SAML 認証の設定を管理する

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目次

SAML 認証の設定を管理する

リモート認証の設定が完了したら、 Security Assertion Markup Language （ SAML ）認証を有効にして、 Unified Manager の Web UI にアクセスするリモートユーザをセキュアなアイデンティティプロバイダ（ IdP ）で認証するように設定できます。

SAML 認証を有効にしたあとで Unified Manager のグラフィカルユーザインターフェイスにアクセスできるのはリモートユーザのみです。ローカルユーザとメンテナンスユーザは UI にアクセスできません。この設定は、メンテナンスコンソールにアクセスするユーザには影響しません。

アイデンティティプロバイダの要件

すべてのリモートユーザについてアイデンティティプロバイダ（ IdP ）を使用して SAML 認証を実行するように Unified Manager で設定するときは、 Unified Manager に正しく接続できるように、いくつかの必要な設定を確認しておく必要があります。

Unified Manager の URI とメタデータを IdP サーバに入力する必要があります。この情報は、 Unified Manager の SAML 認証ページからコピーできます。Unified Manager は、 Security Assertion Markup Language （ SAML ）標準のサービスプロバイダ（ SP ）とみなされます。

サポートされている暗号化標準

- Advanced Encryption Standard （ AES ）： AES-128 および AES-256
- Secure Hash Algorithm （ SHA ）： SHA-1 および SHA-256

検証済みのアイデンティティプロバイダ

- Shibboleth
- Active Directory フェデレーションサービス（ ADFS ）

ADFS の設定要件

- 3 つの要求ルールを次の順序で定義する必要があります。これらは、この証明書利用者信頼エントリに対する ADFS SAML 応答を Unified Manager で解析するために必要です。

要求規則	価値
Sam - アカウント名	名前 ID
Sam - アカウント名	urn ： OID ： 0.9.2342.19200300.100.1.1
トークングループ — 修飾されていない名前	urn ： OID ： 1.3.6.1.4.1.5923.1.5.1.1

- 認証方法を「フォーム認証」に設定する必要があります。設定しないと、 Unified Manager からログアウトするときにユーザにエラーが表示されることがあります。次の手順を実行します。

a. ADFS 管理コンソールを開きます。

b. 左側のツリー・ビューで [Authentication Policies] フォルダをクリックします

c. 右の [アクション] で、 [グローバルプライマリ認証ポリシーの編集] をクリックします。

d. イントラネット認証方式をデフォルトの「 Windows 認証」ではなく「フォーム認証」に設定します。

- Unified Manager のセキュリティ証明書が CA 署名証明書の場合、 IdP 経由でのログインが拒否されることがあります。この問題を解決する方法は 2 つあります。
  - 次のリンクの手順に従って、 CA 証明書チェーンの関連する証明書利用者についての ADFS サーバでの失効チェックを無効にします。

    "証明書利用者信頼ごとの失効チェックを無効にします"

  - ADFS サーバ内にある CA サーバで Unified Manager サーバ証明書要求に署名します。

その他の設定要件

- Unified Manager のクロックスキューは 5 分に設定されているため、 IdP サーバと Unified Manager サーバの時間の差が 5 分を超えないようにします。時間の差が 5 分を超えると認証が失敗します。

SAML 認証の有効化

Security Assertion Markup Language （ SAML ）認証を有効にして、 Unified Manager の Web UI にアクセスするリモートユーザをセキュアなアイデンティティプロバイダ（ IdP ）で認証するように設定できます。

- 必要なもの *
- リモート認証を設定し、正常に実行されることを確認しておく必要があります。
- アプリケーション管理者ロールが割り当てられたリモートユーザまたはリモートグループを少なくとも 1 つ作成しておく必要があります。
- アイデンティティプロバイダ（ IdP ）が Unified Manager でサポートされ、設定が完了している必要があります。
- IdP の URL とメタデータが必要です。
- IdP サーバへのアクセスが必要です。

Unified Manager で SAML 認証を有効にしたあと、 Unified Manager サーバのホスト情報を使用して IdP を設定するまでは、ユーザはグラフィカルユーザインターフェイスにアクセスできません。そのため、設定プロセスを開始する前に、両方の接続を完了できるように準備しておく必要があります。IdP の設定は、 Unified Manager の設定前にも設定後にも実行できます。

SAML 認証を有効にしたあとで Unified Manager のグラフィカルユーザインターフェイスにアクセスできるのはリモートユーザのみです。ローカルユーザとメンテナンスユーザは UI にアクセスできません。この設定は、メンテナンスコンソール、 Unified Manager コマンド、 ZAPI にアクセスするユーザには影響しません。

このページで SAML の設定を完了すると、 Unified Manager が自動的に再起動されます。

手順

1. 左側のナビゲーションペインで、 * General * > * SAML Authentication * をクリックします。
2. Enable SAML authentication * チェックボックスをオンにします。

