



StorageGRID にシングルサインオン (SSO) を使用する

StorageGRID 11.5

NetApp
April 11, 2024

目次

StorageGRID にシングルサインオン (SSO) を使用する	1
シングルサインオンの仕組み	1
シングルサインオンの使用要件	3
シングルサインオンを設定しています	4

StorageGRID にシングルサインオン (SSO) を使用する

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。SSO が有効な場合は、Grid Manager、Tenant Manager、Grid 管理 API、またはテナント管理 API にアクセスするすべてのユーザを外部のアイデンティティプロバイダによって認証する必要があります。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"
- "シングルサインオンの使用要件"
- "シングルサインオンを設定しています"

シングルサインオンの仕組み

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

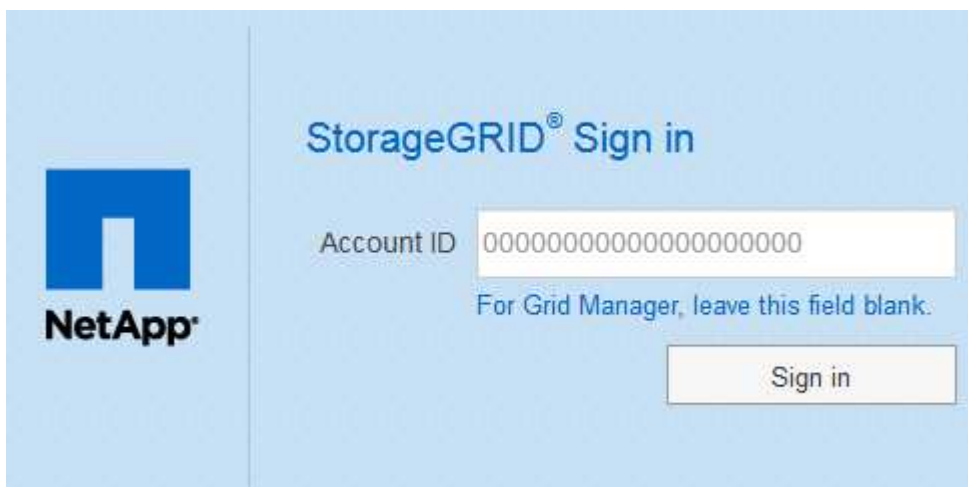
SSO が有効な場合に StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。

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。

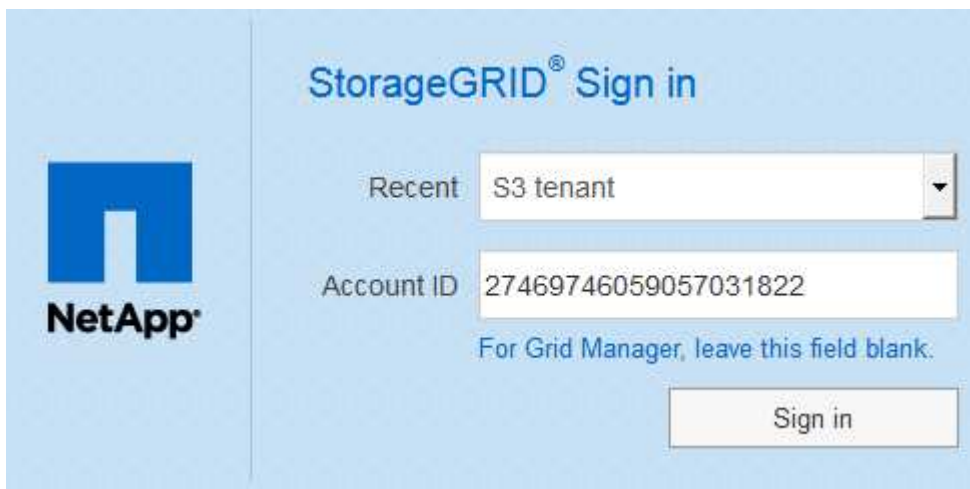
StorageGRID のサインインページが表示されます。

- 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。

A screenshot of the StorageGRID Sign in page. On the left is the NetApp logo. The main content area has the title "StorageGRID® Sign in". Below the title is a form with a label "Account ID" and a text input field containing "00000000000000000000". Below the input field is the text "For Grid Manager, leave this field blank." At the bottom right of the form is a "Sign in" button.

- 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。



The image shows the StorageGRID Sign in page. On the left is the NetApp logo. The main heading is "StorageGRID® Sign in". Below the heading, there is a "Recent" dropdown menu with "S3 tenant" selected. Below that is an "Account ID" text input field containing "27469746059057031822". Underneath the input field is the text "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.



