



テナントユーザのシステムアクセスの管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

テナントユーザのシステムアクセスの管理	1
アイデンティティフェデレーションを使用する	1
グループの管理	6
ローカルユーザの管理	20

テナントユーザのシステムアクセスの管理

テナントアカウントへのアクセス権をユーザに付与するには、フェデレーテッドアイデンティティソースからグループをインポートして、管理権限を割り当てます。StorageGRID システム全体でシングルサインオン (SSO) が有効になっていないかぎり、ローカルテナントグループおよびユーザを作成することもできます。

- ["アイデンティティフェデレーションを使用する"](#)
- ["グループの管理"](#)
- ["ローカルユーザの管理"](#)

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。

- ["フェデレーテッドアイデンティティソースを設定する"](#)
- ["アイデンティティソースとの強制同期"](#)
- ["アイデンティティフェデレーションの無効化"](#)

フェデレーテッドアイデンティティソースを設定する

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

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。
- 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、OpenLDAP、またはOracle Directory Serverを使用している必要があります。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。
- 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。

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.

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サービスのタイプセクションで、* Active Directory、OpenLDAP、または Other * を選択します。

OpenLDAP * を選択した場合は、OpenLDAPサーバを設定します。OpenLDAPサーバの設定に関するガイドラインを参照してください。

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。
 - * User Unique Name * : LDAP ユーザの一意的な 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的な 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 グループの一意的な 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的な 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. Configure LDAP server (LDAPサーバの設定) セクションで、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サーバのホスト名または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

- * 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*グループのベース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。

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 (推奨) * : STARTTLSを使用してLDAPサーバとの通信を保護します。これが推奨されるオプションです。
- * 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。このオプションは互換性を確保するためにサポートされています。
- * 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。

Active DirectoryサーバでLDAP署名を適用する場合は、このオプション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。

8. 「接続のテスト」を選択して、LDAPサーバーの接続設定を検証します。

接続が有効な場合は、ページの右上に確認メッセージが表示されます。

9. 接続が有効な場合は、*保存*を選択します。

次のスクリーンショットは、Active Directoryを使用するLDAPサーバの設定例を示しています。

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

●●●●●●●●

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

関連情報

["テナント管理権限"](#)

["OpenLDAP サーバの設定に関するガイドライン"](#)

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。

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、OpenLDAPの管理者ガイド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。

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。

OpenLDAPの管理者ガイド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。

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。

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。
- 特定のアクセス権限が必要です。
- 保存されたアイデンティティソースが有効になっている必要があります。

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。

アイデンティティフェデレーションページが表示されます。「サーバーの同期」ボタンは、ページの右上にあります。



保存されているアイデンティティソースが有効になっていない場合、*サーバーの同期*ボタンはアクティブになりません。

2. 「サーバの同期」を選択します。

同期が開始されたことを示す確認メッセージが表示されます。

関連情報

["テナント管理権限"](#)

アイデンティティフェデレーションの無効化

この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した場合は、テナント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 システム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。

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。
- 特定のアクセス権限が必要です。

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テナントアカウントにアクセスしたままとなりますが、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ません。

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] チェックボックスをオフにします。
3. [保存 (Save)] を選択します。

関連情報

["テナント管理権限"](#)

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。
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	<ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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ができません。

アクセス権	説明
エンドポイントを管理します	<p>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。</p> <p>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。</p>

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。

The screenshot shows the 'Groups' management page. At the top, it says 'Create and manage local and federated groups. Set group permissions to control access to specific pages and features.' Below this, it indicates '2 groups' and has a 'Create group' button. A table lists the existing groups:

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

At the bottom right, there are navigation arrows: '< Previous 1 Next >'.

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で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。

No S3 Access

Read Only Access

Full Access

Custom
(Must be a valid JSON formatted string.)

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

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 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で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。

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。

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。

Username	Full Name	Denied
User_02	User_02_Managers	

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。

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	User_01	User_01_Applications	

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。

Edit group name ✕

Specify a new name for the group **Applications**.

Must contain at least 1 and no more than 32 characters

Applications

Cancel Save changes

- 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。

- 「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。

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups Create group

Actions ▾

<input type="checkbox"/>	Name ↕	ID ↕	Type ↕	Access mode ↕
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

- 削除するグループのチェックボックスを選択します。
- [* 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。

- [* 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"](#)

ローカルユーザの管理

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。



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。

Usersページへのアクセス

アクセス管理 * > * Users * を選択します。

<input type="checkbox"/>	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

ローカルユーザを作成しています

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。

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する


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。

ローカルユーザの複製

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ています

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。

関連情報

["テナント管理権限"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。