StorageGRID へのアクセスを制御します

StorageGRID

NetApp
April 10, 2024

目次

StorageGRID へのアクセスを制御します

プロビジョニングパスフレーズを変更します

この手順 を使用して、 StorageGRID プロビジョニングパスフレーズを変更します。パスフレーズは、リカバリ、拡張、およびメンテナンスの手順で必要になります。また、リカバリパッケージのバックアップをダウンロードする際にも、 StorageGRID システムのグリッドトポロジ情報、グリッドノードのコンソールパスワード、暗号化キーが含まれている必要があります。

必要なもの

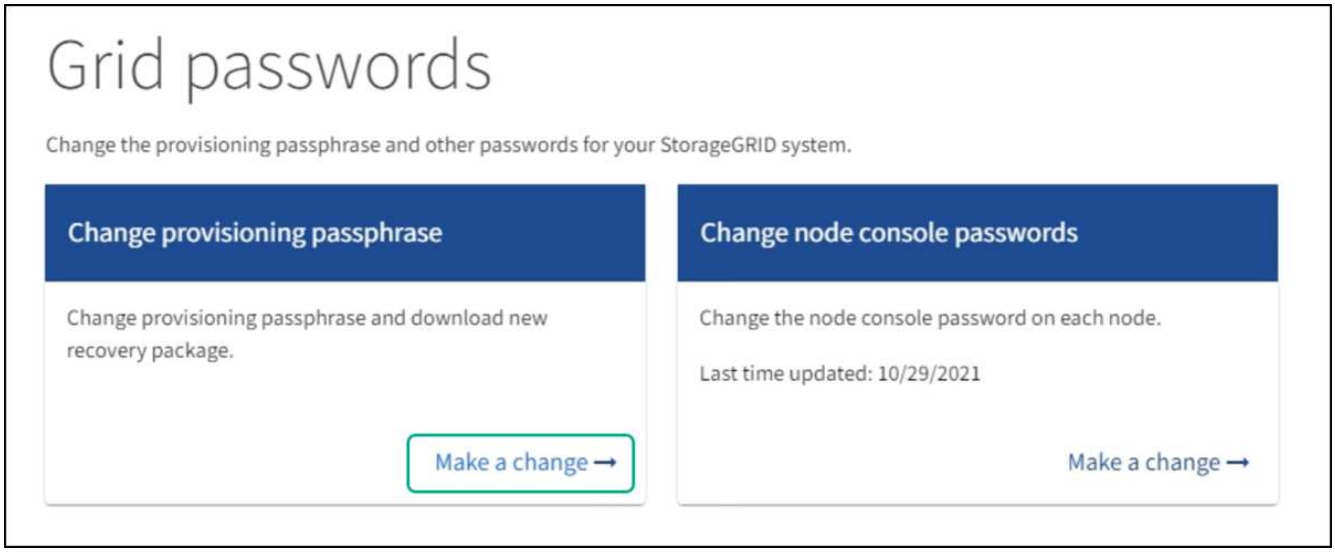
- を使用して Grid Manager にサインインします サポートされている Web ブラウザ。
- Maintenance または Root アクセス権限が必要です。
- 現在のプロビジョニングパスフレーズを用意します。

このタスクについて

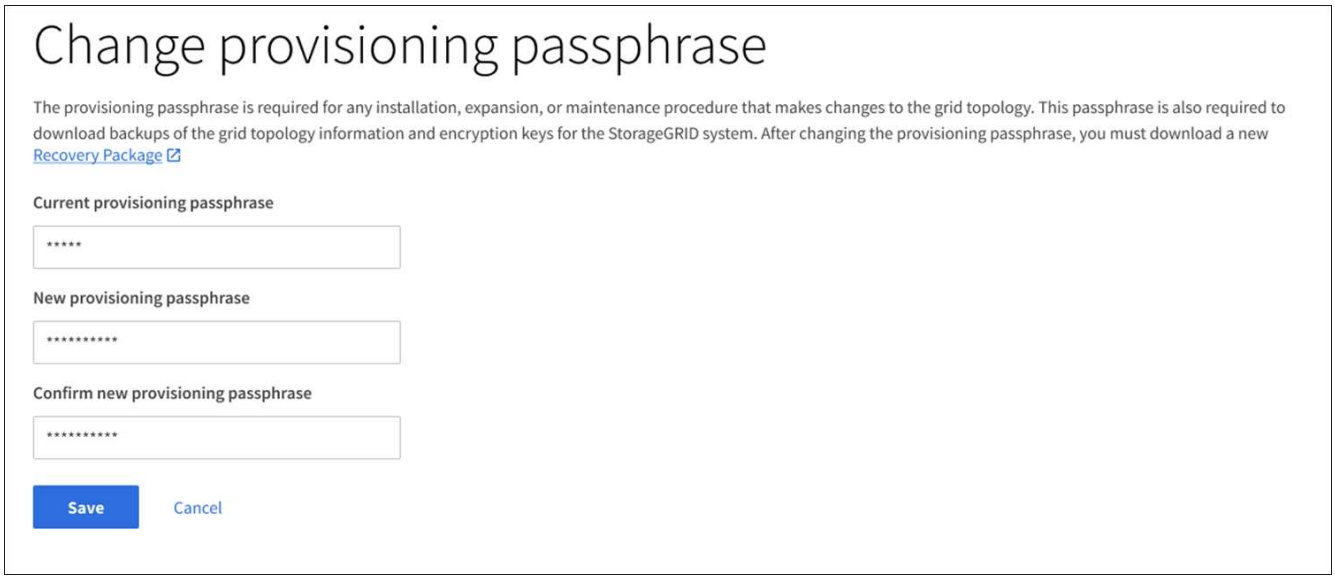
プロビジョニングパスフレーズは、インストールやメンテナンスの手順の多くやで必要になります リカバリパッケージをダウンロードしています。プロビジョニング・パスフレーズは 'passwords.txt ファイルにはリストされていませんプロビジョニングパスフレーズを記録して、安全な場所に保管してください。

手順

1. * 設定 * > * アクセス制御 * > * Grid パスワード * を選択します。

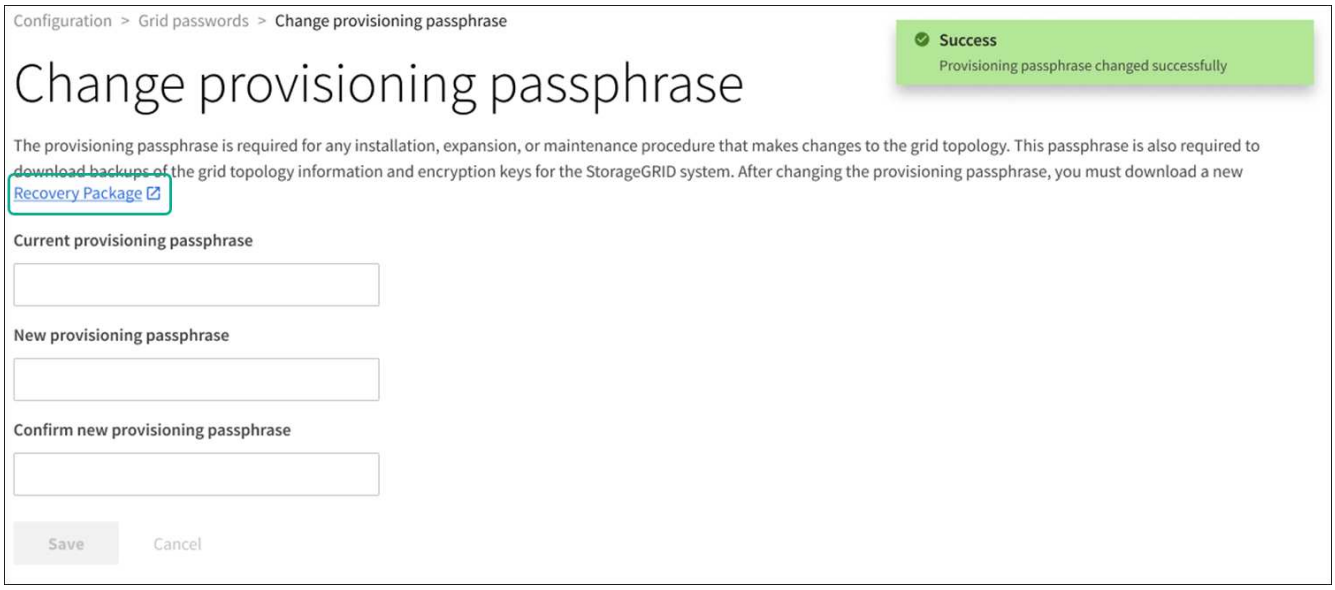


2. [プロビジョニングパスフレーズの変更 *] で [* 変更 *] を選択します。



3. 現在のプロビジョニングパスフレーズを入力します。
4. 新しいパスフレーズを入力します。パスフレーズは 8 文字以上 32 文字以下にする必要があります。パスフレーズでは大文字と小文字が区別されます。
5. 新しいプロビジョニングパスフレーズを安全な場所に保存します。インストール、拡張、およびメンテナンスの手順を実行する必要があります。
6. 新しいパスフレーズをもう一度入力し、「 * 保存 * 」を選択します。

   プロビジョニングパスフレーズの変更が完了すると、成功を示す緑のバナーが表示されます。



7. リカバリパッケージ * を選択します。
8. 新しいプロビジョニングパスフレーズを入力して、新しいリカバリパッケージをダウンロードします。

> プロビジョニングパスフレーズを変更したら、すぐに新しいリカバリパッケージをダウンロードする必要があります。リカバリパッケージファイルは、障害が発生した場合にシステムをリストアするために使用します。

ノードのコンソールパスワードを変更します

グリッド内の各ノードには、一意のノードコンソールパスワードが設定されています。このパスワードを使用してノードにログインする必要があります。次の手順に従って、グリッド内のノードごとに一意のノードコンソールパスワードを変更します。

必要なもの

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Maintenance または Root アクセス権限が必要です。
- 現在のプロビジョニングパスフレーズを用意します。

このタスクについて

ノードのコンソールパスワードを使用して、 SSH を使用して「 admin 」としてノードにログインするか、または VM/ 物理コンソール接続のルートユーザにログインします。ノードコンソールパスワードの変更プロセスでは、グリッド内の各ノードに対して新しいパスワードが作成され、更新されたに格納されます `Passwords.txt` リカバリパッケージ内のファイル。の[Password]列にパスワードが表示されます `Passwords.txt` ファイル。

> ノード間の通信に使用する SSH キー用に、個別の SSH アクセスパスワードがあります。SSH アクセスパスワードはこの手順 によって変更されません。

ウィザードにアクセスします

手順

1. * 設定 * > * アクセス制御 * > * Grid パスワード * を選択します。
2. で、[変更する]*を選択します。

プロビジョニングパスフレーズを入力します

手順

1. グリッドのプロビジョニングパスフレーズを入力します。
2. 「 * Continue * 」を選択します。

現在のリカバリパッケージをダウンロードします

ノードコンソールのパスワードを変更する前に、現在のリカバリパッケージをダウンロードしてください。いずれかのノードでパスワードの変更プロセスが失敗した場合は、このファイルのパスワードを使用できます。

手順

1. [リカバリパッケージのダウンロード] を選択します。
2. リカバリパッケージファイルをコピーします (`.zip`)を2箇所に安全に、安全に、そして別 々 の場所に移動します。

> リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

3. 「 * Continue * 」を選択します。
4. 確認ダイアログが表示されたら、ノードコンソールのパスワードの変更を開始する準備ができている場合は*[はい]*を選択します。

   このプロセスは開始後にキャンセルすることはできません。

ノードのコンソールパスワードを変更します

ノードのコンソールパスワードのプロセスが開始されると、新しいパスワードを含む新しいリカバリパッケージが生成されます。その後、各ノードでパスワードが更新されます。

手順

1. 新しいリカバリパッケージが生成されるまで待ちます。これには数分かかることがあります。
2. [新しいリカバリパッケージのダウンロード] を選択します。
3. ダウンロードが完了したら、次の手順を実行

   a. 「 .zip 」ファイルを開きます。
   b. などのコンテンツにアクセスできることを確認します `Passwords.txt` ファイル。ノードコンソールの新しいパスワードを格納します。
   c. 新しいリカバリパッケージファイルをコピーします (`.zip`)を2箇所に安全に、安全に、そして別 々 の場所に移動します。

