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8月15日月曜日

ADBのアプリケーション・ビルダーをAzure ADにてユーザー認証する

Autonomous DatabaseのAPEXで、アプリケーション・ビルダーのサインインにSocial Sign-Inが使えるようになりました。手順自体は以前に書いた記事 - Azure ADで認証しMicrosoft Graph APIを呼び出す - とあまり違いはありません。

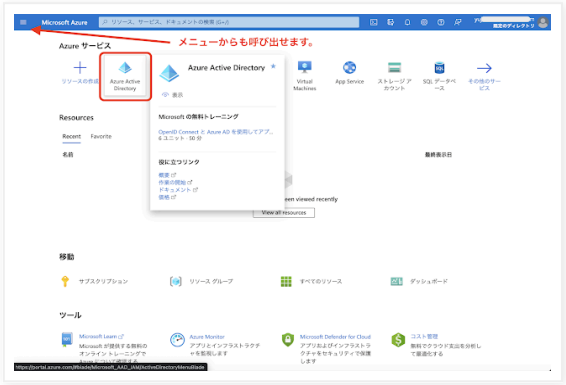
以前の記事を書いたのは1年以上前になります。ADB、APEXおよびAzure ADの画面が変更されているため、作業を一通りやり直してみました。

検証にはAlways FreeのAutonomous Transaction Processingを使用しています。ADBのインスタンスを作成した後、開発用のワークスペースとしてAPEXDEVを追加した状態から作業を始めます。

以下より作業手順を記載します。

最初にAzure ADにアプリケーションを登録します。

Azureのポータルhttps://portal.azure.comにアクセスします。**Azureサービス**の**Azure Active Directory**を開きます。左上のメニューを開いて、Azure Active Directoryを呼び出すこともできます。

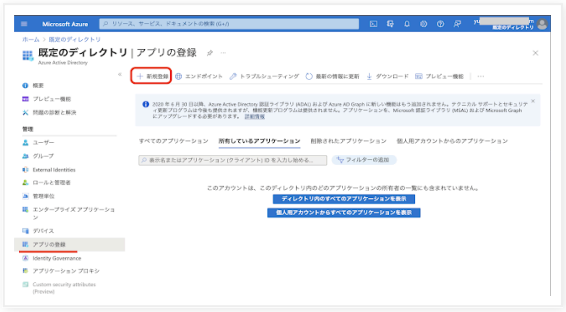


既定のディレクトリの**概要**が開きます。今回使用しているAzure ADの**ライセンス**は、**Azure AD Free**です。

アプリの登録を開きます。

画面の下に**アプリケーションの登録を追加**というショートカットがあるので、それを呼び出すこともできます。**エンタープライズアプリケーションの追加**ではありません。

アプリの登録の**新規登録**を実行します。



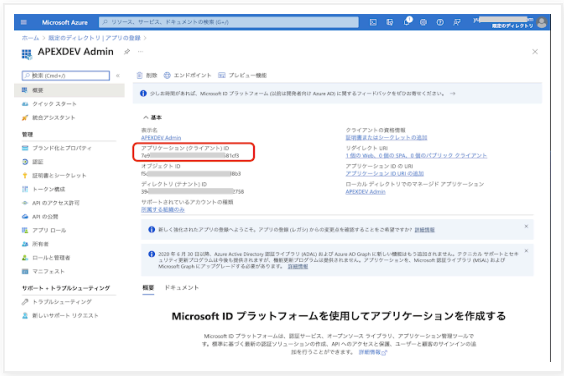
アプリケーションの登録画面が開きます。

アプリケーションの**名前**は任意です。今回は**APEXDEV Admin**としています。**サポートされているアカウントの種類**として、**この組織ディレクトリのみに含まれるアカウント（規定のディレクトリのみ - シングルテナント）**を選択します。以前の記事では、**任意の組織ディレクトリ内のアカウント（任意のAzure ADディレクトリ - マルチテナント）と個人のMicrosoftアカウント（Skype、Xboxなど）**を選んでいます。こちらを選択しても同様に、Azure ADを使ったユーザー認証を構成することができます。**リダイレクトURI**は、Oracle APEX側で認証応答を受け付けるURIです。**APEXのサーバーのベース・パスにapex_authentication.callbackを付加したURI**になります。省略可能となっていますが、APEXでの認証では指定は必須です。

https://<ADBのID>-<ADBインスタンス名>.adb.<リージョン名>.oraclecloudapps.com/ords/apex_authentication.callback

