テナントグループの管理

StorageGRID software

NetApp
December 03, 2025

目次

テナントグループの管理

S3テナントのグループを作成する

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 グループを作成することによって、S3 ユーザー グループの権限を管理できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。
- フェデレーショングループをインポートする予定の場合は、"構成されたID連携" 、フェデレーション グループは構成された ID ソースにすでに存在します。
- テナントアカウントに*グリッドフェデレーション接続を使用する*権限がある場合は、ワークフローと考慮事項を確認しました。"テナントグループとユーザーの複製" 、テナントのソース グリッドにサインインしています。

グループ作成ウィザードにアクセスする

最初のステップとして、グループの作成ウィザードにアクセスします。

手順

1. アクセス管理 > *グループ*を選択します。
2. テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、このグリッドで作成された新しいグループが接続内の他のグリッド上の同じテナントに複製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、テナントの宛先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。

グループの種類を選択

ローカル グループを作成したり、フェデレーション グループをインポートしたりできます。

手順

1. ローカル グループを作成するには ローカル グループ タブを選択し、以前に構成した ID ソースからグループをインポートするには フェデレーション グループ タブを選択します。

   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ーは、グループの権限に基づいてクライアント 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することはできますが、テナント マネージャにサインインすることはできません。

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。表示名は後で編集できます。

     テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合、宛先グリッドのテナントに同じ 一意の名前 がすでに存在すると、複製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、一意の名前は `sAMAccountName`属性。 OpenLDAPの場合、一意の名前は `uid`属性。

3. *続行*を選択します。

グループ権限を管理する

グループ権限は、ユーザーがテナント マネージャー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 では、次のいずれかを選択します。

   - 読み取り/書き込み (デフォルト): ユーザーは Tenant Manager にサインインし、テナント構成を管理できます。
   - 読み取り専用: ユーザーは設定と機能の表示のみが可能です。テナント マネージャーまたはテナント管理 API で変更を加えたり、操作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ーは自分のパスワードを変更できます。

     ユーザーが複数のグループに属しており、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、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

2. このグループに対して 1 つ以上の権限を選択します。

   見る"テナント管理権限" 。

3. *続行*を選択します。

S3グループポリシーを設定する

グループ ポリシーによって、ユーザーに付与される 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 アクセスなし	デフォルト。このグループのユーザーは、バケットポリシーでアクセスが許可されない限り、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、デフォルトではルートユーザーのみが S3 リソースにアクセスできるようになります。
読み取り専用アクセス	このグループのユーザーには、S3 リソースへの読み取り専用アクセス権があります。たとえば、このグループのユーザーはオブジェクトを一覧表示したり、オブジェクトのデータ、メタデータ、タグを読み取ったりできます。このオプションを選択すると、読み取り専用グループ ポリシーの JSON 文字列がテキスト ボックスに表示されます。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ーには、バケットを含む S3 リソースへのフルアクセス権が付与されます。このオプションを選択すると、フルアクセス グループ ポリシーの JSON 文字列がテキスト ボックスに表示されます。この文字列は編集できません。
ランサムウェア対策	このサンプルポリシーは、このテナントのすべてのバケットに適用されます。このグループのユーザーは一般的なアクションを実行できますが、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。 *すべてのバケットの管理*権限を持つテナント マネージャー ユーザーは、このグループ ポリシーを上書きできます。すべてのバケットの管理権限を信頼できるユーザーに制限し、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。

2. *カスタム*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 ポリシーのサイズ制限は 5,120 バイトです。有効な JSON 形式の文字列を入力する必要があります。

   言語構文や例を含むグループポリシーの詳細については、以下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、[続行] を選択します。フェデレーション グループを作成する場合は、[グループの作成] と [完了] を選択します。

ユーザーを追加する（ローカルグループのみ）

ユーザーを追加せずにグループを保存することも、オプションで既存のローカル ユーザーを追加することもできます。

> テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合、ソース グリッドにローカル グループを作成するときに選択したユーザーは、グループが宛先グリッドに複製されるときには含まれません。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、ユーザーを作成するときにグループを選択します。

