



管理租户组 StorageGRID software

NetApp
July 23, 2026

目录

- 管理租户组 1
 - 在 StorageGRID 中为 S3 租户创建组 1
 - 访问"创建组"向导 1
 - 选择组类型 1
 - 管理组权限 2
 - 设置 S3 组策略 2
 - 添加用户（仅限本地组） 3
 - StorageGRID 租户管理权限 3
 - 管理 StorageGRID 租户组 4
 - 查看或编辑组 5
 - 复制组 6
 - 重试组克隆 6
 - 删除一个或多个组 7
 - 设置 AssumeRole 7

管理租户组

在 StorageGRID 中为 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

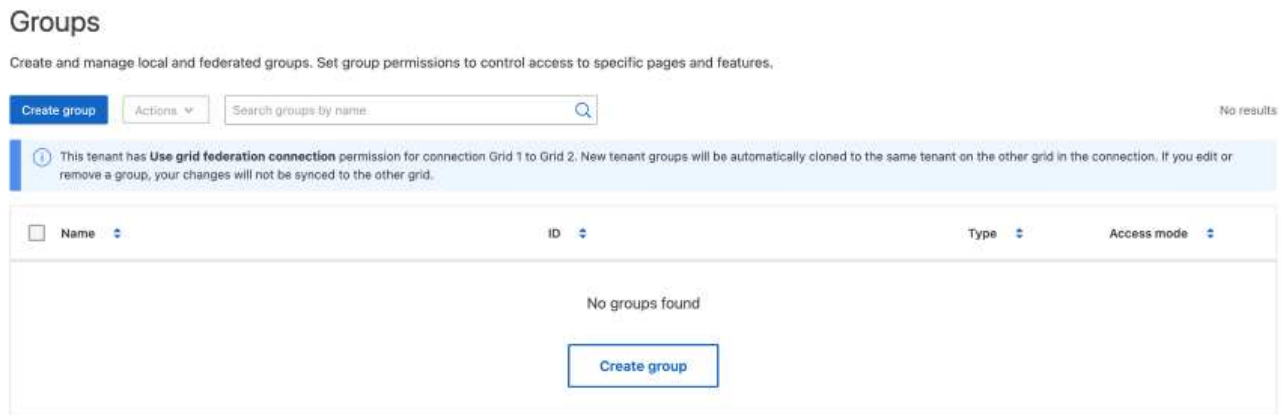
- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。
- 您属于具有 ["root 访问权限"](#) 的用户组。
- 如果您计划导入一个联合组，则您有["已配置身份联盟"](#)，并且该联合组已存在于配置的身份源中。
- 如果您的租户帐户具有*使用网格联合连接*权限，则表示您已查看["克隆租户组 and 用户"](#)的工作流程和注意事项，并且您已登录到租户的源网格。

访问"创建组"向导

第一步，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，请确认出现蓝色横幅，表示在此网格上创建的新组将被克隆到连接中另一个网格上的同一租户。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*创建群组*。

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，尽管他们可以根据组权限使用客户端应用程序来管理租户的资源。

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，则如果目标网格上的租户已存在相同的*唯一名称*，则会出现克隆错误。

- 联合组：输入唯一名称。对于 Active Directory，唯一名称是与 `sAMAccountName` 属性关联的名称。对于 OpenLDAP，唯一名称是与 `uid` 属性关联的名称。

3. 选择 **Continue**。

管理组权限

组权限控制用户可以在 Tenant Manager 和 Tenant Management API 中执行的任务。

步骤

1. 对于*访问模式*，请选择以下选项之一：
- 读写（默认）：用户可以登录 Tenant Manager 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，则该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。

请参阅 ["租户管理权限"](#)。

3. 选择 **Continue**。

设置 S3 组策略

组策略确定用户将具有哪些 S3 访问权限。

步骤

1. 选择要用于此组的策略。

组策略	问题描述
无 S3 访问权限	默认值。此组中的用户无权访问 S3 资源，除非使用存储桶策略授予访问权限。如果选择此选项，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、元数据和标签。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	问题描述
完全访问	此组中的用户具有对 S3 资源（包括存储桶）的完全访问权限。选择此选项时，文本框中将显示完全访问组策略的 JSON 字符串。您无法编辑此字符串。
勒索软件缓解	此示例策略适用于此租户的所有存储桶。此组中的用户可以执行常见操作，但不能从已启用对象版本控制的存储桶中永久删除对象。 拥有“管理所有存储桶”权限的租户管理器用户可以覆盖此组策略。将“管理所有存储桶”权限限制为受信任的用户，并在可用的情况下使用多因素身份验证 (MFA)。
自定义	组中的用户将获得您在文本框中指定的权限。

- 如果您选择了 **Custom**，请输入组策略。每个组策略的大小限制为 5,120 个字节。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”](#)。

- 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*并*完成*。

添加用户（仅限本地组）

您可以在不添加用户的情况下保存组，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，则在将组克隆到目标网格时，不包括在源网格上创建本地组时选择的任何用户。为此，请不要在创建组时选择用户。相反，请在创建用户时选择该组。

步骤

- 可选地，为此组选择一个或多个本地用户。
- 选择*创建群组*并*完成*。

您创建的群组将显示在群组列表中。

如果您的租户帐户具有*使用网格联合连接*权限，并且您在租户的源网格上，则新组将克隆到租户的目标网格。成功*在组的详细信息页面的“概览”部分显示为*克隆状态。

StorageGRID 租户管理权限

在创建租户组之前，请考虑要将哪些权限分配给该组。租户管理权限确定用户可以使用租户管理器或租户管理 API 执行的任务。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 Tenant Manager 或使用 Tenant Management 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都可以执行以下任务：

