シングルサインオン（SSO）を使用

StorageGRID 11.8

NetApp
May 17, 2024

目次

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

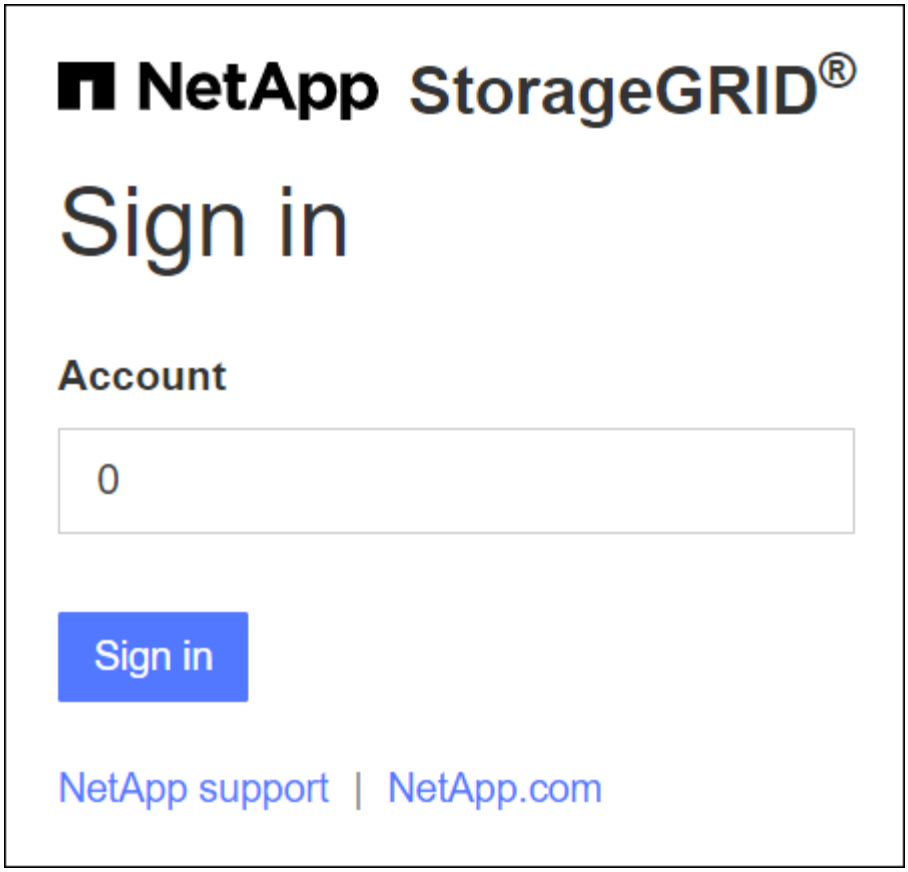
SSO が有効な場合に StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。

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。

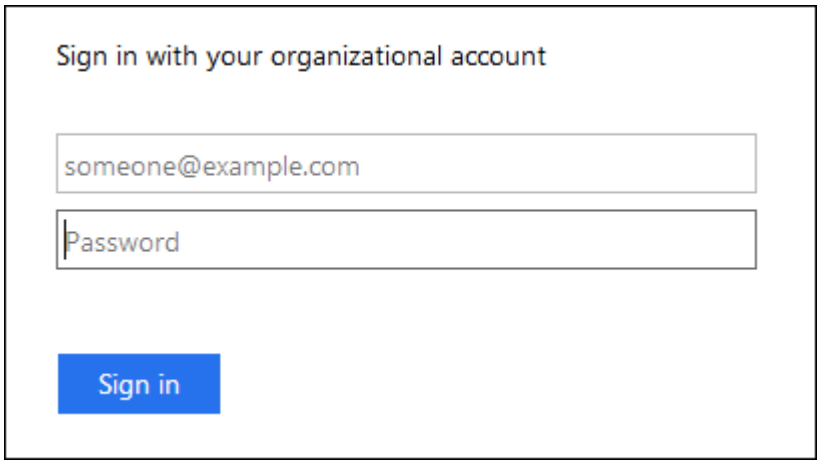


- Grid Manager または Tenant Manager に以前にアクセスしていた場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。

