シングルサインオン（SSO）を使用する

StorageGRID software

NetApp
December 03, 2025

目次

シングルサインオン（SSO）を使用する

シングルサインオンを構成する

シングル サインオン (SSO) が有効になっている場合、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資格情報が承認されている場合にのみ、ユーザーは Grid Manager、Tenant Manager、Grid Management API、または Tenant Management API にアクセスできます。ローカル ユーザーは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) をサポートしています。

シングル サインオン (SSO) を有効にする前に、SSO が有効になっている場合にStorageGRID のサインインおよびサインアウト プロセスがどのように影響を受けるかを確認してください。

SSO が有効になっているときに**Sign in**

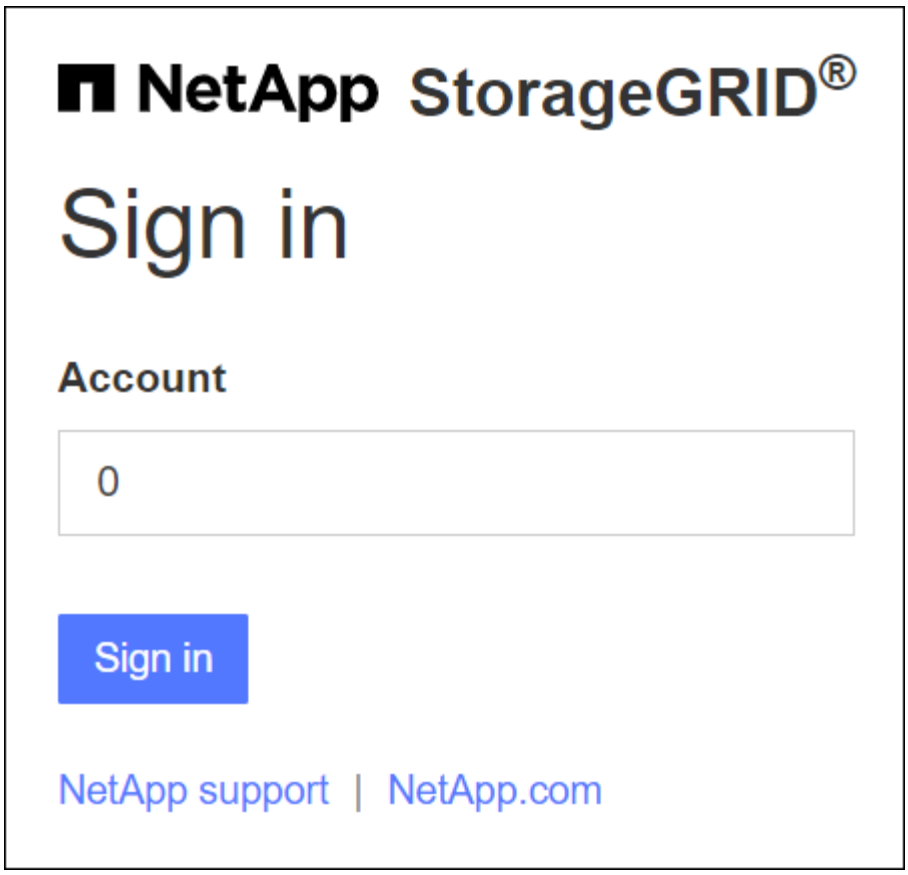
SSO が有効になっているときにStorageGRIDにサインインすると、資格情報を検証するために組織の SSO ページにリダイレクトされます。

手順

1. Web ブラウザに、任意の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。

   StorageGRIDSign inページが表示されます。

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

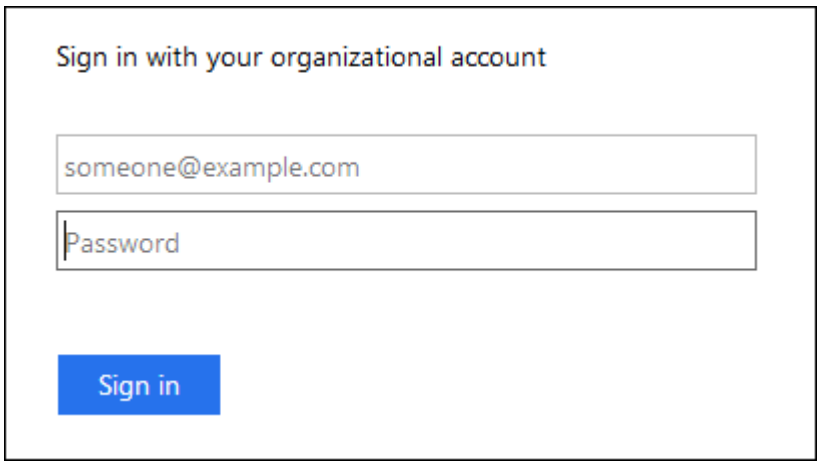


◦ 以前に Grid Manager または Tenant Manager にアクセスしたことがある場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。

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アドレスの後に続く）を入力した場合、 StorageGRIDSign inページは表示されません。 `/?accountId=20-digit-account-id`）。代わりに、組織のSSOサインインページにすぐにリダイレクトされ、SSO認証情報でサインイン 。

2. グリッド マネージャにアクセスするか、テナント マネージャにアクセスするかを指定します。
   - グリッド マネージャーにアクセスするには、アカウント **ID** フィールドを空白のままにするか、アカウント ID として **0** を入力するか、最近のアカウントのリストに グリッド マネージャー が表示されている場合はそれを選択します。
   - テナント マネージャー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. *Sign in*を選択

   StorageGRID は組織の SSO サインイン ページにリダイレクトします。例えば：



4. SSO 資格情報を使用してSign in。

   SSO 資格情報が正しい場合:

   a. アイデンティティ プロバイダー (IdP) は、 StorageGRIDに認証応答を提供します。
   b. StorageGRID は認証応答を検証します。
   c. 応答が有効であり、 StorageGRIDアクセス権限を持つフェデレーション 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 Tenant Manager にサインインします。

   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ション グループに属する既存のユーザーであれば、サインインできます。

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

   SSO 資格情報を再入力する必要はありません。

SSO が有効になっているときにサインアウトする

StorageGRIDで SSO が有効になっている場合、サインアウト時に何が起こるかは、何にサインインしているか、どこからサインアウトしているかによって異なります。

