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2月18日金曜日

OCI IAMユーザーにてAutonomous Databaseに接続する

Autonomous Databaseの機能として、データベースに接続するときにOCI IAMのユーザーが使えるようになっています。

AskTOMのOffice Hourの以下のトピックで、製品マネージャが説明をしています。

Autonomous Database Authentication and Authorization - Integrating ADB-S with OCI IAM

マニュアルの記載は以下です。

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/authenticating-and-authorizing-iam-users-oracle-autonomous-databases.html

APEXの管理者ユーザーと開発者ユーザーはデータベースのユーザーなので、この構成を行えばOCI IAMユーザーでAPEXの管理者ユーザーと開発者ユーザーを作れるか、と考えたのですがそれはできませんでした。

残念な結果でしたが、それとは別に、OCI IAMを使うために行った作業を記録しておきます。

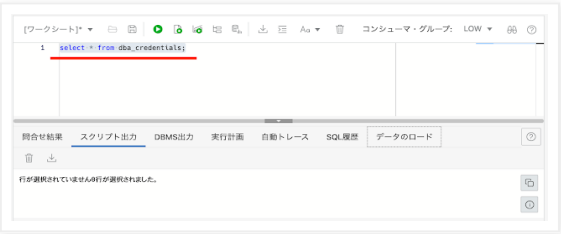
作業はAlways FreeのAutonomous Transaction Processingで行なっています。作成直後の状態から始めます。

リソース・プリンシパルの有効化

Autonomous Databaseのリソース・プリンシパルを有効にします。

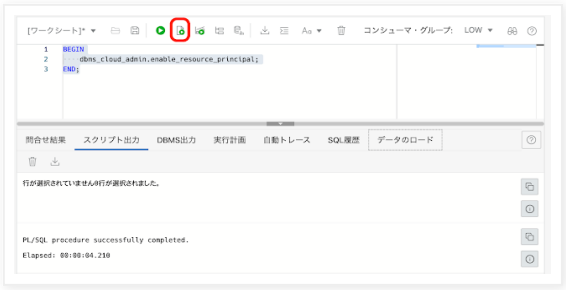
データベース・アクションの**SQL**の画面を開きます。ビュー**DBA_CREDENTIALS**を検索し、**OCI$RESOURCE_PRINCIPAL**がないことを確認します。

```
select * from dba_credentials;
```

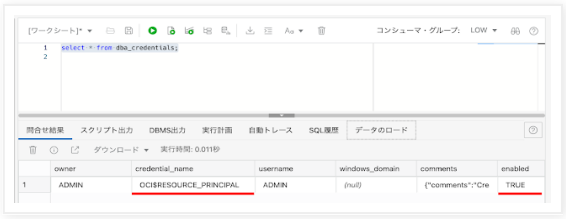


プロシージャDBMS_CLOUD_ADMIN.ENABLE_RESOURCE_PRINCIPALを実行し、リソース・プリンシパルを有効にします。

```
BEGIN
    dbms_cloud_admin.enable_resource_principal;
END;
```



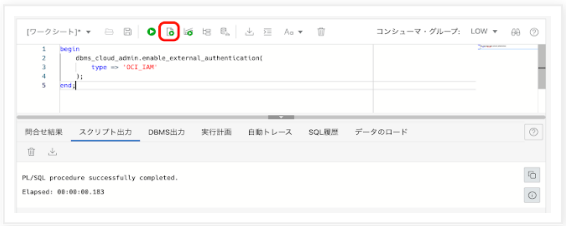
再度、ビューDBA_CREDENTIALSを検索します。**credential_name**として**OCI$RESOURCE_PRINCIPAL**、**enabled**が**TRUE**になっていることを確認します。