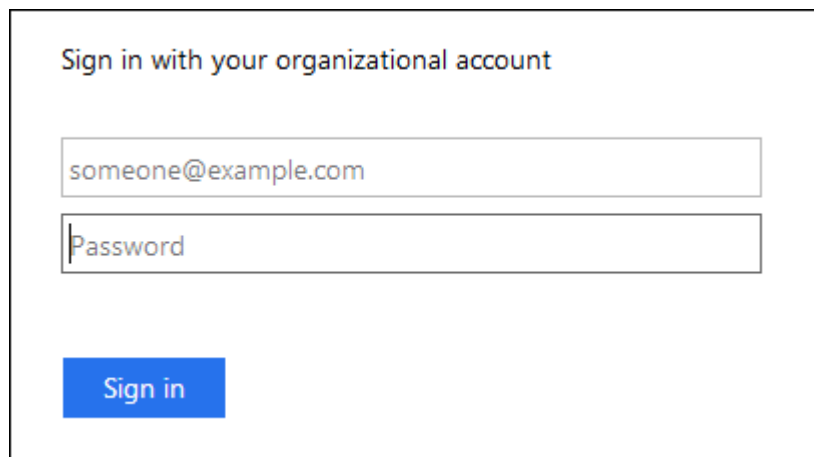
テナントアカウントの完全なURL（完全修飾ドメイン名またはIPアドレスのあとにを追加したもの）を入力すると、StorageGRID のサインインページは表示されません（/?accountId=20-digit-account-id）。代わりに、組織の SSO サインインページがすぐに表示されます。このページでは、を実行できます [SSO クレデンシャルを使用してサインイン](#) します。

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** (アカウントID *)]フィールドを空白のままにします。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「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]をクリックします

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：



The image shows a sign-in form titled "Sign in with your organizational account". It has two input fields: the first contains "someone@example.com" and the second is labeled "Password". Below the fields is a blue "Sign in" button.

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

SSO クレデンシャルを再入力する必要はありません。

SSOが有効な場合はサインアウトします

StorageGRID で SSO が有効になっている場合にサインアウトするとどうなるかは、サインイン先とサインアウト元によって異なります。

手順

1. ユーザインターフェイスの右上隅にある **[Sign Out]** リンクを探します。
2. [サインアウト]をクリックします。

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
1つ以上の管理ノード上の Tenant Manager	任意の管理ノード上の Tenant Manager	すべての管理ノード上の Tenant Manager
Grid Manager と Tenant Manager の両方	Grid Manager の略	Grid Manager のみ。SSO からサインアウトするには、Tenant Manager からもサインアウトする必要があります。



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

シングルサインオンの使用要件

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



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。

アイデンティティプロバイダの要件

SSOのアイデンティティプロバイダ（IdP）は、次の要件を満たしている必要があります。

- 次のいずれかのバージョンのActive Directoryフェデレーションサービス（AD FS）
 - AD FS 4.0はWindows Server 2016に付属しています



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

- AD FS 3.0（Windows Server 2012 R2 Update 以降に付属）。
- Transport Layer Security（TLS）1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以降

サーバ証明書の要件

StorageGRID は、各管理ノード上の管理インターフェイスのサーバ証明書を使用して、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。AD FS でStorageGRID 用にSSOの証明書利用者信頼を設定する際には、このサーバ証明書をAD FSへのStorageGRID 要求の署名証明書として使用します。

管理インターフェイス用のカスタムサーバ証明書をまだインストールしていない場合は、インストールしてください。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AD FSの証明書利用者信頼に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、AD FSの証明書利用者信頼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 `custom-server.crt`。ノードのデフォルトサーバ証明書の名前は `server.crt`。

関連情報

["ファイアウォールによるアクセス制御"](#)

["Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する"](#)

シングルサインオンを設定しています

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。

- "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ておく"
- "サンドボックスモードの使用"
- "AD FSでの証明書利用者信頼の作成"
- "証明書利用者信頼のテスト"
- "シングルサインオンの有効化"
- "シングルサインオンを無効にしています"
- "1つの管理ノードのシングルサインオンの一時的な無効化と再有効化"

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ておく

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- Active Directoryをフェデレーテッドアイデンティティソースとして使用し、AD FSをアイデンティティプロバイダとして使用している。

"シングルサインオンの使用要件"

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. アクセス制御* アイデンティティフェデレーション*を選択します。
 - c. [アイデンティティフェデレーションを有効にする] チェックボックスがオフになっていることを確認します。
 - d. その場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になっていることを確認し、チェックボックスをオフにして*保存*をクリックします。
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 Access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、Root Access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、*アカウントの編集*をクリックします。
 - c. [独自のアイデンティティソースを使用する*]チェックボックスがオンになっている場合は、チェックボックスをオフにして、[保存*]をクリックします。