   古いリカバリパッケージは上書きしないでください。

   リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

4. 新しいリカバリパッケージをダウンロードしてコンテンツを検証したことを示すチェックボックスを選択します。
5. [ノードコンソールパスワードの変更]*を選択し、すべてのノードが新しいパスワードで更新されるまで待ちます。この処理には数分かかることがあります。

   すべてのノードでパスワードを変更した場合は、成功を示す緑のバナーが表示されます。次の手順に進みます。

   更新プロセスでエラーが発生した場合は、バナーメッセージにパスワードを変更できなかったノードの数が表示されます。パスワードを変更できなかったノードに対して、処理が自動的に再試行されます。プロセスが終了してもパスワードが変更されていないノードがある場合は、「 * Retry * 」ボタンが表示されます。

   1 つ以上のノードでパスワードの更新に失敗した場合：

   a. 表に表示されたエラーメッセージを確認します。
   b. 問題を解決します。
   c. [* Retry*] を選択します。

再試行すると、前回のパスワード変更で失敗したノード上のノードコンソールパスワードのみが変更されます。

6. すべてのノードのノードコンソールパスワードを変更したら、を削除します 最初にダウンロードしたリカバリパッケージ。
7. 必要に応じて、 * Recovery パッケージ * リンクを使用して、新しいリカバリパッケージの追加コピーをダウンロードできます。

ファイアウォールによるアクセスの制御

ファイアウォールでアクセスを制御するには、外部ファイアウォールで特定のポートを開くか、または閉じます。

外部ファイアウォールでアクセスを制御します

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、ファイアウォールでテナントが Grid Manager に接続できないようにすることができます。

ポート	説明	ポートが開いている場合
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザと管理 API クライアントは、 Grid Manager 、 Grid 管理 API 、 Tenant Manager 、およびテナント管理 API にアクセスできます。 • 注： * ポート 443 は一部の内部トラフィックにも使用されます。
8443	管理ノード上の制限された Grid Manager ポート	• Web ブラウザと管理 API クライアントは、HTTPS を使用して Grid Manager とグリッド管理 API にアクセスできます。 • Web ブラウザと管理 API クライアントは、Tenant Manager またはテナント管理 API にはアクセスできません。 • 内部コンテンツに対する要求は拒否されます。
ポート 1	管理ノード上の制限された Tenant Manager ポート	• Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。 • Web ブラウザと管理 API クライアントは、 Grid Manager またはグリッド管理 API にはアクセスできません。 • 内部コンテンツに対する要求は拒否されます。

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

関連情報

- Grid Manager にサインインします
- テナントアカウントを作成する
- 外部との通信

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、グループやユーザを迅速に設定できます。また、ユーザは使い慣れたクレデンシャルを使用して StorageGRID にサインインできます。

Grid Manager のアイデンティティフェデレーションを設定する

管理者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、 Grid Manager で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

- を使用して Grid Manager にサインインします 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。
- シングルサインオン（ SSO ）を有効にする場合は、を確認しておきます シングルサインオンの使用要件。
- 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

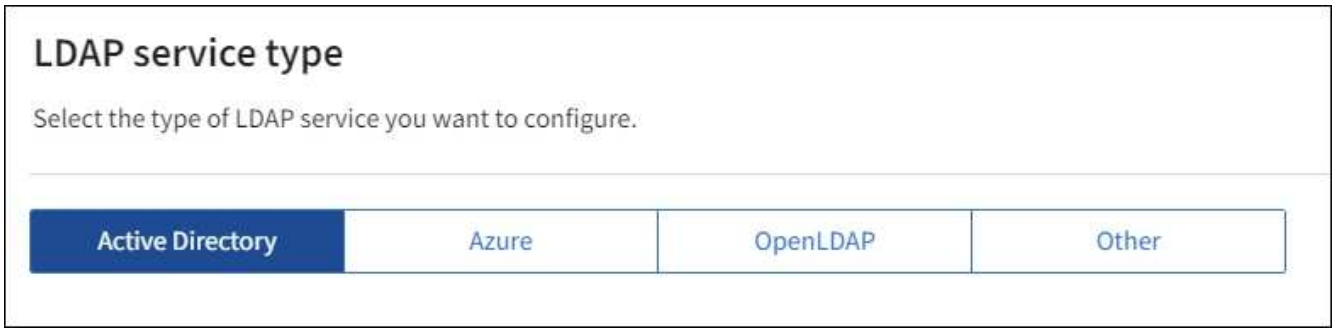
Active Directory 、 Azure AD 、 OpenLDAP 、 Oracle Directory Server などの別のシステムからグループをインポートする場合は、 Grid Manager のアイデンティティソースを設定できます。インポートできるグループのタイプは次のとおりです。

- 管理者グループ。管理者グループ内のユーザは、グループに割り当てられた管理権限に基づいて、 Grid Manager にサインインしてタスクを実行できます。

- 独自のアイデンティティソースを使用しないテナントのテナントユーザグループ。テナントグループ内のユーザは、 Tenant Manager でグループに割り当てられた権限に基づいてタスクを実行し、 Tenant Manager にサインインしてタスクを実行できます。を参照してください テナントアカウントを作成する および テナントアカウントを使用する を参照してください。

設定を入力します

1. [* 設定 * > * アクセス制御 * > * 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。

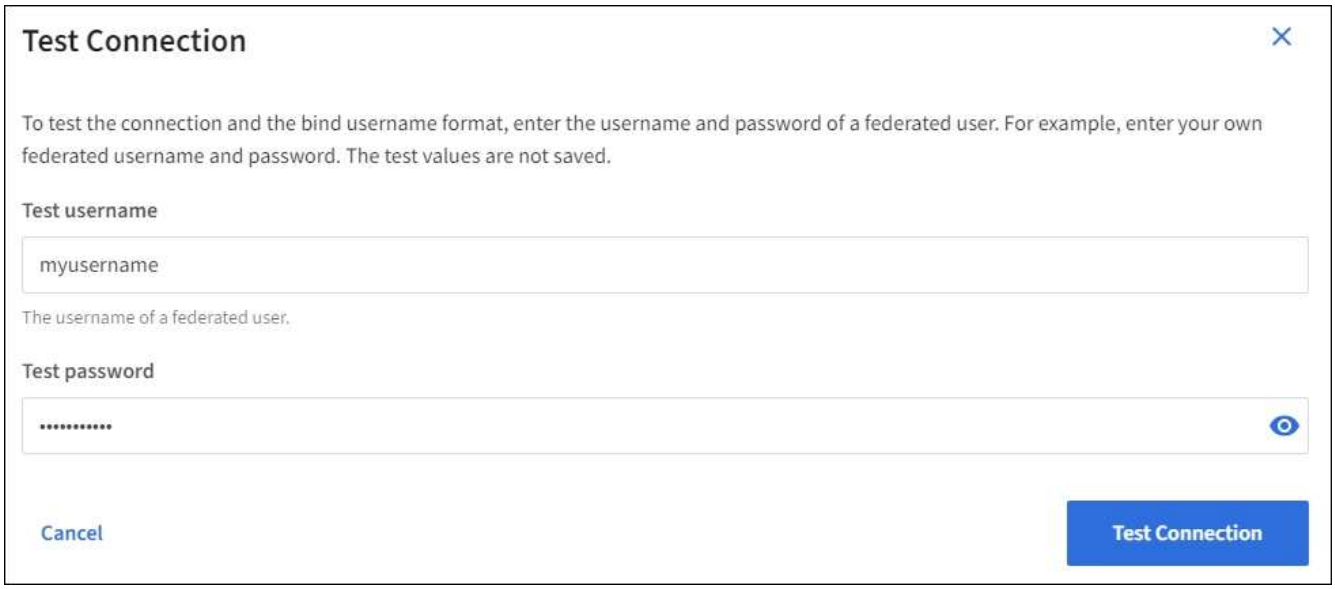
     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

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"^]。

管理者グループを管理する

管理者グループを作成して、 1 人以上の管理者ユーザのセキュリティ権限を管理できます。StorageGRID システムへのアクセスを許可するには、ユーザがグループに属してい

る必要があります。

必要なもの

- を使用して Grid Manager にサインインします 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。
- 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。

管理者グループを作成します

管理者グループを使用すると、 Grid Manager およびグリッド管理 API のどのユーザがどの機能や処理にアクセスできるかを決定できます。

ウィザードにアクセスします

1. * configuration * > * Access control * > * Admin 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。

- ローカルユーザに権限を割り当てる場合は、ローカルグループを作成します。
- アイデンティティソースからユーザをインポートするためのフェデレーテッドグループを作成します。

ローカルグループ

1. * ローカルグループ * を選択します。
2. グループの表示名を入力します。必要に応じてあとから更新できます。たとえば、「 Maintenance Users 」または「 ILM Administrators 」のようになります。
3. グループの一意の名前を入力します。あとで更新することはできません。
4. 「 * Continue * 」を選択します。

フェデレーテッドグループ

1. [フェデレーショングループ] を選択します。
2. インポートするグループの名前を、設定されているアイデンティティソースに表示されているとおりに入力します。
   - Active Directory および Azure の場合は、 sAMAccountName を使用します。
   - OpenLDAP の場合は、 CN （共通名）を使用します。
   - 別の LDAP を使用する場合は、 LDAP サーバに適切な一意の名前を使用します。
3. 「 * Continue * 」を選択します。

グループの権限を管理します

1. * アクセスモード * では、グループ内のユーザが Grid Manager およびグリッド管理 API で設定の変更や処理を実行できるかどうか、あるいは設定と機能のみを表示できるかどうかを選択します。
   - * 読み取り / 書き込み * （デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 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。Grid Manager API や Grid 管理 API で変更や処理を行うことはできません。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。

   ユーザー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、ユーザーは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. 1 つ以上を選択します [グループ権限]。

   各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、グループに属するユーザは StorageGRID にサインインできません。

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）

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、ユーザを追加せずにグループを保存できます。このグループは、ユーザページでユーザに追加できます。を参照してくださいユーザを管理します を参照してください。

2. [グループの作成 *] と [完了 *] を選択します。

管理者グループを表示および編集します

既存のグループの詳細の表示、グループの変更、またはグループの複製を行うことができます。

- すべてのグループの基本情報を表示するには '[グループ] ページの表を確認します
- 特定のグループのすべての詳細を表示したり、グループを編集したりするには、 * アクション * メニューまたは詳細ページを使用します。

タスク	[アクション] メニュー	詳細ページ
グループの詳細を表示します	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループの詳細を表示 *] を選択します。	テーブルでグループ名を選択します。

タスク	[アクション] メニュー	詳細ページ
表示名の編集（ローカルグループのみ）	a. グループのチェックボックスをオンにします。 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ます。 d. 「変更を保存」を選択します。	a. グループ名を選択して詳細を表示します。 b. 編集アイコンを選択します 。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。
アクセスモードまたは権限を編集します	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループの詳細を表示 *] を選択します。 c. 必要に応じて、グループのアクセスモードを変更します。 d. 必要に応じて、を選択または選択解除します [グループ権限]。 e. 「変更を保存」を選択します。	a. グループ名を選択して詳細を表示します。 b. 必要に応じて、グループのアクセスモードを変更します。 c. 必要に応じて、を選択または選択解除します [グループ権限]。 d. 「変更を保存」を選択します。

グループを複製します

1. グループのチェックボックスをオンにします。
2. [* アクション * > * グループの複製 *] を選択します。
3. グループ複製ウィザードを完了します。

グループを削除します

管理者グループを削除すると、システムからそのグループを削除し、グループに関連付けられているすべての権限を削除できます。管理者グループを削除すると、そのグループからすべてのユーザが削除されますが、ユーザは削除されません。

1. [グループ] ページで、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。
2. [* アクション * > * グループの削除 *] を選択します。
3. 「 * グループを削除する * 」を選択します。

グループ権限

管理者ユーザグループを作成する場合は、 Grid Manager の特定の機能へのアクセスを制御する権限を 1 つ以上選択します。その後、作成した 1 つ以上の管理者グループに各ユーザを割り当てて、ユーザが実行できるタスクを決定できます。

各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、そのグループに属するユーザは Grid Manager またはグリッド管理 API にサインインできません。

デフォルトでは、少なくとも 1 つの権限が割り当てられたグループに属するユーザは次のタスクを実行できます。

- Grid Manager にサインインします
- ダッシュボードを表示します
- ノードページを表示します
- グリッドトポロジを監視する
- 現在のアラートと解決済みのアラートを表示します
- 現在のアラームと履歴アラームの表示（従来のシステム）
- 自分のパスワードを変更する（ローカルユーザのみ）
- Configuration ページと Maintenance ページで特定の情報を表示します