   IdP の接続の設定に必要なフィールドが表示されます。

3. IdP の URI と Unified Manager サーバを IdP に接続するために必要な IdP メタデータを入力します。

   IdP サーバに Unified Manager サーバから直接アクセスできる場合は、 IdP の URI を入力したあとに「 * IdP メタデータの取得」ボタンをクリックすると、 IdP のメタデータフィールドに自動的に値が入力されます。

4. Unified Manager のホストメタデータ URI をコピーするか、メタデータを XML テキストファイルに保存します。

   この情報を使用して IdP サーバを設定できます。

5. [保存（ Save ）] をクリックします。

   設定を完了して Unified Manager を再起動するかどうかの確認を求めるメッセージボックスが表示されます。

6. [確認してログアウト *] をクリックすると、 Unified Manager が再起動します。

許可されたリモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から Unified Manager のログインページではなく IdP のログインページに変わります。

まだ完了していない場合は、 IdP にアクセスし、 Unified Manager サーバの URI とメタデータを入力して設定を完了します。

アイデンティティプロバイダに ADFS を使用している場合は、 Unified Manager GUI で ADFS のタイムアウトが考慮されず、 Unified Manager のセッションタイムアウトに達するまでセッションが続行されます。GUI セッションのタイムアウトを変更するには、 * General * > * Feature Settings * > * Inactivity Timeout * をクリックします。

SAML 認証に使用するアイデンティティプロバイダを変更する

Unified Manager でリモートユーザの認証に使用するアイデンティティプロバイダ（ IdP ）を変更することができます。

- 必要なもの *
- IdP の URL とメタデータが必要です。
- IdP へのアクセスが必要です。

新しい IdP の設定は、 Unified Manager の設定前にも設定後にも実行できます。

手順

1. 左側のナビゲーションペインで、 * General * > * SAML Authentication * をクリックします。
2. 新しい IdP の URI と Unified Manager サーバを IdP に接続するために必要な IdP メタデータを入力しま

す。

Unified Manager サーバから IdP に直接アクセスできる場合は、 IdP の URL を入力したあとに「 * IdP メタデータの取得」ボタンをクリックすると、 IdP のメタデータフィールドに自動的に値が入力されます。

3. Unified Manager のメタデータ URI をコピーするか、メタデータを XML テキストファイルに保存します。
4. [構成の保存 *] をクリックします。

   設定を変更するかどうかの確認を求めるメッセージボックスが表示されます。

5. [OK] をクリックします。

新しい IdP にアクセスし、 Unified Manager サーバの URI とメタデータを入力して設定を完了します。

許可されたリモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から古い IdP のログインページではなく新しい IdP のログインページに変わります。

Unified Manager セキュリティ証明書変更後に SAML 認証設定を更新しています

Unified Manager サーバにインストールされている HTTPS セキュリティ証明書が変更されたときは、 SAML 認証の設定を更新する必要があります。証明書は、ホストシステムの名前を変更したり、ホストシステムに新しい IP アドレスを割り当てたり、システムのセキュリティ証明書を手動で変更したりすると更新されます。

セキュリティ証明書が変更されたあとに Unified Manager サーバが再起動されると、 SAML 認証は機能せず、ユーザは Unified Manager のグラフィカルインターフェイスにアクセスできなくなります。ユーザインターフェイスに再びアクセスできるようにするには、 IdP サーバと Unified Manager サーバの両方で SAML 認証の設定を更新する必要があります。

手順

1. メンテナンスコンソールにログインします。
2. メインメニュー * で、 * SAML 認証を無効にする * オプションの番号を入力します。

   SAML 認証を無効にして Unified Manager を再起動することの確認を求めるメッセージが表示されます。

3. 更新された FQDN または IP アドレスを使用して Unified Manager のユーザインターフェイスを起動し、更新されたサーバ証明書をブラウザで受け入れ、メンテナンスユーザのクレデンシャルを使用してログインします。
4. [* Setup/Authentication] ページで [* SAML Authentication*] タブを選択し、 IdP 接続を設定します。
5. Unified Manager のホストメタデータ URI をコピーするか、メタデータを XML テキストファイルに保存します。
6. [保存（ Save ）] をクリックします。

   設定を完了して Unified Manager を再起動するかどうかの確認を求めるメッセージボックスが表示されます。

7. [確認してログアウト *] をクリックすると、 Unified Manager が再起動します。
8. IdP サーバにアクセスし、 Unified Manager サーバの URI とメタデータを入力して設定を完了します。

