StorageGRIDへのアクセスを制御する

StorageGRID software

NetApp
December 03, 2025

目次

StorageGRIDへのアクセスを制御する

StorageGRIDアクセスを制御する

グループとユーザーを作成またはインポートし、各グループに権限を割り当てることで、 StorageGRID にアクセスできるユーザーとユーザーが実行できるタスクを制御できます。オプションで、シングル サインオン (SSO) を有効にしたり、クライアント証明書を作成したり、グリッド パスワードを変更したりすることもできます。

グリッドマネージャーへのアクセスを制御する

アイデンティティ フェデレーション サービスからグループとユーザーをインポートするか、ローカル グループとローカル ユーザーを設定することで、Grid Manager と Grid Management API にアクセスできるユーザーを決定します。

使用"アイデンティティフェデレーション"セットアップが容易"グループ"そして"ユーザ"より高速になり、ユーザーは使い慣れた資格情報を使用してStorageGRIDにサインインできるようになります。 Active Directory、OpenLDAP、または Oracle Directory Server を使用する場合は、ID フェデレーションを構成できます。

> 別の 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。

各ユーザーが実行できるタスクを決定するには、異なる"権限"各グループに。たとえば、あるグループのユーザーに ILM ルールを管理させ、別のグループのユーザーにメンテナンス タスクを実行させたい場合があります。ユーザーがシステムにアクセスするには、少なくとも 1 つのグループに属している必要があります。

必要に応じて、グループを読み取り専用に設定できます。読み取り専用グループのユーザーは、設定と機能の表示のみが可能です。 Grid Manager または Grid Management API で変更を加えたり、操作を実行したりすることはできません。

シングルサインオンを有効にする

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。お先にどうぞ"SSOを設定して有効にする"すべてのユーザーは、グリッド マネージャー、テナント マネージャー、グリッド管理 API、またはテナント管理 API にアクセスする前に、外部 ID プロバイダーによって認証される必要があります。ローカル ユーザーはStorageGRIDにサインインできません。

プロビジョニングパスフレーズを変更する

プロビジョニング パスフレーズは、多くのインストールおよびメンテナンス手順、およびStorageGRIDリカバリ パッケージのダウンロードに必要です。パスフレーズは、 StorageGRIDシステムのグリッド トポロジ情報と暗号化キーのバックアップをダウンロードする場合にも必要です。あなたはできる"パスフレーズを変更する"必要に応じて。

ノードコンソールのパスワードを変更する

グリッド内の各ノードには一意のノード コンソール パスワードがあり、SSH を使用して「admin」としてノードにログインするか、VM/物理コンソール接続で root ユーザーとしてログインする必要があります。必要に

応じて、"ノードコンソールのパスワードを変更する"各ノードに対して。

プロビジョニングパスフレーズを変更する

StorageGRIDプロビジョニング パスフレーズを変更するには、この手順を使用します。パスフレーズは、回復、拡張、およびメンテナンスの手順に必要です。パスフレーズは、グリッド トポロジ情報、グリッド ノード コンソール パスワード、およびStorageGRIDシステムの暗号化キーを含むリカバリ パッケージ バックアップをダウンロードする場合にも必要です。

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" 。
- メンテナンスまたはルートアクセス権限があります。
- 現在のプロビジョニング パスフレーズを持っています。

タスク概要

プロビジョニングパスフレーズは、多くのインストールおよびメンテナンス手順で必要であり、"リカバリパッケージのダウンロード" 。プロビジョニングパスフレーズは、 `Passwords.txt`ファイル。プロビジョニングパスフレーズを必ず文書化し、安全な場所に保管してください。

手順

1. 構成 > アクセス制御 > グリッド 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*の下で*変更する*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。パスフレーズには 8 文字以上 32 文字以下を含める必要があります。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に必要です。
6. 新しいパスフレーズを再度入力し、「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、緑色の成功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後は、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 ファイルを使用すると、障害が発生した場合にシステムを復元できます。

ノードコンソールのパスワードを変更する

グリッド内の各ノードには一意のノード コンソール パスワードがあり、ノードにログインするにはこのパスワードが必要です。グリッド内の各ノードの固有のノード コンソール パスワードを変更するには、次の手順に従います。

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"メンテナンスまたはルートアクセス権限"。
- 現在のプロビジョニング パスフレーズを持っています。

タスク概要

ノード コンソールの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、VM/物理コンソール接続で root ユーザーとしてログインします。ノードコンソールのパスワード変更プロセスは、グリッド内の各ノードに新しいパスワードを作成し、更新されたパスワードを保存します。`Passwords.txt`リカバリ パッケージ内のファイル。パスワードは、Passwords.txt ファイルの「パスワード」列に記載されています。

> ノード間の通信に使用される SSH キーには、個別の SSH アクセス パスワードがあります。この手順では SSH アクセス パスワードは変更されません。

ウィザードにアクセスする

手順

1. 構成 > アクセス制御 > グリッド パスワード を選択します。
2. ノード コンソールのパスワードの変更 の下で、変更を行う を選択します。

プロビジョニングパスフレーズを入力してください

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. *続行*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する

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変更プロセスが失敗した場合は、このファイル内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する(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

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に使用できる暗号化キーとパスワードが含まれているため、セキュリティ保護する必要があります。

3. *続行*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たら [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。

ノードコンソールのパスワードを変更する

ノード コンソールのパスワード プロセスが開始すると、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. 新しい回復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場合があります。
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すると次のようになります。

   a. 開く `.zip`ファイル。

   b. 以下のコンテンツにアクセスできることを確認してください。 `Passwords.txt`ファイルには新しいノード コンソールのパスワードが含まれています。

   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 つの安全でセキュリティ保護された別の場所に保管します。

   古いリカバリ パッケージを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に使用できる暗号化キーとパスワードが含まれているため、セキュリティ保護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、その内容を確認したことを示すには、チェックボックスを選択します。
5. ノード コンソールのパスワードの変更 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。これには数分かかる場合があります。

