An Oracle White Paper

March 2014

Integrating Oracle Database Vault with Oracle Application Express

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Introduction

Oracle Database Vault (DV) provides powerful security controls to help protect application data from unauthorized access, and comply with privacy and regulatory requirements. Controls can be deployed to prevent privileged account access to application data and control sensitive operations inside the database using multi-factor authorization. Oracle Database Vault secures existing Oracle database environments transparently using Database Vault components namely - Realms, Command rules and Factors. Database Vault eliminates the need for costly and time consuming application changes that would otherwise be required to implement the same security benefits.

Oracle Application Express (Oracle APEX) is a rapid Web application development tool for the Oracle Database. The browser based interface, declarative programming framework, and simple wizards make Oracle Application Express easy to learn and enable you to quickly build robust applications.

Oracle Application Express customers can readily utilize Oracle Database Vault's strong security controls to build more secure Web applications.

This paper discusses how both Application Express and Database Vault can be integrated and configured in the Oracle database by making simple changes to Database Vault default Realms and Command rules.

Architecture

Oracle Application Express Architecture

Oracle Application Express consists of a metadata repository that stores the definitions of applications and an engine (called the Application Express engine) that performs page rendering and processing. It lives completely within the Oracle database.

The Oracle Application Express engine manages:

- Session state
- Authentication services

- Authorization services
- Page flow control
- Validations, computations, and processing
- Rendering and page processing

