管理 StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-115/admin/web-browser-requirements.html on April 11, 2024. Always check docs.netapp.com for the latest.

目录

管理 StorageGRID

了解如何配置StorageGRID 系统。

- "管理StorageGRID 系统"
- "控制管理员对StorageGRID 的访问"
- "配置密钥管理服务器"
- "管理租户"
- "配置S3和Swift客户端连接"
- "管理StorageGRID 网络和连接"
- "正在配置 AutoSupport"
- "管理存储节点"
- "管理管理节点"
- "管理归档节点"
- "将数据迁移到StorageGRID"

管理StorageGRID 系统

按照以下说明配置和管理 StorageGRID 系统。

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。

有关使用信息生命周期管理（ ILM ）规则和策略管理对象的说明已移至"使用 ILM 管理对象"。

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。

您需要的内容

- 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。

Web 浏览器要求

您必须使用受支持的 Web 浏览器。

Web 浏览器	支持的最低版本
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84.

您应将浏览器窗口设置为建议的宽度。

浏览器宽度	像素
最小值	1024
最佳	1280

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。

您需要的内容

- 您必须拥有登录凭据。
- 您必须具有网格管理器的URL。
- 您必须使用受支持的Web浏览器。
- 必须在 Web 浏览器中启用 Cookie 。
- 您必须具有特定的访问权限。

关于此任务

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，管理节点不完全相同：

- 在一个管理节点上进行的警报确认（原有系统）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。

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首选主节点、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。

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 ：

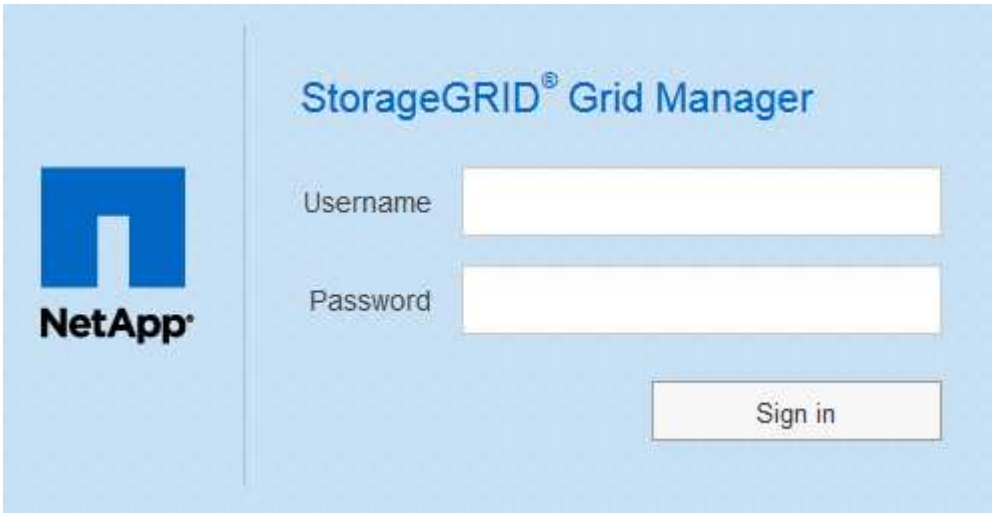
   `https://FQDN_or_Admin_Node_IP/`

   其中： *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的IP地址、或者管理节点HA组的虚拟IP地址。

   如果您必须在HTTPS的标准端口(443)以外的端口上访问网格管理器、请输入以下内容、其中 *FQDN_or_Admin_Node_IP* 是完全限定域名或IP地址、port是端口号：

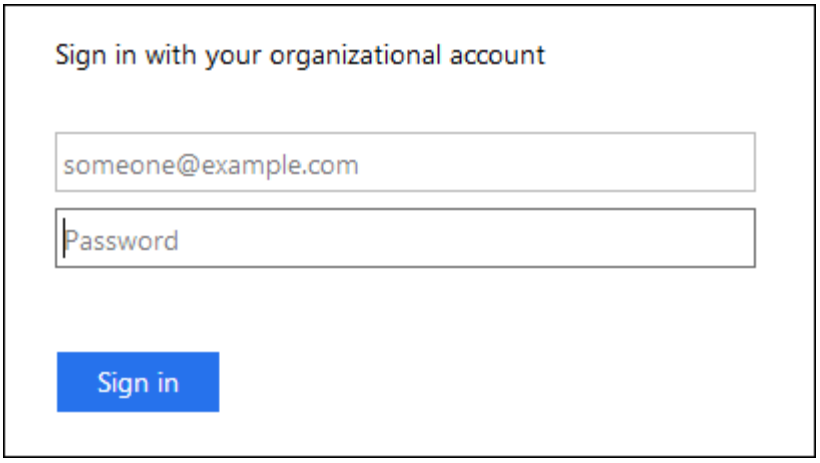
   `https://FQDN_or_Admin_Node_IP:port/`

3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。
4. 登录到网格管理器：
   - 如果 StorageGRID 系统未使用单点登录（ SSO ）：
     i. 输入网格管理器的用户名和密码。
     ii. 单击 * 登录 * 。



   - 如果为 StorageGRID 系统启用了 SSO ，并且这是您首次在此浏览器上访问此 URL ：
     i. 单击 * 登录 * 。您可以将 "Account ID" 字段留空。

     ii. 在组织的 SSO 登录页面上输入标准 SSO 凭据。例如：

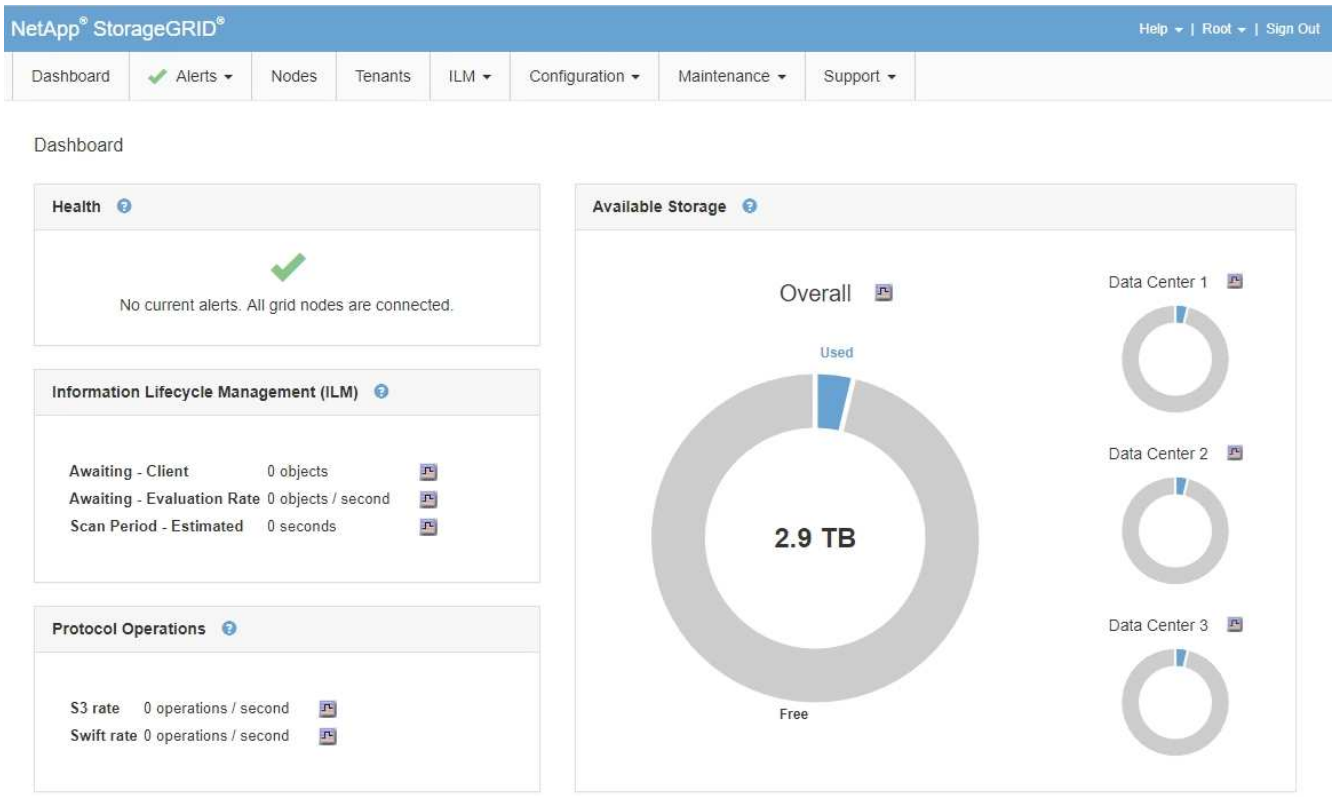


- 如果为 StorageGRID 系统启用了 SSO ，并且您先前已访问网格管理器或租户帐户：

  i. 执行以下任一操作：

  - 输入*。0*(网格管理器的帐户ID)、然后单击*登录*。
  - 如果近期帐户列表中显示*网格管理器*、请选择此选项、然后单击*登录*。

  ii. 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StorageGRID 监控和故障排除说明中的"`查看信息板`"。



5. 如果要登录到另一个管理节点：

选项	步骤
未启用 SSO	a. 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。 b. 输入网格管理器的用户名和密码。 c. 单击 * 登录 * 。
已启用 SSO	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。 如果您已登录到一个管理节点，则无需重新登录即可访问其他管理节点。但是，如果您的 SSO 会话到期，系统会再次提示您输入凭据。 • 注： * 受限网格管理器端口上不提供 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

"Web 浏览器要求"

"通过防火墙控制访问"

"配置服务器证书"

"配置单点登录"

"管理管理组"

"管理高可用性组"

"使用租户帐户"

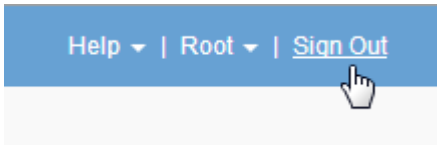
"监控和放大；故障排除"

注销网格管理器

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

步骤

1. 找到用户界面右上角的 * 注销 * 链接。



2. 单击*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，则还必须注销租户帐户才能注销 SSO 。

相关信息

"配置单点登录"

"使用租户帐户"

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。

您需要的内容

您必须使用支持的浏览器登录到网格管理器。

关于此任务

如果您以联合用户身份登录到 StorageGRID 或启用了单点登录（ Single Sign-On ， 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. 单击 * 保存 * 。

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。下载包含网格拓扑信息和StorageGRID 系统加密密钥的恢复软件包备份时、也需要使用密码短语。

您需要的内容

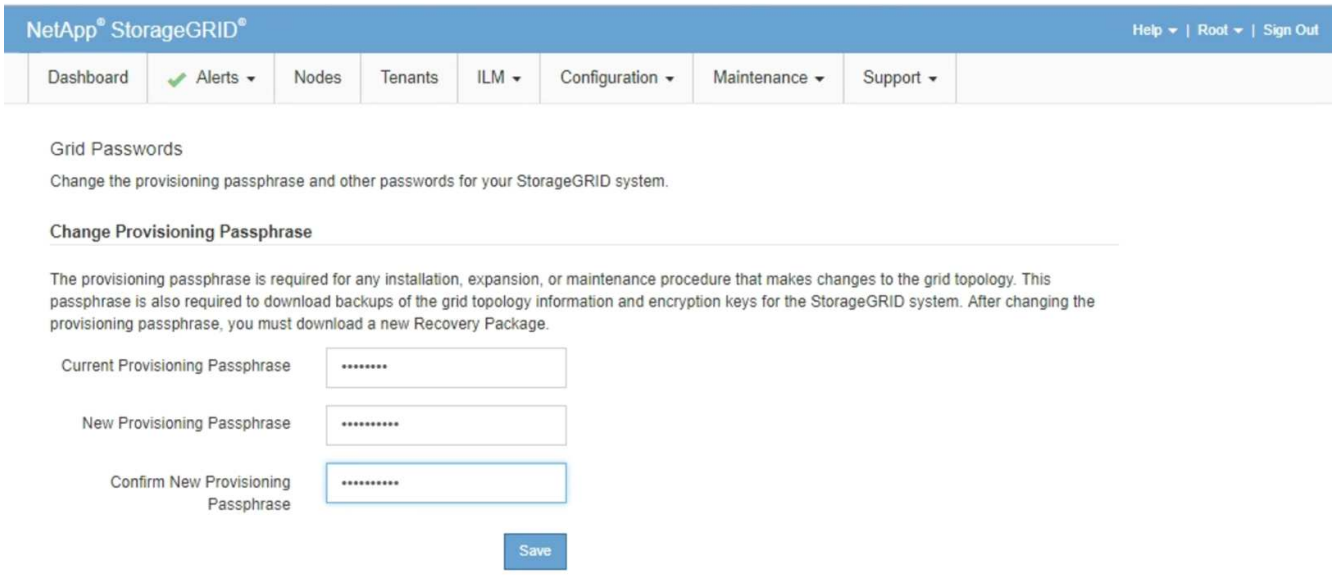
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有维护或根访问权限。
- 您必须具有当前配置密码短语。

关于此任务

许多安装和维护过程以及下载恢复软件包都需要配置密码短语。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*。

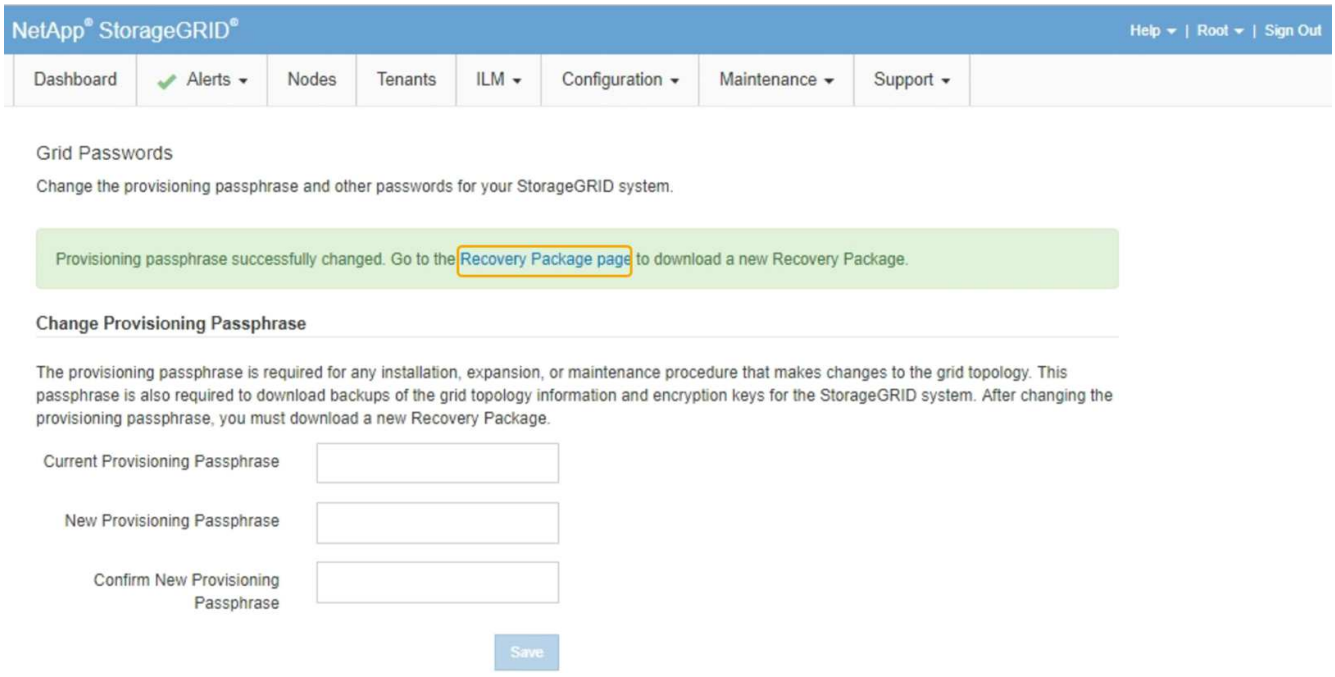


2. 输入当前配置密码短语。
3. 输入新的密码短语。密码短语必须至少包含8个字符、并且不超过32个字符。密码短语区分大小写。

   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。

4. 重新输入新密码短语、然后单击*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。此更改所需时间应少于一分钟。



5. 选择成功横幅中的*恢复软件包页面*链接。
6. 从网格管理器下载新的恢复软件包。选择*维护*>*恢复包*并输入新的配置密码短语。

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。

更改浏览器会话超时

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

GUI 非活动超时默认为 900 秒（ 15 分钟）。如果用户的浏览器会话在此时间内未处于活动状态，则此会话将超时。

您可以根据需要通过设置 GUI 非活动超时显示选项来增加或减少超时时间。

如果启用了单点登录(SSO)、并且用户的浏览器会话超时、则系统的行为就像用户手动单击*注销*一样。用户必须重新输入其 SSO 凭据才能再次访问 StorageGRID 。

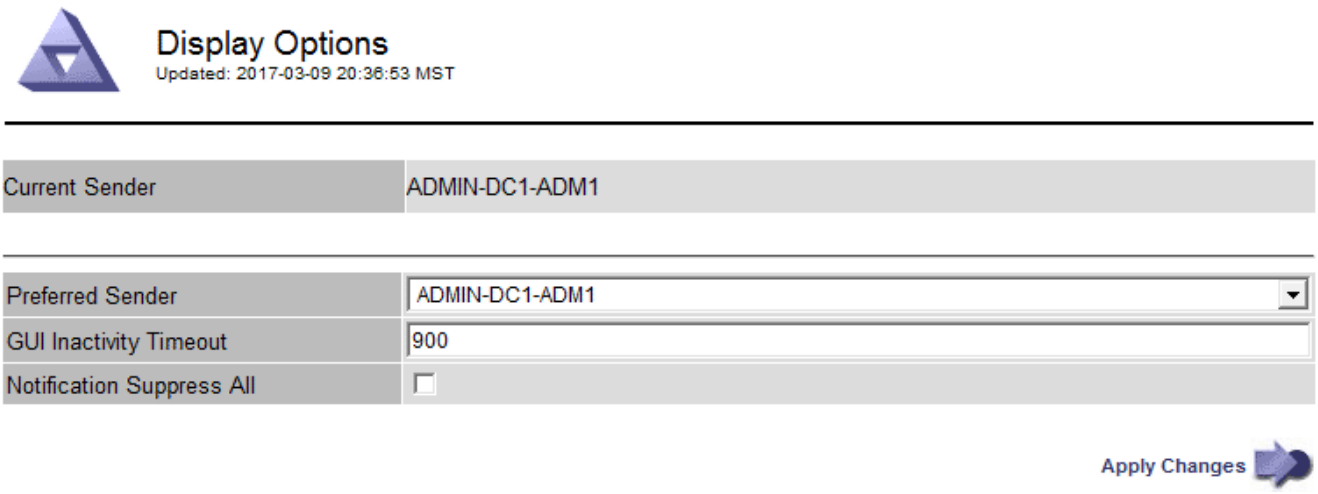
用户会话超时也可通过以下方式控制：

- 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。用户的身份验证过期后，即使尚未达到 GUI 非活动超时值，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（假设已为 StorageGRID 启用 SSO ）。

步骤

1. 选择*配置*>*系统设置*>*显示选项*。
2. 对于 * 图形用户界面非活动超时 * ，请输入 60 秒或更长时间的超时期限。

   如果不想使用此功能，请将此字段设置为 0 。用户在登录后 16 小时，身份验证令牌过期时将注销。



3. 单击 * 应用更改 * 。

   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。

相关信息

"单点登录的工作原理"

"使用租户帐户"

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。

关于此任务

如果问题描述 具有此 StorageGRID 系统的软件许可证，则信息板上的 " 运行状况 " 面板将包含一个 " 许可证状态 " 图标和一个 * 许可证 * 链接。此数字表示存在多少个与许可证相关的问题。

步骤

要查看许可证，请执行以下操作之一：

- 从信息板上的"运行状况"面板中、单击许可证状态图标或*许可证*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。

此时将显示 License 页面，其中提供了有关当前许可证的以下只读信息：

- StorageGRID 系统 ID ，此 ID 是此 StorageGRID 安装的唯一标识号
- 许可证序列号
- 网格的许可存储容量
- 软件许可证结束日期

- 支持服务合同结束日期
- 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。

正在更新**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。

您需要的内容

- 您必须具有一个新的许可证文件才能应用于StorageGRID 系统。
- 您必须具有特定的访问权限。
- 您必须具有配置密码短语。

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。
3. 单击 * 浏览 * 。
4. 在打开对话框中、找到并选择新的许可证文件 (`.txt`)、然后单击*打开*。

   此时将验证并显示新许可证文件。

5. 单击 * 保存 * 。

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。

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。

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、请参见有关使用租户帐户的信息。
- `/private`：访问权限仅限于Grid Manager用户、并且取决于配置的组权限。这些API仅供内部使用、不会公开记录。这些API也可能会更改、恕不另行通知。

相关信息

"使用租户帐户"

"Prometheus：查询基础知识"

网格管理 **API** 操作

网格管理 API 将可用的 API 操作组织到以下几节中。

- * 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情况。
- * 警报 * —用于列出当前警报（旧系统）并返回有关网格运行状况的信息的操作，包括当前警报和节点连接状态摘要。
- **alert-histori** —对已解决警报执行的操作。
- * 警报接收器 * —对警报通知接收器（电子邮件）的操作。
- **alert-rules** —对警报规则执行的操作。
- **alert-silences** —对警报静音执行的操作。
- * 警报 * - 对警报执行的操作。
- * 审核 * —用于列出和更新审核配置的操作。
- * 身份验证 * —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，请参见 "`防止跨站点请求伪造` " 。

- * 客户端证书 * —用于配置客户端证书以便使用外部监控工具安全访问 StorageGRID 的操作。
- **config** —与网格管理 API 的产品版本和版本相关的操作。您可以列出该版本支持的网格管理 API 的产品版本和主要版本，并且可以禁用已弃用的 API 版本。
- "*deactived-features * - 用于查看可能已停用的功能的操作 " 。
- **DNS-servers** —用于列出和更改已配置外部 DNS 服务器的操作。
- * 端点域名 * —用于列出和更改端点域名的操作。
- * 擦除编码 * —擦除编码配置文件的操作。
- * 扩展 * —扩展操作（过程级）。
- * 扩展节点 * —扩展操作（节点级别）。
- * 扩展站点 * —扩展操作（站点级）。
- * 网格网络 * —用于列出和更改网格网络列表的操作。
- * 网格密码 * —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。

- **identity-source** —用于配置外部身份源以及手动同步联合组和用户信息的操作。
- * ILM * —信息生命周期管理（ ILM ）操作。
- * 许可证 * —用于检索和更新 StorageGRID 许可证的操作。
- * 日志 * —用于收集和下载日志文件的操作。
- * 指标 * —对 StorageGRID 指标的操作，包括单个时间点的即时指标查询和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。

- "node-health* " —对节点运行状况执行的操作。
- * ntp-servers* —用于列出或更新外部网络时间协议（ NTP ）服务器的操作。
- * 对象 * - 对对象和对象元数据执行的操作。
- * 恢复 * —恢复操作步骤 的操作。
- **recovery-package** —下载恢复软件包的操作。
- * 区域 * - 用于查看和创建区域的操作。
- * s3-object-lock* —对全局 S3 对象锁定设置执行的操作。
- * 服务器证书 * —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 类 * —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。

发出**API**请求

Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

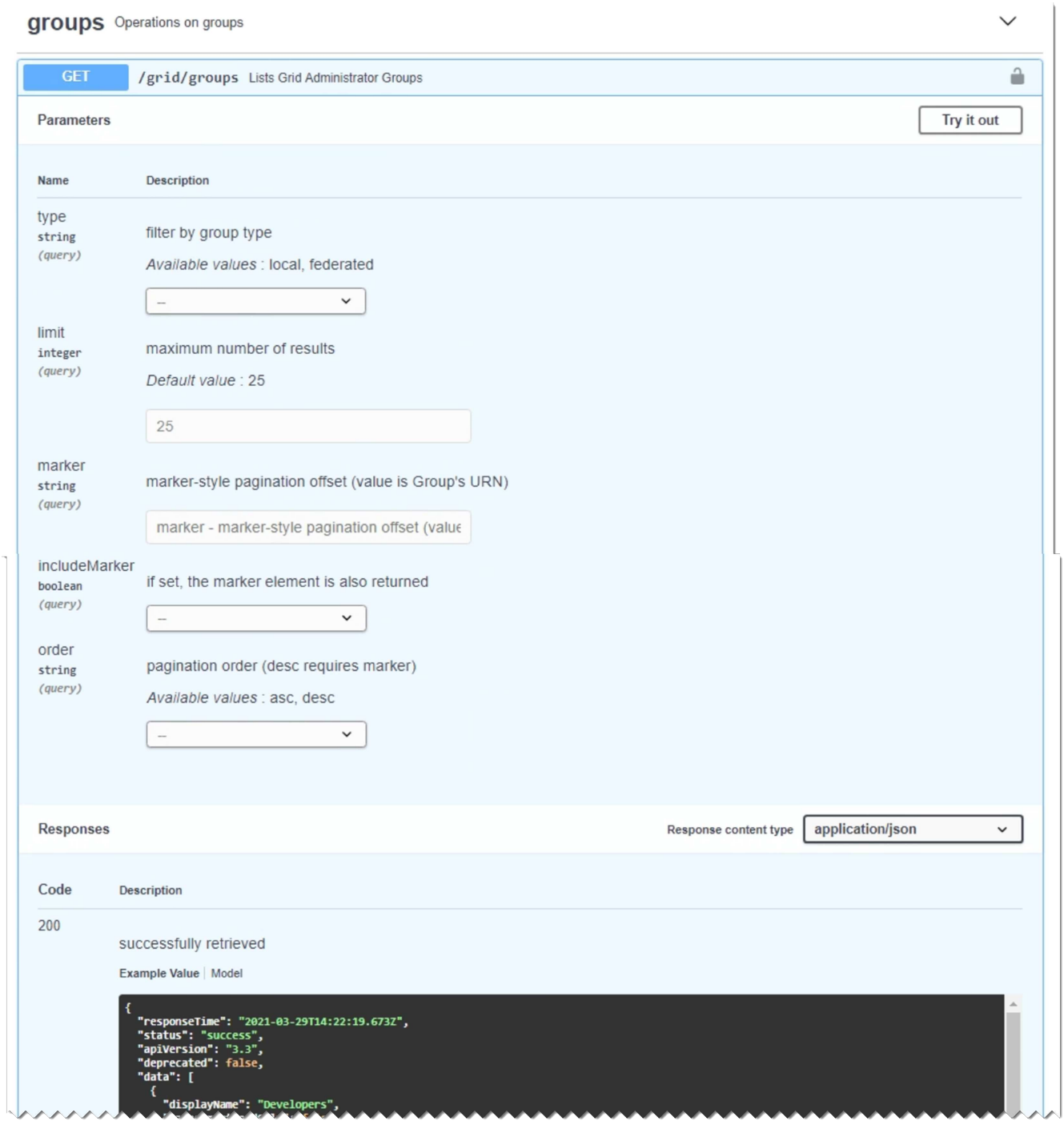
> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

步骤

1. 从网格管理器标题中选择*帮助*>* API文档*。
2. 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 。

3. 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。



4. 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。
5. 确定是否需要修改示例请求正文。如果是、您可以单击*型号*来了解每个字段的要求。
6. 单击 * 试用 * 。
7. 提供所需的任何参数，或根据需要修改请求正文。
8. 单击 * 执行 * 。
9. 查看响应代码以确定请求是否成功。

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
  ]
}
```

为请求指定**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、则使用**API**

如果已为StorageGRID 系统启用单点登录(SSO)、则不能使用标准身份验证API请求登录和注销网格管理API或租户管理API。

如果启用了单点登录、请登录到**API**

如果已启用单点登录(SSO)、则必须对一系列API请求进行问题描述 处理、才能从AD FS获取对网格管理API或租户管理API有效的身份验证令牌。

您需要的内容

- 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 、则可能会看到错误：不受支持的SAML版本。

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 用户名
- 安装 StorageGRID 的域
- StorageGRID 的地址
- 如果要访问租户管理API、请输入租户帐户ID。

+

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 以删除 JSON 编码。

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

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

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

c. 保存 `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=For
msAuthentication" --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、则从**API**中注销

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 。

关于此任务

如果需要，只需从组织的单个注销页面注销即可注销 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=fZDNboMwEI
RfhZ...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
```

使用**StorageGRID** 安全证书

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

StorageGRID 使用两种类型的安全证书：

- 使用 HTTPS 连接时需要 * 服务器证书 * 。服务器证书用于在客户端和服务器之间建立安全连接，向客户端验证服务器的身份并为数据提供安全通信路径。服务器和客户端都有一个证书副本。

- * 客户端证书 * 可对服务器的客户端或用户身份进行身份验证，从而提供比单独使用密码更安全的身份验证。客户端证书不会对数据进行加密。

当客户端使用 HTTPS 连接到服务器时，服务器会使用包含公有 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）。

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 。StorageGRID 还包括一个内置证书颁发机构(Certificate Authority、CA)、用于在系统安装期间生成内部CA证书。默认情况下、这些内部CA证书用于保护内部StorageGRID 流量的安全。虽然您可以在非生产环境中使用内部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。此外，还支持无证书的不安全连接，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符合服务器证书的系统强化准则。

  "系统强化"

- 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。

证书	证书类型	**Description**	导航位置	详细信息
管理员客户端证书	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>*访问控制*>*客户端证书*	"配置管理员客户端证书"

证书	证书类型	**Description**	导航位置	详细信息
身份联合证书	服务器	对StorageGRID 与外部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、从而允许管理组和用户由外部系统进行管理。	配置>*访问控制*>*身份联合*	"使用身份联合"
单点登录（ SSO ）证书	服务器	对用于单点登录(SSO)请求的Active Directory联合身份验证服务(AD FS)和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"
密钥管理服务器（ KMS ）证书	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>*系统设置*>*密钥管理服务器*	"添加密钥管理服务器(KMS)"
通过电子邮件发送警报通知证书	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*	"监控和放大；故障排除"

证书	证书类型	Description	导航位置	详细信息
负载平衡器端点证书	服务器	对S3或Swift客户端与网关节点或管理节点上的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。 *注：*负载平衡器证书是正常StorageGRID 操作期间使用量最多的证书。	配置>*网络设置*>*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 "为 FabricPool 配置 StorageGRID"
管理接口服务器证书	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。 您可以使用内部CA证书或上传自定义证书。	配置>*网络设置*>*服务器证书*	• "配置服务器证书" • "为网格管理器和租户管理器配置自定义服务器证书"
云存储池端点证书	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	"使用 ILM 管理对象"

证书	证书类型	Description	导航位置	详细信息
平台服务端点证书	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 *	"使用租户帐户"
对象存储API服务端点服务器证书	服务器	对与存储节点上的本地分布路由器(LDR)服务或网关节点上已弃用的连接负载平衡器(CLB)服务的安全S3或Swift客户端连接进行身份验证。	配置>*网络设置*>*负载平衡器端点*	"配置自定义服务器证书以连接到存储节点或CLB服务"

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。

控制管理员对**StorageGRID** 的访问

您可以通过以下方式控制管理员对StorageGRID 系统的访问：打开或关闭防火墙端口、管理管理组和用户、配置单点登录(Single Sign-On、SSO)以及提供客户端证书以允许对StorageGRID 指标进行安全外部访问。

- "通过防火墙控制访问"
- "使用身份联合"
- "管理管理组"
- "管理本地用户"
- "对StorageGRID 使用单点登录(SSO)"
- "配置管理员客户端证书"

通过防火墙控制访问

如果要通过防火墙控制访问，请打开或关闭外部防火墙上的特定端口。

在外部防火墙上控制访问

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。

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"

"如果StorageGRID 未使用SSO、则创建租户帐户"

"摘要：客户端连接的 IP 地址和端口"

"管理不可信客户端网络"

"安装 Ubuntu 或 Debian"

"安装 VMware"

"安装 Red Hat Enterprise Linux 或 CentOS"

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 。

配置身份联合

如果您希望在Active Directory、OpenLDAP或Oracle Directory Server等其他系统中管理管理管理组和用户、则可以配置身份联合。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 如果您计划启用单点登录(SSO)、则必须使用Active Directory作为联合身份源、并使用AD FS作为身份提供程序。请参见"`使用单点登录的要求。`"
- 您必须使用Active Directory、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、必须联系技术支持。

- 如果您计划使用传输层安全（ Transport Layer Security ， TLS ）与 LDAP 服务器进行通信，则身份提供程序必须使用 TLS 1.2 或 1.3 。

关于此任务

如果要导入以下类型的联合组、则必须为网格管理器配置身份源：

- 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。

步骤

1. 选择*配置*>*访问控制*>*身份联合*。
2. 选择 * 启用身份联合 * 。

   此时将显示用于配置LDAP服务器的字段。

3. 在 LDAP 服务类型部分中，选择要配置的 LDAP 服务类型。

   您可以选择* Active Directory*、* OpenLDAP*或*其他*。

如果选择* OpenLDAP*、则必须配置OpenLDAP服务器。请参见有关配置OpenLDAP服务器的准则。

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。
   - * 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. 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服务器的服务器主机名或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`
   - * 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。

6. 在*传输层安全(TLS)*部分中、选择一个安全设置。
   - 使用**STARTTLS (**建议**)**：使用STARTTLS保护与LDAP服务器的通信安全。这是建议的选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。出于兼容性原因、支持此选项。
   - * 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。

     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。

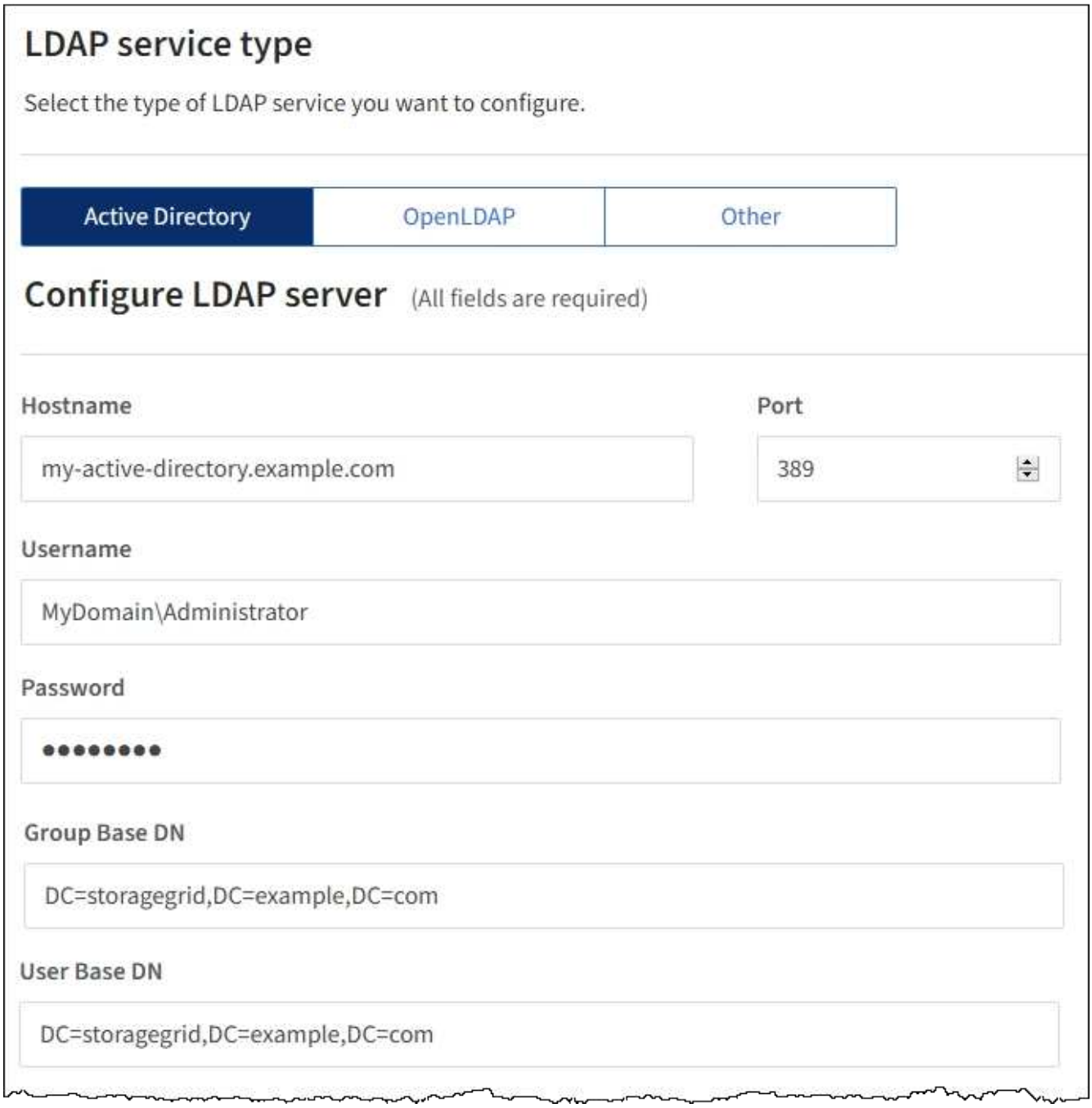
     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

8. 或者、选择*测试连接*以验证LDAP服务器的连接设置。

   如果连接有效、页面右上角将显示一条确认消息。

9. 如果连接有效、请选择*保存*。

   以下屏幕截图显示了使用Active Directory的LDAP服务器的示例配置值。



相关信息

"支持传出 TLS 连接的密码"

"使用单点登录的要求"

"创建租户帐户"

"使用租户帐户"

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。

memberOf 和 fint 覆盖

应启用成员和精简覆盖。有关详细信息、请参见《OpenLDAP管理员指南》中有关反向组成员资格维护的说明。

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OpenLDAP管理员指南中有关反向组成员资格维护的信息。

相关信息

"OpenLDAP 文档：版本 2.4 管理员指南"

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 必须启用身份源。

步骤

1. 选择*配置*>*访问控制*>*身份联合*。

   此时将显示"Identity Federation"页面。*同步*按钮位于页面底部。

2. 单击*同步*。

   确认消息指示同步已成功启动。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。

正在禁用身份联合

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

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*已启用*或*沙盒模式*、则*启用身份联合*复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 * 已禁用 * 。

步骤

1. 选择*配置*>*访问控制*>*身份联合*。
2. 取消选中*启用身份联合*复选框。
3. 单击 * 保存 * 。

相关信息

"禁用单点登录"

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。

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。

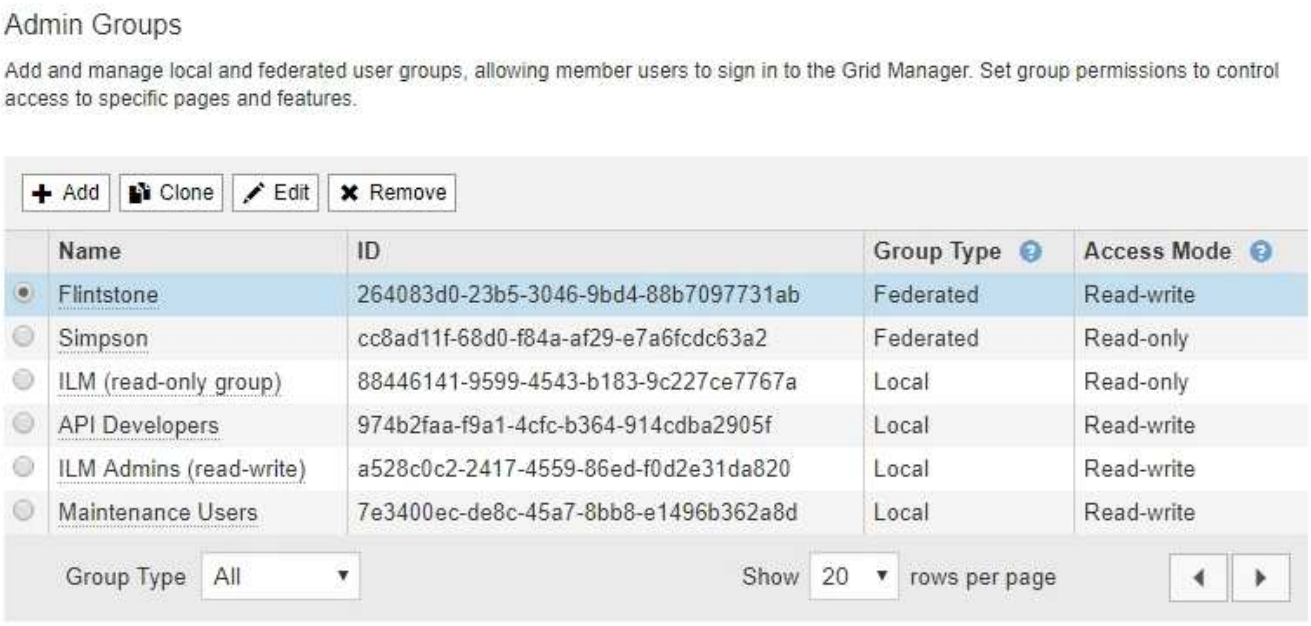
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 如果您计划导入联合组、则必须已配置身份联合、并且已配置的身份源中必须已存在此联合组。

步骤

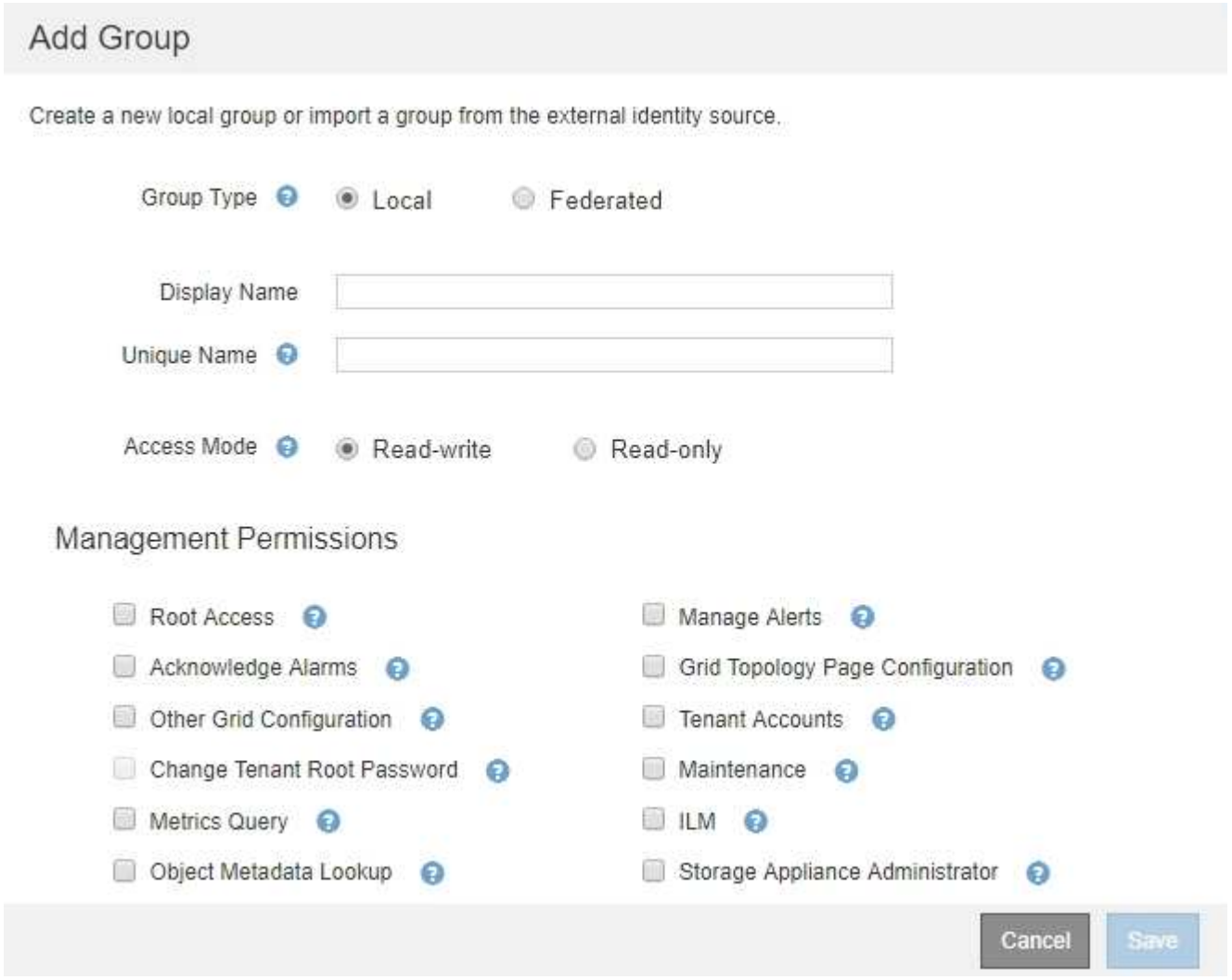
1. 选择*配置访问控制管理组。

   此时将显示Admin Groups页面、其中列出了任何现有的管理组。



2. 选择 * 添加 * 。

此时将显示添加组对话框。



3. 对于组类型、如果要创建仅在StorageGRID 中使用的组、请选择*本地*；如果要从身份源导入组、请选择*联合*。
4. 如果选择了*本地*、请输入组的显示名称。显示名称是显示在网格管理器中的名称。例如，" M维护用户 " 或 "`ILM 管理员。`
5. 输入组的唯一名称。
   - 本地：输入所需的唯一名称。例如、“ILM管理员。”
   - 联合：输入组在配置的身份源中显示的名称。
6. 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。他们不能在网格管理器或网格管理 API 中进行任何更改或执行任何操作。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。

7. 选择一个或多个管理权限。

   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 。
8. 选择 * 保存 * 。

   此时将创建新组。如果此组为本地组、则现在可以添加一个或多个用户。如果这是联合组、则身份源将管理属于该组的用户。

相关信息

"管理本地用户"

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。

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）

- 在配置和维护页面上查看特定信息

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root访问权限。

根访问

通过此权限，可以访问所有网格管理功能。

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。

确认警报(旧系统)

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。

网格拓扑页面配置

通过此权限、您可以访问以下菜单选项：

- 可从*支持*工具网格拓扑*页面访问的配置选项卡。
- 节点***事件*选项卡上的*重置事件计数*链接。

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。

- 警报(旧系统)：
  - 全局警报
  - 旧电子邮件设置
- * ILM ：
  - 存储池
  - 存储等级
- 配置*网络设置
  - 链路成本
- 配置*系统设置：
  - 显示选项
  - 网格选项
  - 存储选项
- 配置*监控*：

- 事件

- 支持：
  - AutoSupport

租户帐户

通过此权限可以访问*租户***租户帐户*页面。

> 网格管理API版本1 (已弃用)使用此权限管理租户组策略、重置Swift管理员密码以及管理root用户S3访问密钥。

更改租户**root**密码

通过此权限、您可以访问租户帐户页面上的*更改根密码*选项、从而可以控制谁可以更改租户的本地root用户的密码。不具有此权限的用户无法看到*更改根密码*选项。

> 您必须先为组分配租户帐户权限、然后才能分配此权限。

维护

通过此权限、您可以访问以下菜单选项：

- 配置*系统设置：
  - 域名*
  - 服务器证书*
- 配置*监控*：
  - 审核*
- 配置*访问控制：
  - 网格密码
- 维护*维护任务*
  - 停用
  - 扩展
  - 恢复
- 维护*网络：
  - DNS服务器*
  - 网格网络*
  - NTP服务器*
- 维护*系统：
  - 许可证*
  - 恢复软件包
  - 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标有星号的页面。

指标查询

通过此权限、您可以访问*支持*工具*指标*页面。通过此权限，还可以使用网格管理 API 的 * 指标 * 部分访问自定义的 Prometheus 指标查询。

ILM

通过此权限，您可以访问以下 * ILM * 菜单选项：

- 擦除编码
- 规则
- * 策略 *
- 区域

> 对* ILM *存储池*和 ILM *存储级别*菜单选项的访问由"其他网格配置"和"网格拓扑页面配置"权限控制。

对象元数据查找

通过此权限可以访问* ILM *对象元数据查找*菜单选项。

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。

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。

从网格管理**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用户和具有root访问权限的组中的用户)都不能更改任何租户帐户的root用户的密码

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 * 活动功能 * 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。

有关详细信息、请参见实施S3或Swift客户端应用程序的说明。

步骤

1. 访问网格管理 API 的 Swagger 文档。
2. 找到停用功能端点。
3. 要停用*更改租户根密码*等功能、请向API发送如下正文：

```
{ "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。`

4. 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。此时、"更改租户根密码"管理权限将显示在用户界面中、如果用户拥有" root访问"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 } }
```

相关信息

"使用网格管理API"

修改管理组

您可以修改管理组以更改与该组关联的权限。对于本地管理组、您还可以更新显示名称。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

步骤

1. 选择*配置访问控制管理组。
2. 选择组。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击 * 编辑 * 。
4. M、对于本地组、输入将显示给用户的组名称、例如"维护用户"。

   您不能更改唯一名称、即内部组名称。

5. 也可以更改组的访问模式。
   - * 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。他们不能在网格管理器或网格管理 API 中进行任何更改或执行任何操作。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。

6. 也可以添加或删除组权限。

   请参见有关管理组权限的信息。

7. 选择 * 保存 * 。

相关信息

[管理组权限]

删除管理组

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。删除管理员组会从该组中删除任何管理员用户、但不会删除这些管理员用户。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

删除组时、分配给该组的用户将丢失对网格管理器的所有访问权限、除非其他组授予了这些用户的权限。

步骤

1. 选择*配置访问控制管理组。

2. 选择组的名称。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 选择 * 删除 * 。
4. 选择 * 确定 * 。

管理本地用户

您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。

网格管理器包括一个名为"`root"的预定义本地用户。`虽然您可以添加和删除本地用户、但不能删除root用户。

> 如果已启用单点登录(SSO)、则本地用户无法登录到StorageGRID。

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

创建本地用户

如果已创建本地管理组、则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组。组的权限控制用户可以访问的网格管理器功能。

关于此任务

您只能创建本地用户、并且只能将这些用户分配给本地管理组。联合用户和联合组使用外部身份源进行管理。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 单击 * 创建 * 。
3. 输入用户的显示名称、唯一名称和密码。
4. 将用户分配给一个或多个控制访问权限的组。

   组名称列表是从组表生成的。

5. 单击 * 保存 * 。

相关信息

"管理管理组"

修改本地用户的帐户

您可以修改本地管理员用户的帐户以更新用户的显示名称或组成员资格。您还可以临时阻止用户访问系统。

关于此任务

您只能编辑本地用户。联合用户详细信息会自动与外部身份源同步。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 选择要编辑的用户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击 * 编辑 * 。
4. 或者、也可以更改名称或组成员资格。
5. 或者、要防止用户临时访问系统、请选中*拒绝访问*。
6. 单击 * 保存 * 。

   新设置将在用户下次注销后重新登录到网格管理器时应用。

删除本地用户的帐户

您可以删除不再需要访问网格管理器的本地用户帐户。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 选择要删除的本地用户。

   您不能删除预定义的root本地用户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击 * 删除 * 。
4. 单击 * 确定 * 。

更改本地用户的密码

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。此外、有权访问Admin Users页面的用户还可以更改其他本地用户的密码。

关于此任务

您只能更改本地用户的密码。联合用户必须在外部身份源中更改自己的密码。

步骤

1. 选择*配置*>*访问控制*>*管理用户*。
2. 从用户页面中、选择用户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。然后、您可以使用浏览器的"查找"功能在当前显示的行中搜索特定项。

3. 单击*更改密码*。

4. 输入并确认密码、然后单击*保存*。

对StorageGRID 使用单点登录(SSO)

StorageGRID 系统支持使用安全断言标记语言 2.0 （ SAML 2.0 ）标准的单点登录（ SSO ）。启用 SSO 后，所有用户都必须经过外部身份提供程序的身份验证，然后才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用户无法登录到 StorageGRID 。

- "单点登录的工作原理"
- "使用单点登录的要求"
- "配置单点登录"

单点登录的工作原理

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。

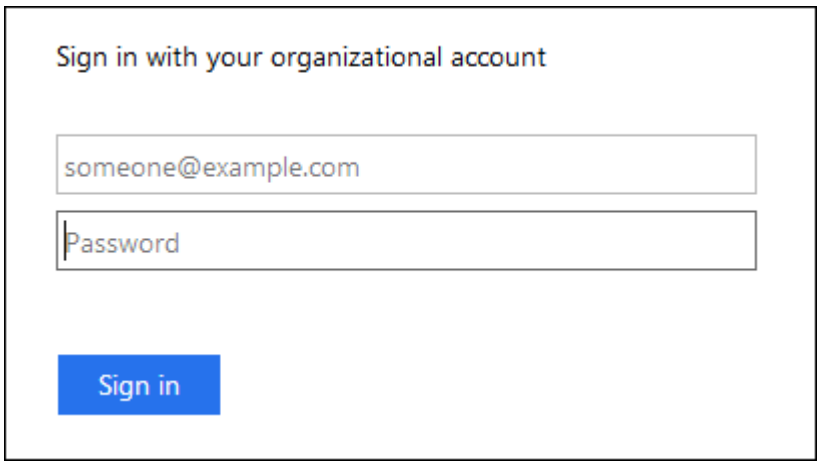
   - 如果这是您首次在此浏览器上访问此 URL ，系统将提示您输入帐户 ID ：

   - 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**、或者如果"*网格管理器"显示在近期帐户列表中、请选择此选项。
   - 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. 单击*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、并且您属于具有足够访问权限的联合组、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。

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. 找到用户界面右上角的 * 注销 * 链接。
2. 单击*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
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。

使用单点登录的要求

在为 StorageGRID 系统启用单点登录（ SSO ）之前，请查看本节中的要求。

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 ）。

身份提供程序要求

用于SSO的身份提供程序(IdP)必须满足以下要求：

- 以下任一版本的Active Directory联合身份验证服务(AD FS)：
  - AD FS 4.0、随Windows Server 2016提供

    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。

- 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

服务器证书要求

StorageGRID 在每个管理节点上使用管理接口服务器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AD FS中为StorageGRID 配置SSO依赖方信任时、您可以使用服务器证书作为向AD FS发出StorageGRID 请求的签名证书。

如果尚未为管理接口安装自定义服务器证书、应立即安装。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 依赖方信任关系中使用该证书。

> 建议不要在AD FS依赖方信任关系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AD FS中的依赖方信任。

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`。

相关信息

"通过防火墙控制访问"

"为网格管理器和租户管理器配置自定义服务器证书"

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 。

- "确认联合用户可以登录"
- "使用沙盒模式"
- "在AD FS中创建依赖方信任"
- "测试依赖方信任"
- "启用单点登录"
- "禁用单点登录"
- "临时禁用并重新启用一个管理节点的单点登录"

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

- 您正在使用Active Directory作为联合身份源、使用AD FS作为身份提供程序。

  "使用单点登录的要求"

步骤

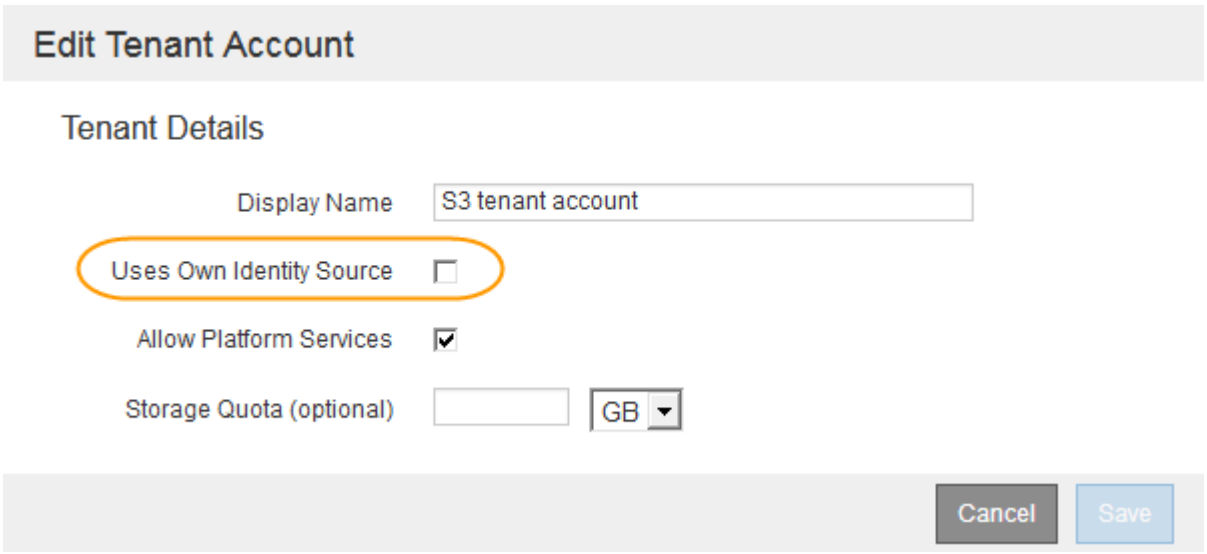
1. 如果存在现有租户帐户，请确认所有租户均未使用其自己的身份源。

   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*访问控制*>*身份联合*。
   c. 确认未选中*启用身份联合*复选框。
   d. 如果是、请确认不再需要可能用于此租户帐户的任何联合组、取消选中此复选框、然后单击*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"根访问"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、然后单击*编辑帐户*。
   c. 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、然后单击*保存*。



   此时将显示租户帐户页面。

   a. 选择租户帐户、单击*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、单击*访问控制*>*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"根访问"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

"使用单点登录的要求"

"管理管理组"

"使用租户帐户"

使用沙盒模式

在为StorageGRID 用户强制实施单点登录(SSO)之前、您可以使用沙盒模式配置和测试依赖方信任的Active Directory联合身份验证服务(AD FS)。启用SSO后、您可以重新启用沙盒模式以配置或测试新的和现有的依赖方信任。重新启用沙盒模式会暂时禁用StorageGRID 用户的SSO。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

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AD FS发送身份验证请求。反过来、AD FS会向StorageGRID 发送身份验证响应、指示授权请求是否成功。对于成功的请求、响应会为用户提供一个通用唯一标识符(UUID)。

要允许StorageGRID (服务提供商)和AD FS (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AD FS为每个管理节点创建依赖方信任。最后，您必须返回到 StorageGRID 以启用 SSO 。

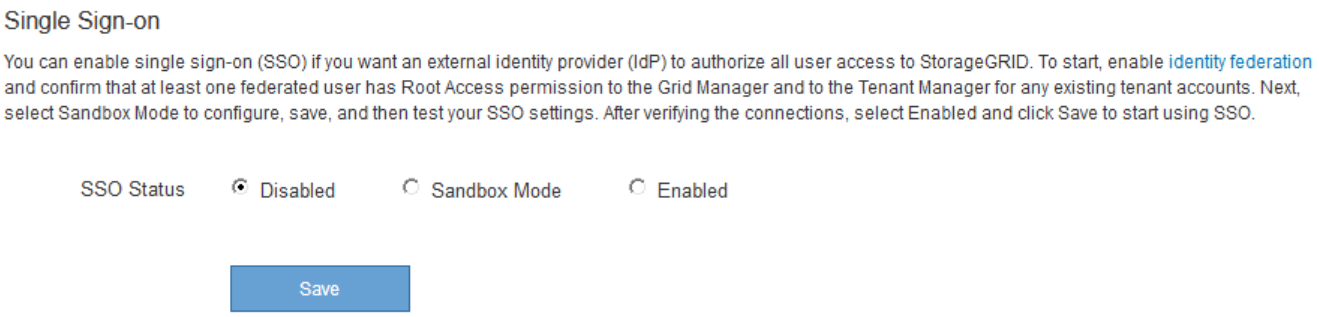
使用沙盒模式，可以轻松执行此背面配置，并在启用 SSO 之前测试所有设置。

强烈建议使用沙盒模式、但严格地说、这并不是必需的。如果您准备在StorageGRID 中配置SSO后立即创建AD FS依赖方信任、您无需测试每个管理节点的SSO和单点注销(SLO)进程、单击*已启用*、输入StorageGRID 设置、为AD FS中的每个管理节点创建依赖方信任、然后单击*保存*以启用SSO。

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、请确认您已将Active Directory配置为联合身份源。请参见"`使用单点登录的要求。`"

2. 选择*沙盒模式*选项。

   此时将显示身份提供程序和依赖方设置。在身份提供程序部分中、*服务类型*字段为只读。它显示了您正在使用的身份联合服务的类型(例如Active Directory)。

3. 在身份提供程序部分中：

   a. 输入与AD FS中显示的名称完全相同的联合服务名称。

      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。

   b. 指定在身份提供程序响应StorageGRID 请求发送SSO配置信息时是否要使用传输层安全(TLS)来保护连接。

      - * 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、请在* CA证书*文本框中复制并粘贴此证书。

      - * 请勿使用 TLS* ： 请勿使用 TLS 证书来保护连接。

4. 在依赖方部分中、指定在配置依赖方信任时要用于StorageGRID 管理节点的依赖方标识符。

   - 例如、如果您的网格只有一个管理节点、并且您预计将来不会添加更多管理节点、请输入 `SG` 或 `StorageGRID`。
   - 如果网格包含多个管理节点、请包含字符串 `[HOSTNAME]` 在标识符中。例如： `SG-[HOSTNAME]`。此操作将生成一个表、其中包含每个管理节点的依赖方标识符、该标识符基于节点的主机名。+注意：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。

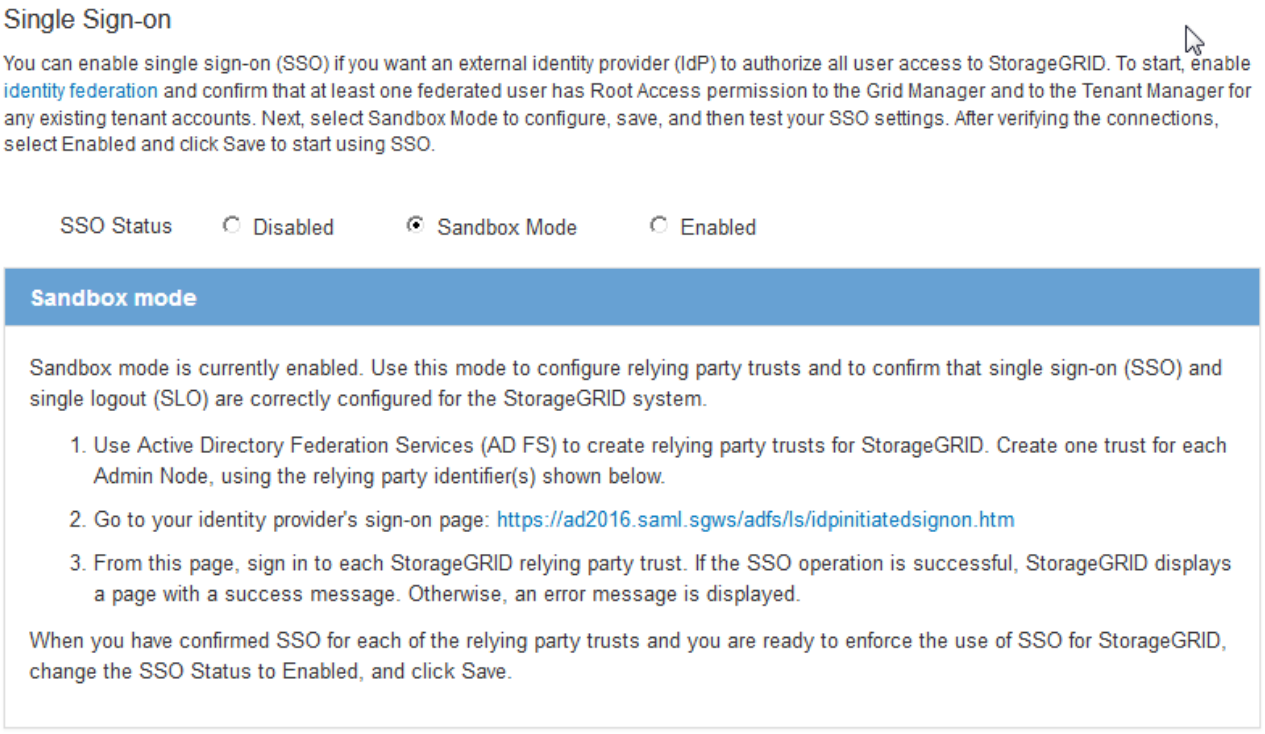
5. 单击 * 保存 * 。

   - 绿色复选标记将在 * 保存 * 按钮上显示几秒钟。

   - 此时将显示沙盒模式确认通知、确认现在已启用沙盒模式。您可以在使用AD FS为每个管理节点配置依

赖方信任并测试单点登录(SSO)和单点注销(SLO)进程时使用此模式。



相关信息

"使用单点登录的要求"