   すべてのノードのパスワードが変更されると、緑色の成功バナーが表示されます。次の手順へ進みます。

   更新プロセス中にエラーが発生した場合、バナー メッセージにパスワードの変更に失敗したノードの数が表示されます。システムは、パスワードの変更に失敗したノードに対してプロセスを自動的に再試行します。一部のノードでパスワードが変更されていない状態でプロセスが終了した場合は、[再試行] 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. 表にリストされているエラー メッセージを確認します。

   b. 問題を解決してください。

c. *再試行*を選択します。

再試行すると、以前のパスワード変更の試行中に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のパスワードが変更されたら、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、リカバリ 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します。

管理ノードのSSHアクセスパスワードを変更する

管理ノードの SSH アクセス パスワードを変更すると、グリッド内の各ノードの一意の内部 SSH キー セットも更新されます。プライマリ管理ノードは、これらの SSH キーを使用して、安全なパスワードレス認証でノードにアクセスします。

SSHキーを使用してノードにログインします `admin`または、VM または物理コンソール接続上の root ユーザーにアクセスします。

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"メンテナンスまたはルートアクセス権限"。
- 現在のプロビジョニング パスフレーズを持っています。

タスク概要

管理ノードの新しいアクセスパスワードと各ノードの新しい内部キーは、 `Passwords.txt`リカバリ パッケージ内のファイル。キーはそのファイルの「パスワード」列にリストされています。

ノード間の通信に使用される SSH キーには、個別の SSH アクセス パスワードがあります。これらはこの手順では変更されません。

ウィザードにアクセスする

手順

1. 構成 > アクセス制御 > グリッド パスワード を選択します。
2. **SSH** キーの変更 の下で、変更を加える 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する

SSH アクセス キーを変更する前に、最新のリカバリ 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キー変更プロセスが失敗した場合は、このファイル内のキーを使用できます。

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. *リカバリ パッケージのダウンロード*を選択します。

3. リカバリパッケージファイルをコピーする(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

   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に使用できる暗号化キーとパスワードが含まれているため、セキュリティ保護する必要があります。

4. *続行*を選択します。
5. 確認ダイアログが表示されたら、SSH アクセス キーの変更を開始する準備ができたら [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。

SSHアクセスキーを変更する

SSH アクセス キーの変更プロセスが開始されると、新しいキー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、各ノードでキーが更新されます。

手順

1. 新しい回復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場合があります。
2. 新しいリカバリパッケージのダウンロードボタンが有効になったら、*新しいリカバリパッケージのダウンロード*を選択し、新しいリカバリパッケージファイルを保存します。(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。
3. ダウンロードが完了すると次のようになります。

   a. 開く `.zip`ファイル。

   b. 以下のコンテンツにアクセスできることを確認してください。 `Passwords.txt`新しい SSH アクセス キーが含まれるファイル。

   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 つの安全でセキュリティ保護された別の場所に保管します。

      古いリカバリ パッケージを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に使用できる暗号化キーとパスワードが含まれているため、セキュリティ保護する必要があります。

4. 各ノードでキーが更新されるまで待ちます。これには数分かかる場合があります。

   すべてのノードのキーが変更されると、緑色の成功バナーが表示されます。

   更新プロセス中にエラーが発生した場合、キーの変更に失敗したノードの数がバナー メッセージにリストされます。システムは、キーの変更に失敗したノード上でプロセスを自動的に再試行します。一部のノードにまだ変更されたキーがない状態でプロセスが終了した場合は、[再試行] ボタンが表示されます。

   1 つ以上のノードでキーの更新に失敗した場合:

   a. 表にリストされているエラー メッセージを確認します。

b. 問題を解決してください。

c. *再試行*を選択します。

再試行すると、以前のキー変更の試行中に失敗したノード上の SSH アクセス キーのみが変更されます。

5. すべてのノードのSSHアクセスキーが変更されたら、最初にダウンロードしたリカバリパッケージ 。
6. オプションで、メンテナンス > システム > リカバリ パッケージ を選択して、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します。

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、グループとユーザーの設定が高速化され、ユーザーは使い慣れた資格情報を使用してStorageGRIDにサインインできるようになります。

Grid Manager の ID フェデレーションを構成する

管理者グループとユーザーを 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 ID フェデレーションを構成できます。

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" 。
- あなたが持っている"特定のアクセス権限"。
- ID プロバイダーとして、Active Directory、Azure AD、OpenLDAP、または Oracle Directory Server を使用しています。

> リストされていない 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 を使用する予定の場合は、OpenLDAP サーバーを構成する必要があります。見るOpenLDAP サーバーの設定ガイドライン 。
- シングルサインオン（SSO）を有効にする予定の場合は、"シングルサインオンの要件と考慮事項" 。
- LDAP サーバーとの通信にトランスポート層セキュリティ (TLS) を使用する予定の場合、ID プロバイダーは TLS 1.2 または 1.3 を使用しています。見る"送信 TLS 接続でサポートされている暗号" 。

タスク概要

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 ID ソースを構成できます。次の種類のグループをインポートできます。

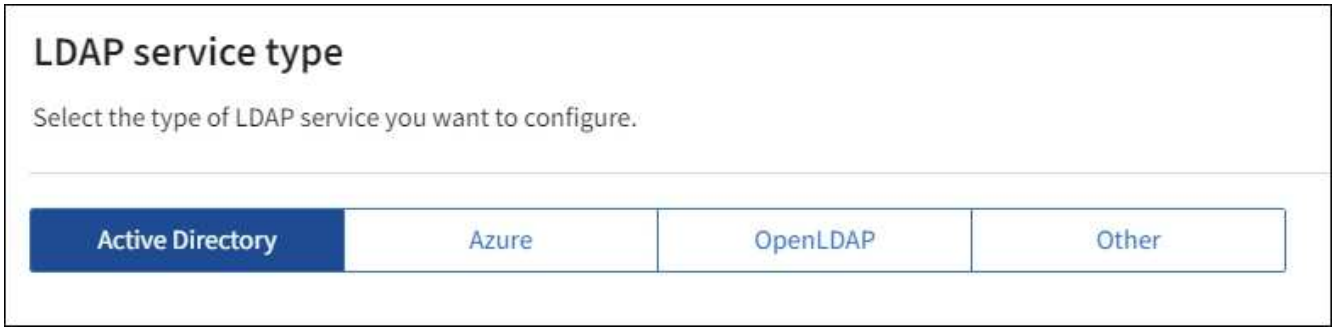
- 管理者グループ。管理グループ内のユーザーは、グループに割り当てられた管理権限に基づいて、グリッド マネージャーにサインインしてタスクを実行できます。
- 独自の ID ソースを使用しないテナントのテナント ユーザー グループ。テナント グループ内のユーザーは、テナント マネージャーにサインインし、テナント マネージャーでグループに割り当てられた権限に基づいてタスクを実行できます。見る"テナントアカウントを作成する"そして"テナントアカウントを使用