手順

1. ユーザー インターフェースの右上隅にある サインアウト リンクを見つけます。
2. *サインアウト*を選択します。

   StorageGRIDSign inページが表示されます。 最近のアカウント ドロップダウンが更新され、グリッド マネージャー またはテナントの名前が含まれるようになったため、今後はこれらのユーザー インターフェイスにすばやくアクセスできるようになります。

...にサインインしている場合	そしてサインアウトします...	ログアウトしています...
1 つ以上の管理ノード上のグリッド マネージャー	任意の管理ノード上のグリッド マネージャー	すべての管理ノード上のグリッド マネージャー 注: SSO に Azure を使用する場合、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テナント マネージャー	任意の管理ノード上のテナント マネージャー	すべての管理ノード上のテナント マネージャー
グリッドマネージャとテナントマネージャの両方	Grid Manager	グリッド マネージャーのみ。SSO からサインアウトするには、テナント マネージャー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すると何が起こるかをまとめたものです。複数のブラウザ セッションにわたって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 は、次の SSO ID プロバイダー (IdP) をサポートしています。

- アクティブ ディレクトリ フェデレーション サービス (AD FS)
- Azure アクティブ ディレクトリ (Azure AD)

- PingFederate

SSO ID プロバイダーを構成する前に、 StorageGRIDシステムの ID フェデレーションを構成する必要があります。 ID 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。

構成された**LDAP**サービスタイプ	**SSO ID** プロバイダーのオプション
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

AD FSの要件

AD FS の次のいずれかのバージョンを使用できます。

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

Windows Server 2016では、 "KB3201845 アップデート" 、またはそれ以上。

その他の要件

- トランスポート層セキュリティ (TLS) 1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以上

Azureに関する考慮事項

SSO タイプとして Azure を使用し、ユーザーのユーザー プリンシパル名にプレフィックスとして sAMAccountName が使用されていない場合、 StorageGRID がLDAP サーバー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。ユーザーがサインインできるようにするには、LDAP サーバーへの接続を復元する必要があります。

サーバー証明書の要件

デフォルトでは、 StorageGRID は各管理ノードで管理インターフェイス証明書を使用して、グリッド マネージャ、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に対して証明書利用者信頼 (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 プロバイダー接続 (PingFederate) を構成する場合は、サーバー証明書をStorageGRID要求の署名証明書として使用します。

まだお持ちでない場合は"管理インターフェース用のカスタム証明書を構成しました"、今すぐそうすべきです。カスタム サーバ証明書をインストールすると、その証明書はすべての管理ノードに使用され、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接続で使用できるようになります。

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接続で管理ノードのデフォルトのサーバー証明書を使用することはお勧めしません。ノードに障害が発生し、それを回復すると、新しいデフォルトのサーバー証明書が生成されます。回復されたノードにサインインする前に、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ー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。カスタムサーバー証明書の名前は `custom-server.crt`。ノードのデフォルトのサーバー証明書の名前は `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。ユーザーをシングル 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。見る"外部ファイアウォールでアクセスを制御する" 。

フェデレーションユーザー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、既存のテナント アカウントの少なくとも 1 人のフェデレーション ユーザーが Grid Manager と 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。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。
- すでに ID フェデレーションを構成しています。

手順

1. 既存のテナント アカウントがある場合は、いずれのテナントも独自の ID 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、テナント マネージャで構成された ID ソースは、グリッド マネージャで構成された ID 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ーは、Grid Manager アイデンティティ ソースのアカウントを持っていない限り、サインインできなくなります。

   a. 各テナント アカウントのテナント マネージャーにSign in。
   b. アクセス管理 > *アイデンティティ連携*を選択します。
   c. **ID** 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. そうである場合は、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ション 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. フェデレーション ユーザーが Grid Manager にアクセスできることを確認します。
   a. グリッド マネージャーから、構成 > アクセス制御 > 管理者グループ を選択します。
   b. 少なくとも 1 つのフェデレーション グループが Active Directory ID ソースからインポートされ、ルート 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。

d. フェデレーション グループ内のユーザーとして Grid Manager に再度サインインできることを確認します。

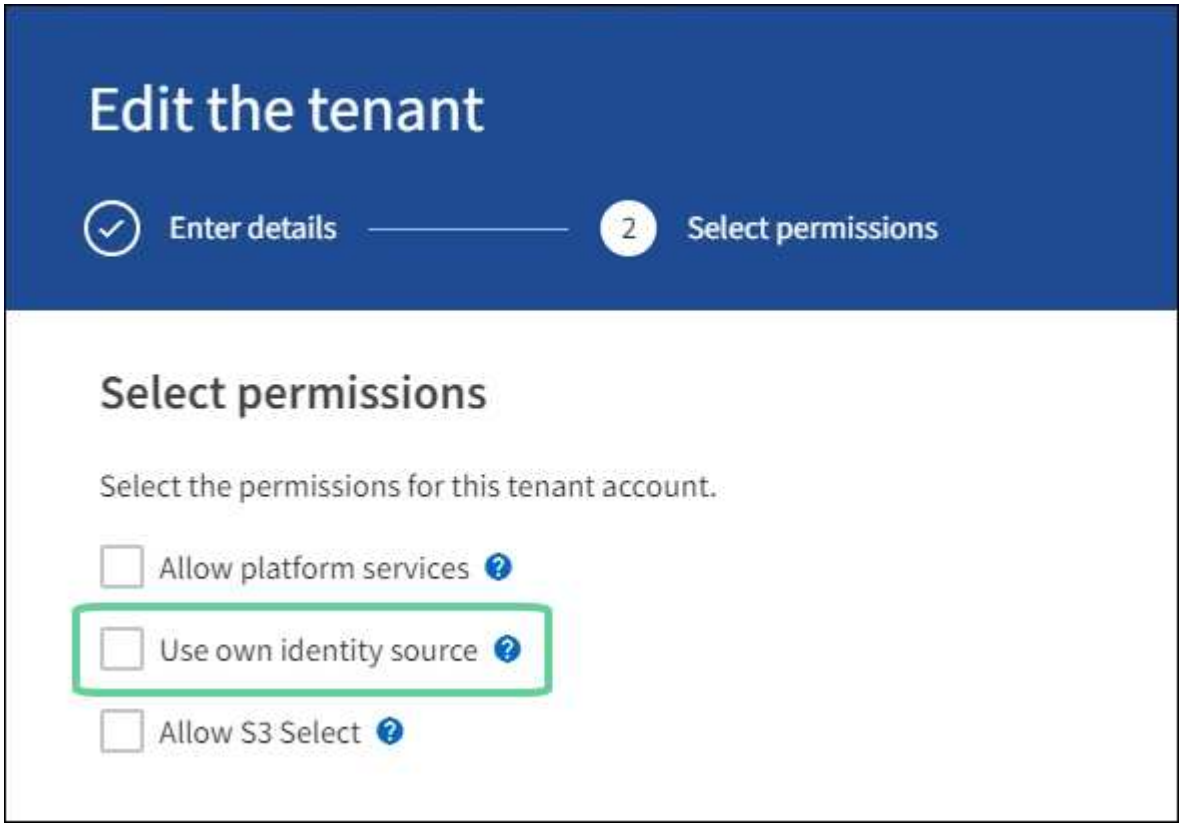
3. 既存のテナント アカウントがある場合は、ルート アクセス権限を持つフェデレーション ユーザーがサインインできることを確認します。

