ORACLE®

APPLICATION EXPRESS

An Oracle White Paper
August 2015

Integrating Oracle Database Vault with Oracle Application Express

ORACLE®

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

Executive Overview

Oracle Database Vault provides powerful security controls to help protect application data from unauthorized access, and comply with privacy and regulatory requirements. Controls can be deployed to block privileged account access to application data and control sensitive operations inside the database using multi-factor authorization. Oracle Database Vault secures existing database environments transparently, using Database Vault components such as Realms, Command Rules, and Factors. Oracle 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 Oracle's primary tool for developing Web applications with SQL and PL/SQL. Using only a web browser, you can develop and deploy professional Web-based applications for desktops and mobile devices. Oracle Application Express is a fully supported, no cost option of the Oracle Database, and is installed by default in all editions of the Oracle Database. Users require only a Web browser to build, develop, and deploy Oracle Application Express applications. No additional client software is required.

Oracle Database Vault restricts access to specific areas in an Oracle database from any user, including users who have administrative access. For example, your enterprise application's requirement is to restrict administrative access to employee salaries, customer credit records, or other sensitive information. By integrating Oracle Database Vault with Oracle Application Express, Oracle Application Express customers can readily utilize Oracle Database Vault's strong security controls to build more secure Web applications. All that is needed is a simple integration of the two products within the Oracle Database.

This paper covers how to integrate and configure Oracle Database Vault and Oracle Application Express in the Oracle Database. It provides a detailed step-by-step approach to this integration in both Oracle Database 11g Release 2 and Oracle Database 12c.

Oracle Application Express Overview

Oracle Application Express is a rapid Web application development tool for the Oracle Database. Oracle Application Express enables you to design, develop and deploy beautiful, responsive, database-driven applications using only your web browser. Oracle Application Express is a no-cost option of the Oracle Database and can be installed into any edition of the Oracle Database 10.2.0.4 and above, which includes Enterprise Edition, Standard Edition, Standard Edition One, and Express Edition (XE).

Oracle Application Express offers all the tools you need to be productive: a modern browser-based IDE, drag and drop layout, sophisticated code editing, and a rich property editor. With Application Express, you can focus on the problem at hand. Much of the development process is managed for you: security, authentication, database interactions, input validation, session state management and many other dependencies work out of the box. All the tools you need are available in a single, extensible platform, which runs as a part of the Oracle Database.

Your application developed in Oracle Application Express does not require complex build scripts to run in production. More importantly, your application automatically scales with your Oracle Database. You can seamlessly move applications to and from the Oracle Database Cloud Service, private (on premise) clouds and other public cloud services.

