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6月15日水曜日

OktaのグループをAPEXに認識させる方法とシングル・サインアウトの設定

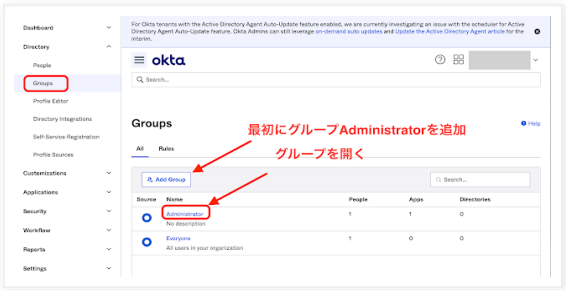
Oktaを使ったSAMLのシングル・サインオンの設定ができたので、さらに追加の構成を確認してみました。

OktaのグループをAPEXのダイナミック・グループとする

Okta側でユーザーが所属しているグループを、APEXアプリケーションのサインイン時にダイナミック・グループとして登録します。結果として、Okta側での所属グループでAPEXアプケーションの認可を制御することができます。

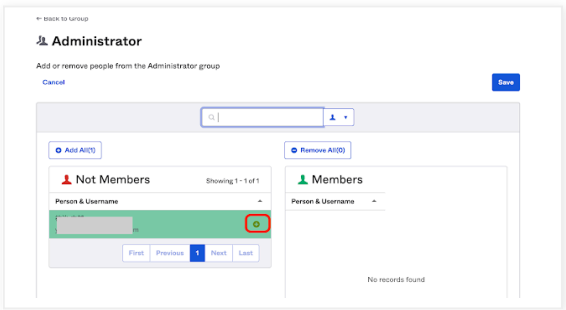
Oktaの設定画面を開き、**Directory**の**Groups**よりグループを作成します。**Everyone**は最初から作成されているので、今回は**Administrator**というグループを追加で作成しています。

Add Groupをクリックし、グループAdministratorを作成します。その後、作成されたグループAdministratorを開きます。

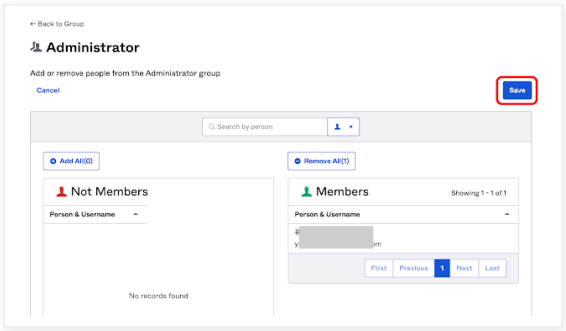


Assign Peopleをクリックし、People（つまりサインインするユーザー）をグループに含めます。

グループに含めるユーザーを**Not Members**から+をクリックして、**Members**へ移動します。

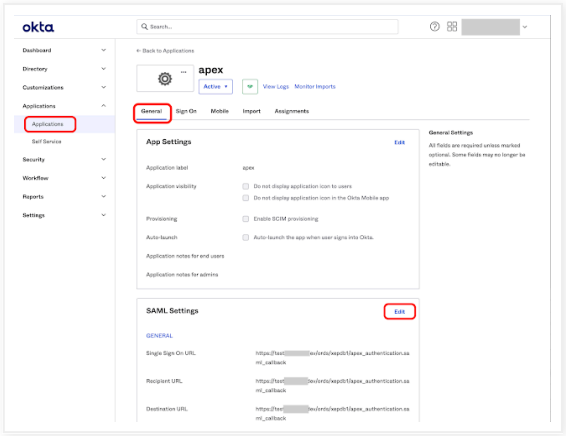


ユーザーをグループに含めたら、**Save**をクリックします。



サインインの際に、Okta（IdP）からSP（APEX）に送信されるレスポンスに、グループの情報を含めます。**Application**の**SAML Settings**に含まれる**GROUP ATTRIBUTE STATEMENTS**に設定を追加します。