する"詳細については。

設定を入力する

手順

1. 構成 > アクセス制御 > **ID** フェデレーション を選択します。
2. **ID** フェデレーションを有効にする を選択します。
3. LDAP サービス タイプ セクションで、構成する LDAP サービスのタイプを選択します。



Oracle Directory Server を使用する LDAP サーバーの値を構成するには、「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。次の手順に進みます。
   - ユーザーの一意の名前: LDAP ユーザーの一意の識別子を含む属性の名前。この属性は、`sAMAccountName` Active Directoryおよび `uid`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `uid`。
   - ユーザー **UUID**: LDAP ユーザーの永続的な一意の識別子を含む属性の名前。この属性は、`objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各ユーザーの値は、16 バイト形式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。
   - グループの一意の名前: LDAP グループの一意の識別子を含む属性の名前。この属性は、`sAMAccountName` Active Directoryおよび `cn`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `cn`。
   - グループ **UUID**: LDAP グループの永続的な一意の識別子を含む属性の名前。この属性は、`objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各グループの値は、16 バイト形式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 サーバーの構成] セクションで必要な LDAP サーバーおよびネットワーク接続情報を入力します。
   - ホスト名: LDAP サーバーの完全修飾ドメイン名 (FQDN) または IP アドレス。
   - ポート: LDAP サーバーに接続するために使用されるポート。

     STARTTLS のデフォルト ポートは 389 で、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る限り、どのポートでも使用できます。

   - ユーザー名: LDAP サーバーに接続するユーザーの識別名 (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。

指定されたユーザーには、グループとユーザーを一覧表示し、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`
- アクティブディレクトリ: `objectSid` 、 `primaryGroupID` 、 `userAccountControl` 、 そして `userPrincipalName`
- アズール: `accountEnabled`そして `userPrincipalName`

◦ パスワード: ユーザー名に関連付けられたパスワード。

> 将来パスワードを変更する場合は、このページで更新する必要があります。

◦ グループ ベース **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 の例 (下記) では、識別名がベース DN (DC=storagegrid、DC=example、DC=com) を基準とするすべてのグループをフェデレーション グループとして使用できます。

> グループの一意の名前*の値は、それが属する *グループ ベース **DN** 内で一意である必要があります。

◦ ユーザー ベース **DN**: ユーザーを検索する LDAP サブツリーの識別名 (DN) の完全パス。

> ユーザー固有名 の値は、それが属する 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 ユーザー名の形式 (オプション): パターンを自動的に決定できない場合にStorageGRIDが使用するデフォルトのユーザー名パターン。

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ーがサインインできるように、バインド ユーザー名形式 を指定することをお勧めします。

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 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`

  [USERNAME] を記載どおりに入力してください。

6. [トランスポート層セキュリティ (TLS)] セクションで、セキュリティ設定を選択します。

◦ **STARTTLS** を使用する: STARTTLS を使用して、LDAP サーバーとの通信を保護します。これは、Active Directory、OpenLDAP、またはその他の場合に推奨されるオプションですが、このオプシ

ョンは Azure ではサポートされていません。

- **LDAPS** を使用する: LDAPS (LDAP over SSL) オプションは、TLS を使用して LDAP サーバーへの接続を確立します。Azure の場合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: StorageGRIDシステムと LDAP サーバー間のネットワーク 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 サーバーが LDAP 署名を強制している場合、「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、接続を保護するため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 Grid CA 証明書を使用して、接続を保護します。
   - カスタム **CA** 証明書を使用する: 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。

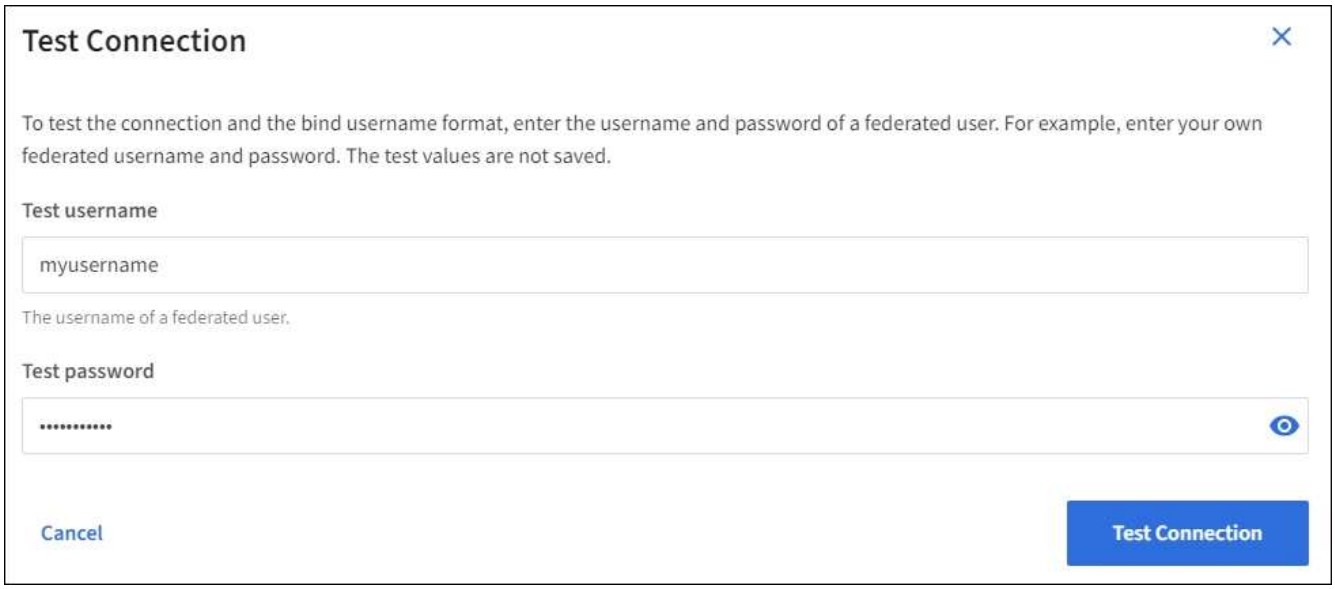
接続をテストし、設定を保存します

すべての値を入力した後、構成を保存する前に接続をテストする必要があります。 StorageGRID は、LDAP サーバーの接続設定と、指定された場合はバインド ユーザー名の形式を検証します。