Oracle Application Express installs with your Oracle Database and is comprised of data in tables and PL/SQL code. Whether you run the Oracle Application Express development environment or an application you built using Oracle Application Express, the process is the same. Your browser sends a URL request that is translated into the appropriate Oracle Application Express PL/SQL call. After the database processes the PL/SQL, the results are relayed back to your browser as HTML. This cycle happens each time you request or submit a page. The application session state is managed in the database tables within Oracle Application Express. It does not use a dedicated database connection. Instead, each request is made through a separate database session, consuming minimal CPU resources.
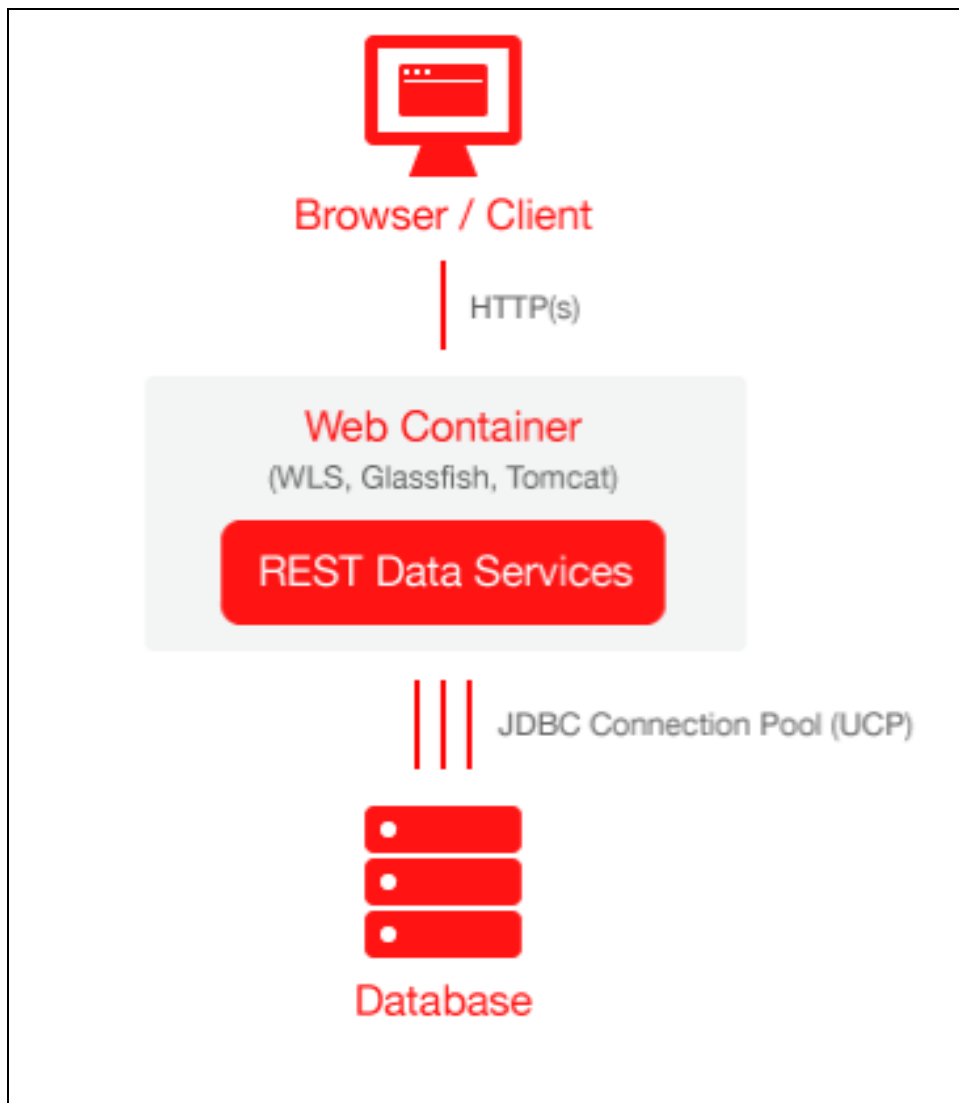

Figure 1. Oracle Application Express Architecture

The Oracle Application Express architecture requires some form of Web server to proxy requests between a client Web browser and the Oracle Application Express engine. The Web server options include:

- **Oracle REST Data Services**: Oracle REST Data Services (ORDS) is a Java based, free tool that is fully supported when used with Oracle WebLogic Server, Oracle Glassfish Server, and Tomcat.
- **Oracle HTTP Server**: The Oracle HTTP Server (Apache) with mod_plsql plugin can be placed on the same physical machine as the database, or on a separate physical machine.
- **Embedded PL/SQL Gateway**: The Embedded PL/SQL Gateway (EPG) runs in the Oracle XML DB Protocol Server within the Oracle Database and includes the core features of mod_plsql.

To learn more about Oracle Application Express, see *Oracle Application Express documentation*.

Oracle Database Vault Overview

Oracle Database Vault comes installed by default with Oracle Database and helps you to control administrative access to your data. It provides powerful security controls to help protect application data from unauthorized access, and comply with privacy and regulatory requirements. You can deploy controls to block privileged account access to application data and control sensitive operations inside the database using multi-factor authorization. Through the analysis of privileges and roles, you can increase the security of existing applications. Oracle Database Vault secures existing database environments transparently, eliminating costly and time consuming application changes.

You can enable Oracle Database Vault on the command line. Once enabled, you need to simply restart the Oracle Database for Oracle Database Vault controls to be in effect. There is no need to install any additional software or re-linking of the Oracle Database executable.

Oracle Database Vault enables you to create the following set of components to manage security for your enterprise database instance:

- **Realms**: A realm is a protection zone inside the database that prevents privileged users such as DBAs from accessing any data inside it. For example, as Oracle Database Vault administrator, you can secure a set of schemas, objects, and roles that are related to accounting, sales, or human resources. After you have secured these into a realm, you can use the realm to control the use of system and object privileges to specific accounts or roles. This enables you to provide fine-grained access controls for anyone who wants to use these schemas, objects, and roles.
- **Command Rules**: A Command Control or a Command Rule is a special security policy that you create to control how users can execute almost any SQL statements including SELECT, ALTER SYSTEM, database definition language (DDL) statements, and data manipulation language (DML) statements. Command rules must work with Rule Sets to determine whether or not a statement is allowed.
- **Factors**: A factor is a named variable or attribute, such as a user location, database IP address, or session user, which Oracle Database Vault can recognize and use. You can use factors in rules to control activities such as authorizing database accounts to connect to the

database or the execution of a specific database command to restrict the visibility and manageability of data.