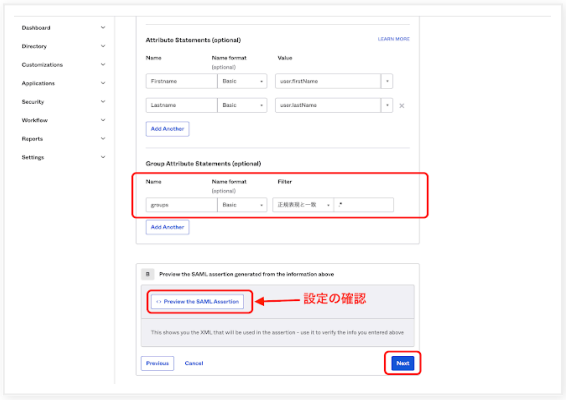
Applicationsを開いて、作成済みのSP（前回の記事では**apex**として作成）を開きます。**General**タブの**SAML Settings**の**Edit**をクリックします。



General Settingsは変更せず、**Next**をクリックします。

次に開く画面の**Group Attribute Statements (optional)**にて、**Name**に**groups**、**Name format**を**Basic**、**Filter**は**正規表現と一致**を選択して**.***を指定します。

設定を行った後に**Preview the SAML Assertions**をクリックし、設定した結果を確認します。



Assertionの内容が表示されます。**NameID**として表示されているユーザーが所属しているグループが、**Attribute**として含まれていることを確認します。

Okta側で必要な変更は以上になります。**Next**をクリックしてこの画面の変更を確定し、最後に**Save**を実行して変更を保存します。

続いて、Oktaが送信してくるレスポンスからグループを取り出し、ダイナミック・グループを設定する処理をAPEX側に設定します。

ダイナミック・グループを設定するコードは以下になります。

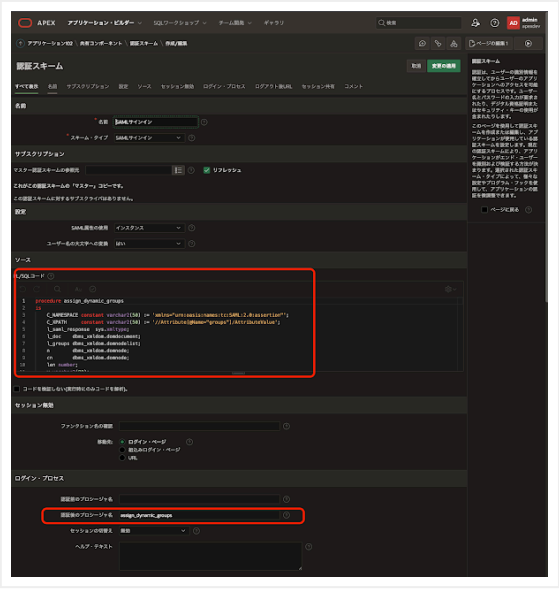
```
procedure assign_dynamic_groups
is
    C_NAMESPACE constant varchar2(50) := 'xmlns="urn:oasis:names:tc:SAML:2.0:assertion"';
    C_XPATH     constant varchar2(50) := '//Attribute[@Name="groups"]/AttributeValue';
    l_saml_response  sys.xmltype;
    l_doc    dbms_xmldom.domdocument;
    l_groups dbms_xmldom.domnodelist;
    n        dbms_xmldom.domnode;
    cn       dbms_xmldom.domnode;
    len number;
    v varchar2(80);
    vs apex_t_varchar2;
begin
    -- SAMLResponseはAPEX_APPLICATION.G_X01として渡される。
    l_saml_response := xmltype(apex_application.g_x01);
    -- AttributeタグでName=groupsの子要素AttributeValueを取り出す。
    l_doc := dbms_xmldom.newdomdocument(
       l_saml_response.extract(C_XPATH, C_NAMESPACE)
    );
    -- XMLTYPEからDOMDocumentに変換する。
    l_groups := dbms_xmldom.getelementsbytagname(l_doc, '*');
    -- 所属しているグループの数をlenに取り出す。
    len := dbms_xmldom.getlength(l_groups);
    for i in 0 .. (len -1)
    loop
        n  := dbms_xmldom.item(l_groups, i);
        cn := dbms_xmldom.getfirstchild(n);
        v  := dbms_xmldom.getnodevalue(cn);
        apex_debug.info('Dynamic Group Assigned = ' || v);
```

```
        apex_string.push(vs,v);
    end loop;
    -- ダイナミック・グループを有効にする。
    apex_authorization.enable_dynamic_groups(vs);
end assign_dynamic_groups;
```

