システムアクセスの管理
StorageGRID

NetApp
October 03, 2025

目次

システムアクセスの管理

アイデンティティフェデレーションを使用する

アイデンティティフェデレーションを使用すると、テナントグループとテナントユーザを迅速に設定できます。またテナントユーザは、使い慣れたクレデンシャルを使用してテナントアカウントにサインインできます。

Tenant Manager 用のアイデンティティフェデレーションを設定する

テナントグループとユーザを Active Directory 、 Azure Active Directory （ Azure AD ）、 OpenLDAP 、 Oracle Directory Server などの別のシステムで管理する場合は、 Tenant Manager 用のアイデンティティフェデレーションを設定できます。

必要なもの

- Tenant Manager にはを使用してサインインします サポートされている Web ブラウザ。
- 特定のアクセス権限が必要です。
- アイデンティティプロバイダとして Active Directory 、 Azure AD 、 OpenLDAP 、または Oracle Directory Server を使用している。

> 記載されていない LDAP v3 サービスを使用する場合は、テクニカルサポートにお問い合わせください。

- OpenLDAP を使用する場合は、 OpenLDAP サーバを設定する必要があります。を参照してください OpenLDAP サーバの設定に関するガイドライン。
- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。を参照してください 発信 TLS 接続でサポートされる暗号。

このタスクについて

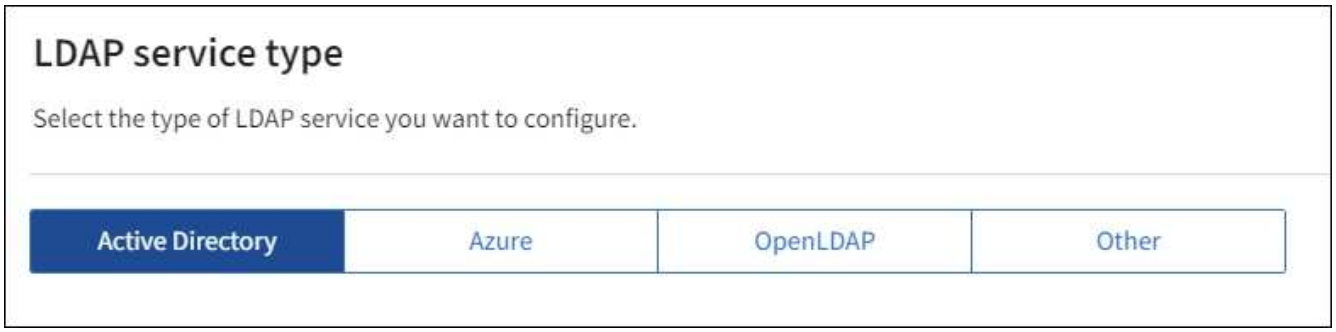
テナントにアイデンティティフェデレーションサービスを設定できるかどうかは、テナントアカウントの設定方法によって異なります。テナントが Grid Manager 用に設定されたアイデンティティフェデレーションサービスを共有する場合があります。アイデンティティフェデレーションページにアクセスしたときにこのメッセージが表示される場合は、このテナント用に別のフェデレーテッドアイデンティティソースを設定することはできません。

> 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.

構成を入力します

手順

1. アクセス管理 * > * アイデンティティフェデレーション * を選択します。
2. ［ * アイデンティティフェデレーションを有効にする * ］ を選択
3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。



Oracle Directory Server を使用する LDAP サーバーの値を設定するには、 * その他 * を選択します。

4. [* その他 *] を選択した場合は、 [LDAP 属性] セクションのフィールドに入力します。それ以外の場合は、次の手順に進みます。
   - * User Unique Name * ： LDAP ユーザの一意な ID が含まれている属性の名前。この属性は、 Active Directory の場合は「 sAMAccountName 」、 OpenLDAP の場合は「 uid 」に相当します。Oracle Directory Server を設定する場合は 'uid' と入力します
   - * User UUID * ： LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性は、 Active Directory の場合は「 objectGUID 」、 OpenLDAP の場合は「 entryUUID 」に相当します。Oracle Directory Server を設定する場合は 'nsuniqueID' と入力します指定した属性の各ユーザの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - * Group Unique Name * ： LDAP グループの一意な ID が含まれている属性の名前。この属性は、 Active Directory の場合は「 sAMAccountName 」、 OpenLDAP の場合は「 cn 」に相当します。Oracle Directory Server を設定する場合は、「 cn 」と入力します。
   - * グループ UUID * ： LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性は、 Active Directory の場合は「 objectGUID 」、 OpenLDAP の場合は「 entryUUID 」に相当します。Oracle Directory Server を設定する場合は 'nsuniqueID' と入力します指定した属性の各グループの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. すべての LDAP サービスタイプについて、 LDAP サーバの設定セクションに必要な LDAP サーバおよびネットワーク接続情報を入力します。
   - * Hostname * ： LDAP サーバの完全修飾ドメイン名（ FQDN ）または IP アドレス。
   - * Port * ： LDAP サーバへの接続に使用するポート。

     STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。

   - * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

     Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

     指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

     - 「 sAMAccountName 」または「 uid 」
     - 「 objectGUID 」、「 entryUUID 」、または「 nsUniqueID 」
     - 「 cn 」

- 「 memberOf 」または「 isMemberOf 」
- **Active Directory**:`objectSID’primaryGroupID’userAccountControl’userPrincipalName`
- **azure**:'accountEnabled' および 'userPrincipalName'

◦ * Password * ：ユーザ名に関連付けられたパスワード。

◦ * Group Base DN * ：グループを検索する LDAP サブツリーの識別名（ DN ）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。

> * グループの一意な名前 * 値は、所属する * グループベース DN * 内で一意である必要があります。

◦ * User Base DN * ：ユーザを検索する LDAP サブツリーの識別名（ DN ）の完全パス。

> * ユーザーの一意な名前 * 値は、それぞれが属する * ユーザーベース DN * 内で一意である必要があります。

◦ * バインドユーザー名形式 * （オプション）：パターンが自動的に判別できない場合は、デフォルトのユーザー名パターン StorageGRID が使用します。

StorageGRID がサービスアカウントにバインドできない場合にユーザがサインインできるようにするため、 * バインドユーザ名形式 * を指定することを推奨します。

次のいずれかのパターンを入力します。

- * UserPrincipalName パターン（ Active Directory および Azure ） * ： [username]@*example*.com
- * ダウンレベルのログオン名パターン (Active Directory および Azure)*:`*EXAMPLE*\[username]`
- * 識別名パターン *:`CN=[username] 、 CN=Users 、 DC=EXAMPLE_, DC=com`

記載されているとおりに * [username] * を含めます。

6. Transport Layer Security （ TLS ）セクションで、セキュリティ設定を選択します。

◦ * STARTTLS を使用 * ： STARTTLS を使用して LDAP サーバとの通信を保護します。Active Directory 、 OpenLDAP 、またはその他のオプションですが、 Azure ではこのオプションはサポートされていません。

◦ * LDAPS を使用 * ： LDAPS （ LDAP over SSL ）オプションでは、 TLS を使用して LDAP サーバへの接続を確立します。Azure ではこのオプションを選択する必要があります。

◦ * TLS を使用しないでください * ： StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。このオプションは Azure ではサポートされていません。

> Active Directory サーバで LDAP 署名が適用される場合、 [TLS を使用しない] オプションの使用はサポートされていません。STARTTLS または LDAPS を使用する必要があります。

7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。

◦ * オペレーティングシステムの CA 証明書を使用 * ：オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。

- * カスタム CA 証明書を使用 * ：カスタムセキュリティ証明書を使用します。

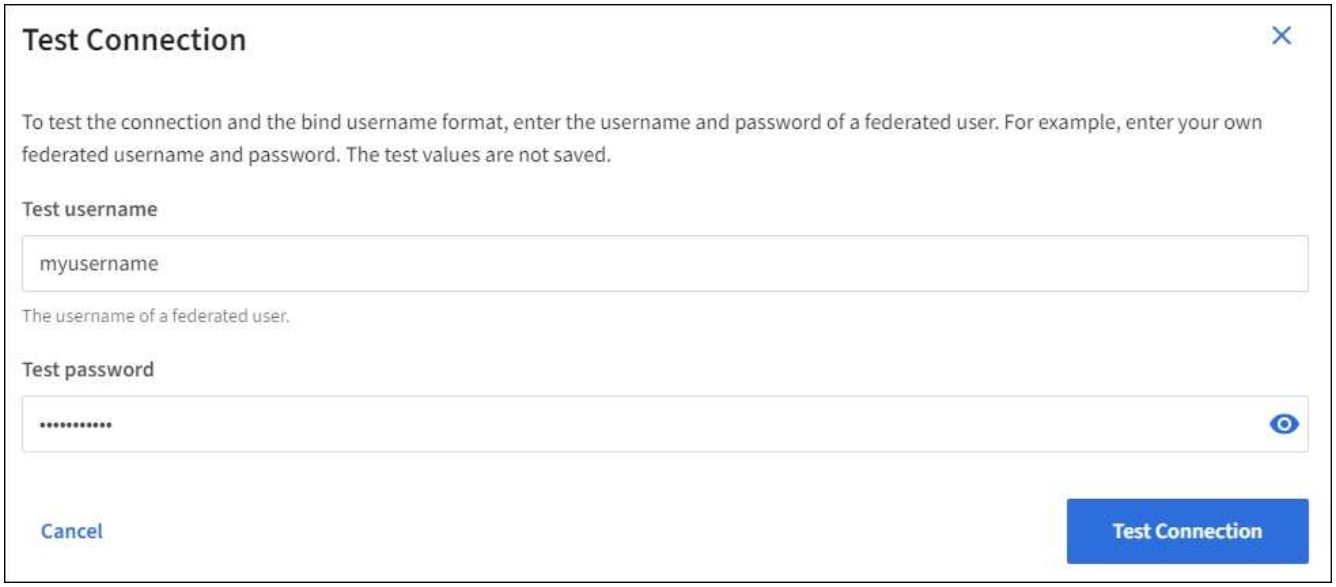
  この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