OCI IAMを使った外部認証の有効化

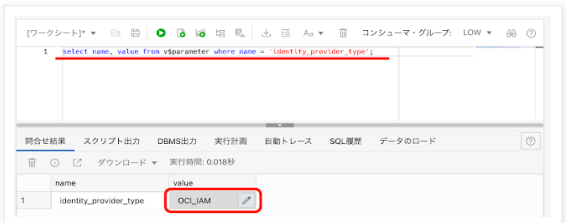
OCI IAMを使った外部認証を有効にします。

データベース・アクションの**SQL**より、プロシージャDBMS_CLOUD_ADMIN.ENABLE_EXTERNAL_AUTHENTICATIONを実行します。引数**type**に**OCI_IAM**を与えます。



初期化パラメータの**identity_provider_type**が**OCI_IAM**になっていることを、以下のSQL文を実行して確認します。

```
select name, value from v$parameter where name = 'identity_provider_type';
```

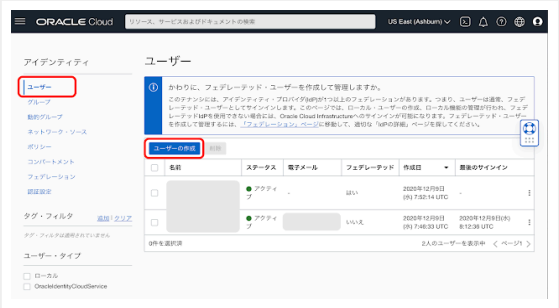


データベース接続ができるIAMユーザーの作成

データベース接続を行うIAMユーザーを、**DBA_Debra**として作成します。

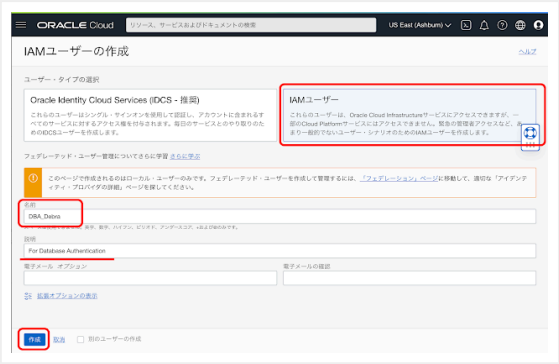
OCIコンソールの**アイデンティティ**の**ユーザー**を開きます。

ユーザーの作成をクリックします。



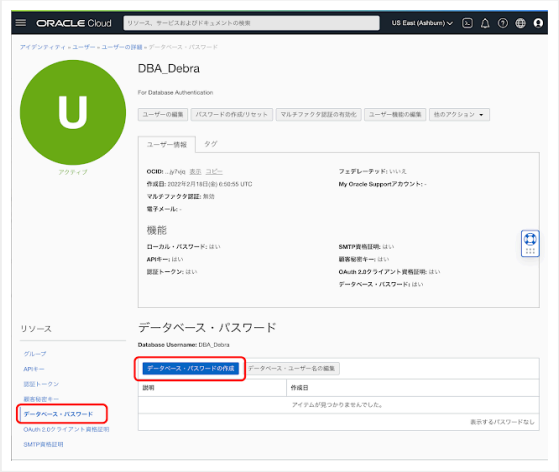
ユーザー・タイプの選択としてIAMユーザーを選びます。**名前**はDBA_Debra、**説明**は必須項目なので、何か記述します。