- **Rule Sets**: A rule set is a collection of one or more rules that you can associate with a realm authorization, command rule, factor assignment, or secure application role. The rule set evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True).
- **Secure Application Roles**: A secure application role is a special Oracle Database role that can be enabled based on the evaluation of an Oracle Database Vault rule set.

Oracle predefined system users such as SYSTEM and roles such as DBA can access any application data within the database. Though organizations enforce strict rules on who can be granted privileged access or DBA access, these accounts and roles are the primary target of hackers. There is also a threat of insiders misusing these accounts and roles to gain access to confidential information. One of the key areas of security implementation in application development therefore, is to ensure controls on privileged and DBA accounts.

By utilizing Realm, Oracle Database Vault prevents access to application data from privileged accounts. However, at the same time, it continues to allow the regular authorized administrative access on the database. You can use Realms around all or specific application tables and schemas to protect them from unauthorized access while continuing to allow access to owners of those tables and schemas and also to users who have been granted direct access to those database objects.

Database consolidation can result in multiple powerful user accounts residing in a single database. This means that in addition to the DBA, individual application schema owners also may have powerful privileges. If you revoke some privileges, it would 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.

Figure 2 shows how an Oracle Database Vault Realm blocks a DBA from accessing the HR Realm and also how it blocks the HR user from accessing the Fin Realm. It illustrates how Oracle Database Vault addresses the following database security concerns:

- **Administrative privileged account access to application data**: 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**: The HR realm owner, created in Oracle Database Vault, has access to the HR realm schemas.

Figure 2 also shows how Oracle Database Vault ensures blocking applications with powerful system-wide privileges from looking at other application's data inside the database. For example, system-wide privileges include select any table, that is generally granted not only to DBAs but also found in many application environments.

Figure 2. Oracle Database Vault Security

The following are a few examples of how Oracle Database Vault affects database operations:

- Oracle Database Vault prevents SYS user and users with DBA role to access schemas or objects protected by Realms
- Some database initialization parameter changes are restricted as ALTER SYSTEM command rule protects these parameters
- Oracle Database users are required to have Oracle Database Vault authorization for data pump and job scheduling on Oracle Database Vault protected schemas.
- Account management duties such as creating, altering and dropping users are assigned to a new role DV_ACCTMGR and therefore a user with DBA role will no longer be able to perform those duties. During the Oracle Database Vault registration process, two specific users are created: One for Database Account Management with DV_ACCTMGR role and the other for Database Vault Owner with DV_OWNER role. Once Oracle Database Vault is enabled, if an administrator with the DBA role creates an user, you see the following error:

```
SQL> create user dvuser1 identified by DvUser1;
create user dvuser1 identified by DvUser1
                                  *
ERROR at line 1:
ORA-01031: insufficient privileges
```

- To restrict SQL command execution, you can use the Oracle Database Vault command rules. 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.
- Once Oracle Database Vault is registered, you need to reconfigure Network ACL

To learn more about Oracle Database Vault, see *Oracle Database Vault Administrator's Guide*.

Prerequisites

Before performing the tasks in this paper, you should have installed the following Oracle software:
- Oracle Database 11g Release 2 or above
- Oracle Application Express 4.2 or later

Oracle Database Vault with Oracle Database is installed by default.

You can download Oracle Database software from the Downloads page on Oracle Technology Network. For more information on how to install Oracle Database, see the *Installation Guide* for your platform.

To download the latest Oracle Application Express, navigate to the Downloads page on Oracle Technology Network. For more information on how to install Oracle Application Express, navigate to the documentation page and review the *Installation Guide.*

The steps and screenshots provided in this white paper use the following software:

- Oracle Database 11g Release 2 (11.2.0.3.0)
- Oracle Database 12c Release 1 (12.1.0.2.0)
- Oracle Application Express 5.0.0.00.31

The screenshots and steps might be different for later versions of the above Oracle products.