手順

1. *テスト接続*を選択します。
2. バインドユーザー名の形式を指定しなかった場合:
   - 接続設定が有効な場合は、「テスト接続が成功しました」というメッセージが表示されます。設定を保存するには、[保存] を選択します。
   - 接続設定が無効な場合、「テスト接続を確立できませんでした」というメッセージが表示されます。 *閉じる*を選択します。次に、問題を解決して、再度接続をテストします。
3. バインド ユーザー名形式を指定した場合は、有効なフェデレーション ユーザーのユーザー名とパスワードを入力します。

   たとえば、独自のユーザー名とパスワードを入力します。ユーザー名には @ や / などの特殊文字を含めないでください。



- 接続設定が有効な場合は、「テスト接続が成功しました」というメッセージが表示されます。設定を保存するには、[保存] を選択します。
- 接続設定、バインド ユーザー名の形式、またはテスト ユーザー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、再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、フェデレーション グループとユーザーを ID ソースから定期的に同期します。できるだけ早くユーザー権限を有効化または制限したい場合は、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*同期サーバー*を選択します。

   環境によっては同期プロセスに時間がかかる場合があります。

   アイデンティティ ソースからのフェデレーション グループとユーザーの同期に問題がある場合、アイデンティティ フェデレーション同期の失敗 アラートがトリガーされます。

ID連携を無効にする

グループおよびユーザーの ID 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 フェデレーションが無効になっている場合、 StorageGRIDとアイデンティティ ソース間の通信は行われません。ただし、構成した設定はすべて保持されるため、将来、簡単に ID フェデレーションを再度有効にすることができます。

タスク概要

ID 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。

- フェデレーション ユーザー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ション ユーザーは、セッションの有効期限が切れるまでStorageGRIDシステムへのアクセスを保持しますが、セッションの有効期限が切れた後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アラートは発生しません。
- シングル サインオン (SSO) が 有効 または サンドボックス モード に設定されている場合、**ID** 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。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 ページの SSO ステータスを 無効 にする必要があります。見る"シングルサインオンを無効にする" 。

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. **ID** 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 サーバーの設定ガイドライン

ID フェデレーションに OpenLDAP サーバーを使用する場合は、OpenLDAP サーバーで特定の設定を構成する必要があります。

> ActiveDirectory または Azure 以外の ID ソースの場合、 StorageGRID は外部的に無効になっているユーザーへの S3 アクセスを自動的にブロックしません。S3 アクセスをブロックするには、ユーザーの S3 キーを削除するか、すべてのグループからユーザーを削除します。

Memberof と **refint** オーバーレイ

memberof および 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、http://www.openldap.org/doc/admin24/index.html["OpenLDAP 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

指定されたインデックス キーワードを使用して、次の OpenLDAP 属性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`

さらに、最適なパフォーマンスを得るために、ユーザー名のヘルプに記載されているフィールドがインデックス化されていることを確認してください。

逆グループメンバーシップ維持に関する情報は、http://www.openldap.org/doc/admin24/index.html["OpenLDAP ドキュメント: バージョン 2.4 管理者ガイド"^] 。

管理者グループの管理

管理者グループを作成して、1 人以上の管理者ユーザー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権を付与するには、ユーザーはグループに属

している必要があります。

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"。
- フェデレーション グループをインポートする予定の場合は、ID フェデレーションが構成されており、構成された ID ソースにフェデレーション グループがすでに存在します。

管理者グループを作成する

管理者グループを使用すると、グリッド マネージャーおよびグリッド管理 API のどの機能と操作にどのユーザーが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する

手順

1. 構成 > アクセス制御 > *管理者グループ*を選択します。
2. *グループを作成*を選択します。

グループの種類を選択

ローカル グループを作成したり、フェデレーション グループをインポートしたりできます。

- ローカル ユーザー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 ソースからユーザーをインポートするためのフェデレーション グループを作成します。

ローカルグループ

手順

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。これは必要に応じて後で更新できます。たとえば、「メンテナンスユーザー」や「ILM 管理者」などです。
3. グループの一意の名前を入力します。この名前は後で更新できません。
4. *続行*を選択します。

連合グループ

手順

1. *フェデレーション グループ*を選択します。
2. 構成された ID ソースに表示されるとおりに、インポートするグループの名前を入力します。
   - 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 の場合は、LDAP サーバーの適切な一意の名前を使用します。
3. *続行*を選択します。

グループ権限を管理する

手順

1. アクセス モード では、グループ内のユーザーが Grid Manager および Grid Management API で設定を変更したり操作を実行したりできるか、それとも設定と機能の表示のみが可能かを選択します。
   - 読み取り/書き込み (デフォルト): ユーザーは設定を変更したり、管理権限で許可された操作を実行したりできます。
   - 読み取り専用: ユーザーは設定と機能の表示のみが可能です。 Grid Manager または Grid Management API で変更を加えたり、操作を実行したりすることはできません。ローカルの読み取り専用ユーザー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おり、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対して読み取り専用アクセス権を持ちます。

2. 1つ以上選択してください"管理者グループの権限"。

   各グループに少なくとも 1 つ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ーはStorageGRIDにサインインできなくなります。

3. ローカル グループを作成する場合は、[続行] を選択します。フェデレーション グループを作成する場合は、[グループの作成] と [完了] を選択します。

ユーザーを追加する（ローカルグループのみ）

手順

1. 必要に応じて、このグループのローカル ユーザーを 1 人以上選択します。

   ローカル ユーザーをまだ作成していない場合は、ユーザーを追加せずにグループを保存できます。このグループをユーザー ページに追加できます。見る"ユーザの管理"詳細については。