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。

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。

您需要的内容

- 您已在StorageGRID 中配置SSO、并且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。

关于此任务

这些说明适用于Windows Server 2016附带的AD FS 4.0。如果您使用的是Windows 2012 R2附带的AD FS 3.0、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。

步骤

1. 从Windows开始菜单中、右键单击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. 单击*应用*、然后单击*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. 单击*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*、然后单击*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. 单击*完成*、然后单击*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，请确认联合元数据地址是否正确，或者只需手动输入值即可。

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 和 "测试所有依赖方信任" 以确认配置正确。

通过导入联合元数据创建依赖方信任

您可以通过访问每个管理节点的 SAML 元数据来导入每个依赖方信任的值。

您需要的内容

- 您已在StorageGRID 中配置SSO、并且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。

关于此任务

这些说明适用于Windows Server 2016附带的AD FS 4.0。如果您使用的是Windows 2012 R2附带的AD FS 3.0、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。

步骤

1. 在Windows Server Manager中、单击*工具*、然后选择* AD FS管理*。
2. 在操作下、单击*添加依赖方信任*。
3. 在Welcome页面上、选择*声明感知*、然后单击*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. 单击*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*、然后单击*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. 单击*完成*、然后单击*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，请确认联合元数据地址是否正确，或者只需手动输入值即可。

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 和 "测试所有依赖方信任" 以确认配置正确。

手动创建依赖方信任

如果您选择不导入依赖部件信任的数据，则可以手动输入值。

您需要的内容

- 您已在StorageGRID 中配置SSO、并且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。

- 您已获得为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。
- 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。

关于此任务

这些说明适用于Windows Server 2016附带的AD FS 4.0。如果您使用的是Windows 2012 R2附带的AD FS 3.0、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。

步骤

1. 在Windows Server Manager中、单击*工具*、然后选择* AD FS管理*。
2. 在操作下、单击*添加依赖方信任*。
3. 在Welcome页面上、选择*声明感知*、然后单击*开始*。
4. 选择*手动输入有关依赖方的数据*、然后单击*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. 要启动声明规则向导、请单击*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*、然后单击*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. 单击*完成*、然后单击*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. 单击*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. 单击 * 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. 单击*应用*、然后单击*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 和 "测试所有依赖方信任" 以确认配置正确。

测试依赖方信任

在对StorageGRID 强制使用单点登录(SSO)之前、请确认已正确配置单点登录和单点注销(SLO)。如果您为每个管理节点创建了依赖方信任、请确认您可以对每个管理节点使用SSO和SLO。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您已在AD FS中配置一个或多个依赖方信任。

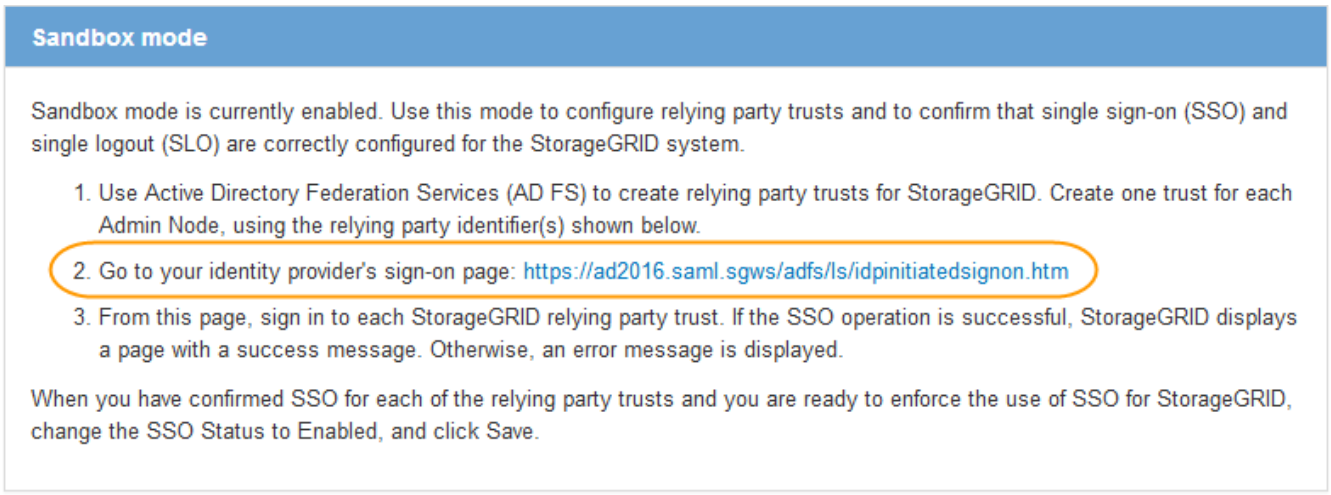
步骤

1. 选择*配置访问控制单点登录*。

此时将显示Single Sign-On页面、并选择了*沙盒模式*选项。

2. 在沙盒模式说明中、找到指向身份提供程序登录页面的链接。

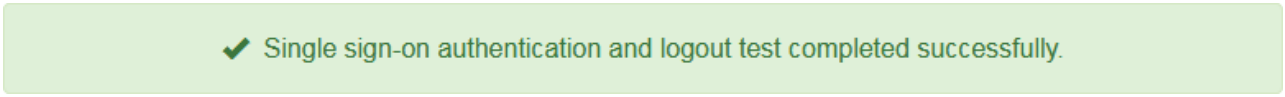
此URL是从您在*联合服务名称*字段中输入的值派生的。



3. 单击此链接、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。
4. 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、然后单击*登录*。

系统将提示您输入用户名和密码。

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



   - 如果 SSO 操作失败，则会显示一条错误消息。修复问题描述 ，清除浏览器的 Cookie 并重试。
6. 重复上述步骤以确认您可以登录到任何其他管理节点。

如果所有SSO登录和注销操作均成功、则可以启用SSO。

启用单点登录

在使用沙盒模式测试所有StorageGRID 依赖方信任之后、您可以启用单点登录(SSO)。

您需要的内容

- 您必须已从身份源导入至少一个联合组、并已将root访问管理权限分配给该组。对于任何现有租户帐户、您必须确认至少有一个联合用户对网格管理器和租户管理器具有root访问权限。
- 您必须已使用沙盒模式测试所有依赖方信任。

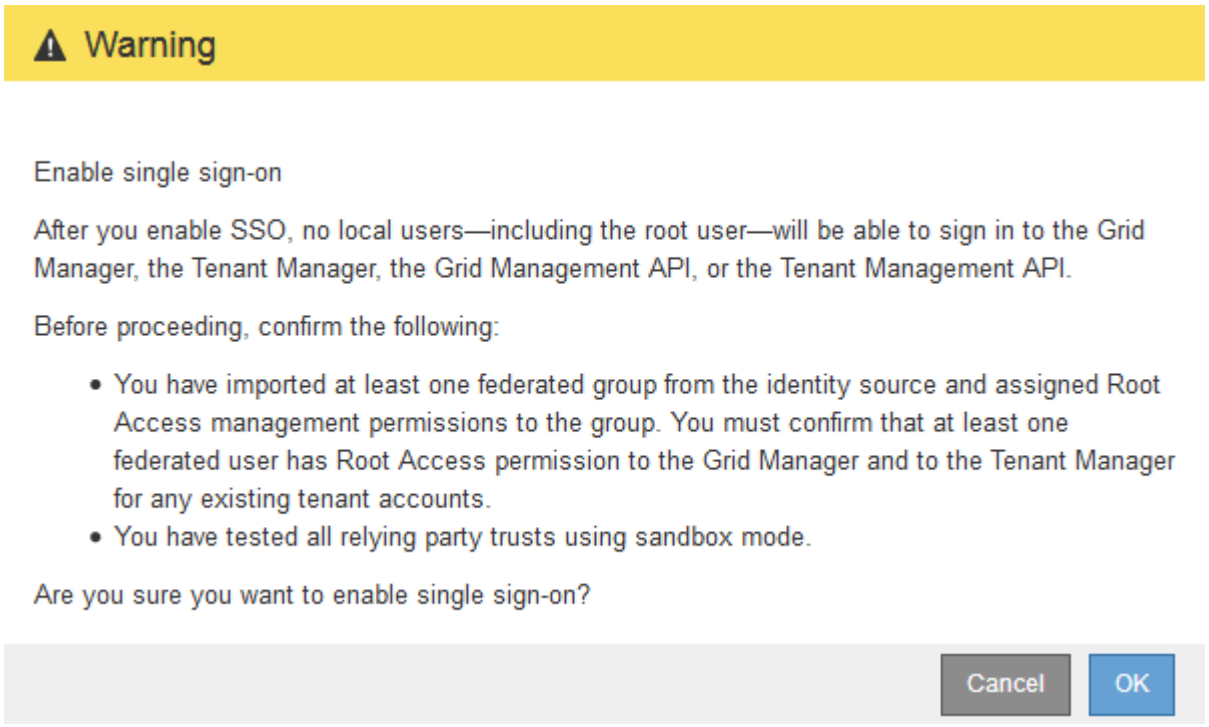
步骤

1. 选择*配置访问控制单点登录*。

   此时将显示Single Sign-On页面、并选择了*沙盒模式*。

2. 将 SSO 状态更改为 * 已启用 * 。
3. 单击 * 保存 * 。

   此时将显示一条警告消息。



4. 查看警告、然后单击*确定*。

   现在，已启用单点登录。

> 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 。

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。

- 您必须具有特定的访问权限。

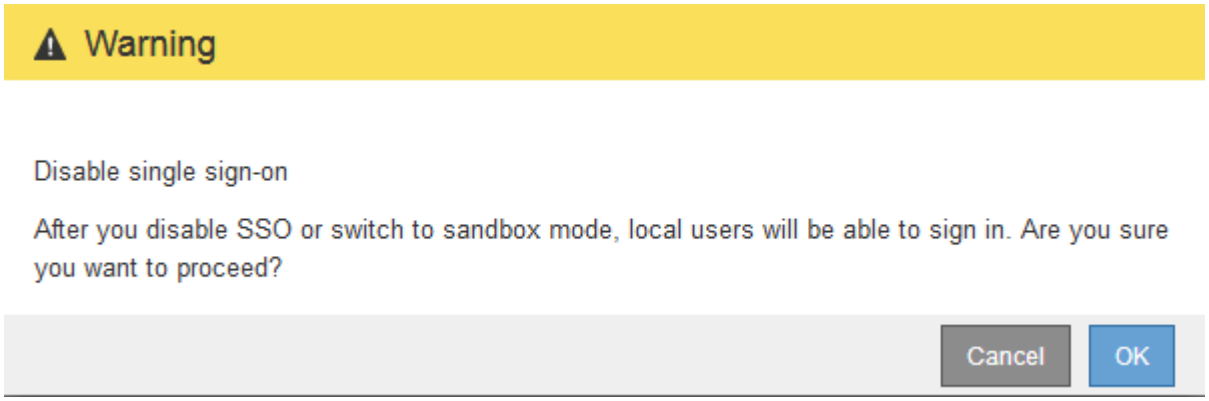
步骤

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. 单击 * 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. 单击 * 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 。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `Passwords.txt` 文件
- 您必须知道本地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。网格管理器的单点登录页面上的 * 启用 SSO* 复选框将保持选中状态，并且所有现有的 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. 单击 * 保存 * 。

      单击Single Sign-On页面中的*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. 单击*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。

相关信息

"配置单点登录"

配置管理员客户端证书

您可以使用客户端证书允许授权的外部客户端访问StorageGRID Prometheus数据库。客户端证书提供了一种使用外部工具监控StorageGRID 的安全方式。

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。

添加管理员客户端证书

要添加客户端证书、您可以提供自己的证书或使用网格管理器生成一个证书。

您需要的内容

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须知道管理节点的IP地址或域名。
- 您必须已配置StorageGRID 管理接口服务器证书并具有相应的CA包
- 如果要上传您自己的证书、则本地计算机上必须提供此证书的公有 密钥和专用密钥。

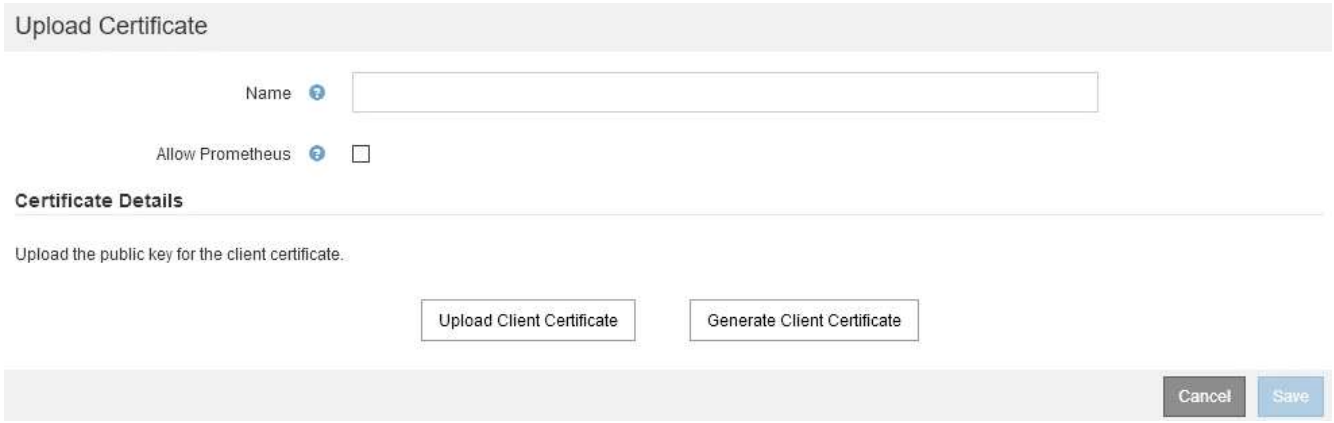
步骤

1. 在网格管理器中、选择*配置*>*访问控制*>*客户端证书*。

   此时将显示客户端证书页面。

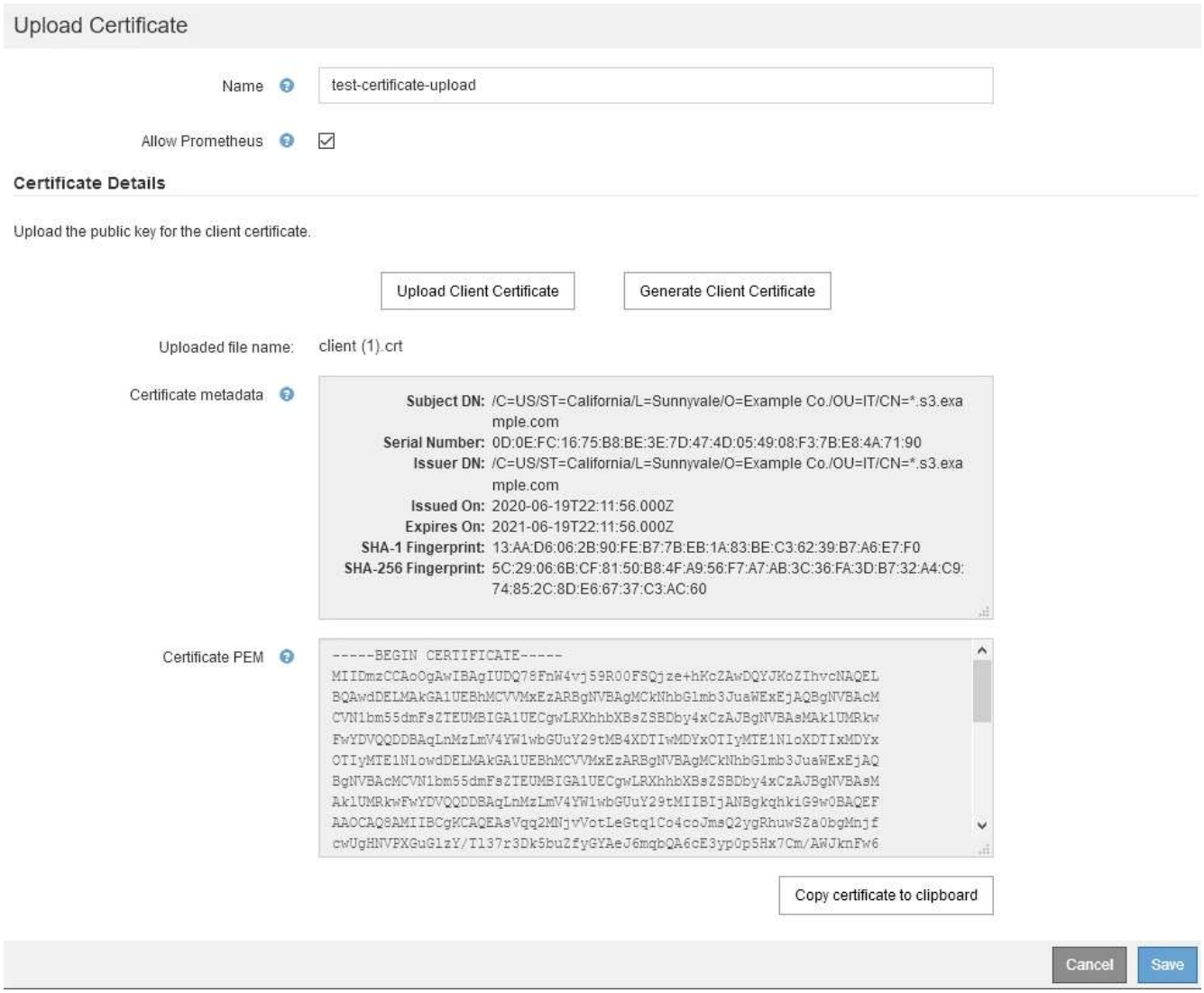
2. 选择 * 添加 * 。

   此时将显示上传证书页面。



3. 键入一个介于1到32个字符之间的证书名称。
4. 要使用外部监控工具访问Prometheus指标、请选中*允许Prometheus*复选框。
5. 上传或生成证书：
   a. 要上传证书、请转至 此处。
   b. 要生成证书、请转至 此处。
6. 要上传证书、请执行以下操作：
   a. 选择*上传客户端证书*。
   b. 浏览此证书的公有 密钥。

      上传证书的公有 密钥后、系统将填充*证书元数据*和*证书PEM*字段。



a. 选择*将证书复制到剪贴板*、然后将证书粘贴到外部监控工具中。

b. 使用编辑工具将私钥复制并粘贴到外部监控工具中。

c. 选择*保存*以在网格管理器中保存证书。

7. 要生成证书、请执行以下操作：

a. 选择*生成客户端证书*。

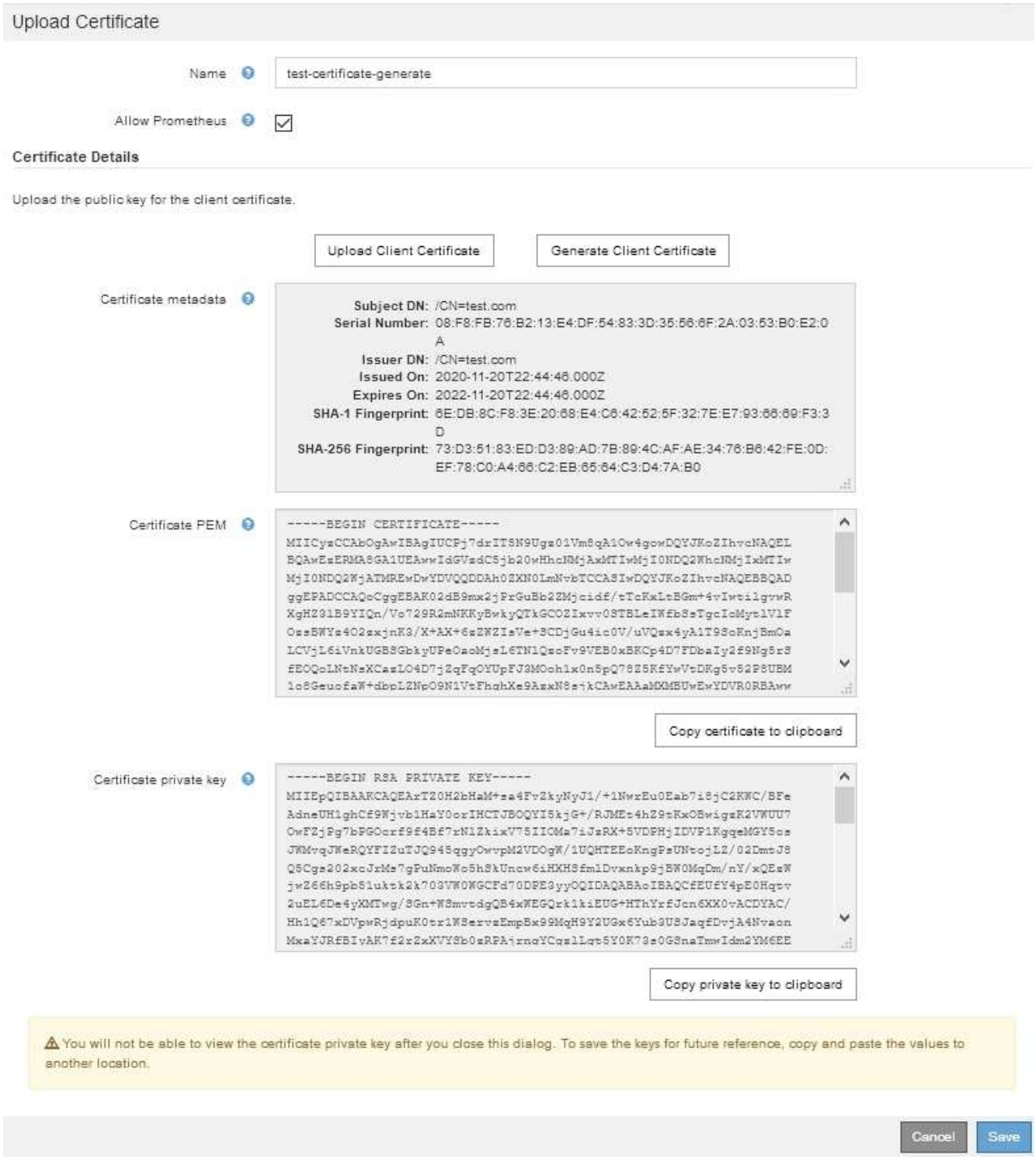
b. 输入管理节点的域名或IP地址。

c. (可选)输入一个X.509主题(也称为可分辨名称(Distinguished Name、DN))、以确定拥有证书的管理员。

d. (可选)选择证书的有效天数。默认值为730天。

e. 选择 * 生成 * 。

此时将填充*证书元数据*、*证书PEM*和*证书专用密钥*字段。



a. 选择*将证书复制到剪贴板*、然后将证书粘贴到外部监控工具中。

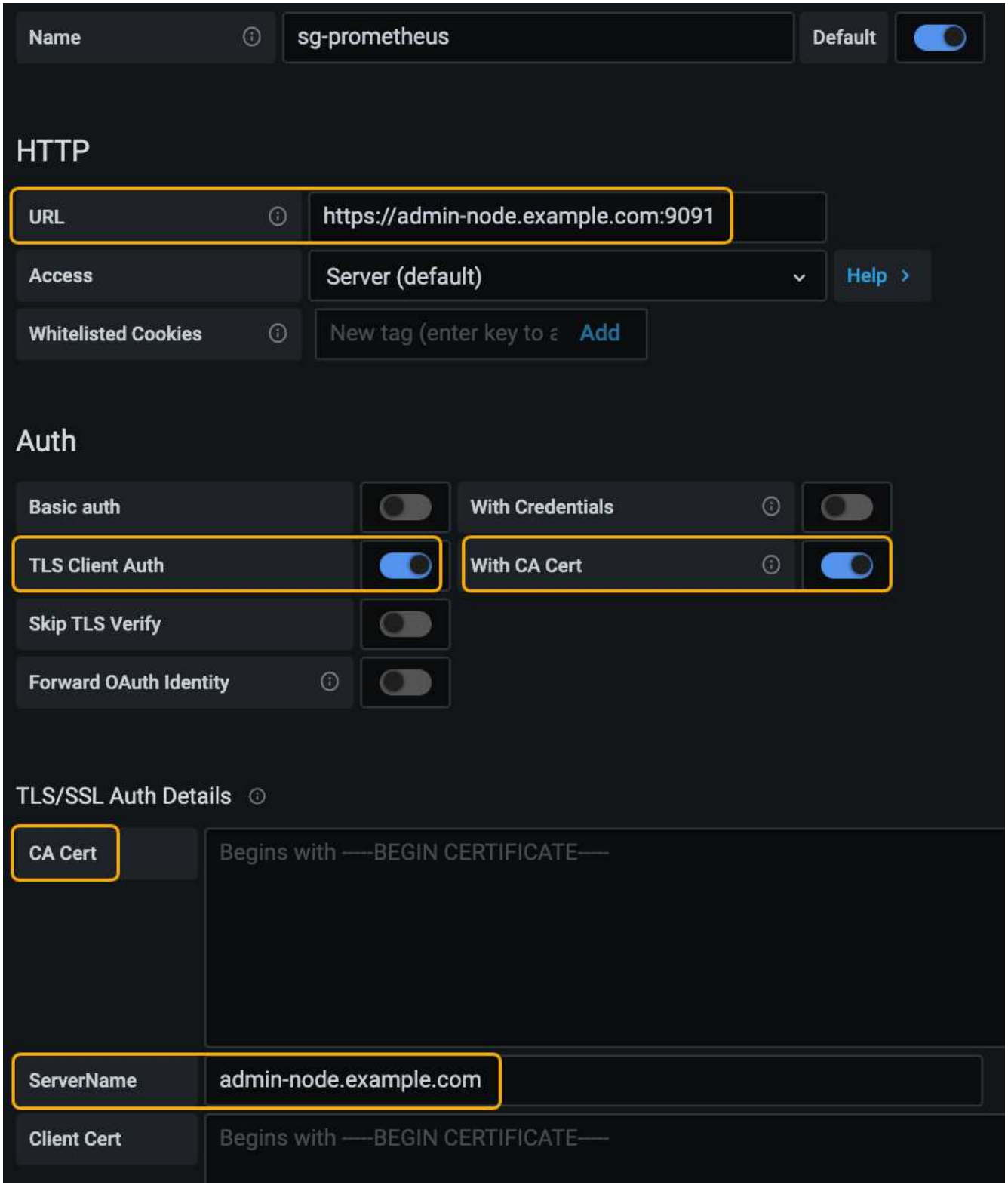
b. 选择*将私钥复制到剪贴板*、然后将密钥粘贴到外部监控工具中。

> 关闭此对话框后、您将无法查看此私钥。将密钥复制到安全位置。

c. 选择*保存*以在网格管理器中保存证书。

8. 在外部监控工具上配置以下设置，例如 Grafana 。

以下屏幕截图显示了一个 Grafana 示例：



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客户端授权*和*使用CA证书*。

d. 将管理接口服务器证书或CA捆绑包复制并粘贴到TLS/SSL身份验证详细信息下的"CA证书"中。

e. * 服务器名称 * ： 输入管理节点的域名。

服务器名称必须与管理接口服务器证书中显示的域名匹配。

f. 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StorageGRID 监控和故障排除说明。

相关信息

"使用StorageGRID 安全证书"

"为网格管理器和租户管理器配置自定义服务器证书"

"监控和放大；故障排除"

编辑管理员客户端证书

您可以编辑证书以更改其名称、启用或禁用Prometheus访问、或者在当前证书已过期时上传新证书。

您需要的内容

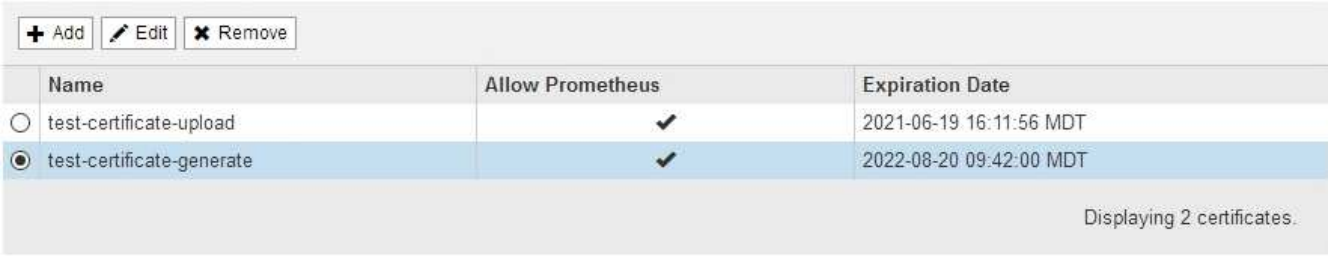
- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须知道管理节点的IP地址或域名。
- 如果您要上传新证书和私钥、它们必须在本地计算机上可用。

步骤

1. 选择*配置*>*访问控制*>*客户端证书*。

此时将显示客户端证书页面。此时将列出现有证书。

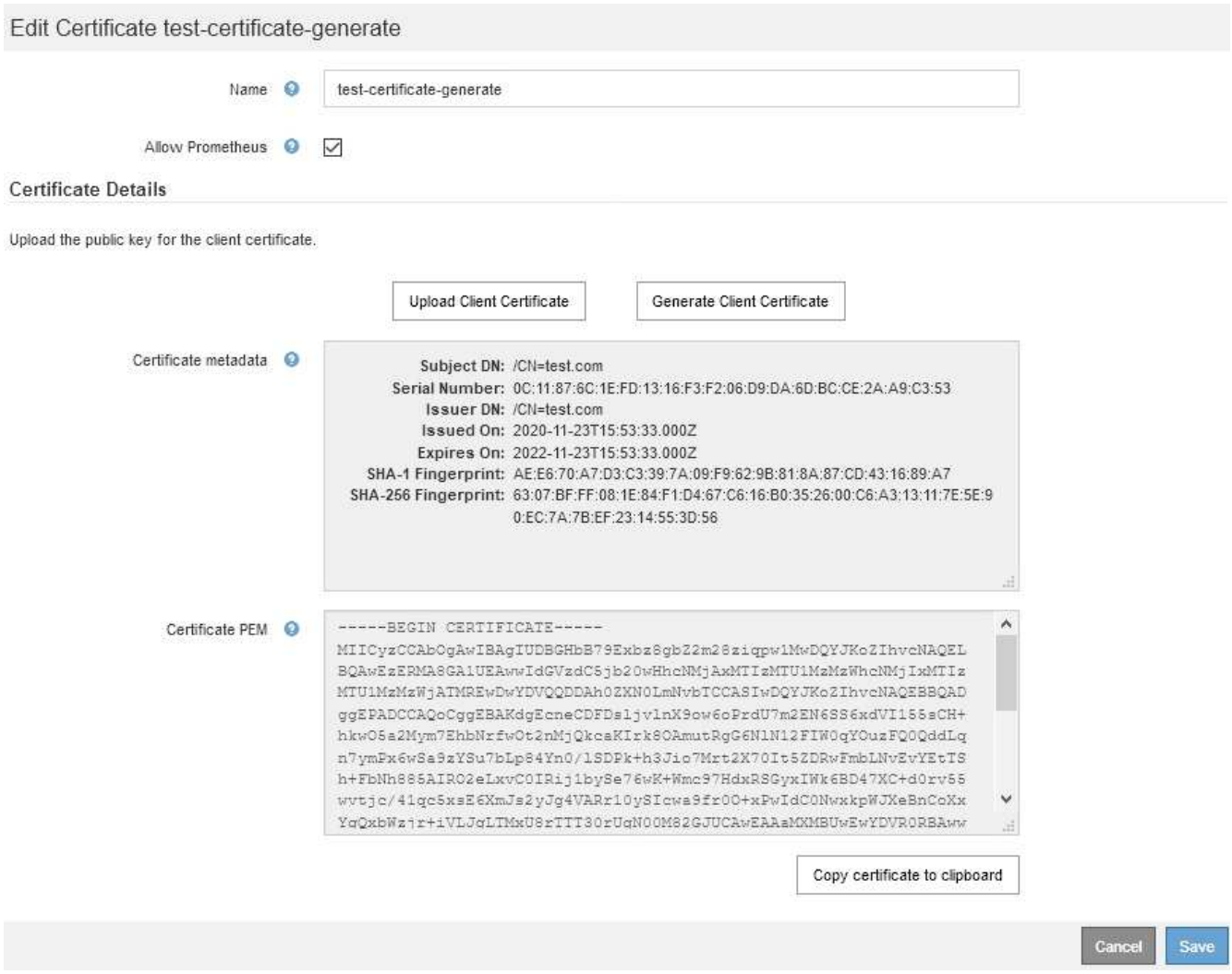
表中列出了证书到期日期。如果证书即将过期或已过期，则表中会显示一条消息并触发警报。



2. 选择要编辑的证书左侧的单选按钮。

3. 选择 * 编辑 * 。

此时将显示编辑证书对话框。



4. 对证书进行所需的更改。
5. 选择*保存*以在网格管理器中保存证书。
6. 如果您上传了新证书：
   a. 选择*将证书复制到剪贴板*将证书粘贴到外部监控工具。
   b. 使用编辑工具将新的私钥复制并粘贴到外部监控工具中。
   c. 在外部监控工具中保存并测试证书和私钥。
7. 如果生成了新证书：
   a. 选择*将证书复制到剪贴板*将证书粘贴到外部监控工具。
   b. 选择*将私钥复制到剪贴板*将证书粘贴到外部监控工具。

      关闭此对话框后、您将无法查看或复制此私钥。将密钥复制到安全位置。

   c. 在外部监控工具中保存并测试证书和私钥。

正在删除管理员客户端证书

如果您不再需要证书、可以将其删除。

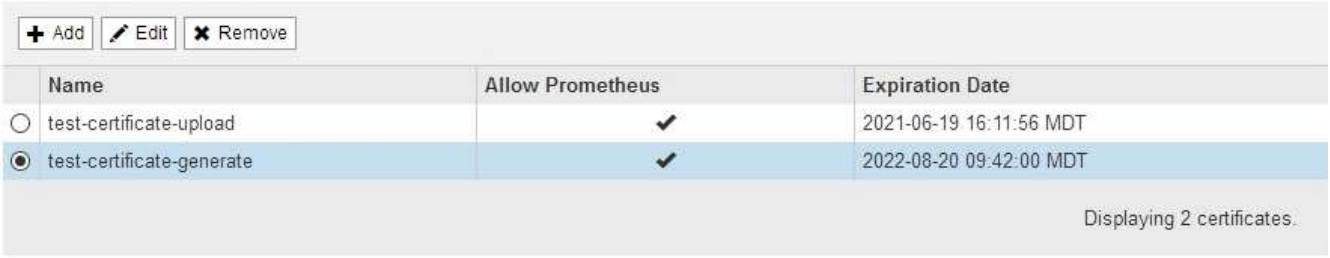
您需要的内容

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

步骤

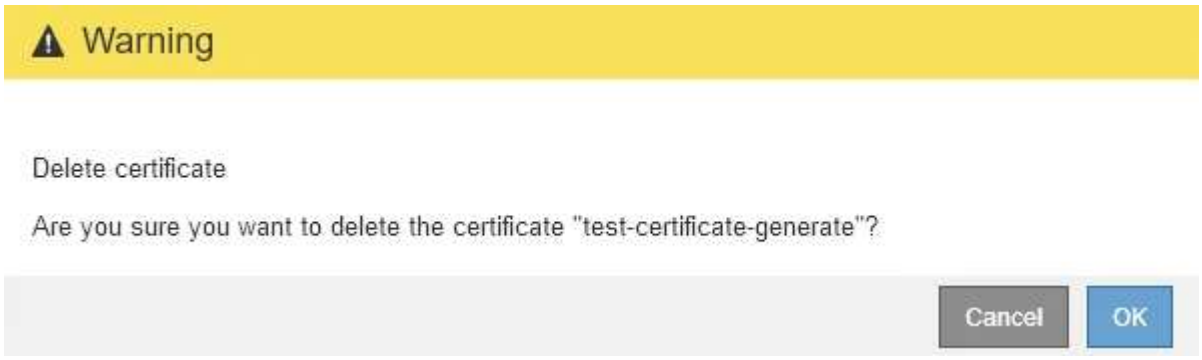
1. 选择*配置*>*访问控制*>*客户端证书*。

   此时将显示客户端证书页面。此时将列出现有证书。



2. 选择要删除的证书左侧的单选按钮。
3. 选择 * 删除 * 。

   此时将显示确认对话框。



4. 选择 * 确定 * 。

   此证书将被删除。

配置密钥管理服务器

您可以配置一个或多个外部密钥管理服务器（ KMS ）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，除非节点可以与 KMS 通信，否则无法访问设备上的任何数据。

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。

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 ）	您可以为StorageGRID 站点配置密钥管理服务器(配置>*系统设置*>*密钥管理服务器*)、并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。可与某些 StorageGRID 存储和服务设备结合使用。
SANtricity System Manager 中的驱动器安全性	如果为存储设备启用了驱动器安全功能，则可以使用 SANtricity 系统管理器创建和管理安全密钥。要访问受保护驱动器上的数据，需要使用此密钥。	具有全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， 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。 "SG6000 存储设备" "SG5700 存储设备" "SG5600 存储设备"
存储对象加密网格选项	可以在网格管理器中启用*存储对象加密*选项(配置>*系统设置*>*网格选项*)。启用后，任何未在存储分段级别或对象级别加密的新对象都会在载入期间进行加密。	新载入的S3和Swift对象数据。现有存储的对象不会加密。对象元数据和其他敏感数据未加密。 "配置存储的对象加密"

加密选项	工作原理	适用场景
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。任何未在对象级别加密的新对象都会在载入期间进行加密。	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未加密。 "使用 S3"
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。必须为此对象指定加密。对象元数据和其他敏感数据未加密。 StorageGRID 负责管理密钥。 "使用 S3"
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。必须为此对象指定加密。对象元数据和其他敏感数据未加密。 密钥在 StorageGRID 之外进行管理。 "使用 S3"
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：

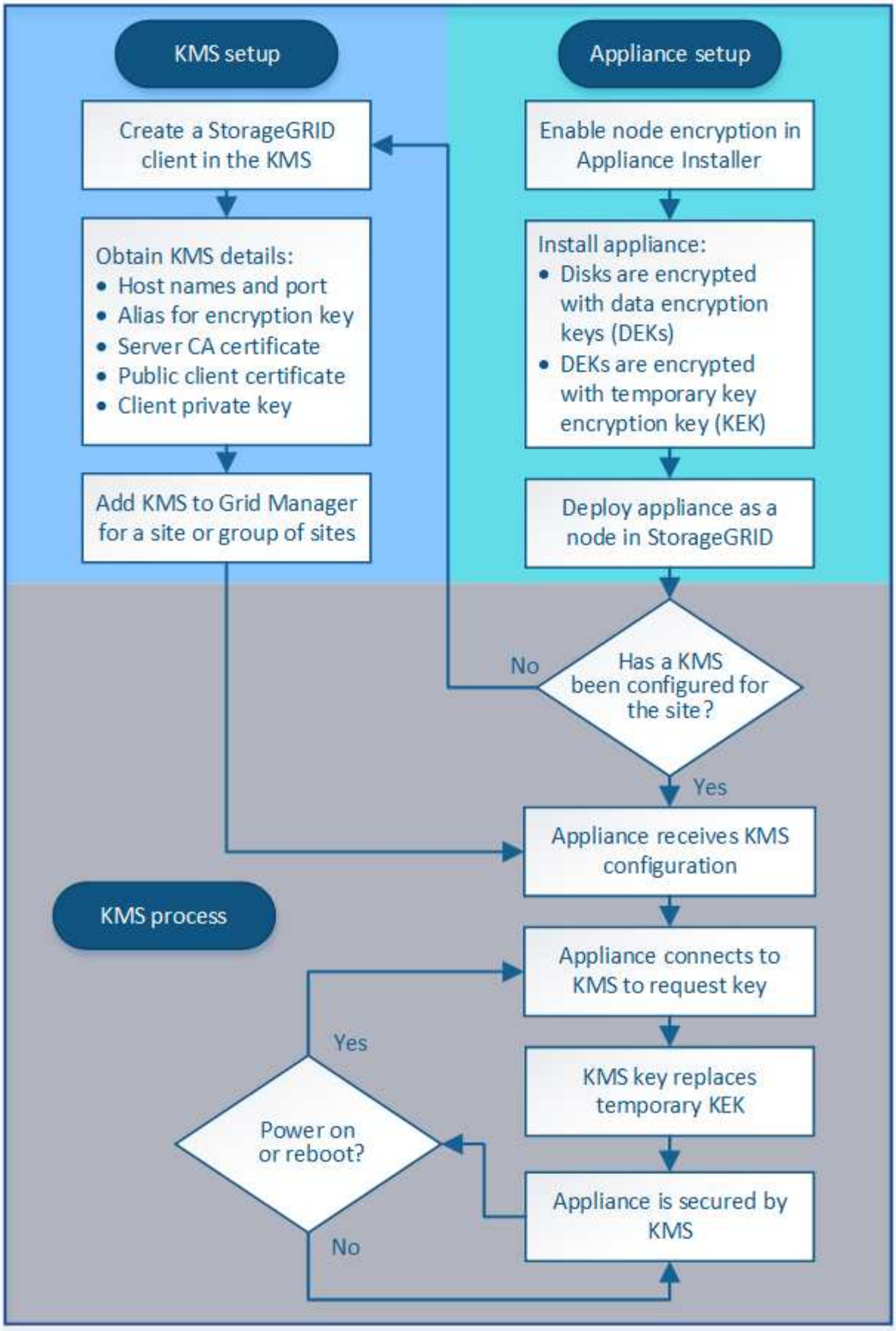
- 您可以使用 KMS 来保护设备节点，也可以使用 SANtricity 系统管理器中的驱动器安全功能在同一设备中的自加密驱动器上 " d 进行灵活加密 " 数据。
- 您可以使用 KMS 来保护设备节点上的数据安全，也可以使用存储对象加密网格选项在载入所有对象时对其进行加密。

如果只有一小部分对象需要加密，请考虑在存储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。

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。

   在将设备添加到网格后，您无法启用 * 节点加密 * 设置，也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。这些密钥是通过设备操作系统中的 Linux 统一密钥设置（ LUKS ）磁盘加密生成的，不能更改。
   - 每个 DEK 都通过主密钥加密密钥（ KEK ）进行加密。初始 KEK 是一个临时密钥，用于对密钥进行加密，直到设备可以连接到 KMS 为止。
3. 将设备节点添加到 StorageGRID 。

有关详细信息，请参阅以下内容：

- "SG100和AMP；SG1000服务设备"
- "SG6000 存储设备"
- "SG5700 存储设备"
- "SG5600 存储设备"

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。保存在易失性内存中的密钥在断电或重新启动后无法生存。

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。

> 在将设备添加到网格后，您无法启用节点加密，并且不能对未启用节点加密的设备使用外部密钥管理。

您可以对以下 StorageGRID 设备和设备节点使用已配置的 KMS ：

设备	节点类型
SG1000 服务设备	管理节点或网关节点
SG100 服务设备	管理节点或网关节点

设备	节点类型
SG6000 存储设备	存储节点
SG5700 存储设备	存储节点
SG5600 存储设备	存储节点

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Docker容器中部署的节点

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。

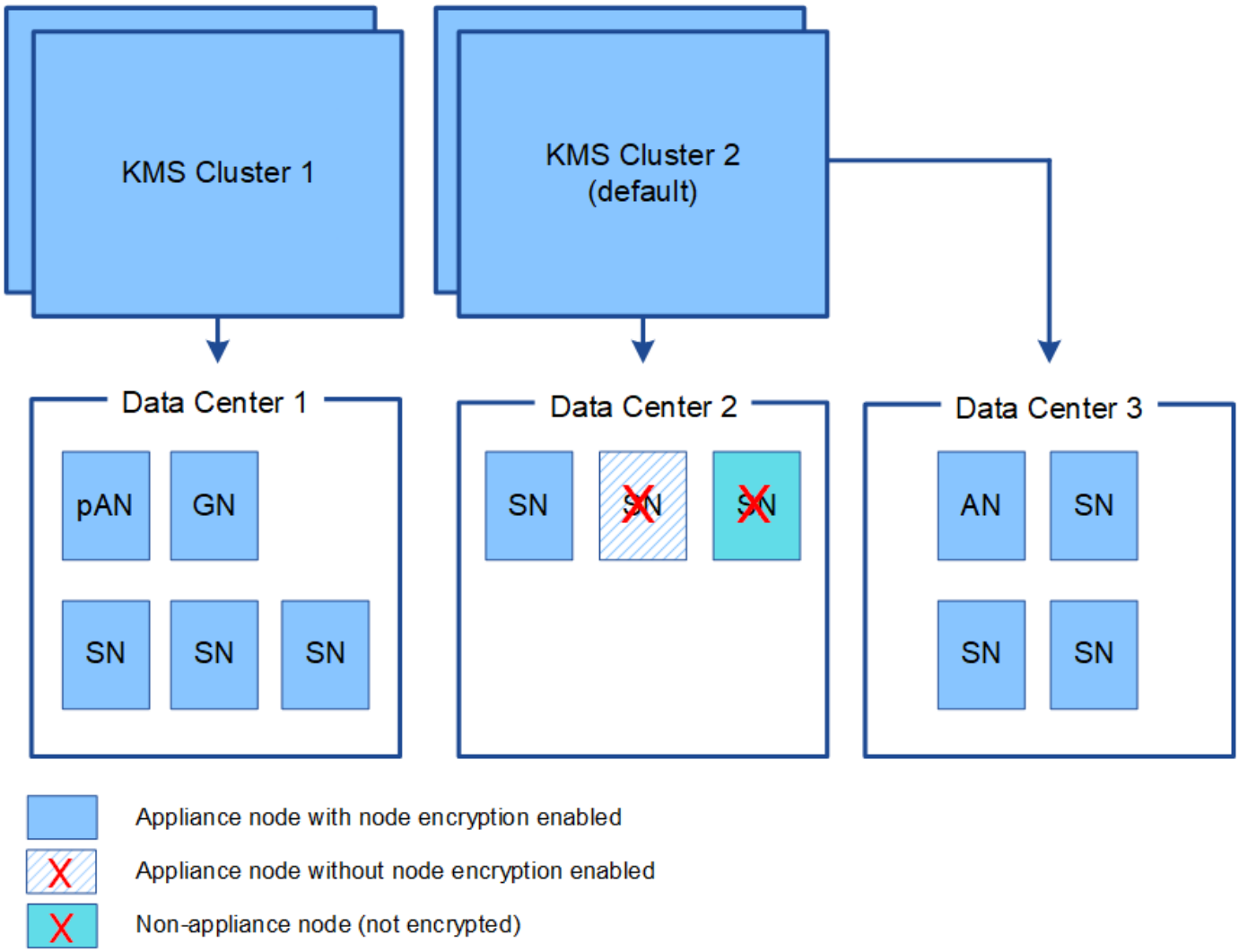
我需要多少个密钥管理服务器？

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在安装期间未启用 * 节点加密 * 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。请勿旋转到完全不同的密钥。

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。

"SG100和AMP；SG1000服务设备"

"SG6000 存储设备"

"SG5700 存储设备"

"SG5600 存储设备"

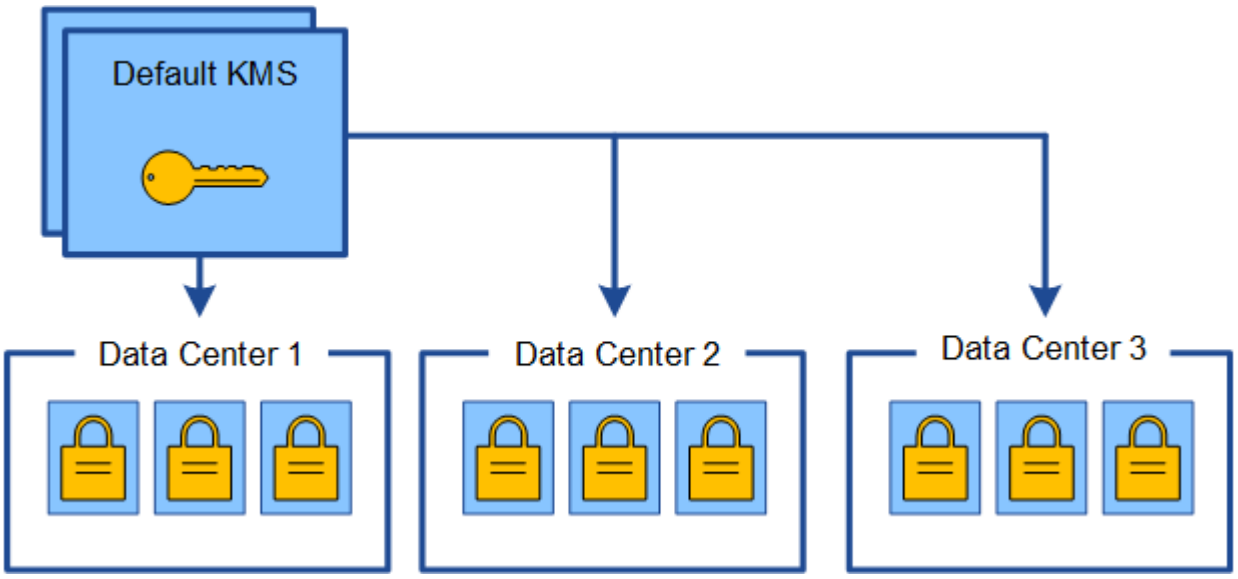
更改站点的 KMS 的注意事项

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。

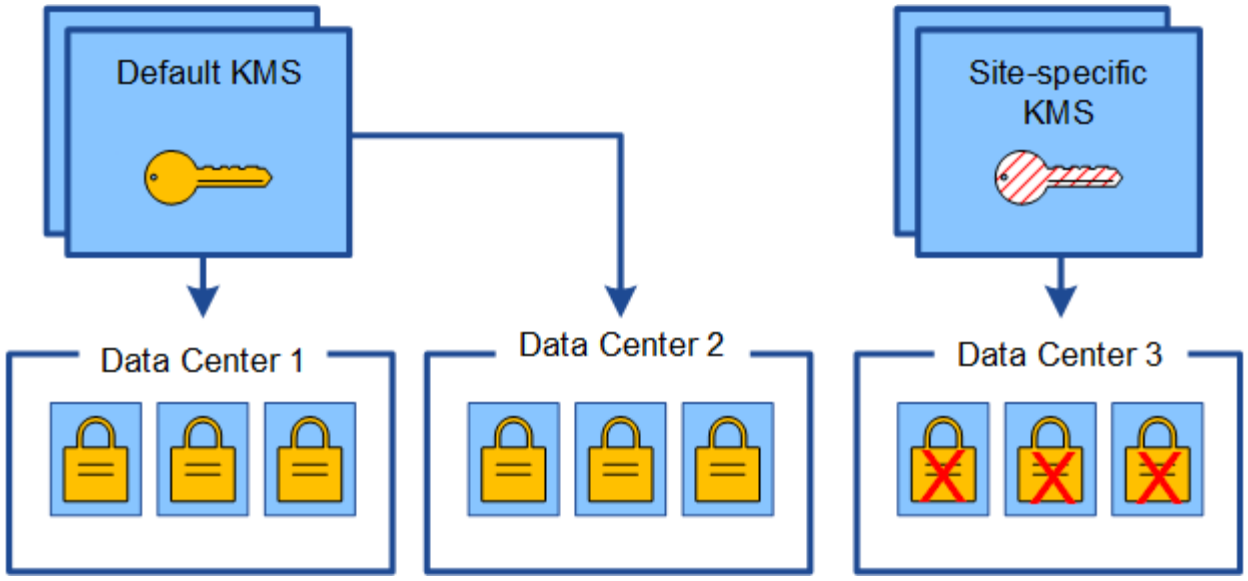
例如：

1. 您最初会配置一个默认 KMS ，以便对没有专用 KMS 的所有站点进行适用场景 。
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。

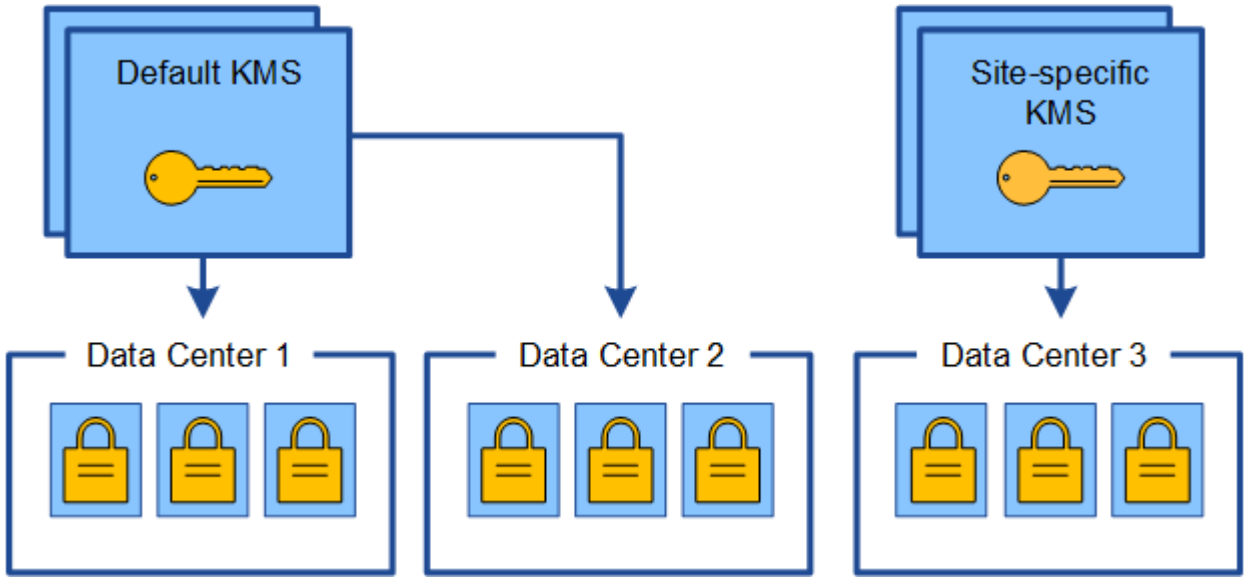


3. 您决定为一个站点（图中的数据中心 3 ）添加站点专用的 KMS 。但是，由于设备节点已加密，因此在尝试保存站点专用 KMS 的配置时会发生验证错误。之所以出现此错误，是因为站点特定的 KMS 没有正确的密

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。您不希望对新站点使用默认 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

这些说明适用于 Thales CipherTrust Manager k170v 2.0 ， 2.1 和 2.2 版。如果您对在 StorageGRID 中使用其他密钥管理服务器有任何疑问，请联系技术支持。

"Thales CipherTrust Manager"

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。

   加密密钥需要可导出。

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。

您需要的内容

- 您必须已查看 "使用密钥管理服务器的注意事项和要求"。
- 您必须拥有 "已在 KMS 中将 StorageGRID 配置为客户端"和必须具有每个KMS或KMS集群的所需信息
- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

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 。

"更改站点的 KMS 的注意事项"

步骤

1. "第 1 步：输入 KMS 详细信息"
2. "第 2 步：上传服务器证书"
3. "第 3 步：上传客户端证书"

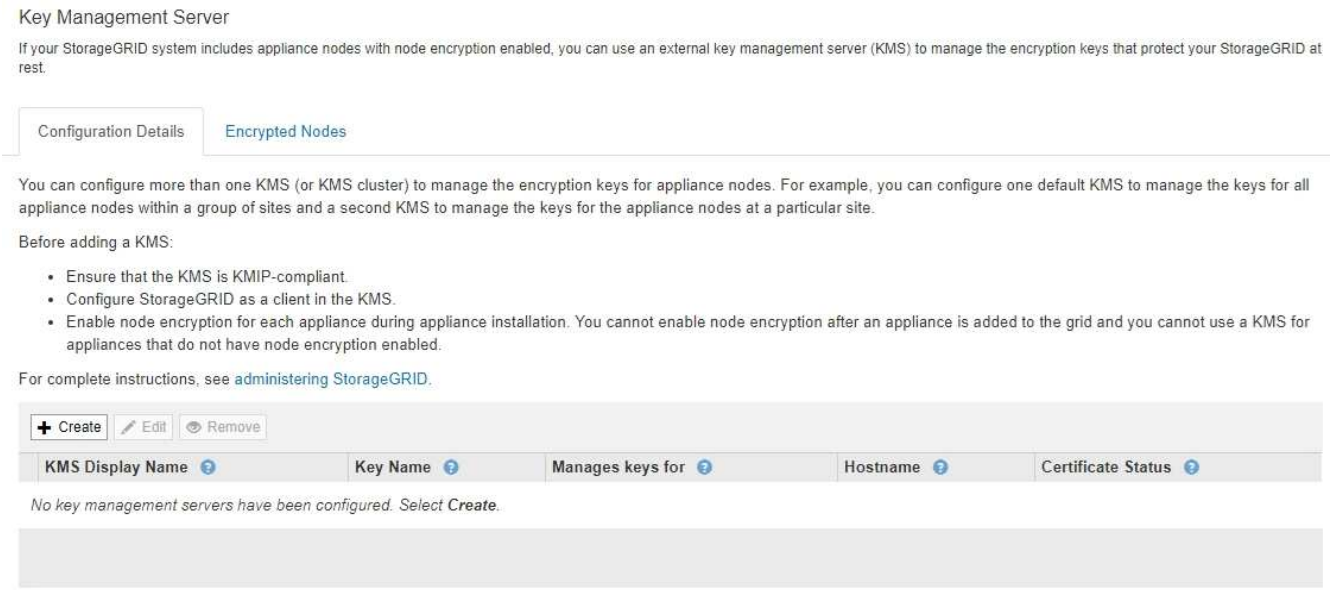
第 1 步：输入 KMS 详细信息

在添加密钥管理服务器向导的步骤 1 （输入 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

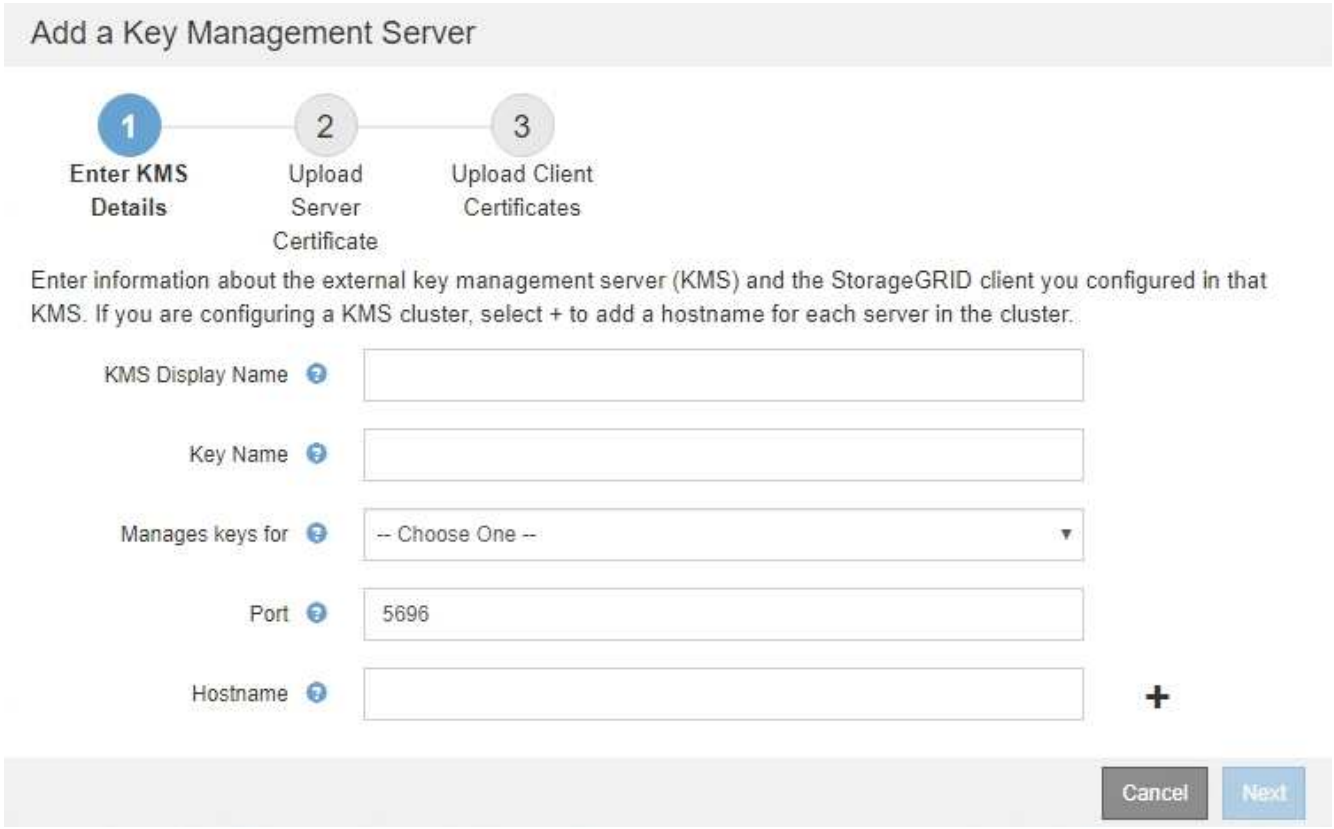
1. 选择*配置系统设置密钥管理服务器*。

   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 * 。

   此时将显示添加密钥管理服务器向导的第 1 步（输入 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 显示名称	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。
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 * 不受其他 KMS 管理的站点（默认 KMS ）* 可配置一个默认 KMS ，该 KMS 将应用于没有专用 KMS 的任何站点以及您在后续扩展中添加的任何站点。 ◦ 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。

字段	Description
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： * 服务器证书的 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. 如果您使用的是 KMS 集群，请选择加号 ➕ 为集群中的每个服务器添加主机名。
5. 选择 * 下一步 * 。

