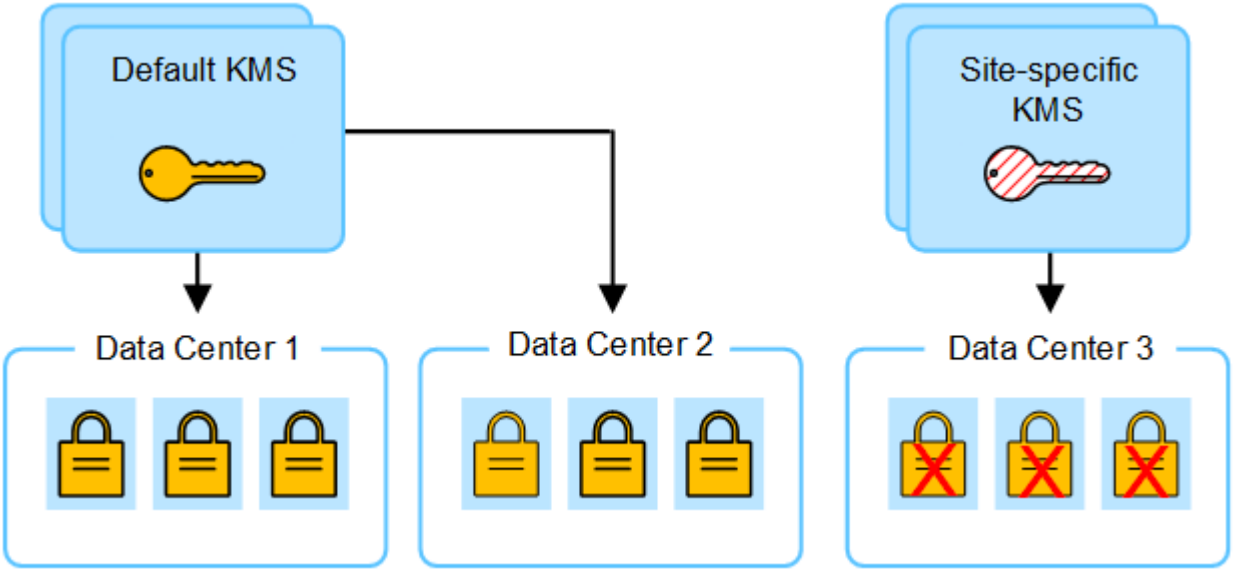
如果更改站点使用的 KMS ，则必须确保可以使用存储在新 KMS 上的密钥对该站点上先前加密的设备节点进行解密。在某些情况下，您可能需要将当前版本的加密密钥从原始 KMS 复制到新 KMS 。您必须确保 KMS 具有正确的密钥，以便对站点上的加密设备节点进行解密。

例如：

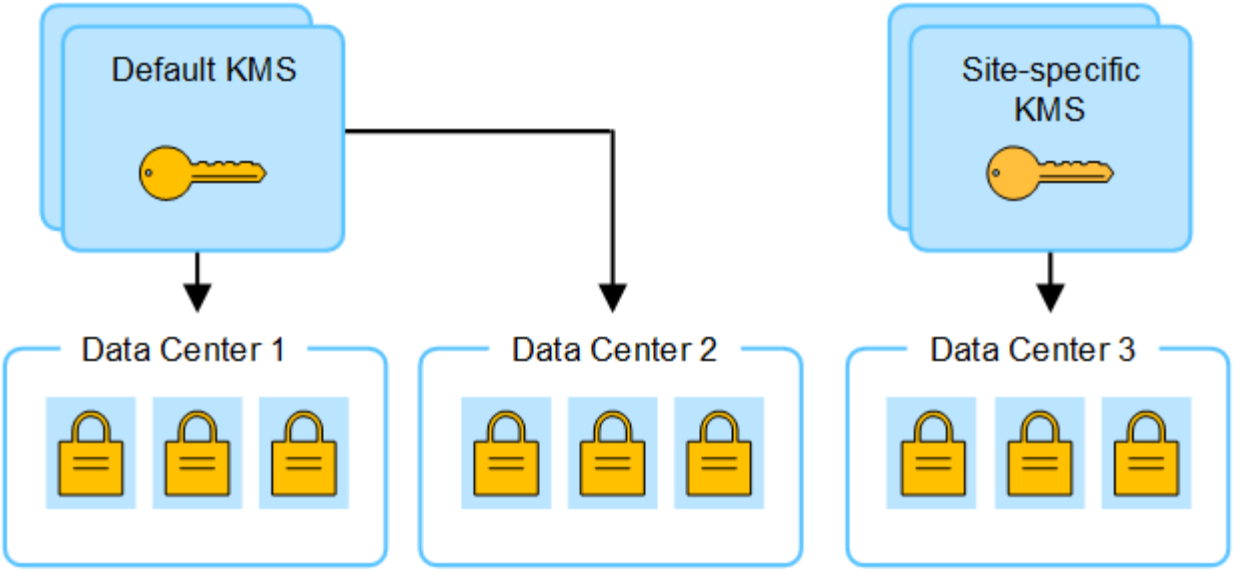
1. 您最初会配置一个默认KMS、用于适用场景 所有没有专用KMS的站点。
2. 保存 KMS 后，所有启用了 * 节点加密 * 设置的设备节点都会连接到 KMS 并请求加密密钥。此密钥用于对所有站点上的设备节点进行加密。此外，还必须使用此相同密钥对这些设备进行解密。



3. 您决定为一个站点（图中的数据中心 3 ）添加站点专用的 KMS 。但是，由于设备节点已加密，因此在尝试保存站点专用 KMS 的配置时会发生验证错误。之所以出现此错误，是因为站点特定的 KMS 没有正确的密钥来对该站点上的节点进行解密。



4. 要解决问题描述 问题，请将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。（从技术上讲，您可以将原始密钥复制到具有相同别名的新密钥。原始密钥将成为新密钥的先前版本。） 现在，站点特定的 KMS 具有用于对数据中心 3 上的设备节点进行解密的正确密钥，因此可以将其保存在 StorageGRID 中。



更改站点使用的 **KMS** 的用例

下表总结了更改站点 KMS 的最常见情况下所需的步骤。

更改站点 **KMS** 的用例	所需步骤
您有一个或多个站点特定的 KMS 条目，并且希望使用其中一个条目作为默认 KMS 。	编辑站点特定的 KMS 。在 * 管理密钥 * 字段中，选择 * 不受其他 KMS （默认 KMS ）管理的站点 * 。现在，站点专用的 KMS 将用作默认 KMS 。它将适用于没有专用KMS的任何站点。 "编辑密钥管理服务器（KMS）"
您有一个默认 KMS ，并且在扩展中添加了一个新站点。您不想对新站点使用默认KMS。	1. 如果新站点上的设备节点已被默认 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从默认 KMS 复制到新 KMS 。 2. 使用网格管理器添加新的 KMS 并选择站点。 "添加密钥管理服务器（KMS）"
您希望站点的 KMS 使用其他服务器。	1. 如果站点上的设备节点已由现有 KMS 加密，请使用 KMS 软件将当前版本的加密密钥从现有 KMS 复制到新 KMS 。 2. 使用网格管理器编辑现有 KMS 配置并输入新的主机名或 IP 地址。 "添加密钥管理服务器（KMS）"

在 **KMS** 中将 **StorageGRID** 配置为客户端

您必须将 StorageGRID 配置为每个外部密钥管理服务器或 KMS 集群的客户端，然后才能将 KMS 添加到 StorageGRID 。

关于此任务

以下说明适用于Thles CipherTrust Manager。有关支持的版本列表、请使用 "NetApp 互操作性表工具（IMT）"。

步骤

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

   每个 KMS 都会为单个站点或一组站点上的 StorageGRID 设备节点管理一个加密密钥。

2. 在 KMS 软件中，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。

3. 记录每个 KMS 或 KMS 集群的以下信息。

   将 KMS 添加到 StorageGRID 时需要此信息。

   - 每个服务器的主机名或 IP 地址。
   - KMS 使用的 KMIP 端口。
   - KMS 中加密密钥的密钥别名。

     此加密密钥必须已存在于 KMS 中。StorageGRID 不会创建或管理 KMS 密钥。

4. 对于每个 KMS 或 KMS 集群，获取一个由证书颁发机构（CA）签名的服务器证书，或者一个包含 PEM 编码的每个 CA 证书文件的证书捆绑包，这些证书按证书链顺序串联。

   通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

   - 证书必须使用 Privacy Enhanced Mail （PEM） Base — 64 编码的 X.509 格式。
   - 每个服务器证书中的 " 使用者备用名称（SAN） " 字段必须包含 StorageGRID 要连接到的完全限定域名（FQDN）或 IP 地址。

     在 StorageGRID 中配置 KMS 时，必须在 * 主机名 * 字段中输入相同的 FQDN 或 IP 地址。

   - 服务器证书必须与 KMS 的 KMIP 接口使用的证书匹配，该接口通常使用端口 5696 。

5. 获取外部 KMS 颁发给 StorageGRID 的公有 客户端证书以及客户端证书的专用密钥。

   客户端证书允许 StorageGRID 向 KMS 进行身份验证。

添加密钥管理服务器（**KMS**）

您可以使用 StorageGRID 密钥管理服务器向导添加每个 KMS 或 KMS 集群。

开始之前

- 您已查看 "使用密钥管理服务器的注意事项和要求"。
- 您已拥有 "已在 KMS 中将 StorageGRID 配置为客户端"和您具有每个 KMS 或 KMS 集群所需的信息。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

关于此任务

如果可能，请先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对所有不受另一个 KMS 管理的站点进行适用场景 。如果首先创建默认 KMS ，则网格中所有节点加密的设备都将使用默认 KMS 进行加密。如果要稍后创建站点专用的 KMS ，则必须先将当前版本的加密密钥从默认 KMS 复制到新的 KMS 。请参见 "更改站点的 KMS 的注意事项" 了解详细信息。

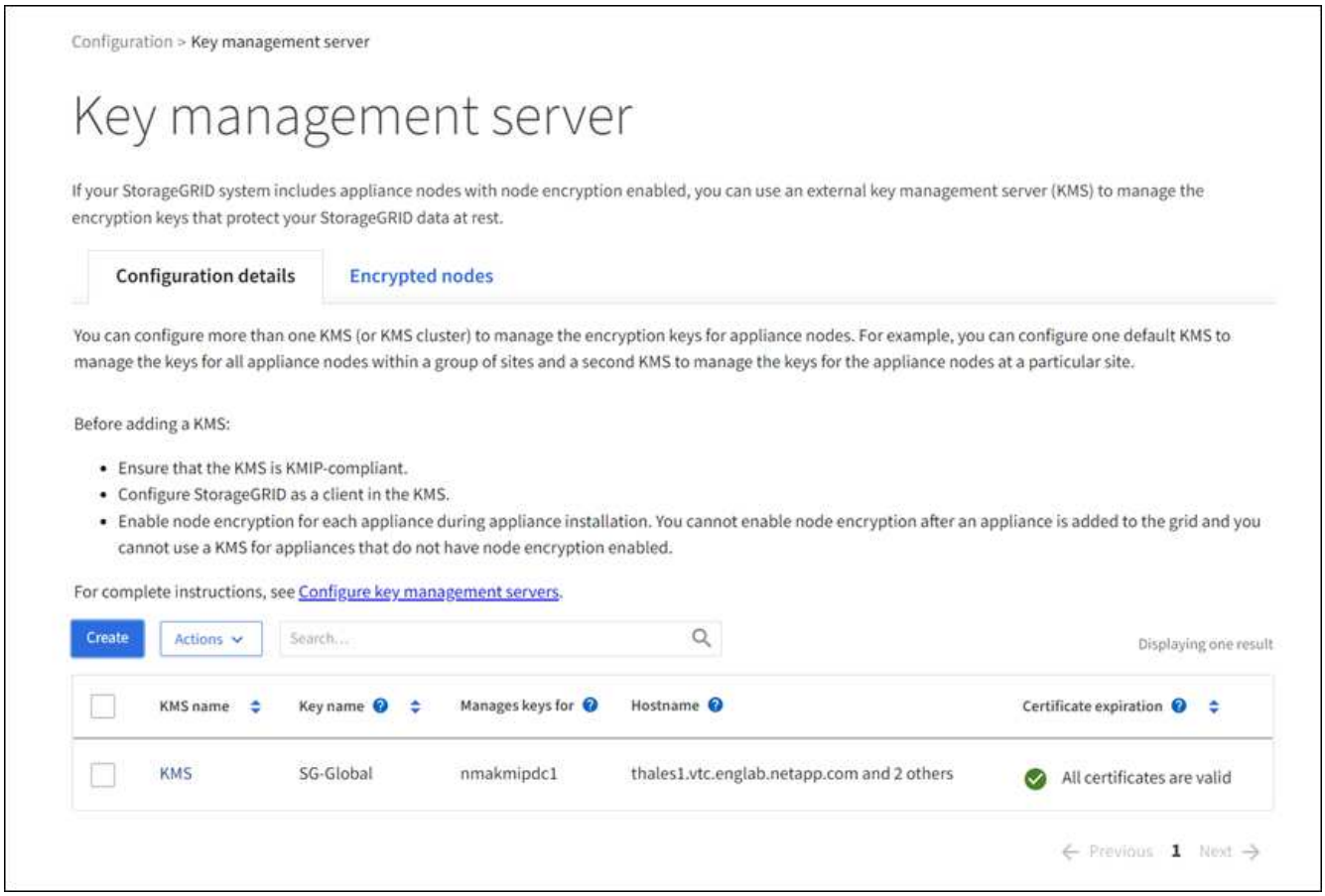
第1步：公里详细信息

在添加密钥管理服务器向导的步骤1 (KMS详细信息)中、您可以提供有关KMS或KMS集群的详细信息。

步骤

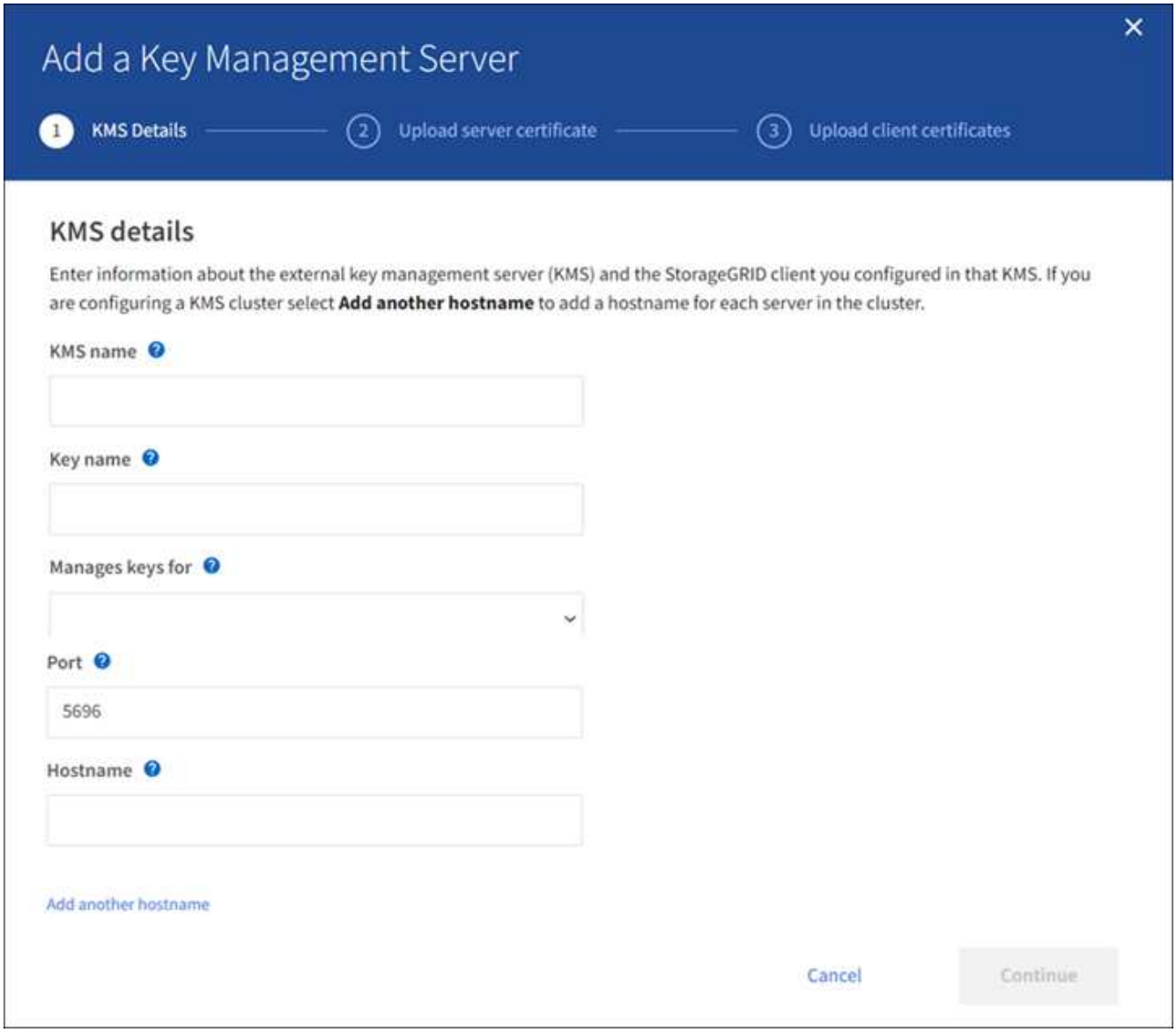
1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面、并选中配置详细信息选项卡。



2. 选择 * 创建 * 。

   此时将显示"Add a Key Management Server"(添加密钥管理服务器)向导的第1步(KMS详细信息)。



3. 为 KMS 和您在该 KMS 中配置的 StorageGRID 客户端输入以下信息。

字段	Description
Kms名称	一个描述性名称，可帮助您标识此 KMS 。必须介于 1 到 64 个字符之间。
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。

字段	Description
管理的密钥	将与此 KMS 关联的 StorageGRID 站点。如果可能，您应先配置任何站点特定的密钥管理服务器，然后再配置一个默认 KMS ，以便对不受另一个 KMS 管理的所有站点进行适用场景 。 • 如果此 KMS 将管理特定站点上设备节点的加密密钥，请选择一个站点。 • 选择*不由其他KMS管理的站点(默认KMS)*以配置默认KMS，该KMS将应用于任何没有专用KMS的站点以及您在后续扩展中添加的任何站点。 ◦ 注意： * 如果您选择的站点先前已被默认 KMS 加密，但未向新 KMS 提供当前版本的原始加密密钥，则保存 KMS 配置时将发生验证错误。
Port	KMS 服务器用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口。默认为 5696 ，即 KMIP 标准端口。
主机名	KMS 的完全限定域名或 IP 地址。 *注意：*服务器证书的使用者替代名称(SAN)字段必须包含您在此处输入的FQDN或IP地址。否则， StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

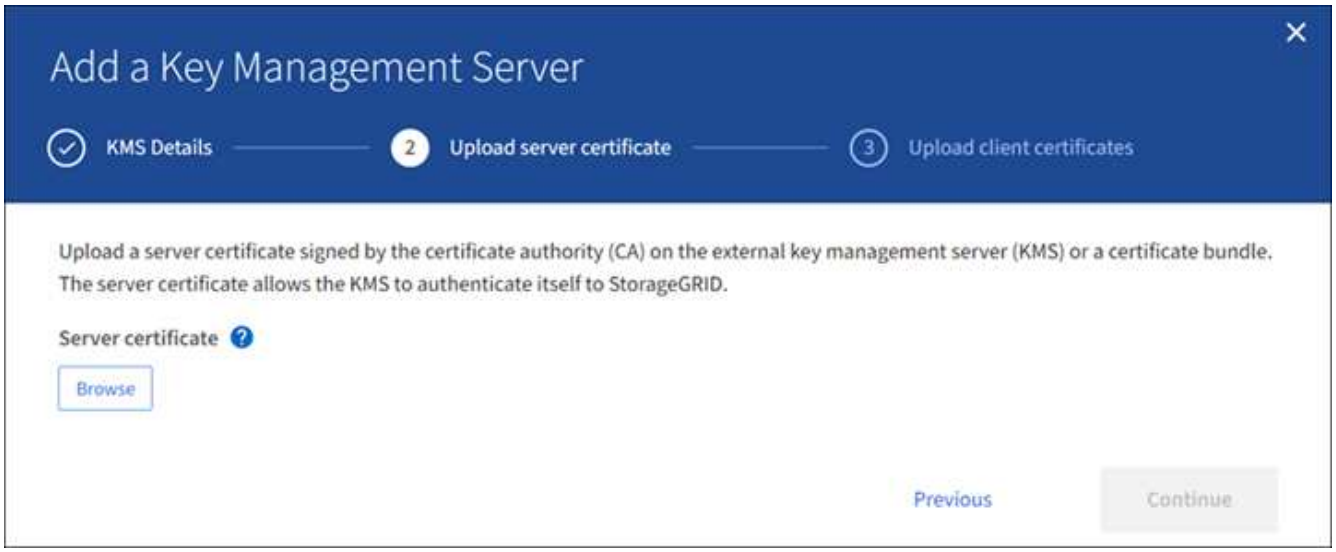
4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。
5. 选择 * 继续 * 。

第2步：上传服务器证书

在添加密钥管理服务器向导的步骤2 (上传服务器证书)中、您可以上传KMS的服务器证书(或证书包)。通过服务器证书，外部 KMS 可以向 StorageGRID 进行身份验证。

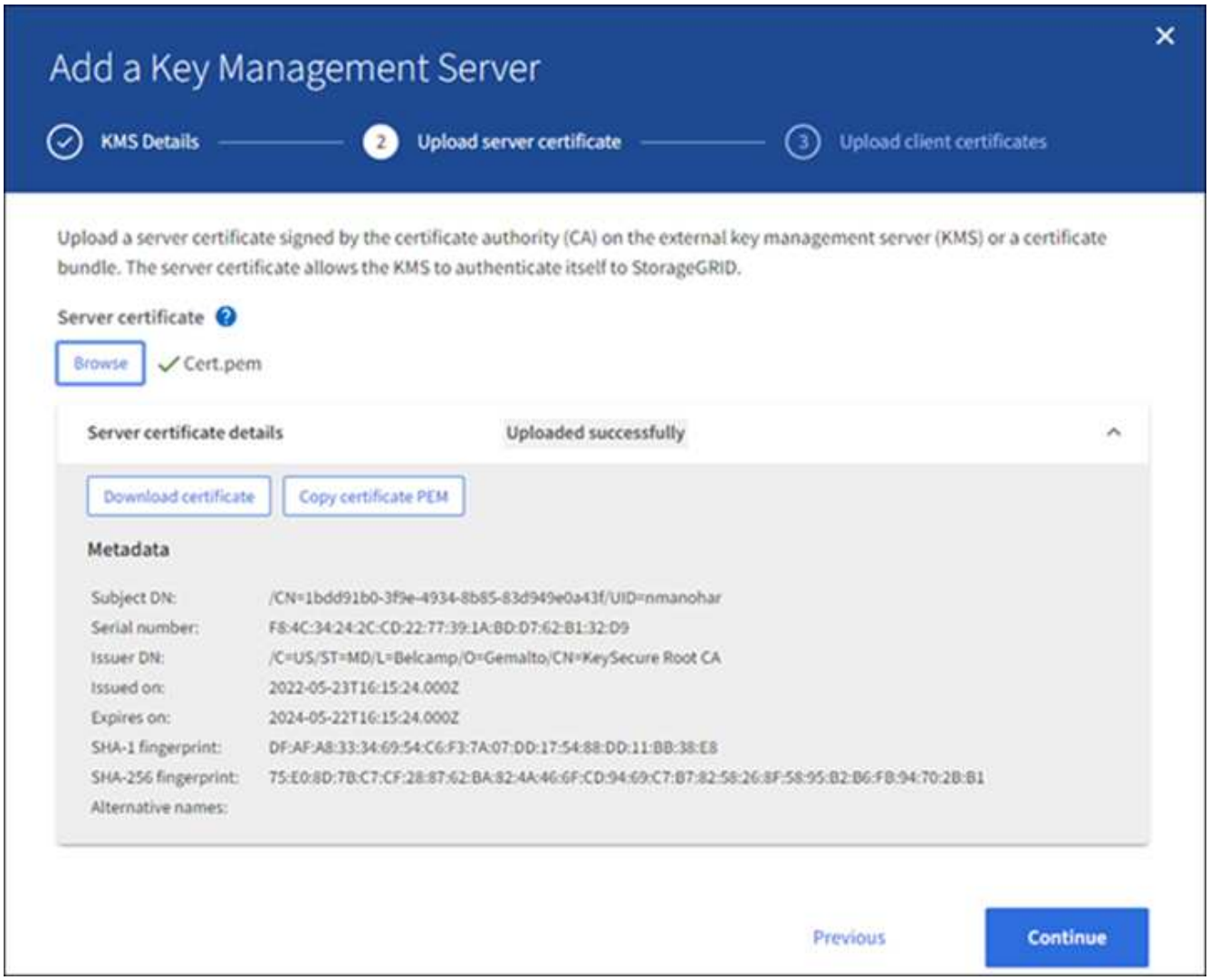
步骤

1. 从*步骤2 (上载服务器证书)*中，浏览到保存的服务器证书或证书包所在的位置。



2. 上传证书文件。

此时将显示服务器证书元数据。



如果您上传的是证书捆绑包，则每个证书的元数据将显示在其自己的选项卡上。

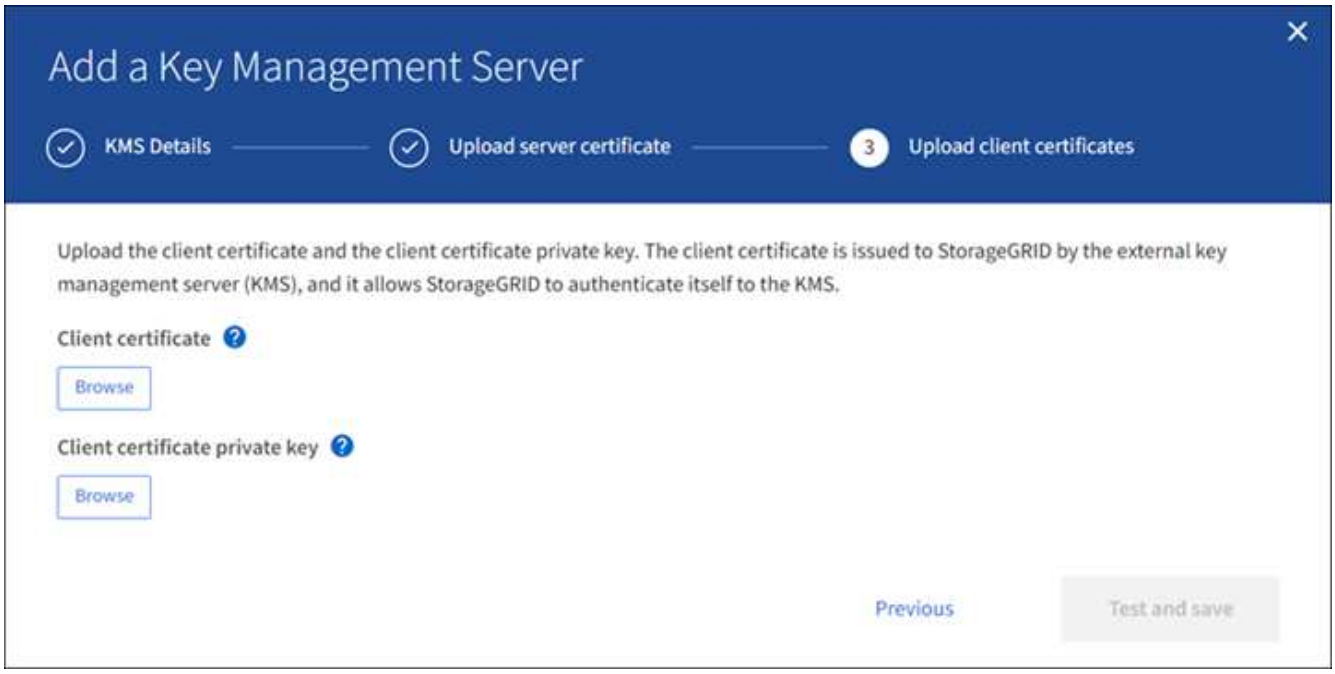
3. 选择 * 继续 * 。

第3步：上传客户端证书

在添加密钥管理服务器向导的步骤3 (上传客户端证书)中、您可以上传客户端证书和客户端证书专用密钥。客户端证书允许 StorageGRID 向 KMS 进行身份验证。

步骤

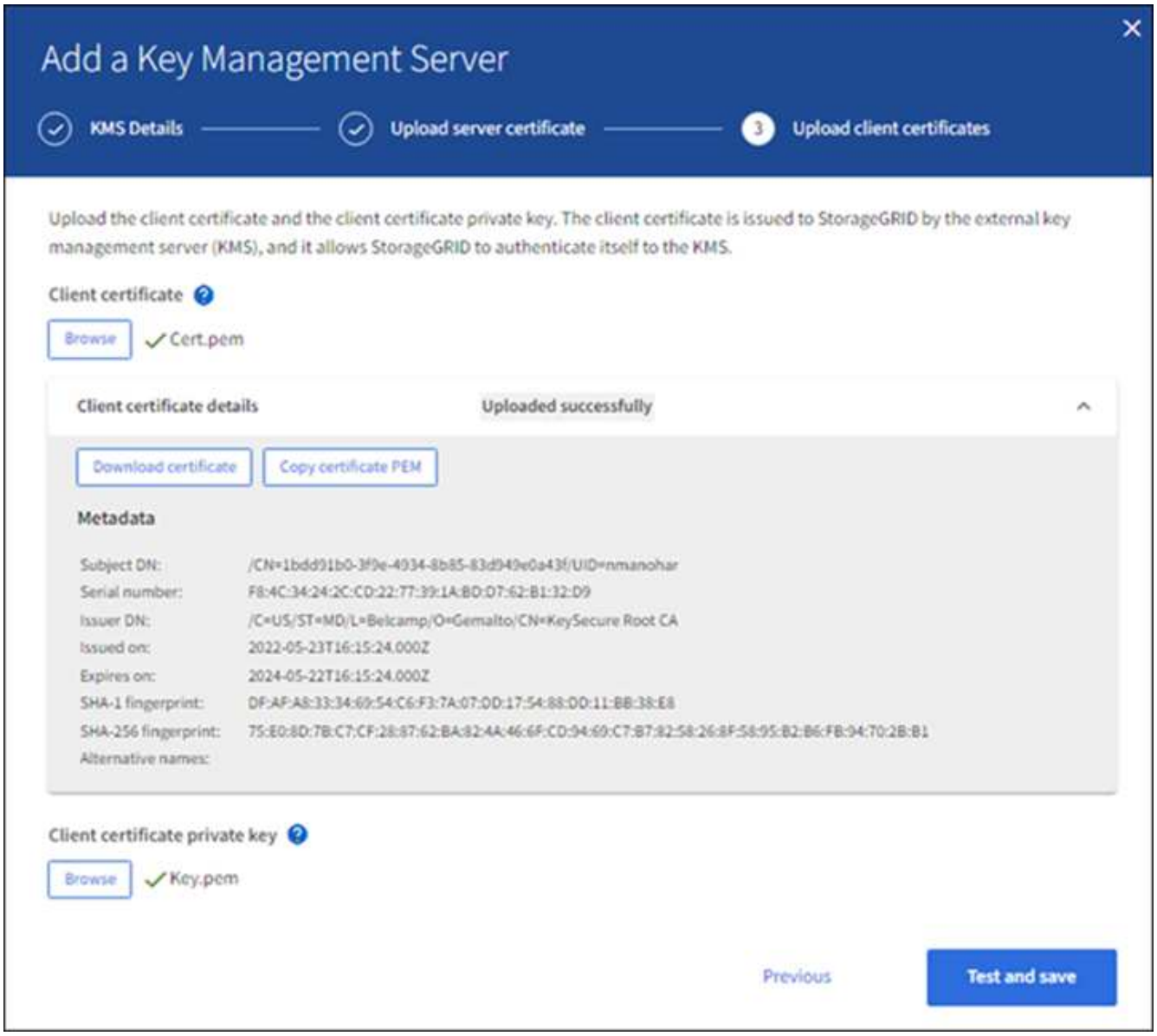
1. 从*步骤3 (上传客户端证书)*中，浏览到客户端证书的位置。



2. 上传客户端证书文件。

   此时将显示客户端证书元数据。

3. 浏览到客户端证书的专用密钥位置。
4. 上传私钥文件。



5. 选择*测试并保存*。

   测试密钥管理服务器与设备节点之间的连接。如果所有连接均有效，并且在 KMS 上找到正确的密钥，则新的密钥管理服务器将添加到密钥管理服务器页面上的表中。

   > 添加 KMS 后，密钥管理服务器页面上的证书状态将立即显示为未知。StorageGRID 可能需要长达 30 分钟才能获取每个证书的实际状态。您必须刷新 Web 浏览器才能查看当前状态。

6. 如果在选择*测试并保存*时出现错误信息，请查看消息详细信息，然后选择*OK*。

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

7. 如果需要在不测试外部连接的情况下保存当前配置，请选择*Force save*。

   > 选择*强制保存*可保存KMS配置，但不会测试从每个设备到该KMS的外部连接。如果具有此配置的问题描述 ，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

8. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 * 。

   已保存 KMS 配置，但未测试与 KMS 的连接。

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，包括服务器和客户端证书的当前状态。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面。配置详细信息选项卡将显示已配置的任何密钥管理服务器。

2. 查看每个 KMS 的表中的信息。

字段	**Description**
Kms名称	KMS 的描述性名称。
密钥名称	KMS 中 StorageGRID 客户端的密钥别名。
管理的密钥	与 KMS 关联的 StorageGRID 站点。 此字段显示特定 StorageGRID 站点的名称或 * 不由其他 KMS （默认 KMS ）管理的站点。 *
主机名	KMS 的完全限定域名或 IP 地址。 如果集群包含两个密钥管理服务器，则会列出这两个服务器的完全限定域名或 IP 地址。如果集群中有两个以上的密钥管理服务器，则会列出第一个 KMS 的完全限定域名或 IP 地址以及集群中其他密钥管理服务器的数量。 例如： `10.10.10.10 and 10.10.10.11` 或 `10.10.10.10 and 2 others`。 要查看集群中的所有主机名，请打开KMS并选择*Edit* 或*Actions*>*Edit*。
证书到期	服务器证书，可选 CA 证书和客户端证书的当前状态：有效，已过期，即将到期或未知。 注意： StorageGRID 可能需要长达30分钟才能获得证书到期更新。您必须刷新 Web 浏览器才能查看当前值。

3. 如果证书到期时间未知、请等待30分钟、然后刷新Web浏览器。

> 添加KMS后、"密钥管理服务器"页面上的证书过期将立即显示为"未知"。StorageGRID 可能需要长达 30 分钟才能获取每个证书的实际状态。您必须刷新 Web 浏览器才能查看实际状态。

4. 如果证书到期列指示某个证书已到期或即将到期、请尽快联系问题描述。

   触发*KMS CA证书到期*、*KMS客户端证书到期*和*KMS服务器证书到期*警报时，请记下每个警报的问题描述 并执行建议的操作。

   > 要保持数据访问，您必须尽快解决任何证书问题。

5. 要查看此KMS的证书详细信息、请从表中选择KMS名称。
6. 在KMS摘要页面上、查看服务器证书和客户端证书的元数据和证书PEM。根据需要，选择*编辑证书*以将证书替换为新证书。

查看加密节点

您可以查看有关 StorageGRID 系统中已启用 * 节点加密 * 设置的设备节点的信息。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面。配置详细信息选项卡显示已配置的任何密钥管理服务器。

2. 从页面顶部选择*加密节点*选项卡。

   加密节点选项卡列出了StorageGRID 系统中启用了*Node Encryption *设置的设备节点。

3. 查看表中每个设备节点的信息。

列	**Description**
Node name	设备节点的名称。
节点类型	节点的类型：存储，管理或网关。
站点	安装节点的 StorageGRID 站点的名称。
Kms名称	用于节点的 KMS 的描述性名称。 如果未列出KMS、请选择配置详细信息选项卡以添加KMS。 "添加密钥管理服务器（KMS）"
密钥 UID	用于对设备节点上的数据进行加密和解密的加密密钥的唯一 ID 。要查看整个密钥UID、请将光标置于单元格上方。 短划线（ - ）表示密钥 UID 未知，可能是因为设备节点和 KMS 之间存在连接问题描述 。

列	Description
Status	KMS 与设备节点之间的连接状态。如果节点已连接，则时间戳每 30 分钟更新一次。更改 KMS 配置后，可能需要几分钟才能更新连接状态。 • 注意： * 您必须刷新 Web 浏览器才能查看新值。

4. 如果状态列指示 KMS 问题描述 ，请立即解决此问题描述 。

   在正常的 KMS 操作期间，状态将为 * 已连接到 KMS* 。如果节点与网格断开连接，则会显示节点连接状态（ administratively down 或 Unknown ）。

   其他状态消息对应于同名的 StorageGRID 警报：

   - 无法加载 Kms 配置
   - Kms 连接错误
   - 未找到 Kms 加密密钥名称
   - Kms 加密密钥轮换失败
   - Kms 密钥无法对设备卷进行解密
   - 未配置公里

   对这些警报执行建议的操作。

   > 您必须立即解决任何问题，以确保您的数据得到完全保护。

编辑密钥管理服务器（ **KMS** ）

例如，如果证书即将到期，您可能需要编辑密钥管理服务器的配置。

开始之前

- 您已查看 "使用密钥管理服务器的注意事项和要求"。
- 如果您计划更新为 KMS 选择的站点，则已查看 "更改站点的 KMS 的注意事项"。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面、并显示已配置的所有密钥管理服务器。

2. 选择要编辑的KMS，然后选择*Actions*>*Edit*。

   您也可以通过在表中选择KMS名称并在KMS详细信息页面上选择*Edit*来编辑KMS。

3. (可选)更新编辑密钥管理服务器向导的*步骤1 (KMS详细信息)*中的详细信息。

字段	Description
Kms名称	一个描述性名称，可帮助您标识此 KMS 。必须介于 1 到 64 个字符之间。
密钥名称	StorageGRID 客户端在 KMS 中的确切密钥别名。必须介于 1 到 255 个字符之间。 在极少数情况下，您只需要编辑密钥名称。例如，如果在 KMS 中重命名了别名，或者先前密钥的所有版本都已复制到新别名的版本历史记录中，则必须编辑密钥名称。 切勿尝试通过更改 KMS 的密钥名称（别名）来旋转密钥。而是通过更新 KMS 软件中的密钥版本来轮换密钥。StorageGRID 要求使用相同密钥别名从 KMS 访问以前使用的所有密钥版本（以及将来的任何密钥版本）。如果更改已配置 KMS 的密钥别名，则 StorageGRID 可能无法对数据进行解密。 "使用密钥管理服务器的注意事项和要求"
管理的密钥	如果您正在编辑特定于站点的KMS，并且还没有默认的KMS，则可以选择*不由另一个KMS管理的站点(默认KMS)*。此选择会将特定于站点的KMS转换为默认KMS、这将应用于没有专用KMS的所有站点以及扩展中添加的任何站点。 *注:*如果您正在编辑特定于站点的KMS，则不能选择其他站点。如果您正在编辑默认KMS、则无法选择特定站点。
Port	KMS 服务器用于密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）通信的端口。默认为 5696 ，即 KMIP 标准端口。
主机名	KMS 的完全限定域名或 IP 地址。 *注意：*服务器证书的使用者替代名称(SAN)字段必须包含您在此处输入的FQDN或IP地址。否则， StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

4. 如果要配置KMS群集，请选择*添加另一主机名*为群集中的每台服务器添加主机名。
5. 选择 * 继续 * 。

   此时将显示编辑密钥管理服务器向导的第2步(上传服务器证书)。

6. 如果需要替换服务器证书，请选择 * 浏览 * 并上传新文件。
7. 选择 * 继续 * 。

   此时将显示编辑密钥管理服务器向导的第3步(上传客户端证书)。

8. 如果需要替换客户端证书和客户端证书专用密钥，请选择 * 浏览 * 并上传新文件。
9. 选择*测试并保存*。

测试密钥管理服务器与受影响站点上的所有节点加密设备节点之间的连接。如果所有节点连接均有效，并且在 KMS 上找到正确的密钥，则密钥管理服务器将添加到密钥管理服务器页面上的表中。

10. 如果显示错误消息，请查看消息详细信息，然后选择 * 确定 * 。

    例如，如果为此 KMS 选择的站点已由另一个 KMS 管理，或者连接测试失败，则可能会收到 422 ：Unprocessable Entity 错误。

11. 如果需要在解决连接错误之前保存当前配置，请选择*Force save*。

    > 选择*强制保存*可保存KMS配置，但不会测试从每个设备到该KMS的外部连接。如果具有此配置的问题描述 ，则可能无法重新启动受影响站点上已启用节点加密的设备节点。在问题解决之前，您可能无法访问数据。

    此时将保存 KMS 配置。

12. 查看确认警告，如果确实要强制保存配置，请选择 * 确定 * 。

    已保存 KMS 配置，但未测试与 KMS 的连接。

删除密钥管理服务器（ **KMS** ）

在某些情况下，您可能需要删除密钥管理服务器。例如，如果您已停用站点，则可能需要删除站点专用的 KMS 。

开始之前

- 您已查看 "使用密钥管理服务器的注意事项和要求"。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

关于此任务

在以下情况下，您可以删除 KMS ：

- 如果站点已停用，或者站点中没有启用节点加密的设备节点，则可以删除站点专用的 KMS 。
- 如果每个站点已存在站点专用的 KMS ，并且已启用设备节点加密，则可以删除默认 KMS 。

步骤

1. 选择 * 配置 * > * 安全性 * > * 密钥管理服务器 * 。

   此时将显示密钥管理服务器页面、并显示已配置的所有密钥管理服务器。

2. 选择要删除的KMS，然后选择*Actions*>*Remove*。

   您也可以通过在表中选择KMS名称并从KMS详细信息页面中选择*Remove*来删除KMS。

3. 确认满足以下条件：
   - 您要删除某个站点的特定于站点的KMS、而此站点没有启用节点加密的设备节点。
   - 您要删除默认KMS、但每个站点都已存在具有节点加密的站点专用KMS。

4. 选择 * 是 * 。

   此时将删除 KMS 配置。

管理代理设置

配置存储代理设置

如果您使用的是平台服务或云存储池，则可以在存储节点和外部 S3 端点之间配置非透明代理。例如，您可能需要一个非透明代理来允许将平台服务消息发送到外部端点，例如 Internet 上的端点。

开始之前

- 您具有特定的访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

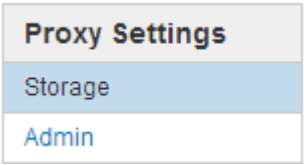
关于此任务

您可以为单个存储代理配置设置。

步骤

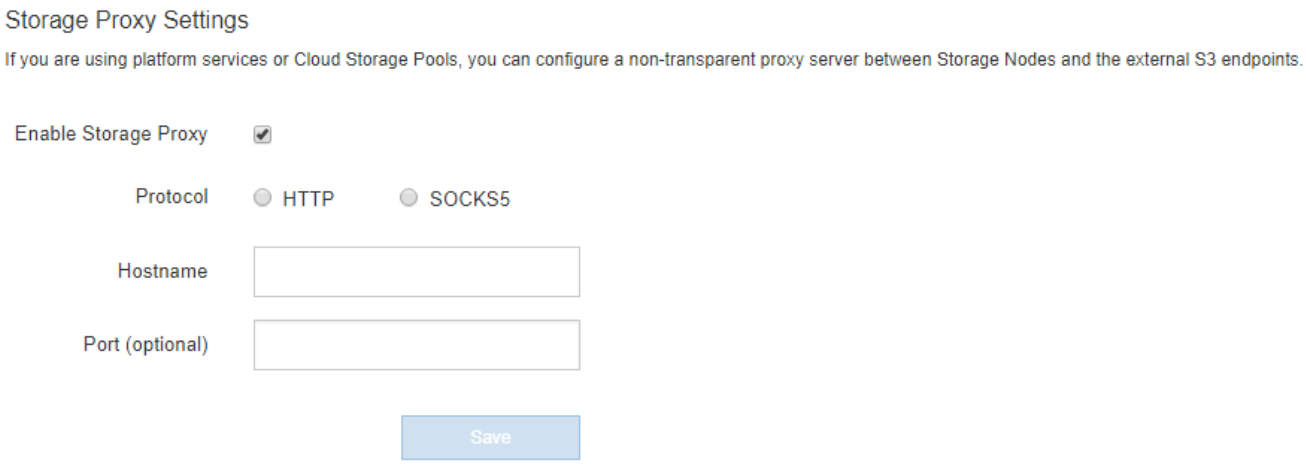
1. 选择 * 配置 * > * 安全性 * > * 代理设置 * 。

   此时将显示存储代理设置页面。默认情况下，在边栏菜单中选择了 * 存储 * 。



2. 选中*启用存储代理*复选框。

   此时将显示用于配置存储代理的字段。



3. 为非透明存储代理选择协议。

4. 输入代理服务器的主机名或 IP 地址。
5. （可选）输入用于连接到代理服务器的端口。

   如果对协议使用默认端口，则可以将此字段留空： 80 表示 HTTP ， 1080 表示 SOCKS5 。

6. 选择 * 保存 * 。

   保存存储代理后，可以配置和测试平台服务或云存储池的新端点。

   > 代理更改可能需要长达 10 分钟才能生效。

7. 检查代理服务器的设置，以确保不会阻止来自 StorageGRID 的平台服务相关消息。

完成后

如果需要禁用存储代理，请清除*启用存储代理*复选框，然后选择*保存*。

相关信息

- "用于平台服务的网络和端口"
- "使用 ILM 管理对象"

配置管理员代理设置

如果使用 HTTP 或 HTTPS 发送 AutoSupport 消息（请参见 "配置 AutoSupport"），您可以在管理节点和技术支持（AutoSupport）之间配置非透明代理服务器。

开始之前

- 您具有特定的访问权限。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。

关于此任务

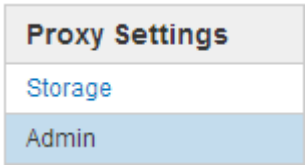
您可以为单个管理员代理配置设置。

步骤

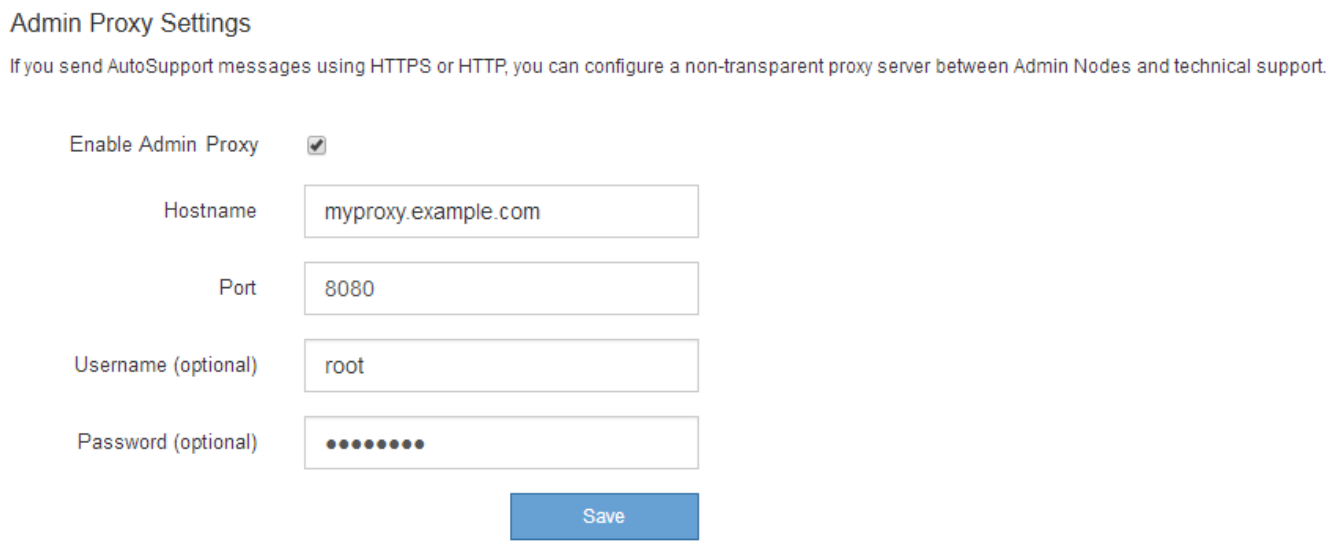
1. 选择 * 配置 * > * 安全性 * > * 代理设置 * 。

   此时将显示 Admin Proxy Settings 页面。默认情况下，在边栏菜单中选择了 * 存储 * 。

2. 从边栏菜单中选择 * 管理 * 。



3. 选中*启用管理员代理*复选框。



4. 输入代理服务器的主机名或 IP 地址。
5. 输入用于连接到代理服务器的端口。
6. （可选）输入代理用户名。

   如果您的代理服务器不需要用户名，请将此字段留空。

7. （可选）输入代理密码。

   如果您的代理服务器不需要密码，请将此字段留空。

8. 选择 * 保存 * 。

   保存管理代理后，将在管理节点和技术支持之间配置代理服务器。

   > 代理更改可能需要长达 10 分钟才能生效。

9. 如果需要禁用代理，请清除*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访问

您可以在外部防火墙处打开或关闭特定端口。

您可以通过在外部防火墙中打开或关闭特定端口来控制对 StorageGRID 管理节点上用户界面和 API 的访问。例如，除了使用其他方法控制系统访问之外，您可能还希望防止租户能够在防火墙处连接到网格管理器。

如果要配置StorageGRID 内部防火墙、请参见 "配置内部防火墙"。

Port	Description	端口是否已打开 ...
443.	管理节点的默认 HTTPS 端口	Web 浏览器和管理 API 客户端可以访问网格管理器，网格管理 API ，租户管理器和租户管理 API 。 • 注： * 端口 443 也用于某些内部流量。
8443	管理节点上的网格管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问网格管理器和网格管理 API 。 • Web浏览器和管理API客户端无法访问租户管理器或租户管理API。 • 请求内部内容将被拒绝。
9443	管理节点上的租户管理器端口受限	• Web 浏览器和管理 API 客户端可以使用 HTTPS 访问租户管理器和租户管理 API 。 • Web浏览器和管理API客户端无法访问网格管理器或网格管理API。 • 请求内部内容将被拒绝。