以上を設定し、**登録**を実行します。

アプリケーション**APEXDEV Admin**が作成されます。**アプリケーション(クライアント)ID**の情報をOracle APEXに**OAuth2資格証明**の**クライアントID**として登録するので、コピーしておきます。

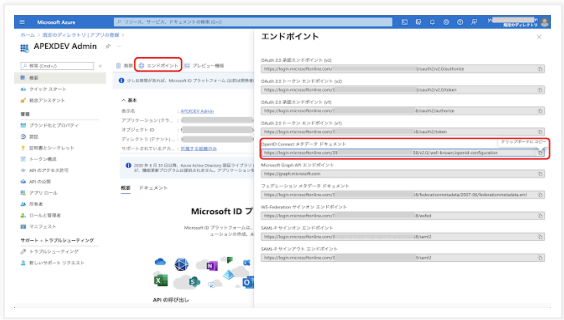


エンドポイントを開き、**OpenID Connect メタデータ ドキュメント**のURLをコピーします。

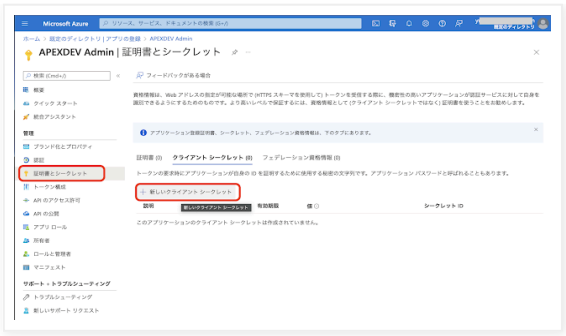
アカウントの種類として、**任意の組織ディレクトリ内のアカウント（任意のAzure ADディレクトリ - マルチテナント）と個人のMicrosoftアカウント（Skype、Xboxなど）**を選択している場合は、**OpenID Connect メタデータ ドキュメント**のURLは以下になります。

https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration

このURLを、APEXに**Discovery URL**として登録します。Azure ADに登録したアプリケーションによって異なるため、必ず**エンドポイント**を開いて確認します。

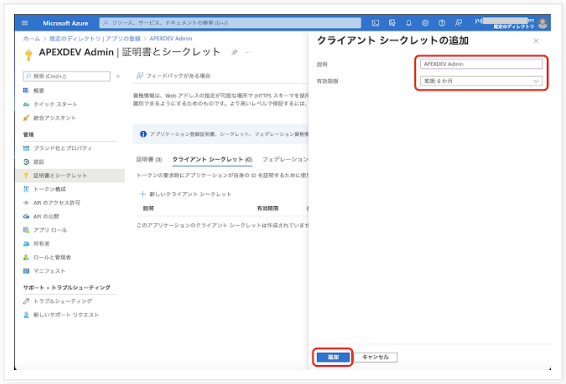


証明書とシークレットを開き、**新しいクライアント シークレット**を作成します。



画面右にドロワーが開きます。**説明**を入力し、**有効期限**を選択します。今回は**説明**に**APEXDEV Admin**、**有効期限**は**推奨: 6か月**を選択しています。

