管理组和用户

StorageGRID 11.7

NetApp
April 12, 2024

目录

管理组和用户

使用身份联合

使用身份联合可以加快租户组和用户的设置速度，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

如果您希望在 Active Directory ， Azure Active Directory （Azure AD ）， OpenLDAP 或 Oracle Directory Server 等其他系统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"。
- 您正在使用 Active Directory ， Azure AD ， OpenLDAP 或 Oracle Directory Server 作为身份提供程序。

  > 如果要使用未列出的 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。请参见 配置 OpenLDAP 服务器的准则。
- 如果您计划使用传输层安全（Transport Layer Security ， 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 。请参见 "支持传出 TLS 连接的密码"。

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网格管理器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。

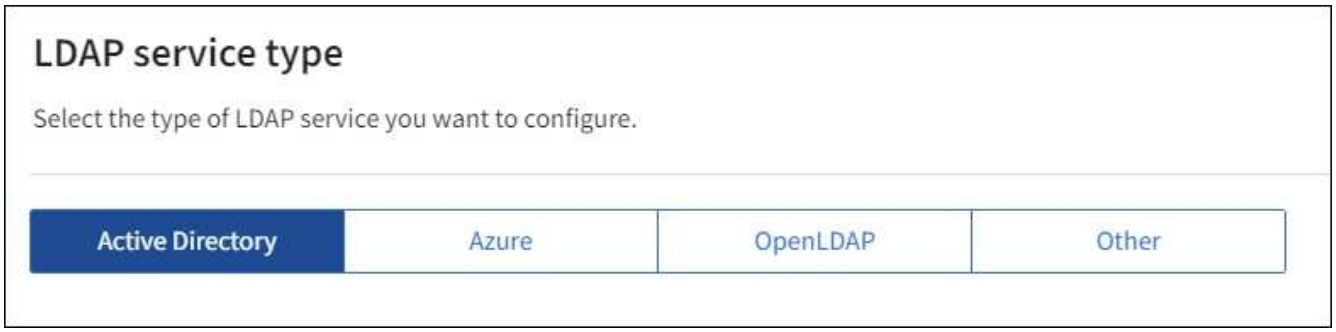
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

进入配置

在配置"标识联盟"时、您可以提供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 服务类型部分中，选择要配置的 LDAP 服务类型。



选择 * 其他 * 可为使用 Oracle 目录服务器的 LDAP 服务器配置值。

4. 如果选择了 * 其他 * ，请填写 LDAP 属性部分中的字段。否则，请继续执行下一步。
   - * 用户唯一名称 *： 包含 LDAP 用户唯一标识符的属性的名称。此属性等效于 `sAMAccountName` 适用于Active Directory和 `uid` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `uid`。
   - * 用户 UID*： 包含 LDAP 用户的永久唯一标识符的属性的名称。此属性等效于 `objectGUID` 适用于Active Directory和 `entryUUID` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `nsuniqueid`。每个用户在指定属性中的值都必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
   - * 组唯一名称 *： 包含 LDAP 组唯一标识符的属性的名称。此属性等效于 `sAMAccountName` 适用于Active Directory和 `cn` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `cn`。
   - * 组 UID*： 包含 LDAP 组的永久唯一标识符的属性的名称。此属性等效于 `objectGUID` 适用于Active Directory和 `entryUUID` 对于OpenLDAP。如果要配置Oracle Directory Server、请输入 `nsuniqueid`。每个组在指定属性中的值必须是一个 32 位十六进制数字，采用 16 字节或字符串格式，其中会忽略连字符。
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 *： 要连接到 LDAP 服务器的用户的可分辨名称（ DN ）的完整路径。

     对于 Active Directory ，您还可以指定低级别的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`
     - * Azure *： `accountEnabled` 和 `userPrincipalName`

- * 密码 * ： 与用户名关联的密码。
- * 组基本 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，可分辨名称相对于基础 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。