権限とアクセスモードの相互作用

すべての権限について、グループの * アクセスモード * 設定は、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みを表示できるかどうかを決定します。ユーザー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、ユーザーは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。

以降のセクションでは、管理者グループの作成時または編集時に割り当てることができる権限について説明します。明示的に言及されていない機能には、 * Root Access * 権限が必要です。

ルートアクセス

この権限は、すべてのグリッド管理機能へのアクセスを許可します。

アラームへの確認応答（レガシー）

アラームの確認と応答を許可します（従来型システム）。サインインしたすべてのユーザが現在のアラームと履歴アラームを表示できます。

ユーザにグリッドトポロジの監視とアラームへの確認応答だけを許可するには、この権限を割り当てる必要があります。

テナントの **root** パスワードを変更する

この権限は、テナントページの * root パスワードの変更 * オプションへのアクセスを許可し、テナントのローカル root ユーザのパスワードを変更できるユーザを制御することを可能にします。この権限は、 S3 キーのインポート機能が有効になっている場合に S3 キーの移行にも使用されます。この権限を持たないユーザには、*Change root password * オプションは表示されません。

> Change root password * オプションが含まれている tenants ページへのアクセスを許可するには、 * Tenant accounts * 権限を割り当てます。

Grid トポロジページの設定

この権限では、サポート * > * ツール * > * グリッドトポロジ * ページの構成タブにアクセスできます。

ILM

この権限は、次の * ILM * メニュー・オプションへのアクセスを提供します。

- ルール
- ポリシー
- イレイジャーコーディング
- リージョン
- ストレージプール

> ストレージグレードを管理するには、ユーザに * Other Grid Configuration * 権限と * Grid Topology Page Configuration * 権限が必要です。

メンテナンス

これらのオプションを使用するには、 Maintenance 権限が必要です。

- * 設定 * > * アクセス制御 * ：
  - Grid のパスワード
- * メンテナンス * > * タスク * ：
  - 運用停止
  - 拡張
  - オブジェクトの存在チェック
  - リカバリ
- * メンテナンス * > * システム * ：
  - リカバリパッケージ
  - ソフトウェアの更新
- * サポート * > * ツール * ：
  - ログ

Maintenance 権限がないユーザは、次のページを表示できますが、編集することはできません。

- * メンテナンス * > * ネットワーク * ：
  - DNS サーバ
  - Grid ネットワーク
  - NTP サーバ
- * メンテナンス * > * システム * ：
  - 使用許諾
- * 設定 * > * セキュリティ * ：
  - 証明書

    - ドメイン名
- * コンフィグレーション * > * モニタリング * ：
    - 監査と syslog サーバ

アラートの管理

この権限では、アラートを管理するためのオプションにアクセスできます。サイレンス、アラート通知、アラートルールを管理するには、この権限が必要です。

指標クエリ

この権限は、 **support**>*Tools*>*Metrics* ページにアクセスする権限を提供します。また、グリッド管理 API の「指標」セクションを使用して、カスタムの Prometheus 指標クエリにアクセスすることもできます。

オブジェクトメタデータの検索

この権限は、 * ILM * > * Object metadata lookup * ページへのアクセスを提供します。

その他のグリッド設定

この権限で、追加のグリッド設定オプションにアクセスできます。

> これらの追加オプションを表示するには、ユーザに * Grid トポロジページの設定 * 権限が必要です。

- * ILM * ：
    - ストレージグレード
- * 設定 * > * ネットワーク * ：
    - リンクコスト
- * コンフィグレーション * > * システム * ：
    - 表示オプション
    - グリッドオプション
    - ストレージオプション
- * サポート * > * アラーム（レガシー） * ：
    - カスタムイベント
    - グローバルアラーム
    - 従来の E メール設定

ストレージアプライアンス管理者

この権限は、グリッドマネージャを介してストレージアプライアンスの E シリーズ SANtricity システムマネージャにアクセスすることを許可します。

テナントアカウント

テナントページにアクセスし、テナントアカウントを作成、編集、削除できます。この権限を持つユーザは、既存のトラフィック分類ポリシーを表示することもできます。

API で機能を非アクティブ化します

グリッド管理 API を使用すると、 StorageGRID システムの特定の機能を完全に非アクティブ化できます。機能を非アクティブ化すると、その機能に関連するタスクを実行する権限をユーザに割り当てることができなくなります。

このタスクについて

非活動化されたフィーチャーシステムを使用すると、 StorageGRID システムの特定のフィーチャーへのアクセスを禁止できます。機能の非アクティブ化は、 root ユーザまたは * Root Access * 権限を持つ管理者グループに属するユーザがその機能を使用できないようにする唯一の方法です。

この機能がどのように役立つかを理解するために、次のシナリオを検討してください。

_Company A は、テナントアカウントを作成して StorageGRID システムのストレージ容量をリースするサービスプロバイダです。容量をリースしている顧客のオブジェクトのセキュリティを保護するために、 A 社では、アカウントの導入後に自社の従業員がテナントアカウントにアクセスできないようにしたいと考えています。 _

_ 企業 A は、グリッド管理 API で Deactivate Features システムを使用することで、この目的を達成できます。Grid Manager （ UI と API の両方）で * テナントの root パスワードの変更 * 機能を完全に非アクティブ化することで、 A 社は、 root ユーザおよび * Root Access * 権限を持つグループに属するユーザを含むすべての Admin ユーザが、任意のテナントアカウントの root ユーザのパスワードを変更できるようにすることができます。 _

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。を参照してください グリッド管理 API を使用します。
2. Deactivate Features エンドポイントを探します。
3. テナントの root パスワードの変更などの機能を非アクティブ化するには、次のような本文を API に送信します。

   '{" グリッド ":{" changeTenantRootPassword":true}`

   要求が完了すると、テナントの root パスワードの変更機能が無効になります。テナントの root パスワードを変更する * 管理権限がユーザインターフェイスに表示されなくなり、テナントの root パスワードを変更する API 要求はすべて「 403 Forbidden 」エラーで失敗します。

非アクティブ化した機能を再アクティブ

デフォルトでは、グリッド管理 API を使用して、非アクティブ化した機能を再アクティブ化できます。ただし、非アクティブ化された機能が再アクティブ化されないようにするには、 * activateFeatures * 機能自体を非アクティブ化します。

> * activateFeatures * 機能を再アクティブ化できません。この機能を非アクティブ化すると、非アクティブ化した他の機能を永続的に再アクティブ化できなくなることに注意してください。失われた機能をリストアするには、テクニカルサポートにお問い合わせください。

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。
2. Deactivate Features エンドポイントを探します。
3. すべての機能を再アクティブ化するには、次のような本文を API に送信します。

   '{"grid":null}`

   この要求が完了すると、テナントの root パスワード変更機能を含むすべての機能が再アクティブ化されます。ユーザに * Root access * 権限または * Change tenant root password * 管理権限が割り当てられている場合、テナントの root パスワードを変更する API 要求はすべてユーザインターフェイスに表示され、テナントの root パスワードを変更する API 要求は成功します。

> 前述の例は、 _all_deactivated 機能を再アクティブ化します。非アクティブ化したままにする必要がある他の機能が非アクティブ化されている場合は、 PUT 要求でそれらを明示的に指定する必要があります。たとえば、テナントのルートパスワード変更機能を再アクティブ化し、アラーム確認応答機能を非アクティブ化し続けるには、次の PUT 要求を送信します。
>
> '{"grid" ： {"alarmAcknowledgement" ： true}`

ユーザを管理します

ローカルユーザとフェデレーテッドユーザを表示できます。また、ローカルユーザを作成してローカル管理者グループに割り当て、そのユーザがアクセスできる Grid Manager 機能を決定することもできます。

必要なもの

- を使用して Grid Manager にサインインします 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。

ローカルユーザを作成します

1 人以上のローカルユーザを作成し、各ユーザを 1 つ以上のローカルグループに割り当てることができます。このグループの権限は、ユーザがアクセスできる Grid Manager および Grid 管理 API 機能を制御します。

作成できるのはローカルユーザのみです。外部のアイデンティティソースを使用して、フェデレーテッドユーザとフェデレーテッドグループを管理します。

Grid Manager には ' ルートという名前の ' 事前定義されたローカル・ユーザが 1 つ含まれています root ユーザを削除することはできません。

> 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 StorageGRID にサインインできません。

ウィザードにアクセスします

1. [* 設定 * > * アクセス制御 * > * 管理者ユーザー *] を選択します。
2. 「 * ユーザーの作成 * 」を選択します。

ユーザクレデンシャルを入力します

1. ユーザのフルネーム、一意なユーザ名、およびパスワードを入力します。
2. 必要に応じて、このユーザに Grid Manager または Grid 管理 API へのアクセスを禁止する場合は「 * Yes 」を選択します。
3. 「 * Continue * 」を選択します。

グループに割り当てます

1. 必要に応じて、ユーザを 1 つ以上のグループに割り当てて、そのユーザの権限を決定します。

   まだグループを作成していない場合は、グループを選択せずにユーザを保存できます。このユーザーは、[グループ] ページでグループに追加できます。

   ユーザが複数のグループに属している場合は、権限の累積数が算出されます。を参照してください管理者グループを管理する を参照してください。

2. [Create user*] を選択し、 [**Finish**] を選択します。

ローカルユーザを表示および編集します

既存のローカルユーザとフェデレーテッドユーザの詳細を表示できます。ローカルユーザを変更して、ユーザのフルネーム、パスワード、またはグループメンバーシップを変更できます。また、ユーザが Grid Manager およびグリッド管理 API にアクセスすることを一時的に禁止することもできます。

編集できるのはローカルユーザのみです。外部のアイデンティティソースを使用してフェデレーテッドユーザを管理します。

- 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を表示するには、ユーザページのテーブルを確認してください。
- 特定のユーザの詳細をすべて表示したり、ローカルユーザを編集したり、ローカルユーザのパスワードを変更したりするには、 * Actions * メニューまたは詳細ページを使用します。

  編集内容は、次回ユーザがグリッドマネージャからサインアウトして再度サインインしたときに適用されます。

> ローカルユーザは、 Grid Manager のバナーで * Change Password * オプションを使用して自分のパスワードを変更できます。

タスク	[アクション] メニュー	詳細ページ
ユーザの詳細を表示します	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。	テーブルでユーザの名前を選択します。
フルネームの編集（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. * アクション * > * 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。	a. 詳細を表示するユーザの名前を選択します。 b. 編集アイコンを選択します 。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。
StorageGRID アクセスを拒否または許可します	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [アクセス] タブを選択します。 d. ユーザが Grid Manager または Grid 管理 API にサインインできないようにするには「 * Yes 」を選択します。サインインできるようにするには、「 * No * 」を選択します。 e. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [アクセス] タブを選択します。 c. ユーザが Grid Manager または Grid 管理 API にサインインできないようにするには「 * Yes 」を選択します。サインインできるようにするには、「 * No * 」を選択します。 d. 「変更を保存」を選択します。
パスワードを変更（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [パスワード] タブを選択します。 d. 新しいパスワードを入力します。 e. [パスワードの変更 *] を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [パスワード] タブを選択します。 c. 新しいパスワードを入力します。 d. [パスワードの変更 *] を選択します。

タスク	[アクション] メニュー	詳細ページ
変更グループ（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [グループ] タブを選択します。 d. 必要に応じて、グループ名のあとのリンクを選択し、新しいブラウザタブでグループの詳細を表示します。 e. 「 * グループを編集」を選択して、別のグループを選択します。 f. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [グループ] タブを選択します。 c. 必要に応じて、グループ名のあとのリンクを選択し、新しいブラウザタブでグループの詳細を表示します。 d. 「 * グループを編集」を選択して、別のグループを選択します。 e. 「変更を保存」を選択します。

ユーザを複製します

既存のユーザを複製して、同じ権限を持つ新しいユーザを作成することができます。

1. ユーザのチェックボックスを選択します。
2. * アクション * > * ユーザーの複製 * を選択します。
3. 複製ユーザーウィザードを完了します。

ユーザを削除します

ローカルユーザを削除して、そのユーザをシステムから完全に削除できます。

root ユーザを削除することはできません。

1. [ユーザー] ページで、削除する各ユーザー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. 「 * ユーザーの削除 * 」を選択します。

シングルサインオン（ SSO ）を使用

シングルサインオンを設定します

シングルサインオン（ SSO ）が有効な場合、ユーザは、組織によって実装された SSO サインインプロセスを使用してクレデンシャルが許可されている場合にのみ、 Grid Manager 、テナントマネージャ、 Grid 管理 API 、またはテナント管理 API にアクセスできます。ローカルユーザは StorageGRID にサインインできません。

シングルサインオンの仕組み

StorageGRID システムでは、 Security Assertion Markup Language 2.0 （ SAML 2.0 ）標準を使用したシングルサインオン（ SSO ）がサポートされます。

シングルサインオン（ SSO ）を有効にする前に、 SSO が有効になった場合に StorageGRID のサインインとサインアウトのプロセスにどのような影響があるかを確認してください。

SSO が有効な場合はサインインします

SSO が有効な場合に StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。

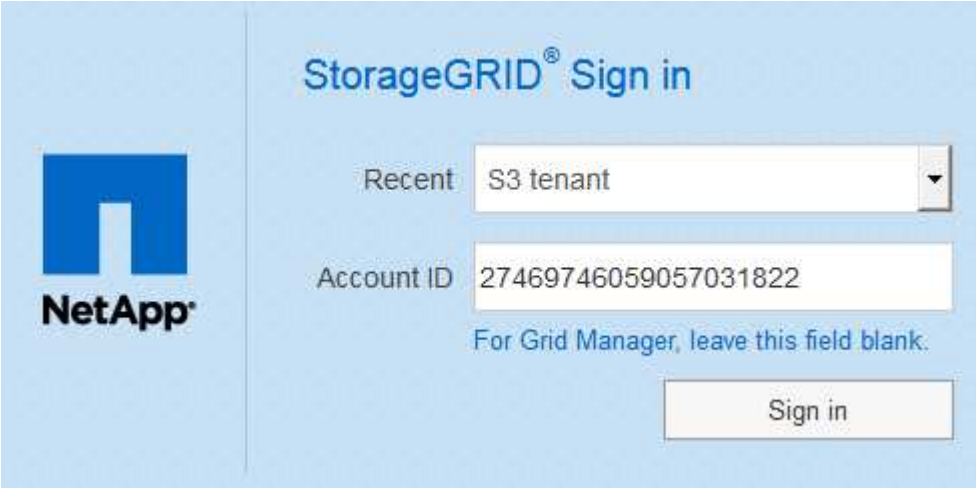
手順

1. Web ブラウザで、 StorageGRID 管理ノードの完全修飾ドメイン名または IP アドレスを入力します。

   StorageGRID のサインインページが表示されます。

   - このブラウザで初めて URL にアクセスした場合は、アカウント ID の入力を求められます。

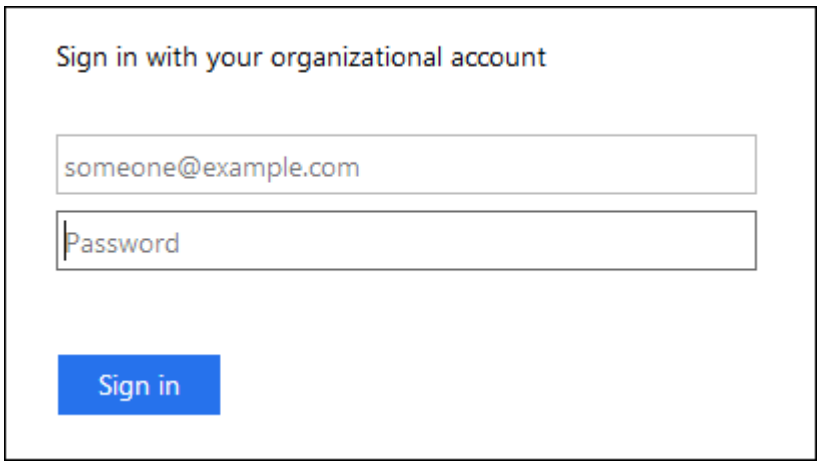
   - Grid Manager または Tenant Manager に以前にアクセスしていた場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。



> テナントアカウントの完全な URL （完全修飾ドメイン名または IP アドレスのあとに「 / ？ accountId=*20* 桁の *account-id* 」）を入力すると、 StorageGRID サインインページは表示されません。代わりに、組織の SSO サインインページがすぐに表示されます。このページでは、を実行できます SSO クレデンシャルを使用してサインインします。

2. Grid Manager と Tenant Manager のどちらにアクセスするかを指定します。
   - Grid Manager にアクセスするには、 * Account ID * フィールドを空白のままにします。アカウント ID に「 * 0 」と入力するか、最近のアカウントのリストに * Grid Manager * が表示されている場合はそれを選択します。
   - Tenant Manager にアクセスするには、 20 桁のテナントアカウント ID を入力するか、最近のアカウントのリストにテナントが表示されている場合は名前でテナントを選択します。
3. 「サインイン」を選択します

   StorageGRID は、組織の SSO サインインページにリダイレクトします。例：



4. [[signin_soS] SSO クレデンシャルを使用してサインインします。

   SSO クレデンシャルが正しい場合：

   a. アイデンティティプロバイダ（ IdP ）が StorageGRID に認証応答を返します。
   b. StorageGRID が認証応答を検証します。
   c. 応答が有効で、 StorageGRID アクセス権限のあるフェデレーテッドグループに属している場合は、選択したアカウントに応じて、 Grid Manager またはテナントマネージャにサインインされます。

   > サービスアカウントにアクセスできない場合でも、 StorageGRID アクセス権限を持つフェデレーテッドグループに属する既存のユーザであれば、サインインできます。

5. 必要に応じて、他の管理ノードにアクセスします。または、適切な権限がある場合は Grid Manager またはテナントマネージャにアクセスします。

   SSO クレデンシャルを再入力する必要はありません。

SSO が有効な場合はサインアウトします

StorageGRID で SSO が有効になっている場合にサインアウトするとどうなるかは、サインイン先とサインア

ウト元によって異なります。

手順

1. ユーザインターフェイスの右上隅にある [**Sign Out**] リンクを探します。
2. 「サインアウト」を選択します。

   StorageGRID のサインインページが表示されます。[Recent Accounts] * ドロップダウンが更新されて、 * Grid Manager * またはテナント名が表示されるようになり、これらのユーザインターフェイスにあとからすばやくアクセスできるようになります。

サインイン先	サインアウト元	サインアウトされる対象
1 つ以上の管理ノードでグリッドマネージャを使用します	任意の管理ノード上の Grid Manager	すべての管理ノード上の Grid Manager • 注： * SSO に Azure を使用している場合、すべての管理ノードからサインアウトするまでに数分かかることがあります。
1 つ以上の管理ノード上の Tenant Manager	任意の管理ノード上の Tenant Manager	すべての管理ノード上の Tenant Manager
Grid Manager と Tenant Manager の両方	Grid Manager の略	Grid Manager のみ。SSO からサインアウトするには、 Tenant Manager からもサインアウトする必要があります。

次の表は、単一のブラウザセッションを使用している場合にサインアウトしたときの動作をまとめたものです。複数のブラウザセッションで StorageGRID にサインインしている場合は、すべてのブラウザセッションから個別にサインアウトする必要があります。

シングルサインオンの使用要件

StorageGRID システムでシングルサインオン（ SSO ）を有効にする前に、このセクションの要件を確認してください。

アイデンティティプロバイダの要件

StorageGRID では、次の SSO アイデンティティプロバイダ（ IdP ）をサポートしています。

- Active Directory フェデレーションサービス（ AD FS ）
- Azure Active Directory （ Azure AD ）
- PingFederate

SSO アイデンティティプロバイダを設定する前に、 StorageGRID システムのアイデンティティフェデレーションを設定する必要があります。アイデンティティフェデレーションに使用する LDAP サービスのタイプに

よって、実装できる SSO のタイプが制御されます。

LDAP サービスタイプが設定されました	SSO アイデンティティプロバイダのオプション
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

AD FS の要件

次のいずれかのバージョンの AD FS を使用できます。

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 でが使用されている必要があります "KB3201845 の更新プログラム"またはそれ以上。

- AD FS 3.0 （ Windows Server 2012 R2 Update 以降に付属）。

その他の要件

- Transport Layer Security （ TLS ） 1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以降

サーバ証明書の要件

デフォルトでは、 StorageGRID は各管理ノード上の管理インターフェイス証明書を使用して、 Grid Manager 、テナントマネージャ、グリッド管理 API 、およびテナント管理 API へのアクセスを保護します。StorageGRID 用の証明書利用者信頼（ AD FS ）、エンタープライズアプリケーション（ Azure ）、またはサービスプロバイダ接続（ PingFederate ）を設定するときは、 StorageGRID 要求の署名証明書としてサーバ証明書を使用します。

まだお持ちでない場合は 管理インターフェイス用のカスタム証明書を設定しましたでは、今すぐ実行してください。インストールしたカスタムサーバ証明書はすべての管理ノードで使用され、すべての StorageGRID 証明書利用者信頼、エンタープライズアプリケーション、または SP 接続で使用できます。

> 管理ノードのデフォルトサーバ証明書を証明書利用者信頼、エンタープライズアプリケーション、または SP 接続で使用することは推奨されません。ノードに障害が発生した場合にそのノードをリカバリすると、新しいデフォルトサーバ証明書が生成されます。リカバリしたノードにサインインするには、証明書利用者信頼、エンタープライズアプリケーション、または SP 接続を新しい証明書で更新する必要があります。

管理ノードのサーバ証明書にアクセスするには、ノードのコマンドシェルにログインし、「 /var/local/mgmt-api 」ディレクトリに移動します。カスタムサーバ証明書の名前は「 custom-server.crt 」です。ノードのデフォルトのサーバ証明書の名前は 'server.crt' です

ポート要件

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。を参照してください ファイアウォールによるアクセスの制御。

フェデレーテッドユーザがサインインできることを確認する

シングルサインオン（ SSO ）を有効にする前に、少なくとも 1 人のフェデレーテッドユーザが既存のテナントアカウント用に Grid Manager および Tenant Manager にサインインできることを確認する必要があります。

必要なもの

- を使用して Grid Manager にサインインします 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。
- アイデンティティフェデレーションがすでに設定されている。

手順

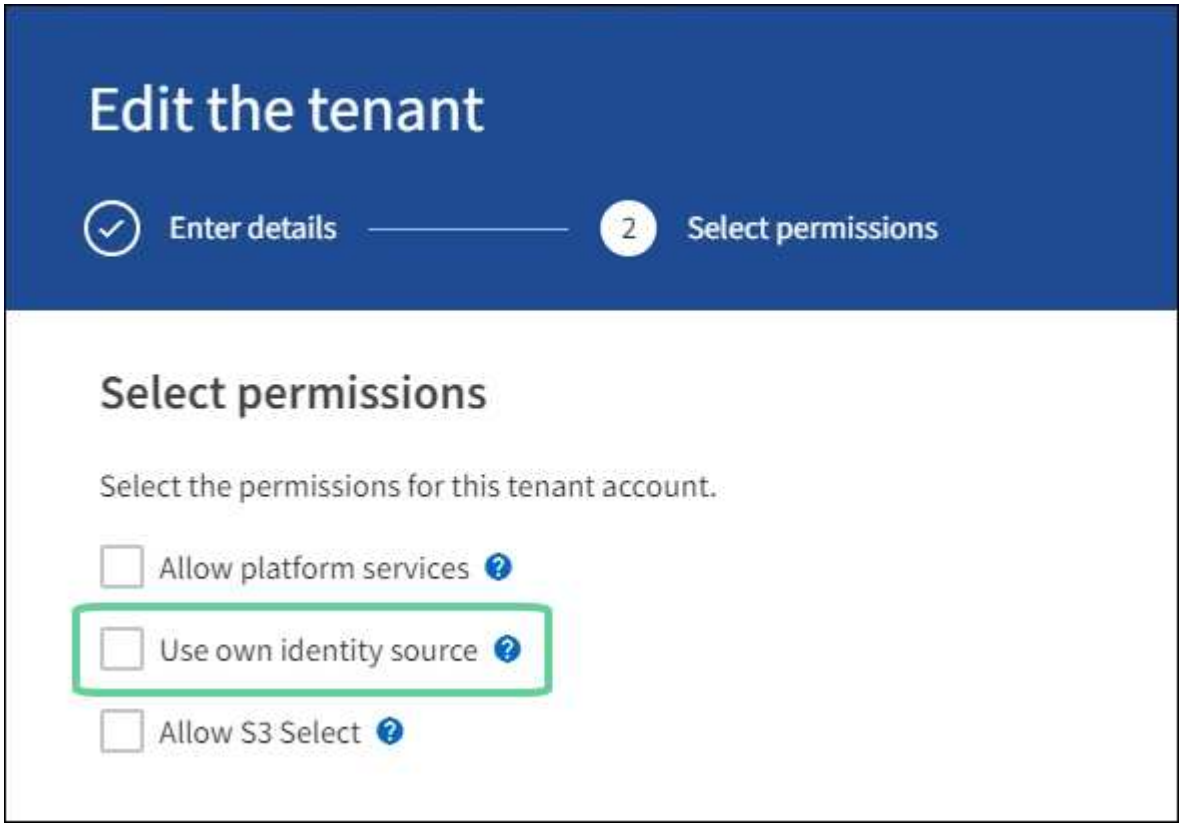
1. 既存のテナントアカウントがある場合は、テナントが独自のアイデンティティソースを使用していないことを確認します。