手順

1. 必要に応じて、このグループのローカル ユーザーを 1 人以上選択します。
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 グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドにいる場合、新しいグループはテナントの宛先グリッドに複製されます。グループの詳細ページの概要セクションに、*複製ステータス*として*成功*が表示されます。

Swiftテナントのグループを作成する

フェデレーション グループをインポートするか、ローカル グループを作成することによって、Swift テナント アカウントのアクセス権限を管理できます。少なくとも 1 つのグループに Swift 管理者権限が必要です。この権限は、Swift テナント アカウントのコンテナーとオブジェクトを管理するために必要なものです。

Swift クライアント アプリケーションのサポートは非推奨となり、将来のリリースでは削除される予定です。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。
- フェデレーショングループをインポートする予定の場合は、"構成されたID連携" 、フェデレーション グループは構成された ID 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する

手順

最初のステップとして、グループの作成ウィザードにアクセスします。

1. アクセス管理 > *グループ*を選択します。
2. *グループを作成*を選択します。

グループの種類を選択

ローカル グループを作成したり、フェデレーション グループをインポートしたりできます。

手順

1. ローカル グループを作成するには ローカル グループ タブを選択し、以前に構成した ID ソースからグループをインポートするには フェデレーション グループ タブを選択します。

   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ーは、グループの権限に基づいてクライアント 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することはできますが、テナント マネージャにサインインすることはできません。

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。表示名は後で編集できます。
   - 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、一意の名前は `sAMAccountName`属性。 OpenLDAPの場合、一意の名前は `uid`属性。
3. *続行*を選択します。

グループ権限を管理する

グループ権限は、ユーザーがテナント マネージャー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 では、次のいずれかを選択します。
   - 読み取り/書き込み (デフォルト): ユーザーは Tenant Manager にサインインし、テナント構成を管理できます。
   - 読み取り専用: ユーザーは設定と機能の表示のみが可能です。テナント マネージャーまたはテナント管理 API で変更を加えたり、操作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ーは自分のパスワードを変更できます。

   > ユーザーが複数のグループに属しており、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、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

2. グループ ユーザーが Tenant Manager または Tenant Management API にサインインする必要がある場合は、ルート アクセス チェックボックスをオンにします。
3. *続行*を選択します。

Swiftグループポリシーを設定する

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

1. グループ ユーザーが Swift REST API を使用してコンテナーとオブジェクトを管理する必要がある場合は、**Swift** 管理者 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、[続行] を選択します。フェデレーション グループを作成する場合は、[グループの作成] と [完了] を選択します。

ユーザーを追加する（ローカルグループのみ）

ユーザーを追加せずにグループを保存することも、オプションで既存のローカル ユーザーを追加することもできます。

手順

1. 必要に応じて、このグループのローカル ユーザーを 1 人以上選択します。

   ローカル ユーザーをまだ作成していない場合は、[ユーザー] ページでこのグループをユーザーに追加できます。見る"ローカルユーザーの管理" 。

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。テナント管理権限によって、ユーザーがテナント マネージャーまたはテナント管理 API を使用して実行できるタスクが決まります。ユーザーは 1 つ以上のグループに所属できます。ユーザーが複数のグループに属している場合、権限は累積されます。

テナント マネージャーにサインインしたり、テナント管理 API を使用したりするには、ユーザーは少なくとも 1 つの権限を持つグループに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ーは、次のタスクを実行できます。

- ダッシュボードを見る
- 自分のパスワードを変更する（ローカルユーザーの場合）

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、ユーザーが設定を変更して操作を実行できるかどうか、または関連する設定と機能の表示のみが可能かどうかが決まります。

> ユーザーが複数のグループに属しており、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、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

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 テナントには異なるグループ権限があることに注意してください。

