アイデンティティフェデレーションを使用する
StorageGRID 11.5

NetApp
April 11, 2024

目次

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

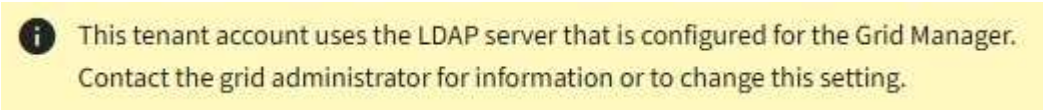
テナントグループとユーザをActive Directory、OpenLDAP、Oracle Directory Serverなどの別のシステムで管理する場合は、アイデンティティフェデレーションを設定できます。

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。
- 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。



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. 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。

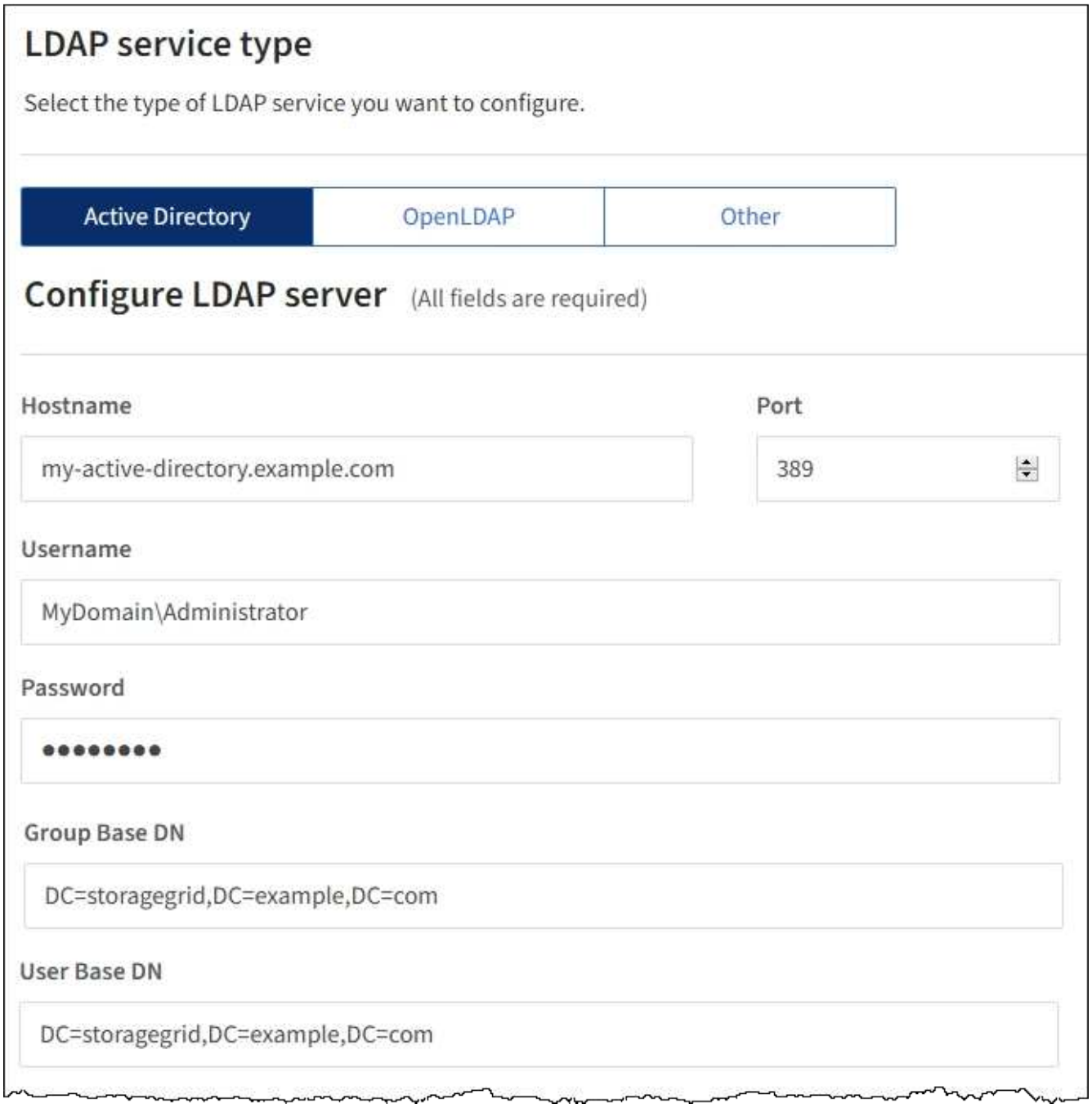
     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

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。



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"

著作権に関する情報

商標に関する情報