To perform the steps required to integrate Oracle Database Vault with Oracle Application Express, you need to first download and unzip the **apex-dbv-files.zip** to your working directory.

Note:
- If Oracle Database Vault is already registered in your Oracle Database, and enabled, you must first disable it before installing Oracle Application Express. Once Oracle Application Express is installed, you can again enable Oracle Database Vault. See the *Disabling and Enabling Oracle Database Vault* section, later in this document, for the steps required for your specific Oracle Database version.
- Oracle Application Express post installation tasks such as embedded PL/SQL Gateway, or Oracle HTTP Server configuration have no dependency on Oracle Database Vault enable status

Integrating Oracle Database Vault with Oracle Application Express

Integrating Oracle Database Vault with Oracle Application Express involves the following steps:

1. Installing Oracle Database
2. Installing Oracle Application Express
3. Verifying if Oracle Database Vault is enabled or disabled
4. Registering Oracle Database Vault with an Oracle Database
5. Configuring the Oracle Application Express – Oracle Database Vault environment
6. Testing the environment

This white paper covers Oracle Database Vault in both Oracle Database 11g Release 2 and Oracle Database 12c. Depending upon your Oracle Database version, you should review the appropriate section.

After you install Oracle Database and Oracle Application Express, you must register (that is, configure and enable) Oracle Database Vault. Oracle Database includes Database Vault when you choose to include a default database in the installation process, but you must register it before you can use it. If you create a custom database, then you can use DBCA to install and enable Database Vault for it. As part of the registration process, you create the Database Vault administrative accounts. The registration process also creates the Database Vault DVSYS and DVF schemas. The registration process enables Oracle Label Security if it is not already enabled.

You can verify if Oracle Database Vault is enabled or disabled, by querying the V$OPTION data dictionary view. Any user can query this view. If Oracle Database Vault is enabled, the query returns TRUE. Otherwise, it returns FALSE. Note that the PARAMETER column value is case sensitive.

```
sqlplus sys as sysdba
Enter password: password

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

Oracle Database Vault in Oracle Database 11g Release 2

To perform the tasks discussed in this white paper, you should have already installed Oracle Database and Oracle Application Express. See the *Prerequisites* section. In this section, you learn how to integrate Oracle Application Express with Oracle Database Vault in Oracle Database 11g Release 2.
First, connect as any user and run the query on V$OPTION data dictionary view. The query should return FALSE, if not see the *Disabling and Enabling Oracle Database Vault* section later in this paper.

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

Registering Database Vault with Oracle Database

The registration process creates Database Vault administrative accounts and also the DVSYS and DVF schemas for Database Vault. Perform the following steps:

1. From the command line, verify the status of Database Console.

   ```
   ./emctl status dbconsole
   ```

2. Connect to SQL*Plus as SYS user with the SYSOPER privilege and shut down the database

   ```
   CONNECT sys as sysoper
   Enter password: password
   SQL> SHUTDOWN IMMEDIATE
   SQL> EXIT
   ```

3. Using the command line, stop the Database Console process and listener.

   ```
   emctl stop dbconsole
   lsnrctl stop [listener_name]
   ```

4. Before you can use Oracle Database Vault, you must enable Oracle Label Security. The `make` command enables both Oracle Database Vault (`dv_on`) and Oracle Label Security (`lbac_on`).

   ```
   cd $ORACLE_HOME/rdbms/lib
   make -f ins_rdbms.mk dv_on lbac_on ioracle
   ```

5. Log in to SQL*Plus as user SYS with the SYSOPER privilege and restart the database. Then from the command line, restart the listener.

   ```
   sqlplus sys as sysoper
   Enter password: password
   SQL> STARTUP
   SQL> EXIT

   lsnrctl start [listener_name]
   ```

6. Start Database Configuration Assistant. By default, dbca is in $ORACLE_HOME/bin directory.

   ```
   dbca
   ```

7. In the Welcome page, click Next.
8. In the Operations page, select Configure Database Options and click Next.
9. In the Database page, select the database where you installed Oracle Database and then click Next.
10. Now the Database Content page appears. If Oracle Label Security is already enabled, select the Oracle Database Vault option and click Next. But, if Oracle Label Security is not

enabled, first select Oracle Label Security and then select Oracle Database Vault option. Then, click Next.

11. In the Oracle Database Vault Credentials page, specify the name and password for Database Vault Owner and Database Vault Account Manager. Then, click Next.

12. In the Connection Mode page, select either Dedicated Server Mode or Shared Server Mode depending on the selection you made when you created the database. Click Finish and then click OK in the confirmation pages.

13. Exit Database Configuration Assistant

14. Using the command line, restart the Database Console process