a. グリッド マネージャーから、**TENANTS** を選択します。

b. テナント アカウントを選択し、[アクション] > [編集] を選択します。

c. 詳細入力タブで、[続行] を選択します。

d. 独自の **ID** ソースを使用する チェックボックスが選択されている場合は、チェックボックスをオフにして 保存 を選択します。



テナント ページが表示されます。

a. テナント アカウントを選択し、[**Sign in**] を選択して、ローカル ルート ユーザーとしてテナント アカウントにサインインします。

b. テナント マネージャーから、アクセス管理 > グループ を選択します。

c. グリッド マネージャーからの少なくとも 1 つのフェデレーション グループに、このテナントのルート 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。

e. フェデレーション グループ内のユーザー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"

- "管理者グループの管理"
- "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

すべてのStorageGRIDユーザーに対してシングル サインオン (SSO) を有効にする前に、サンドボックス モードを使用してシングル サインオン (SSO) を構成してテストすることができます。 SSO を有効にした後は、構成を変更または再テストする必要があるときはいつでもサンドボックス モードに戻ることができます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。
- StorageGRIDシステムの ID フェデレーションを構成しました。
- ID フェデレーションの **LDAP** サービス タイプ では、使用する予定の SSO ID プロバイダーに基づいて、Active Directory または Azure のいずれかを選択しました。

構成された**LDAP**サービスタイプ	**SSO ID** プロバイダーのオプション
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

タスク概要

SSO が有効になっていて、ユーザーが管理ノードにサインインしようとすると、 StorageGRID はSSO ID プロバイダーに認証要求を送信します。次に、SSO ID プロバイダーは、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。リクエストが成功した場合:

- Active Directory または PingFederate からの応答には、ユーザーのユニバーサル一意識別子 (UUID) が含まれます。
- Azure からの応答には、ユーザー プリンシパル名 (UPN) が含まれます。

StorageGRID (サービス プロバイダー) と SSO ID プロバイダーがユーザー認証要求について安全に通信できるようにするには、 StorageGRIDで特定の設定を構成する必要があります。次に、SSO ID プロバイダーのソフトウェアを使用して、各管理ノードに対して証明書利用者信頼 (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 プロバイダー (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。

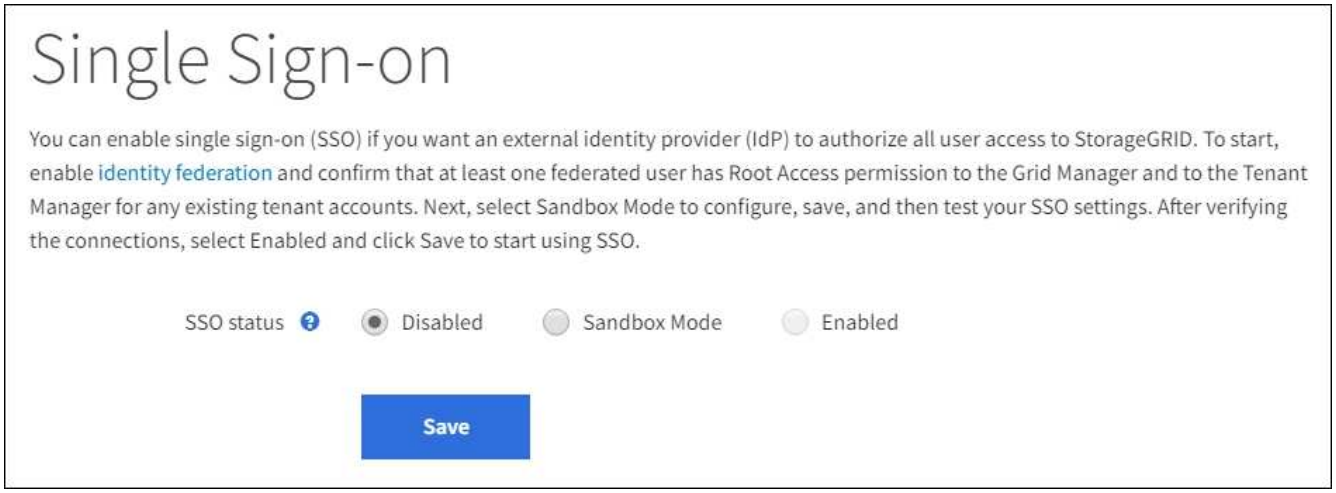
サンドボックス モードを使用すると、この双方向の構成を簡単に実行でき、SSO を有効にする前にすべての設定をテストできます。サンドボックス モードを使用している場合、ユーザーは SSO を使用してサインインできません。

サンドボックスモードにアクセスする

手順

1. 構成 > アクセス制御 > シングル サインオン を選択します。

   *無効*オプションが選択された状態で、シングル サインオン ページが表示されます。



   SSO ステータス オプションが表示されない場合は、ID プロバイダーをフェデレーション ID ソースとして構成していることを確認してください。見る"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。

   アイデンティティプロバイダーセクションが表示されます。

IDプロバイダーの詳細を入力してください

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、アイデンティティ プロバイダー セクションのフィールドに入力します。

Active Directory

a. Active Directory フェデレーション サービス (AD FS) に表示されるとおりに、ID プロバイダーのフェデレーション サービス名 を入力します。

