# グループとユーザを管理します

StorageGRID 11.8

NetApp
March 19, 2024

# 目次

# グループとユーザを管理します

## 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。

作業を開始する前に

- 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"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。
- 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。[Identity Federation]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.

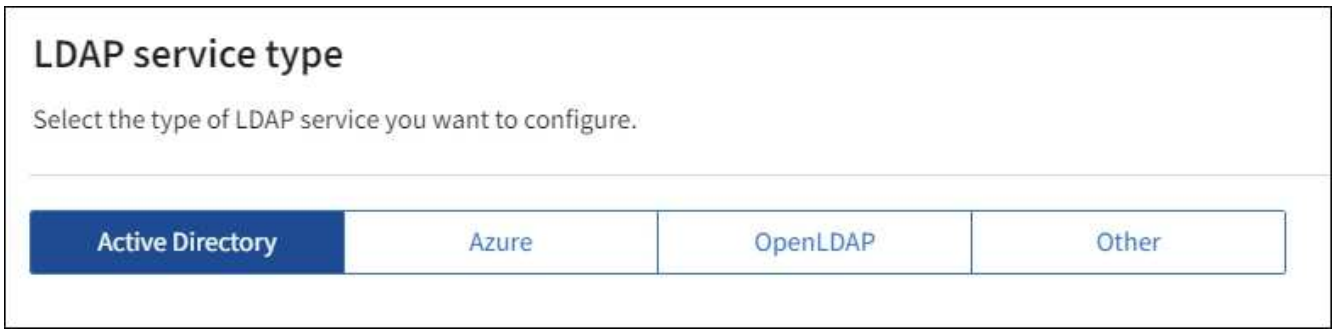
構成を入力します

フェデレーションの識別を設定するときは、StorageGRID がLDAPサービスに接続するために必要な値を指定します。

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。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `uid` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `uid`。
   - * 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。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。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。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `cn` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `cn`。
   - * 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。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。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`および `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。

> 今後パスワードを変更する場合は、このページでパスワードを更新する必要があります。

◦ * 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。

◦ ユーザー名のバインド形式（オプション）：パターンを自動的に決定できない場合にStorageGRID が使用するデフォルトのユーザー名パターン。

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`
- 下位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。

