

# 日々是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。

2021年8月16日月曜日

## データベース・セキュリティの活用(11) - Database Vault

最後にアプリケーションの利用者からのアクセスではなく、管理者からのアクセスからデータを保護してみます。

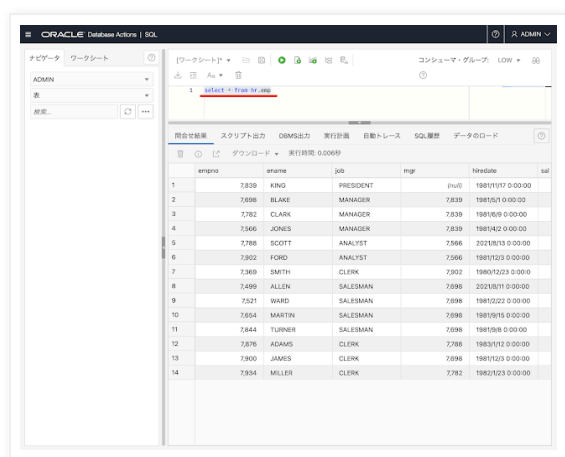
データベース・アクションにユーザーADMINで接続し、以下のSQLを実行します。

```
select * from hr.emp;
```

seminar210825-select\_hr\_emp.sql hosted with ❤ by GitHub

[view raw](#)

ユーザーADMINはデータベースの管理者なので強い権限を持っており、表HR.EMPの内容のすべてを参照することができます。



empno	ename	job	mgr	hiredate	sal
1	7350	KING	PRESIDENT	1981/01/17 0:00:00	
2	7698	BLAKE	MANAGER	1981/05/01 0:00:00	
3	7782	CLARK	MANAGER	1981/06/09 0:00:00	
4	7566	JONES	MANAGER	1981/04/02 0:00:00	
5	7788	SCOTT	ANALYST	2021/06/13 0:00:00	
6	7362	FORD	ANALYST	1981/12/23 0:00:00	
7	7369	SMITH	CLERK	1980/12/23 0:00:00	
8	7499	ALLEN	SALESMAN	2021/06/17 0:00:00	
9	7521	WARD	SALESMAN	1981/02/22 0:00:00	
10	7554	MARTIN	SALESMAN	1981/02/15 0:00:00	
11	7844	TURNER	SALESMAN	1981/09/08 0:00:00	
12	7788	ADAMS	CLERK	1983/01/12 0:00:00	
13	7800	JAMES	CLERK	1981/02/23 0:00:00	
14	7834	MILLER	CLERK	1982/12/23 0:00:00	

しかし、データベースの管理者が人事情報を参照できるのは不適切であり、可能であればアクセスは禁止すべきです。

Oracle DatabaseおよびAutonomous DatabaseではDatabase Vaultを構成することにより、管理者ユーザーからのデータのアクセスを禁止することが可能です。

以下より、Autonomous DatabaseにDatabase Vaultを構成することにより、ユーザーADMINのよる表HR.EMPの参照と操作を禁止してみます。

最初にDatabase Vaultの構成状況を確認します。ビューDBA\_DV\_STATUSを参照します。

```
select * from dba_dv_status;
```

seminar210825-dbv\_status.sql hosted with ❤ by GitHub

[view raw](#)

The screenshot shows a SQL Developer window with a query: `select * from dba_dv_status;` The result is a table with 3 rows and 2 columns: name and status.

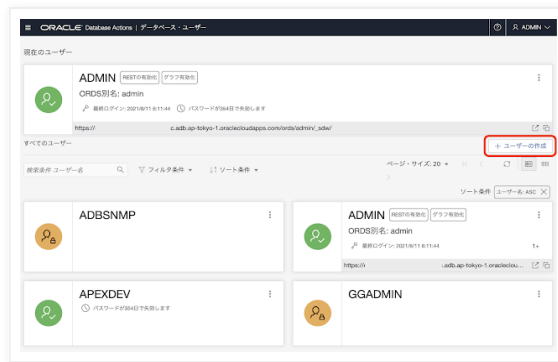
	name	status
1	DV_APP_PROTECTION	NOT CONFIGURED
2	DV_CONFIGURE_STATUS	FALSE
3	DV_ENABLE_STATUS	FALSE

Autonomous Databaseのインスタンス作成後でDatabase Vaultが未構成であればDV\_CONFIGURE\_STATUSおよびDV\_ENABLE\_STATUSともにFALSEです。

それではDatabase Vaultを構成していきます。

Database Vaultを構成するために使用するふたつのデータベース・ユーザー、ADB\_DBV\_OWNERおよびADB\_DBV\_ACCTMGRを作成します。

データベース・アクションにユーザーADMINで接続します。管理のデータベース・ユーザーを開き、ユーザーの作成を実行します。



ユーザーADB\_DBV\_OWNERを作成します。Database Vaultの設定はこのユーザーでデータベース・アクションに接続して実施するため、WebアクセスはONにします。

ユーザーの作成

ユーザー 2 付与されたロール

ユーザー名 \* ADB\_DBV\_OWNER

パスワード \* .....