2. *グループの作成*と*完了*を選択します。

管理者グループの表示と編集

既存のグループの詳細を表示したり、グループを変更したり、グループを複製したりできます。

- 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。

Task	[操作]メニュー	詳細ページ
グループの詳細を表示	a. グループのチェックボックスを選択します。 b. アクション > *グループの詳細を表示*を選択します。	表内のグループ名を選択します。
表示名を編集する（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選択します。 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てください。 d. *変更を保存*を選択します。	a. グループ名を選択すると詳細が表示されます。 b. 編集アイコンを選択。 c. 新しい名前を入力してください。 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する	a. グループのチェックボックスを選択します。 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. 必要に応じて選択またはクリアします"管理者グループの権限"。 e. *変更を保存*を選択します。	a. グループ名を選択すると詳細が表示されます。 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. 必要に応じて選択またはクリアします"管理者グループの権限"。 d. *変更を保存*を選択します。

グループを複製する

手順

1. グループのチェックボックスを選択します。
2. アクション > *グループの複製*を選択します。

3. 複製グループウィザードを完了します。

グループを削除する

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

手順

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選択します。
2. アクション > *グループの削除*を選択します。
3. *グループの削除*を選択します。

管理者グループの権限

管理者ユーザー グループを作成するときは、グリッド マネージャーの特定の機能へのアクセスを制御するための 1 つ以上の権限を選択します。その後、各ユーザーを 1 つ以上の管理者グループに割り当てて、そのユーザーが実行できるタスクを決定できます。

各グループに少なくとも 1 つ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ーは Grid Manager または Grid Management API にサインインできなくなります。

デフォルトでは、少なくとも 1 つの権限を持つグループに属するすべてのユーザーは、次のタスクを実行できます。

- グリッドマネージャーにSign in
- ダッシュボードを見る
- ノードページを表示する
- 現在のアラートと解決済みのアラートを表示する
- 自分のパスワードを変更する（ローカル ユーザーのみ）
- 構成ページとメンテナンスページで提供される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 設定によって、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表示のみが可能かどうかが決まります。ユーザーが複数のグループに属しており、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対して読み取り専用アクセス権を持ちます。

次のセクションでは、管理者グループを作成または編集するときに割り当てることができる権限について説明します。明示的に記載されていない機能には、ルート アクセス 権限が必要です。

ルート アクセス

この権限により、すべてのグリッド管理機能にアクセスできます。

テナントのルートパスワードを変更する

この権限により、テナント ページの ルート パスワードの変更 オプションにアクセスでき、テナントのローカル ルート ユーザーのパスワードを変更できるユーザーを制御できます。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 キーを移行するためにも使用されます。この権限を持たないユーザーには、ルート パスワードの変更 オプションは表示されません。

> ルート パスワードの変更 オプションを含むテナント ページへのアクセスを許可するには、テナント アカウント 権限も割り当てます。

グリッドトポロジページの構成

この権限により、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。

> グリッド トポロジ ページは非推奨となり、将来のリリースで削除される予定です。

ILM

この権限により、次の **ILM** メニュー オプションにアクセスできます。

- ルール
- ポリシー
- ポリシータグ
- ストレージプール
- 保管グレード
- 地域
- オブジェクトメタデータ検索

> ストレージ グレードを管理するには、ユーザーは その他のグリッド構成 および グリッド トポロジ ページ構成 権限を持っている必要があります。

メンテナンス

これらのオプションを使用するには、ユーザーはメンテナンス権限を持っている必要があります。

- 構成 > アクセス制御:
  - グリッドパスワード
- 設定 > ネットワーク:
  - S3エンドポイントのドメイン名
- 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:
    - 回復パッケージ
    - ソフトウェアアップデート
- サポート > ツール:
    - Logs

メンテナンス権限を持たないユーザーは、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
    - グリッド ネットワーク
    - NTPサーバ
- メンテナンス > システム:
    - ライセンス
- 設定 > ネットワーク:
    - S3エンドポイントのドメイン名
- 構成 > セキュリティ:
    - 証明書
- 構成 > 監視:
    - 監査および Syslog サーバー

アラートを管理する

この権限により、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、ユーザーにこの権限が必要です。

メトリクスクエリ

この権限により、次のものへのアクセスが提供されます:

- サポート > ツール > メトリクス ページ
- グリッド管理 API の **Metrics** セクションを使用したカスタム Prometheus メトリック クエリ
- メトリックを含むグリッド マネージャー ダッシュボード カード

オブジェクトメタデータ検索

この権限により、**ILM** > オブジェクト メタデータ検索 ページへのアクセスが提供されます。

その他のグリッド構成

この権限により、追加のグリッド構成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、ユーザーは グリッド トポロジ ページの構成 権限も持っている必要があります。

- **ILM**:
  - 保管グレード
- 構成 > システム:
- サポート > その他:
  - リンクコスト

ストレージアプライアンス管理者

この権限により、次のことが提供されます。

- グリッド マネージャーを介してストレージ アプライアンス上の E シリーズSANtricityシステム マネージャーにアクセスします。
- これらの操作をサポートするアプライアンスの「ドライブの管理」タブでトラブルシューティングおよびメンテナンス タスクを実行する機能。

テナントアカウント

この権限により、次のことが可能になります:

- テナントページにアクセスして、テナントアカウントを作成、編集、削除できます。
- 既存のトラフィック分類ポリシーを表示する
- テナントの詳細を含むグリッド マネージャー ダッシュボード カードを表示する

ユーザの管理

ローカル ユーザーとフェデレーション ユーザーを表示できます。ローカル ユーザーを作成してローカル管理者グループに割り当て、これらのユーザーがアクセスできる Grid Manager 機能を決定することもできます。

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" 。
- あなたが持っている"特定のアクセス権限"。

ローカルユーザーを作成する

1 人以上のローカル ユーザーを作成し、各ユーザーを 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。グループの権限は、ユーザーがアクセスできる Grid Manager および Grid Management API 機能を制御します。