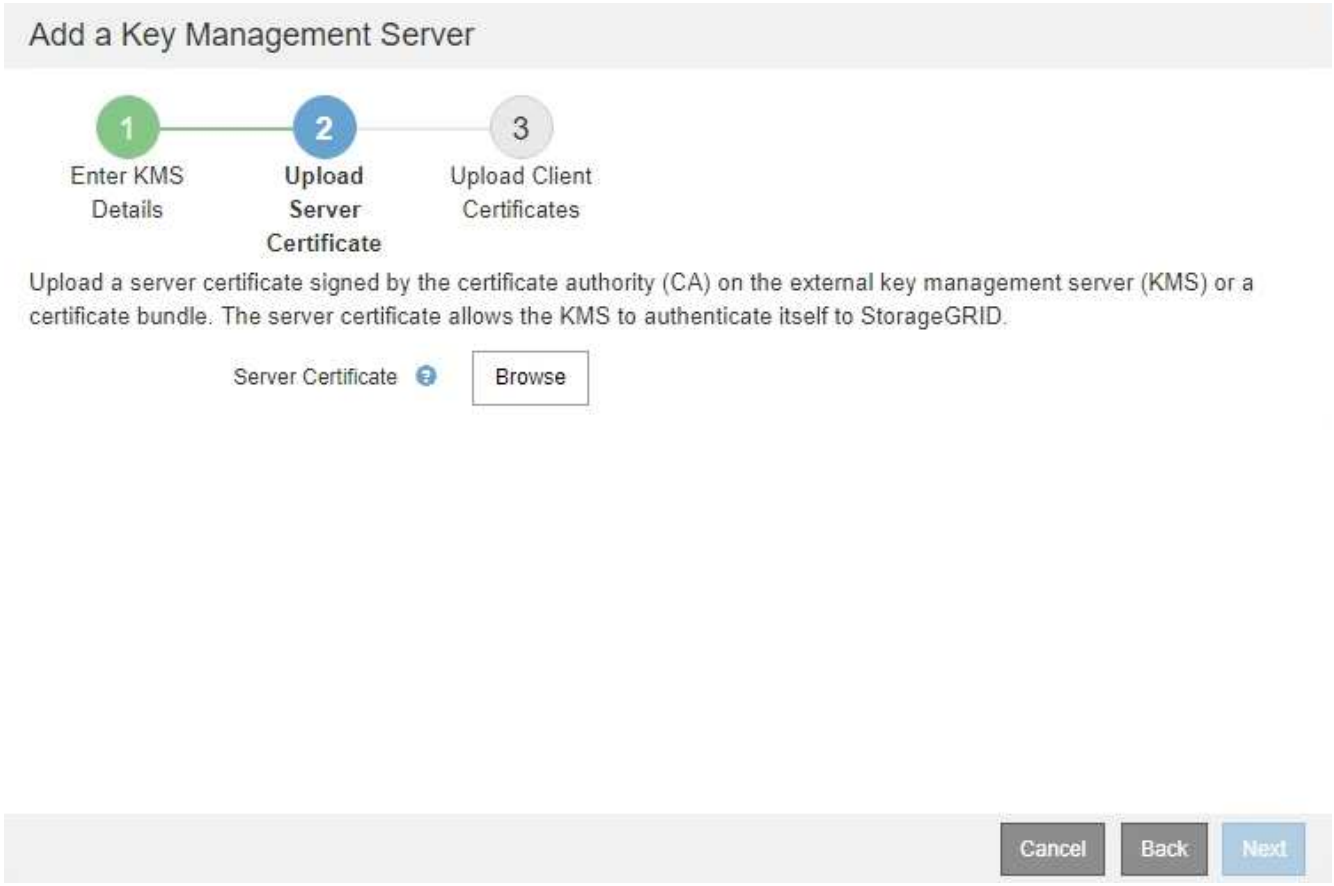
   此时将显示添加密钥管理服务器向导的第2步(上传服务器证书)。

第 **2** 步：上传服务器证书

在添加密钥管理服务器向导的第 2 步（上传服务器证书）中，您可以上传 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。

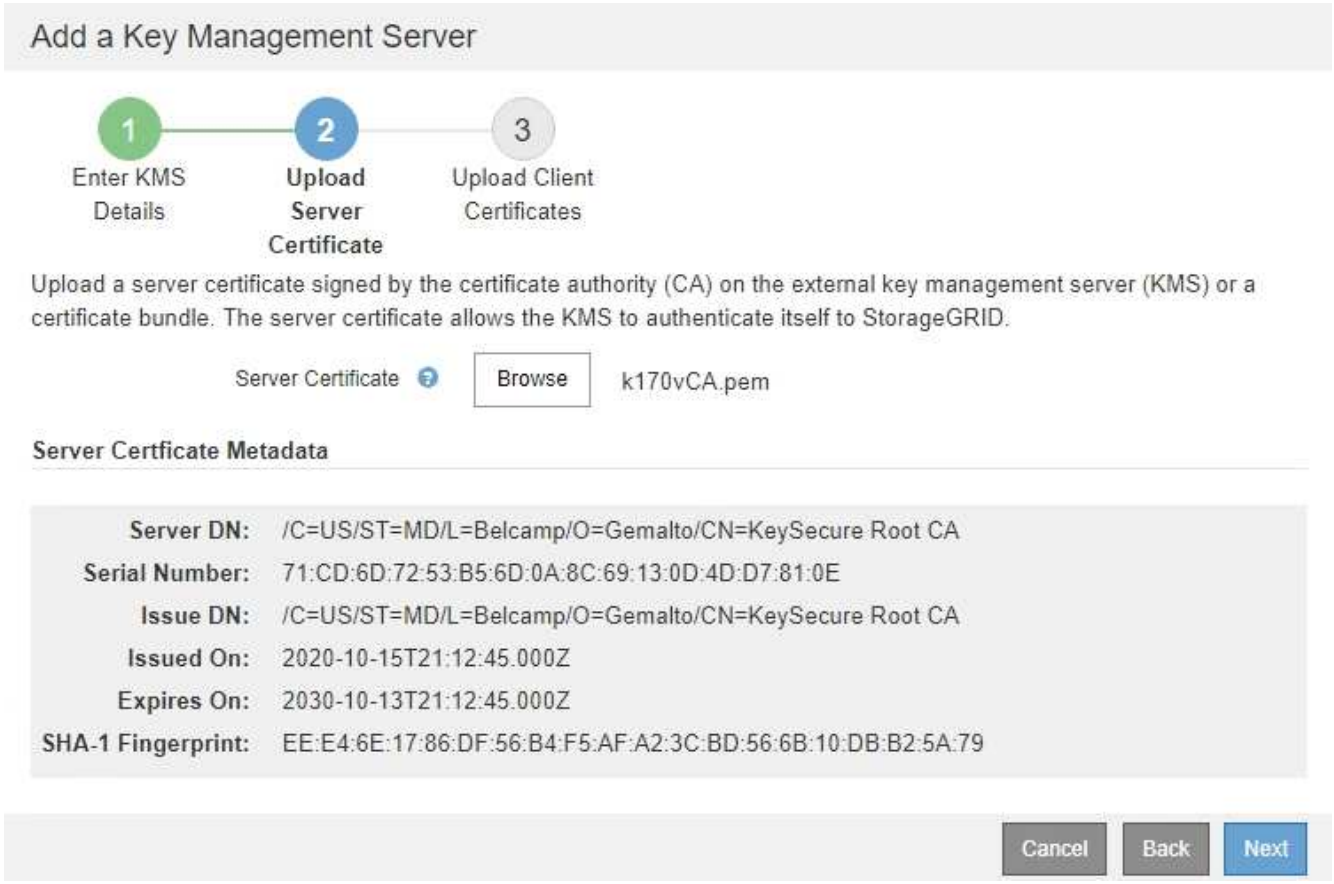
步骤

1. 从 * 步骤 2 （上传服务器证书） * 中，浏览到保存的服务器证书或证书包的位置。



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 * 下一步 * 。

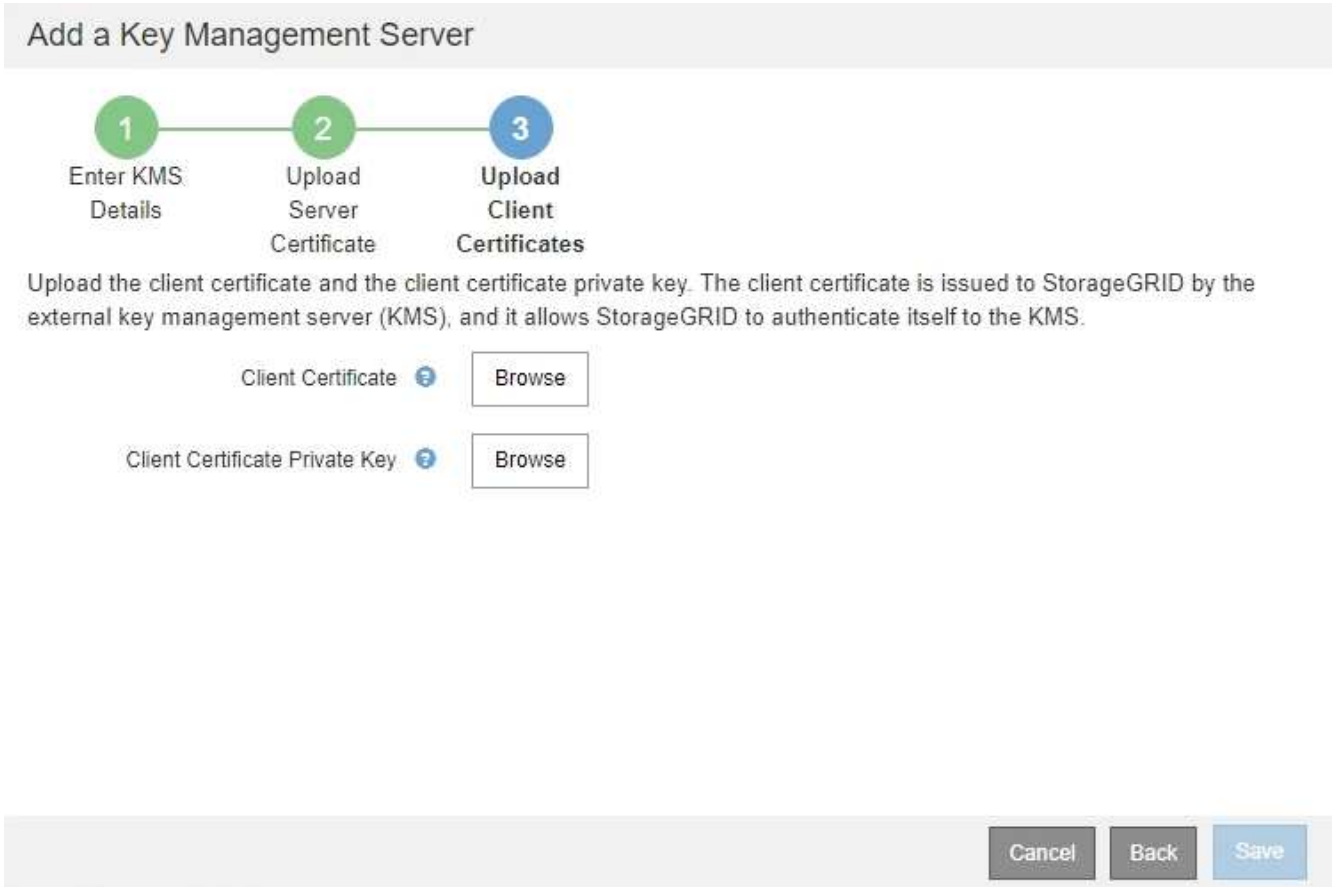
   此时将显示添加密钥管理服务器向导的第3步(上传客户端证书)。

第 **3** 步：上传客户端证书

在添加密钥管理服务器向导的第 3 步（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。

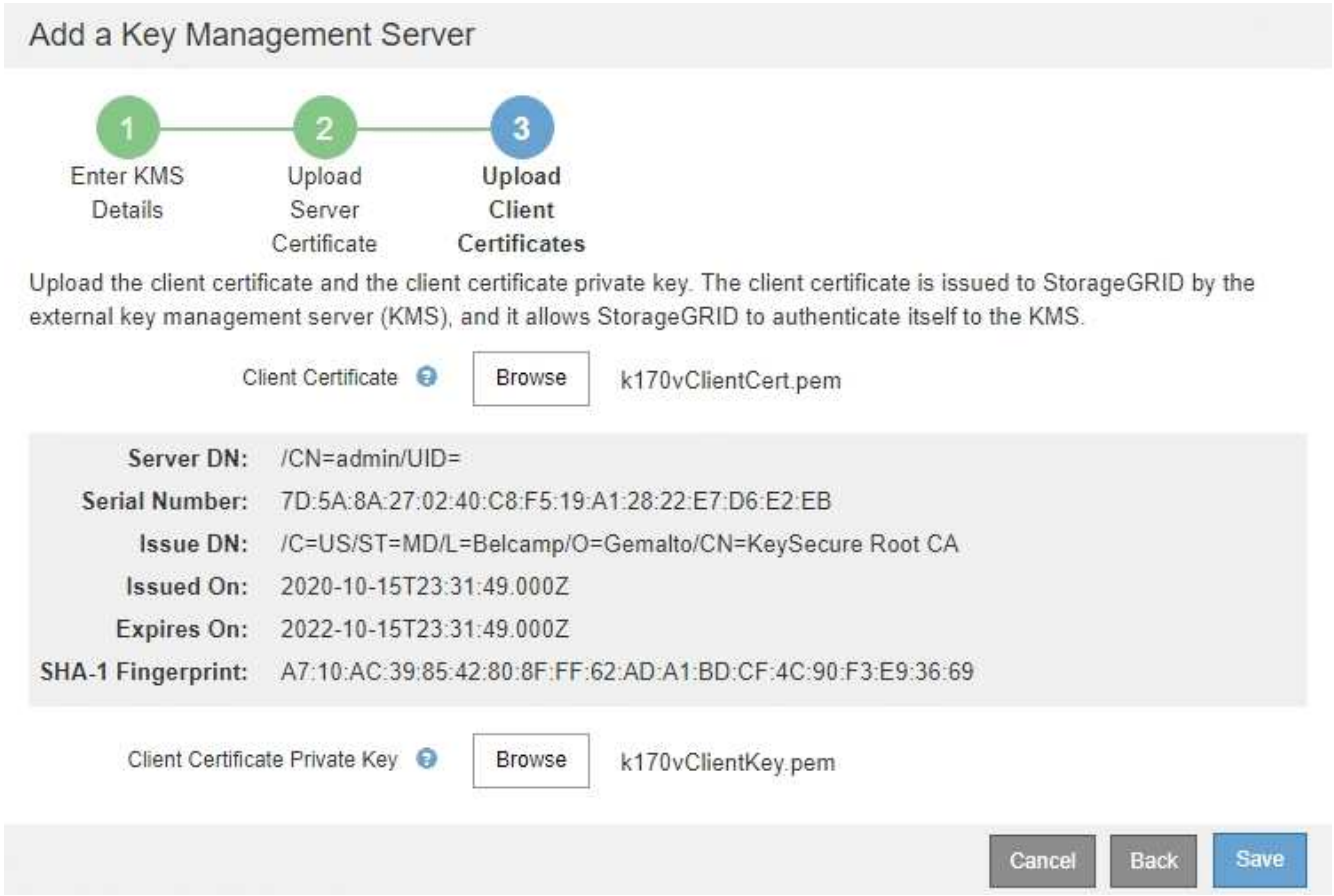


2. 上传客户端证书文件。

   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。

   此时将显示客户端证书和客户端证书专用密钥的元数据。



5. 选择 * 保存 * 。

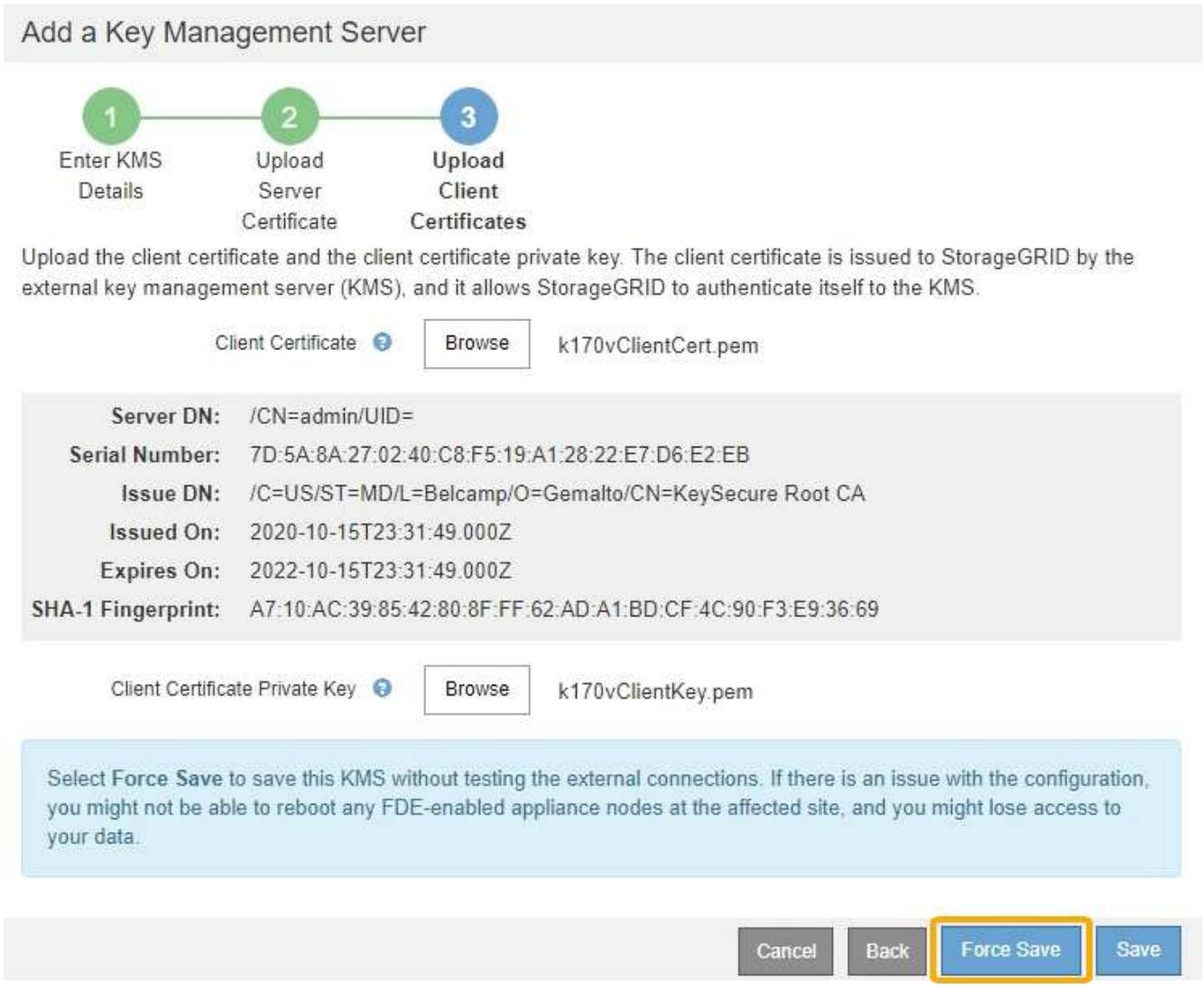
   测试密钥管理服务器与设备节点之间的连接。如果所有连接均有效，并且在 KMS 上找到正确的密钥，则新的密钥管理服务器将添加到密钥管理服务器页面上的表中。

   > 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. 如果选择 * 保存 * 时显示错误消息，请查看消息详细信息，然后选择 * 确定 * 。

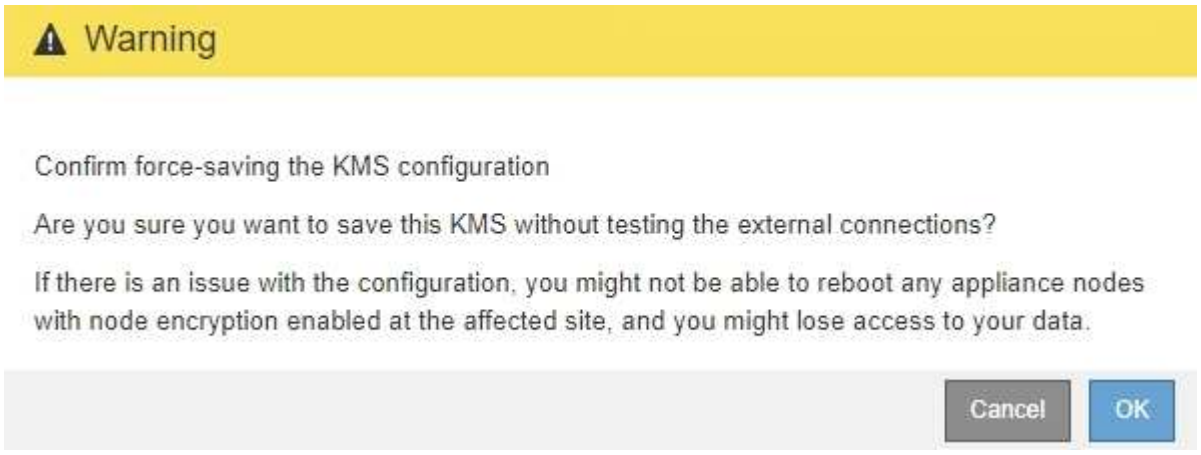
   例如，如果连接测试失败，您可能会收到 422 ： Unprocessable Entity 错误。

7. 如果需要保存当前配置而不测试外部连接，请选择 * 强制保存 * 。



选择 * 强制保存 * 可保存 KMS 配置，但不会测试每个设备与该 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。

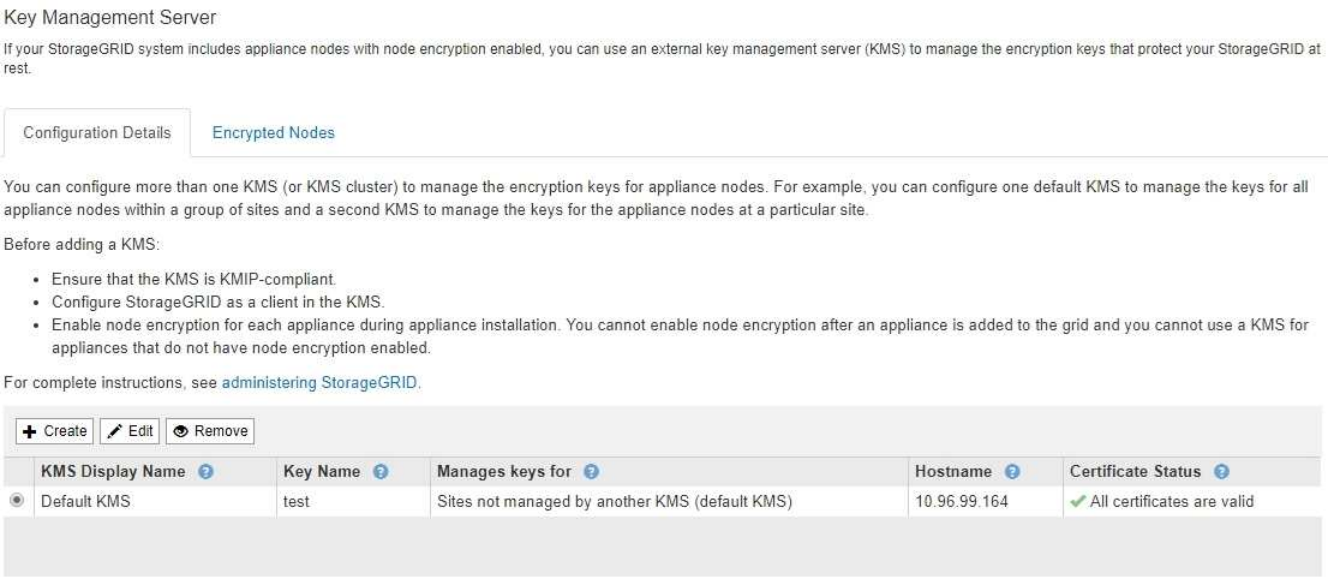
查看**KMS**详细信息

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*配置系统设置密钥管理服务器*。

   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了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 显示名称	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。 *

字段	Description
主机名	KMS 的完全限定域名或 IP 地址。 如果集群包含两个密钥管理服务器，则会列出这两个服务器的完全限定域名或 IP 地址。如果集群中有两个以上的密钥管理服务器，则会列出第一个 KMS 的完全限定域名或 IP 地址以及集群中其他密钥管理服务器的数量。 例如： `10.10.10.10 and 10.10.10.11` 或 `10.10.10.10 and 2 others`。 要查看集群中的所有主机名，请选择一个 KMS ，然后选择 * 编辑 * 。
证书状态	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 分钟才能更新证书状态。您必须刷新 Web 浏览器才能查看当前值。

3. 如果证书状态为未知，请等待长达 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 浏览器才能查看实际状态。

4. 如果证书状态列指示证书已过期或即将到期，请尽快解决问题描述 。

有关StorageGRID 的监控和故障排除说明、请参见针对* KMS CA证书到期*、* KMS客户端证书到期*和* KMS服务器证书到期*警报的建议操作。

> 要保持数据访问，您必须尽快解决任何证书问题。

相关信息

"监控和放大；故障排除"

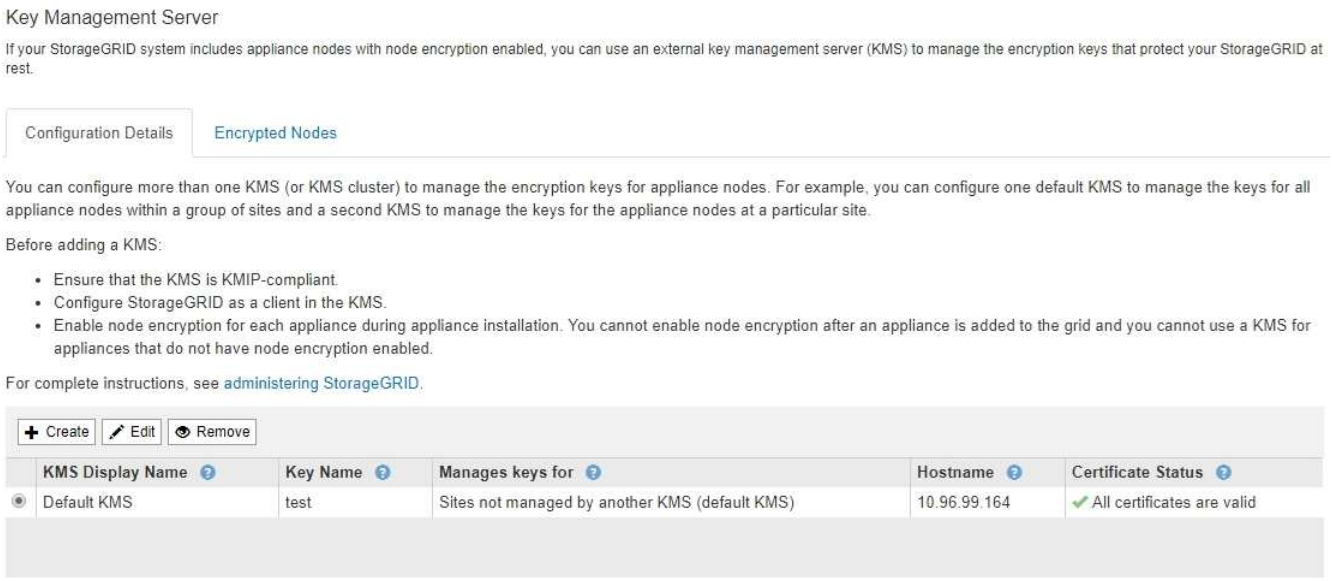
查看加密节点

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*配置系统设置密钥管理服务器*。

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 系统中已启用 * 节点加密 * 设置的设备节点。

3. 查看表中每个设备节点的信息。

列	Description
节点名称	设备节点的名称。
节点类型	节点的类型：存储，管理或网关。
站点	安装节点的 StorageGRID 站点的名称。

列	Description
Kms 显示名称	用于节点的 KMS 的描述性名称。 如果未列出任何 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 ，请将光标悬停在单元格上方。 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 。
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Kms请参见StorageGRID 监控和故障排除说明中针对这些警报建议的操作。

   ⓘ 您必须立即解决任何问题，以确保您的数据得到完全保护。

相关信息

"监控和放大；故障排除"

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。

您需要的内容

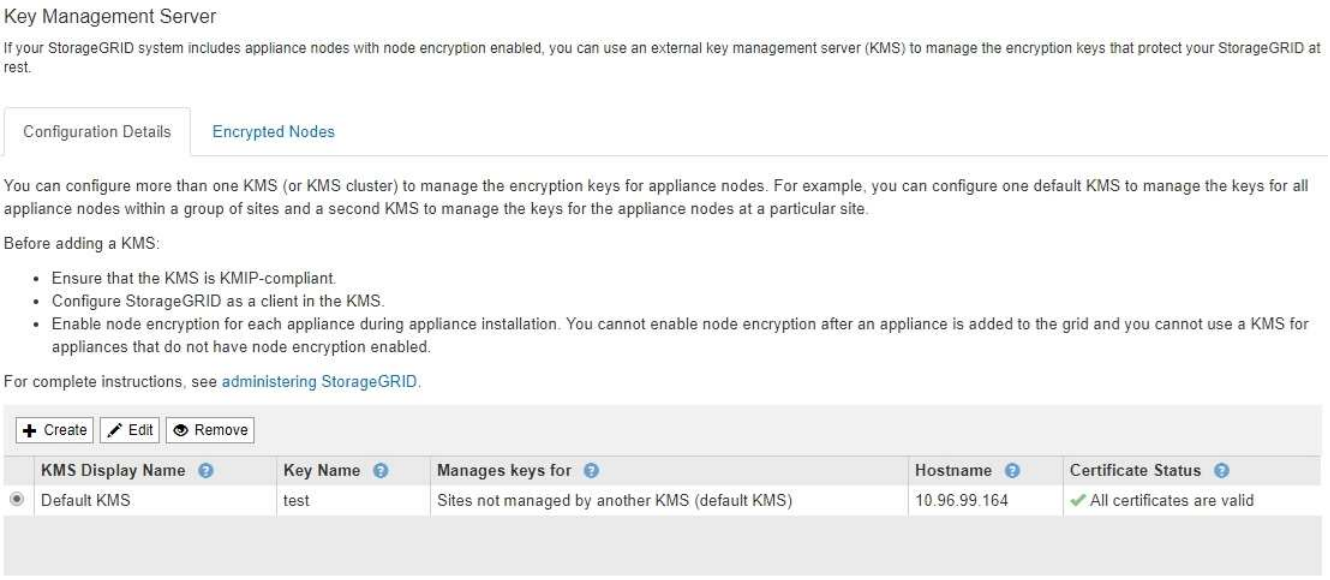
- 您必须已查看 "使用密钥管理服务器的注意事项和要求"。
- 如果您计划更新为KMS选择的站点、则必须已查看 "更改站点的 KMS 的注意事项"。

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

步骤

1. 选择*配置系统设置密钥管理服务器*。

   此时将显示密钥管理服务器页面，其中显示了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 * 编辑 * 。
3. 或者，更新编辑密钥管理服务器向导的 * 步骤 1 （输入 KMS 详细信息） * 中的详细信息。

字段	Description
Kms 显示名称	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"

字段	Description
管理的密钥	如果您正在编辑站点特定的 KMS ，并且尚未设置默认 KMS ，则也可以选择 * 不由其他 KMS 管理的站点（默认 KMS ） * 。此选项会将站点特定的 KMS 转换为默认 KMS ，该 KMS 将应用于没有专用 KMS 的所有站点以及在扩展中添加的任何站点。 • 注意： * 如果要编辑站点特定的 KMS ，则无法选择其他站点。如果要编辑默认 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： * 服务器证书的 SAN 字段必须包含您在此处输入的 FQDN 或 IP 地址。否则， StorageGRID 将无法连接到 KMS 或 KMS 集群中的所有服务器。

4. 如果要配置 KMS 集群，请选择加号 ➕ 为集群中的每个服务器添加主机名。
5. 选择 * 下一步 * 。

   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 * 下一步 * 。

   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 * 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 * 。

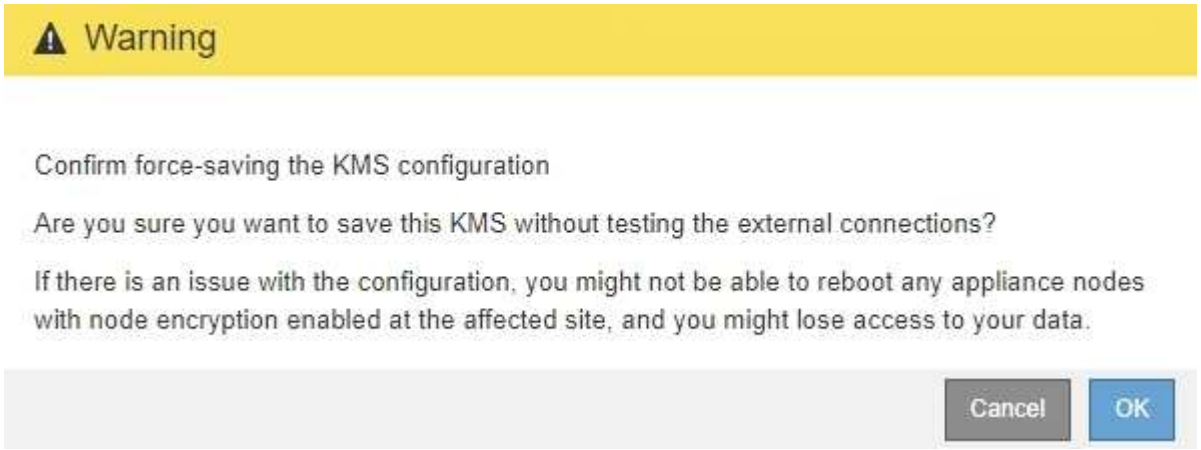
    例如，如果为此 KMS 选择的站点已由另一个 KMS 管理，或者连接测试失败，则可能会收到 422 ： Unprocessable Entity 错误。

11. 如果在解决连接错误之前需要保存当前配置，请选择 * 强制保存 * 。

    选择 * 强制保存 * 可保存 KMS 配置，但不会测试每个设备与该 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 。

您需要的内容

- 您必须已查看 "使用密钥管理服务器的注意事项和要求"。
- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

关于此任务

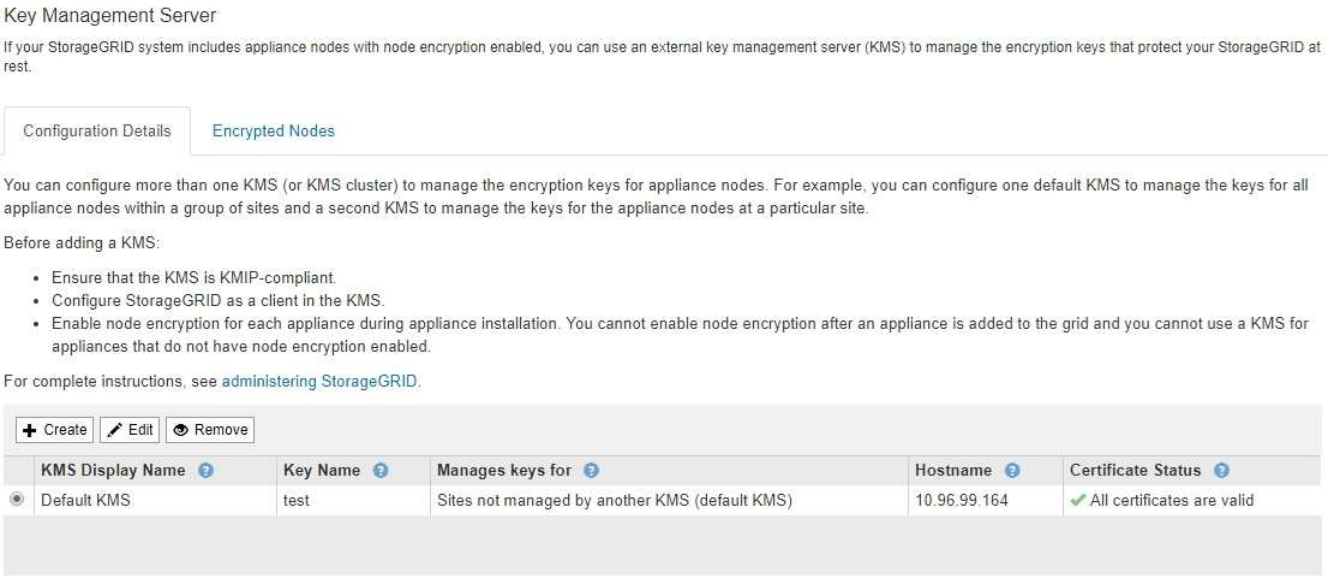
在以下情况下，您可以删除 KMS ：

- 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 。

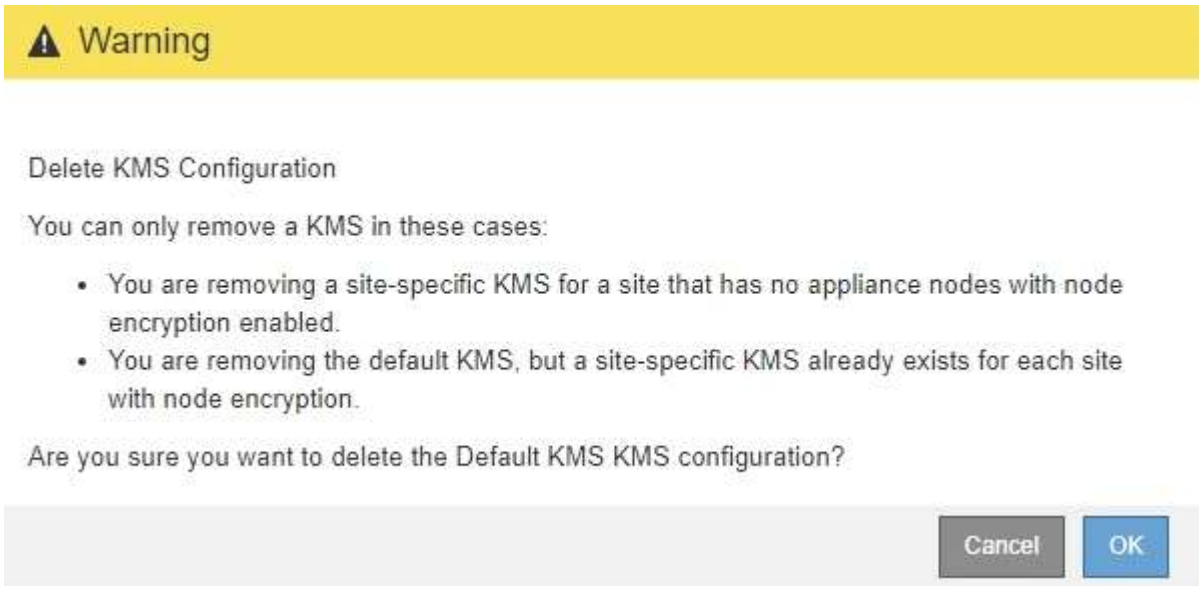
步骤

1. 选择*配置系统设置密钥管理服务器*。

   此时将显示密钥管理服务器页面，其中显示了已配置的所有密钥管理服务器。



2. 选择要删除的 KMS 的单选按钮，然后选择 * 删除 * 。
3. 查看警告对话框中的注意事项。



4. 选择 * 确定 * 。

   此时将删除 KMS 配置。

管理租户

作为网格管理员，您可以创建和管理 S3 和 Swift 客户端用来存储和检索对象，监控存储使用情况以及管理客户端使用 StorageGRID 系统能够执行的操作的租户帐户。

什么是租户帐户

租户帐户允许使用简单存储服务（ S3 ） REST API 或 Swift REST API 的客户端应用程序在 StorageGRID 上存

储和检索对象。

每个租户帐户都支持使用一个协议，您可以在创建帐户时指定该协议。要将对象存储和检索到使用这两种协议的 StorageGRID 系统，您必须创建两个租户帐户：一个用于 S3 分段和对象，一个用于 Swift 容器和对象。每个租户帐户都有自己的帐户 ID ，授权组和用户，分段或容器以及对象。

或者，如果要将系统上存储的对象隔离为不同的实体，则可以创建其他租户帐户。例如，您可以在以下任一使用情形中设置多个租户帐户：

- * 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，则只需使用 S3 分段和分段策略来隔离企业中各个部门之间的对象即可。您不需要使用租户帐户。有关详细信息，请参见实施 S3 客户端应用程序的说明。

- * 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。

创建和配置租户帐户

创建租户帐户时，您可以指定以下信息：

- 租户帐户的显示名称。
- 租户帐户（ S3 或 Swift ）将使用哪种客户端协议。
- 对于 S3 租户帐户：租户帐户是否有权对 S3 分段使用平台服务。如果您允许租户帐户使用平台服务，则必须确保已将网格配置为支持其使用。请 `M` " 管理平台服务 " 。
- （可选）租户帐户的存储配额—租户对象可用的最大 GB ， TB 或 PB 数。如果超过配额，租户将无法创建新对象。

  租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。

- 如果为 StorageGRID 系统启用了身份联合，则哪个联合组具有 " 根访问 " 权限来配置租户帐户。
- 如果 StorageGRID 系统未使用单点登录（ SSO ），则表示租户帐户是使用自己的身份源还是共享网格的身份源，以及租户的本地 root 用户的初始密码。

创建租户帐户后，您可以执行以下任务：

- * 管理网格的平台服务 * ：如果您为租户帐户启用平台服务，请确保您了解如何传送平台服务消息以及使用平台服务对 StorageGRID 部署的网络要求。
- * 监控租户帐户的存储使用情况 * ：租户开始使用其帐户后，您可以使用 Grid Manager 监控每个租户占用的存储容量。

  如果已为租户设置配额，则可以启用 * 租户配额使用量高 * 警报以确定租户是否正在使用其配额。如果启用，则在租户已使用其配额的 90% 时触发此警报。有关详细信息，请参见 StorageGRID 监控和故障排除说明中的警报参考。

- * 配置客户端操作 * ：您可以配置是否禁止某些类型的客户端操作。

配置S3租户

创建 S3 租户帐户后，租户用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享）并创建本地组和用户
- 管理 S3 访问密钥
- 创建和管理 S3 存储分段
- 监控存储使用情况
- 使用平台服务（如果已启用）

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，但必须使用 S3 客户端应用程序载入和管理对象。

配置Swift租户

创建 Swift 租户帐户后，租户的 root 用户可以访问租户管理器以执行如下任务：

- 设置身份联合（除非身份源与网格共享），并创建本地组和用户
- 监控存储使用情况

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 " 权限不允许用户向 Swift REST API 进行身份验证以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。

相关信息

"使用租户帐户"

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。

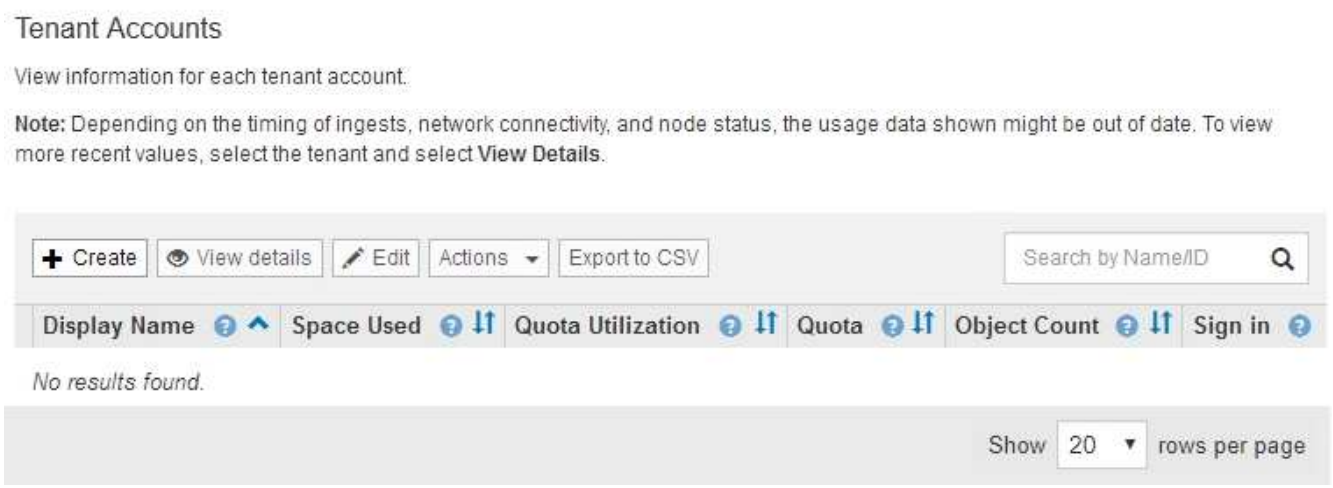
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

步骤

1. 选择*租户*。

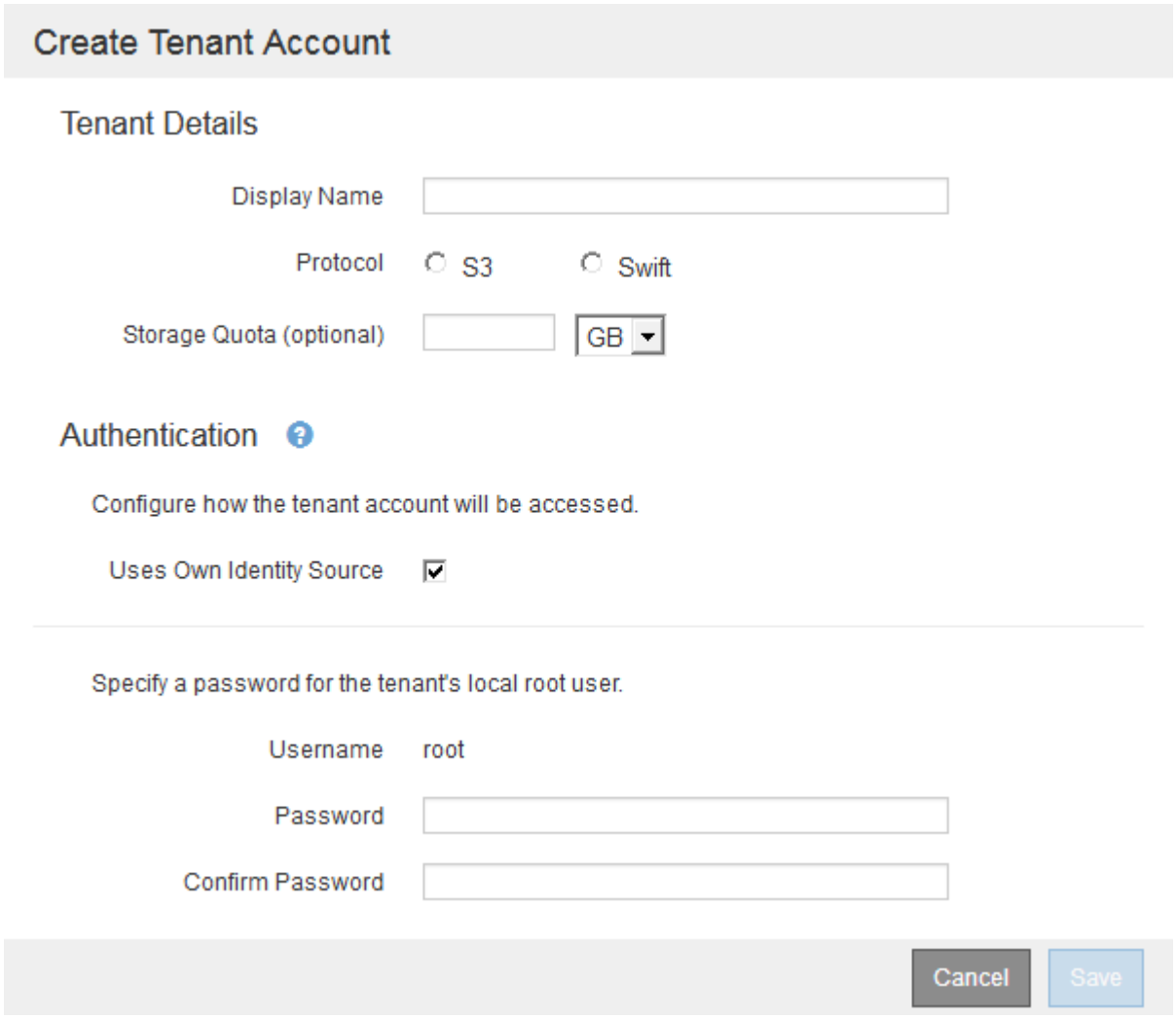
   此时将显示租户帐户页面、并列出任何现有租户帐户。



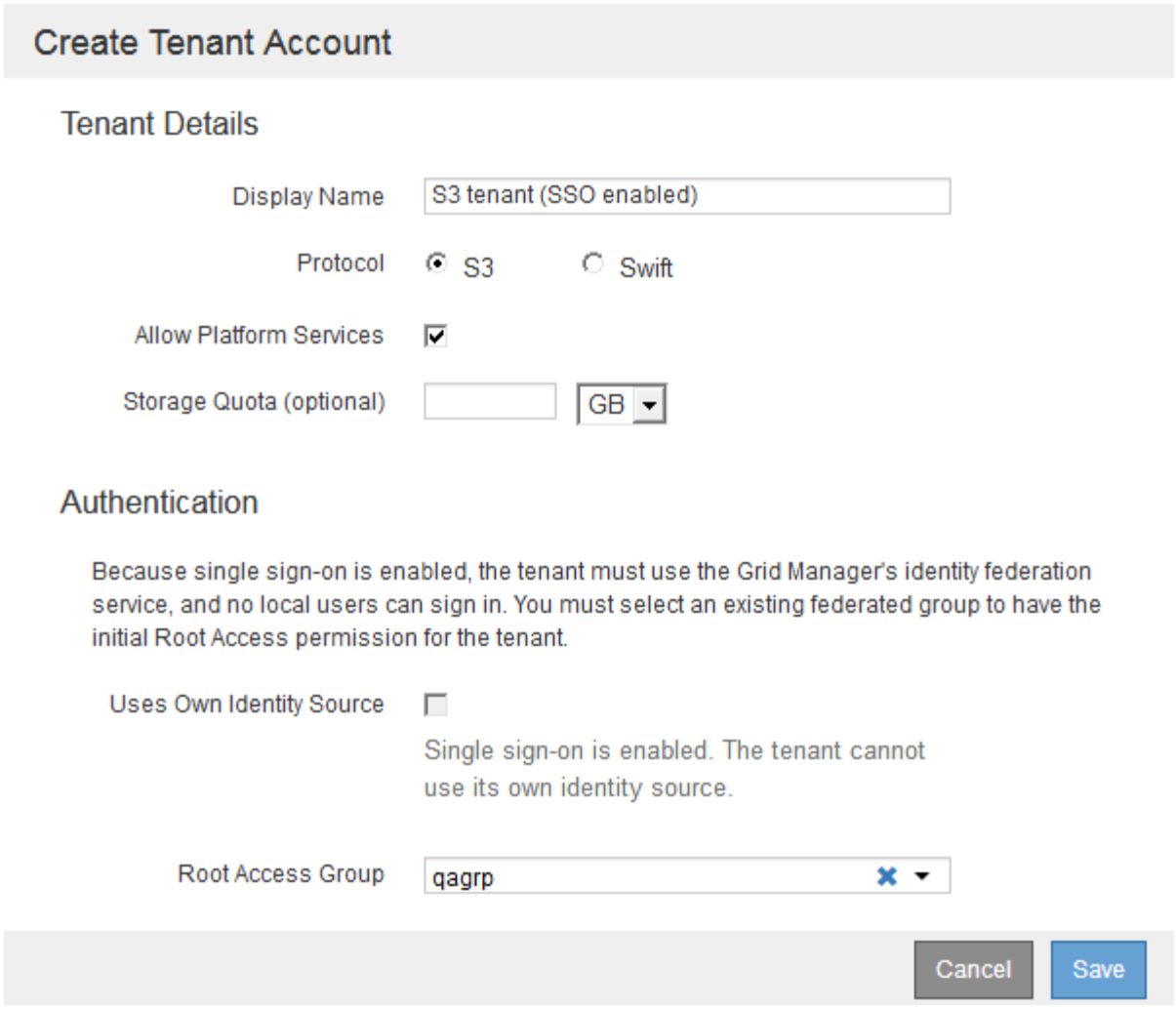
2. 选择 * 创建 * 。

   此时将显示创建租户帐户页面。此页面中包含的字段取决于是否已为StorageGRID 系统启用单点登录(SSO)。

   - 如果未使用SSO、则创建租户帐户页面将如下所示。



   - 如果启用了SSO、则创建租户帐户页面将如下所示。



相关信息

"使用身份联合"

"配置单点登录"

如果**StorageGRID** 未使用**SSO**、则创建租户帐户

创建租户帐户时，您可以指定名称，客户端协议以及存储配额（可选）。如果StorageGRID 未使用单点登录(SSO)、则还必须指定租户帐户是否使用自己的身份源、并为租户的本地root用户配置初始密码。

关于此任务

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、则必须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 Grid Manager 权限。请参见的说明 "管理管理组"。

步骤

1. 在*显示名称*文本框中、输入此租户帐户的显示名称。

   显示名称不必唯一。创建租户帐户时、它会收到一个唯一的数字帐户ID。

2. 选择此租户帐户要使用的客户端协议、可以是* S3或* Swift*。
3. 对于S3租户帐户、请保持选中*允许平台服务*复选框、除非您不希望此租户对S3分段使用平台服务。

   如果启用了平台服务，则租户可以使用 CloudMirror 复制等功能来访问外部服务。您可能需要禁用这些功能来限制租户使用的网络带宽或其他资源量。请 M" 管理平台服务 " 。
4. 在*存储配额*文本框中、也可以输入要为此租户对象提供的最大GB、TB或PB数。然后、从下拉列表中选择单位。

   如果希望此租户拥有无限配额、请将此字段留空。

   租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。ILM副本和纠删编码不会影响所使用的配额量。如果超过配额、租户帐户将无法创建新对象。

   要监控每个租户帐户的存储使用情况、请选择*使用情况*。租户帐户还可以通过租户管理器中的信息板或租户管理API监控自己的存储使用情况。请注意、如果节点与网格中的其他节点隔离、则租户的存储使用量值可能会过时。恢复网络连接后，总数将更新。
5. 如果租户要管理自己的组和用户、请按照以下步骤进行操作。
   a. 选中*使用自己的身份源*复选框(默认)。

      如果选中此复选框、并且您要对租户组和用户使用身份联合、则租户必须配置自己的身份源。请参见有关使用租户帐户的说明。
   b. 为租户的本地root用户指定密码。
6. 如果租户要使用为网格管理器配置的组和用户、请按照以下步骤进行操作。
   a. 取消选中*使用自己的身份源*复选框。
   b. 执行以下操作之一或同时执行这两项操作：
      - 在根访问组字段中、从网格管理器中选择一个应具有租户初始根访问权限的现有联合组。

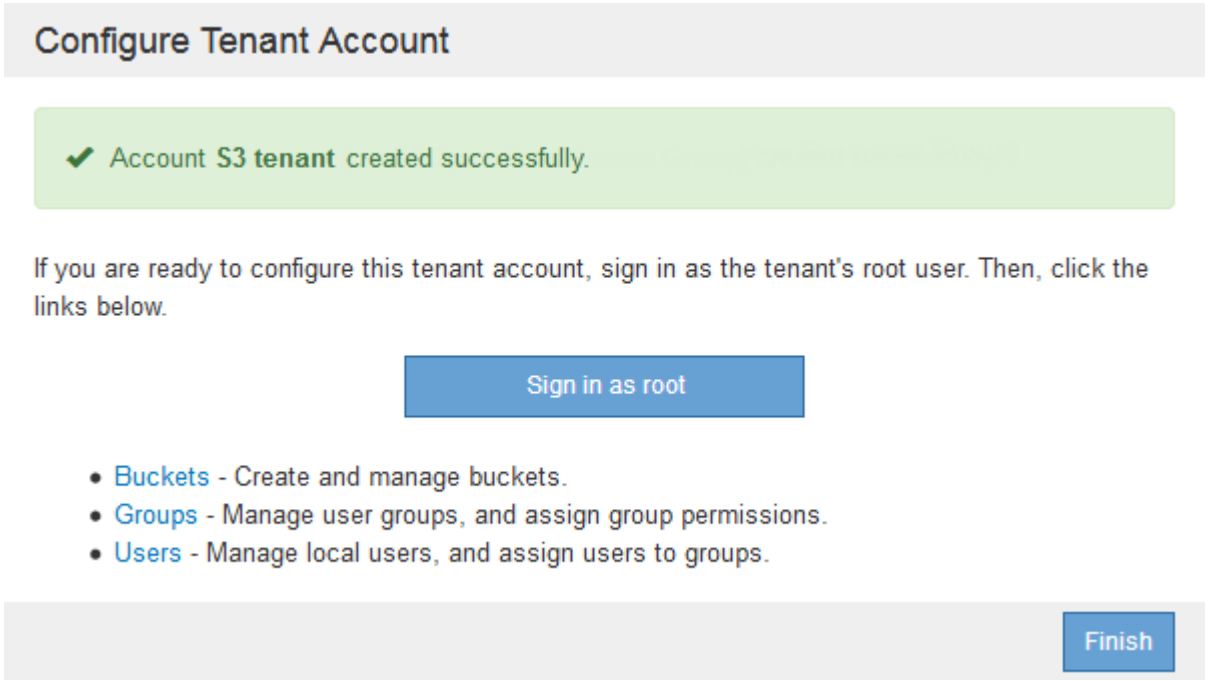
        如果您拥有足够的权限、则在单击此字段时会列出网格管理器中的现有联合组。否则，请输入组的唯一名称。
      - 为租户的本地root用户指定密码。
7. 单击 * 保存 * 。

   此时将创建租户帐户。
8. (可选)访问新租户。否则、请转至的步骤 稍后访问租户。

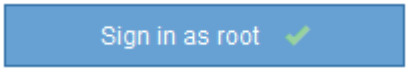
如果您 ...	执行此操作 ...
在受限端口上访问网格管理器	单击*受限*了解有关访问此租户帐户的更多信息。 租户管理器的 URL 格式如下： `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *FQDN_or_Admin_Node_IP* 是完全限定域名或管理节点的IP地址 • *port* 是仅租户端口 • *20-digit-account-id* 是租户的唯一帐户ID
在端口443上访问网格管理器、但未为本地root用户设置密码	单击*登录*、然后输入root访问联合组中某个用户的凭据。
通过端口443访问网格管理器、并为本地root用户设置密码	转至下一步 以root用户身份登录。

9. 【step_sign_in_as_root]]以root身份登录到租户：

   a. 在配置租户帐户对话框中、单击*以root身份登录*按钮。



   此按钮上会显示一个绿色复选标记、表示您现在已以root用户身份登录到租户帐户。



   a. 单击链接以配置租户帐户。

每个链接都会在租户管理器中打开相应的页面。要完成此页面、请参见有关使用租户帐户的说明。

b. 单击 * 完成 * 。

10. 要稍后访问租户、请执行以下操作：

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*、然后单击租户名称右侧的*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*、然后单击*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

相关信息

"通过防火墙控制访问"

"管理S3租户帐户的平台服务"

"使用租户帐户"

如果启用了**SSO**、则创建租户帐户

创建租户帐户时，您可以指定名称，客户端协议以及存储配额（可选）。如果为StorageGRID 启用了单点登录(SSO)、则还可以指定具有root访问权限的联合组来配置租户帐户。

步骤

1. 在*显示名称*文本框中、输入此租户帐户的显示名称。

显示名称不必唯一。创建租户帐户时、它会收到一个唯一的数字帐户ID。

2. 选择此租户帐户要使用的客户端协议、可以是* S3或* Swift*。
3. 对于S3租户帐户、请保持选中*允许平台服务*复选框、除非您不希望此租户对S3分段使用平台服务。

   如果启用了平台服务，则租户可以使用 CloudMirror 复制等功能来访问外部服务。您可能需要禁用这些功能来限制租户使用的网络带宽或其他资源量。请 M" 管理平台服务 " 。
4. 在*存储配额*文本框中、也可以输入要为此租户对象提供的最大GB、TB或PB数。然后、从下拉列表中选择单位。

   如果希望此租户拥有无限配额、请将此字段留空。

   租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。ILM副本和纠删编码不会影响所使用的配额量。如果超过配额、租户帐户将无法创建新对象。

   要监控每个租户帐户的存储使用情况、请选择*使用情况*。租户帐户还可以通过租户管理器中的信息板或租户管理API监控自己的存储使用情况。请注意、如果节点与网格中的其他节点隔离、则租户的存储使用量值可能会过时。恢复网络连接后，总数将更新。
5. 请注意、未选中和禁用*使用自己的身份源*复选框。

   由于启用了SSO、租户必须使用为网格管理器配置的身份源。没有本地用户可以登录。
6. 在*根访问组*字段中、从网格管理器中选择一个现有联合组、以便为租户提供初始根访问权限。

   如果您拥有足够的权限、则在单击此字段时会列出网格管理器中的现有联合组。否则，请输入组的唯一名称。
7. 单击 * 保存 * 。

   此时将创建租户帐户。此时将显示租户帐户页面、其中包含新租户对应的行。
8. 如果您是root访问组中的用户、也可以单击新租户的*登录*链接以立即访问租户管理器、您可以在其中配置租户。否则、请将*登录*链接的URL提供给租户帐户的管理员。(租户的URL是任何管理节点的完全限定域名或IP地址、后跟 `/?accountId=20-digit-account-id`)

   如果单击*登录*、则会显示访问被拒绝消息、但您不属于租户帐户的根访问组。

相关信息

"配置单点登录"

"管理S3租户帐户的平台服务"

"使用租户帐户"

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

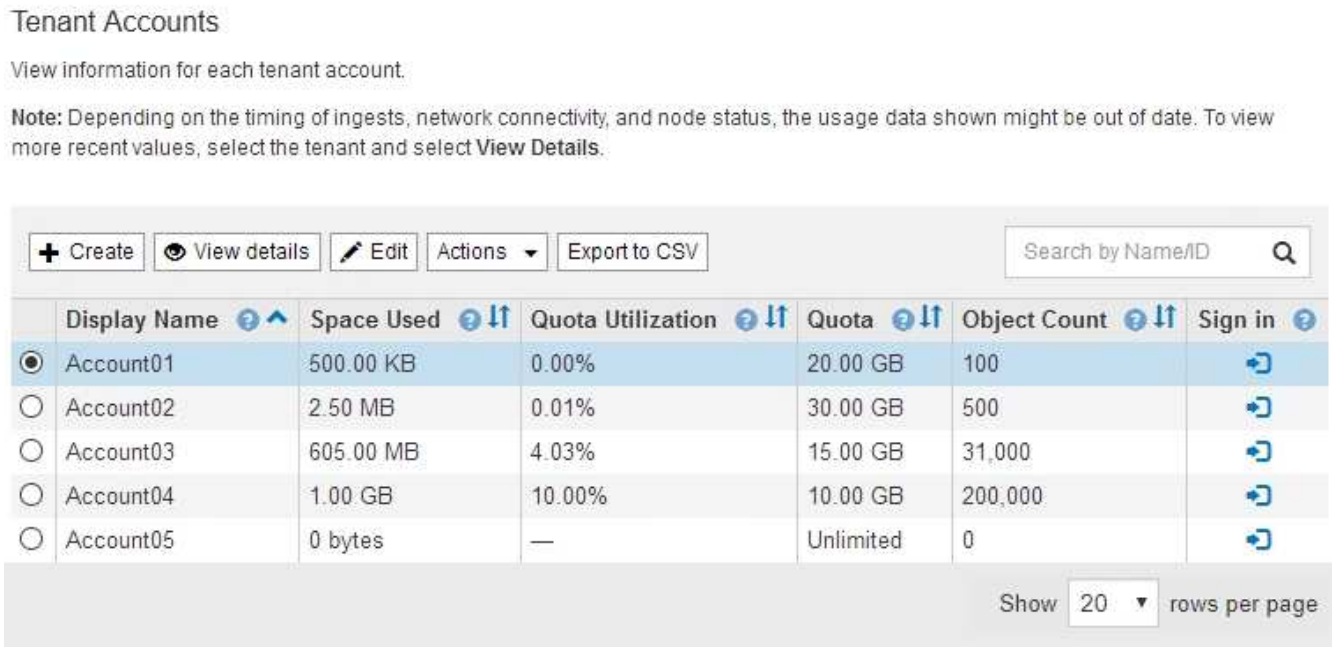
关于此任务

如果为 StorageGRID 系统启用了单点登录（ SSO ），则本地 root 用户将无法登录到租户帐户。要执行root用户任务、用户必须属于对租户具有root访问权限的联合组。