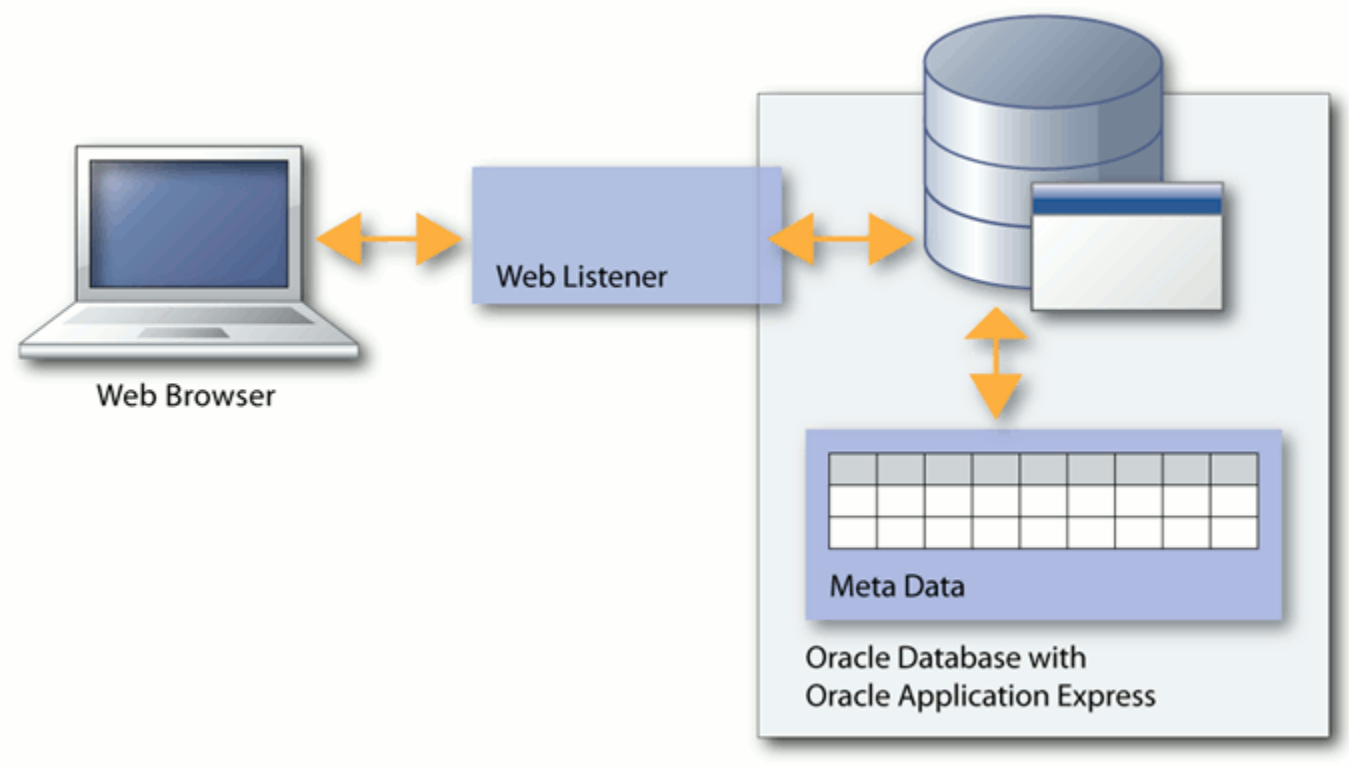


Figure 1 - Application Express Architecture

The asynchronous session state management architecture ensures that minimal CPU resources are consumed. The browser sends a URL request which is translated into the appropriate Oracle Application Express PL/SQL call. After the database processes the PL/SQL request from Oracle Application Express engine, the results are relayed back to the browser as HTML. This cycle happens for each request or submission of a page. The session state is managed in the database and does not use a dedicated database connection to manage Oracle Application Express application session state. After each request to the Oracle Application Express engine, the database session is returned to the Oracle database session pool, and is available for the next request. Thus database resources are only consumed when the Application Express engine processes or renders a page.

Oracle Database Vault Architecture

Oracle Database Vault is built into the Oracle Database kernel and is highly optimized to provide transparency to existing application performance profiles. Oracle Database Vault protects applications sensitive data from unauthorized users including users with DBA privileges. It hardens the Oracle Database and enforces industry standard best practices in terms of separating duties and access control.

Oracle Database Vault has the following components which help enterprises manage security inside the Oracle database:

- *Realms*
  - A realm is a functional grouping of database schemas, objects, and roles that must be secured. Once a realm is created, it can be used to control the use of system privileges on specific users or roles.
- *Command Rules*
  - A command rule is a special rule that can be used to control how users can execute almost any SQL statement, including SELECT, ALTER SYSTEM, database definition language (DDL), and data manipulation language (DML) statements based on ruleset evaluation.
- *Factors*
  - A factor is a named variable or attribute, such as user location, database IP address, or session user, which Oracle Database Vault can recognize and secure.
- *Rulesets*
  - A rule set is a collection of one or more rules that can be associated with a realm authorization, command rule, or factor assignment. The rule set evaluates to true or false based on the evaluation of each rule it contains and the evaluation type.

Figure 2 illustrates how Oracle Database Vault addresses the following database security concerns:

- Administrative privileged account access to application data:
  - In this case, Oracle Database Vault prevents the database administrator from accessing the schemas that are protected by the Finance realm. Although the

database administrator is the most powerful and trusted user, this administrator does not need access to application data residing within the database.

- Separation of duties for application data access:
    - In this case, the HR realm owner, created in Oracle Database Vault, has access only to the HR realm schemas and will not be able to access schemas in either the Finance realm or the Procurement realm.