```
emctl start dbconsole
```

Configuring and Testing the Database Vault - Application Express Environment

In this section, you run the **apex_dv_setup_112.sql** script which allows the Oracle Application Express development environment to work with Oracle Database Vault seamlessly. In addition, it enables Oracle Application Express, in its provisioning process, to create new database schemas. Logging in as the Oracle Database Vault owner, you can create a new realm for each schema created by Application Express provisioning and protect the data in those schemas.

1. Before configuring the Oracle Database Vault – Oracle Application Express environment, perform a quick test by manually creating a new Workspace in Oracle Application Express. Perform the following steps:
   a) In a web browser, navigate to Oracle Application Express Administration Services and sign in using the Instance Administrator credentials
   b) Click Manage Workspaces
   c) Under Workspace Actions, click Create Workspace
   d) For Identify Workspace, enter a unique Workspace name and specify description. Leave Workspace ID blank and click Next.
   e) For Identify Schema, select No for Re-use existing Schema, enter a unique name for Schema Name, specify the Schema Password, and then click Next
   f) For Identify Administrator, enter the Workspace Administrator name, password, Email and click Next
   g) Confirm your selections and click Create Workspace
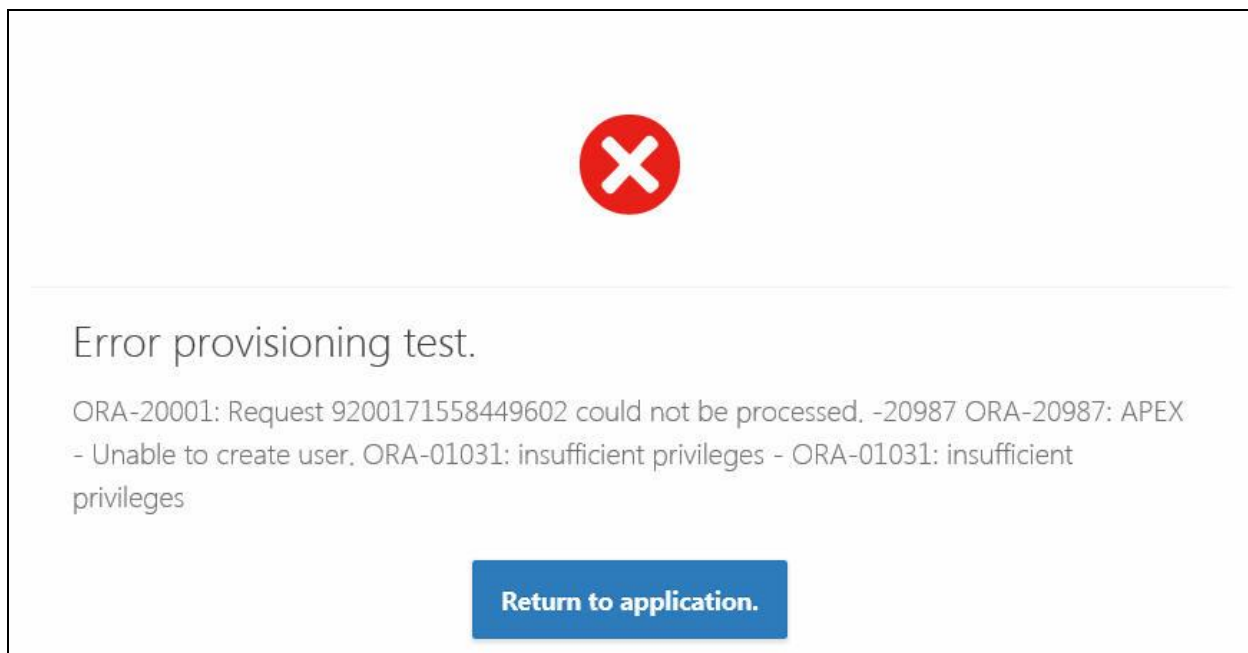
   Now you should see an error as shown in Figure 3.

Figure 3. Application Express Workspace Provisioning Error

Note: For more information on Oracle Application Express instance administration, see *Oracle Application Express Administrator's Guide*.

2. Connect to SQL*Plus and run **apex_dv_setup_112.sql**. You use *Database Vault Owner* and *Database Vault Account Manager* credentials.

Note: You should have downloaded the **apex_dv_setup_112.sql** script to your working directory in the Prerequisites section.