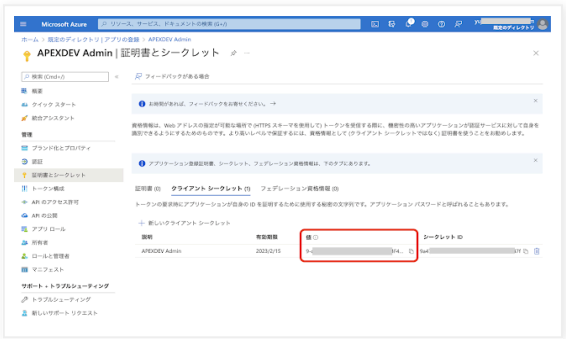
追加をクリックします。



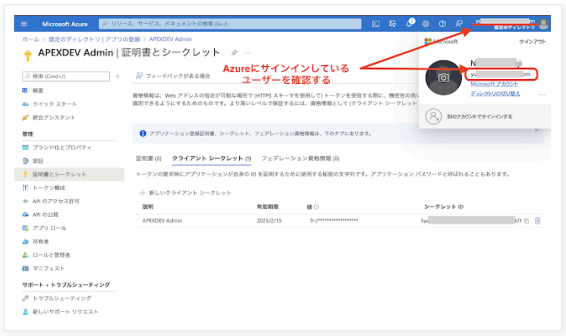
クライアント シークレットが作成されます。この**値**をAPEX側の**クライアント・シークレットまたはパスワード**として登録します。シークレットIDは使用しません。

クライアント シークレットの**値**をコピーしておきます。

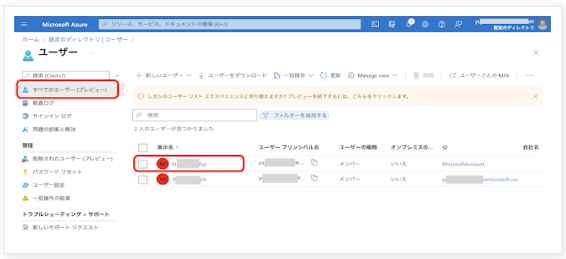
有効期限が切れる前に新しく**クライアント シークレット**を作成し、APEX側の**クライアント・シークレットまたはパスワード**を更新する必要があります。



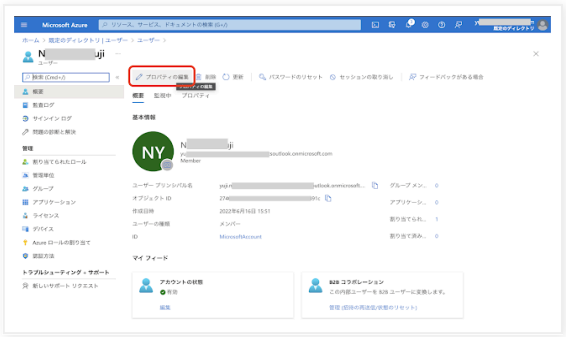
現在Azure ADにサインインしているユーザーを確認します。**メール・アドレスがID**になっていることを想定しています。



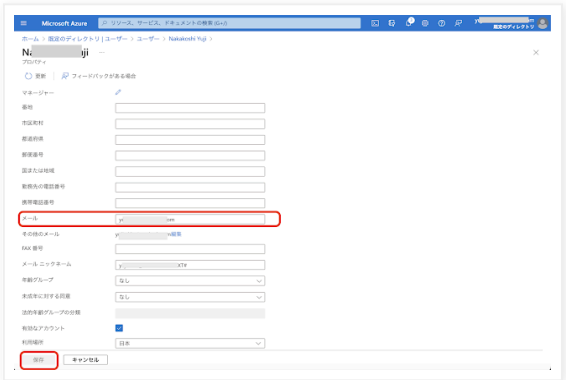
既定のディレクトリに作成されている**ユーザー**情報を確認します。**ユーザー**を開き、Azureポータルに現在サインイン中のユーザーの**名前をクリック**します。



プロパティの編集を開きます。



プロパティの**メール**が空白の場合は、**IDと同じ値を設定**します。プロパティを変更した後、**保存**をクリックします。

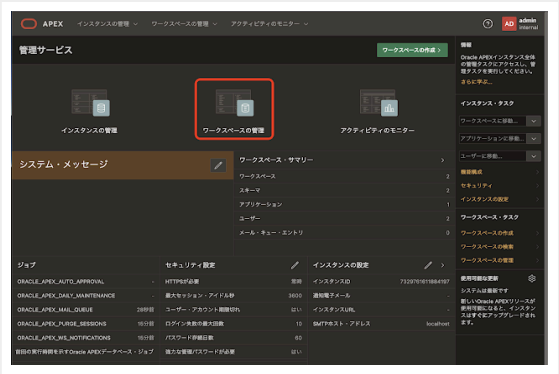


Azure Active Directoryでの設定は以上で完了です。

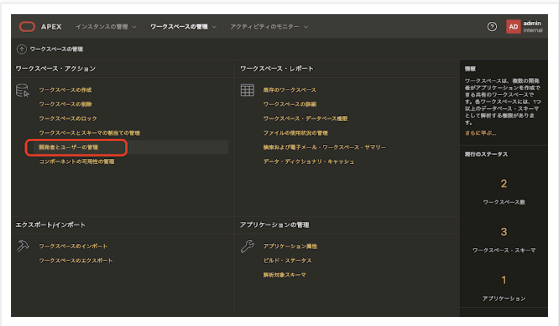
APEXの**管理サービス**にサインインします。ユーザー**ADMIN**のパスワードを入力します。

