管理组

StorageGRID 11.5

NetApp
April 11, 2024

目录

管理组

您可以为用户组分配权限，以控制租户用户可以执行的任务。您可以从身份源（例如 Active Directory 或 OpenLDAP ）导入联合组，也可以创建本地组。

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，但他们可以根据组权限访问 S3 和 Swift 资源。

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。由于缓存，更改可能需要长达 15 分钟才能生效。

权限	**Description**
根访问	提供对租户管理器和租户管理 API 的完全访问权限。 • 注： * 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	仅限 S3 租户。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 * 存储（ S3 ） * > * 我的 S3 访问密钥 * 菜单选项。

权限	Description
管理所有分段	• 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。 没有此权限的用户不会看到 * 分段 * 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： * 您只能通过租户管理 API 为 Swift 组分配 " 管理所有分段 " 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	仅限 S3 租户。允许用户使用租户管理器或租户管理 API 创建或编辑端点，这些端点用作 StorageGRID 平台服务的目标。 没有此权限的用户不会看到 * 平台服务端点 * 菜单选项。

相关信息

"使用 S3"

"使用 Swift"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选择 * 创建组 * 。
3. 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。

4. 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。
5. 选择 * 继续 * 。
6. 选择访问模式。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。
   - * 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。他们不能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。
7. 选择此组的组权限。

   请参见有关租户管理权限的信息。

8. 选择 * 继续 * 。
9. 选择组策略以确定此组的成员将拥有哪些 S3 访问权限。
   - * 无 S3 访问 * ： 默认值。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。您不能编辑此字符串。

- * 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。您不能编辑此字符串。
- * 自定义 * ： 组中的用户将获得您在文本框中指定的权限。有关组策略的详细信息，包括语言语法和示例，请参见实施 S3 客户端应用程序的说明。

10. 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。

    在此示例中，只允许组成员列出和访问指定存储分段中与其用户名（密钥前缀）匹配的文件夹。请注意，在确定其他组策略和存储分段策略的隐私时，应考虑这些文件夹的访问权限。

11. 根据要创建的是联合组还是本地组，选择显示的按钮：

    - 联合组： * 创建组 *
    - 本地组： * 继续 *

    如果要创建本地组，请在选择 * 继续 * 后显示步骤 4 （添加用户）。对于联合组，不会显示此步骤。

12. 选中要添加到组的每个用户对应的复选框，然后选择 * 创建组 * 。

    或者，您也可以在不添加用户的情况下保存组。您可以稍后将用户添加到组中，也可以在添加新用户时选择组。

13. 选择 * 完成 * 。

    您创建的组将显示在组列表中。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

"使用 S3"

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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。
- 如果您计划导入联合组，则表示已配置身份联合，并且已配置的身份源中已存在此联合组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选择 * 创建组 * 。
3. 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。

4. 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。

5. 选择 * 继续 * 。
6. 选择访问模式。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。
   - * 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。他们不能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。
7. 设置组权限。
   - 如果用户需要登录到租户管理器或租户管理 API ，请选中 * 根访问 * 复选框。（默认）
   - 如果用户不需要访问租户管理器或租户管理 API ，请取消选中 * 根访问 * 复选框。例如，取消选中不需要访问租户的应用程序对应的复选框。然后，分配 * Swift 管理员 * 权限，以允许这些用户管理容器和对象。
8. 选择 * 继续 * 。
9. 如果用户需要能够使用 Swift REST API ，请选中 * Swift administrator* 复选框。

   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。
10. 根据要创建的是联合组还是本地组，选择显示的按钮：
    - 联合组： * 创建组 *
    - 本地组： * 继续 *

      如果要创建本地组，请在选择 * 继续 * 后显示步骤 4 （添加用户）。对于联合组，不会显示此步骤。
11. 选中要添加到组的每个用户对应的复选框，然后选择 * 创建组 * 。

    或者，您也可以在不添加用户的情况下保存组。您可以稍后将用户添加到组中，也可以在创建新用户时选择组。
12. 选择 * 完成 * 。

    您创建的组将显示在组列表中。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

"使用 Swift"