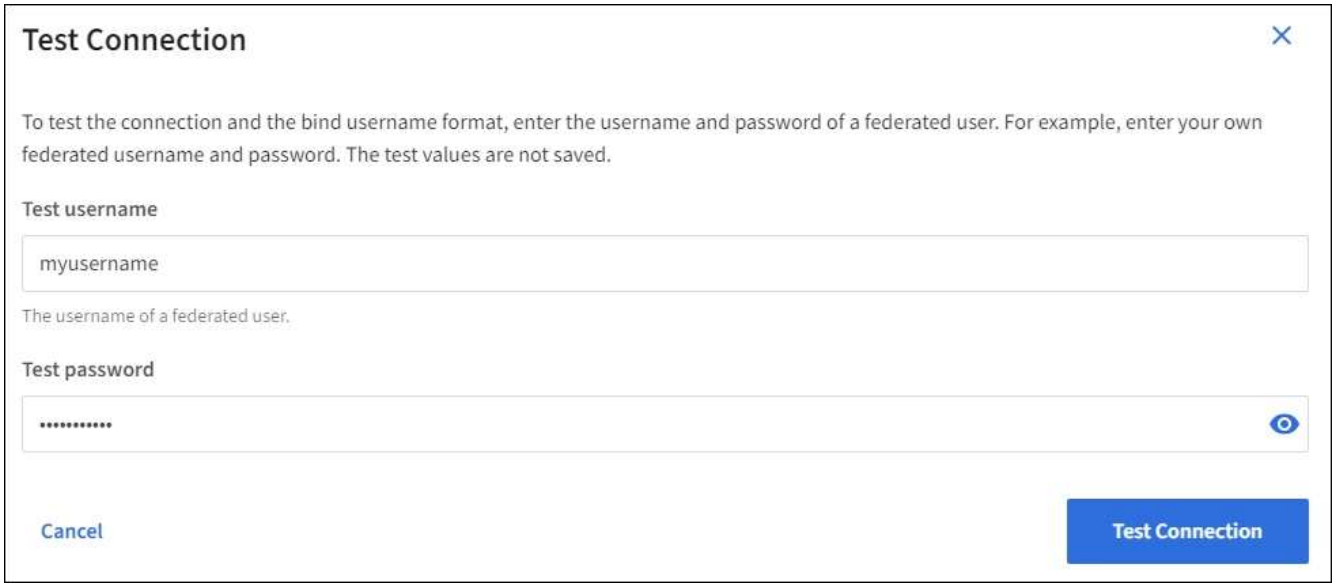
接続をテストして設定を保存します

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。

手順

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。
   - 接続設定が有効な場合は、「Test connection successful」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。ユーザ名に特殊文字（@、/など）を使用しないでください。




   - 接続設定が有効な場合は、「Test connection successful」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*有効*または*サンドボックスモード*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やAzure以外のアイデンティティソースの場合、StorageGRID は外部で無効にしたユーザへのS3アクセスを自動的にブロックしません。S3アクセスをブロックするには、そのユーザのS3キーをすべて削除するか、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 "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 "OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"。

# テナントグループを管理する

## 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。

作業を開始する前に

- 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"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。
- フェデレーテッドグループをインポートする場合は、を用意しておきます "アイデンティティフェデレーションが設定された"および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ます。
- テナントアカウントに* Use grid federation connection *権限が割り当てられている場合は、のワークフローと考慮事項を確認しておきます "テナントグループおよびテナントユーザのクローニング"をクリックし、テナントのソースグリッドにサインインします。

グループ作成ウィザードにアクセスします

最初に、グループ作成ウィザードにアクセスします。

手順

1. * access management * > * Groups * を選択します。
2. テナントアカウントに「Use grid federation connection *」権限がある場合は、このグリッドに作成された新しいグループが接続内の他のグリッドの同じテナントにクローニングされることを示す青いバナーが表示されることを確認します。このバナーが表示されない場合は、テナントのデスティネーショングリッドにサインインしている可能性があります。


3. 「 * グループを作成 * 」を選択します。

グループタイプを選択します

ローカルグループを作成するか、フェデレーテッドグループをインポートできます。

手順

1. [ 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。

2. 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。

     テナントアカウントで* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ unique name *がすでに存在すると、クローニングエラーが発生します。

   - * 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）：
3. 「 * Continue * 」を選択します。

グループの権限を管理します

グループ権限は、ユーザがTenant Managerおよびテナント管理APIで実行できるタスクを制御します。

手順

1. [アクセスモード]*で、次のいずれかを選択します。
   - * Read-write *（デフォルト）：ユーザはTenant Managerにサインインしてテナント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、変更を加えたり処理を実行したり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。

   > 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。

2. このグループの権限を1つ以上選択します。

   を参照してください "テナント管理権限"。

3. 「 * Continue * 」を選択します。

**S3**グループポリシーを設定

グループポリシーによって、ユーザに付与するS3アクセス権限が決まります。

手順

1. このグループに使用するポリシーを選択します。

| グループポリシー | 説明 |
| --- | --- |
| S3アクセスがありません | 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。 |

| グループポリシー | 説明 |
| --- | --- |
| ランサムウェアの軽減 | この例では、このテナントのすべてのバケットを環境するポリシーを示します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。<br><br>このグループポリシーは、* Manage all buckets *権限を持つTenant Managerユーザが上書きできます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証（MFA）を使用します。 |
| カスタム | グループ内のユーザには、テキストボックスで指定した権限が付与されます。 |

2. 「 * 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。

   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、を参照してください "グループポリシーの例"。

3. ローカルグループを作成する場合は、「 * Continue * 」を選択します。フェデレーテッドグループを作成する場合は、 * Create group * および * Finish * を選択します。