最初にAzure ADの既定のディレクトリに登録されているユーザーを、Oracle APEXに登録します。Azure ADのユーザーと同じ名前のユーザーをOracle APEXに登録することにより、そのユーザーでの認証をAzure ADで実施します。

ワークスペースの管理を開きます。



開発者とユーザーの管理を開きます。



ユーザーの作成をクリックします。

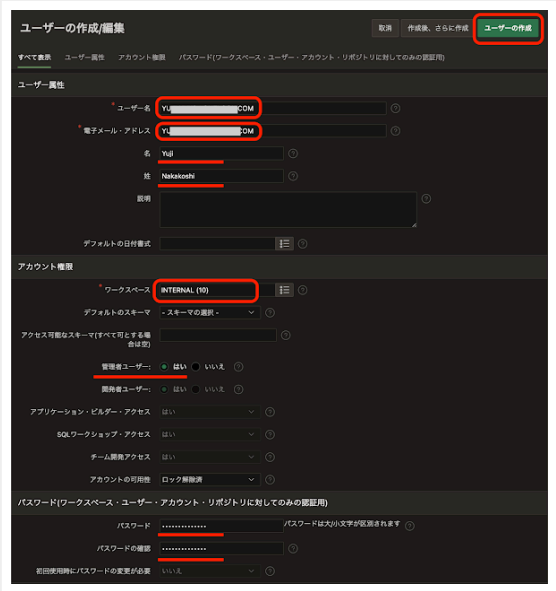
ユーザーを作成します。

ユーザー名、**電子メール・アドレス**として、**Azureポータルにサインインしたユーザーの**IDを大文字で入力します。その他の**ユーザー属性**として、**名**、**姓**を入力します。

アカウント権限の**ワークスペース**としてINTERNALを選択します。**管理者ユーザー**として**はい**を選択します。

パスワード(ワークスペース・ユーザー・アカウント・リポジトリに対してのみの認証用)を入力します。アプリケーション・ビルダーへのサインインには、Azure ADが使用されるため、ここで指定するパスワードは使用されません。

以上を設定し、**作成**を実行します。



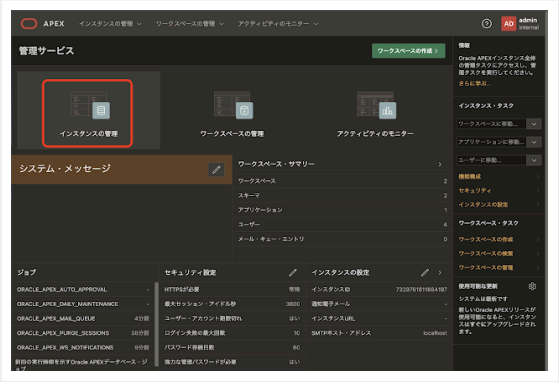
同じ手順を繰り返し、別のワークスペースに同じユーザー名のユーザー（Azureポータルにサインインしたユーザー）を作成します。

アカウント権限の**ワークスペース**に**APEXDEV**（アプリケーションを開発するためのワークスペース）を選択します。

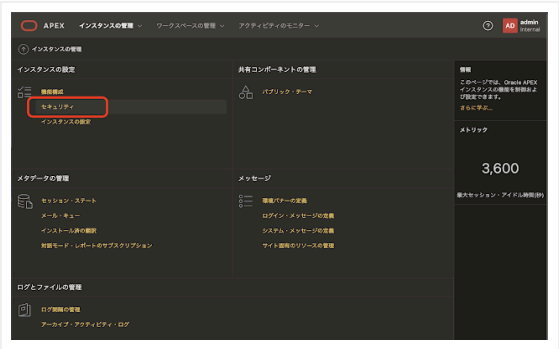
ワークスペースINTERNALとAPEXDEVに、同じ名前のユーザーが作成されました。

