



开始使用**Grid Manager** StorageGRID 11.7

NetApp
April 12, 2024

目录

- 开始使用Grid Manager..... 1
 - Web 浏览器要求..... 1
 - 登录到网格管理器..... 1
 - 注销 Grid Manager..... 7
 - 更改密码..... 7
 - 查看 StorageGRID 许可证信息..... 8
 - 更新 StorageGRID 许可证信息..... 9
 - 使用 API..... 9

开始使用Grid Manager

Web 浏览器要求

您必须使用受支持的 Web 浏览器。

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

您应将浏览器窗口设置为建议的宽度。

浏览器宽度	像素
最小值	1024
最佳	1280

登录到网格管理器

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

概述

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

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

连接到HA组

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

使用SSO

如果、则登录步骤略有不同 ["已配置单点登录\(SSO\)"](#)。

在第一个管理节点上登录到网格管理器

开始之前

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

`https://FQDN_or_Admin_Node_IP/`

您可以使用完全限定域名、管理节点的IP地址或管理节点HA组的虚拟IP地址。

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

`https://FQDN_or_Admin_Node_IP:port/`



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

步骤

1. 启动受支持的 Web 浏览器。
2. 在浏览器的地址栏中、输入网格管理器的URL。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。请参见 ["管理安全证书"](#)。
4. 登录到网格管理器。

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

未使用SSO

- a. 输入网格管理器的用户名和密码。
- b. 选择 * 登录 *。



The image shows the login interface for NetApp StorageGRID Grid Manager. At the top, the NetApp logo is followed by 'StorageGRID®' and 'Grid Manager' in a large font. Below this, there are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a vertical cursor. The 'Password' field has a grey border. Below the password field is a blue 'Sign in' button. At the bottom, there are three links: 'Tenant sign in', 'NetApp support', and 'NetApp.com'.

使用SSO

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



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. 在组织的 SSO 登录页面上输入标准 SSO 凭据。例如：

Sign in with your organizational account

Sign in

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

The image shows a web interface for NetApp StorageGRID. At the top, there is a logo consisting of a square icon followed by the text "NetApp StorageGRID®". Below the logo is the heading "Sign in". Underneath the heading, there is a section labeled "Recent" with a dropdown menu showing "Grid Manager". Below that is a section labeled "Account" with a text input field containing the number "0". At the bottom of the form is a blue button with the text "Sign in". Below the button, there is a link that says "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

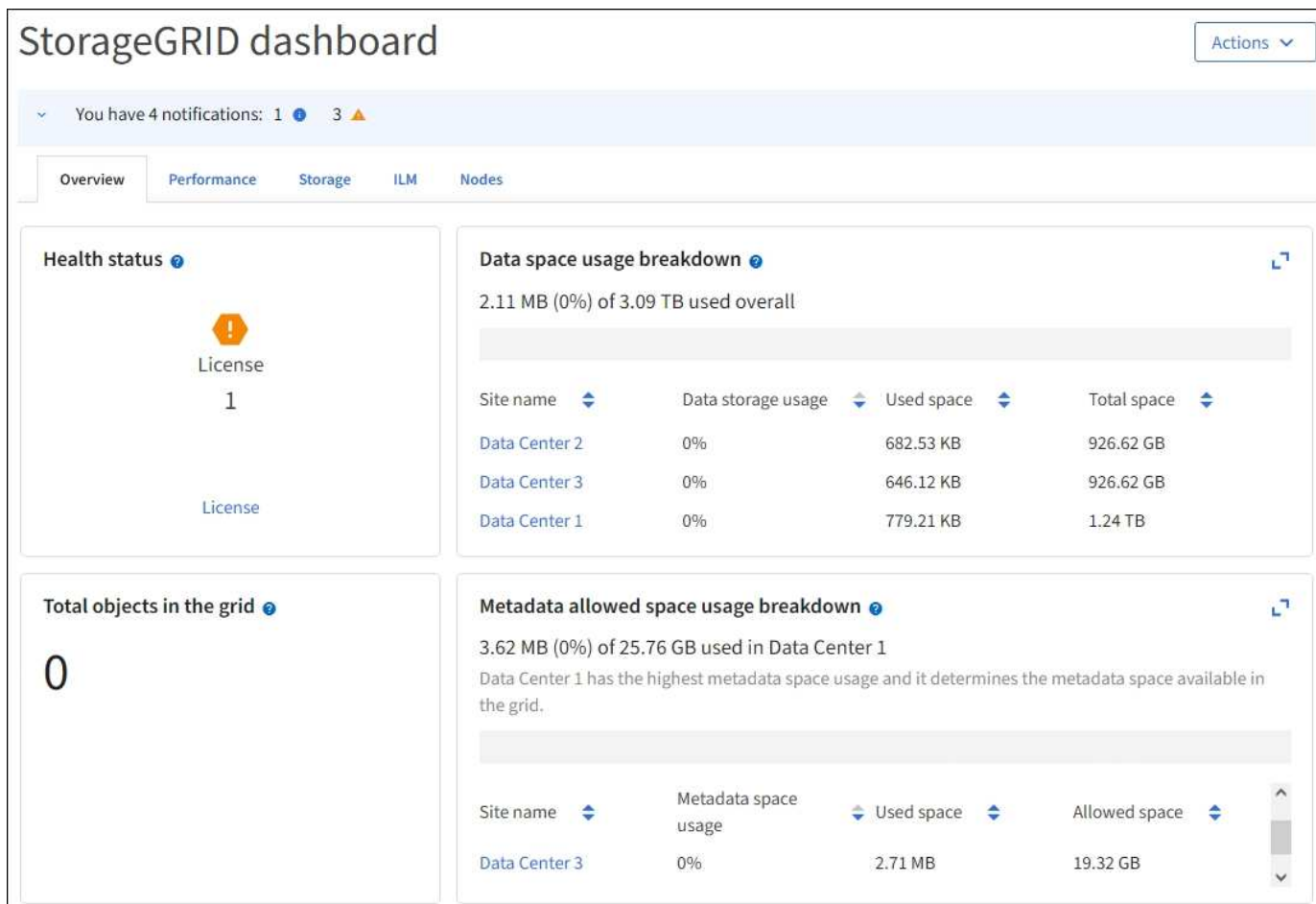
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. 选择 * 登录 *。
- iii. 在您组织的 SSO 登录页面上使用您的标准 SSO 凭据登录。