查看和编辑组详细信息

查看组的详细信息时，您可以更改组的显示名称，权限，策略以及属于该组的用户。

您需要的内容

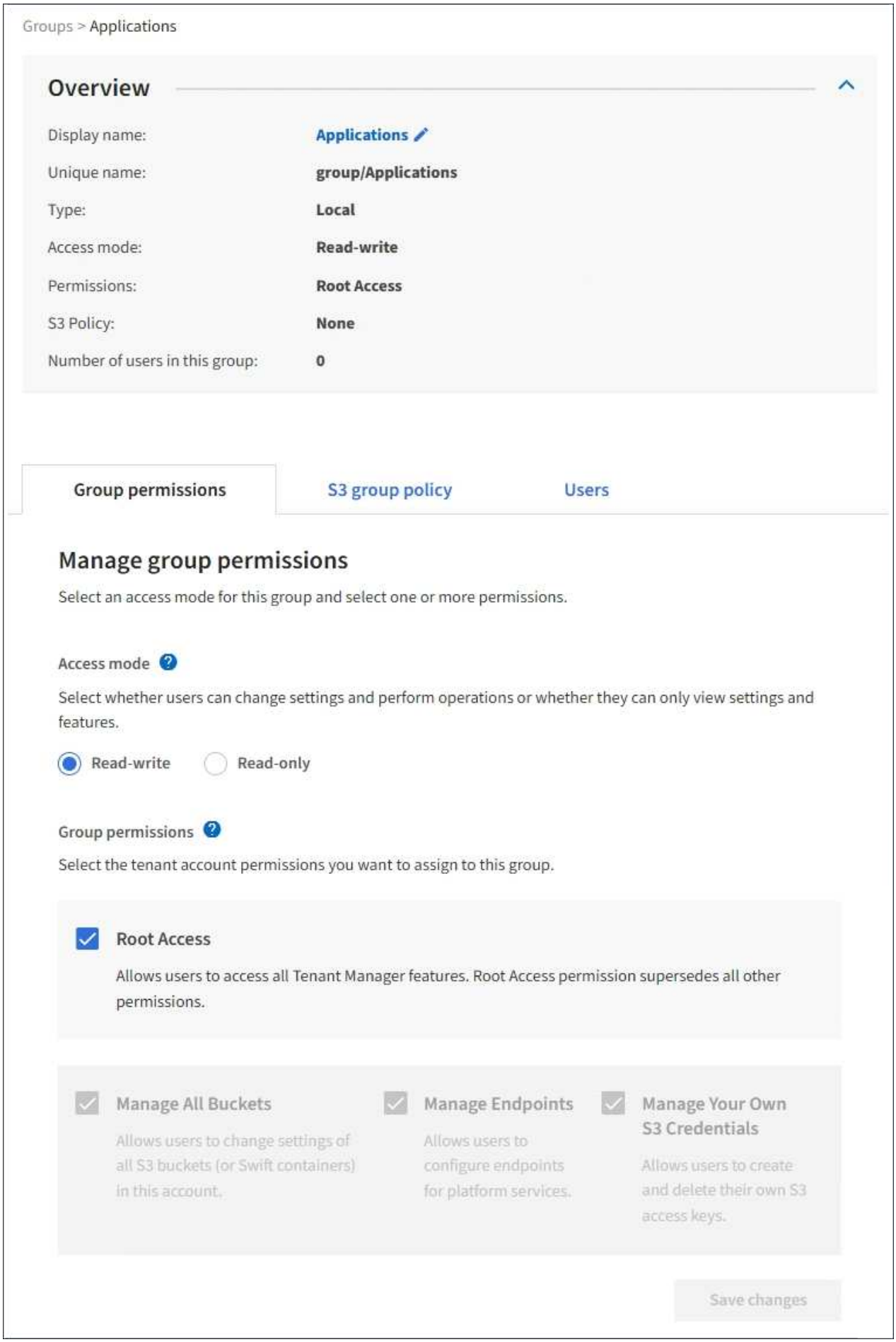
- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选择要查看或编辑其详细信息的组的名称。

   或者，您也可以选择 * 操作 * > * 查看组详细信息 * 。

   此时将显示组详细信息页面。以下示例显示了 S3 组详细信息页面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 根据需要更改组设置。