続いて、Social Sign-Inの設定を行います。

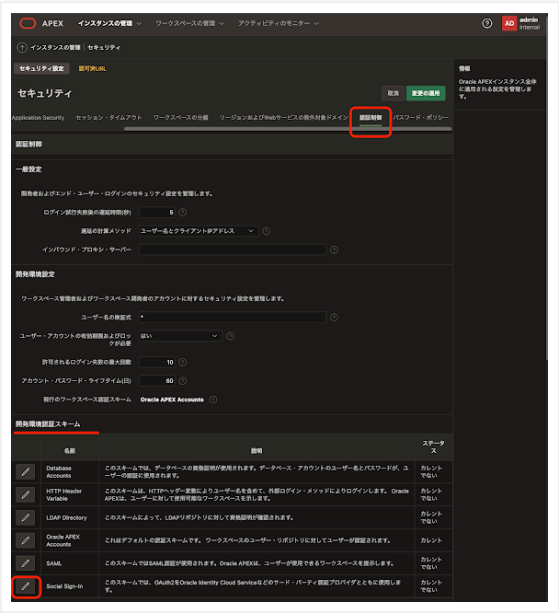
インスタンスの管理を開きます。



インスタンスの設定の**セキュリティ**を開きます。



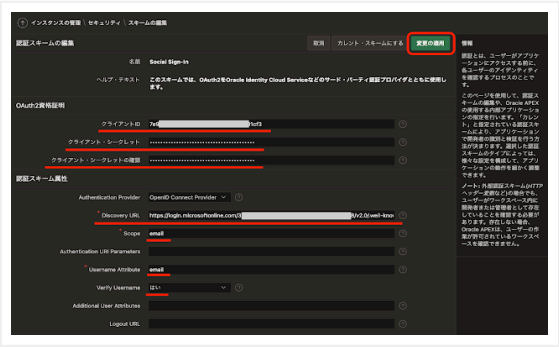
認証制御の**開発環境認証スキーム**のSocial Sign-Inを開きます。



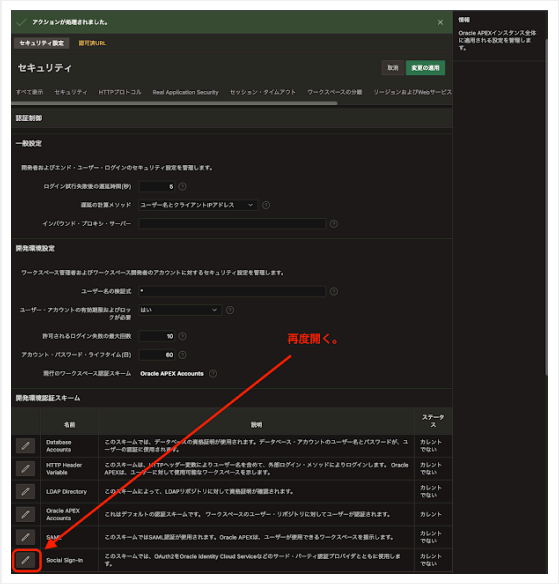
クライアントIDとして、Azure ADに登録したアプリの**アプリケーション(クライアント)ID**を指定します。**クライアント・シークレット**として、Azure ADのアプリに作成した**クライアント・シークレット**の**値**を指定します。

認証スキーム属性の**Authentication Provider**として**OpenID Connect Provider**を選択し、**Discovery URL**として、Azure ADのアプリの**エンドポイント**を開いて確認した、**OpenID Connect メタデータ ドキュメント**のURLを指定します。

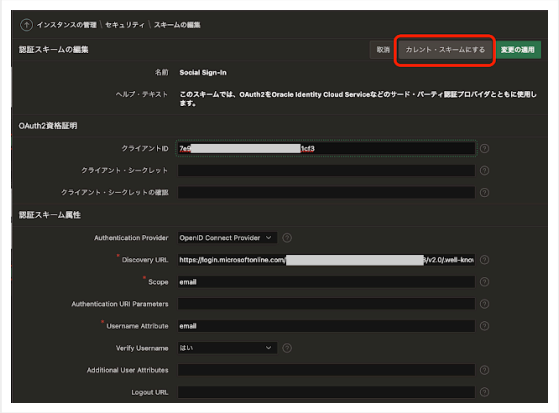
Scopeは**email**、**Username Attribute**も**email**とし、**Verify Username**に**はい**を指定して、**変更の適用**を実行します。



