グループの管理
StorageGRID 11.5

NetApp
April 11, 2024

目次

グループの管理

テナントユーザが実行できるタスクを制御するには、ユーザグループに権限を割り当てます。Active Directory や OpenLDAP などのアイデンティティソースからフェデレーテッドグループをインポートすることも、ローカルグループを作成することもできます。

StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルユーザはテナントマネージャにサインインできません。ただし、グループの権限に基づいて S3 リソースと Swift リソースにアクセスすることはできます。

テナント管理権限

テナントグループを作成する前に、そのグループに割り当てる権限を検討してください。テナント管理権限は、 Tenant Manager またはテナント管理 API を使用してユーザが実行できるタスクを決定します。ユーザは 1 つ以上のグループに属することができます。権限は、ユーザが複数のグループに属している場合に累積されます。

Tenant Manager にサインインするには、またはテナント管理 API を使用するには、少なくとも 1 つの権限が割り当てられたグループにユーザが属している必要があります。サインインできるすべてのユーザは、次のタスクを実行できます。

- ダッシュボードを表示します
- 自分のパスワードを変更する（ローカルユーザの場合）

すべての権限について、グループのアクセスモード設定によって、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかが決まります。

ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

グループには次の権限を割り当てることができます。S3 テナントと Swift テナントではグループの権限が異なるので注意してください。キャッシングに時間がかかるため変更には最大で 15 分を要します。

アクセス権	説明
ルートアクセス（ Root Access ）	Tenant Manager とテナント管理 API へのフルアクセスを提供します。 • 注： * Swift ユーザがテナントアカウントにサインインするには、 Root Access 権限が必要です。
管理者	Swift テナントのみ。このテナントアカウントの Swift コンテナとオブジェクトへのフルアクセスを提供します • 注： * Swift ユーザが Swift REST API を使用して処理を実行するには、 Swift 管理者の権限が必要です。

アクセス権	説明
自分の S3 クレデンシャルを管理します	S3 テナントのみ。ユーザに自分の S3 アクセスキーの作成および削除を許可します。この権限を持たないユーザには、「 * storage （ S3 ） * > * My S3 access keys * 」メニューオプションは表示されません。
すべてのバケットを管理します	• S3 テナント： S3 のバケットまたはグループポリシーに関係なく、ユーザに Tenant Manager とテナント管理 API を使用して S3 バケットの作成と削除を許可し、テナントアカウント内のすべての S3 バケットの設定を管理することを許可します。 この権限を持たないユーザには、 **Bucket** メニューオプションは表示されません。 • Swift テナント： Swift ユーザにテナント管理 API を使用して Swift コンテナの整合性レベルを制御することを許可します。 • 注： * テナント管理 API から Swift グループに割り当てることができるのは、 Manage All Buckets 権限だけです。この権限は、 Tenant Manager を使用して Swift グループに割り当てることはできません。
エンドポイントを管理します	S3 テナントのみ。ユーザが Tenant Manager またはテナント管理 API を使用して、 StorageGRID プラットフォームサービスのデスティネーションとして使用するエンドポイントを作成または編集できるようにします。 この権限を持たないユーザーには、 * プラットフォームサービスエンドポイント * メニューオプションは表示されません。

関連情報

"S3 を使用する"

"Swift を使用します"

S3テナント用のグループの作成

S3 ユーザグループの権限を管理するには、フェデレーテッドグループをインポートするか、ローカルグループを作成します。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、フェデレーテッドグループが設定済みのアイデンティティソースにすでに存在している必要があります。

手順

1. * access management * > * Groups * を選択します。

2. 「 * グループを作成 * 」を選択します。
3. [ローカルグループ *] タブを選択してローカルグループを作成するか、または [フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

4. グループの名前を入力します。
   - * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
   - * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です `sAMAccountName` 属性（Attribute）：OpenLDAPの場合は、に関連付けられている一意の名前です `uid` 属性（Attribute）：
5. 「 * Continue * 」を選択します。
6. アクセスモードを選択します。ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。
   - * Read-Write * （デフォルト）：ユーザは Tenant Manager にログインしてテナントの設定を管理できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Tenant Manager またはテナント管理 API では、変更や処理を実行することはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。
7. このグループのグループ権限を選択します。