   要确保更改已保存，请在每个部分进行更改后选择 * 保存更改 * 。保存所做的更改后，页面右上角将显示一条确认消息。

   a. 也可以选择显示名称或编辑图标 更新显示名称。

      您不能更改组的唯一名称。您不能编辑联合组的显示名称。

   b. 也可以更新权限。

   c. 对于组策略，请为 S3 或 Swift 租户进行相应的更改。

      - 如果要编辑 S3 租户的组，也可以选择其他 S3 组策略。如果选择自定义 S3 策略，请根据需要更新 JSON 字符串。
      - 如果要编辑 Swift 租户的组，也可以选中或取消选中 * Swift 管理员 * 复选框。

        有关 Swift 管理员权限的详细信息，请参见有关为 Swift 租户创建组的说明。

   d. 也可以添加或删除用户。

4. 确认您已为更改的每个部分选择 * 保存更改 * 。

   由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"为S3租户创建组"

"为Swift租户创建组"

将用户添加到本地组

您可以根据需要将用户添加到本地组。

您需要的内容

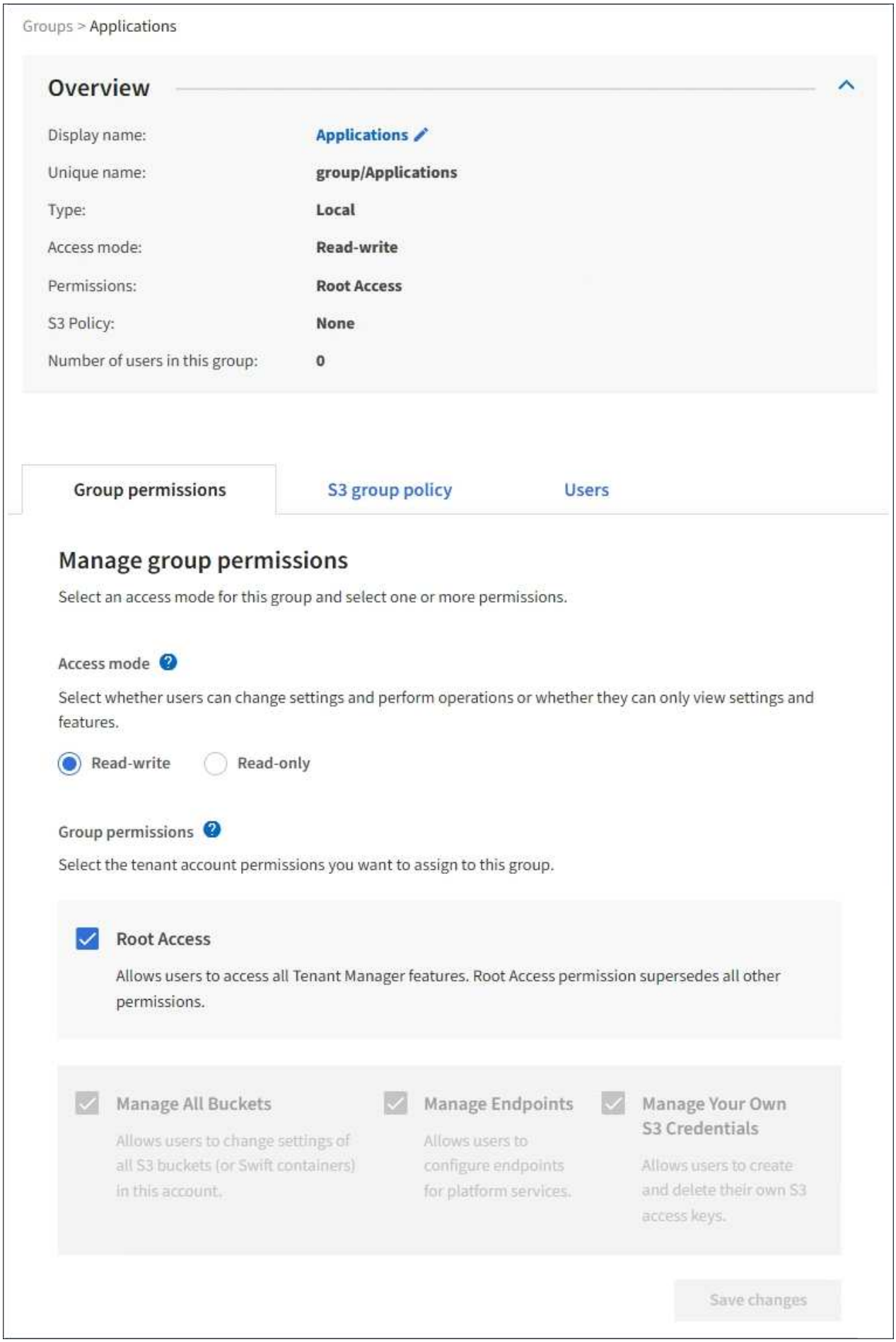
- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