受限网格管理器或租户管理器端口上不提供单点登录（ SSO ）。如果您希望用户通过单点登录进行身份验证，则必须使用默认 HTTPS 端口（ 443 ）。

相关信息

- "登录到网格管理器"
- "创建租户帐户"
- "外部通信"

管理内部防火墙控制

StorageGRID 在每个节点上都包含一个内部防火墙、可通过控制对节点的网络访问来增强网格的安全性。使用防火墙可阻止对特定网格部署所需端口以外的所有端口进行网络访问。在防火墙控制页面上所做的配置更改将部署到每个节点。

使用防火墙控制页面上的三个选项卡自定义网格所需的访问权限。

- 特权地址列表：使用此选项卡允许对关闭的端口进行选定访问。您可以使用CIDR表示法添加IP地址或子网、以访问使用管理外部访问选项卡关闭的端口。
- 管理外部访问：使用此选项卡关闭默认打开的端口，或重新打开先前关闭的端口。
- 不可信客户端网络：使用此选项卡指定节点是否信任来自客户端网络的入站流量。

  此选项卡还提供了指定在配置了不可信客户端网络时要打开的其他端口的选项。这些端口可以提供对网格管理器和/或租户管理器的访问。

  此选项卡上的设置将覆盖管理外部访问选项卡中的设置。

- 具有不可信客户端网络的节点仅接受在该节点上配置的负载平衡器端点端口(全局端点、节点接口和受节点类型制约的端点)上的连接。
- 在不可信客户端网络选项卡下打开的其他端口将在所有不可信客户端网络上打开、即使未配置负载平衡器端点也是如此。
- 无论"管理外部网络"选项卡上的设置如何、负载平衡器端点端口和选定的其他端口_都是不可信客户端网络上唯一打开的端口_。
- 如果受信任、则可以访问在"管理外部访问"选项卡下打开的所有端口以及在客户端网络上打开的任何负载平衡器端点。

> 您在一个选项卡上所做的设置可能会影响您在另一个选项卡上所做的访问更改。请务必检查所有选项卡上的设置、以确保您的网络按预期方式运行。

要配置内部防火墙控制、请参见 "配置防火墙控件"。

有关外部防火墙和网络安全的详细信息、请参阅 "在外部防火墙处控制访问"。

特权地址列表和管理外部访问选项卡

通过特权地址列表选项卡、您可以注册一个或多个被授予对关闭的网格端口访问权限的IP地址。通过"管理外部访问"选项卡、您可以关闭对选定外部端口或所有打开的外部端口的外部访问(默认情况下、外部端口可由非网格节点访问)。这两个选项卡通常可结合使用来定制网格所需的确切网络访问。

> 默认情况下、有权限的IP地址不具有内部网格端口访问权限。

示例**1**：使用跳转主机执行维护任务

假设您要使用跳转主机(一个增强安全的主机)进行网络管理。您可以使用以下常规步骤：

1. 使用特权地址列表选项卡添加跳转主机的IP地址。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后、网格中管理节点上的所有外部端口都将被阻止用于除跳转主机之外的所有主机。然后、您可以使用跳转主机更安全地在网格上执行维护任务。

示例**2**：限制对网格管理器和租户管理器的访问

假设出于安全原因、您希望限制对网格管理器和租户管理器的访问。您可以使用以下常规步骤：

1. 使用"管理外部访问"选项卡上的切换功能阻止端口443。
2. 使用管理外部访问选项卡上的切换以允许访问端口8443。
3. 使用管理外部访问选项卡上的切换以允许访问端口9443。

保存配置后、主机将无法访问端口443、但仍可通过端口8443访问网格管理器、并通过端口9443访问租户管理器。

示例**3**：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(例如、端口22上的SSH)。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服务的主机授予访问权限。
2. 使用管理外部访问选项卡阻止所有端口。

> 在阻止端口443和8443之前、请添加特权IP地址。当前连接到被阻止端口的任何用户(包括您)将无法访问Grid Manager、除非其IP地址已添加到特权地址列表中。

保存配置后、端口22和SSH服务将可供特权地址列表中的主机使用。无论请求来自哪个接口、所有其他主机都将被拒绝访问此服务。

示例**4**：禁止访问未使用的服务

在网络级别、您可以禁用一些不打算使用的服务。例如、如果您不提供Swift访问、则应执行以下常规步骤：

1. 使用管理外部访问选项卡上的切换功能阻止端口18083。
2. 使用管理外部访问选项卡上的切换功能阻止端口18085。

保存配置后、存储节点将不再允许Swift连接、而是继续允许访问未阻止的端口上的其他服务。

不可信客户端网络选项卡

如果您使用的是客户端网络、则可以通过仅在显式配置的端点或您在此选项卡上选择的其他端口上接受入站客户端流量来帮助保护StorageGRID 免受恶意攻击。

默认情况下，每个网格节点上的客户端网络均为 *trusted* 。也就是说、默认情况下、StorageGRID 信任所有网格节点的入站连接 "可用外部端口"。

您可以通过指定每个节点上的客户端网络为 *untrused_* 来减少对 StorageGRID 系统的恶意攻击威胁。如果节点的客户端网络不可信、则该节点仅接受显式配置为负载平衡器端点的端口以及使用防火墙控制页面上的不可信客户端网络选项卡指定的任何其他端口上的入站连接。请参见 "配置负载平衡器端点" 和 "配置防火墙控件"。

示例 **1** ： 网关节点仅接受 **HTTPS S3** 请求

假设您希望网关节点拒绝客户端网络上除 HTTPS S3 请求以外的所有入站流量。您应执行以下常规步骤：

1. 从 "负载平衡器端点" 页面上、通过端口443为基于HTTPS的S3配置负载平衡器端点。
2. 在防火墙控制页面中、选择不可信以指定网关节点上的客户端网络不可信。

保存配置后，网关节点客户端网络上的所有入站流量都会被丢弃，但端口 443 上的 HTTPS S3 请求和 ICMP 回显（ ping ）请求除外。

示例 **2** ： 存储节点发送 **S3** 平台服务请求

假设您要启用来自存储节点的出站S3平台服务流量、但要阻止客户端网络上与该存储节点的任何入站连接。您应执行此常规步骤：

- 在防火墙控制页面的不可信客户端网络选项卡中、指示存储节点上的客户端网络不可信。

保存配置后、存储节点将不再接受客户端网络上的任何传入流量、但仍允许向已配置的平台服务目标发出出站请求。

示例**3**：限制对网格管理器的子网访问

假设您希望仅允许对特定子网进行网格管理器访问。您应执行以下步骤：

1. 将管理节点的客户端网络连接到子网。
2. 使用不可信客户端网络选项卡将客户端网络配置为不可信。
3. 在选项卡的*在不可信客户端网络上打开的其他端口*部分，添加端口443或8443。
4. 使用管理外部访问选项卡阻止所有外部端口(无论是否为该子网以外的主机设置了特权IP地址)。

保存配置后、只有指定子网上的主机才能访问网格管理器。所有其他主机均被阻止。

配置内部防火墙

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

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您已查看中的信息 "管理防火墙控制" 和 "网络连接准则"。
- 如果您希望管理节点或网关节点仅在显式配置的端点上接受入站流量，则已定义负载平衡器端点。

> 更改客户端网络的配置时、如果未配置负载平衡器端点、现有客户端连接可能会失败。

关于此任务

StorageGRID 在每个节点上都有一个内部防火墙、可用于打开或关闭网格节点上的部分端口。您可以使用防火墙控制选项卡打开或关闭网格网络、管理网络和客户端网络上默认打开的端口。您还可以创建一个可访问关闭的网格端口的特权IP地址列表。如果您使用的是客户端网络、则可以指定节点是否信任客户端网络的入站流量、并且可以配置客户端网络上特定端口的访问。

将向网格外部的IP地址开放的端口数限制为仅限绝对必要的端口、可增强网格的安全性。您可以使用三个防火墙控制选项卡中每个选项卡上的设置来确保仅打开所需的端口。

有关使用防火墙控件的详细信息(包括示例)、请参见 "管理防火墙控制"。

有关外部防火墙和网络安全的详细信息、请参阅 "在外部防火墙处控制访问"。

访问防火墙控件

步骤

1. 选择*configuration*>*Security*>*Firewall control*。

   介绍了此页面上的三个选项卡 "管理防火墙控制"。

2. 选择任何选项卡以配置防火墙控件。

您可以按任意顺序使用这些选项卡。您在一个选项卡上设置的配置不会限制在其他选项卡上可以执行的操作；但是、在一个选项卡上进行的配置更改可能会更改在其他选项卡上配置的端口的行为。

特权地址列表

您可以使用特权地址列表选项卡授予主机对默认关闭或通过管理外部访问选项卡上的设置关闭的端口的访问权限。

默认情况下、有权限的IP地址和子网不具有内部网格访问权限。此外、即使在"管理外部访问"选项卡中阻止了负载平衡器端点和在"特权地址列表"选项卡中打开的其他端口、也可以访问。

> 特权地址列表选项卡上的设置不能覆盖不可信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*以CIDR表示法添加其他IP地址或子网*以添加其他有权限的客户端。

   > 向特权列表中添加尽可能少的地址。

3. (可选)选择*允许有权限的IP地址访问StorageGRID 内部端口*。请参见 "StorageGRID 内部端口"。

   > 此选项会删除对内部服务的一些保护。如果可能、请将其禁用。

4. 选择 * 保存 * 。

管理外部访问

在"管理外部访问"选项卡中关闭某个端口后、任何非网格IP地址都无法访问该端口、除非您将该IP地址添加到特权地址列表中。您只能关闭默认情况下处于打开状态的端口、并且只能打开已关闭的端口。

> "管理外部访问"选项卡上的设置无法覆盖"不可信客户端网络"选项卡上的设置。例如、如果节点不可信、则客户端网络上会阻止端口SSH/ 22、即使此端口在管理外部访问选项卡上打开也是如此。不可信客户端网络选项卡上的设置会覆盖客户端网络上已关闭的端口(例如443、8443、9443)。

步骤

1. 选择*管理外部访问*。此选项卡将显示一个表、其中包含网格中节点的所有外部端口(默认情况下可由非网格节点访问的端口)。
2. 使用以下选项配置要打开和关闭的端口：
   - 使用每个端口旁边的切换键打开或关闭选定端口。
   - 选择*打开所有显示的端口*以打开表中列出的所有端口。
   - 选择*关闭所有显示的端口*以关闭表中列出的所有端口。

   > 如果关闭网格管理器端口443或8443、则当前连接到被阻止端口的任何用户(包括您)将无法访问网格管理器、除非其IP地址已添加到特权地址列表中。

> 使用表右侧的滚动条确保您已查看所有可用端口。使用搜索字段输入端口号以查找任何外部端口的设置。您可以输入部分端口号。例如，如果输入*2*，则会显示名称中包含字符串“2”的所有端口。

3. 选择 * 保存 *

不可信客户端网络

如果节点的客户端网络不可信、则该节点仅接受配置为负载平衡器端点的端口以及您在此选项卡上选择的其他端口(可选)上的入站流量。您还可以使用此选项卡为扩展中添加的新节点指定默认设置。

> 如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

在*不可信客户端网络*选项卡上所做的配置更改将覆盖*管理外部访问*选项卡上的设置。

步骤

1. 选择*不可信客户端网络*。
2. 在设置新节点默认值部分中、指定在扩展操作步骤 中向网格添加新节点时的默认设置。
   - 可信(默认)：在扩展中添加节点时、其客户端网络是可信的。
   - * 不可信 * ：在扩展中添加节点时，其客户端网络不可信。

     您可以根据需要返回此选项卡来更改特定新节点的设置。

     > 此设置不会影响 StorageGRID 系统中的现有节点。

3. 使用以下选项选择仅允许在显式配置的负载平衡器端点或其他选定端口上进行客户端连接的节点：
   - 选择*在显示的节点上取消信任*，将表中显示的所有节点添加到不可信客户端网络列表中。
   - 选择*在显示的节点上信任*，从不可信客户端网络列表中删除表中显示的所有节点。
   - 使用每个端口旁边的切换功能将选定节点的客户端网络设置为可信或不可信。

     例如，您可以选择*Untrust on displayed N点*将所有节点添加到Untrusted Client Network列表中，然后使用单个节点旁边的切换将该单个节点添加到Trusted Client Network列表中。

     > 使用表右侧的滚动条确保您已查看所有可用节点。使用搜索字段输入节点名称以查找任何节点的设置。您可以输入部分名称。例如，如果输入*GW*，则会显示名称中包含字符串"gw"的所有节点。

4. (可选)选择要在不可信客户端网络上打开的任何其他端口。这些端口可以提供对网格管理器和/或租户管理器的访问。

   例如、您可能希望使用此选项来确保可以在客户端网络上访问网格管理器进行维护。

   > 这些附加端口在客户端网络上处于打开状态、无论它们是否在管理外部访问选项卡中关闭。

5. 选择 * 保存 * 。

此时将立即应用并实施新的防火墙设置。如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

管理租户

管理租户：概述

作为网格管理员、您可以创建和管理S3和Swift客户端用于存储和检索对象的租户帐户。

> 对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

什么是租户帐户？

租户帐户允许您使用简单存储服务（ S3 ） REST API 或 Swift REST API 在 StorageGRID 系统中存储和检索对象。

每个租户帐户都具有联合组或本地组、用户、S3分段或Swift容器以及对象。

租户帐户可用于按不同实体隔离存储的对象。例如，以下任一使用情形均可使用多个租户帐户：

- * 企业用例： * 如果您在企业应用程序中管理 StorageGRID 系统，则可能需要按组织中的不同部门隔离网格的对象存储。在这种情况下，您可以为营销部门，客户支持部门，人力资源部门等创建租户帐户。

  > 如果使用S3客户端协议、则可以使用S3分段和分段策略在企业的各个部门之间隔离对象。您不需要使用租户帐户。请参见实施说明 "S3存储分段和存储分段策略" 有关详细信息 ...

- * 服务提供商用例： * 如果您将 StorageGRID 系统作为服务提供商进行管理，则可以按要在网格上租用存储的不同实体来隔离网格的对象存储。在这种情况下，您将为公司 A ，公司 B ，公司 C 等创建租户帐户。

有关详细信息，请参见 "使用租户帐户"。

如何创建租户帐户？

创建租户帐户时，您可以指定以下信息：

- 基本信息、包括租户名称、客户端类型(S3或Swift)和可选存储配额。
- 租户帐户的权限、例如租户帐户是否可以使用S3平台服务、配置自己的身份源、使用S3 Select或使用网格联盟连接。
- 租户的初始root访问权限、具体取决于StorageGRID 系统是使用本地组和用户、身份联合还是单点登录(SSO)。

此外、如果S3租户帐户需要符合法规要求、您可以为StorageGRID 系统启用S3对象锁定设置。启用 S3 对象锁定后，所有 S3 租户帐户均可创建和管理合规的存储分段。

租户管理器的用途是什么？

创建租户帐户后、租户用户可以登录到租户管理器来执行如下任务：

- 设置身份联合(除非身份源与网格共享)

- 管理组和用户
- 使用网格联盟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存储分段
- 使用S3平台服务
- 使用 S3 Select
- 监控存储使用情况

> 虽然S3租户用户可以使用租户管理器创建和管理S3访问密钥和存储分段、但他们必须使用S3客户端应用程序来加存和管理对象。请参见 "使用S3 REST API" 了解详细信息。

> Swift 用户必须具有 root 访问权限才能访问租户管理器。但是， " 根 " 访问权限不允许用户通过 Swift REST API 的身份验证来创建容器和载入对象。用户必须具有 Swift 管理员权限才能向 Swift REST API 进行身份验证。

创建租户帐户

您必须至少创建一个租户帐户，才能控制对 StorageGRID 系统中存储的访问。

创建租户帐户的步骤因是否使用而异 "身份联合" 和 "单点登录" 已配置，并且您用于创建租户帐户的网格管理器帐户是否属于具有 root 访问权限的管理组。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有root访问权限或租户帐户权限。
- 如果租户帐户将使用为网格管理器配置的身份源，并且您要将租户帐户的 root 访问权限授予某个联合组，则您已将该联合组导入到网格管理器中。您无需为此管理员组分配任何网格管理器权限。请参见 "管理管理组"。
- 如果要允许S3租户克隆帐户数据并使用网格联合连接将存储分段对象复制到另一个网格：
  - 您已拥有 "已配置网格联合连接"。
  - 连接状态为*已连接*。
  - 您具有 root 访问权限。
  - 您已查看的注意事项 "管理网格联盟允许的租户"。
  - 如果租户帐户将使用为Grid Manager配置的身份源、则您已将同一联盟组导入到两个网格上的Grid Manager中。

    创建租户时、您需要选择此组、以获得源租户帐户和目标租户帐户的初始root访问权限。

    > 如果在创建租户之前此管理员组不在两个网格上、则不会将租户复制到目标。

访问向导

步骤

1. 选择 * 租户 * 。
2. 选择 * 创建 * 。

输入详细信息

步骤

1. 输入租户的详细信息。

字段	Description
Name	租户帐户的名称。租户名称不需要唯一。创建租户帐户时、它会收到一个唯一的20位数帐户ID。
问题描述 (可选)	用于帮助识别租户的问题描述。 如果您要创建将使用网格联合连接的租户、也可以使用此字段帮助确定哪个是源租户、哪个是目标租户。例如、对于在网格1上创建的租户、如果该租户复制到网格2、则也会显示此问题描述："This租户was created on Grid 1"(此租户已在网格1上创建)。
客户端类型	此租户将使用的客户端协议类型，即*S3*或*swift。 注意：对Swift客户端应用程序的支持已弃用、将在未来版本中删除。
存储配额(可选)	如果希望此租户具有存储配额、则为配额和单位指定一个数值。

2. 选择 * 继续 * 。

选择权限

步骤

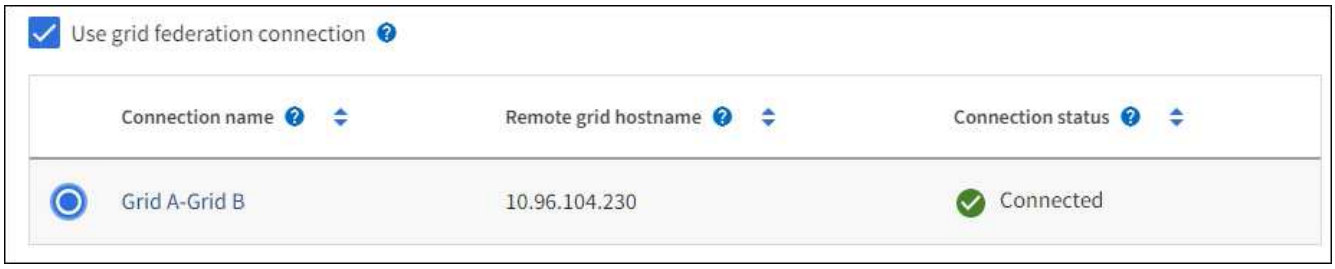
1. (可选)选择希望此租户拥有的任何权限。

其中某些权限还有其他要求。有关详细信息、请选择每个权限的帮助图标。

权限	如果选择…
允许平台服务	租户可以使用CloudMirror等S3平台服务。请参见 "管理 S3 租户帐户的平台服务"。
使用自己的身份源	租户可以为联盟组和用户配置和管理自己的身份源。如果您有、此选项将被禁用 "已配置SSO" 适用于您的StorageGRID 系统。

权限	如果选择...
允许S3选择	租户可以通过问题描述 S3选择对象内容API请求筛选和检索对象数据。请参见 "管理租户帐户的 S3 Select"。 重要：选择对象内容请求会降低所有S3客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。
使用网格联合连接	租户可以使用网格联合连接。 选择此选项： • 使此租户以及添加到帐户的所有租户组和用户从此网格(_ssource grid _)克隆到选定连接中的另一网格(_dDestination grid _)。 • 允许此租户在每个网格上的相应分段之间配置跨网格复制。 请参见 "管理网格联盟允许的租户"。 注意：创建新S3租户时、您只能选择*使用网格联合连接*；不能为现有租户选择此权限。

2. 如果选择了*使用网格联合连接*，请选择一个可用的网格联合连接。



3. 选择 * 继续 * 。

定义root访问权限并创建租户

步骤

1. 根据您的StorageGRID 系统是使用身份联合、单点登录(SSO)还是同时使用这两者、定义租户帐户的root访问权限。

选项	执行此操作 ...
如果未启用身份联合	指定以本地root用户身份登录租户时要使用的密码。
如果启用了身份联合	a. 选择一个现有联盟组、以便对租户具有root访问权限。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择一个现有联盟组、以便对租户具有root访问权限。没有本地用户可以登录。

2. 选择 * 创建租户 * 。

   此时将显示一条成功消息、新租户将列在租户页面上。要了解如何查看租户详细信息和监控租户活动、请参阅 "监控租户活动"。

3. 如果为租户选择了*使用网格联合连接*权限：

   a. 确认已将同一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位数帐户ID、名称、问题描述 、配额和权限。

   > 如果您看到错误消息"`租户在未克隆的情况下创建、`"、请参阅中的说明 "对网格联合错误进行故障排除"。

   b. 如果您在定义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" 复制的租户。

   > 在更改密码之前、本地root用户无法登录到目标网格上的租户管理器。

登录到租户(可选)

您可以根据需要立即登录到新租户以完成配置、也可以稍后登录到租户。登录步骤取决于您是使用默认端口(443)还是使用受限端口登录到网格管理器。请参见 "在外部防火墙处控制访问"。

立即登录

如果您使用的是 ...	执行此操作 ...
端口443、并且您为本地root用户设置了密码	1. 选择*以root身份登录*。 登录时、将显示用于配置分段、身份联合、组和用户的链接。 2. 选择用于配置租户帐户的链接。 每个链接都会在租户管理器中打开相应的页面。要完成此页面，请参见 "有关使用租户帐户的说明"。
端口443、并且您没有为本地root用户设置密码	选择*Sign In*，然后输入root访问联合组中用户的凭据。

如果您使用的是 ...	执行此操作 ...
受限端口	1. 选择*完成* 2. 在租户表中选择*受限*、了解有关访问此租户帐户的更多信息。 租户管理器的 URL 格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ° *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的IP地址 ° *port* 是仅租户端口 ° *20-digit-account-id* 是租户的唯一帐户ID

请稍后登录

如果您使用的是 ...	执行以下操作之一 ...
端口 443	• 在网格管理器中，选择 * 租户 * ，然后选择租户名称右侧的 * 登录 * 。 • 在 Web 浏览器中输入租户的 URL ： `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ° *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的IP地址 ° *20-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 * 租户 * ，然后选择 * 受限 * 。 • 在 Web 浏览器中输入租户的 URL ： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ° *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的IP地址 ° *port* 是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

按照中的说明进行操作 "使用租户帐户" 要管理租户组和用户、需要使用S3访问密钥、分段、平台服务以及帐户克隆和跨网格复制。

编辑租户帐户

您可以编辑租户帐户以更改显示名称、存储配额或租户权限。

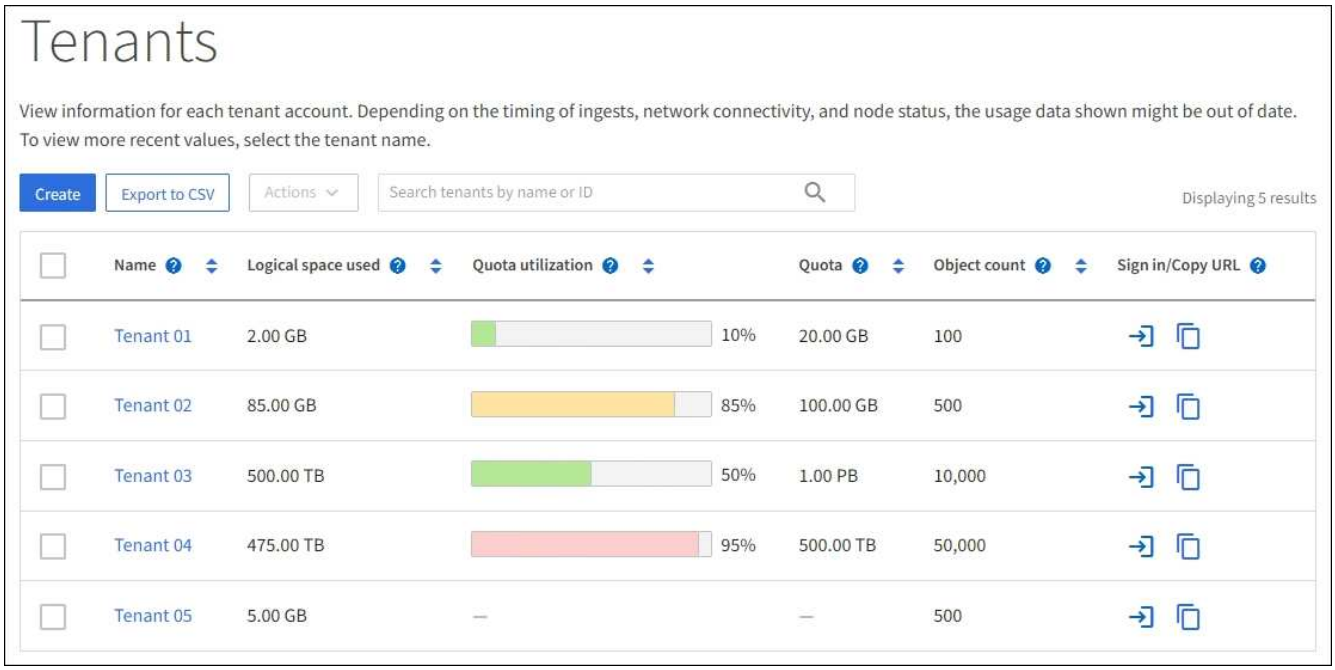
> 如果租户具有*使用网格联合连接*权限、您可以从连接中的任一网格编辑租户详细信息。但是、您对连接中一个网格所做的任何更改都不会复制到另一个网格。如果要使租户详细信息在网格之间保持精确同步、请在两个网格上进行相同的编辑。请参见 "管理网格联盟连接允许的租户"。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有root访问权限或租户帐户权限。

步骤

1. 选择 * 租户 * 。



2. 找到要编辑的租户帐户。

   使用搜索框按名称或租户ID搜索租户。

3. 选择租户。您可以执行以下任一操作：
   - 选中租户对应的复选框，然后选择*Actions*>*Edit*。
   - 选择租户名称以显示详细信息页面，然后选择*Edit*。
4. (可选)更改以下字段的值：
   - * 名称 *
   - * 问题描述 *
   - * 存储配额 *
5. 选择 * 继续 * 。
6. 选择或清除租户帐户的权限。
   - 如果对已在使用 * 平台服务 * 的租户禁用此服务，则其为 S3 分段配置的服务将停止工作。不会向租户发送任何错误消息。例如，如果租户已为 S3 存储分段配置了 CloudMirror 复制，则他们仍可将对象存储在存储分段中，但这些对象的副本将不再创建在已配置为端点的外部 S3 存储分段中。请参见 "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使用为网格管理器配置的身份源。

  如果*使用自己的身份源*为：

  - 已禁用并选中、租户已启用自己的身份源。租户必须先禁用其身份源，然后才能使用为网格管理器配置的身份源。
  - 已禁用但未选中、已为StorageGRID 系统启用SSO。租户必须使用为网格管理器配置的身份源。

- 根据需要选中或清除*允许S3 Select*权限。请参见 "管理租户帐户的 S3 Select"。
- 要删除*使用网格联合连接*权限，请按照的说明进行操作 "删除租户使用网格联盟的权限"。

更改租户的本地 root 用户的密码

如果 root 用户被锁定在帐户之外，您可能需要更改租户的本地 root 用户的密码。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

如果为StorageGRID 系统启用了单点登录(SSO)、则本地root用户无法登录到租户帐户。要执行 root 用户任务，用户必须属于对租户具有 root 访问权限的联合组。

步骤

1. 选择 * 租户 * 。

2. 选择租户帐户。您可以执行以下任一操作：
   - 选中租户对应的复选框，然后选择*Actions*>*更改root密码*。

    - 选择租户的名称以显示详细信息页面，然后选择*Actions*>*更改root密码*。
3. 输入租户帐户的新密码。
4. 选择 * 保存 * 。

删除租户帐户

如果要永久删除租户对系统的访问权限，可以删除租户帐户。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。
- 您已删除与租户帐户关联的所有分段(S3)、容器(Swift)和对象。
- 如果允许租户使用网格联盟连接、则您已查看了的注意事项 "删除具有使用网格联盟连接权限的租户"。

步骤

1. 选择 * 租户 * 。
2. 找到要删除的租户帐户。

   使用搜索框按名称或租户ID搜索租户。

3. 要删除多个租户，请选中复选框，然后选择*Actions*>*Delete*。
4. 要删除单个租户、请执行以下操作之一：
    - 选中该复选框，然后选择*Actions*>*Delete*。
    - 选择租户名称以显示详细信息页面、然后选择*操作*>*删除*。
5. 选择 * 是 * 。

管理平台服务

管理租户的平台服务：概述

如果为 S3 租户帐户启用平台服务，则必须配置网格，以便租户可以访问使用这些服务所需的外部资源。

什么是平台服务？

平台服务包括 CloudMirror 复制，事件通知和搜索集成服务。

这些服务允许租户对其 S3 分段使用以下功能：

- * CloudMirror 复制 *： StorageGRID CloudMirror 复制服务用于将特定对象从 StorageGRID 存储分段镜像到指定的外部目标。

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

> CloudMirror复制与跨网格复制功能有一些重要的相似之处和不同之处。要了解更多信息，请参见 "请比较跨网格复制和CloudMirror复制"。

> 如果源存储分段启用了 S3 对象锁定，则不支持 CloudMirror 复制。

- 通知：每个存储分段的事件通知用于将有关对对象执行的特定操作的通知发送到指定的外部Amazon Simple Notification Service™(Amazon SNS)。

  例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

  > 虽然可以在启用了 S3 对象锁定的存储分段上配置事件通知，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留至日期和合法保留状态）。

- * 搜索集成服务 * ：搜索集成服务用于将 S3 对象元数据发送到指定的 Elasticsearch 索引，在此索引中可以使用外部服务搜索或分析元数据。

  例如，您可以将存储分段配置为将 S3 对象元数据发送到远程 Elasticsearch 服务。然后，您可以使用 Elasticsearch 跨存储分段执行搜索，并对对象元数据中存在的模式执行复杂的分析。

  > 虽然可以在启用了 S3 对象锁定的情况下在存储分段上配置 Elasticsearch 集成，但通知消息中不会包含对象的 S3 对象锁定元数据（包括保留截止日期和合法保留状态）。

通过平台服务，租户可以对其数据使用外部存储资源，通知服务以及搜索或分析服务。由于平台服务的目标位置通常位于 StorageGRID 部署外部，因此您必须确定是否要允许租户使用这些服务。如果是，则必须在创建或编辑租户帐户时启用平台服务。您还必须配置网络，使租户生成的平台服务消息能够访问其目标。

使用平台服务的建议

在使用平台服务之前，请注意以下建议：

- 如果 StorageGRID 系统中的 S3 存储分段同时启用了版本控制和 CloudMirror 复制，则还应为目标端点启用 S3 存储分段版本控制。这样， CloudMirror 复制就可以在端点上生成类似的对象版本。
- 如果 S3 请求需要进行 CloudMirror 复制，通知和搜索集成，则使用的活动租户不应超过 100 个。如果活动租户超过 100 个，则可能会导致 S3 客户端性能下降。
- 发送到无法完成的端点的请求最多将排队到500、000个请求。此限制在活动租户之间平均共享。允许新租户暂时超过此500、000限制、以便新创建的租户不会受到不公平的处罚。

相关信息

- "使用租户帐户"
- "配置存储代理设置"
- "监控StorageGRID"

用于平台服务的网络和端口

如果允许 S3 租户使用平台服务，则必须为网格配置网络连接，以确保平台服务消息可以传送到其目标。

在创建或更新 S3 租户帐户时，您可以为该租户帐户启用平台服务。如果启用了平台服务，则租户可以创建端点，用作 CloudMirror 复制，事件通知或从其 S3 存储分段搜索集成消息的目标。这些平台服务消息会从运行此 ADA 服务的存储节点发送到目标端点。

例如，租户可以配置以下类型的目标端点：

- 本地托管的 Elasticsearch 集群
- 支持接收简单通知服务(Simple Notification Service、Amazon SNS)消息的本地应用程序
- 同一个或另一个 StorageGRID 实例上本地托管的 S3 存储分段
- 外部端点，例如 Amazon Web Services 上的端点。

要确保可以传送平台服务消息，您必须配置一个或多个包含此 ADA 存储节点的网络。您必须确保可使用以下端口向目标端点发送平台服务消息。

默认情况下，平台服务消息在以下端口上发送：

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

租户可以在创建或编辑端点时指定其他端口。

> 如果使用 StorageGRID 部署作为 CloudMirror 复制的目标，则可能会在 80 或 443 以外的端口上收到复制消息。确保已在端点中指定目标 StorageGRID 部署用于 S3 的端口。

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

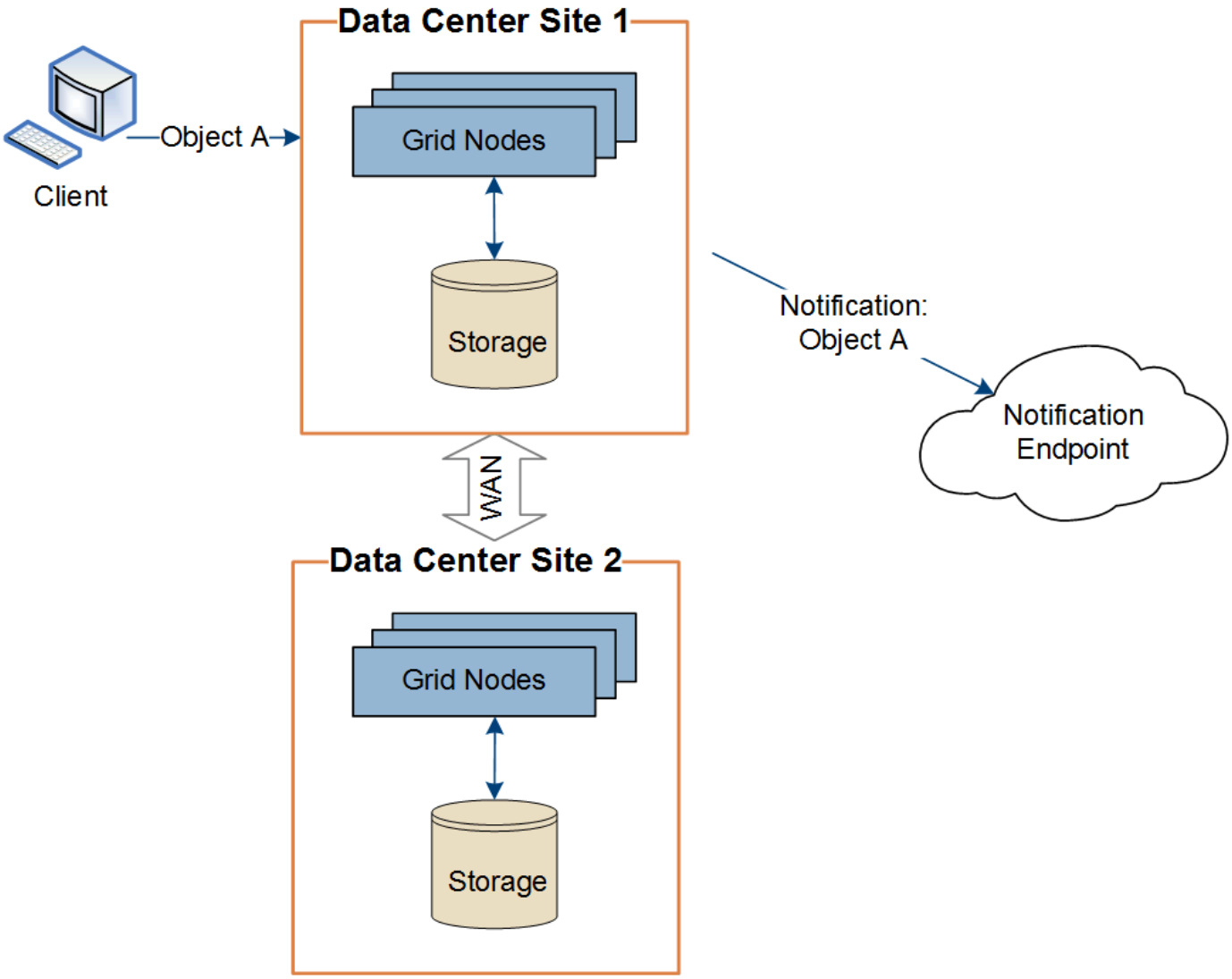
相关信息

- "使用租户帐户"

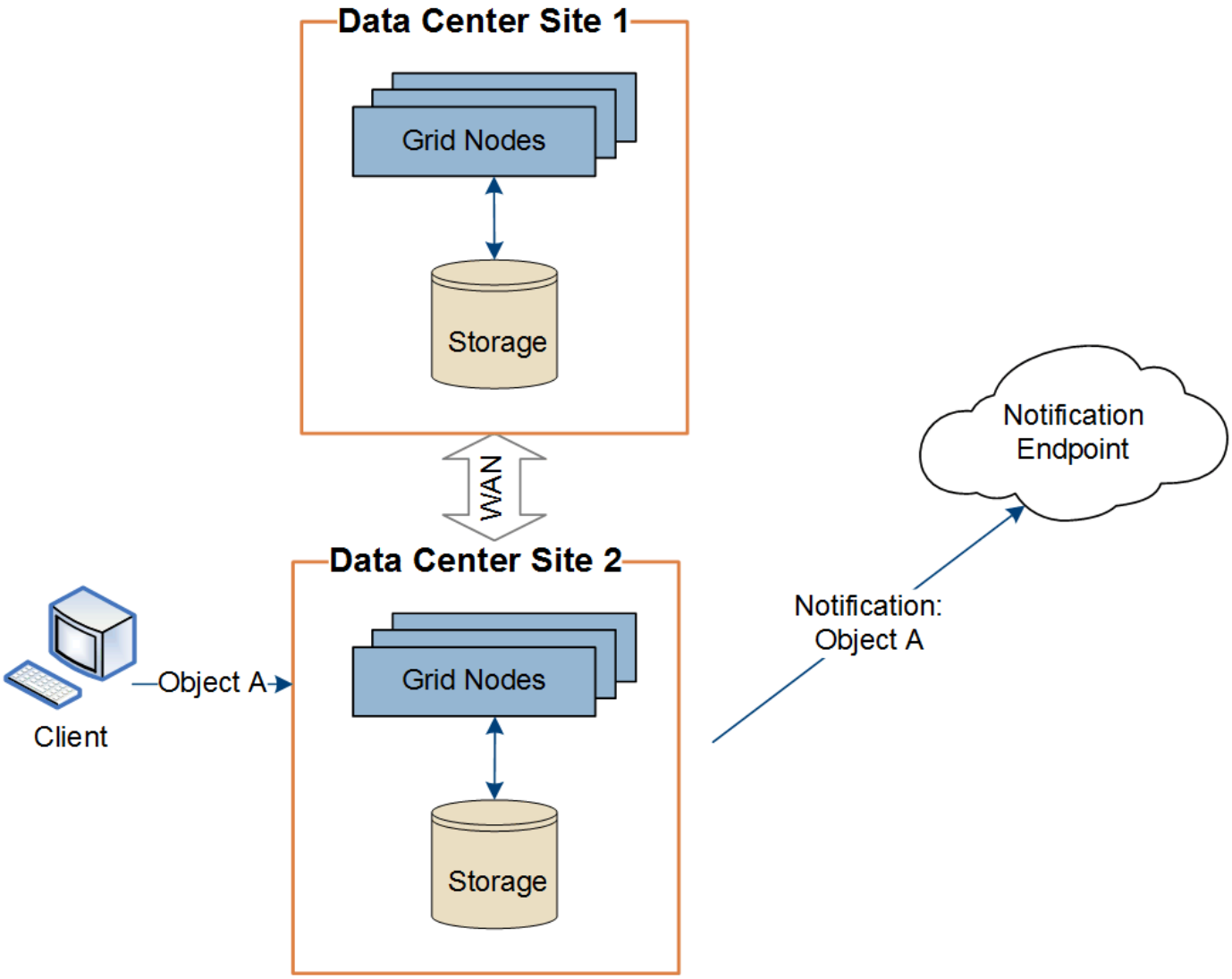
按站点交付平台服务消息

所有平台服务操作均按站点执行。

也就是说，如果租户使用客户端通过连接到数据中心站点 1 的网关节点对对象执行 S3 API 创建操作，则会从数据中心站点 1 触发并发送有关该操作的通知。



如果客户端随后从数据中心站点 2 对同一对象执行 S3 API 删除操作，则会从数据中心站点 2 触发并发送有关删除操作的通知。



请确保在每个站点上配置网络，以便平台服务消息可以传送到其目标。

对平台服务进行故障排除

平台服务中使用的端点由租户管理器中的租户用户创建和维护；但是，如果租户在配置或使用平台服务时遇到问题，您可能可以使用网格管理器帮助解决问题描述 。

新端点出现问题

租户必须先使用租户管理器创建一个或多个端点，才能使用平台服务。每个端点表示一个平台服务的外部目标，例如 StorageGRID S3 存储分段， Amazon Web 服务分段，简单通知服务主题或本地或 AWS 上托管的 Elasticsearch 集群。每个端点都包括外部资源的位置以及访问该资源所需的凭据。

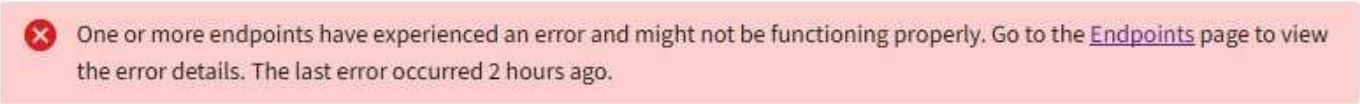
租户创建端点时， StorageGRID 系统会验证此端点是否存在，以及是否可以使用指定的凭据访问此端点。系统会从每个站点的一个节点验证与端点的连接。

如果端点验证失败，则会显示一条错误消息，说明端点验证失败的原因。租户用户应解析问题描述 ，然后重新尝试创建端点。

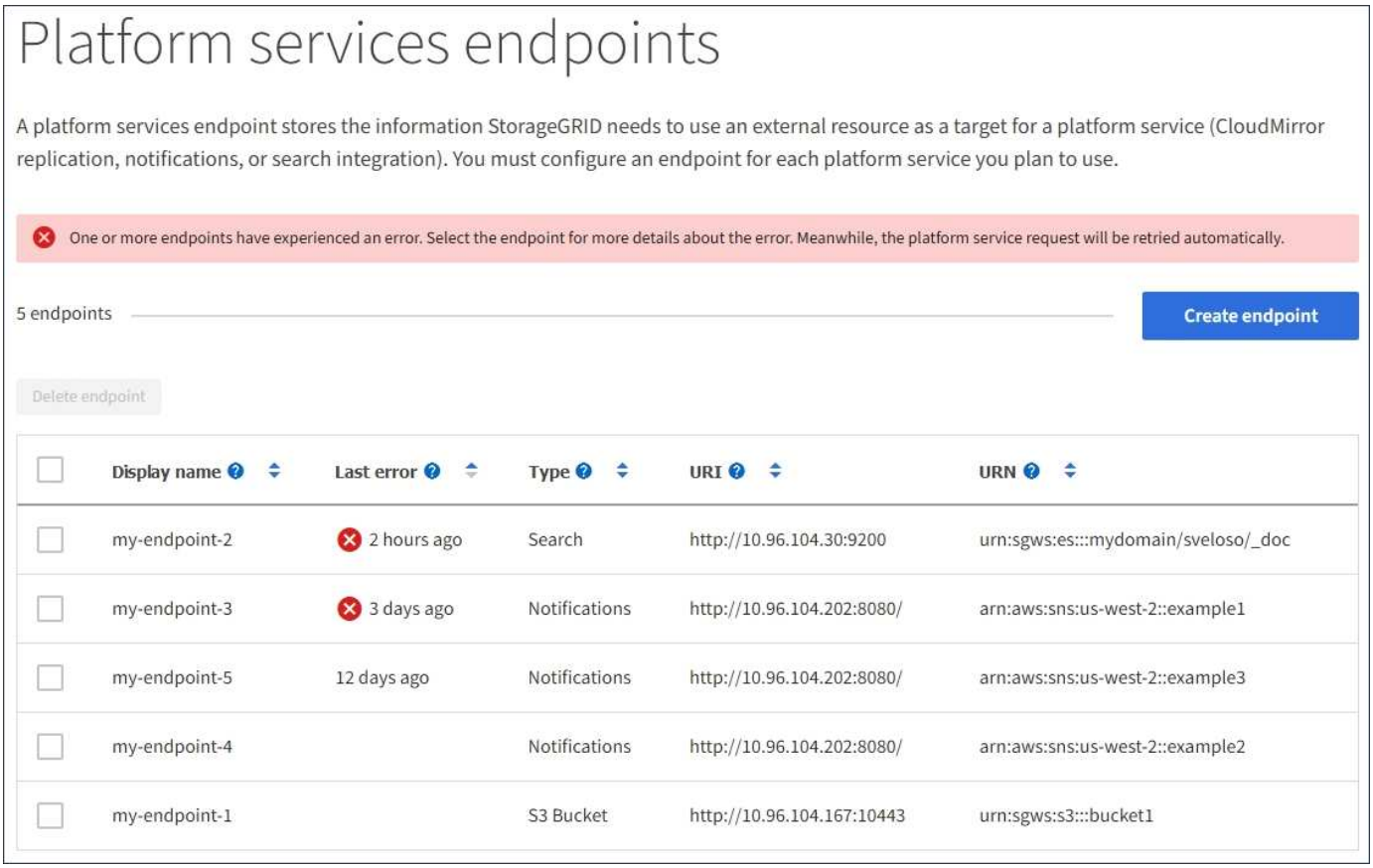
> 如果未为租户帐户启用平台服务、则端点创建将失败。

现有端点存在问题

如果在StorageGRID 尝试访问现有端点时发生错误、租户管理器的信息板上将显示一条消息。



租户用户可以转到 " 端点 " 页面查看每个端点的最新错误消息，并确定错误发生多长时间。"* 最后一个错误 * " 列显示每个端点的最新错误消息，并指示错误发生的时间。包含的错误 图标在过去 7 天内出现。



* 最后一个错误 * 列中的某些错误消息可能会在圆括号中包含日志 ID 。网格管理员或技术支持可以使用此 ID 在 bycast.log 中查找有关此错误的更多详细信息。

与代理服务器相关的问题

如果您已配置 "存储代理" 在存储节点与平台服务端点之间、如果代理服务不允许来自StorageGRID 的消息、则可能会发生错误。要解决这些问题、请检查代理服务器的设置、以确保不会阻止与平台服务相关的消息。

确定是否发生错误

如果在过去7天内发生任何端点错误、租户管理器中的信息板将显示警报消息。您可以转到 " 端点 " 页面以查看有关此错误的更多详细信息。

客户端操作失败

某些平台服务问题可能会导致 S3 存储分段上的发生原因 客户端操作失败。例如，如果内部复制状态计算机（ RSM ）服务停止，或者排队等待传送的平台服务消息太多， S3 客户端操作将失败。

要检查服务状态，请执行以下操作：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* > * SSM* > * 服务 * 。

可恢复和不可恢复的端点错误

创建端点后，平台服务请求错误可能会因各种原因而发生。某些错误可通过用户干预进行恢复。例如，可能会发生可恢复的错误，原因如下：

- 用户凭据已删除或已过期。
- 目标存储分段不存在。
- 无法传送通知。

如果 StorageGRID 遇到可恢复的错误，将重试平台服务请求，直到成功。

其他错误不可恢复。例如，如果删除端点，则会发生不可恢复的错误。

如果 StorageGRID 遇到不可恢复的端点错误，则会在网格管理器中触发总事件（ SMTT） 原有警报。要查看总事件旧警报，请执行以下操作：

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 节点 _* > * SSM* > * 事件 * 。
3. 在表顶部查看上次事件。

   事件消息也会在中列出 `/var/local/log/bycast-err.log`。

4. 按照 SMT 警报内容中提供的指导更正问题描述 。
5. 选择 * 配置 * 选项卡以重置事件计数。
6. 将尚未传送平台服务消息的对象通知租户。
7. 指示租户通过更新对象的元数据或标记来重新触发失败的复制或通知。

   租户可以重新提交现有值，以避免进行不必要的更改。

无法传送平台服务消息

如果目标遇到的问题描述 阻止其接受平台服务消息，则在存储分段上执行的客户端操作将成功，但不会传送平台服务消息。例如，如果更新了目标上的凭据，使 StorageGRID 无法再向目标服务进行身份验证，则可能会发生此错误。

如果平台服务消息因不可恢复的错误而无法传送、则会在网格管理器中触发事件总数(SMTT)原有警报。

降低平台服务请求的性能

如果发送请求的速率超过目标端点接收请求的速率， StorageGRID 软件可能会限制传入的存储分段 S3 请求。只有在等待发送到目标端点的请求积压时，才会发生限制。