   テナント管理権限に関する情報を参照してください。

8. 「 * Continue * 」を選択します。
9. グループポリシーを選択して、このグループのメンバーに付与する S3 アクセス権限を決定します。

- * S3 アクセスなし * ：デフォルト。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザは S3 リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- * 読み取り専用アクセス * ：このグループのユーザには、 S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * フルアクセス * ：このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * カスタム * ：グループ内のユーザーには、テキストボックスで指定した権限が付与されます。言語の構文や例など、グループポリシーの詳細については、 S3 クライアントアプリケーションを実装する手順を参照してください。

10. 「 * Custom * 」を選択した場合は、グループポリシーを入力します。各グループポリシーのサイズは 5 、 120 バイトまでに制限されています。有効な JSON 形式の文字列を入力する必要があります。

    この例では、指定したバケット内のユーザ名（キープレフィックス）に一致するフォルダの表示とアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

11. フェデレーテッドグループとローカルグループのどちらを作成するかに応じて、表示されるボタンを選択します。

    - フェデレーテッドグループ： * グループを作成 *
    - ローカルグループ： * 続行 *

ローカルグループを作成している場合は、「 * Continue * 」を選択すると、ステップ 4 （ユーザーの追加）が表示されます。この手順は、フェデレーテッドグループに対しては表示されません。

12. グループに追加する各ユーザーのチェックボックスをオンにし、 * グループの作成 * を選択します。

    必要に応じて、ユーザを追加せずにグループを保存することもできます。後でグループにユーザを追加することも、新しいユーザを追加するときにグループを選択することもできます。

13. [完了] を選択します。

    作成したグループがグループのリストに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

"S3 を使用する"

Swiftテナント用のグループの作成

Swift テナントアカウントに対するアクセス権限を管理するには、フェデレーテッドグループをインポートするか、ローカルグループを作成します。Swift テナントアカウントのコンテナとオブジェクトを管理するには、少なくとも 1 つのグループが Swift 管理者権限を持っている必要があります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、フェデレーテッドグループが設定済みのアイデンティティソースにすでに存在している必要があります。

手順

1. * access management * > * Groups * を選択します。

2. 「 * グループを作成 * 」を選択します。
3. [ローカルグループ *] タブを選択してローカルグループを作成するか、または [フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

4. グループの名前を入力します。
   - * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
   - * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です `sAMAccountName` 属性（Attribute）：OpenLDAPの場合は、に関連付けられている一意の名前です `uid` 属性（Attribute）：
5. 「 * Continue * 」を選択します。
6. アクセスモードを選択します。ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。
   - * Read-Write * （デフォルト）：ユーザは Tenant Manager にログインしてテナントの設定を管理できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Tenant Manager またはテナント管理 API では、変更や処理を実行することはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。
7. グループ権限を設定します。
   - ユーザが Tenant Manager またはテナント管理 API にサインインする必要がある場合は、 * Root Access * チェックボックスをオンにします。（デフォルト）
   - ユーザが Tenant Manager またはテナント管理 API にアクセスする必要がない場合は、 * Root Access * チェックボックスをオフにします。たとえば、テナントにアクセスする必要がないアプリケーションのチェックボックスをオフにします。次に、 * Swift Administrator * 権限を割り当てて、これらのユー

ザにコンテナとオブジェクトの管理を許可します。

8. 「 * Continue * 」を選択します。
9. Swift REST API を使用する必要がある場合は、 * Swift 管理者 * チェックボックスを選択します。

   Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

10. フェデレーテッドグループとローカルグループのどちらを作成するかに応じて、表示されるボタンを選択します。
    - フェデレーテッドグループ： * グループを作成 *
    - ローカルグループ： * 続行 *

      ローカルグループを作成している場合は、「 * Continue * 」を選択すると、ステップ 4 （ユーザーの追加）が表示されます。この手順は、フェデレーテッドグループに対しては表示されません。

11. グループに追加する各ユーザーのチェックボックスをオンにし、 * グループの作成 * を選択します。

    必要に応じて、ユーザを追加せずにグループを保存することもできます。このグループにあとでユーザを追加することも、新しいユーザを作成するときにグループを選択することもできます。

12. [完了] を選択します。

    作成したグループがグループのリストに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

"Swift を使用します"