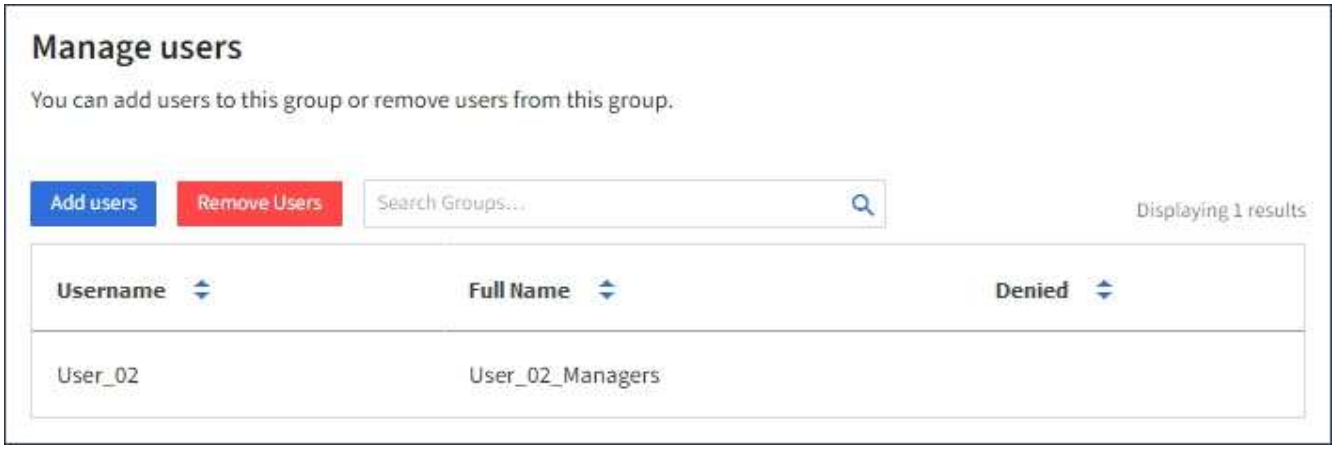
1. 选择 * 访问管理 * > * 组 * 。
2. 选择要将用户添加到的本地组的名称。

   或者，您也可以选择 * 操作 * > * 查看组详细信息 * 。

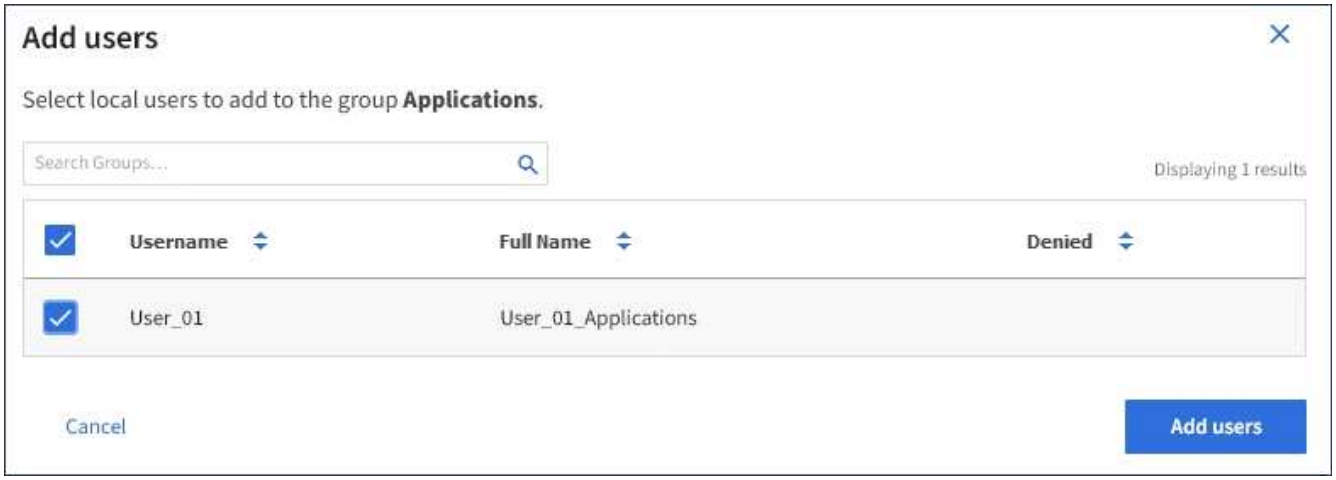
   此时将显示组详细信息页面。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 选择*管理用户*、然后选择*添加用户*。