步骤

1. 选择*租户*。

   此时将显示租户帐户页面、其中列出了所有现有租户帐户。

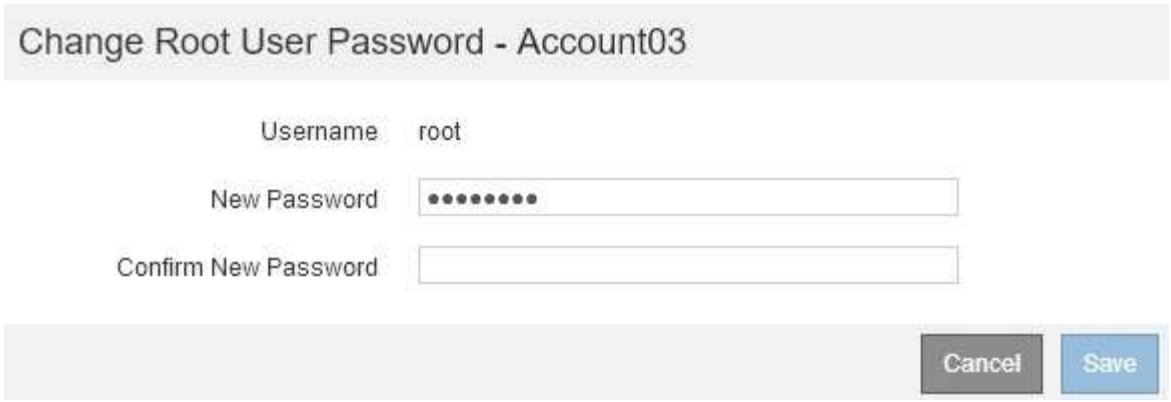


2. 选择要编辑的租户帐户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。使用搜索框按显示名称或租户ID搜索租户帐户。

   此时将启用查看详细信息、编辑和操作按钮。

3. 从*操作*下拉列表中、选择*更改根密码*。



4. 输入租户帐户的新密码。
5. 选择 * 保存 * 。

相关信息

"控制管理员对StorageGRID 的访问"

编辑租户帐户

您可以编辑租户帐户以更改显示名称，更改身份源设置，允许或禁止平台服务或输入存储配额。

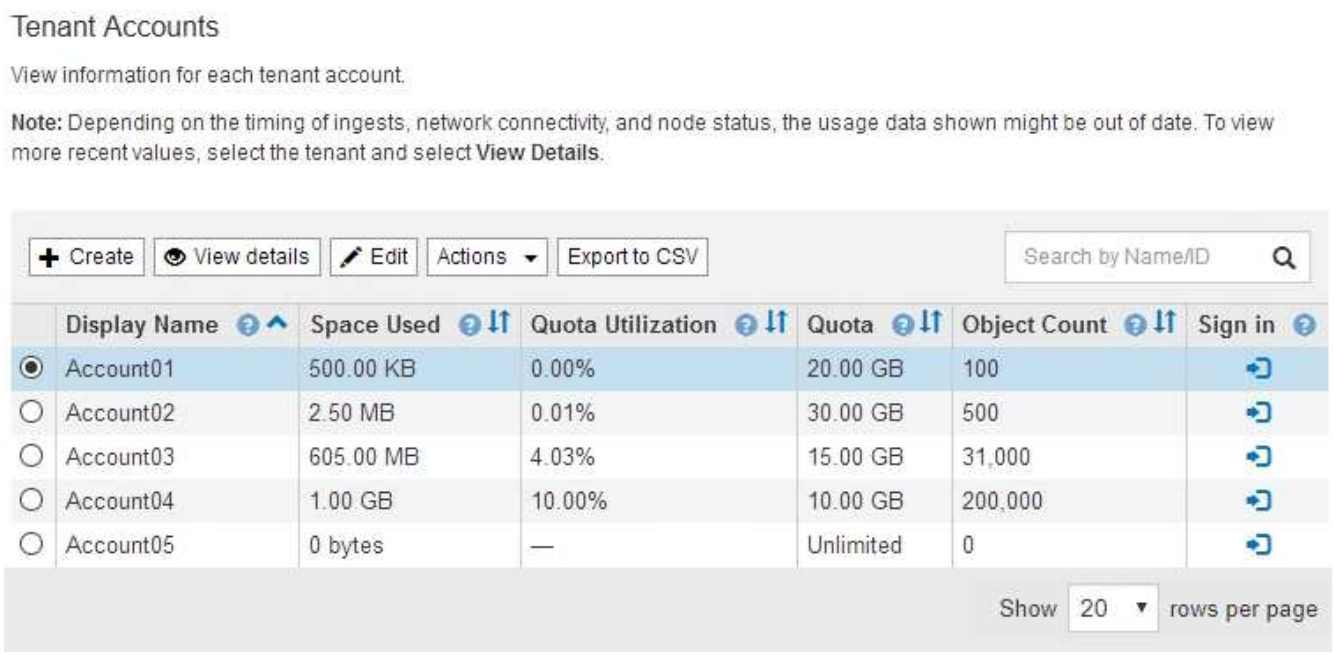
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

步骤

1. 选择*租户*。

   此时将显示租户帐户页面、其中列出了所有现有租户帐户。

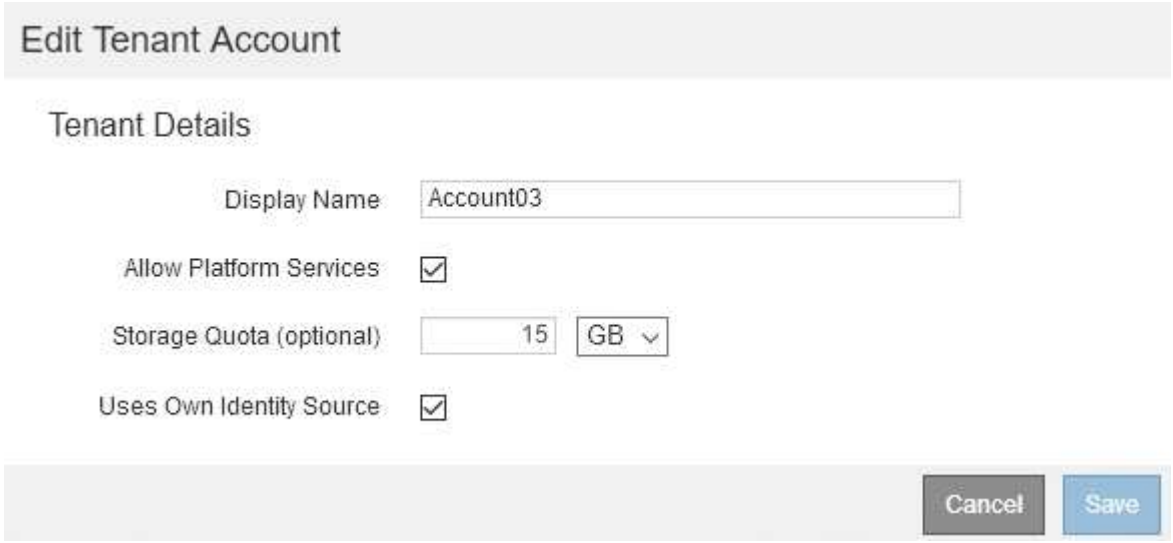


2. 选择要编辑的租户帐户。

   如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。使用搜索框按显示名称或租户ID搜索租户帐户。

3. 选择 * 编辑 * 。

   此时将显示编辑租户帐户页面。此示例适用于不使用单点登录（ SSO ）的网格。此租户帐户未配置其自己的身份源。



4. 根据需要更改字段的值。
   a. 更改此租户帐户的显示名称。
   b. 更改*允许平台服务*复选框的设置、以确定租户帐户是否可以对其S3分段使用平台服务。

如果为已在使用平台服务的租户禁用平台服务、则他们为其S3存储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。

c. 对于*存储配额*、更改此租户对象可用的最大GB、TB或PB数、或者如果希望此租户拥有无限配额、则将此字段留空。

租户的存储配额表示逻辑容量（对象大小），而不是物理容量（磁盘大小）。ILM副本和纠删编码不会影响所使用的配额量。

要监控每个租户帐户的存储使用情况、请选择*使用情况*。租户帐户还可以通过租户管理器中的信息板或租户管理API监控自己的使用情况。请注意、如果节点与网格中的其他节点隔离、则租户的存储使用量值可能会过时。恢复网络连接后，总数将更新。

d. 更改*使用自己的身份源*复选框的设置、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*复选框为：

- 已禁用并选中租户已启用其自己的身份源。租户必须先禁用其身份源，然后才能使用为网格管理器配置的身份源。
- 已禁用并取消选中，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。

5. 选择 * 保存 * 。

相关信息

"管理S3租户帐户的平台服务"

"使用租户帐户"

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您必须已删除与租户帐户关联的所有分段（ S3 ），容器（ Swift ）和对象。

步骤

1. 选择*租户*。
2. 选择要删除的租户帐户。

如果您的系统包含20个以上的项目、则可以指定一次在每个页面上显示的行数。使用搜索框按显示名称或租户ID搜索租户帐户。

3. 从*操作*下拉列表中、选择*删除*。
4. 选择 * 确定 * 。

相关信息

"控制管理员对StorageGRID 的访问"

管理S3租户帐户的平台服务

如果为 S3 租户帐户启用平台服务，则必须配置网格，以便租户可以访问使用这些服务所需的外部资源。

- "什么是平台服务"
- "用于平台服务的网络和端口"
- "按站点交付平台服务消息"
- "对平台服务进行故障排除"

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。

  > 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向指定的外部 Amazon Simple Notification Service （ SNS ）发送有关对对象执行的特定操作的通知。

  例如，您可以配置向管理员发送有关添加到存储分段中的每个对象的警报，这些对象表示与关键系统事件关联的日志文件。

  > 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，您必须了解以下建议：

- 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。
- 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。

相关信息

"使用租户帐户"

"配置存储代理设置"

"监控和放大；故障排除"

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
- 一种支持接收简单通知服务（ 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。

如果您使用的是非透明代理服务器、则还必须配置存储代理设置、以允许将消息发送到外部端点、例如Internet上的端点。

相关信息

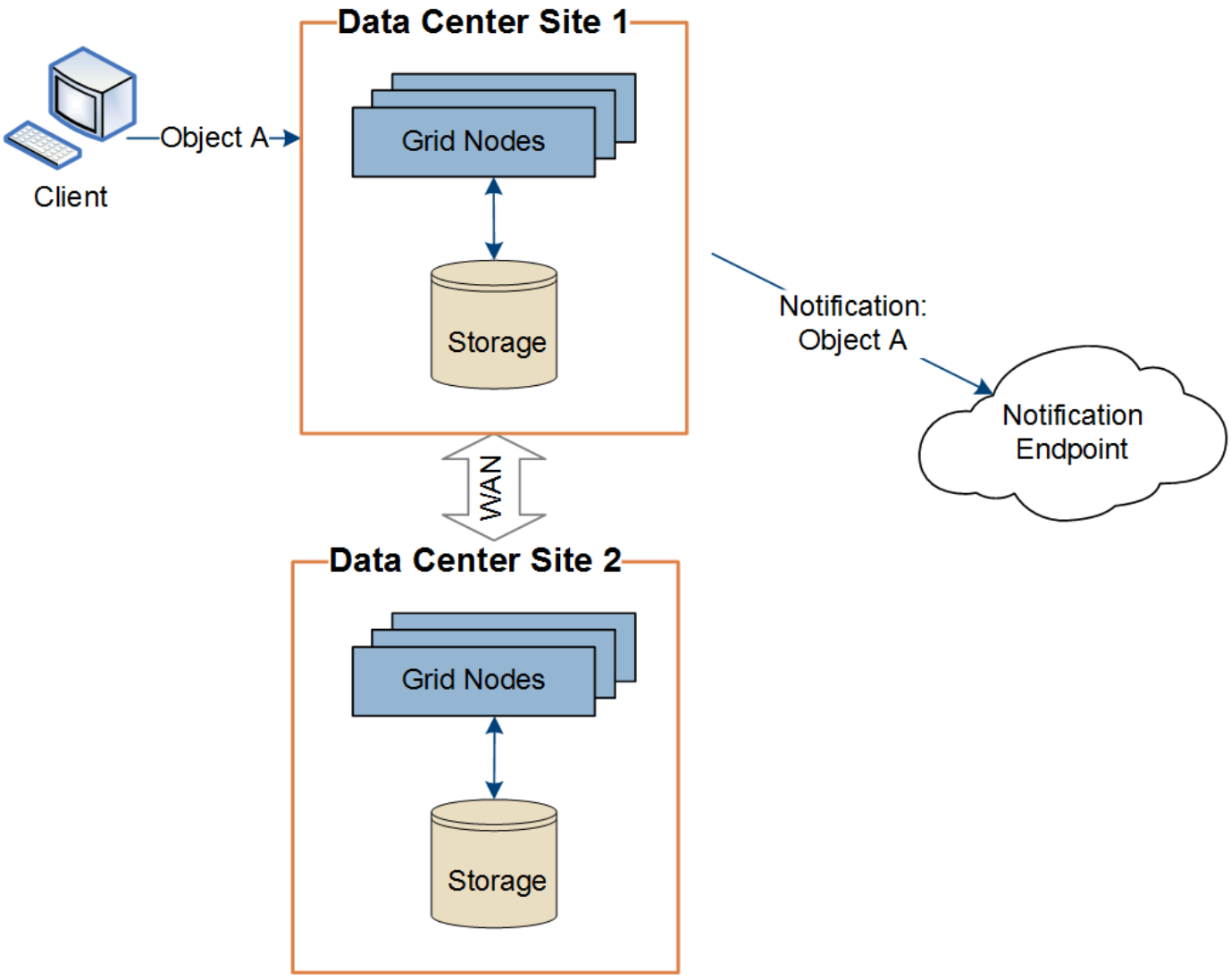
"配置存储代理设置"

"使用租户帐户"

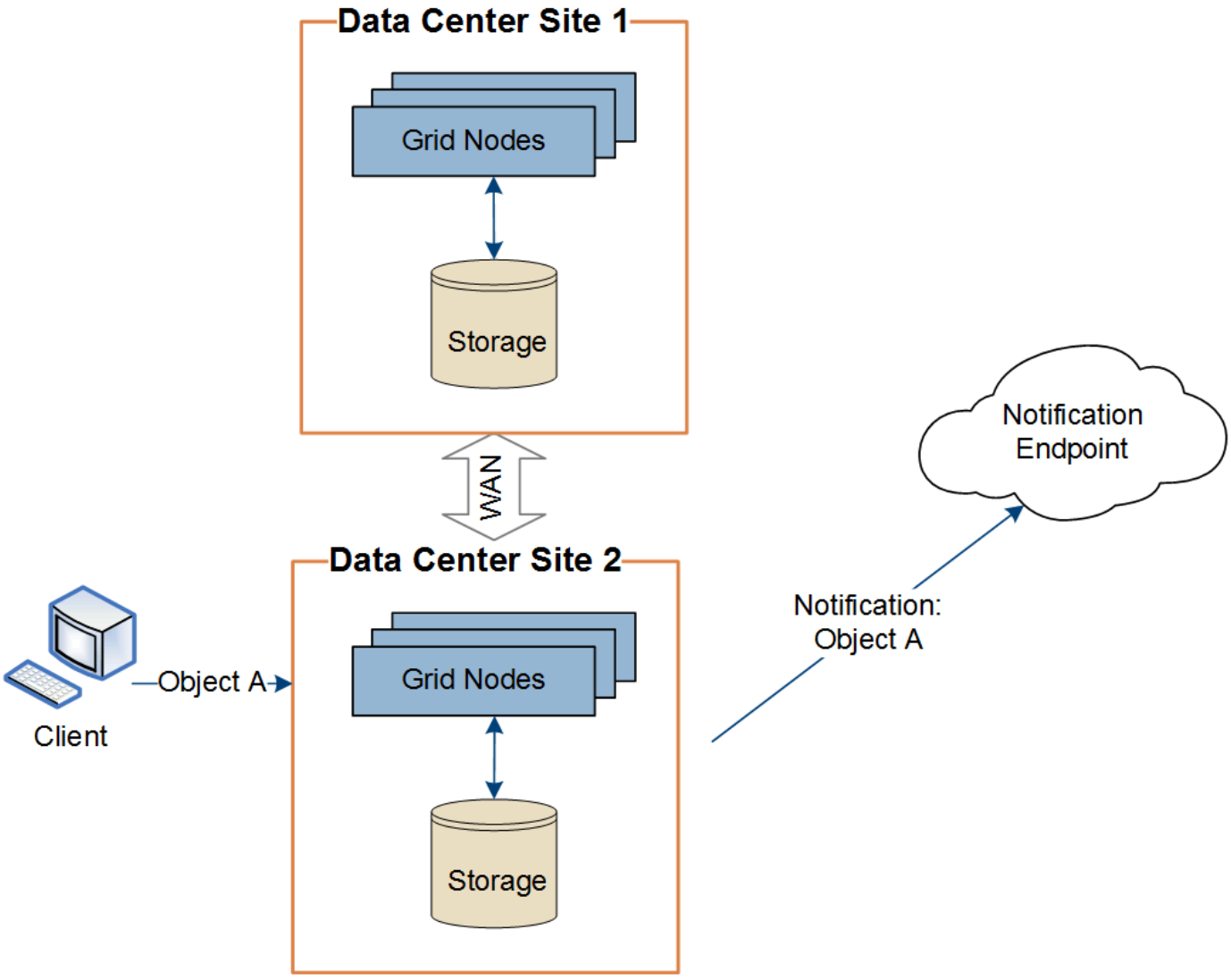
按站点交付平台服务消息

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。

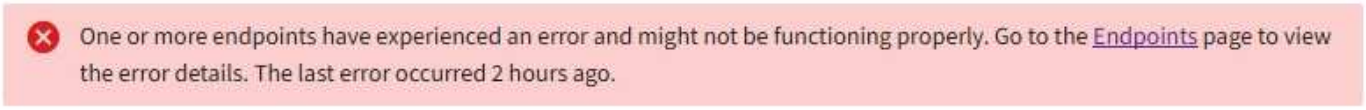
租户创建端点时， StorageGRID 系统会验证此端点是否存在，以及是否可以使用指定的凭据访问此端点。系统会从每个站点的一个节点验证与端点的连接。

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。

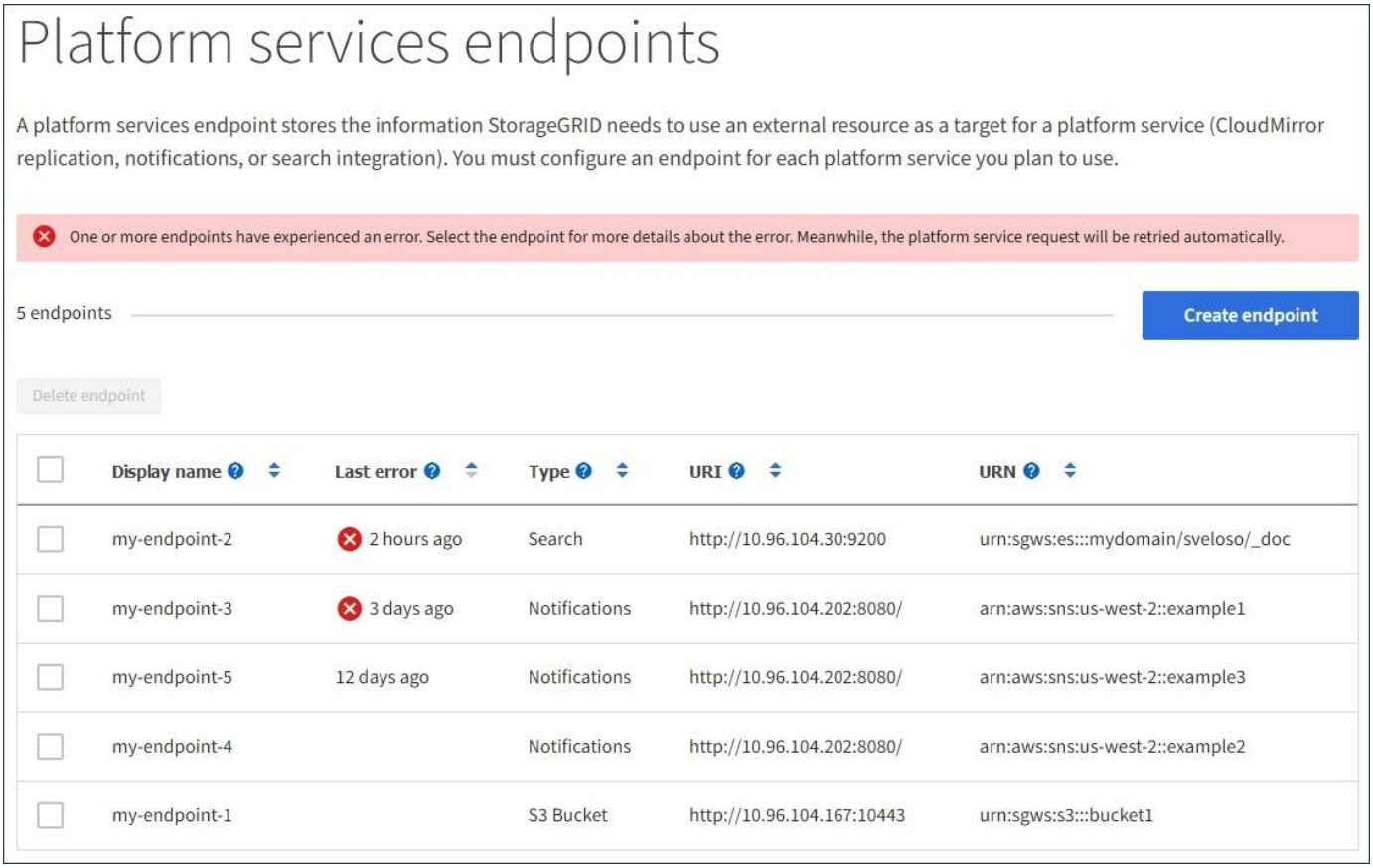
如果未为租户帐户启用平台服务，则端点创建将失败。

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，则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

如果您在存储节点和平台服务端点之间配置了存储代理，则如果您的代理服务不允许来自 StorageGRID 的消息，则可能会发生错误。要解决这些问题，请检查代理服务器的设置，以确保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，则租户管理器中的信息板将显示一条警报消息。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）警报。要查看事件总数警报、请执行以下操作：

1. 选择*节点*。
2. 选择*站点_*>*网格节点_*>*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. 单击*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。

如果由于不可恢复的错误而无法传送平台服务消息、则会在网格管理器中触发总事件(SMT)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. 查看请求故障率图表。

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。

有关追加信息 对平台服务端点进行故障排除的信息、请参见有关使用租户帐户的说明。

"使用租户帐户"

相关信息

"监控和放大；故障排除"

"配置存储代理设置"

配置S3和Swift客户端连接

作为网格管理员，您可以管理控制 S3 和 Swift 租户如何将客户端应用程序连接到 StorageGRID 系统以存储和检索数据的配置选项。有多种不同的选项可满足不同的客户端和租户要求。

客户端应用程序可以通过连接到以下任一项来存储或检索对象：

- 管理节点或网关节点上的负载平衡器服务，或者也可以是管理节点或网关节点高可用性（ HA ）组的虚拟 IP 地址
- 网关节点上的 CLB 服务，或者也可以是网关节点高可用性组的虚拟 IP 地址

> CLB 服务已弃用。在 StorageGRID 11.3 版本之前配置的客户端可以继续在网关节点上使用 CLB 服务。所有其他依靠 StorageGRID 提供负载平衡的客户端应用程序都应使用负载平衡器服务进行连接。

- 存储节点，具有或不具有外部负载平衡器

您可以选择在 StorageGRID 系统上配置以下功能：

- 负载平衡器服务：您可以通过为客户端连接创建负载平衡器端点来使客户端能够使用负载平衡器服务。创建负载平衡器端点时，您可以指定端口号，端点是否接受 HTTP 或 HTTPS 连接，将使用此端点的客户端类型（ S3 或 Swift ）以及用于 HTTPS 连接的证书（如果适用）。
- * 不可信客户端网络 * ：您可以通过将客户端网络配置为不可信来提高其安全性。如果客户端网络不可信，则客户端只能使用负载平衡器端点进行连接。
- 高可用性组：您可以创建一个由网关节点或管理节点组成的HA组来创建主动备份配置、也可以使用轮循DNS或第三方负载平衡器以及多个HA组来实现主动-主动配置。客户端连接使用 HA 组的虚拟 IP 地址进行。

此外，您还可以为直接连接到存储节点或使用 CLB 服务（已弃用）连接到 StorageGRID 的客户端启用 HTTP ，并且可以为 S3 客户端配置 S3 API 端点域名。

摘要：客户端连接的 IP 地址和端口

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 。如果配置了高可用性（ HA ）组，则客户端应用程序可以使用 HA 组的虚拟 IP 地址进行连接。

关于此任务

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。这些说明介绍了在已配置负载平衡器端点和高可用性（ HA ）组的情况下如何在网格管理器中查找此信息。

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	• 负载平衡器端点端口
HA 组	CLB • 注： * CLB 服务已弃用。	HA 组的虚拟 IP 地址	默认 S3 端口： • HTTPS： 8082 • HTTP： 8084 默认 Swift 端口： • HTTPS： 8083 • HTTP： 8085
管理节点	负载平衡器	管理节点的 IP 地址	• 负载平衡器端点端口
网关节点	负载平衡器	网关节点的 IP 地址	• 负载平衡器端点端口
网关节点	CLB • 注： * CLB 服务已弃用。	网关节点的 IP 地址 • 注意： * 默认情况下，CLB 和 LDR 的 HTTP 端口未启用。	默认 S3 端口： • HTTPS： 8082 • HTTP： 8084 默认 Swift 端口： • HTTPS： 8083 • HTTP： 8085
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

要将 S3 客户端连接到网关节点 HA 组的负载平衡器端点，请使用以下结构化 URL ：

- `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 ，而 S3 负载平衡器端点的端口号为 10443 ，则 S3 客户端可以使用以下 URL 连接到 StorageGRID ：

- `https://192.0.2.5:10443`

要将 Swift 客户端连接到网关节点 HA 组的负载平衡器端点，请使用以下结构化 URL ：

- `https://VIP-of-HA-group:LB-endpoint-port`

例如，如果 HA 组的虚拟 IP 地址为 192.0.2.6 ， Swift 负载平衡器端点的端口号为 10444 ，则 Swift 客户端可以使用以下 URL 连接到 StorageGRID ：

- `https://192.0.2.6:10444`

可以为客户端用于连接到 StorageGRID 的 IP 地址配置 DNS 名称。请与本地网络管理员联系。

步骤

1. 使用支持的浏览器登录到网格管理器。
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. 单击*显示更多*以查看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*>*网络设置*>*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*>*网络设置*>*负载平衡器端点*。

      此时将显示负载平衡器端点页面，其中显示了已配置的端点列表。

   b. 选择一个端点、然后单击*编辑端点*。

      此时将打开编辑端点窗口，并显示有关此端点的其他详细信息。

c. 确认已将选定端点配置为使用正确的协议(S3或Swift)、然后单击*取消*。

d. 记下要用于客户端连接的端点的端点端口号。

> 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保留的。所有其他端口都在网关节点和管理节点上进行配置。

管理负载平衡

您可以使用 StorageGRID 负载平衡功能处理从 S3 和 Swift 客户端载入和检索工作负载。负载平衡通过在多个存储节点之间分布工作负载和连接来最大限度地提高速度和连接容量。

您可以通过以下方式在StorageGRID 系统中实现负载平衡：

- 使用负载平衡器服务，该服务安装在管理节点和网关节点上。负载平衡器服务提供第 7 层负载平衡，并对客户端请求执行 TLS 终止，检查请求并建立与存储节点的新安全连接。这是建议的负载平衡机制。
- 使用连接负载平衡器(CLB)服务、该服务仅安装在网关节点上。CLB 服务提供第 4 层负载平衡并支持链路成本。

  > CLB 服务已弃用。

- 集成第三方负载平衡器。有关详细信息，请联系您的 NetApp 客户代表。

负载平衡的工作原理—负载平衡器服务

负载平衡器服务将传入的网络连接从客户端应用程序分发到存储节点。要启用负载平衡，必须使用网格管理器配置负载平衡器端点。

您只能为管理节点或网关节点配置负载平衡器端点，因为这些节点类型包含负载平衡器服务。您不能为存储节点或归档节点配置端点。

每个负载平衡器端点都指定一个端口、一个协议(HTTP或HTTPS)、一个服务类型(S3或Swift)和一个绑定模式。HTTPS 端点需要服务器证书。通过绑定模式，您可以将端点端口的可访问性限制为：

- 特定高可用性(HA)虚拟IP地址(VIP)
- 特定节点的特定网络接口

端口注意事项

客户端可以访问您在运行负载平衡器服务的任何节点上配置的任何端点，但有两个例外：端口 80 和 443 在管理节点上保留，因此在这些端口上配置的端点仅支持网关节点上的负载平衡操作。

如果已重新映射任何端口，则不能使用相同的端口配置负载平衡器端点。您可以使用重新映射的端口创建端点，但这些端点将重新映射到原始 CLB 端口和服务，而不是负载平衡器服务。按照恢复和维护说明中的步骤删除端口重新映射。

> CLB 服务已弃用。

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。

相关信息

"保持并恢复()"

配置负载平衡器端点

您可以创建、编辑和删除负载平衡器端点。

正在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、一个网络协议(HTTP或HTTPS)和一个服务类型(S3或Swift)。如果创建HTTPS端点、则必须上传或生成服务器证书。

您需要的内容

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。
- 如果先前已重新映射要用于负载平衡器服务的端口、则必须已删除重新映射。

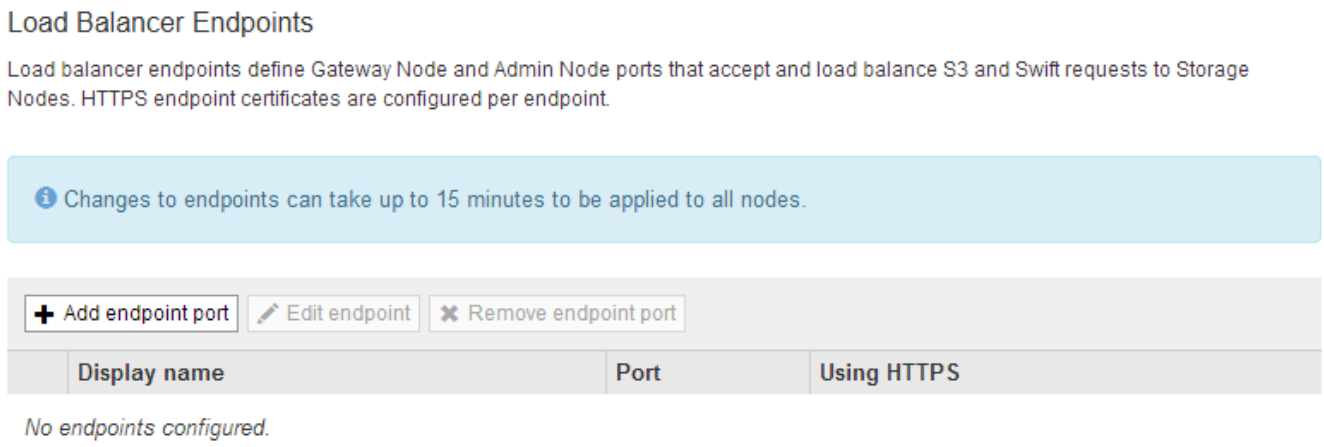
> 如果已重新映射任何端口，则不能使用相同的端口配置负载平衡器端点。您可以使用重新映射的端口创建端点，但这些端点将重新映射到原始 CLB 端口和服务，而不是负载平衡器服务。按照恢复和维护说明中的步骤删除端口重新映射。

> CLB 服务已弃用。

步骤

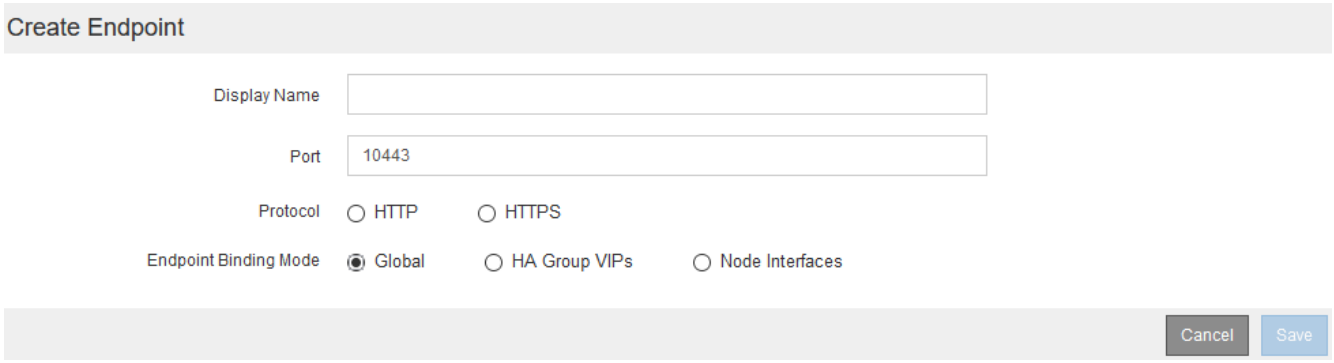
1. 选择*配置*>*网络设置*>*负载平衡器端点*。

   此时将显示负载平衡器端点页面。



2. 选择*添加端点*。

   此时将显示创建端点对话框。



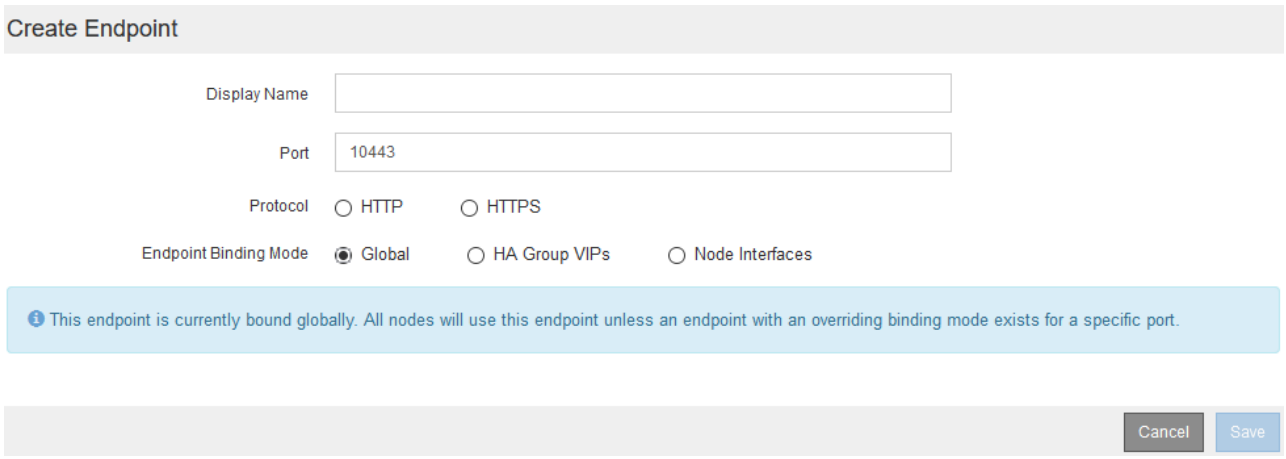
3. 输入端点的显示名称、此名称将显示在负载平衡器端点页面的列表中。
4. 输入端口号、或者保留预先填充的端口号不变。

   如果输入端口号80或443、则仅会在网关节点上配置端点、因为这些端口是在管理节点上保留的。

   不允许其他网格服务使用的端口。有关用于内部和外部通信的端口列表、请参见网络连接准则。

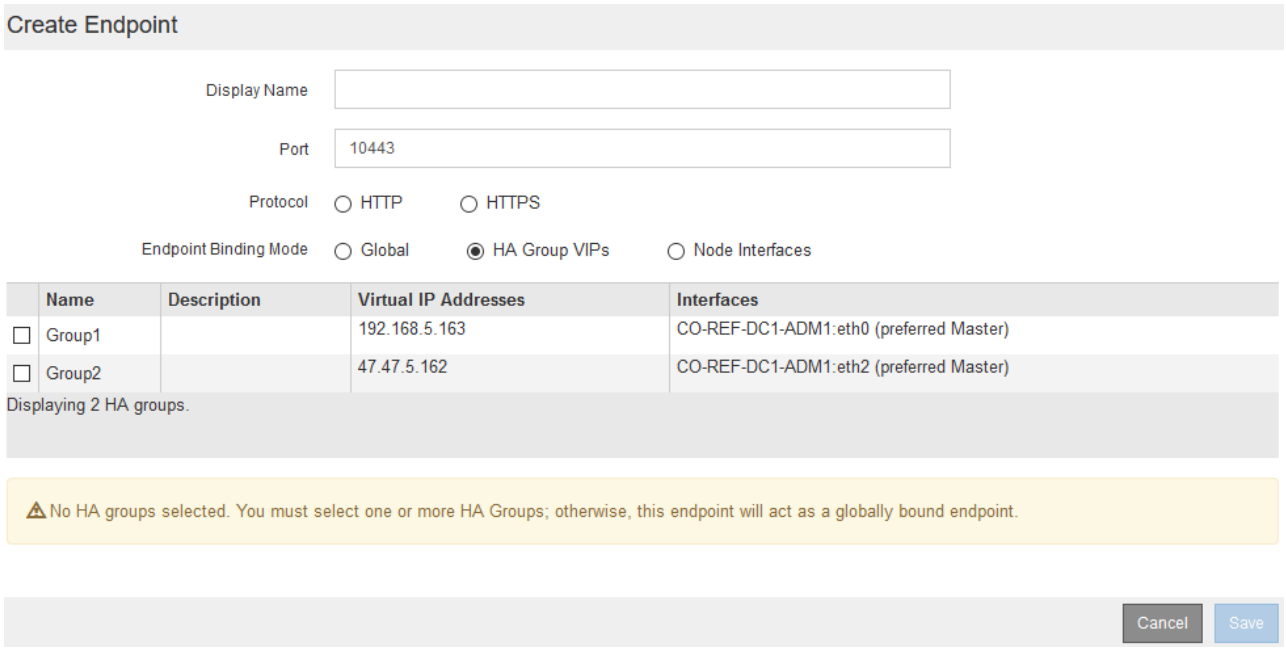
5. 选择* HTTP 或 HTTPS *以指定此端点的网络协议。
6. 选择端点绑定模式。

   - 全局(默认)：可以通过指定端口号在所有网关节点和管理节点上访问此端点。



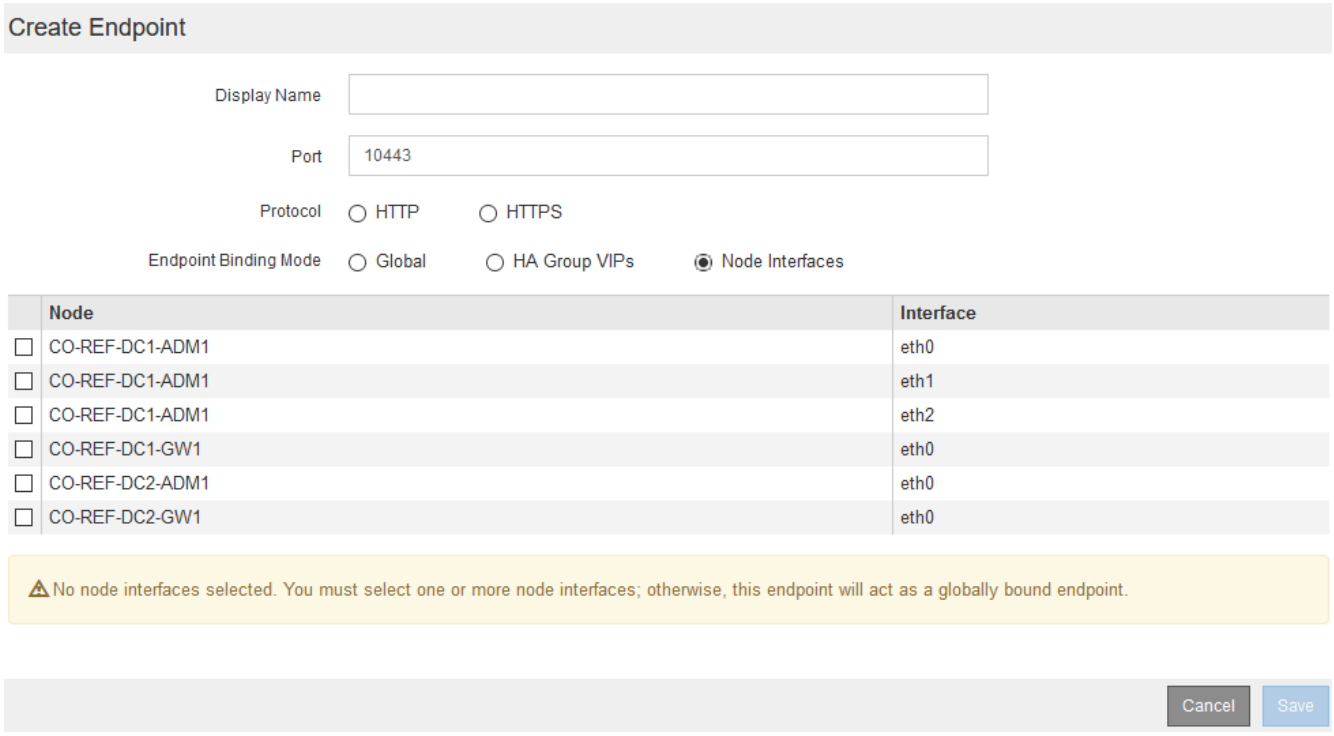
- * HA组VIP*：只有为选定HA组定义的虚拟IP地址才能访问此端点。在此模式下定义的端点可以重复使用相同的端口号、只要这些端点定义的HA组不会彼此重叠。

  选择包含要显示端点的虚拟IP地址的HA组。



- 节点接口：仅可在指定节点和网络接口上访问此端点。在此模式下定义的端点可以重复使用相同的端口号、只要这些接口不会彼此重叠。

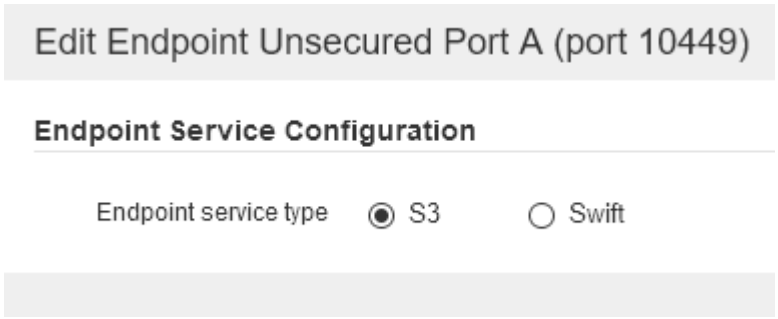
  选择要显示端点的节点接口。



7. 选择 * 保存 * 。

   此时将显示编辑端点对话框。

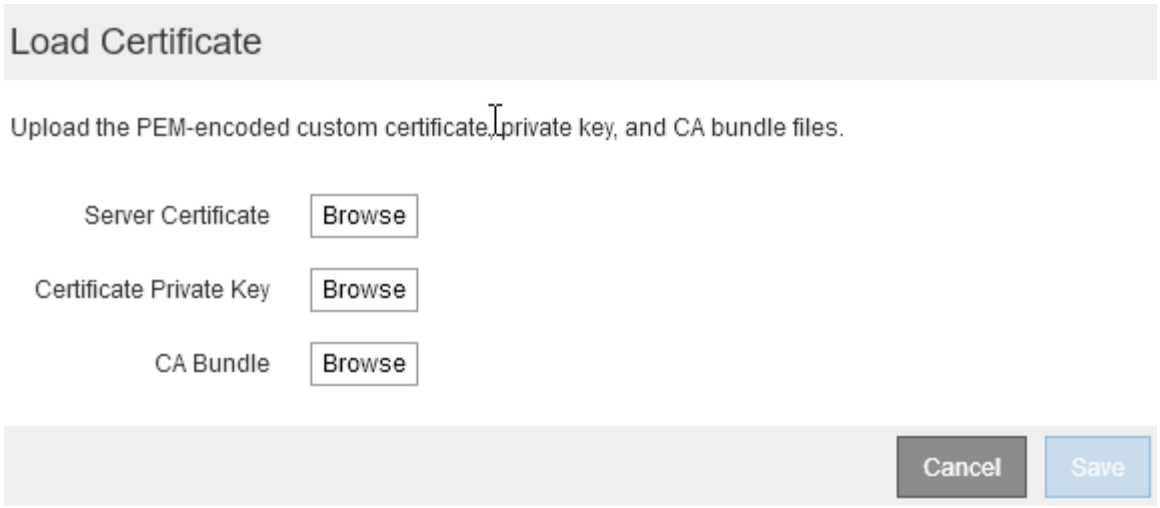
8. 选择* S3 或 Swift*以指定此端点将提供的流量类型。



9. 如果选择了* HTTP 、请选择*保存。

   此时将创建不安全的端点。负载平衡器端点页面上的表列出了端点的显示名称、端口号、协议和端点ID。

10. 如果选择了* HTTPS 并要上传证书、请选择*上传证书。



a. 浏览服务器证书和证书专用密钥。

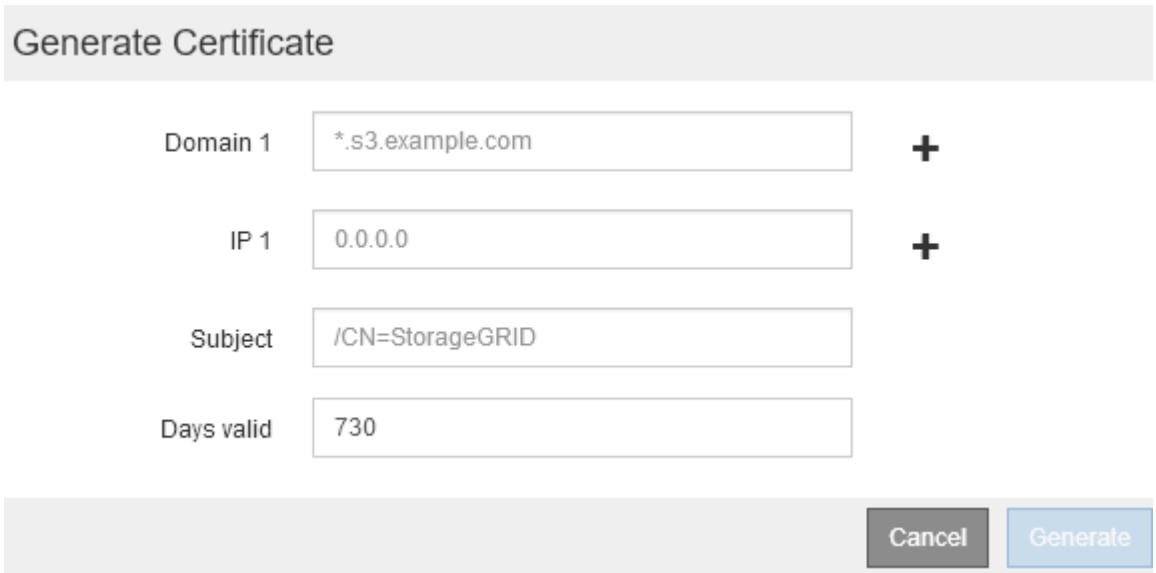
   要使S3客户端能够使用S3 API端点域名进行连接、请使用与客户端可能用于连接到网格的所有域名匹配的多域或通配符证书。例如、服务器证书可能使用域名 `*.example.com`。

"配置S3 API端点域名"

a. 也可以浏览CA包。
b. 选择 * 保存 * 。

   此时将显示端点的PEM编码证书数据。

11. 如果选择了* HTTPS 并要生成证书、请选择*生成证书。



a. 输入域名或IP地址。

   您可以使用通配符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：`*.sgws.foo.com` 使用*通配符表示 `gn1.sgws.foo.com` 和 `gn2.sgws.foo.com`。

"配置S3 API端点域名"

a. 选择 … ➕ 以添加任何其他域名或IP地址。

   如果您使用的是高可用性(HA)组、请添加HA虚拟IP的域名和IP地址。

b. (可选)输入一个X.509主题(也称为可分辨名称(Distinguished Name、DN))、以确定谁拥有此证书。

c. (可选)选择证书的有效天数。默认值为730天。

d. 选择 * 生成 * 。

   此时将显示端点的证书元数据和PEM编码的证书数据。

12. 单击 * 保存 * 。

此时将创建端点。负载平衡器端点页面上的表列出了端点的显示名称、端口号、协议和端点ID。

相关信息

"保持并恢复()"

"网络准则"

"管理高可用性组"

"管理不可信客户端网络"

编辑负载平衡器端点

对于不安全的(HTTP)端点、您可以在S3和Swift之间更改端点服务类型。对于安全(HTTPS)端点、您可以编辑端点服务类型并查看或更改安全证书。

您需要的内容

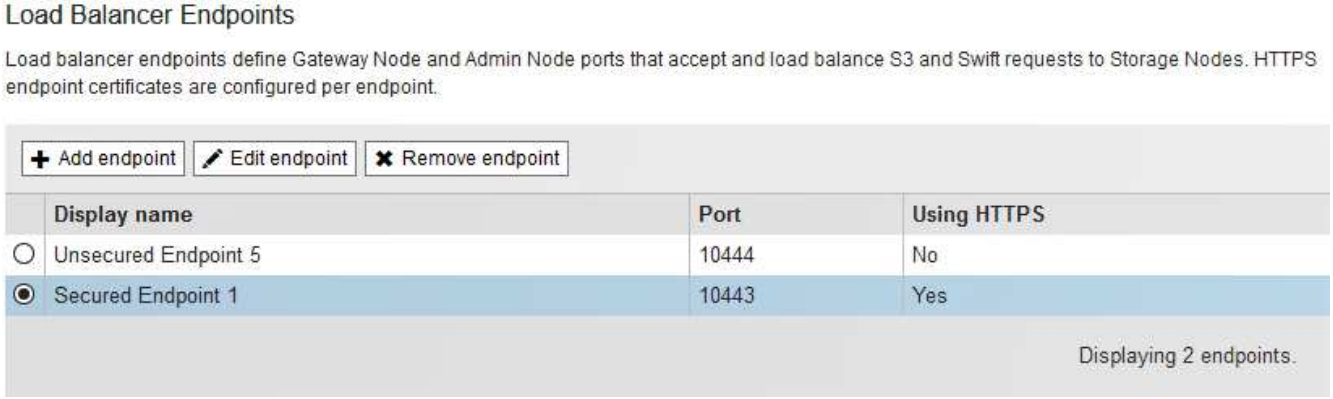
- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

步骤

1. 选择*配置*>*网络设置*>*负载平衡器端点*。

   此时将显示负载平衡器端点页面。表中列出了现有端点。

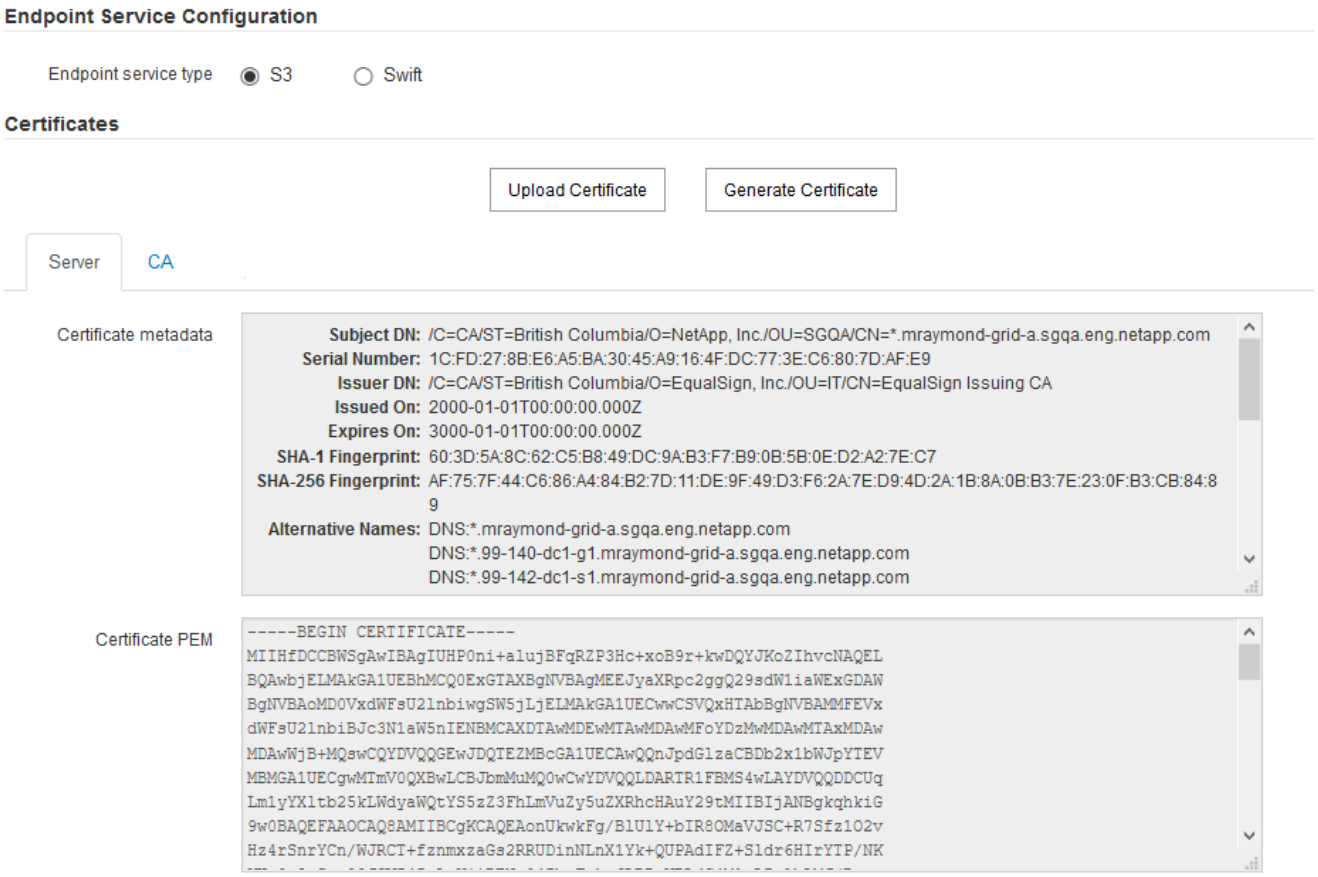
   表中标识了证书即将过期的端点。



2. 选择要编辑的端点。
3. 单击*编辑端点*。

   此时将显示编辑端点对话框。

   对于不安全的(HTTP)端点、仅会显示对话框的端点服务配置部分。对于安全(HTTPS)端点、此时将显示对话框的端点服务配置和证书部分、如以下示例所示。



4. 对端点进行所需的更改。

   对于不安全的(HTTP)端点、您可以：

   - 在S3和Swift之间更改端点服务类型。
   - 更改端点绑定模式。对于安全(HTTPS)端点、您可以：
   - 在S3和Swift之间更改端点服务类型。
   - 更改端点绑定模式。
   - 查看安全证书。
   - 当前证书到期或即将到期时、上传或生成新的安全证书。

     选择一个选项卡以显示有关已上传的默认StorageGRID 服务器证书或CA签名证书的详细信息。

   要更改现有端点的协议、例如从HTTP更改为HTTPS、必须创建一个新端点。按照说明创建负载平衡器端点、然后选择所需的协议。

5. 单击 * 保存 * 。

相关信息

[正在创建负载平衡器端点]

正在删除负载平衡器端点

如果您不再需要负载平衡器端点、可以将其删除。

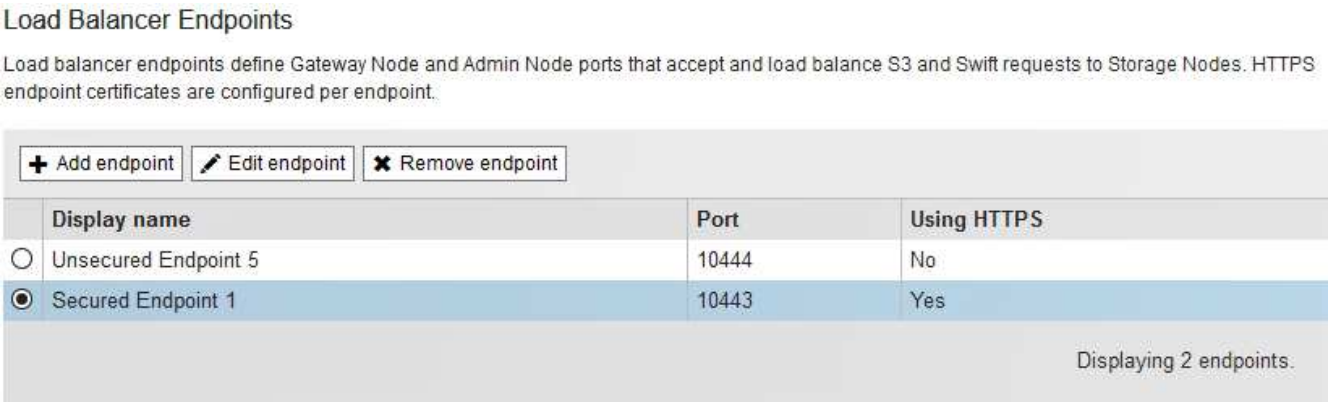
您需要的内容

- 您必须具有 root 访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

步骤

1. 选择*配置*>*网络设置*>*负载平衡器端点*。

   此时将显示负载平衡器端点页面。表中列出了现有端点。



2. 选择要删除的端点左侧的单选按钮。
3. 单击*删除端点*。

   此时将显示确认对话框。

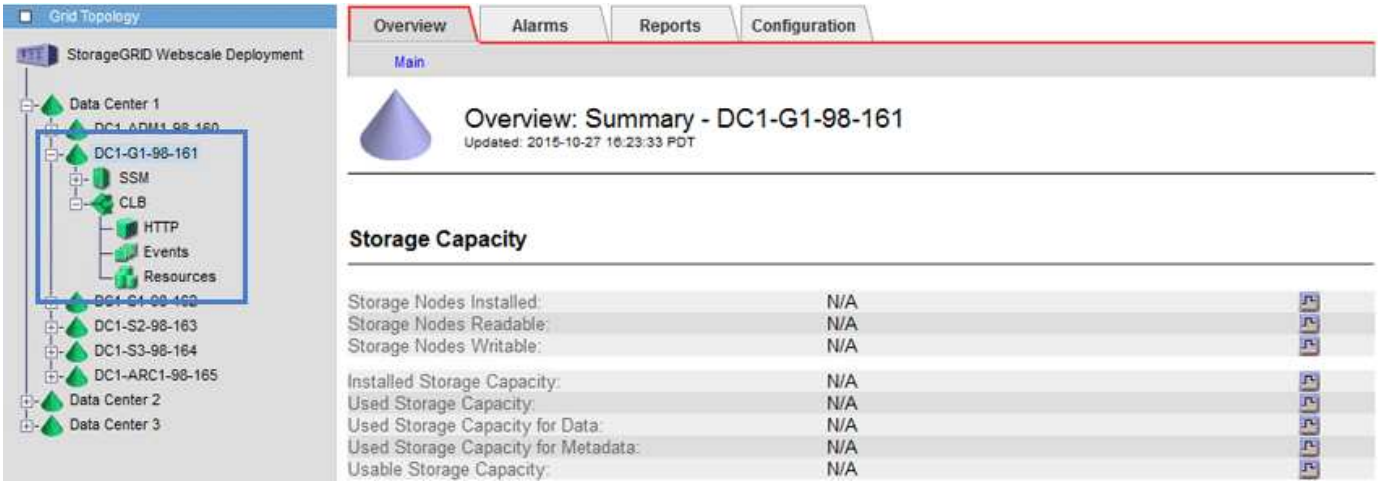
4. 单击 * 确定 * 。

   此端点将被删除。

网关节点上的连接负载平衡器（ CLB ）服务已弃用。现在，建议使用负载平衡器服务。

CLB 服务使用第 4 层负载平衡功能，根据可用性，系统负载和管理员配置的链路成本，将传入的 TCP 网络连接从客户端应用程序分发到最佳存储节点。选择最佳存储节点后， CLB 服务将建立双向网络连接，并将流量转发到选定节点和从选定节点转发流量。在定向传入网络连接时， CLB 不考虑网格网络配置。

要查看有关CLB服务的信息、请选择*支持*>*工具*>*网格拓扑*、然后展开网关节点、直到可以选择* CLB*及其下方的选项为止。



如果您选择使用 CLB 服务，则应考虑为 StorageGRID 系统配置链路成本。

相关信息

"链路成本是多少"

"更新链路成本"

管理不可信客户端网络

如果您使用的是客户端网络，则可以通过仅在显式配置的端点上接受入站客户端流量来帮助保护 StorageGRID 免受恶意攻击。

默认情况下，每个网格节点上的客户端网络均为 *trusted* 。也就是说、默认情况下、StorageGRID 会信任所有可用外部端口上与每个网格节点的入站连接(请参见网络准则中有关外部通信的信息)。

您可以通过指定每个节点上的客户端网络为 *untrused_* 来减少对 StorageGRID 系统的恶意攻击威胁。如果节点的客户端网络不可信，则节点仅接受显式配置为负载平衡器端点的端口上的入站连接。

示例 **1** ： 网关节点仅接受 **HTTPS S3** 请求

假设您希望网关节点拒绝客户端网络上除 HTTPS S3 请求以外的所有入站流量。您应执行以下常规步骤：

1. 在负载平衡器端点页面中，通过 HTTPS 在端口 443 上为 S3 配置负载平衡器端点。
2. 在不可信客户端网络页面中，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

假设您要从存储节点启用出站 S3 平台服务流量，但要阻止与客户端网络上的该存储节点建立任何入站连接。您应执行此常规步骤：

- 在不可信客户端网络页面中，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，但它仍允许向 Amazon Web Services 发出出站请求。

相关信息

"网络准则"

"配置负载平衡器端点"

指定节点的客户端网络不可信

如果您使用的是客户端网络，则可以指定每个节点的客户端网络是可信还是不可信。您还可以为扩展中添加的新节点指定默认设置。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。
- 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。

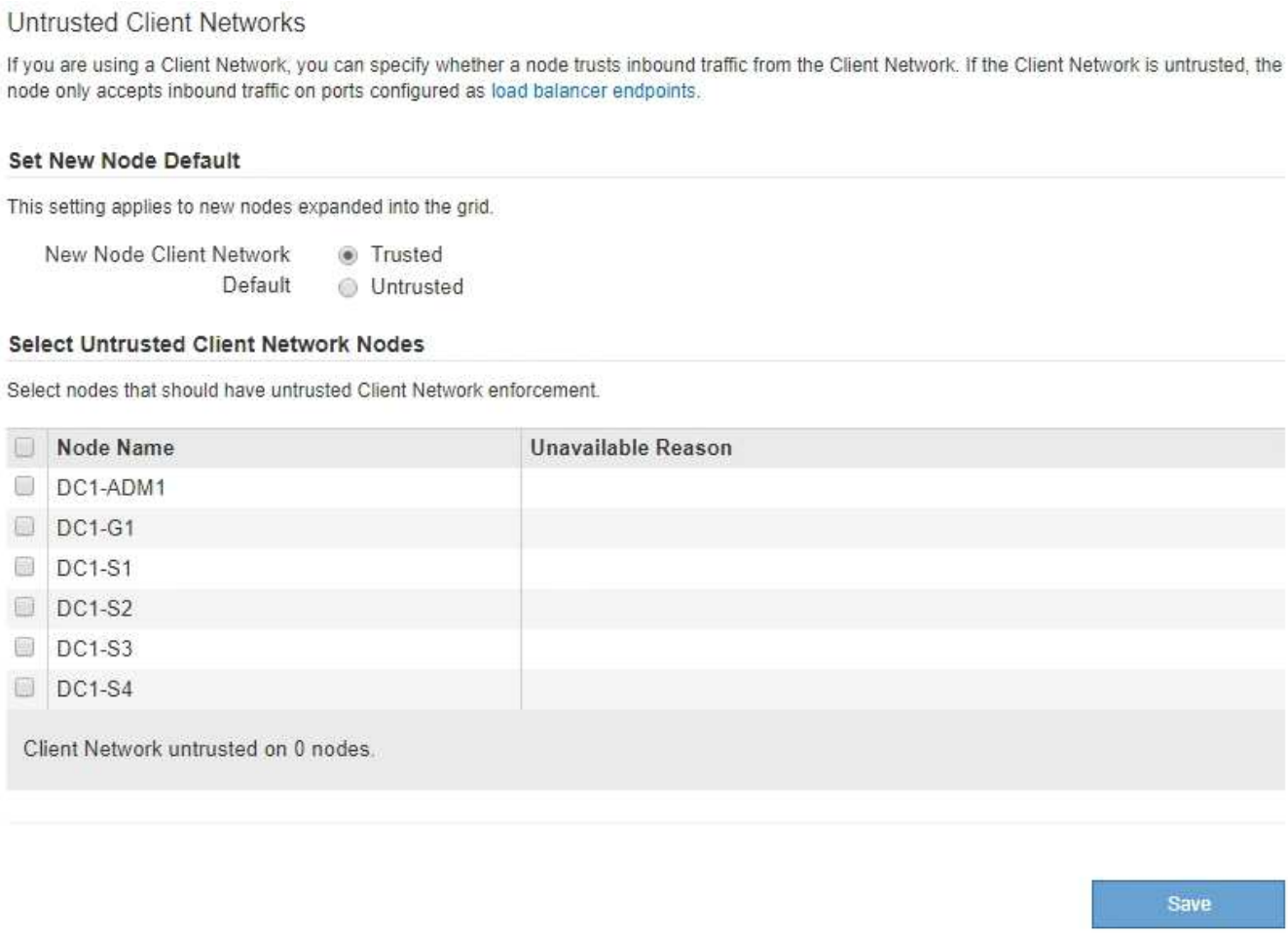
> 如果尚未配置负载平衡器端点，现有客户端连接可能会失败。

步骤

1. 选择*配置网络设置不可信客户端网络*。

   此时将显示不可信客户端网络页面。

   此页面列出了StorageGRID 系统中的所有节点。如果节点上的客户端网络必须可信，则不可用原因列将包含一个条目。



2. 在 * 设置新节点默认值 * 部分中，指定在扩展操作步骤 的网格中添加新节点时应采用的默认设置。
   - * 可信 * ： 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。根据需要，您可以返回此页面以更改特定新节点的设置。