グループの詳細を表示および編集する

グループの詳細を表示する際に、グループの表示名、権限、ポリシー、およびグループに属するユーザを変更することができます。

必要なもの

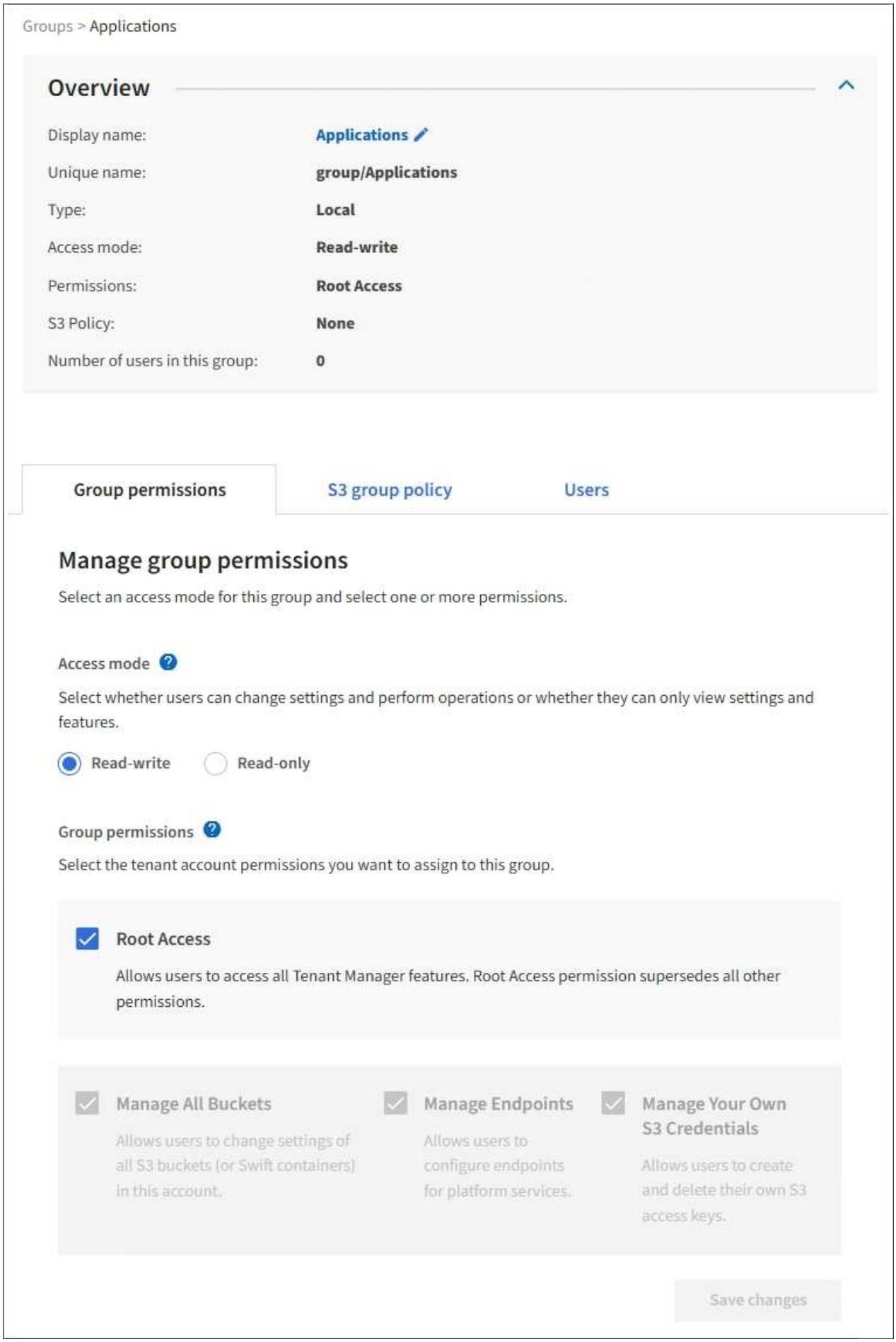
- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 詳細を表示または編集するグループの名前を選択します。

   または、 * Actions * > * View group details * を選択します。

   グループの詳細ページが表示されます。次の例は、 S3 グループの詳細ページを表示します。


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. 必要に応じてグループ設定を変更します。

   変更内容を確実に保存するには、各セクションで変更を行った後に「変更を保存」を選択します。変更を保存すると、ページの右上に確認メッセージが表示されます。

   a. 必要に応じて、表示名または編集アイコンを選択します 表示名を更新します。

      グループの一意の名前は変更できません。フェデレーテッドグループの表示名は編集できません。

   b. 必要に応じて、権限を更新します。

   c. グループポリシーの場合は、 S3 または Swift テナントに適した変更を行います。

      - S3 テナントのグループを編集する場合は、必要に応じて別の S3 グループポリシーを選択します。カスタムの S3 ポリシーを選択した場合は、 JSON 文字列を必要に応じて更新します。
      - Swift テナントのグループを編集する場合は、必要に応じて、 * Swift Administrator * チェックボックスをオンまたはオフにします。