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



登录到其他管理节点

按照以下步骤登录到其他管理节点。

未使用SSO

步骤

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

使用SSO

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

步骤

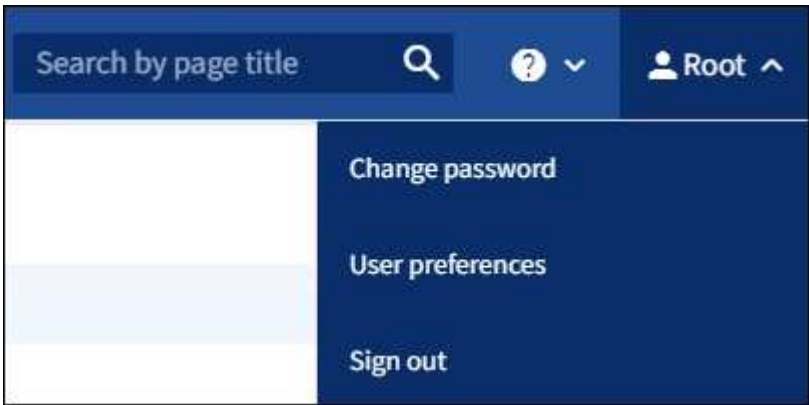
1. 在浏览器的地址栏中输入另一个管理节点的完全限定域名或IP地址。
2. 如果您的SSO会话已过期、请重新输入您的凭据。

注销 Grid Manager

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

步骤

1. 在右上角选择您的用户名。



2. 选择*注销*。

选项	Description
SSO 未使用	<p>您已从管理节点注销。</p> <p>此时将显示网格管理器登录页面。</p> <ul style="list-style-type: none">• 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	<p>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 。</p> <p>*注意： *如果启用了SSO、并且您还登录到租户管理器、则还必须登录"注销租户帐户" to "注销SSO"。</p>