ユーザの追加（ローカルグループのみ）

ユーザを追加せずにグループを保存することも、必要に応じて既存のローカルユーザを追加することもできます。

> テナントアカウントに* Use grid federation connection *権限がある場合、ソースグリッドでローカルグループを作成するときに選択したユーザは、グループをデスティネーショングリッドにクローニングするときに含まれません。このため、グループを作成するときにユーザーを選択しないでください。代わりに、ユーザの作成時にグループを選択します。

手順

1. 必要に応じて、このグループに対して 1 人以上のローカルユーザを選択します。
2. [ グループの作成 *] と [ 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。

   テナントアカウントに* Use grid federation connection 権限があり、テナントのソースグリッドにアクセスしている場合、新しいグループはテナントのデスティネーショングリッドにクローニングされます。Success は、グループの詳細ページの**Overview**セクションに Cloning status *として表示されます。

## 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。

Swiftクライアントアプリケーションのサポートは廃止され、今後のリリースで削除される予定です。

作業を開始する前に

- 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"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。
- フェデレーテッドグループをインポートする場合は、を用意しておきます "アイデンティティフェデレーションが設定された"および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ます。

グループ作成ウィザードにアクセスします

手順

最初に、グループ作成ウィザードにアクセスします。

1. * access management * > * Groups * を選択します。
2. 「 * グループを作成 * 」を選択します。

グループタイプを選択します

ローカルグループを作成するか、フェデレーテッドグループをインポートできます。

手順

1. [ 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。

2. 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）：
3. 「 * Continue * 」を選択します。

グループの権限を管理します

グループ権限は、ユーザがTenant Managerおよびテナント管理APIで実行できるタスクを制御します。

手順

1. [アクセスモード]*で、次のいずれかを選択します。
   - * Read-write *（デフォルト）：ユーザはTenant Managerにサインインしてテナント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、変更を加えたり処理を実行したり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。

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。

2. グループユーザが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選択します。
3. 「 * Continue * 」を選択します。

**Swift**グループポリシーを設定します

Swiftユーザは、Swift REST APIに認証してコンテナを作成し、オブジェクトを取り込むための管理者権限が必要です。

1. グループユーザがSwift REST APIを使用してコンテナとオブジェクトを管理する必要がある場合は、* Swift administrator *チェックボックスをオンにします。
2. ローカルグループを作成する場合は、「 * Continue * 」を選択します。フェデレーテッドグループを作成する場合は、 * Create group * および * Finish * を選択します。

ユーザの追加（ローカルグループのみ）

ユーザを追加せずにグループを保存することも、必要に応じて既存のローカルユーザを追加することもできます。

手順

1. 必要に応じて、このグループに対して 1 人以上のローカルユーザを選択します。

   ローカルユーザをまだ作成していない場合は、[ユーザ]ページでこのグループをユーザに追加できます。を参照してください "ローカルユーザを管理します"。

2. [ グループの作成 *] と [ 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。

## 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。

| アクセス権 | 説明 | 詳細 |
| --- | --- | --- |
| ルートアクセス | Tenant Manager とテナント管理 API へのフルアクセスを提供します。 | 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 | SwiftユーザがSwift REST APIを使用して処理を実行するには、Swift Administrator権限が必要です。 |
| 自分のS3クレデンシャルを管理します | 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。 | この権限がないユーザには、* storage（S3）> My S3 access keys *メニューオプションが表示されません。 |
| すべてのバケットを表示 | • S3テナント*：すべてのバケットとバケットの設定を表示できます。<br>• Swiftテナント*：Swiftユーザに、テナント管理APIを使用してすべてのコンテナとコンテナ設定を表示することを許可します。 | View All Buckets権限またはManage All Buckets権限がないユーザには、* Buckets *メニューオプションは表示されません。<br><br>この権限は、Manage All Buckets権限よりも優先されます。S3クライアントまたはS3コンソールで使用されるS3バケットポリシーやグループポリシーには影響しません。<br><br>この権限をSwiftグループに割り当てるには、テナント管理APIを使用する必要があります。Tenant Managerを使用してSwiftグループにこの権限を割り当てることはできません。 |