4. 选择要添加到组中的用户，然后选择 * 添加用户 * 。



页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

编辑组名称

您可以编辑组的显示名称。您不能编辑组的唯一名称。

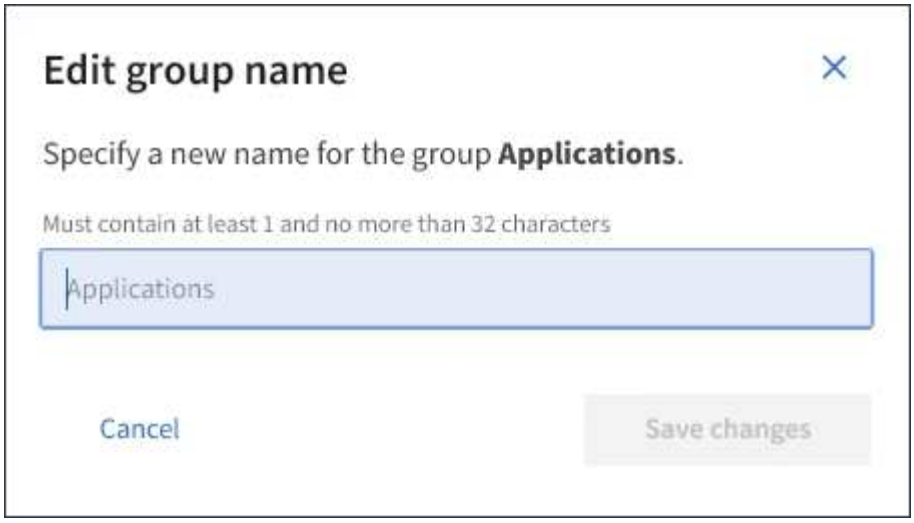
您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。
2. 选中要编辑其显示名称的组对应的复选框。
3. 选择 * 操作 * > * 编辑组名称 * 。

   此时将显示编辑组名称对话框。



4. 如果要编辑本地组，请根据需要更新显示名称。

   您不能更改组的唯一名称。您不能编辑联合组的显示名称。

5. 选择 * 保存更改 * 。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"

复制组

您可以通过复制现有组来更快地创建新组。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

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 * 复制组 * 。有关创建组的其他详细信息、请参见有关为S3租户或Swift租户创建组的说明。
4. 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。

5. 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。

6. 选择 * 继续 * 。
7. 根据需要修改此组的权限。
8. 选择 * 继续 * 。
9. 如果要为 S3 租户复制组，可以根据需要从 * 添加 S3 策略 * 单选按钮中选择其他策略。如果选择了自定义策略，请根据需要更新 JSON 字符串。
10. 选择 * 创建组 * 。

相关信息

"为S3租户创建组"

"为Swift租户创建组"

"租户管理权限"

删除组

您可以从系统中删除组。仅属于该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。

您需要的内容

- 您必须使用支持的浏览器登录到租户管理器。
- 您必须属于具有 root 访问权限的用户组。

步骤

1. 选择 * 访问管理 * > * 组 * 。

2. 选中要删除的组对应的复选框。
3. 选择 * 操作 * > * 删除组 * 。

   此时将显示一条确认消息。

4. 选择 * 删除组 * 确认要删除确认消息中指示的组。

   页面右上角将显示一条确认消息。由于缓存，更改可能需要长达 15 分钟才能生效。

相关信息

"租户管理权限"