更改密码

如果您是网格管理器的本地用户，则可以更改自己的密码。

开始之前

您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。

关于此任务

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

步骤

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

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

4. 重新输入新密码。
5. 选择 * 保存 *。

查看 StorageGRID 许可证信息

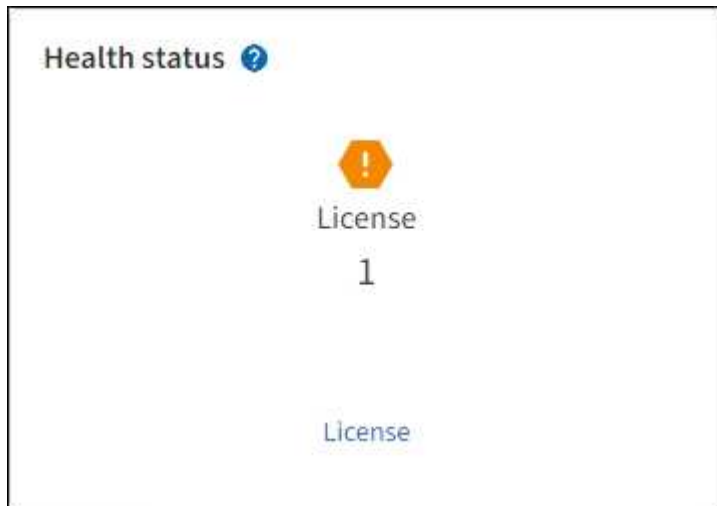
您可以根据需要查看 StorageGRID 系统的许可证信息，例如网格的最大存储容量。

开始之前

- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。

关于此任务

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



步骤

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

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

此日期是从当前许可证文件中读取的、如果您在获取许可证文件后延长或续订了支持服务合同、则此日期可能已过时。要更新此值、请参见 ["更新 StorageGRID 许可证信息"](#)。您还可以使用Active IQ 查看实际合同结束日期。

- 许可证文本文件的内容



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

更新 StorageGRID 许可证信息

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

开始之前

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

步骤

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

此时将验证并显示新许可证文件。

4. 选择 * 保存 *。

使用 API

使用网格管理 API

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

顶级资源

网格管理 API 可提供以下顶级资源：

- /grid: 访问权限仅限于Grid Manager用户、并且取决于配置的组权限。
- /org: 只有属于租户帐户的本地或联合LDAP组的用户才能访问。有关详细信息，请参见 ["使用租户帐户"](#)。
- /private: 访问权限仅限于Grid Manager用户、并且取决于配置的组权限。专用 API 如有更改，恕不另行通知。StorageGRID 私有端点也会忽略此请求的 API 版本。

问题描述 **API** 请求

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

Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。

开始之前

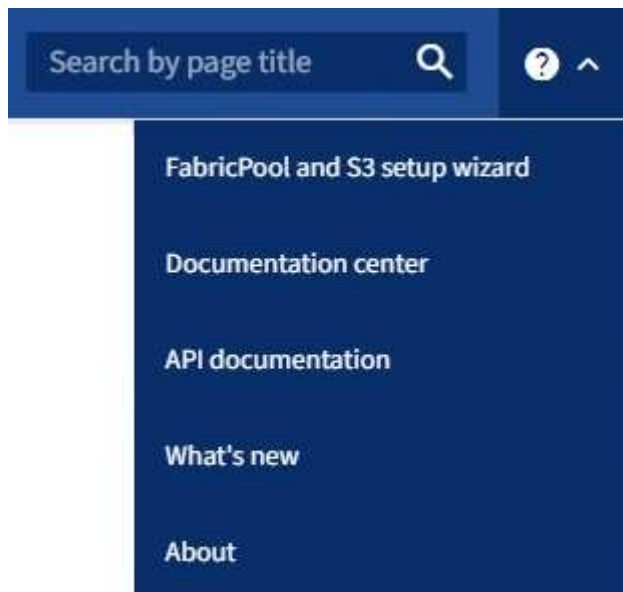
- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您具有特定的访问权限。



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

步骤

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



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

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

3. 选择所需的操作。

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

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

GET `/grid/groups` Lists Grid Administrator Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated <div>— ▼</div>
limit integer (query)	maximum number of results Default value : 25 <div>25</div>
marker string (query)	marker-style pagination offset (value is Group's URN) <div>marker - marker-style pagination offset (value</div>
includeMarker boolean (query)	if set, the marker element is also returned <div>— ▼</div>
order string (query)	pagination order (desc requires marker) Available values : asc, desc <div>— ▼</div>

Responses Response content type `application/json` ▼

Code	Description
200	successfully retrieved <div>Example Value Model</div> <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

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

网络管理 API 操作

网络管理 API 将可用操作组织到以下部分中。



此列表仅包含公有 API 中可用的操作。

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

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



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

有关提高身份验证安全性的信息，请参阅“防止跨站点请求伪造”。

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

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



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

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

网络管理 API 版本控制

网络管理 API 使用版本控制来支持无中断升级。

例如, 此请求 URL 指定 API 版本 3 。

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

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

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

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



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

已过时的请求将通过以下方式标记为已弃用：

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

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

确定当前版本支持哪些 **API** 版本

请使用以下 API 请求返回受支持的 API 主要版本列表：

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

指定请求的 **API** 版本

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

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

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

防止跨站点请求伪造（**CSRF**）

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

API 客户端可以选择在登录时是否启用此功能。

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

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

要启用此功能、请设置 `csrfToken` 参数设置为 `true` 身份验证期间。默认值为 `false`。

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

如果为 `true`、则为 `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：`AccountCsrfToken` 表单编码的请求正文参数。