アイデンティティプロバイダ	設定手順
ADFS （ ADFS ）	a. ADFS 管理 GUI で、既存の証明書利用者信頼エントリを削除します。 b. を使用して、新しい証明書利用者信頼エントリを追加します `saml_sp_metadata.xml` 更新したUnified Managerサーバを使用します。 c. Unified Manager がこの証明書利用者信頼エントリに対する ADFS SAML 応答を解析するために必要な 3 つの要求規則を定義します。 d. ADFS Windows サービスを再開します。
Shibboleth	a. Unified Managerサーバの新しいFQDNをで更新します `attribute-filter.xml` および `relying-party.xml` ファイル。 b. Apache Tomcat Web サーバを再起動し、ポート 8005 がオンラインになるまで待ちます。

9. Unified Manager にログインし、 IdP 経由で SAML 認証が想定どおりに機能することを確認します。

SAML 認証を無効にします

Unified Manager Web UI にログインするリモートユーザのセキュアなアイデンティティプロバイダ（ IdP ）による認証を中止する場合は、 SAML 認証を無効にします。SAML 認証が無効な場合は、 Active Directory や LDAP などの設定済みのディレクトリサービスプロバイダがサインオン認証を実行します。

SAML 認証を無効にすると、設定されているリモートユーザに加え、ローカルユーザとメンテナンスユーザもグラフィカルユーザインターフェイスにアクセスできるようになります。

SAML 認証は、グラフィカルユーザインターフェイスにアクセスできない場合は Unified Manager メンテナンスコンソールを使用して無効にすることもできます。

SAML 認証を無効にしたあと、 Unified Manager が自動的に再起動されます。

手順

1. 左側のナビゲーションペインで、 * General * > * SAML Authentication * をクリックします。
2. [SAML 認証を有効にする *] チェックボックスをオフにします。
3. [保存（ Save ）] をクリックします。

   設定を完了して Unified Manager を再起動するかどうかの確認を求めるメッセージボックスが表示されます。

4. [確認してログアウト *] をクリックすると、 Unified Manager が再起動します。

リモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から IdP のログインページではなく Unified Manager のログインページに変わります。

IdP にアクセスし、 Unified Manager サーバの URI とメタデータを削除します。

メンテナンスコンソールから SAML 認証を無効にする

Unified Manager GUI にアクセスできない場合は、必要に応じてメンテナンスコンソールから SAML 認証を無効にすることができます。この状況は、設定に誤りがある場合や IdP にアクセスできない場合に発生します。

- 必要なもの *

メンテナンスコンソールにメンテナンスユーザとしてアクセスできる必要があります。

SAML 認証が無効な場合は、 Active Directory や LDAP などの設定済みのディレクトリサービスプロバイダがサインオン認証を実行します。設定されているリモートユーザに加え、ローカルユーザとメンテナンスユーザもグラフィカルユーザインターフェイスにアクセスできるようになります。

SAML 認証は、 UI のセットアップ / 認証のページから無効にすることもできます。

SAML 認証を無効にしたあと、 Unified Manager が自動的に再起動されます。

手順

1. メンテナンスコンソールにログインします。
2. メインメニュー * で、 * SAML 認証を無効にする * オプションの番号を入力します。

   SAML 認証を無効にして Unified Manager を再起動することの確認を求めるメッセージが表示されます。

3. 「 * y * 」と入力して Enter キーを押すと、 Unified Manager が再起動します。

リモートユーザが Unified Manager のグラフィカルインターフェイスにアクセスする際にクレデンシャルを入力するページが、次回から IdP のログインページではなく Unified Manager のログインページに変わります。

必要に応じて、 IdP にアクセスして Unified Manager サーバの URL とメタデータを削除します。

SAML Authentication ページ

SAML 認証ページを使用して、 Unified Manager の Web UI にログインするリモートユーザを SAML を使用してセキュアなアイデンティティプロバイダ（ IdP ）で認証するように Unified Manager を設定できます。

- SAML 設定を作成または変更するには、アプリケーション管理者ロールが必要です。
- リモート認証を設定しておく必要があります。
- リモートユーザまたはリモートグループを少なくとも 1 つ設定しておく必要があります。

リモート認証とリモートユーザの設定が完了したら、 SAML 認証を有効にするチェックボックスをオンにして、セキュアなアイデンティティプロバイダを使用した認証を有効にすることができます。

- * IdP URI *

  Unified Manager サーバから IdP にアクセスするための URI 。URI の例を次に示します。

  ADFS の URI の例：

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth の URI の例：

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- * IdP メタデータ *

  XML 形式の IdP メタデータ。

  Unified Manager サーバから IdP の URL にアクセスできる場合は、「 * IdP メタデータの取得方法 * 」ボタンをクリックしてこのフィールドに値を入力できます。

- * ホストシステム（ FQDN ） *

  インストール時に定義された Unified Manager ホストシステムの FQDN 。この値は必要に応じて変更できます。

- *ホストURI *

  IdP から Unified Manager ホストシステムにアクセスするための URI 。

- * ホストメタデータ *

  XML 形式のホストシステムメタデータ

著作権に関する情報

商標に関する情報