パスワードの確認 \* .....

表領域の割当て制限 DATA

デフォルトの割当て制限を使用

パスワードの有効期限切れ (ユーザーの変更が必要です)

アカウントがロックされています

グラフ 2

OML 2

Webアクセス 2

Webアクセス拡張機能

ユーザーの作成 取消

ユーザーADB\_DBV\_ACCTMGRを作成します。

ユーザーの作成

ユーザー 0 付与されたロール

ユーザー名 \* ADB\_DBV\_ACCTMGR

パスワード \* .....

パスワードの確認 \* .....

表領域の割当て制限 DATA

デフォルトの割当て制限を使用

パスワードの有効期限切れ (ユーザーの変更が必要です)

アカウントがロックされています

グラフ 2

OML 2

Webアクセス 2

Webアクセス拡張機能

ユーザーの作成 取消

開発のSQLを開き、Database Vaultの構成と有効化を行います。プロシージャ  
[DBMS\\_CLOUD\\_MACADM.CONFIGURE\\_DATABASE\\_VAULT](#)を呼び出しDatabase Vaultを構成したのち、  
[DBMS\\_CLOUD\\_MACADM.ENABLE\\_DATABASE\\_VAULT](#)を呼び出し有効化します。

```
begin
  dbms_cloud_macadm.configure_database_vault(
    'ADB_DBV_OWNER',
```

```
'ADB_DBV_ACCTMGR'

);

end;

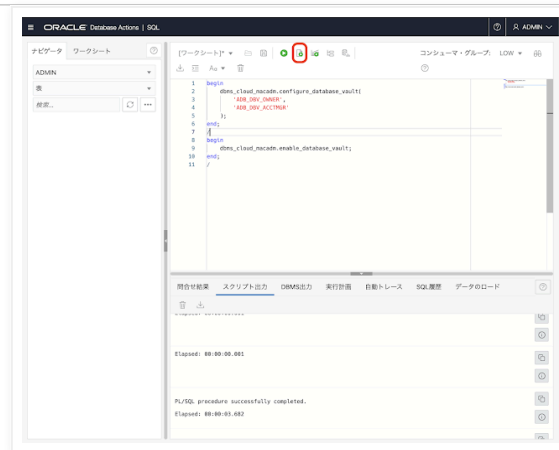
/

begin
    dbms_cloud_macadm.enable_database_vault;
end;

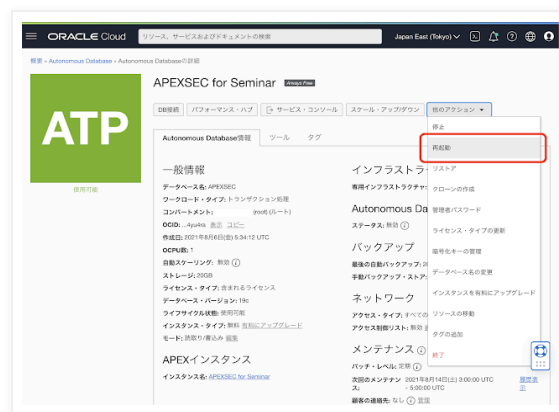
/
```

seminar210825-config\_enable\_dbv.sql hosted with ❤ by GitHub

[view raw](#)



スクリプトの実行後、データベースの再起動を行います。再起動後にDatabase Vaultが有効になります。



再起動が完了したら、データベース・アクションにユーザーADB\_DBV\_OWNERにてサインインします。

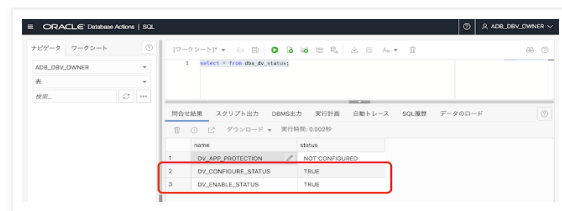
再度Database Vaultのステータスを確認します。

```
select * from dba_dv_status;
```

seminar210825-dbv\_status.sql hosted with ❤ by GitHub

[view raw](#)