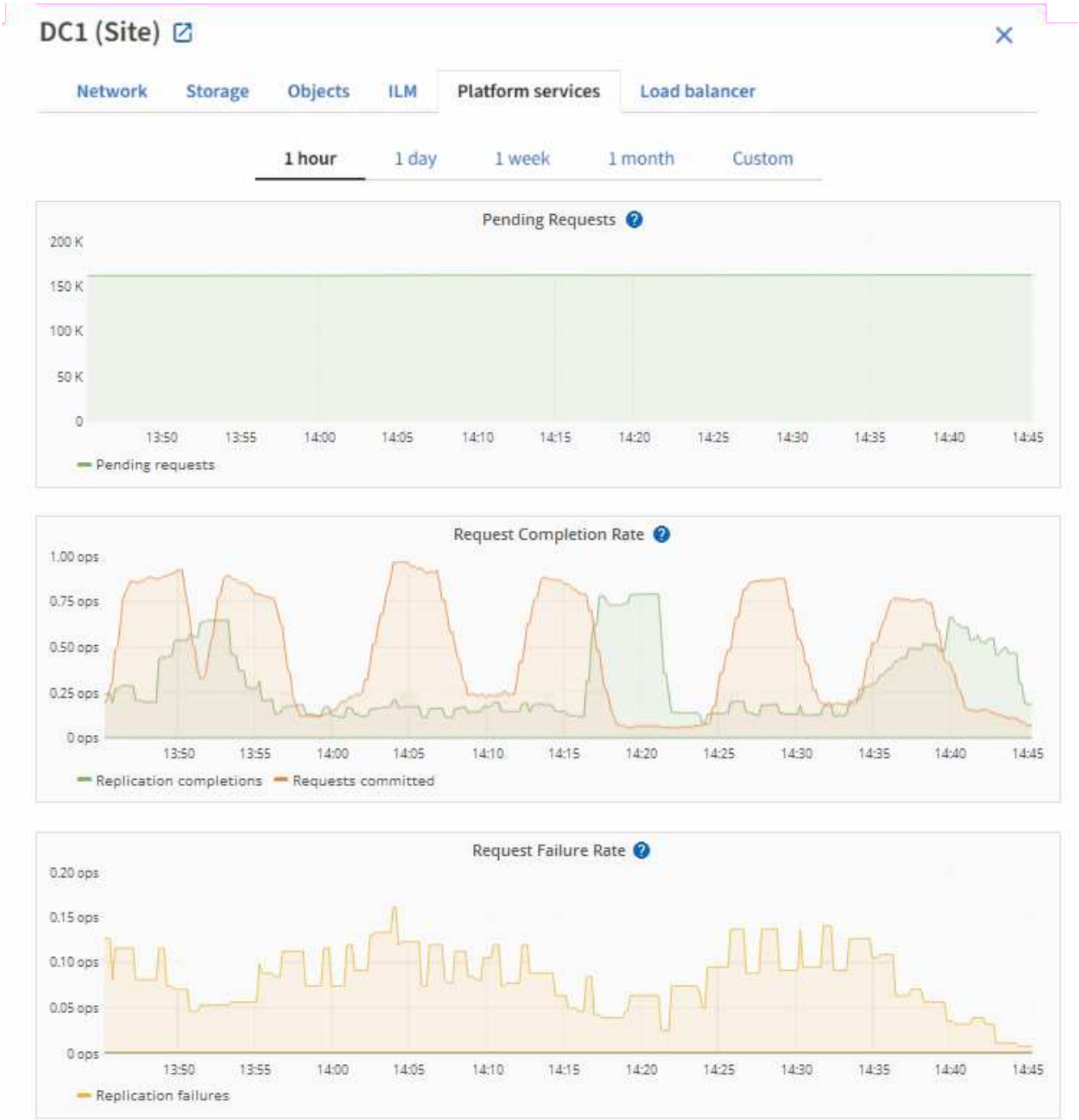
唯一明显的影响是，传入的 S3 请求执行时间较长。如果您开始检测到性能明显较慢，则应降低载入速率或使用容量较高的端点。如果积压的请求持续增加，客户端 S3 操作（例如 PUT 请求）最终将失败。

CloudMirror 请求更有可能受到目标端点性能的影响，因为这些请求所涉及的数据传输通常多于搜索集成或事件通知请求。

平台服务请求失败

要查看平台服务的请求失败率，请执行以下操作：

1. 选择 * 节点 * 。
2. 选择 ***site*** > * 平台服务 * 。
3. 查看请求错误率图表。



平台服务不可用警报

" 平台服务不可用 * " 警报表示无法在站点上执行平台服务操作，因为运行或可用的 RSM 服务存储节点太少。

RSM 服务可确保将平台服务请求发送到其各自的端点。

要解决此警报，请确定站点上的哪些存储节点包含 RSM 服务。（RSM 服务位于也包含此 ADC 服务的存储节点上。） 然后，确保这些存储节点中的大多数都在运行且可用。

> 如果某个站点上有多个包含 RSM 服务的存储节点出现故障，则该站点的任何待定平台服务请求都将丢失。

有关平台服务端点的其他故障排除指南

有关追加信息 、请参见 "使用租户帐户gt；对平台服务端点进行故障排除"。

相关信息

- "排除StorageGRID 系统故障"

管理租户帐户的 **S3 Select**

您可以允许某些 S3 租户对单个对象使用 S3 Select 到问题描述 SelectObjectContent 请求。

S3 Select 可以高效地搜索大量数据，而无需部署数据库和相关资源即可启用搜索。它还可以降低检索数据的成本和延迟。

什么是 **S3 Select** ？

S3 Select 允许 S3 客户端使用 SelectObjectContent 请求仅筛选和检索对象所需的数据。S3 Select 的 StorageGRID 实施包括部分 S3 Select 命令和功能。

使用 **S3 Select** 的注意事项和要求

网格管理要求

网格管理员必须授予租户S3选择功能。选择 * 允许 S3 选择 * 时间 "创建租户" 或 "编辑租户"。

对象格式要求

要查询的对象必须采用以下格式之一：

- **CSX**。可以按原样使用、也可以压缩到GZIP或bzip2归档中。
- 镶木地板。对镶木地板对象的其他要求：
  - S3 Select仅支持使用GZIP或Snappy进行列式压缩。S3 Select不支持对镶木地板对象进行整体对象压缩。
  - S3 Select不支持镶木地板输出。必须将输出格式指定为CSV或JSON。
  - 最大未压缩行组大小为512 MB。
  - 您必须使用对象架构中指定的数据类型。
  - 不能使用间隔、JSON、列表、时间或UUID逻辑类型。

端点要求

SelectObjectContent 请求必须发送到 "StorageGRID 负载平衡器端点"。

端点使用的管理节点和网关节点必须为以下选项之一：

- SG100或SG1000设备节点
- 基于VMware的软件节点

- 运行已启用cgroup v2的内核的裸机节点

General considerations

查询不能直接发送到存储节点。

> SelectObjectContent 请求会降低所有 S3 客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。

请参见 "有关使用 S3 Select 的说明"。

以查看 "Grafana 图表" 对于随时间变化的 S3 Select 操作，请在网格管理器中选择 * 支持 * > * 工具 * > * 指标 * 。

配置客户端连接

配置S3和Swift客户端连接：概述

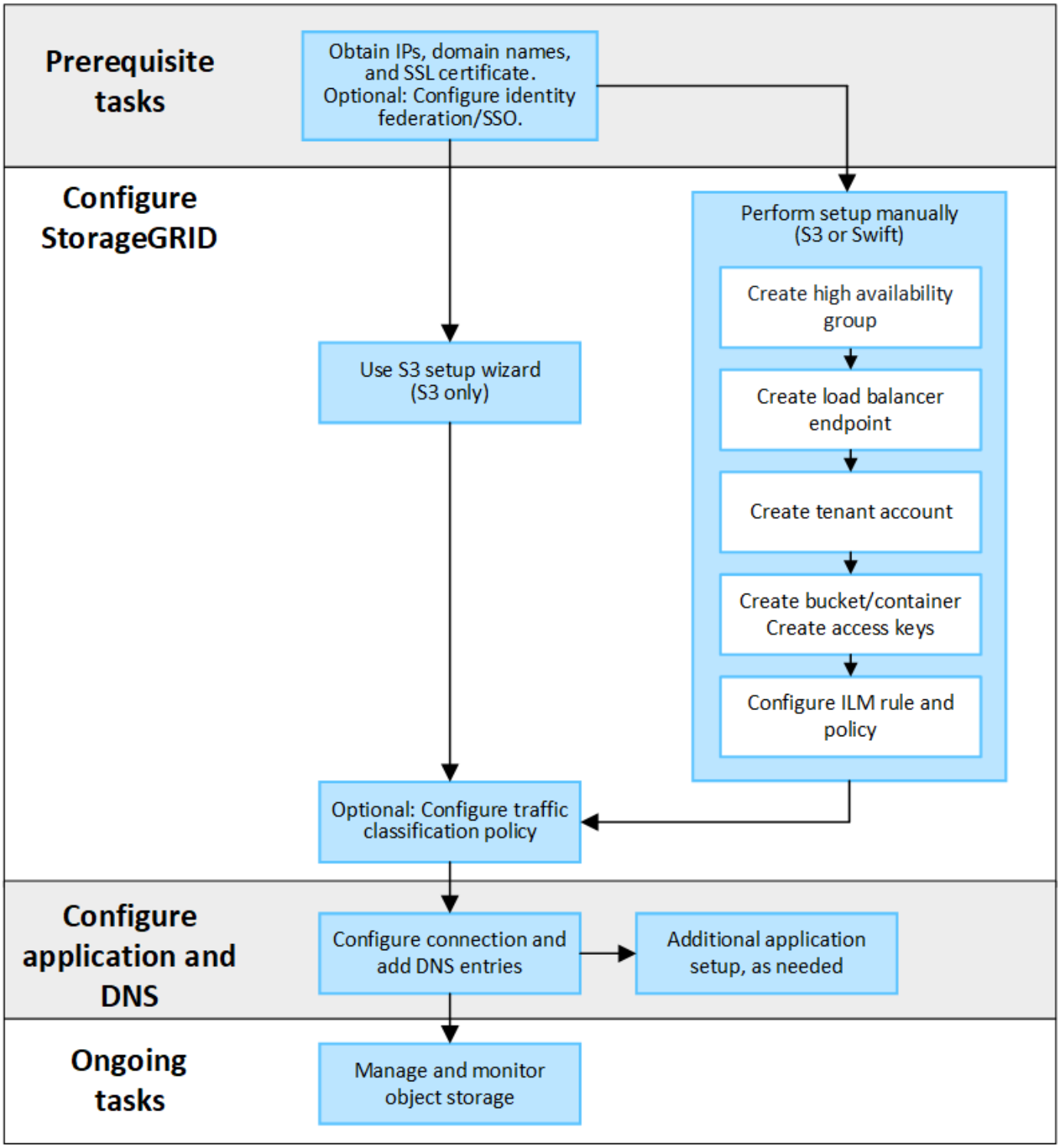
作为网格管理员、您可以管理一些配置选项、这些配置选项用于控制S3和Swift客户端应用程序如何连接到StorageGRID 系统以存储和检索数据。

> 对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

配置工作流

如工作流图所示、将StorageGRID 连接到任何S3或Swift应用程序主要有四个步骤：

1. 根据客户端应用程序连接到StorageGRID 的方式、在StorageGRID 中执行必备任务。
2. 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。
3. 使用S3或Swift应用程序完成与StorageGRID 的连接。创建DNS条目以将IP地址与计划使用的任何域名关联起来。
4. 在应用程序和StorageGRID 中执行持续任务、以管理和监控一段时间内的对象存储。



将**StorageGRID** 连接到客户端应用程序所需的信息

在将StorageGRID 连接到S3或Swift客户端应用程序之前、您必须在StorageGRID 中执行配置步骤并获取特定值。

我需要什么值?

下表显示了您必须在StorageGRID 中配置的值、以及S3或Swift应用程序和DNS服务器使用这些值的位置。

价值	其中、值已配置	使用值的位置
虚拟IP (VIP)地址	StorageGRID > HA组	DNS条目
Port	StorageGRID >负载平衡器端点	客户端应用程序
SSL 证书	StorageGRID >负载平衡器端点	客户端应用程序
服务器名称(FQDN)	StorageGRID >负载平衡器端点	• 客户端应用程序 • DNS条目
S3访问密钥ID和机密访问密钥	StorageGRID >租户和存储分段	客户端应用程序
存储分段/容器名称	StorageGRID >租户和存储分段	客户端应用程序

如何获取这些值?

根据您的要求、您可以执行以下任一操作来获取所需信息：

- *使用 "S3设置向导"*S3设置向导可帮助您在StorageGRID 中快速配置所需的值、并输出一个或两个文件、您可以在配置S3应用程序时使用这些文件。此向导将指导您完成所需的步骤、并帮助您确保设置符合StorageGRID 最佳实践。

  > 如果要配置S3应用程序、建议使用S3设置向导、除非您知道自己有特殊要求、否则实施需要大量自定义。

- *使用 "FabricPool 设置向导"*与S3设置向导类似、FabricPool 设置向导可帮助您快速配置所需值并输出一个文件、您可以在ONTAP 中配置FabricPool 云层时使用该文件。

  > 如果您计划使用StorageGRID 作为FabricPool 云层的对象存储系统、建议使用FabricPool 设置向导、除非您知道自己有特殊要求或实施需要大量自定义。

- 手动配置项目。如果您要连接到Swift应用程序(或者要连接到S3应用程序而不想使用S3设置向导)、则可以通过手动执行配置来获取所需的值。请按照以下步骤操作：

  a. 配置要用于S3或Swift应用程序的高可用性(HA)组。请参见 "配置高可用性组"。

  b. 创建S3或Swift应用程序要使用的负载平衡器端点。请参见 "配置负载平衡器端点"。

  c. 创建S3或Swift应用程序要使用的租户帐户。请参见 "创建租户帐户"。

  d. 对于S3租户、请登录到租户帐户、并为要访问该应用程序的每个用户生成访问密钥ID和机密访问密钥。请参见 "创建您自己的访问密钥"。

  e. 在租户帐户中创建一个或多个S3存储分段或Swift容器。对于S3、请参见 "创建 S3 存储分段"。对于Swift、请使用 "放置容器请求"。

  f. 要为属于新租户或存储分段/容器的对象添加特定放置说明、请创建新的ILM规则并激活新的ILM策略以使用该规则。请参见 "创建 ILM 规则" 和 "创建 ILM 策略"。

使用S3设置向导

使用S3设置向导：注意事项和要求

您可以使用S3设置向导将StorageGRID 配置为S3应用程序的对象存储系统。

何时使用S3设置向导

S3设置向导将指导您完成配置StorageGRID 以用于S3应用程序的每个步骤。完成此向导期间、您可以下载一些文件、用于在S3应用程序中输入值。使用向导可以更快地配置系统、并确保您的设置符合StorageGRID 最佳实践。

如果您具有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、也可以稍后访问并完成该向导。根据您的要求、您还可以手动配置部分或全部所需项、然后使用向导收集S3应用程序所需的值。

在使用向导之前

在使用向导之前、请确认您已满足这些前提条件。

获取IP地址并设置VLAN接口

如果要配置高可用性(HA)组、您就知道S3应用程序要连接到哪些节点以及要使用哪些StorageGRID 网络。您还知道要为子网CIDR、网关IP地址和虚拟IP (VIP)地址输入哪些值。

如果您计划使用虚拟LAN将流量与S3应用程序隔离、则已配置VLAN接口。请参见 "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。此外、您还知道哪个联盟组应该对S3应用程序要使用的租户帐户具有root访问权限。请参见 "使用身份联合" 和 "配置单点登录"。

获取并配置域名

您知道要用于StorageGRID 的完全限定域名(FQDN)。域名服务器(DNS)条目会将此FQDN映射到您使用向导创建的HA组的虚拟IP (VIP)地址。

如果您计划使用S3虚拟托管模式请求、则应具有 "已配置S3端点域名"。建议使用虚拟托管模式请求。

查看负载平衡器和安全证书要求

如果您计划使用StorageGRID 负载平衡器、则已查看负载平衡的一般注意事项。您拥有要上传的证书或生成证书所需的值。

如果您计划使用外部(第三方)负载平衡器端点、则具有该负载平衡器的完全限定域名(FQDN)、端口和证书。

配置任何网格联合连接

如果要允许S3租户使用网格联合连接克隆帐户数据并将存储分段对象复制到另一个网格、请在启动向导之前确认以下内容：

- 您已拥有 "已配置网格联合连接"。

- 连接状态为*已连接*。
- 您具有 root 访问权限。

访问并完成**S3**设置向导

您可以使用S3设置向导配置StorageGRID 以用于S3应用程序。设置向导提供了应用程序访问StorageGRID 存储分段和保存对象所需的值。

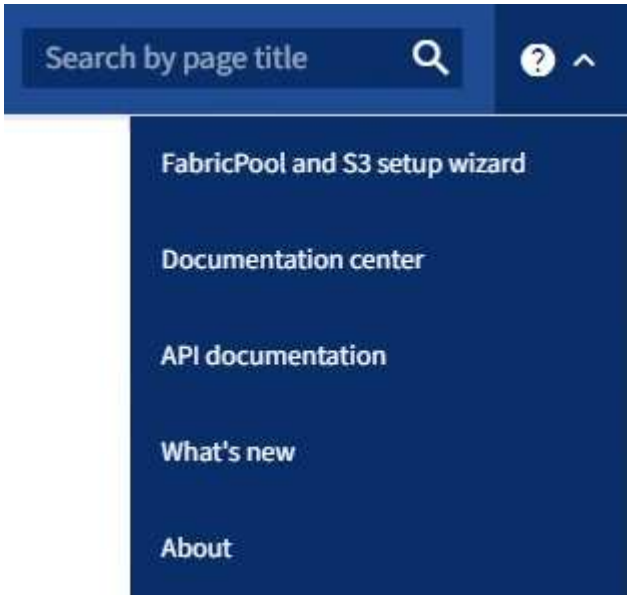
开始之前

- 您拥有 "root访问权限"。
- 您已查看 "注意事项和要求" 用于使用向导。

访问向导

步骤

1. 使用登录到网格管理器 "支持的 Web 浏览器"。
2. 如果信息板上显示了FabricPool and S3 setup wizard*横幅，请选择横幅中的链接。如果横幅不再显示，请从网格管理器的标题栏中选择帮助图标，然后选择FabricPool and S3 setup wizard*。



3. 在FabricPool and S3设置向导页面的S3应用程序部分中，选择*立即配置*。

第**1**步(共**6**步)：配置**HA**组

HA组是一组节点、每个节点都包含StorageGRID 负载平衡器服务。HA组可以包含网关节点、管理节点或同时包含这两者。

您可以使用HA组帮助保持S3数据连接可用。如果HA组中的活动接口发生故障、备份接口可以管理工作负载、而对S3操作的影响微乎其微。

有关此任务的详细信息，请参见 "管理高可用性组"。

步骤

1. 如果您计划使用外部负载平衡器、则无需创建HA组。选择*跳过此步骤*并转到 [第2步(共6步)：配置负载平衡器端点]。
2. 要使用StorageGRID 负载平衡器、您可以创建新的HA组或使用现有HA组。

创建 **HA** 组

a. 要创建新的HA组，请选择*创建HA组*。

b. 对于“输入详细信息”步骤，请填写以下字段。

字段	**Description**
HA组名称	此HA组的唯一显示名称。
问题描述 (可选)	此HA组的问题描述。

c. 对于*Add interfaces*步骤，选择要在此HA组中使用的节点接口。

使用列标题对行进行排序，或者输入搜索词以更快地找到接口。

您可以选择一个或多个节点、但只能为每个节点选择一个接口。

d. 对于“确定接口优先级”步骤，请确定此HA组的主接口和任何备份接口。

拖动行以更改*优先级顺序*列中的值。

列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。

如果HA组包含多个接口、而活动接口发生故障、则虚拟IP (VIP)地址将按优先级顺序移至第一个备份接口。如果该接口发生故障， VIP 地址将移至下一个备份接口，依此类推。解决故障后、VIP地址将移回可用的最高优先级接口。

e. 对于“输入**IP**地址”步骤，请填写以下字段。

字段	**Description**
Subnet CIDR	采用CIDR表示法的VIP子网地址&#8212；后跟斜杠的IPv4地址和子网长度(0-32)。 网络地址不能设置任何主机位。例如： `192.16.0.0/22`。
网关IP地址(可选)	如果用于访问StorageGRID 的S3 IP地址与StorageGRID VIP地址不在同一子网上、请输入StorageGRID VIP本地网关IP地址。本地网关 IP 地址必须位于 VIP 子网中。
虚拟IP地址	为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网内。 必须至少有一个地址为IPv4。您也可以指定其他 IPv4 和 IPv6 地址。

f. 选择*创建HA组*，然后选择*完成*返回S3设置向导。

g. 选择*继续*以转到负载平衡器步骤。

使用现有**HA**组

a. 要使用现有HA组，请从*选择HA组*中选择HA组名称。

b. 选择*继续*以转到负载平衡器步骤。

第**2**步(共**6**步)：配置负载平衡器端点

StorageGRID 使用负载平衡器管理客户端应用程序中的工作负载。负载平衡可最大限度地提高多个存储节点的速度和连接容量。

您可以使用所有网关和管理节点上的StorageGRID 负载平衡器服务、也可以连接到外部(第三方)负载平衡器。建议使用StorageGRID 负载平衡器。

有关此任务的详细信息，请参见 "负载平衡注意事项"。

要使用StorageGRID 负载平衡器服务，请选择StorageGRID 负载平衡器*选项卡，然后创建或选择要使用的负载平衡器端点。要使用外部负载平衡器，请选择*外部负载平衡器*选项卡，并提供有关已配置的系统的详细信息。

创建端点

步骤

1. 要创建负载平衡器端点，请选择*Create endpoint*。
2. 对于*输入端点详细信息*步骤，请填写以下字段。

字段	Description
Name	端点的描述性名称。
Port	要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入任何未使用的外部端口。如果输入80或443、则仅在网关节点上配置端点、因为这些端口是在管理节点上预留的。 *注意：*不允许使用其他网格服务使用的端口。请参见"网络端口参考"。
客户端类型	必须为*S3*。
网络协议	选择 * HTTPS * 。 注意：支持在不使用TLS加密的情况下与StorageGRID 通信，但不建议这样做。

3. 对于*选择绑定模式*步骤，指定绑定模式。绑定模式控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

选项	Description
全局（默认）	客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。 除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。
HA 组的虚拟 IP	客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。 具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。
节点接口	客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。
节点类型	根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。

4. 对于租户访问步骤、选择以下选项之一：

字段	Description
允许所有租户(默认)	所有租户帐户都可以使用此端点来访问其分段。
允许选定租户	只有选定租户帐户才能使用此端点访问其分段。
阻止选定租户	选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。

5. 对于*attach certificer*步骤，选择以下选项之一：

字段	Description
上传证书(建议)	使用此选项可上传CA签名的服务器证书、证书专用密钥和可选的CA包。
生成证书	使用此选项可生成自签名证书。请参见 "配置负载平衡器端点" 有关输入内容的详细信息。
使用StorageGRID S3和Swift证书	仅当您已上传或生成自定义版本的StorageGRID 全局证书时、才使用此选项。请参见 "配置 S3 和 Swift API 证书" 了解详细信息。

6. 选择*完成*以返回S3设置向导。
7. 选择*继续*转到租户和存储分段步骤。

> 对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

使用现有负载平衡器端点

步骤

1. 要使用现有端点，请从*选择负载平衡器端点*中选择其名称。
2. 选择*继续*转到租户和存储分段步骤。

使用外部负载平衡器

步骤

1. 要使用外部负载平衡器、请填写以下字段。

字段	Description
FQDN	外部负载平衡器的完全限定域名(FQDN)。
Port	S3应用程序将用于连接到外部负载平衡器的端口号。
证书	复制外部负载平衡器的服务器证书并将其粘贴到此字段中。

2. 选择*继续*转到租户和存储分段步骤。

第3步(共6步)：创建租户和存储分段

租户是一种可以使用S3应用程序在StorageGRID 中存储和检索对象的实体。每个租户都有自己的用户、访问密钥、分段、对象和一组特定功能。您必须先创建租户、然后才能创建S3应用程序用于存储其对象的存储分段。

分段是一种用于存储租户对象和对象元数据的容器。虽然某些租户可能具有许多存储分段、但此向导可帮助您以最快、最简单的方式创建租户和存储分段。您可以稍后使用租户管理器添加所需的任何其他分段。

您可以为此S3应用程序创建一个新租户。您也可以选择为新租户创建存储分段。最后、您可以允许向导为租户的root用户创建S3访问密钥。

有关此任务的详细信息，请参见 "创建租户帐户" 和"创建 S3 存储分段"。

步骤

1. 选择 * 创建租户 * 。
2. 对于输入详细信息步骤、请输入以下信息。

字段	Description
Name	租户帐户的名称。租户名称不需要唯一。创建租户帐户时，它会收到一个唯一的数字帐户 ID 。
问题描述 (可选)	用于帮助识别租户的问题描述。
客户端类型	此租户将使用的客户端协议类型。对于S3设置向导，已选择*S3*，并且该字段已禁用。
存储配额(可选)	如果希望此租户具有存储配额、则为配额和单位指定一个数值。

3. 选择 * 继续 * 。
4. (可选)选择希望此租户拥有的任何权限。

其中某些权限还有其他要求。有关详细信息、请选择每个权限的帮助图标。

权限	如果选择...
允许平台服务	租户可以使用CloudMirror等S3平台服务。请参见 "管理 S3 租户帐户的平台服务"。
使用自己的身份源	租户可以为联盟组和用户配置和管理自己的身份源。如果您有、此选项将被禁用 "已配置SSO" 适用于您的StorageGRID 系统。

权限	如果选择...
允许S3选择	租户可以通过问题描述 S3选择对象内容API请求筛选和检索对象数据。请参见 "管理租户帐户的 S3 Select"。 重要：选择对象内容请求会降低所有S3客户端和所有租户的负载平衡器性能。仅在需要时才启用此功能，并且仅适用于受信任租户。
使用网格联合连接	租户可以使用网格联合连接。 选择此选项： • 使此租户以及添加到帐户的所有租户组和用户从此网格(_ssource grid _)克隆到选定连接中的另一网格(_dDestination grid _)。 • 允许此租户在每个网格上的相应分段之间配置跨网格复制。 请参见 "管理网格联盟允许的租户"。 注意：创建新S3租户时、您只能选择*使用网格联合连接*；不能为现有租户选择此权限。

5. 如果选择了*使用网格联合连接*，请选择一个可用的网格联合连接。
6. 根据StorageGRID 系统是否使用、定义租户帐户的root访问权限 "身份联合"， "单点登录(SSO)"或两者。

选项	执行此操作 ...
如果未启用身份联合	指定以本地root用户身份登录租户时要使用的密码。
如果启用了身份联合	a. 选择一个现有联盟组、以便对租户具有root访问权限。 b. (可选)指定以本地root用户身份登录到租户时要使用的密码。
如果同时启用了身份联合和单点登录(SSO)	选择一个现有联盟组、以便对租户具有root访问权限。没有本地用户可以登录。

7. 如果希望向导为root用户创建访问密钥ID和机密访问密钥，请选择*自动创建root用户S3访问密钥*。

> 如果租户的唯一用户是root用户、请选择此选项。如果其他用户要使用此租户、请使用租户管理器配置密钥和权限。

8. 选择 * 继续 * 。
9. 对于创建分段步骤、可以选择为租户的对象创建分段。否则、请选择*创建不含存储分段的租户*以转到 下载数据步骤。

> 如果为网格启用了S3对象锁定、则在此步骤中创建的分段不会启用S3对象锁定。如果需要对此S3应用程序使用S3对象锁定分段，请选择*创建不包含分段的租户*。然后、使用租户管理器 "创建存储分段" 而是。

a. 输入S3应用程序要使用的存储分段的名称。例如： `S3-bucket`。

> 创建存储分段后、无法更改存储分段名称。

b. 为此存储分段选择*区域*。

   使用默认区域(us-east-1)、除非您希望将来使用ILM根据存储分段的区域筛选对象。

c. 如果要将每个对象的每个版本存储在此存储分段中，请选择*启用对象版本控制*。

d. 选择*创建租户和存储分段*并转到下载数据步骤。

第4步(共6步)：下载数据

在下载数据步骤中、您可以下载一个或两个文件以保存刚刚配置的内容的详细信息。

步骤

1. 如果选择了*自动创建root用户S3访问密钥*，请执行以下一项或两项操作：
   - 选择*下载访问密钥*以下载 `.csv` 包含租户帐户名称、访问密钥ID和机密访问密钥的文件。
   - 选择复制图标()将访问密钥ID和机密访问密钥复制到剪贴板。
2. 选择*下载配置值*以下载 `.txt` 包含负载平衡器端点、租户、存储分段和root用户设置的文件。
3. 将此信息保存到安全位置。

> 在复制两个访问密钥之前、请勿关闭此页面。关闭此页面后、密钥将不可用。请确保将此信息保存在安全位置、因为此信息可用于从StorageGRID 系统获取数据。

4. 如果出现提示、请选中此复选框以确认您已下载或复制密钥。
5. 选择*继续*以转到ILM规则和策略步骤。

第5步(共6步)：查看S3的ILM规则和ILM策略

信息生命周期管理(ILM)规则控制StorageGRID 系统中所有对象的放置、持续时间和加载行为。StorageGRID 附带的ILM策略会为所有对象创建两个复制副本。此策略将一直有效、直到您创建新的建议策略并将其激活为止。

步骤

1. 查看页面上提供的信息。
2. 如果要为属于新租户或存储分段的对象添加特定说明、请创建新规则和新策略。请参见 "创建 ILM 规则" 和 "创建 ILM 策略：概述"。
3. 选择*我已查看这些步骤并了解我需要执行的操作*。
4. 选中此复选框以指示您了解下一步要做什么。
5. 选择*继续*以转到*摘要*。

第6步(共6步)：查看摘要

步骤

1. 查看摘要。

2. 记下后续步骤中的详细信息、这些详细信息介绍了在连接到S3客户端之前可能需要的其他配置。例如，选择*以root身份登录*将转到租户管理器，您可以在其中添加租户用户、创建其他存储分段以及更新存储分段设置。
3. 选择 * 完成 * 。
4. 使用从StorageGRID 下载的文件或手动获取的值配置应用程序。

管理HA组

管理高可用性（ HA ）组：概述

您可以将多个管理节点和网关节点的网络接口分组到一个高可用性（ HA ）组中。如果 HA 组中的活动接口发生故障，则备份接口可以管理工作负载。

什么是 HA 组?

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

每个 HA 组均可访问选定节点上的共享服务。

- 包括网关节点，管理节点或两者在内的 HA 组可为 S3 和 Swift 客户端提供高可用性数据连接。
- 仅包含管理节点的 HA 组可提供与网格管理器和租户管理器的高可用性连接。
- 如果 HA 组仅包含 SG100 或 SG1000 设备以及基于 VMware 的软件节点，则可以为提供高可用性连接 "使用 S3 Select 的 S3 租户"。建议在使用 S3 Select 时使用 HA 组，但不要求使用 HA 组。

如何创建 HA 组?

1. 您可以为一个或多个管理节点或网关节点选择一个网络接口。您可以使用网格网络（ eth0 ）接口，客户端网络（ eth2 ）接口， VLAN 接口或已添加到节点的访问接口。

   > 如果某个接口具有DHCP分配的IP地址、则无法将其添加到HA组。

2. 您可以指定一个接口作为主接口。主接口是活动接口，除非发生故障。
3. 您可以确定任何备份接口的优先级顺序。
4. 您可以为组分配 1 到 10 个虚拟 IP （ VIP ）地址。客户端应用程序可以使用其中任何 VIP 地址连接到 StorageGRID 。

有关说明，请参见 "配置高可用性组"。

什么是活动接口?

在正常操作期间， HA 组的所有 VIP 地址都会添加到主接口，这是优先级顺序中的第一个接口。只要主接口保持可用，客户端就会连接到组的任何 VIP 地址。也就是说，在正常操作期间，主接口是组的 "`active` " 接口。

同样，在正常操作期间， HA 组的任何低优先级接口都充当 "`backup` " 接口。除非主(当前处于活动状态)接口不可用、否则不会使用这些备份接口。

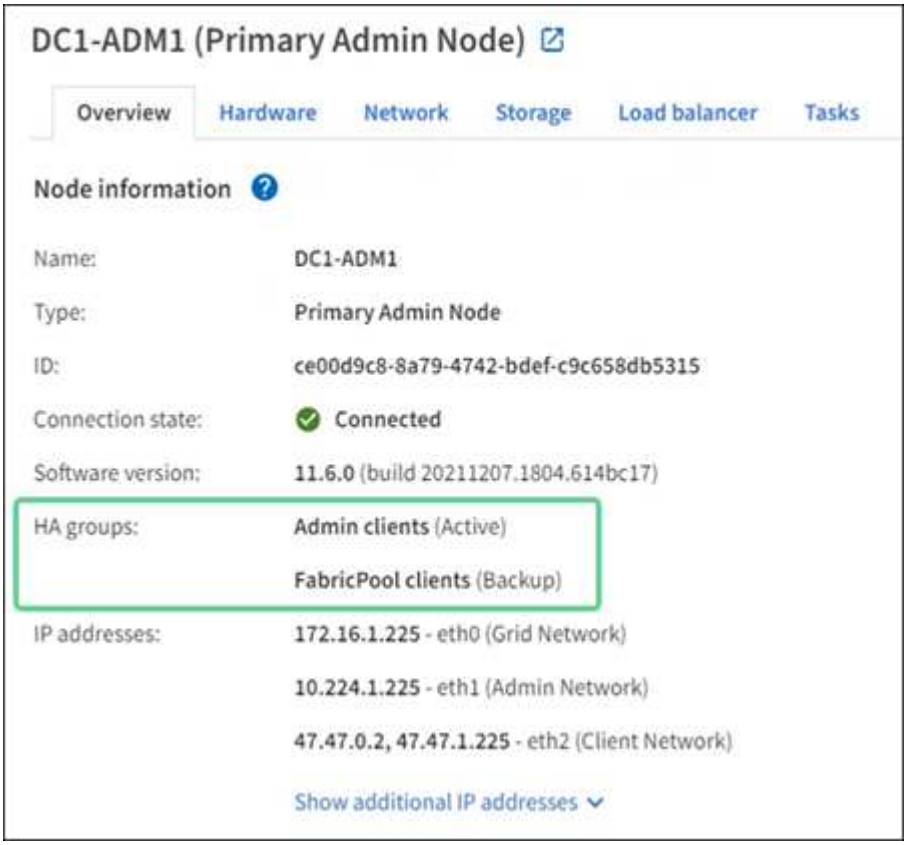
查看节点的当前 **HA** 组状态

要查看节点是否已分配给 HA 组并确定其当前状态，请选择 * 节点 * > * 节点 _节点 _* 。

如果 * 概述 * 选项卡包含 * HA 组 * 的条目，则节点将分配给列出的 HA 组。组名称后面的值是 HA 组中节点的当前状态：

- * 活动 *： HA 组当前正在此节点上托管。
- * 备份 *： HA 组当前未使用此节点；这是一个备份接口。
- 已停止：无法在此节点上托管HA组、因为已手动停止高可用性(keepalived)服务。
- 故障：由于以下一项或多项原因、无法在此节点上托管HA组：
  - 此节点上未运行负载平衡器（ nginx -gw ）服务。
  - 节点的 eth0 或 VIP 接口已关闭。
  - 节点已关闭。

在此示例中，主管理节点已添加到两个 HA 组中。此节点当前是管理客户端组的活动接口，也是 FabricPool 客户端组的备份接口。



活动接口发生故障时会发生什么情况?

当前托管 VIP 地址的接口是活动接口。如果 HA 组包含多个接口且活动接口发生故障，则 VIP 地址将按优先级顺序移至第一个可用的备份接口。如果该接口发生故障， VIP 地址将移至下一个可用备份接口，依此类推。

触发故障转移的原因如下：

- 配置接口的节点将关闭。
- 配置了该接口的节点与所有其他节点的连接至少断开 2 分钟。
- 活动接口关闭。
- 负载平衡器服务将停止。
- 高可用性服务将停止。

> 托管活动接口的节点外部的网络故障可能不会触发故障转移。同样、网格管理器或租户管理器的服务也不会触发故障转移。

故障转移过程通常只需几秒钟，并且速度足以使客户端应用程序不会受到任何影响，并且可以依靠正常的重试行为来继续运行。

解决故障后，如果更高优先级的接口再次可用，则 VIP 地址会自动移至可用的最高优先级接口。

如何使用 **HA** 组?

您可以使用高可用性（ High Availability ， HA ）组提供与 StorageGRID 的高可用性连接，以用于对象数据和管理目的。

- HA 组可以为网格管理器或租户管理器提供高度可用的管理连接。
- HA 组可以为 S3 和 Swift 客户端提供高可用性数据连接。
- 如果 HA 组仅包含一个接口，则可以提供多个 VIP 地址并明确设置 IPv6 地址。

只有当 HA 组中包含的所有节点都提供相同的服务时， HA 组才能提供高可用性。创建 HA 组时，请从提供所需服务的节点类型中添加接口。

- * 管理节点 * ：包括负载平衡器服务，并允许访问网格管理器或租户管理器。
- 网关节点：包括负载平衡器服务。

HA 组的用途	将此类型的节点添加到 **HA** 组
访问 Grid Manager	• 主管理节点（ * 主 * ） • 非主管理节点 • 注： * 主管理节点必须为主接口。某些维护过程只能从主管理节点执行。
仅访问租户管理器	• 主管理节点或非主管理节点
S3 或 Swift 客户端访问—负载平衡器服务	• 管理节点 • 网关节点

HA 组的用途	将此类型的节点添加到 HA 组
的 S3 客户端访问 "S3 Select"	• SG100 或 SG1000 设备 • 基于 VMware 的软件节点 • 注 * ： 使用 S3 Select 时建议使用 HA 组，但不要求使用 HA 组。

将 **HA** 组与 **Grid Manager** 或租户管理器结合使用的限制

如果 Grid Manager 或租户管理器服务失败，则不会触发 HA 组故障转移。

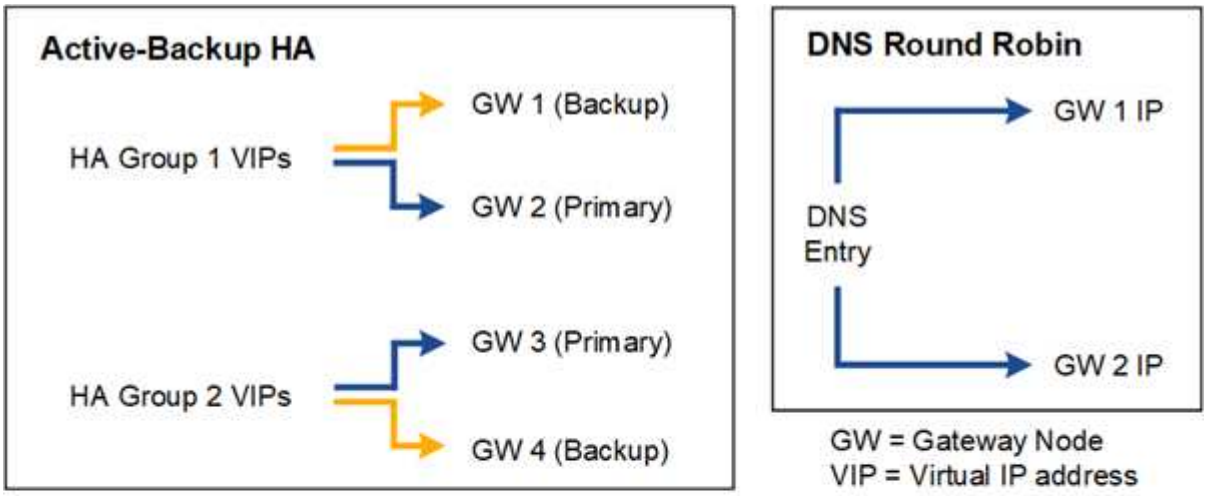
如果在发生故障转移时登录到网格管理器或租户管理器，则您将注销并必须重新登录才能恢复任务。

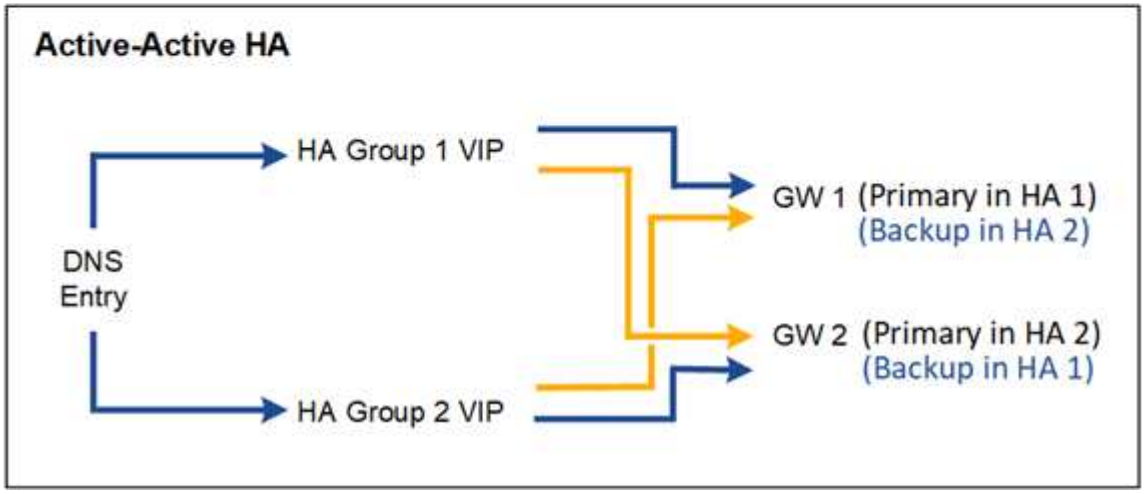
当主管理节点不可用时、无法执行某些维护过程。在故障转移期间，您可以使用网格管理器监控 StorageGRID 系统。

HA 组的配置选项

下图举例说明了配置 HA 组的不同方式。每个选项都有优缺点。

在图中，蓝色表示 HA 组中的主接口，黄色表示 HA 组中的备份接口。





下表总结了图中所示每个 HA 配置的优势。

Configuration	优势	缺点
主动备份 HA	• 由 StorageGRID 管理，无外部依赖关系。 • 快速故障转移。	• 一个 HA 组中只有一个节点处于活动状态。每个 HA 组至少有一个节点处于空闲状态。
DNS 轮循	• 提高聚合吞吐量。 • 无闲置主机。	• 故障转移速度较慢，这可能取决于客户端行为。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。
主动 - 主动 HA	• 流量分布在多个 HA 组中。 • 可随 HA 组数量扩展的高聚合吞吐量。 • 快速故障转移。	• 配置更复杂。 • 需要在 StorageGRID 之外配置硬件。 • 需要客户实施的运行状况检查。

配置高可用性组

您可以配置高可用性（ High Availability ， HA ）组，以提供对管理节点或网关节点上服务的高可用性访问。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。
- 如果您计划在 HA 组中使用 VLAN 接口，则已创建 VLAN 接口。请参见 "配置 VLAN 接口"。
- 如果您计划对 HA 组中的节点使用访问接口，则已创建此接口：
  - * Red Hat Enterprise Linux 或 CentOS （安装节点之前） *： "创建节点配置文件"
  - * Ubuntu 或 Debian （安装节点之前） *： "创建节点配置文件"
  - * Linux （安装节点后） *： "Linux： 向节点添加中继或访问接口"
  - * VMware （安装节点后） *： "VMware： 向节点添加中继或访问接口"

创建高可用性组

创建高可用性组时，您可以选择一个或多个接口并按优先级顺序对其进行组织。然后，您将一个或多个 VIP 地址分配给该组。

接口必须是要将网关节点或管理节点包含在 HA 组中的接口。一个 HA 组只能对任何给定节点使用一个接口；但是，同一节点的其他接口也可以在其他 HA 组中使用。

访问向导

步骤

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。
2. 选择 * 创建 * 。

输入 **HA** 组的详细信息

步骤

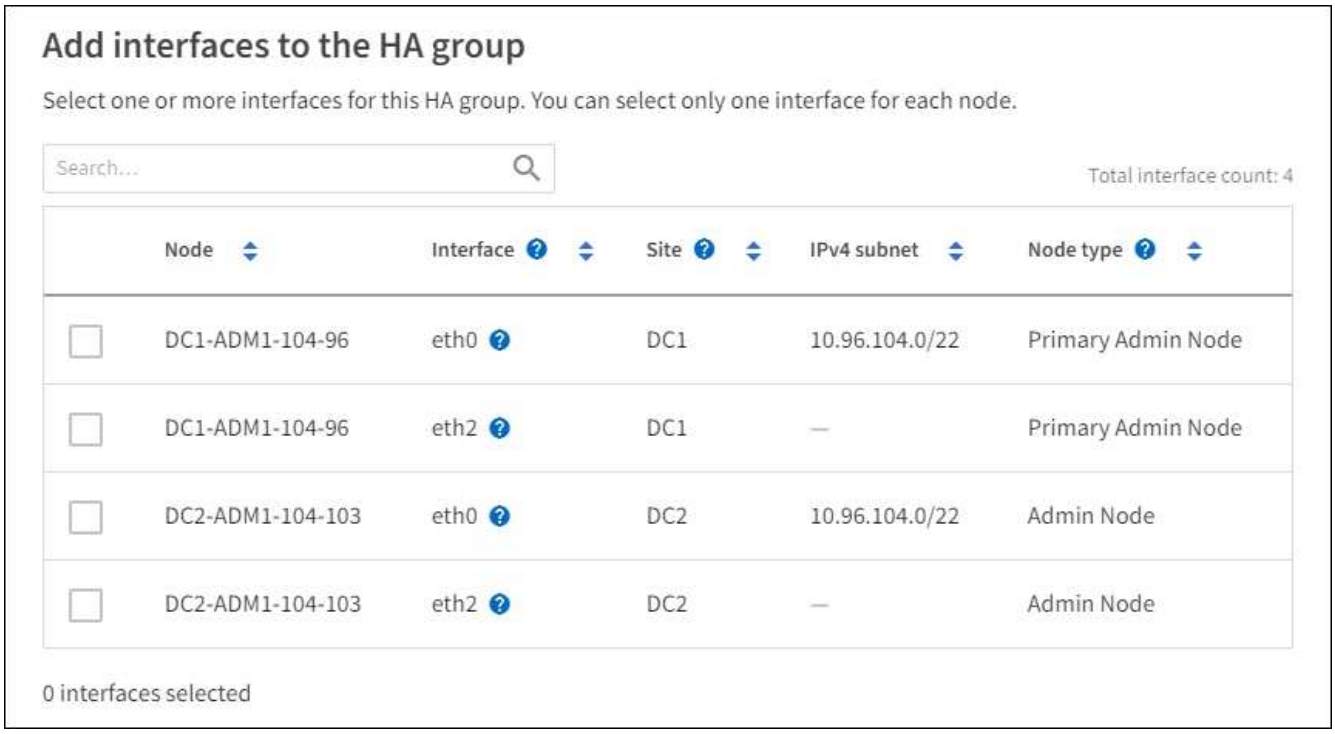
1. 为 HA 组提供一个唯一名称。
2. 或者，输入 HA 组的问题描述 。
3. 选择 * 继续 * 。

向 **HA** 组添加接口

步骤

1. 选择一个或多个接口以添加到此 HA 组。

   使用列标题对行进行排序，或者输入搜索词以更快地找到接口。



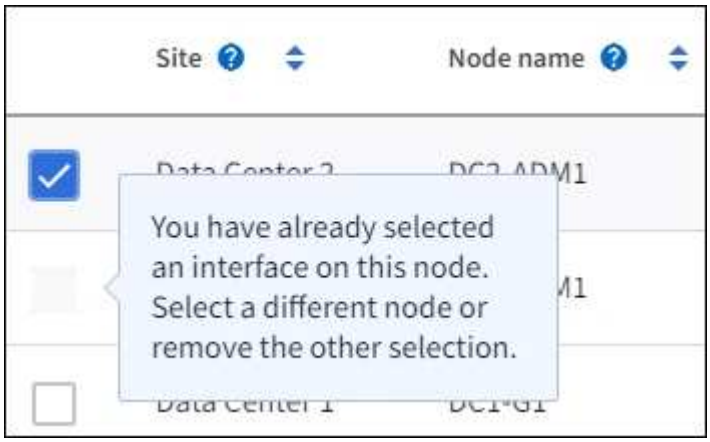
   创建 VLAN 接口后，请等待最多 5 分钟，使新接口显示在表中。

   选择接口的准则

   - 必须至少选择一个接口。
   - 您只能为一个节点选择一个接口。
   - 如果 HA 组用于管理节点服务（包括网格管理器和租户管理器）的 HA 保护，请仅选择管理节点上的接口。
   - 如果 HA 组用于对 S3 或 Swift 客户端流量进行 HA 保护，请选择管理节点，网关节点或两者上的接口。
   - 如果选择不同类型节点上的接口，则会显示一条信息性注释。系统会提醒您，如果发生故障转移，则新

活动节点上可能无法使用先前活动节点提供的服务。例如、备份网关节点无法为管理节点服务提供HA保护。同样、备份管理节点无法执行主管理节点可以提供的所有维护过程。

- 如果无法选择接口、则会禁用其复选框。工具提示提供了更多信息。



- 如果某个接口的子网值或网关与另一个选定接口冲突、则无法选择该接口。
- 如果已配置接口没有静态IP地址、则无法选择该接口。

2. 选择 * 继续 * 。

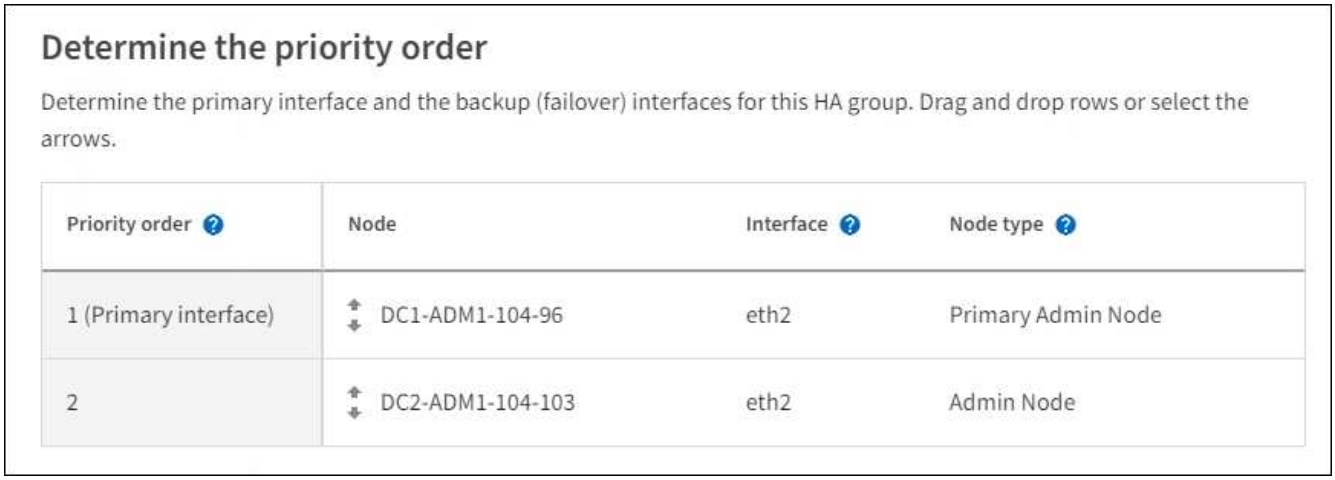
确定优先级顺序

如果HA组包含多个接口、则可以确定哪个是主接口、哪些是备份(故障转移)接口。如果主接口发生故障、VIP地址将移至可用的最高优先级接口。如果该接口发生故障， VIP 地址将移至可用的下一个最高优先级接口，依此类推。

