管理组和用户

StorageGRID software

NetApp
July 23, 2026

目录

管理组和用户

在 StorageGRID 中使用身份联合

使用身份联合可以更快地设置租户组和用户，并允许租户用户使用熟悉的凭据登录到租户帐户。

为租户管理器配置身份联合

如果希望在其他系统（如 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server）中管理租户组和用户，则可以为租户管理器配置身份联合。

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。
- 您正在使用 Active Directory、Microsoft Entra ID、OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  如果希望使用未列出的 LDAP v3 服务，请联系技术支持。

- 如果您计划使用 OpenLDAP，则必须配置 OpenLDAP 服务器。请参阅 配置 OpenLDAP 服务器的指南。
- 如果您计划使用传输层安全 (TLS) 与 LDAP 服务器进行通信，则身份提供程序必须使用 TLS 1.2 或 1.3。请参阅 "传出 TLS 连接支持的密码"。

关于此任务

是否可以为租户配置身份联合服务取决于租户帐户的设置方式。您的租户可能会共享为 Grid Manager 配置的身份联合服务。如果在访问"身份联合"页面时看到此消息，则无法为此租户配置单独的联合身份源。

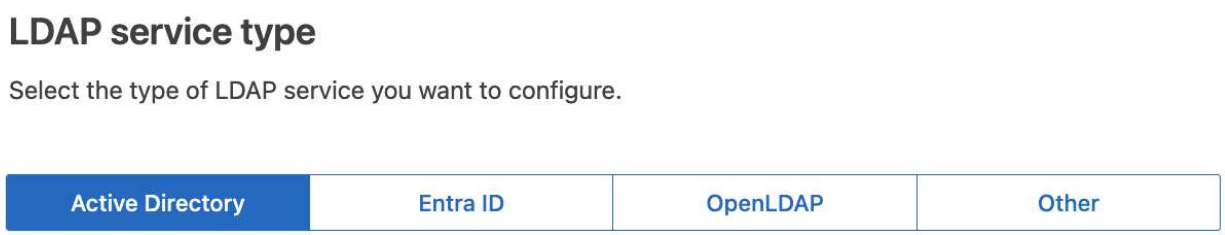
This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

输入配置

配置身份联合时，请提供 StorageGRID 连接到 LDAP 服务所需的值。

步骤

1. 选择*访问管理* > 身份联合。
2. 选择*启用身份联合*。
3. 在 LDAP 服务类型部分，选择要配置的 LDAP 服务类型。



选择*其他*以配置使用 Oracle Directory Server 的 LDAP 服务器的值。

4. 如果您选择了*其他*，请填写 LDAP 属性部分中的字段。否则，请转至下一步。
   - 用户唯一名称：包含 LDAP 用户唯一标识符的属性名称。此属性等效于 Active Directory 的 `sAMAccountName`和 `OpenLDAP 的 `uid`。如果要配置 Oracle Directory Server，请输入 `uid`。
   - 用户 **UUID**：包含 LDAP 用户永久唯一标识符的属性名称。此属性等效于 Active Directory 的 `objectGUID`和 `OpenLDAP 的 `entryUUID`。如果要配置 Oracle Directory Server，请输入 `nsuniqueid`。每个用户的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数字，其中连字符将被忽略。
   - 组唯一名称：包含 LDAP 组唯一标识符的属性名称。此属性等效于 Active Directory 的 `sAMAccountName`和 `OpenLDAP 的 `cn`。如果要配置 Oracle Directory Server，请输入 `cn`。
   - 组 **UUID**：包含 LDAP 组的永久唯一标识符的属性名称。此属性等效于 Active Directory 的 `objectGUID`和 `OpenLDAP 的 `entryUUID`。如果要配置 Oracle Directory Server，请输入 `nsuniqueid`。每个组的指定属性值必须是 16 字节或字符串格式的 32 位十六进制数字，其中连字符将被忽略。
5. 对于所有 LDAP 服务类型，请在"配置 LDAP 服务器"部分中输入所需的 LDAP 服务器和网络连接信息。
   - 主机名：LDAP 服务器的完全限定域名 (FQDN) 或 IP 地址。
   - 端口：用于连接到 LDAP 服务器的端口。

     STARTTLS 的默认端口为 389，LDAPS 的默认端口为 636。但是，只要防火墙配置正确，您就可以使用任何端口。

   - 用户名：将连接到 LDAP 服务器的用户的可分辨名称 (DN) 的完整路径。

     对于 Active Directory，还可以指定下层登录名称或用户主体名称。

     指定的用户必须具有列出组和用户以及访问以下属性的权限：

     - `sAMAccountName` 或 `uid`
     - `objectGUID`， `entryUUID`，或 `nsuniqueid`
     - `cn`
     - `memberOf` 或 `isMemberOf`
     - **Active Directory**： `objectSid`、 `primaryGroupID`、 `userAccountControl`和 `userPrincipalName`
     - **Entra ID**： `accountEnabled`和 `userPrincipalName`

- 密码：与用户名关联的密码。

  > 如果以后更改密码，则必须在此页面上进行更新。

- **Group Base DN**：要搜索组的 LDAP 子树的可分辨名称 (DN) 的完整路径。在 Active Directory 示例（如下）中，其可分辨名称相对于基本 DN (DC=storagegrid,DC=example,DC=com) 的所有组均可用作联合组。

  > 组唯一名称*值在其所属的*组基本 **DN** 中必须是唯一的。

- 用户群 **DN**：要搜索用户的 LDAP 子树的标识名 (DN) 的完整路径。

  > 用户唯一名称*值在其所属的*用户基础 **DN** 中必须是唯一的。

- 绑定用户名格式（可选）：如果无法自动确定模式，StorageGRID 应使用的默认用户名模式。

  建议提供*绑定用户名格式*，因为如果 StorageGRID 无法与服务帐户绑定，它仍可允许用户登录。

  输入以下模式之一：

  - **UserPrincipalName** 模式（**AD** 和 **Entra ID**）： `[USERNAME]@example.com`
  - 下级登录名称模式（**AD** 和 **Entra ID**）： `example\[USERNAME]`
  - 辨识名模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    请按原样填写 **[USERNAME]**。

6. 在传输层安全性 (TLS) 部分，选择一个安全设置。
   - 使用 **STARTTLS**：使用 STARTTLS 保护与 LDAP 服务器的通信。这是 Active Directory、OpenLDAP 或其他选项的推荐选项，但 Microsoft Entra ID 不支持此选项。
   - 使用 **LDAPS**：LDAPS（LDAP over SSL）选项使用 TLS 建立与 LDAP 服务器的连接。您必须为 Microsoft Entra ID 选择此选项。
   - 不使用 **TLS**：StorageGRID 系统与 LDAP 服务器之间的网络流量将不受保护。Microsoft Entra ID 不支持此选项。

     > 如果您的 Active Directory 服务器强制执行 LDAP 签名，则不支持使用*不使用 TLS* 选项。您必须使用 STARTTLS 或 LDAPS。

7. 如果选择了 STARTTLS 或 LDAPS，请选择用于保护连接的证书。
   - **Use operating system CA certificate**：使用操作系统上安装的默认网格 CA 证书来保护连接。
   - 使用自定义 **CA** 证书：使用自定义安全证书。

     如果选择此设置，请将自定义安全证书复制并粘贴到 CA 证书文本框中。

测试连接并保存配置

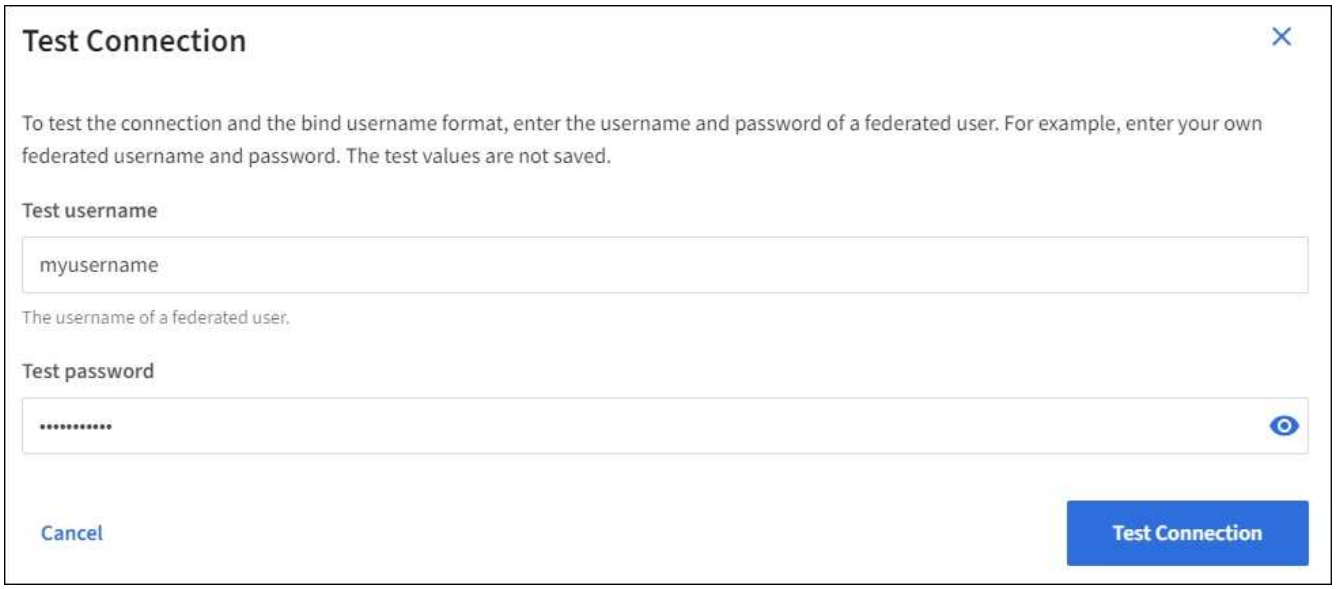
输入所有值后，必须先测试连接，然后才能保存配置。StorageGRID 验证 LDAP 服务器的连接设置以及绑定用

户名格式（如果已提供）。

步骤

1. 选择*测试连接*。
2. 如果未提供绑定用户名格式：
   - 如果连接设置有效，则会显示"Test connection successful"（测试连接成功）消息。选择 **Save** 保存配置。
   - 如果连接设置无效，将显示"无法建立测试连接"消息。选择*Close*。然后，解决任何问题并再次测试连接。
3. 如果您提供了绑定用户名格式，请输入有效的联合用户的用户名和密码。

   例如，请输入您自己的用户名和密码。请勿在用户名中包含任何特殊字符，例如@或/。



   - 如果连接设置有效，则会显示"Test connection successful"（测试连接成功）消息。选择 **Save** 保存配置。
   - 如果连接设置、绑定用户名格式或测试用户名和密码无效，则会显示错误消息。请解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统定期从身份源同步联合组和用户。如果要尽快启用或限制用户权限，可以强制启动同步。

步骤

1. 转到"身份联合"页面。
2. 选择页面顶端的*同步服务器*。

   同步过程可能需要一段时间，具体取决于您的环境。

   如果从身份源同步联合组和用户时出现问题，则会触发*身份联合同步失败*警报。

禁用身份联合

您可以暂时或永久禁用组和用户的身份联合。禁用身份联合后，StorageGRID 与身份源之间将不再进行通信。但是，您已配置的所有设置将被保留，以便将来可以轻松重新启用身份联合。

关于此任务

在禁用身份联合之前，应注意以下事项：

- 联合用户将无法登录。
- 当前登录的联合用户将在其会话过期之前保留对 StorageGRID 系统的访问权限，但在其会话过期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，也不会针对尚未同步的帐户发出警报。
- 如果单点登录 (SSO) 状态为*已启用*或*沙盒模式*，则*启用身份联合*复选框将被禁用。必须先将单点登录页面上的 SSO 状态设置为*已禁用*，然后才能禁用身份联合。请参阅 "禁用单点登录"。

步骤

1. 转到"身份联合"页面。
2. 取消选中*启用身份联合*复选框。

配置 OpenLDAP 服务器的指南

如果要将 OpenLDAP 服务器用于身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于不是 Active Directory 或 Microsoft Entra ID 的身份源，StorageGRID 不会自动阻止对外部禁用的用户进行 S3 访问。要阻止 S3 访问，请删除该用户的任何 S3 密钥或从所有组中删除该用户。

Memberof和refint叠加层

应启用 memberof 和 refint 叠加层。有关详细信息，请参见 "OpenLDAP 文档：Version 2.4 Administrator's Guide" 中的反向组成员资格维护说明。

索引

必须使用指定的索引关键字配置以下 OpenLDAP 属性：

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

此外，请确保用户名帮助中提到的字段已编入索引，以实现最佳性能。

请参见 "OpenLDAP 文档：Version 2.4 Administrator's Guide" 中有关反向组成员资格维护的信息。

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

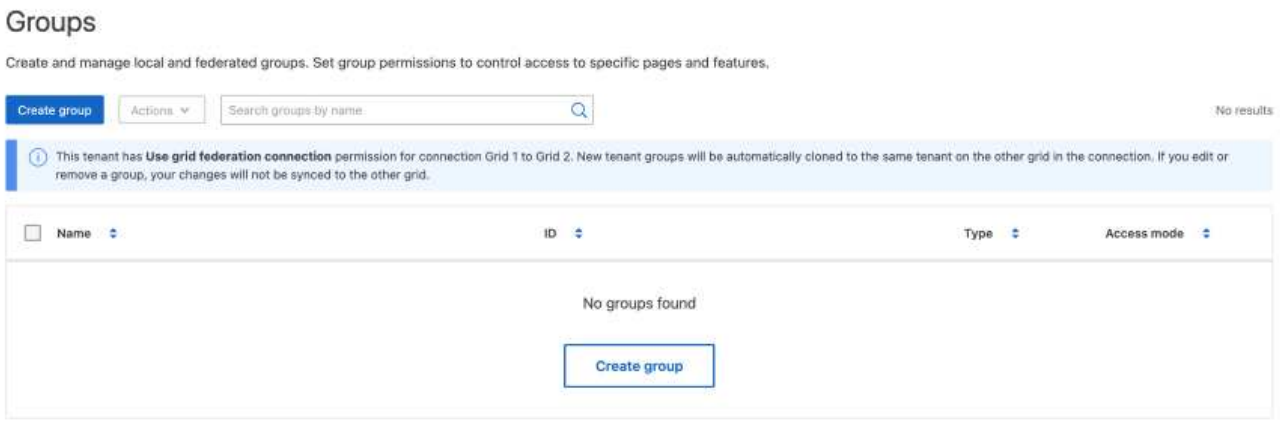
- 您已使用 "支持的 Web 浏览器" 登录到租户管理器。
- 您属于具有 "root 访问权限" 的用户组。
- 如果您计划导入一个联合组，则您有"已配置身份联盟"，并且该联合组已存在于配置的身份源中。
- 如果您的租户帐户具有*使用网格联合连接*权限，则表示您已查看"克隆租户组和用户"的工作流程和注意事项，并且您已登录到租户的源网格。

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。

2. 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"。

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*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

1. 可选地，为此组选择一个或多个本地用户。
2. 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 "克隆租户组和用户"。

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。如果需要保持此信息同步，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"。

管理 StorageGRID 租户用户

您可以创建本地用户并将其分配给本地组，以确定这些用户可以访问哪些功能。您还可以导入联合用户。Tenant Manager 包括一个名为"root"的预定义本地用户。虽然您可以添加和删除本地用户，但无法删除 root 用户。

如果为 StorageGRID 系统启用了单点登录 (SSO)，本地用户将无法登录到租户管理器或租户管理 API，尽管他们可以根据组权限使用客户端应用程序访问租户的资源。

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"克隆租户组和用户"的工作流程和注意事项，并且您已登录到租户的源网格。

创建本地用户

您可以创建本地用户并将其分配给一个或多个本地组，以控制其访问权限。

不属于任何组的 S3 用户没有应用管理权限或 S3 组策略。这些用户可能具有通过存储桶策略授予的 S3 存储桶访问权限。

访问"创建用户"向导

步骤

1. 选择*访问管理* > 用户。

   如果您的租户帐户具有*使用网格联合连接*权限，则蓝色横幅表示这是租户的源网格。您在此网格上创建的任何本地用户将被克隆到连接中的另一个网格。

2. 选择*创建用户*。

输入凭据

步骤

1. 对于*输入用户凭据*步骤，请填写以下字段。

字段	问题描述
全名	此用户的全名，例如，人员的名字和姓氏或应用程序的名称。
用户名	此用户将用于登录的名称。用户名必须唯一，且无法更改。 注意：如果您的租户帐户具有*使用网格联合连接*权限，且目标网格上的租户已存在相同的*用户名*，则会出现克隆错误。
密码和确认密码	用户登录时最初将使用的密码。
拒绝访问	选择*是*可阻止此用户登录到租户帐户，即使他们仍可能属于一个或多个组。 例如，选择*是*可暂时暂停用户的登录权限。

2. 选择 **Continue**。

分配到组

步骤

1. 将用户分配给一个或多个本地组，以确定他们可以执行哪些任务。

   将用户分配给组是可选的。如果您愿意，可以在创建或编辑组时选择用户。

   不属于任何组的用户将没有管理权限。权限是累积的。用户将拥有其所属所有组的所有权限。请参阅"租户管

理权限"。

2. 选择*创建用户*。

   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，则会将新的本地用户克隆到租户的目标网格。成功*在用户详细信息页面的"概览"部分显示为*克隆状态。

3. 选择*完成*以返回"用户"页面。

查看或编辑本地用户

步骤

1. 选择*访问管理* > 用户。
2. 查看"用户"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用户的基本信息。

   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用户：

   - 横幅消息表示，如果编辑或删除用户，则您所做的更改将不会同步到其他网格。
   - 根据需要，横幅消息指示用户是否未克隆到目标网格上的租户。您可以 重试失败的用户克隆。

3. 如果希望更改用户的全名：
   a. ${post_edited_translations.segment}
   b. 选择*操作* > 编辑全名。
   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：
   - 选择用户名。
   - 选中用户的复选框，然后选择*操作* > 查看用户详细信息。
5. 查看概述部分，其中显示了每个用户的以下信息：
   - 全名
   - 用户名
   - 用户类型
   - 拒绝访问
   - 访问模式
   - 组成员身份
   - 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用户，则显示附加字段：
     - 克隆状态，成功*或*失败
     - 一个蓝色横幅，表示如果编辑此用户，则您所做的更改将不会同步到其他网格。
6. 根据需要编辑用户设置。有关输入内容的详细信息，请参阅 创建本地用户。
   a. 在概述部分，通过选择名称或编辑图标 更改全名。

您无法更改用户名。

b. 在*密码*选项卡上，更改用户的密码，然后选择*保存更改*。

c. 在*访问权限*选项卡上，选择*否*以允许用户登录，或选择*是*以阻止用户登录。然后，选择*保存更改*。

d. 在*访问密钥*选项卡上，选择*创建密钥*，然后按照 "创建其他用户的 S3 访问密钥" 的说明进行操作。

e. 在*组*选项卡上，选择*编辑组*以将用户添加到组或从组中删除用户。然后，选择*保存更改*。

7. 确认您已为更改的每个部分选择*保存更改*。

导入联合用户

${post_edited_translations.segment}

步骤

1. 选择*访问管理* > 用户。
2. ${post_edited_translations.segment}
3. 输入一个或多个联合用户的 UUID 或用户名。

   对于多个条目，请在新行中添加每个 UUID 或用户名。

4. 选择*导入*。

   如果一个或多个用户的"用户"字段导入失败，请执行以下步骤：

   a. ${post_edited_translations.segment}

   b. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

复制本地用户

您可以复制本地用户以更快地创建新用户。

> 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用户，则复制的用户将被克隆到租户的目标网格。

步骤

1. 选择*访问管理* > 用户。
2. 选中要复制的用户的复选框。
3. 选择*操作* > 复制用户。
4. 请参见创建本地用户以了解有关要输入的内容的详细信息。
5. 选择*创建用户*。

重试用户克隆

要重试失败的克隆，请执行以下操作：

1. 选择用户名下方显示_（克隆失败）_的每个用户。
2. 选择*操作* > 克隆用户。
3. 从要克隆的每个用户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 "克隆租户组和用户"。

删除一个或多个本地用户

您可以永久删除一个或多个不再需要访问 StorageGRID 租户帐户的本地用户。

> 如果您的租户帐户具有*使用网格联合连接*权限，并且您删除了本地用户，StorageGRID 将不会删除其他网格上的相应用户。如果需要保持此信息同步，则必须从两个网格中删除同一用户。

> 您必须使用联合身份源删除联合用户。

步骤

1. 选择*访问管理* > 用户。
2. 选中要删除的每个用户的复选框。
3. 选择 **Actions** > **Delete user** 或 **Actions** > **Delete users**。

   此时将显示确认对话框。

4. 选择 **Delete user** 或 **Delete users**。