作成をクリックします。

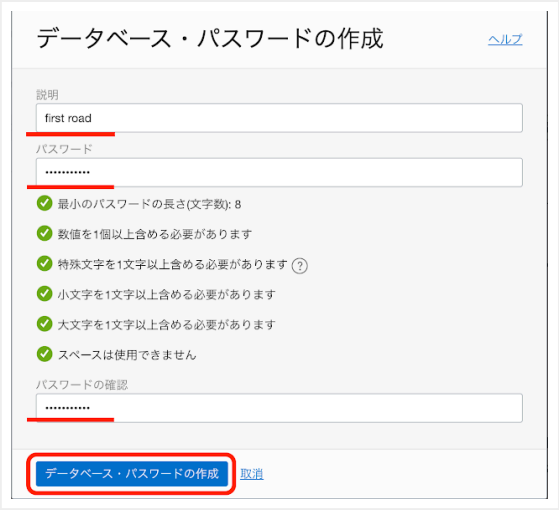


ユーザーDBA_Debraが作成されます。

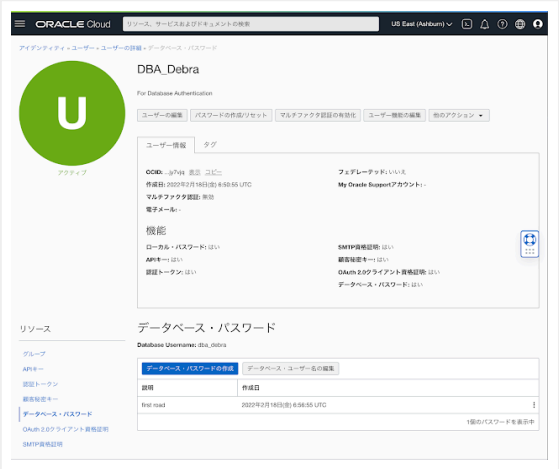
リソースの**データベース・パスワード**を開き、**データベース・パスワードの作成**を実行します。



説明と**パスワード**となる文字列を２回入力し、**データベース・パスワードの作成**をクリックします。



以上でIAMユーザーの作成は完了です。



データベースのユーザーとロールに対応するグループの作成

データベース側に作成するグローバル・ユーザーおよびグローバル・ロールに対応するグループを作成します。

グローバル・ユーザーに対応するグループは**All_DB_Users**、グローバル・ロールに対応するグループは**DB_Admin**とします。

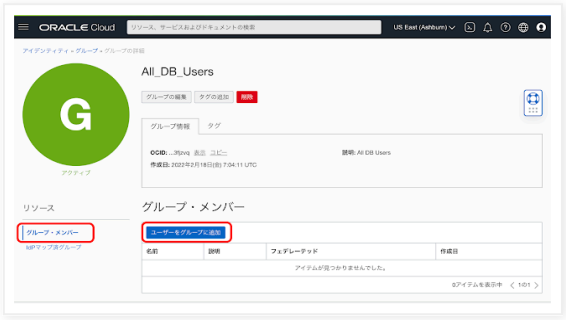
OCIコンソールの**アイデンティティ**の**グループ**を開きます。

グループの作成をクリックします。

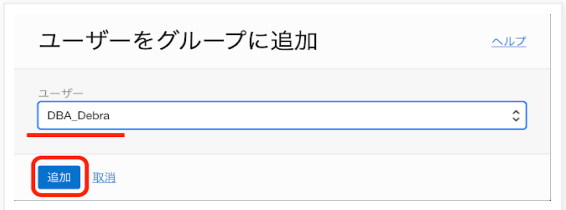
名前は**All_DB_Users**、**説明**は必須項目なので何か記述し、**作成**をクリックします。

グループAll_DB_Usersが作成されます。

ユーザーをグループに追加をクリックし、ユーザー**DBA_Debra**を追加します。



ユーザーに**DBA_Debra**を選択し、**追加**をクリックします。



同じ手順でグループ**DB_Admin**を作成します。

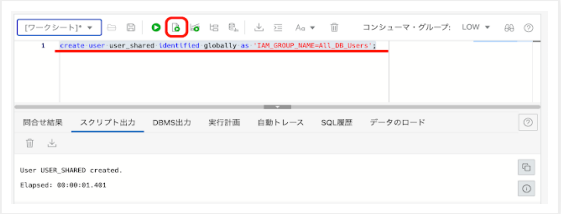
グループ**All_DB_Users**および**DB_Admin**が作成され、両方にユーザー**DBA_Debra**が所属していれば、OCI IAMの設定は完了です。