> 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アドレスのあとにを追加したもの）を入力すると、StorageGRID のサインインページは表示されません `/?accountId=20-digit-account-id`）。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[サインアウト]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要件と考慮事項

StorageGRID システムでシングルサインオン（SSO）を有効にする前に、要件と考慮事項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。

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

Azureに関する考慮事項

SSOタイプとしてAzureを使用し、ユーザがsAMAccountNameをプレフィックスとして使用しないユーザプリンシパル名を持っている場合、StorageGRID がLDAPサーバとの接続を失うと、ログインの問題が発生する可能性があります。ユーザがサインインできるようにするには、LDAPサーバへの接続を復元する必要があります。

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てに移動します `/var/local/mgmt-api` ディレクトリ。カスタムサーバ証明書の名前はです `custom-server.crt`。ノードのデフォルトサーバ証明書の名前はです `server.crt`。

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 "外部ファイアウォールでアクセスを制御します"。

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。

作業を開始する前に

- 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"。
- これで完了です "特定のアクセス権限"。
- 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選択されていないことを確認します。
   d. 該当する場合は、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たことを確認し、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。

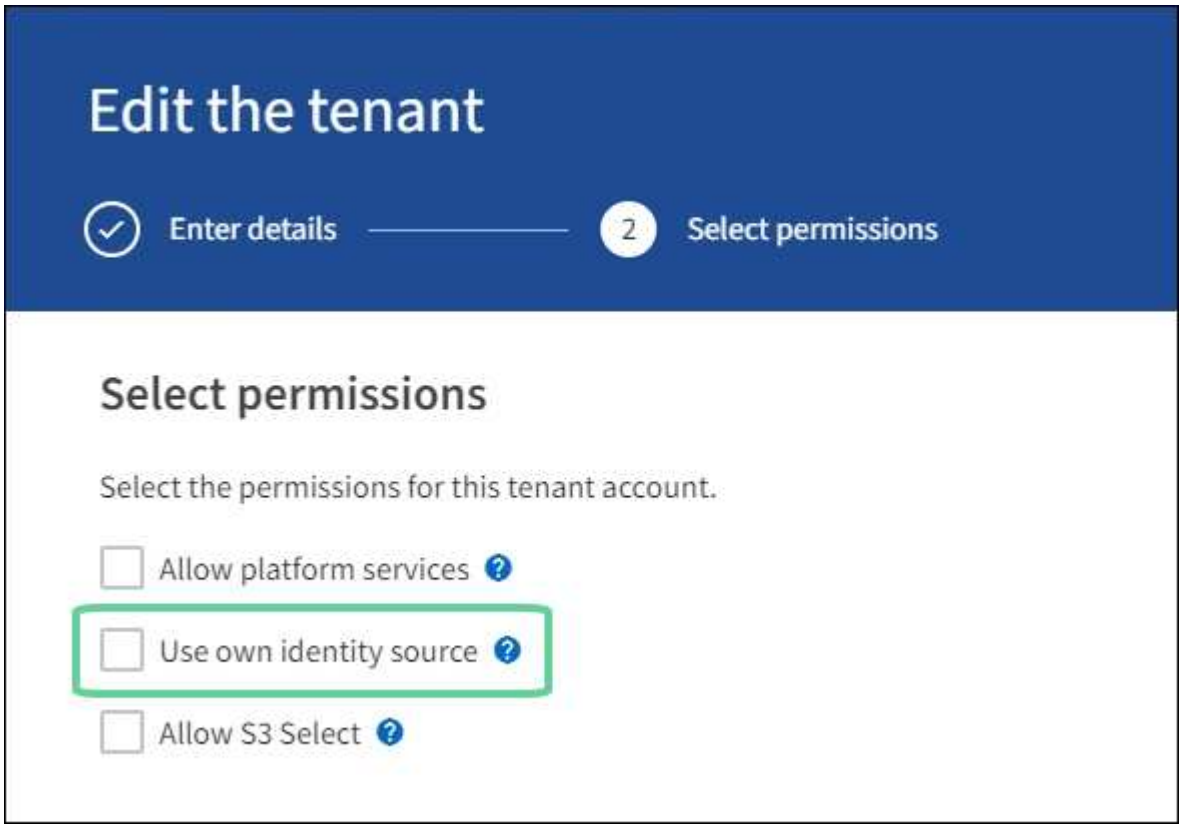
3. 既存のテナントアカウントがある場合は、次の手順を実行して、 Root アクセス権限を持つフェデレーテッドユーザがサインインできることを確認します。