ローカル ユーザーのみを作成できます。外部 ID ソースを使用して、フェデレーション ユーザーとグループを管理します。

グリッド マネージャーには、「root」という名前の定義済みローカル ユーザーが 1 人含まれています。ルートユーザー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 ユーザーはStorageGRIDにサインインできません。

ウィザードにアクセスする

手順

1. 構成 > 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。

ユーザー資格情報を入力してください

手順

1. ユーザーのフルネーム、一意のユーザー名、およびパスワードを入力します。
2. オプションで、このユーザーに Grid Manager または Grid Management API へのアクセスを許可しない場合は、「はい」を選択します。
3. *続行*を選択します。

グループに割り当てる

手順

1. 必要に応じて、ユーザーを 1 つ以上のグループに割り当てて、ユーザー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ーを保存できます。このユーザーをグループ ページでグループに追加できます。

   ユーザーが複数のグループに属している場合、権限は累積されます。見る"管理者グループの管理"詳細については。

2. *ユーザーの作成*を選択し、*完了*を選択します。

ローカルユーザーの表示と編集

既存のローカル ユーザーとフェデレーション ユーザーの詳細を表示できます。ローカル ユーザーを変更して、ユーザーのフルネーム、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、ユーザーが Grid Manager および Grid Management API にアクセスできないように一時的に設定することもできます。

編集できるのはローカル ユーザーのみです。外部 ID ソースを使用してフェデレーション ユーザーを管理します。

- すべてのローカル ユーザーとフェデレーション ユーザーの基本情報を表示するには、[ユーザー] ページの表を確認します。

- 特定のユーザーの詳細をすべて表示したり、ローカル ユーザーを編集したり、ローカル ユーザーのパスワードを変更したりするには、[アクション] メニューまたは詳細ページを使用します。

  編集内容は、ユーザーが次回グリッド マネージャーからサインアウトし、再度サインインしたときに適用されます。

  > ローカル ユーザーは、Grid Manager バナーの パスワードの変更 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。

Task	[操作]メニュー	詳細ページ
ユーザーの詳細を表示	a. ユーザー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。	表からユーザーの名前を選択します。
フルネームを編集する（ローカルユーザーのみ）	a. ユーザー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てください。 d. *変更を保存*を選択します。	a. 詳細を表示するには、ユーザーの名前を選択します。 b. 編集アイコンを選択。 c. 新しい名前を入力してください。 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する	a. ユーザー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. ユーザーが Grid Manager または Grid Management API にサインインできないようにするには [はい] を選択し、ユーザーがサインインできるようにするには [いいえ] を選択します。 e. *変更を保存*を選択します。	a. 詳細を表示するには、ユーザーの名前を選択します。 b. [アクセス]タブを選択します。 c. ユーザーが Grid Manager または Grid Management API にサインインできないようにするには [はい] を選択し、ユーザーがサインインできるようにするには [いいえ] を選択します。 d. *変更を保存*を選択します。
パスワードの変更（ローカルユーザーのみ）	a. ユーザー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. 詳細を表示するには、ユーザー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。

Task	[操作]メニュー	詳細ページ
グループの変更（ローカルユーザーのみ）	a. ユーザー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、グループ名の後のリンクを選択して、新しいブラウザ タブでグループの詳細を表示します。 e. 別のグループを選択するには、「グループの編集」を選択します。 f. *変更を保存*を選択します。	a. 詳細を表示するには、ユーザー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、グループ名の後のリンクを選択して、新しいブラウザ タブでグループの詳細を表示します。 d. 別のグループを選択するには、「グループの編集」を選択します。 e. *変更を保存*を選択します。

ユーザーを複製する

既存のユーザーを複製して、同じ権限を持つ新しいユーザーを作成できます。

手順

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

ユーザーを削除する

ローカル ユーザーを削除すると、そのユーザーをシステムから完全に削除できます。

ルートユーザーを削除することはできません。

手順

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選択します。
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

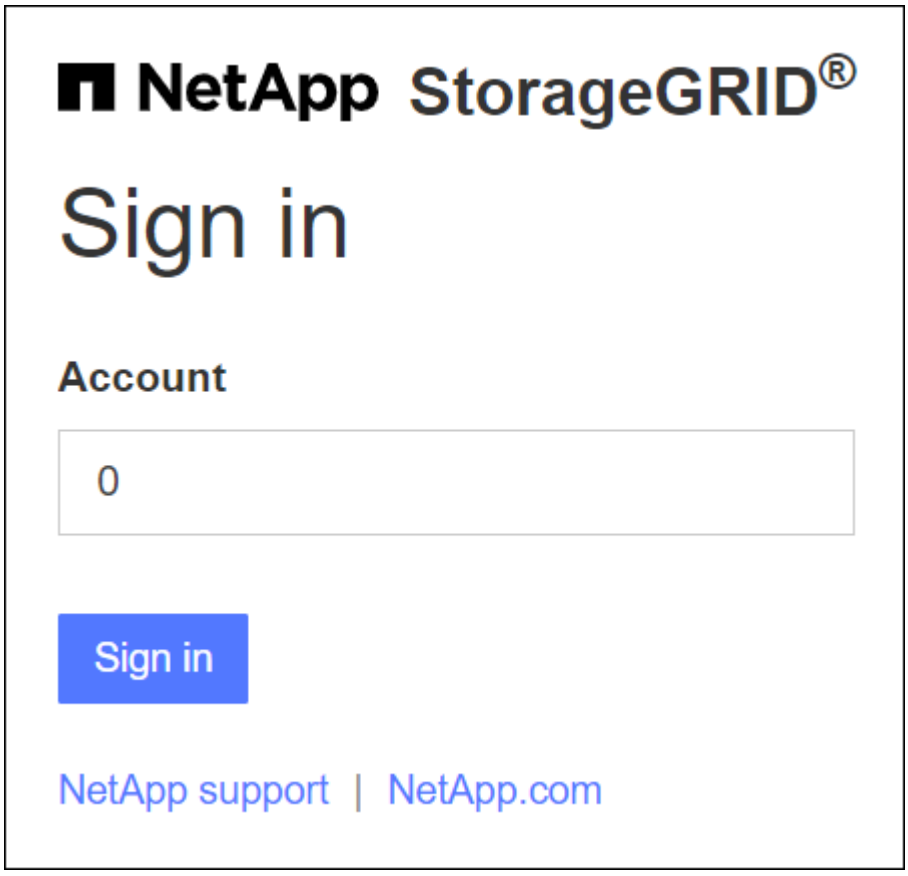
SSO が有効になっているときにStorageGRIDにサインインすると、資格情報を検証するために組織の SSO ページにリダイレクトされます。