   此设置不会影响 StorageGRID 系统中的现有节点。

3. 在 * 选择不可信客户端网络节点 * 部分中，选择应仅允许在显式配置的负载平衡器端点上进行客户端连接的节点。

   您可以选中或取消选中标题中的复选框以选择或取消选择所有节点。

4. 单击 * 保存 * 。

   此时将立即添加并强制实施新的防火墙规则。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。

相关信息

"配置负载平衡器端点"

管理高可用性组

高可用性(High Availability、HA)组可用于为S3和Swift客户端提供高可用性数据连接。HA

组还可用于提供与网格管理器和租户管理器的高可用性连接。

- "什么是HA组"
- "如何使用HA组"
- "HA 组的配置选项"
- "创建高可用性组"
- "编辑高可用性组"
- "删除高可用性组"

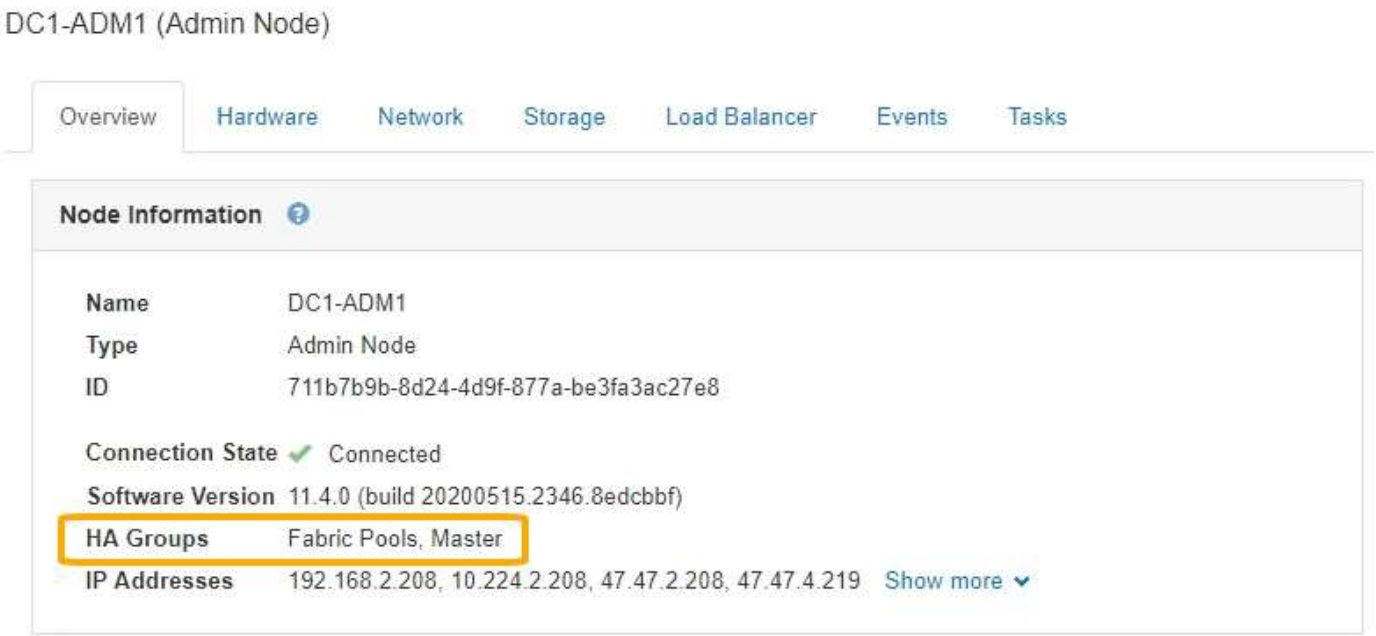
什么是**HA**组

高可用性组使用虚拟IP地址(VIP)为网关节点或管理节点服务提供主动备份访问。

HA组由管理节点和网关节点上的一个或多个网络接口组成。创建HA组时、您可以选择属于网格网络(eth0)或客户端网络(eth2)的网络接口。HA组中的所有接口必须位于同一网络子网中。

HA组维护一个或多个虚拟IP地址、这些地址会添加到组中的活动接口中。如果活动接口不可用、则虚拟IP地址将移至另一个接口。此故障转移过程通常只需几秒钟，并且速度足以使客户端应用程序不会受到任何影响，并且可以依靠正常的重试行为继续运行。

HA组中的活动接口被指定为主接口。所有其他接口均指定为备份。要查看这些指定值、请选择*节点*>*节点_*>*概述*。



创建HA组时、您可以指定一个接口作为首选主接口。首选主接口是活动接口、除非发生故障、导致VIP地址重新分配给备份接口。解决故障后、VIP地址会自动移回首选主节点。

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， CLB 服务（已弃用）或网格管理器或租户管理器服务失败也不会触发故障转移。

如果HA组包含来自两个以上节点的接口、则在故障转移期间、活动接口可能会移至任何其他节点的接口。

如何使用**HA**组

出于多种原因、您可能希望使用高可用性(HA)组。

- HA 组可以为网格管理器或租户管理器提供高度可用的管理连接。
- HA 组可以为 S3 和 Swift 客户端提供高可用性数据连接。
- 如果 HA 组仅包含一个接口，则可以提供多个 VIP 地址并明确设置 IPv6 地址。

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和 CLB 服务（已弃用）。

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(首选主节点) • 非主管理节点 *注：*主管理节点必须是首选主节点。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
S3 或 Swift 客户端访问— CLB 服务 • 注： * CLB 服务已弃用。	• 网关节点

将 **HA** 组与 **Grid Manager** 或租户管理器结合使用的限制

网格管理器或租户管理器的服务出现故障不会在HA组中触发故障转移。

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。

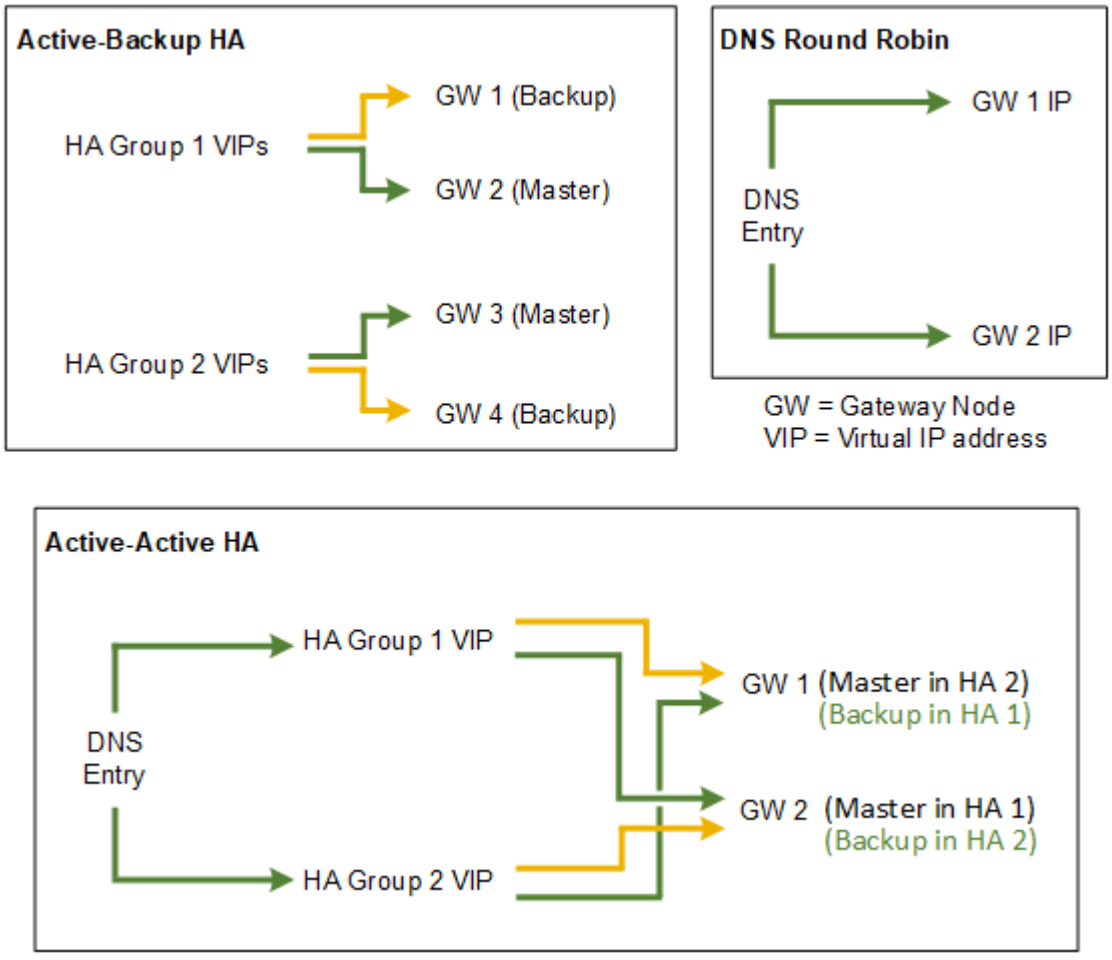
将 **HA** 组与 **CLB** 服务结合使用的限制

CLB 服务发生故障不会在 HA 组中触发故障转移。

CLB 服务已弃用。

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。



创建多个重叠的HA组时、如主动-主动HA示例所示、总吞吐量会随节点和HA组的数量进行扩展。对于三个或更多节点以及三个或更多HA组、您还可以使用任何VIP继续操作、即使在需要使节点脱机的维护过程中也是如此。

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。

Configuration	优势	缺点
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	• 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。

创建高可用性组

您可以创建一个或多个高可用性(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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

关于此任务

接口必须满足以下条件才能包含在HA组中：

- 接口必须用于网关节点或管理节点。
- 接口必须属于网格网络(eth0)或客户端网络(eth2)。
- 接口必须使用固定或静态IP地址配置、而不是使用DHCP配置。

步骤

1. 选择*配置*>*网络设置*>*高可用性组*。

   此时将显示高可用性组页面。

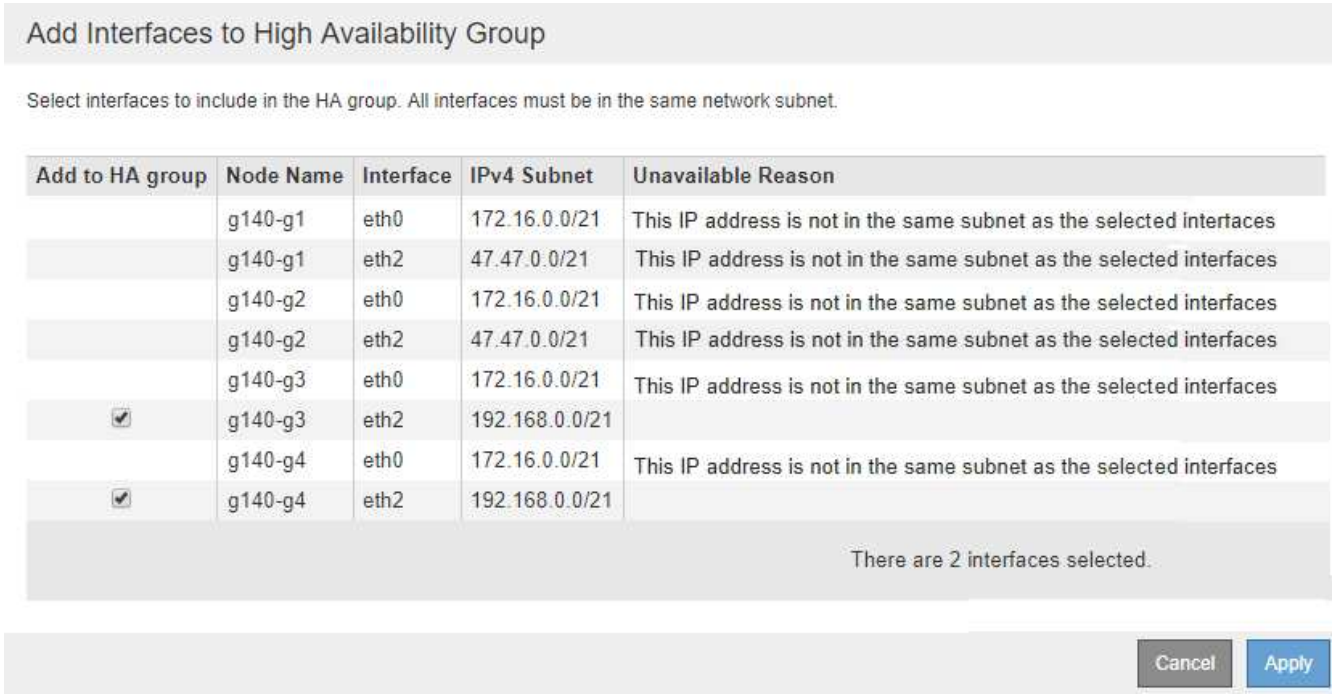
   

2. 单击 * 创建 * 。

   此时将显示创建高可用性组对话框。

3. 键入HA组的名称、如果需要、还可以键入问题描述。
4. 单击*选择接口*。

   此时将显示向高可用性组添加接口对话框。此表列出了符合条件的节点、接口和IPv4子网。



   如果某个接口的IP地址是由DHCP分配的、则该接口不会显示在列表中。

5. 在*添加到HA组*列中、选中要添加到HA组的接口对应的复选框。

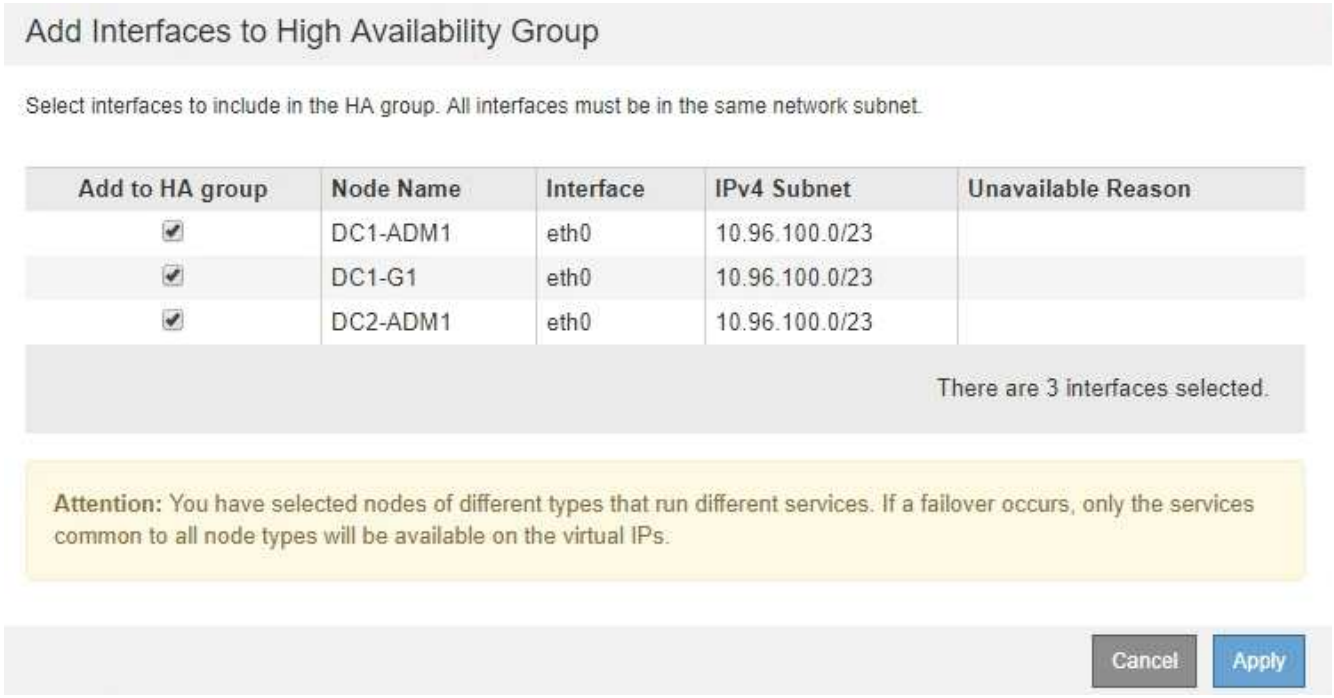
   请注意以下接口选择准则：

   - 必须至少选择一个接口。
   - 如果选择多个接口、则所有接口都必须位于网格网络(eth0)或客户端网络(eth2)上。
   - 所有接口都必须位于同一子网中、或者位于具有通用前缀的子网中。

     IP地址将限制为最小子网(前缀最大的子网)。

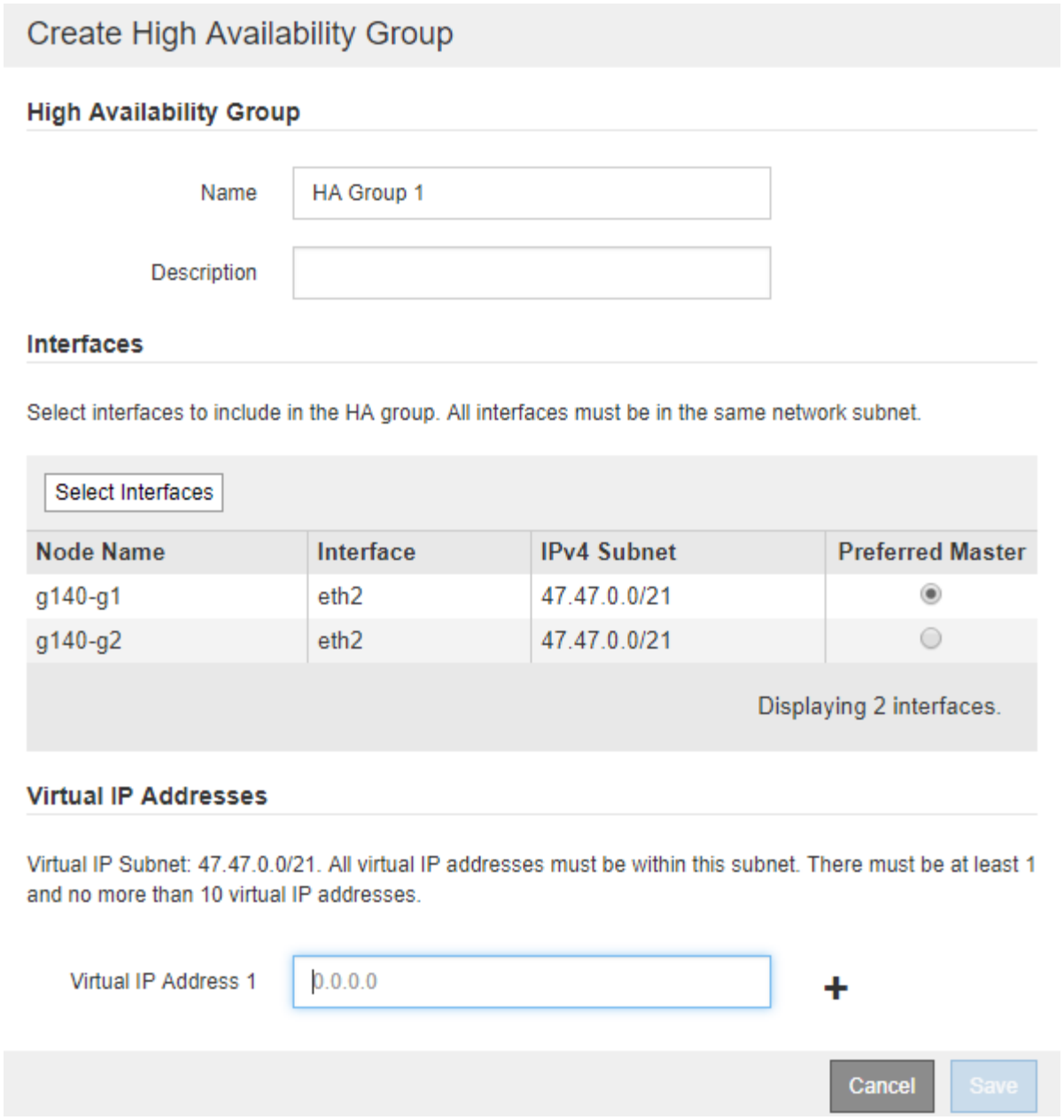
   - 如果您在不同类型的节点上选择接口、并且发生了故障转移、则虚拟IP上只会提供选定节点通用的服务。
     - 选择两个或多个管理节点以保护网格管理器或租户管理器的HA。
     - 为负载平衡器服务的HA保护选择两个或更多管理节点、网关节点或两者。
     - 选择两个或更多网关节点以对CLB服务进行HA保护。

       CLB 服务已弃用。



6. 单击 * 应用 * 。

   您选择的接口将在创建高可用性组页面的接口部分中列出。默认情况下、列表中的第一个接口被选择为首选主接口。



7. 如果要将其他接口作为首选主接口、请在*首选主接口*列中选择该接口。

   首选主接口是活动接口、除非发生故障、导致VIP地址重新分配给备份接口。

   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接口作为首选主节点。某些维护过程只能从主管理节点执行。

8. 在页面的虚拟IP地址部分中、为HA组输入1到10个虚拟IP地址。单击加号(+)以添加多个IP地址。

   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。

   IPv4地址必须位于所有成员接口共享的IPv4子网内。

9. 单击 * 保存 * 。

   此时将创建 HA 组，您现在可以使用已配置的虚拟 IP 地址。

相关信息

"安装 Red Hat Enterprise Linux 或 CentOS"

"安装 VMware"

"安装 Ubuntu 或 Debian"

"管理负载平衡"

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、或者添加或更新虚拟IP地址。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

关于此任务

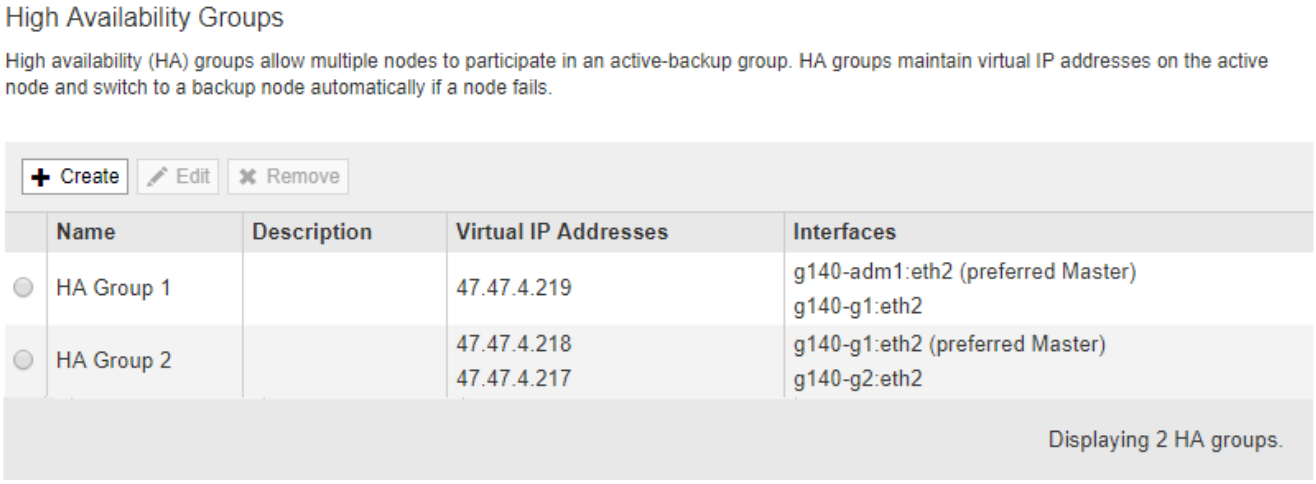
编辑HA组的一些原因如下：

- 向现有组添加接口。接口IP地址必须与已分配给组的其他接口位于同一子网中。
- 从HA组中删除接口。例如、如果HA组中使用了网格网络或客户端网络的节点接口、则无法启动站点或节点停用操作步骤。

步骤

1. 选择*配置*>*网络设置*>*高可用性组*。

   此时将显示高可用性组页面。



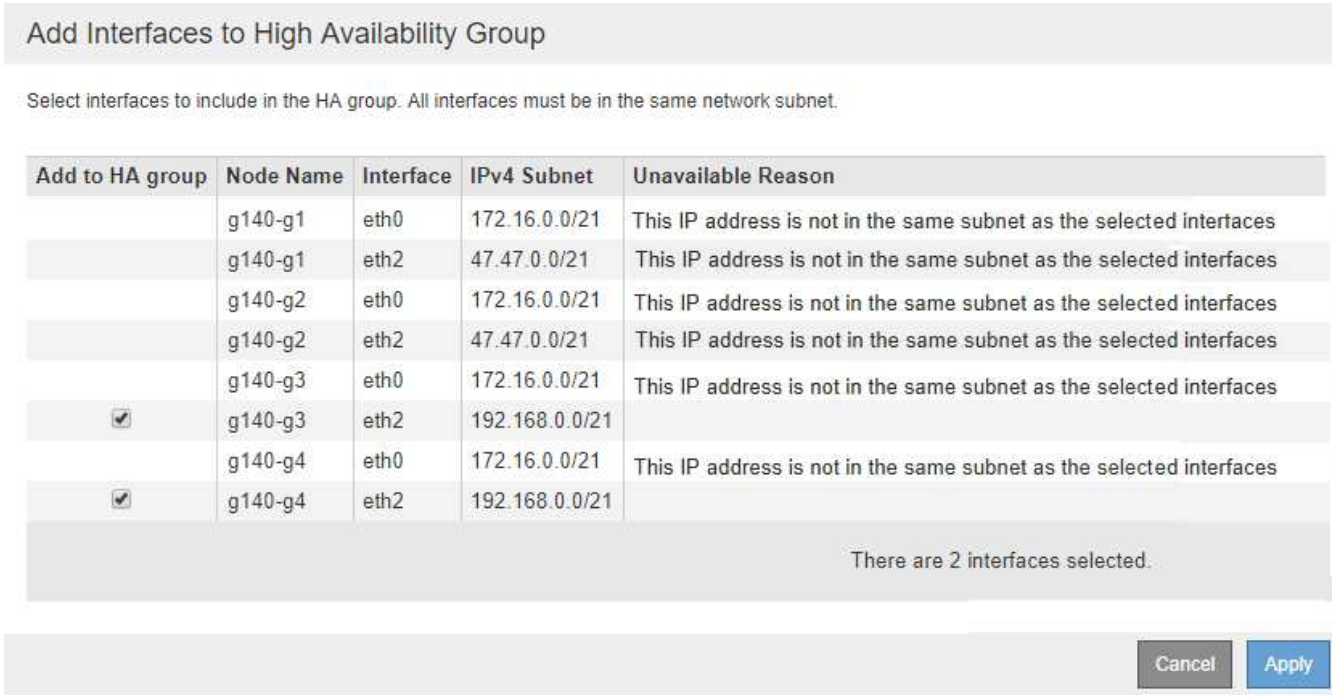
2. 选择要编辑的HA组、然后单击*编辑*。

   此时将显示编辑高可用性组对话框。

3. （可选）更新组的名称或问题描述 。

4. 或者、也可以单击*选择接口*以更改HA组的接口。

   此时将显示向高可用性组添加接口对话框。



   如果某个接口的IP地址是由DHCP分配的、则该接口不会显示在列表中。

5. 选中或取消选中要添加或删除接口的复选框。

   请注意以下接口选择准则：

   - 必须至少选择一个接口。
   - 如果选择多个接口、则所有接口都必须位于网格网络(eth0)或客户端网络(eth2)上。
   - 所有接口都必须位于同一子网中、或者位于具有通用前缀的子网中。

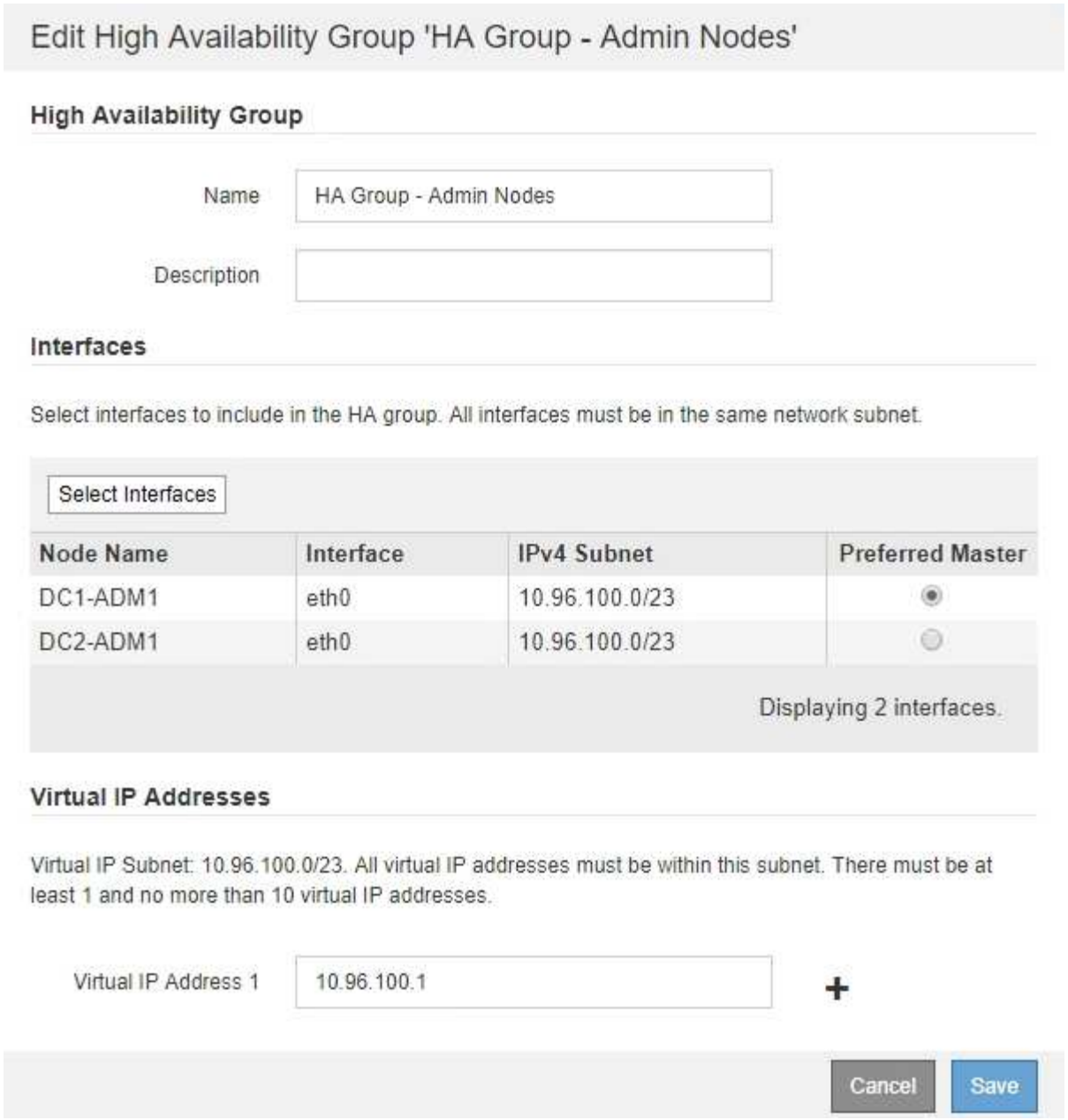
     IP地址将限制为最小子网(前缀最大的子网)。

   - 如果您在不同类型的节点上选择接口、并且发生了故障转移、则虚拟IP上只会提供选定节点通用的服务。
     - 选择两个或多个管理节点以保护网格管理器或租户管理器的HA。
     - 为负载平衡器服务的HA保护选择两个或更多管理节点、网关节点或两者。
     - 选择两个或更多网关节点以对CLB服务进行HA保护。

       CLB 服务已弃用。

6. 单击 * 应用 * 。

   您选择的接口将在页面的接口部分中列出。默认情况下、列表中的第一个接口被选择为首选主接口。



7. 如果要将其他接口作为首选主接口、请在*首选主接口*列中选择该接口。

   首选主接口是活动接口、除非发生故障、导致VIP地址重新分配给备份接口。

   > 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接口作为首选主节点。某些维护过程只能从主管理节点执行。

8. (可选)更新HA组的虚拟IP地址。

   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。

   IPv4地址必须位于所有成员接口共享的IPv4子网内。

9. 单击 * 保存 * 。

   此时将更新HA组。

删除高可用性组

您可以删除不再使用的高可用性(HA)组。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

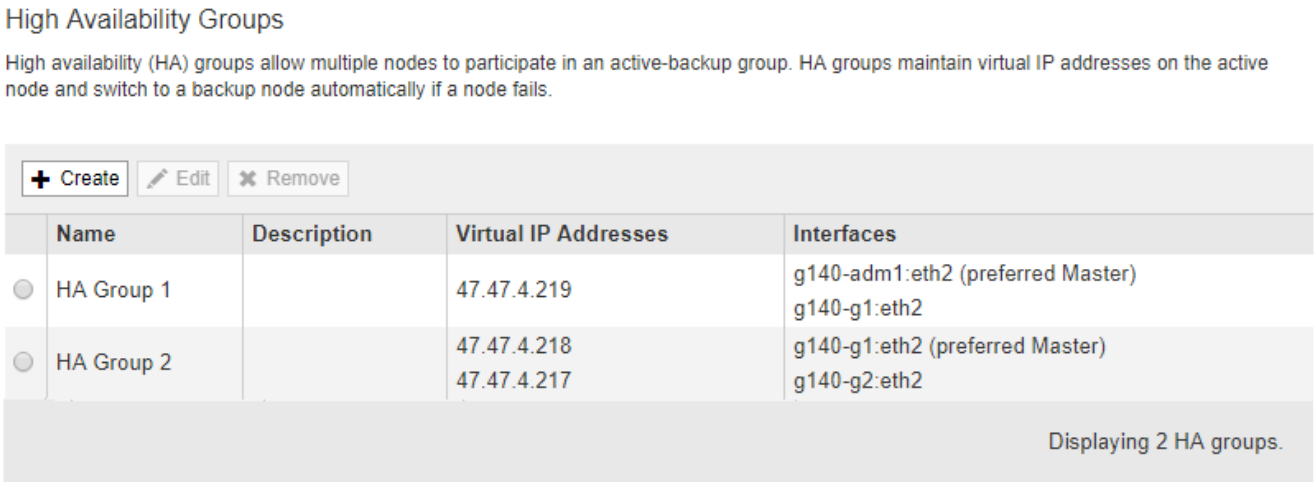
介绍此任务

如果删除HA组、则任何配置为使用该组的一个虚拟IP地址的S3或Swift客户端将无法再连接到StorageGRID。为防止客户端中断、应在删除HA组之前更新所有受影响的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、不同HA组的虚拟IP地址或在安装期间或使用DHCP为接口配置的IP地址。

步骤

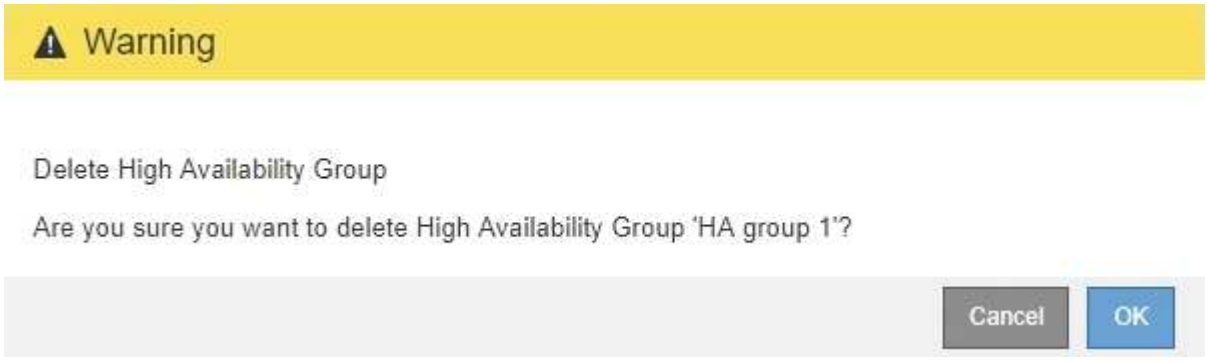
1. 选择*配置*>*网络设置*>*高可用性组*。

   此时将显示高可用性组页面。



2. 选择要删除的HA组、然后单击*删除*。

   此时将显示删除高可用性组警告。



3. 单击 * 确定 * 。

   此时将删除HA组。

配置S3 API端点域名

要支持 S3 虚拟托管模式请求，您必须使用网格管理器配置 S3 客户端连接到的端点域名列表。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您必须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任务：

- 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 的 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。为客户端用于建立连接的 IP 地址提供 DNS 记录，并确保这些记录引用所有必需的端点域名，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。

客户端用于HTTPS连接的证书取决于客户端如何连接到网格：

- 如果客户端使用负载平衡器服务进行连接、则会对特定负载平衡器端点使用证书。

> 每个负载平衡器端点都有自己的证书，并且可以对每个端点进行配置以识别不同的端点域名。

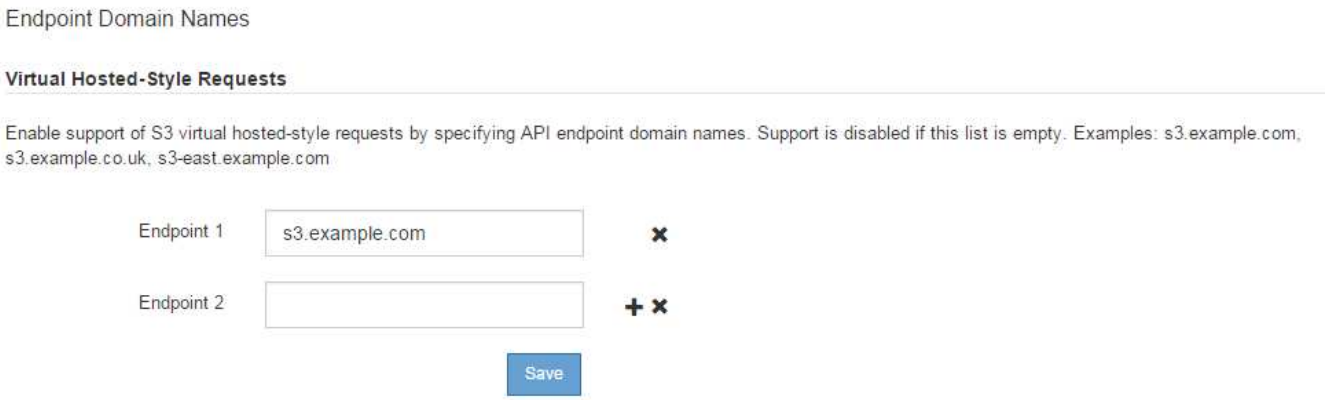
- 如果客户端连接到存储节点或网关节点上的CLB服务、则客户端将使用网格自定义服务器证书、该证书已更新、以包含所有必需的端点域名。

> CLB 服务已弃用。

步骤

1. 选择*配置*>*网络设置*>*域名*。

   此时将显示 Endpoint Domain Names 页面。



2. 使用(+)图标添加其他字段、在*端点*字段中输入S3 API端点域名列表。

   如果此列表为空，则会禁用对 S3 虚拟托管模式请求的支持。

3. 单击 * 保存 * 。
4. 确保客户端使用的服务器证书与所需的端点域名匹配。
   - 对于使用负载平衡器服务的客户端、更新与该客户端连接的负载平衡器端点关联的证书。
   - 对于直接连接到存储节点或在网关节点上使用CLB服务的客户端、请更新网格的自定义服务器证书。
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。

相关信息

"使用 S3"

"查看IP地址"

"创建高可用性组"

"配置自定义服务器证书以连接到存储节点或CLB服务"

"配置负载平衡器端点"

为客户端通信启用HTTP

默认情况下，客户端应用程序会使用 HTTPS 网络协议连接到存储节点或网关节点上已弃用的 CLB 服务。您可以选择为这些连接启用 HTTP ，例如在测试非生产网格时。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

只有当 S3 和 Swift 客户端需要直接与存储节点或网关节点上已弃用的 CLB 服务建立 HTTP 连接时，才能完成

此任务。

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，您无需完成此任务（因为您可以将每个负载平衡器端点配置为使用 HTTP 或 HTTPS ）。有关详细信息，请参见有关配置负载平衡器端点的信息。

请参见 "摘要：客户端连接的 IP 地址和端口" 了解使用 HTTP 或 HTTPS 连接到存储节点或已弃用的 CLB 服务时 S3 和 Swift 客户端使用的端口

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。

步骤

1. 选择*配置系统设置网格选项*。
2. 在网络选项部分中，选中 * 启用 HTTP 连接 * 复选框。

3. 单击 * 保存 * 。

相关信息

"配置负载平衡器端点"

"使用 S3"

"使用 Swift"

控制允许执行哪些客户端操作

您可以选择阻止客户端修改网格选项来拒绝特定的 HTTP 客户端操作。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

" 阻止客户端修改 " 是系统范围的设置。选择阻止客户端修改选项后，以下请求将被拒绝：

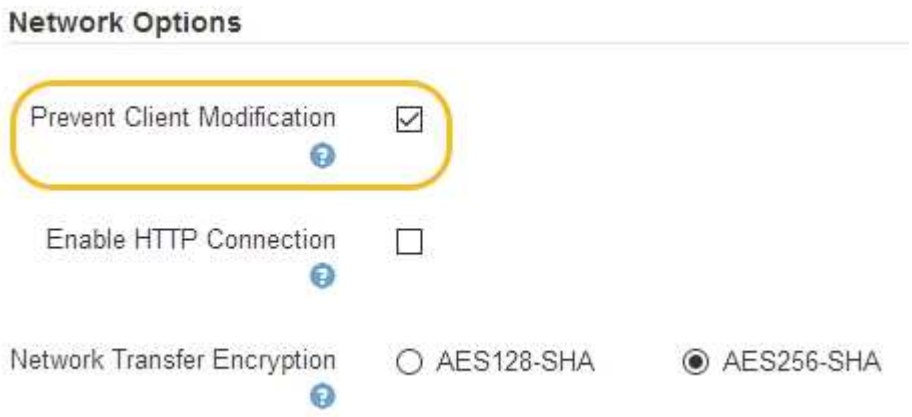
- * S3 REST APi*
  - 删除存储分段请求
  - 修改现有对象数据，用户定义的元数据或 S3 对象标记的任何请求

此设置不适用于启用了版本控制的存储分段。版本控制已阻止对对象数据，用户定义的元数据和对象标记进行修改。

- * 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。

步骤

1. 选择*配置系统设置网格选项*。
2. 在网络选项部分中，选中 * 阻止客户端修改 * 复选框。



3. 单击 * 保存 * 。

管理StorageGRID 网络和连接

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。

- "StorageGRID 网络准则"
- "查看IP地址"
- "支持传出 TLS 连接的密码"
- "更改网络传输加密"
- "配置服务器证书"
- "配置存储代理设置"
- "配置管理员代理设置"
- "管理流量分类策略"
- "链路成本是多少"

StorageGRID 网络准则

StorageGRID 在每个网格节点上最多支持三个网络接口，使您可以根据安全和访问要求为每个网格节点配置网络。

要修改或添加网格节点的网络、请参见恢复和维护说明。有关网络拓扑的详细信息、请参见网络连接说明。

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。
- 一个网格节点在一个网络上不能有多个接口。
- 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。

相关信息

"保持并恢复()"

"网络准则"

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。

您需要的内容

您必须使用支持的浏览器登录到网格管理器。

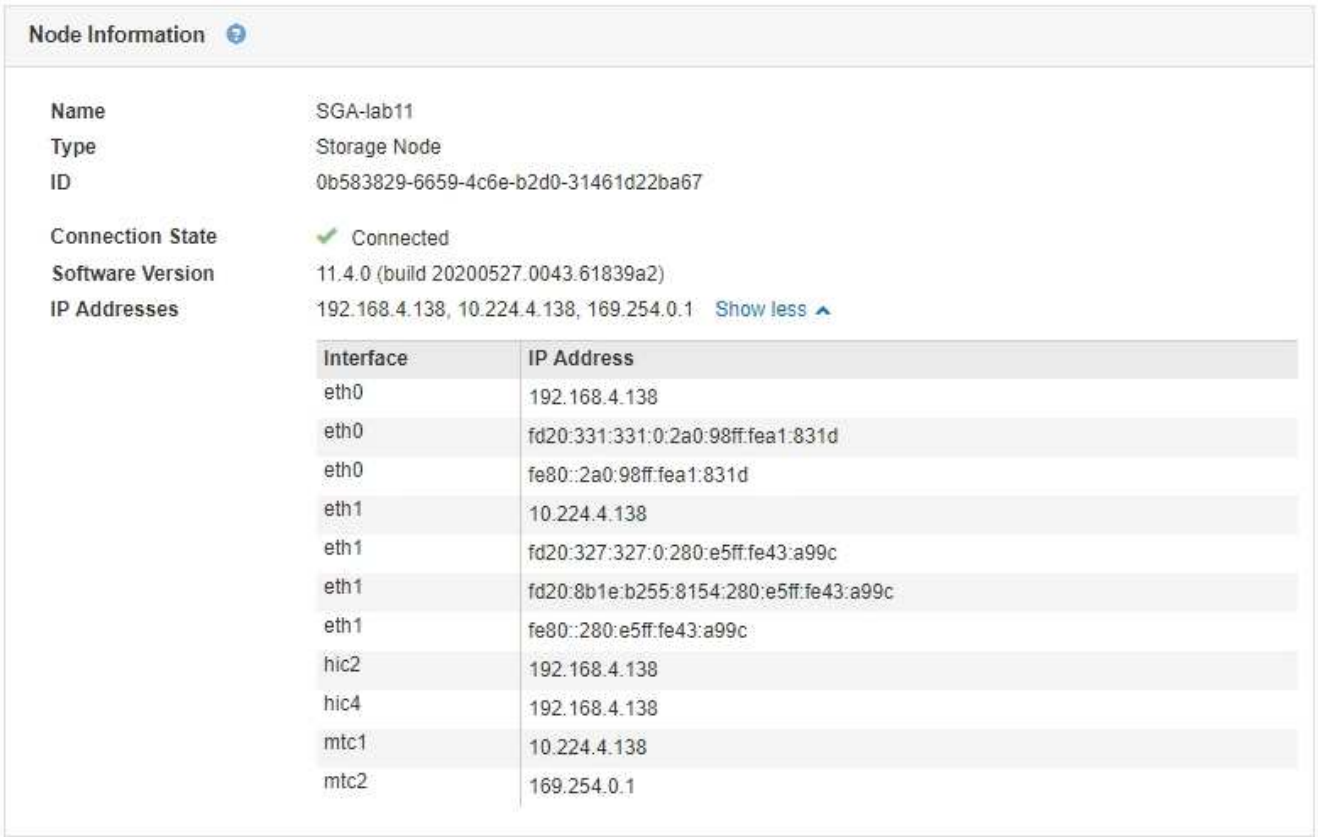
关于此任务

有关更改IP地址的信息、请参见恢复和维护说明。

步骤

1. 选择*节点*>*网格节点_*>*概述*。
2. 单击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。



相关信息

"保持并恢复()"

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。

> 协议版本，密码，密钥交换算法和 MAC 算法等 TLS 配置选项在 StorageGRID 中不可配置。如果您对这些设置有特定要求，请联系您的 NetApp 客户代表。

支持的 **TLS 1.2** 密码套件

支持以下 TLS 1.2 密码套件：

- tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256
- tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_ECDSA_WIT_AES_128_GCM_SHA256
- tls_ECDHE_ECDSA_WIT_AES_256_GCM_SHA384
- tls_ECDHE_RSA_WIT_CHACHA20_POLY1305
- tls_ECDHE_ECDSA_ING_CHACHA20_POLY1305
- tls_rsa_and_aes_128_gcm_SHA256
- tls_rsa_and_aes_256_gcm_SHA384

支持的 **TLS 1.3** 密码套件

支持以下 TLS 1.3 密码套件：

- tls_aes_256_gcm_SHA384
- tls_chacHA20_POLY1305_SHA256
- tls_aes_128_gcm_SHA256

更改网络传输加密

StorageGRID 系统使用传输层安全（ Transport Layer Security ， TLS ）保护网格节点之间的内部控制流量。网络传输加密选项用于设置 TLS 用于加密网格节点之间的控制流量的算法。此设置不会影响数据加密。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

默认情况下，网络传输加密使用 AES256-SHA 算法。此外，还可以使用 AES128-SHA 算法对控制流量进行加密。

步骤

1. 选择*配置系统设置网格选项*。
2. 在网络选项部分中，将网络传输加密更改为 * AES128-SHA* 或 * AES256-SHA* （默认）。

3. 单击 * 保存 * 。

配置服务器证书

您可以自定义StorageGRID 系统使用的服务器证书。

StorageGRID 系统将安全证书用于多种不同的用途：

- 管理接口服务器证书：用于保护对网格管理器、租户管理器、网格管理API和租户管理API的访问。
- 存储API服务器证书：用于保护对存储节点和网关节点的访问、API客户端应用程序使用这些节点上传和下载对象数据。

您可以使用在安装期间创建的默认证书、也可以将其中一种或两种默认类型的证书替换为您自己的自定义证书。

支持的自定义服务器证书类型

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

有关StorageGRID 如何为REST API保护客户端连接的详细信息、请参见S3或Swift实施指南。

负载平衡器端点的证书

StorageGRID 单独管理用于负载平衡器端点的证书。要配置负载平衡器证书、请参见有关配置负载平衡器端点的说明。

相关信息

"使用 S3"

"使用 Swift"

"配置负载平衡器端点"

为网格管理器和租户管理器配置自定义服务器证书

您可以将默认 StorageGRID 服务器证书替换为一个自定义服务器证书，该证书允许用户访问网格管理器和租户管理器，而不会遇到安全警告。

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服务器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服务器证书、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浏览器中安装根CA证书。

> 为了确保操作不会因服务器证书失败而中断、当此服务器证书即将过期时、系统会触发*管理接口的服务器证书到期*警报和原有的管理接口证书到期(Management Interface Certificate Expiration、MCEP)警报。根据需要、您可以选择*支持*>*工具*>*网格拓扑*来查看当前服务证书到期前的天数。然后、选择*主管理节点_*>*。CMN*>*资源*。

> 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服务器证书将过期。
> - 您可以从自定义管理接口服务器证书还原到默认服务器证书。

步骤

1. 选择*配置*>*网络设置*>*服务器证书*。
2. 在管理接口服务器证书部分中、单击*安装自定义证书*。
3. 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 (`.crt`）。
   - 服务器证书专用密钥：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。
4. 单击 * 保存 * 。

   自定义服务器证书将用于所有后续的新客户端连接。

   选择一个选项卡以显示有关已上传的默认StorageGRID 服务器证书或CA签名证书的详细信息。

   > 上传新证书后、请留出最多一天的时间来清除任何相关证书到期警报(或旧警报)。

5. 刷新页面以确保 Web 浏览器已更新。

还原网格管理器和租户管理器的默认服务器证书

您可以还原为使用网格管理器和租户管理器的默认服务器证书。

步骤

1. 选择*配置*>*网络设置*>*服务器证书*。
2. 在管理接口服务器证书部分中、单击*使用默认证书*。
3. 单击确认对话框中的 * 确定 * 。

   还原默认服务器证书时、您配置的自定义服务器证书文件将被删除、无法从系统中恢复。默认服务器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。

配置自定义服务器证书以连接到存储节点或**CLB**服务

您可以替换用于通过S3或Swift客户端连接到存储节点或网关节点上的CLB服务(已弃用)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、用户可能还需要在用于访问系统的S3或Swift API客户端中安装根CA证书、具体取决于所使用的根证书颁发机构(CA)。

> 为了确保操作不会因服务器证书失败而中断、在根服务器证书即将过期时、系统会触发*存储API端点服务器证书到期*警报和原有的存储API服务端点证书到期(SCEP)警报。根据需要、您可以选择*支持工具*网格拓扑*来查看当前服务证书到期前的天数。然后、选择*主管理节点_ **CMN**资源。

只有当客户端在网关节点上使用已弃用的CLB服务连接到StorageGRID 或直接连接到存储节点时、才会使用自定义证书。在管理节点或网关节点上使用负载平衡器服务连接到StorageGRID 的S3或Swift客户端使用为负载平衡器端点配置的证书。

> 负载平衡器端点的*负载平衡器端点证书到期*警报将触发、该端点不久将过期。

步骤

1. 选择*配置*>*网络设置*>*服务器证书*。
2. 在对象存储API服务端点服务器证书部分中、单击*安装自定义证书*。
3. 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（`.crt`）。
   - 服务器证书专用密钥：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。

4. 单击 * 保存 * 。

   自定义服务器证书用于所有后续新的API客户端连接。

   选择一个选项卡以显示有关已上传的默认StorageGRID 服务器证书或CA签名证书的详细信息。

   上传新证书后、请留出最多一天的时间来清除任何相关证书到期警报(或旧警报)。

5. 刷新页面以确保 Web 浏览器已更新。

相关信息

"使用 S3"

"使用 Swift"

"配置S3 API端点域名"

还原**S3**和**Swift REST API**端点的默认服务器证书

您可以还原为对S3和Swift REST API端点使用默认服务器证书。

步骤

1. 选择*配置*>*网络设置*>*服务器证书*。
2. 在对象存储API服务端点服务器证书部分中、单击*使用默认证书*。
3. 单击确认对话框中的 * 确定 * 。

   还原对象存储API端点的默认服务器证书时、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。默认服务器证书将用于所有后续的新API客户端连接。

4. 刷新页面以确保 Web 浏览器已更新。

复制**StorageGRID** 系统的**CA**证书

StorageGRID 使用内部证书颁发机构(CA)来保护内部流量的安全。如果您上传自己的证书，则此证书不会更改。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

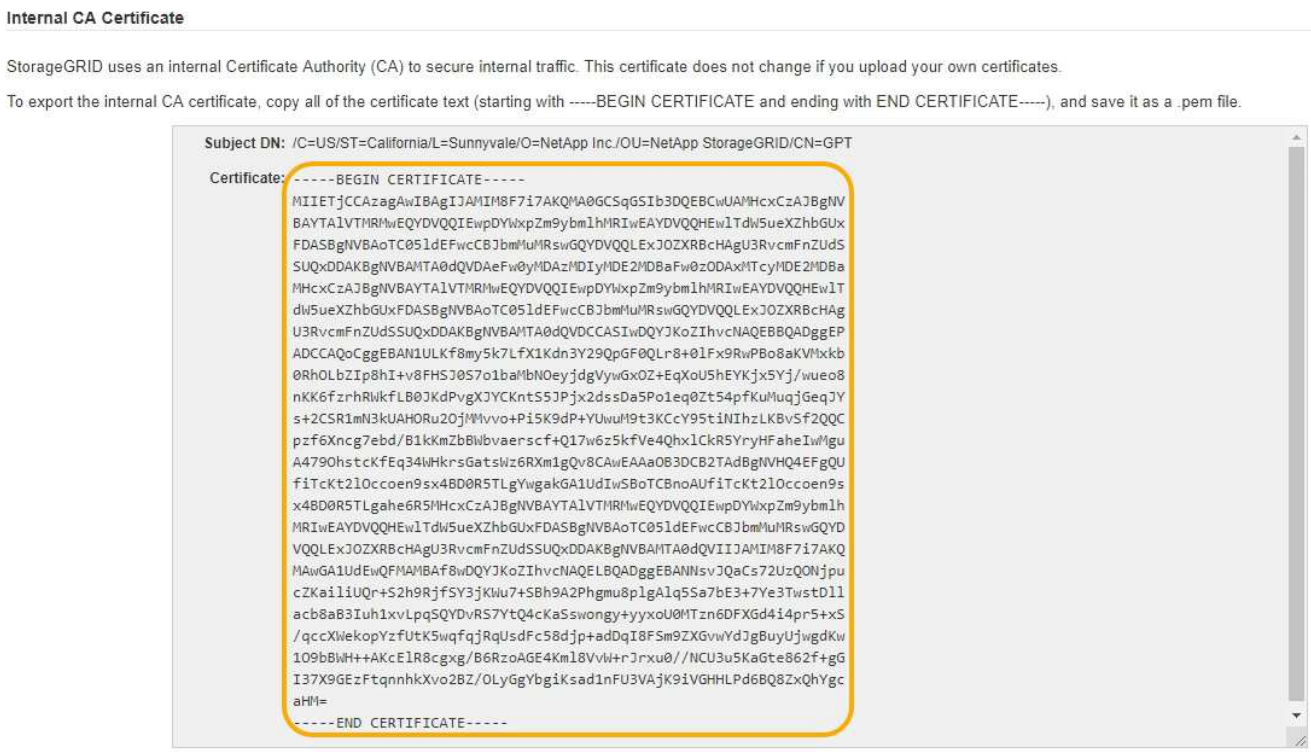
关于此任务

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*>*网络设置*>*服务器证书*。
2. 在*内部CA证书*部分中、选择所有证书文本。

   您必须包括 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 您选择的内容。



3. 右键单击选定文本、然后选择*复制*。
4. 将复制的证书粘贴到文本编辑器中。
5. 使用扩展名保存文件 `.pem`。

   例如： `storagegrid_certificate.pem`

为**FabricPool** 配置**StorageGRID** 证书

对于执行严格主机名验证且不支持禁用严格主机名验证的 S3 客户端，例如使用 FabricPool 的 ONTAP 客户端，您可以在配置负载平衡器端点时生成或上传服务器证书。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

关于此任务

创建负载平衡器端点时、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、请参见有关为FabricPool配置StorageGRID 的说明。

网关节点上的单独连接负载平衡器（ CLB ）服务已弃用，不再建议用于 FabricPool 。

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。

相关信息

"为 FabricPool 配置 StorageGRID"

为管理接口生成自签名服务器证书

您可以使用脚本为需要严格主机名验证的管理API客户端生成自签名服务器证书。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `Passwords.txt` 文件

关于此任务

在生产环境中、您应使用由已知证书颁发机构(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。

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API客户端与StorageGRID 同步到同一时间源；否则、客户端可能会拒绝此证书。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

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*配置服务器证书管理接口服务器证书*。
7. 将管理API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。

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。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

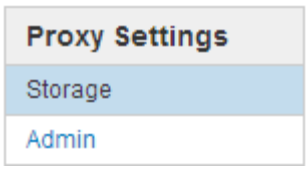
关于此任务

您可以为单个存储代理配置设置。

步骤

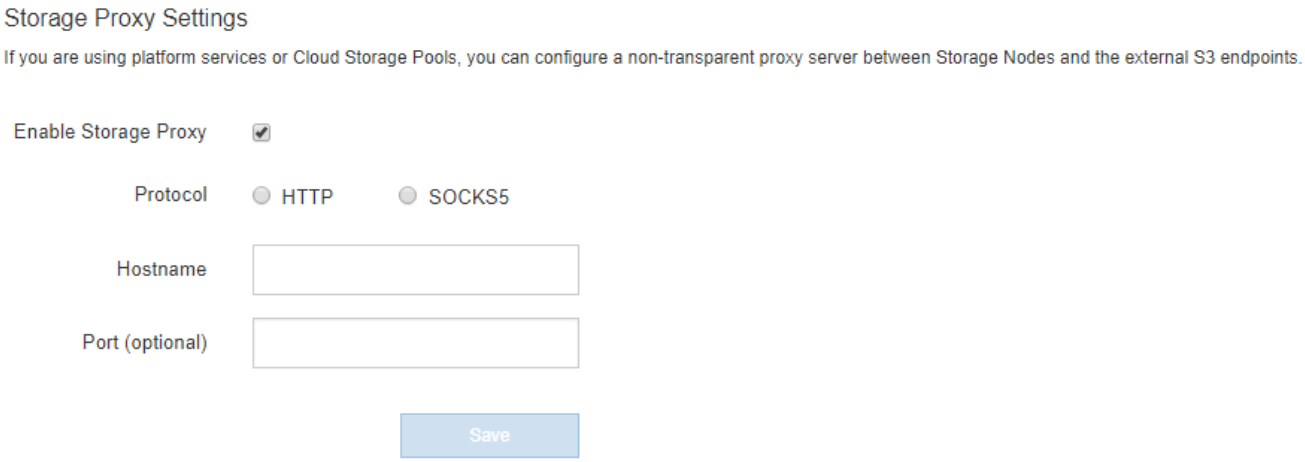
1. 选择*配置网络设置代理设置。

   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. 单击 * 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、请取消选中*启用存储代理*复选框、然后单击*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、则可以在管理节点和技术支持(AutoSupport)之间配置非透明代理服务器。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须使用支持的浏览器登录到网格管理器。

关于此任务

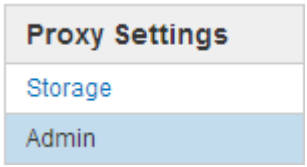
您可以为单个管理员代理配置设置。

步骤

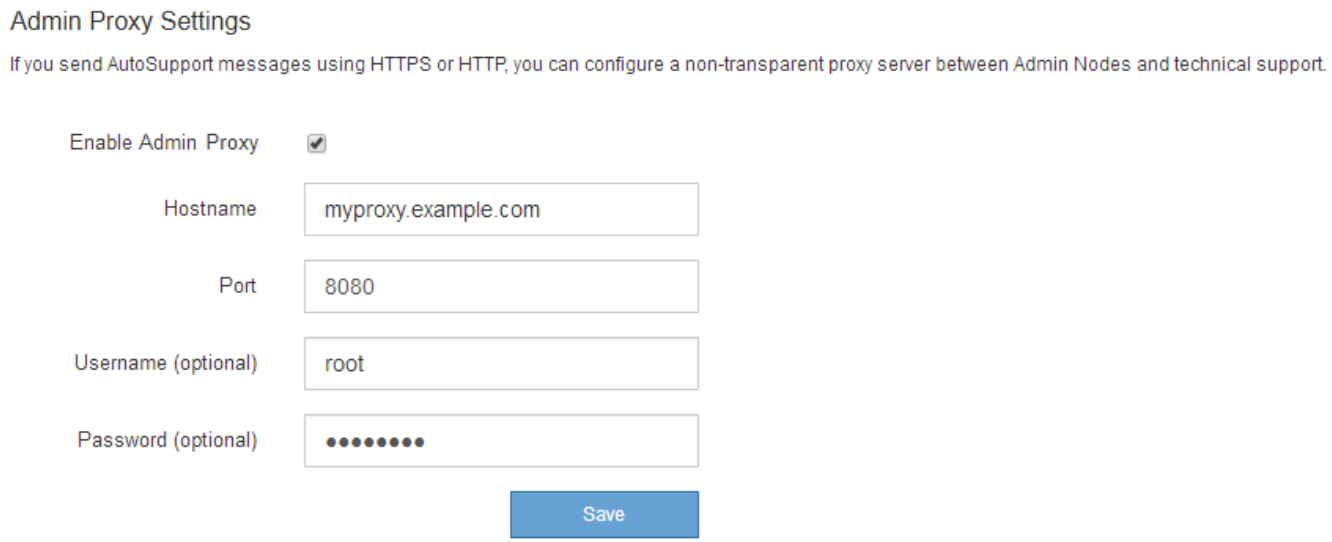
1. 选择*配置网络设置代理设置。

   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. 单击 * 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、请取消选中*启用管理代理*复选框、然后单击*保存*。