- * 用户基础 DN* ： 要搜索用户的 LDAP 子树的可分辨名称（ 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 无法绑定到服务帐户，它可以允许用户登录。

  输入以下模式之一：

  - **UserPrincipalName模式(Active Directory和Azure)**： `[USERNAME]@example.com`
  - 低级登录名称模式**(Active Directory和Azure)**： `example\[USERNAME]`
  - 可分辨名称模式： `CN=[USERNAME],CN=Users,DC=example,DC=com`

    与写入的内容完全相同，请包含 * 。

6. 在传输层安全（ TLS ）部分中，选择一个安全设置。
   - * 使用 STARTTLS * ： 使用 STARTTLS 确保与 LDAP 服务器的通信安全。这是建议的 Active Directory ， OpenLDAP 或其他选项，但 Azure 不支持此选项。
   - * 使用 LDAPS* ： LDAPS （基于 SSL 的 LDAP ）选项使用 TLS 与 LDAP 服务器建立连接。您必须为 Azure 选择此选项。
   - * 请勿使用 TLS* ： StorageGRID 系统与 LDAP 服务器之间的网络流量将不会受到保护。Azure 不支持此选项。

     > 如果 Active Directory 服务器强制实施 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 STARTTLS 或 LDAPS ，请选择用于保护连接安全的证书。
   - * 使用操作系统 CA 证书 * ： 使用操作系统上安装的默认网格 CA 证书确保连接安全。
   - * 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。