> SSO を有効にすると、 Tenant Manager で設定されたアイデンティティソースが Grid Manager で設定されたアイデンティティソースによって上書きされます。テナントのアイデンティティソースに属するユーザは、 Grid Manager アイデンティティソースのアカウントがないかぎり、サインインできなくなります。

   a. 各テナントアカウントの Tenant Manager にサインインします。
   b. 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。
   c. ［ * アイデンティティフェデレーションを有効にする * ］ チェックボックスがオフになっていることを確認します。
   d. その場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になっていることを確認し、チェックボックスをオフにして * 保存 * を選択します。
2. フェデレーテッドユーザが Grid Manager にアクセスできることを確認します。
   a. Grid Manager から * configuration * > * Access control * > * Admin groups * を選択します。
   b. Active Directory アイデンティティソースから少なくとも 1 つのフェデレーテッドグループがインポートされていて、そのグループに Root アクセス権限が割り当てられていることを確認します。
   c. サインアウトします。
   d. フェデレーテッドグループ内のユーザとして Grid Manager に再度サインインできることを確認します。
3. 既存のテナントアカウントがある場合は、次の手順を実行して、 Root アクセス権限を持つフェデレーテッドユーザがサインインできることを確認します。
   a. Grid Manager から * tenants * を選択します。
   b. テナントアカウントを選択し、 * Actions * > * Edit * を選択します。

c. Enter details （詳細の入力）タブで、 * Continue （続行） * を選択します。

d. [独自のアイデンティティソースを使用する *] チェックボックスがオンになっている場合は、チェックボックスをオフにして、 [保存 *] を選択します。



Tenant ページが表示されます。

a. テナントアカウントを選択し、 * サインイン * を選択して、ローカルの root ユーザとしてテナントアカウントにサインインします。

b. Tenant Manager で、 * access management * > * Groups * を選択します。

c. Grid Manager から少なくとも 1 つのフェデレーテッドグループにこのテナントに対する Root アクセス権限が割り当てられていることを確認します。

d. サインアウトします。

e. フェデレーテッドグループ内のユーザとしてテナントに再度サインインできることを確認します。

関連情報

- シングルサインオンの使用要件
- 管理者グループを管理する
- テナントアカウントを使用する

サンドボックスモードを使用する

サンドボックスモードを使用すると、すべての StorageGRID ユーザに対してシングルサインオン（ SSO ）を有効にする前に、シングルサインオン（ SSO ）を設定およびテストできます。SSO を有効にした後は、設定を変更したり再テストしたりする必要がある

場合に、サンドボックスモードに戻ることができます。

必要なもの

- を使用して Grid Manager にサインインします サポートされている Web ブラウザ。
- Root アクセス権限が割り当てられている。
- StorageGRID システムにアイデンティティフェデレーションを設定しておきます。
- アイデンティティフェデレーション * LDAP サービスタイプ * では、使用する SSO アイデンティティプロバイダに基づいて、 Active Directory または Azure のいずれかを選択しました。

LDAP サービスタイプが設定されました	**SSO** アイデンティティプロバイダのオプション
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

このタスクについて

SSO が有効な場合、ユーザが管理ノードにサインインしようとすると、 StorageGRID から SSO アイデンティティプロバイダに認証要求が送信されます。次に、 SSO アイデンティティプロバイダは、認証要求が成功したかどうかを示す認証応答を StorageGRID に返します。成功した要求の場合：

- Active Directory または PingFederate からの応答には、ユーザの Universally Unique Identifier （ UUID ）が含まれています。
- Azure からの応答には、ユーザプリンシパル名（ UPN ）が含まれます。

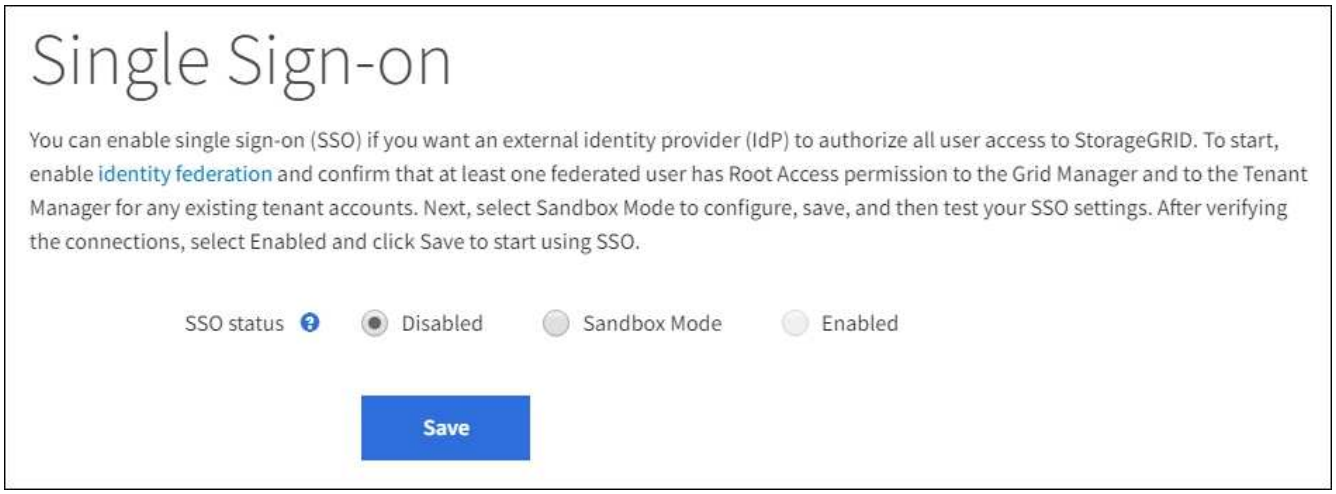
StorageGRID （サービスプロバイダ）と SSO アイデンティティプロバイダがユーザ認証要求についてセキュアに通信できるようにするには、 StorageGRID で特定の設定を行う必要があります。次に、 SSO アイデンティティプロバイダのソフトウェアを使用して、管理ノードごとに証明書利用者信頼（ AD FS ）、エンタープライズアプリケーション（ Azure ）、またはサービスプロバイダ（ PingFederate ）を作成する必要があります。最後に、 StorageGRID に戻って SSO を有効にする必要があります。

サンドボックスモードでは、 SSO を有効にする前に、この手順を簡単に実行し、すべての設定をテストできます。サンドボックスモードを使用している場合、ユーザーは SSO を使用してサインインできません。

サンドボックスモードにアクセスします

1. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。

   [Single Sign-On] ページが表示され、 [**Disabled**] オプションが選択されます。



SSO Status オプションが表示されない場合は、アイデンティティプロバイダがフェデレーテッドアイデンティティソースとして設定されていることを確認します。を参照してください シングルサインオンの使用要件。

2. [* サンドボックスモード *] を選択します。

   [Identity Provider] セクションが表示されます。

アイデンティティプロバイダの詳細を入力します

1. ドロップダウンリストから * SSO タイプ * を選択します。
2. 選択した SSO タイプに基づいて、 [Identity Provider] セクションのフィールドに入力します。

Active Directory

1. アイデンティティプロバイダの * フェデレーションサービス名 * を、 Active Directory フェデレーションサービス（ AD FS ）に表示されているとおりに入力します。

> フェデレーションサービス名を確認するには、 Windows Server Manager に移動します。[ツール *>*AD FS 管理 *] を選択します。[アクション] メニューから、 [* フェデレーションサービスのプロパティの編集 *] を選択します。フェデレーションサービス名が 2 番目のフィールドに表示されます。

2. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。
   - * 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 CA 証明書を使用して接続を保護します。

     この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

   - * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。
3. 証明書利用者セクションで、 StorageGRID の * 証明書利用者 ID * を指定します。この値は、 AD FS の各証明書利用者信頼に使用する名前を制御します。
   - たとえば、グリッドに管理ノードが 1 つしかなく、今後管理ノードを追加する予定がない場合は、「 SG 」または「 StorageGRID 」と入力します。
   - グリッドに複数の管理ノードが含まれている場合は、識別子に「 [HOSTNAME] 」という文字列を含めます。たとえば 'SG-[hostname]` のようにしますこれにより、ノードのホスト名に基づいて、システム内の管理ノードごとの証明書利用者 ID を示すテーブルが生成されます。

> 証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

4. [保存（ Save ）] を選択します。

   数秒間、 * Save *（保存）ボタンに緑色のチェックマークが表示されます。

Azure

1. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。
   - * 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 CA 証明書を使用して接続を保護します。

この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

- * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。

2. [エンタープライズアプリケーション] セクションで、 StorageGRID のエンタープライズアプリケーション名 * を指定します。この値は、 Azure AD の各エンタープライズアプリケーションに使用する名前を制御します。

   - たとえば、グリッドに管理ノードが 1 つしかなく、今後管理ノードを追加する予定がない場合は、「 SG 」または「 StorageGRID 」と入力します。
   - グリッドに複数の管理ノードが含まれている場合は、識別子に「 [HOSTNAME] 」という文字列を含めます。たとえば 'SG-[hostname]` のようにしますこれにより、システム内の管理ノードごとに、そのノードのホスト名に基づいてエンタープライズアプリケーション名が表形式で表示されます。

> StorageGRID システムで管理ノードごとにエンタープライズアプリケーションを作成する必要があります。管理ノードごとにエンタープライズアプリケーションを用意することで、ユーザはどの管理ノードに対しても安全にサインイン / サインアウトすることができます。

3. の手順に従います Azure AD でエンタープライズアプリケーションを作成 表に記載されている管理ノードごとにエンタープライズアプリケーションを作成するには、次の手順を実行します。
4. Azure AD から、各エンタープライズアプリケーションのフェデレーションメタデータの URL をコピーします。次に、この URL を StorageGRID の対応する * フェデレーションメタデータ URL* フィールドに貼り付けます。
5. すべての管理ノードのフェデレーションメタデータの URL をコピーして貼り付けたら、「 * 保存 * 」を選択します。

   数秒間、 * Save * （保存）ボタンに緑色のチェックマークが表示されます。

PingFederate

1. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。

   - * 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 CA 証明書を使用して接続を保護します。

     この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

   - * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。

2. Service Provider （ SP ；サービスプロバイダ）セクションで、 StorageGRID の * SP 接続 ID * を指定します。この値は、 PingFederate の各 SP 接続に使用する名前を制御します。

   - たとえば、グリッドに管理ノードが 1 つしかなく、今後管理ノードを追加する予定がない場合

は、「 SG 」または「 StorageGRID 」と入力します。

- グリッドに複数の管理ノードが含まれている場合は、識別子に「 [HOSTNAME] 」という文字列を含めます。たとえば 'SG-[hostname]` のようにしますこれにより、システム内の管理ノードごとに、そのノードのホスト名に基づいて SP 接続 ID を示す表が生成されます。

> StorageGRID システムで管理ノードごとに SP 接続を作成する必要があります。管理ノードごとに SP 接続を確立することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