相关信息

"指定AutoSupport 消息的协议"

管理流量分类策略

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。

匹配规则和可选限制

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
- Tenants
- 子网（包含客户端的 IPv4 子网）
- 端点（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。

您也可以根据以下参数为策略设置限制：

- 中的聚合带宽
- 聚合带宽不足
- 并发读取请求
- 并发写入请求
- 每个请求的带宽
- 每个请求的带宽不足
- 读取请求速率
- 写入请求速率

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。

流量限制

创建流量分类策略后、流量将根据您设置的规则和限制类型进行限制。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。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。

将流量分类策略与**SLA**结合使用

您可以将流量分类策略与容量限制和数据保护结合使用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。

每个负载平衡器都会实施流量分类限制。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。

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	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

如果要按分段，租户， IP 子网或负载平衡器端点监控网络流量，并可选择限制此流量，则可以创建流量分类策略。您也可以根据带宽，并发请求数或请求率为策略设置限制。

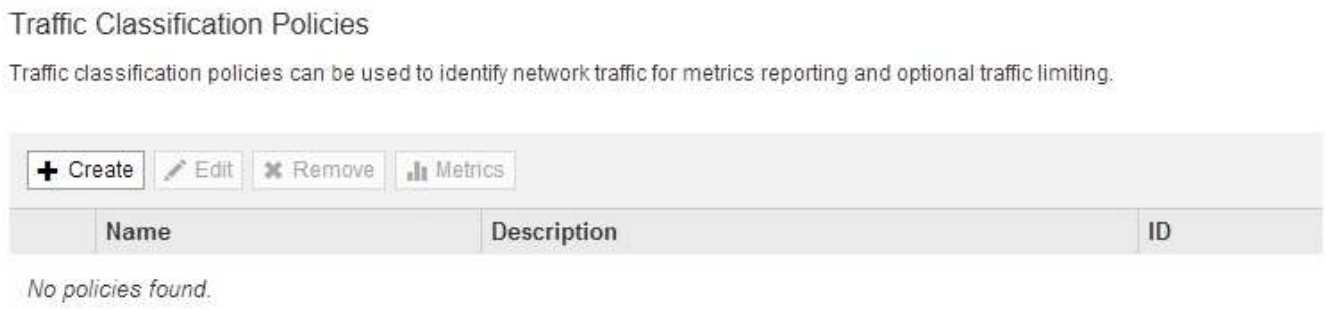
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。
- 您必须已创建要匹配的任何负载平衡器端点。
- 您必须已创建要匹配的任何租户。

步骤

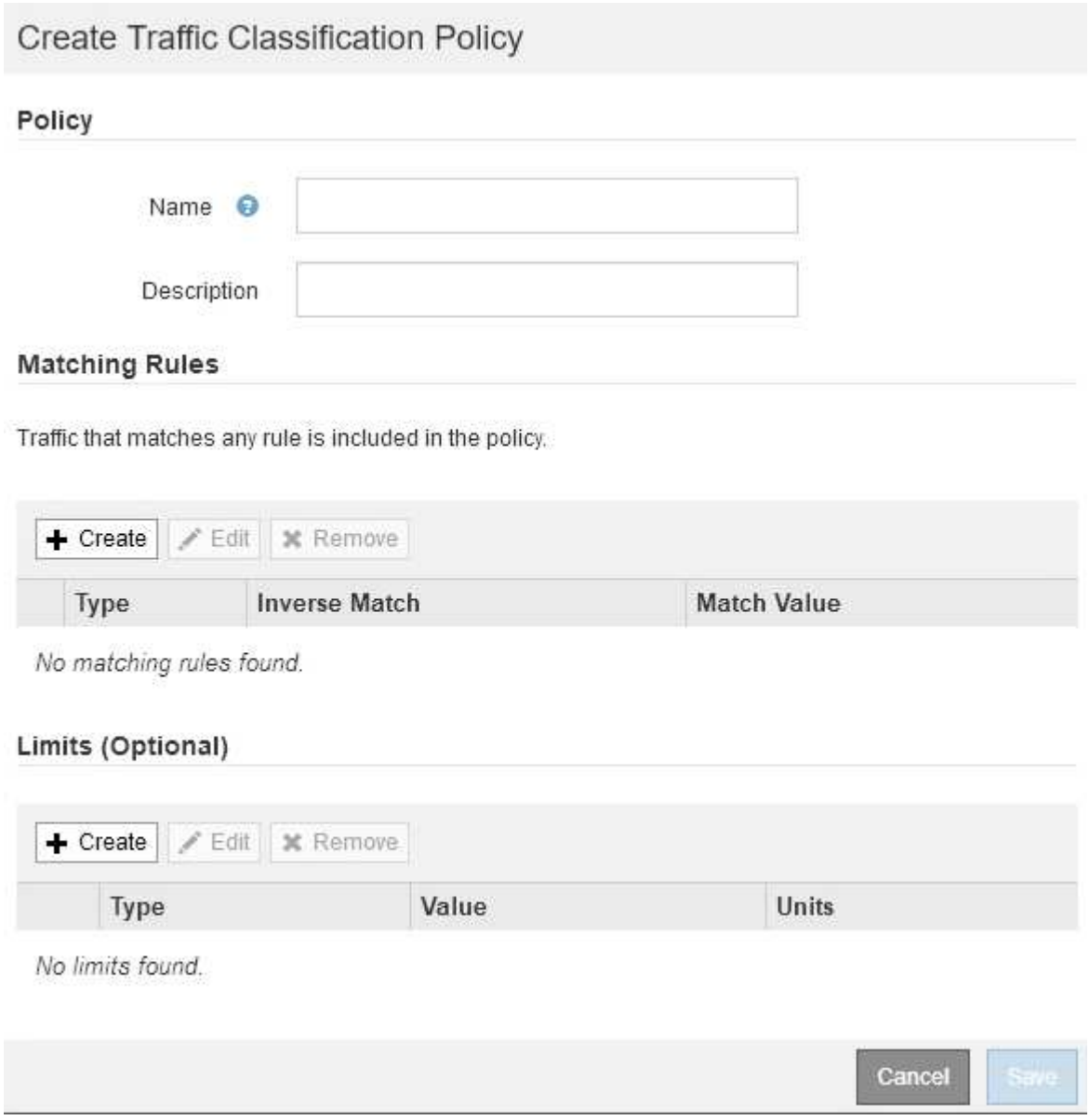
1. 选择*配置*>*网络设置*>*流量分类*。

   此时将显示 " 流量分类策略 " 页面。



2. 单击 * 创建 * 。

   此时将显示创建流量分类策略对话框。



3. 在 * 名称 * 字段中，输入策略的名称。

   输入描述性名称，以便识别策略。

4. 也可以在 * 问题描述 * 字段中为策略添加问题描述 。

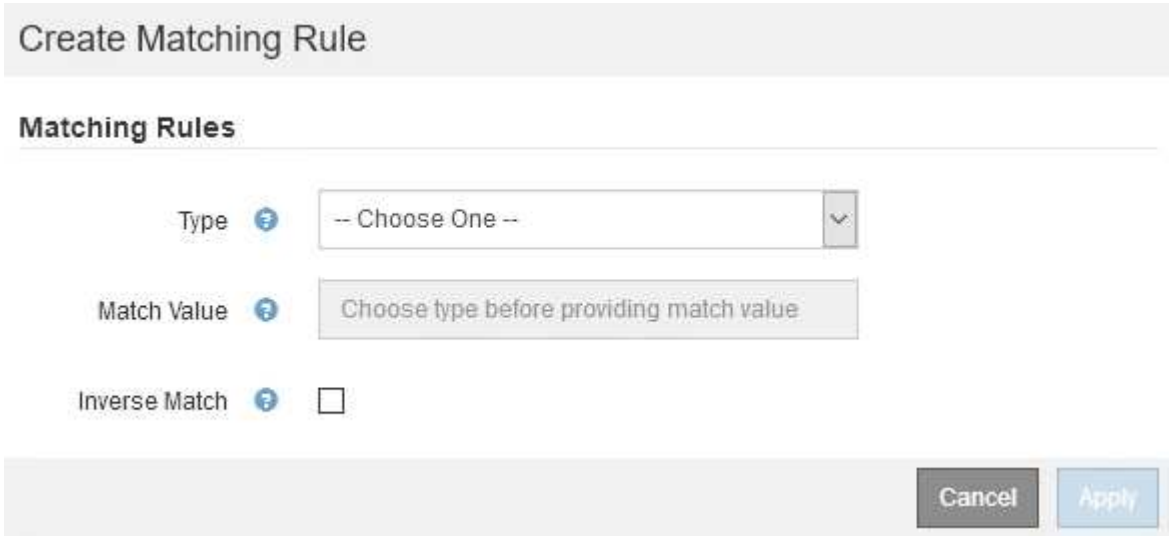
   例如，描述此流量分类策略适用场景 及其限制。

5. 为策略创建一个或多个匹配规则。

   匹配规则控制哪些实体将受此流量分类策略的影响。例如，如果要将此策略应用于特定租户的网络流量，请选择租户。或者，如果要将此策略应用于特定负载平衡器端点上的网络流量，请选择 Endpoint 。

   a. 单击*匹配规则*部分中的*创建*。

      此时将显示创建匹配规则对话框。



   b. 从 * 类型 * 下拉列表中，选择要包含在匹配规则中的实体类型。

   c. 在 * 匹配值 * 字段中，根据您选择的实体类型输入匹配值。

      - 存储分段：输入存储分段名称。
      - Bucket Rex ： 输入用于匹配一组存储分段名称的正则表达式。

        正则表达式已取消锁定。使用 ｛ caret ｝ 定位点在存储分段名称开头匹配，并使用 $ 定位点在存储分段名称末尾匹配。

      - CIDR ： 以 CIDR 表示法输入与所需子网匹配的 IPv4 子网。
      - Endpoint ： 从现有端点列表中选择一个端点。这些是您在负载平衡器端点页面上定义的负载平衡器端点。
      - 租户：从现有租户列表中选择一个租户。租户匹配取决于所访问的存储分段的所有权。对存储分段的匿名访问与拥有存储分段的租户匹配。

   d. 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 _except _ 流量，请选中 * 反向 * 复选框。否则，请取消选中此复选框。

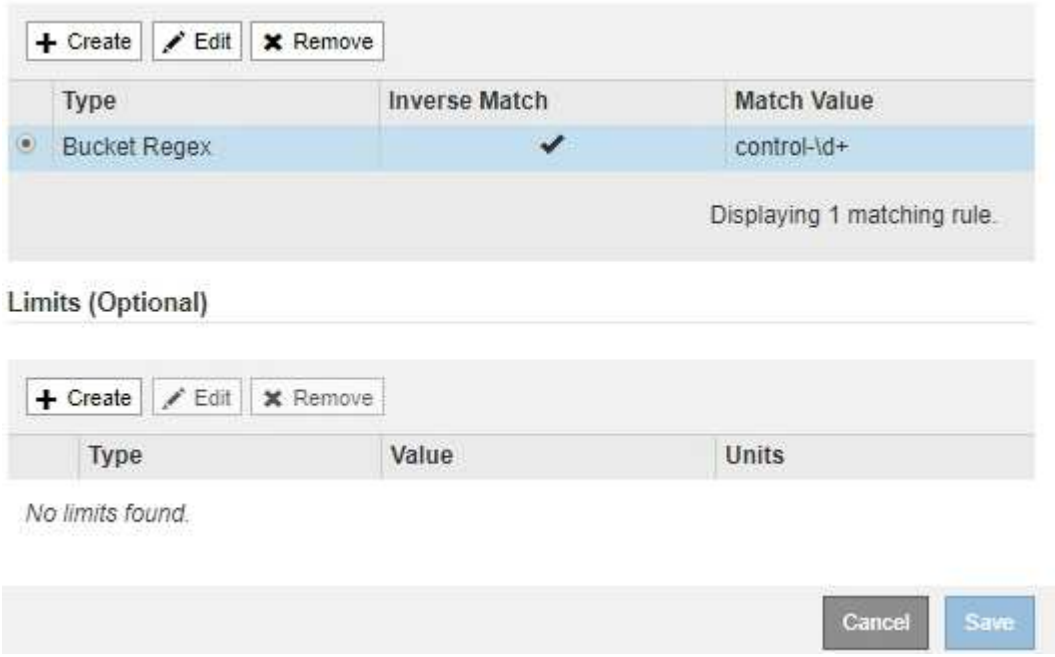
      例如，如果要将此策略应用于除一个负载平衡器端点之外的所有其他端点，请指定要排除的负载平衡器

端点，然后选择 * 反向 * 。

> 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。

e. 单击 * 应用 * 。

此时将创建此规则，并将其列在匹配规则表中。



a. 对要为策略创建的每个规则重复上述步骤。

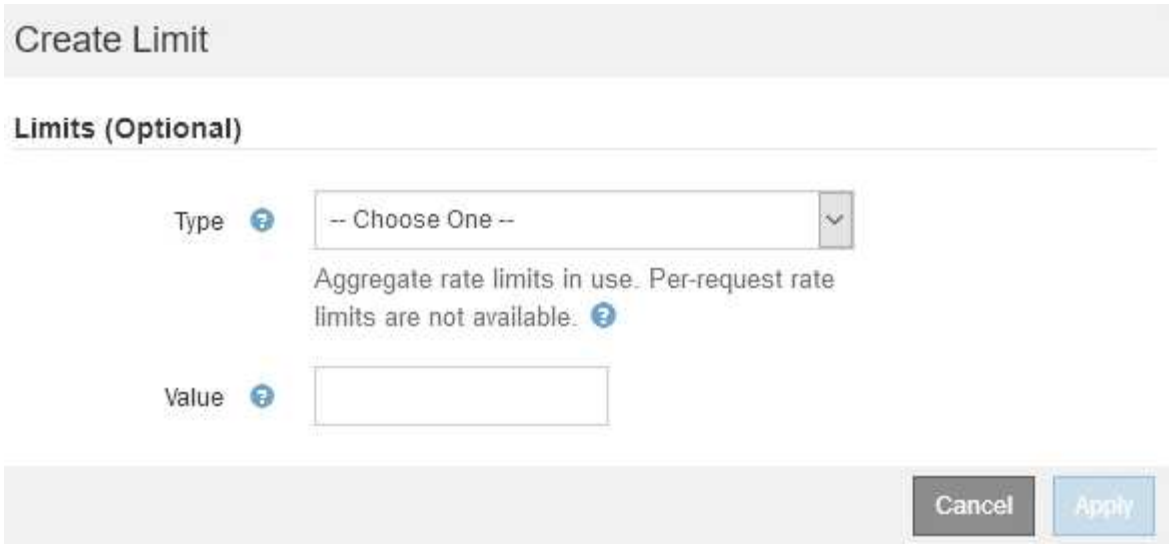
> 与任何规则匹配的流量由策略处理。

6. 也可以为策略创建限制。

> 即使不创建限制， StorageGRID 也会收集指标，以便监控与策略匹配的网络流量。

a. 单击*限制*部分中的*创建*。

此时将显示创建限制对话框。



b. 从 * 类型 * 下拉列表中，选择要应用于策略的限制类型。

在以下列表中， * 输入 * 是指从 S3 或 Swift 客户端到 StorageGRID 负载平衡器的流量， * 输出 * 是指从负载平衡器到 S3 或 Swift 客户端的流量。

- 中的聚合带宽
- 聚合带宽不足
- 并发读取请求
- 并发写入请求
- 每个请求的带宽
- 每个请求的带宽不足
- 读取请求速率
- 写入请求速率

> 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 "`最佳` " 匹配的带宽限制：

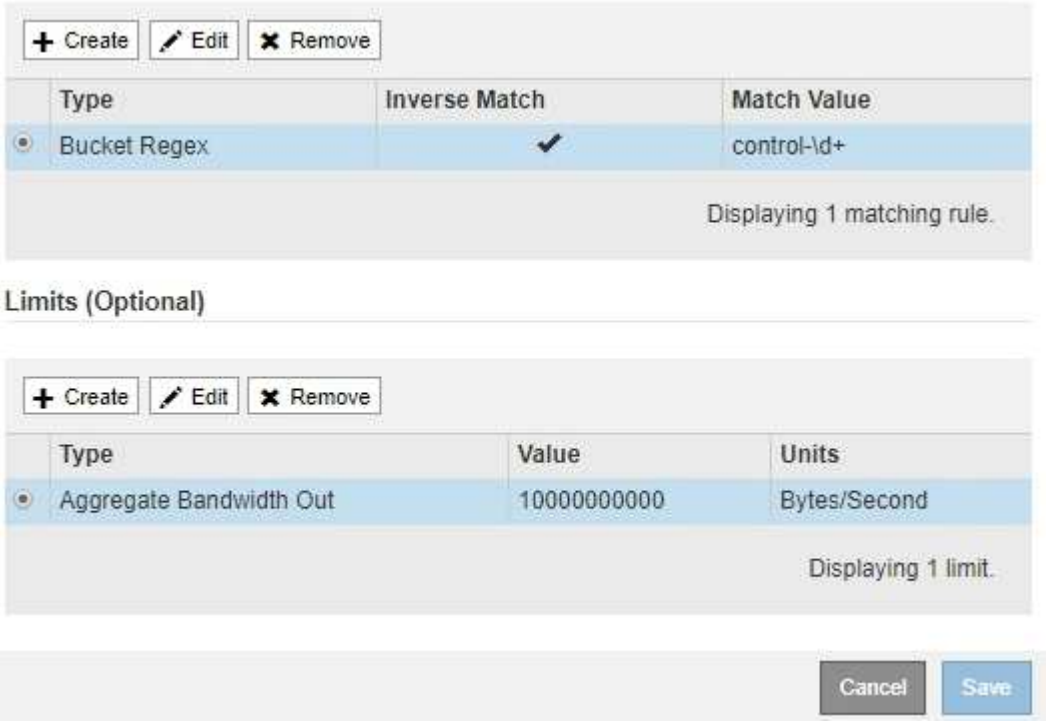
- 确切的 IP 地址（ /32 掩码）
- 确切的存储分段名称
- 分段正则表达式
- 租户
- 端点
- 非精确的 CIDR 匹配项（非 /32 ）
- 反向匹配

c. 在 * 值 * 字段中，输入所选限制类型的数值。

选择限制时，系统将显示预期单位。

d. 单击 * 应用 * 。

此时将创建此限制，并将其列在限制表中。



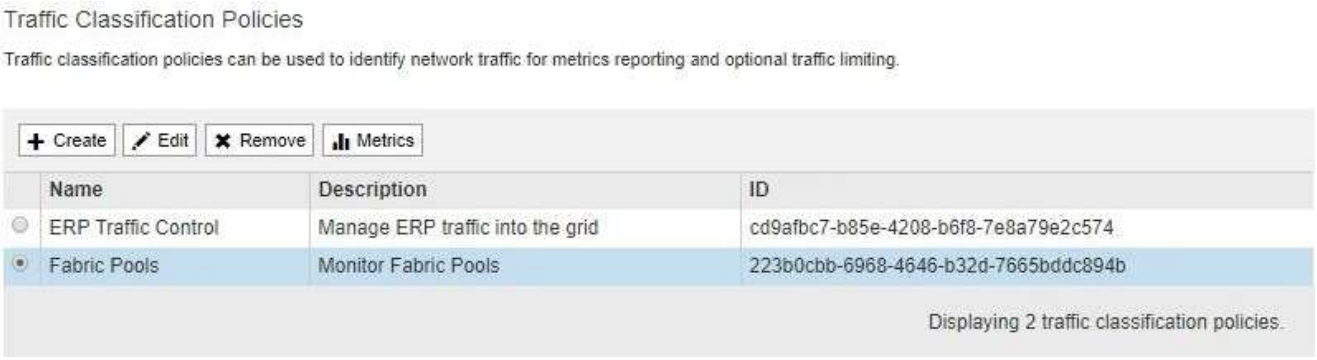
e. 对要添加到策略中的每个限制重复上述步骤。

例如，如果要为 SLA 层创建 40 Gbps 带宽限制，请创建 " 聚合带宽限制 " 和 " 聚合带宽超限 " ，并将每个限制设置为 40 Gbps 。

要将每秒兆字节数转换为每秒千兆位数，请乘以 8 。例如， 125 MB/ 秒相当于 1 ， 000 Mbps 或 1 Gbps 。

7. 创建完规则和限制后、单击*保存*。

此策略将保存并列出在 " 流量分类策略 " 表中。



现在， S3 和 Swift 客户端流量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。

相关信息

"管理负载平衡"

"查看网络流量指标"

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。

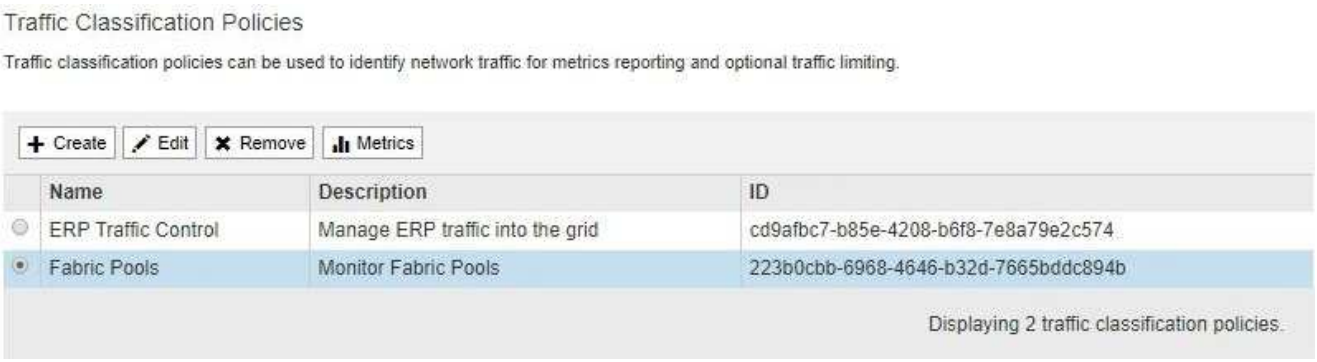
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

步骤

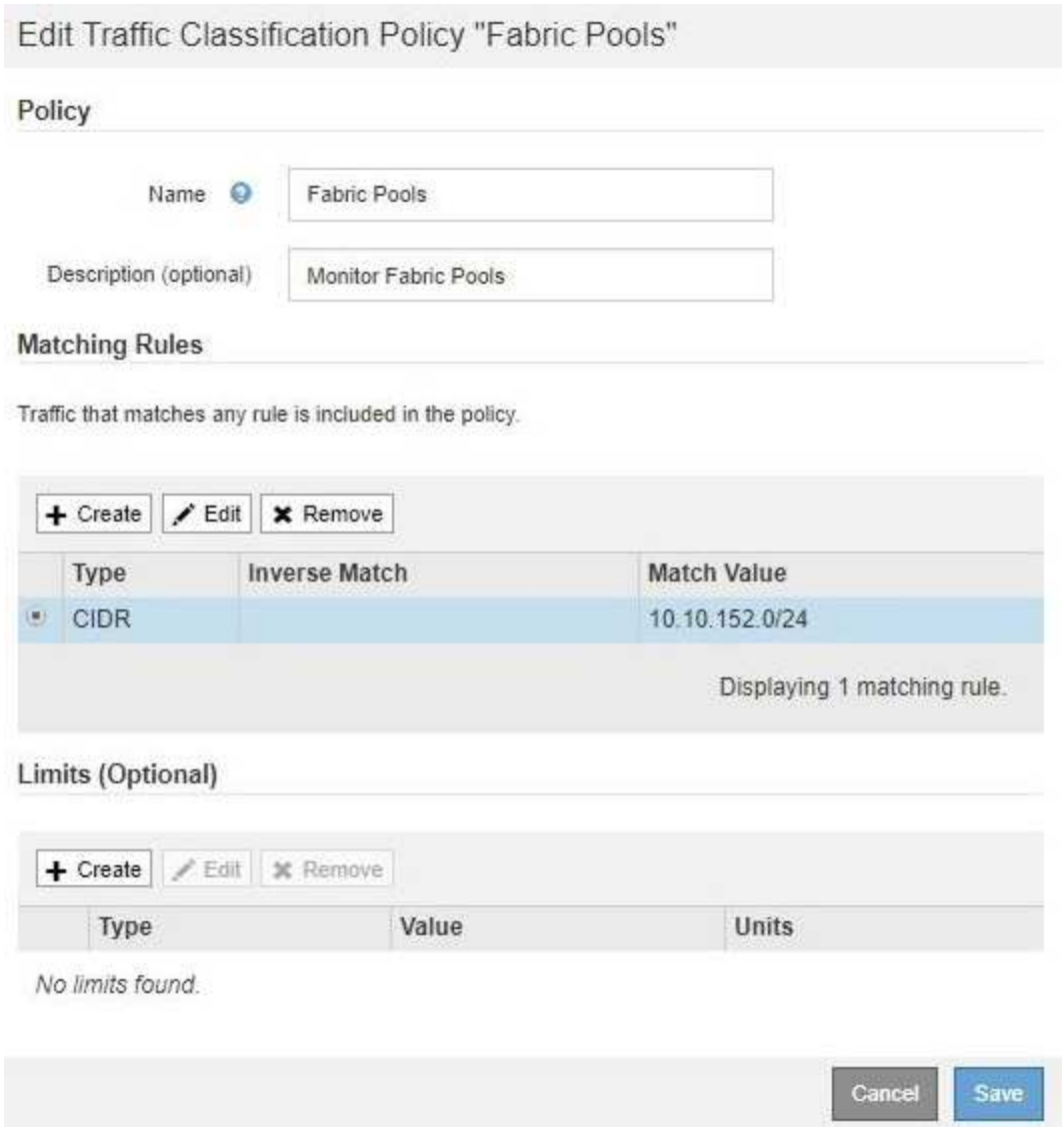
1. 选择*配置*>*网络设置*>*流量分类*。

   此时将显示 " 流量分类策略 " 页面，并在表中列出现有策略。



2. 选择要编辑的策略左侧的单选按钮。
3. 单击 * 编辑 * 。

   此时将显示编辑流量分类策略对话框。



4. 根据需要创建，编辑或删除匹配的规则和限制。
   a. 要创建匹配的规则或限制、请单击*创建*、然后按照说明创建规则或创建限制。
   b. 要编辑匹配的规则或限制、请选择规则或限制的单选按钮、单击*匹配规则*部分或*限制*部分中的*编辑*、然后按照说明创建规则或创建限制。
   c. 要删除匹配的规则或限制、请选择该规则或限制的单选按钮、然后单击*删除*。然后、单击*确定*以确认要删除此规则或限制。
5. 创建或编辑规则或限制后、单击*应用*。
6. 编辑完策略后、单击*保存*。

   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

如果您不再需要流量分类策略，可以将其删除。

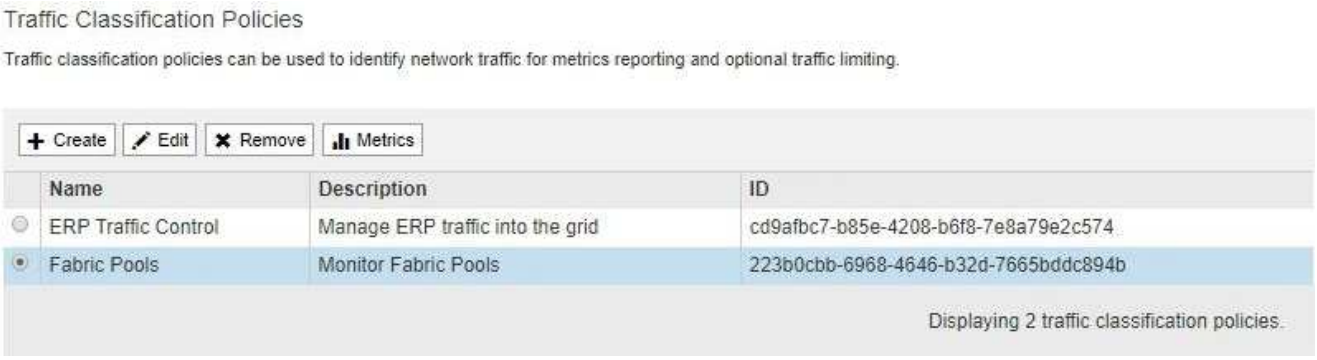
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

步骤

1. 选择*配置*>*网络设置*>*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. 选择要删除的策略左侧的单选按钮。
3. 单击 * 删除 * 。

   此时将显示警告对话框。

4. 单击*确定*确认要删除此策略。

   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 " 页面上的图形来监控网络流量。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 root 访问权限。

关于此任务

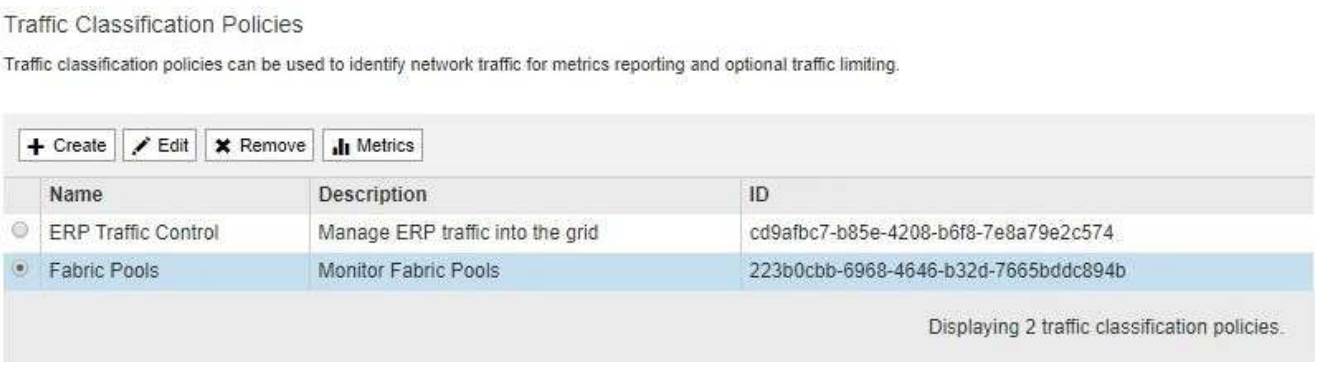
对于任何现有流量分类策略，您可以查看负载平衡器服务的指标，以确定该策略是否成功限制网络中的流量。图形中的数据可以帮助您确定是否需要调整策略。

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*>*网络设置*>*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. 选择要查看指标的策略左侧的单选按钮。
3. 单击*指标*。

   此时将打开一个新浏览器窗口，并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。

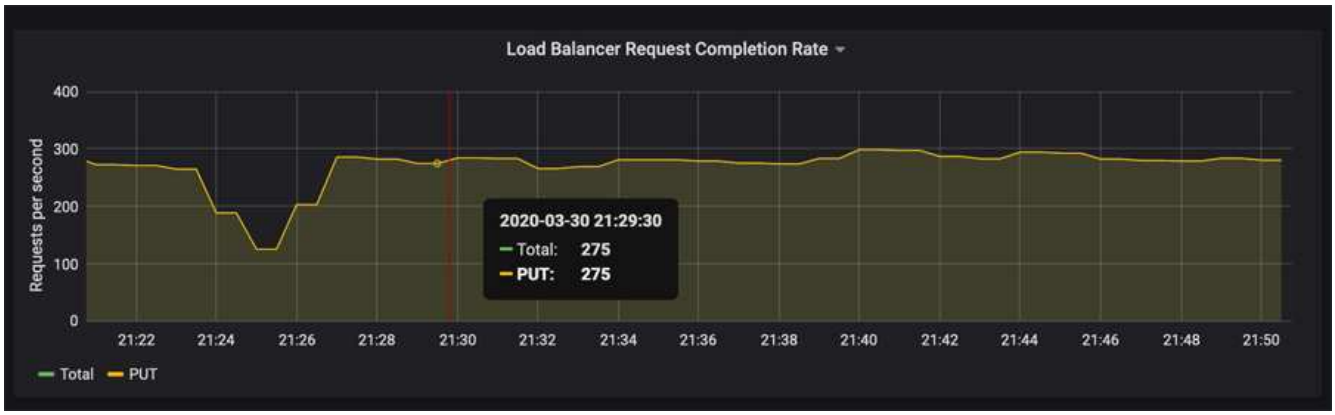
   您可以使用 * 策略 * 下拉列表选择其他要查看的策略。

   网页上包含以下图形。

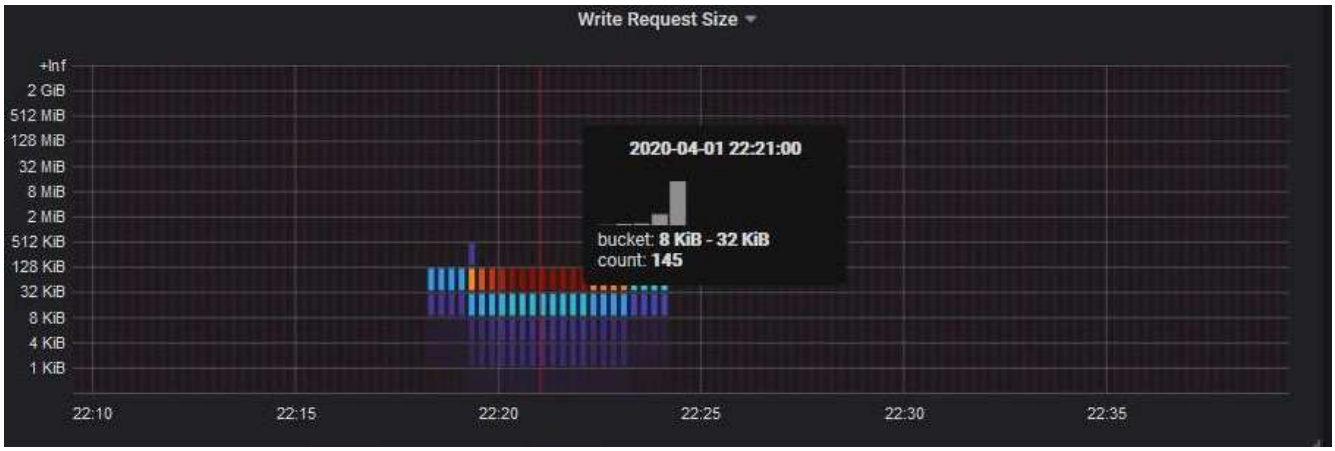
   - 负载平衡器请求流量：此图提供负载平衡器端点与发出请求的客户端之间传输的数据吞吐量的 3 分钟移动平均值，以每秒位数为单位。
   - 负载平衡器请求完成率：此图按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分，提供每秒已完成请求数的 3 分钟移动平均值。验证新请求的标头后，此值将更新。

- 错误响应率：此图提供了每秒返回给客户端的错误响应数的 3 分钟移动平均值，并按错误响应代码进行细分。
- 平均请求持续时间（非错误）：此图提供了按请求类型（ GET ， PUT ， HEAD 和 DELETE ）细分的 3 分钟移动平均请求持续时间。每个请求持续时间从负载平衡器服务解析请求标头时开始，到将完整的响应正文返回给客户端时结束。
- 按对象大小划分的写入请求速率：此热图根据对象大小提供 3 分钟的写入请求完成速率移动平均值。在这种情况下，写入请求仅指 PUT 请求。
- 按对象大小划分的读取请求速率：此热图提供了根据对象大小完成读取请求的 3 分钟移动平均值。在这种情况下，读取请求仅指获取请求。热图中的颜色表示各个图形中对象大小的相对频率。较冷的颜色（例如紫色和蓝色）表示相对速率较低，较热的颜色（例如橙色和红色）表示相对速率较高。

4. 将光标悬停在折线图上可查看该图特定部分的值弹出窗口。



5. 将光标悬停在热图上可看到一个弹出窗口，其中显示样本的日期和时间，聚合到计数中的对象大小以及该时间段内的每秒请求数。



6. 使用左上角的 * 策略 * 下拉列表选择其他策略。

   此时将显示选定策略的图形。

7. 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. 在页面的 * Grafan* 部分中，选择 * 流量分类策略 * 。
   c. 从页面左上角的下拉列表中选择策略。

流量分类策略通过其 ID 进行标识。策略 ID 会列在 " 流量分类策略 " 页面上。

8. 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。

相关信息

"监控和放大；故障排除"

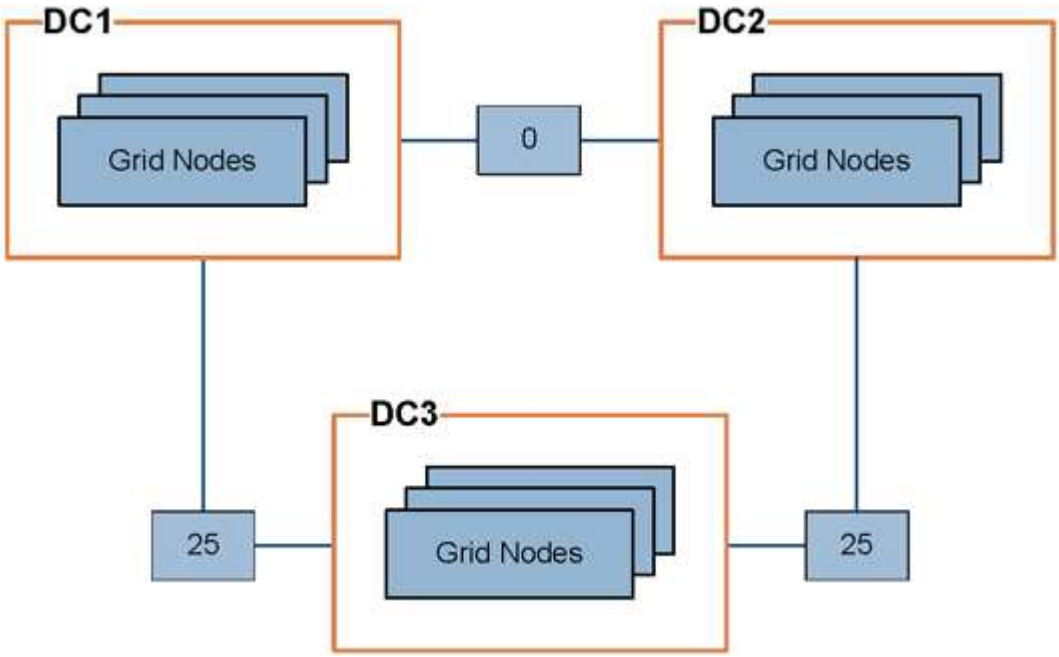
链路成本是多少

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。

- 链接成本用于确定用于实现对象检索的对象副本的优先级。
- 网格管理 API 和租户管理 API 使用链路成本来确定要使用的内部 StorageGRID 服务。
- 链路成本由网关节点上的CLB服务用于指导客户端连接。

> CLB 服务已弃用。

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：



- 网关节点上的 CLB 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任何数据中心站点，链路成本为 0 。

  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 上的客户端应用程序检索存储在 DC1 和 DC3 上的对象，则会从 DC1 检索该对象，因为从 DC1 到 D2 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。

相关信息

"负载平衡的工作原理— CLB 服务"

更新链路成本

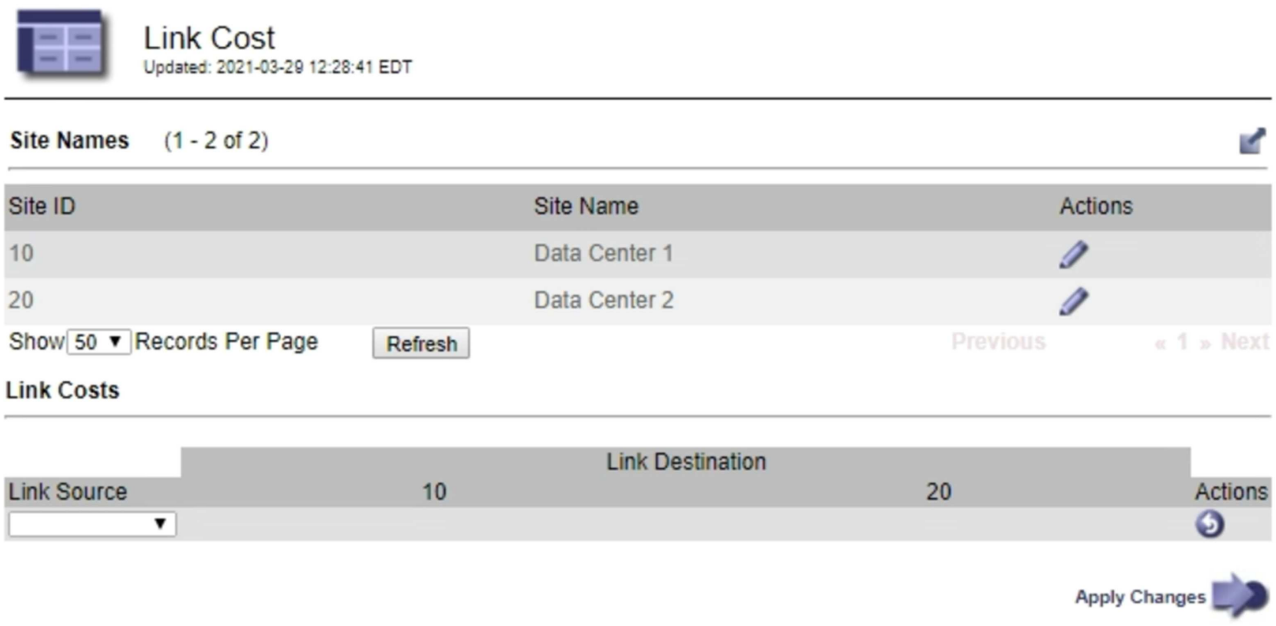
您可以更新数据中心站点之间的链路成本，以反映站点之间的延迟。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有网格拓扑页面配置权限。

步骤

1. 选择*配置*>*网络设置*>*链路成本*。



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，则无法更改链路成本。

   要取消更改、请单击 * 还原 * 。

3. 单击 * 应用更改 * 。

正在配置 AutoSupport

通过 AutoSupport 功能， StorageGRID 系统可以向技术支持发送运行状况和状态消息。使用 AutoSupport 可以显著加快问题的确定和解决速度。技术支持还可以监控系统的存储需求，并帮助您确定是否需要添加新节点或站点。您也可以将 AutoSupport 消息配置为发送到另一个目标。

AutoSupport 消息中包含的信息

AutoSupport 消息包含如下信息：

- StorageGRID 软件版本
- 操作系统版本
- 系统级别和位置级别属性信息
- 近期警报和警报（旧系统）
- 所有网格任务的当前状态，包括历史数据
- *节点*网格节点_*事件*页面上列出的事件信息
- 管理节点数据库使用情况
- 丢失或缺失对象的数量
- 网格配置设置
- NMS 实体
- 活动 ILM 策略
- 已配置网格规范文件
- 诊断指标

您可以在首次安装 StorageGRID 时启用 AutoSupport 功能和各个 AutoSupport 选项，也可以稍后启用它们。如果未启用AutoSupport 、则网格管理器信息板上会显示一条消息。此消息包含指向 AutoSupport 配置页面的链接。

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

使用Active IQ

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

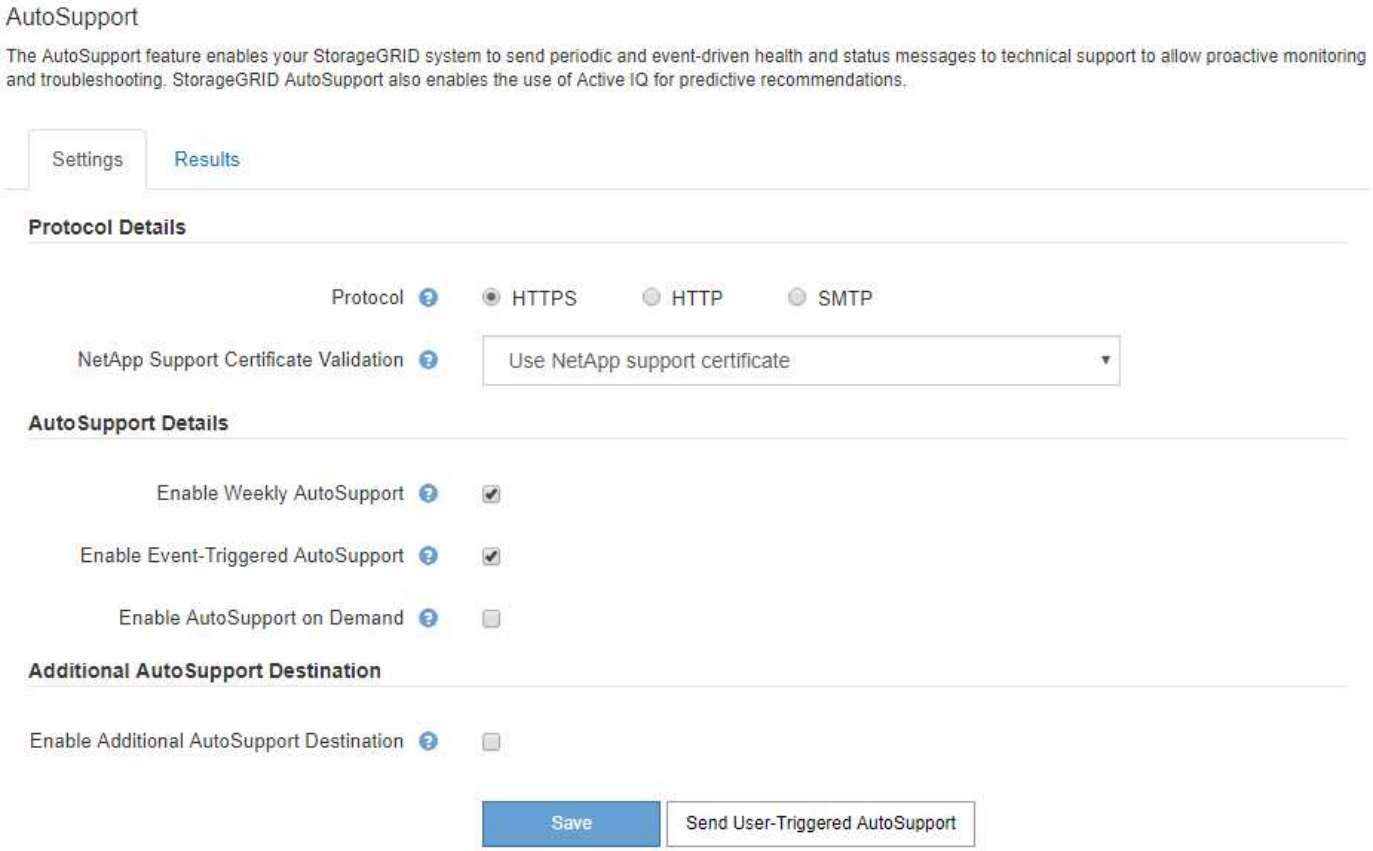
性。

如果要使用 NetApp 支持站点上的 Active IQ 信息板和功能，则必须启用 AutoSupport。

"Active IQ Digital Advisor 文档"

访问AutoSupport 设置

您可以使用网格管理器配置AutoSupport (支持>*工具*>* AutoSupport)。 AutoSupport * 页面有两个选项卡： * 设置 * 和 * 结果 * 。



用于发送 AutoSupport 消息的协议

您可以选择以下三种协议之一来发送 AutoSupport 消息：

- HTTPS
- HTTP
- SMTP

如果使用 HTTPS 或 HTTP 发送 AutoSupport 消息，则可以在管理节点和技术支持之间配置非透明代理服务器。

如果使用 SMTP 作为 AutoSupport 消息的协议，则必须配置 SMTP 邮件服务器。

AutoSupport 选项

您可以使用以下选项的任意组合向技术支持发送 AutoSupport 消息：

- * 每周 * ： 每周自动发送一次 AutoSupport 消息。默认设置： enabled 。
- * 事件触发 * ： 每小时或发生重大系统事件时自动发送 AutoSupport 消息。默认设置： enabled 。
- * 按需 * ： 允许技术支持请求您的 StorageGRID 系统自动发送 AutoSupport 消息，这在他们正在使用问题描述 （需要 HTTPS AutoSupport 传输协议）时非常有用。默认设置： disabled 。
- * 用户触发 * ： 随时手动发送 AutoSupport 消息。

相关信息

"NetApp 支持"

指定AutoSupport 消息的协议

您可以使用以下三种协议之一发送AutoSupport 消息。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。
- 如果要使用HTTPS或HTTP协议发送AutoSupport 消息、则必须已直接或使用代理服务器提供对主管理节点的出站Internet访问(不需要入站连接)。
- 如果要使用HTTPS或HTTP协议、并且要使用代理服务器、则必须已配置管理员代理服务器。
- 如果要使用SMTP作为AutoSupport 消息的协议、则必须已配置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）。

关于此任务

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。HTTPS 协议使用端口 443 。如果要启用 AutoSupport On Demand 功能，则必须使用 HTTPS 协议。
- * HTTP * ： 此协议不安全，除非在可信环境中使用，在该环境中，代理服务器在通过 Internet 发送数据时会转换为 HTTPS 。HTTP 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(支持*警报(旧版)旧版电子邮件设置)上配置SMTP邮件服务器。

> 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。

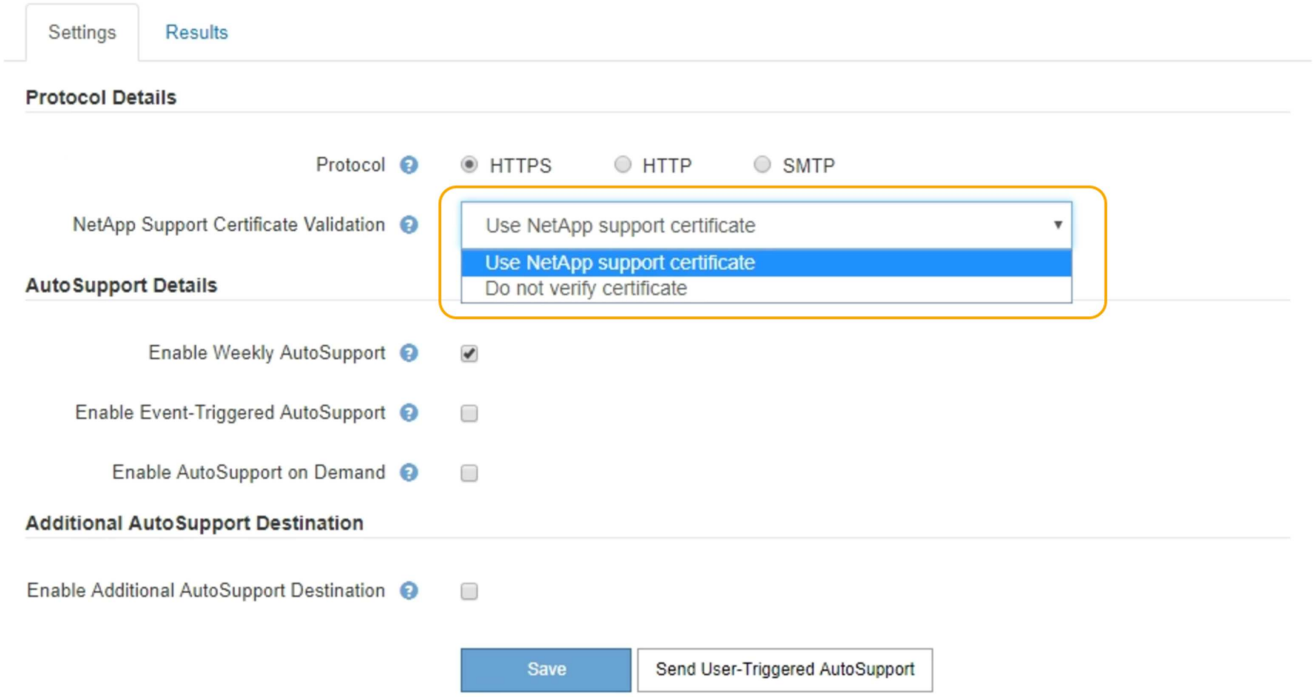
您设置的协议用于发送所有类型的 AutoSupport 消息。

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. 选择"* NetApp支持证书验证"*。
   - 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。
   - Do not verify certificate：仅当您有充分理由不使用证书验证时、例如证书出现临时问题时、才选择此选项。
4. 选择 * 保存 * 。

   所有每周消息，用户触发的消息和事件触发的消息均使用选定协议发送。

相关信息

"配置管理员代理设置"

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。启用AutoSupport on Demand后、技术支持可以请求发送AutoSupport 消息、而无需您的干预。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。
- 您必须已启用每周AutoSupport 消息。
- 您必须已将传输协议设置为HTTPS。

关于此任务

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。

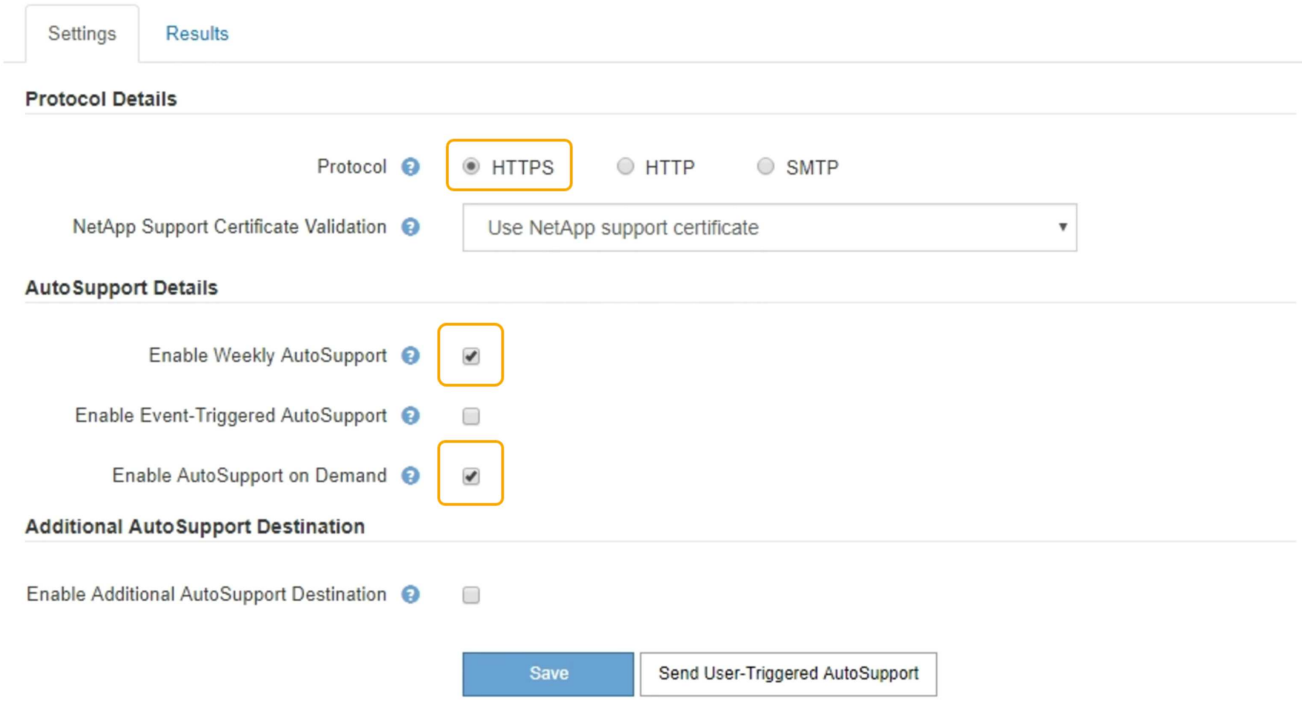
技术支持无法启用或禁用 AutoSupport On Demand 。

步骤

1. 选择*支持*>*工具*>* AutoSupport *。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

2. 在页面的*协议详细信息*部分中选择HTTPS单选按钮。



3. 选中 * 启用每周 AutoSupport * 复选框。
4. 选中 * 启用按需 AutoSupport * 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。

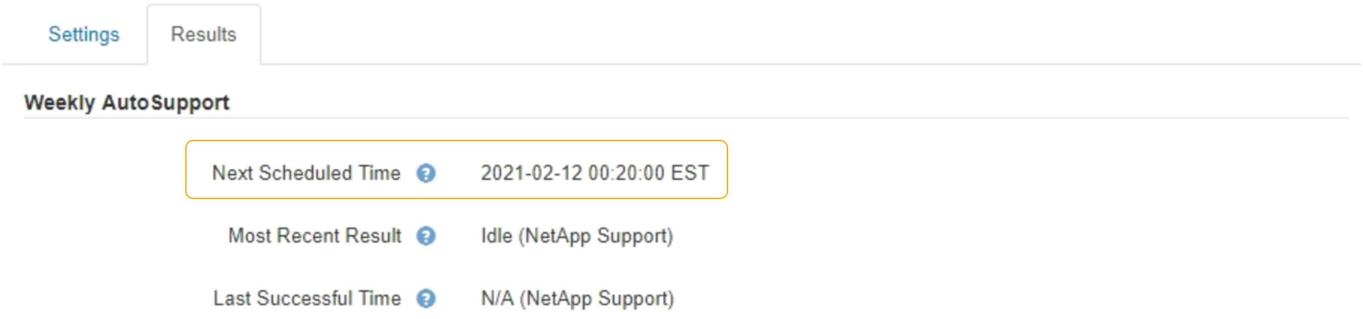
您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。

关于此任务

要确定每周AutoSupport 消息的发送时间、请参见*每周AutoSupport 下的*下一计划时间、其位于* AutoSupport

*>*结果*页面上。



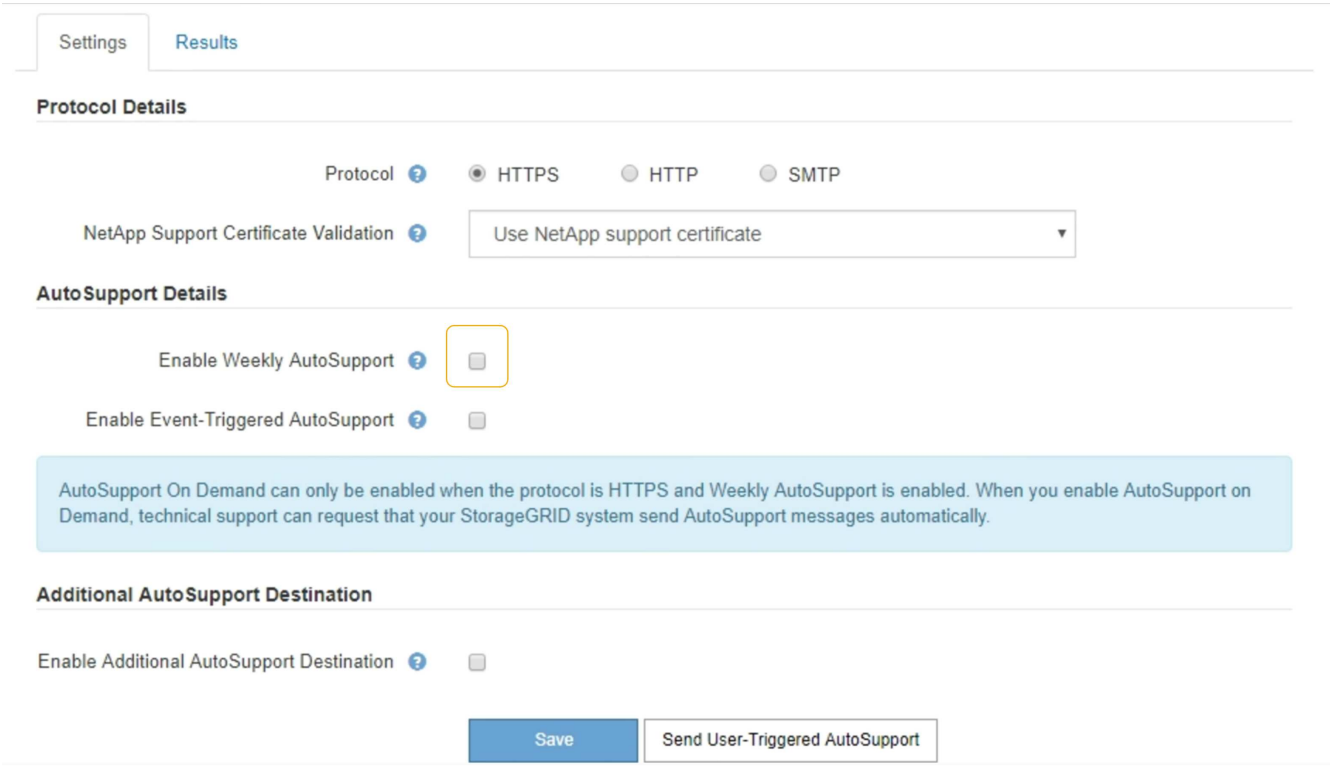
您可以随时禁止自动发送AutoSupport 消息。

步骤

1. 选择*支持*>*工具*>* AutoSupport *。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。

关于此任务

您可以随时禁用事件触发的 AutoSupport 消息。

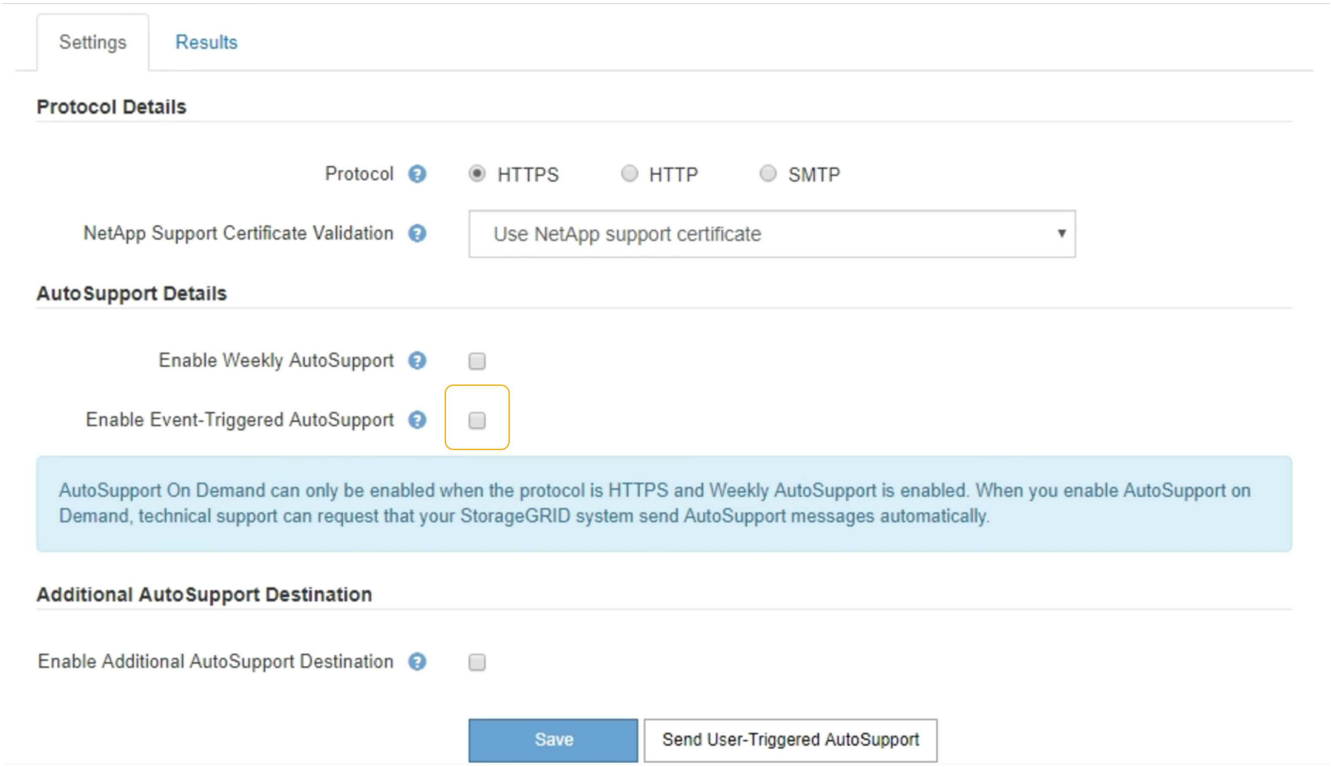
> 在系统范围内禁止电子邮件通知时，也会禁止显示事件触发的 AutoSupport 消息。(选择*配置系统设置显示选项*。然后，选择 * 通知禁止全部 * 。）