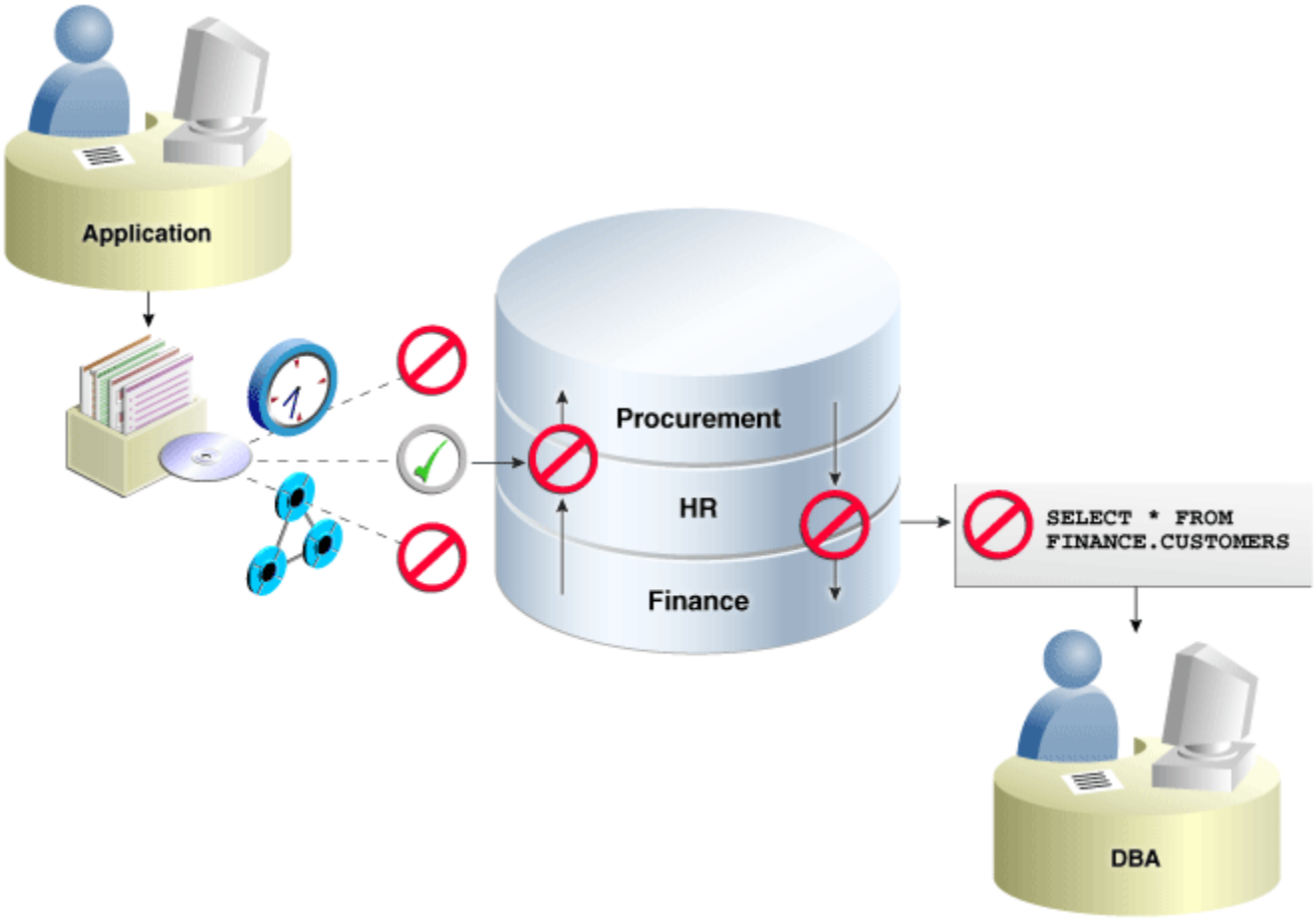


Figure 2 - Oracle Database Vault Architecture

Database consolidation can result in multiple powerful user accounts residing in a single database. This means that in addition to the overall database administrator, individual application schema owners also may have powerful privileges. Revoking some privileges may adversely affect existing applications. However, using Oracle Database Vault realms, you can enforce access to applications through a trusted path, preventing database users who have not been specifically authorized from

using powerful privileges to look at other application data. For example, an application administrator or schema owner who has SELECT ANY TABLE system privilege can be prevented from using that privilege to view other application data residing in the same database.

Prerequisites

- Oracle Database Enterprise Edition 11gR2 or above.
- Oracle Application Express 4.2.0 or later.
- Oracle Database Vault (which is released in conjunction with Oracle Database releases).