        Swift Administrator 権限の詳細については、 Swift テナント用のグループを作成する手順を参照してください。

   d. 必要に応じて、ユーザを追加または削除します。

4. 変更したセクションごとに「変更を保存」を選択したことを確認します。

   キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"S3テナント用のグループの作成"

"Swiftテナント用のグループの作成"

ローカルグループへのユーザの追加

必要に応じて、ローカルグループにユーザを追加できます。

必要なもの

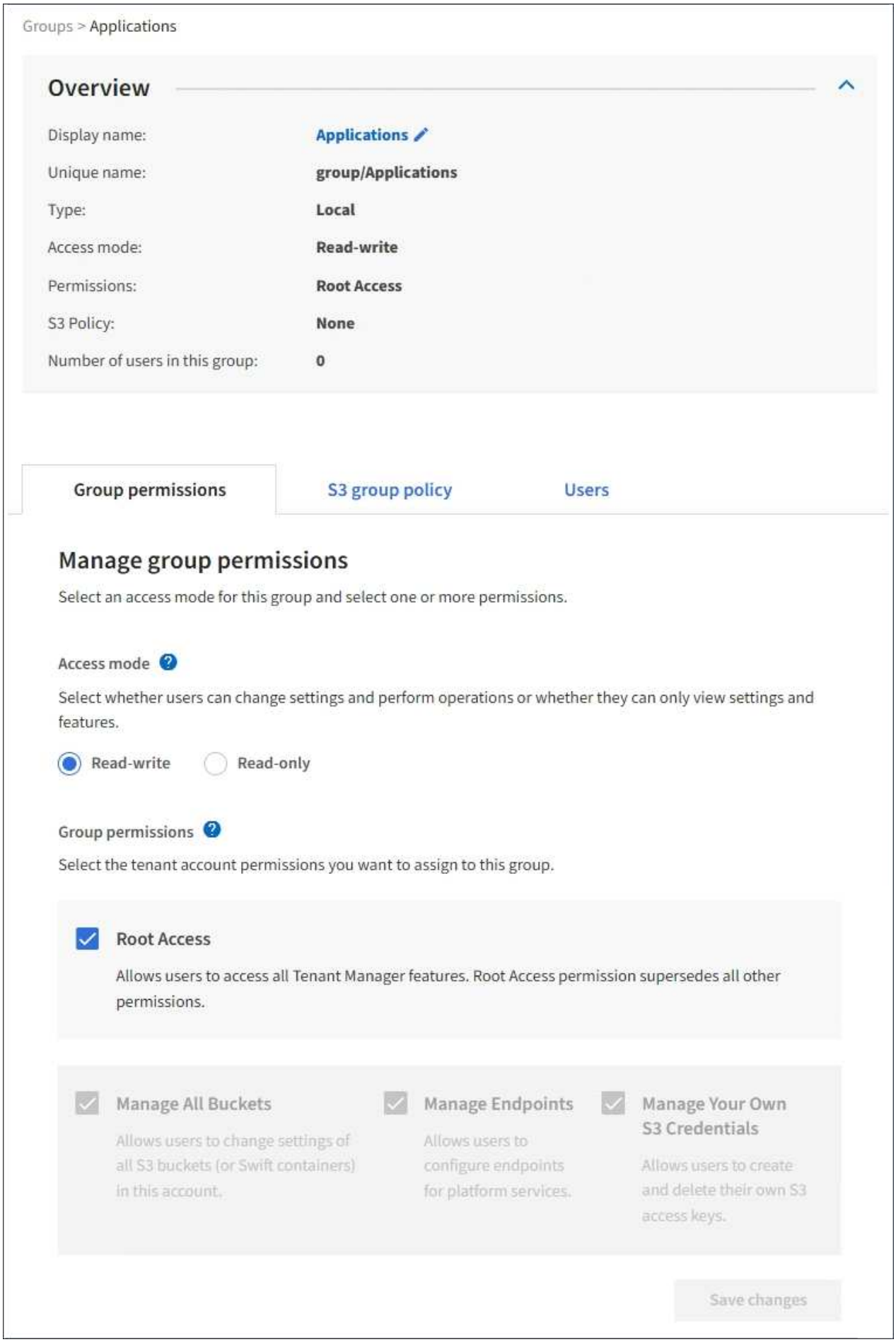
- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