步骤

1. 拖动*优先级顺序*列中的行以确定主接口和任何备份接口。

   列表中的第一个接口是主接口。主接口是活动接口，除非发生故障。



   如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行。

2. 选择 * 继续 * 。

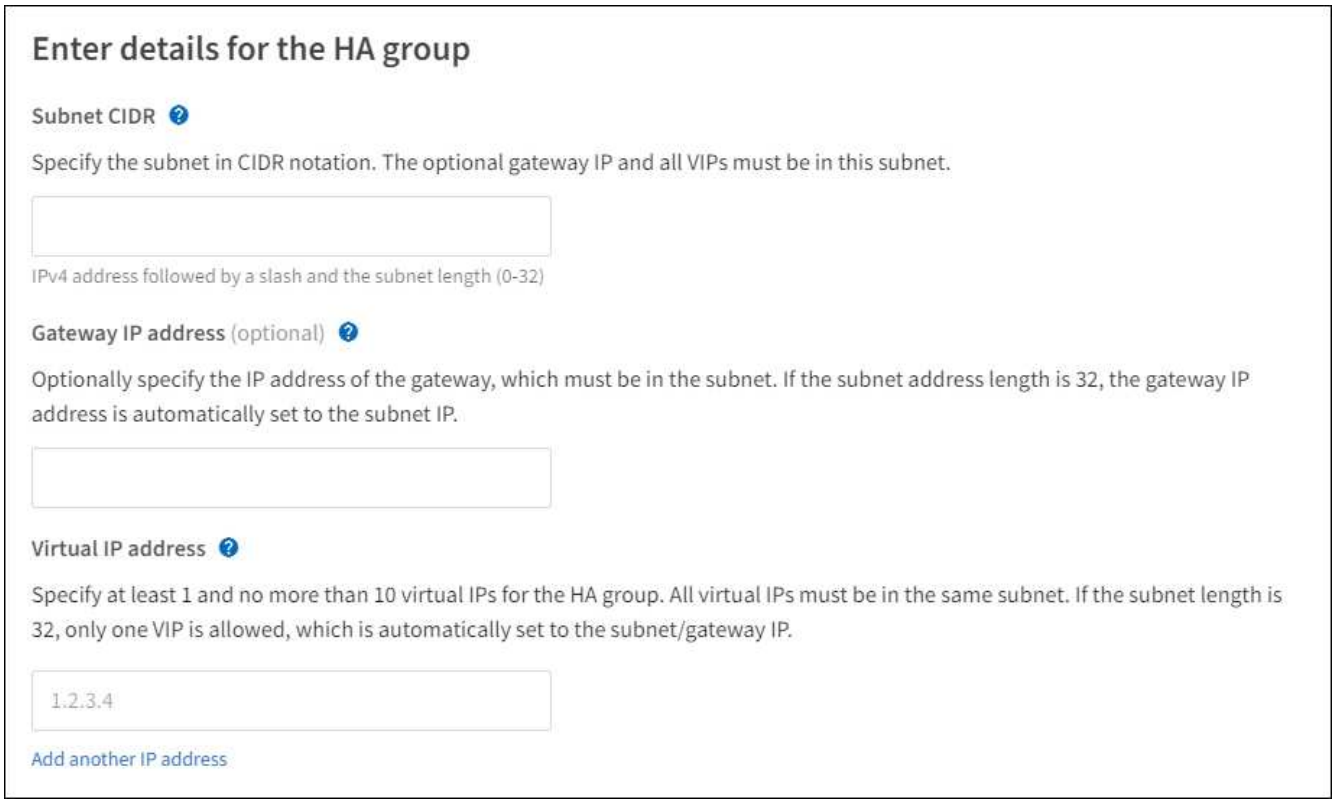
输入 **IP** 地址

步骤

1. 在 * 子网 CIDR * 字段中，以 CIDR 表示法指定 VIP 子网— IPv4 地址后跟斜杠和子网长度（ 0-32 ）。

   网络地址不能设置任何主机位。例如： `192.16.0.0/22`。

   > 如果使用 32 位前缀，则 VIP 网络地址也会用作网关地址和 VIP 地址。

2. 或者，如果任何 S3 ， Swift ，管理或租户客户端要从其他子网访问这些 VIP 地址，请输入 * 网关 IP 地址 * 。网关地址必须在 VIP 子网中。

   客户端和管理员用户将使用此网关访问虚拟 IP 地址。

3. 为HA组中的活动接口至少输入一个VIP地址、最多输入十个VIP地址。所有VIP地址都必须位于VIP子网中、并且所有VIP地址都将在活动接口上同时处于活动状态。

   您必须至少提供一个 IPv4 地址。您也可以指定其他 IPv4 和 IPv6 地址。

4. 选择 * 创建 HA 组 * 并选择 * 完成 * 。

   此时将创建 HA 组，您现在可以使用已配置的虚拟 IP 地址。

   > 等待长达 15 分钟，以便对 HA 组所做的更改应用于所有节点。

后续步骤

如果要使用此 HA 组进行负载平衡，请创建一个负载平衡器端点以确定端口和网络协议并附加任何所需的证书。请参见 "配置负载平衡器端点"。

编辑高可用性组

您可以编辑高可用性（ High Availability ， HA ）组以更改其名称和问题描述 ，添加或删除接口，更改优先级顺序或添加或更新虚拟 IP 地址。

例如，如果要删除与站点或节点停用操作步骤 中选定接口关联的节点，则可能需要编辑 HA 组。

步骤

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。

   " 高可用性组 " 页面显示所有现有的 HA 组。

2. 选中要编辑的HA组对应的复选框。
3. 根据要更新的内容执行以下操作之一：
   - 选择 * 操作 * > * 编辑虚拟 IP 地址 * 以添加或删除 VIP 地址。
   - 选择 * 操作 * > * 编辑 HA 组 * 可更新组的名称或问题描述 ，添加或删除接口，更改优先级顺序或添加或删除 VIP 地址。
4. 如果选择了 * 编辑虚拟 IP 地址 * ：
   a. 更新 HA 组的虚拟 IP 地址。
   b. 选择 * 保存 * 。
   c. 选择 * 完成 * 。
5. 如果选择了 * 编辑 HA 组 * ：
   a. （可选）更新组的名称或问题描述 。
   b. (可选)选中或清除相应复选框以添加或删除接口。

      > 如果 HA 组提供对网格管理器的访问权限，则必须选择主管理节点上的一个接口作为主接口。某些维护过程只能从主管理节点执行

   c. (可选)拖动行以更改此HA组的主接口和任何备份接口的优先级顺序。
   d. 也可以更新虚拟 IP 地址。
   e. 选择 * 保存 * ，然后选择 * 完成 * 。

> 等待长达 15 分钟，以便对 HA 组所做的更改应用于所有节点。

删除高可用性组

您可以一次删除一个或多个高可用性（ HA ）组。

> 如果HA组绑定到负载平衡器端点、则无法删除该HA组。要删除HA组、必须将其从使用该组的任何负载平衡器端点中删除。

为防止客户端中断，请在删除 HA 组之前更新任何受影响的 S3 或 Swift 客户端应用程序。更新每个客户端以使用其他 IP 地址进行连接，例如，安装期间为接口配置的不同 HA 组的虚拟 IP 地址或 IP 地址。

步骤

1. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。
2. 查看要删除的每个HA组的*负载平衡器端点*列。如果列出了任何负载平衡器端点：
   a. 转到*configuration*>*Network*>*负载平衡器端点*。
   b. 选中此端点对应的复选框。
   c. 选择 * 操作 * > * 编辑端点绑定模式 * 。
   d. 更新绑定模式以删除HA组。
   e. 选择 * 保存更改 * 。
3. 如果未列出负载平衡器端点、请选中要删除的每个HA组对应的复选框。
4. 选择*Actions*>*Remove HA group*。
5. 查看此消息并选择 * 删除 HA 组 * 以确认您的选择。

   选定的所有 HA 组都将被删除。高可用性组页面上会显示一个绿色的成功横幅。

管理负载平衡

负载平衡注意事项

您可以使用负载平衡处理来自S3和Swift客户端的载入和检索工作负载。

什么是负载平衡?

当客户端应用程序从StorageGRID 系统保存或检索数据时、StorageGRID 使用负载平衡器管理载入和检索工作负载。负载平衡通过在多个存储节点之间分布工作负载、最大限度地提高速度和连接容量。

StorageGRID 负载平衡器服务安装在所有管理节点和所有网关节点上，并提供第 7 层负载平衡。它会终止客户端请求，检查请求并与存储节点建立新的安全连接。

将客户端流量转发到存储节点时，每个节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。

> 虽然建议使用 StorageGRID 负载平衡器服务来平衡负载，但您可能希望集成第三方负载平衡器。有关信息，请联系您的 NetApp 客户代表或参阅 "TR-4626： StorageGRID 第三方和全局负载平衡器"。

我需要多少个负载平衡节点?

作为一般最佳实践， StorageGRID 系统中的每个站点都应包含两个或更多具有负载平衡器服务的节点。例如，一个站点可能包含两个网关节点，或者同时包含一个管理节点和一个网关节点。无论您使用的是 SG100 或

SG1000 服务设备，裸机节点还是基于虚拟机（ VM ）的节点，确保每个负载平衡节点都有足够的网络，硬件或虚拟化基础架构。

什么是负载平衡器端点？

负载平衡器端点定义了传入和传出客户端应用程序请求用来访问包含负载平衡器服务的节点的端口和网络协议(HTTPS或HTTP)。端点还可以定义客户端类型(S3或Swift)、绑定模式以及允许或阻止的租户列表(可选)。

要创建负载平衡器端点，请选择*配置*>*网络*>*负载平衡器端点*或完成FabricPool 和S3设置向导。有关说明：

- "配置负载平衡器端点"
- "使用S3设置向导"
- "使用FabricPool 设置向导"

端口注意事项

对于您创建的第一个端点、负载平衡器端点的端口默认为10433、但您可以指定介于1到65535之间的任何未使用的外部端口。如果使用端口80或443、则端点将仅在网关节点上使用负载平衡器服务。这些端口在管理节点上预留。如果对多个端点使用同一端口、则必须为每个端点指定不同的绑定模式。

不允许其他网格服务使用的端口。请参见 "网络端口参考"。

网络协议注意事项

在大多数情况下、客户端应用程序和StorageGRID 之间的连接应使用传输层安全(Transport Layer Security、TLS)加密。支持在不使用TLS加密的情况下连接到StorageGRID 、但不建议这样做、尤其是在生产环境中。为StorageGRID 负载平衡器端点选择网络协议时，应选择*HTTPS*。

负载平衡器端点证书的注意事项

如果选择*HTTPS*作为负载平衡器端点的网络协议，则必须提供安全证书。在创建负载平衡器端点时、您可以使用以下三个选项中的任何一个：

- 上传签名证书**(**建议**)**。此证书可以由公共信任的证书颁发机构(CA)或私有证书颁发机构(CA)签名。最佳做法是、使用公共信任的CA服务器证书来保护连接安全。与生成的证书不同、由CA签名的证书可以无干扰地轮换、这有助于避免过期问题。

  在创建负载平衡器端点之前、您必须获取以下文件：

  - 自定义服务器证书文件。
  - 自定义服务器证书专用密钥文件。
  - (可选)来自每个中间颁发证书颁发机构的证书的CA包。
- 生成自签名证书。
- 使用全局**StorageGRID S3**和**Swift**证书。您必须先上传或生成此证书的自定义版本、然后才能为负载平衡器端点选择此证书。请参见 "配置 S3 和 Swift API 证书"。

我需要什么值？

要创建证书、您必须知道S3或Swift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*Subject DN*(可分辨名称)条目必须包含客户端应用程序将用于StorageGRID 的完全限定域名。例如：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

根据需要、此证书可以使用通配符来表示运行负载平衡器服务的所有管理节点和网关节点的完全限定域名。例如：`*.storagegrid.example.com` 使用*通配符表示 `adm1.storagegrid.example.com` 和 `gn1.storagegrid.example.com`。

如果您计划使用S3虚拟托管模式请求，则证书还必须为每个包含一个*备用名称*条目 "S3端点域名" 您已配置、包括任何通配符名称。例如：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> 如果域名使用通配符、请查看 "服务器证书的强化准则"。

您还必须为安全证书中的每个名称定义一个DNS条目。

如何管理即将到期的证书？

> 如果用于保护S3应用程序和StorageGRID 之间连接的证书到期、则该应用程序可能会暂时无法访问StorageGRID。

要避免证书到期问题、请遵循以下最佳实践：

- 请仔细监控任何警告证书到期日期即将到来的警报，例如S3和Swift API*警报的*负载平衡器端点证书到期*和*全局服务器证书到期。
- 请始终保持StorageGRID 和S3应用程序的证书版本同步。如果要替换或续订用于负载平衡器端点的证书、则必须替换或续订S3应用程序使用的等效证书。
- 使用公共签名的CA证书。如果使用由CA签名的证书、则可以无系统地替换即将到期的证书。
- 如果您已生成自签名StorageGRID 证书、并且该证书即将过期、则必须在现有证书过期之前手动替换StorageGRID 和S3应用程序中的证书。

绑定模式的注意事项

通过绑定模式、您可以控制可用于访问负载平衡器端点的IP地址。如果端点使用绑定模式、则客户端应用程序仅在使用允许的IP地址或其对应的完全限定域名(FQDN)时才能访问该端点。使用任何其他IP地址或FQDN的客户端应用程序无法访问此端点。

您可以指定以下任意绑定模式：

- 全局(默认)：客户端应用程序可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。除非需要限制端点的可访问性、否则请使用此设置。
- * HA组的虚拟IP *。客户端应用程序必须使用HA组的虚拟IP地址(或相应的FQDN)。
- 节点接口。客户端必须使用选定节点接口的IP地址(或相应FQDN)。

- 节点类型。根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)。

租户访问注意事项

租户访问是一项可选的安全功能、可用于控制哪些StorageGRID 租户帐户可以使用负载平衡器端点来访问其分段。您可以允许所有租户访问某个端点(默认)、也可以为每个端点指定允许或阻止的租户列表。

您可以使用此功能在租户及其端点之间提供更好的安全隔离。例如、您可以使用此功能来确保一个租户所拥有的绝密或高度机密材料始终不会被其他租户完全访问。

> 出于访问控制的目的、租户是根据客户端请求中使用的访问密钥来确定的、如果在请求中未提供访问密钥(例如匿名访问)、则使用存储分段所有者来确定租户。

租户访问示例

要了解此安全功能的工作原理、请考虑以下示例：

1. 您已创建两个负载平衡器端点、如下所示：
    - *公共*端点：使用端口10443并允许所有租户访问。
    - *top密钥*端点：使用端口10444并仅允许访问*top密钥*租户。系统将阻止所有其他租户访问此端点。
2. 。 `top-secret.pdf` 位于*top密钥*租户拥有的存储分段中。

以访问 `top-secret.pdf`，“Top SECRELE*”租户中的用户可以向其发送问题描述 GET请求 `https://w.x.y.z:10444/top-secret.pdf`。由于允许此租户使用10444端点、因此用户可以访问此对象。但是、如果属于任何其他租户的用户向同一URL发出相同请求、他们将收到"立即拒绝访问"消息。即使凭据和签名有效、访问也会被拒绝。

CPU 可用性

在向存储节点转发 S3 或 Swift 流量时，每个管理节点和网关节点上的负载平衡器服务会独立运行。通过加权过程，负载平衡器服务会将更多请求路由到 CPU 可用性更高的存储节点。节点 CPU 负载信息每隔几分钟更新一次，但权重可能会更频繁地更新。即使节点报告利用率为 100% 或未能报告利用率，也会为所有存储节点分配最小基本权重值。

在某些情况下，有关 CPU 可用性的信息仅限于负载平衡器服务所在的站点。

配置负载平衡器端点

负载平衡器端点决定了 S3 和 Swift 客户端在连接到网关和管理节点上的 StorageGRID 负载平衡器时可以使用的端口和网络协议。

> 对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。
- 您已查看 "负载平衡注意事项"。

- 如果您先前已重新映射要用于负载平衡器端点的端口，则表示您已重新映射 "已删除端口重新映射"。
- 您已创建计划使用的任何高可用性（ HA ）组。建议使用 HA 组，但不要求使用 HA 组。请参见 "管理高可用性组"。
- 负载平衡器端点是否将由使用 "S3 Select 的 S3 租户"，不能使用任何裸机节点的 IP 地址或 FQDN 。用于 S3 Select 的负载平衡器端点仅允许使用 SG100 或 SG1000 设备以及基于 VMware 的软件节点。
- 您已配置计划使用的任何 VLAN 接口。请参见 "配置 VLAN 接口"。
- 如果要创建 HTTPS 端点（建议），则您具有服务器证书的信息。

  > 对端点证书所做的更改可能需要长达 15 分钟才能应用于所有节点。

  - 要上传证书，您需要服务器证书，证书专用密钥以及 CA 捆绑包（可选）。
  - 要生成证书，您需要 S3 或 Swift 客户端用于访问此端点的所有域名和 IP 地址。您还必须知道主题（可分辨名称）。
  - 如果要使用 StorageGRID S3 和 Swift API 证书（也可用于直接连接到存储节点），则已将默认证书替换为由外部证书颁发机构签名的自定义证书。请参见"配置 S3 和 Swift API 证书"。

创建负载平衡器端点

每个负载平衡器端点都指定一个端口，一个客户端类型（ S3 或 Swift ）和一个网络协议（ HTTP 或 HTTPS ）。

访问向导

步骤

1. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。
2. 选择 * 创建 * 。

输入端点详细信息

步骤

1. 输入端点的详细信息。

字段	**Description**
Name	端点的描述性名称，将显示在负载平衡器端点页面的表中。
Port	要用于负载平衡的 StorageGRID 端口。对于您创建的第一个端点、此字段默认为10433、但您可以输入介于1到65535之间的任何未使用的外部端口。 如果输入 * 。 80* 或 * 。 443* ，则仅在网关节点上配置端点。这些端口在管理节点上预留。
客户端类型	要使用此端点的客户端应用程序类型，可以是 * S3 或 * Swift* 。

字段	Description
网络协议	客户端在连接到此端点时将使用的网络协议。 • 选择 * HTTPS * 可进行安全的 TLS 加密通信（建议）。您必须附加安全证书，然后才能保存此端点。 • 选择 * HTTP * 可实现不太安全的未加密通信。对于非生产网格，请仅使用 HTTP 。

2. 选择 * 继续 * 。

选择绑定模式

步骤

1. 为端点选择绑定模式、以控制如何使用任何IP地址或特定IP地址和网络接口访问端点。

选项	Description
全局（默认）	客户端可以使用任何网关节点或管理节点的IP地址、任何网络上任何HA组的虚拟IP (VIP)地址或相应的FQDN访问端点。 除非需要限制此端点的可访问性，否则请使用 * 全局 * 设置（默认）。
HA 组的虚拟 IP	客户端必须使用HA组的虚拟IP地址(或相应的FQDN)才能访问此端点。 具有此绑定模式的端点都可以使用相同的端口号、只要为端点选择的HA组不重叠即可。
节点接口	客户端必须使用选定节点接口的IP地址(或相应FQDN)才能访问此端点。
节点类型	根据您选择的节点类型、客户端必须使用任何管理节点的IP地址(或相应的FQDN)或任何网关节点的IP地址(或相应的FQDN)来访问此端点。

> 如果多个端点使用同一端口，StorageGRID 将使用此优先级顺序来确定要使用的端点：**HA**组的虚拟**IP *>*Node interfaces**>*Node type*>*Global"。

2. 如果选择了 * HA 组的虚拟 IP * ，请选择一个或多个 HA 组。
3. 如果选择了 * 节点接口 * ，请为要与此端点关联的每个管理节点或网关节点选择一个或多个节点接口。
4. 如果选择了*Node type*，请选择管理节点(包括主管理节点和任何非主管理节点)或网关节点。

控制租户访问

步骤

1. 对于*租户访问*步骤，请选择以下选项之一：

字段	Description
允许所有租户(默认)	所有租户帐户都可以使用此端点来访问其分段。 如果尚未创建任何租户帐户、则必须选择此选项。添加租户帐户后、您可以编辑负载平衡器端点以允许或阻止特定帐户。
允许选定租户	只有选定租户帐户才能使用此端点访问其分段。
阻止选定租户	选定租户帐户无法使用此端点访问其分段。所有其他租户均可使用此端点。

2. 如果要创建*HTTP*端点，则不需要附加证书。选择 * 创建 * 以添加新的负载平衡器端点。然后，转到 完成后。否则，请选择 * 继续 * 以附加证书。

附加证书

步骤

1. 如果要创建 * HTTPS * 端点，请选择要附加到该端点的安全证书类型。

   此证书可保护 S3 和 Swift 客户端之间的连接以及管理节点或网关节点上的负载平衡器服务。

   - * 上传证书 * 。如果您要上传自定义证书，请选择此选项。
   - * 生成证书 * 。如果您具有生成自定义证书所需的值，请选择此选项。
   - * 使用 StorageGRID S3 和 Swift 证书 * 。如果要使用全局 S3 和 Swift API 证书，则选择此选项，此证书也可用于直接连接到存储节点。

     除非将默认的S3和Swift API证书(由网格CA签名)替换为由外部证书颁发机构签名的自定义证书、否则无法选择此选项。请参见"配置 S3 和 Swift API 证书"。

2. 如果您未使用StorageGRID S3和Swift证书、请上传或生成此证书。

上传证书

a. 选择 * 上传证书 * 。

b. 上传所需的服务器证书文件：

- * 服务器证书 * ： PEM 编码的自定义服务器证书文件。
- 证书专用密钥:自定义服务器证书专用密钥文件（`.key`）。

> EC 专用密钥必须大于或等于 224 位。RSA 私钥必须大于或等于 2048 位。

- * CA bundle* ：一个可选文件，其中包含来自每个中间颁发证书颁发机构（ CA ）的证书。此文件应包含 PEM 编码的每个 CA 证书文件，并按证书链顺序串联。

c. 展开 * 证书详细信息 * 以查看您上传的每个证书的元数据。如果您上传了可选的 CA 包，则每个证书都会显示在其自己的选项卡上。

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

  指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

  例如： `storagegrid_certificate.pem`

- 选择 * 复制证书 PEM* 或 * 复制 CA 捆绑包 PEM* ，将证书内容复制到其他位置进行粘贴。

d. 选择 * 创建 * 。+ 已创建负载平衡器端点。自定义证书用于 S3 和 Swift 客户端与端点之间的所有后续新连接。

生成证书

a. 选择 * 生成证书 * 。

b. 指定证书信息：

字段	**Description**
域名	要包含在证书中的一个或多个完全限定域名。使用 * 作为通配符表示多个域名。
IP	要包含在证书中的一个或多个IP地址。
主题(可选)	证书所有者的X.509主题或可分辨名称(DN)。 如果未在此字段中输入值、则生成的证书将使用第一个域名或IP地址作为使用者公用名(CN)。
有效天数	创建后证书过期的天数。

字段	Description
添加密钥用法扩展	如果选中(默认值和建议值)、则会将密钥用法和扩展密钥用法扩展添加到生成的证书中。 这些扩展定义了证书中所含密钥的用途。 注意：除非证书包含这些扩展时遇到与旧客户端的连接问题，否则请保持选中此复选框。

c. 选择 * 生成 * 。

d. 选择 * 证书详细信息 * 可查看生成的证书的元数据。

   - 选择 * 下载证书 * 以保存证书文件。

     指定证书文件名和下载位置。使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

   - 选择 * 复制证书 PEM* 将证书内容复制到其他位置进行粘贴。

e. 选择 * 创建 * 。

   此时将创建负载平衡器端点。自定义证书用于 S3 和 Swift 客户端与此端点之间的所有后续新连接。

完成后

步骤

1. 如果使用DNS、请确保DNS包含一条记录、用于将StorageGRID 完全限定域名(FQDN)与客户端用于建立连接的每个IP地址相关联。

   在 DNS 记录中输入的 IP 地址取决于您是否使用的是由负载平衡节点组成的 HA 组：

   - 如果已配置HA组、则客户端将连接到该HA组的虚拟IP地址。
   - 如果不使用HA组、则客户端将使用网关节点或管理节点的IP地址连接到StorageGRID 负载平衡器服务。

     此外，还必须确保 DNS 记录引用所有必需的端点域名，包括任何通配符名称。

2. 为 S3 和 Swift 客户端提供连接到端点所需的信息：
   - 端口号
   - 完全限定域名或 IP 地址
   - 任何必需的证书详细信息

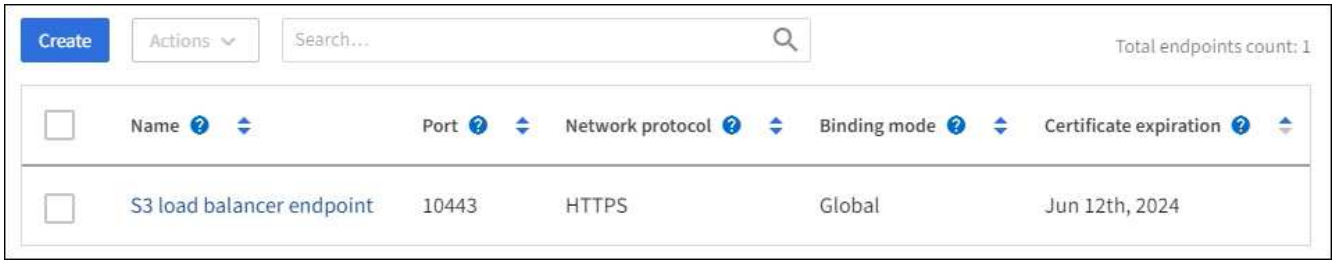
查看和编辑负载平衡器端点

您可以查看现有负载平衡器端点的详细信息，包括安全端点的证书元数据。您还可以更改端点的名称或绑定模式

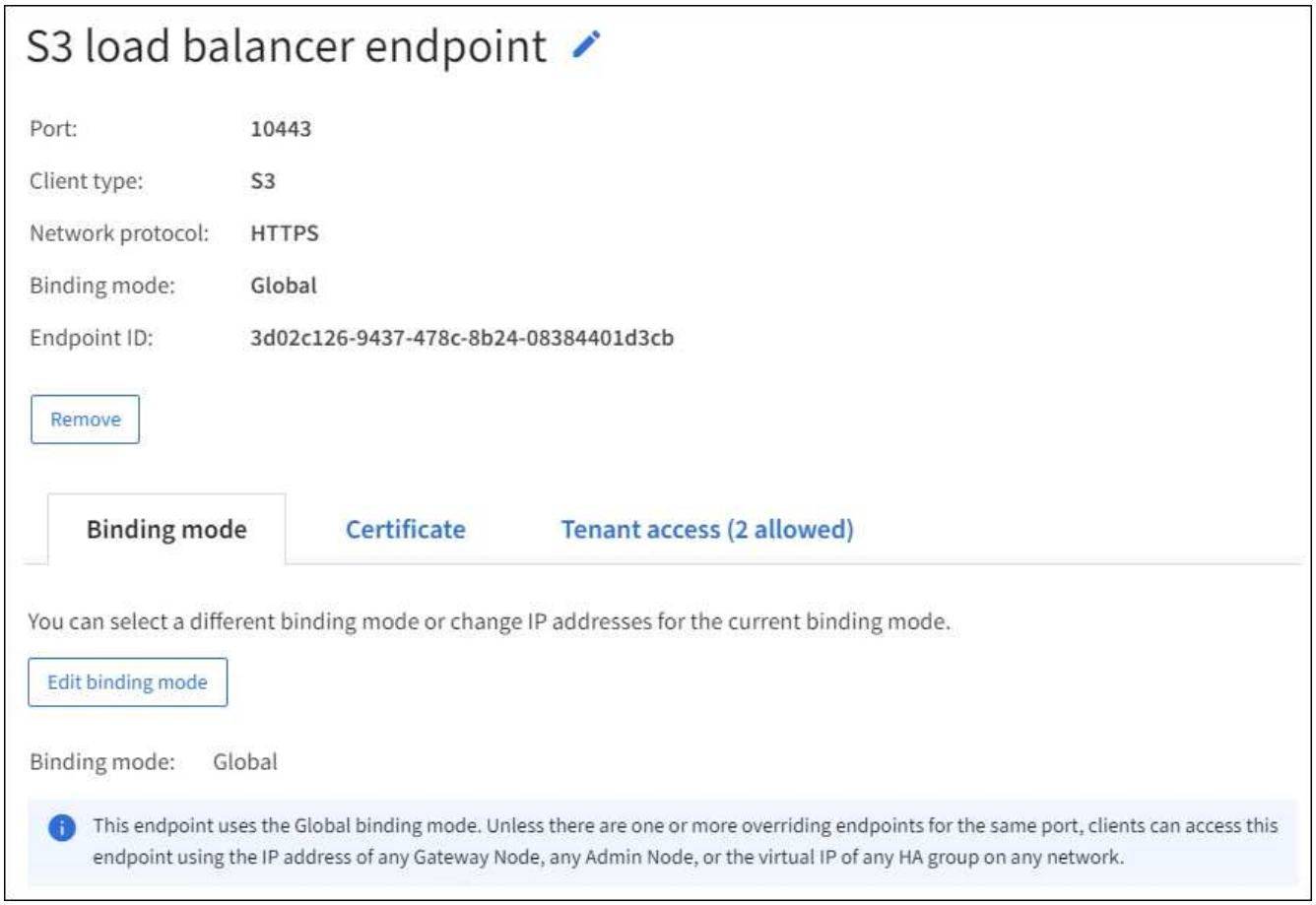
，并更新任何关联的证书。

您不能更改服务类型(S3或Swift)、端口或协议(HTTP或HTTPS)。

- 要查看所有负载平衡器端点的基本信息，请查看负载平衡器端点页面上的表。



- 要查看有关特定端点的所有详细信息，包括证书元数据，请在表中选择端点的名称。



- 要编辑端点，请使用负载平衡器端点页面上的 * 操作 * 菜单或特定端点的详细信息页面。

> 编辑端点后，您可能需要等待长达 15 分钟，才能将所做的更改应用于所有节点。

任务	操作菜单	详细信息页面
编辑端点名称	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点名称 * 。 c. 输入新名称。 d. 选择 * 保存 * 。	a. 选择端点名称以显示详细信息。 b. 选择编辑图标 。 c. 输入新名称。 d. 选择 * 保存 * 。
编辑端点绑定模式	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 编辑绑定模式 * 。 c. 根据需要更新绑定模式。 d. 选择 * 保存更改 * 。
编辑端点证书	a. 选中此端点对应的复选框。 b. 选择 * 操作 * > * 编辑端点证书 * 。 c. 根据需要上传或生成新的自定义证书或开始使用全局 S3 和 Swift 证书。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择 * 证书 * 选项卡。 c. 选择 * 编辑证书 * 。 d. 根据需要上传或生成新的自定义证书或开始使用全局 S3 和 Swift 证书。 e. 选择 * 保存更改 * 。
编辑租户访问	a. 选中此端点对应的复选框。 b. 选择*操作*>*编辑租户访问*。 c. 选择其他访问选项、从列表中选择或删除租户、或者同时执行这两项操作。 d. 选择 * 保存更改 * 。	a. 选择端点名称以显示详细信息。 b. 选择*租户访问*选项卡。 c. 选择*编辑租户访问*。 d. 选择其他访问选项、从列表中选择或删除租户、或者同时执行这两项操作。 e. 选择 * 保存更改 * 。

删除负载平衡器端点

您可以使用 * 操作 * 菜单删除一个或多个端点，也可以从详细信息页面中删除单个端点。

> 为防止客户端中断，请在删除负载平衡器端点之前更新任何受影响的 S3 或 Swift 客户端应用程序。更新每个客户端以使用分配给另一个负载平衡器端点的端口进行连接。请务必同时更新所需的任何证书信息。

- 删除一个或多个端点：
  a. 在"负载平衡器"页面中、选中要删除的每个端点对应的复选框。
  b. 选择 * 操作 * > * 删除 * 。
  c. 选择 * 确定 * 。

- 从详细信息页面中删除一个端点：
  a. 从负载平衡器页面。选择端点名称。
  b. 在详细信息页面上选择 * 删除 * 。
  c. 选择 * 确定 * 。

配置S3端点域名

要支持S3虚拟托管模式请求、必须使用网格管理器配置S3客户端连接到的S3端点域名列表。

> 不支持使用IP地址作为端点域名。未来版本将禁止此配置。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您已拥有 "特定访问权限"。
- 您已确认网格升级未在进行中。

> 在进行网格升级时、请勿对域名配置进行任何更改。

关于此任务

要使客户端能够使用 S3 端点域名，您必须执行以下所有操作：

- 使用网格管理器将 S3 端点域名添加到 StorageGRID 系统。
- 确保 "客户端用于与StorageGRID 进行HTTPS连接的证书" 已针对客户端所需的所有域名进行签名。

  例如、如果端点为 `s3.company.com`、您必须确保用于HTTPS连接的证书包括 `s3.company.com` 端点和端点的通配符使用者备用名称(SAN)： `*.s3.company.com`。

- 配置客户端使用的 DNS 服务器。包括客户端用于建立连接的IP地址的DNS记录、并确保这些记录引用所有必需的S3端点域名、包括任何通配符名称。

> 客户端可以使用网关节点，管理节点或存储节点的 IP 地址或连接到高可用性组的虚拟 IP 地址连接到 StorageGRID 。您应了解客户端应用程序如何连接到网格，以便在 DNS 记录中包含正确的 IP 地址。

使用 HTTPS 连接（建议）连接到网格的客户端可以使用以下任一证书：

- 连接到负载平衡器端点的客户端可以对该端点使用自定义证书。可以对每个负载平衡器端点进行配置、使其能够识别不同的S3端点域名。
- 连接到负载平衡器端点或直接连接到存储节点的客户端可以自定义全局S3和Swift API证书、以包含所有必需的S3端点域名。

> 如果不添加S3端点域名且此列表为空、则会禁用对S3虚拟托管模式请求的支持。

添加S3端点域名

步骤

1. 选择*配置*>*网络*>* S3端点域名*。
2. 在*域名1*字段中输入域名。选择*添加其他域名*以添加更多域名。
3. 选择 * 保存 * 。
4. 确保客户端使用的服务器证书与所需的S3端点域名匹配。
   - 如果客户端连接到使用自己的证书的负载平衡器端点、 "更新与此端点关联的证书"。
   - 如果客户端连接到使用全局S3和Swift API证书的负载平衡器端点、或者直接连接到存储节点、 "更新全局S3和Swift API证书"。
5. 添加所需的 DNS 记录，以确保可以解决端点域名请求。

结果

现在、当客户端使用端点时 `bucket.s3.company.com`、DNS服务器解析到正确的端点、证书将按预期对端点进行身份验证。

重命名S3端点域名

如果更改S3应用程序使用的名称、虚拟托管模式请求将失败。

步骤

1. 选择*配置*>*网络*>* S3端点域名*。
2. 选择要编辑的域名字段并进行必要的更改。
3. 选择 * 保存 * 。
4. 选择*是*确认更改。

删除S3端点域名

如果删除S3应用程序使用的名称、虚拟托管模式请求将失败。

步骤

1. 选择*配置*>*网络*>* S3端点域名*。
2. 选择删除图标 ✕ 域名旁边。
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"

摘要：客户端连接的 IP 地址和端口

要存储或检索对象、S3和Swift客户端应用程序会连接到负载平衡器服务(包含在所有管理

节点和网关节点上)或本地分发路由器(LDR)服务(包含在所有存储节点上)。

客户端应用程序可以使用网格节点的IP地址以及该节点上服务的端口号连接到StorageGRID。或者、您也可以为负载平衡节点创建高可用性(HA)组、以提供使用虚拟IP (VIP)地址的高可用性连接。如果要使用完全限定域名(FQDN)而不是IP或VIP地址连接到StorageGRID 、则可以配置DNS条目。

此表总结了客户端连接到 StorageGRID 的不同方式以及每种连接类型所使用的 IP 地址和端口。如果已创建负载平衡器端点和高可用性(HA)组、请参见 从何处查找IP地址 在网格管理器中查找这些值。

建立连接的位置	客户端连接到的服务	**IP** 地址	**Port**
HA 组	负载平衡器	HA 组的虚拟 IP 地址	分配给负载平衡器端点的端口
管理节点	负载平衡器	管理节点的 IP 地址	分配给负载平衡器端点的端口
网关节点	负载平衡器	网关节点的 IP 地址	分配给负载平衡器端点的端口
存储节点	LDR	存储节点的 IP 地址	默认 S3 端口： • HTTPS： 18082 • HTTP： 18084 默认 Swift 端口： • HTTPS： 18083 • HTTP： 18085

示例**URL**

要将客户端应用程序连接到网关节点HA组的负载平衡器端点、请使用如下所示的URL结构：

```
https://VIP-of-HA-group:LB-endpoint-port
```

例如、如果HA组的虚拟IP地址为192.0.2.5、负载平衡器端点的端口号为10443、则应用程序可以使用以下URL连接到StorageGRID ：

```
https://192.0.2.5:10443
```

从何处查找**IP**地址

1. 使用登录到网格管理器 "支持的 Web 浏览器"。
2. 要查找网格节点的 IP 地址，请执行以下操作：
   a. 选择 * 节点 * 。
   b. 选择要连接到的管理节点，网关节点或存储节点。

c. 选择 * 概述 * 选项卡。

d. 在节点信息部分中，记下节点的 IP 地址。

e. 选择 * 显示更多 * 可查看 IPv6 地址和接口映射。

   您可以建立从客户端应用程序到列表中任何 IP 地址的连接：

   - * eth0： * 网格网络
   - * eth1： * 管理网络（可选）
   - * eth2： * 客户端网络（可选）

   > 如果您正在查看管理节点或网关节点，并且该节点是高可用性组中的活动节点，则 eth2 上会显示 HA 组的虚拟 IP 地址。

3. 要查找高可用性组的虚拟 IP 地址，请执行以下操作：

   a. 选择 * 配置 * > * 网络 * > * 高可用性组 * 。

   b. 在表中，记下 HA 组的虚拟 IP 地址。

4. 查找负载平衡器端点的端口号：

   a. 选择 * 配置 * > * 网络 * > * 负载平衡器端点 * 。

   b. 记下要使用的端点的端口号。

   > 如果端口号为80或443、则仅在网关节点上配置端点、因为这些端口是在管理节点上预留的。所有其他端口都在网关节点和管理节点上进行配置。

   c. 从表中选择端点的名称。

   d. 确认*客户端类型*(S3或Swift)与要使用端点的客户端应用程序匹配。

管理网络和连接

配置网络设置：概述

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

配置 **VLAN** 接口

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

流量分类策略

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

StorageGRID 网络准则

您可以使用网格管理器配置和管理 StorageGRID 网络和连接。

请参见 "配置 S3 和 Swift 客户端连接" 了解如何连接 S3 或 Swift 客户端。

默认 StorageGRID 网络

默认情况下， StorageGRID 支持每个网格节点使用三个网络接口，从而可以根据您的安全和访问要求为每个网格节点配置网络。

有关网络拓扑的详细信息，请参见 "网络连接准则"。

网格网络

Required网格网络用于所有内部 StorageGRID 流量。它可以在网格中的所有节点之间以及所有站点和子网之间建立连接。

管理网络

可选。管理网络通常用于系统管理和维护。它也可用于客户端协议访问。管理网络通常是一个专用网络，不需要在站点之间进行路由。

客户端网络

可选。客户端网络是一种开放网络，通常用于提供对 S3 和 Swift 客户端应用程序的访问，因此网格网络可以进行隔离和保护。客户端网络可以与可通过本地网关访问的任何子网进行通信。

准则

- 每个 StorageGRID 网格节点都需要为其分配到的每个网络配置一个专用网络接口， IP 地址，子网掩码和网关。
- 一个网格节点不能在一个网络上具有多个接口。
- 支持每个网格节点在每个网络上使用一个网关，并且该网关必须与节点位于同一子网中。如果需要，您可以在网关中实施更复杂的路由。
- 在每个节点上，每个网络都映射到一个特定的网络接口。

网络	接口名称
网格	eth0
admin （可选）	Eth1
客户端（可选）	Eth2

- 如果节点连接到 StorageGRID 设备，则每个网络都使用特定端口。有关详细信息，请参见适用于您的设备的安装说明。
- 每个节点都会自动生成默认路由。如果启用了 eth2 ，则 0.0.0.0/0 将在 eth2 上使用客户端网络。如果未启用 eth2 ，则 0.0.0.0/0 将在 eth0 上使用网格网络。

- 只有在网格节点加入网格后，客户端网络才会正常运行
- 可以在网格节点部署期间配置管理网络，以便在网格完全安装之前能够访问安装用户界面。

可选接口

您也可以向节点添加额外的接口。例如，您可能希望将中继接口添加到管理节点或网关节点，以便可以使用 "VLAN 接口" 隔离属于不同应用程序或租户的流量。或者，您可能希望添加要在中使用的访问接口 "高可用性（HA）组"。

要添加中继或访问接口，请参见以下内容：

- * VMware （安装节点后） *： "VMware： 向节点添加中继或访问接口"
  - * RHEL 或 CentOS （安装节点之前） *： "创建节点配置文件"
  - * Ubuntu 或 Debian （安装节点之前） *： "创建节点配置文件"
  - * RHEL， CentOS， Ubuntu 或 Debian （安装节点后） *： "Linux： 向节点添加中继或访问接口"

查看 IP 地址

您可以查看 StorageGRID 系统中每个网格节点的 IP 地址。然后、您可以使用此IP地址通过命令行登录到网格节点并执行各种维护过程。

开始之前

您将使用登录到网格管理器 "支持的 Web 浏览器"。

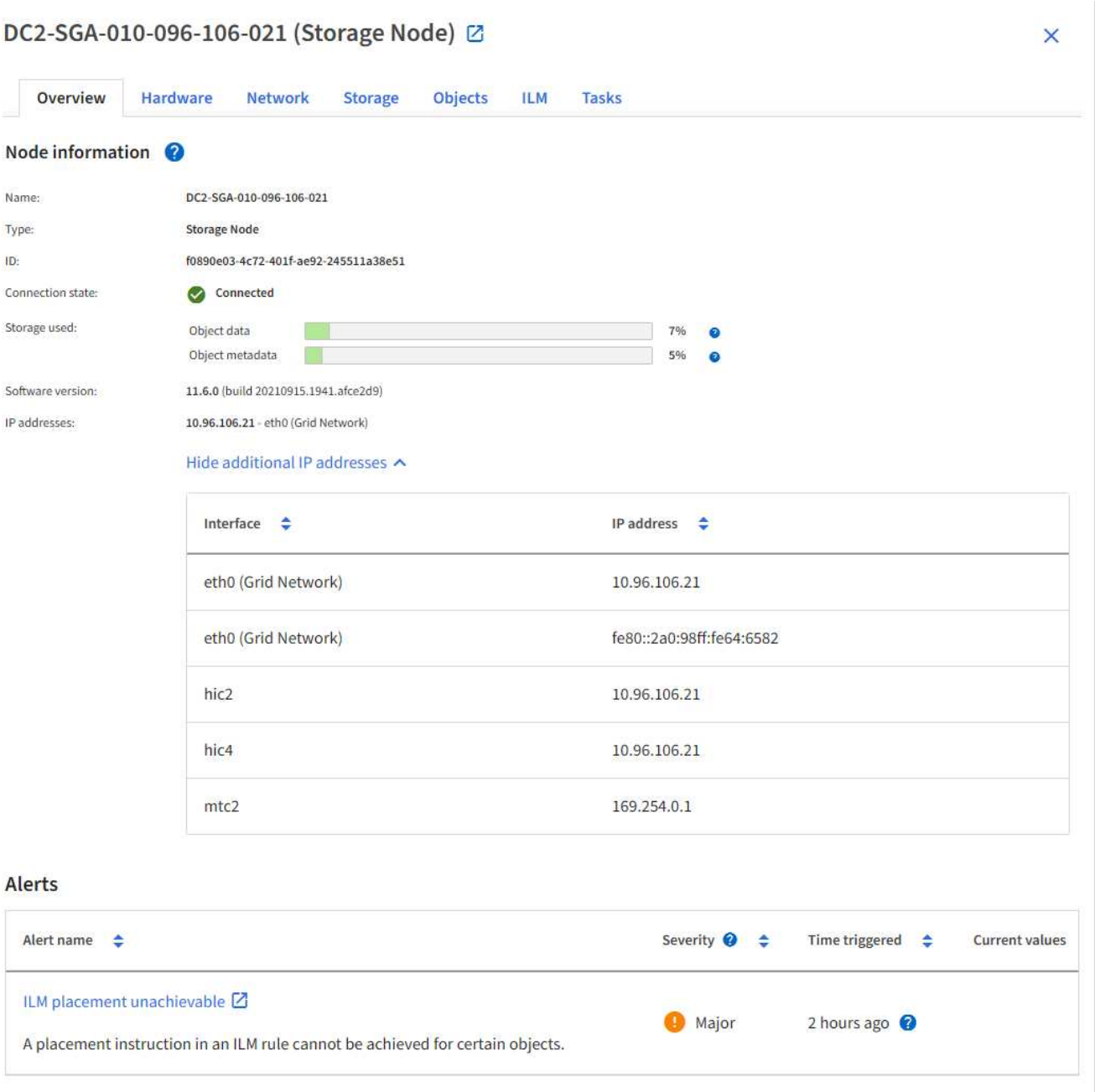
关于此任务

有关更改IP地址的信息、请参见 "配置 IP 地址"。

步骤

1. 选择 * 节点 * > * 网格节点 _* > * 概述 * 。
2. 选择 IP 地址标题右侧的 * 显示更多 * 。

   此网格节点的 IP 地址会在表中列出。



支持传出 TLS 连接的密码

StorageGRID 系统支持一组有限的密码套件，用于将传输层安全（Transport Layer Security， TLS）连接到用于身份联合和云存储池的外部系统。

支持的 TLS 版本

StorageGRID 支持使用 TLS 1.2 和 TLS 1.3 连接到用于身份联合和云存储池的外部系统。

为了确保与一系列外部系统兼容，我们选择了可与外部系统结合使用的 TLS 密码。此列表大于支持在 S3 或 Swift 客户端应用程序中使用的密码列表。要配置加密方法，请进入*configuration*>*Security*>*Security settings，然后选择*TLS和SSH policies*。

在StorageGRID 中、无法配置协议版本、密码、密钥交换算法和MAC算法等TLS配置选项。如果您对这些设置有特定要求，请联系您的 NetApp 客户代表。

配置 VLAN 接口

您可以在管理节点和网关节点上创建虚拟 LAN （ VLAN ）接口，并在 HA 组和负载平衡器端点中使用这些接口隔离和分区流量，以提高安全性，灵活性和性能。

VLAN 接口注意事项

- 您可以通过输入 VLAN ID 并在一个或多个节点上选择父接口来创建 VLAN 接口。
- 必须在交换机上将父接口配置为中继接口。
- 父接口可以是网格网络（ eth0 ），客户端网络（ eth2 ），也可以是虚拟机或裸机主机的附加中继接口（例如 ens256 ）。
- 对于每个 VLAN 接口，您只能为给定节点选择一个父接口。例如、不能将同一网关节点上的网格网络接口和客户端网络接口用作同一VLAN的父接口。
- 如果 VLAN 接口用于管理节点流量，其中包括与网格管理器和租户管理器相关的流量，请仅选择管理节点上的接口。
- 如果 VLAN 接口用于 S3 或 Swift 客户端流量，请选择管理节点或网关节点上的接口。
- 如果需要添加中继接口，请参见以下内容了解详细信息：
  - * VMware （安装节点后）*： "VMware： 向节点添加中继或访问接口"
  - * RHEL 或 CentOS （安装节点之前）*： "创建节点配置文件"
  - * Ubuntu 或 Debian （安装节点之前）*： "创建节点配置文件"
  - * RHEL ， CentOS ， Ubuntu 或 Debian （安装节点后）*： "Linux： 向节点添加中继或访问接口"

创建 VLAN 接口

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。
- 已在网络中配置中继接口并将其连接到 VM 或 Linux 节点。您知道中继接口的名称。
- 您知道要配置的 VLAN 的 ID 。

关于此任务

网络管理员可能已配置一个或多个中继接口以及一个或多个 VLAN ，以隔离属于不同应用程序或租户的客户端或管理流量。每个 VLAN 都通过一个数字 ID 或标记来标识。例如，您的网络可能使用 VLAN 100 传输 FabricPool 流量，而使用 VLAN 200 传输归档应用程序。

您可以使用网格管理器创建 VLAN 接口，以允许客户端访问特定 VLAN 上的 StorageGRID 。创建 VLAN 接口时，您可以指定 VLAN ID 并选择一个或多个节点上的父（中继）接口。

访问向导

步骤

1. 选择 * 配置 * > * 网络 * > * VLAN 接口 * 。
2. 选择 * 创建 * 。

输入 **VLAN** 接口的详细信息

步骤

1. 指定网络中 VLAN 的 ID 。您可以输入 1 到 4094 之间的任何值。

   VLAN ID不需要唯一。例如，您可以对一个站点的管理流量使用 VLAN ID 200 ，而对另一个站点的客户端流量使用相同的 VLAN ID 。您可以在每个站点使用不同的父接口集创建单独的 VLAN 接口。但是、具有相同ID的两个VLAN接口不能在一个节点上共享同一个接口。如果指定的 ID 已被使用，则会显示一条消息。