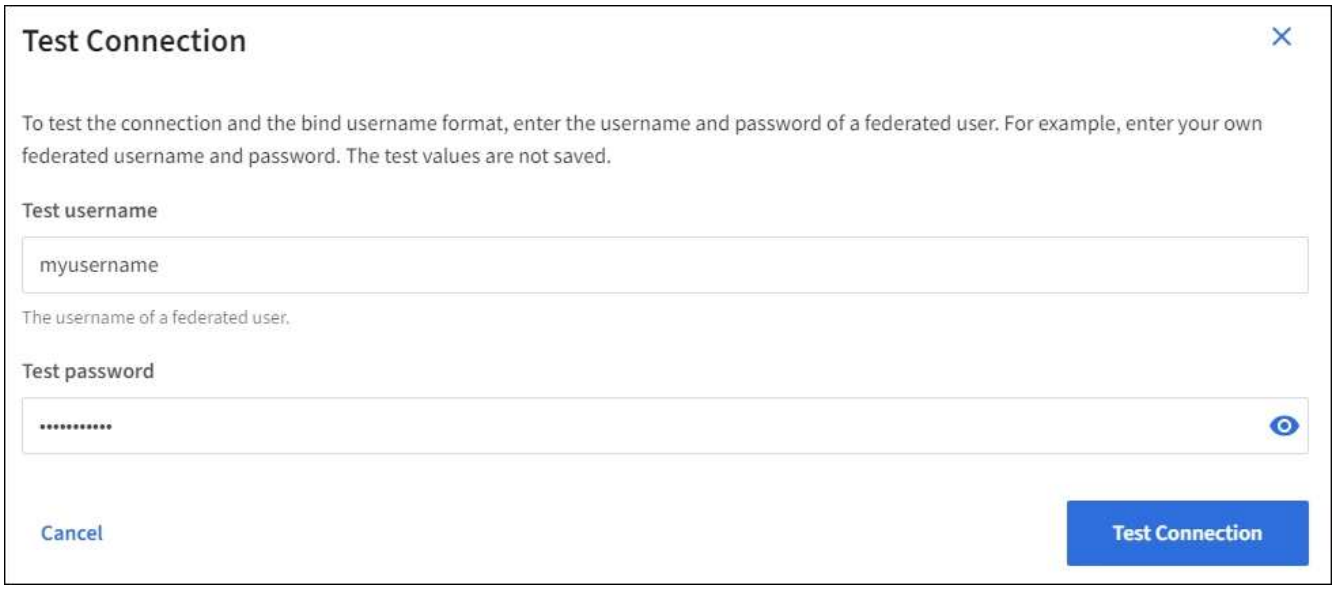
测试连接并保存配置

输入所有值后，必须先测试连接，然后才能保存配置。如果您提供了 LDAP 服务器的连接设置和绑定用户名格式，则 StorageGRID 会对其进行验证。

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` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置无效，则会显示 "`test connection could not be established` " 消息。选择 * 关闭 * 。然后，解决所有问题并重新测试连接。
3. 如果您提供了绑定用户名格式，请输入有效联合用户的用户名和密码。

   例如，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` " 消息。选择 * 保存 * 以保存配置。
   - 如果连接设置，绑定用户名格式或测试用户名和密码无效，则会显示一条错误消息。解决所有问题并重新测试连接。

强制与身份源同步

StorageGRID 系统会定期同步身份源中的联合组和用户。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. 选择页面顶部的 * 同步服务器 * 。

   同步过程可能需要一些时间，具体取决于您的环境。

   > 如果存在正在同步身份源中的联合组和用户的问题描述 ，则会触发 * 身份联合同步失败 * 警报。

禁用身份联合

您可以临时或永久禁用组和用户的身份联合。禁用身份联合后， StorageGRID 与身份源之间不会进行通信。但是，您配置的任何设置都将保留下来，以便将来可以轻松地重新启用身份联合。

关于此任务

在禁用身份联合之前，您应注意以下事项：

- 联合用户将无法登录。
- 当前已登录的联合用户将保留对 StorageGRID 系统的访问权限，直到其会话到期为止，但在其会话到期后将无法登录。
- StorageGRID 系统与身份源之间不会进行同步，并且不会为尚未同步的帐户发出警报或警报。
- 如果单点登录(SSO)设置为*Enabled"或*Sandbox Mode*，则*启用身份联合*复选框将被禁用。在禁用身份联合之前，单点登录页面上的 SSO 状态必须为 * 已禁用 * 。请参见 "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 服务器的准则

如果要使用 OpenLDAP 服务器进行身份联合，则必须在 OpenLDAP 服务器上配置特定设置。

> 对于非ActiveDirectory或Azure身份源、StorageGRID 不会自动阻止外部禁用的用户进行S3访问。要阻止S3访问、请删除此用户的任何S3密钥或从所有组中删除此用户。

memberOf 和 fint 覆盖

应启用成员和精简覆盖。有关详细信息，请参见中有关反向组成员资格维护的说明http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

索引编制

您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，请确保已为用户名帮助中提及的字段编制索引，以获得最佳性能。

请参见中有关反向组成员资格维护的信息http://www.openldap.org/doc/admin24/index.html["OpenLDAP 文档：版本 2.4 管理员指南"^]。

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 "克隆租户组和用户"，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。
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。

组策略	Description
勒索软件防护	此示例策略适用场景 all分段for this租户。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**
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。 注意： 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 • 注： * 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。
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。

权限	Description
管理所有存储分段	• 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。 没有此权限的用户看不到“存储桶”菜单选项。 • Swift 租户：允许 Swift 用户使用租户管理 API 控制 Swift 容器的一致性级别。 *注意：*您只能从租户管理API为Swift组分配"管理所有存储分段"权限。您不能使用租户管理器将此权限分配给Swift组。
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控制台管理对象	与管理所有存储分段权限结合使用时、允许用户从存储分段页面访问体验S3控制台。具有此权限但不具有"管理所有存储分段"权限的用户仍可直接导航到体验S3控制台。