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。

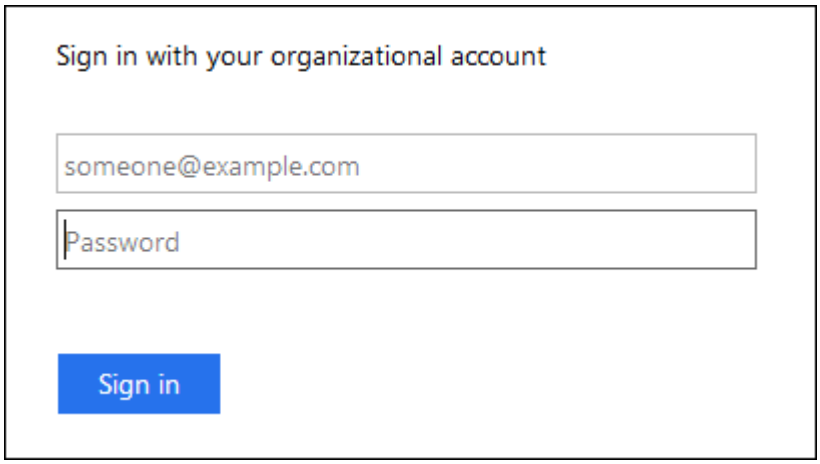


   - 以前に Grid Manager または Tenant Manager にアクセスしたことがある場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。