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. 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[Save]*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要件と考慮事項"
- "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。

作業を開始する前に

- 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"。
- を使用することができます "rootアクセス権限"。
- 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。

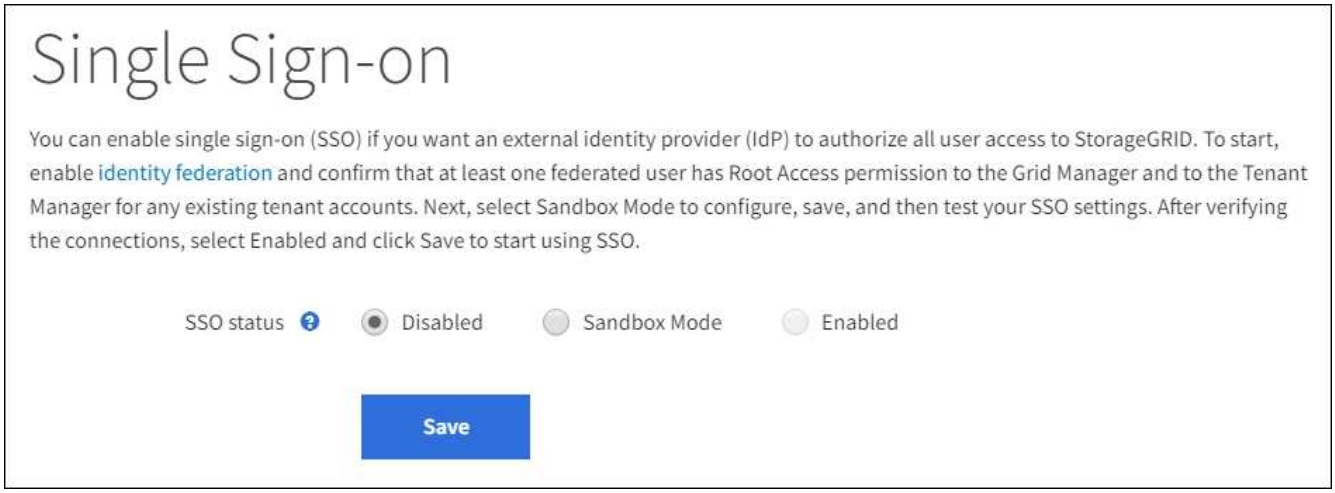
サンドボックスモードでは、 SSO を有効にする前に、この手順を簡単に実行し、すべての設定をテストできます。サンドボックスモードを使用している場合、ユーザはSSOを使用してサインインできません。

サンドボックスモードにアクセスします

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、 [**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をフェデレーテッドアイデンティティソースとして設定し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要件と考慮事項"。

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

手順

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。

     > CA証明書をすぐに変更する場合は、 "管理ノードでmgmt-apiサービスを再起動します。" Grid ManagerへのSSOが成功するかどうかをテストします。

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、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。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。

> CA証明書をすぐに変更する場合は、 "管理ノードでmgmt-apiサービスを再起動します。" Grid ManagerへのSSOが成功するかどうかをテストします。

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、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。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。

> CA証明書をすぐに変更する場合は、 "管理ノードでmgmt-apiサービスを再起動します。" Grid ManagerへのSSOが成功するかどうかをテストします。

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、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。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