> フェデレーション サービス名を見つけるには、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 サービス名は 2 番目のフィールドに表示されます。

b. アイデンティティ プロバイダーがStorageGRID要求に応答して SSO 構成情報を送信するときに、接続を保護するために使用する TLS 証明書を指定します。

- オペレーティング システムの **CA** 証明書を使用する: 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** 証明書を使用する: 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。

- **TLS** を使用しない: 接続を保護するために TLS 証明書を使用しません。

> CA証明書を変更する場合は、直ちに"管理ノードで mgmt-api サービスを再起動します。"グリッド マネージャーへの SSO が成功するかどうかをテストします。

c. 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 内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、将来的に管理ノードを追加する予定がない場合は、次のように入力します。 `SG`または `StorageGRID`。
- グリッドに複数の管理ノードが含まれている場合は、文字列 `[HOSTNAME]`識別子内。例：`SG-[HOSTNAME]`。これにより、ノードのホスト名に基づいて、システム内の各管理ノードの依存パーティ識別子を示すテーブルが生成されます。

> StorageGRIDシステム内の各管理ノードに対して、証明書利用者信頼を作成する必要があります。各管理ノードに証明書利用者信頼を設定することで、ユーザーはどの管理ノードに対しても安全にサインインおよびサインアウトできるようになります。

d. *保存*を選択します。

*保存*ボタンに緑色のチェックマークが数秒間表示されます。

Azure

a. アイデンティティ プロバイダーがStorageGRID要求に応答して SSO 構成情報を送信するとき

に、接続を保護するために使用する TLS 証明書を指定します。

- オペレーティング システムの **CA** 証明書を使用する: 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** 証明書を使用する: 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。

- **TLS** を使用しない: 接続を保護するために TLS 証明書を使用しません。

> CA証明書を変更する場合は、直ちに"管理ノードで mgmt-api サービスを再起動します。"グリッド マネージャーへの SSO が成功するかどうかをテストします。

b. 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 内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、将来的に管理ノードを追加する予定がない場合は、次のように入力します。 `SG`または `StorageGRID`。
- グリッドに複数の管理ノードが含まれている場合は、文字列 `[HOSTNAME]`識別子内。例：`SG-[HOSTNAME]`。これにより、ノードのホスト名に基づいて、システム内の各管理ノードのエンタープライズ アプリケーション名を表示するテーブルが生成されます。

> StorageGRIDシステム内の各管理ノードに対してエンタープライズ アプリケーションを作成する必要があります。各管理ノード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、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

c. 以下の手順に従ってください"Azure AD でエンタープライズ アプリケーションを作成する"表にリストされている各管理ノードに対してエンタープライズ アプリケーションを作成します。

d. 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 URL をコピーします。次に、この URL をStorageGRIDの対応する **Federation metadata URL** フィールドに貼り付けます。

e. すべての管理ノードのフェデレーション メタデータ URL をコピーして貼り付けたら、[保存] を選択します。

*保存*ボタンに緑色のチェックマークが数秒間表示されます。

PingFederate

a. アイデンティティ プロバイダーがStorageGRID要求に応答して SSO 構成情報を送信するときに、接続を保護するために使用する TLS 証明書を指定します。

- オペレーティング システムの **CA** 証明書を使用する: 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** 証明書を使用する: 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。

- **TLS** を使用しない: 接続を保護するために TLS 証明書を使用しません。

> CA証明書を変更する場合は、直ちに"管理ノードで mgmt-api サービスを再起動します。"グリッド マネージャーへの SSO が成功するかどうかをテストします。

b. サービス プロバイダー (SP) セクションで、 StorageGRIDの * SP接続 ID* を指定します。この値は、PingFederate 内の各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、将来的に管理ノードを追加する予定がない場合は、次のように入力します。 `SG`または `StorageGRID。
- グリッドに複数の管理ノードが含まれている場合は、文字列 `[HOSTNAME]`識別子内。例： `SG-[HOSTNAME]` 。これにより、ノードのホスト名に基づいて、システム内の各管理ノードのSP接続 ID を示すテーブルが生成されます。

> StorageGRIDシステム内の各管理ノードに対してSP接続を作成する必要があります。各管理ノードにSP接続があると、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

c. フェデレーション メタデータ **URL** フィールドに各管理ノードのフェデレーション メタデータ URL を指定します。

次の形式を使用してください。

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

d. *保存*を選択します。

*保存*ボタンに緑色のチェックマークが数秒間表示されます。

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接続を構成する

設定が保存されると、サンドボックス モードの確認通知が表示されます。この通知は、サンドボックス モードが有効になったことを確認し、概要の手順を示します。

StorageGRID は、必要な限りサンドボックス 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 が選択されている場合、すべてのStorageGRIDユーザーに対して SSO が無効になります。ローカルユーザーのみがサインインできます。

証明書利用者信頼 (Active Directory) を構成する、エンタープライズ アプリケーション (Azure) を完了する、またはSP接続 (PingFederate) を構成するには、次の手順に従います。

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シングル サインオン ページの表に示されている各証明書利用者 ID を使用して、StorageGRIDに対して 1 つ以上の証明書利用者信頼を作成します。

   表に示されている管理ノードごとに 1 つの信頼を作成する必要があります。

   手順については、"AD FS で証明書利用者信頼を作成する" 。

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 ページで、SAML メタデータをダウンロードして保存するためのボタンを選択します。
2. 次に、グリッド内の他の管理ノードに対して、次の手順を繰り返します。
   a. ノードにSign in。
   b. 構成 > 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 ポータルに移動します。
4. 以下の手順に従ってください"Azure AD でエンタープライズ アプリケーションを作成する"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 ページで、SAML メタデータをダウンロードして保存するためのボタンを選択します。
2. 次に、グリッド内の他の管理ノードに対して、次の手順を繰り返します。
   a. ノードにSign in。
   b. 構成 > 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 にアクセスします。
4. "StorageGRIDの 1 つ以上のサービス プロバイダー (SP) 接続を作成します。" 。各管理ノードのSP接続 ID (StorageGRIDシングル サインオン ページの表に表示) 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。