Edit Tenant Account

Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional) GB ▼

Cancel Save

Tenant Accounts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*をクリックして、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 Control > Groups *をクリックします。
- 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用のRoot Access権限が割り当てられていることを確認します。
- d. サインアウトします。
- e. フェデレーテッドグループ内のユーザとしてテナントに再度サインインできることを確認します。

関連情報

["シングルサインオンの使用要件"](#)

["管理者グループの管理"](#)

["テナントアカウントを使用する"](#)

サンドボックスモードの使用

サンドボックスモードを使用すると、StorageGRID ユーザにシングルサインオン (SSO) を適用する前に、Active Directory フェデレーションサービス (AD FS) の証明書利用者信頼を設定およびテストできます。SSOを有効にしたあとにサンドボックスモードを再度有効にすると、新規および既存の証明書利用者信頼を設定またはテストできます。サンドボックスモードを再度有効にすると、StorageGRID ユーザーのSSOは一時的に無効に

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

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、StorageGRID からAD FSに認証要求が送信されます。次に、AD FS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。要求が成功した場合、応答にはユーザのUniversally Unique Identifier (UUID) が含まれます。

StorageGRID (サービスプロバイダ) とAD FS (アイデンティティプロバイダ) がユーザの認証要求を安全にやり取り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、AD FSを使用して、管理ノードごとに証明書利用者信頼を作成します。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は使用することを推奨しますが、必須ではありません。StorageGRID でSSOを設定した直後にAD FSの証明書利用者信頼を作成する準備ができている場合は、また、管理ノードごとにSSOプロセスとシングルログアウト (SLO) プロセスをテストする必要はありません。* enabled をクリックし、**StorageGRID** 設定を入力して、**AD FS**内の管理ノードごとに証明書利用者信頼を作成し、Save *をクリックしてSSOを有効にします。

手順

1. 「* Configuration * Access Control * Single Sign-On *」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。

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Save



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

2. [サンドボックスモード]オプションを選択します。

アイデンティティプロバイダと証明書利用者の設定が表示されます。[アイデンティティプロバイダ] セクションでは、[サービスタイプ] フィールドは読み取り専用です。ここには、使用しているアイデンティティフェデレーションサービスのタイプ (Active Directoryなど) が表示されます。

3. アイデンティティプロバイダセクションで、次の手順を実行します。

a. フェデレーションサービス名を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。

b. 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、Transport Layer Security (TLS) を使用して接続を保護するかどうかを指定します。

- * 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、証明書を* CA証明書*テキストボックスにコピーして貼り付けます。

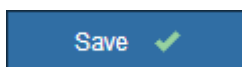
- * Do not use TLS* : TLS 証明書を使用して接続を保護しないでください。

4. 証明書利用者セクションで、StorageGRID 管理ノードに使用する証明書利用者信頼を設定するときに使用する証明書利用者IDを指定します。

- 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、管理ノードのホスト名に基づいて、各管理ノードの証明書利用者IDを含むテーブルが生成されます。+注: 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。

5. [保存 (Save)] をクリックします。

- 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。



- サンドボックスモードの確認メッセージが表示され、サンドボックスモードが有効になっていることが確認されます。AD FSの使用時にもこのモードを使用して、管理ノードごとに証明書利用者信頼を設定し、シングルサインイン (SSO) プロセスとシングルログアウト (SLO) プロセスをテストできます。

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Sandbox mode

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

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

関連情報

["シングルサインオンの使用要件"](#)

AD FSでの証明書利用者信頼の作成

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。

Windows PowerShellを使用した証明書利用者信頼の作成

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。

必要なもの

- StorageGRID でSSOを設定し、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。



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。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0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。

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_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)]をクリックし、[OK]をクリックします

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. [ルール追加]をクリックします。
- 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] をクリックします。
- e. [ルールの設定] ページで、このルールの表示名を入力します。

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

- f. 属性ストアで、* Active Directory * を選択します。
- g. マッピングテーブルの LDAP 属性列に、* objectGUID * と入力します。
- h. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

- i. [完了]をクリックし、[OK]をクリックします。
7. メタデータが正常にインポートされたことを確認します。
 - a. 証明書利用者信頼を右クリックしてプロパティを開きます。
 - b. **[Endpoints]**、**[*Identifiers]**、および **[Signature]** タブのフィールドに値が入力されていることを確認します。

メタデータがない場合は、フェデレーションメタデータアドレスが正しいことを確認するか、値を手動で入力します。
 8. 上記の手順を繰り返して、StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
 9. 完了したら、StorageGRID およびに戻ります **"すべての証明書利用者信頼をテストします"** 正しく設定されていることを確認します。

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。

必要なもの

- StorageGRID でSSOを設定し、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。



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。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0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。

手順

1. Windows Server Managerで、* Tools をクリックし、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) *をクリックします。
3. [ようこそ]ページで、[クレーム対応]を選択し、[開始]をクリックします。
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. [ルール追加:] をクリックします。
 - 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] をクリックします。
 - d. [ルール設定] ページで、このルールの表示名を入力します。