手順

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

手順

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

手順

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

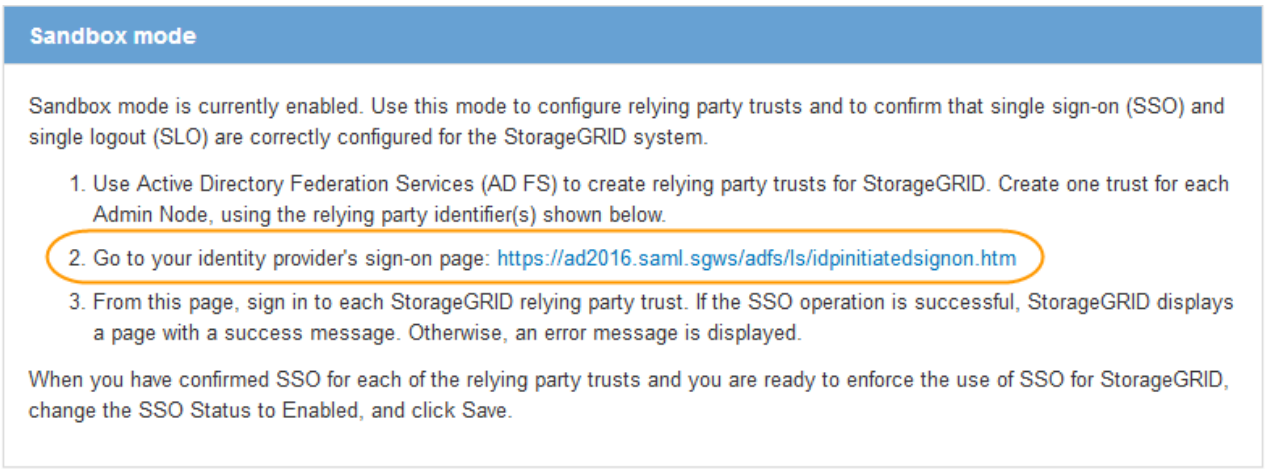
ングルログアウトが正しく設定されていることを確認する必要があります。

Active Directory

手順

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。

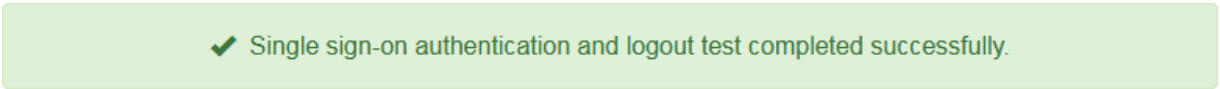
   

2. リンクを選択するか、 URL をコピーしてブラウザに貼り付け、アイデンティティプロバイダのサインオンページにアクセスします。

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

手順

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.

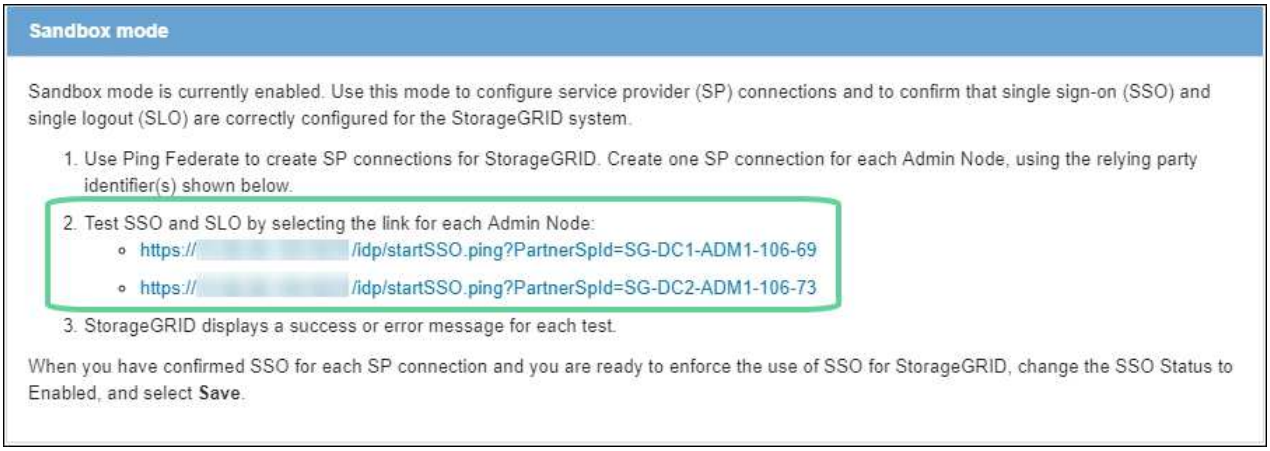
   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
4. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