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。

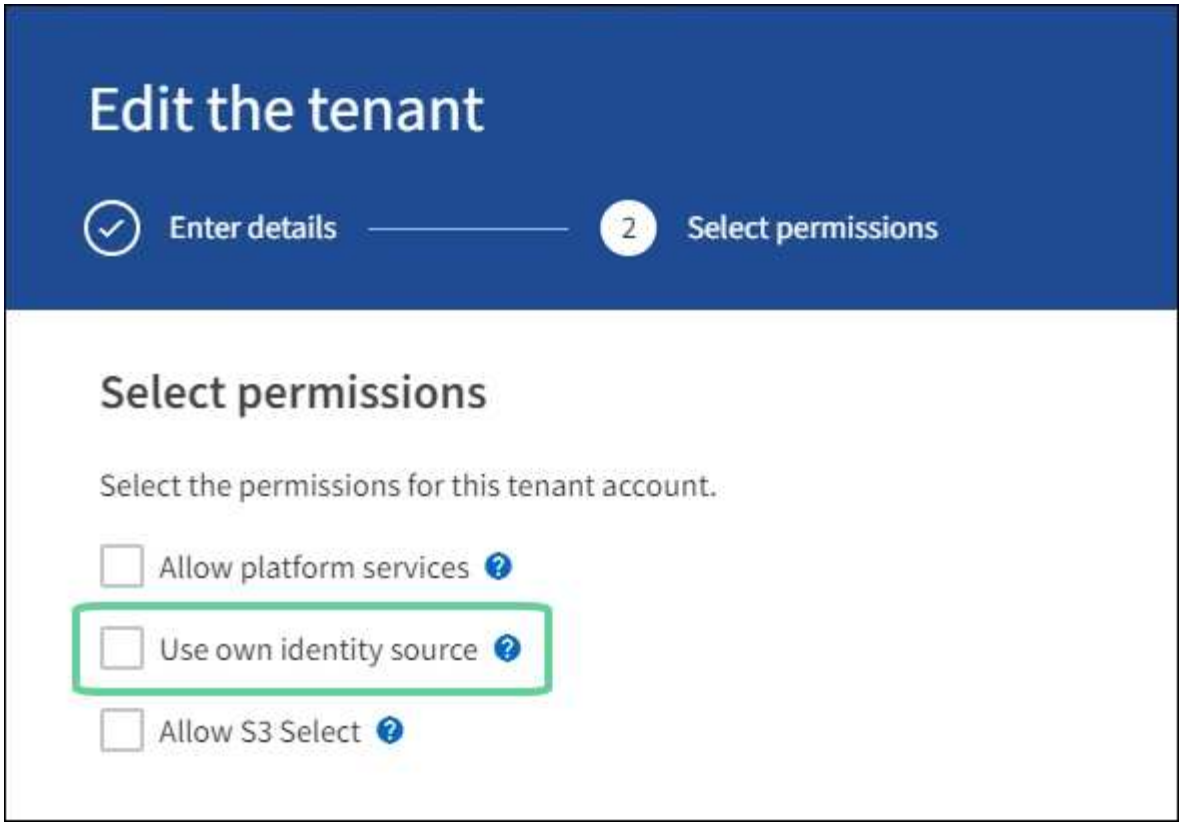
手順

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。

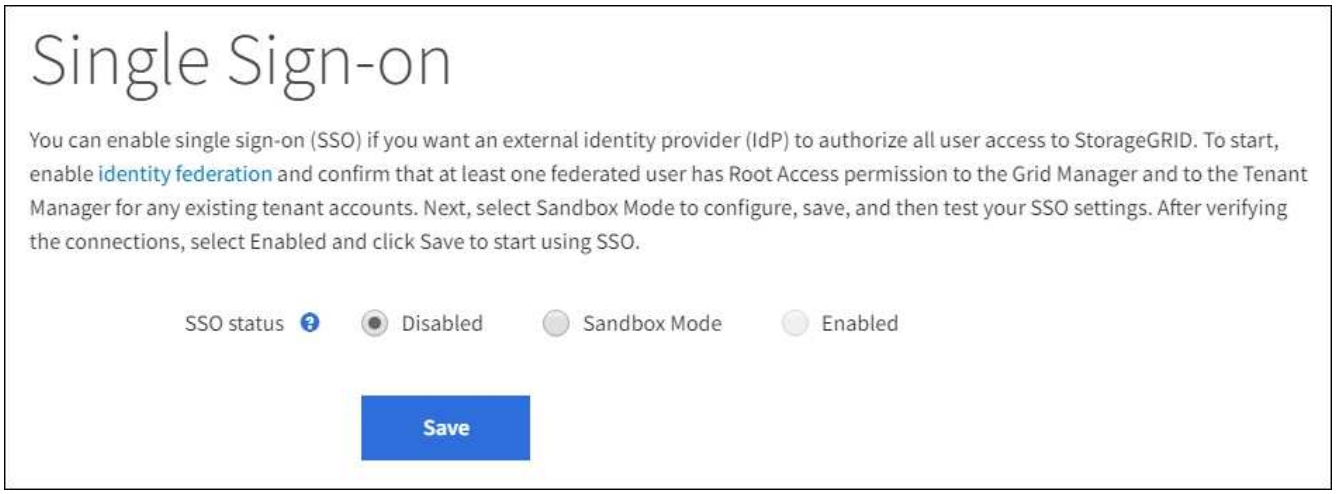
サンドボックス モードを使用すると、この双方向の構成を簡単に実行でき、SSO を有効にする前にすべての設定をテストできます。サンドボックス モードを使用している場合、ユーザーは SSO を使用してサインインできません。

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

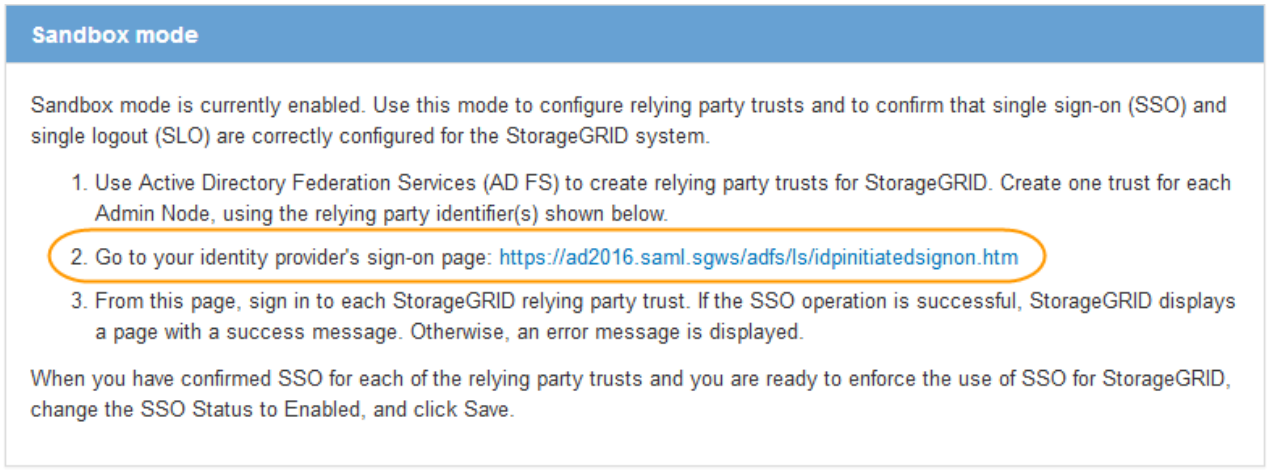
StorageGRIDシステム全体にシングル サインオンの使用を強制する前に、各管理ノードに対してシングル サインオンとシングル ログアウトが正しく設定されていることを確認する必要があります。

Active Directory

手順

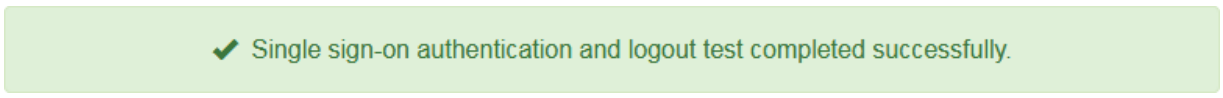
1. StorageGRIDシングル サインオン ページで、サンドボックス モード メッセージ内のリンクを見つけます。

   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.

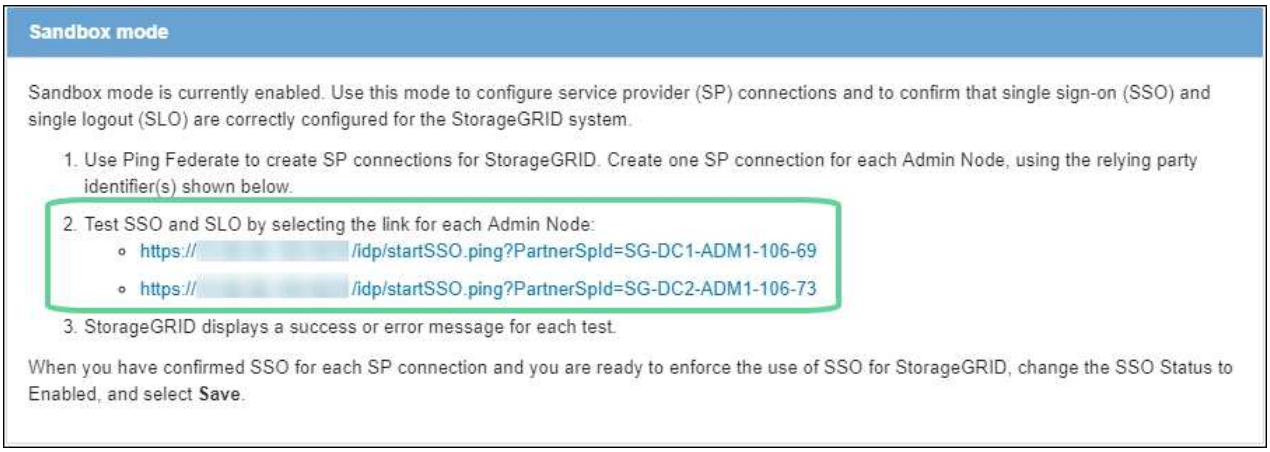
   - SSO 操作が失敗した場合、エラー メッセージが表示されます。問題を修正し、ブラウザの Cookie をクリアして、もう一度お試しください。
4. これらの手順を繰り返して、グリッド内の各管理ノードの SSO 接続を確認します。

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_reference_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