



使用网格管理API

StorageGRID

NetApp
October 03, 2025

目录

- 使用网格管理API 1
 - 顶级资源 1
 - 网格管理 API 操作 1
 - 发出API请求 3
 - 网格管理 API 版本控制 5
 - 确定当前版本支持哪些API版本 5
 - 为请求指定API版本 6
 - 防止跨站点请求伪造(CSRF) 6
 - 如果启用了单点登录、则使用API 7
 - 如果启用了单点登录、请登录到API 7
 - 如果启用了单点登录、则从API中注销 12

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-history** —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。
- ***deactivated-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。

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 Example Value Model <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、您可以单击*型号*来了解每个字段的要求。
- 单击 * 试用 *。
- 提供所需的任何参数，或根据需要修改请求正文。
- 单击 * 执行 *。
- 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。

```
python3 /tmp/storagegrid-ssoauth.py
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-af0b-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` 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=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

- e. 保存响应中的客户端请求 ID。

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

- f. 将您的凭据发送到上一响应中的表单操作。

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

AD FS 返回 302 重定向，并在标题中显示追加信息。



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

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTOMwFIZfhh...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。


```
{
  "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://ads.example.com/ads/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
```

版权信息

版权所有 © 2025 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。