グローバル・ユーザーとグローバル・ロールの作成

データベース・アクションの**SQL**より、グローバル・ユーザー**USER_SHARED**とグローバル・ロール**SR_DBA_ROLE**を作成します。

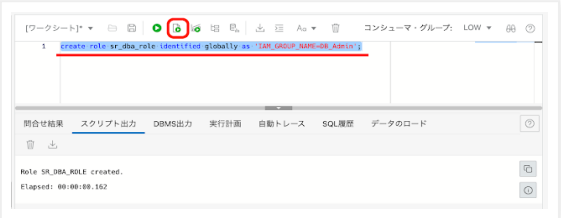
以下の**CREATE USER**文を実行し、グローバル・ユーザーUSER_SHAREDを作成します。

```
create user user_shared identified globally as 'IAM_GROUP_NAME=All_DB_Users';
```



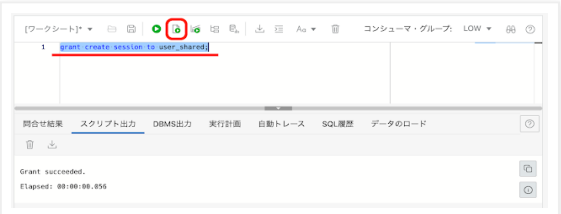
続いて、グローバル・ロール**SR_DBA_ROLE**を作成します。以下の**CREATE ROLE**文を実行します。

```
create role sr_dba_role identified globally as 'IAM_GROUP_NAME=DB_Admin';
```



データベースへ接続できるようにユーザー**USER_SHARED**に**CREATE SESSION**権限を与えます。

```
grant create session to user_shared;
```



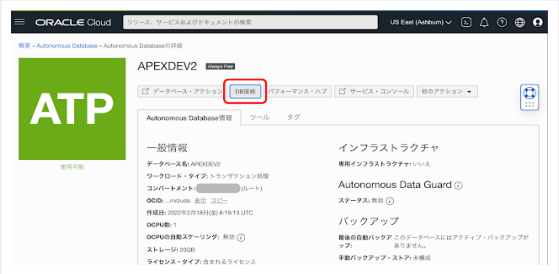
グローバル・ロールSR_DBA_ROLEには、DBAとして必要な権限が与えられることが想定されていますが、今回の作業からは割愛します。

以上で、ユーザーDBA_Debraにて、データベースに接続できるようになりました。

接続の確認

SQLclとAutonomous Databaseのウォレットを使って接続確認を行います。

Autonomous Databaseの画面より、**DB接続**を開いてウォレットをダウンロードします。



SQLclは[こちら]よりダウンロードできます。

インスタンス名を**APEXDEV2**とした場合、以下で接続します。

sql -cloudconfig Wallet_APEXDEV2.zip DBA_Debra@apexdev2_low

IAMユーザーの**データベース・パスワード**として設定したパスワードを正しく入力すると、データベースに接続できます。

```
% sql -cloudconfig Wallet_APEXDEV2.zip DBA_Debra@apexdev2_low


SQLcl: 金 2月 18 16:23:39 2022のリリース21.4 Production

Copyright (c) 1982, 2022, Oracle.  All rights reserved.

パスワード (**********?) ***********
接続先:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.14.0.1.0

SQL>
```

接続に使ったユーザーはDBA_Debraですが、CURRENT_USERはUSER_SHAREDになります。

```
SQL> select sys_context('USERENV','CURRENT_USER') from dual;

   SYS_CONTEXT('USERENV','CURRENT_USER')
_________________________________________
USER_SHARED

SQL>
```

ビューSESSION_ROLESを確認すると、ロールとしてSR_DBA_ROLEが割り当たっていることが確認できます。

```
SQL> select * from session_roles;

          ROLE
```

```
SR_DBA_ROLE

SQL>
```

以上でOCI IAMユーザーにてAutonomous Databaseに接続できることが確認できました。

完

Yuji N. 時刻: 16:43

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