2. 或者，输入 VLAN 接口的短问题描述 。
3. 选择 * 继续 * 。

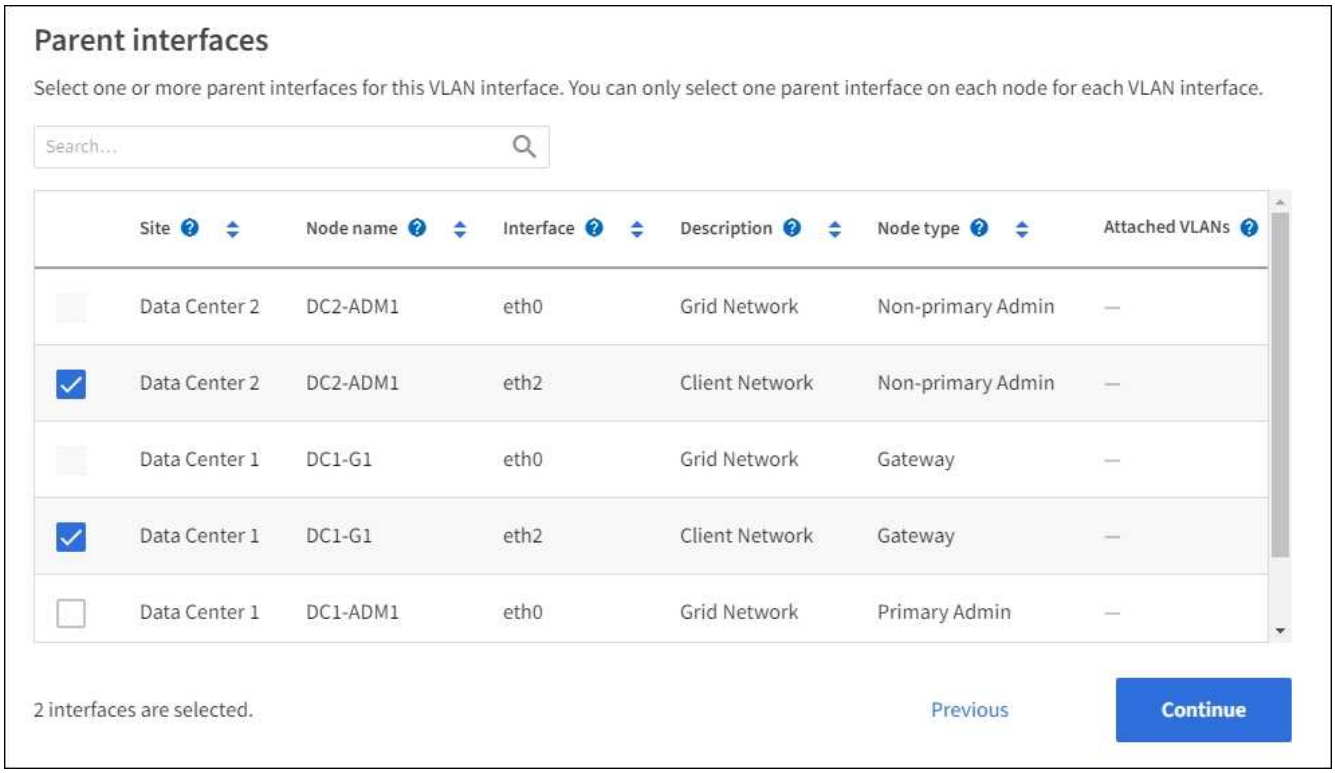
选择父接口

下表列出了网格中每个站点上所有管理节点和网关节点的可用接口。管理网络(eth1)接口不能用作父接口、因此不会显示出来。

步骤

1. 选择一个或多个要将此 VLAN 连接到的父接口。

   例如，您可能希望将 VLAN 连接到网关节点和管理节点的客户端网络（ eth2 ）接口。



2. 选择 * 继续 * 。

确认设置

步骤

1. 查看配置并进行任何更改。
   - 如果需要更改 VLAN ID 或问题描述 ，请选择页面顶部的 * 输入 VLAN 详细信息 * 。
   - 如果需要更改父接口，请选择页面顶部的 * 选择父接口 * 或选择 * 上一个 * 。
   - 如果需要删除父接口，请选择垃圾桶 。
2. 选择 * 保存 * 。
3. 等待 5 分钟，使新接口显示为 " 高可用性组 " 页面上的一个选项，并在节点的 * 网络接口 * 表中列出（ * 节点 * > * 父接口节点 _* > * 网络 * ）。

编辑 **VLAN** 接口

编辑 VLAN 接口时，可以进行以下类型的更改：

- 更改 VLAN ID 或问题描述 。
- 添加或删除父接口。

例如，如果您计划停用关联节点，则可能需要从 VLAN 接口中删除父接口。

请注意以下事项：

- 如果在 HA 组中使用 VLAN 接口，则无法更改 VLAN ID 。
- 如果父接口在 HA 组中使用，则不能删除该父接口。

  例如，假设 VLAN 200 连接到节点 A 和 B 上的父接口如果 HA 组对节点 A 使用 VLAN 200 接口，而对节点 B 使用 eth2 接口，则可以删除节点 B 未使用的父接口，但不能删除节点 A 使用的父接口

步骤

1. 选择 * 配置 * > * 网络 * > * VLAN 接口 * 。
2. 选中要编辑的VLAN接口对应的复选框。然后，选择 * 操作 * > * 编辑 * 。
3. 也可以更新 VLAN ID 或问题描述 。然后，选择 * 继续 * 。

   如果在 HA 组中使用 VLAN ，则无法更新 VLAN ID 。
4. (可选)选中或清除相应复选框以添加父接口或删除未使用的接口。然后，选择 * 继续 * 。
5. 查看配置并进行任何更改。
6. 选择 * 保存 * 。

删除 **VLAN** 接口

您可以删除一个或多个 VLAN 接口。

如果 VLAN 接口当前正在 HA 组中使用，则无法将其删除。必须先从 HA 组中删除 VLAN 接口，然后才能将其删除。

要避免客户端流量发生任何中断，请考虑执行以下操作之一：

- 在删除此 VLAN 接口之前，请向 HA 组添加一个新的 VLAN 接口。
- 创建不使用此 VLAN 接口的新 HA 组。
- 如果要删除的 VLAN 接口当前为活动接口，请编辑 HA 组。将要删除的 VLAN 接口移至优先级列表的底部。等待新主接口建立通信，然后从 HA 组中删除旧接口。最后，删除该节点上的 VLAN 接口。

步骤

1. 选择 * 配置 * > * 网络 * > * VLAN 接口 * 。
2. 选中要删除的每个VLAN接口对应的复选框。然后，选择 * 操作 * > * 删除 * 。
3. 选择 * 是 * 确认您的选择。

   选定的所有 VLAN 接口都将被删除。VLAN 接口页面上会显示一个绿色的成功横幅。

管理流量分类策略

管理流量分类策略：概述

为了增强服务质量（QoS）服务，您可以创建流量分类策略来识别和监控不同类型的网络流量。这些策略有助于限制和监控流量。

流量分类策略应用于网关节点和管理节点的 StorageGRID 负载平衡器服务上的端点。要创建流量分类策略，必须已创建负载平衡器端点。

匹配规则

每个流量分类策略都包含一个或多个匹配规则，用于标识与以下一个或多个实体相关的网络流量：

- 存储分段
- Subnet
- 租户
- 负载平衡器端点

StorageGRID 会根据规则的目标监控与策略中任何规则匹配的流量。与某个策略的任何规则匹配的任何流量均由该策略处理。相反，您可以设置规则来匹配除指定实体之外的所有流量。

流量限制

您也可以将以下限制类型添加到策略中：

- 聚合带宽
- 每个请求的带宽
- 并发请求

- 请求率

限制值按负载平衡器强制实施。如果流量同时分布在多个负载平衡器上，则总最大速率是您指定的速率限制的倍数。

> 您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是、StorageGRID 不能同时限制这两种类型的带宽。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。

对于聚合或每个请求的带宽限制，请求将以您设置的速率传入或移出。StorageGRID 只能强制执行一个速度，因此，按匹配器类型强制执行最具体的策略匹配。此请求占用的带宽不会计入包含聚合带宽限制策略的其他不太特定的匹配策略。对于所有其他限制类型，客户端请求会延迟 250 毫秒，对于超过任何匹配策略限制的请求，客户端请求会收到 503 个响应速度较慢的响应。

在网格管理器中，您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

使用具有 SLA 的流量分类策略

您可以将流量分类策略与容量限制和数据保护结合使用来实施服务级别协议（ SLA ），这些协议提供了有关容量，数据保护和性能的具体信息。

以下示例显示了一个 SLA 的三个层。您可以创建流量分类策略以实现每个 SLA 层的性能目标。

服务级别层	**Capacity**	数据保护	允许的最高性能	成本
金牌	允许 1 PB 存储	3 复制 ILM 规则	25 K 请求 / 秒 5 GB/ 秒（ 40 Gbps ）带宽	每月 $$
银牌	允许使用 250 TB 存储	2 复制 ILM 规则	每秒 10 K 个请求 1.25 GB/ 秒（ 10 Gbps ）带宽	每月 $$
铜牌	允许 100 TB 存储	2 复制 ILM 规则	5 K 请求 / 秒 1 GB/ 秒（ 8 Gbps ）带宽	每月 $

创建流量分类策略

如果要监控网络流量、您可以创建流量分类策略、也可以选择按分段、分段正则表达式、CIDR、负载平衡器端点或租户限制网络流量。您也可以根据带宽，并发请求数或请求率为策略设置限制。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

- 您已创建要匹配的任何负载平衡器端点。
- 您已创建要匹配的任何租户。

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。
2. 选择 * 创建 * 。
3. 为策略输入名称和问题描述 (可选)，然后选择*CONTINUE*。

   例如，描述此流量分类策略适用场景 及其限制。

4. 选择*添加规则*并指定以下详细信息，为策略创建一个或多个匹配规则。您创建的任何策略都应至少具有一个匹配规则。选择 * 继续 * 。

字段	Description
Type	选择与规则适用场景 匹配的流量类型。流量类型包括存储分段、存储分段正则表达式、CIDR、负载平衡器端点和租户。
匹配值	输入与选定类型匹配的值。 • 存储分段：输入一个或多个存储分段名称。 • b分 段正则表达式：输入用于匹配一组分段名称的一个或多个正则表达式。 正则表达式已取消锁定。在分段名称的开头使用^锚定进行匹配、在名称的结尾使用$锚定进行匹配。正则表达式匹配支持PCRE (Perl兼容正则表达式)语法的子集。 • cidr：以CIDR表示法输入一个或多个与所需子网匹配的IPv4子网。 • 负载平衡器端点：选择端点名称。这些是您在上定义的负载平衡器端点 "配置负载平衡器端点"。 • 租户：租户匹配使用访问密钥ID。如果此请求不包含访问密钥ID (例如、匿名访问)、则会使用所访问存储分段的所有权来确定租户。
反向匹配	如果要匹配与刚刚定义的类型和匹配值一致的所有网络流量_例外_流量，请选中*反向匹配*复选框。否则、请清除此复选框。 例如，如果要将此策略应用于除一个负载平衡器端点之外的所有端点，请指定要排除的负载平衡器端点，然后选择*Inverse Match*。 对于包含多个匹配器且至少有一个是反向匹配器的策略，请注意不要创建与所有请求匹配的策略。

5. (可选)选择*添加限制*，然后选择以下详细信息以添加一个或多个限制，以控制规则匹配的网络流量。

   即使您未添加任何限制、StorageGRID 也会收集指标、以便您了解流量趋势。

字段	Description
Type	要应用于规则匹配的网络流量的限制类型。例如、您可以限制带宽或请求速率。 注意：您可以创建策略来限制聚合带宽或限制每个请求的带宽。但是、StorageGRID 不能同时限制这两种类型的带宽。使用聚合带宽时、每个请求的带宽不可用。相反、如果正在使用每个请求的带宽、则聚合带宽将不可用。聚合带宽限制可能会对非受限流量产生额外的轻微性能影响。 对于带宽限制， StorageGRID 会应用与设置的限制类型最匹配的策略。例如，如果您的策略仅限制一个方向的流量，则相反方向的流量将是无限制的，即使存在与具有带宽限制的其他策略匹配的流量也是如此。StorageGRID 按以下顺序实施带宽限制的"最佳"匹配： • 确切的 IP 地址（ /32 掩码） • 确切的存储分段名称 • 分段正则表达式 • 租户 • 端点 • 非精确的 CIDR 匹配项（非 /32 ） • 反向匹配
适用场景	这是否会限制适用场景 客户端读取请求(GET或HEAD)或写入请求(Put、POST或DELETE)。
价值	根据您选择的单位、网络流量将限制为的值。例如、输入10并选择MiB/秒、以防止与此规则匹配的网络流量超过10 MiB/秒 注意：根据单位设置，可用单位可以是二进制(例如GiB)或十进制(例如GB)。要更改单位设置，请选择网格管理器右上角的用户下拉列表，然后选择*用户首选项*。
Unit	描述您输入的值的单位。

例如、如果要为SLA层创建40 Gb/秒带宽限制、请创建两个聚合带宽限制：GET /机头为40 Gb/秒、而Put / POST / DELETE为40 Gb/秒

6. 选择 * 继续 * 。
7. 阅读并查看流量分类策略。使用*上一步*按钮返回并根据需要进行更改。对策略满意后，选择*保存并继续*。

   现在、S3和Swift客户端流量将根据流量分类策略进行处理。

完成后

"查看网络流量指标" 验证策略是否强制实施了预期的流量限制。

编辑流量分类策略

您可以编辑流量分类策略以更改其名称或问题描述，或者创建，编辑或删除此策略的任何规则或限制。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示"流量分类策略"页面、并在表中列出现有策略。

2. 使用操作菜单或详细信息页面编辑策略。请参见 "创建流量分类策略" 输入内容。

   操作菜单

   a. 选中策略对应的复选框。
   b. 选择*Actions*>*Edit*。

   详细信息页面

   a. 选择策略名称。
   b. 选择策略名称旁边的*Edit*按钮。

3. 对于输入策略名称步骤，可选择编辑策略名称或问题描述，然后选择*CONTINUOD*。
4. 对于添加匹配规则步骤，可选择添加规则或编辑现有规则的*Type*和*Match Value*，然后选择*Continue*。
5. 对于“设置限制”步骤，可以选择添加、编辑或删除限制，然后选择*CONTINUOD*。
6. 查看更新后的策略，然后选择*保存并继续*。

   您对策略所做的更改将被保存，网络流量现在将根据流量分类策略进行处理。您可以查看流量图表并验证策略是否正在强制实施预期的流量限制。

删除流量分类策略

您可以删除不再需要的流量分类策略。请确保删除正确的策略、因为删除策略后无法检索到该策略。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

此时将显示"流量分类策略"页面、其中的现有策略在表中列出。

2. 使用操作菜单或详细信息页面删除策略。

   操作菜单

   a. 选中策略对应的复选框。
   b. 选择 * 操作 * > * 删除 * 。

   策略详细信息页面

   a. 选择策略名称。
   b. 选择策略名称旁边的*Remove*按钮。

3. 选择*是*确认要删除策略。

   此策略将被删除。

查看网络流量指标

您可以通过查看"流量分类策略"页面中提供的图形来监控网络流量。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有root访问权限或租户帐户权限。

关于此任务

对于任何现有流量分类策略、您可以查看负载平衡器服务的指标、以确定该策略是否成功限制网络中的流量。图形中的数据可以帮助您确定是否需要调整策略。

即使没有为流量分类策略设置限制，也会收集指标，并且图形可提供有用的信息来了解流量趋势。

步骤

1. 选择 * 配置 * > * 网络 * > * 流量分类 * 。

   此时将显示"流量分类策略"页面、表中将列出现有策略。

2. 选择要查看其指标的流量分类策略名称。
3. 选择*Metrics *选项卡。

   此时将显示流量分类策略图形。这些图形仅显示与选定策略匹配的流量的指标。

   页面上包含以下图形。

   - 请求速率：此图提供与所有负载平衡器处理的此策略匹配的带宽量。收到的数据包括所有请求的请求标头以及包含正文数据的响应的正文数据大小。Sent包括所有请求的响应标头以及响应中包含正文数据的请求的响应正文数据大小。

请求完成后、此图表仅显示带宽使用量。对于速度较慢或较大的对象请求、实际瞬时带宽可能与此图中报告的值不同。

- 错误响应率：此图提供了与此策略匹配的请求向客户端返回错误(HTTP状态代码>= 400)的大致速率。
- 平均请求持续时间(无错误)：此图形提供与此策略匹配的成功请求的平均持续时间。
- 策略带宽使用量：此图提供与所有负载平衡器处理的此策略匹配的带宽量。收到的数据包括所有请求的请求标头以及包含正文数据的响应的正文数据大小。Sent包括所有请求的响应标头以及响应中包含正文数据的请求的响应正文数据大小。

4. 将光标置于折线图上方、可查看该图特定部分上的值弹出窗口。
5. 选择指标标题下方的* Grafana DDashboard *以查看策略的所有图形。除了*Metrics *选项卡中的四个图形之外，您还可以查看另外两个图形：
   - Write Request Rate by object size：与此策略匹配的放置/后置/删除请求的速率。单个单元格上的定位显示每秒的速率。悬停视图中显示的速率会被截断为整数、如果存储分段中存在非零请求、则可能会报告0。
   - 按对象大小划分的读取请求速率：与此策略匹配的GET或HEAD请求的速率。单个单元格上的定位显示每秒的速率。悬停视图中显示的速率会被截断为整数、如果存储分段中存在非零请求、则可能会报告0。
6. 或者，也可以从 * 支持 * 菜单访问这些图形。
   a. 选择 * 支持 * > * 工具 * > * 指标 * 。
   b. 从* Grafana 部分选择*交通分类政策。
   c. 从页面左上角的菜单中选择策略。
   d. 将光标置于图形上方可查看一个弹出窗口、其中显示了样本的日期和时间、汇总到计数中的对象大小以及该时间段内每秒的请求数。

      流量分类策略通过其 ID 进行标识。策略ID将在"流量分类策略"页面上列出。
7. 分析图形以确定策略限制流量的频率以及是否需要调整策略。

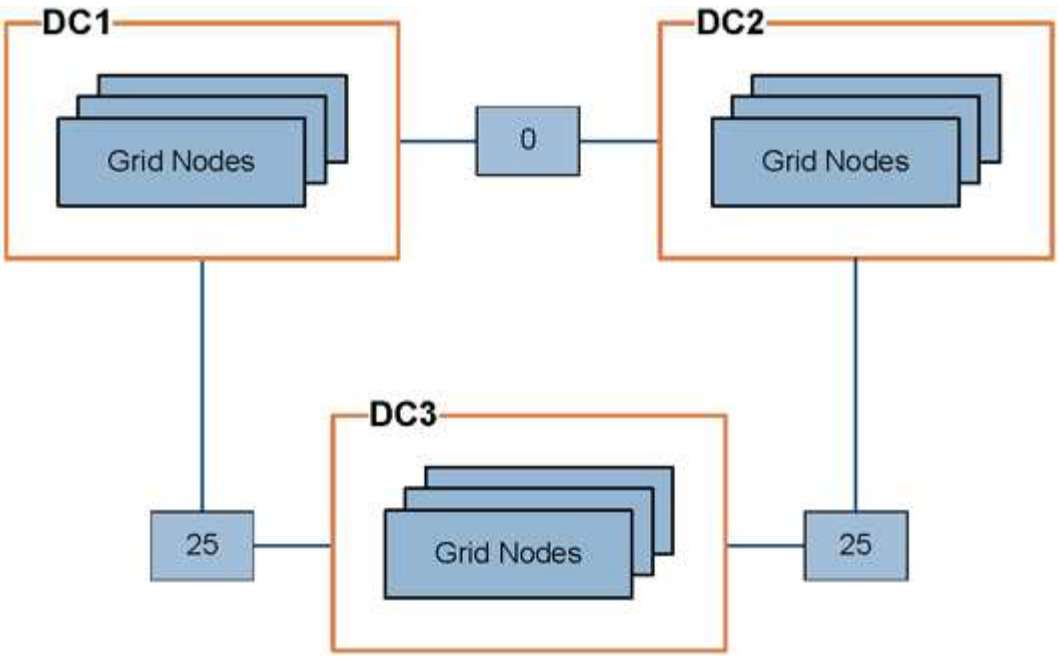
管理链路成本

链路成本可用于确定存在两个或更多数据中心站点时哪个数据中心站点提供请求的服务的优先级。您可以调整链路成本以反映站点之间的延迟。

什么是链路成本？

- 链接成本用于确定用于实现对象检索的对象副本的优先级。
- 网格管理 API 和租户管理 API 使用链路成本来确定要使用的内部 StorageGRID 服务。
- 管理节点和网关节点上的负载平衡器服务使用链路开销来指导客户端连接。请参见 "负载平衡注意事项"。

此图显示了一个三站点网格，其中在站点之间配置了链路成本：



- 管理节点和网关节点上的负载平衡器服务会将客户端连接平均分布到同一数据中心站点上的所有存储节点以及链路成本为0的任何数据中心站点。

  在此示例中，数据中心站点 1 （ DC1 ）的网关节点会将客户端连接平均分布到 DC1 的存储节点和 DC2 的存储节点。DC3 上的网关节点仅向 DC3 上的存储节点发送客户端连接。

- 在检索作为多个复制副本存在的对象时， StorageGRID 会在链路成本最低的数据中心检索此副本。

  在此示例中、如果DC2的客户端应用程序检索到同时存储在DC1和DC3的对象、则会从DC1检索该对象、因为从DC1到DC2的链路成本为0、低于从DC3到DC2的链路成本(25)。

链路成本是任意的相对数字，没有特定的度量单位。例如，使用链路成本 50 比使用链路成本 25 更低。下表显示了常用链路成本。

链接。	链路成本	注释：
物理数据中心站点之间	25 （默认）	通过 WAN 链路连接的数据中心。
位于同一物理位置的逻辑数据中心站点之间	0	逻辑数据中心位于通过 LAN 连接的同一物理建筑或园区中。

更新链路成本

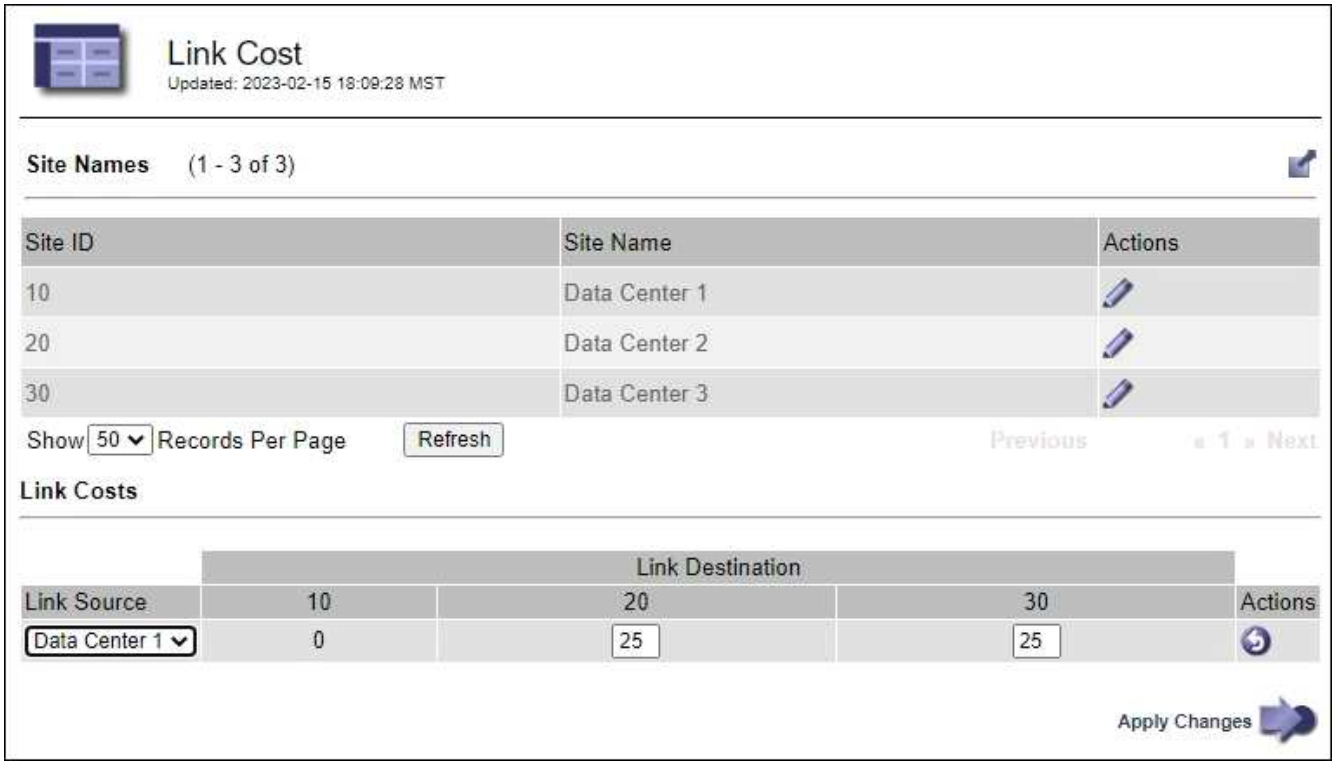
您可以更新数据中心站点之间的链路成本，以反映站点之间的延迟。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您拥有 "网格拓扑页面配置权限"。

步骤

1. 选择*support*>*other *>*Link cost *。



2. 在 * 链路源 * 下选择一个站点，然后在 * 链路目标 * 下输入一个介于 0 和 100 之间的成本值。

   如果源与目标相同、则无法更改链接成本。

   要取消更改，请选择 * 还原 * 。

3. 选择 * 应用更改 * 。

使用 AutoSupport

使用AutoSupport： 概述

通过 AutoSupport 功能， StorageGRID 系统可以向技术支持发送运行状况和状态消息。

使用 AutoSupport 可以显著加快问题的确定和解决速度。技术支持还可以监控系统的存储需求，并帮助您确定是否需要添加新节点或站点。您也可以将 AutoSupport 消息配置为发送到另一个目标。

您应仅在主管理节点上配置StorageGRID AutoSupport。但是、您必须配置 Hardware AutoSupport (硬件配置) 在每个设备上。

AutoSupport 消息中包含的信息

AutoSupport 消息包含如下信息：

- StorageGRID 软件版本
- 操作系统版本

- 系统级别和位置级别属性信息
- 近期警报和警报（旧系统）
- 所有网格任务的当前状态，包括历史数据
- 管理节点数据库使用情况
- 丢失或缺失对象的数量
- 网格配置设置
- NMS 实体
- 活动 ILM 策略
- 已配置网格规范文件
- 诊断指标

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

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

什么是 **Active IQ** ？

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

如果要在NetApp 支持站点 上使用Active IQ 信息板和功能、则必须启用AutoSupport。

"Active IQ Digital Advisor 文档"

用于发送 **AutoSupport** 消息的协议

您可以选择以下三种协议之一来发送 AutoSupport 消息：

- HTTPS
- HTTP
- SMTP

如果使用 SMTP 作为 AutoSupport 消息的协议，则必须配置 SMTP 邮件服务器。

AutoSupport 选项

您可以使用以下选项的任意组合向技术支持发送 AutoSupport 消息：

- * 每周 *：每周自动发送一次 AutoSupport 消息。默认设置： enabled 。

- * 事件触发 * ： 每小时或发生重大系统事件时自动发送 AutoSupport 消息。默认设置： enabled 。
- * 按需 * ： 允许技术支持请求您的 StorageGRID 系统自动发送 AutoSupport 消息，这在他们正在使用问题描述 （需要 HTTPS AutoSupport 传输协议）时非常有用。默认设置： disabled 。
- * 用户触发 * ： 随时手动发送 AutoSupport 消息。

适用于设备的**AutoSupport**

适用于设备的AutoSupport 报告StorageGRID 硬件问题、而StorageGRID AutoSupport 报告StorageGRID 软件问题(SGF6112除外、其中StorageGRID AutoSupport 同时报告硬件和软件问题)。您必须在每个设备上配置AutoSupport 、但SGF6112除外、它不需要额外配置。对于服务和存储设备、AutoSupport 的实施方式有所不同。

您必须在SANtricity 中为每个存储设备启用AutoSupport。您可以在初始设备设置期间或安装设备后配置SANtricity AutoSupport ：

- 对于SG6000和SG5700设备、 "在SANtricity 系统管理器中配置AutoSupport"

如果您在中配置了通过代理传送AutoSupport 、则可以将来自E系列设备的AutoSupport 消息包含在StorageGRID AutoSupport 中 "SANtricity 系统管理器"。

StorageGRID AutoSupport 不会报告硬件问题、例如DIMM或主机接口卡(Host Interface Card、HIC)故障。但是、某些组件可能会触发故障 "硬件警报"。对于带有底板管理控制器(BMC)的StorageGRID 设备、例如SG100、SG1000、SG6060或SGF6024、您可以配置电子邮件和SNMP陷阱来报告硬件故障：

- "为警报设置电子邮件通知"
- "配置SNMP设置" 对于SG6000-CN控制器或SG100和SG1000服务设备

相关信息

"NetApp 支持"

配置 AutoSupport

您可以在首次安装 StorageGRID 时启用 AutoSupport 功能和各个 AutoSupport 选项，也可以稍后启用它们。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限或其他网格配置权限。
- 如果您要使用HTTPS发送AutoSupport 消息、则表示您已直接或提供了对主管理节点的出站Internet访问 "使用代理服务器" (不需要入站连接)。
- 如果在"HTTPS"页面上选择了StorageGRID AutoSupport 、则表示您已将代理服务器配置为以HTTPS形式转发AutoSupport 消息。NetApp的AutoSupport 服务器将拒绝使用HTTP发送的消息。

  "了解如何配置管理代理设置"。

- 如果要使用 SMTP 作为 AutoSupport 消息的协议，则表示已配置 SMTP 邮件服务器。警报电子邮件通知使用相同的邮件服务器配置（旧系统）。

指定 **AutoSupport** 消息的协议

您可以使用以下任一协议发送 AutoSupport 消息：

- * HTTPS ： 这是新安装的默认和建议设置。此协议使用端口443。如果您要 … 启用AutoSupport On Demand功能，则必须使用HTTPS。
- **HTTPS**：如果选择HTTP，则必须将代理服务器配置为以HTTPS形式转发AutoSupport 消息。NetApp的AutoSupport 服务器会拒绝使用HTTP发送的消息。此协议使用端口80。
- * SMTP ： 如果要通过电子邮件发送 AutoSupport 消息，请使用此选项。如果使用 SMTP 作为 AutoSupport 消息的协议，则必须在 " 旧电子邮件设置 " 页面上配置 SMTP 邮件服务器（ * 支持 * > * 警报（旧） * > * 旧电子邮件设置 * ）。

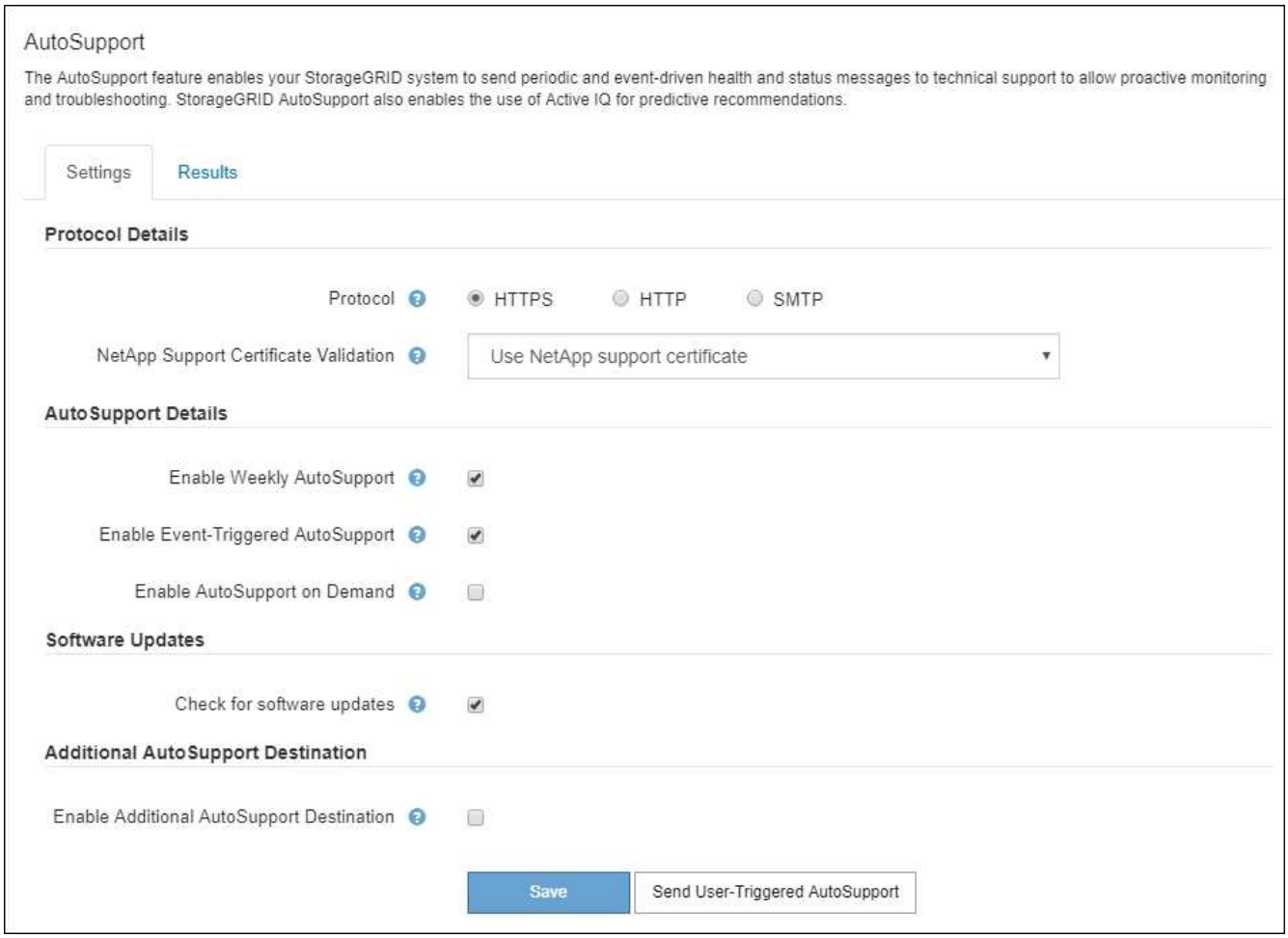
> 在 StorageGRID 11.2 版本之前， SMTP 是唯一可用于 AutoSupport 消息的协议。如果您最初安装的是早期版本的 StorageGRID ，则可能选择了 SMTP 协议。

您设置的协议用于发送所有类型的 AutoSupport 消息。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。

   此时将显示 AutoSupport 页面，并选择 * 设置 * 选项卡。



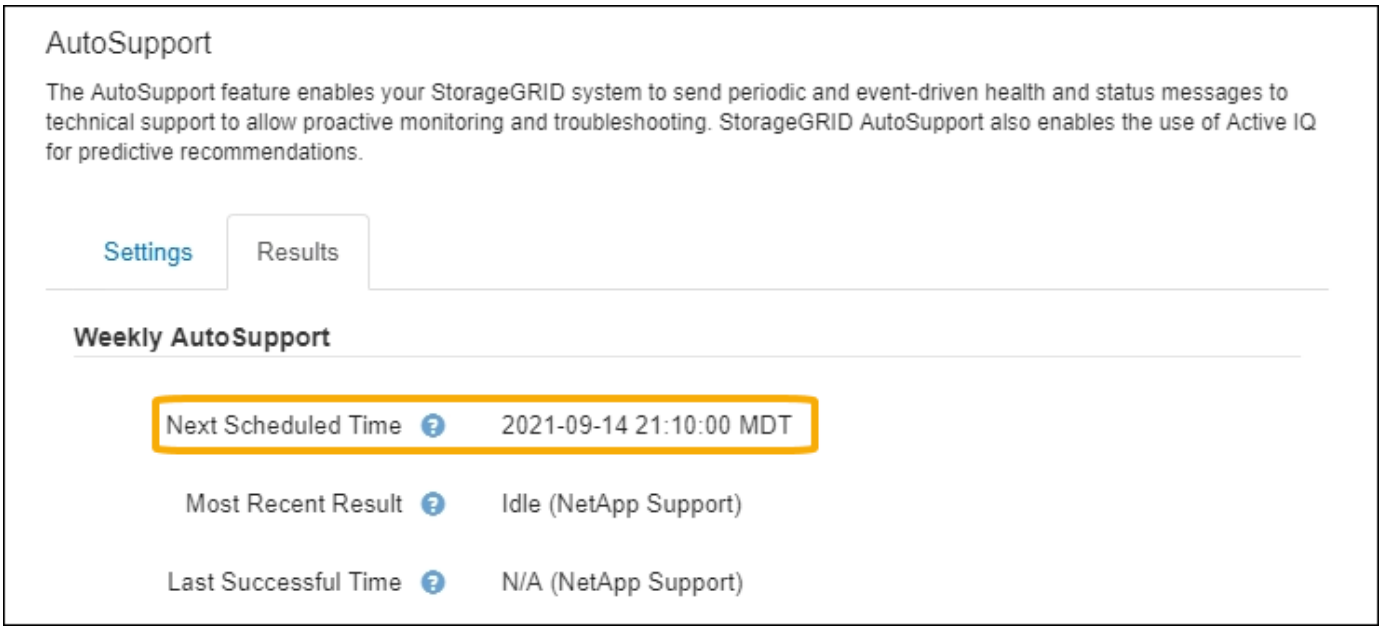
2. 选择要用于发送 AutoSupport 消息的协议。
3. 如果选择了 * HTTPS * ，请选择是否使用 TLS 证书来保护与 NetApp 支持服务器的连接。
   - * 使用 NetApp 支持证书 * （默认）： 证书验证可确保 AutoSupport 消息的传输安全。NetApp 支持证书已随 StorageGRID 软件一起安装。
   - * 不验证证书 * ： 只有当您有充分理由不使用证书验证时，例如证书出现临时问题时，才选择此选项。
4. 选择 * 保存 * 。

   所有每周消息，用户触发的消息和事件触发的消息均使用选定协议发送。

禁用每周 **AutoSupport** 消息

默认情况下， StorageGRID 系统配置为每周向 NetApp 支持发送一次 AutoSupport 消息。

要确定每周 AutoSupport 消息的发送时间，请转到 * AutoSupport * > * 结果 * 选项卡。在 * 每周 AutoSupport * 部分中，查看 * 下一计划时间 * 的值。



您可以随时禁止自动发送每周 AutoSupport 消息。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 清除*启用每周AutoSupport *复选框。
3. 选择 * 保存 * 。

禁用事件触发的 **AutoSupport** 消息

默认情况下， StorageGRID 系统配置为在发生重要警报或其他重要系统事件时向 NetApp 支持发送 AutoSupport 消息。

您可以随时禁用事件触发的 AutoSupport 消息。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 清除*启用事件触发的AutoSupport *复选框。
3. 选择 * 保存 * 。

启用 **AutoSupport On Demand**

AutoSupport On Demand 可帮助解决技术支持正在积极处理的问题。

默认情况下， AutoSupport On Demand 处于禁用状态。启用此功能后，技术支持可以请求 StorageGRID 系统自动发送 AutoSupport 消息。技术支持还可以为 AutoSupport On Demand 查询设置轮询时间间隔。

技术支持无法启用或禁用AutoSupport On Demand。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 为协议选择 * HTTPS * 。
3. 选中*启用每周AutoSupport *复选框。
4. 选中*启用AutoSupport On Demand*复选框。
5. 选择 * 保存 * 。

   已启用 AutoSupport On Demand ，技术支持可以将 AutoSupport On Demand 请求发送到 StorageGRID 。

禁用软件更新检查

默认情况下， StorageGRID 会联系 NetApp 以确定您的系统是否有可用的软件更新。如果提供了 StorageGRID 修补程序或新版本，则新版本将显示在 StorageGRID 升级页面上。

根据需要，您可以选择禁用软件更新检查。例如，如果您的系统无法访问 WAN ，则应禁用此检查以避免下载错误。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 清除*检查软件更新*复选框。
3. 选择 * 保存 * 。

添加其他 **AutoSupport** 目标

启用AutoSupport 后、运行状况和状态消息将发送给NetApp支持部门。您可以为所有 AutoSupport 消息指定一个其他目标。

要验证或更改用于发送 AutoSupport 消息的协议，请参见中的说明 指定 AutoSupport 消息的协议。

> 您不能使用SMTP协议将AutoSupport 消息发送到其他目标。

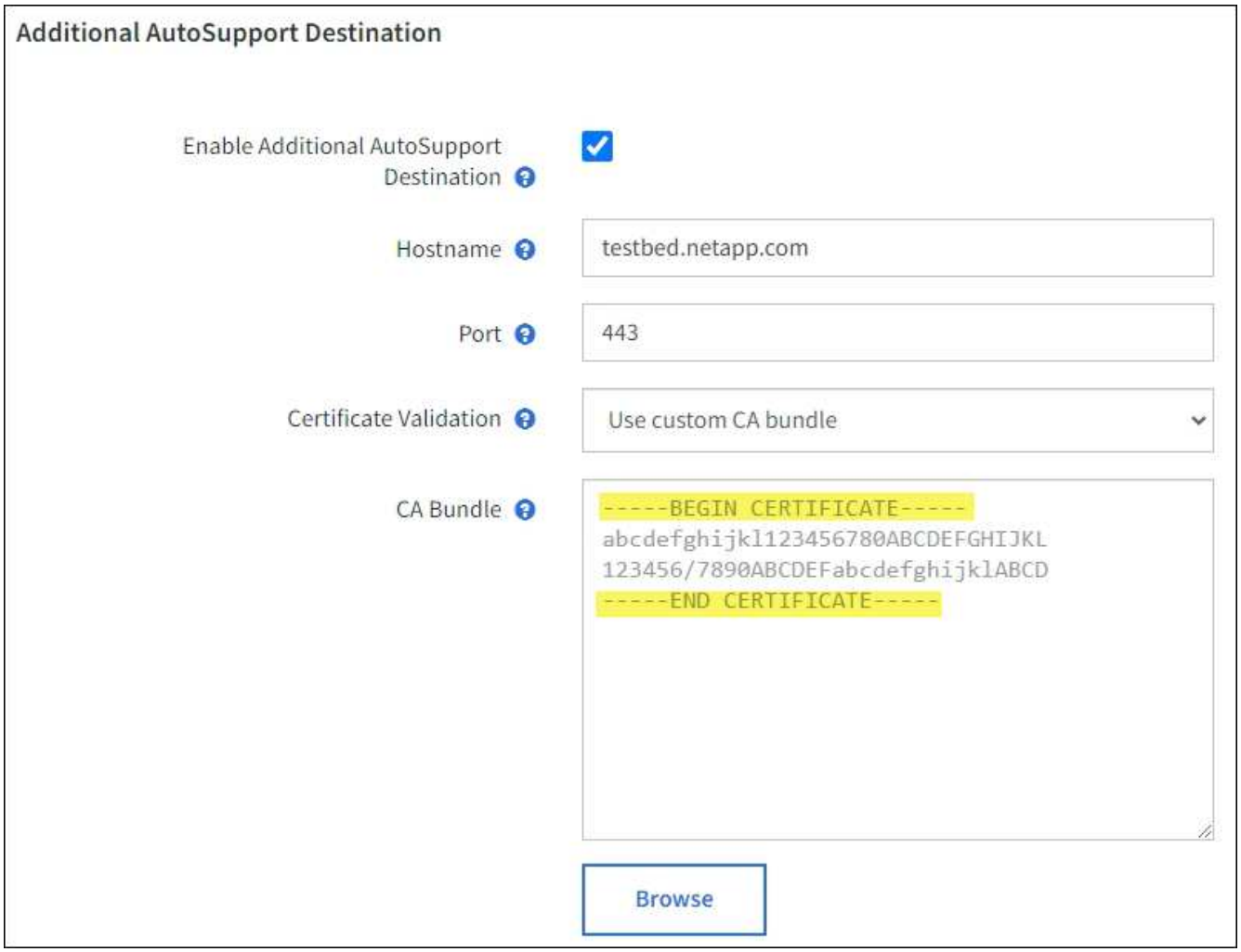
步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 选择*启用其他AutoSupport 目标*。
3. 指定以下内容：

字段	**Description**
主机名	附加AutoSupport 目标服务器的服务器主机名或IP地址。 注:只能输入一个附加目的地。
Port	用于连接到其他AutoSupport 目标服务器的端口。对于HTTP、默认为端口80；对于HTTPS、默认为端口443。
认证验证	是否使用TLS证书来保护与其他目标的连接。 • 选择*不验证证书*发送AutoSupport 消息而不验证证书。 只有当您有充分的理由不使用证书验证时，例如证书出现临时问题时，才选择此选项。 • 选择*使用自定义CA包*以使用证书验证。

4. 如果选择了*使用自定义CA包*，请执行以下操作之一：
   - 选择 * 浏览 * ，导航到包含证书的文件，然后选择 * 打开 * 上传文件。
   - 使用编辑工具将PEM编码的每个CA证书文件的所有内容复制并粘贴到按证书链顺序连接的*CA Bundle*字段中。

     您必须包括 `----BEGIN CERTIFICATE----` 和 `----END CERTIFICATE----` 您选择的内容。



5. 选择 * 保存 * 。

   未来所有每周，事件触发和用户触发的 AutoSupport 消息都将发送到其他目标。

手动触发 **AutoSupport** 消息

为了帮助技术支持解决 StorageGRID 系统的问题，您可以手动触发要发送的 AutoSupport 消息。

开始之前

- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您必须具有root访问权限或其他网格配置权限。

步骤

1. 选择 * 支持 * > * 工具 * > * AutoSupport * 。
2. 在*设置*选项卡上，选择*发送用户触发的AutoSupport *。

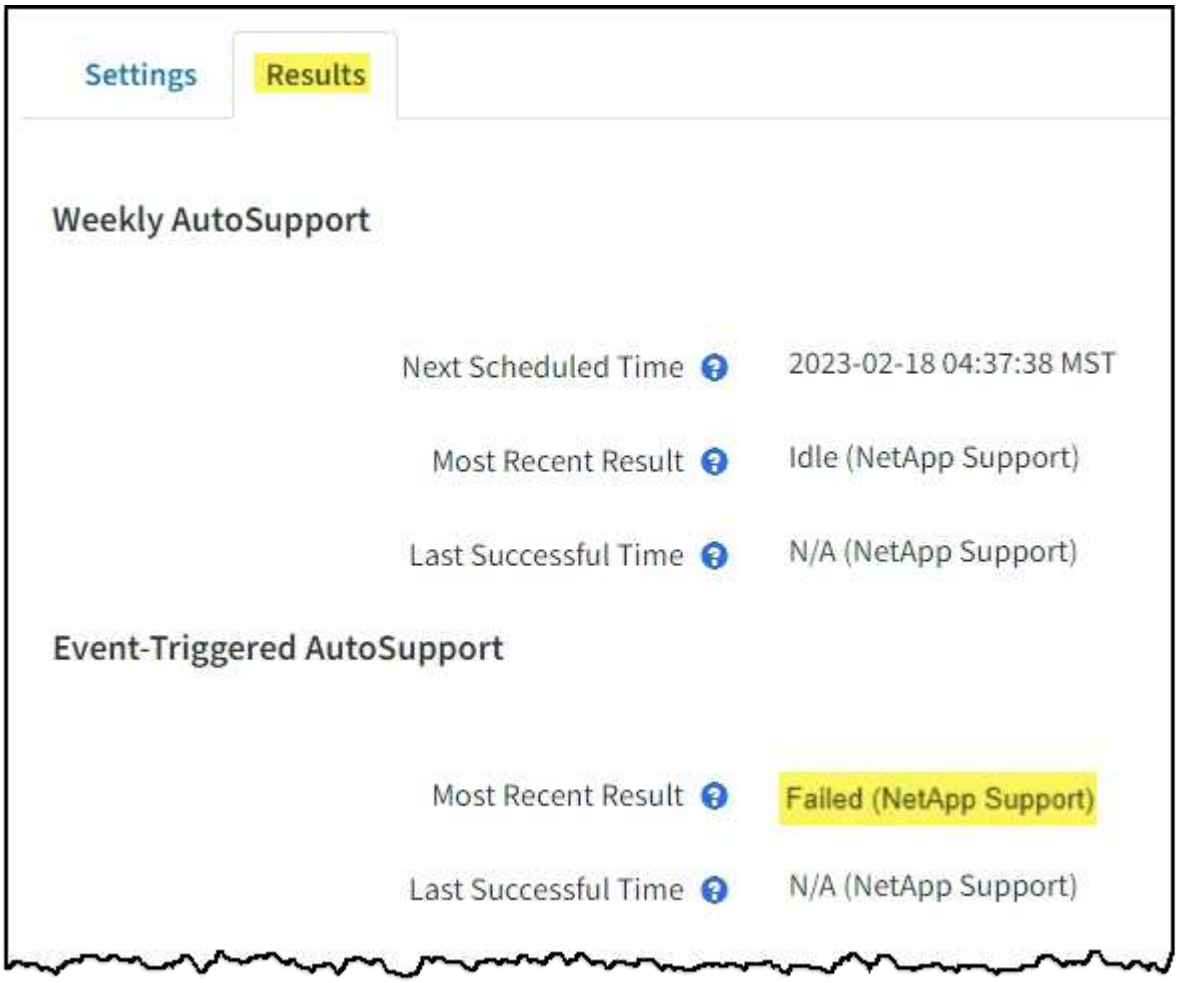
   StorageGRID 尝试向技术支持发送 AutoSupport 消息。如果尝试成功，则会更新 * 结果 * 选项卡上的 * 最新结果 * 和 * 最后成功时间 * 值。如果出现问题， * 最新结果 * 值将更新为 " 失败 " ， StorageGRID 不会再尝试发送 AutoSupport 消息。

发送用户触发的 AutoSupport 消息后，请在 1 分钟后刷新浏览器中的 AutoSupport 页面以访问最新结果。

对 **AutoSupport** 消息进行故障排除

如果尝试发送 AutoSupport 消息失败， StorageGRID 系统将根据 AutoSupport 消息的类型采取不同的操作。您可以通过选择 * 支持 * > * 工具 * > * AutoSupport * > * 结果 * 来检查 AutoSupport 消息的状态。

如果 AutoSupport 消息无法发送，则 "`failed` " 将显示在 * AutoSupport * 页面的 * 结果 * 选项卡上。



如果您配置了代理服务器以将AutoSupport消息转发到NetApp、则应这样做 "验证代理服务器配置设置是否正确"。

每周 **AutoSupport** 消息失败

如果每周 AutoSupport 消息无法发送， StorageGRID 系统将执行以下操作：

1. 更新最新的 result 属性以重试。
2. 尝试每四分钟重新发送 15 次 AutoSupport 消息，持续一小时。

3. 发送失败一小时后，将最新结果属性更新为 Failed 。
4. 尝试在下次计划的时间重新发送 AutoSupport 消息。
5. 如果消息因 NMS 服务不可用而失败，并且消息在七天之前发送，则会保留常规 AutoSupport 计划。
6. 当 NMS 服务再次可用时，如果消息在七天或更长时间内未发送，则会立即发送 AutoSupport 消息。