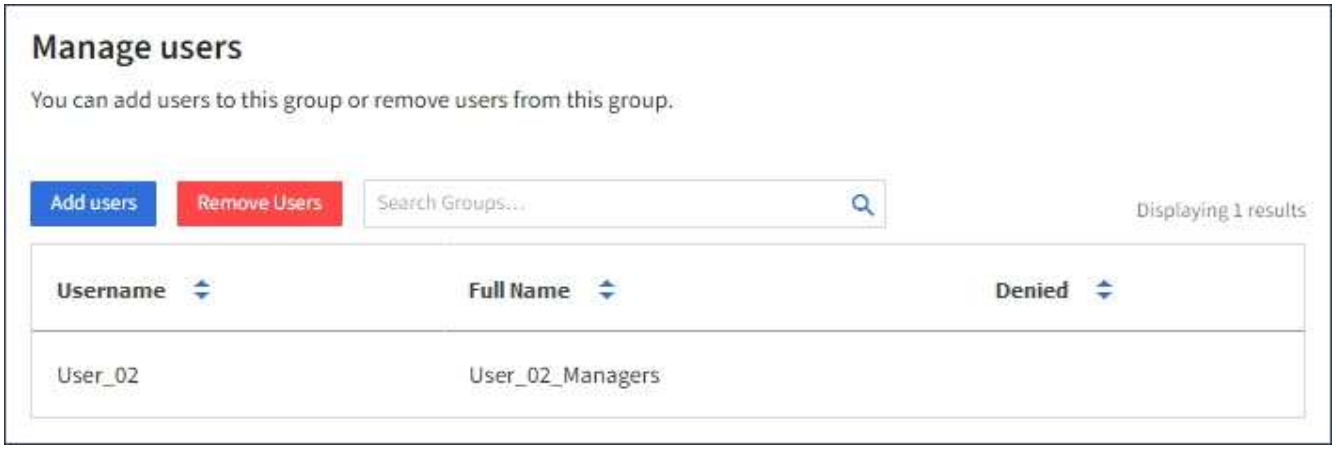
1. * access management * > * Groups * を選択します。
2. ユーザを追加するローカルグループの名前を選択します。

   または、 * Actions * > * View group details * を選択します。

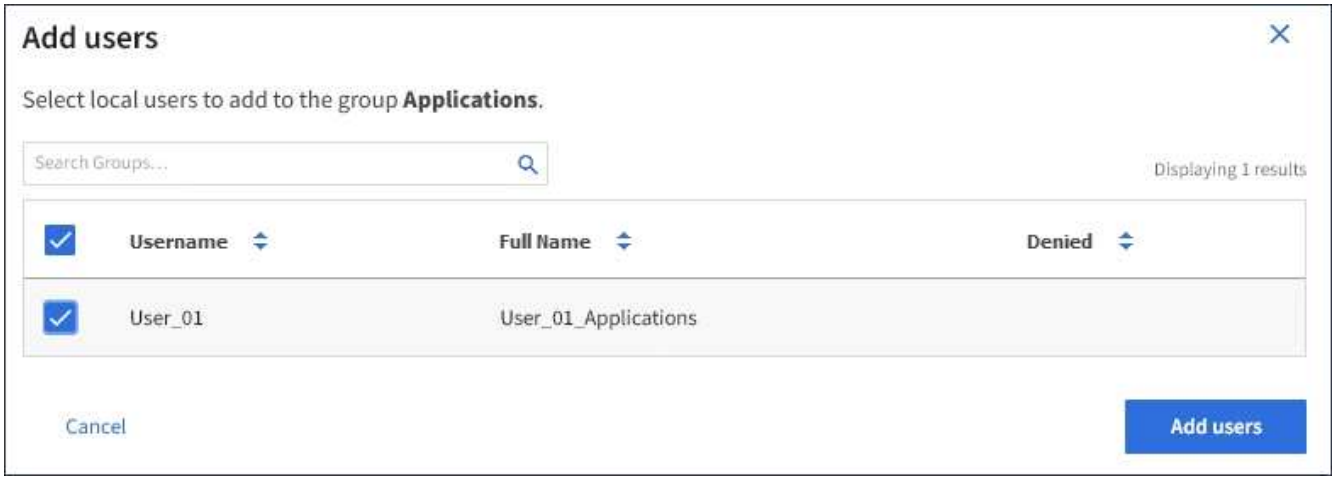
   グループの詳細ページが表示されます。


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. 「ユーザーの管理」を選択し、「ユーザーの追加」を選択します。