接続をテストして設定を保存します

すべての値を入力したら、設定を保存する前に接続をテストする必要があります。StorageGRID では、LDAP サーバの接続設定とバインドユーザ名の形式が指定されている場合は検証されます。

1. [接続のテスト *] を選択します。
2. バインドユーザ名の形式を指定しなかった場合は、次の手順を実行します。
   - 接続設定が有効である場合は、「 Test connection successful(接続のテストに成功しました) 」というメッセージが表示されます。[保存（ Save ）] を選択して、構成を保存します。
   - 接続設定が無効な場合は、「 test connection could not be established 」というメッセージが表示されます。[閉じる（ Close ）] を選択します。その後、問題を解決して接続を再度テストします。
3. バインドユーザ名の形式を指定した場合は、有効なフェデレーテッドユーザのユーザ名とパスワードを入力します。

   たとえば、自分のユーザ名とパスワードを入力します。ユーザ名に @ や / などの特殊文字は使用しないでください。



   - 接続設定が有効である場合は、「 Test connection successful(接続のテストに成功しました) 」というメッセージが表示されます。[保存（ Save ）] を選択して、構成を保存します。
   - 接続設定、バインドユーザ名形式、またはテストユーザ名とパスワードが無効な場合は、エラーメッセージが表示されます。問題を解決してから、もう一度接続をテストしてください。

アイデンティティソースとの強制同期

StorageGRID システムは、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およびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

手順

1. アイデンティティフェデレーションページに移動します。
2. ページの上部にある「 * サーバーを同期」を選択します。

   環境によっては、同期プロセスにしばらく時間がかかることがあります。

   アイデンティティフェデレーション同期エラー * アラートは、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とユーザを同期する問題 がある場合にトリガーされます。

アイデンティティフェデレーションを無効にする

グループとユーザのアイデンティティフェデレーションを一時的または永続的に無効にすることができます。アイデンティティフェデレーションを無効にすると、 StorageGRID とアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

このタスクについて

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRID システムとアイデンティティソース間の同期は行われず、同期されていないアカウントに対してはアラートやアラームが生成されません。
- シングルサインオン（ SSO ）が * Enabled * または * Sandbox Mode * に設定されている場合、 * アイデンティティフェデレーションを有効にする * チェックボックスは無効になります。アイデンティティフェデレーションを無効にするには、シングルサインオンページの SSO ステータスが * 無効 * になっている必要があります。を参照してください シングルサインオンを無効にします。

手順

1. アイデンティティフェデレーションページに移動します。
2. [アイデンティティフェデレーションを有効にする *] チェックボックスをオフにします。

OpenLDAP サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、 OpenLDAP サーバで特定の設定が必要です。

ActiveDirectory または Azure 以外の ID ソースについては、外部で無効になっているユーザへの S3 アクセスは StorageGRID によって自動的にブロックされません。S3 アクセスをブロックするには、ユーザの S3 キーをすべて削除し、すべてのグループからユーザを削除します。

memberof オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、『』のリバースグループメンバーシップのメンテナンス手順を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

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

また、パフォーマンスを最適化するには、 Username のヘルプで説明されているフィールドにインデックスを設定してください。

のリバースグループメンバーシップのメンテナンスに関する情報を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

グループを管理します

S3 テナント用のグループを作成します

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 にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- 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。を参照してください テナント管理権限。
- 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。

S3 の詳細については、を参照してください S3 を使用する。

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 の場合は 'sAMAccountName 属性に関連付けられた一意の名前ですOpenLDAP の場合 ' 一意の名前は 'uid' 属性に関連付けられている名前です
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。

Swift テナント用のグループを作成します

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 にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- 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 の場合は 'sAMAccountName 属性に関連付けられた一意の名前ですOpenLDAP の場合 ' 一意の名前は 'uid' 属性に関連付けられている名前です
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

