



使用租户管理器 StorageGRID 11.5

NetApp
April 11, 2024

目录

使用租户管理器	1
使用StorageGRID 租户帐户	1
Web 浏览器要求	2
登录到租户管理器	3
注销租户管理器	5
了解租户管理器信息板	6
了解租户管理API	9

使用租户管理器

租户管理器允许您管理 StorageGRID 租户帐户的所有方面。

您可以使用租户管理器监控租户帐户的存储使用情况，并通过身份联合或创建本地组 and 用户来管理用户。对于 S3 租户帐户，您还可以管理 S3 密钥，管理 S3 存储分段以及配置平台服务。

使用StorageGRID 租户帐户

租户帐户允许您使用简单存储服务（S3） REST API 或 Swift REST API 在 StorageGRID 系统中存储和检索对象。

每个租户帐户都有自己的联合或本地组，用户，S3 分段或 Swift 容器以及对象。

也可以使用租户帐户按不同的实体隔离存储的对象。例如，以下任一使用情形均可使用多个租户帐户：

- * 企业用例：* 如果在企业中使用 StorageGRID 系统，则网格的对象存储可能会被组织中的不同部门隔离。例如，可能存在营销部门，客户支持部门，人力资源部门等的租户帐户。



如果使用 S3 客户端协议，则还可以使用 S3 分段和分段策略在企业中的各个部门之间隔离对象。您无需创建单独的租户帐户。请参见有关实施 S3 客户端应用程序的说明。

- * 服务提供商用例：* 如果服务提供商正在使用 StorageGRID 系统，则网格的对象存储可能会被租用该存储的不同实体分隔。例如，可能存在公司 A，公司 B，公司 C 等的租户帐户。

创建租户帐户

租户帐户由 StorageGRID 网络管理员使用网络管理器创建。创建租户帐户时，网络管理委员会会指定以下信息：

- 租户的显示名称（租户的帐户 ID 会自动分配，不能更改）。
- 租户帐户是使用 S3 还是 Swift。
- 对于 S3 租户帐户：是否允许租户帐户使用平台服务。如果允许使用平台服务，则必须对网格进行配置，以支持使用这些服务。
- （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。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。

此外，如果 S3 租户帐户需要符合法规要求，网络管理员可以为 StorageGRID 系统启用 S3 对象锁定设置。启用 S3 对象锁定后，所有 S3 租户帐户均可创建和管理合规的存储分段。

配置S3租户

创建 S3 租户帐户后，您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）或创建本地组 and 用户

- 管理 S3 访问密钥
- 创建和管理 S3 存储分段，包括合规存储分段
- 使用平台服务（如果已启用）
- 监控存储使用情况



虽然您可以使用租户管理器创建和管理 S3 存储分段，但您必须具有 S3 访问密钥，并使用 S3 REST API 载入和管理对象。

配置Swift租户

创建 Swift 租户帐户后，具有 root 访问权限的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 and 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

["管理 StorageGRID"](#)

["使用 S3"](#)

["使用 Swift"](#)

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

登录到租户管理器

您可以通过在支持的 Web 浏览器的地址栏中输入租户的 URL 来访问租户管理器。

您需要的内容

- 您必须拥有登录凭据。
- 您必须具有网格管理员提供的用于访问租户管理器的 URL。URL 将类似于以下示例之一：

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

此 URL 始终包含用于访问管理节点的完全限定域名（FQDN）或 IP 地址，也可以包括端口号，20 位租户帐户 ID 或这两者。

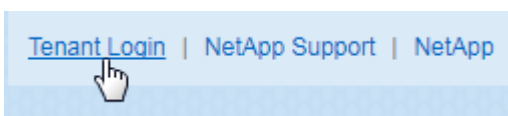
- 如果 URL 不包含租户的 20 位帐户 ID，则必须具有此帐户 ID。
- 您必须使用受支持的 Web 浏览器。
- 必须在 Web 浏览器中启用 Cookie。
- 您必须具有特定的访问权限。

步骤

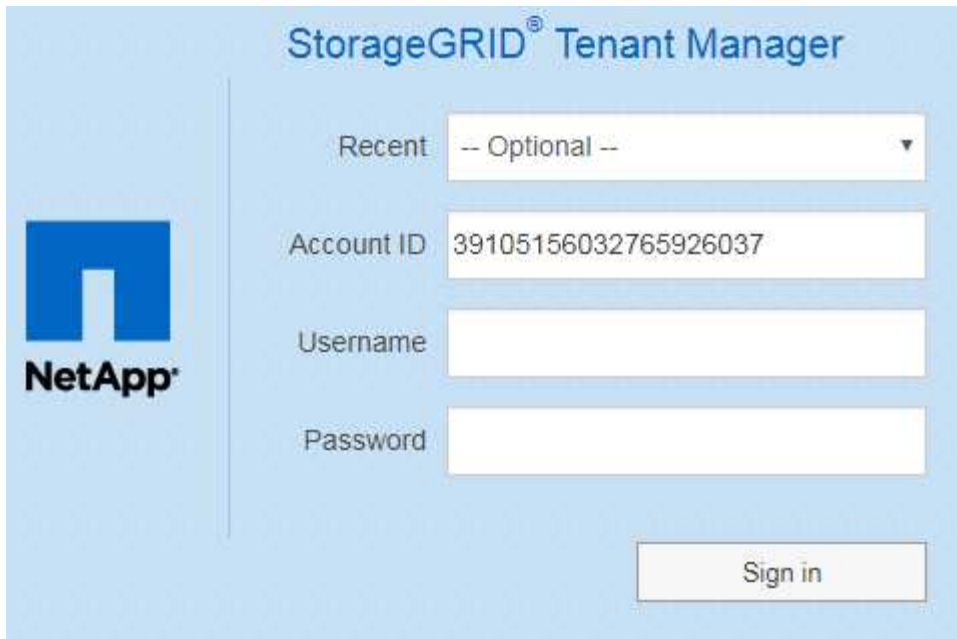
1. 启动受支持的 Web 浏览器。
2. 在浏览器的地址栏中，输入用于访问租户管理器的 URL。
3. 如果系统提示您显示安全警报，请使用浏览器的安装向导安装证书。
4. 登录到租户管理器。

您看到的登录屏幕取决于您输入的 URL 以及您的组织是否使用单点登录（SSO）。您将看到以下屏幕之一：

- 网格管理器登录页面。单击右上角的 * 租户登录 * 链接。



- 租户管理器登录页面。* 帐户 ID * 字段可能已完成，如下所示。

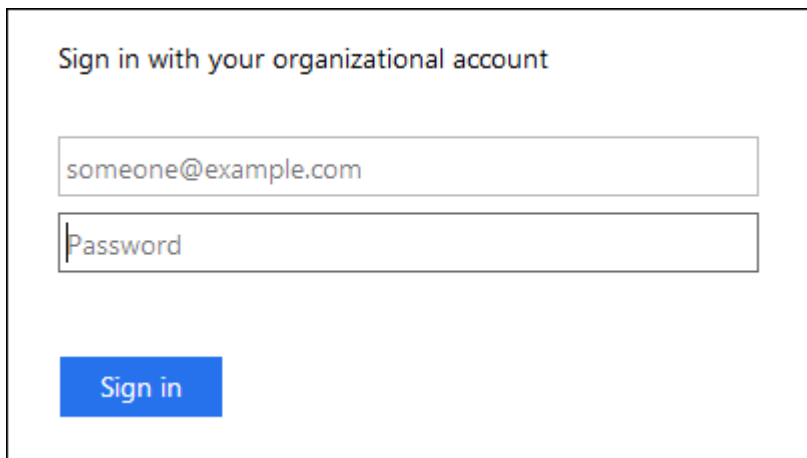


The image shows the StorageGRID Tenant Manager login page. On the left is the NetApp logo. The main area has a light blue background with the title 'StorageGRID® Tenant Manager'. Below the title is a 'Recent' dropdown menu with the text '-- Optional --'. Below that is an 'Account ID' field containing the value '39105156032765926037'. Below the Account ID are 'Username' and 'Password' input fields. At the bottom right is a 'Sign in' button.

- i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。
- ii. 输入用户名和密码。
- iii. 单击 * 登录 * 。

此时将显示租户管理器信息板。

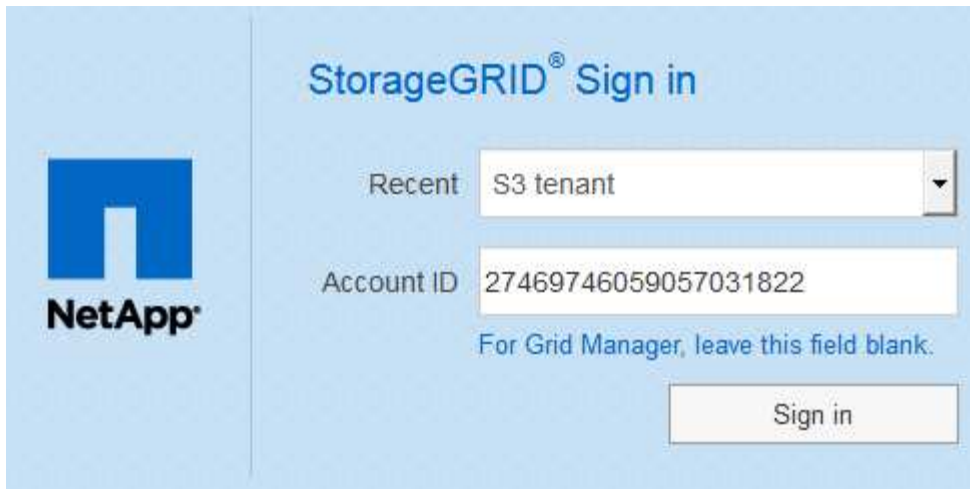
- 如果在网络上启用了 SSO ，则为您所在组织的 SSO 页面。例如：



The image shows an SSO login form. It has a title 'Sign in with your organizational account'. Below the title are two input fields: the first contains the email address 'someone@example.com' and the second is labeled 'Password'. At the bottom left is a blue 'Sign in' button.

输入标准 SSO 凭据，然后单击 * 登录 * 。

- 租户管理器 SSO 登录页面。



- i. 如果未显示租户的 20 位帐户 ID ，请选择最近帐户列表中显示的租户帐户名称，或者输入帐户 ID 。
- ii. 单击 * 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。

此时将显示租户管理器信息板。

5. 如果您从其他人收到初始密码，请更改密码以保护您的帐户。选择 *。 username_ * > * 更改密码 * 。



如果为 StorageGRID 系统启用了 SSO ，则无法从租户管理器更改密码。

相关信息

["管理 StorageGRID"](#)

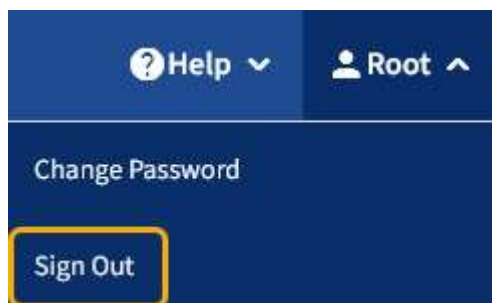
["Web 浏览器要求"](#)

注销租户管理器

使用租户管理器后，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用户名下拉列表。



2. 选择用户名，然后选择 * 注销 * 。

选项	Description
SSO 未使用	您已从管理节点注销。此时将显示租户管理器登录页面。 • 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。您刚刚访问的租户帐户的名称将在 * 近期帐户 * 下拉列表中列为默认名称，并显示租户的 * 帐户 ID*。 *注意：*如果启用了SSO、并且您还登录到网格管理器、则还必须注销网格管理器才能注销SSO。

了解租户管理器信息板

租户管理器信息板概述了租户帐户的配置以及租户分段（S3）或容器（Swift）中的对象所使用的空间量。如果租户有配额，信息板将显示配额的已用量和剩余量。如果存在与租户帐户相关的任何错误，则这些错误将显示在信息板上。



" 已用空间 " 值是估计值。这些估计值受载入时间，网络连接和节点状态的影响。

上传对象后，信息板类似于以下示例：

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups










1 User
View users

Storage usage

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining




Bucket name	Space used	Number of objects
 Bucket-15	969.2 GB	913,425
 Bucket-04	937.2 GB	576,806
 Bucket-13	815.2 GB	957,389
 Bucket-06	812.5 GB	193,843
 Bucket-10	473.9 GB	583,245
 Bucket-03	403.2 GB	981,226
 Bucket-07	362.5 GB	420,726
 Bucket-05	294.4 GB	785,190
 8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details

Name Human Resources
ID 4955 9096 9804 4285 4354

 View the instructions for Tenant Manager.

[Go to documentation](#) 

租户帐户摘要

信息板顶部包含以下信息：

- 已配置的分段或容器，组和用户的数量
- 已配置的平台服务端点数量（如果有）

您可以选择这些链接来查看详细信息。

信息板右侧包含以下信息：

- 租户的对象总数。
对于 S3 帐户，如果尚未载入任何对象，并且您具有 root 访问权限，则会显示入门准则，而不是对象总数。
- 租户帐户名称和ID。
- 指向StorageGRID 文档的链接。

存储和配额使用量

存储使用情况面板包含以下信息：

- 租户的对象数据量。



此值表示已上传的对象数据总量，不表示用于存储这些对象及其元数据副本的空间。

- 如果设置了配额，则表示可用于对象数据的总空间量以及剩余空间量和百分比。配额限制了可载入的对象数据量。



配额利用率基于内部估计值，在某些情况下可能会超出此值。例如，当租户开始上传对象时，StorageGRID 会检查配额，如果租户超过配额，则会拒绝新的载入。但是，在确定是否超过配额时，StorageGRID 不会考虑当前上传的大小。如果删除对象，则可能会暂时阻止租户上传新对象，直到重新计算配额利用率为止。配额利用率计算可能需要 10 分钟或更长时间。