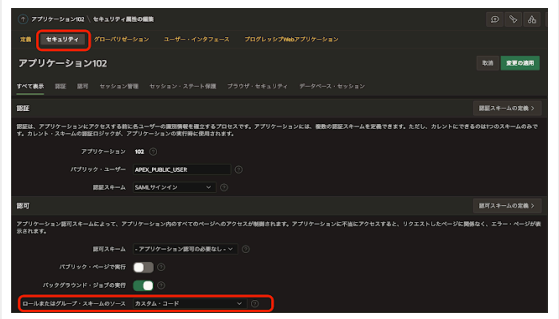
okta_assign_dynamic_groups.sql hosted with ❤️ by GitHub view raw

APEXアプリケーションの**SAMLサインイン**の認証スキームを開き、**ソース**の**PL/SQLコード**に上記のコードを記載します。

ログイン・プロセスの**認証後のプロシージャ名**に、ソースに記述したプロシージャ**assign_dynamic_groups**を設定します。



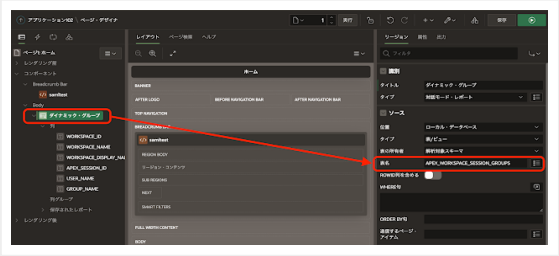
アプリケーション定義の**セキュリティ**を開き、**認可**の**ロールまたはグループ・スキームのソース**を**カスタム・コード**に変更します。



以上で、APEXアプリケーション側の設定も完了です。

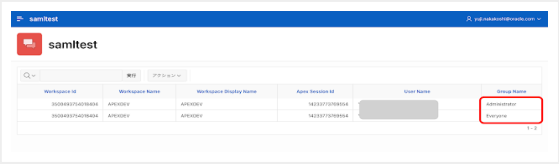
ダイナミック・グループが正しく設定されているか確認するために、SAML認証の確認のために作成したアプリケーションsamltestに、対話モード・レポートのリージョンを作成します。

識別の**タイトル**は**ダイナミック・グループ**とします。**ソース**の**表名**にAPEXの標準ビュー**APEX_WORKSPACE_SESSION_GROUPS**を指定します。



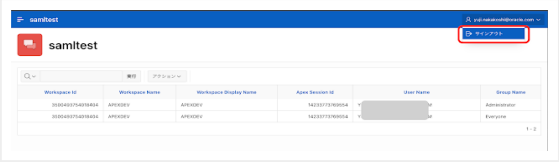
対話モード・レポートを追加したので、アプリケーションを実行します。Oktaでサインインしたのち、アプリケーションのホーム・ページが表示されます。