DV\_CONFIGURE\_STATUS、DV\_ENABLE\_STATUSともにTRUEになっていることが確認できます。

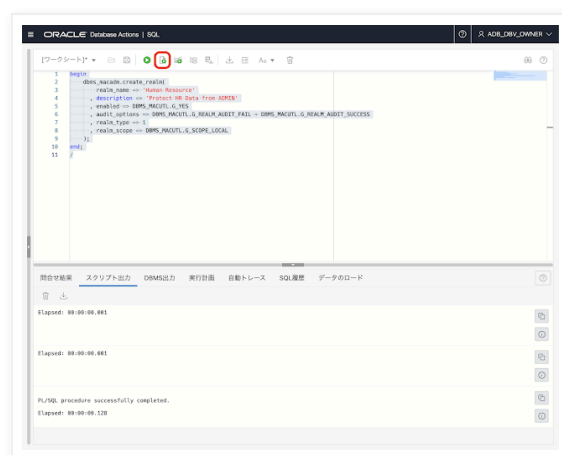


最初にレルム**Human Resource**を作成します。プロシージャ**DBMS\_MACADM.CREATE\_REALM**を呼び出します。

```
begin
  dbms_macadm.create_realm(
    realm_name => 'Human Resource'
  , description => 'Protect HR Data from ADMIN'
  , enabled => DBMS_MACUTL.G_YES
  , audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL + DBMS_MACUTL.G_REALM_AUDIT_SUCCESS
  , realm_type => 1
  , realm_scope => DBMS_MACUTL.G_SCOPE_LOCAL
  );
end;
```

seminar210825-create\_dbv\_realm.sql hosted with ❤ by GitHub

[view raw](#)



作成したレルムはビュー**DBA\_DV\_REALM**より確認できます。

作成したレルム**Human Resource**に保護対象となるオブジェクトを含めます。スキーマ**HR**のオブジェクトすべてを対象とします。プロシージャ**DBMS\_MACADM.ADD\_OBJECT\_TO\_REALM**を呼び出します。

```
begin
  dbms_macadm.add_object_to_realm(
    realm_name => 'Human Resource'
  , object_owner => 'HR'
  , object_name => '%'
  , object_type => '%'
  );
```

```
end;
```

```
/
```

seminar210825-add\_object\_to\_realm.sql hosted with ❤ by GitHub

[view raw](#)

保護対象としたオブジェクトは、ビュー[DBA\\_DV\\_REALM\\_OBJECT](#)より確認できます。

保護対象のオブジェクトへアクセスできるユーザーを設定します。プロシージャ **DBMS\_MACADM.ADD\_AUTH\_TO\_REALM**を呼び出します。

APEXのアプリケーションの開発時は、スキーマHRへのアクセスはユーザー**APEXDEV**として行われます。そのためAPEXDEVにレルム**Human Resource**へのアクセス権限を与えています。テスト用アプリケーションの認証スキームは、Real Application Securityが有効化されているため、スキーマHRへのアクセスはアプリケーション・ユーザーの権限で行われます。そのためアプリケーション・ロール**EMPLOYEE**にアクセス権限を与えています。

```
begin
    dbms_macadm.add_auth_to_realm(
        realm_name => 'Human Resource'
        , grantee => 'APEXDEV'
        , auth_options => DBMS_MACUTL.G_REALM_AUTH_OWNER
    );
end;
/
begin
    dbms_macadm.add_auth_to_realm(
        realm_name => 'Human Resource'
        , grantee => 'EMPLOYEE'
        , auth_options => DBMS_MACUTL.G_REALM_AUTH_PARTICIPANT
    );
end;
/
```

seminar200825-add\_auth\_to\_realm.sql hosted with ❤ by GitHub

[view raw](#)

レルムにアクセスできるユーザーまたはロールは、ビュー[DBA\\_DV\\_REALM\\_AUTH](#)より確認できます。

以上でスキーマHRのオブジェクトを含んだレルムHuman Resourceの構成が完了しました。レルムHuman Resourceは、ユーザーAPEXDEVとアプリケーション・ロールEMPLOYEEのみにアクセスを制限しており、管理者ユーザーであるADMINには権限を与えていません。結果として、ADMINは表HR.EMPにアクセスできません。

実際に保護の状態を確認してみます。

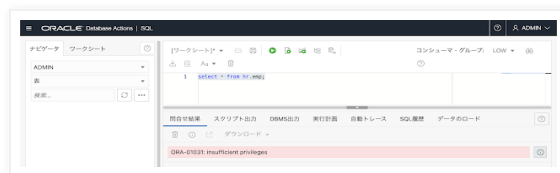
**データベース・アクション**にユーザー**ADMIN**でサインインし、表HR.EMPを検索します。

```
select * from hr.emp;
```

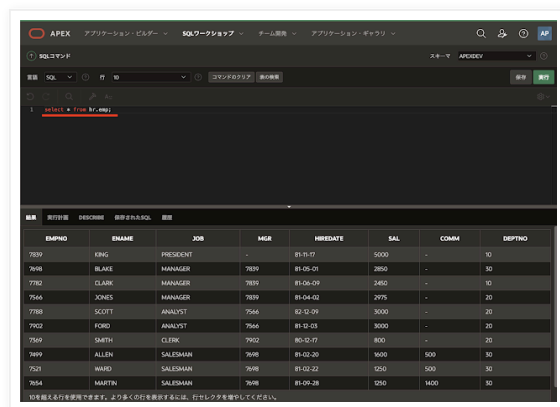
seminar210825-select\_hr\_emp.sql hosted with ❤ by GitHub