APEXの開発環境認証スキームが設定されました。再度、**Social Sign-In**を開き、Social Sign-Inをカレントのスキームに切り替えます。

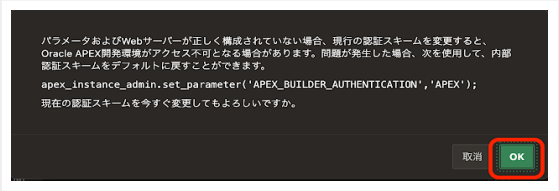


カレント・スキームにするをクリックします。

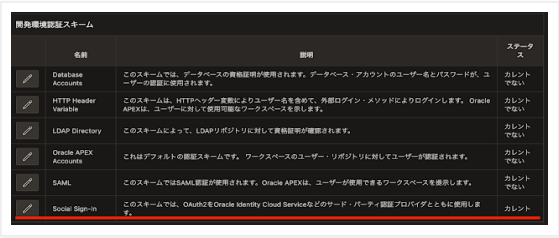


開発環境の認証スキームを切り替えると、認証スキームの設定に不備があるとサインインができなくなると警告されます。メッセージでは認証スキームとしてOracle APEX Accountsに戻すコマンドが示されています。Autonomous Databaseの場合は、Database Accountsに戻す必要があります。以下のコマンドを**データベース・アクション**の**SQL**で実行すると、認証スキームを戻すことができます。

```
apex_instance_admin.set_parameter('APEX_BUILDER_AUTHENTICATION','DB');
```



開発環境認証スキームとしてSocial Sign-Inがカレントに変わります。



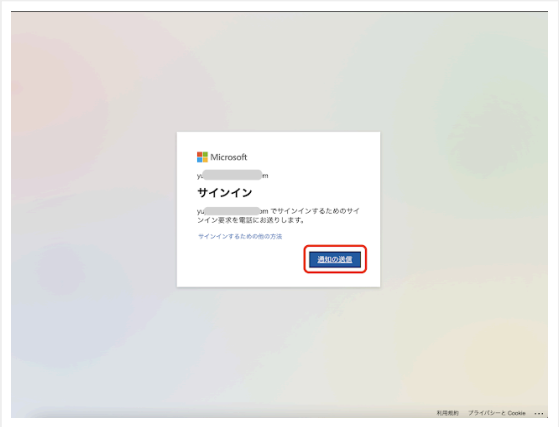
以上で、開発環境の認証にAzure ADを使う設定ができました。

実際にサインインを行ってみます。以下のURLにアクセスします。

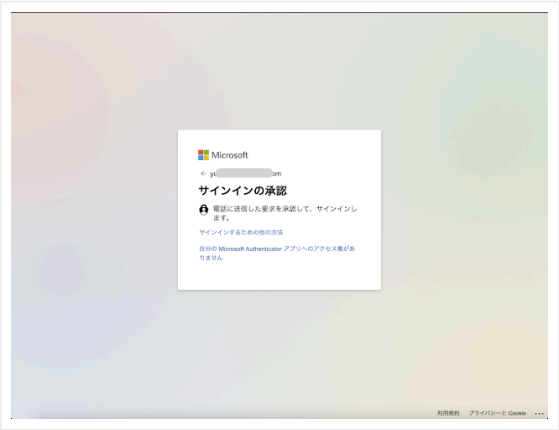
https://<ADBのID>-<ADBインスタンス名>.adb.<リージョン名>.oraclecloudapps.com/ords/

Microsoftのサインイン画面が開きます。アカウントを選択します。これからの手順は、Microsoft Authenticatorを使って認証を行なっています。