Group Nameとして**Administrator**および**Everyone**がリストされていれば、正しく設定できています。



シングル・サインアウトを設定する

アプリケーションからサインアウトを実行します。

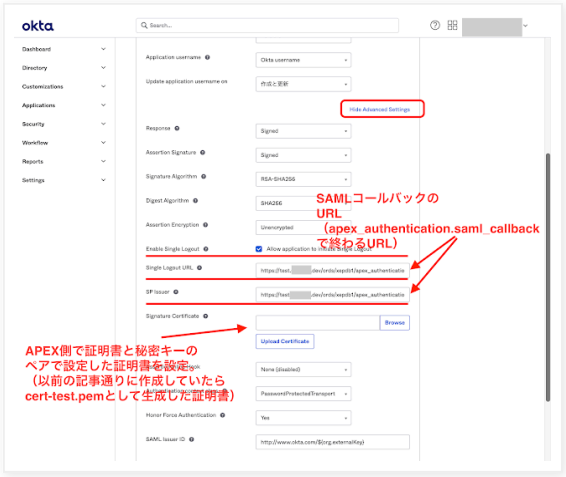


Oktaではサインアウトがエラーになり、以下の画面が表示されます。

このエラーを回避するために、Okta側でシングル・サインアウトの設定を行います。

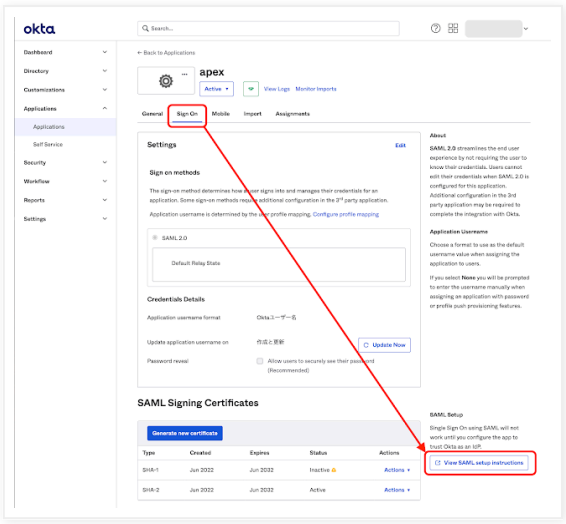
アプリケーションの**SAML Settings**を編集します。**Advanced Settings**を開き、**Enable Single Logout**の**Allow application to initiate Single Logout**に**チェック**を入れます。**Single Logout URL**、**SP Issuer**共に、APEX側の**SAMLコールバックURL**を設定します。apex_authentication.saml_callbackで終わるURLで、このアプリケーションの**Single sign on URL**および**Audience URI(SP Entity ID)**として設定しているURLと同一のURLです。

Signature Certificateとして、APEX側の**内部およびワークスペース・アプリケーション用のSAML: APEX属性**の**証明書**として設定した証明書を設定します。以前の記事通りの手順であれば、**cert-test.pem**として生成した証明書になります。

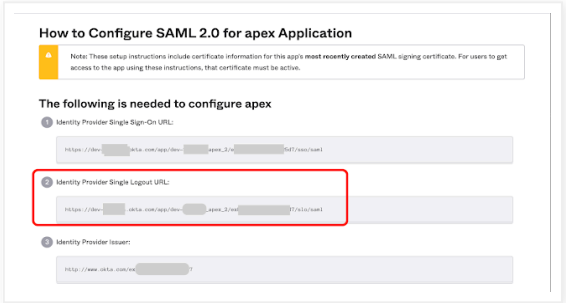


以上でOkta側のシングル・サインアウトの設定は完了です。**Next**をクリックして作業を進め、最終的に**Save**を実行して変更した設定を保存します。

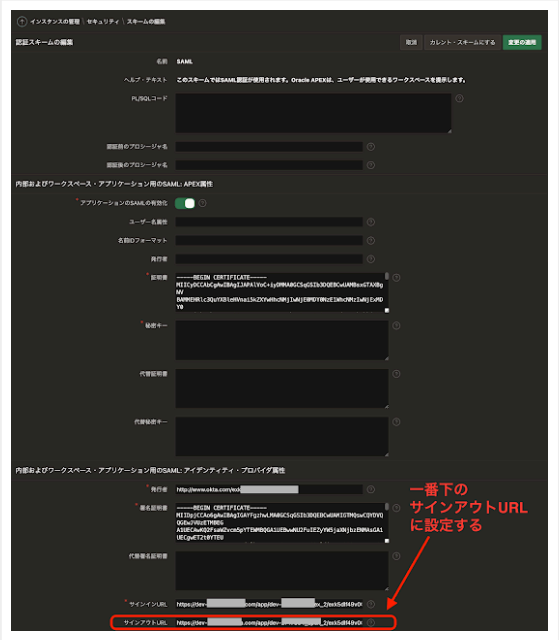
Okta側で生成された**Single Logout URL**を確認します。アプリケーションの**Sign On**タブを開いて、**SAML Setup**の**View SAML setup instructions**を開きます。



②の**Identity Provider Single Logout URL**をコピーし、APEX側に設定します。

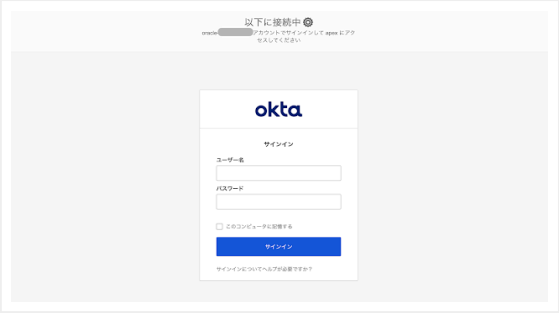


APEXの**認証制御**の**SAML**の設定画面を開き、一番下にある**サインアウトURL**に上記のURLを設定します。



以上でシングル・サインアウトの設定は完了です。

APEXアプリケーションからサインアウトを実行すると、Oktaのログイン画面に戻ります。



Oracle APEXのSAML認証でOktaをIdPに使用するにあたって、利用可能な追加設定の説明は以上になります。

Oracle APEXのアプリケーション作成の参考になれば幸いです。

完

Yuji N. 時刻: 16:19

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