   表に示されている管理ノードごとに 1 つのSP接続を作成する必要があります。

SSO接続をテストする

StorageGRIDシステム全体にシングル サインオンの使用を強制する前に、各管理ノードに対してシングル サ

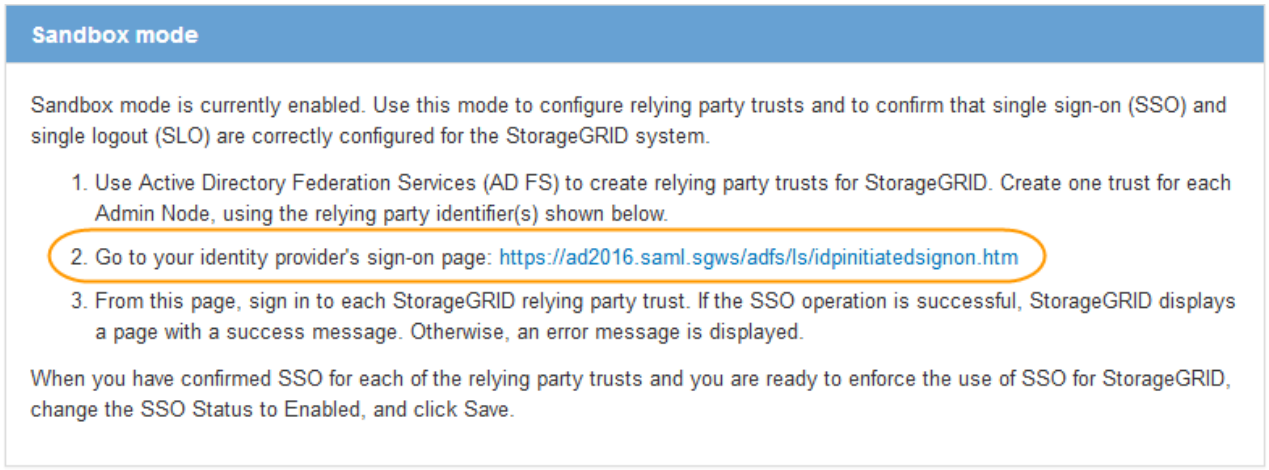
インオンとシングル ログアウトが正しく設定されていることを確認する必要があります。

Active Directory

手順

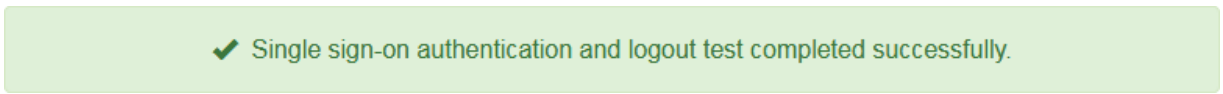
1. StorageGRIDシングル サインオン ページで、サンドボックス モード メッセージ内のリンクを見つけます。

   URL は、「フェデレーション サービス名」フィールドに入力した値から派生します。



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、ID プロバイダーのサインオン 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Sign in* 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、**Sign in** を選択します。

4. フェデレーションユーザー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操作が成功すると、成功メッセージが表示されます。



   - SSO 操作が失敗した場合、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 Cookie をクリアして、もう一度お試しください。
5. これらの手順を繰り返して、グリッド内の各管理ノードの 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*を選択します。
3. フェデレーション ユーザーの資格情報を入力します。
   - SSO サインインおよびログアウト操作が成功すると、成功メッセージが表示されます。

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

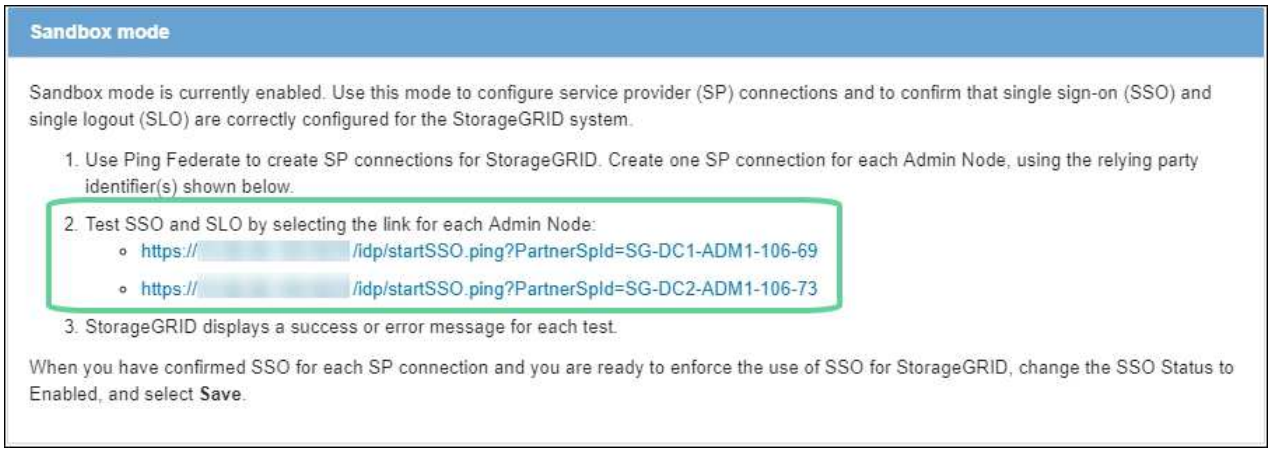
   - SSO 操作が失敗した場合、エラー メッセージが表示されます。問題を修正し、ブラウザの Cookie をクリアして、もう一度お試しください。
4. これらの手順を繰り返して、グリッド内の各管理ノードの SSO 接続を確認します。

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. フェデレーション ユーザーの資格情報を入力します。
   - SSO サインインおよびログアウト操作が成功すると、成功メッセージが表示されます。

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

   - SSO 操作が失敗した場合、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 Cookie をクリアして、もう一度お試しください。
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、ブラウザの「戻る」ボタンを選択し、資格情報を再送信してください。

シングルサインオンを有効にする

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システム全体に対して SSO を有効にできます。

SSO が有効になっている場合、すべてのユーザーは Grid Manager、Tenant Manager、Grid Management API、および Tenant Management API にアクセスするために SSO を使用する必要があります。ローカル ユーザーはStorageGRIDにアクセスできなくなります。

手順

1. 構成 > 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 有効 に変更します。
3. *保存*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 にアクセスするために使用するのと同じコンピューターからStorageGRIDにアクセスする場合は、Azure ポータル ユーザーが承認されたStorageGRIDユーザー (StorageGRIDにインポートされたフェデレーション グループ内のユーザー) であることを確認するか、 StorageGRIDにサインインする前に Azure ポータルからログアウトしてください。

AD FS で証明書利用者信頼を作成する

システム内の各管理ノードに対して証明書利用者信頼を作成するには、Active Directory フェデレーション サービス (AD FS) を使用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、データを手動で入力することで、証明書利用者信頼を作成できます。

開始する前に

- StorageGRIDのシングル サインオンを構成し、SSO タイプとして **AD FS** を選択しました。
- グリッド マネージャーのシングル 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。見る"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) と証明書利用者識別子がわかっています。これらの値は、StorageGRID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で確認できます。

StorageGRIDシステム内の各管理ノードに対して、証明書利用者信頼を作成する必要があります。各管理ノードに証明書利用者信頼を設定することで、ユーザーはどの管理ノードに対しても安全にサインインおよびサインアウトできるようになります。

- AD FS で証明書利用者信頼を作成した経験があるか、Microsoft AD FS ドキュメントにアクセス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おり、Administrators グループに属しています。

- 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アップロードされたカスタム証明書があるか、コマンド シェルから管理ノードにログインする方法を知っている必要があります。

タスク概要

これらの手順は、Windows Server 2016 AD FS に適用されます。異なるバージョンの AD FS を使用している場合は、手順が若干異なります。ご質問がある場合は、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する

Windows PowerShell を使用すると、1 つ以上の証明書利用者信頼をすばやく作成できます。

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-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - のために *Admin_Node_Identifier*、シングル サインオン ページに表示されるとおりに、管理ノードの証明書利用者識別子を入力します。例： `SG-DC1-ADM1` 。
   - のために *Admin_Node_FQDN*、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、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたときにはこの証明書利用者信頼を更新または再作成する必要があることに注意してください。
3. Windows Server Manager から、[ツール] > [AD FS 管理] 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. 新しく作成され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. 先ほど作成した証明書利用者信頼を見つけます。
   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*を選択し、*OK*を選択します。
6. 新しく作成された証明書利用者信頼にクレーム発行ポリシーを追加します。
   a. 先ほど作成した証明書利用者信頼を見つけます。
   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. *ルールを追加*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. 「ルールの構成」ページで、このルールの表示名を入力します。

   たとえば、**ObjectGUID** から **Name ID** または **UPN** から **Name ID** です。

f. 属性ストアには、**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、**User-Principal-Name** を選択します。

h. マッピング テーブルの [送信クレーム 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、そのプロパティを開きます。

   b. エンドポイント、識別子、*署名*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、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. これら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構成します。

9. 完了したら、 StorageGRIDに戻り、すべての証明書利用者信頼をテストして、正しく構成されていることを確認します。見る"サンドボックスモードを使用する"手順についてはこちらをご覧ください。

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する

各管理ノードの SAML メタデータにアクセスすることで、各証明書利用者信頼の値をインポートできます。

手順

1. Windows Server Manager で、[ツール] を選択し、[AD FS 管理] を選択します。
2. [アクション] の下で、[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`

   のために *Admin_Node_FQDN*、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、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたときにはこの証明書利用者信頼を更新または再作成する必要があることに注意してください。

6. 証明書利用者信頼ウィザードを完了し、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、グリッド マネージャーのシングル サインオン ページに表示されるとおりに、管理ノードの依存パーティ識別子を使用します。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*を選択します:
   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. 「ルールの構成」ページで、このルールの表示名を入力します。

      たとえば、**ObjectGUID** から **Name ID** または **UPN** から **Name ID** です。

   e. 属性ストアには、**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、**User-Principal-Name** を選択します。
   g. マッピング テーブルの [送信クレーム 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、そのプロパティを開きます。
   b. エンドポイント、識別子、*署名*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、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. これら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構成します。
10. 完了したら、 StorageGRIDに戻り、すべての証明書利用者信頼をテストして、正しく構成されていることを確認します。見る"サンドボックスモードを使用する"手順についてはこちらをご覧ください。

証明書利用者信頼を手動で作成する

依存部分信頼のデータをインポートしない場合は、値を手動で入力できます。

手順

1. Windows Server Manager で、[ツール] を選択し、[AD FS 管理] を選択します。
2. [アクション] の下で、[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*を選択し、*次へ*を選択します。
5. 証明書利用者信頼ウィザードを完了します。
   a. この管理ノードの表示名を入力します。

      一貫性を保つために、グリッド マネージャーのシングル サインオン ページに表示されるとおりに、管理ノードの依存パーティ ID を使用します。例： `SG-DC1-ADM1` 。

   b. オプションのトークン暗号化証明書を構成する手順をスキップします。

c. [URL の構成] 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 URL を入力します。

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

のために *Admin_Node_FQDN*、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、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたときにはこの証明書利用者信頼を更新または再作成する必要があることに注意してください。

e. 「識別子の構成」ページで、同じ管理ノードの依存パーティ識別子を指定します。

```
Admin_Node_Identifier
```

のために *Admin_Node_Identifier*、シングル サインオン ページに表示されるとおりに、管理ノードの証明書利用者識別子を入力します。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. 「ルールの構成」ページで、このルールの表示名を入力します。

たとえば、**ObjectGUID** から **Name ID** または **UPN** から **Name ID** です。

c. 属性ストアには、**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、**User-Principal-Name** を選択します。

e. マッピング テーブルの [送信クレーム 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、そのプロパティを開きます。

8. エンドポイント タブで、シングル ログアウト (SLO) のエンドポイントを構成します。

a. *SAML の追加*を選択します。

b. エンドポイント タイプ > **SAML** ログアウト を選択します。

c. バインド > *リダイレクト*を選択します。

d. 信頼できる **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`

のために *Admin_Node_FQDN*、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、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたときにはこの証明書利用者信頼を更新または再作成する必要があることに注意してください。

a. 「OK」を選択します。

9. *署名*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。
      - カスタム証明書をお持ちでない場合は、管理ノードにログインし、 `/var/local/mgmt-api`管理ノードのディレクトリに `custom-server.crt`証明書ファイル。

      管理ノードのデフォルト証明書を使用する(`server.crt`）は推奨されません。管理ノードに障害が発生した場合、ノードを回復すると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*を選択し、*OK*を選択します。

      依存パーティのプロパティが保存され、閉じられます。

10. これら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構成します。
11. 完了したら、 StorageGRIDに戻り、すべての証明書利用者信頼をテストして、正しく構成されていることを確認します。見る"サンドボックスモードを使用する"手順についてはこちらをご覧ください。

Azure AD でエンタープライズ アプリケーションを作成する

Azure AD を使用して、システム内の各管理ノードに対してエンタープライズ アプリケーションを作成します。

開始する前に

- StorageGRIDのシングル サインオンの構成を開始し、SSO タイプとして **Azure** を選択しました。
- グリッド マネージャーのシングル 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。見る"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には エンタープライズ アプリケーション名 があります。これらの値は、StorageGRID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システム内の各管理ノードに対してエンタープライズ アプリケーションを作成する必要があります。各管理ノード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、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

- 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こと。
- アクティブなサブスクリプションを持つ Azure アカウントがあります。

- Azure アカウントで、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、またはサービス プリンシパルの所有者のいずれかのロールを持っていること。

Azure AD にアクセスする

手順

1. ログイン "Azureポータル"。
2. 移動先 "Azure アクティブ ディレクトリ"。
3. 選択 "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構成を保存する

StorageGRIDに Azure の SSO 構成を保存するには、Azure を使用して各管理ノードのエンタープライズ アプリケーションを作成する必要があります。 Azure からフェデレーション メタデータ URL をコピーし、StorageGRID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 **URL** フィールドに貼り付けます。

手順

1. 各管理ノードに対して次の手順を繰り返します。
   a. Azure エンタープライズ アプリケーション ペインで、新しいアプリケーション 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. ギャラリーに見つからないその他のアプリケーションを統合する **(**ギャラリー以外**)** ラジオ ボタンを選択したままにします。
   e. *作成*を選択します。
   f. **2** の *開始 リンクを選択します。 シングル サインオンの設定 ボックスをクリックするか、左余白のシングル 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. ステップ **3 SAML** 署名証明書 の下にある アプリ フェデレーション メタデータ **URL** をコピーします。
   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 構成に必要なその他の変更をすべて行った後、 StorageGRIDシングル サインオン ページで [保存] を選択します。

すべての管理ノードの**SAML**メタデータをダウンロードする

SSO 構成を保存した後、 StorageGRIDシステム内の各管理ノードの SAML メタデータ ファイルをダウンロードできます。

手順

1. 各管理ノードに対してこれらの手順を繰り返します。
   a. 管理ノードからStorageGRIDにSign in。

b. 構成 > 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. ファイルを保存します。このファイルは Azure AD にアップロードされます。

各エンタープライズアプリケーションにSAMLメタデータをアップロードする

各StorageGRID管理ノードの SAML メタデータ ファイルをダウンロードした後、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. 各エンタープライズ アプリケーションに対して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 ページを更新する必要がある場合があります。

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. *割り当てが必要*を*いいえ*に設定します（割り当てを個別に構成する場合を除く）。

c. シングル サインオン ページに移動します。

d. SAML 構成を完了します。

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. ファイルが読み込まれたら、[保存] を選択し、[**X**] を選択してペインを閉じます。 SAML を使用したシングル サインオンの設定ページに戻ります。

3. 以下の手順に従ってください"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ー（SP）接続を作成する

PingFederate を使用して、システム内の各管理ノードのサービス プロバイダー (SP) 接続を作成します。プロセスを高速化するには、 StorageGRIDから SAML メタデータをインポートします。

開始する前に

- StorageGRIDのシングル サインオンを構成し、SSO タイプとして **Ping Federate** を選択しました。
- グリッド マネージャーのシングル 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。見る"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には * SP接続 ID* があります。これらの値は、StorageGRID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で確認できます。
- システム内の各管理ノードの **SAML** メタデータ をダウンロードしました。
- PingFederate Server でSP接続を作成した経験があること。
- あなた はhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_refer

ence_guide.html["管理者リファレンスガイド"^]PingFederate サーバー用。PingFederate のドキュメントには、詳細な手順と説明がステップバイステップで記載されています。

- あなたは"管理者権限"PingFederate サーバー用。

タスク概要

これらの手順は、PingFederate Server バージョン 10.3 をStorageGRIDの SSO プロバイダーとして構成する方法をまとめたものです。 PingFederate の別のバージョンを使用している場合は、これらの手順を調整する必要がある可能性があります。ご使用のリリースの詳細な手順については、PingFederate Server のドキュメントを参照してください。

PingFederateの前提条件を完了する

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

データストアを作成する

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ためのデータ ストアを作成します。使用した値を使用してください"アイデンティティ連携の設定"StorageGRIDで。

- タイプ: ディレクトリ (LDAP)
- **LDAP** タイプ: アクティブ ディレクトリ
- バイナリ属性名: LDAP バイナリ属性タブに、表示されているとおりに **objectGUID** を入力します。

パスワード認証情報検証ツールを作成する

まだ作成していない場合は、パスワード資格情報検証を作成してください。

- タイプ: LDAP ユーザー名 パスワード 資格情報検証
- 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 からの情報を入力します (例: DC=saml、DC=sgws)。
- 検索フィルター: sAMAccountName=${username}
- スコープ: サブツリー

IdPアダプタインスタンスを作成する

まだ作成していない場合は、IdP アダプター インスタンスを作成します。

手順

1. 認証 > 統合 > **IdP** アダプタ に移動します。
2. *新しいインスタンスの作成*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」に新しい行を追加する を選択します。
5. 選択してくださいパスワード認証検証ツールあなたが作成したもの。
6. [アダプタ属性] タブで、**Pseudonym** の **username** 属性を選択します。

7. *保存*を選択します。

署名証明書を作成またはインポートする

署名証明書をまだ作成またはインポートしていない場合は、作成またはインポートします。

手順

1. セキュリティ > 署名と復号化キーと証明書 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接続を作成する

PingFederate でSP接続を作成するときは、管理ノードのStorageGRIDからダウンロードした SAML メタデータをインポートします。メタデータ ファイルには、必要な特定の値が多数含まれています。

ユーザーがどのノードにも安全にサインインおよびサインアウトできるように、 StorageGRIDシステム内の各管理ノードに対してSP接続を作成する必要があります。最初のSP接続を作成するには、次の手順に従います。次に、追加のSP接続を作成する必要な追加の接続を作成します。

SP接続タイプを選択

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. *この接続にはテンプレートを使用しない*を選択します。
4. プロトコルとして*ブラウザSSOプロファイル*と*SAML 2.0*を選択します。

SPメタデータをインポートする

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. メタデータの概要と、[一般情報] 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**SSO**を構成する

手順

1. [ブラウザ SSO] タブから、[ブラウザ SSO の構成] を選択します。
2. SAML プロファイル タブで、* SP開始 SSO*、* SP開始 SLO*、* IdP 開始 SSO*、および * IdP 開始 SLO*

オプションを選択します。

3. *次へ*を選択します。
4. 「アサーションの有効期間」タブでは、変更を加えません。
5. [アサーション作成] タブで、[アサーション作成の構成] 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. [属性コントラクト] タブで、属性コントラクトとして **SAML_SUBJECT** を使用し、インポートされた未指定の名前形式を使用します。
6. 契約の延長の場合は、「削除」を選択して削除します。 `urn:oid`は使用されません。

マップアダプタインスタンス

手順

1. 認証ソース マッピング タブで、新しいアダプタ インスタンスのマップ を選択します。
2. アダプタインスタンスタブで、アダプタインスタンスあなたが作成したもの。
3. マッピング方法タブで、*データ ストアから追加の属性を取得する*を選択します。
4. [属性ソースとユーザー検索] 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説明を入力し、データストアと追加しました。
6. LDAP ディレクトリ検索タブ:
   - **Base DN** を入力します。これは、LDAP サーバーのStorageGRIDで入力した値と完全に一致する必要があります。
   - 検索範囲として、「サブツリー」を選択します。
   - ルート オブジェクト クラスの場合は、**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 バイナリ属性エンコード タイプ タブで、**objectGUID** 属性に **Base64** を選択します。
8. LDAP フィルター タブで、**sAMAccountName=${username}** と入力します。
9. [属性コントラクトの履行] 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** または **userPrincipalName** のいずれかを選択します。
10. 属性ソースを確認して保存します。
11. フェールセーブ属性ソースタブで、*SSO トランザクションを中止する*を選択します。
12. 概要を確認し、[完了] を選択します。
13. *完了*を選択します。

プロトコル設定を構成する

手順

1. * SP接続* > * ブラウザ SSO* > * プロトコル設定* タブで、* プロトコル設定の構成* 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（バインディングおよび `/api/saml-response`エンドポイント URL 用)。
3. SLO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（バインディングおよび `/api/saml-logout`エンドポイント URL 用。

4. [許可される SAML バインディング] タブで、**ARTIFACT** と **SOAP** をクリアします。 **POST** と **REDIRECT** のみが必要です。
5. [署名ポリシー] タブで、[認証リクエストに署名を要求する] および [アサーションに常に署名する] 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、[完了] 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接続タブから、*資格情報*を選択します。
2. [資格情報] タブから、[資格情報の構成] を選択します。
3. 選択してください署名証明書作成またはインポートした。
4. *次へ*を選択して*署名検証設定の管理*に進みます。
   a. [信頼モデル] タブで、[アンカーなし] を選択します。
   b. [署名検証証明書] タブで、 StorageGRID SAML メタデータからインポートされ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**接続を作成する

最初のSP接続をコピーして、グリッド内の各管理ノードに必要な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、署名検証、および SLO 応答 URL を除き、同一の設定が使用されます。

手順

1. 追加の管理ノードごとに初期SP接続のコピーを作成するには、[アクション] > [コピー] を選択します。
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*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** の構成 **>** アサーション作成の構成 **>** 属性コントラクト を選択します。
   c. **urn:oid** のエントリを削除します。

d. *保存*を選択します。

シングルサインオンを無効にする

この機能を使用したくなくなった場合は、シングル サインオン (SSO) を無効にすることができます。 ID フェデレーションを無効にする前に、シングル サインオンを無効にする必要があります。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

手順

1. 構成 > アクセス制御 > シングル サインオン を選択します。

   シングル サインオン ページが表示されます。

2. *無効*オプションを選択します。
3. *保存*を選択します。

   ローカル ユーザー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きに、 StorageGRIDSign inページが表示されるので、ローカルまたはフェデレーションStorageGRIDユーザーのユーザー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、再度有効にする

シングル サインオン (SSO) システムがダウンした場合、Grid Manager にサインインできない可能性があります。この場合、1 つの管理ノードに対して SSO を一時的に無効にし、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。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- あなたは `Passwords.txt`ファイル。
- ローカル ルート ユーザーのパスワードを知っています。

タスク概要

1 つの管理ノードの SSO を無効にした後、ローカル ルート ユーザーとして Grid Manager にサインインできます。 StorageGRIDシステムを保護するには、サインアウトしたらすぐにノードのコマンド シェルを使用して管理ノードで SSO を再度有効にする必要があります。

1 つの管理ノードの 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。グリッド マネージャーのシングル 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選択されたままになり、更新しない限り既存の SSO 設定はすべて維持されます。

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. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

      ルートとしてログインすると、プロンプトは `$`に `#`。
2. 次のコマンドを実行します。`disable-saml`

   メッセージは、コマンドがこの管理ノードにのみ適用されることを示します。
3. SSO を無効にすることを確認します。

   ノード上でシングル サインオンが無効になっている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グリッド マネージャーにアクセスします。

   SSO が無効になっているため、Grid Manager のサインイン ページが表示されます。
5. ユーザー名 root とローカル root ユーザーのパスワードでSign in。
6. SSO 構成を修正する必要があったために SSO を一時的に無効にした場合:
   a. 構成 > アクセス制御 > シングル サインオン を選択します。
   b. 不正確または古い SSO 設定を変更します。
   c. *保存*を選択します。

      シングル サインオン ページで [保存] を選択すると、グリッド全体の SSO が自動的に再度有効になります。
7. 他の理由でグリッド マネージャーにアクセスする必要があったため、SSO を一時的に無効にした場合:
   a. 実行する必要があるタスクをすべて実行します。
   b. *サインアウト*を選択し、グリッド マネージャーを閉じます。
   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できます。

      - 次のコマンドを実行します。 `enable-saml`

        メッセージは、コマンドがこの管理ノードにのみ適用されることを示します。

      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ていることを示すメッセージが表示されます。

- グリッド ノードを再起動します。 `reboot`

8. Web ブラウザから、同じ管理ノードからグリッド マネージャーにアクセスします。
9. StorageGRIDSign inページが表示され、Grid Manager にアクセスするには SSO 資格情報を入力する必要があることを確認します。

著作権に関する情報

商標に関する情報