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

- e. 属性ストアで、* Active Directory * を選択します。
 - f. マッピングテーブルの LDAP 属性列に、* objectGUID * と入力します。
 - g. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
 - h. [完了] をクリックし、[OK] をクリックします。
8. メタデータが正常にインポートされたことを確認します。
 - a. 証明書利用者信頼を右クリックしてプロパティを開きます。
 - b. [Endpoints]、[*Identifiers]、および [Signature] タブのフィールドに値が入力されていることを確認します。

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

9. 上記の手順を繰り返して、StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
10. 完了したら、StorageGRID およびに戻ります **"すべての証明書利用者信頼をテストします"** 正しく設定されていることを確認します。

証明書利用者信頼の手動作成

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。

必要なもの

- StorageGRID でSSOを設定し、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。



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。

- 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しておきます。または、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。
- 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。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0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。

手順

1. Windows Server Managerで、* Tools をクリックし、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) *をクリックします。
3. [ようこそ]ページで、[クレーム対応]を選択し、[開始]をクリックします。
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]をクリックします。
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] をクリックします。
 - 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] をクリックします。
 - b. [ルールの設定] ページで、このルールの表示名を入力します。

たとえば、**ObjectGUID to Name ID** と入力します。
 - c. 属性ストアで、*Active Directory* を選択します。
 - d. マッピングテーブルのLDAP属性列に、*objectGUID* と入力します。
 - e. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから *名前 ID* を選択します。
 - f. [完了] をクリックし、[OK] をクリックします。

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の追加* をクリックします。
- 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] をクリックします。

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進みます `/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)] をクリックし、[OK] をクリックします。

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 およびに戻ります **"すべての証明書利用者信頼をテストします"** 正しく設定されていることを確認します。

証明書利用者信頼のテスト

StorageGRID に対するシングルサインオン (SSO) の使用を適用する前に、シングルサインオンとシングルログアウト (SLO) が正しく設定されていることを確認します。管理ノードごとに証明書利用者信頼を作成した場合は、管理ノードごとにSSOとSLOを使用できることを確認します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- AD FSに1つ以上の証明書利用者信頼を設定しておきます。

手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

[シングルサインオン]ページが表示され、[サンドボックスモード]オプションが選択されます。

2. サンドボックスモードの手順で、アイデンティティプロバイダのサインオンページへのリンクを探します。

このURLは、[**Federated Service Name**]フィールドに入力した値から取得されます。

Sandbox mode

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

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. リンクをクリックするか、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。
4. 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*をクリックします。

You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

ユーザ名とパスワードの入力を求めるプロンプトが表示されます。

5. 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。

✔ 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。
6. 上記の手順を繰り返して、他のすべての管理ノードにサインインできることを確認します。

すべてのSSOサインインおよびログアウト処理が成功したら、SSOを有効にすることができます。

シングルサインオンの有効化

サンドボックスモードを使用してすべてのStorageGRID 証明書利用者信頼をテストしたら、シングルサインオン（SSO）を有効にすることができます。

必要なもの

- 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をインポートして、そのグループにRoot Access管理権限を割り当てておく必要があります。既存のテナントアカウントに対して、少なくとも1人のフェデレーテッドユーザがGrid ManagerとTenant ManagerへのRoot Access権限を持っていることを確認する必要があります。
- サンドボックスモードを使用して、すべての証明書利用者信頼をテストしておく必要があります。

手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

[シングルサインオン]ページが開き、[サンドボックスモード]が選択されます。

2. SSO ステータスを * Enabled * に変更します。
3. [保存 (Save)]をクリックします。

警告メッセージが表示されます。

⚠ Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. 警告を確認し、* OK *をクリックします。

シングルサインオンが有効になりました。



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。

シングルサインオンを無効にしています

不要になった場合はシングルサインオン（SSO）を無効にすることができます。アイデンティティフェデレーションを無効にする場合は、事前にシングルサインオンを無効にする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「* Configuration * Access Control * Single Sign-On *」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)] をクリックします。

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。

⚠ Warning

Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel

OK

4. [OK] をクリックします。

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の一時的な無効化と再有効化

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

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります 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く必要があります。

このタスクについて

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



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

手順

1. 管理ノードにログインします。
 - a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
 - b. 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. 「* Configuration * Access Control * Single Sign-On *」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)] をクリックします。

シングルサインオンページで * Save * をクリックすると、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] をクリックして、Grid Manager を閉じます。

c. 管理ノードで SSO を再度有効にします。次のいずれかの手順を実行します。

▪ 次のコマンドを実行します。 `enable-saml`

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

SSO を有効にすることを確認します。

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

◦ 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。

関連情報

["シングルサインオンを設定しています"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。