| アクセス権 | 説明 | 詳細 |
| --- | --- | --- |
| すべてのバケットを管理 | • 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、テナントマネージャとテナント管理APIを使用してS3バケットを作成および削除し、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ユーザに許可します。<br>• Swiftテナント*：Swiftユーザにテナント管理APIを使用してSwiftコンテナの整合性を制御することを許可します。 | View All Buckets権限またはManage All Buckets権限がないユーザには、* Buckets *メニューオプションは表示されません。<br><br>この権限は、View All Buckets権限よりも優先されます。S3クライアントまたはS3コンソールで使用されるS3バケットポリシーやグループポリシーには影響しません。<br><br>この権限をSwiftグループに割り当てるには、テナント管理APIを使用する必要があります。Tenant Managerを使用してSwiftグループにこの権限を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 | ユーザに、テナントマネージャ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プラットフォームサービスエンドポイントを作成または編集することを許可します。 | この権限がないユーザーには、*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。 |
| S3コンソールタブを使用 | View All Buckets権限またはManage All Buckets権限と組み合わせると、ユーザはバケットの詳細ページにあるS3 Consoleタブでオブジェクトの表示と管理を行うことができます。 | |

## グループを管理します

## 必要に応じてテナントグループを管理し、グループの表示、編集、複製などを行います。

作業を開始する前に

- 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"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。

グループを表示または編集します

各グループの基本情報と詳細を表示および編集できます。

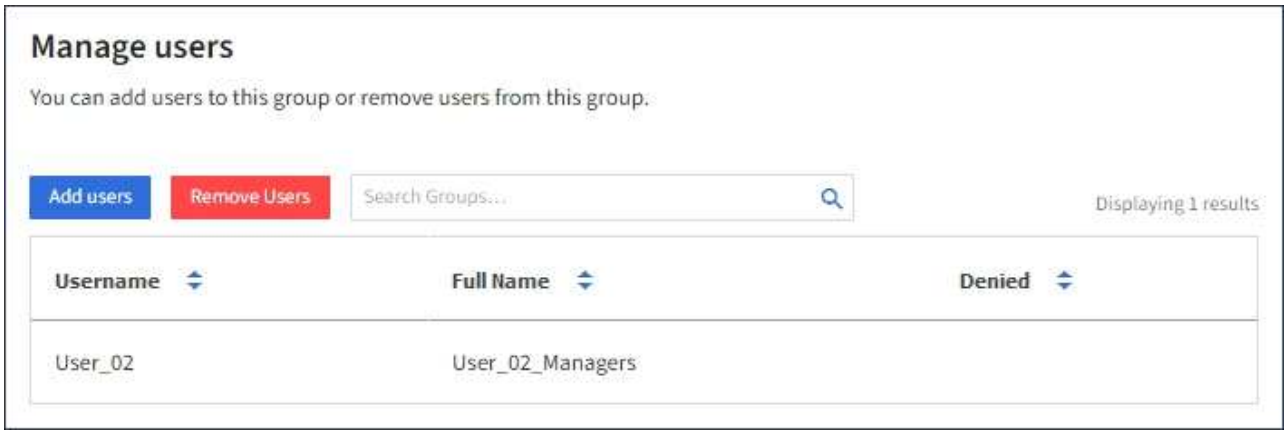
手順

1. * access management * > * Groups * を選択します。
2. [Groups]ページに表示される情報を確認します。このテナントアカウントのすべてのローカルグループとフェデレーテッドグループの基本情報が表示されます。

   テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッド上のグループを表示している場合：

- バナーメッセージは、グループを編集または削除すると、変更内容が他のグリッドに同期されないことを示します。
- 必要に応じて、デスティネーショングリッドでグループがテナントにクローニングされなかったかどうかを示すバナーメッセージが表示されます。可能です グループクローンの再試行 失敗した