Installation steps for Oracle Application Express

Application Express is installed by default when you install the seed database with Oracle Database 11gR2 and above.

To determine whether Oracle Application Express is installed into your Oracle database and what release is installed then perform the following steps:

1. Start SQL*Plus and connect to the Oracle Database as SYS specifying the SYSDBA role. For example:
   $ sqlplus /nolog
   SQL> CONNECT SYS as SYSDBA
   Enter password: SYS_password

2. Run the following SQL statement to identify any Application Express installation:

   SQL> SELECT username FROM dba_users
   WHERE username LIKE 'FLOWS_%'
   OR username LIKE 'APEX_%';

If the SQL statement returns a username of APEX_040200 then Oracle Application Express 4.2 is already installed within your Oracle database. Therefore, you should not attempt to re-install Oracle Application Express and you should skip to the next chapter. However, if the SQL Statement returns no rows or returns rows, but does not include APEX_040200, then you will need to install

Oracle Application Express 4.2 into the Oracle Database. Usernames such as FLOWS_020100, APEX_030200, or APEX_040000 indicate that a prior release of Application Express is installed within your Oracle Database.

If Oracle Database Vault is already installed into your Oracle database then disable Database Vault before starting the installation process for Oracle Application Express, Database Vault can be disabled by following the instructions provided in Appendix A. Refer to:

- Oracle Database 11.2.x release; or
- Oracle Database 12.1.x release

Oracle recommends installing the latest version of Oracle Application Express available from the Oracle Technology Network (OTN). At the time of writing this paper the latest version available on OTN is Application Express 4.2.4.00.08. To download and install Oracle Application Express go to http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html. After reviewing and accepting the License Agreement, download the Application Express software. Follow the Oracle Application Express 4.2 Installation Guide link below to install it into your Oracle Database. http://docs.oracle.com/cd/E37097_01/doc/install.42/e35123/toc.htm

If you disabled Oracle Database Vault before installing Oracle Application Express then it is important to re-enable Database Vault before proceeding. To enable Database Vault follow the instructions provided in Appendix A. Refer to:

- Oracle Database 11.2.x release; or
- Oracle Database 12.1.x release

Note: Post installation tasks such as embedded PLSQL gateway or Oracle HTTP server configuration will have no dependency on Database Vault enable status. But please note that, user management tasks, for example ALTER USER, are now assigned to DV_ACCTMGR role as described in How Database Vault affects Database Operations section.

Installation steps for Database Vault

Oracle database includes Database Vault by default, but you must register before you can use it. In order to determine whether Database Vault is registered and enabled in your Oracle database, please perform the following query using any user connected to the database. If Oracle Database Vault is enabled, the query returns TRUE. Otherwise, it returns FALSE.

Remember that the PARAMETER column value is case sensitive.

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Oracle Database Vault';
```

If you are using Oracle Database release 11gr2 and Database Vault is not already registered, please follow Database Vault Administrator's Guide – 3 Registering Oracle Database Vault http://docs.oracle.com/cd/E11882_01/server.112/e23090/getting_started.htm#DVADM30031 to register and enable Database Vault:

If you are using Oracle Database 12c and Oracle Database Vault is not already registered, please use the following steps to register and enable Database Vault:

1. Use manual instructions provided at http://docs.oracle.com/cd/E16655_01/server.121/e17608/getting_started.htm#DVADM30031 to register and enable Database Vault
2. Alternatively, Database Configuration Assistant (DBCA) can also be used to register and enable Database Vault.

How Database Vault affects the database operations

1. Oracle Database Vault prevents SYS user and users with DBA role to access schemas or objects protected by realms.
2. Some database initialization parameter changes are restricted as ALTER SYSTEM command rule protects these parameters.
3. Oracle Database users are required to have Oracle Database Vault authorization for data pump and job scheduling on Database Vault protected schemas.
4. Account management duties such as creating, altering and dropping users are assigned to a new role called DV_ACCTMGR and a user with DBA role will no longer be able to

perform those duties. Note that while registering Database Vault in section Installation steps for Database Vault, there were two Database Vault specific users created – a user for Database Account Management with DV_ACCTMGR role and another user for Database Vault Owner with DV_OWNER role.

For example, when administrators with the DBA role attempt to create a user when Database Vault is enabled, Oracle Database Vault will throw the following error –