步骤

1. 选择*支持*>*工具*>* AutoSupport *。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

2. 清除*启用事件触发的AutoSupport *复选框。



3. 选择 * 保存 * 。

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。

步骤

1. 选择*支持*>*工具*>* AutoSupport *。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

2. 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。

添加其他**AutoSupport** 目标

启用 AutoSupport 后，系统会向 NetApp 支持部门发送运行状况和状态消息。您可以为所有 AutoSupport 消息指定一个其他目标。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有 " 根访问 " 或 " 其他网格配置 " 权限。

关于此任务

要验证或更改用于发送AutoSupport 消息的协议、请参见有关指定AutoSupport 协议的说明。

您不能使用 SMTP 协议将 AutoSupport 消息发送到其他目标。

"指定AutoSupport 消息的协议"

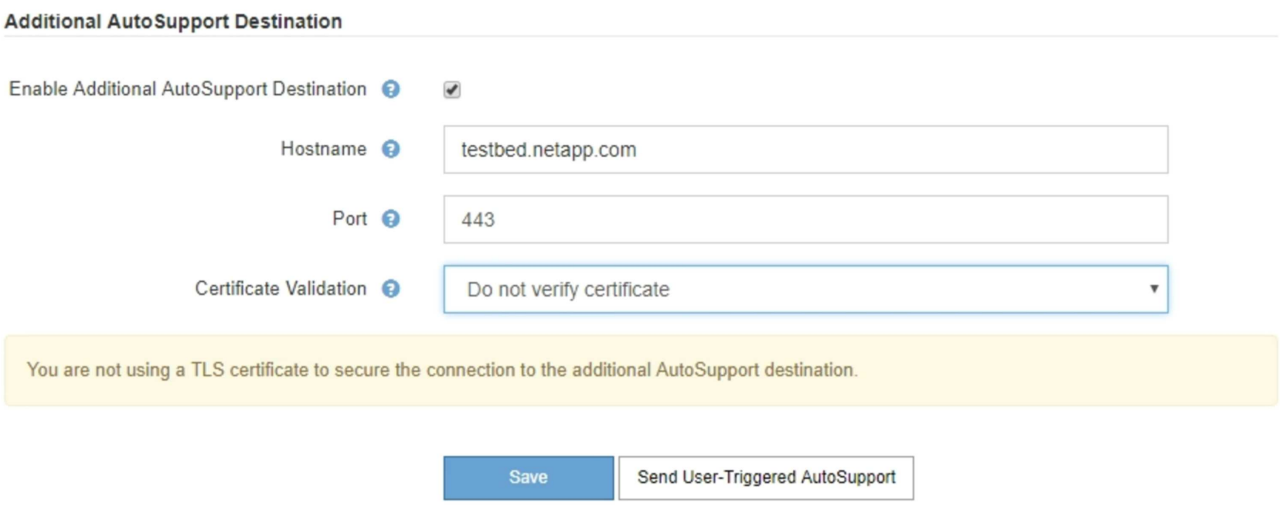
步骤

1. 选择*支持*>*工具*>* AutoSupport *。

   此时将显示 AutoSupport 页面，并选择了 * 设置 * 选项卡。

2. 选择 * 启用其他 AutoSupport 目标 * 。

   此时将显示其他 AutoSupport 目标字段。



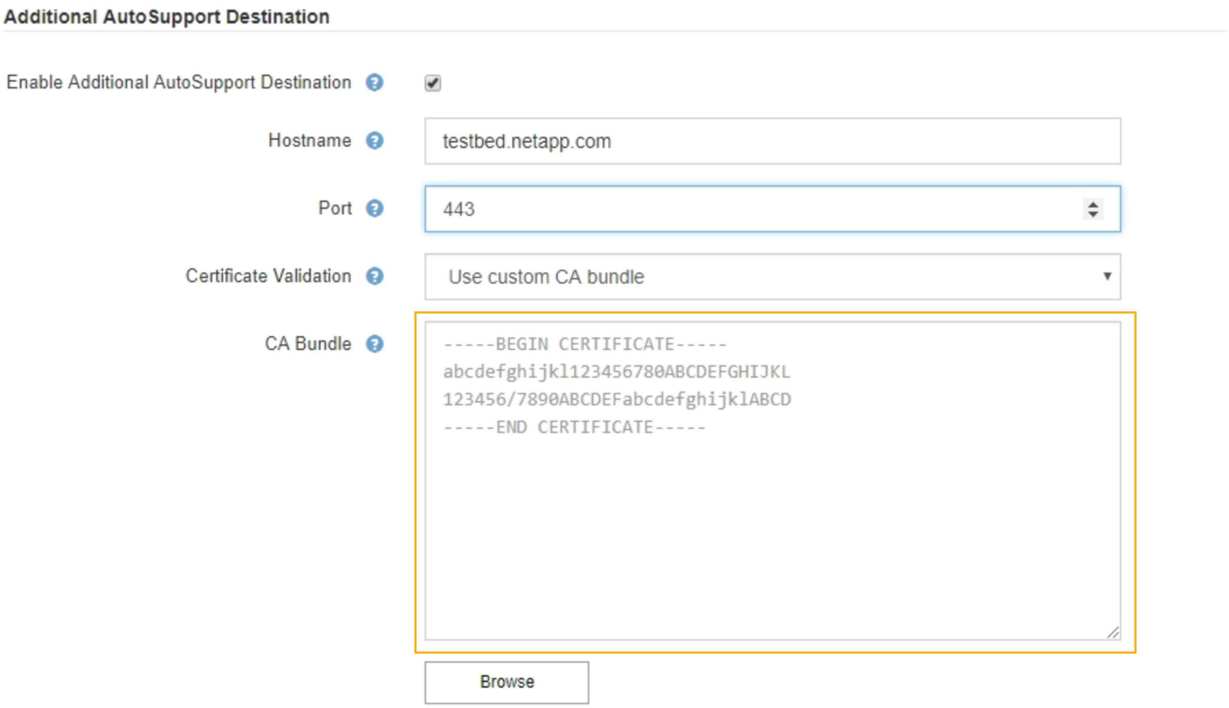
3. 输入其他 AutoSupport 目标服务器的服务器主机名或 IP 地址。

   您只能输入一个附加目标。

4. 输入用于连接到其他 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 ）。

5. 要发送包含证书验证的 AutoSupport 消息，请在 * 证书验证 * 下拉列表中选择 * 使用自定义 CA 捆绑包 * 。然后，执行以下操作之一：

   - 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 * CA bundle* 字段中，该字段按证书链顺序串联。您必须包括 `----BEGIN CERTIFICATE----` 和 `----END CERTIFICATE----` 您选择的内容。



   - 选择 * 浏览 * ，导航到包含证书的文件，然后选择 * 打开 * 上传文件。证书验证可确保 AutoSupport 消息的传输安全。

6. 要在不验证证书的情况下发送 AutoSupport 消息，请在 * 证书验证 * 下拉列表中选择 * 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。

   警告此时将显示一条消息： " 您未使用 TLS 证书来保护与其他 AutoSupport 目标的连接。 "

7. 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。

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的管理端口向技术支持发送E系列SANtricity System Manager AutoSupport 消息。

您需要的内容

- 您将使用受支持的Web浏览器登录到网格管理器。
- 您具有存储设备管理员权限或root访问权限。

> 要使用网格管理器访问 SANtricity 系统管理器，您必须具有 SANtricity 固件 8.70 或更高版本。

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。

在 SANtricity 系统管理发生原因 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 消息与可能已在网格管理器中配置的首选发件人和管理员代理设置相关。

如果要在网格管理器中配置管理代理服务器、请参见有关配置管理代理设置的说明。

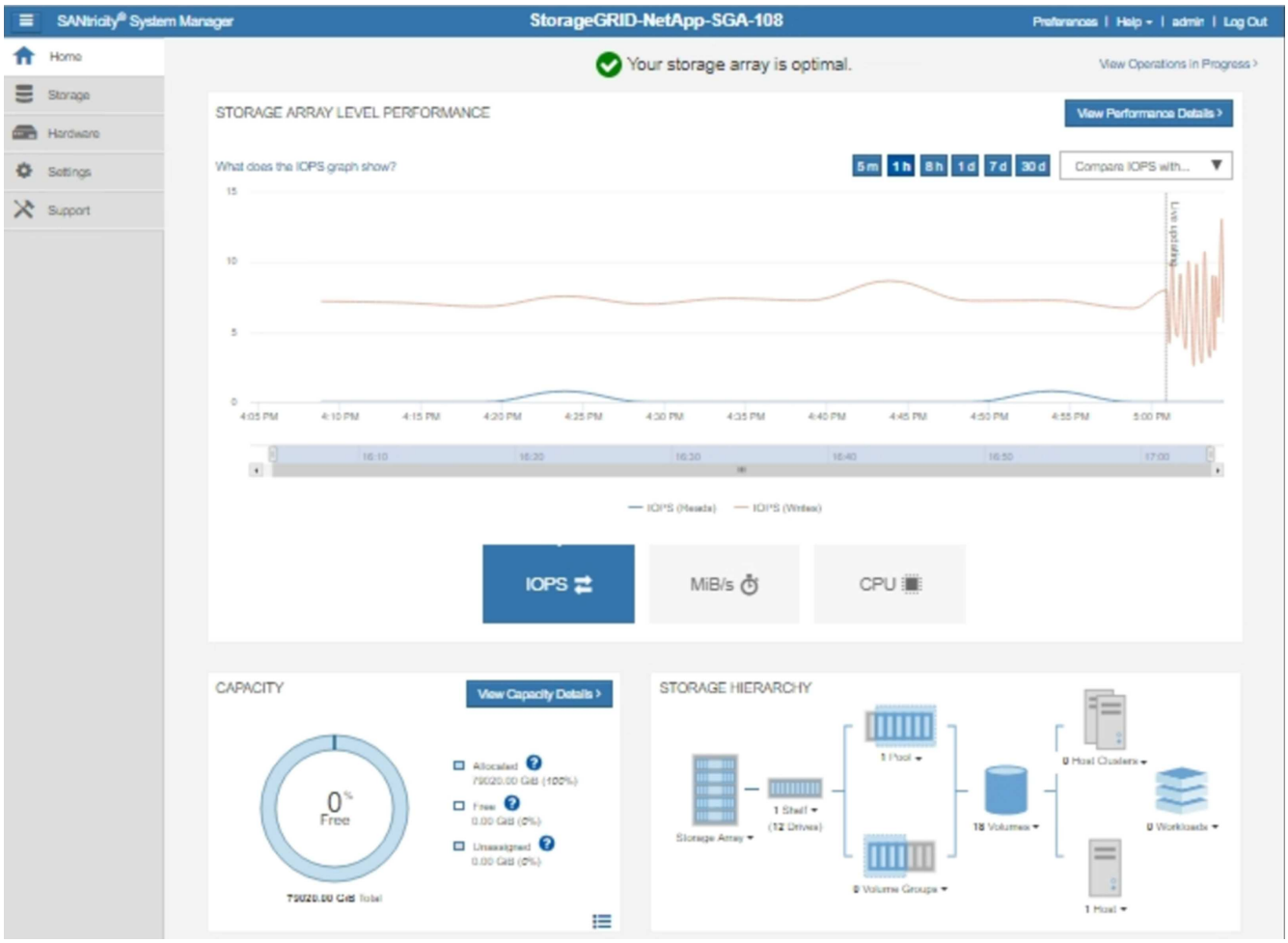
"配置管理员代理设置"

> 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 配置信息的更多详细信息、请参见E系列文档中心。
>
> "NetApp E系列系统文档中心"

步骤

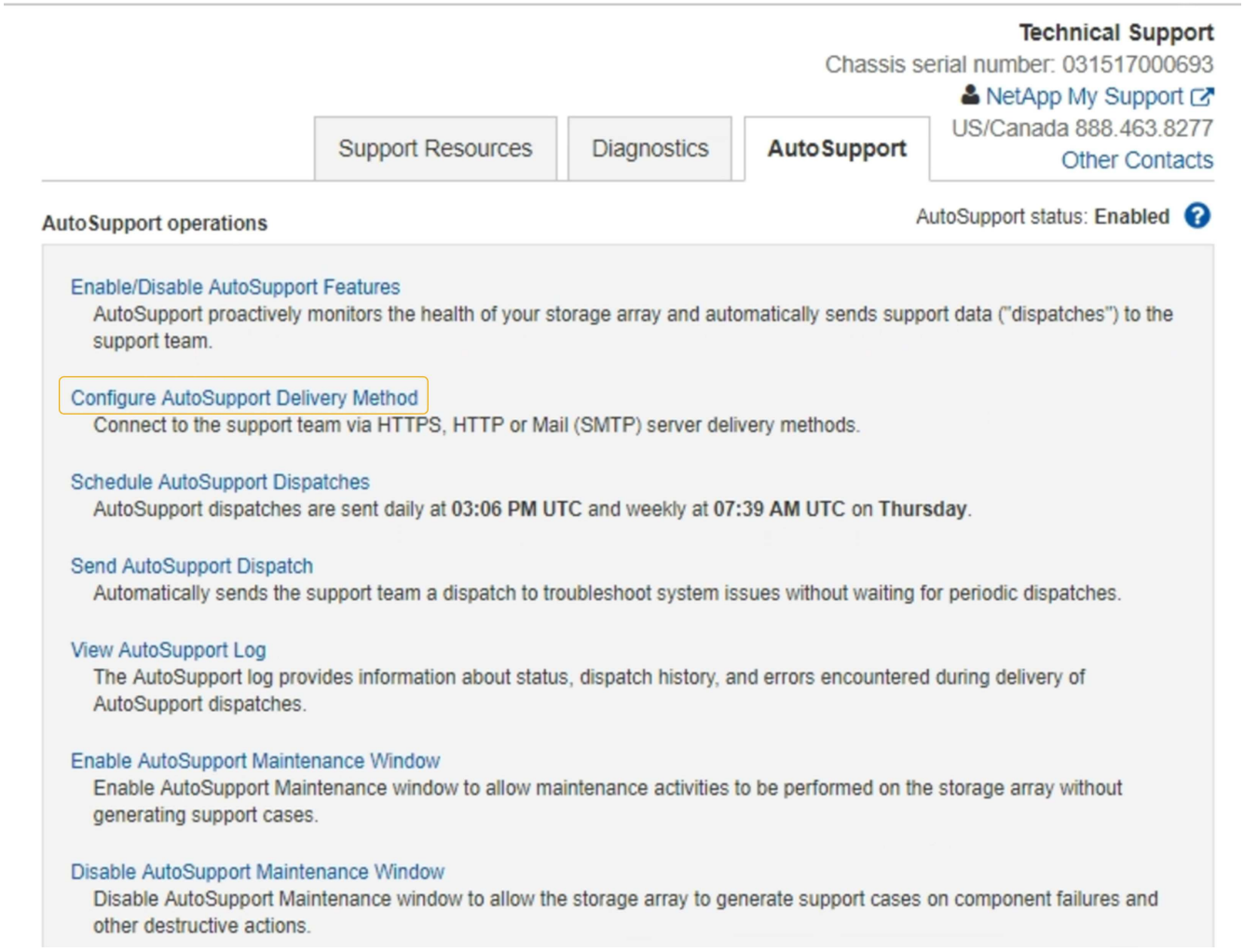
1. 在网格管理器中、选择*节点*。
2. 从左侧的节点列表中，选择要配置的存储设备节点。
3. 选择 * SANtricity 系统管理器 * 。

   此时将显示 SANtricity System Manager 主页。



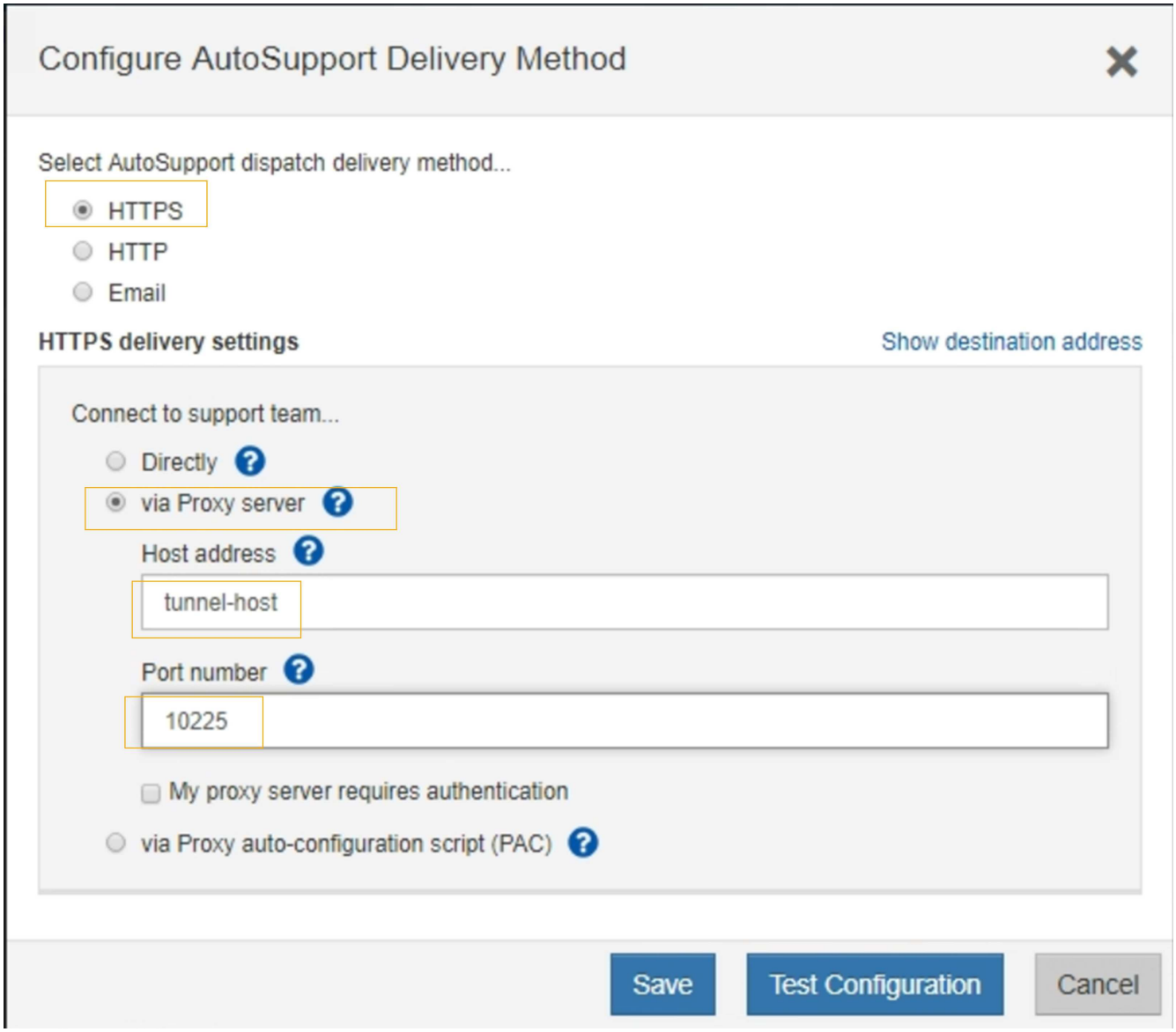
4. 选择*支持*>*支持中心*>* AutoSupport *。

   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。

   启用 HTTPS 协议的证书已预先安装。

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 设置和网络连接，确保首选

发件人管理节点可以连接到 NetApp 支持站点，然后重试此测试。

11. 选择 * 保存 * 。

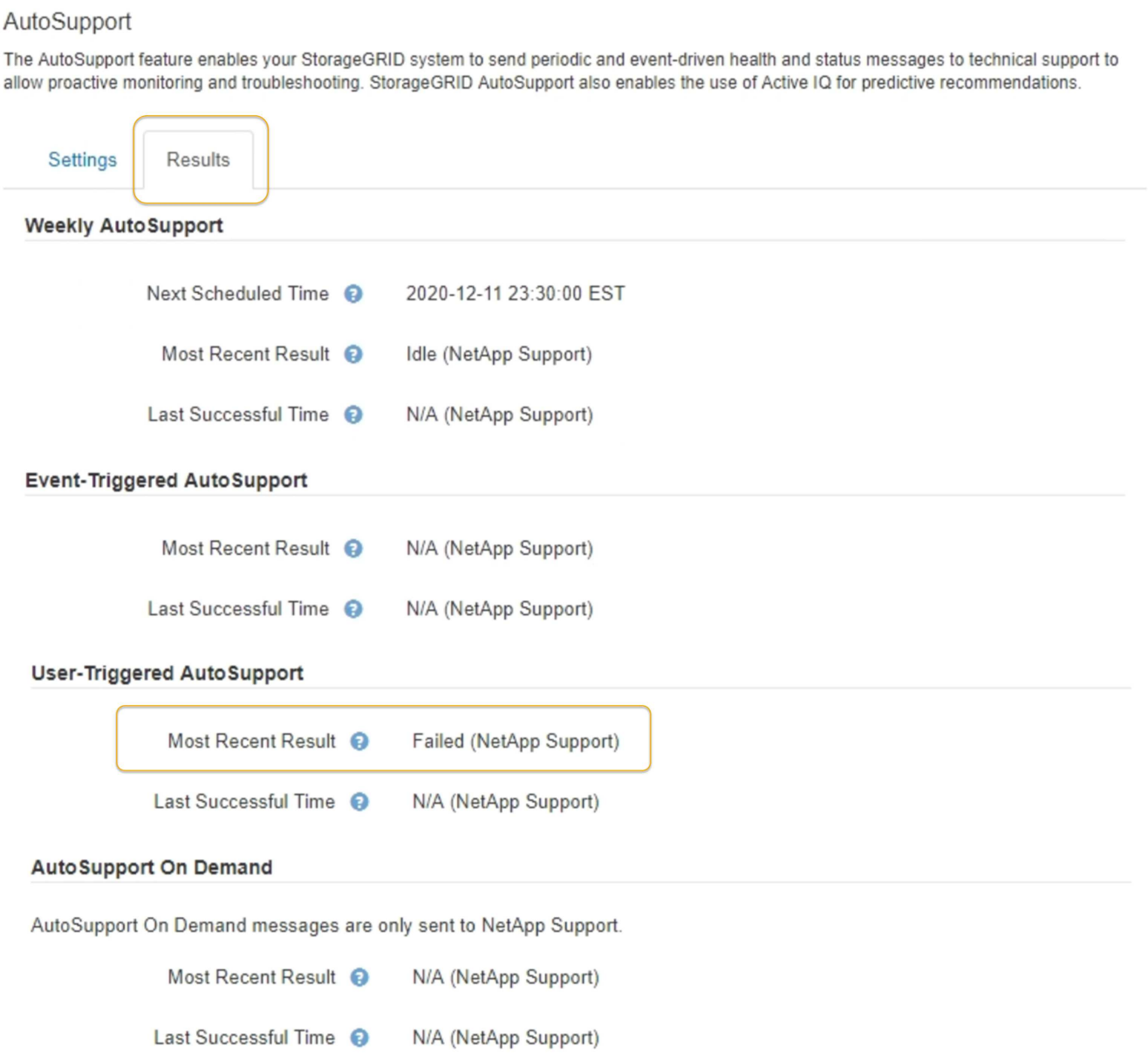
    此时将保存此配置，并显示一条确认消息： "`AutoSupport delivery method has been configured 。` "

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。

> 如果在系统范围内禁止发送电子邮件通知，则会禁止显示事件触发的 AutoSupport 消息。(选择*配置系统设置显示选项*。然后，选择 * 通知禁止全部 * 。）

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。



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您的电子邮件服务器是否正在运行(支持**警报(原有)*旧版电子邮件设置)。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.`

了解如何在中配置电子邮件服务器设置 "监控放大器；故障排除说明"。

更正**AutoSupport** 消息失败

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.`

相关信息

"监控和放大；故障排除"

管理存储节点

存储节点可提供磁盘存储容量和服务。管理存储节点需要监控每个节点上的可用空间量，使用水印设置以及应用存储节点配置设置。

- "什么是存储节点"
- "管理存储选项"
- "管理对象元数据存储"
- "为已存储对象配置全局设置"
- "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**ADC**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。

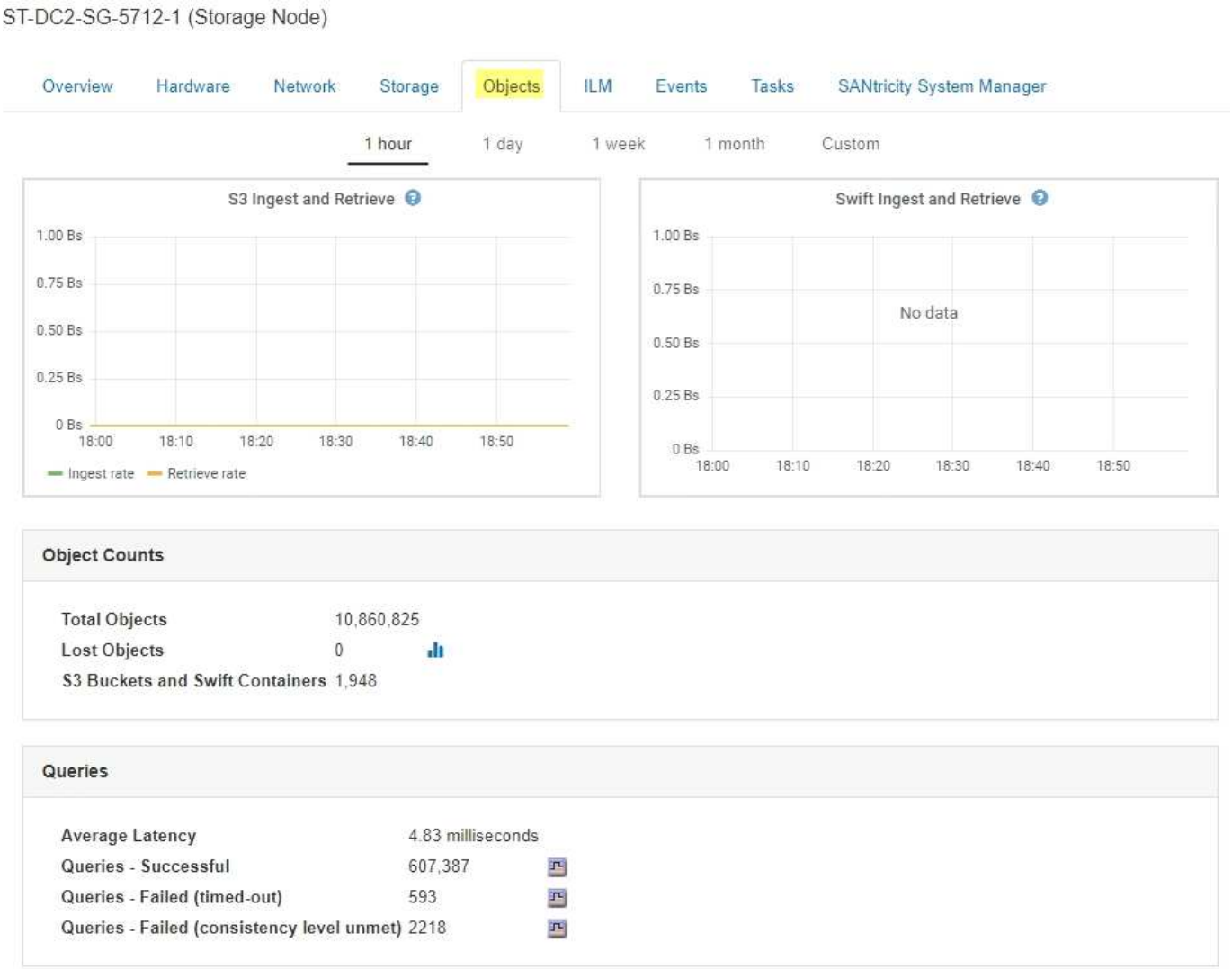
什么是**DDS**服务

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节点页面对象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 " 页面获取网格当前状态的追加信息 。请参见 "运行诊断"。

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 系统的大部分繁重工作。

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 " 页面获取网格当前状态的追加信息 。请参见 "运行诊断"。

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。您可以在信息板或每个存储节点的节点页面ILM选项卡上查看这些指标。

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	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	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。

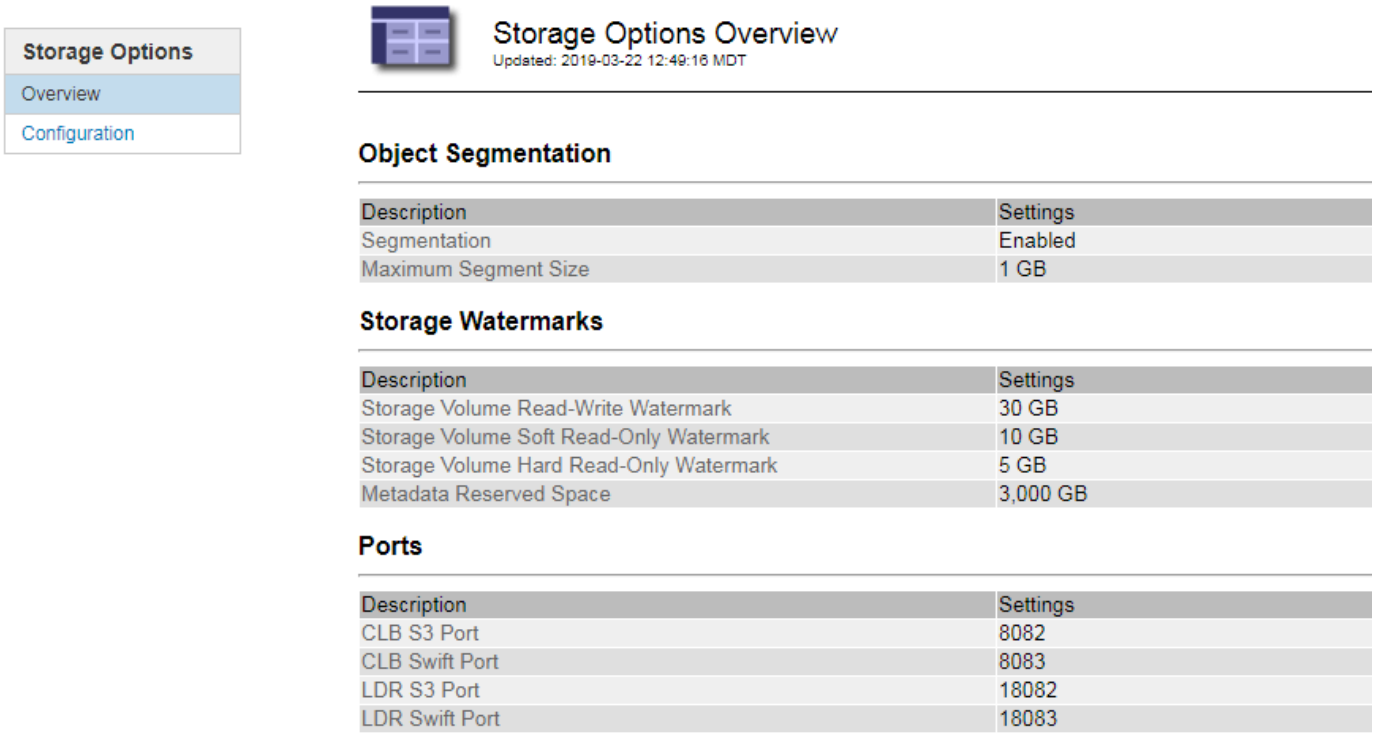
为了确保冗余并防止丢失，每个站点维护三个对象元数据副本。这些副本会均匀分布在每个站点的所有存储节点上。此复制不可配置，并且会自动执行。

"管理对象元数据存储"

管理存储选项

您可以使用网格管理器中的配置菜单查看和配置存储选项。存储选项包括对象分段设置和存储水印的当前值。您还可以查看网关节点上已弃用的 CLB 服务以及存储节点上的 LDR 服务使用的 S3 和 Swift 端口。

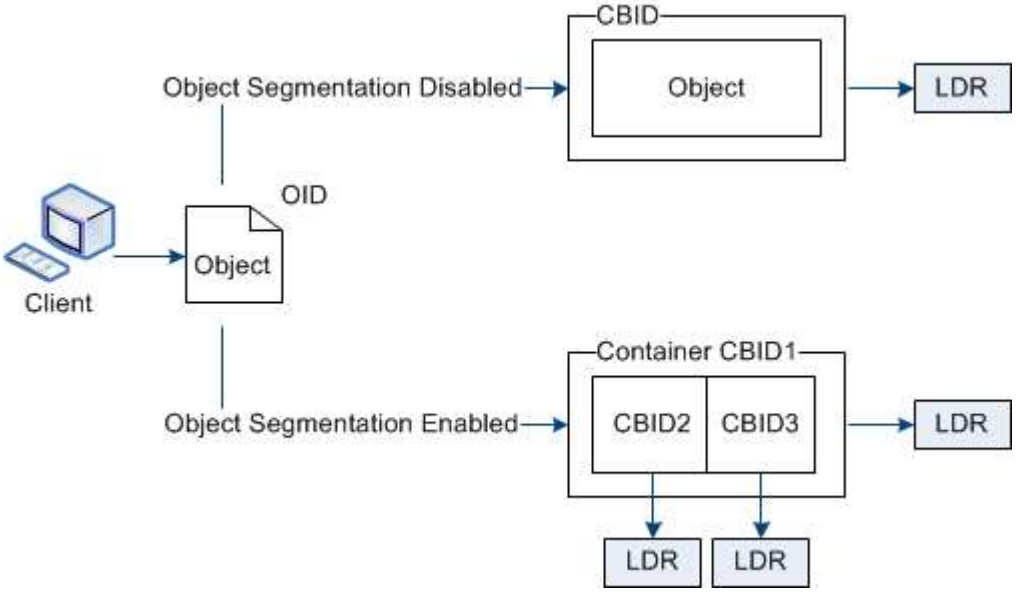
有关端口分配的信息、请参见 "摘要：客户端连接的 IP 地址和端口"。



什么是对象分段

对象分段是指将对象拆分成一组固定大小的较小对象，以优化大型对象的存储和资源使用量的过程。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。



如果您的StorageGRID 系统包含一个归档节点、其目标类型为云分层-简单存储服务、而目标归档存储系统为Amazon Web Services (AWS)、则最大分段大小必须小于或等于4.5 GiB (4、831、838、208字节)。此上限可确保不会超过AWS PUT的五GB限制。超过此值的AWS请求将失败。

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。

容器和分段不一定存储在同一个存储节点上。容器和分段可以存储在任何存储节点上。

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：

分段容器 + 分段 1 + 分段 2 = 三个已存储对象

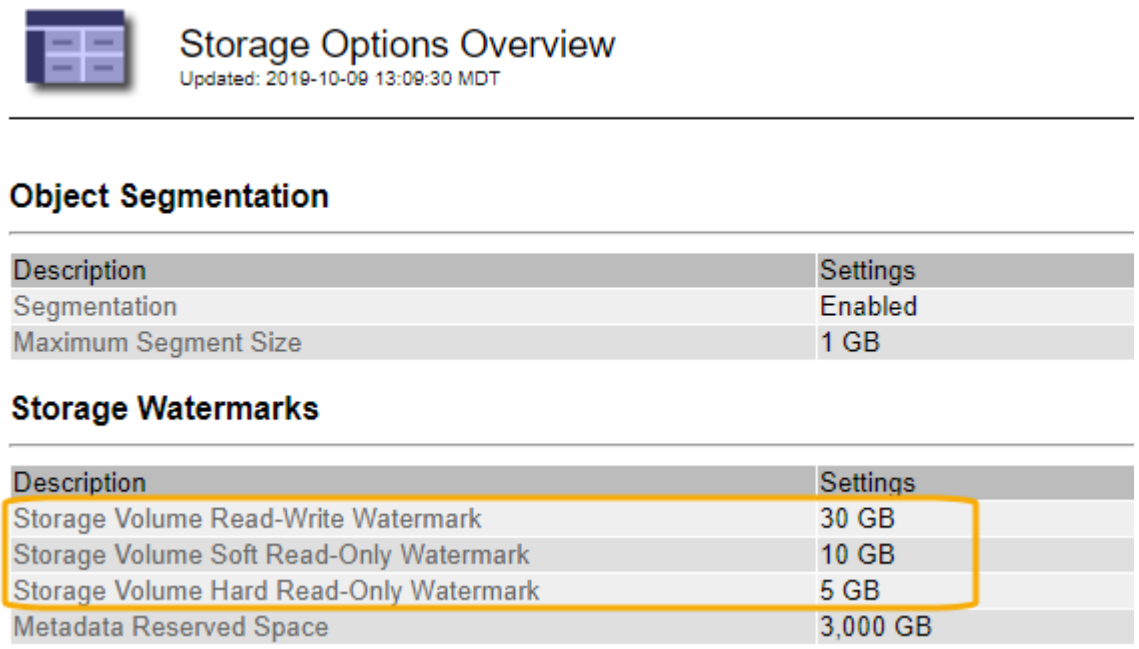
您可以通过确保以下各项来提高处理大型对象时的性能：

- 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。
- 每个存储节点都具有足够的磁盘 IO 性能来满足所需的吞吐量。

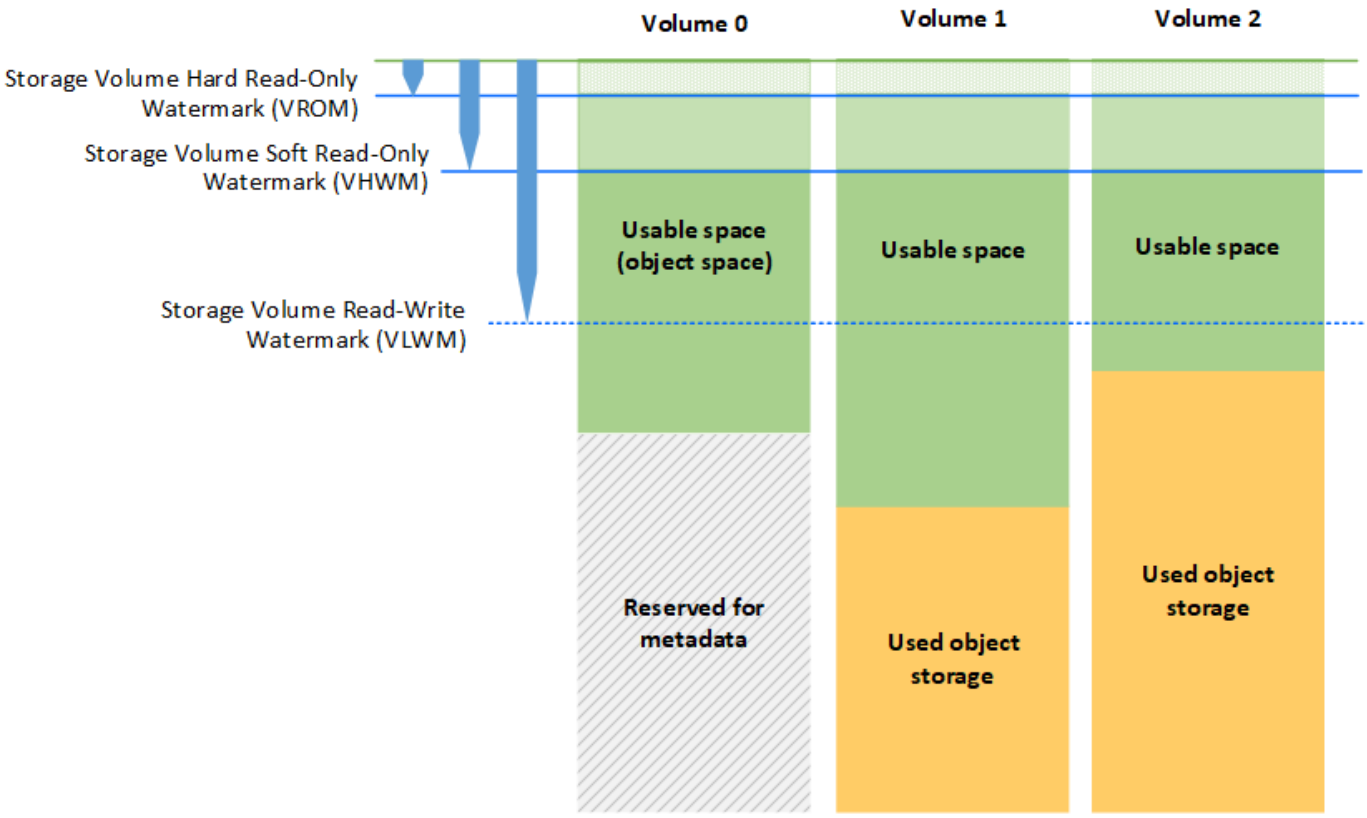
什么是存储卷水印

StorageGRID 使用存储卷水印来监控存储节点上的可用空间量。如果节点上的可用空间量小于配置的水印设置、则会触发存储状态(SSTS)警报、以便您确定是否需要添加存储节点。

要查看存储卷水印的当前设置、请选择*配置存储选项*概述。



下图显示了一个包含三个卷的存储节点、并显示了三个存储卷水印的相对位置。在每个存储节点中、StorageGRID 会在卷0上为对象元数据预留空间；该卷上的任何剩余空间将用于对象数据。所有其他卷仅用于对象数据、其中包括复制的副本和经过纠删编码的片段。



存储卷水印是系统范围的默认设置、表示存储节点中每个卷所需的最小可用空间量、以防止StorageGRID 更改节点的读写行为或触发警报。请注意、在StorageGRID 执行操作之前、所有卷都必须达到水印。如果某些卷的可用空间量超过所需的最小可用空间量、则不会触发警报、并且节点的读写行为也不会发生变化。

存储卷软只读水印(VHWM)

存储卷软只读水印是第一个用于指示节点的对象数据可用空间即将用尽的水印。此水印表示存储节点中的每个卷上必须有多少可用空间、才能防止节点进入"软只读模式"。`s`软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。

如果每个卷上的可用空间量小于此水印的设置、则存储状态(SSTS)警报将在通知级别触发、并且存储节点将过渡到软只读模式。

例如，假设存储卷软只读水印设置为 10 GB ，这是其默认值。如果存储节点中每个卷上的可用空间不足10 GB、则在通知级别触发SSTS警报、并且存储节点将过渡到软只读模式。

存储卷硬只读水印(VROM)

下一个水印是Storage Volume硬只读水印、用于指示节点的对象数据可用空间正在变满。此水印表示存储节点中的每个卷必须有多少可用空间、才能防止节点进入"`硬只读模式"。`硬只读模式表示存储节点为只读、不再接受写入请求。

如果存储节点中每个卷上的可用空间量小于此水印的设置、则存储状态(SSTS)警报将在主要级别触发、而存储节点将过渡到硬只读模式。

例如、假设存储卷硬只读水印设置为5 GB、这是其默认值。如果存储节点中的每个存储卷上的可用空间不足5 GB、则在主要级别触发SSTS警报、并且存储节点将过渡到硬只读模式。

存储卷硬只读水印的值必须小于存储卷软只读水印的值。

存储卷读写水印**(VLWM)**

存储卷读写水印仅用于标记已过渡到只读模式的适用场景 存储节点。此水印用于确定何时允许存储节点重新变为读写状态。

例如、假设某个存储节点已过渡到硬只读模式。如果存储卷读写水印设置为30 GB (默认值)、则存储节点中每个存储卷上的可用空间必须从5 GB增加到30 GB、然后该节点才能重新变为读写状态。

存储卷读写水印的值必须大于存储卷软只读水印的值。

相关信息

"管理完整存储节点"

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。

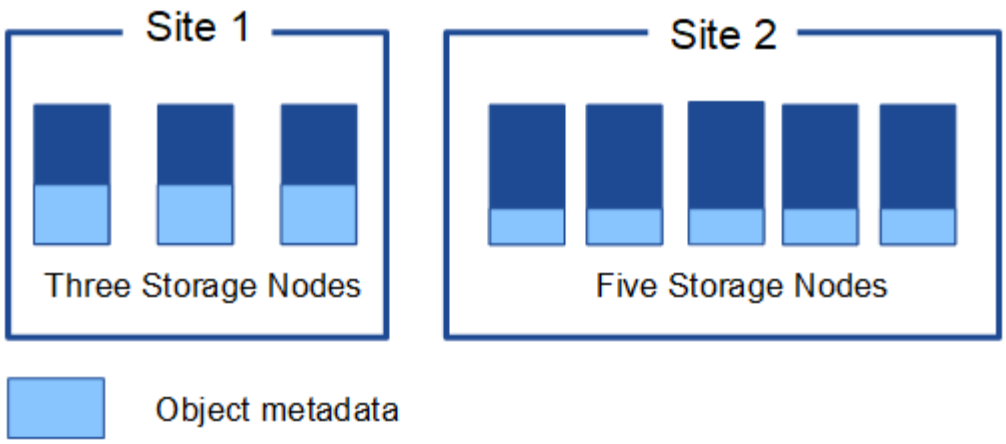
对于 StorageGRID 中的对象，对象元数据包括以下类型的信息：

- 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?

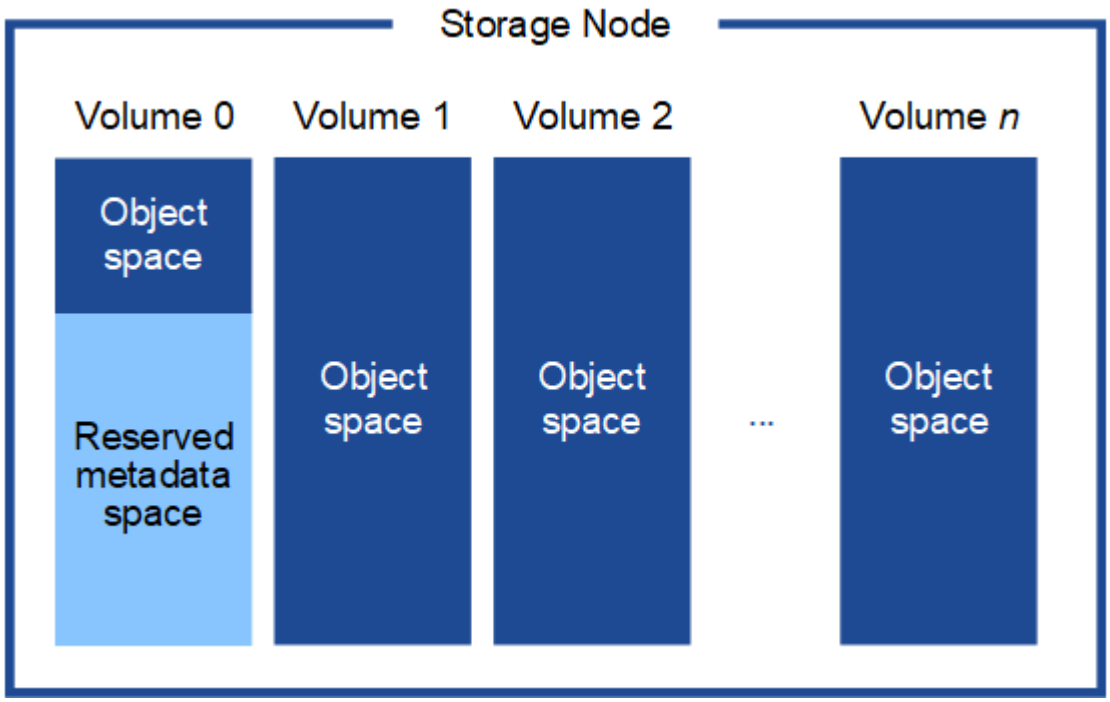
StorageGRID 在 Cassandra 数据库中维护对象元数据，该数据库独立于对象数据进行存储。为了提供冗余并防止对象元数据丢失， StorageGRID 会为每个站点的系统中的所有对象存储三个元数据副本。对象元数据的三个副本均匀分布在每个站点的所有存储节点上。

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，这些元数据会在该站点的存储节点之间平均分布。



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）。

为特定存储节点上的对象元数据预留的空间量取决于多种因素，如下所述。

元数据预留空间设置

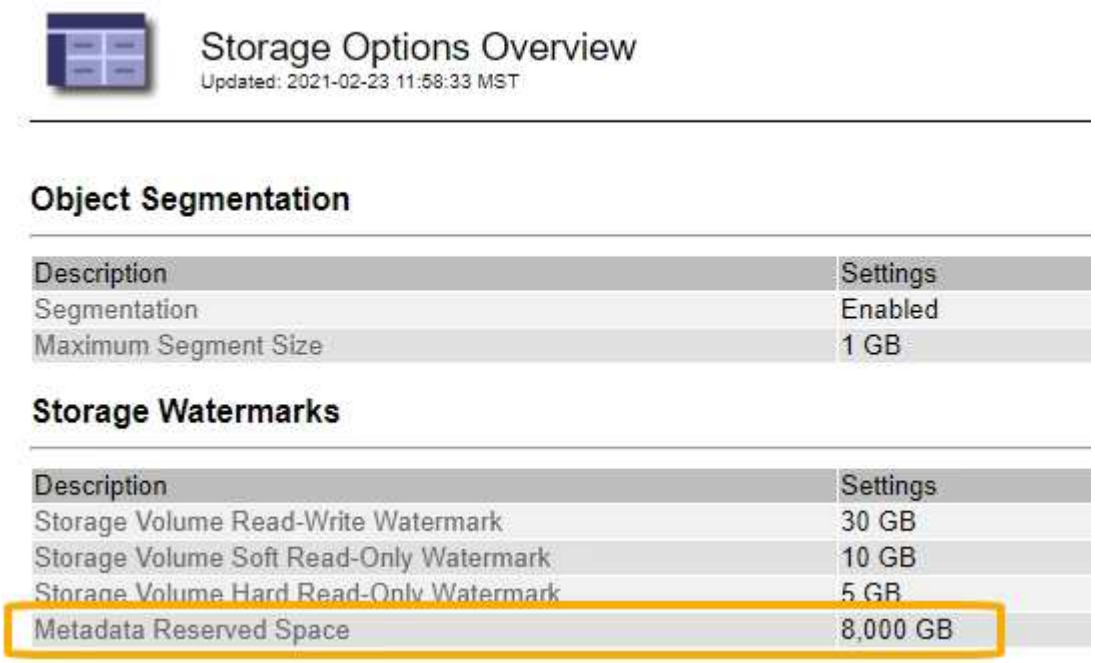
元数据预留空间 _ 是一个系统范围设置，表示将为每个存储节点的卷 0 上的元数据预留的空间量。如表所示、StorageGRID 11.5的此设置的默认值基于以下内容：

- 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	**StorageGRID 11.5**的默认元数据预留空间设置
11.5	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 ）

要查看 StorageGRID 系统的元数据预留空间设置，请执行以下操作：

1. 选择*配置*>*系统设置*>*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StorageGRID 11.5安装的默认设置、其中每个存储节点的RAM均为128 GB或以上。

元数据的实际预留空间

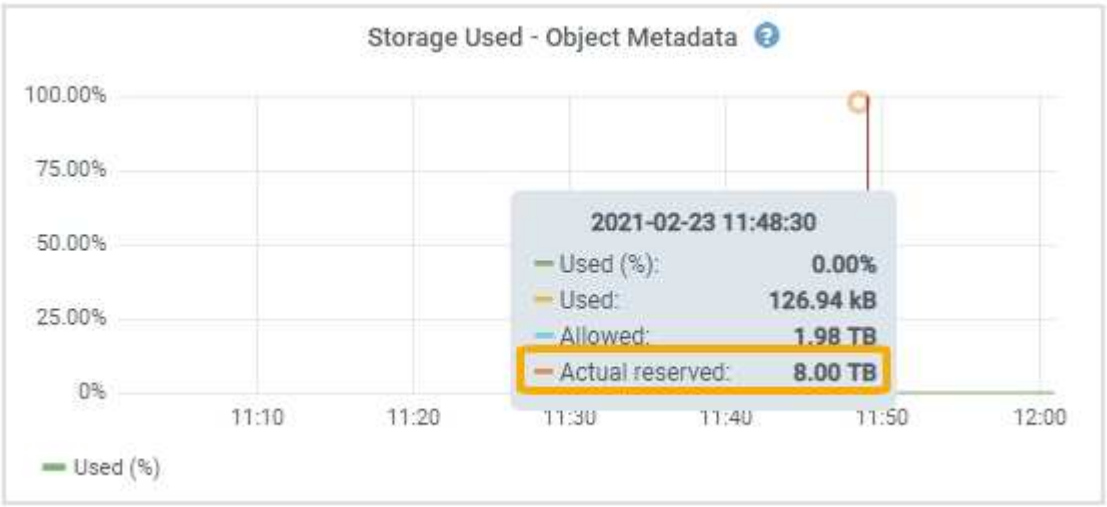
与系统范围的元数据预留空间设置不同，系统会为每个存储节点确定对象元数据的 *actual reserved space* 。对于任何给定的存储节点，元数据的实际预留空间取决于节点的卷 0 大小以及系统范围的 * 元数据预留空间 * 设

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

要查看特定存储节点上元数据的实际预留空间，请执行以下操作：

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. 将光标悬停在 "Storage Used - Object Metadata " 图表上，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安装的StorageGRID 11.5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*值对应于此Prometheus指标：

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

实际预留的元数据空间示例

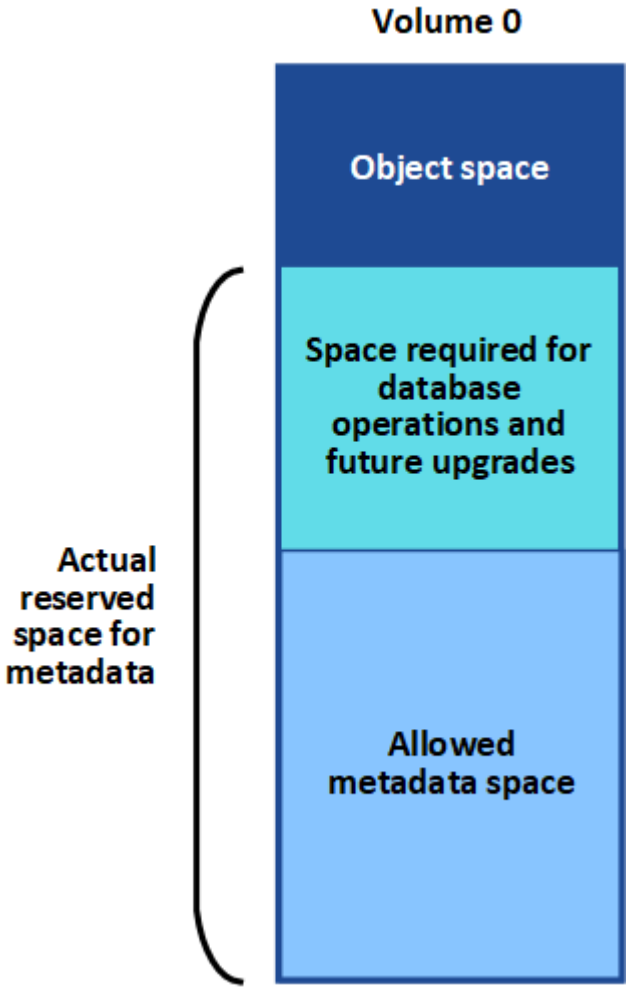
假设您安装的是使用11.5版的新StorageGRID 系统。在此示例中，假设每个存储节点的 RAM 超过 128 GB ，并且存储节点 1 （ SN1 ）的卷 0 为 6 TB 。基于以下值：

- 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StorageGRID 11.5安装的默认值。)

- 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。



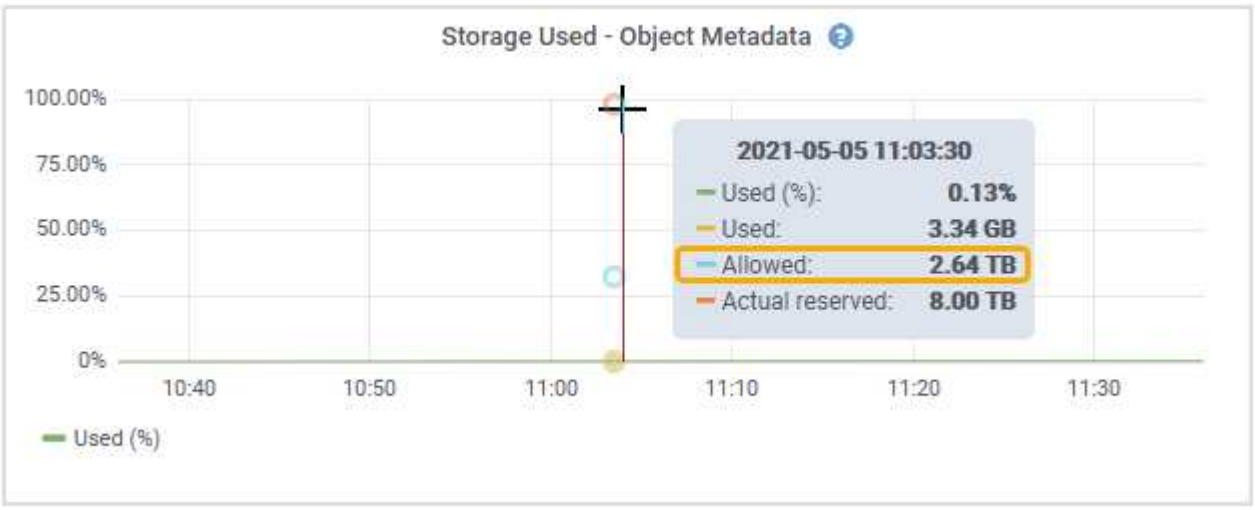
下表总结了 StorageGRID 如何确定存储节点的允许元数据空间值。

元数据的实际预留空间	允许的元数据空间
4 TB或更少	元数据实际预留空间的 60% ，最大 1.98 TB
超过4 TB	(元数据的实际预留空间−1 TB)×60%、最多2.64 TB

如果您的StorageGRID 系统在任何存储节点上存储(或预期存储)的元数据超过2.64 TB、则在某些情况下、允许的元数据空间可能会增加。如果您的每个存储节点的RAM均超过128 GB、并且存储卷0上有可用空间、请联系您的NetApp客户代表。如果可能、NetApp将审核您的要求并增加每个存储节点的允许元数据空间。

要查看存储节点允许的元数据空间，请执行以下操作：

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. 将光标悬停在已用存储 - 对象元数据图表上，找到 * 允许 * 值。



在屏幕截图中， * 允许 * 值为 2.64 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11.5版的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 11.5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。）
- SN1 上允许的元数据空间为 2.64 TB 。（这是实际预留空间的最大值。）

不同大小的存储节点如何影响对象容量

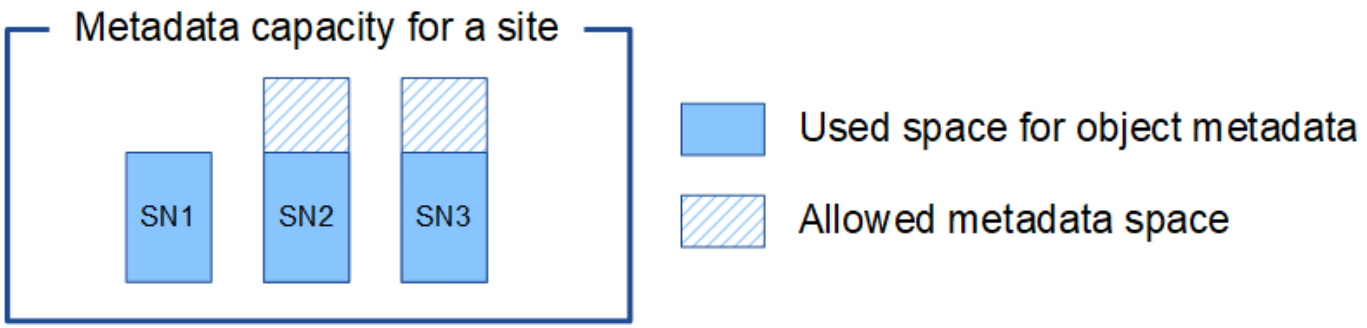
如上所述， StorageGRID 会在每个站点的存储节点之间均匀分布对象元数据。因此，如果某个站点包含不同大小的存储节点，则该站点上最小的节点将决定该站点的元数据容量。

请考虑以下示例：

- 您有一个单站点网格，其中包含三个大小不同的存储节点。
- * 元数据预留空间 * 设置为 4 TB 。
- 对于实际预留的元数据空间和允许的元数据空间，存储节点具有以下值。

存储节点	卷 **0** 的大小	实际预留的元数据空间	允许的元数据空间
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

由于对象元数据在站点的存储节点之间平均分布，因此本示例中的每个节点只能持有 1.32 TB 的元数据。不能使用 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、请执行以下操作：

  "监控和放大；故障排除"

- 要增加系统的对象元数据容量、必须添加新的存储节点：

  "扩展网格"

为已存储对象配置全局设置

您可以使用网格选项为存储在 StorageGRID 系统中的所有对象配置设置，包括存储的对象压缩和存储的对象加密。和存储的对象哈希。

- "配置存储的对象压缩"
- "配置存储的对象加密"
- "配置存储的对象哈希"

配置存储的对象压缩

您可以使用 " 压缩存储的对象 " 网格选项减小 StorageGRID 中存储的对象的大小，从而减

少对象占用的存储。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

默认情况下， " 压缩存储的对象 " 网格选项处于禁用状态。如果启用此选项，则 StorageGRID 会在保存每个对象时尝试使用无损压缩对其进行压缩。

> 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。

启用此选项之前，请注意以下事项：

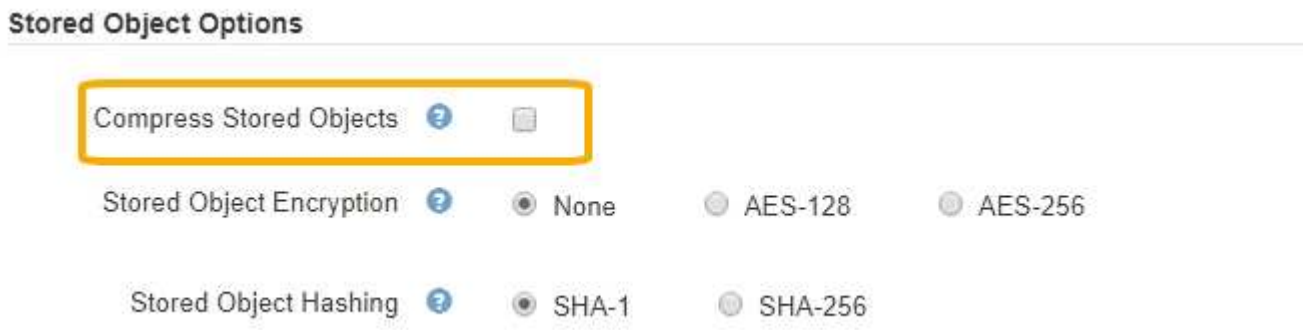
- 除非您知道要存储的数据是可压缩的，否则不应启用数据压缩。
- 将对象保存到 StorageGRID 的应用程序可能会在保存对象之前对其进行压缩。如果客户端应用程序在将对象保存到 StorageGRID 之前已对其进行了压缩，则启用压缩存储的对象不会进一步减小对象的大小。
- 如果将 NetApp FabricPool 与 StorageGRID 结合使用，请勿启用数据压缩。
- 如果启用了 " 压缩存储的对象 " 网格选项，则 S3 和 Swift 客户端应用程序应避免执行指定要返回的字节数范围的 GET 对象操作。这些 "`range read` " 操作效率低下，因为 StorageGRID 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*配置系统设置网格选项*。
2. 在存储的对象选项部分中，选中 * 压缩存储的对象 * 复选框。