許可	説明	詳細
ルート アクセス	テナント マネージャーとテナント管理 API へのフル アクセスを提供します。	Swift ユーザーは、テナント アカウントにサインインするためにルート アクセス権限を持っている必要があります。
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 ユーザーは、Swift REST API を使用して操作を実行するために、Swift 管理者権限を持っている必要があります。
独自のS3認証情報を管理する	ユーザーが独自の S3 アクセスキーを作成および削除できるようにします。	この権限を持たないユーザーには、ストレージ **(S3)** > マイ **S3** アクセス キー メニュー オプションは表示されません。

許可	説明	詳細
すべてのバケットを表示	**S3** テナント: ユーザーがすべてのバケットとバケット構成を表示できるようにします。 **Swift** テナント: Swift ユーザーがテナント管理 API を使用してすべてのコンテナとコンテナ構成を表示できるようにします。	すべてのバケットの表示権限またはすべてのバケットの管理権限を持たないユーザーには、バケット メニュー オプションは表示されません。 この権限は、すべてのバケットの管理権限に置き換えられます。これは、S3 クライアントまたは S3 コンソールで使用される S3 バケットまたはグループ ポリシーには影響しません。 この権限は、テナント管理 API から Swift グループにのみ割り当てることができます。テナント マネージャーを使用して、Swift グループにこの権限を割り当てることはできません。
すべてのバケットを管理する	**S3** テナント: ユーザーがテナント マネージャーとテナント管理 API を使用して S3 バケットを作成および削除したり、S3 バケットまたはグループ ポリシーに関係なく、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したりできるようにします。 **Swift** テナント: Swift ユーザーがテナント管理 API を使用して Swift コンテナの一貫性を制御できるようにします。	すべてのバケットの表示権限またはすべてのバケットの管理権限を持たないユーザーには、バケット メニュー オプションは表示されません。 この権限は、「すべてのバケットを表示」権限よりも優先されます。これは、S3 クライアントまたは S3 コンソールで使用される S3 バケットまたはグループ ポリシーには影響しません。 この権限は、テナント管理 API から Swift グループにのみ割り当てることができます。テナント マネージャーを使用して、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する	ユーザーがテナント 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 サービスの宛先として使用され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。
S3コンソールタブを使用する	「すべてのバケットの表示」または「すべてのバケットの管理」権限と組み合わせると、ユーザーはバケットの詳細ページの S3 コンソール タブからオブジェクトを表示および管理できるようになります。	

グループの管理

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。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。

グループを表示または編集する

各グループの基本情報や詳細を表示、編集できます。

手順

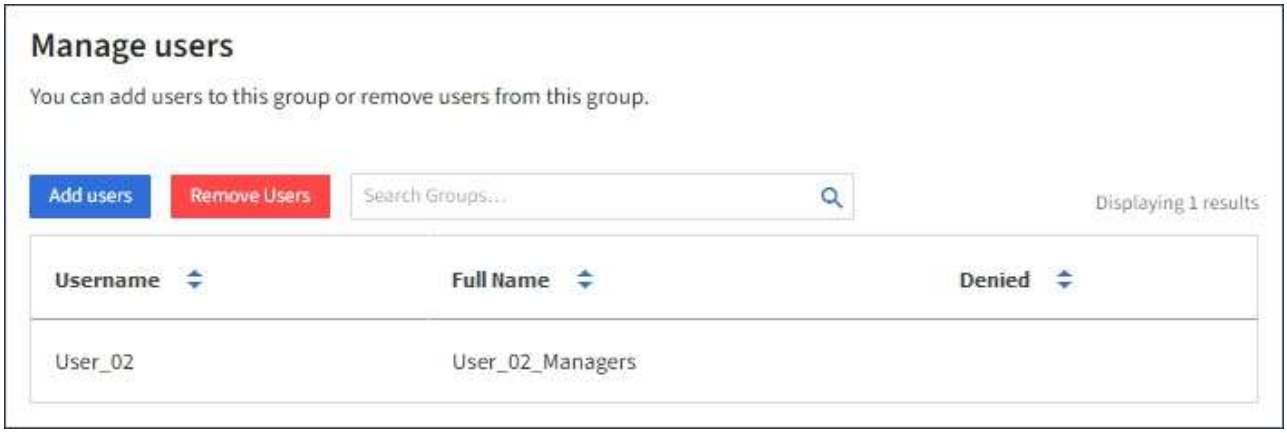
1. アクセス管理 > *グループ*を選択します。
2. [グループ] ページに提供される情報を確認します。このページには、このテナント アカウントのすべてのローカル グループとフェデレーション グループの基本情報が一覧表示されます。