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

グループの詳細を表示および編集します

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

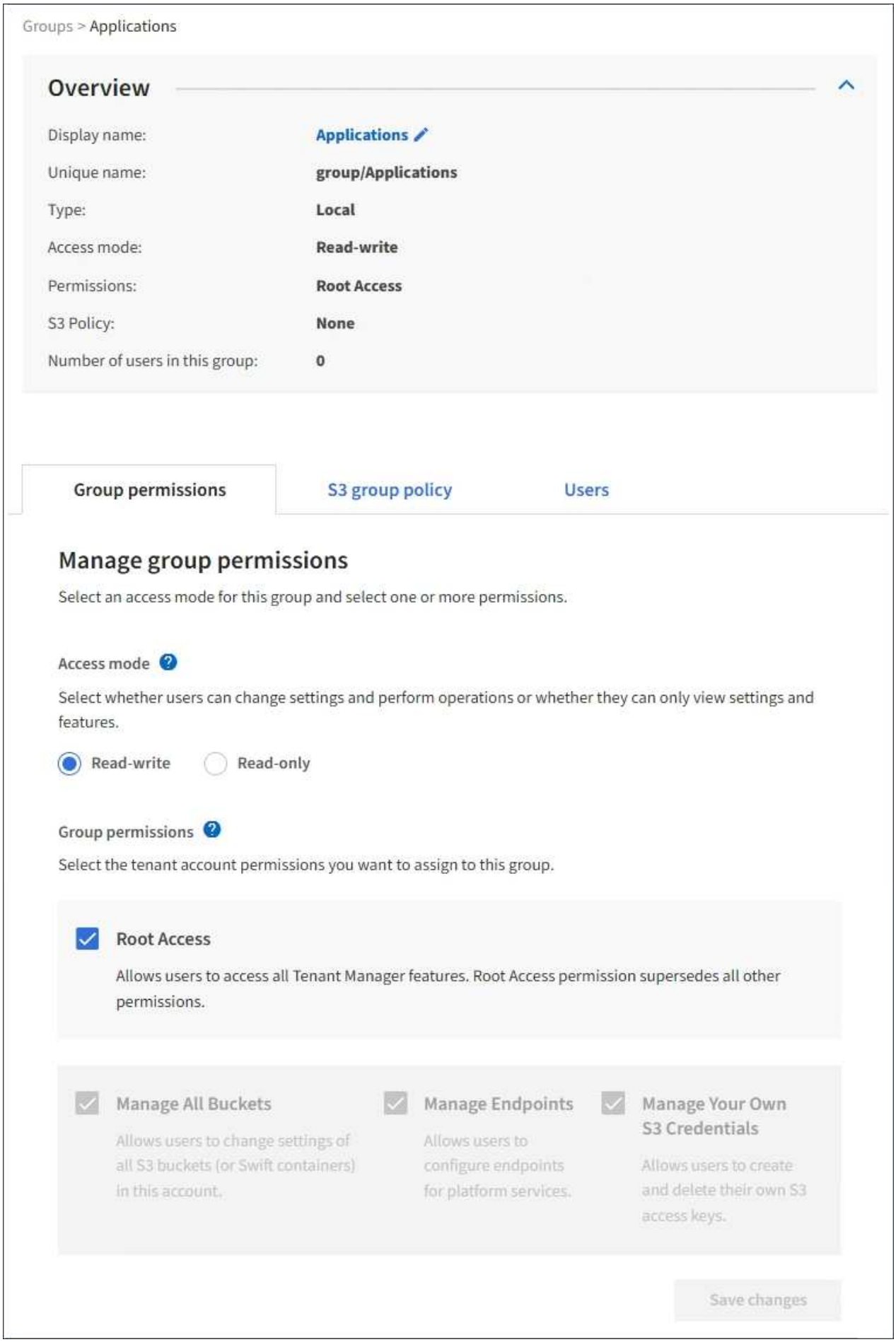
- Tenant Manager にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- Root Access 権限を持つユーザグループに属している必要があります。

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を作成します

Swift テナント用のグループを作成します

ローカルグループにユーザを追加します

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

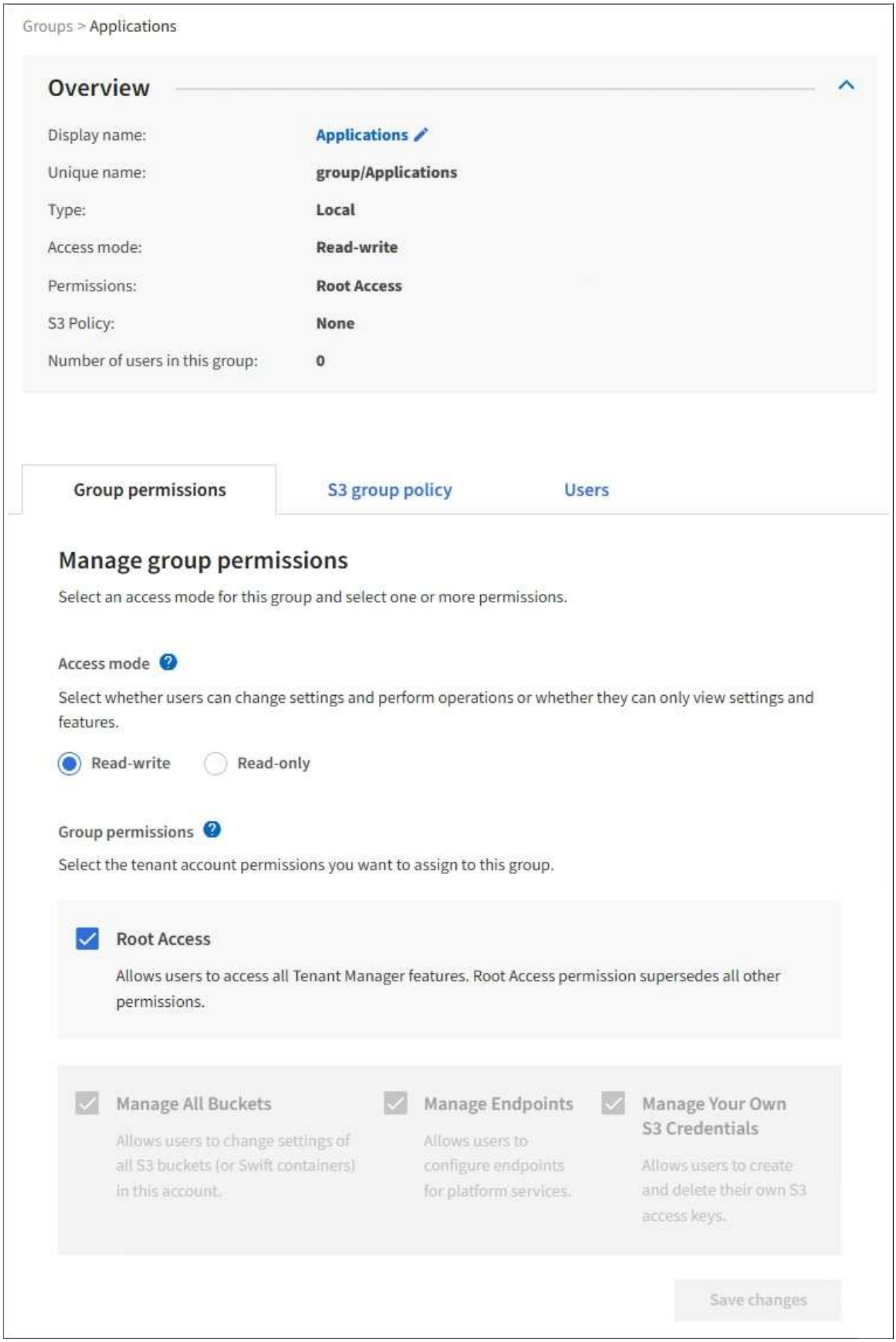
- Tenant Manager にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

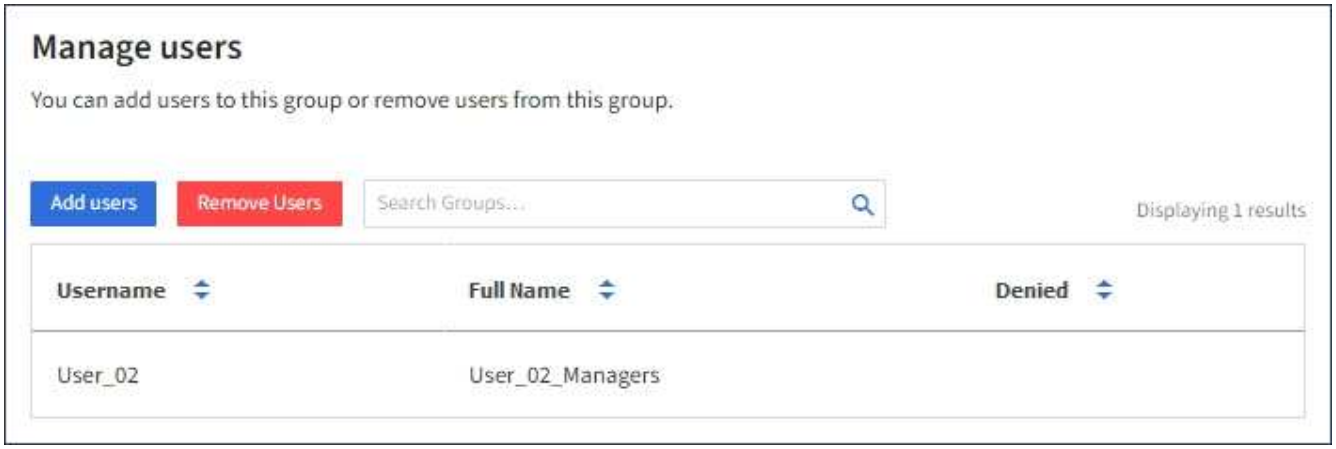
1. * access management * > * Groups * を選択します。
2. ユーザを追加するローカルグループの名前を選択します。

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

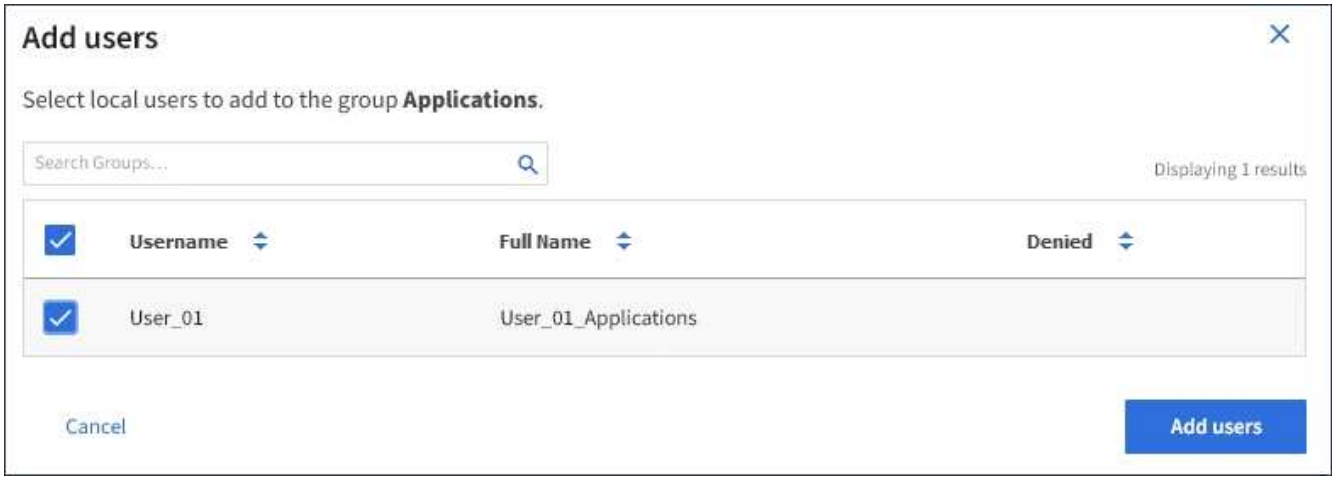
   グループの詳細ページが表示されます。


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. [**Users**] 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。

グループ名を編集します

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。

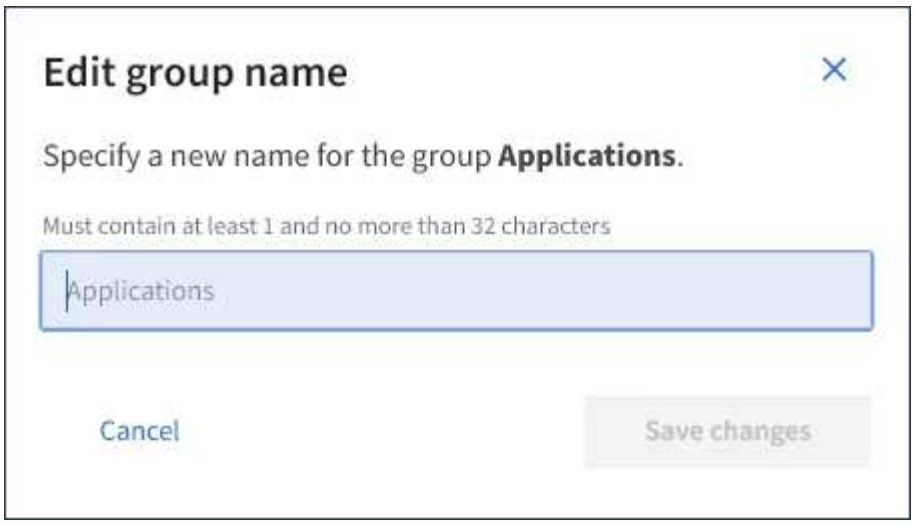
必要なもの

- Tenant Manager にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- 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。を参照してください テナント管理権限。