4. グループに追加するユーザーを選択し、 * ユーザーの追加 * を選択します。



ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

グループ名を編集する

グループの表示名を編集できます。グループの一意の名前は編集できません。

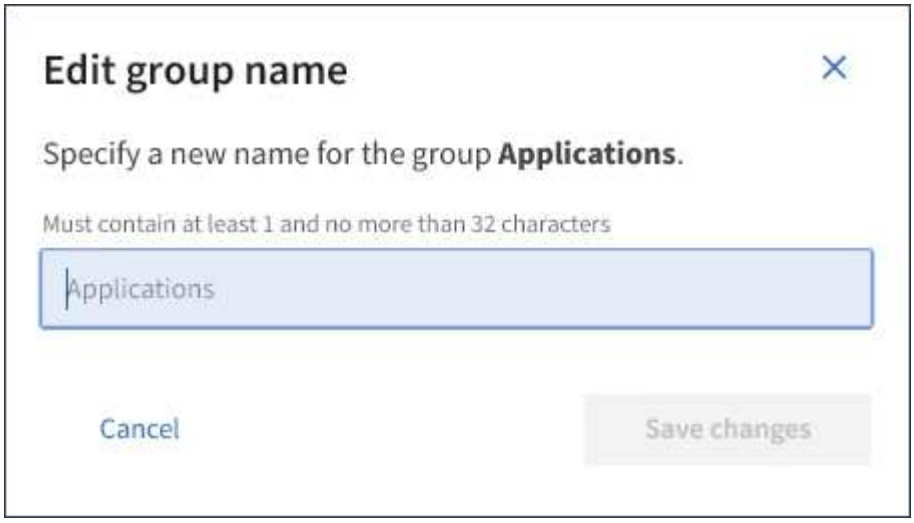
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 表示名を編集するグループのチェックボックスを選択します。
3. [* アクション * > * グループ名の編集 *] を選択します。

   Edit group name （グループ名の編集）ダイアログボックスが表示されます。



4. ローカルグループを編集する場合は、必要に応じて表示名を更新します。

   グループの一意の名前は変更できません。フェデレーテッドグループの表示名は編集できません。

5. 「変更を保存」を選択します。

   ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

グループを複製する

既存のグループを複製することで、新しいグループをより迅速に作成できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 複製するグループのチェックボックスをオンにします。
3. 「 * グループを複製 * 」を選択します。グループの作成の詳細については、S3テナントまたはSwiftテナントのグループを作成する手順を参照してください。
4. [ローカルグループ *] タブを選択してローカルグループを作成するか、または [フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

5. グループの名前を入力します。

- * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
- * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です `sAMAccountName` 属性（Attribute）：OpenLDAPの場合は、に関連付けられている一意の名前です `uid` 属性（Attribute）：

6. 「 * Continue * 」を選択します。
7. 必要に応じて、このグループの権限を変更します。
8. 「 * Continue * 」を選択します。
9. 必要に応じて、 S3 テナントのグループを複製する場合は、 * S3 ポリシーの追加 * オプションボタンとは別のポリシーを選択します。カスタムポリシーを選択した場合は、 JSON 文字列を必要に応じて更新します。
10. 「 * グループを作成 * 」を選択します。

関連情報

"S3テナント用のグループの作成"

"Swiftテナント用のグループの作成"

"テナント管理権限"

グループを削除しています

システムからグループを削除できます。そのグループに属するユーザは、 Tenant Manager にサインインしたりテナントアカウントを使用したりすることはできなくなります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。

2. 削除するグループのチェックボックスを選択します。
3. [* アクション * > * グループの削除 *] を選択します。

   確認メッセージが表示されます。

4. ［ * グループの削除 * ］ を選択して、確認メッセージに示されたグループを削除することを確認します。

   ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

著作権に関する情報

商標に関する情報