用户触发或事件触发的 **AutoSupport** 消息失败

如果用户触发或事件触发的 AutoSupport 消息无法发送， StorageGRID 系统将执行以下操作：

1. 如果已知错误，则显示错误消息。例如、如果用户在选择SMTP协议时未提供正确的电子邮件配置设置、则会显示以下错误： `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. 不会再次尝试发送消息。
3. 将此错误记录在中 `nms.log`。

如果发生故障且所选协议为 SMTP ，请验证 StorageGRID 系统的电子邮件服务器是否已正确配置且电子邮件服务器是否正在运行（ * 支持 * > * 警报（原有） * > * > 旧电子邮件设置 * ）。AutoSupport 页面可能会显示以下错误消息： `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

了解操作方法 "配置电子邮件服务器设置"。

更正 **AutoSupport** 消息故障

如果发生故障且所选协议为 SMTP ，请验证 StorageGRID 系统的电子邮件服务器是否已正确配置且您的电子邮件服务器是否正在运行。AutoSupport 页面可能会显示以下错误消息： `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

通过 **StorageGRID** 发送 **E** 系列 **AutoSupport** 消息

您可以通过 StorageGRID 管理节点而不是存储设备管理端口向技术支持发送 E 系列 SANtricity System Manager AutoSupport 消息。

请参见 "E系列硬件AutoSupport" 有关将AutoSupport 与E系列设备结合使用的详细信息、请参见。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有存储设备管理员权限或root访问权限。
- 您已配置SANtricity AutoSupport：
  - 对于SG6000和SG5700设备、 "在SANtricity 系统管理器中配置AutoSupport"

> 要使用网格管理器访问 SANtricity 系统管理器，您必须具有 SANtricity 固件 8.70 或更高版本。

关于此任务

E 系列 AutoSupport 消息包含存储硬件的详细信息，比 StorageGRID 系统发送的其他 AutoSupport 消息更具体。

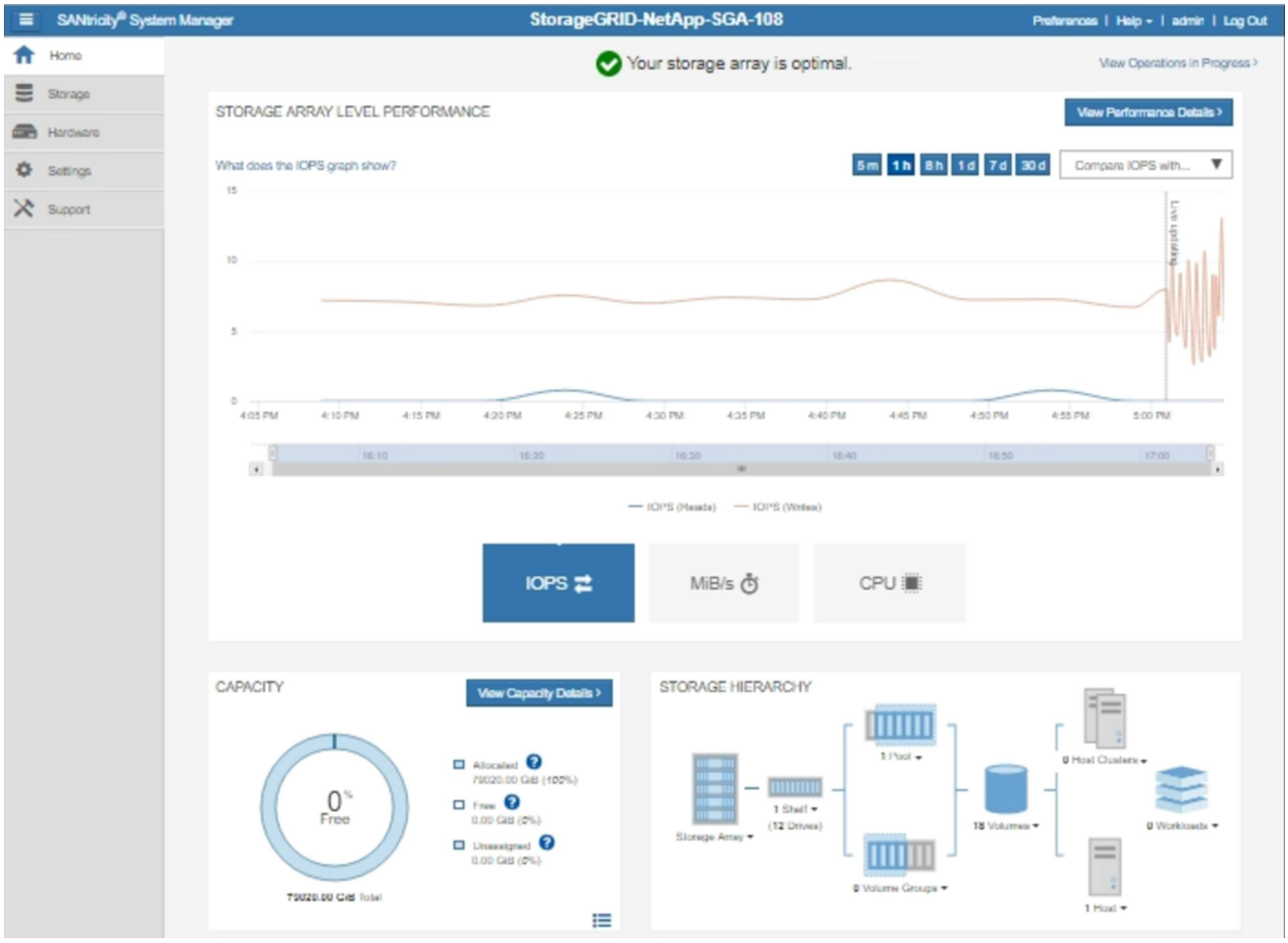
您可以在SANtricity 系统管理器中配置一个特殊的代理服务器地址、以便在不使用设备管理端口的情况下通过StorageGRID 管理节点传输AutoSupport 消息。以这种方式传输的AutoSupport 消息由发送 "首选发件人管理节点"他们使用任何 "管理代理设置" 已在网格管理器中配置。

> 此操作步骤 仅用于为 E 系列 AutoSupport 消息配置 StorageGRID 代理服务器。有关 E 系列 AutoSupport 配置的更多详细信息，请参见 "NetApp E 系列和 SANtricity 文档"。

步骤

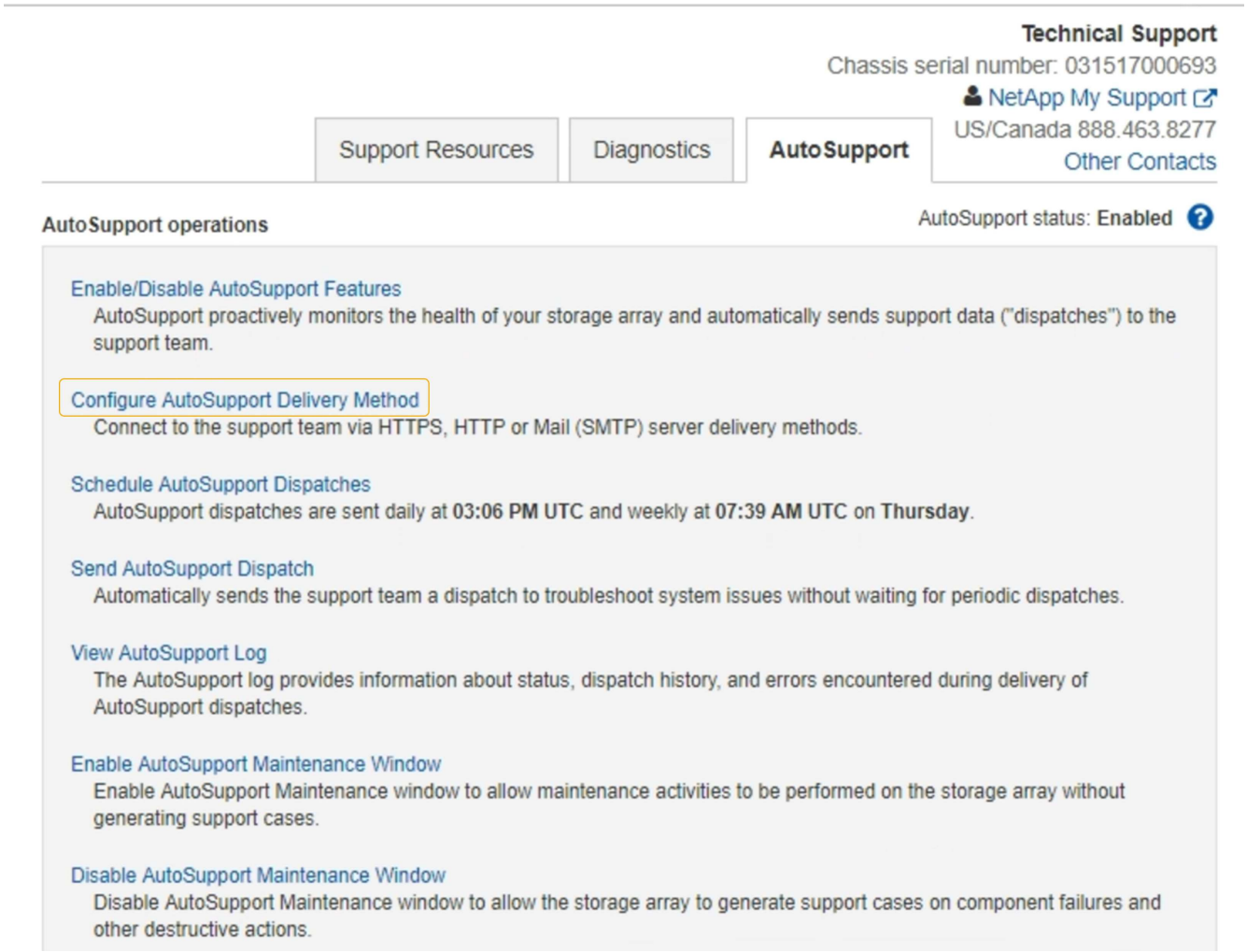
1. 在网格管理器中，选择 * 节点 * 。
2. 从左侧的节点列表中，选择要配置的存储设备节点。
3. 选择 * SANtricity 系统管理器 * 。

   此时将显示 SANtricity System Manager 主页。



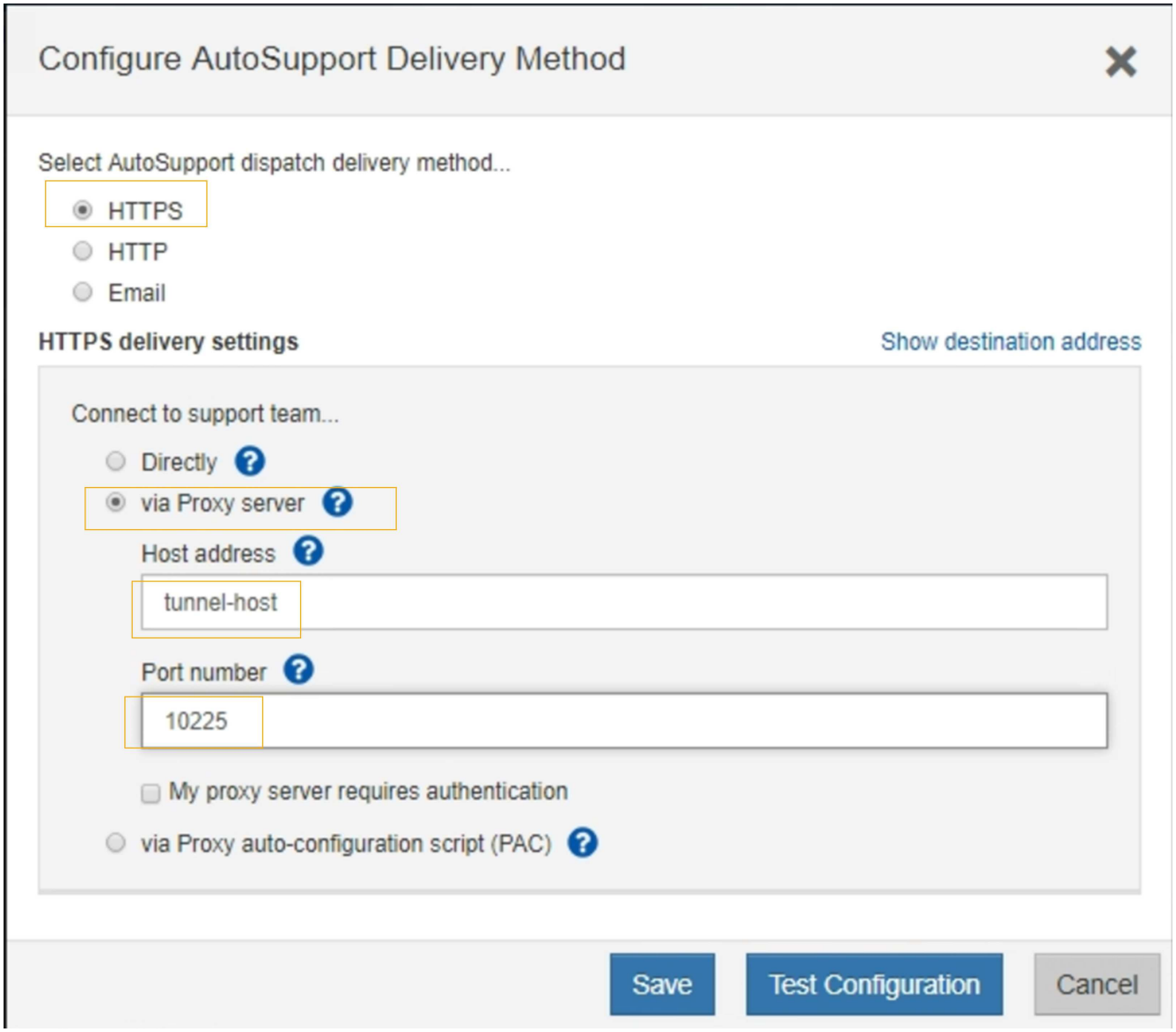
4. 选择 * 支持 * > * 支持中心 * > * AutoSupport * 。

   此时将显示 AutoSupport 操作页面。



5. 选择 * 配置 AutoSupport 交付方法 * 。

   此时将显示配置 AutoSupport 交付方法页面。



6. 选择 * HTTPS * 作为传送方法。

   已预安装启用HTTPS的证书。

7. 选择 * 通过代理服务器 * 。
8. 输入 … `tunnel-host` 用于*主机地址*。

   `tunnel-host` 是使用管理节点发送E系列AutoSupport 消息的特殊地址。

9. 输入 … `10225` 端口号*。

   `10225` 是StorageGRID 代理服务器上从设备中的E系列控制器接收AutoSupport 消息的端口号。

10. 选择 * 测试配置 * 以测试 AutoSupport 代理服务器的路由和配置。

    如果正确，则绿色横幅中会显示一条消息： "`您的 AutoSupport 配置已验证。` "

    如果测试失败，则会在红色横幅中显示一条错误消息。检查StorageGRID DNS设置和网络、确保 "首选发件

人管理节点" 可以连接到NetApp 支持站点 、然后重试测试。

11. 选择 * 保存 * 。

    此时将保存此配置，并显示一条确认消息： "`AutoSupport delivery method has been configured 。` "

管理存储节点

管理存储节点：概述

存储节点可提供磁盘存储容量和服务。管理存储节点需要执行以下操作：

- 管理存储选项
- 了解什么是存储卷水印，以及如何使用水印覆盖来控制存储节点何时变为只读
- 监控和管理用于对象元数据的空间
- 为已存储对象配置全局设置
- 正在应用存储节点配置设置
- 管理完整存储节点

什么是存储节点？

存储节点可管理和存储对象数据和元数据。每个 StorageGRID 系统必须至少具有三个存储节点。如果您有多个站点，则 StorageGRID 系统中的每个站点也必须有三个存储节点。

存储节点包括在磁盘上存储，移动，验证和检索对象数据和元数据所需的服务和进程。您可以在 * 节点 * 页面上查看有关存储节点的详细信息。

什么是模数转换器服务？

管理域控制器（ADC-A）服务对网格节点及其彼此连接进行身份验证。一个站点的前三个存储节点中的每个存储节点都托管了此类模块转换服务。

此 ADA 服务可维护拓扑信息，包括服务的位置和可用性。当网格节点需要来自另一个网格节点的信息或由另一个网格节点执行操作时，它会联系一个模数转换器服务来查找处理其请求的最佳网格节点。此外，该 StorageGRID 服务还会保留一份部署配置包的副本，以便任何网格节点都可以检索当前配置信息。您可以在网格拓扑页面（ * 支持 * > * 网格拓扑 * ）上查看存储节点的数据转换信息。

为了便于分布式和孤岛式操作，每个 StorageGRID 服务会将证书，配置包以及有关服务和拓扑的信息与系统中的其他 ADE 服务进行同步。

通常，所有网格节点都会至少与一个 ADC 服务保持连接。这样可以确保网格节点始终访问最新信息。当网格节点连接时，它们会缓存其他网格节点的` 证书，从而使系统能够继续使用已知网格节点运行，即使某个模数转换器服务不可用也是如此。新的网格节点只能通过使用模数转换器服务建立连接。

通过每个网格节点的连接，可以使此 ADA 服务收集拓扑信息。此网格节点信息包括 CPU 负载，可用磁盘空间（如果有存储），支持的服务以及网格节点的站点 ID 。其他服务则通过拓扑查询向此类服务请求拓扑信息。对于从 StorageGRID 系统收到的最新信息，此 ADA 服务会对每个查询做出响应。

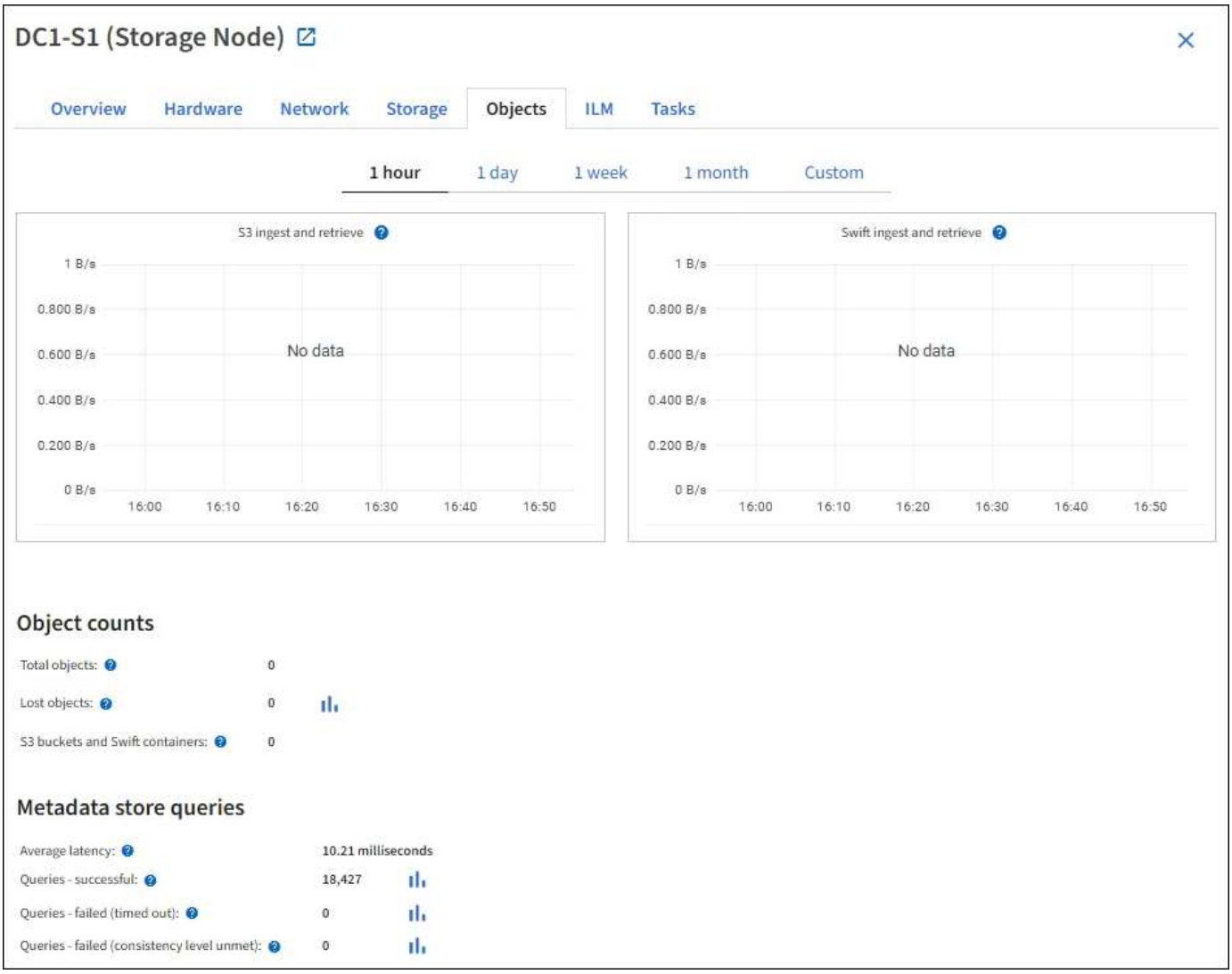
什么是 **DDS** 服务？

分布式数据存储（ DDS ）服务由存储节点托管，它与 Cassandra 数据库建立接口，以便对存储在 StorageGRID 系统中的对象元数据执行后台任务。

对象计数

DDS 服务可跟踪载入到 StorageGRID 系统中的对象总数，以及通过每个系统支持的接口（ S3 或 Swift ）载入的对象总数。

您可以在任何存储节点的 "Nodes" 页面 >"Object" 选项卡上查看对象总数。



查询

您可以确定通过特定 DDS 服务对元数据存储运行查询所需的平均时间，成功查询的总数以及因问题描述 超时而失败的查询总数。

您可能希望查看查询信息以监控元数据存储 Cassandra 的运行状况，这会影响系统的载入和检索性能。例如，如果平均查询的延迟较慢，并且因超时而导致查询失败的次数较多，则元数据存储可能会遇到较高的负载或执行其他操作。

您还可以查看因一致性失败而失败的查询总数。通过特定 DDS 服务执行查询时，可用元数据存储数量不足，导

致一致性级别失败。

您可以使用诊断页面获取有关网格当前状态的追加信息。请参见 "Run diagnostics"。

一致性保证和控制

StorageGRID 保证新创建的对象的写入后读一致性。成功完成 PUT 操作后的任何 GET 操作都将能够读取新写入的数据。现有对象的覆盖，元数据更新和删除操作最终保持一致。

什么是 **LDR** 服务?

本地分发路由器（ LDR ）服务由每个存储节点托管，负责处理 StorageGRID 系统的内容传输。内容传输包含许多任务，包括数据存储，路由和请求处理。LDR服务通过处理数据传输负载和数据流量功能来完成StorageGRID 系统的大部分艰苦工作。

LDR 服务可处理以下任务：

- 查询
- 信息生命周期管理（ ILM ）活动
- 对象删除
- 对象数据存储
- 从其他 LDR 服务（存储节点）传输对象数据
- 数据存储管理
- 协议接口（ S3 和 Swift ）

此外， LDR 服务还可管理 S3 和 Swift 对象到 StorageGRID 系统为每个载入对象分配的唯一 "`content handles` " （ UUID ）的映射。

查询

LDR 查询包括在检索和归档操作期间查询对象位置。您可以确定运行查询所需的平均时间，成功查询的总数以及因超时问题描述 而失败的查询总数。

您可以查看查询信息以监控元数据存储的运行状况，这会影响系统的载入和检索性能。例如，如果平均查询的延迟较慢，并且因超时而导致查询失败的次数较多，则元数据存储可能会遇到较高的负载或执行其他操作。

您还可以查看因一致性失败而失败的查询总数。通过特定 LDR 服务执行查询时，可用元数据存储数量不足会导致一致性级别失败。

您可以使用诊断页面获取有关网格当前状态的追加信息。请参见 "Run diagnostics"。

ILM 活动

通过信息生命周期管理（ ILM ）指标，您可以监控对象在实施 ILM 时的评估速率。您可以在信息板或*节点*>*存储节点_*>* ILM中查看这些指标。

对象存储

LDR 服务的底层数据存储分为固定数量的对象存储（也称为存储卷）。每个对象存储都是一个单独的挂载点。

您可以在节点页面 > 存储选项卡上查看存储节点的对象存储。

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

存储在存储节点中的对象使用从 0000 到 002F 的十六进制数字进行标识，该数字称为卷 ID 。在第一个对象存储（卷 0 ）中预留空间用于 Cassandra 数据库中的对象元数据；该卷上的任何剩余空间用于对象数据。所有其他对象存储仅用于对象数据，其中包括复制的副本和经过纠删编码的片段。

为了确保复制的副本的空间使用量均匀，给定对象的对象数据会根据可用存储空间存储到一个对象存储中。当一个或多个对象存储填满容量时，其余对象存储将继续存储对象，直到存储节点上没有更多空间为止。

元数据保护

对象元数据是指与对象或对象的问题描述 相关的信息，例如对象修改时间或存储位置。StorageGRID 将对象元数据存储在与 LDR 服务连接的 Cassandra 数据库中。

为了确保冗余并防止丢失，每个站点维护三个对象元数据副本。此复制不可配置，并且会自动执行。

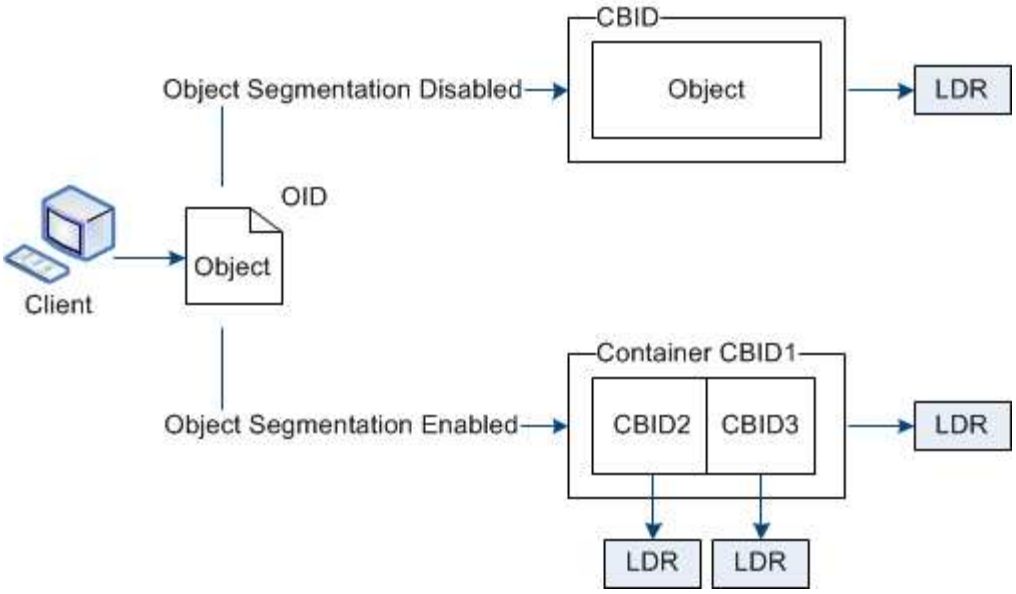
"管理对象元数据存储"

使用存储选项

什么是对象分段?

对象分段是指将对象拆分为一组大小固定的较小对象的过程、用于优化大型对象的存储和资源使用。S3 多部分上传还会创建分段对象，其中每个部分都有一个对象。

将对象载入 StorageGRID 系统后， LDR 服务会将该对象拆分为多个区块，并创建一个区块容器，其中会将所有区块的标题信息列为内容。



检索分段容器时， LDR 服务会从其分段中汇集原始对象并将该对象返回给客户端。

容器和区块不一定存储在同一个存储节点上。容器和分段可以存储在 ILM 规则中指定的存储池中的任何存储节点上。

StorageGRID 系统会单独处理每个区块，并计入受管对象和存储对象等属性的数量。例如，如果存储在 StorageGRID 系统中的对象拆分为两个区块，则在载入完成后，受管对象的值将增加三个，如下所示：

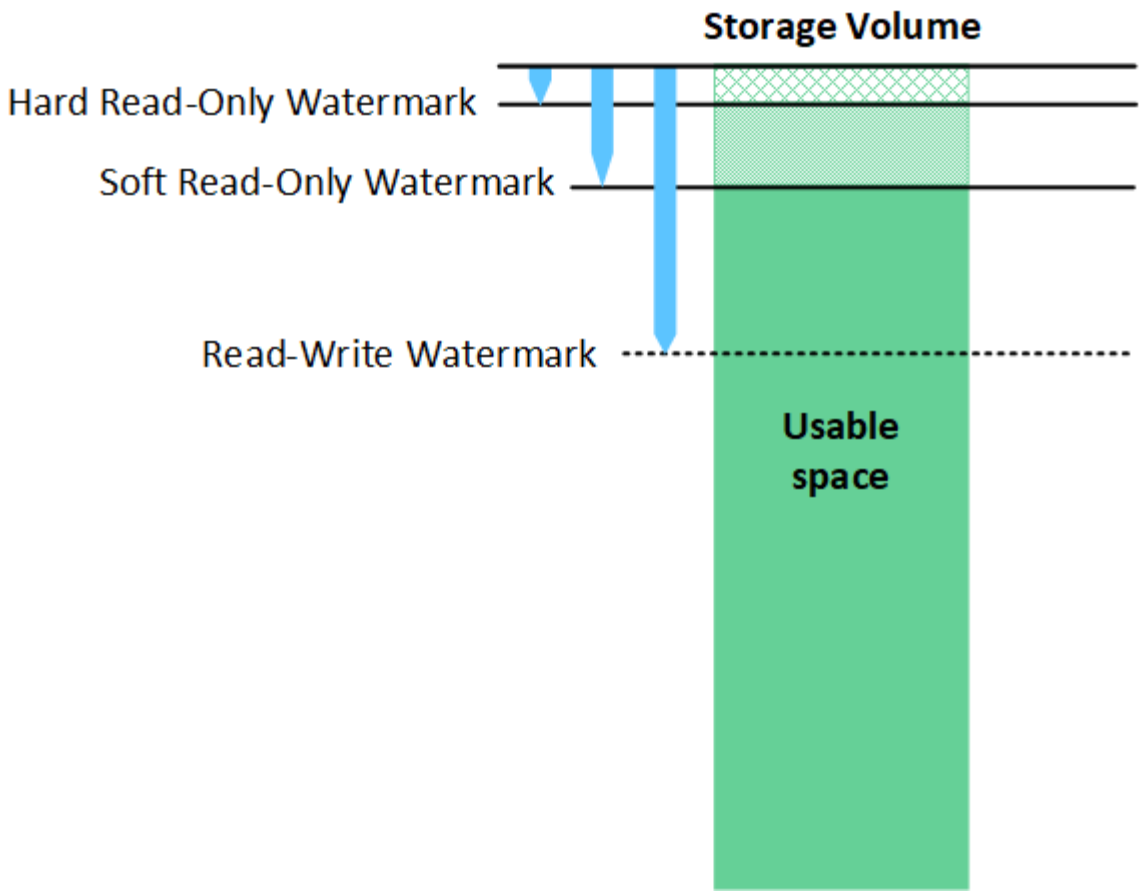
```
segment container + segment 1 + segment 2 = three stored objects
```

您可以通过确保以下各项来提高处理大型对象时的性能：

- 每个网关和存储节点都有足够的网络带宽来满足所需的吞吐量。例如，在 10 Gbps 以太网接口上配置单独的网格网络和客户端网络。
- 已部署足够多的网关和存储节点以满足所需的吞吐量。
- 每个存储节点都有足够的磁盘I/O性能来满足所需的吞吐量。

什么是存储卷水印？

StorageGRID 使用三个存储卷水印来确保存储节点在空间严重不足之前安全地过渡到只读状态，并允许已过渡到只读状态的存储节点再次变为读写状态。



存储卷水印仅适用于用于复制和擦除编码对象数据的空间。要了解为卷 0 上的对象元数据预留的空间，请转至"管理对象元数据存储"。

什么是软只读水印?

第一个水印是 * 存储卷软只读水印 * ，用于指示存储节点用于对象数据的可用空间正在变满。

如果存储节点中的每个卷的可用空间小于该卷的软只读水印，则存储节点将过渡到 _read-only mode" 。只读模式表示存储节点向 StorageGRID 系统的其余部分公布只读服务，但满足所有待处理的写入请求。

例如，假设存储节点中的每个卷都有一个 10 GB 的软只读水印。一旦每个卷的可用空间小于 10 GB ，存储节点就会过渡到软只读模式。

什么是硬只读水印?

下一个水印是 * 存储卷硬只读水印 * ，用于指示节点的对象数据可用空间正在变满。

如果卷上的可用空间小于该卷的硬只读水印，则写入该卷将失败。但是，可以继续向其他卷写入数据，直到这些卷上的可用空间小于其硬只读水印为止。

例如，假设存储节点中的每个卷都有一个 5 GB 的硬只读水印。一旦每个卷的可用空间小于 5 GB ，存储节点就不再接受任何写入请求。

硬只读水印始终小于软只读水印。

什么是读写水印?

- 存储卷读写水印 * 仅适用于已过渡到只读模式的适用场景 存储节点。它可确定节点何时可以重新变为读写状态。如果存储节点中任一存储卷上的可用空间大于该卷的读写水印，则该节点会自动过渡回读写状态。

例如，假设存储节点已过渡到只读模式。另外，假设每个卷都有一个读写水印 30 GB 。任何卷的可用空间增加到 30 GB 后，节点将再次变为读写状态。

读写水印始终大于软只读水印和硬只读水印。

查看存储卷水印

您可以查看当前水印设置和系统优化的值。如果未使用优化水印、您可以确定是否可以或应该调整设置。

开始之前

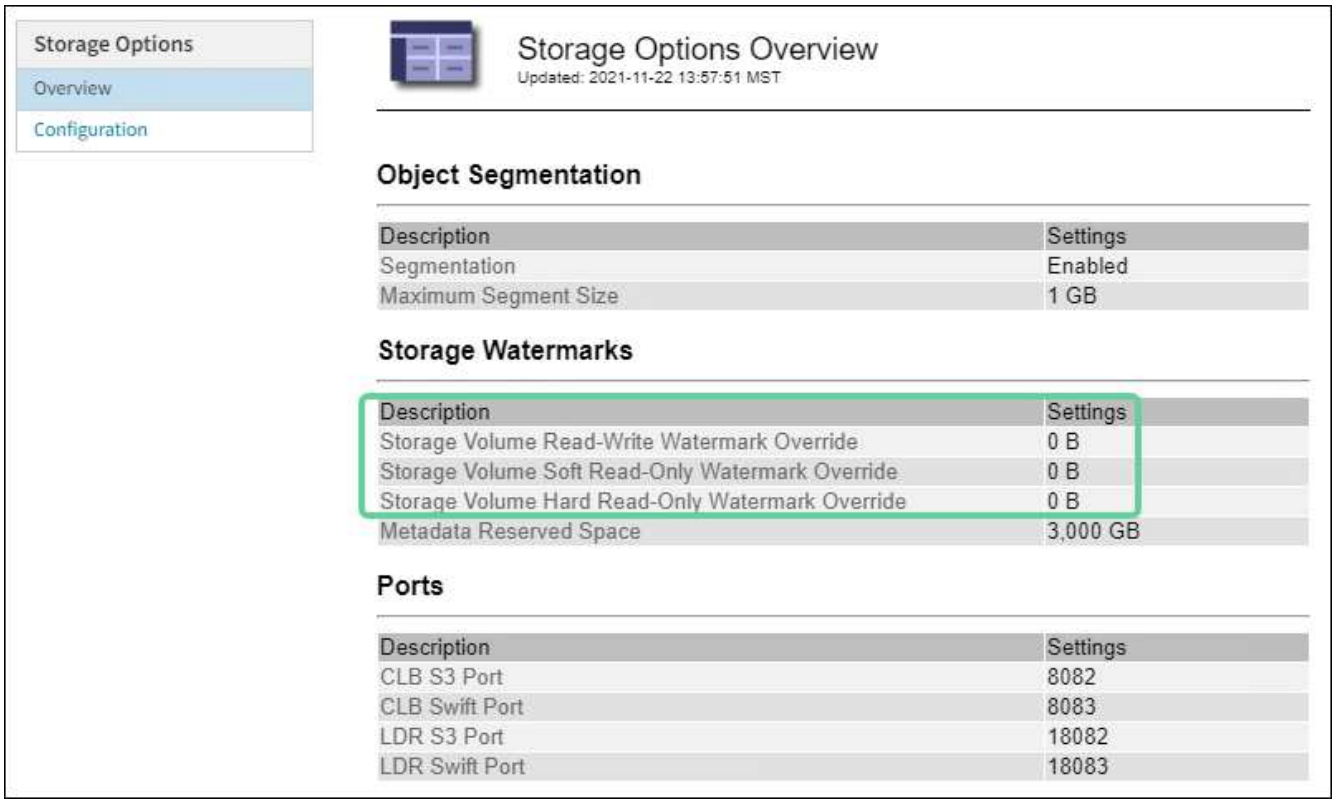
- 您已完成StorageGRID 11.6或更高版本的升级。
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有 root 访问权限。

查看当前水印设置

您可以在网格管理器中查看当前存储水印设置。

步骤

1. 选择 * 配置 * > * 系统 * > * 存储选项 * 。
2. 在存储水印部分中，查看三个存储卷水印覆盖的设置。



- 如果水印覆盖为 * 0 * ，则所有三个水印都会根据存储节点的大小和卷的相对容量针对每个存储节点上的每个存储卷进行优化。

  这是默认的建议设置。您不应更新这些值。根据需要，您可以选择 [查看优化的存储水印]。

- 如果水印覆盖值不是 0 ，则会使用自定义（非优化）水印。不建议使用自定义水印设置。按照说明进行操作 "对低只读水印覆盖警报进行故障排除" 以确定是否可以或应该调整设置。

查看优化的存储水印

StorageGRID 使用两个 Prometheus 指标来显示它为 * 存储卷软只读水印 * 计算的优化值。您可以查看网格中每个存储节点的最小和最大优化值。

1. 选择 * 支持 * > * 工具 * > * 指标 * 。
2. 在 Prometheus 部分中，选择用于访问 Prometheus 用户界面的链接。
3. 要查看建议的最小软只读水印，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最小优化值。如果此值大于 * 存储卷软只读水印 * 的自定义设置，则会为存储节点触发 * 低只读水印覆盖 * 警报。

4. 要查看建议的最大软只读水印数，请输入以下 Prometheus 指标，然后选择 * 执行 * ：

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最后一列显示每个存储节点上所有存储卷的软只读水印的最大优化值。

管理对象元数据存储

StorageGRID 系统的对象元数据容量用于控制可存储在该系统上的最大对象数。为了确保 StorageGRID 系统有足够的空间来存储新对象，您必须了解 StorageGRID 在何处以及如何存储对象元数据。

什么是对象元数据?

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

对于 StorageGRID 中的对象，对象元数据包括以下类型的信息：

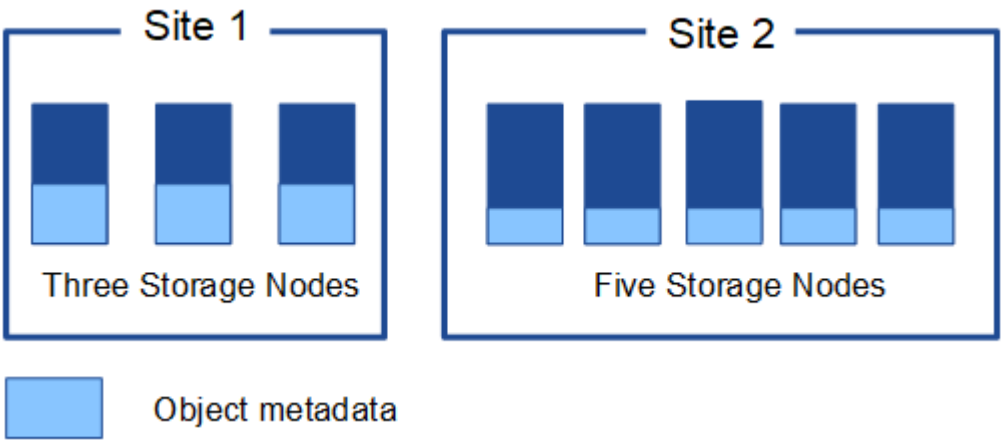
- 系统元数据，包括每个对象的唯一 ID （ UUID ），对象名称， S3 存储分段或 Swift 容器的名称，租户帐户名称或 ID ，对象的逻辑大小，首次创建对象的日期和时间， 以及上次修改对象的日期和时间。
- 与对象关联的任何自定义用户元数据键值对。
- 对于 S3 对象，是指与该对象关联的任何对象标记键值对。
- 对于复制的对象副本，为每个副本提供当前存储位置。
- 对于经过擦除编码的对象副本，为每个片段的当前存储位置。

- 对于云存储池中的对象副本，此对象的位置，包括外部存储分段的名称和对象的唯一标识符。
- 对于分段对象和多部分对象，分段标识符和数据大小。

如何存储对象元数据？

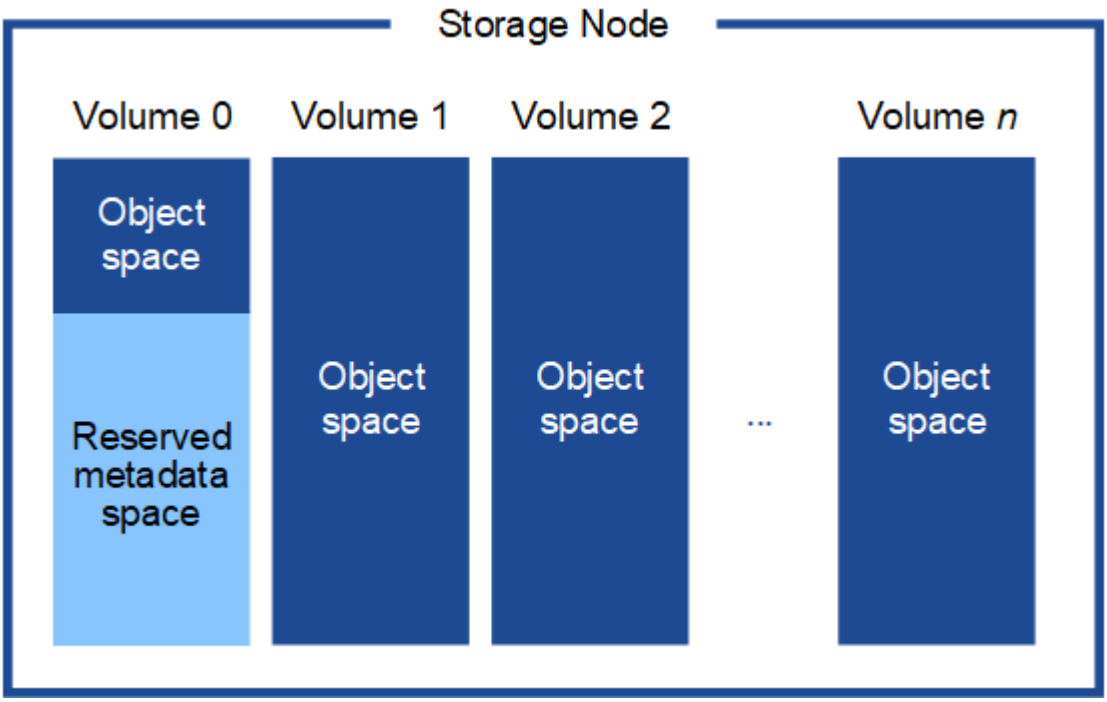
StorageGRID 在 Cassandra 数据库中维护对象元数据，该数据库独立于对象数据进行存储。为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。

此图表示两个站点上的存储节点。每个站点都具有相同数量的对象元数据、每个站点的元数据会细分为该站点的所有存储节点。



对象元数据存储在何处？

此图表示单个存储节点的存储卷。



如图所示， StorageGRID 会为每个存储节点的存储卷 0 上的对象元数据预留空间。它会使用预留空间存储对象元数据并执行基本数据库操作。存储卷 0 和存储节点中所有其他存储卷上的任何剩余空间仅用于对象数据（复

制的副本和经过纠删编码的片段）。

在特定存储节点上为对象元数据预留的空间量取决于多个因素、如下所述。

元数据预留空间设置

元数据预留空间 _ 是一个系统范围设置，表示将为每个存储节点的卷 0 上的元数据预留的空间量。如表所示、此设置的默认值基于：

- 最初安装 StorageGRID 时使用的软件版本。
- 每个存储节点上的 RAM 量。

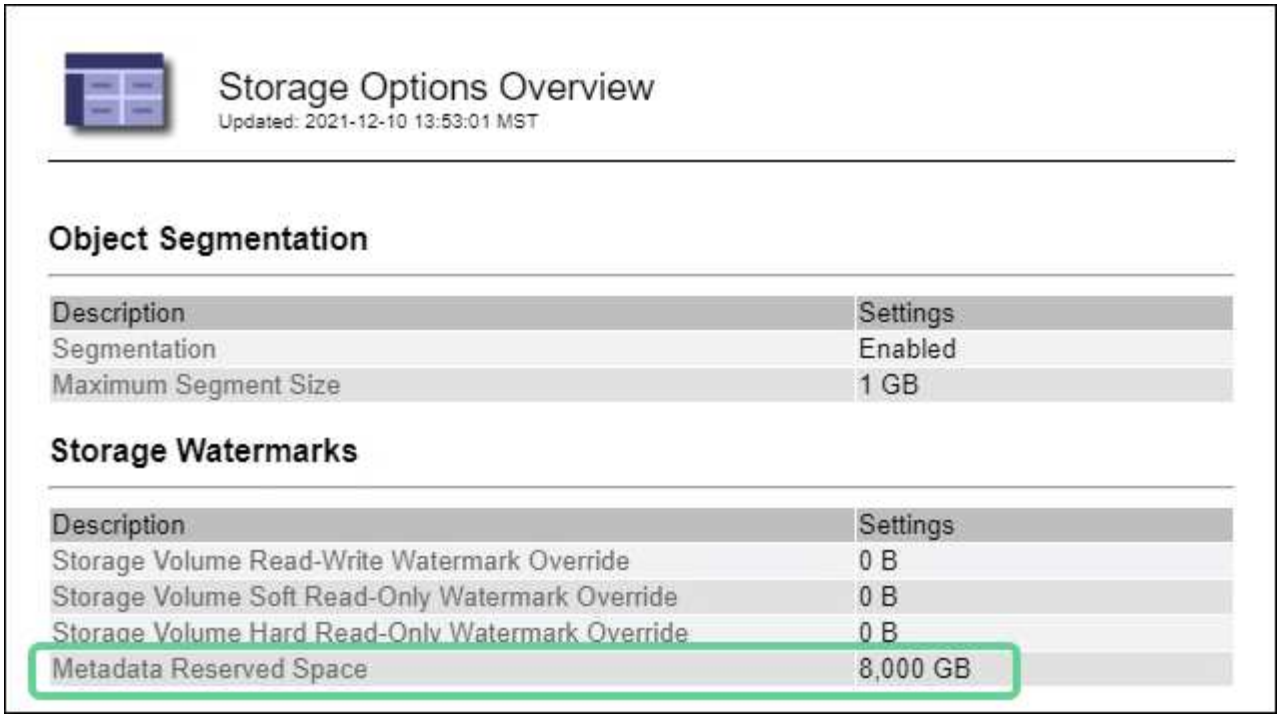
用于初始 **StorageGRID** 安装的版本	存储节点上的 **RAM** 量	默认的元数据预留空间设置
11.5至11.7	网格中的每个存储节点上的容量为 128 GB 或更大	8 TB （8， 000 GB）
	网格中任何存储节点上的容量小于 128 GB	3 TB （3， 000 GB）
11.1 到 11.4	任何一个站点的每个存储节点上的容量为 128 GB 或更大	4 TB （4， 000 GB）
	每个站点的任何存储节点上的容量小于 128 GB	3 TB （3， 000 GB）
11.0 或更早版本	任意数量	2 TB （2， 000 GB）

查看元数据预留空间设置

按照以下步骤查看StorageGRID 系统的元数据预留空间设置。

步骤

1. 选择 * 配置 * > * 系统 * > * 存储选项 * 。
2. 在存储水印表中，找到 * 元数据预留空间 * 。



在屏幕截图中， * 元数据预留空间 * 值为 8 ， 000 GB （ 8 TB ）。这是新安装的StorageGRID 11.6或更高版本的默认设置、其中每个存储节点具有128 GB或更多RAM。

元数据的实际预留空间

与系统范围的元数据预留空间设置不同，系统会为每个存储节点确定对象元数据的 *actual reserved space* 。对于任何给定的存储节点，元数据的实际预留空间取决于节点的卷 0 大小以及系统范围的 * 元数据预留空间 * 设置。

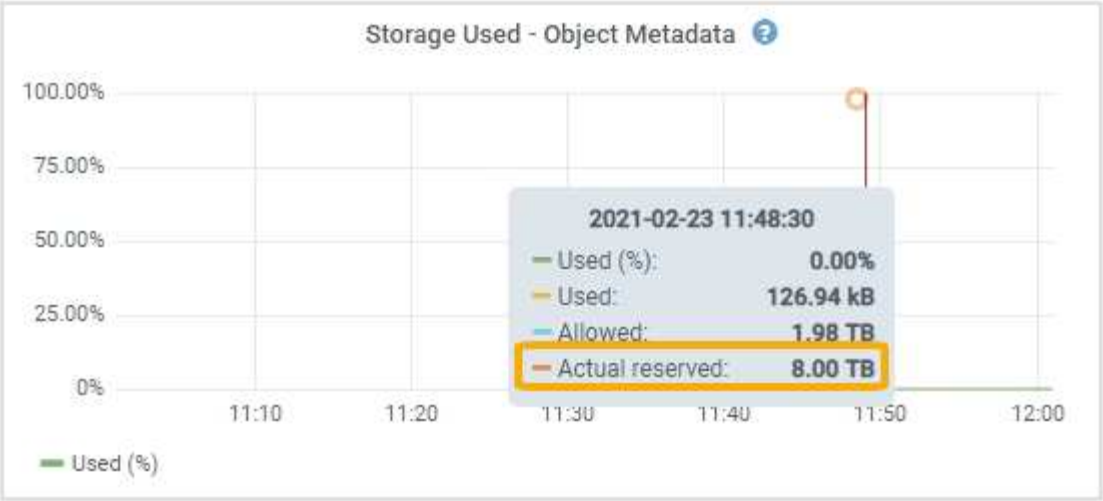
节点的卷 **0** 大小	元数据的实际预留空间
小于 500 GB （非生产用）	卷 0 的 10%
500 GB 或更大	这些值中较小的值： • 卷 0 • 元数据预留空间设置