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。

グループが重複しています

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 にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- 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。を参照してください テナント管理権限。

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、のグループ作成手順を参照してください S3 テナント またはの場合 Swift テナント。
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テナントのリソースを管理できます。 グループの権限に基づきます。

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 の場合は 'sAMAccountName 属性に関連付けられた一意の名前ですOpenLDAP の場合 ' 一意の名前は 'uid' 属性に関連付けられている名前です

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。

グループを削除します

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 にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- 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。を参照してください テナント管理権限。

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。

ローカルユーザを管理します

ローカルユーザを作成してローカルグループに割り当て、ユーザがアクセスできる機能を決定することができます。Tenant Manager には、「 root 」という名前の事前定義されたローカルユーザが 1 つ含まれています。 ローカルユーザは追加および削除できますが、 root ユーザを削除することはできません。

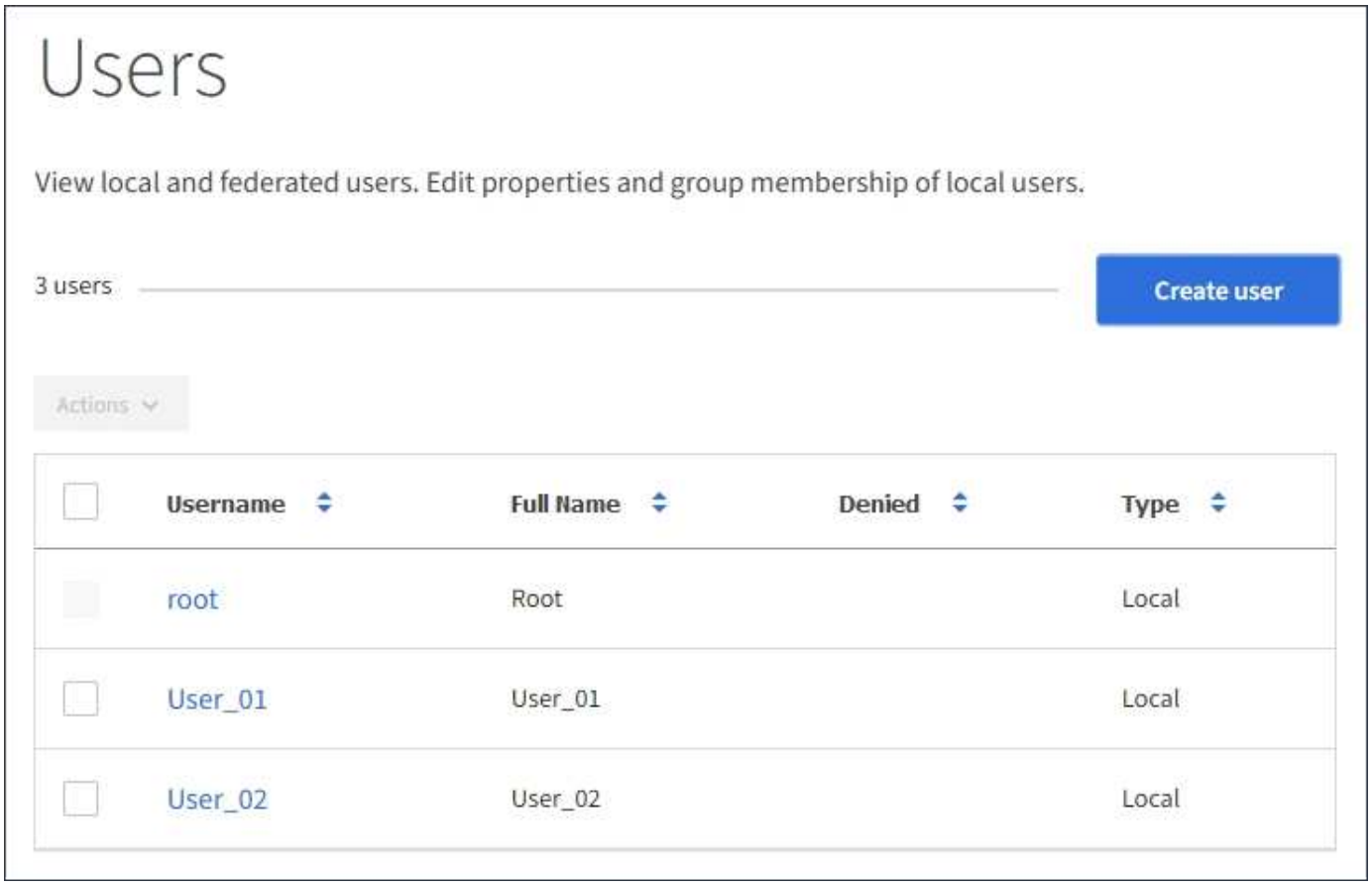
必要なもの

- Tenant Manager にはを使用してサインインする必要があります サポートされている Web ブラウザ。
- Root Access 権限が設定された読み取り / 書き込みユーザグループに属している必要があります。を参照してください テナント管理権限。