```
SQL> create user dvuser1 identified by DvUser1;
create user dvuser1 identified by DvUser1
                                  *

ERROR at line 1:
ORA-01031: insufficient privileges
```

5. Oracle Database Vault command rules can be used to restrict SQL command execution by defining rules that can be enforced when the command is executed. For example, a command rule can be defined to restrict the ALTER USER command. A rule can be associated with a command to allow or disallow execution when certain conditions defined in the rule are met.
6. Once Database Vault is registered, reconfiguration of Network ACL is needed. Please refer http://docs.oracle.com/cd/E11882_01/server.112/e23633/afterup.htm#UPGRD12428 to create a new Network ACL for the Oracle Application Express user APEX_040200.

For more details on Database Vault security restrictions, and realm and command rule configurations, please see Database Vault Administrator Guide for 12.1 or Database Vault Administrator Guide for 11.2

Note: Please review the Known issues and limitations section and apply relevant patches before proceeding.

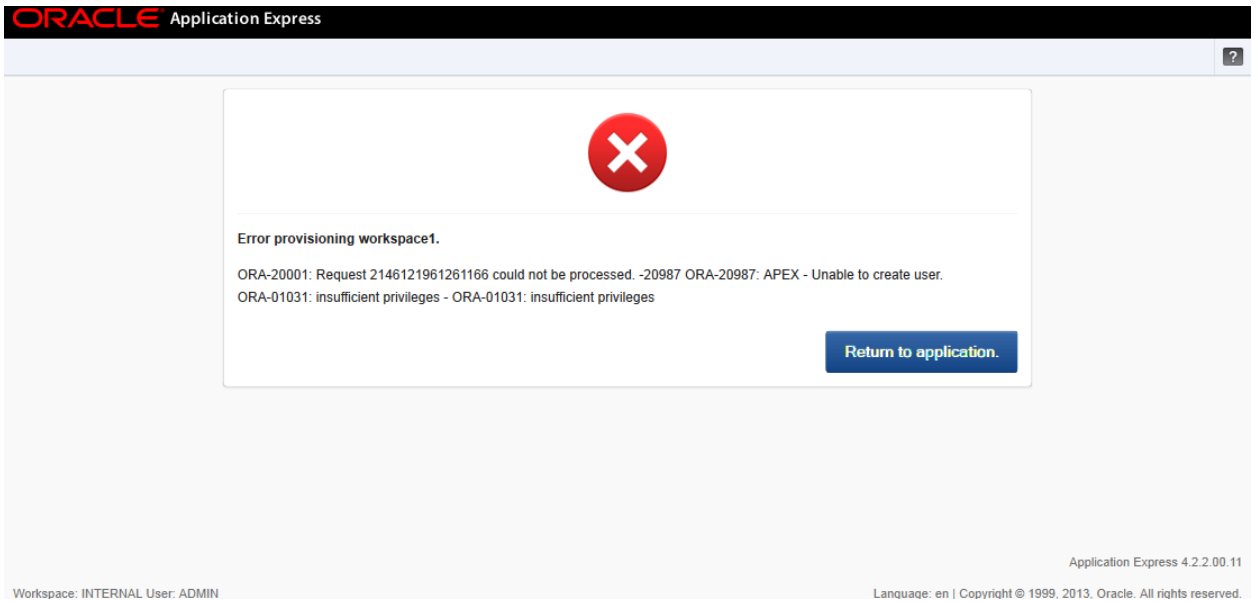
Using Oracle Application Express on a Database Vault enabled Oracle Database

Before starting Oracle Application Express application development on an Oracle Database Vault enabled Oracle database, the APEX_040200 user must be given the appropriate access to Database Vault default realms and command rules. This user should also be able to create new schemas within the Oracle database when provisioning a new workspace. To achieve this, please run the scripts

listed in Appendix A to enable Oracle Application Express schema user, APEX_040200, to get the required Database Vault authorizations. Note that the Oracle Database 12.1.x version of the script is different from the one for Oracle Database 11.2.x. Therefore, please make sure to run the appropriate script for your environment. In addition, if you choose not to allow Oracle Application Express to create new schemas, as part of provisioning a workspace, then please modify the script to remove the grant of DV_ACCTMGR role to APEX_040200 user.

Configuring Oracle Application Express-Database Vault environment

Before configuring the Oracle Application Express-Database Vault environment, by running the scripts provided in Appendix A, please note that when workspace creation is attempted with a new schema, Oracle Application Express throws an ORA-1031 error as shown below:



Before running the script, please gather *Database Vault Owner user name and password*, and *Database Vault Account Manager user name and password* details. Create an SQL file called apex_dv_setup.sql by copying the relevant script from Appendix A, based on your database version, and then run this script using SQL*Plus. You should see the output given below:

```
$ sqlplus /nolog
```

```
SQL*Plus: Release 11.2.0.3.0 Production on ..
Copyright (c) 1982, 2011, Oracle.  All rights reserved.
SQL> @apex_dv_setup.sql
DV OWNER USERNAME: <DATABASE VAULT OWNER USER NAME>
DV OWNER USER PASSWORD:
DV ACCOUNTMGR USERNAME: <DATABASE VAULT ACCT MGR USER NAME>
DV ACCOUNTMGR USER PASSWORD:
Connected.
Connected.
Connected.
MAX(USERNAME)
------------------------------
APEX_040200

old   4:                 grantee         => '&apex_user',
new   4:                 grantee         => 'APEX_040200',

PL/SQL procedure successfully completed.
old   4:                 grantee         => '&apex_user',
new   4:                 grantee         => 'APEX_040200',
PL/SQL procedure successfully completed.

PL/SQL procedure successfully completed.
PL/SQL procedure successfully completed.
Connected.
old   1: grant dv_acctmgr to &apex_user
new   1: grant dv_acctmgr to APEX_040200
Grant succeeded.

SQL> exit
Disconnected from Oracle Database 11g Enterprise Edition
Release 11.2.0.3.0 - 64bit Production
```

```
With the Partitioning, Oracle Label Security, OLAP, Data
Mining,
Oracle Database Vault and Real Application Testing options
```

Running this script allows the Oracle Application Express development environment to work with Database Vault seamlessly. In addition, it enables Application Express, in its provisioning process, to create new database schemas. Logging in as the Oracle Database Vault owner, one can create a new realm for each schema created by Application Express provisioning and protect the data in those schemas.

Patching Oracle Application Express when Database Vault is enabled

If you wish to upgrade Oracle Application Express to a later patch set then you must first disable Database Vault, applying the Application Express patch, and then re-enable Database Vault. This process is the very similar to the steps provided in the Installation steps for Oracle Application Express section. Follow these steps to patch Oracle Application Express 4.2 –

1. Disable Database Vault using the instructions provided based on your Oracle Database release
    a. Oracle Database 11.2.x release
    b. Oracle Database 12.1.x release
2. Download the relevant patch set from My Oracle Support using the Patch Number provided on the Application Express 4.2 Downloads page. Follow the instructions provided within the Patch Set Notes on this same page.
3. Once Oracle Application Express is patched, enable Database Vault using the instructions provided based on your Oracle Database release
    a. Oracle Database 11.2.x release
    b. Oracle Database 12.1.x release

Conclusion

Oracle Database Vault provides additional security capabilities for Oracle Application Express applications, by protecting database dictionary objects and enabling administrators to create realms on schemas that are associated with Oracle Application Express workspaces. In addition, Database Vault's separation of duties can be used to restrict the administrators from accessing application data and limit Oracle Application Express developers, and the applications they develop, from executing specific SQL commands or accessing specific data.

Known issues and limitations

Bug# 16571244	DBMS_RLS may fail on Database Vault protected objects with ORA-1031 in Database Vault environment when the package is invoked through other PL/SQL procedures.
Bug# 16524926	Error ORA-1031 with Oracle Multimedia and Database Vault Realm protected DB Schema.
Bug# 16675668	A query on spatial data may fail with ORA-1031 when Database Vault is enabled.
Bug# 16718622	Error ORA-1031 when using Oracle Text index type with Database Vault.
Bug# 16264991	Error ORA-1031 when scheduler job is running in Database Vault enabled environment.

Appendix A

Oracle Database 11.2.x (apex_dv_setup_112.sql)