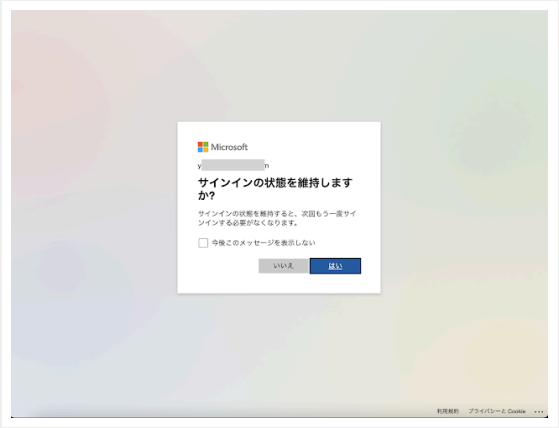
通知の送信を行います。



Microsoft Authenticatorでの承認待ちになります。

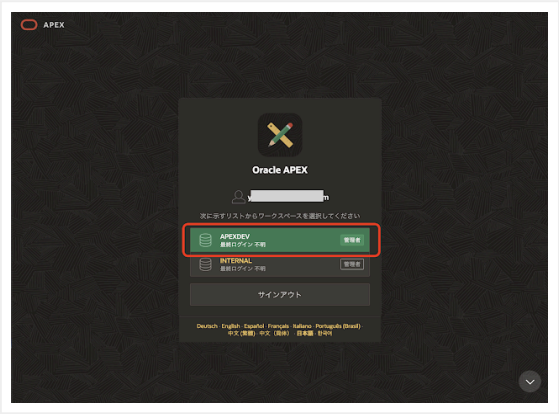


サインインの状態を維持しますか？と確認されます。この選択は、どちらでも構いません。



サインインが完了します。操作できるワークスペースが一覧されます。

アプリケーション・ビルダーにサインインするため、APEXDEVを選択します。

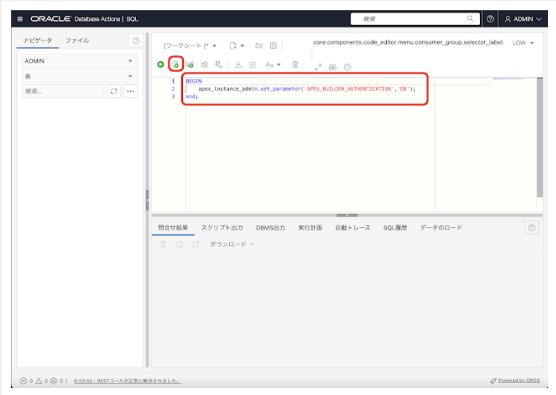


Azure ADで認証したユーザーで、ワークスペースAPEXDEVにサインインできました。

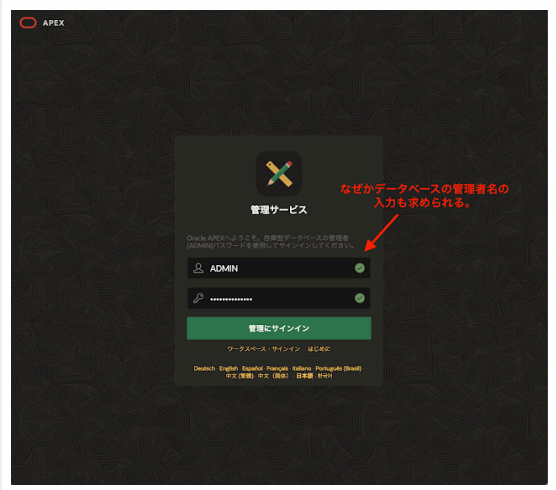
なお、設定に問題がありAzure ADをによるサインインに失敗した場合は、管理サービスにもサインインできません。

その場合は、データベース・アクションのSQLを開き、以下のコマンドを実行します。

```
BEGIN
    apex_instance_admin.set_parameter('APEX_BUILDER_AUTHENTICATION','DB');
end;
```



認証スキームをDatabase Accountsに戻した後は、ユーザー**ADMIN**にて**管理サービス**にサインインできます。



元々はデータベース管理者の名前はADMIN決め打ちで、入力フィールドは存在しません。上記の手順で認証スキームを回復すると、データベースのユーザー名の入力フィールドが表示されるようになります。こちらは常にADMINと入力します。

以上になります。

完

Yuji N. 時刻: 15:52

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