> 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またはテナント管理 API 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 または Swift クライアントアプリケーションを使用してテナントのリソースにアクセスすることはできます。

ユーザページにアクセスします

アクセス管理 * > * Users * を選択します。



ローカルユーザを作成する

ローカルユーザを作成して 1 つ以上のローカルグループに割り当て、ユーザのアクセス権限を制御することができます。

いずれのグループにも属していない S3 ユーザには、管理権限または S3 グループポリシーが適用されません。これらのユーザは、バケットポリシーを通じて S3 バケットアクセスを許可されている場合があります。

グループに属していない Swift ユーザには、管理権限または Swift コンテナへのアクセスは付与されません。

手順

1. 「 * ユーザーの作成 * 」を選択します。
2. 次のフィールドに値を入力します。
   - * フルネーム * ：このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
   - * ユーザ名 * ：このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。
   - * Password * ：ユーザがサインイン時に使用するパスワード。
   - * パスワードの確認 * ： [パスワード] フィールドに入力したパスワードと同じパスワードを入力します。
   - * アクセスを拒否 * ：「 * はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

たとえば、この機能を使用すると、ユーザが一時的にサインインできないようにすることができます。

3. 「 * Continue * 」を選択します。
4. 1 つ以上のローカルグループにユーザを割り当てます。

   グループに属していないユーザには管理権限は付与されません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。

5. 「 * ユーザーの作成 * 」を選択します。

   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。

ユーザの詳細を編集します

ユーザの詳細を編集する際に、ユーザのフルネームとパスワードを変更したり、ユーザを別のグループに追加したり、ユーザがテナントにアクセスできないようにしたりできます。

手順

1. [ユーザー] リストで、詳細を表示または編集するユーザーの名前を選択します。

   または、ユーザーのチェックボックスをオンにして、 * アクション * > * ユーザーの詳細を表示 * を選択することもできます。

2. 必要に応じてユーザ設定を変更します。
   a. フルネームまたは編集アイコンを選択して、必要に応じてユーザのフルネームを変更します をクリックします。

      ユーザ名は変更できません。

   b. [パスワード *] タブで、必要に応じてユーザーのパスワードを変更します。
   c. [* アクセス *] タブで、ユーザーがサインインすることを許可するか（ [* いいえ *] を選択）、ユーザーが必要に応じてサインインしないようにします（ [* はい *] を選択）。
   d. [* グループ *] タブで、ユーザーをグループに追加するか、必要に応じてグループから削除します。
   e. 必要に応じて、 [変更を保存（ Save Changes ）] を選択します。

      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。

ローカルユーザが重複しています

ローカルユーザを複製して新しいユーザを迅速に作成することができます。

手順

1. [ユーザー] リストで、複製するユーザーを選択します。
2. 「 * ユーザーを複製 * 」を選択します。
3. 新しいユーザの次のフィールドを変更します。

- * フルネーム * ：このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
- * ユーザ名 * ：このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。
- * Password * ：ユーザがサインイン時に使用するパスワード。
- * パスワードの確認 * ： [パスワード] フィールドに入力したパスワードと同じパスワードを入力します。
- * アクセスを拒否 * ：「 * はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

  たとえば、この機能を使用すると、ユーザが一時的にサインインできないようにすることができます。

4. 「 * Continue * 」を選択します。
5. 1 つ以上のローカルグループを選択します。

   グループに属していないユーザには管理権限は付与されません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。

6. 「 * ユーザーの作成 * 」を選択します。

   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。

ローカルユーザを削除します

StorageGRID テナントアカウントにアクセスする必要がなくなったローカルユーザは、完全に削除できます。

Tenant Manager を使用して、フェデレーテッドユーザは削除できますが、フェデレーテッドユーザは削除できません。フェデレーテッドユーザを削除するには、フェデレーテッドアイデンティティソースを使用する必要があります。

手順

1. [ユーザ] リストで、削除するローカルユーザのチェックボックスをオンにします。
2. * アクション * > * ユーザーの削除 * を選択します。
3. 確認ダイアログボックスで、「 * ユーザーの削除 * 」を選択して、システムからユーザーを削除することを確認します。

   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。

著作権に関する情報

商標に関する情報