   テナント アカウントに グリッド フェデレーション接続の使用 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:

   - グループを編集または削除した場合、変更内容は他のグリッドに同期されないことを示すバナーメッセージが表示されます。
   - 必要に応じて、グループが宛先グリッドのテナントに複製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。あなたはできるグループのクローンを再試行するそれは失敗しました。
3. グループの名前を変更する場合:
   a. グループのチェックボックスを選択します。
   b. アクション > *グループ名の編集*を選択します。
   c. 新しい名前を入力してください。
   d. *変更を保存*を選択します。
4. 詳細を表示したり、追加の編集を行ったりする場合は、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、[アクション] > [グループの詳細を表示] を選択します。
5. 各グループの次の情報が表示される概要セクションを確認します。
   - 表示名
   - 一意の名前
   - タイプ
   - アクセス モード
   - 権限
   - S3ポリシー
   - このグループのユーザー数
   - テナント アカウントに グリッド フェデレーション接続の使用 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の追加フィールド:

- クローン作成ステータス（成功*または*失敗）
- このグループを編集または削除しても、変更内容は他のグリッドに同期されないことを示す青いバナー。

6. 必要に応じてグループ設定を編集します。見る"S3テナントのグループを作成する"そして"Swiftテナントのグループを作成する"入力内容の詳細については、こちらをご覧ください。
   a. 概要セクションで、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. *グループの権限*タブで権限を更新し、*変更を保存*を選択します。
   c. グループ ポリシー タブで変更を行い、変更の保存 を選択します。
      - S3 グループを編集している場合は、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 グループを編集している場合は、オプションで **Swift** 管理者 チェックボックスをオンまたはオフにします。
7. 1 人以上の既存のローカル ユーザーをグループに追加するには:
   a. [ユーザー]タブを選択します。



   b. *ユーザーを追加*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 ユーザーを削除するには:
   a. [ユーザー]タブを選択します。
   b. *ユーザーを削除*を選択します。
   c. 削除するユーザーを選択し、「ユーザーの削除」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。

重複グループ

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 グリッド フェデレーション接続の使用 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場合、複製されたグループはテナントの宛先グリッドに複製されます。

手順

1. アクセス管理 > *グループ*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選択します。
3. アクション > *グループの複製*を選択します。
4. 見る"S3テナントのグループを作成する"または"Swiftテナントのグループを作成する"入力内容の詳細については、こちらをご覧ください。
5. *グループを作成*を選択します。

グループのクローンを再試行する

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「(複製失敗)」と表示されている各グループを選択します。
2. アクション > *グループの複製*を選択します。
3. 複製する各グループの詳細ページから複製操作のステータスを表示します。

詳細については、"テナントグループとユーザーの複製"を参照してください。

1つ以上のグループを削除する

1 つ以上のグループを削除できます。削除されたグループにのみ属しているユーザーは、テナント マネージャー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 グリッド フェデレーション接続の使用 権限があり、グループを削除した場合、 StorageGRID は他のグリッド上の対応するグループを削除しません。この情報を同期させておく必要がある場合は、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. アクセス管理 > *グループ*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選択します。
3. アクション > 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。

   確認ダイアログボックスが表示されます。

4. *グループの削除*または*グループの削除*を選択します。

著作権に関する情報

商標に関する情報