查看元数据的实际预留空间

按照以下步骤查看特定存储节点上为元数据预留的实际空间。

步骤

1. 在网格管理器中，选择 * 节点 * > * 存储节点 _* 。
2. 选择 * 存储 * 选项卡。
3. 将光标置于"已用存储-对象元数据"图表上、然后找到*实际预留*值。



在屏幕截图中， * 实际预留 * 值为 8 TB 。此屏幕截图适用于新 StorageGRID 11.6 安装中的大型存储节点。由于此存储节点的系统范围元数据预留空间设置小于卷 0 ，因此此节点的实际预留空间等于元数据预留空间设置。

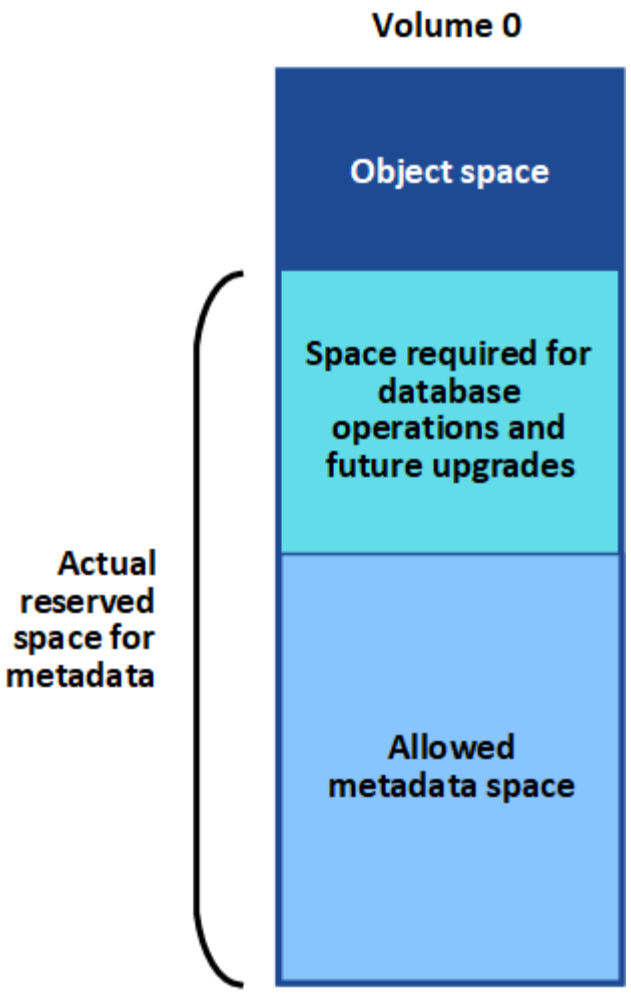
实际预留的元数据空间示例

假设您使用11.7版安装了一个新的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 。基于以下值：

- 系统范围的 * 元数据预留空间 * 设置为 8 TB 。(如果每个存储节点的RAM超过128 GB、则这是新安装的StorageGRID 11.6或更高版本的默认值。)
- SN1 元数据的实际预留空间为 6 TB 。（由于卷 0 小于 * 元数据预留空间 * 设置，因此会保留整个卷。）

允许的元数据空间

每个存储节点为元数据实际预留的空间细分为可用于对象元数据的空间（允许的元数据空间 _ ）以及基本数据库操作（如数据缩减和修复）以及未来硬件和软件升级所需的空间。允许的元数据空间用于控制整体对象容量。



下表显示了StorageGRID 如何根据不同存储节点的内存量和元数据的实际预留空间计算不同存储节点的*允许元数据空间*。

		存储节点上的内存量	
	&lt； 128 GB	&gt； = 128 GB	元数据的实际预留空间
&lt； = 4 TB	元数据的实际预留空间的 60%，最多 1.32 TB	元数据实际预留空间的 60%，最大 1.98 TB	管理； 4 TB

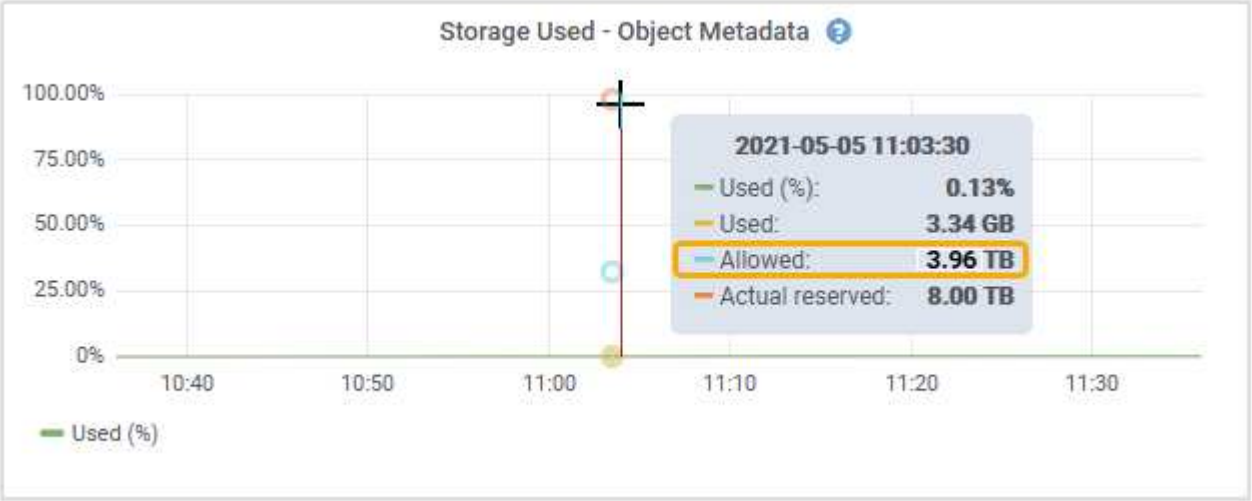
查看允许的元数据空间

按照以下步骤查看存储节点允许的元数据空间。

步骤

1. 在网格管理器中，选择 * 节点 * 。
2. 选择存储节点。
3. 选择 * 存储 * 选项卡。

4. 将光标置于已用存储-对象元数据图表上、然后找到*允许*值。



在屏幕截图中、*允许*值为3.96 TB、这是存储节点的最大值、该存储节点的元数据实际预留空间超过4 TB。

- 允许 * 值对应于此 Prometheus 指标：

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

允许的元数据空间示例

假设您安装的是使用版本 11.6 的 StorageGRID 系统。在此示例中，假设每个存储节点的 RAM 超过 128 GB ，并且存储节点 1 （ SN1 ）的卷 0 为 6 TB 。基于以下值：

- 系统范围的 * 元数据预留空间 * 设置为 8 TB 。(当每个存储节点的RAM超过128 GB时、这是StorageGRID 11.6或更高版本的默认值。)
- SN1 元数据的实际预留空间为 6 TB 。（由于卷 0 小于 * 元数据预留空间 * 设置，因此会保留整个卷。）
- 根据中所示的计算、SN1上的元数据允许的空间为3 TB 元数据允许的空间表：(元数据的实际预留空间−1 TB)×60%、最多3.96 TB。

不同大小的存储节点如何影响对象容量

如上所述， StorageGRID 会在每个站点的存储节点之间均匀分布对象元数据。因此，如果某个站点包含不同大小的存储节点，则该站点上最小的节点将决定该站点的元数据容量。

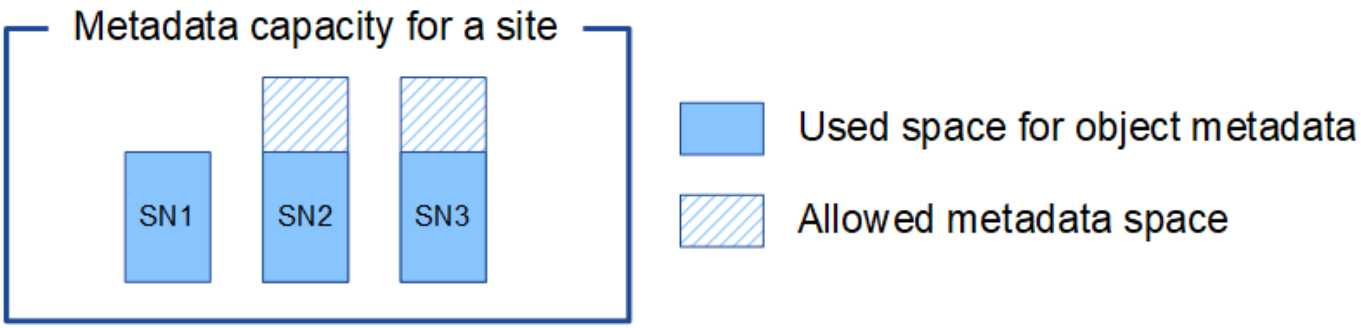
请考虑以下示例：

- 您有一个单站点网格，其中包含三个大小不同的存储节点。
- * 元数据预留空间 * 设置为 4 TB 。
- 对于实际预留的元数据空间和允许的元数据空间，存储节点具有以下值。

存储节点	卷 **0** 的大小	实际预留的元数据空间	允许的元数据空间
SN1	2.2 TB	2.2 TB	1.32 TB

存储节点	卷 **0** 的大小	实际预留的元数据空间	允许的元数据空间
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

由于对象元数据在站点的存储节点之间平均分布，因此本示例中的每个节点只能持有 1.32 TB 的元数据。无法使用SN2和SN3允许的额外0.66 TB元数据空间。



同样，由于 StorageGRID 会维护每个站点上 StorageGRID 系统的所有对象元数据，因此 StorageGRID 系统的整体元数据容量取决于最小站点的对象元数据容量。

由于对象元数据容量控制最大对象数，因此当一个节点用尽元数据容量时，网格实际上已满。

相关信息

- 要了解如何监控每个存储节点的对象元数据容量、请参见的说明 "监控StorageGRID"。
- 要增加系统的对象元数据容量、 "扩展网格" 添加新存储节点。

压缩存储的对象

您可以启用对象压缩以减小StorageGRID 中存储的对象大小、从而减少对象占用的存储空间。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

默认情况下、对象压缩处于禁用状态。如果启用数据压缩、则StorageGRID 会在保存每个对象时尝试使用无结果压缩。

> 如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

启用对象压缩之前、请注意以下事项：

- 除非您知道所存储的数据是可压缩的，否则不应选择*压缩存储的对象*。

- 将对象保存到 StorageGRID 的应用程序可能会在保存对象之前对其进行压缩。如果客户端应用程序在将对象保存到StorageGRID 之前已经对其进行了压缩、则选择此选项不会进一步减小对象的大小。
- 如果将NetApp FabricPool 与StorageGRID 结合使用、请勿选择*压缩存储的对象*。
- 如果选择*压缩存储的对象*，S3和Swift客户端应用程序应避免执行指定返回字节数范围的GET对象操作。这些 "`range read` " 操作效率低下，因为 StorageGRID 必须有效解压缩对象以访问请求的字节。从非常大的对象请求少量字节的获取对象操作效率尤其低下；例如，从 50 GB 压缩对象读取 10 MB 范围的操作效率低下。

  如果从压缩对象读取范围，则客户端请求可能会超时。

  > 如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

步骤

1. 选择*configuration*>*System*>*Object Comp其 压缩*。
2. 选中*压缩存储的对象*复选框。
3. 选择 * 保存 * 。

存储节点配置设置

每个存储节点都使用多个配置设置和计数器。您可能需要查看当前设置或重置计数器才能清除警报（旧系统）。

> 除非文档中有明确说明，否则在修改任何存储节点配置设置之前，应咨询技术支持。您可以根据需要重置事件计数器以清除原有警报。

按照以下步骤访问存储节点的配置设置和计数器。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 站点 _* > * 存储节点 _* 。
3. 展开存储节点并选择服务或组件。
4. 选择 * 配置 * 选项卡。

下表汇总了存储节点配置设置。

LDR

属性名称	代码	**Description**
HTTP 状态	HSTE	用于S3、Swift和其他内部StorageGRID 流量的HTTP 的当前状态： • 脱机：不允许执行任何操作，任何尝试打开与 LDR 服务的 HTTP 会话的客户端应用程序都会收到错误消息。活动会话正常关闭。 • 联机：操作继续正常
自动启动 HTTP	HTA	• 如果选择此选项，则重新启动时系统的状态取决于 * LDR* > * 存储 * 组件的状态。如果重新启动时 * LDR* > * 存储 * 组件为只读，则 HTTP 接口也为只读。如果 * LDR* > * 存储 * 组件为联机，则 HTTP 也为联机。否则， HTTP 接口将保持脱机状态。 • 如果未选中，则 HTTP 接口将保持脱机状态，直到显式启用为止。

LDR > 数据存储

属性名称	代码	**Description**
重置丢失的对象计数	RCOR	重置此服务中丢失的对象数量的计数器。

LDR > 存储

属性名称	代码	**Description**
存储状态—所需	SSD	用户可配置的存储组件所需状态设置。LDR 服务将读取此值并尝试与此属性指示的状态匹配。此值在重新启动后保持不变。 例如，您可以使用此设置强制存储成为只读存储，即使有足够的可用存储空间也是如此。这对于故障排除非常有用。 属性可以采用以下值之一： • 脱机：当所需状态为脱机时， LDR 服务会使 * LDR* > * 存储 * 组件脱机。 • 只读：当所需状态为只读时， LDR 服务会将存储状态移至只读状态并停止接受新内容。请注意，内容可能会继续短时间保存到存储节点中，直到打开的会话关闭为止。 • 联机：在正常系统操作期间，将此值保留为联机。存储状态—存储组件的当前状态将由服务根据 LDR 服务的状况（例如可用对象存储空间量）动态设置。如果空间不足，则组件将变为只读。
运行状况检查超时	SHCT	运行状况检查测试必须完成才能将存储卷视为运行状况良好的时间限制（以秒为单位）。只有在支持部门要求更改此值时，才更改此值。

LDR > 验证

属性名称	代码	**Description**
重置缺少的对象计数	VNMI	重置检测到的缺失对象数（ Oomis ）。请仅在对象存在检查完成后使用。StorageGRID 系统会自动还原缺少的复制对象数据。
验证率	VPRI.	设置进行后台验证的速率。请参见有关配置后台验证速率的信息。
重置损坏对象计数	VCCR	重置在后台验证期间发现的已复制对象数据损坏的计数器。此选项可用于清除检测到损坏的对象（ OCOR ）警报条件。

属性名称	代码	Description
删除隔离的对象	OQRT	从隔离目录中删除损坏的对象，将隔离对象的计数重置为零，然后清除检测到的隔离对象（ OQRT ）警报。在 StorageGRID 系统自动还原损坏的对象后，将使用此选项。 如果触发对象丢失警报，技术支持可能希望访问隔离的对象。在某些情况下，隔离的对象对于数据恢复或调试导致对象副本损坏的底层问题可能很有用。

LDR > 擦除编码

属性名称	代码	Description
重置写入失败计数	RSWF	将擦除编码对象数据写入失败时的计数器重置到存储节点。
重置读取失败计数	RSRF	重置从存储节点读取经过纠删编码的对象数据失败的计数器。
重置删除失败计数	RSDF	重置从存储节点删除经过纠删编码的对象数据失败的计数器。
重置检测到的损坏副本计数	RSCC	重置存储节点上经过纠删编码的对象数据的损坏副本数计数器。
重置检测到的损坏片段计数	RSCD	重置存储节点上擦除编码对象数据损坏片段的计数器。
重置检测到的缺失片段计数	R贴 片式	重置存储节点上缺少纠删编码对象数据片段的计数器。请仅在对象存在检查完成后使用。

LDR > 复制

属性名称	代码	Description
重置入站复制失败计数	RICR	重置入站复制失败的计数器。此操作可用于清除 RIRF （入站复制 - 失败）警报。
重置出站复制失败计数	ROCR	重置出站复制失败的计数器。此操作可用于清除 RORF （出站复制 - 失败）警报。

属性名称	代码	Description
禁用入站复制	DSIR	选择此项可在维护或测试操作步骤 过程中禁用入站复制。在正常操作期间保持未选中状态。 禁用入站复制后、可以从存储节点中检索对象以复制到StorageGRID 系统中的其他位置、但无法从其他位置将对象复制到此存储节点：LDR服务为只读。
禁用出站复制	DSOR	选择此选项可在维护或测试操作步骤 过程中禁用出站复制（包括 HTTP 检索的内容请求）。在正常操作期间保持未选中状态。 禁用出站复制后、可以将对象复制到此存储节点、但无法从此存储节点检索对象以复制到StorageGRID 系统中的其他位置。LDR 服务为只写服务。

管理完整存储节点

当存储节点达到容量时，您必须通过添加新存储来扩展 StorageGRID 系统。有三种选项可供选择：添加存储卷，添加存储扩展架和添加存储节点。

添加存储卷

每个存储节点均支持最大数量的存储卷。定义的最大值因平台而异。如果存储节点包含的存储卷数少于最大数量，则可以添加卷以增加其容量。请参见的说明 "扩展 StorageGRID 系统"。

添加存储扩展架

某些 StorageGRID 设备存储节点（例如 SG6060 ）可以支持更多存储架。如果您的 StorageGRID 设备具有扩展功能，但尚未扩展到最大容量，则可以添加存储架以增加容量。请参见的说明 "扩展 StorageGRID 系统"。

添加存储节点

您可以通过添加存储节点来增加存储容量。添加存储时，必须仔细考虑当前活动的 ILM 规则和容量要求。请参见的说明 "扩展 StorageGRID 系统"。

管理管理节点

什么是管理节点?

管理节点可提供系统配置，监控和日志记录等管理服务。每个网格都必须有一个主管理节点，并且可能有任意数量的非主管理节点，以实现冗余。

登录到网格管理器或租户管理器时，您正在连接到管理节点。您可以连接到任何管理节点，每个管理节点都会显示一个类似的 StorageGRID 系统视图。但是，必须使用主管理节点执行维护过程。

管理节点还可用于对 S3 和 Swift 客户端流量进行负载平衡。

首选发件人是什么

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

在正常系统操作下、只有首选发送方会发送通知。但是、所有其他管理节点都会监控首选发件人。如果检测到问题、其他管理节点将充当_standby senders。

在以下情况下、可能会发送多个通知：

- 如果管理节点彼此"被拒"、则首选发件人和备用发件人都将尝试发送通知、并且可能会收到多个通知副本。
- 如果备用发件人检测到首选发件人的问题并开始发送通知、则首选发件人可能会重新获得发送通知的能力。如果发生这种情况，可能会发送重复的通知。当备用发件人不再检测到首选发件人的错误时，它将停止发送通知。

> 测试AutoSupport 消息时、所有管理节点都会发送测试电子邮件。在测试警报通知时，您必须登录到每个管理节点以验证连接。

管理节点的主服务

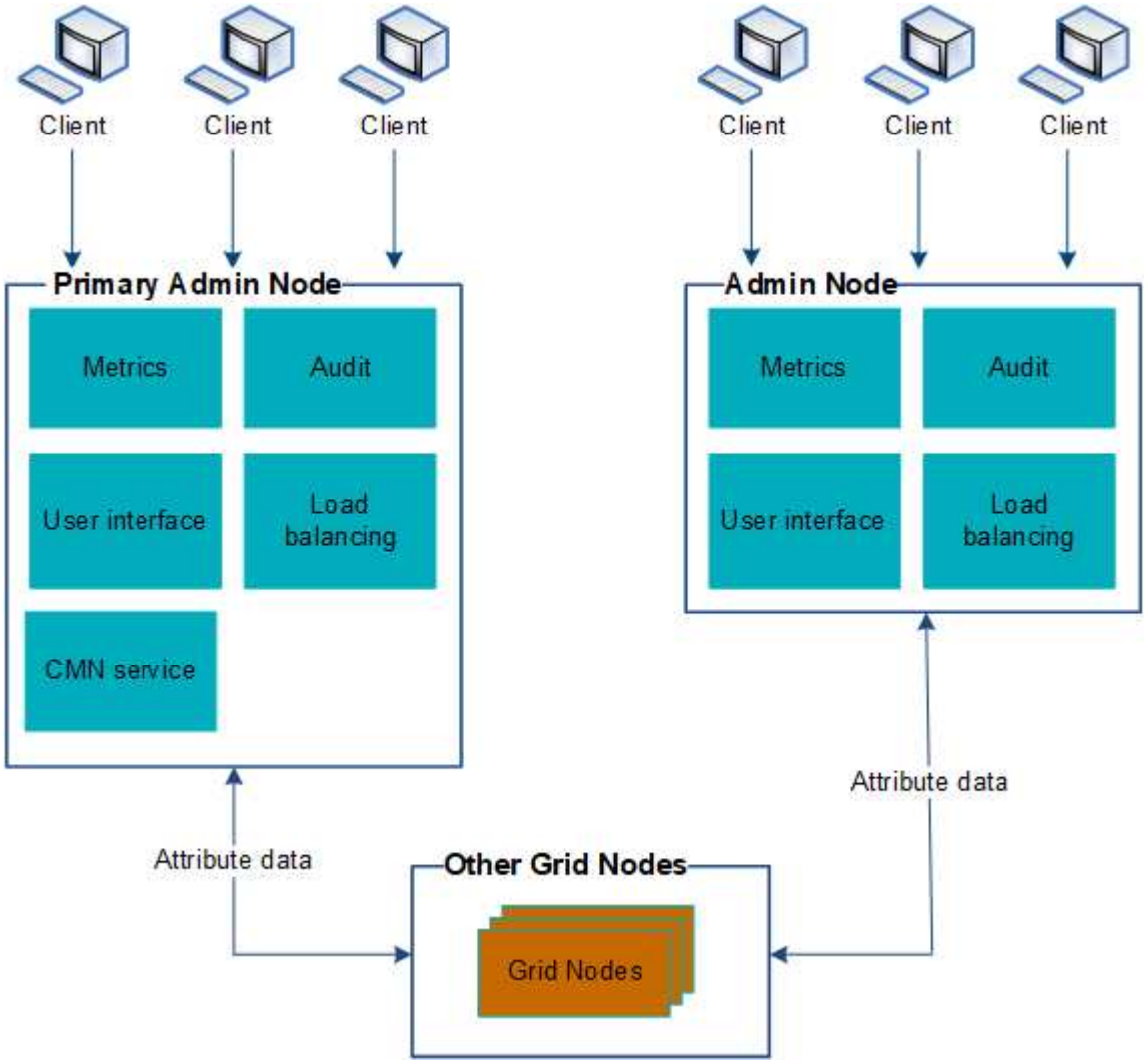
下表显示了管理节点的主服务；但是，此表并未列出所有节点服务。

服务	关键功能
审核管理系统（AMS）	跟踪系统活动和事件。
配置管理节点（CMN）	管理系统范围的配置。仅限主管理节点。
管理应用程序程序接口（mgmt-API）	处理来自网格管理 API 和租户管理 API 的请求。
高可用性	管理管理节点和网关节点组的高可用性虚拟 IP 地址。 • 注：* 此服务也可在网关节点上找到。
负载平衡器	为从客户端到存储节点的 S3 和 Swift 流量提供负载平衡。 • 注：* 此服务也可在网关节点上找到。
网络管理系统（NMS）	提供网格管理器的功能。
Prometheus	从所有节点上的服务收集和存储时间序列指标。
服务器状态监控器（SSM）	监控操作系统和底层硬件。

使用多个管理节点

一个 StorageGRID 系统可以包含多个管理节点，这样，即使一个管理节点出现故障，您也可以持续监控和配置 StorageGRID 系统。

如果管理节点不可用，则属性处理将继续，警报和警报（旧系统）仍会触发，同时仍会发送电子邮件通知和 AutoSupport 消息。但是，拥有多个管理节点不会提供故障转移保护，但通知和 AutoSupport 消息除外。特别是、从一个管理节点发出的警报鸣响不会复制到其他管理节点。



如果管理节点出现故障，可以通过两种方法继续查看和配置 StorageGRID 系统：

- Web 客户端可以重新连接到任何其他可用的管理节点。
- 如果系统管理员配置了高可用性管理节点组，则 Web 客户端可以继续使用 HA 组的虚拟 IP 地址访问网格管理器或租户管理器。请参见 "管理高可用性组"。

> 使用HA组时、如果活动管理节点发生故障、则访问将中断。用户必须在 HA 组的虚拟 IP 地址故障转移到组中的另一个管理节点后重新登录。

某些维护任务只能使用主管理节点执行。如果主管理节点出现故障，则必须先对其进行恢复，然后 StorageGRID 系统才能重新完全正常运行。

确定主管理节点

主管理节点托管 CMN 服务。某些维护过程只能使用主管理节点执行。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ； site_* > * 管理节点 * ，然后选择 ✚ 展开拓扑树并显示此管理节点上托管的服务。

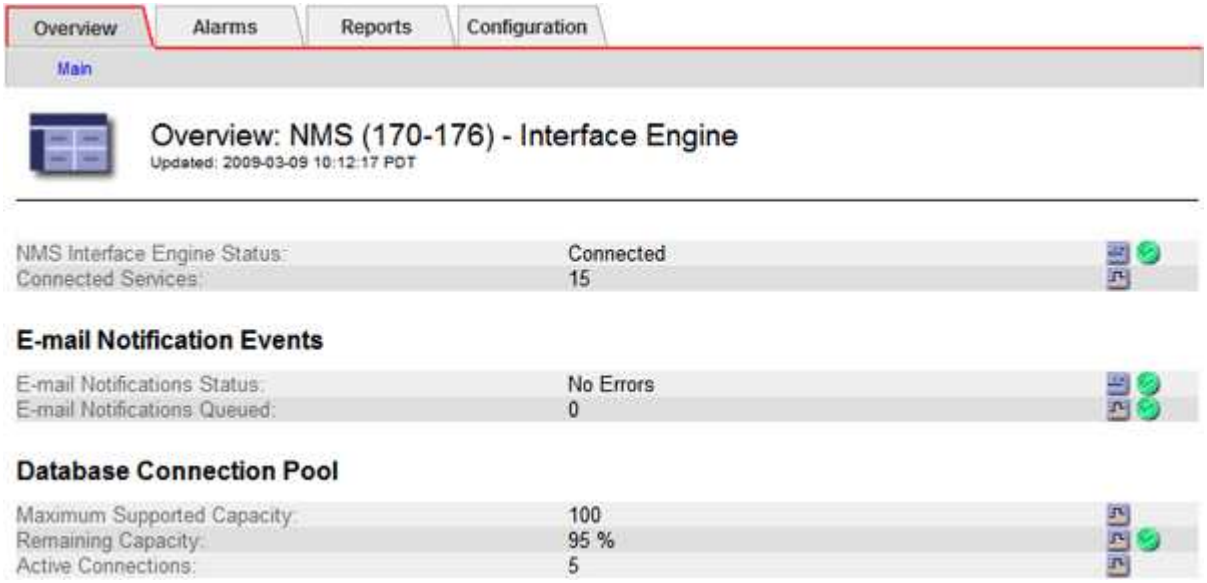
   主管理节点托管 CMN 服务。

3. 如果此管理节点不托管 CMN 服务，请检查其他管理节点。

查看通知状态和队列

管理节点上的网络管理系统（ Network Management System ， NMS ）服务会向邮件服务器发送通知。您可以在接口引擎页面上查看 NMS 服务的当前状态及其通知队列大小。

要访问接口引擎页面，请选择 * 支持 * > * 工具 * > * 网格拓扑 * 。最后，选择 * 站点 _* > * 管理节点 _* > * NMS* > * 接口引擎 * 。



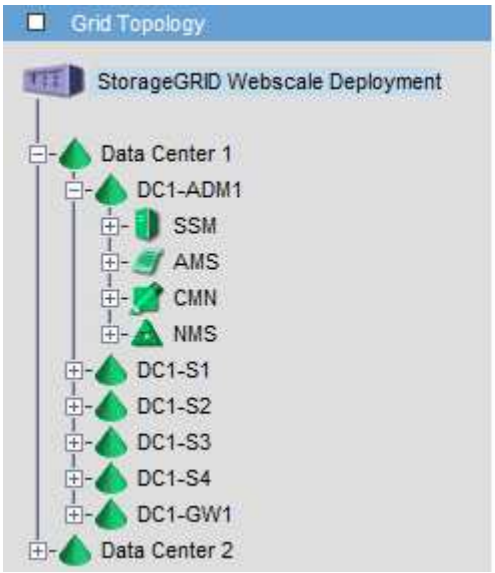
通知通过电子邮件通知队列进行处理，并按触发顺序逐个发送到邮件服务器。如果出现问题（例如网络连接错误），并且在尝试发送通知时邮件服务器不可用，则尽力将通知重新发送到邮件服务器的操作将持续 60 秒。如果通知在 60 秒后未发送到邮件服务器，则通知将从通知队列中删除，并尝试在队列中发送下一个通知。

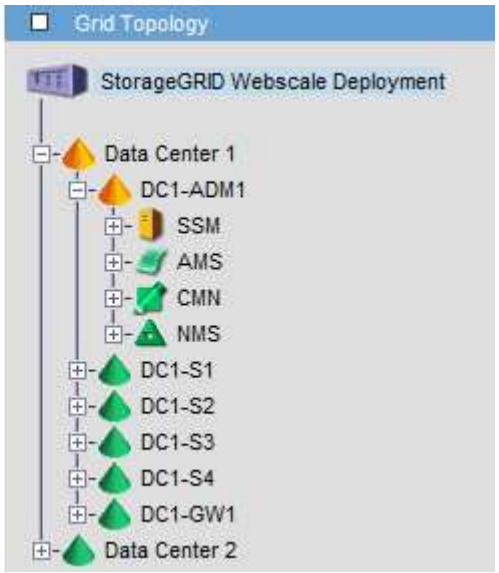
由于通知可以从通知队列中删除而不发送，因此，在不发送通知的情况下，可能会触发警报。如果从队列中删除通知而未发送、则会触发分钟(电子邮件通知状态)次要警报。

管理节点如何显示已确认的警报（旧系统）

在一个管理节点上确认警报时，已确认的警报不会复制到任何其他管理节点。由于不会将此类信息复制到其他管理节点、因此每个管理节点的网格拓扑树可能看起来不同。

在连接 Web 客户端时，这种差异非常有用。根据管理员的需求， Web 客户端可以具有不同的 StorageGRID 系统视图。





请注意，通知是从发生确认的管理节点发送的。

配置审核客户端访问

配置**NFS**的审核客户端访问

管理节点通过审核管理系统（ Audit Management System ， AMS ）服务将所有审核的系统事件记录到可通过审核共享访问的日志文件中，该文件会在安装时添加到每个管理节点中。审核共享会自动启用为只读共享。

要访问审核日志、您可以配置客户端对NFS审核共享的访问权限。或者、您也可以 "使用外部系统日志服务器"。

StorageGRID 系统会使用肯定确认来防止在将审核消息写入日志文件之前丢失这些消息。消息会一直在服务中排队，直到 AMS 服务或中间审核中继服务确认对其进行控制为止。有关详细信息，请参见 "查看审核日志"。

开始之前

- 您拥有 `Passwords.txt` 具有root/admin密码的文件。
- 您拥有 `Configuration.txt` 文件(在恢复软件包中提供)。
- 审核客户端正在使用 NFS 版本 3 （ NFSv3 ）。

关于此任务

对 StorageGRID 部署中要从中检索审核消息的每个管理节点执行此操作步骤 。

步骤

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

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 确认所有服务的状态均为正在运行或已验证。输入 ... `storagegrid-status`

   如果任何服务未列为"正在运行"或"已验证"、请先解决问题、然后再继续。

3. 返回到命令行。按 * 。 Ctrl+* 。
4. 启动 NFS 配置实用程序。输入 ... `config_nfs.rb`

```
-----------------------------------------------------------------
| Shares                | Clients               | Config          |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-----------------------------------------------------------------
```

5. 添加审核客户端： `add-audit-share`
   a. 出现提示时、输入审核客户端的审核共享IP地址或IP地址范围： `client_IP_address`
   b. 出现提示时，按 * 输入 * 。
6. 如果允许多个审核客户端访问审核共享、请添加其他用户的IP地址： `add-ip-to-share`
   a. 输入审核共享的编号： *`audit_share_number`*
   b. 出现提示时、输入审核客户端的审核共享IP地址或IP地址范围： *`client_IP_address`*
   c. 出现提示时，按 * 输入 * 。

      此时将显示 NFS 配置实用程序。

   d. 对有权访问审核共享的其他每个审核客户端重复这些子步骤。
7. （可选）验证您的配置。
   a. 输入以下内容： `validate-config`

      此时将检查并显示这些服务。

   b. 出现提示时，按 * 输入 * 。

此时将显示 NFS 配置实用程序。

c. 关闭NFS配置实用程序： `exit`

8. 确定是否必须在其他站点启用审核共享。
   - 如果 StorageGRID 部署是单个站点，请转至下一步。
   - 如果 StorageGRID 部署包括其他站点的管理节点，请根据需要启用这些审核共享：
     i. 远程登录到站点的管理节点：
        A. 输入以下命令： `ssh admin@grid_node_IP`
        B. 输入中列出的密码 `Passwords.txt` 文件
        C. 输入以下命令切换到root： `su -`
        D. 输入中列出的密码 `Passwords.txt` 文件
     ii. 重复上述步骤为每个附加管理节点配置审核共享。
     iii. 关闭远程安全 Shell 登录到远程管理节点。输入 … `exit`
9. 从命令Shell中注销： `exit`

   NFS 审核客户端将根据其 IP 地址获得对审核共享的访问权限。通过将新 NFS 审核客户端的 IP 地址添加到共享中来向该客户端授予对审核共享的访问权限，或者通过删除现有审核客户端的 IP 地址来删除该客户端。

将 **NFS** 审核客户端添加到审核共享

NFS 审核客户端将根据其 IP 地址获得对审核共享的访问权限。通过将新 NFS 审核客户端的 IP 地址添加到审核共享，将审核共享的访问权限授予给该客户端。

开始之前

- 您拥有 `Passwords.txt` 具有root/admin帐户密码的文件。
- 您拥有 `Configuration.txt` 文件(在恢复软件包中提供)。
- 审核客户端正在使用 NFS 版本 3 （ NFSv3 ）。

步骤

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

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 启动NFS配置实用程序： `config_nfs.rb`

```
-------------------------------------------------------------------
| Shares                | Clients               | Config          |
-------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-------------------------------------------------------------------
```

3. 输入 … `add-ip-to-share`

   此时将显示在管理节点上启用的 NFS 审核共享列表。审核共享列出为： `/var/local/audit/export`

4. 输入审核共享的编号： *`audit_share_number`*
5. 出现提示时、输入审核客户端的审核共享IP地址或IP地址范围： *`client_IP_address`*

   此时，审核客户端将添加到审核共享中。

6. 出现提示时，按 * 输入 * 。

   此时将显示 NFS 配置实用程序。

7. 对应添加到审核共享中的每个审核客户端重复上述步骤。
8. (可选)验证您的配置： `validate-config`

   此时将检查并显示这些服务。

   a. 出现提示时，按 * 输入 * 。

      此时将显示 NFS 配置实用程序。

9. 关闭NFS配置实用程序： `exit`
10. 如果 StorageGRID 部署是单个站点，请转至下一步。

    否则，如果 StorageGRID 部署包括其他站点的管理节点，则可以根据需要选择启用这些审核共享：

    a. 远程登录到站点的管理节点：
       i. 输入以下命令： `ssh admin@`*`grid_node_IP`*
       ii. 输入中列出的密码 `Passwords.txt` 文件
       iii. 输入以下命令切换到root： `su -`
       iv. 输入中列出的密码 `Passwords.txt` 文件
    b. 重复上述步骤为每个管理节点配置审核共享。
    c. 关闭远程安全Shell登录到远程管理节点： `exit`
11. 从命令Shell中注销： `exit`

验证 **NFS** 审核集成

配置审核共享并添加 NFS 审核客户端后，您可以挂载审核客户端共享并验证这些文件是否可从审核共享访问。

步骤

1. 使用托管 AMS 服务的管理节点的客户端 IP 地址验证连接（或客户端系统的变体）。输入 … `ping IP_address`

   验证服务器是否响应，指示连接。

2. 使用适用于客户端操作系统的命令挂载审核只读共享。Linux 命令示例为（在一行中输入）：

   `mount -t nfs -o hard,intr` *`Admin_Node_IP_address`*`:/var/local/audit/export` *`myAudit`*

   使用托管 AMS 服务的管理节点的 IP 地址以及审核系统的预定义共享名称。挂载点可以是客户端选择的任何名称(例如、 *`myAudit`* 在上一个命令中)。

3. 验证这些文件是否可从审核共享访问。输入 … `ls` *`myAudit`* `/*`

   其中： *`myAudit`* 是审核共享的挂载点。应至少列出一个日志文件。

从审核共享中删除 **NFS** 审核客户端

NFS 审核客户端将根据其 IP 地址获得对审核共享的访问权限。您可以通过删除现有审核客户端的 IP 地址来删除此客户端。

开始之前

- 您拥有 `Passwords.txt` 具有root/admin帐户密码的文件。
- 您拥有 `Configuration.txt` 文件(在恢复软件包中提供)。

关于此任务

您无法删除允许访问审核共享的最后一个IP地址。

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@`*`primary_Admin_Node_IP`*
   b. 输入中列出的密码 `Passwords.txt` 文件
   c. 输入以下命令切换到root： `su -`
   d. 输入中列出的密码 `Passwords.txt` 文件

      以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 启动NFS配置实用程序： `config_nfs.rb`

```
-------------------------------------------------------------------
| Shares                | Clients               | Config          |
-------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-------------------------------------------------------------------
```

3. 从审核共享中删除IP地址： `remove-ip-from-share`

   此时将显示服务器上配置的审核共享的编号列表。审核共享列出为： `/var/local/audit/export`

4. 输入与审核共享对应的数字： *`audit_share_number`*

   此时将显示允许访问审核共享的 IP 地址的编号列表。

5. 输入与要删除的 IP 地址对应的数字。

   此时将更新审核共享，并且不再允许使用此 IP 地址的任何审核客户端进行访问。

6. 出现提示时，按 * 输入 * 。

   此时将显示 NFS 配置实用程序。

7. 关闭NFS配置实用程序： `exit`
8. 如果您的 StorageGRID 部署为多数据中心站点部署，而其他站点上有更多管理节点，请根据需要禁用这些审核共享：
   a. 远程登录到每个站点的管理节点：
      i. 输入以下命令： `ssh admin@`*`grid_node_IP`*
      ii. 输入中列出的密码 `Passwords.txt` 文件
      iii. 输入以下命令切换到root： `su -`
      iv. 输入中列出的密码 `Passwords.txt` 文件
   b. 重复上述步骤为每个附加管理节点配置审核共享。
   c. 关闭远程安全Shell登录到远程管理节点： `exit`
9. 从命令Shell中注销： `exit`

更改 **NFS** 审核客户端的 **IP** 地址

如果需要更改 NFS 审核客户端的 IP 地址，请完成以下步骤。

步骤

1. 向现有 NFS 审核共享添加新 IP 地址。

2. 删除原始 IP 地址。

相关信息

- "将 NFS 审核客户端添加到审核共享"
- "从审核共享中删除 NFS 审核客户端"

管理归档节点

什么是归档节点?

您也可以选择使用归档节点部署每个 StorageGRID 数据中心站点，以便连接到目标外部归档存储系统，例如 Tivoli Storage Manager （ TSM ）。

> 已弃用对归档节点的支持(使用S3 API归档到云以及使用TSM中间件归档到磁带)、并将在未来版本中删除。将对象从归档节点移动到外部归档存储系统已被提供更多功能的ILM云存储池所取代。
>
> 请参见
>
> - "将对象迁移到云存储池"
> - "使用云存储池"
>
> 此外、在StorageGRID 11.7或更早版本中、您应从活动ILM策略中删除归档节点。删除存储在归档节点上的对象数据将简化将来的升级。请参见 "使用ILM规则和ILM策略"。

归档节点提供了一个接口，您可以通过该接口将外部归档存储系统作为长期存储对象数据的目标。归档节点还会监控此连接以及 StorageGRID 系统与目标外部归档存储系统之间的对象数据传输。

配置与外部目标的连接后，您可以配置归档节点以优化 TSM 性能，在 TSM 服务器容量接近或不可用时使归档节点脱机，以及配置复制和检索设置。您还可以为归档节点设置自定义警报。

无法删除但未定期访问的对象数据可以随时从存储节点的旋转磁盘移至外部归档存储、例如云或磁带。对象数据的这种归档是通过配置数据中心站点的归档节点以及配置 ILM 规则来实现的，在这些规则中，此归档节点被选为内容放置说明的 " 目标 " 。归档节点不会管理归档对象数据本身；这可通过外部归档设备实现。

> 对象元数据不会归档，但会保留在存储节点上。

什么是 **ARC-Service**

归档节点上的归档（ Archive ， ARC-） 服务提供了一个管理界面，您可以使用此界面来配置通过 TSM 中间件连接到外部归档存储（例如磁带）的连接。

它是一种可与外部归档存储系统交互的应用程序服务，用于为近线存储发送对象数据，并在客户端应用程序请求归档对象时执行检索。当客户端应用程序请求归档对象时，存储节点会从 ARC-Service 请求对象数据。ARC-Service 会向外部归档存储系统发出请求，该系统会检索请求的对象数据并将其发送到 ARC-Service 。此应用程序服务会验证对象数据并将其转发到存储节点，然后存储节点会将此对象返回到请求的客户端应用程序。

通过 TSM 中间件将对象数据归档到磁带的请求可以进行管理，以提高检索效率。可以对请求进行排序，以便按同一顺序请求按顺序存储在磁带上的对象。然后，请求将排队等待提交到存储设备。根据归档设备的不同，可以

同时处理对不同卷上的对象的多个请求。

通过 S3 API 归档到云

您可以将归档节点配置为直接连接到 Amazon Web Services （AWS）或可通过 S3 API 连接到 StorageGRID 系统的任何其他系统。

> 已弃用对归档节点的支持(使用S3 API归档到云以及使用TSM中间件归档到磁带)、并将在未来版本中删除。将对象从归档节点移动到外部归档存储系统已被提供更多功能的ILM云存储池所取代。
>
> 请参见 "使用云存储池"。

配置 S3 API 的连接设置

如果要使用 S3 接口连接到归档节点，则必须配置 S3 API 的连接设置。在配置这些设置之前，由于无法与外部归档存储系统进行通信，因此， ARC-Service 将保持主要警报状态。

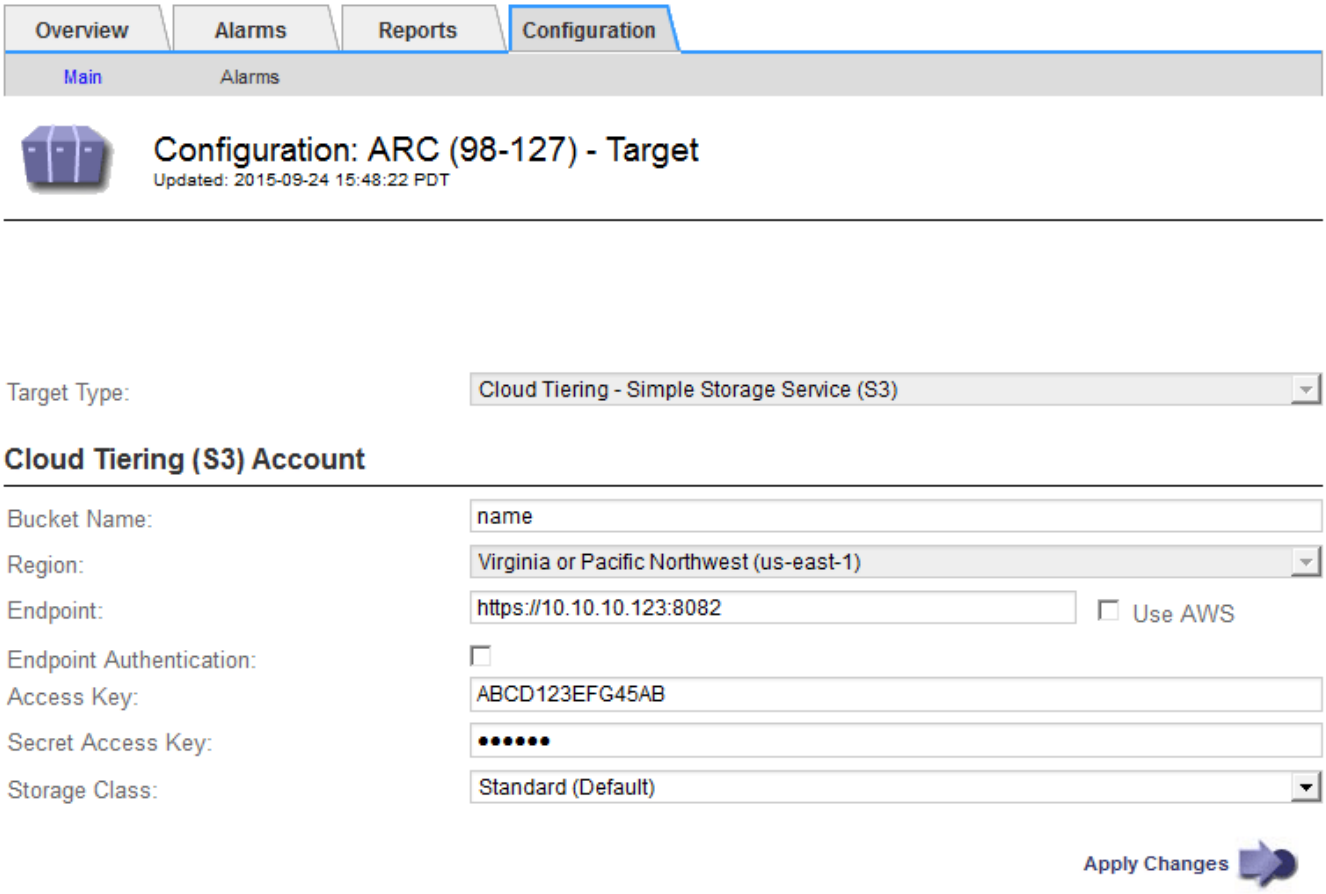
> 已弃用对归档节点的支持(使用S3 API归档到云以及使用TSM中间件归档到磁带)、并将在未来版本中删除。将对象从归档节点移动到外部归档存储系统已被提供更多功能的ILM云存储池所取代。
>
> 请参见 "使用云存储池"。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。
- 您已在目标归档存储系统上创建存储分段：
  - 此存储分段专用于一个归档节点。其他归档节点或其他应用程序不能使用它。
  - 存储分段已为您的位置选择相应的区域。
  - 应在存储分段配置中暂停版本控制。
- 已启用对象分段，并且最大分段大小小于或等于 4.5 GiB （4， 831， 838， 208 字节）。如果使用 S3 作为外部归档存储系统，超过此值的 S3 API 请求将失败。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARE* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。



4. 从目标类型下拉列表中选择 * 云分层 - 简单存储服务（ S3 ） * 。

> 只有在选择目标类型后，配置设置才可用。

5. 配置云分层（ S3 ）帐户，归档节点将通过该帐户连接到支持 S3 的目标外部归档存储系统。

   此页面上的大多数字段都是不言自明的。下面介绍了可能需要指导的字段。

   - * 地区 * ： 仅在选择 * 使用 AWS* 时可用。您选择的区域必须与存储分段的区域匹配。
   - * 端点 * 和 * 使用 AWS* ： 对于 Amazon Web Services （ AWS ），请选择 * 使用 AWS* 。然后，系统会根据 " 分段名称 " 和 " 区域 " 属性自动为 * 端点 * 填充端点 URL 。例如：

     ```
     https://bucket.region.amazonaws.com
     ```

     对于非 AWS 目标，输入托管存储分段的系统的 URL ，包括端口号。例如：

```
https://system.com:1080
```

   - * 端点身份验证 * ： 默认情况下处于启用状态。如果外部归档存储系统的网络可信、则可以清除此复选框以禁用目标外部归档存储系统的端点SSL证书和主机名验证。如果StorageGRID 系统的另一个实例是目标归档存储设备、并且系统配置了公共签名证书、则可以保持选中此复选框。
   - * 存储类 * ： 选择 * 标准（默认） * 作为常规存储。仅为易于重新创建的对象选择 * 精简冗余 * 。* 冗余减少 * 可降低存储成本，降低可靠性。如果目标归档存储系统是 StorageGRID 系统的另一个实例，则如果在目标系统上载入对象时使用了双提交，则 * 存储类 * 将控制在目标系统上载入时为该对象创建的中间副本数。

6. 选择 * 应用更改 * 。

   系统将验证指定的配置设置并将其应用于 StorageGRID 系统。配置后、无法更改目标。

修改 **S3 API** 的连接设置

将归档节点配置为通过 S3 API 连接到外部归档存储系统后，如果连接发生变化，您可以修改某些设置。

开始之前

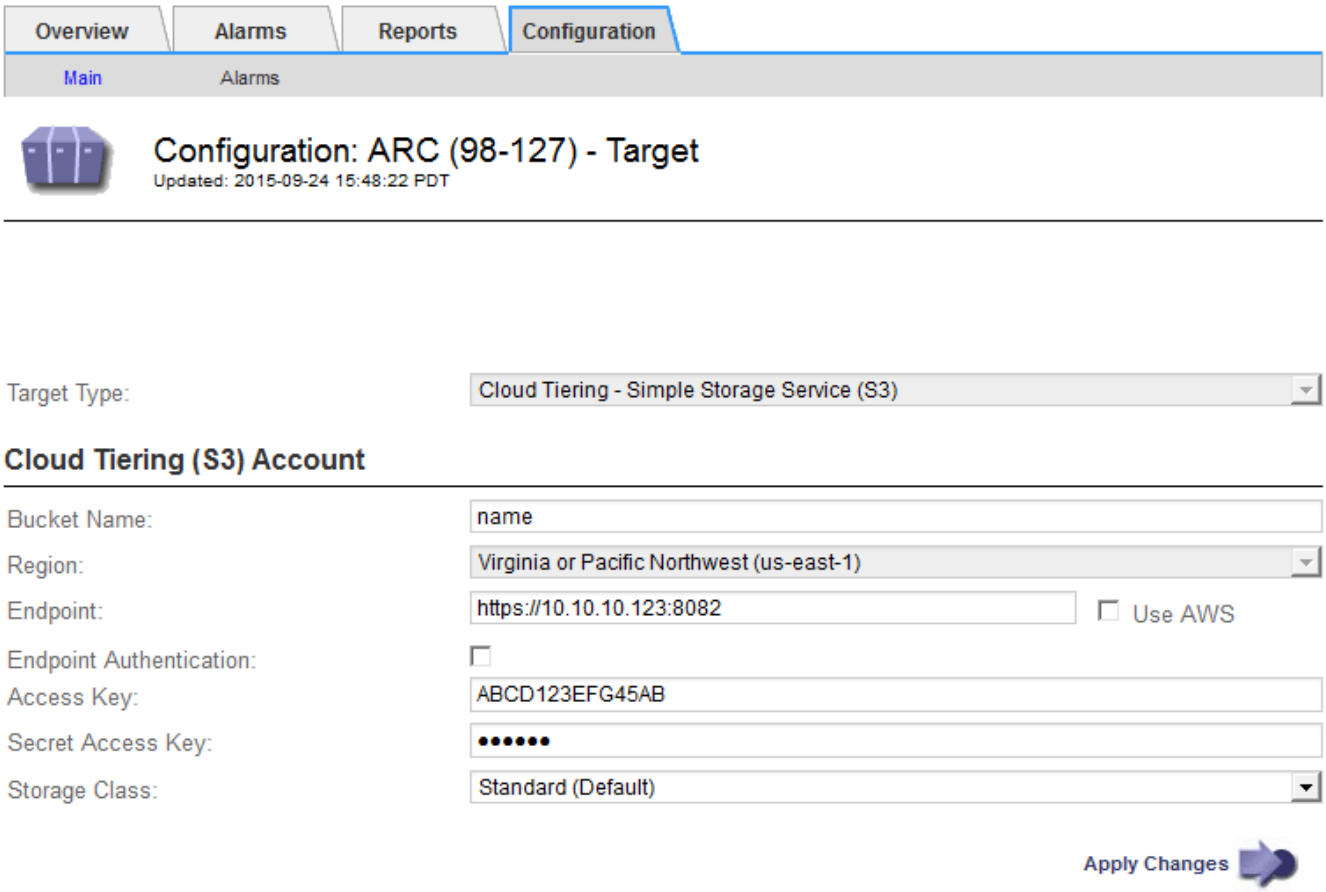
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

如果更改 Cloud Tiering （ S3 ）帐户，则必须确保用户访问凭据对存储分段具有读 / 写访问权限，包括先前归档节点向存储分段载入的所有对象。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。



4. 根据需要修改帐户信息。

如果更改存储类，则新对象数据将与新存储类一起存储。载入时，现有对象仍存储在存储类集下。

> 存储分段名称、区域和端点使用AWS值、无法更改。

5. 选择 * 应用更改 * 。

修改 **Cloud Tiering Service** 状态

您可以通过更改 Cloud Tiering 服务的状态来控制归档节点对通过 S3 API 连接的目标外部归档存储系统的读写能力。

开始之前

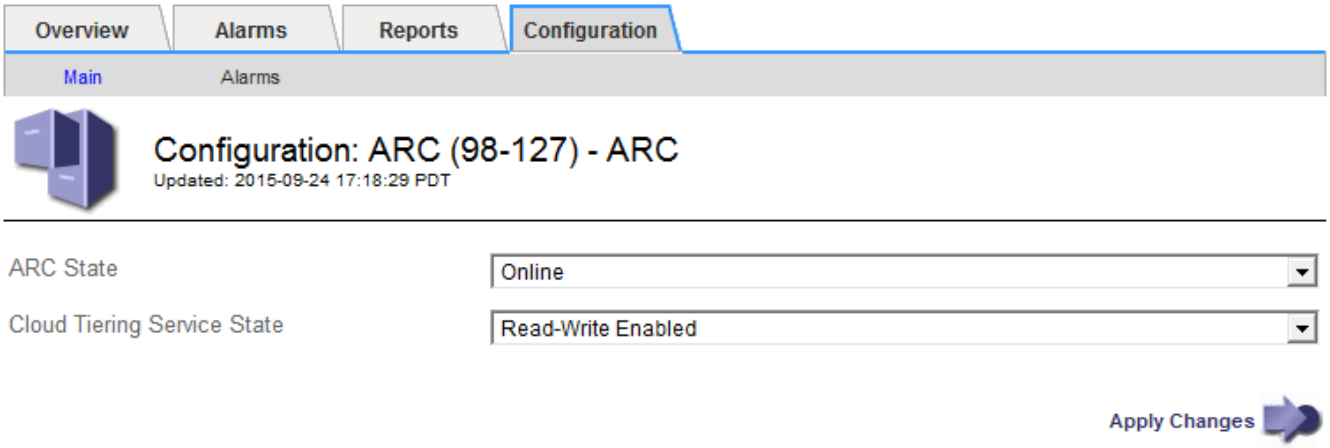
- 您必须使用登录到网格管理器 "支持的 Web 浏览器"。
- 您必须具有特定的访问权限。
- 必须配置归档节点。

关于此任务

通过将 Cloud Tiering 服务状态更改为 * 已禁用读写 * ，可以有效地使归档节点脱机。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 。归档节点 _* > * 。 ARR* 。
3. 选择 * 配置 * > * 主 * 。



4. 选择 * 云分层服务状态 * 。
5. 选择 * 应用更改 * 。

重置 **S3 API** 连接的存储故障计数

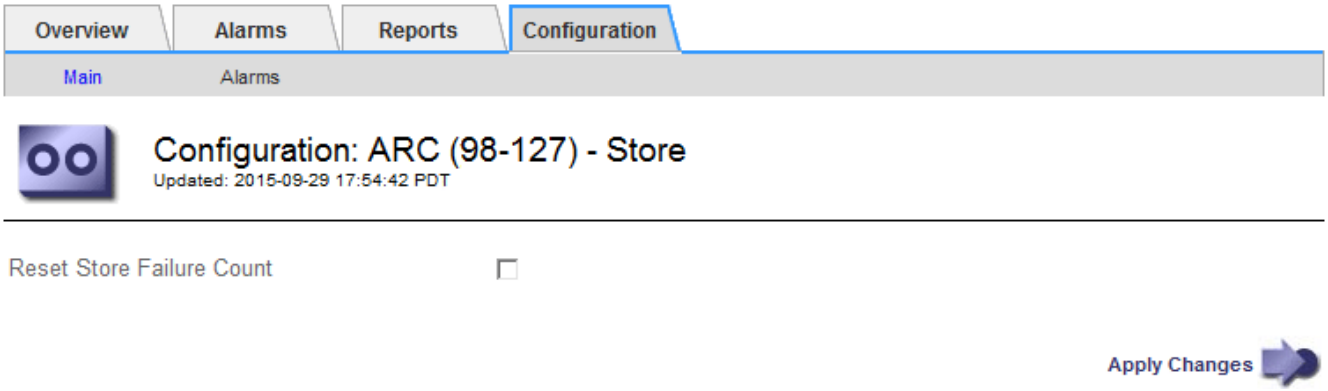
如果归档节点通过 S3 API 连接到归档存储系统，则可以重置存储故障计数，此计数可用于清除 ARVF （存储故障）警报。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 存储 * 。
3. 选择 * 配置 * > * 主 * 。



4. 选择 * 重置存储故障计数 * 。
5. 选择 * 应用更改 * 。

   存储故障属性重置为零。

将对象从 **Cloud Tiering - S3** 迁移到云存储池

如果您当前正在使用*云分层-简单存储服务(S3)*功能将对象数据分层到S3存储分段，则应将对象迁移到云存储池。云存储池提供了一种可扩展的方法，可利用 StorageGRID 系统中的所有存储节点。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。
- 您已将对象存储在为 Cloud Tiering 配置的 S3 存储分段中。

> 迁移对象数据之前，请联系您的 NetApp 客户代表，了解并管理任何相关成本。

关于此任务

从 ILM 角度来看，云存储池与存储池类似。但是，虽然存储池包含 StorageGRID 系统中的存储节点或归档节点，但云存储池包含一个外部 S3 存储分段。

在将对象从 Cloud Tiering - S3 迁移到云存储池之前，必须先创建 S3 存储分段，然后在 StorageGRID 中创建云存储池。然后，您可以创建一个新的 ILM 策略，并将用于存储 Cloud Tiering 分段中对象的 ILM 规则替换为在 Cloud Storage Pool 中存储相同对象的克隆 ILM 规则。

> 当对象存储在云存储池中时、这些对象的副本不能同时存储在StorageGRID 中。如果您当前用于云分层的 ILM 规则配置为同时将对象存储在多个位置，请考虑是否仍要执行此可选迁移，因为您将丢失此功能。如果继续执行此迁移，则必须创建新规则，而不是克隆现有规则。

步骤

1. 创建云存储池。

   为云存储池使用新的 S3 存储分段，以确保其仅包含由云存储池管理的数据。

2. 在活动 ILM 策略中找到要存储在云分层分段中的发生原因 对象的任何 ILM 规则。
3. 克隆上述每个规则。
4. 在克隆的规则中，将放置位置更改为新的云存储池。
5. 保存克隆的规则。
6. 创建使用新规则的新策略。
7. 模拟并激活新策略。

   激活新策略并进行 ILM 评估后，对象将从为 Cloud Tiering 配置的 S3 存储分段移动到为 Cloud Storage Pool 配置的 S3 存储分段。网格上的可用空间不受影响。将对象移至云存储池后，这些对象将从 Cloud Tiering 分段中删除。

相关信息

"使用 ILM 管理对象"

通过 **TSM** 中间件归档到磁带

您可以将归档节点配置为以 Tivoli Storage Manager （TSM）服务器为目标，该服务器可提供逻辑接口，用于将对象数据存储和检索到随机或顺序访问存储设备，包括磁带库。

归档节点的 ARC 服务充当 TSM 服务器的客户端，使用 Tivoli Storage Manager 作为与归档存储系统通信的中间件。

> 已弃用对归档节点的支持(使用S3 API归档到云以及使用TSM中间件归档到磁带)、并将在未来版本中删除。将对象从归档节点移动到外部归档存储系统已被提供更多功能的ILM云存储池所取代。
>
> 请参见 "使用云存储池"。

TSM 管理类

TSM 中间件定义的管理类概括了 TSM's 备份和归档操作的工作原理，可用于为 TSM 服务器应用的内容指定规则。此类规则独立于 StorageGRID 系统的 ILM 策略运行，并且必须符合 StorageGRID 系统的要求，即对象永久存储，并且始终可供归档节点检索。在归档节点将对象数据发送到 TSM 服务器后，将应用 TSM 生命周期和保留规则，同时将对象数据存储到 TSM 服务器管理的磁带。

在归档节点将对象发送到 TSM 服务器后， TSM 服务器将使用 TSM 管理类应用数据位置或保留规则。例如，标识为数据库备份的对象（可使用较新数据覆盖的临时内容）可以与应用程序数据（必须无限期保留的固定内容）不同。

要使归档节点能够与Tivoli Storage Manager (TSM)中间件进行通信、您必须先配置多项设置。

开始之前

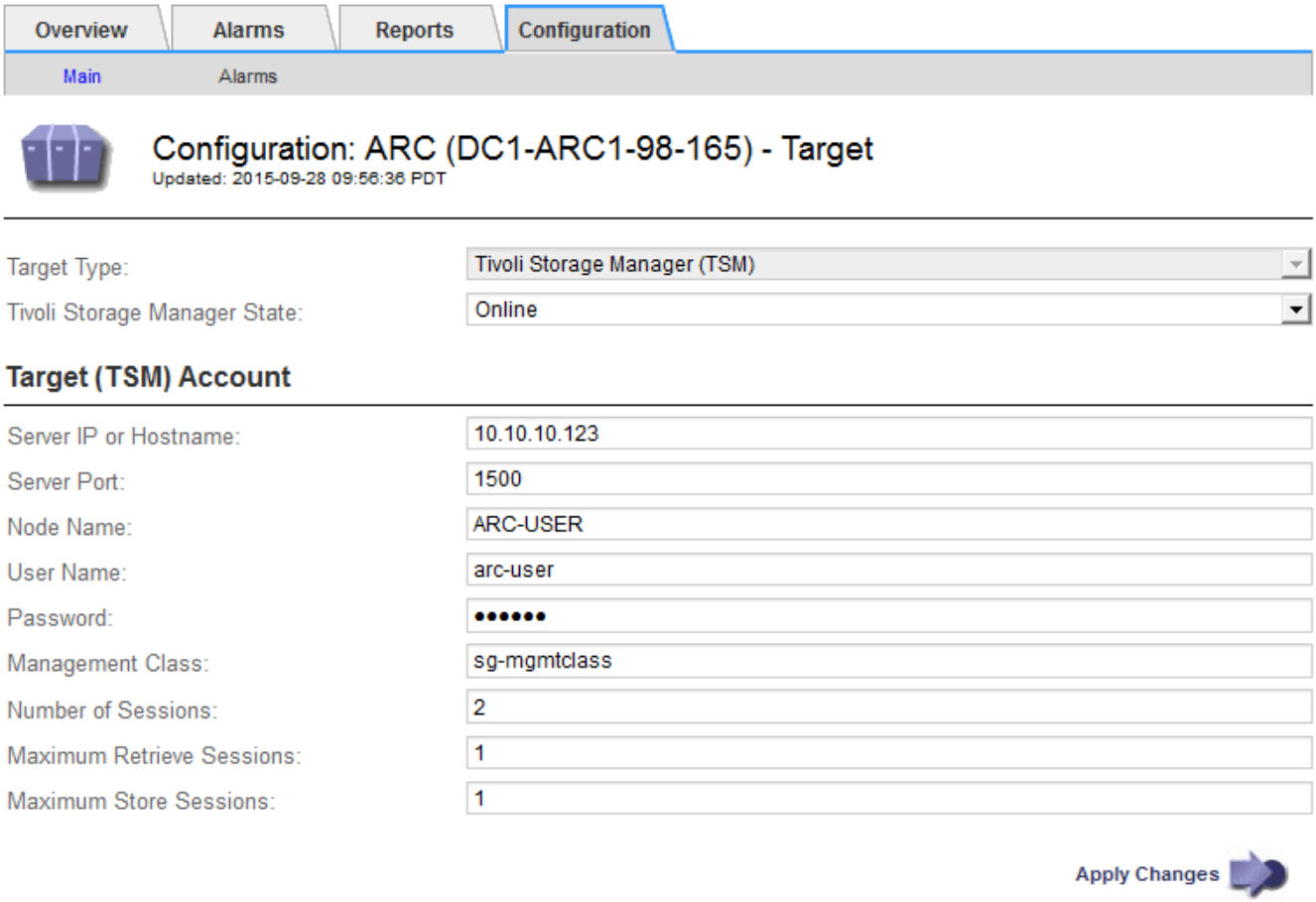
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

在配置这些设置之前，由于无法与 Tivoli Storage Manager 进行通信，因此，此 ARC-Service 仍会处于主要警报状态。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。



4. 从 * 目标类型 * 下拉列表中，选择 * Tivoli Storage Manager （ TSM ） * 。
5. 对于 * Tivoli Storage Manager State* ，请选择 * 脱机 * 以防止从 TSM 中间件服务器进行检索。

   默认情况下， Tivoli Storage Manager 状态设置为联机，这意味着归档节点能够从 TSM 中间件服务器检索对象数据。

6. 填写以下信息：

   - * 服务器 IP 或主机名 *： 指定用于此 ART 服务的 TSM 中间件服务器的 IP 地址或完全限定域名。默认 IP 地址为 127.0.0.1 。
   - * 服务器端口 *： 指定此 ARE 服务将连接到的 TSM 中间件服务器上的端口号。默认值为 1500 。
   - * 节点名称 *： 指定归档节点的名称。您必须输入在 TSM 中间件服务器上注册的名称（ arc - user ）。
   - * 用户名 *： 指定应用程序中心服务用于登录到 TSM 服务器的用户名。输入为归档节点指定的默认用户名（ arc - user ）或管理用户。
   - * 密码 *： 指定用于登录到 TSM 服务器的应用程序服务的密码。
   - * 管理类 *： 指定在将对象保存到 StorageGRID 系统时未指定管理类或在 TSM 中间件服务器上未定义指定管理类时要使用的默认管理类。
   - * 会话数 *： 指定 TSM 中间件服务器上专用于归档节点的磁带驱动器数量。归档节点会同时为每个挂载点最多创建一个会话，并另外创建少量会话（少于五个）。

     您必须将此值更改为与注册或更新归档节点时为 MAXNUMMP （最大挂载点数）设置的值相同。（在 register 命令中，如果未设置任何值，则使用的 MAXNUMMP 默认值为 1 。）

   此外，您还必须将 TSM 服务器的 MaxSessions 值更改为至少与为该应用程序服务设置的会话数相同的数字。TSM 服务器上的 MaxSessions 默认值为 25 。

   - * 最大检索会话数 *： 指定可由应用程序控制的服务为 TSM 中间件服务器打开以执行检索操作的最大会话数。在大多数情况下，适当的值为会话数减去最大存储会话数。如果需要共享一个磁带驱动器以进行存储和检索，请指定一个等于会话数的值。
   - * 最大存储会话数 *： 指定可通过应用程序中心服务打开到 TSM 中间件服务器进行归档操作的最大并发会话数。

     此值应设置为 1 ，但目标归档存储系统已满且只能执行检索时除外。将此值设置为零可使用所有会话进行检索。

7. 选择 * 应用更改 * 。

针对 **TSM** 中间件会话优化归档节点

您可以通过配置归档节点的会话来优化连接到 Tivoli Server Manager （ TSM ）的归档节点的性能。

开始之前

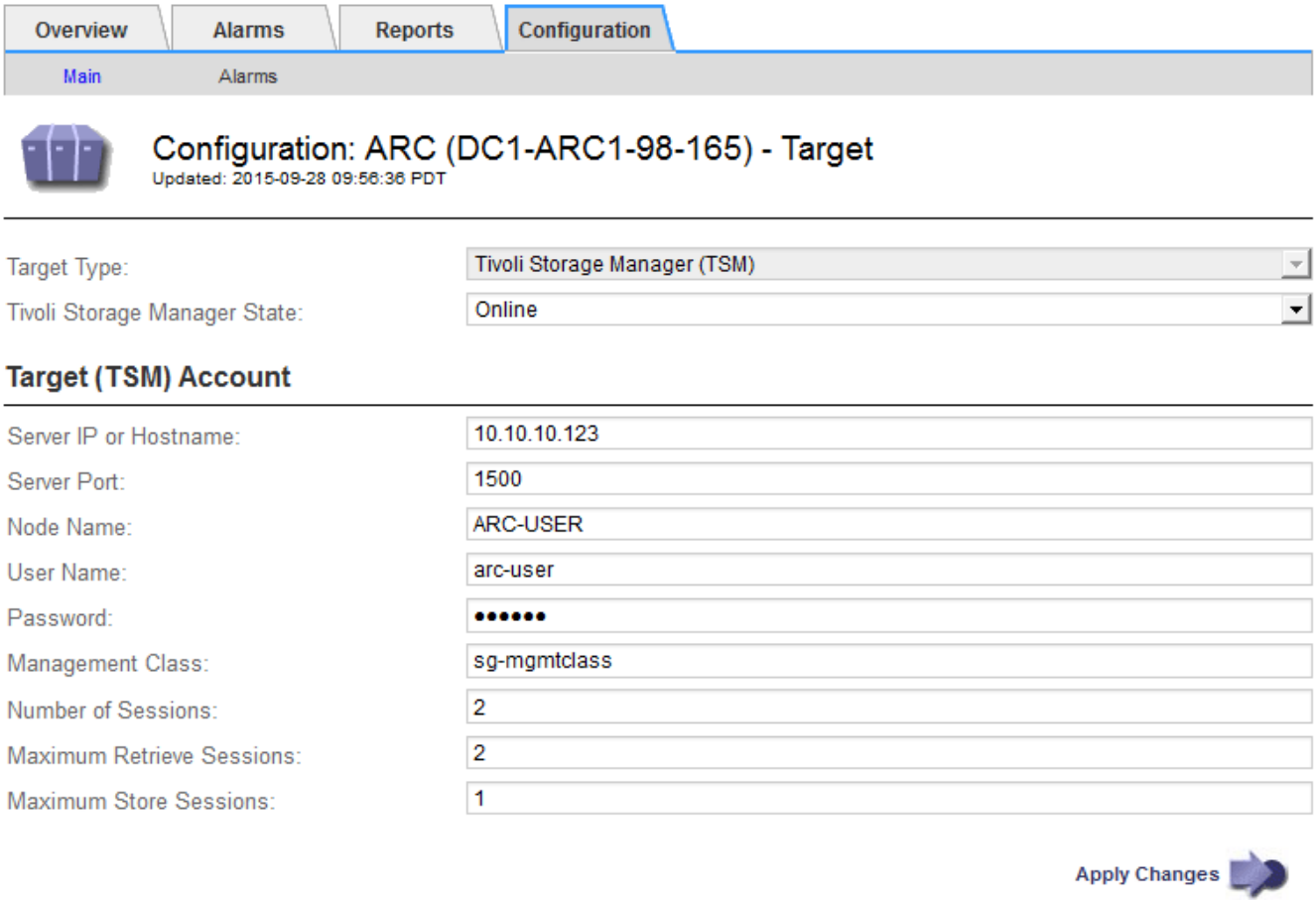
- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

通常，归档节点向 TSM 中间件服务器打开的并发会话数会设置为 TSM 服务器专用于归档节点的磁带驱动器数。一个磁带驱动器分配给存储，而其余磁带驱动器分配给检索。但是，如果要从归档节点副本重建存储节点或归档节点以只读模式运行，则可以通过将最大检索会话数设置为与并发会话数相同来优化 TSM 服务器性能。这样，所有驱动器都可以同时用于检索，如果适用，这些驱动器中最多有一个也可以用于存储。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。
4. 将 * 最大检索会话数 * 更改为与 * 会话数 * 相同。



5. 选择 * 应用更改 * 。

配置 **TSM** 的归档状态和计数器

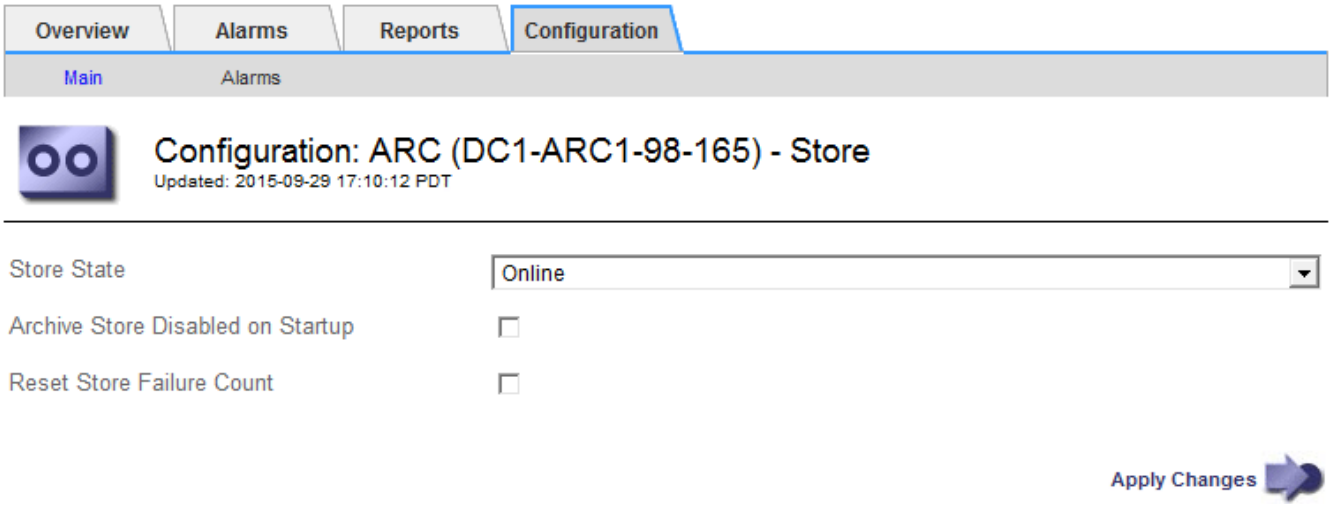
如果归档节点连接到 TSM 中间件服务器，则可以将归档节点的归档存储状态配置为联机或脱机。您还可以在归档节点首次启动时禁用归档存储，或者重置为关联警报跟踪的故障计数。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 存储 * 。
3. 选择 * 配置 * > * 主 * 。



4. 根据需要修改以下设置：
   - 存储状态：将组件状态设置为：
     - 联机：归档节点可用于处理要存储到归档存储系统的对象数据。
     - 脱机：归档节点不可用于将要存储的对象数据处理到归档存储系统。
   - 启动时禁用归档存储：选中后，重新启动时归档存储组件将保持只读状态。用于持久禁用目标归档存储系统的存储。当目标归档存储系统无法接受内容时，此功能非常有用。
   - Reset Store Failure Count ：重置存储故障计数器。此选项可用于清除 ARVF （存储故障）警报。
5. 选择 * 应用更改 * 。

相关信息

"在 TSM 服务器达到容量时管理归档节点"

在 **TSM** 服务器达到容量时管理归档节点

当 TSM 数据库或 TSM 服务器管理的归档介质存储即将达到容量时， TSM 服务器无法通知归档节点。可以通过主动监控 TSM 服务器来避免这种情况。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

关于此任务

在 TSM 服务器停止接受新内容后，归档节点将继续接受要传输到 TSM 服务器的对象数据。无法将此内容写入TSM服务器管理的介质。如果发生这种情况，将触发警报。

阻止应用程序保护服务向 **TSM** 服务器发送内容

为了防止此 ARC-Service 向 TSM 服务器发送更多内容，您可以使归档节点的 * ARC/ * 组件脱机，从而使其 * 存储 * 组件脱机。此操作步骤 还有助于防止在 TSM 服务器不可维护时发出警报。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。

2. 选择 * ： 归档节点 _* > * 。 ARR* > * 存储 * 。
3. 选择 * 配置 * > * 主 * 。

4. 将*存储状态*更改为 `Offline`。
5. 选择 * 启动时已禁用归档存储 * 。
6. 选择 * 应用更改 * 。

如果 **TSM** 中间件达到容量，请将归档节点设置为只读

如果目标 TSM 中间件服务器达到容量，则可以对归档节点进行优化，使其仅执行检索。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ： 归档节点 _* > * 。 ARR* > * 目标 * 。
3. 选择 * 配置 * > * 主 * 。
4. 将最大检索会话数更改为与会话数中列出的并发会话数相同。
5. 将最大存储会话数更改为 0 。

> 如果归档节点为只读，则无需将最大存储会话数更改为 0 。不会创建存储会话。

6. 选择 * 应用更改 * 。

配置归档节点检索设置

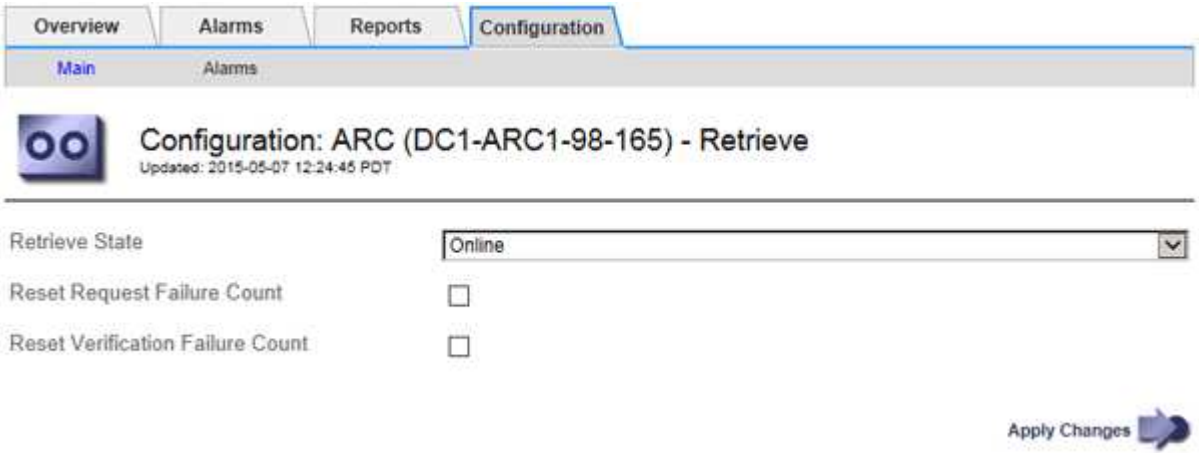
您可以配置归档节点的检索设置，将状态设置为联机或脱机，或者重置为关联警报跟踪的故障计数。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * 归档节点 * > * ARC/ * 检索 * 。
3. 选择 * 配置 * > * 主 * 。



4. 根据需要修改以下设置：
   - * 检索状态 * ：将组件状态设置为：
     - 联机：网格节点可用于从归档介质设备检索对象数据。
     - 脱机：网格节点不可用于检索对象数据。
   - 重置请求失败计数：选中此复选框可重置请求失败计数器。此选项可用于清除 ARRF （请求失败）警报。
   - 重置验证失败计数：选中此复选框可重置检索到的对象数据的验证失败计数器。此操作可用于清除 ARRV （验证失败）警报。
5. 选择 * 应用更改 * 。

配置归档节点复制

您可以为归档节点配置复制设置并禁用入站和出站复制，或者重置为关联警报跟踪的故障计数。

开始之前

- 您将使用登录到网格管理器 "支持的 Web 浏览器"。
- 您具有特定的访问权限。

步骤

1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。
2. 选择 * ：归档节点 _* > * 。 ARR* > * 复制 * 。
3. 选择 * 配置 * > * 主 * 。

4. 根据需要修改以下设置：
   - * 重置入站复制失败计数 * ：选择此项可重置入站复制失败的计数器。此操作可用于清除 RIRF （入站复

制 - 失败）警报。

- * 重置出站复制失败计数 *： 选择此项可重置出站复制失败的计数器。此操作可用于清除 RORF （出站复制 - 失败）警报。
- * 禁用入站复制 *： 选择此项可在维护或测试操作步骤 过程中禁用入站复制。在正常操作期间保持清除状态。

  禁用入站复制后、可以从ARC服务检索对象数据、以便复制到StorageGRID 系统中的其他位置、但无法从其他系统位置将对象复制到此ARC服务。此‐服务为只读。

- 禁用出站复制：选中此复选框可在维护或测试操作步骤 期间禁用出站复制(包括HTTP检索的内容请求)。在正常操作期间保持未选中状态。

  禁用出站复制后、可以将对象数据复制到此ARC服务以满足ILM规则、但无法从ARC服务检索对象数据以复制到StorageGRID 系统中的其他位置。此 ARC 服务为 write‐only 。

5. 选择 * 应用更改 * 。

为归档节点设置自定义警报

您应为 ARQL 和 ARLRL 属性建立自定义警报，用于监控归档节点从归档存储系统检索对象数据的速度和效率。

- ARQL： 平均队列长度。从归档存储系统中检索对象数据的平均排队时间（以微秒为单位）。
- ARRL： 平均请求延迟。归档节点从归档存储系统检索对象数据所需的平均时间（以微秒为单位）。

这些属性的可接受值取决于归档存储系统的配置和使用方式。（转至 * ARC/ * * 检索 * > * 概述 * > * 主要 * 。）为请求超时设置的值以及可用于检索请求的会话数尤其具有影响。

集成完成后，监控归档节点的对象数据检索，以确定正常检索时间和队列长度的值。然后，为 ARQL 和 ARLRL 创建自定义警报，以便在出现异常运行状况时触发警报。请参见的说明 "管理警报(传统系统)"。

集成 **Tivoli Storage Manager**

归档节点配置和操作

您的 StorageGRID 系统会将归档节点作为一个位置来管理，在该位置，对象会无限期地存储，并且始终可以访问。

在载入对象时，系统会根据为 StorageGRID 系统定义的信息生命周期管理（ ILM ）规则将副本复制到所有必需的位置，包括归档节点。归档节点充当 TSM 服务器的客户端， TSM 客户端库通过 StorageGRID 软件安装过程安装在归档节点上。定向到归档节点进行存储的对象数据会在收到时直接保存到 TSM 服务器。归档节点不会在将对象数据保存到 TSM 服务器之前暂存对象数据，也不会执行对象聚合。但是，如果数据速率需要，归档节点可以在一个事务中向 TSM 服务器提交多个副本。

在归档节点将对象数据保存到 TSM 服务器后， TSM 服务器将使用其生命周期 / 保留策略来管理对象数据。必须定义这些保留策略，使其与归档节点的操作兼容。也就是说，归档节点保存的对象数据必须无限期存储，并且必须始终可由归档节点访问，除非归档节点将其删除。

StorageGRID 系统的 ILM 规则与 TSM 服务器的生命周期 / 保留策略之间没有连接。每个对象彼此独立运行；但是，在将每个对象载入 StorageGRID 系统时，您可以为其分配一个 TSM 管理类。此管理类将与对象数据一起

传递到 TSM 服务器。通过将不同的管理类分配给不同的对象类型，您可以将 TSM 服务器配置为将对象数据放置在不同的存储池中，或者根据需要应用不同的迁移或保留策略。例如，标识为数据库备份的对象（临时内容，不能使用较新的数据覆盖）的处理方式可能与应用程序数据（必须无限期保留的固定内容）不同。

归档节点可以与新的或现有的 TSM 服务器集成；它不需要专用的 TSM 服务器。TSM 服务器可以与其他客户端共享，但前提是 TSM 服务器的大小应适合最大预期负载。TSM 必须安装在与归档节点不同的服务器或虚拟机上。

可以将多个归档节点配置为写入同一个 TSM 服务器；但是，只有当归档节点向 TSM 服务器写入不同的数据集时，才建议使用此配置。当每个归档节点向归档写入相同对象数据的副本时，建议不要将多个归档节点配置为写入同一 TSM 服务器。在后一种情况下，对于对象数据的独立冗余副本，这两个副本都会发生单点故障（ TSM 服务器）。

归档节点不使用TSM的分层存储管理(HSM)组件。

配置最佳实践

在调整 TSM 服务器的大小并对其进行配置时，应应用一些最佳实践来优化它，以便与归档节点配合使用。

在估算 TSM 服务器的规模并对其进行配置时，应考虑以下因素：

- 由于归档节点在将对象保存到 TSM 服务器之前不会聚合对象，因此必须对 TSM 数据库进行大小调整，以保留对要写入归档节点的所有对象的引用。
- 归档节点软件无法容忍将对象直接写入磁带或其他可移动介质所涉及的延迟。因此，无论何时使用可移动介质， TSM 服务器都必须配置一个磁盘存储池，用于初始存储归档节点保存的数据。
- 您必须配置 TSM 保留策略，以使用基于事件‐的保留。归档节点不支持基于创建的 TSM 保留策略。在保留策略中使用以下建议设置 remin=0 和 rever=0 （这表示保留从归档节点触发保留事件时开始，并在此之后保留 0 天）。但是， remin 和 rever 的这些值是可选的。

必须对磁盘池进行配置，以便将数据迁移到磁带池（即，磁带池必须是磁盘池的 NXTSTGPOOL ）。不能将磁带池配置为磁盘池的副本池、并同时向这两个池写入数据(即、磁带池不能是磁盘池的COPYSTGPOOL)。要为包含归档节点数据的磁带创建脱机副本，请为 TSM 服务器配置第二个磁带池，该磁带池是用于归档节点数据的磁带池的副本池。

完成归档节点设置

完成安装过程后，归档节点无法正常运行。在 StorageGRID 系统将对象保存到 TSM 归档节点之前，您必须完成 TSM 服务器的安装和配置，并配置归档节点以与 TSM 服务器进行通信。

在准备 TSM 服务器以便与 StorageGRID 系统中的归档节点集成时，请根据需要参考以下 IBM 文档：

- "《 IBM 磁带设备驱动程序安装和用户指南》"
- "《 IBM 磁带设备驱动程序编程参考》"

安装新的 **TSM** 服务器

您可以将归档节点与新的或现有的 TSM 服务器集成在一起。如果要安装新的 TSM 服务器，请按照 TSM 文档中的说明完成安装。

归档节点不能与TSM服务器共同托管。

配置 **TSM** 服务器

本节介绍了按照 TSM 最佳实践准备 TSM 服务器的示例说明。

以下说明将指导您完成以下过程：

- 在 TSM 服务器上定义磁盘存储池和磁带存储池（如果需要）
- 为从归档节点保存的数据定义使用 TSM 管理类的域策略，并注册节点以使用此域策略

这些说明仅供参考；它们不能替代TSM文档、也不能提供适用于所有配置的完整而全面的说明。应由熟悉您的详细要求和一整套 TSM Server 文档的 TSM 管理员提供部署特定的说明。

定义 **TSM** 磁带和磁盘存储池

归档节点将写入磁盘存储池。要将内容归档到磁带，必须配置磁盘存储池以将内容移动到磁带存储池。

关于此任务

对于 TSM 服务器，您必须在 Tivoli Storage Manager 中定义磁带存储池和磁盘存储池。定义磁盘池后，创建一个磁盘卷并将其分配给磁盘池。如果您的 TSM 服务器仅使用磁盘‐存储，则不需要磁带池。

您必须先在TSM服务器上完成多个步骤、然后才能创建磁带存储池。（在磁带库中创建一个磁带库和至少一个驱动器。定义从服务器到库以及从服务器到驱动器的路径，然后为驱动器定义设备类。） 根据站点的硬件配置和存储要求，这些步骤的详细信息可能会有所不同。有关详细信息，请参见 TSM 文档。

以下一组说明说明了此过程。请注意，根据部署要求，您的站点可能会有所不同。有关配置详细信息和说明，请参见 TSM 文档。

您必须使用管理权限登录到服务器、并使用dsmadmc工具执行以下命令。

步骤

1. 创建磁带库。

   `define library` *`tapelibrary`* `libtype=`*`scsi`*

   其中 *`tapelibrary`* 是为磁带库选择的任意名称以及的值 `libtype` 可能因磁带库类型而异。

2. 定义从服务器到磁带库的路径。

   `define path` *`servername tapelibrary`* `srctype=server desttype=library device=`*`lib-devicename`*

   - *`servername`* 是TSM服务器的名称
   - *`tapelibrary`* 是您定义的磁带库名称
   - *`lib-devicename`* 是磁带库的设备名称

3. 为库定义驱动器。

   `define drive *tapelibrary drivename*`

   - *drivename* 是要为驱动器指定的名称
   - *tapelibrary* 是您定义的磁带库名称

     根据您的硬件配置，您可能需要配置一个或多个驱动器。（例如，如果 TSM 服务器连接到一个光纤通道交换机，而该交换机具有来自磁带库的两个输入，则您可能需要为每个输入定义一个驱动器。）

4. 定义从服务器到您定义的驱动器的路径。

   `define path *servername* drivename srctype=server desttype=drive library=*tapelibrary* device=*drive-dname*`

   - *drive-dname* 是驱动器的设备名称
   - *tapelibrary* 是您定义的磁带库名称

     使用单独的对为磁带库定义的每个驱动器重复上述步骤 *drivename* 和 *drive-dname* 每个驱动器。

5. 为驱动器定义设备类。

   `define devclass *DeviceClassName* devtype=*lto* library=*tapelibrary* format=*tapetype*`

   - *DeviceClassName* 是设备类的名称
   - *lto* 是连接到服务器的驱动器类型
   - *tapelibrary* 是您定义的磁带库名称
   - *tapetype* 是磁带类型；例如ultrium3

6. 将磁带卷添加到库的清单中。

   `checkin libvolume *tapelibrary*`

   tapelibrary 是您定义的磁带库名称。

7. 创建主磁带存储池。

   `define stgpool *SGWSTapePool DeviceClassName* description=*description collocate=filespace* maxscratch=*XX*`

   - *SGWSTapePool* 是归档节点的磁带存储池的名称。您可以为磁带存储池选择任何名称（只要该名称使用 TSM 服务器预期的语法约定）。
   - *DeviceClassName* 是磁带库的设备类名称。
   - *description* 是存储池的问题描述 、可以使用在TSM服务器上显示 `query stgpool` 命令：例如： "` 归档节点的磁带存储池。` "
   - *collocate=filespace* 指定TSM服务器应将同一文件空间中的对象写入单个磁带。

- `XX` 是以下项之一：
  - 磁带库中的空磁带数量（如果归档节点是唯一使用该库的应用程序）。
  - 分配给 StorageGRID 系统使用的磁带数量（在共享磁带库的情况下）。

8. 在 TSM 服务器上，创建磁盘存储池。在 TSM 服务器的管理控制台中，输入

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *`SGWSDiskPool`* 是归档节点的磁盘池的名称。您可以为磁盘存储池选择任何名称（只要该名称使用 TSM 预期的语法约定）。
   - *`description`* 是存储池的问题描述 、可以使用在TSM服务器上显示 `query stgpool` 命令：例如， " 为归档节点设置 `D` 存储池。 "
   - *`maximum_file_size`* 强制将大于此大小的对象直接写入磁带、而不是缓存在磁盘池中。建议设置 *`maximum_file_size`* 到10 GB。
   - *`nextstgpool=SGWSTapePool`* 将磁盘存储池引用为归档节点定义的磁带存储池。
   - *`percent_high`* 设置磁盘池开始将其内容迁移到磁带池时的值。建议设置 *`percent_high`* 设置为0、以便立即开始数据迁移
   - *`percent_low`* 设置停止迁移到磁带池的值。建议设置 *`percent_low`* 设置为0以清除磁盘池。

9. 在 TSM 服务器上，创建一个或多个磁盘卷并将其分配给磁盘池。

   ```
   define volume SGWSDiskPool volume_name formatsize=size
   ```

   - *`SGWSDiskPool`* 是磁盘池名称。
   - *`volume_name`* 是卷所在位置的完整路径(例如、 `/var/local/arc/stage6.dsm`)、以便写入磁盘池的内容、以便为传输到磁带做好准备。
   - *`size`* 是磁盘卷的大小、以MB为单位。

     例如，要创建一个磁盘卷，使磁盘池的内容填满一个磁带，请在磁带卷的容量为 200 GB 时将大小值设置为 200 ， 000 。

     但是，可能需要创建多个较小大小的磁盘卷，因为 TSM 服务器可以向磁盘池中的每个卷写入数据。例如，如果磁带大小为 250 GB ，请创建 25 个磁盘卷，每个卷的大小为 10 GB （ 10000 ）。

   TSM 服务器会在目录中为磁盘卷预先分配空间。此操作可能需要一段时间才能完成（对于 200 GB 磁盘卷，需要三个多小时）。

定义域策略并注册节点

您需要为从归档节点保存的数据定义一个使用 TSM 管理类的域策略，然后注册一个节点以使用此域策略。

> 如果 Tivoli Storage Manager （ TSM ）中归档节点的客户端密码过期，则归档节点进程可能会泄漏内存。确保已配置 TSM 服务器，以便归档节点的客户端用户名 / 密码永不过期。

在 TSM 服务器上注册节点以使用归档节点（或更新现有节点）时，必须通过在注册节点命令中指定 MAXNUMMP 参数来指定节点可用于写入操作的挂载点数量。挂载点的数量通常等于分配给归档节点的磁带驱动器头的数量。为TSM服务器上的MAXNUMMP指定的数字必须至少与为归档节点的*ARC*>*目标*>*配置*>*主*>*最大存储会话数*设置的值相同， 值设置为0或1、因为归档节点不支持并发存储会话。

为 TSM 服务器设置的 MaxSessions 值用于控制所有客户端应用程序可向 TSM 服务器打开的最大会话数。在 TSM 上指定的 MaxSessions 值必须至少与在网格管理器中为归档节点指定的 * ARC* > * 目标 * > * 配置 * > * 主 * > * 会话数 * 的值相同。归档节点会同时为每个挂载点最多创建一个会话，并另外创建少量（ < 5 ）个会话。

分配给归档节点的TSM节点使用自定义域策略 `tsm-domain`。。 `tsm-domain` 域策略是"tandard `s`"域策略的修改版本、配置为写入磁带、并将归档目标设置为`StorageGRID` 系统的存储池 （`*SGWSDiskPool*`）。

> 您必须使用管理权限登录到 TSM 服务器，并使用 dsmadc 工具创建和激活域策略。

创建并激活域策略

您必须创建一个域策略，然后将其激活，以配置 TSM 服务器以保存从归档节点发送的数据。

步骤

1. 创建域策略。

   ```
   copy domain standard tsm-domain
   ```

2. 如果不使用现有管理类、请输入以下内容之一：

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` 是部署的默认管理类。

3. 创建一个副本组到相应的存储池。在一行中输入：

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` 是归档节点的默认管理类。的值 `retinit`， `retmin`，和 `retver` 已选择此选项以反映归档节点当前使用的保留行为

   > 请勿设置 `retinit` to `retinit=create`。正在设置 ... `retinit=create` 阻止归档节点删除内容、因为保留事件用于从TSM服务器中删除内容。

4. 将管理类分配为默认值。

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. 将新策略集设置为活动。

   ```
   activate policyset tsm-domain standard
   ```

请忽略输入 activate 命令时显示的 "`no backup copy group` " 警告。

6. 注册一个节点以使用在 TSM 服务器上设置的新策略。在 TSM 服务器上，输入（在一行上）：

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

arc-user 和 arc-password 与您在归档节点上定义的客户端节点名称和密码相同，并且 MAXNUMMP 的值设置为为归档节点存储会话预留的磁带驱动器数量。

> 默认情况下，注册节点会创建一个由客户端所有者授权的管理用户 ID ，并为此节点定义密码。

将数据迁移到 StorageGRID

您可以将大量数据迁移到 StorageGRID 系统，同时使用 StorageGRID 系统执行日常操作。

在计划将大量数据迁移到StorageGRID 系统时、请使用本指南。本指南不是数据迁移的通用指南，也不包括执行迁移的详细步骤。请遵循本节中的准则和说明，确保在不影响日常操作的情况下将数据高效迁移到 StorageGRID 系统中，并确保 StorageGRID 系统能够正确处理迁移的数据。

确认 StorageGRID 系统的容量

在将大量数据迁移到 StorageGRID 系统之前，请确认 StorageGRID 系统具有处理预期卷所需的磁盘容量。

如果StorageGRID 系统包含一个归档节点、并且已将迁移对象的副本保存到近线存储(例如磁带)、请确保归档节点的存储具有足够的容量来容纳预期的已迁移数据卷。

在容量评估过程中，请查看计划迁移的对象的数据配置文件，并计算所需的磁盘容量。有关监控 StorageGRID 系统磁盘容量的详细信息，请参见 "管理存储节点" 以及的说明 "监控StorageGRID"。

确定已迁移数据的 ILM 策略

StorageGRID 系统的 ILM 策略可确定创建的副本数，副本存储到的位置以及这些副本的保留时间。ILM 策略由一组 ILM 规则组成，这些规则介绍如何筛选对象以及如何随着时间的推移管理对象数据。

根据迁移数据的使用方式以及迁移数据的要求，您可能需要为迁移的数据定义与日常操作所使用的 ILM 规则不同的唯一 ILM 规则。例如，如果日常数据管理的法规要求与迁移中包含的数据的法规要求不同，则您可能需要在不同级别的存储上为迁移的数据创建不同数量的副本。

如果可以唯一区分已迁移数据和通过日常操作保存的对象数据，则可以配置专用于已迁移数据的规则。

如果您可以使用元数据条件之一可靠地区分数据类型，则可以使用此条件定义仅适用于已迁移数据的 ILM 规则。

在开始数据迁移之前，请确保您了解 StorageGRID 系统的 ILM 策略及其如何应用于迁移的数据，并且已对 ILM 策略进行了更改并进行了测试。请参见 "使用 ILM 管理对象"。

> 如果未正确指定 ILM 策略发生原因 ，则可能会导致无法恢复的数据丢失。在激活 ILM 策略之前 ，请仔细查看对该策略所做的所有更改，以确保该策略按预期运行。

评估迁移对操作的影响

StorageGRID 系统旨在为对象存储和检索提供高效操作，并通过无缝创建对象数据和元数据的冗余副本提供出色的数据保护，防止数据丢失。

但是、必须按照本指南中的说明仔细管理数据迁移、以避免影响日常系统操作、或者在极端情况下、避免在StorageGRID 系统发生故障时使数据面临丢失的风险。

迁移大量数据会给系统带来额外的负载。当 StorageGRID 系统负载过重时，它对存储和检索对象的请求响应速度较慢。这可能会干扰日常操作不可或缺的存储和检索请求。迁移还可以发生原因 解决其他操作问题。例如，当存储节点接近容量时，由于批量载入而产生的大量间歇性负载可以对存储节点进行发生原因 ，使其在只读和读写之间循环，从而生成通知。

如果负载仍然繁重，则可以为 StorageGRID 系统必须执行的各种操作开发队列，以确保对象数据和元数据完全冗余。

必须按照本文档中的准则仔细管理数据迁移，以确保 StorageGRID 系统在迁移期间安全高效地运行。迁移数据时，请批量载入对象或持续限制载入。然后、持续监控StorageGRID 系统以确保不会超过各种属性值。

计划和监控数据迁移

必须根据需要计划和监控数据迁移，以确保在所需时间内根据 ILM 策略放置数据。

计划数据迁移

避免在核心运行时间迁移数据。将数据迁移限制为晚上，周末以及系统使用率较低的其他时间。

如果可能、请勿在活动频繁期间计划数据迁移。但是，如果完全避免高活动期限不可行，只要您密切监控相关属性并在其超过可接受值时采取措施，就可以安全地继续操作。

监控数据迁移

此表列出了在数据迁移期间必须监控的属性及其所代表的问题。

如果您使用具有速率限制的流量分类策略来限制载入，则可以结合下表所述的统计信息来监控观察到的速率，并根据需要降低这些限制。

监控	Description
等待 ILM 评估的对象数量	1. 选择 * 支持 * > * 工具 * > * 网格拓扑 * 。 2. 选择 * ； deployment_* > * 概述 * > * 主要 * 。 3. 在 "ILM Activity" 部分中，监控为以下属性显示的对象数量： ◦ * 正在等待 - 全部（ XQUZ ） *： 等待 ILM 评估的对象总数。 ◦ * 正在等待 - 客户端（ XQZ ） *： 等待通过客户端操作（例如载入）进行 ILM 评估的对象总数。 4. 如果为其中任一属性显示的对象数量超过 100 ， 000 个，请限制对象的载入速率，以减少 StorageGRID 系统上的负载。
目标归档系统的存储容量	如果 ILM 策略将已迁移数据的副本保存到目标归档存储系统（磁带或云），请监控目标归档存储系统的容量，以确保已迁移数据具有足够的容量。
• 归档节点 * > * ARC/ * 存储 *	如果触发了针对 * 存储故障（ ARVF ） * 属性的警报，则目标归档存储系统可能已达到容量。检查目标归档存储系统并解决触发警报的任何问题。