```
--#####- START OF SCRIPT apex_dv_setup_112.sql  -###############
--#############################################################
--# Grant dv_acctmgr, ODD and Account manager for APEX_0XXXXX;
--# Update command rules
--# Please note that if the database has multiple APEX_0* schema, please replace
--# APEX_0% with APEX_  schema name that is relevant to your environment if right
APEX_
--# schema is not selected.
--#############################################################
ACCEPT DVOWNER PROMPT "DV OWNER USERNAME: "
ACCEPT DVOWNERPWD hide PROMPT "DV OWNER USER PASSWORD: "
ACCEPT DVACCTMGR PROMPT "DV ACCOUNTMGR USERNAME: "
ACCEPT DVACCTMGRPWD hide PROMPT "DV ACCOUNTMGR USER PASSWORD:"


connect &DVOWNER/&DVOWNERPWD

whenever sqlerror exit sql.sqlcode

connect &DVACCTMGR/&DVACCTMGRPWD

connect &DVOWNER/&DVOWNERPWD

column max(username) new_val apex_user

select max(username) from all_users where username like 'APEX_0%';

whenever sqlerror continue



--#################################################################
-- If already granted, delete authorizations to the default realms for Oracle
Application Express schema user.
-- Ignore ORA-47261 error if authorizations are not granted before
--#################################################################
begin
        dbms_macadm.delete_auth_from_realm(
                realm_name      => 'Oracle Data Dictionary',
                grantee         => '&apex_user');
```

```
end;
/
begin
        dbms_macadm.delete_auth_from_realm(
                realm_name      => 'Database Vault Account Management',
                grantee         => '&apex_user');
end;
/
whenever sqlerror exit sql.sqlcode
begin
        dbms_macadm.add_auth_to_realm(
                realm_name      => 'Oracle Data Dictionary',
                grantee         => '&apex_user',
                rule_set_name   => null,
                auth_options    => dbms_macutl.g_realm_auth_owner);
end;
/
begin
        dbms_macadm.add_auth_to_realm(
                realm_name      => 'Database Vault Account Management',
                grantee         => '&apex_user',
                rule_set_name   => null,
                auth_options    => dbms_macutl.g_realm_auth_owner);
end;
/
exec dbms_macadm.update_rule('Is User Manager',
'DVSYS.DBMS_MACUTL.USER_HAS_ROLE_VARCHAR(''DV_ACCTMGR'',SYS_CONTEXT(''userenv'',''curr
ent_user'')) = ''Y''')


exec  dbms_macadm.update_rule('Is Alter DVSYS Allowed',
'DVSYS.DBMS_MACADM.IS_ALTER_USER_ALLOW_VARCHAR(SYS_CONTEXT(''userenv'',''current_user'
')) = ''Y''')


connect &DVACCTMGR/&DVACCTMGRPWD


grant dv_acctmgr to &apex_user;


--#####- END OF SCRIPT apex_dv_setup_112.sql  -#################
================================================================
```

Oracle Database 12.1.x (apex_dv_setup_121.sql)