- 一个条形图，表示最大分段或容器的相对大小。

您可以将光标置于任何图表区块上方，以查看该分段或容器占用的总空间。



- 要与条形图相对应，需要列出最大的分段或容器，包括对象数据总量以及每个分段或容器的对象数量。

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

如果租户具有九个以上的分段或容器，则所有其他分段或容器将合并到列表底部的一个条目中。


配额使用情况警报

如果已在网格管理器中启用配额使用情况警报，则在配额不足或超过配额时，这些警报将显示在租户管理器中，如下所示：

如果已使用租户配额的 90% 或更多，则会触发 * 租户配额使用量高 * 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。

 Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

如果超过配额，则无法上传新对象。


 The quota has been met. You cannot upload new objects.



要查看其他详细信息以及管理警报规则和通知，请参见有关监控 StorageGRID 和对其进行故障排除的说明。

端点错误

如果您已使用网格管理器配置一个或多个端点以用于平台服务，则如果在过去七天内发生任何端点错误，则租户管理器信息板将显示警报。

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

要查看有关端点错误的详细信息，请选择端点以显示端点页面。

相关信息

["解决平台服务端点错误"](#)

["监控和放大；故障排除"](#)

了解租户管理API

您可以使用租户管理 REST API 执行系统管理任务，而不是使用租户管理器用户界面。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。

租户管理API使用Swagger开源API平台。Swagger 提供了一个直观的用户界面，支持开发人员和非开发人员与 API 进行交互。Swagger 用户界面提供了每个 API 操作的完整详细信息和文档。

要访问租户管理 API 的 Swagger 文档，请执行以下操作：

步骤

1. 登录到租户管理器。
2. 从租户管理器标题中选择*帮助*>* API文档*。

API 操作

租户管理 API 将可用的 API 操作组织到以下部分中：

- * 帐户 * - 对当前租户帐户执行的操作，包括获取存储使用情况信息。
- * 身份验证 * —执行用户会话身份验证的操作。

租户管理 API 支持不承载令牌身份验证方案。对于租户登录、您可以在身份验证请求的JSON正文中提供用户名、密码和帐户ID (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 (" 授权: 承载令牌 ") 。

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" 。



如果为 StorageGRID 系统启用了单点登录 (SSO) ，则必须执行不同的步骤进行身份验证。请参见管理StorageGRID 的说明中的"如果启用了单点登录、请参见`对API进行身份验证`"。

- **config** —与租户管理 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产品版本和主要 API 版本。
- * 容器 * —对 S3 存储分段或 Swift 容器执行的操作如下：

协议	权限允许
S3	<ul style="list-style-type: none"> • 创建合规和不合规的存储分段 • 修改原有合规性设置 • 为对对象执行的操作设置一致性控制 • 创建、更新和删除存储分段的CORS配置 • 启用和禁用对象的上次访问时间更新 • 管理平台服务的配置设置、包括CloudMirror复制、通知和搜索集成(元数据通知) • 正在删除空存储分段
Swift	设置用于容器的一致性级别

- **"*deactivated-features *** - 用于查看可能已停用的功能的操作 "。
- * 端点 * —用于管理端点的操作。通过端点， S3 存储分段可以使用外部服务进行 StorageGRID CloudMirror 复制，通知或搜索集成。
- * 组 * —用于管理本地租户组和从外部身份源检索联合租户组的操作。
- **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。
- * 区域 * - 用于确定已为 StorageGRID 系统配置哪些区域的操作。
- * S3 * —用于管理租户用户 S3 访问密钥的操作。
- * s3-object-lock*—用于确定如何为StorageGRID 系统配置全局S3对象锁定(合规性)的操作。
- * 用户 * —用于查看和管理租户用户的操作。

操作详细信息

展开每个 API 操作时，您可以看到其 HTTP 操作，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。

groups Operations on groups

GET

/org/groups Lists Tenant User Groups

Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses

Response content type

application/json

Code Description

200

Example Value Model

```
{  
  "responseTime": "2018-02-01T16:22:31.066Z",  
  "status": "success",  
  "apiVersion": "2.1"
```

发出API请求



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. 单击HTTP操作可查看请求详细信息。
2. 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。
3. 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。
4. 单击 * 试用 *。

5. 提供所需的任何参数，或根据需要修改请求正文。
6. 单击 * 执行 *。
7. 查看响应代码以确定请求是否成功。

相关信息

["防止跨站点请求伪造\(CSRF\)"](#)

["管理 StorageGRID"](#)

租户管理 API 版本控制

租户管理 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租户管理 API。但是，在将 StorageGRID 升级到新功能版本后，您仍可访问至少一个 StorageGRID 功能版本的旧版 API。

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

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、

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。