3. グループの名前を変更する場合は、次の手順を実行します。
   a. グループのチェックボックスをオンにします。
   b. **>**[グループ名の編集]*を選択します。
   c. 新しい名前を入力します。
   d. [変更を保存]*を選択します
4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
   - グループ名を選択します。
   - グループのチェックボックスを選択し、**[**操作**]>***[グループの詳細を表示]*を選択します。
5. [Overview]セクションには、グループごとに次の情報が表示されます。
   - 表示名
   - 一意の名前
   - を入力します
   - アクセスモード
   - 権限
   - S3ポリシー
   - このグループのユーザ数
   - テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッドでグループを表示している場合は、次のフィールドが追加されます。
     - クローニングステータス（* Success または Failure *）
     - このグループを編集または削除すると、変更内容が他のグリッドに同期されないことを示す青のバナーが表示されます。
6. 必要に応じてグループ設定を編集します。を参照してください "S3 テナント用のグループを作成します" および "Swift テナント用のグループを作成します" を参照してください。
   a. [Overview]セクションで、名前または編集アイコンを選択して表示名を変更します 。
   b. [グループ権限]タブで権限を更新し、*[変更の保存]*を選択します。
   c. タブで、変更を加えて[変更の保存]*を選択します。
      - S3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するか、カスタムポリシーのJSON文字列を入力します。
      - Swift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。
7. 既存のローカルユーザをグループに追加するには、次の手順を実行します。
   a. [Users]タブを選択します。




b. [ユーザの追加]*を選択します。

c. 追加する既存のユーザーを選択し、*ユーザーの追加*を選択します。

右上に成功メッセージが表示されます。

8. グループからローカルユーザを削除するには、次の手順を実行します

a. [Users]タブを選択します。

b. [ユーザの削除]*を選択します。

c. 削除するユーザを選択し、*[ユーザの削除]*を選択します。

右上に成功メッセージが表示されます。

9. 変更した各セクションで[変更を保存]*が選択されていることを確認します。

グループが重複しています

既存のグループを複製して、新しいグループをより迅速に作成できます。

テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッドからグループを複製すると、複製されたグループがテナントのデスティネーショングリッドにクローニングされます。

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. [ * アクション * > * グループの複製 * ] を選択します。
4. を参照してください "S3 テナント用のグループを作成します" または "Swift テナント用のグループを作成します" を参照してください。
5. 「 * グループを作成 * 」を選択します。

グループクローンの再試行

失敗したクローンを再試行するには：

1. グループ名の下に_（Cloning failed）_と表示されている各グループを選択します。
2. >[クローングループ]*を選択します。
3. クローニングする各グループの詳細ページで、クローニング処理のステータスを確認します。

追加情報の場合は、を参照してください "テナントグループとテナントユーザのクローンを作成します"。

**1**つ以上のグループを削除します

1つ以上のグループを削除できます。削除したグループにのみ属しているユーザは、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できなくなります。

テナントアカウントに* Use grid federation connection *権限が割り当てられている場合にグループを削除すると、StorageGRID はもう一方のグリッド上の対応するグループを削除しません。この情報を同期する必要がある場合は、両方のグリッドから同じグループを削除する必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 削除する各グループのチェックボックスをオンにします。
3. >[グループの削除]または[アクション]>[グループの削除]*を選択します。

   確認のダイアログボックスが表示されます。

4. または[グループの削除]*を選択します。

# 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人含まれています。 ローカルユーザは追加および削除できますが、rootユーザは削除できません。

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、ローカルユーザはクライアントアプリケーションを使用してグループ権限に基づいてテナントのリソースにアクセスできますが、Tenant Managerまたはテナント管理APIにサインインすることはできません。

作業を開始する前に

- 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"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。
- テナントアカウントに* Use grid federation connection *権限が割り当てられている場合は、のワークフローと考慮事項を確認しておきます "テナントグループおよびテナントユーザのクローニング"をクリックし、テナントのソースグリッドにサインインします。

## ローカルユーザを作成します

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。

どのグループにも属していないS3ユーザには、管理権限やS3グループポリシーが適用されていません。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。

