SAMLを使用

SANtricity 11.8

NetApp
December 16, 2024

目次

SAMLを使用

SAMLの設定

アクセス管理用の認証を設定するには、ストレージアレイに組み込みのSecurity Assertion Markup Language（SAML）機能を使用できます。この設定により、アイデンティティプロバイダとストレージプロバイダの間の接続が確立されます。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ストレージアレイのコントローラのIPアドレスまたはドメイン名を確認しておく必要があります。
- IdP管理者がIdPシステムの設定を完了している必要があります。
- IdP管理者が、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。
- IdPサーバとコントローラのクロックが同期されていることを確認しておきます（NTPサーバを使用するかコントローラのクロックの設定を調整します）。
- IdPのメタデータファイルをIdPシステムからダウンロードし、Unified Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。

タスクの内容

アイデンティティプロバイダ（IdP）は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証を提供し、Active Directoryなどの任意のユーザデータベースを使用するようにIdPを設定できます。IdPの保守はセキュリティチームが行います。サービスプロバイダ（SP）は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLが設定されている場合、ストレージアレイはアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。IdPとストレージアレイの間の接続を確立するには、この2つのエンティティ間でメタデータファイルを共有します。次に、IdPのユーザエンティティをストレージアレイのロールにマッピングします。最後に、接続とSSOログインをテストしたうえでSAMLを有効にします。

- SAMLとディレクトリサービス*。認証方式としてディレクトリサービスを設定している場合にSAMLを有効にすると、Unified ManagerではSAMLがディレクトリサービスよりも優先されます。SAMLをあとで無効にすると、ディレクトリサービスの設定は以前の設定に戻ります。

*編集と無効化。*SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

SAML認証の設定は複数の手順で構成されます。

手順1：IdPのメタデータファイルをアップロードする

ストレージアレイにIdPの接続情報を提供するには、Unified ManagerにIdPメタデータをインポートします。このメタデータは、IdPシステムが認証要求を正しいURLにリダイレクトし、受信した応答を検証するために必要です。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。

   設定手順の概要が表示されます。

3. アイデンティティプロバイダ（IdP）ファイルのインポート*リンクをクリックします。

   [Import Identity Provider File]ダイアログボックスが開きます。

4. Browse *をクリックして、ローカルシステムにコピーしたIdPメタデータファイルを選択してアップロードします。

   ファイルを選択すると、IdPのエンティティIDが表示されます。

5. [* インポート *] をクリックします。

手順2：サービスプロバイダのファイルをエクスポートする

IdPとストレージアレイの間の信頼関係を確立するには、サービスプロバイダのメタデータをIdPにインポートします。このメタデータは、IdPがコントローラとの信頼関係を確立し、許可要求を処理するために必要です。このファイルには、IdPがサービスプロバイダと通信できるように、コントローラのドメイン名やIPアドレスなどの情報が含まれています。

手順

1. [サービスプロバイダファイルのエクスポート*]リンクをクリックします。

   [サービスプロバイダファイルのエクスポート]ダイアログボックスが開きます。

2. コントローラのIPアドレスまたはDNS名を[*コントローラA *]フィールドに入力し、[*エクスポート]をクリックしてメタデータファイルをローカルシステムに保存します。

   「* Export」をクリックすると、サービスプロバイダのメタデータがローカルシステムにダウンロードされます。ファイルが保存されている場所をメモします。

3. ローカルシステムで、エクスポートしたXML形式のサービスプロバイダメタデータファイルを探します。
4. IdPサーバから、サービスプロバイダのメタデータファイルをインポートして信頼関係を確立します。ファイルを直接インポートすることも、ファイルからコントローラ情報を手動で入力することもできます。

手順3：ロールをマッピングする

Unified Managerへのアクセスをユーザに許可するには、IdPユーザの属性とグループメンバーシップをストレージアレイの事前定義されたロールにマッピングする必要があります。

開始する前に

- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- IdPのメタデータファイルをUnified Managerにインポートします。
- コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。

手順

1. 「mapping Unified Manager * roles」のリンクをクリックします。

   ロールマッピング(Role Mapping)ダイアログボックスが開きます

2. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。

フィールドの詳細

設定	製品説明
マッピング	ユーザ属性
マッピングするSAMLグループの属性（「member of」など）を指定します。	属性値
マッピングするグループの属性値を指定します。正規表現がサポートされています。(\`正規表現パターンに含まれていない特殊な正規表現文字は、バックスラッシュでエスケープする必要があります。\.[]{}()<>*+-=!?^$	
役割	フィールド内をクリックし、属性にマッピングするストレージアレイのロールを1つ選択します。含めるロールをそれぞれ個別に選択する必要があります。MonitorロールはUnified Managerにログインするために必要な他のロールと一緒に指定する必要があります。少なくとも1つのグループにはSecurity Adminロールも必要です。 各ロールの権限は次のとおりです。 • * Storage admin *--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。 • * Security admin *--アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMbol）のオン/オフの切り替え機能。 • * Support admin *--ストレージアレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。 • *Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。

Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

3. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。

ロールのマッピングは、SAMLを有効にしたあとに変更できます。

4. マッピングが終了したら、*保存*をクリックします。

手順4：SSOログインをテストする

IdPシステムとストレージアレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

開始する前に

- IdPのメタデータファイルをUnified Managerにインポートします。
- コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。

手順

1. [Test SSO Login*]リンクを選択します。

   SSOクレデンシャルを入力するためのダイアログボックスが開きます。

2. Security AdminとMonitorの両方の権限を持つユーザのログインクレデンシャルを入力します。

   ログインのテスト中は、ダイアログボックスが開きます。

3. テストに成功したことを示すメッセージを確認します。テストに成功した場合は、SAMLを有効にする次の手順に進みます。

   テストが正常に完了しなかった場合は、エラーメッセージと詳細情報が表示されます。次の点を確認してください。

   - ユーザがSecurity AdminとMonitorの権限を持つグループに属していること。
   - アップロードしたIdPサーバのメタデータが正しいこと。
   - SPメタデータファイル内のコントローラアドレスが正しい。

手順5：SAMLを有効にする

最後に、ユーザ認証用のSAMLの設定を完了します。このプロセスでは、SSOログインのテストも求められます。SSOログインのテストプロセスについては、前の手順で説明しています。

開始する前に

- IdPのメタデータファイルをUnified Managerにインポートします。
- コントローラのサービスプロバイダメタデータファイルが、信頼関係のIdPシステムにインポートされている。
- 少なくともMonitorロールとSecurity Adminロールを1つずつマッピングしておきます。

*編集と無効化。*SAMLを有効にすると、ユーザインターフェイスで無効にしたり、IdP設定を編集したりすることはできなくなります。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

手順

1. [* SAML]タブで、[SAMLを有効にする]リンクを選択します。

   [SAMLの有効化の確認]ダイアログボックスが開きます。

2. と入力し `enable`、*[有効化]*をクリックします。
3. SSOログインテスト用のユーザクレデンシャルを入力します。

結果

SAMLが有効になると、アクティブなセッションはすべて終了され、SAMLを使用したユーザの認証が開始されます。

SAMLロールマッピングの変更

アクセス管理用にSAMLを設定している場合は、IdPグループとストレージアレイの事前定義されたロールの間のロールマッピングを変更できます。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- SAMLを設定して有効にします。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。
3. [役割のマッピング]を選択します。

   ロールマッピング(Role Mapping)ダイアログボックスが開きます

4. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。

   SAMLが有効になっている間は権限を削除しないように注意してください。削除すると、Unified Managerにアクセスできなくなります。

フィールドの詳細

設定	製品説明
マッピング	ユーザ属性
マッピングするSAMLグループの属性（「member of」など）を指定します。	属性値
マッピングするグループの属性値を指定します。	役割

Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールが割り当てられていないユーザのUnified Managerは正しく動作しません。

5. 必要に応じて、* Add another mapping *をクリックして、グループとロールのマッピングをさらに入力します。
6. [保存（ Save ）] をクリックします。

結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザーセッションのみが保持されます。

SAMLサービスプロバイダファイルのエクスポート

必要に応じて、ストレージアレイのサービスプロバイダメタデータをエクスポートし、そのファイルをアイデンティティプロバイダ（IdP）システムに再インポートできます。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- SAMLを設定して有効にします。

タスクの内容

このタスクでは、コントローラからメタデータをエクスポートします。このメタデータは、IdPがコントローラとの信頼関係を確立し、認証要求を処理するために必要です。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPで要求の送信に使用できる情報が含まれています。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。
3. 「書き出し」を選択します。

[サービスプロバイダファイルのエクスポート]ダイアログボックスが開きます。

4. [エクスポート]*をクリックして、メタデータファイルをローカルシステムに保存します。

   ドメイン名フィールドは読み取り専用です。

   ファイルが保存されている場所をメモします。

5. ローカルシステムで、エクスポートしたXML形式のサービスプロバイダメタデータファイルを探します。
6. IdPサーバから、サービスプロバイダのメタデータファイルをインポートします。ファイルを直接インポートすることも、コントローラ情報を手動で入力することもできます。
7. [* 閉じる *] をクリックします。

著作権に関する情報

商標に関する情報