PingFederate

手順

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。

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。

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。
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。

作業を開始する前に

- 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 "https://Admin_Node_FQDN/api/saml-metadata"

   - の場合 `Admin_Node_Identifier`では、管理ノードの証明書利用者`ID`を`Single Sign-On`ページに表示されるとおりに入力します。例： `SG-DC1-ADM1`。
   - の場合 `Admin_Node_FQDN`をクリックし、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*または* UPN to Name ID*などです。

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 」と入力するか、[ユーザープリンシパル名]* を選択します。

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。

      メタデータが見つからない場合は、フェデレーションメタデータの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
   ```

   の場合 `*Admin_Node_FQDN*` をクリックし、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。例： `SG-DC1-ADM1`。

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*または* UPN to Name ID*などです。

   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 」と入力するか、[ユーザープリンシパル名]* を選択します。
   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。

      メタデータが見つからない場合は、フェデレーションメタデータの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。例： `SG-DC1-ADM1`。

   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`

      の場合 `*Admin_Node_FQDN*` で、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`

      の場合 `Admin_Node_Identifier` では、管理ノードの証明書利用者`ID`を`Single Sign-On`ページに表示されるとおりに入力します。例： `SG-DC1-ADM1`。

   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*または* UPN to Name ID*などです。

   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 」と入力するか、[ユーザープリンシパル名]*を選択します。

   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
```

の場合 `*Admin_Node_FQDN*` をクリックし、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てに移動します `/var/local/mgmt-api` 管理ノードのディレクトリにを追加します `custom-server.crt` 証明書ファイル。

        *注：*管理ノードのデフォルト証明書を使用 (`server.crt`）は推奨されません。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。

作業を開始する前に

- 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

手順

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。

手順

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。

手順

1. 管理ノードごとに上記の手順を繰り返します。
   a. 管理ノードから StorageGRID 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. 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。
   d. 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。

手順

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。

作業を開始する前に

- 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 "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。
- を使用することができます "管理者権限" PingFederate サーバー用。

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。

手順

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。

手順

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

手順

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

手順

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. [Metadata Summary]と[General Info]タブに表示される情報を確認します。

   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

手順

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. [Extend the Contract]で、*[Delete]*を選択してを削除します `urn:oid`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

手順

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]で、*objectGUID*または*userPrincipalName*のいずれかの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. [Attribute Contract Fulfillment]タブで、[Source]ドロップダウンから*を選択し、**[Value]**ドロップダウンから objectGUID または userPrincipalName *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

手順

1. * SP Connection * > * Browser SSO * > * Protocol Settings * タブで、 * Configure Protocol Settings * を選択します。
2. [アサーションコンシューマサービス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を受け入れます（バインドおよびの場合は* POST *） `/api/saml-response` （エンドポイントURLの場合）。
3. [SLOサービスURLs]タブで、StorageGRID SAMLメタデータ（バインドおよび用の* redirect*）からインポートされたデフォルト値を受け入れます `/api/saml-logout` エンドポイントURLの場合。
4. [Allowable SAML Bindings]タブで、[**artifact**]および[**SOAP**]を選択解除します。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]チェックボックスと[* 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

手順

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 。

手順

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。

作業を開始する前に

- 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"。
- これで完了です "特定のアクセス権限"。

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。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を使用することができます `Passwords.txt` ファイル。
- 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[Single Sign-on]ページの[Enable SSO]*チェックボックスは選択されたままになり、既存のSSO設定は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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
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、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。

  - グリッドノードをリブートします。 `reboot`

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。