- 查看控制面板
- 更改自己的密码（针对本地用户）

对于所有权限，组的访问模式设置决定用户是否可以更改设置并执行操作，或者他们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，则该用户将对所有选定设置和功能具有只读访问权限。

您可以将以下权限分配给组。

权限	问题描述	详细信息
Root 访问	提供对租户管理器和租户管理 API 的完全访问权限。	
管理自己的 S3 凭据	允许用户创建和删除自己的 S3 访问密钥。	没有此权限的用户不会看到 STORAGE (S3) > My S3 access keys 菜单选项。
查看所有存储桶	允许用户查看所有存储桶和存储桶配置。	没有"查看所有存储桶"或"管理所有存储桶"权限的用户不会看到 Buckets 菜单选项。 此权限被"管理所有存储桶"权限所取代。它不影响 S3 客户端或 S3 控制台使用的 S3 存储桶或组策略。
管理所有存储桶	允许用户使用 Tenant Manager 和租户管理 API 创建和删除 S3 存储桶，并管理租户帐户中所有 S3 存储桶的设置，无论 S3 存储桶或组策略如何。	没有"查看所有存储桶"或"管理所有存储桶"权限的用户不会看到 Buckets 菜单选项。 此权限取代查看所有存储桶权限。它不影响 S3 客户端或 S3 控制台使用的 S3 存储桶或组策略。
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 Console 选项卡	与"查看所有存储桶"或"管理所有存储桶"权限结合使用时，允许用户从存储桶的详细信息页面上的 S3 Console 选项卡查看和管理对象。	

管理 StorageGRID 租户组

根据需要管理租户组，以查看、编辑或复制组等。

开始之前

- 您已使用 ["支持的 Web 浏览器"](#) 登录到租户管理器。

- 您属于具有 "root 访问权限" 的用户组。

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和联合组的基本信息。

如果租户帐户具有*使用网格联合连接*权限，并且您正在租户的源网格上查看组：

- 横幅消息表示，如果编辑或删除组，则您所做的更改将不会同步到另一个网格。
- 根据需要，横幅消息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](#)失败的组。

3. 如果希望更改组的名称：
 - a. 选中该组的复选框。
 - b. 选择*操作* > 编辑组名称。
 - 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。
 - 选中该组的复选框，然后选择*操作* > 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
 - 类型
 - 访问模式
 - 权限
 - S3 策略
 - 此组中的用户数
 - 如果租户帐户具有 **Use grid federation connection** 权限，并且您正在租户的源网格上查看组，则显示附加字段：
 - 克隆状态，成功*或*失败
 - 一个蓝色横幅，表示如果编辑或删除此组，则您所做的更改将不会同步到其他网格。
6. 根据需要编辑组设置。有关输入内容的详细信息，请参阅 ["为 S3 租户创建组"](#)。
 - a. 在概述部分，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*。

可根据需要选择其他 S3 组策略或输入自定义策略的 JSON 字符串。

7. 将一个或多个现有本地用户添加到组：

- 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*。

成功消息显示在右上角。

8. 从组中删除本地用户：

- a. 选择"用户"选项卡。

- b. 选择*移除用户*。

- c. 选择要删除的用户，然后选择*删除用户*。

成功消息显示在右上角。

9. 确认您已为更改的每个部分选择*保存更改*。

复制组

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，并且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. 选中要复制的组的复选框。
3. 选择*操作* > 复制组。
4. 请参见["为 S3 租户创建组"](#)以了解有关要输入的内容的详细信息。
5. 选择*创建群组*。

重试组克隆

要重试失败的克隆，请执行以下操作：

1. 选择组名称下方表示_（克隆失败）_的每个组。
2. 选择*操作* > 克隆组。
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。

有关更多信息，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，并且您删除了一个组，StorageGRID 将不会删除另一个网格上的相应组。如果需保持此信息同步，则必须从两个网格中删除相同的组。

步骤

1. 选择*访问管理* > 组。
2. 选中要删除的每个组的复选框。
3. 选择*操作* > 删除组*或*操作 > 删除组。

此时将显示确认对话框。

4. 选择*Delete group*或*Delete groups*。

设置 AssumeRole

开始之前

您必须是管理员才能设置 AssumeRole。

关于此任务

若要设置 AssumeRole，请创建要假定的目标组（如果该组尚不存在）。编辑组的 S3 策略，以指定假定此组的允许操作。编辑组的 S3 信任策略，以指定允许使用 AssumeRole API 承担组的受信任用户。

通过承担此组创建的临时安全凭据在有限的持续时间内有效。会话时长为 15 分钟至 12 小时，默认会话时长为 1 小时。从组的 S3 信任策略中删除用户后，该用户将无法再承担此组。

步骤

1. 选择*访问管理* > 组。
2. 单击组名称。
3. 选择 **S3 trust policy** 选项卡。
4. 添加 S3 信任策略，包括可以执行 AssumeRole 的用户列表。
5. 选择 **Save changes**。
6. 选择 **S3 group policy** 选项卡。
7. 编辑 S3 策略，仅为此组的 S3 信任策略中添加的受信任用户指定所需的 S3 操作。
8. 选择 **Save changes**。

AssumeRole S3 信任策略示例

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

配置完成后，S3 信任策略中列出的用户可以执行 AssumeRole 并接收凭据。最终权限由组策略、存储区策略和会话策略确定。有关详细信息，请参见 ["使用访问策略"](#)。

版权信息

版权所有 © 2026 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。