



管理租户组

StorageGRID 11.8

NetApp
March 19, 2024

目录

管理租户组	1
为 S3 租户创建组	1
为 Swift 租户创建组	3
租户管理权限	5
管理组	6

管理租户组

为 S3 租户创建组

您可以通过导入联合组或创建本地组来管理 S3 用户组的权限。

开始之前

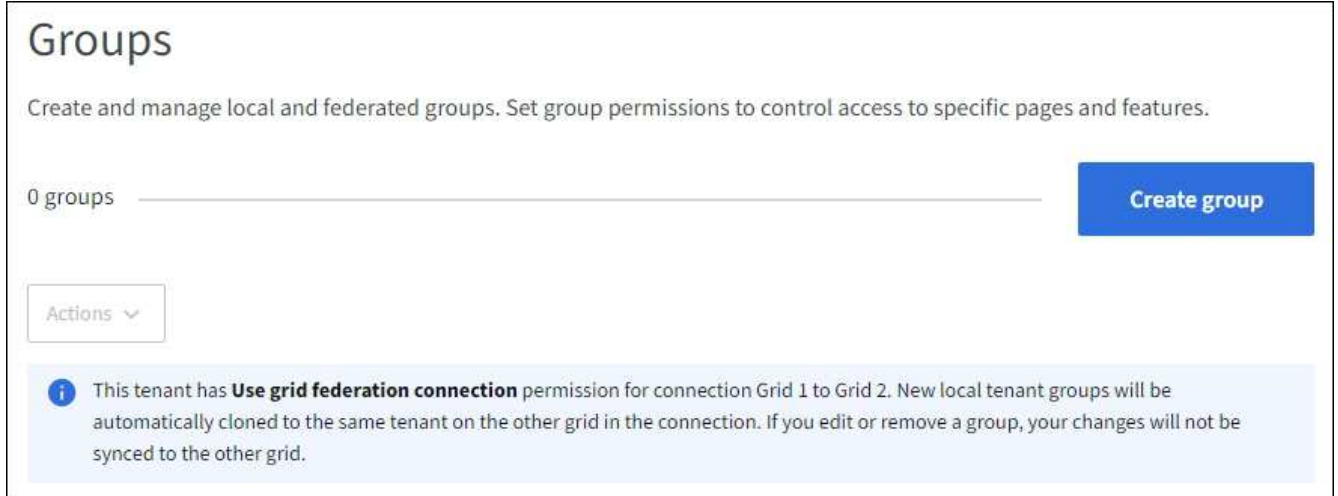
- 您将使用登录到租户管理器 ["支持的 Web 浏览器"](#)。
- 您属于具有的用户组 ["root访问权限"](#)。
- 如果您计划导入联盟组、则需要 ["已配置身份联合"](#)，并且已配置的身份源中已存在联盟组。
- 如果您的租户帐户具有[*使用网格联合连接*](#)权限、则您已查看的工作流和注意事项 ["克隆租户组 and 用户"](#)，您将登录到租户的源网格。

访问创建组向导

首先、访问创建组向导。

步骤

1. 选择 [* 访问管理 *](#) > [* 组 *](#)。
2. 如果您的租户帐户具有[*使用网格联合连接*](#)权限、请确认显示蓝色横幅、指示在此网格上创建的新组将克隆到连接中另一网格上的同一租户。如果未显示此横幅、则您可能已登录到租户的目标网格。



3. 选择 [* 创建组 *](#)。

选择组类型

您可以创建本地组或导入联合组。

步骤

1. 选择 [* 本地组 *](#) 选项卡以创建本地组，或者选择 [* 联合组 *](#) 选项卡以从先前配置的身份源导入组。

如果为 StorageGRID 系统启用了单点登录（SSO），则属于本地组的用户将无法登录到租户管理器，但他

们可以根据组权限使用客户端应用程序管理租户的资源。

2. 输入组的名称。

- * 本地组 *：输入显示名称和唯一名称。您可以稍后编辑显示名称。



如果您的租户帐户具有*使用网格联合连接*权限、并且目标网格上的租户已存在相同的*唯一名称*、则会发生克隆错误。

- * 联合组 *：输入唯一名称。对于Active Directory、唯一名称是与关联的名称 sAMAccountName 属性。对于OpenLDAP、唯一名称是与关联的名称 uid 属性。

3. 选择 * 继续 *。

管理组权限

组权限控制用户可在租户管理器和租户管理API中执行的任务。

步骤

1. 对于*Access mode*，请选择以下选项之一：

- 读写(默认)：用户可以登录到租户管理器并管理租户配置。
- * 只读 *：用户只能查看设置和功能。他们无法在租户管理器或租户管理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。