有关其他示例和详细信息，请参见联机 API 文档。



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

如果启用了单点登录，请使用 **API**

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

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

如果启用了单点登录，请登录到 **API**

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

开始之前

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

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

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

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



示例 cURL 工作流不会保护密码不会被其他用户看到。

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

步骤

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

出现提示时，输入以下参数的值：

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

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

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

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

3. 如果要使用 `curl` 请求，请使用以下操作步骤。
 - a. 声明登录所需的变量。

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



要访问网格管理API、请使用0作为 TENANTACCOUNTID。

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

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

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

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

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

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

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

- d. 从 AD FS 获取包含客户端请求 ID 的完整 URL 。

一种方法是使用上一响应中的 URL 请求登录表单。

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

此响应包括客户端请求 ID：

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&client-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=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS 返回 302 重定向，并在标题中显示追加信息。



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

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%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
XFxVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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="PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. 保存 SAMLResponse 在隐藏字段中：

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

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

证令牌请求。

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

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

响应包括身份验证令牌。

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

- a. 将响应中的身份验证令牌另存为 MYTOKEN。

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

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

如果启用了单点登录，请注销 **API**

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

关于此任务

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

步骤

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

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

返回注销 URL：

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

2. 保存注销 URL。

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

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

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

返回 302 响应。此重定向位置不适用于纯 API 注销。

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

4. 删除 StorageGRID 承载令牌。

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

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

答 204 No Content 响应指示用户现在已注销。

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

如果启用了单点登录，请使用 **API (Azure)**

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

如果启用了 **Azure** 单点登录，请登录到 **API**

如果您使用 Azure 作为 SSO 身份提供程序，则以下说明适用

开始之前

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

关于此任务

要获取身份验证令牌，可以使用以下示例脚本：

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

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

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

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

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

步骤

1. 安装所需的依赖关系，如下所示：

- a. 安装 Node.js （请参见 "<https://nodejs.org/en/download/>"）。
- b. 安装所需的 Node.js 模块（ puppeteer 和 jsdom ）：

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

2. 将 Python 脚本传递给 Python 解释器以运行此脚本。

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

3. 出现提示时，输入以下参数的值（或使用参数传递这些值）：

- 用于登录到 Azure 的 SSO 电子邮件地址

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

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

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

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



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

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

如果启用了单点登录，请使用 **API (PingFederate)**

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

如果启用了单点登录，请登录到 **API**

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

开始之前

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

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

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

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



示例 cURL 工作流不会保护密码不会被其他用户看到。

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

步骤

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

出现提示时，输入以下参数的值：

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

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

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

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

3. 如果要使用 `curl` 请求，请使用以下操作步骤。
 - a. 声明登录所需的变量。

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



要访问网格管理API、请使用0作为 `TENANTACCOUNTID`。

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

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

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

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

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

c. 保存 SAMLRequest 从响应中获取、以便在后续命令中使用。

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

d. 导出响应和 cookie ，并对响应执行回显：

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

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

e. 导出 "pf.adapterId" 值，并对响应执行回显：

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

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

f. 导出 "href" 值（删除后斜杠 /），并对响应执行回显：

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

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

g. 导出 "act" 值:

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

h. 发送 Cookie 以及凭据:

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

i. 保存 SAMLResponse 在隐藏字段中:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

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

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

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

响应包括身份验证令牌。

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

a. 将响应中的身份验证令牌另存为 MYTOKEN。

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

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

如果启用了单点登录，请注销 **API**

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

关于此任务

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

步骤

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

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

返回注销 URL：

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

2. 保存注销 URL。

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

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

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

返回 302 响应。此重定向位置不适用于纯 API 注销。

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

4. 删除 StorageGRID 承载令牌。

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

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

答 204 No Content 响应指示用户现在已注销。

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

使用 API 停用功能

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

关于此任务

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

要了解此功能的有用程度，请考虑以下情形：

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

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

步骤

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

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

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

重新激活已停用的功能

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



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

步骤

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

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

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



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

```
{ "grid": { "alarmAcknowledgment": true } }
```

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。