3. 各管理ノードのフェデレーションメタデータの URL を * Federation metadata url * フィールドで指定します。

   次の形式を使用します。

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
ID>
```

4. [保存（ Save ）] を選択します。

   数秒間、 * Save * （保存）ボタンに緑色のチェックマークが表示されます。

証明書利用者信頼、エンタープライズアプリケーション、または **SP** 接続を設定する

設定を保存すると、サンドボックスモードの確認メッセージが表示されます。サンドボックスモードが有効になったことを確認し、概要を示します。

StorageGRID は、必要に応じてサンドボックスモードのままにすることができます。ただし、シングルサインオンページで * サンドボックスモード * を選択すると、すべての StorageGRID ユーザーに対して SSO が無効になります。サインインできるのはローカルユーザのみです。

証明書利用者信頼（ Active Directory ）、完全なエンタープライズアプリケーション（ Azure ）、または SP 接続（ PingFederate ）を設定するには、次の手順を実行します。

Active Directory

1. Active Directory フェデレーションサービス（ AD FS ）に移動します。
2. StorageGRID のシングルサインオンページの表に示す各証明書利用者 ID を使用して、StorageGRID 用の証明書利用者信頼を 1 つ以上作成します。

   次の表に示す管理ノードごとに信頼を 1 つ作成する必要があります。

   手順については、を参照してください AD FS に証明書利用者信頼を作成します。

Azure

1. 現在サインインしている管理ノードのシングルサインオンページから、 SAML メタデータをダウンロードして保存するボタンを選択します。
2. グリッド内の他の管理ノードについて、上記の手順を繰り返します。
   a. ノードにサインインします。
   b. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
   c. そのノードの SAML メタデータをダウンロードして保存します。
3. Azure ポータルにアクセスします。
4. の手順に従います Azure AD でエンタープライズアプリケーションを作成 をクリックして、各管理ノードの SAML メタデータファイルを対応する Azure エンタープライズアプリケーションにアップロードします。

PingFederate

1. 現在サインインしている管理ノードのシングルサインオンページから、 SAML メタデータをダウンロードして保存するボタンを選択します。
2. グリッド内の他の管理ノードについて、上記の手順を繰り返します。
   a. ノードにサインインします。
   b. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
   c. そのノードの SAML メタデータをダウンロードして保存します。
3. 「 PingFederate 」に移動します。
4. StorageGRID 用に 1 つ以上の SP 接続を作成します。各管理ノードの SP 接続 ID （ StorageGRID の Single Sign-On ページの表を参照）と、その管理ノード用にダウンロードした SAML メタデータを使用します。

   次の表に示す管理ノードごとに 1 つの SP 接続を作成する必要があります。

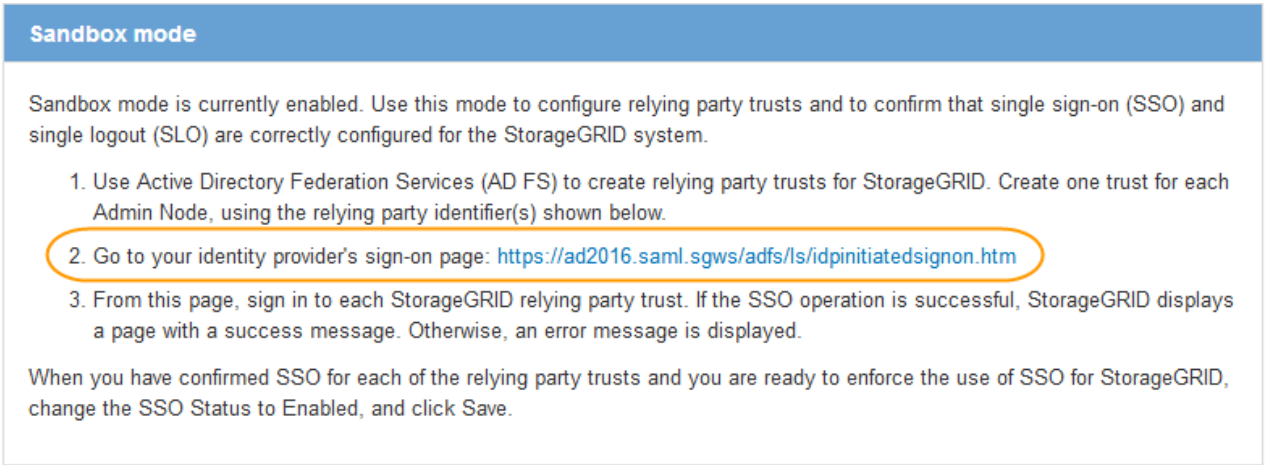
SSO 接続をテストします

StorageGRID システム全体にシングルサインオンを適用する前に、各管理ノードでシングルサインオンとシングルログアウトが正しく設定されていることを確認する必要があります。

Active Directory

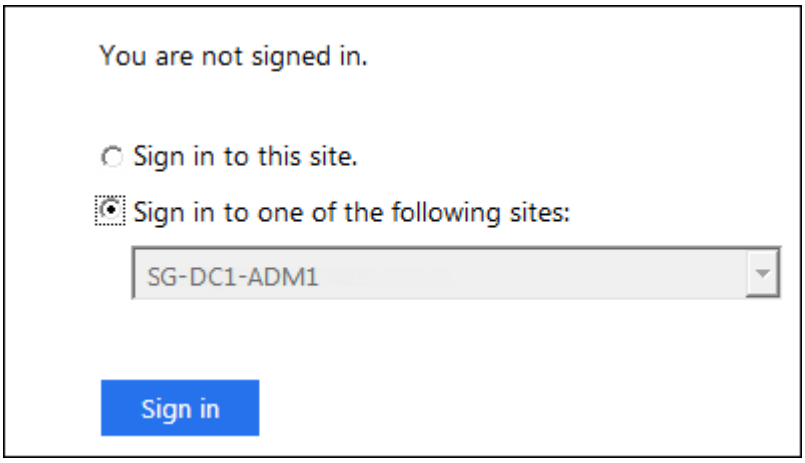
1. StorageGRID のシングルサインオンページで、サンドボックスモードメッセージ内のリンクを探します。

   URL は、 [* フェデレーションサービス名 * （ * Federation service name * ）] フィールドに入力した値から取得されます。

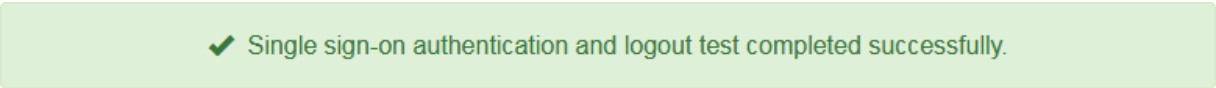
   

2. リンクを選択するか、 URL をコピーしてブラウザに貼り付け、アイデンティティプロバイダのサインオンページにアクセスします。

3. SSO を使用して StorageGRID にサインインできることを確認するには、 * 次のいずれかのサイトにサインイン * を選択し、プライマリ管理ノードの証明書利用者 ID を選択して * サインイン * を選択します。

4. 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。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。

   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。

5. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

Azure

1. Azure ポータルのシングルサインオンページに移動します。
2. [このアプリケーションをテストする *] を選択します。
3. フェデレーテッドユーザのクレデンシャルを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
4. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

PingFederate

1. StorageGRID シングルサインオンページで、サンドボックスモードメッセージの最初のリンクを選択します。

   一度に 1 つのリンクを選択してテストします。

   Sandbox mode

   Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

   1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
   2. Test SSO and SLO by selecting the link for each Admin Node:
      - https:// /idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69
      - https:// /idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73
   3. StorageGRID displays a success or error message for each test.

   When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. フェデレーテッドユーザのクレデンシャルを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
3. 次のリンクを選択して、グリッド内の各管理ノードの SSO 接続を確認します。

   「ページの有効期限が切れました」というメッセージが表示された場合は、ブラウザで「 * 戻る * 」ボタンを選択し、クレデンシャルを再送信してください。

シングルサインオンを有効にします

SSO を使用して各管理ノードにサインインできることを確認したら、 StorageGRID システム全体で SSO を有効にできます。

> SSO が有効になっている場合は、すべてのユーザが SSO を使用して Grid Manager 、テナントマネージャ、グリッド管理 API 、およびテナント管理 API にアクセスする必要があります。ローカルユーザは StorageGRID にアクセスできなくなります。

1. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
2. SSO ステータスを * Enabled * に変更します。
3. [保存（ Save ）] を選択します。
4. 警告メッセージを確認し、「 * OK 」を選択します。

   シングルサインオンが有効になりました。

> Azure ポータルを使用しており、 Azure へのアクセスに使用するコンピュータから StorageGRID にアクセスする場合は、 Azure ポータルユーザが StorageGRID ユーザとしても許可されている（フェデレーテッドグループ内のユーザが StorageGRID にインポートされている）ことを確認してください。 または、 StorageGRID にサインインする前に Azure Portal からログアウトします。

AD FS に証明書利用者信頼を作成します

Active Directory フェデレーションサービス（ AD FS ）を使用して、システム内の管理ノードごとに証明書利用者信頼を作成する必要があります。PowerShell コマンドを使用するか、 StorageGRID から SAML メタデータをインポートするか、またはデータを手動で入力することによって、証明書利用者信頼を作成できます。

必要なもの

- StorageGRID のシングルサインオンを設定し、 SSO タイプとして **AD FS** を選択しました。
- * Grid Manager のシングルサインオンページでサンドボックスモード * が選択されています。を参照してください サンドボックスモードを使用する。
- システム内の各管理ノードの完全修飾ドメイン名（または IP アドレス）と証明書利用者 ID を確認しておきます。これらの値は、 StorageGRID のシングルサインオンページの管理ノード詳細テーブルにあります。

> 証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。
- 証明書利用者信頼を手動で作成する場合は、 StorageGRID 管理インターフェイス用にカスタム証明書をアップロードするか、コマンドシェルから管理ノードにログインする方法を確認しておきます。

このタスクについて

以下の手順は、 Windows Server 2016 AD FS に該当します。別のバージョンの AD FS を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

Windows PowerShell を使用して証明書利用者信頼を作成します

Windows PowerShell を使用して証明書利用者信頼を簡単に作成できます。

手順

1. Windows のスタートメニューから PowerShell アイコンを右クリックし、 * 管理者として実行 * を選択します。
2. PowerShell コマンドプロンプトで、次のコマンドを入力します。

   「 Add-AdfsRelifyPartyTrust - 名前」 Admin_Node_Identifier 」 -MetadataURL "<a href="https://Admin_Node_FQDN/api/saml-metadata"`" class="bare">https://<em>Admin_Node_FQDN</em>/api/saml-metadata"`

   - 「 *Admin_Node_Identifier* 」には、管理ノードの証明書利用者識別子を入力します。これは、 Single Sign-On ページに表示されるとおりです。たとえば 'SG-DC1-ADM1' と入力します
   - 「 *Admin_Node_FQDN*` 」には、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。
3. Windows Server Manager で、 * Tools * > * AD FS Management * を選択します。

   AD FS 管理ツールが表示されます。
4. 「 * AD FS * > * 証明書利用者信頼」を選択します。

   証明書利用者信頼のリストが表示されます。
5. 新しく作成した証明書利用者信頼にアクセス制御ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 * アクセス制御ポリシーの編集 * を選択します。
   c. アクセス制御ポリシーを選択します。
   d. [* 適用（ Apply ）] を選択し、 [* OK] を選択します
6. 新しく作成した証明書利用者信頼に要求発行ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   c. [* ルールの追加 *] を選択します。
   d. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。
   e. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、 **ObjectGUID to Name ID** と入力します。

f. 属性ストアで、 * Active Directory * を選択します。

g. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。

h. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

i. 「完了」を選択し、「 * OK 」を選択します。

7. メタデータが正常にインポートされたことを確認します。

   a. 証明書利用者信頼を右クリックしてプロパティを開きます。

   b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータがない場合は、フェデレーションメタデータアドレスが正しいことを確認するか、値を手動で入力します。

8. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。

9. 完了したら、 StorageGRID に戻ってすべての証明書利用者信頼をテストし、正しく設定されていることを確認します。を参照してください サンドボックスモードを使用する 手順については、を参照し

フェデレーションメタデータをインポートして、証明書利用者信頼を作成します

各証明書利用者信頼の値をインポートするには、各管理ノードの SAML メタデータにアクセスします。

手順

1. Windows Server Manager で、 * Tools * を選択し、 * AD FS Management * を選択します。

2. Actions （アクション）で、 * Add （証明書利用者信頼の追加） * を選択します。

3. [ようこそ] ページで、 [* クレーム対応 *] を選択し、 [開始 *] を選択します。

4. [* オンラインまたはローカルネットワーク上で公開されている証明書利用者に関するデータをインポートする *] を選択します。

5. * フェデレーションメタデータアドレス（ホスト名または URL ） * に、この管理ノードの SAML メタデータの場所を入力します。

   https://*Admin_Node_FQDN*/api/saml-metadata`

   「 *Admin_Node_FQDN*` 」には、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

6. 証明書利用者信頼の追加ウィザードを実行し、証明書利用者信頼を保存して、ウィザードを閉じます。

   > 表示名を入力するときは、管理ノードの証明書利用者 ID を使用します。これは、 Grid Manager のシングルサインオンページに表示される情報とまったく同じです。たとえば 'SG-DC1-ADM1' と入力します