2. 为此组选择一个或多个权限。

请参见 "[租户管理权限](#)"。

3. 选择 * 继续 *。

设置S3组策略

组策略用于确定用户将拥有哪些S3访问权限。

步骤

1. 选择要用于此组的策略。

组策略	Description
无S3访问	默认。此组中的用户无权访问S3资源、除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
只读访问	此组中的用户对S3资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据，元数据和标记。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。

组策略	Description
完全访问	此组中的用户对S3资源(包括分段)具有完全访问权限。选择此选项后,完全访问组策略的JSON字符串将显示在文本框中。您无法编辑此字符串。
勒索软件防护	此示例策略适用场景此租户的所有分段。此组中的用户可以执行常见操作、但无法从启用了对象版本控制的分段中永久删除对象。 具有*管理所有存储分段*权限的租户管理器用户可以覆盖此组策略。将"管理所有分段"权限限制为受信任用户、并在可用时使用多因素身份验证(Multi-FactorAuthentication、MFA)。
自定义	组中的用户将被授予您在文本框中指定的权限。

2. 如果选择 * 自定义 * , 请输入组策略。每个组策略的大小限制为 5 , 120 字节。您必须输入有效的 JSON 格式字符串。

有关组策略的详细信息、包括语言语法和示例、请参见 ["组策略示例"](#)。

3. 如果要创建本地组, 请选择 * 继续 * 。如果要创建联合组, 请选择 * 创建组 * 和 * 完成 * 。

添加用户 (仅限本地组)

您可以保存组而不添加用户、也可以选择添加任何已存在的本地用户。



如果您的租户帐户具有*使用网格联合连接*权限、则在源网格上创建本地组时选择的任何用户在克隆到目标网格时不会包括在其中。因此、请勿在创建组时选择用户。而是在创建用户时选择组。

步骤

1. 或者, 为此组选择一个或多个本地用户。
2. 选择 * 创建组 * 和 * 完成 * 。

您创建的组将显示在组列表中。

如果您的租户帐户具有*使用网格联合连接*权限、而您位于租户的源网格上、则新组将克隆到租户的目标网格。成功*显示为组详细信息页面的"概述"部分中的*克隆状态。

为 Swift 租户创建组

您可以通过导入联合组或创建本地组来管理 Swift 租户帐户的访问权限。至少有一个组必须具有 Swift 管理员权限, 这是管理 Swift 租户帐户的容器和对象所必需的。



对Swift客户端应用程序的支持已弃用、将在未来版本中删除。

开始之前

- 您将使用登录到租户管理器 ["支持的 Web 浏览器"](#)。
- 您属于具有的用户组 ["root访问权限"](#)。
- 如果您计划导入联盟组、则需要 ["已配置身份联合"](#)，并且已配置的身份源中已存在联盟组。

访问创建组向导

步骤

首先、访问创建组向导。

1. 选择 [* 访问管理 *](#) > [* 组 *](#)。
2. 选择 [* 创建组 *](#)。

选择组类型

您可以创建本地组或导入联合组。

步骤

1. 选择 [* 本地组 *](#) 选项卡以创建本地组，或者选择 [* 联合组 *](#) 选项卡以从先前配置的身份源导入组。

如果为 StorageGRID 系统启用了单点登录（SSO），则属于本地组的用户将无法登录到租户管理器，但他们可以根据组权限使用客户端应用程序管理租户的资源。

2. 输入组的名称。
 - [* 本地组 *](#)：输入显示名称和唯一名称。您可以稍后编辑显示名称。
 - [* 联合组 *](#)：输入唯一名称。对于Active Directory、唯一名称是与关联的名称 `sAMAccountName` 属性。对于OpenLDAP、唯一名称是与关联的名称 `uid` 属性。
3. 选择 [* 继续 *](#)。

管理组权限

组权限控制用户可在租户管理器和租户管理API中执行的任务。

步骤

1. 对于[*Access mode*](#)，请选择以下选项之一：
 - [读写\(默认\)](#)：用户可以登录到租户管理器并管理租户配置。
 - [* 只读 *](#)：用户只能查看设置和功能。他们无法在租户管理器或租户管理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。

2. 如果组用户需要登录到租户管理器或租户管理API、请选中[* root访问*](#)复选框。
3. 选择 [* 继续 *](#)。

设置Swift组策略

Swift用户需要管理员权限才能通过Swift REST API的身份验证来创建容器和导入对象。

1. 如果组用户需要使用Swift REST API来管理容器和对象、请选中* Swift administrator*复选框。
2. 如果要创建本地组，请选择 * 继续 * 。如果要创建联合组，请选择 * 创建组 * 和 * 完成 * 。

添加用户（仅限本地组）

您可以保存组而不添加用户、也可以选择添加任何已存在的本地用户。

步骤

1. 或者，为此组选择一个或多个本地用户。

如果尚未创建本地用户、则可以在用户页面上将此组添加到用户。请参见 ["管理本地用户"](#)。

2. 选择 * 创建组 * 和 * 完成 * 。

您创建的组将显示在组列表中。

租户管理权限

在创建租户组之前，请考虑要分配给该组的权限。租户管理权限用于确定用户可以使用租户管理器或租户管理 API 执行的任务。一个用户可以属于一个或多个组。如果用户属于多个组，则权限是累积的。

要登录到租户管理器或使用租户管理 API ，用户必须属于至少具有一个权限的组。所有可以登录的用户均可执行以下任务：

- 查看信息板
- 更改自己的密码（适用于本地用户）

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。

您可以为组分配以下权限。请注意， S3 租户和 Swift 租户具有不同的组权限。

权限	Description	详细信息
root 访问权限	提供对租户管理器和租户管理 API 的完全访问权限。	Swift用户必须具有root访问权限才能登录到租户帐户。
管理员	仅限 Swift 租户。提供对此租户帐户的 Swift 容器和对象的完全访问权限	Swift用户必须具有Swift管理员权限才能使用Swift REST API执行任何操作。

权限	Description	详细信息
管理您自己的S3凭据	允许用户创建和删除自己的 S3 访问密钥。	没有此权限的用户看不到*storage (S3)*>*My S3 access keys*菜单选项。
查看所有存储分段	<p>S3租户：允许用户查看所有存储分段和存储分段配置。</p> <p>Swift租户：允许Swift用户使用租户管理API查看所有容器和容器配置。</p>	<p>没有“查看所有存储分段”或“管理所有存储分段”权限的用户不会看到“存储分段”菜单选项。</p> <p>此权限将被“管理所有存储分段”权限所取代。它不会影响S3客户端或S3控制台使用的S3存储分段或组策略。</p> <p>您只能从租户管理API将此权限分配给Swift组。您不能使用租户管理器将此权限分配给Swift组。</p>
管理所有存储分段	<ul style="list-style-type: none"> • S3租户*：允许用户使用租户管理器和租户管理API创建和删除S3存储分段、并管理租户帐户中所有S3存储分段的设置、而不管S3存储分段或组策略如何。 <p>Swift租户：允许Swift用户使用租户管理API控制Swift容器的一致性。</p>	<p>没有“查看所有存储分段”或“管理所有存储分段”权限的用户不会看到“存储分段”菜单选项。</p> <p>此权限将取代查看所有存储分段权限。它不会影响S3客户端或S3控制台使用的S3存储分段或组策略。</p> <p>您只能从租户管理API将此权限分配给Swift组。您不能使用租户管理器将此权限分配给Swift组。</p>
管理端点	允许用户使用租户管理器或租户管理API创建或编辑平台服务端点、这些端点用作StorageGRID 平台服务的目标。	没有此权限的用户看不到“平台服务端点”菜单选项。
使用S3控制台选项卡	与查看所有存储分段或管理所有存储分段权限结合使用时、用户可以从存储分段详细信息页面上的S3控制台选项卡查看和管理对象。	

管理组

根据需要管理租户组以查看、编辑或复制组等。

开始之前

- 您将使用登录到租户管理器 ["支持的 Web 浏览器"](#)。
- 您属于具有的用户组 ["root访问权限"](#)。

查看或编辑组


您可以查看和编辑每个组的基本信息和详细信息。

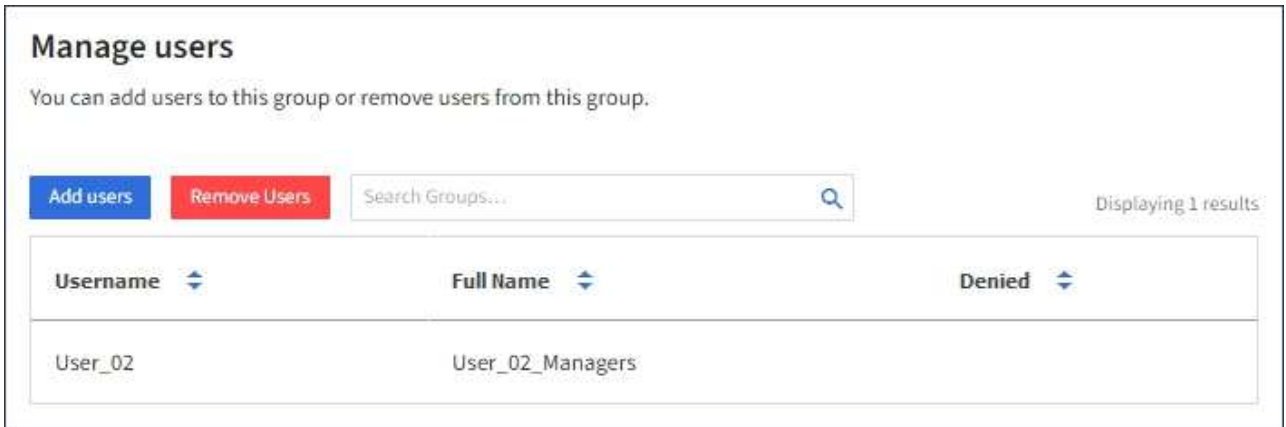
步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 查看"组"页面上提供的信息、其中列出了此租户帐户的所有本地组和联盟组的基本信息。