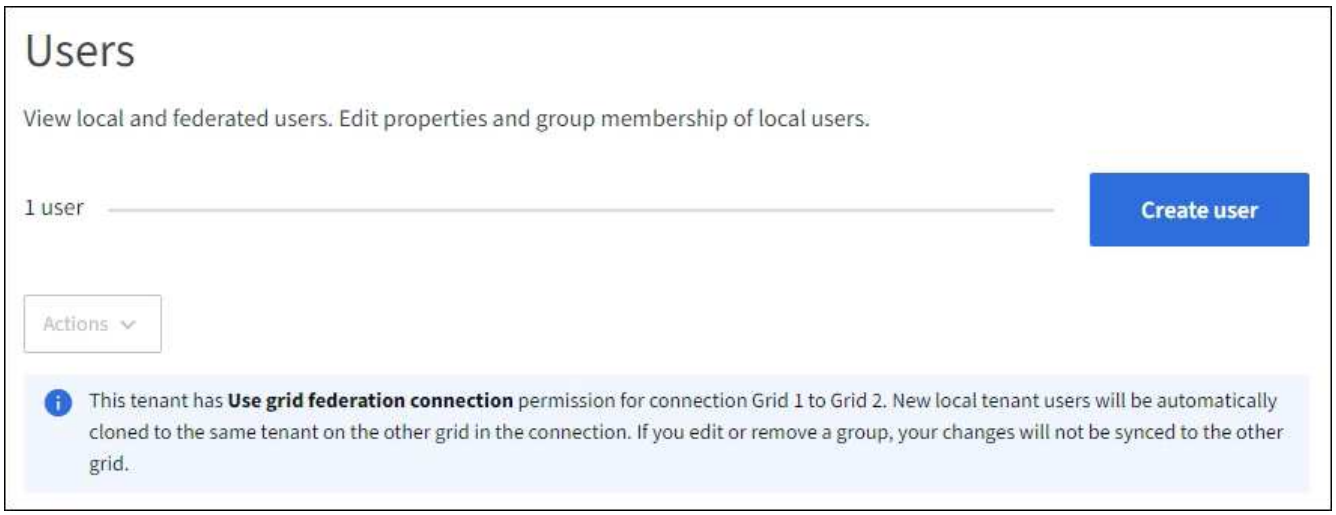
いずれのグループにも属していないSwiftユーザには、管理権限やSwiftコンテナへのアクセス権がありません。

### **Create user**ウィザードにアクセスします

手順

1. アクセス管理 * > * Users * を選択します。

   テナントアカウントで* Use grid federation connection *権限が割り当てられている場合は、青のバナーがテナントのソースグリッドであることを示します。このグリッドに作成したローカルユーザは、接続内の他のグリッドにクローニングされます。




2. 「 * ユーザーの作成 * 」を選択します。

### 資格情報を入力します

手順

1. [ユーザクレデンシャルの入力]*ステップで、次のフィールドに値を入力します。

| フィールド | 説明 |
| --- | --- |
| フルネーム | このユーザーのフルネーム（ユーザーの名と姓、アプリケーションの名前など）。 |

| フィールド | 説明 |
| --- | --- |
| 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。<br><br>注：テナントアカウントに* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ Username *がすでに存在すると、クローニングエラーが発生します。 |
| | ユーザがサインイン時に最初に使用するパスワード。 |
| アクセスを拒否します | このユーザが1つ以上のグループに属している場合でもテナントアカウントにサインインできないようにするには、*[はい]*を選択します。<br><br>たとえば、*[はい]*を選択すると、ユーザーのサインイン機能が一時的に中断されます。 |

2. 「 * Continue * 」を選択します。

グループに割り当てます

手順

1. ユーザを1つ以上のローカルグループに割り当てて、実行できるタスクを決定します。

   グループへのユーザの割り当ては任意です。必要に応じて、グループを作成または編集するときにユーザーを選択できます。

   どのグループにも属していないユーザには、管理権限はありません。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。を参照してください "テナント管理権限"。

2. 「 * ユーザーの作成 * 」を選択します。

   テナントアカウントに* Use grid federation connection 権限があり、テナントのソースグリッドにアクセスしている場合は、新しいローカルユーザがテナントのデスティネーショングリッドにクローニングされます。 Success は、ユーザーの詳細ページの**Overview**セクションに Cloning status *として表示されます。