管理组

您可以查看组；编辑组的名称、权限、策略和用户；复制组； 或删除组。

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。

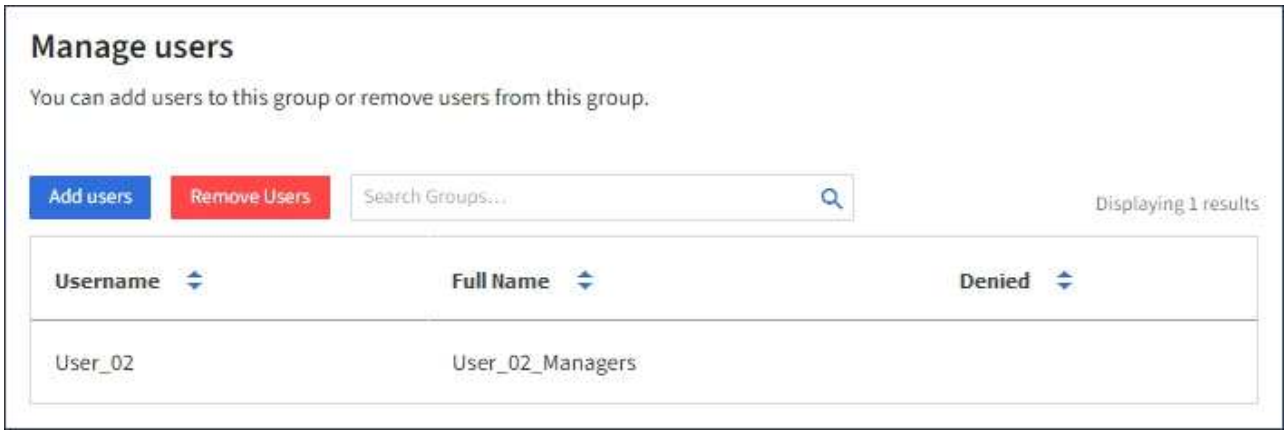
步骤

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、并且您正在查看租户源网格上的组、则蓝色横幅表示、如果您编辑或删除某个组、您所做的更改不会同步到另一个网格。请参见 "克隆租户组和用户"。

3. 如果要更改组的名称：
   a. 选中组对应的复选框。
   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 * 。

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。如果需要保持此信息同步、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*。

管理本地用户

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。租户管理器包括一个预定义的本地用户、名为"`root.`" 虽然您可以添加和删除本地用户、但不能删除root用户。

如果为StorageGRID 系统启用了单点登录(SSO)、则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 "克隆租户组和用户"，您将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用户不具有管理权限或应用了S3组策略。这些用户可能已通过存储分段策略授予 S3 存储分段访问权限。