7. クレームルールを追加します。

   a. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。

b. [* ルールを追加 * （ Add rule * ）] を

c. ［ルールテンプレートの選択］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。

d. ［ルールの設定］ ページで、このルールの表示名を入力します。

たとえば、 **ObjectGUID to Name ID** と入力します。

e. 属性ストアで、 * Active Directory * を選択します。

f. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。

g. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

h. 「完了」を選択し、「 * OK 」を選択します。

8. メタデータが正常にインポートされたことを確認します。

a. 証明書利用者信頼を右クリックしてプロパティを開きます。

b. [**Endpoints]** 、 **[*Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

メタデータがない場合は、フェデレーションメタデータアドレスが正しいことを確認するか、値を手動で入力します。

9. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。

10. 完了したら、 StorageGRID に戻ってすべての証明書利用者信頼をテストし、正しく設定されていることを確認します。を参照してください サンドボックスモードを使用する 手順については、を参照し

証明書利用者信頼を手動で作成します

証明書利用者信頼のデータをインポートしないことを選択した場合は、値を手動で入力できます。

手順

1. Windows Server Manager で、 * Tools * を選択し、 * AD FS Management * を選択します。

2. Actions （アクション）で、 * Add （証明書利用者信頼の追加） * を選択します。

3. [ようこそ] ページで、 [* クレーム対応 *] を選択し、 [開始 *] を選択します。

4. [* 証明書利用者に関するデータを手動で入力する *] を選択し、 [* 次へ *] を選択します。

5. 証明書利用者信頼の追加ウィザードを実行します。

a. この管理ノードの表示名を入力します。

整合性を確保するために、管理ノードの証明書利用者 ID を使用してください。この ID は、 Grid Manager のシングルサインオンページに表示されます。たとえば 'SG-DC1-ADM1' と入力します

b. オプションのトークン暗号化証明書を設定する手順は省略してください。

c. ［ URL の設定］ ページで、 ［ * SAML 2.0 WebSSO プロトコルのサポートを有効にする * ］ チェックボックスをオンにします。

d. 管理ノードの SAML サービスエンドポイントの URL を入力します。

https://*Admin_Node_FQDN*/api/saml-response`

「 *Admin_Node_FQDN*` 」には、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

e. Configure Identifiers ページで、同じ管理ノードの証明書利用者 ID を指定します。

'_Admin_Node_Identifier

「 *Admin_Node_Identifier* 」には、管理ノードの証明書利用者識別子を入力します。これは、 Single Sign-On ページに表示されるとおりです。たとえば 'SG-DC1-ADM1' と入力します

f. 設定を確認し、証明書利用者信頼を保存して、ウィザードを閉じます。

[クレーム発行ポリシーの編集] ダイアログボックスが表示されます。

> ダイアログボックスが表示されない場合は、信頼を右クリックし、 * クレーム発行ポリシーの編集 * を選択します。

6. ［ クレームルール ］ ウィザードを開始するには、 ［ * ルールの追加 * ］ を選択します。

a. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。

b. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

たとえば、 **ObjectGUID to Name ID** と入力します。

c. 属性ストアで、 * Active Directory * を選択します。

d. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。

e. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

f. 「完了」を選択し、「 * OK 」を選択します。

7. 証明書利用者信頼を右クリックしてプロパティを開きます。

8. [* Endpoints] タブで、シングルログアウト（ SLO ）のエンドポイントを設定します。

a. 「 * SAML を追加」を選択します。

b. [* Endpoint Type*>*SAML Logout*] を選択します。

c. 「 * Binding * > * Redirect * 」を選択します。

d. [**Trusted URL**] フィールドに、この管理ノードからのシングルログアウト（ SLO ）に使用する URL を入力します。

https://*Admin_Node_FQDN*/api/saml-logout`

「 *Admin_Node_FQDN*` 」には、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

a. 「 * OK 」を選択します。

9. [* Signature*] タブで、この証明書利用者信頼の署名証明書を指定します。

   a. カスタム証明書を追加します。

      - StorageGRID にアップロードしたカスタム管理証明書がある場合は、その証明書を選択します。
      - カスタム証明書がない場合は、管理ノードにログインし、管理ノードの /var/local/mgmt-api ディレクトリに移動して、「 custom-server.crt 」証明書ファイルを追加します。
        - 注意： * 管理ノードのデフォルト証明書 (server.crt') の使用はお勧めしません。管理ノードで障害が発生した場合、ノードをリカバリする際にデフォルトの証明書が再生成されるため、証明書利用者信頼を更新する必要があります。

   b. [* 適用（ Apply ）] を選択し、 [* OK] を選択します。

      証明書利用者のプロパティが保存されて閉じられます。

10. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。

11. 完了したら、 StorageGRID に戻ってすべての証明書利用者信頼をテストし、正しく設定されていることを確認します。を参照してください サンドボックスモードを使用する 手順については、を参照し

Azure AD でエンタープライズアプリケーションを作成

Azure AD を使用して、システム内の管理ノードごとにエンタープライズアプリケーションを作成します。

必要なもの

- StorageGRID 用のシングルサインオンの設定を開始し、 SSO タイプとして「 * Azure* 」を選択しました。
- * Grid Manager のシングルサインオンページでサンドボックスモード * が選択されています。を参照してください サンドボックスモードを使用する。
- システム内の管理ノードごとに * Enterprise アプリケーション名 * を用意しておきます。これらの値は、StorageGRID のシングルサインオンページの管理ノードの詳細テーブルからコピーできます。

> StorageGRID システムで管理ノードごとにエンタープライズアプリケーションを作成する必要があります。管理ノードごとにエンタープライズアプリケーションを用意することで、ユーザはどの管理ノードに対しても安全にサインイン / サインアウトすることができます。

- Azure Active Directory でエンタープライズアプリケーションを作成した経験がある。
- アクティブなサブスクリプションを持つ Azure アカウントが必要です。
- Azure アカウントに、グローバル管理者、クラウドアプリケーション管理者、アプリケーション管理者、サービスプリンシパルの所有者のいずれかのロールが割り当てられている。

Azure AD にアクセスします

1. にログインします "Azure ポータル"。
2. に移動します "Azure Active Directory の略"。

3. 選択するオプション "エンタープライズアプリケーション"。

エンタープライズアプリケーションを作成し、 **StorageGRID SSO** 設定を保存します

Azure の SSO 設定を StorageGRID に保存するには、 Azure を使用して管理ノードごとにエンタープライズアプリケーションを作成する必要があります。フェデレーションメタデータの URL を Azure からコピーし、 StorageGRID のシングルサインオンページの対応する * フェデレーションメタデータの URL * フィールドに貼り付けます。

1. 管理ノードごとに次の手順を繰り返します。
   a. Azure Enterprise アプリケーションペインで、 * 新規アプリケーション * を選択します。
   b. 「 * 独自のアプリケーションを作成する * 」を選択します。
   c. 名前には、 StorageGRID のシングルサインオンページの管理ノード詳細テーブルからコピーした * エンタープライズアプリケーション名 * を入力します。
   d. ギャラリー (ギャラリー以外) で見つからない他のアプリケーションを統合 * ラジオボタンを選択したままにします。
   e. 「 * Create * 」を選択します。
   f. 2 の * Get started * リンクを選択します。シングルサインオン * ボックスを設定するか、左マージンの * シングルサインオン * リンクを選択します。
   g. [* SAML *] ボックスを選択します。
   h. 「 * アプリフェデレーションメタデータ URL * 」をコピーします。この URL は「 * ステップ 3 SAML 署名証明書 * 」にあります。
   i. StorageGRID シングルサインオンページに移動し、使用した * エンタープライズアプリケーション名 * に対応する * フェデレーションメタデータ URL* フィールドに URL を貼り付けます。
2. 各管理ノードのフェデレーションメタデータ URL を貼り付け、 SSO 設定に必要なその他の変更をすべて行ったら、 StorageGRID のシングルサインオンページで「 * 保存」を選択します。

管理ノードごとに **SAML** メタデータをダウンロードします

SSO 設定を保存したら、 StorageGRID システム内の管理ノードごとに SAML メタデータファイルをダウンロードできます。

管理ノードごとに上記の手順を繰り返します。

1. 管理ノードから StorageGRID にサインインします。
2. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
3. ボタンを選択して、その管理ノードの SAML メタデータをダウンロードします。
4. Azure AD にアップロードするファイルを保存します。

SAML メタデータを各エンタープライズアプリケーションにアップロードする

StorageGRID 管理ノードごとに SAML メタデータファイルをダウンロードしたら、 Azure AD で次の手順を実行します。

1. Azure ポータルに戻ります。

2. エンタープライズアプリケーションごとに、次の手順を繰り返します。

> 以前にリストに追加したアプリケーションを表示するには、 [エンタープライズアプリケーション] ページの更新が必要な場合があります。

   a. エンタープライズアプリケーションのプロパティページに移動します。
   b. [Assignment Required*] を [**No**] に設定します（個別に割り当てを設定する場合を除く）。
   c. シングルサインオンページに移動します。
   d. SAML の設定を完了します。
   e. メタデータファイルのアップロードボタンを選択し、対応する管理ノード用にダウンロードした SAML メタデータファイルを選択します。
   f. ファイルがロードされたら、「 * 保存」を選択し、「 * X * 」を選択してパネルを閉じます。SAML を使用してシングルサインオンを設定するページに戻ります。

3. の手順に従います サンドボックスモードを使用する 各アプリケーションをテストします。

PingFederate でサービスプロバイダ（ SP ）接続を作成します

PingFederate を使用して、システム内の管理ノードごとにサービスプロバイダ（ SP ）接続を作成します。処理時間を短縮するために、 StorageGRID から SAML メタデータをインポートします。

必要なもの

- StorageGRID にシングルサインオンを設定し、 SSO タイプとして「 Ping federate * 」を選択しました。
- * Grid Manager のシングルサインオンページでサンドボックスモード * が選択されています。を参照してください サンドボックスモードを使用する。
- システム内の管理ノードごとに * SP 接続 ID * を用意しておきます。これらの値は、 StorageGRID のシングルサインオンページの管理ノード詳細テーブルにあります。
- システムの管理ノードごとに * SAML メタデータ * をダウンロードしておきます。
- PingFederate サーバーで SP 接続を作成した経験があります。
- を使用することができますhttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["管理者向けリファレンスガイド"^] PingFederate サーバー用。PingFederate ドキュメントでは、詳細な手順と説明を説明しています。
- PingFederate サーバーの管理者権限があります。

このタスクについて

ここでは、 StorageGRID の SSO プロバイダとして PingFederate Server バージョン 10.3 を設定する方法を簡単に説明します。別のバージョンの PingFederate を使用している場合は、これらの指示を適用する必要があります。ご使用のリリースの詳細な手順については、 PingFederate Server のマニュアルを参照してください。

PingFederate の前提条件を完了します

StorageGRID に使用する SP 接続を作成する前に、 PingFederate で前提条件のタスクを完了する必要があります。SP 接続を設定するときは、これらの前提条件の情報を使用します。

データストアの作成[[data-store]

まだ作成していない場合は、 PingFederate を AD FS LDAP サーバーに接続するデータストアを作成します。使用した値は、のときに使用したものです アイデンティティフェデレーションの設定 StorageGRID の場合。

- * タイプ * ：ディレクトリ（ LDAP ）
- * LDAP タイプ * ： Active Directory
- * バイナリ属性名 *: 「 LDAP バイナリ属性」タブに * objectGUID * を正確に入力します。