```
--#####- START OF SCRIPT apex_dv_setup_121.sql  -###############
--############################################################
--# Grant dv_acctmgr, ODD and Account manager for APEX_0XXXXX;
--# Update command rules
--# Please note that if the database has multiple APEX_0* schema, please replace
--# APEX_0% with APEX_  schema name that is relevant to your environment if right
APEX_
--# schema is not selected.
--############################################################


ACCEPT DVOWNER PROMPT "DV OWNER USERNAME: "
ACCEPT DVOWNERPWD hide PROMPT "DV OWNER USER PASSWORD: "
ACCEPT DVACCTMGR PROMPT "DV ACCOUNTMGR USERNAME: "
ACCEPT DVACCTMGRPWD hide PROMPT "DV ACCOUNTMGR USER PASSWORD: "


connect &DVOWNER/&DVOWNERPWD

whenever sqlerror exit sql.sqlcode

connect &DVACCTMGR/&DVACCTMGRPWD

connect &DVOWNER/&DVOWNERPWD

column max(username) new_val apex_user

select max (username) from all_users where username like 'APEX_0%';

whenever sqlerror continue


--############################################################
-- If already granted, delete authorizations to the default realms for Oracle
Application Express schema user.
-- Ignore ORA-47261 error if authorizations are not granted before
--############################################################


begin
        dbms_macadm.delete_auth_from_realm(
                realm_name      => 'Oracle Default Schema Protection Realm',
                grantee         => '&apex_user');
end;
/
begin
        dbms_macadm.delete_auth_from_realm(
```

```
                realm_name      => 'Oracle System Privilege and Role Management
Realm',
                grantee         => '&apex_user');
end;
/
begin
        dbms_macadm.delete_auth_from_realm(
                realm_name      => 'Oracle Default Component Protection Realm',
                grantee         => '&apex_user');
end;
/
begin
        dbms_macadm.delete_auth_from_realm(
                realm_name      => 'Database Vault Account Management',
                grantee         => '&apex_user');
end;
/
whenever sqlerror exit sql.sqlcode

begin
        dbms_macadm.add_auth_to_realm(
                realm_name      => 'Oracle Default Schema Protection Realm',
                grantee         => '&apex_user',
                rule_set_name   => null,
                auth_options    => dbms_macutl.g_realm_auth_owner);
end;
/
begin
        dbms_macadm.add_auth_to_realm(
                realm_name      => 'Oracle System Privilege and Role Management
Realm',
                grantee         => '&apex_user',
                rule_set_name   => null,
                auth_options    => dbms_macutl.g_realm_auth_owner);
end;
/
begin
        dbms_macadm.add_auth_to_realm(
                realm_name      => 'Oracle Default Component Protection Realm',
                grantee         => '&apex_user',
```

```
                rule_set_name   => null,
                auth_options    => dbms_macutl.g_realm_auth_owner);
end;
/
begin
        dbms_macadm.add_auth_to_realm(
                realm_name      => 'Database Vault Account Management',
                grantee         => '&apex_user',
                rule_set_name   => null,
                auth_options    => dbms_macutl.g_realm_auth_owner);
end;
/


exec dbms_macadm.update_rule('Is User Manager',
'DVSYS.DBMS_MACUTL.USER_HAS_ROLE_VARCHAR(''DV_ACCTMGR'',SYS_CONTEXT(''userenv'',''curr
ent_user'')) = ''Y''')


exec  dbms_macadm.update_rule('Is Alter DVSYS Allowed',
'DVSYS.DBMS_MACADM.IS_ALTER_USER_ALLOW_VARCHAR(SYS_CONTEXT(''userenv'',''current_user'
')) = ''Y''')


connect &DVACCTMGR/&DVACCTMGRPWD


grant dv_acctmgr to &apex_user;


--#####- END OF SCRIPT apex_dv_setup_121.sql  -################
```

Integrating Oracle Database Vault with Oracle Application Express
March 2014
Author: Sarma Namuduri
Contributing Authors: Joel Kallman, Kamal Tbeileh, Chaitanya Koratamaddi and Ji-won Byun

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment