日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

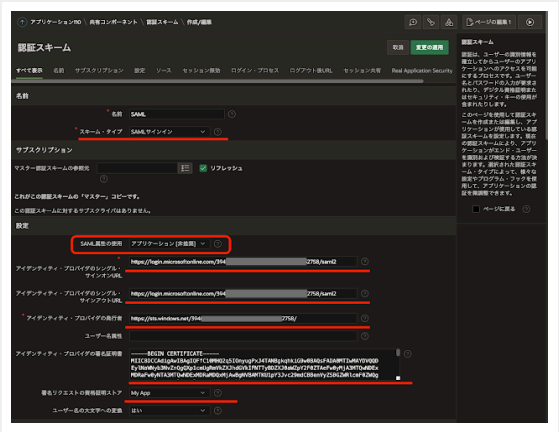
2022年7月14日木曜日

アプリケーションごとのSAML認証を試してみる

Oracle APEXとしては非推奨となっているのですが、アプリケーションごとのSAML認証の設定を試してみました。Azure ADをIdPとして使っています。

認証スキームの**スキーム・タイプ**に**SAMLサインイン**を選択し、**設定**の**SAML属性の使用**として**アプリケーション[非推奨]**を選択します。

設定手順は、インスタンス単位での手順を参照していただくこととし、異なる点を説明します。



設定の**アイデンティティ・プロバイダのシングル・サインオンURL**、**アイデンティティ・プロバイダのシングル・サインアウトURL**、**アイデンティティ・プロバイダの発行者**は、インスタンスでの設定と同様に、Azure ADのエンタープライズ・アプリケーションの以下の情報を参照します。対応は以下になります。

アイデンティティ・プロバイダのシングル・サインオンURL = ログインURL
アイデンティティ・プロバイダのシングル・サインアウトURL = ログアウトURL
アイデンティティ・プロバイダの発行者 = Azure AD識別子

アイデンティティ・プロバイダの署名証明書は、Azure ADよりダウンロードした証明書を貼り付けます。形式は**Base64**を選択します。

署名リクエストの資格証明ストアとしてワークスペースの**Web資格証明**として作成した、証明書と秘密キーのペアを保存している資格証明を指定します。

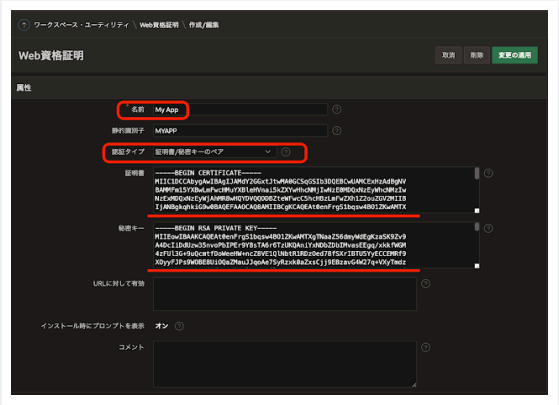
アプリケーション・ビルダーの**ワークスペース・ユーティリティ**を開きます。

ワークスペース・ユーティリティの**Web資格証明**を開きます。

以前のAPEXのバージョンでは、**共有コンポーネント**に**Web資格証明**へのリンクが含まれていた覚えがあるのですが、現行のバージョンでは**資格証明**へのリンクは**右隅**に移動しています。

Web資格証明の**属性**として**名前**を設定します。ここで指定した名前をSAMLの**設定**の**署名リクエストの資格証明ストア**として指定します。

認証タイプとして**証明書/秘密キーのペア**を選択します。証明書/秘密キーのペアはopensslを使って生成します。手順については、Oktaの記事に記載しています。



APEX側の設定は以上です。Azure ADのIdP自体は、インスタンス単位かアプリケーションごとかに関わらず同じなので、設定に大きな違いはありません。

APEXのアプリケーションごとにSAML認証を設定する場合、Azure AD側の**基本的なSAML構成**は、以下のように変わります。

SP（サービス・プロバイダ）はAPEXのインスタンスではなくAPEXアプリケーションであるため、**識別子（エンティティID）**と**サインオンURL**はインスタンスを示すURLから、**アプリケーションを示すURL**に変更します。**応答URL（Assertion Consumer Service URL）**は、**SAMLコールバックとなるURL**で、こちらはインスタンス・レベルと同じURLを指定します

識別子:　https://ホスト名/ords/f?p=アプリケーションID
応答URL: https://ホスト名/ords/apex_authentication.saml_callback
サインオンURL: https://ホスト名/ords/f?p=アプリケーションID

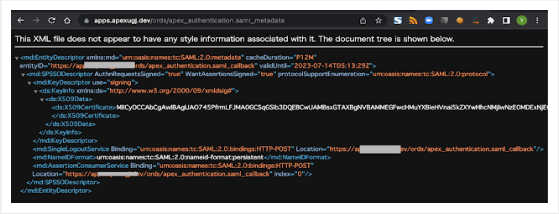
インスタンス・レベルでのSAML認証の設定と、アプリケーションごとのSAML認証の設定の違いは以上になります。

Azure ADのエンタープライズ・アプリケーションとAPEXアプリケーションが１対１で登録されているため、インスタンス・レベルでのSAML認証と異なり、IdPからAPEXアプリケーションにサインインすることができます。

つまり、Azure ADでSAML認証を構成したときの最後のステップである**Test**も成功します。

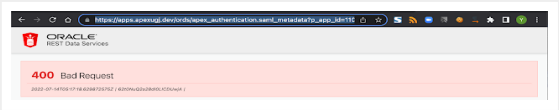
Oracle APEXでは、パッケージAPEX_AUTHENTICATIONに含まれるSAML_METADATAというプロシージャを呼び出すことにより、SPのメタデータを取得できます。

https://ホスト名/ords/apex_authentication.saml_metadata



引数**p_app_id**に**アプリケーションID**を指定することにより、APEXアプリケーションごとのSAML SPのメタデータが取得できるはずなのですが、エラーが発生します。おそらく不具合と思われますが、エンティティIDやログインURLはメタデータを参照しなくても分かるため、問題にはならないでしょう。

https://ホスト名/ords/apex_authentication.saml_metadata?p_app_id=アプリケーションID



アプリケーションの認証スキームとしてSAMLが構成されていないと、アプリケーションIDを指定してもインスタンス・レベルの構成情報が返されます。SAML_METADATAの呼び出しが正常終了していても、エンティティIDの末尾がsaml_callbackとなっている場合は、APEXアプリケーションを対象としたメタデータではないので注意が必要です。

完

Yuji N. 時刻: 14:41

共有

‹ ホーム ›

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示