パスワードクレデンシャルバリデータの作成

パスワード認証情報バリデータをまだ作成していない場合は、作成します。

- * 「 * 」と入力します。 LDAP ユーザ名パスワード資格情報検証ツール
- * データストア *: 作成したデータストアを選択します。
- * 検索ベース * ： LDAP から情報を入力します（例： DC=SAML 、 DC=sgws ）。
- * 検索フィルタ * ： sAMAccountName = $ ｛ userName ｝
- * スコープ * ：サブツリー

IdPアダプタインスタンス**[**アダプタインスタンス**]**を作成します

IdP アダプタのインスタンスをまだ作成していない場合は作成します。

1. 「 * 認証 * > * 統合 * > * IdP アダプタ * 」に移動します。
2. [新規インスタンスの作成（ Create New Instance ）] を選択します
3. [タイプ] タブで、 [* HTML フォーム IdP アダプタ *] を選択します。
4. [IdP アダプタ] タブで、 [資格情報検証ツール] に新しい行を追加する *] を選択します。
5. を選択します パスワードクレデンシャルバリデータ を作成しました。
6. [アダプタの属性] タブで、 **pseudonym** * の ***username** 属性を選択します。
7. [保存（ Save ）] を選択します。

署名証明書の作成またはインポート**[signing-certificate]**

署名証明書を作成またはインポートしていない場合は、作成します。

1. 「 * Security * > * Signing & Decryption keys & Certificates * 」に移動します。
2. 署名証明書を作成またはインポートします。

PingFederate で **SP** 接続を作成します

PingFederate で SP 接続を作成すると、管理ノード用に StorageGRID からダウンロードした SAML メタデータがインポートされます。メタデータファイルには、必要な値の多くが含まれています。

ユーザが任意のノードに対して安全にサインインおよびサインアウトできるように、StorageGRID システム内の管理ノードごとに SP 接続を作成する必要があります。次の手順に従って、最初の SP 接続を作成します。次に、に進みます 追加の SP 接続を作成します 追加の接続を作成するには、次の手順を実行します。

SP 接続タイプを選択します

1. [* アプリケーション * > * 統合 * > * SP 接続 *] に移動します。
2. [接続の作成 *] を選択します。
3. 「 * この接続にテンプレートを使用しない * 」を選択します。
4. ブラウザ SSO プロファイル * および * SAML 2.0 * をプロトコルとして選択します。

SP メタデータをインポートします

1. メタデータのインポートタブで、 * ファイル * を選択します。
2. 管理ノードの StorageGRID シングルサインオンページからダウンロードした SAML メタデータファイルを選択します。
3. メタデータの概要と [一般情報] タブの情報を確認します。

   パートナーのエンティティ ID と接続名は、 StorageGRID SP 接続 ID に設定されています。（例：10.96.105.200-DC1-ADM1-105-200 ）。ベース URL は、 StorageGRID 管理ノードの IP です。

4. 「 * 次へ * 」を選択します。

IdP ブラウザの **SSO** を設定する

1. ブラウザ SSO タブで、 * ブラウザ SSO の設定 * を選択します。
2. SAML プロファイルタブで、 * SP が開始した SSO * 、 * SP - 初期 SLO * 、 * IdP が開始した SSO * 、および * IdP によって開始された SLO * オプションを選択します。
3. 「 * 次へ * 」を選択します。
4. [Assertion Lifetime （アサーションの有効期間）] タブで、変更を行いません。
5. [アサーションの作成] タブで、 [* アサーションの作成の設定 *] を選択します。
   a. [ID マッピング] タブで、 [* 標準 *] を選択します。
   b. [属性契約（ Attribute Contract ）] タブで、属性契約として * sama_subject * を使用し、インポートされた名前形式を指定しません。
6. 契約を延長するには **'Delete** を選択して 'urn:oid' を削除しますが ' これは使用されません

アダプタインスタンスをマッピングします

1. [Authentication Source Mapping] タブで、 [* Map New Adapter Instance] を選択します。
2. [アダプタインスタンス] タブで、を選択します アダプタインスタンス を作成しました。
3. [マッピング方法] タブで、 [データストアから追加属性を取得する *] を選択します。
4. [属性ソースとユーザールックアップ] タブで、 [属性ソースの追加] を選択します。

5. [データストア] タブで、概要 を入力し、を選択します データストア を追加しました。
6. LDAP ディレクトリ検索タブで、次の手順を実行します。
   - 「 * ベース DN * 」を入力します。この DN は、 LDAP サーバの StorageGRID で入力した値と完全に一致している必要があります。
   - 検索範囲（ Search Scope ）で、 * サブツリー * （ * Subtree * ）を選択します。
   - ルートオブジェクトクラスの場合は、 * objectGUID * 属性を検索して追加します。
7. [LDAP Binary Attribute Encoding Types] タブで、 *objectGUID * 属性として *Base64 * を選択します。
8. LDAP Filter タブで、 * sAMAccountName = $ ｛ userName ｝ * と入力します。
9. [属性契約履行] タブで、 [ソース] ドロップダウンから [**LDAP(** 属性 **)**] を選択し、 [値] ドロップダウンから [**objectGUID**] を選択します。
10. 属性ソースを確認して保存します。
11. Failsave Attribute Source タブで、 * Abort the SSO Transaction * を選択します。
12. 概要を確認し、「 * Done * 」を選択します。
13. 「 Done （完了）」を選択します。

プロトコルを設定します

1. * SP Connection * > * Browser SSO * > * Protocol Settings * タブで、 * Configure Protocol Settings * を選択します。
2. [Assertion Consumer Service URL] タブで、 StorageGRID SAML メタデータからインポートされたデフォルト値（バインドの場合は * POST * 、エンドポイント URL の場合は「 /api/saml-response 」）を受け入れます。
3. [SLO Service URL] タブで、 StorageGRID SAML メタデータからインポートされたデフォルト値（バインドの場合は *redirect * 、エンドポイント URL の場合は「 /api/saml-logout 」）を受け入れます。
4. [Allowable SAML Binding] タブで、 [**Artifact**] と [**SOAP**] の選択を解除します。必要なのは、 * POST * および * redirect * のみです。
5. [Signature Policy] タブで、 [**Require Authn Requests to be signed**] および [*Always Sign Assertion *] チェックボックスをオンのままにします。
6. ［ 暗号化ポリシー ］ タブで、 ［ * なし * ］ を選択します。
7. 概要を確認し、「 * Done * 」を選択してプロトコル設定を保存します。
8. 概要を確認し、「完了」を選択して、ブラウザ SSO 設定を保存します。

クレデンシャルを設定

1. ［ SP 接続 ］ タブで ' ［ * 資格情報 * ］ を選択します
2. 資格情報タブで、 * 資格情報の設定 * を選択します。
3. を選択します 署名証明書 を作成またはインポートしました。
4. 「 * 次へ * 」を選択して、「 * 署名検証設定の管理 * 」に移動します。
   a. [信頼モデル] タブで、 [*Unanchored] を選択します。
   b. [Signature Verification Certificate] タブで、 StorageGRID SAML メタデータからインポートした署名証

明書情報を確認します。

5. 概要画面を確認し、 ［ * 保存 * ］ を選択して SP 接続を保存します。

追加の **SP** 接続を作成します

最初の SP 接続をコピーして、グリッド内の管理ノードごとに必要な SP 接続を作成できます。コピーごとに新しいメタデータをアップロードします。

> 異なる管理ノードの SP 接続では、パートナーのエンティティ ID 、ベース URL 、接続 ID 、接続名、署名の検証を除き、同じ設定を使用します。 と SLO 応答 URL 。

1. * Action * > * Copy * を選択して、追加の管理ノードごとに最初の SP 接続のコピーを作成します。
2. コピーの接続 ID と接続名を入力し、 * 保存 * を選択します。
3. 管理ノードに対応するメタデータファイルを選択します。
   a. 「 * アクション * > * メタデータで更新 * 」を選択します。
   b. 「 * ファイルを選択」を選択し、メタデータをアップロードします。
   c. 「 * 次へ * 」を選択します。
   d. [保存（ Save ）] を選択します。
4. 未使用の属性によるエラーを解決します。
   a. 新しい接続を選択します。
   b. ブラウザ SSO の設定 > アサーションの作成の設定 > 属性契約 * を選択します。
   c. urn ： Oid * のエントリを削除します。
   d. [保存（ Save ）] を選択します。

シングルサインオンを無効にします

不要になった場合はシングルサインオン（ SSO ）を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場合は、事前にシングルサインオンを無効にする必要があります。

必要なもの

- を使用して Grid Manager にサインインします 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。

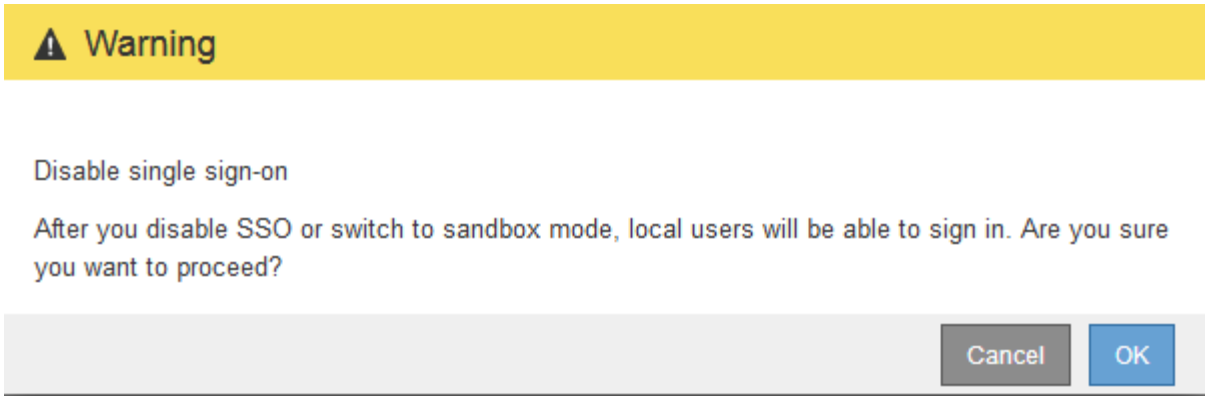
手順

1. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。

   [Single Sign-On] ページが表示されます。

2. [* Disabled * （無効 * ）] オプションを選択します。
3. [保存（ Save ）] を選択します。

   ローカルユーザがサインインできるようになったことを示す警告メッセージが表示されます。



4. 「 * OK 」を選択します。

   次回 StorageGRID にサインインすると、 StorageGRID のサインインページが表示され、ローカルユーザまたはフェデレーテッド StorageGRID ユーザのユーザ名とパスワードを入力する必要があります。

1 つの管理ノードのシングルサインオンを一時的に無効にしてから再度有効にする

シングルサインオン（ SSO ）システムが停止すると、 Grid Manager にサインインできない場合があります。この場合は、 1 つの管理ノードに対して SSO を一時的に無効にしてから再度有効にすることができます。SSO を無効にしてから再度有効にするには、ノードのコマンドシェルにアクセスする必要があります。

必要なもの

- 特定のアクセス権限が必要です。
- 「 passwords.txt 」ファイルがあります。
- ローカルの root ユーザのパスワードを確認しておきます。

このタスクについて

1 つの管理ノードに対して SSO を無効にすると、ローカルの root ユーザとして Grid Manager にサインインできます。StorageGRID システムを保護するために、ノードのコマンドシェルを使用してサインアウト後すぐに管理ノードの SSO を再度有効にする必要があります。

> 1 つの管理ノードに対して SSO を無効にしても、グリッド内の他の管理ノードの SSO 設定には影響しません。Grid Manager のシングルサインオンページの * SSO * を有効にするチェックボックスはオンのままで、既存の SSO 設定はすべて更新しないかぎり維持されます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 ssh admin@Admin_Node_ip'
   b. 「 passwords.txt 」ファイルに記載されたパスワードを入力します。
   c. root に切り替えるには、次のコマンドを入力します
   d. 「 passwords.txt 」ファイルに記載されたパスワードを入力します。

      root としてログインすると、プロンプトは「 $` 」から「 #」 に変わります。

2. 次のコマンドを実行します :`disable-saml``

   環境 this admin Node only コマンドのメッセージが表示されます。

3. SSO を無効にすることを確認します。

   ノードでシングルサインオンが無効になったことを示すメッセージが表示されます。

4. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。

   SSO を無効にしたため、 Grid Manager のサインインページが表示されます。

5. ユーザ名「 root 」とローカルの root ユーザのパスワードを使用してサインインします。
6. SSO 設定の修正が必要なために SSO を一時的に無効にした場合は、次の手順を実行します
   a. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
   b. 正しくない SSO 設定または古い SSO 設定を変更します。
   c. [保存（ Save ）] を選択します。

      シングルサインオンページから * Save * を選択すると、グリッド全体で SSO が自動的に再有効化されます。

7. 他の理由で Grid Manager へのアクセスが必要であったために SSO を一時的に無効にした場合は、次の手順を実行します。

   a. 必要なタスクを実行します。
   b. 「サインアウト」を選択して Grid Manager を閉じます。
   c. 管理ノードで SSO を再度有効にします。次のいずれかの手順を実行します。

      - 次のコマンドを実行します :'enable-saml

        環境 this admin Node only コマンドのメッセージが表示されます。

      SSO を有効にすることを確認します。

   ノードでシングルサインオンが有効になったことを示すメッセージが表示されます。

   - Grid ノードを再起動します
8. Web ブラウザから、同じ管理ノードから Grid Manager にアクセスする。
9. StorageGRID のサインインページが表示され、グリッドマネージャにアクセスするには SSO クレデンシャルを入力する必要があることを確認します。