管理StorageGRID 系统

StorageGRID 11.5

NetApp
April 11, 2024

目录

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 ：

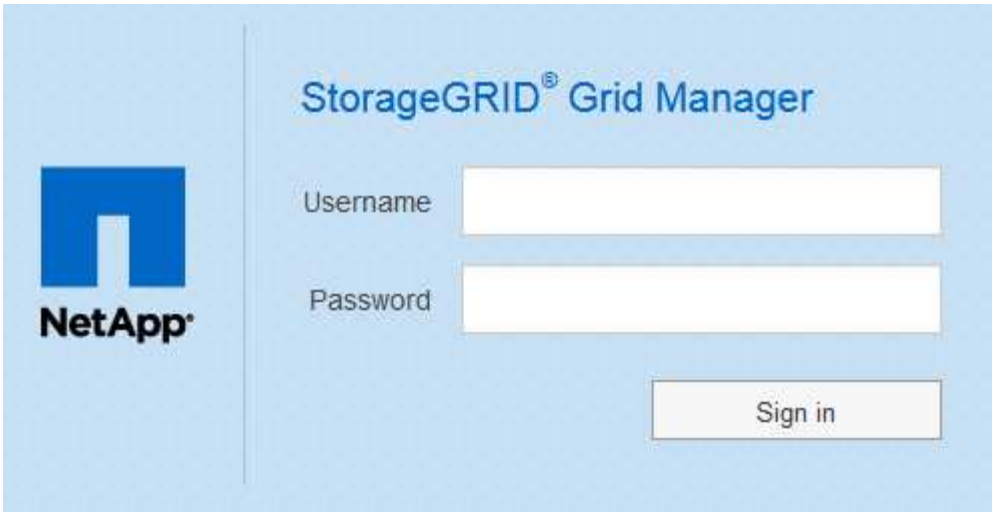
   `https://FQDN_or_Admin_Node_IP/`

   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：

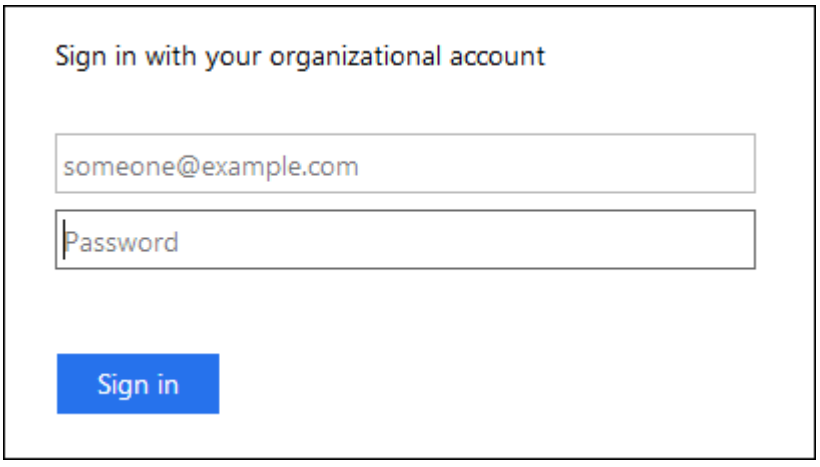
   `https://FQDN_or_Admin_Node_IP:port/`

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。

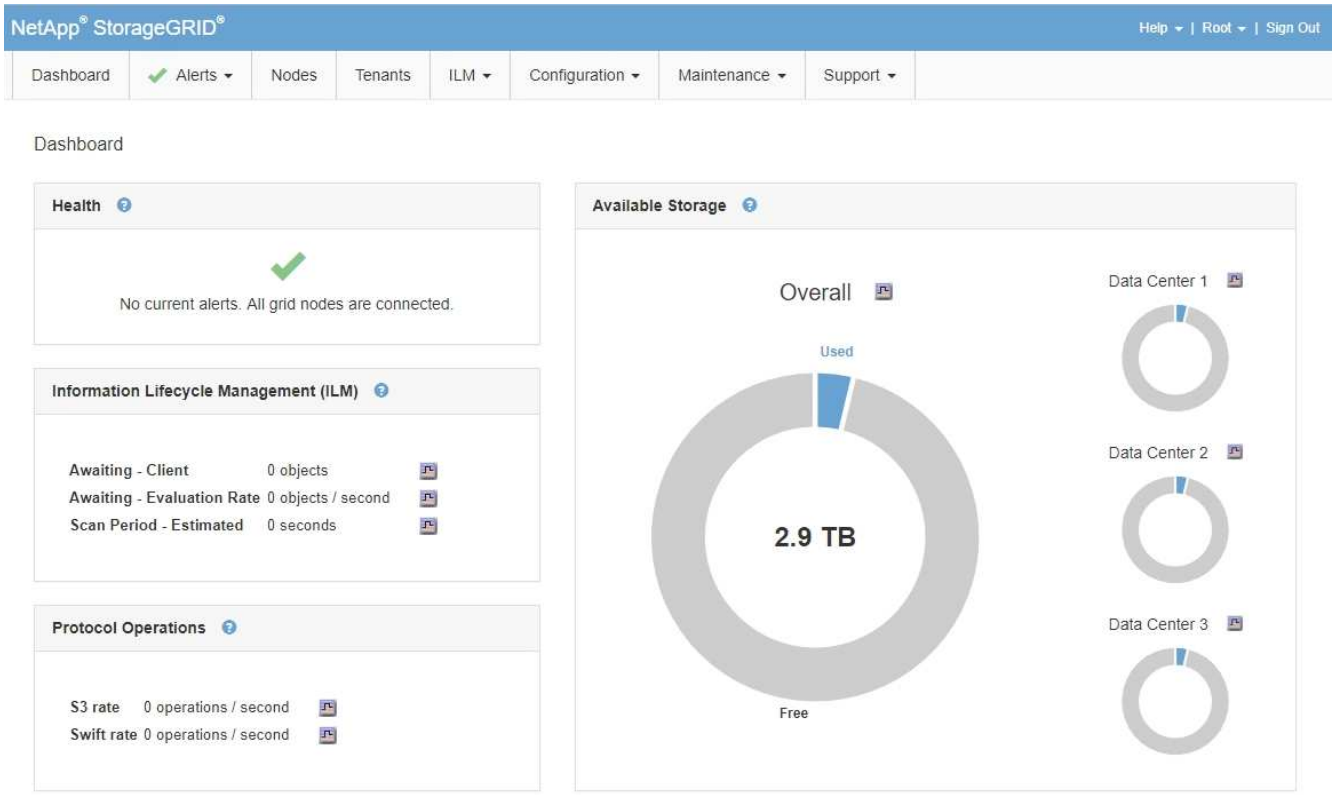
  ii. 在组织的 SSO 登录页面上输入标准 SSO 凭据。例如：



- 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"

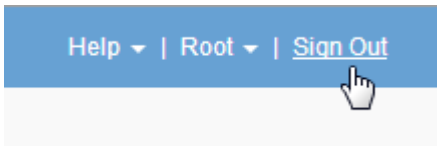
"监控和放大；故障排除"

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

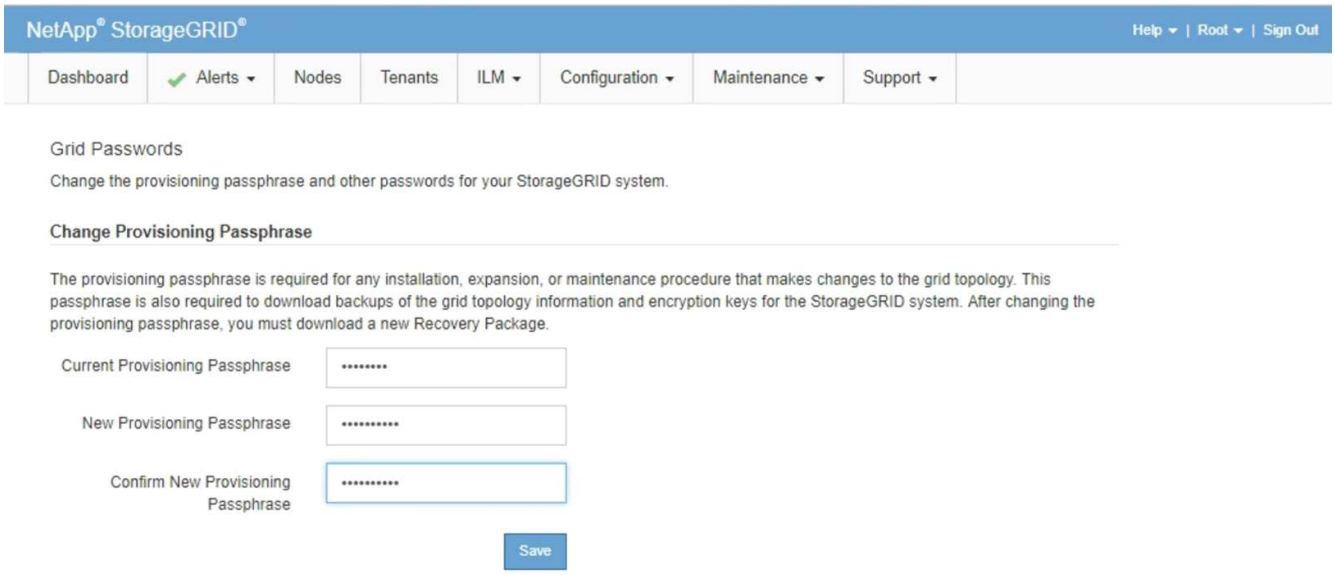
- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有维护或根访问权限。
- 您必须具有当前配置密码短语。

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*。

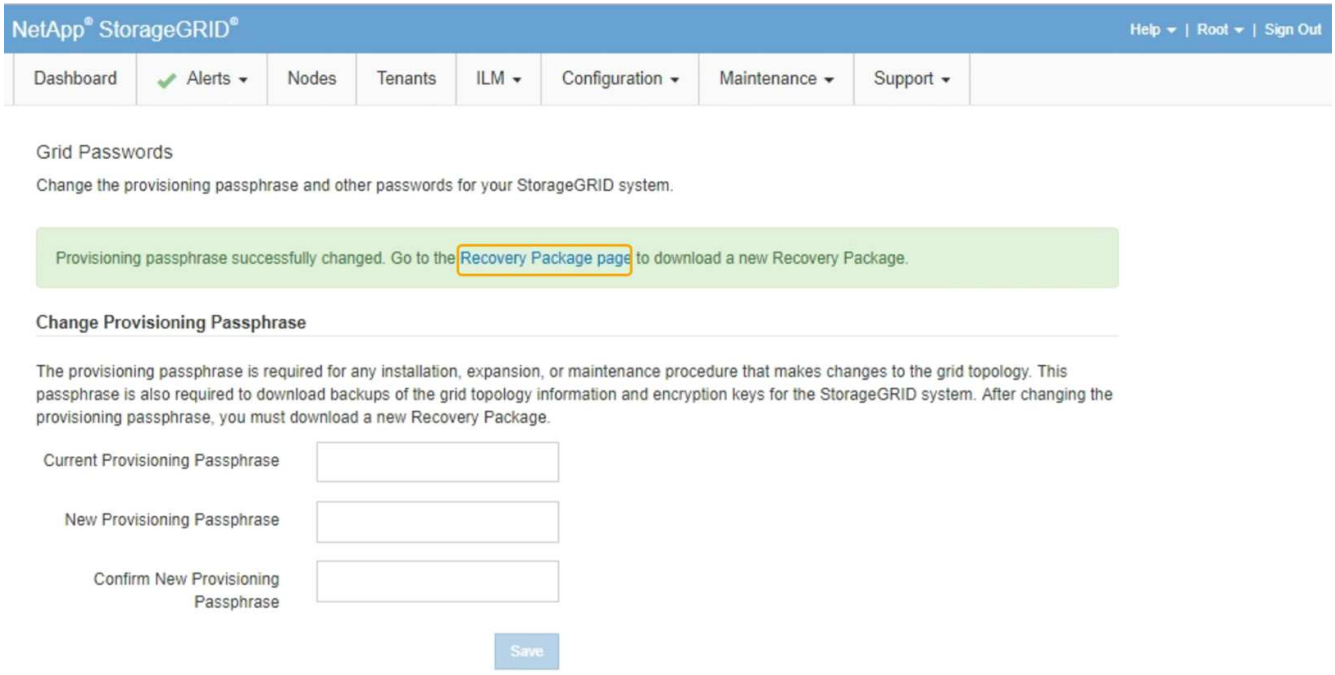


2. 输入当前配置密码短语。
3. 输入新的密码短语。密码短语必须至少包含8个字符、并且不超过32个字符。密码短语区分大小写。

   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 。

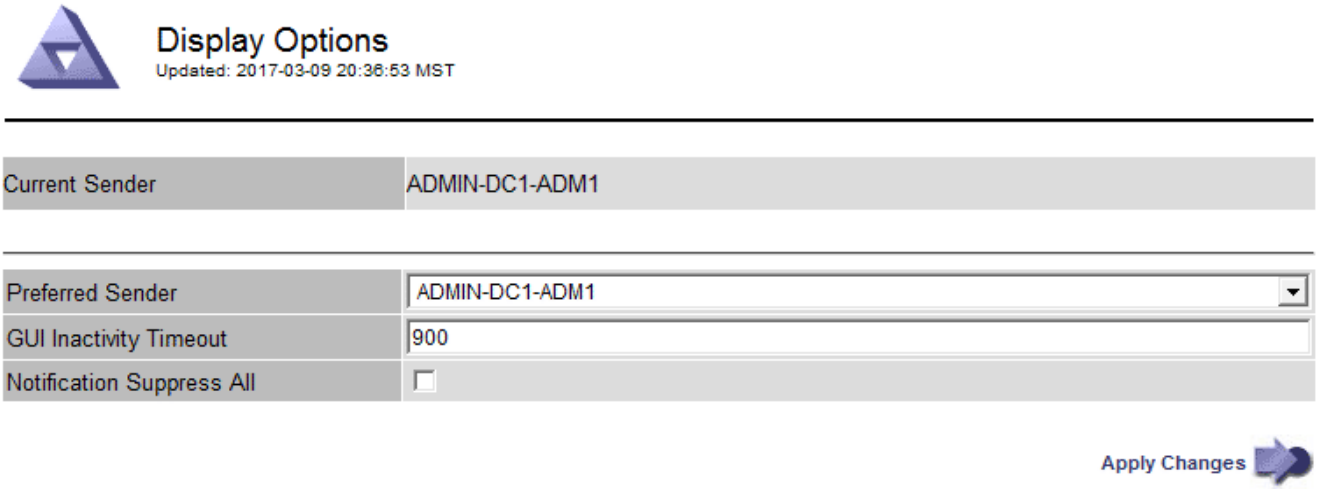
用户会话超时也可通过以下方式控制：

- 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。

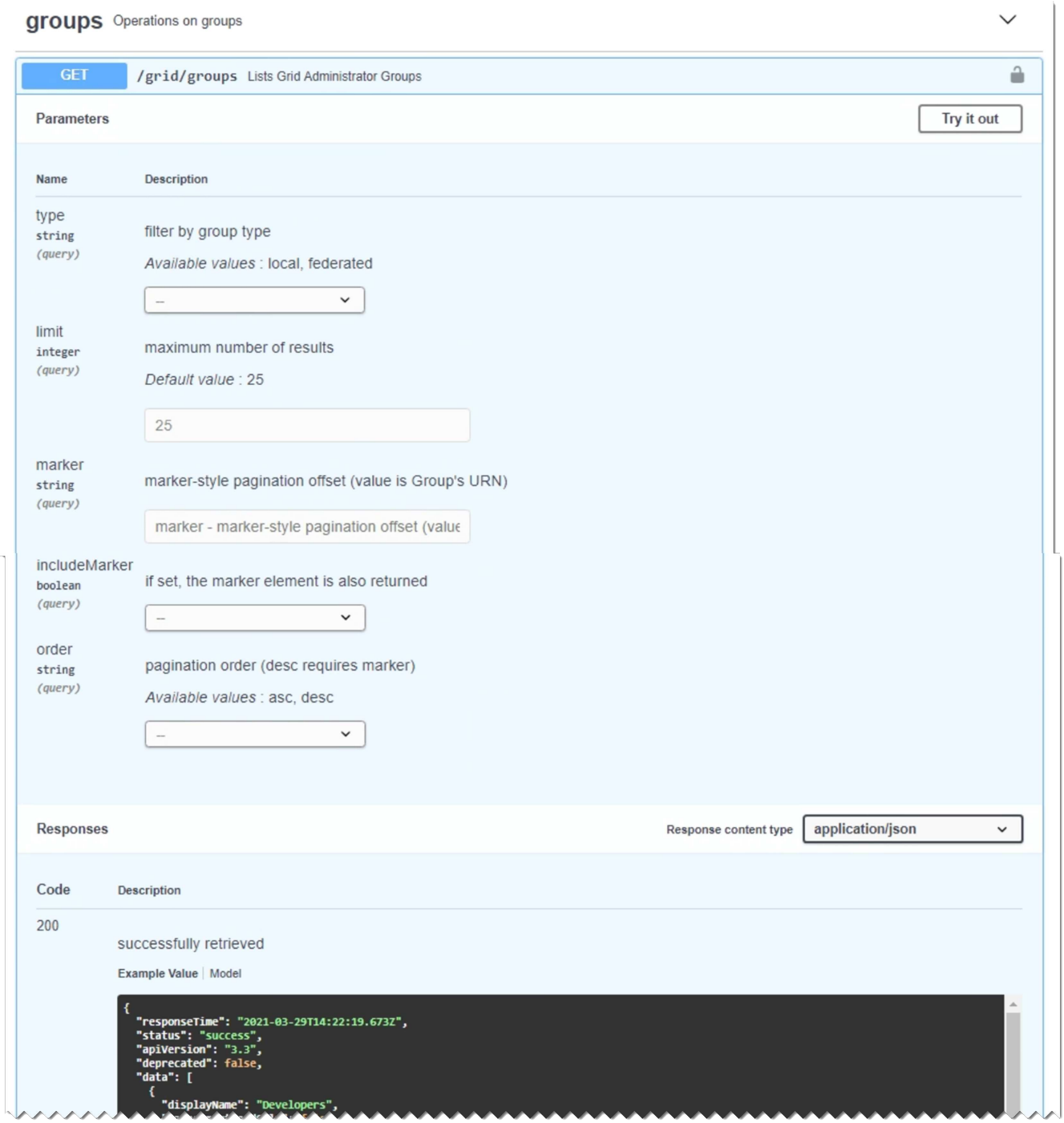
> 使用 API 文档网页执行的任何 API 操作均为实时操作。请注意，不要错误地创建，更新或删除配置数据或其他数据。

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 版本控制

网格管理 API 使用版本控制来支持无中断升级。

例如，此请求 URL 指定 API 版本 3 。

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

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

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

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

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

已过时的请求将通过以下方式标记为已弃用：

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

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

确定当前版本支持哪些API版本

请使用以下 API 请求返回受支持的 API 主要版本列表：

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

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。