3. [完了]*を選択して[ユーザー]ページに戻ります。

## ローカルユーザを表示または編集します

手順

1. アクセス管理 * > * Users * を選択します。
2. [Users]ページに表示される情報を確認します。このテナントアカウントのすべてのローカルユーザとフェデレーテッドユーザの基本情報が表示されます。

   テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッドでユーザを表示している場合は、次の手順を実行します。

- バナーメッセージは、ユーザを編集または削除すると、変更内容が他のグリッドに同期されないことを示します。
- 必要に応じて、ユーザがデスティネーショングリッドのテナントにクローニングされていないかどうかを示すバナーメッセージが表示されます。可能です 失敗したユーザクローンを再試行します。。

3. ユーザのフルネームを変更する場合は、次の手順を実行します。
   a. ユーザのチェックボックスを選択します。
   b. **>**[フルネームの編集]*を選択します。
   c. 新しい名前を入力します。
   d. [変更を保存]*を選択します
4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
   - ユーザ名を選択します。
   - ユーザのチェックボックスを選択し、**[**操作**]>**[ユーザの詳細を表示]*を選択します。
5. [Overview]セクションには、ユーザごとに次の情報が表示されます。
   - フルネーム
   - ユーザ名
   - ユーザタイプ
   - アクセスを拒否しました
   - アクセスモード
   - グループメンバーシップ
   - テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッドでユーザを表示している場合は、次のフィールドが追加されます。
     - クローニングステータス（* Success または Failure *）
     - このユーザを編集すると、変更内容が他のグリッドに同期されないことを示す青いバナーが表示されます。
6. 必要に応じてユーザー設定を編集します。を参照してください ローカルユーザを作成します を参照してください。
   a. [Overview]セクションで、名前または編集アイコンを選択してフルネームを変更します 。

      ユーザー名は変更できません。

   b. タブで、ユーザのパスワードを変更し、[変更を保存]*を選択します。
   c. [アクセス]タブで、**[**いいえ**]**を選択してユーザーがサインインできるようにするか、[はい]を選択してユーザーがサインインできないようにします。次に、*変更を保存*を選択します。
   d. [アクセスキー]タブで、*[キーの作成]*を選択し、の手順に従います "別のユーザのS3アクセスキーを作成しています"。
   e. タブで[グループの編集]*を選択して、ユーザーをグループに追加するか、ユーザーをグループから削除します。次に、*変更を保存*を選択します。
7. 変更した各セクションで[変更を保存]*が選択されていることを確認します。

## 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。

> テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッドからユーザを複製すると、複製されたユーザはテナントのデスティネーショングリッドにクローニングされます。

手順

1. アクセス管理 * > * Users * を選択します。
2. 複製するユーザのチェックボックスをオンにします。
3. >[ユーザーの複製]*を選択します。
4. を参照してください ローカルユーザを作成します を参照してください。
5. 「 * ユーザーの作成 * 」を選択します。

## ユーザクローンの再試行

失敗したクローンを再試行するには：

1. ユーザ名の下に_（Cloning failed）_と表示されている各ユーザを選択します。
2. >[ユーザのクローン]*を選択します。
3. クローニングする各ユーザの詳細ページで、クローニング処理のステータスを確認します。

追加情報の場合は、を参照してください "テナントグループとテナントユーザのクローンを作成します"。

## 1人以上の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1人以上のローカルユーザを完全に削除できます。

> テナントアカウントに* Use grid federation connection *権限が割り当てられている場合にローカルユーザを削除すると、StorageGRID はもう一方のグリッド上の対応するユーザを削除しません。この情報を同期する必要がある場合は、両方のグリッドから同じユーザーを削除する必要があります。

> 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. アクセス管理 * > * Users * を選択します。
2. 削除する各ユーザのチェックボックスをオンにします。
3. >[ユーザーの削除]または[操作]>[ユーザーの削除]*を選択します。

   確認のダイアログボックスが表示されます。

4. または[ユーザの削除]*を選択します。

## 著作権に関する情報



## 商標に関する情報