[view raw](#)

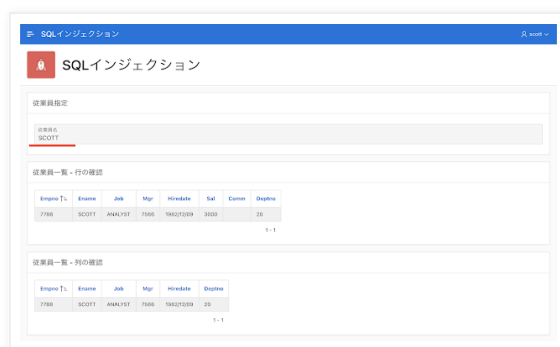
ORA-1031: insufficient privilegesのエラーが発生し、一番強い権限を持つユーザーADMINからのアクセスが拒否されていることが確認できます。



APEXのSQLワークショップのSQLコマンドからは検索できます。ユーザーAPEXDEVからのアクセスを許可しているためです。



Real Application Securityが有効になっているAPEXアプリケーションからもアクセスできます。アプリケーション・ロールEMPLOYEEを持っているとアクセスを許可しているためです。



以上でDatabase Vaultを構成し、管理者からのアクセスを禁止することができました。

Database Vaultを無効にするには、プロシージャDBMS\_CLOUD\_MACADM.DISABLE\_DATABASE\_VAULTをユーザーADB\_DBV\_OWNERにて実行します。

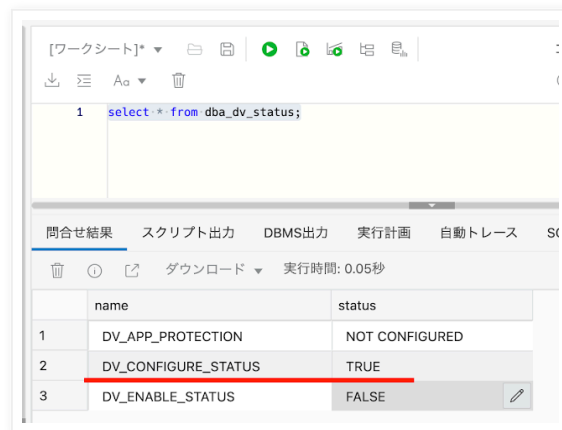
```
begin
    dbms_cloud_macadm.disable_database_vault;
end;
```

seminar200825-disable\_dbv.sql hosted with ❤ by GitHub

[view raw](#)

構成の変更は、Autonomous Databaseの再起動後に有効になります。

ビューDBA\_DV\_STATUSを確認すると、DV\_ENABLE\_STATUSはFALSEになりますが、DV\_CONFIGURE\_STATUSはTRUEのままです。



	name	status
1	DV_APP_PROTECTION	NOT CONFIGURED
2	DV_CONFIGURE_STATUS	TRUE
3	DV_ENABLE_STATUS	FALSE

一旦Database Vaultを構成すると、構成する前に戻すということはできません。無効にすることはできるため、構成前に戻す必要はありません。

Database Vaultの構成を削除するには、プロシージャ

[DBMS\\_MACADM.DELETE\\_AUTH\\_FROM\\_REALM](#)、[DBMS\\_MACADM.DELETE\\_OBJECT\\_FROM\\_REALM](#)および[DBMS\\_MACADM.DELETE\\_REALM](#)または[DBMS\\_MACADM.DELETE\\_REALM\\_CASCADE](#)を呼び出します。

```
begin
  dbms_macadm.delete_auth_from_realm(
    realm_name => 'Human Resource'
  , grantee => 'APEXDEV'
  , auth_scope => DBMS_MACUTL.G_SCOPE_LOCAL
  );
  dbms_macadm.delete_auth_from_realm(
    realm_name => 'Human Resource'
  , grantee => 'EMPLOYEE'
  , auth_scope => DBMS_MACUTL.G_SCOPE_LOCAL
  );
  dbms_macadm.delete_object_from_realm(
    realm_name => 'Human Resource'
  , object_owner => 'HR'
  , object_name => '%'
  , object_type => '%'
  );
  dbms_macadm.delete_realm(
    realm_name => 'Human Resource'
  );
end;
```

seminar200825-delete\_realm.sql hosted with ❤ by GitHub

[view raw](#)

データベース・セキュリティの活用のシリーズは本記事をもって、すべて終了です。



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: 17:51

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](#)

Powered by Blogger.

---