3. 单击 * 保存 * 。

配置存储的对象加密

如果要确保在对象存储受到影响时无法以可读形式检索数据，则可以对存储的对象进行加密。默认情况下，对象不会加密。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

存储的对象加密可对通过 S3 或 Swift 载入的所有对象数据进行加密。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，则当前加密的对象将保持加密状态，但新载入的对象不会加密。

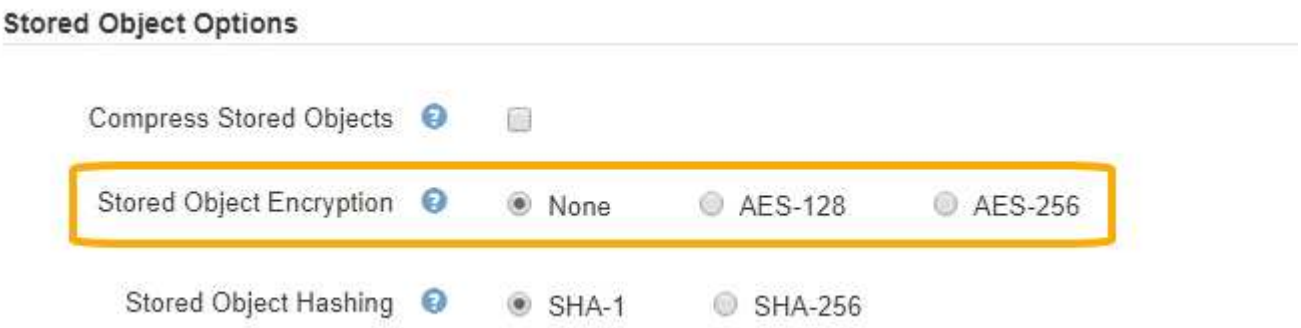
如果更改此设置，则应用新设置需要大约一分钟的时间。已配置的值将进行缓存以提高性能和扩展能力。

存储的对象可以使用 AES - 128 或 AES - 256 加密算法进行加密。

存储对象加密设置仅适用于尚未通过存储分段级别或对象级别加密进行加密的 S3 对象。

步骤

1. 选择*配置系统设置网格选项*。
2. 在存储的对象选项部分中，将存储的对象加密更改为 * 无 * （默认）， * AES-128* 或 * AES-256* 。



3. 单击 * 保存 * 。

配置存储的对象哈希

存储对象哈希选项指定用于验证对象完整性的哈希算法。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

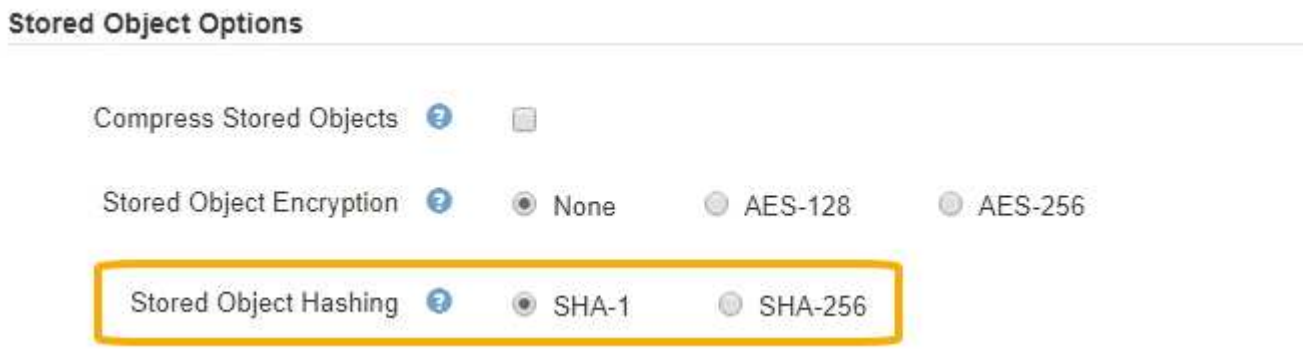
默认情况下、使用SHA - 1算法对对象数据进行哈希。SHA-256 算法需要额外的 CPU 资源，通常不建议用于完

整性验证。

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。

步骤

1. 选择*配置系统设置网格选项*。
2. 在存储的对象选项部分中，将存储的对象哈希更改为 * SHA-1* （默认）或 * SHA-256* 。



3. 单击 * 保存 * 。

存储节点配置设置

每个存储节点都使用许多配置设置和计数器。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。

要访问存储节点的配置设置和计数器，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 _* 。
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	S3 ， Swift 和其他内部 StorageGRID 流量的 HTTP 协议的当前状态： • 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 ）。请仅在前台验证完成后使用。StorageGRID 系统会自动还原缺少的复制对象数据。
验证	FVOV	选择要执行前台验证的对象存储。
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。有关详细信息，请参见 StorageGRID 监控和故障排除说明。

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。请仅在前台验证完成后使用。

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，可以从存储节点检索对象以复制到 StorageGRID 系统中的其他位置，但不能从其他位置将对象复制到此存储节点： LDR 服务为只读服务。
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。

相关信息

"监控和放大；故障排除"

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。请参见有关扩展 StorageGRID 系统的说明。

添加存储扩展架

某些 StorageGRID 设备存储节点（例如 SG6060 ）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。请参见有关扩展 StorageGRID 系统的说明。

正在添加存储节点

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。请参见有关扩展 StorageGRID 系统的说明。

相关信息

"扩展网格"

管理管理节点

StorageGRID 部署中的每个站点都可以有一个或多个管理节点。

- "什么是管理节点"

- "使用多个管理节点"
- "确定主管理节点"
- "选择首选发件人"
- "查看通知状态和队列"
- "管理节点如何显示已确认的警报（旧系统）"
- "配置审核客户端访问"

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。

管理节点托管以下服务：

- AMS 服务
- CMN 服务
- NMS 服务
- Prometheus 服务
- 负载平衡器和高可用性服务（用于支持 S3 和 Swift 客户端流量）

管理节点还支持管理应用程序程序接口（ Management Application Program Interface ， mgmt-API ）处理来自网格管理 API 和租户管理 API 的请求。

什么是 **AMS** 服务

审核管理系统（ Audit Management System ， AMS ）服务可跟踪系统活动和事件。

什么是 **CMN** 服务

配置管理节点（ CMN ）服务负责管理所有服务所需的连接和协议功能的系统范围配置。此外， CMN 服务还用于运行和监控网格任务。每个 StorageGRID 部署只有一个 CMN 服务。托管 CMN 服务的管理节点称为主管理节点。

什么是 **NMS** 服务

网络管理系统（ Network Management System ， NMS ）服务为通过网格管理器（ StorageGRID 系统基于浏览器的界面）显示的监控，报告和配置选项提供支持。

什么是 **Prometheus** 服务

Prometheus 服务从所有节点上的服务收集时间序列指标。

相关信息

"使用网格管理API"

"使用租户帐户"

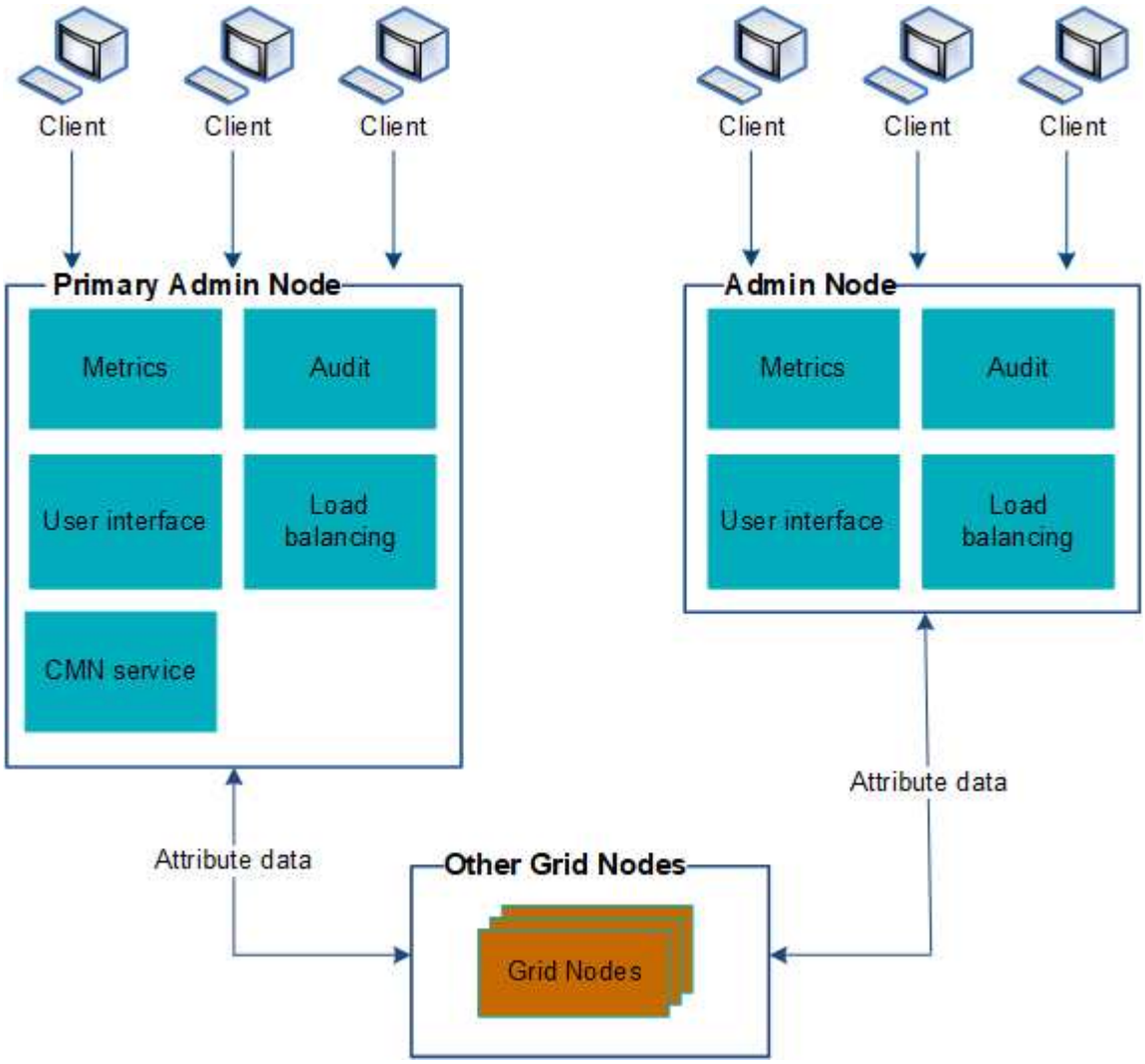
"管理负载平衡"

"管理高可用性组"

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确认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。

> 使用 HA 组时，如果主管理节点出现故障，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。

相关信息

"管理高可用性组"

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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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、然后单击 ➕ 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。

选择首选发件人

如果您的 StorageGRID 部署包含多个管理节点，则可以选择哪个管理节点应是通知的首选发送方。默认情况下，系统会选择主管理节点，但任何管理节点都可以是首选发送方。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

"配置*系统设置*显示选项"页面显示了当前选择用作首选发送方的管理节点。默认情况下会选择主管理节点。

在正常系统操作下，只有首选发件人才会发送以下通知：

- AutoSupport 消息
- SNMP 通知
- 警报电子邮件

- 警报电子邮件（旧系统）

但是，所有其他管理节点（备用发送器）都会监控首选发送器。如果检测到问题，备用发件人也可以发送这些通知。

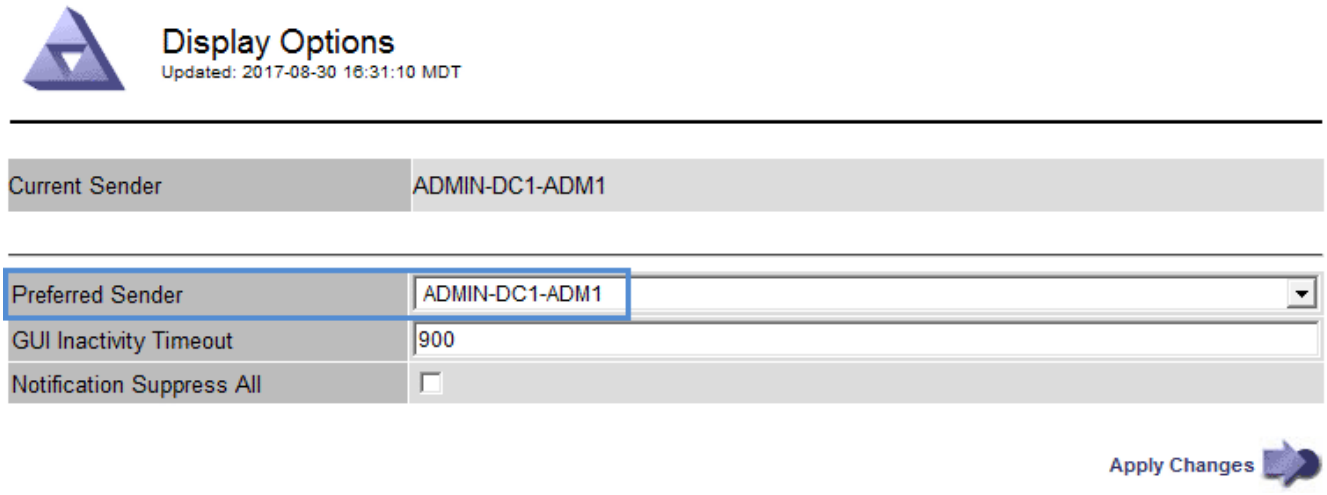
在以下情况下，首选发件人和备用发件人都可能发送通知：

- 如果管理节点彼此变为 "`islanded` " ，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。
- 备用发件人检测到首选发件人存在问题并开始发送通知后，首选发件人可能会重新获得其发送通知的能力。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。

在测试警报通知和 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。

步骤

1. 选择*配置*>*系统设置*>*显示选项*。
2. 从显示选项菜单中，选择 * 选项 * 。
3. 从下拉列表中选择要设置为首选发送方的管理节点。



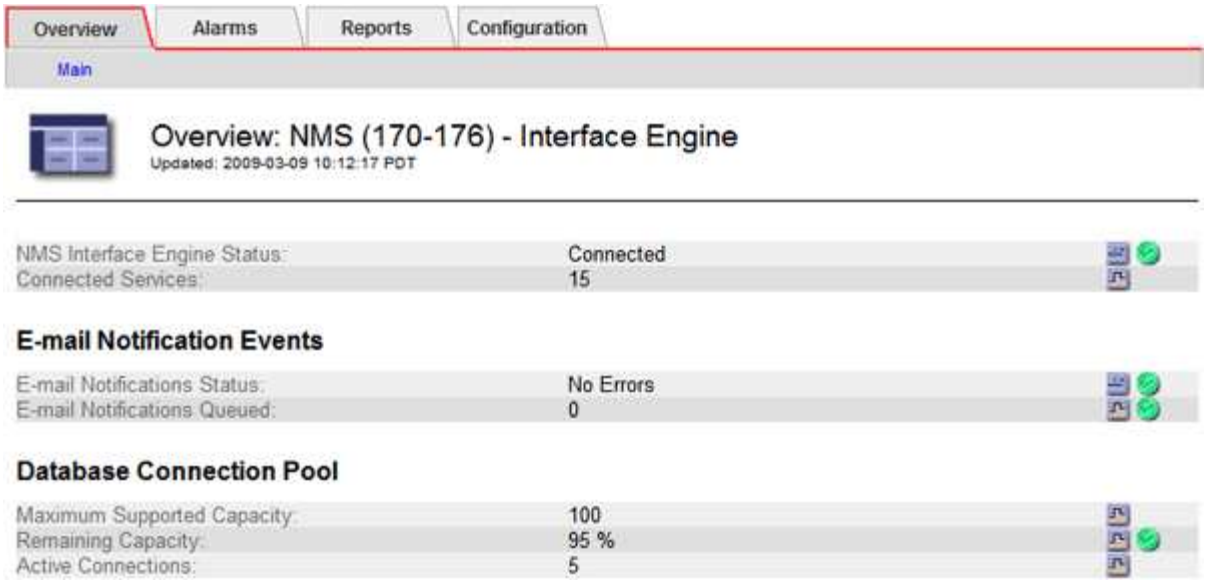
4. 单击 * 应用更改 * 。

   管理节点设置为通知的首选发件人。

查看通知状态和队列

管理节点上的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 * 。

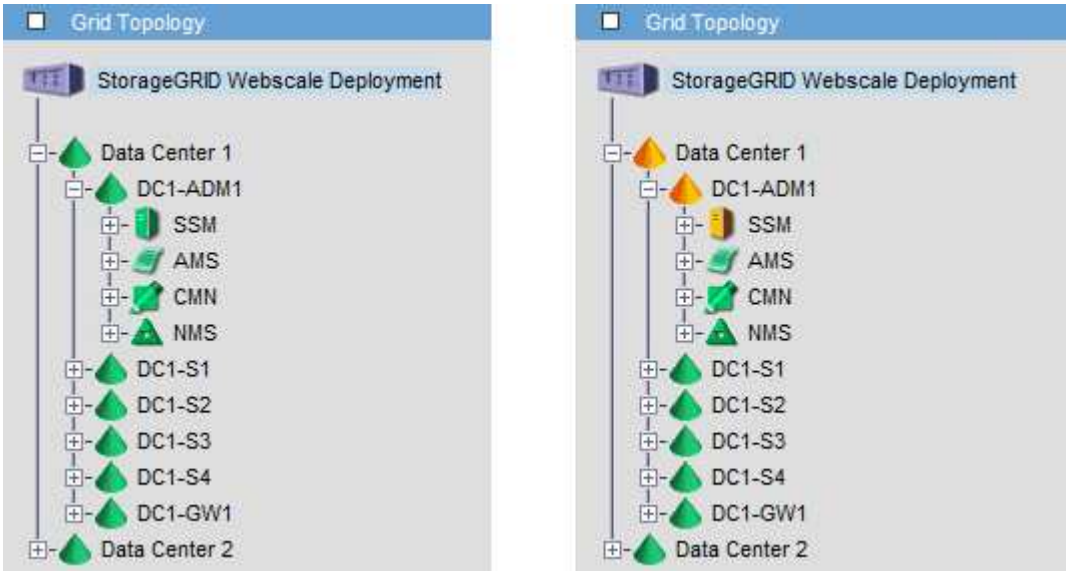


通知通过电子邮件通知队列进行处理，并按触发顺序逐个发送到邮件服务器。如果出现问题（例如网络连接错误），并且在尝试发送通知时邮件服务器不可用，则尽力将通知重新发送到邮件服务器的操作将持续 60 秒。如果通知在 60 秒后未发送到邮件服务器，则通知将从通知队列中删除，并尝试在队列中发送下一个通知。由于通知可以从通知队列中删除而不发送，因此，在不发送通知的情况下，可能会触发警报。如果通知从队列中删除而未发送，则会触发分钟（电子邮件通知状态）次要警报。

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。由于确认不会复制到其他管理节点，因此对于每个管理节点，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

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。为了便于访问审核日志，您可以配置客户端对 CIFS 和 NFS 的审核共享的访问权限。

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、请参见了解审核消息的说明。

> 如果您可以选择使用 CIFS 或 NFS ，请选择 NFS 。

> 已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

相关信息

"什么是管理节点"

"查看审核日志"

"升级软件"

为**CIFS**配置审核客户端

用于配置审核客户端的操作步骤 取决于身份验证方法： Windows 工作组或 Windows Active Directory （ AD ）。添加后，审核共享将自动启用为只读共享。

> 已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

相关信息

"升级软件"

为工作组配置审核客户端

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 。

您需要的内容

- 您必须具有 `Passwords.txt` 具有root/admin帐户密码的文件(可在上述软件包中找到)。
- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。

关于此任务

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

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： `storagegrid-status`

如果所有服务均未运行或未验证，请先解决问题，然后再继续。

3. 返回命令行，按 * 。 Ctrl+* 。 c* 。

4. 启动CIFS配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. 为 Windows 工作组设置身份验证：

如果已设置身份验证，则会显示一条建议消息。如果已设置身份验证，请转至下一步。

a. 输入 ... `set-authentication`

b. 当系统提示您安装Windows工作组或Active Directory时、输入： `workgroup`

c. 出现提示时、输入工作组的名称： *`workgroup_name`*

d. 出现提示时、创建有意义的NetBIOS名称： *`netbios_name`*

或

按 * 输入 * 以使用管理节点的主机名作为 NetBIOS 名称。

此脚本将重新启动 Samba 服务器并应用更改。此操作需要不到一分钟的时间。设置身份验证后，添加审核客户端。

a. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

6. 添加审核客户端：

a. 输入 ... `add-audit-share`

> 共享将自动添加为只读。

b. 出现提示时、添加用户或组： *user*

c. 出现提示时、输入审核用户名： *audit_user_name*

d. 出现提示时、输入审核用户的密码： *password*

e. 出现提示时、重新输入同一密码以进行确认： *password*

f. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

> 无需输入目录。已预定义审核目录名称。

7. 如果允许多个用户或组访问审核共享，请添加其他用户：

a. 输入 ... `add-user-to-share`

此时将显示已启用共享的编号列表。

b. 出现提示时、输入审核导出共享的编号： *share_number*

c. 出现提示时、添加用户或组： `user`

或 `group`

d. 出现提示时、输入审核用户或组的名称： *audit_user or audit_group*

e. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

f. 对有权访问审核共享的每个其他用户或组重复这些子步骤。

8. (可选)验证您的配置： `validate-config`

此时将检查并显示这些服务。您可以安全地忽略以下消息：

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. 出现提示时，按 * 输入 * 。

此时将显示审核客户端配置。

b. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

9. 关闭CIFS配置实用程序： `exit`
10. 启动Samba服务： `service smbd start`
11. 如果 StorageGRID 部署是单个站点，请转至下一步。

或

或者，如果 StorageGRID 部署包括其他站点的管理节点，则根据需要启用这些审核共享：

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`

12. 从命令Shell中注销： `exit`

相关信息

"升级软件"

为**Active Directory**配置审核客户端

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 。

您需要的内容

- 您必须具有 `Passwords.txt` 具有root/admin帐户密码的文件(可在上述软件包中找到)。
- 您必须具有CIFS Active Directory用户名和密码。
- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

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： `storagegrid-status`

   如果所有服务均未运行或未验证，请先解决问题，然后再继续。

3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 启动CIFS配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. 为Active Directory设置身份验证： `set-authentication`

   在大多数部署中，您必须在添加审核客户端之前设置身份验证。如果已设置身份验证，则会显示一条建议消息。如果已设置身份验证，请转至下一步。

   a. 当系统提示您安装工作组或Active Directory时： `ad`
   b. 出现提示时，输入 AD 域的名称（短域名）。
   c. 出现提示时，输入域控制器的 IP 地址或 DNS 主机名。
   d. 出现提示时，输入完整的域域名。

      使用大写字母。

   e. 当系统提示您启用 winbind 支持时，键入 * 。

      winbind 用于解析 AD 服务器中的用户和组信息。

   f. 出现提示时，输入 NetBIOS 名称。
   g. 出现提示时，按 * 输入 * 。

      此时将显示 CIFS 配置实用程序。

6. 加入域：

   a. 如果尚未启动、请启动CIFS配置实用程序： `config_cifs.rb`
   b. 加入域： `join-domain`

c. 系统会提示您测试管理节点当前是否为有效的域成员。如果此管理节点先前未加入此域、请输入： `no`

d. 出现提示时、请提供管理员的用户名： *`administrator_username`*

   其中： *`administrator_username`* 是CIFS Active Directory用户名、而不是StorageGRID 用户名。

e. 出现提示时、请提供管理员密码： *`administrator_password`*

   是 *`administrator_password`* 是CIFS Active Directory用户名、而不是StorageGRID 密码。

f. 出现提示时，按 * 输入 * 。

   此时将显示 CIFS 配置实用程序。

7. 验证您是否已正确加入域：

   a. 加入域： `join-domain`

   b. 当系统提示测试服务器当前是否为域的有效成员时、输入： `y`

      如果您收到消息 "`join is OK ，` " you have successfully joined the domain.如果未收到此响应，请尝试设置身份验证并重新加入域。

   c. 出现提示时，按 * 输入 * 。

      此时将显示 CIFS 配置实用程序。

8. 添加审核客户端： `add-audit-share`

   a. 当系统提示您添加用户或组时、输入： `user`

   b. 当系统提示您输入审核用户名时，请输入审核用户名。

   c. 出现提示时，按 * 输入 * 。

      此时将显示 CIFS 配置实用程序。

9. 如果允许多个用户或组访问审核共享、请添加其他用户： `add-user-to-share`

   此时将显示已启用共享的编号列表。

   a. 输入审核导出共享的编号。

   b. 当系统提示您添加用户或组时、输入： `group`

      系统将提示您输入审核组名称。

   c. 当系统提示您输入审核组名称时，输入审核用户组的名称。

   d. 出现提示时，按 * 输入 * 。

      此时将显示 CIFS 配置实用程序。

   e. 对有权访问审核共享的每个其他用户或组重复此步骤。

10. (可选)验证您的配置： `validate-config`

此时将检查并显示这些服务。您可以安全地忽略以下消息：

- 找不到包含文件 `/etc/samba/includes/cifs-interfaces.inc`
- 找不到包含文件 `/etc/samba/includes/cifs-filesystem.inc`
- 找不到包含文件 `/etc/samba/includes/cifs-interfaces.inc`
- 找不到包含文件 `/etc/samba/includes/cifs-custom-config.inc`
- 找不到包含文件 `/etc/samba/includes/cifs-shares.inc`
- rlimit_max ：将 rlimit_max （ 1024 ）增加到最小 Windows 限制（ 16384 ）

> 请勿将设置 "security=ads" 与 "password server" 参数结合使用。（默认情况下， Samba 会自动发现要联系的正确 DC ）。

i. 出现提示时，按 * 输入 * 以显示审核客户端配置。

ii. 出现提示时，按 * 输入 * 。

此时将显示 CIFS 配置实用程序。

11. 关闭CIFS配置实用程序： `exit`
12. 如果 StorageGRID 部署是单个站点，请转至下一步。

或

或者，如果 StorageGRID 部署包括其他站点的管理节点，则根据需要启用这些审核共享：

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登录到管理节点： `exit`

13. 从命令Shell中注销： `exit`

相关信息

"升级软件"

将用户或组添加到**CIFS**审核共享

您可以将用户或组添加到与 AD 身份验证集成的 CIFS 审核共享。

您需要的内容

- 您必须具有 `Passwords.txt` 具有root/admin帐户密码的文件(可在上述软件包中找到)。

- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。

关于此任务

以下操作步骤 适用于与 AD 身份验证集成的审核共享。

> 已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

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`

   如果所有服务均未运行或未验证，请先解决问题，然后再继续。

3. 返回命令行，按 * 。 Ctrl+* 。 c* 。
4. 启动CIFS配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. 开始添加用户或组： `add-user-to-share`

   此时将显示已配置的审核共享的编号列表。

6. 出现提示时、输入审核共享(审核-导出)的编号： *`audit_share_number`*

   系统会询问您是否要授予用户或组对此审核共享的访问权限。

7. 出现提示时、添加用户或组： `user` 或 `group`

8. 当系统提示您输入此 AD 审核共享的用户或组名称时，请输入此名称。

   此用户或组将作为审核共享的只读添加到服务器的操作系统和 CIFS 服务中。系统将重新加载 Samba 配置，以使用户或组能够访问审核客户端共享。

9. 出现提示时，按 * 输入 * 。

   此时将显示 CIFS 配置实用程序。

10. 对有权访问审核共享的每个用户或组重复上述步骤。
11. (可选)验证您的配置： `validate-config`

    此时将检查并显示这些服务。您可以安全地忽略以下消息：

    - 找不到 include 文件 /etc/samba/includes/cifs-interfaces.inc
    - 找不到 include 文件 /etc/samba/includes/cifs-filesystem.inc
    - 找不到 include 文件 /etc/samba/includes/cifs-custom-config.inc
    - 找不到 include 文件 /etc/samba/includes/cifs-shares.inc
      i. 出现提示时，按 * 输入 * 以显示审核客户端配置。
      ii. 出现提示时，按 * 输入 * 。
12. 关闭CIFS配置实用程序： `exit`
13. 确定是否需要启用其他审核共享，如下所示：
    - 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： `exit`
14. 从命令Shell中注销： `exit`

从**CIFS**审核共享中删除用户或组

您不能删除允许访问审核共享的最后一个用户或组。

您需要的内容

- 您必须具有 `Passwords.txt` 包含root帐户密码的文件(可在上述软件包中找到)。
- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。

关于此任务

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

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CIFS配置实用程序： `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. 开始删除用户或组： `remove-user-from-share`

   此时将显示一个编号列表，其中列出了管理节点的可用审核共享。审核共享标记为 audit-export 。

4. 输入审核共享的编号： *audit_share_number*
5. 当系统提示删除用户或组时： `user` 或 `group`

   此时将显示审核共享的用户或组的编号列表。

6. 输入与要删除的用户或组对应的数字： *number*

   此时将更新审核共享，并且不再允许用户或组访问此审核共享。例如：

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. 关闭CIFS配置实用程序： `exit`
8. 如果 StorageGRID 部署包括其他站点的管理节点，请根据需要在每个站点禁用审核共享。
9. 配置完成后、从每个命令Shell中注销： `exit`

相关信息

"升级软件"

更改CIFS审核共享用户或组名称

您可以通过添加新用户或组并删除旧用户或组来更改 CIFS 审核共享的用户或组名称。

关于此任务

已弃用通过 CIFS/Samba 进行审核导出，并将在未来的 StorageGRID 版本中删除。

步骤

1. 将名称已更新的新用户或组添加到审核共享中。
2. 删除旧用户或组名称。

相关信息

"升级软件"

"将用户或组添加到CIFS审核共享"

"从CIFS审核共享中删除用户或组"

验证CIFS审核集成

审核共享为只读。日志文件可由计算机应用程序读取，验证不包括打开文件。我们认为，审核日志文件是否显示在 Windows 资源管理器窗口中已足够验证。验证连接后，关闭所有窗口。

审核共享会自动启用为只读共享。

您需要的内容

- 您必须具有 `Passwords.txt` 具有root/admin密码的文件(可在上述软件包中找到)。
- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。
- 审核客户端必须使用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 "Running or Verifified （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。

您需要的内容

- 您必须具有 `Passwords.txt` 具有root/admin帐户密码的文件(可在上述软件包中找到)。
- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。
- 审核客户端必须使用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。

您需要的内容

- 您必须具有 `Passwords.txt` 具有root/admin帐户密码的文件(可在上述软件包中找到)。
- 您必须具有 `Configuration.txt` 文件(在上述软件包中提供)。

关于此任务

您不能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

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

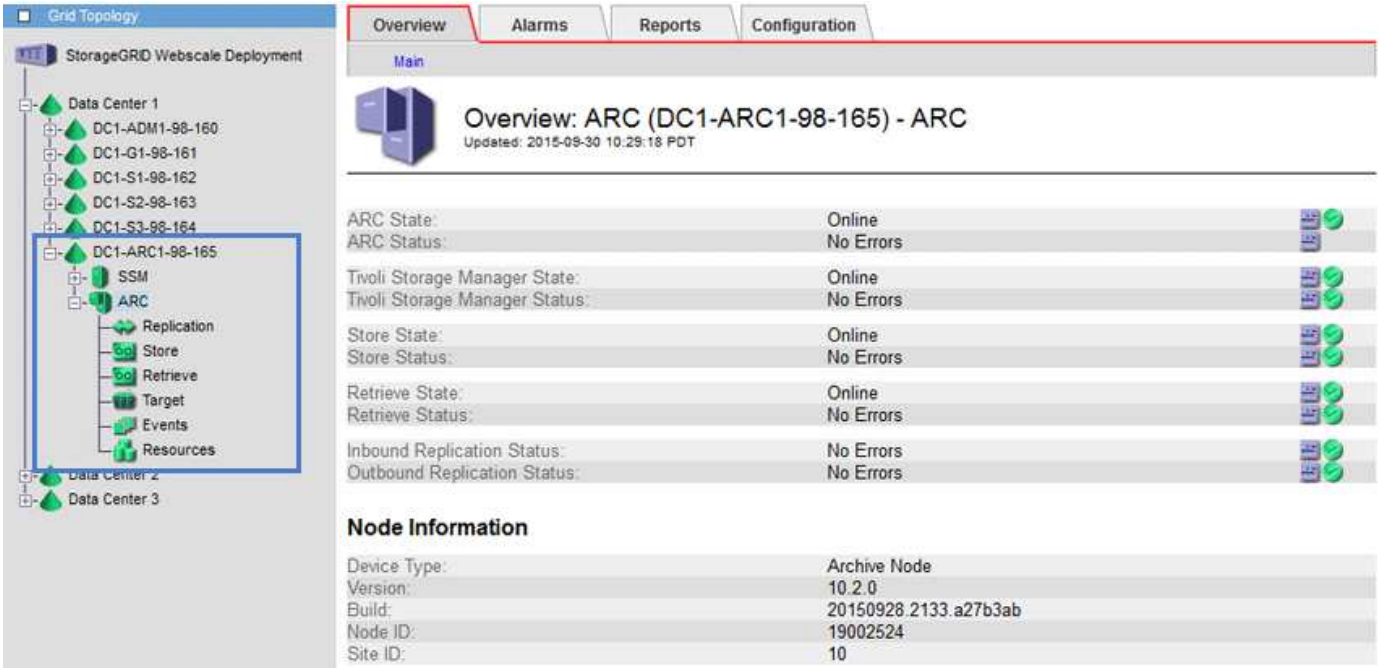
您也可以选择使用归档节点部署StorageGRID 系统的每个数据中心站点、以便连接到目标外部归档存储系统、例如Tivoli Storage Manager (TSM)。

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。

- "什么是归档节点"
- "配置归档节点与归档存储的连接"
- "为归档节点设置自定义警报"
- "集成Tivoli Storage Manager"

什么是归档节点

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。



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出，并移至云或磁带等外部归档存储。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**

归档节点的归档(Archive Node、ARC-）服务提供了一个管理界面、您可以使用此界面配置与外部归档存储(例如、通过TSM中间件连接到磁带)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。

配置归档节点与归档存储的连接

将归档节点配置为与外部归档连接时、必须选择目标类型。

StorageGRID 系统支持通过S3接口将对象数据归档到云、或通过Tivoli Storage Manager (TSM)中间件将对象数据归档到磁带。

为归档节点配置归档目标类型后、无法更改此目标类型。

- "通过S3 API归档到云"

- "通过TSM中间件归档到磁带"
- "配置归档节点检索设置"
- "配置归档节点复制"

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。

通过 S3 API 将对象从归档节点移动到外部归档存储系统已被 ILM 云存储池所取代，它可提供更多功能。仍然支持 * 云分层 - 简单存储服务（ S3 ） * 选项，但您可能更喜欢实施云存储池。

如果您当前正在使用具有 * 云分层 - 简单存储服务（ S3 ） * 选项的归档节点，请考虑将对象迁移到云存储池。请参见有关通过信息生命周期管理来管理对象的说明。

相关信息

"使用 ILM 管理对象"

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。

通过 S3 API 将对象从归档节点移动到外部归档存储系统已被 ILM 云存储池所取代，它可提供更多功能。仍然支持 * 云分层 - 简单存储服务（ S3 ） * 选项，但您可能更喜欢实施云存储池。

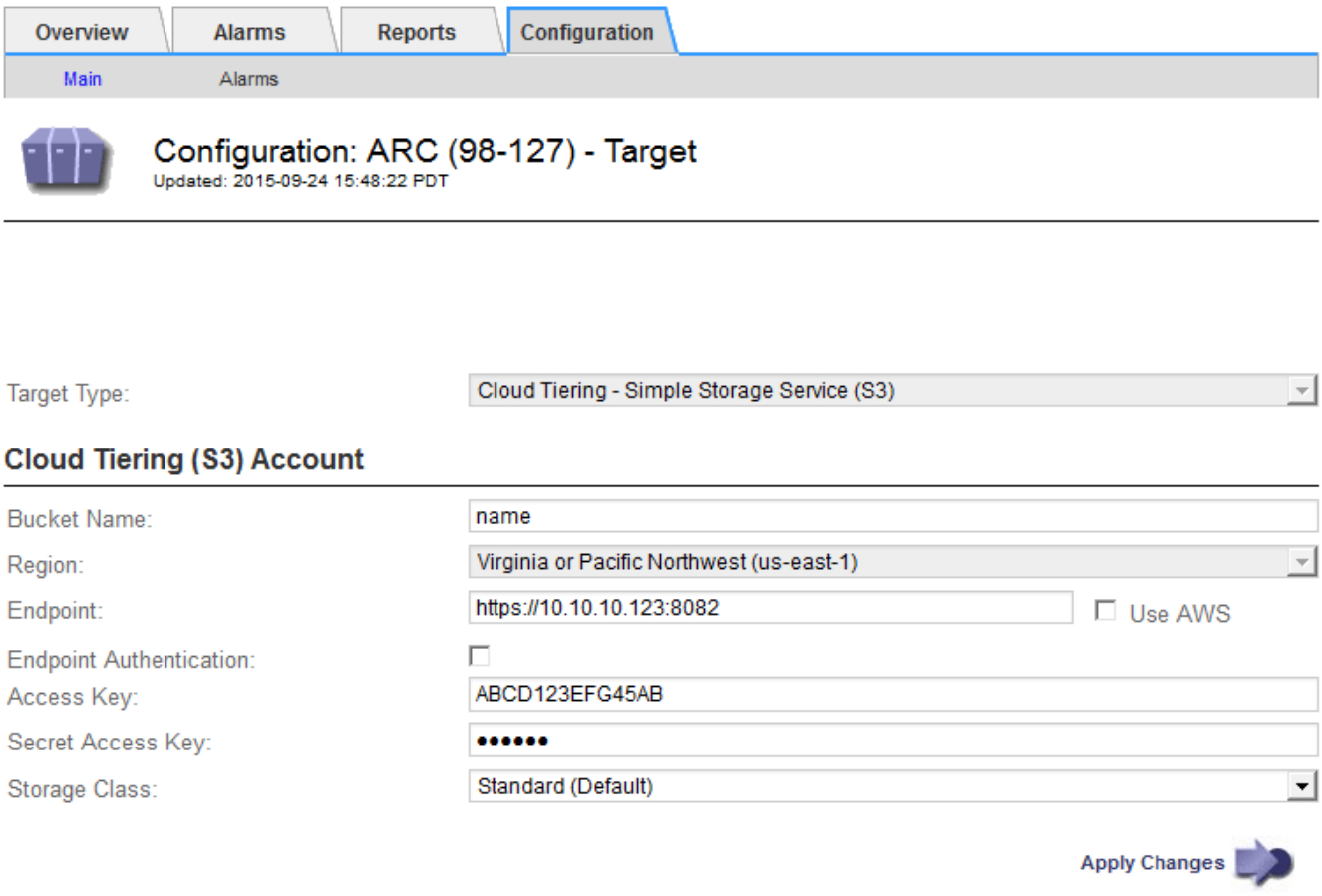
如果您当前正在使用具有 * 云分层 - 简单存储服务（ S3 ） * 选项的归档节点，请考虑将对象迁移到云存储池。请参见有关通过信息生命周期管理来管理对象的说明。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您必须已在目标归档存储系统上创建存储分段：
  - 此存储分段必须专用于一个归档节点。它不能由其他归档节点或其他应用程序使用。
  - 必须为存储分段选择适合您所在位置的区域。
  - 应在存储分段配置中暂停版本控制。
- 必须启用对象分段、并且最大分段大小必须小于或等于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** ARC/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是可信的，则可以取消选中此复选框，以便为目标外部归档存储系统禁用端点 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. 单击 * 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。

相关信息

"使用 ILM 管理对象"

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。

您需要的内容

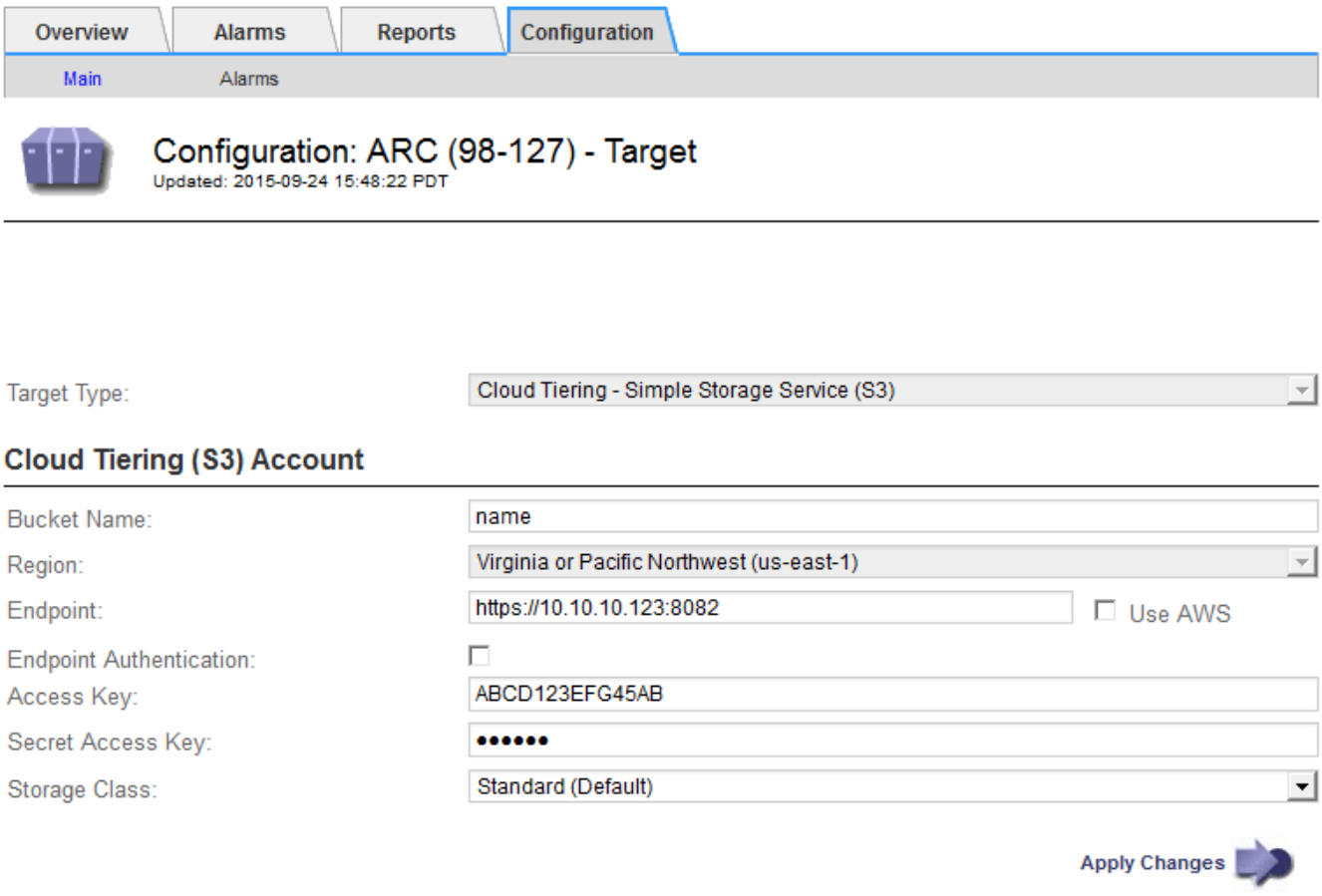
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

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。

   分段名称，区域和端点，使用 AWS 值，不能更改。

5. 单击 * 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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 必须配置归档节点。

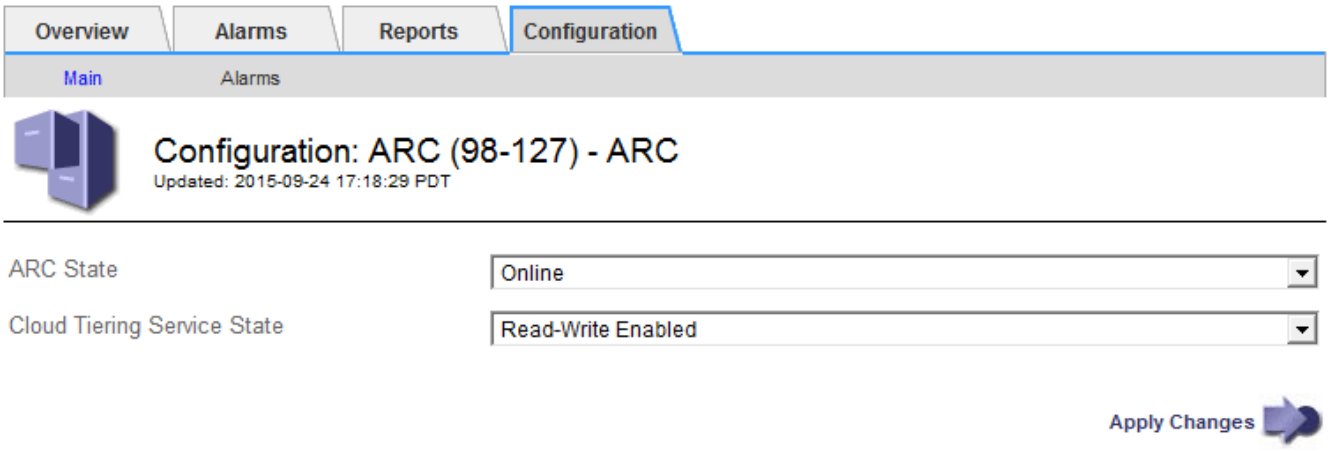
关于此任务

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. 单击 * 应用更改 * 。

重置**S3 API**连接的存储故障计数

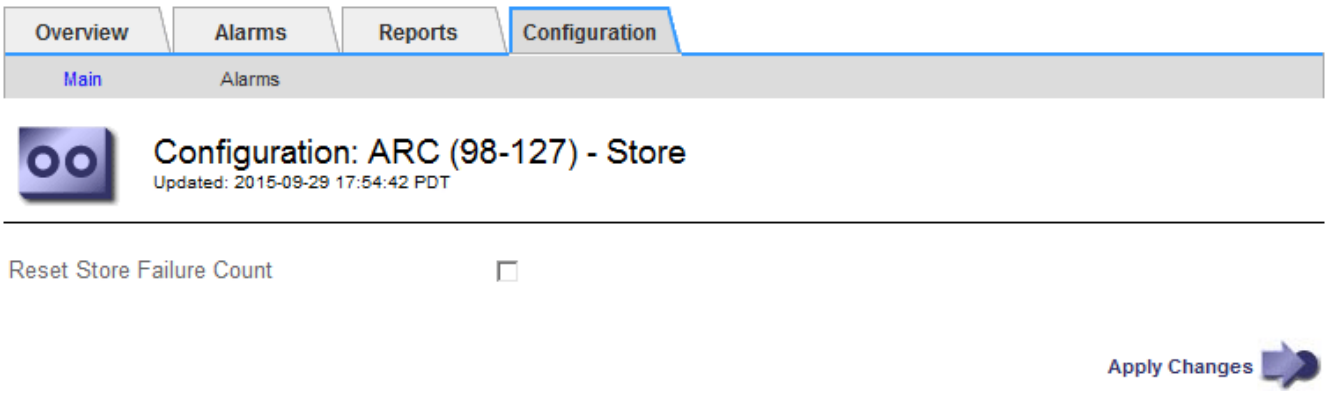
如果归档节点通过 S3 API 连接到归档存储系统，则可以重置存储故障计数，此计数可用于清除 ARVF （存储故障）警报。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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. 单击 * 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，请考虑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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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。

如果对象存储在云存储池中，则这些对象的副本也无法存储在 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。

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。

配置与**TSM**中间件的连接

在归档节点能够与 Tivoli Storage Manager （ TSM ）中间件进行通信之前，您必须配置多项设置。

您需要的内容

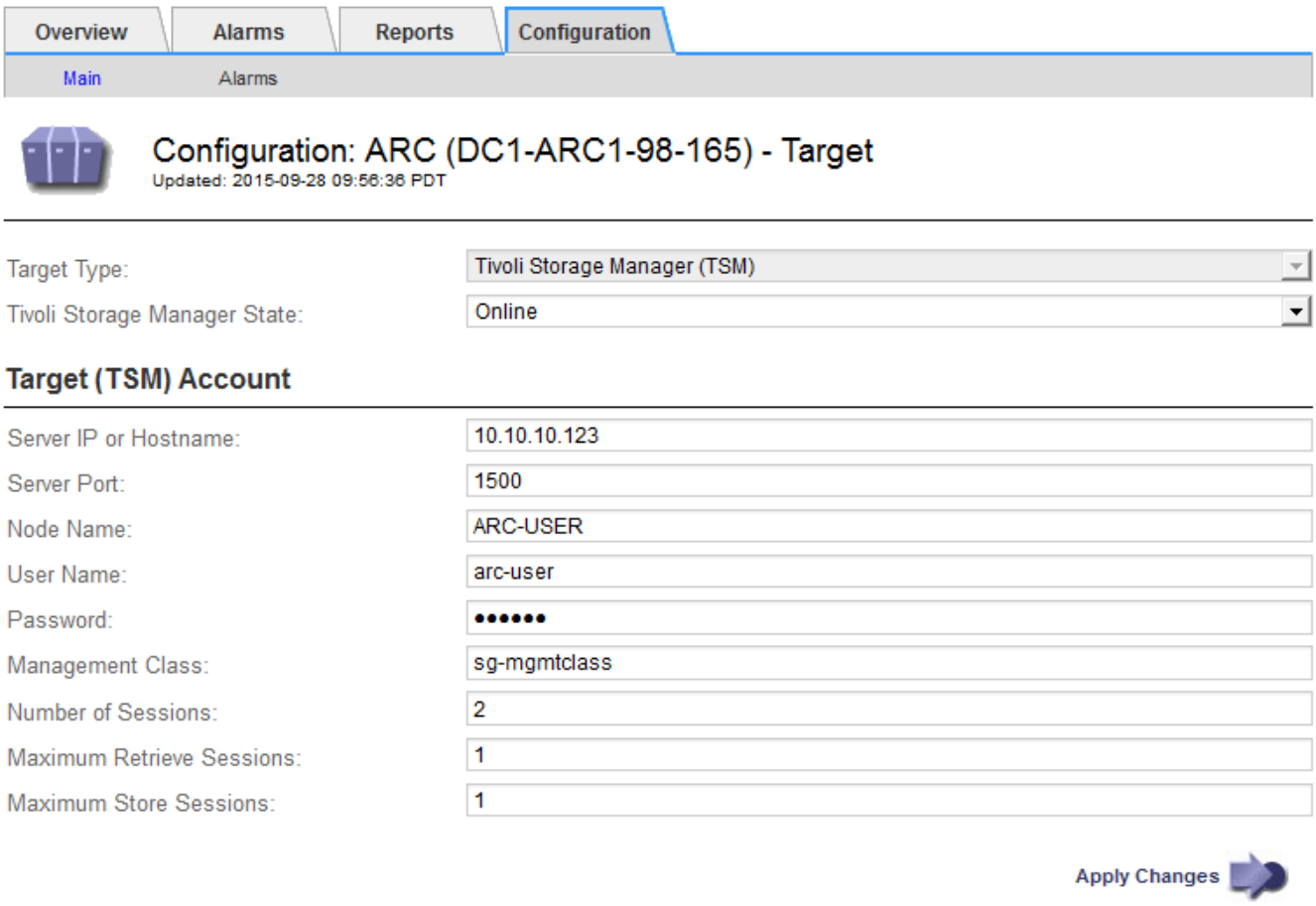
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

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. 单击 * 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。

您需要的内容

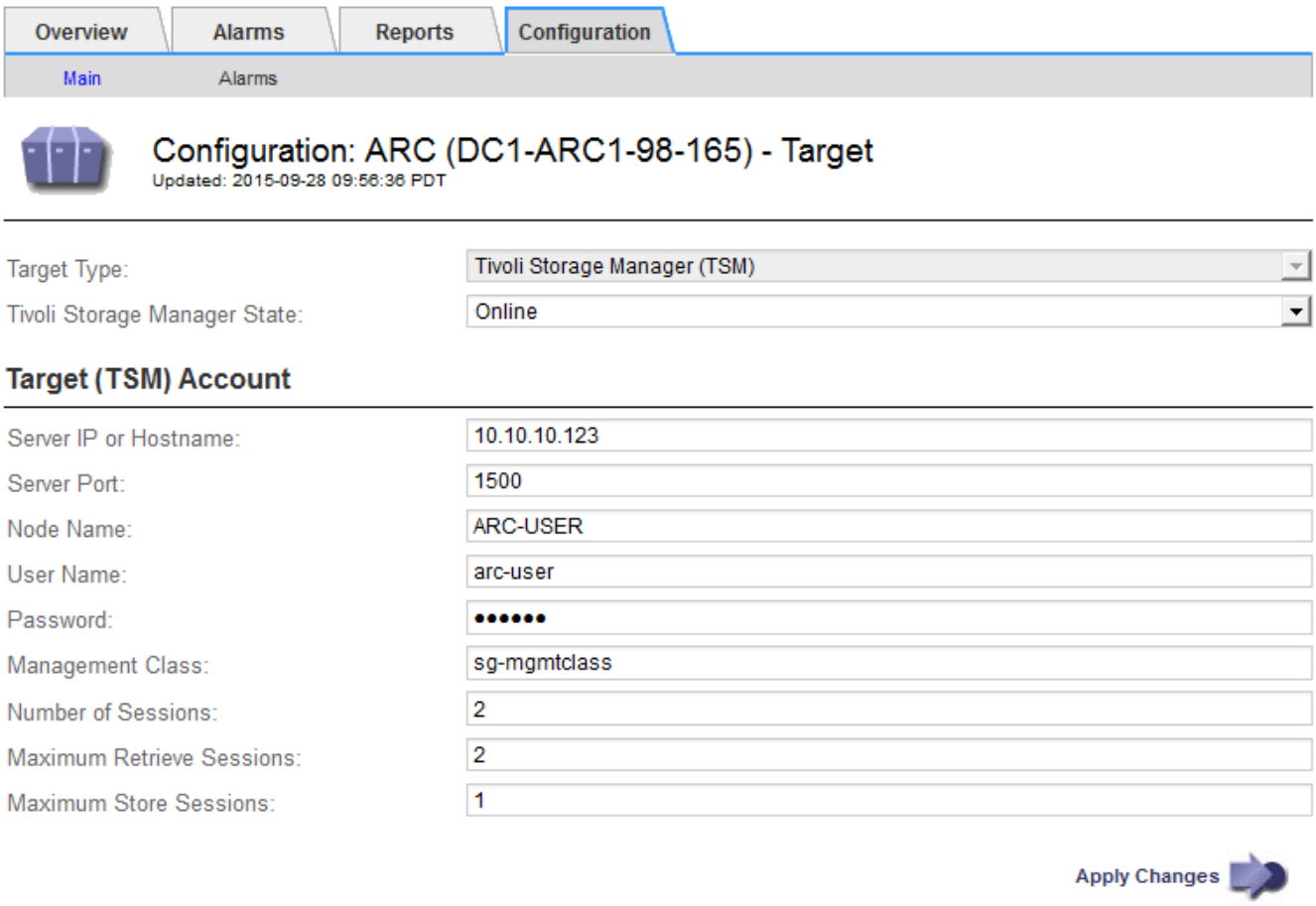
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

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. 单击 * 应用更改 * 。

配置**TSM**的归档状态和计数器

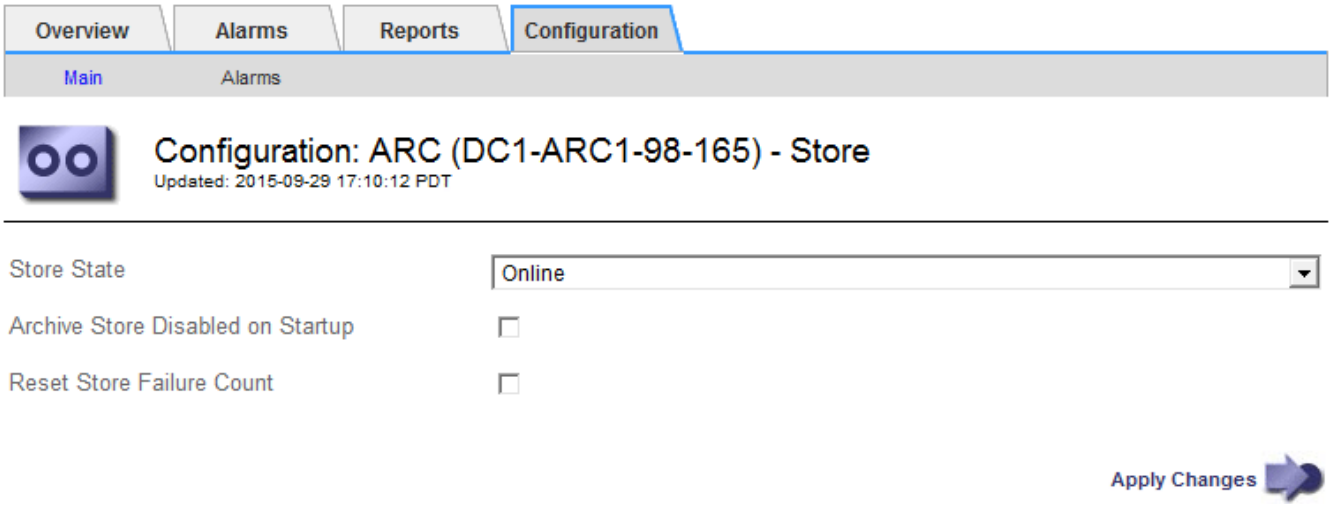
如果归档节点连接到 TSM 中间件服务器，则可以将归档节点的归档存储状态配置为联机或脱机。您还可以在归档节点首次启动时禁用归档存储，或者重置为关联警报跟踪的故障计数。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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. 单击 * 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。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。此内容无法写入 TSM 服务器管理的介质。如果发生这种情况，将触发警报。可以通过主动监控 TSM 服务器来避免这种情况。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

为了防止此ARC-Service向TSM服务器发送更多内容、您可以通过使其* ARC/**存储*组件脱机来使归档节点脱机。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. 单击 * 应用更改 * 。

在**TSM**中间件达到容量时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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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**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. 单击 * 应用更改 * 。

配置归档节点检索设置

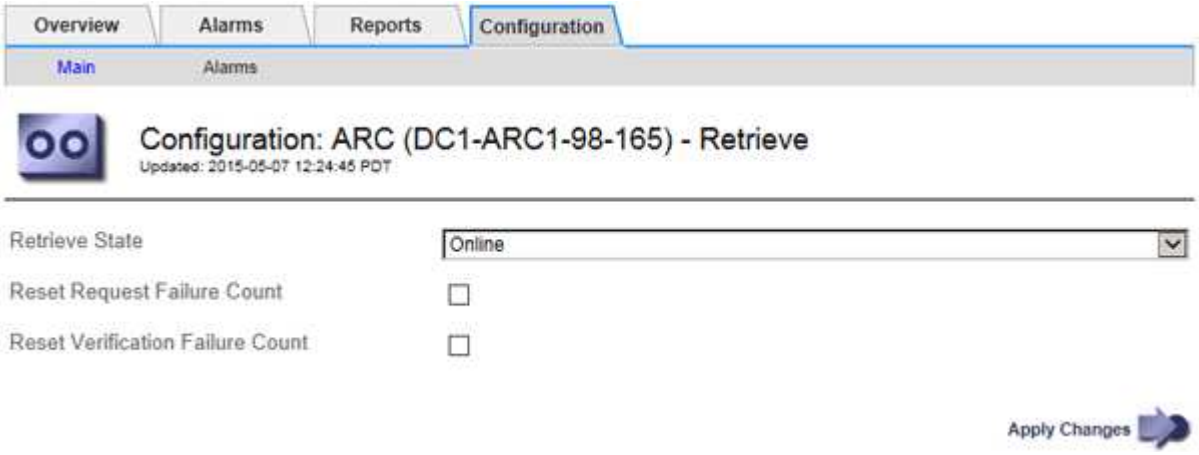
您可以配置归档节点的检索设置，将状态设置为联机或脱机，或者重置为关联警报跟踪的故障计数。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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的计数器。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已检索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. 单击 * 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。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须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，可以从应用程序中心服务检索对象数据，以便复制到 StorageGRID 系统中的其他位置，但不能将对象从其他系统位置复制到此应用程序中心服务。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 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，可以将对象数据复制到此应用程序中心服务以满足 ILM 规则的要求，但无法从应用程序中心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. 单击 * 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。

相关信息

"监控和放大；故障排除"

集成Tivoli Storage Manager

本节介绍将归档节点与Tivoli Storage Manager (TSM)服务器集成的最佳实践和设置信息、包括影响TSM服务器配置的归档节点操作详细信息。

- "归档节点配置和操作"
- "配置最佳实践"
- "正在完成归档节点设置"

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）。

归档节点不会使用 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。
- 归档节点软件不能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。

正在完成归档节点设置

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。

有关优化TSM检索和存储会话的详细信息、请参见有关管理归档存储的信息。

- "管理归档节点"

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

这些说明仅供您参考；它们并不是为了取代 TSM 文档，也不是为了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 dsmadc 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。在 TSM 服务器上为 MAXNUMMP 指定的数量必须至少与为归档节点的 * ARC* > * 目标 * > * 配置 * > * 主 * > * 最大存储会话 * 设置的值相同。 该值设置为 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. 如果您使用的不是现有管理类，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。

下一节将指导您了解并规划将大量数据迁移到 StorageGRID 系统。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"
- "确定已迁移数据的ILM策略"
- "迁移对操作的影响"
- "计划数据迁移"
- "监控数据迁移"
- "为迁移警报创建自定义通知"

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）中，请确保归档节点的存储具有足够的容量来容纳所迁移数据的预期卷。

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 系统的磁盘容量的详细信息、请参见有关监控StorageGRID 和对其进行故障排除的说明。

相关信息

"监控和放大；故障排除"

"管理存储节点"

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。

> 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。

相关信息

"使用 ILM 管理对象"

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，必须按照本章中的说明仔细管理数据迁移，以避免对日常系统操作造成影响，或者在极端情况下，在 StorageGRID 系统发生故障时使数据面临丢失风险。

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，以确保不超过各种属性值。

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。

相关信息

"监控数据迁移"

监控数据迁移

必须根据需要监控和调整数据迁移、以确保在所需时间内根据ILM策略放置数据。

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_* **Overview*** Main*。 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。

为迁移警报创建自定义通知

如果某些值超过建议的阈值、您可能希望StorageGRID 向负责监控迁移的系统管理员发送警报通知或警报(传统系统)通知。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。
- 您必须已为警报(或警报)通知配置电子邮件设置。

步骤

1. 为要在数据迁移期间监控的每个Prometheus指标或StorageGRID 属性创建自定义警报规则或全局自定义警报。

   警报将根据Prometheus指标值触发。根据属性值触发警报。有关详细信息、请参见StorageGRID 监控和故障排除说明。

2. 数据迁移完成后、禁用自定义警报规则或全局自定义警报。

   请注意、全局自定义警报会覆盖默认警报。

相关信息

"监控和放大；故障排除"

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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