如果租户帐户具有*使用网格联合连接*权限、而您正在查看租户源网格上的组：

- 横幅消息指示、如果您编辑或删除某个组、您所做的更改将不会同步到其他网格。
- 根据需要、横幅消息会指示是否未将组克隆到目标网格上的租户。您可以 [重试组克隆](#) 失败了。

3. 如果要更改组的名称：
 - a. 选中组对应的复选框。
 - b. 选择*Actions*>*Edit group name*。
 - c. 输入新名称。
 - d. 选择*保存更改。*
4. 如果要查看更多详细信息或进行其他编辑、请执行以下操作之一：
 - 选择组名称。
 - 选中组对应的复选框，然后选择*Actions*>*查看组详细信息*。
5. 查看概述部分、其中显示了每个组的以下信息：
 - 显示名称
 - 唯一名称
 - Type
 - 访问模式
 - 权限
 - S3策略
 - 此组中的用户数
 - 如果租户帐户具有*使用网格联合连接*权限且您正在查看租户源网格上的组、则添加以下字段：
 - 克隆状态：成功*或*失败
 - 蓝色横幅、表示编辑或删除此组时、您所做的更改不会同步到其他网格。
6. 根据需要编辑组设置。请参见 "[为 S3 租户创建组](#)" 和 "[为 Swift 租户创建组](#)" 有关输入内容的详细信息。
 - a. 在概述部分中、通过选择名称或编辑图标来更改显示名称 。
 - b. 在*组权限*选项卡上，更新权限，然后选择*保存更改*。
 - c. 在*组策略*选项卡上，进行任何更改，然后选择*保存更改*。
 - 如果要编辑S3组、也可以根据需要选择其他S3组策略或输入自定义策略的JSON字符串。
 - 如果要编辑Swift组，可以选择选中或清除*Swift管理员*复选框。
7. 要将一个或多个现有本地用户添加到组、请执行以下操作：
 - a. 选择用户选项卡。



- b. 选择*添加用户*。
- c. 选择要添加的现有用户，然后选择*添加用户*。

右上角将显示一条成功消息。

8. 要从组中删除本地用户、请执行以下操作：
 - a. 选择用户选项卡。
 - b. 选择*删除用户*。
 - c. 选择要去除的用户，然后选择*Remove Users *

右上角将显示一条成功消息。

9. 确认您为每个更改的部分选择了*保存更改*。

重复的组

您可以复制现有组、以更快地创建新组。



如果您的租户帐户具有*使用网格联合连接*权限、而您从租户的源网格复制了一个组、则复制的组将克隆到租户的目标网格。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要复制的组对应的复选框。
3. 选择 * 操作 * > * 复制组 * 。
4. 请参见 ["为 S3 租户创建组"](#) 或 ["为 Swift 租户创建组"](#) 有关输入内容的详细信息。
5. 选择 * 创建组 * 。

[[CLONE GROUP]]重试组克隆

重试失败的克隆：

1. 选择组名称下方指示_(克隆失败)_的每个组。

2. 选择*Actions*>*Clone Groups*。
3. 从要克隆的每个组的详细信息页面查看克隆操作的状态。

对于追加信息，请参见 ["克隆租户组 and 用户"](#)。

删除一个或多个组

您可以删除一个或多个组。仅属于已删除组的任何用户将无法再登录到租户管理器或使用租户帐户。



如果您的租户帐户具有*使用网格联合连接*权限、而您删除了某个组、则StorageGRID 不会删除另一个网格上的相应组。如果保持此信息同步、则必须从两个网格中删除同一个组。

步骤

1. 选择 * 访问管理 * > * 组 *。
2. 选中要删除的每个组对应的复选框。
3. 选择*Actions*>*Delete group*或*Actions*>*Delete Groups*。

此时将显示确认对话框。

4. 选择*删除组*或*删除组*。

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。