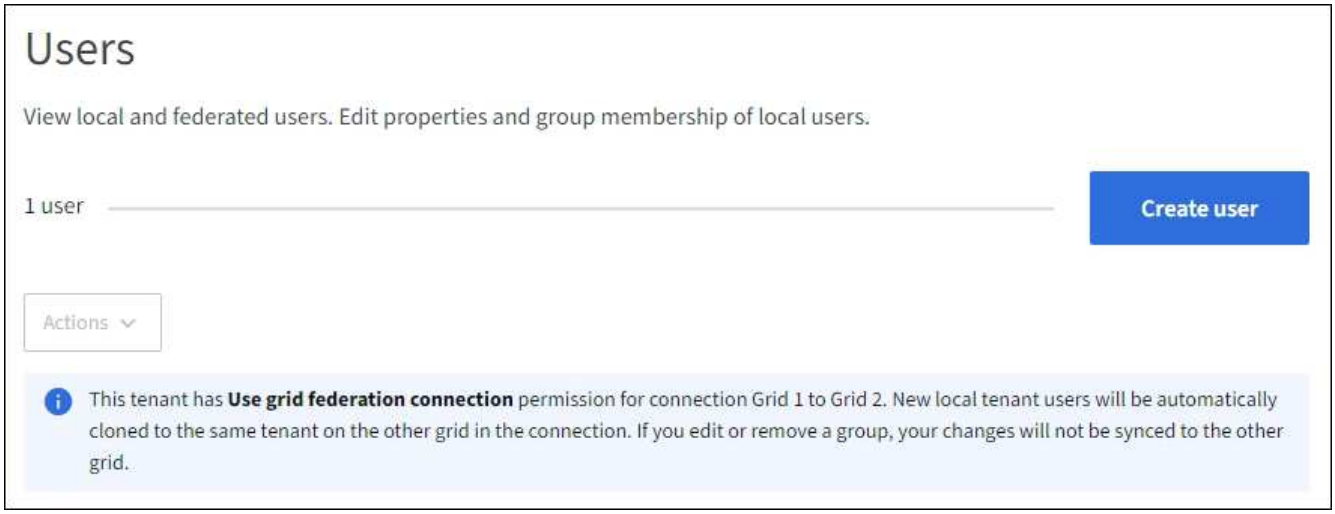
不属于任何组的Swift用户没有管理权限或Swift容器访问权限。

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、则蓝色横幅指示这是租户的源网格。您在此网格上创建的任何本地用户都将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	Description
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。
Username	此用户用于登录的名称。用户名必须唯一、并且无法更改。 注意：如果您的租户帐户具有*使用网格联合连接*权限、则如果目标网格上的租户已存在相同的*用户名*、则会发生克隆错误。
密码和确认密码	用户在登录时最初使用的密码。
拒绝访问	选择*是*可防止此用户登录到租户帐户、即使他们可能仍属于一个或多个组也是如此。 例如，选择*Yes*可暂时暂停用户的登录能力。

2. 选择 * 继续 * 。

分配给组

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。

   将用户分配到组是可选的。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无管理权限。权限是累积的。用户将对其所属的所有组拥有所有权限。请参见 "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、而您位于租户的源网格上、则新的本地用户将克隆到租户的目标网格。在用户的详细信息页面的"概述"部分中、成功*显示为*克隆状态。

3. 选择*完成*返回用户页。

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盟用户的基本信息。

   如果租户帐户具有*使用网格联合连接*权限、而您正在租户的源网格上查看用户、则蓝色横幅指示编辑或删除用户时、您所做的更改不会同步到其他网格。

3. 如果要更改用户的全名：
   a. 选中用户对应的复选框。
   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。
   - 选中用户对应的复选框，然后选择*Actions*>*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
   - Username
   - 用户类型
   - 拒绝访问
   - 访问模式
   - 组成员资格
   - 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用户、则添加以下字段：
     - 克隆状态：成功*或*失败
     - 蓝色横幅、表示如果编辑此用户、您所做的更改不会同步到其他网格。
6. 根据需要编辑用户设置。请参见 创建本地用户 有关输入内容的详细信息。

   a. 在概述部分中、选择名称或编辑图标以更改全名 。

      您不能更改用户名。

   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*选项卡上，选择*否*允许用户登录，或选择*是*阻止用户登录。然后，选择*保存更改*。

   d. 在*Access keys*选项卡上，选择*Create key*并按照的说明进行操作 "正在创建其他用户的S3访问密钥"。

   e. 在*组*选项卡上，选择*编辑组*将用户添加到组或从组中删除用户。然后，选择*保存更改*。
7. 确认您为每个更改的部分选择了*保存更改*。

本地用户重复

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、而您从租户的源网格复制了一个用户、则复制的用户将克隆到租户的目标网格。

步骤

1. 选择 * 访问管理 * > * 用户 * 。
2. 选中要复制的用户对应的复选框。
3. 选择 * 操作 * > * 复制用户 * 。
4. 请参见 创建本地用户 有关输入内容的详细信息。

5. 选择 * 创建用户 * 。

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、而您删除了本地用户、则StorageGRID 不会删除其他网格上的相应用户。如果需要使此信息保持同步、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对应的复选框。
3. 选择*Actions*>*Delete user*或*Actions*>*Delete user*。

   此时将显示确认对话框。

4. 选择*删除用户*或*删除用户*。