```
$ sqlplus /nolog
SQL*Plus: Release 11.2.0.3.0 Production on ..
Copyright (c) 1982, 2011, Oracle.  All rights reserved.
SQL> @apex_dv_setup_112.sql
```

3. To test the above Oracle Application Express – Oracle Database Vault environment again, repeat Step 1 above. Now you notice that the Workspace is created successfully.

Oracle Database Vault in Oracle Database 12c Non-Multitenant Environment

You can integrate Oracle Database Vault with Oracle Application Express in Oracle Database 12c Non-Multitenant as well as Multitenant environment. For the tasks discussed in this section, you should have already installed Oracle Database and Oracle Application Express. See the *Prerequisites* section.

In this section, you perform the specific steps required to integrate Oracle Application Express with Oracle Database Vault in Oracle Database 12c Non-Multitenant environment.

Registering Database Vault with Oracle Database 12c in a Non-Multitenant Environment

You can register Oracle Database Vault from SQL*Plus in a non-multitenant environment. Perform the following steps:

1. Log into the database instance as SYS user with the SYSDBA administrative privilege.

   ```
   sqlplus sys as sysdba
   Enter password: password
   ```

2. Create two user accounts to be used as the Database Vault accounts. One account will be the Database Vault Owner user and the second account will be the Database Vault Account Manager account. Ensure that they have at minimum the CREATE SESSION privilege.

   ```
   GRANT CREATE SESSION TO dbv_owner IDENTIFIED BY password;
   GRANT CREATE SESSION TO dbv_acctmgr IDENTIFIED BY password;
   ```

3. Configure the Database Vault user accounts.

   ```
   BEGIN
    DVSYS.CONFIGURE_DV (
       dvowner_uname          => 'dbv_owner',
       dvacctmgr_uname        => 'dbv_acctmgr');
    END;
   /
   ```

4. Run the utlrp.sql script to recompile invalidated objects.

   ```
   @?/rdbms/admin/utlrp.sql
   ```

5. Connect as the Database Vault Owner user that you just configured.

   ```
   CONNECT dbv_owner
   Enter password: password
   ```

6. Enable Oracle Database Vault.

   ```
   EXEC DVSYS.DBMS_MACADM.ENABLE_DV;
   ```

7. Connect with the SYSDBA administrative privilege.

   ```
   CONNECT / AS SYSDBA
   ```

8. Restart the database.

   ```
   SHUTDOWN IMMEDIATE
   STARTUP
   ```

9. Test if Oracle Database Vault and Oracle Label Security are enabled. You should see a result of TRUE by running each of the following two commands:

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

Configuring and Testing the Database Vault – Application Express Environment

In this section, you perform the steps to configure Oracle Application Express with Oracle Database Vault in an Oracle Database 12c non-multitenant environment.

1. Before configuring the Oracle Database Vault – Oracle Application Express environment, perform a quick test by manually creating a new Workspace in Oracle Application Express. You see an ORA-01031 error. Perform the following steps:

   a) In a web browser, navigate to Oracle Application Express Administration Services and sign in using the Instance Administrator credentials
   b) Click Manage Workspaces
   c) Under Workspace Actions, click Create Workspace
   d) For Identify Workspace, enter a unique Workspace name and specify description. Leave Workspace ID blank and click Next.
   e) For Identify Schema, select No for Re-use existing Schema, enter a unique name for Schema Name, specify the Schema Password, and then click Next
   f) For Identify Administrator, enter the Workspace Administrator name, password, Email and click Next
   g) Confirm your selections and click Create Workspace

2. Connect to SQL*Plus and run **apex_dv_setup_121.sql**. You use *Database Vault Owner* and *Database Vault Account Manager* credentials.

   Note: You should have downloaded the **apex_dv_setup_121.sql** script to your working directory in the Prerequisites section.

   ```
   $sqlplus /nolog
   SQL*Plus: Release 12.1.0.2.0 Production on Thu May 21 10:09:15 2015
   Copyright (c) 1982, 2014, Oracle.  All rights reserved.
   Connected to:
   Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
   Production
   With the Partitioning, Oracle Label Security, OLAP, Advanced Analytics,
   Oracle Database Vault and Real Application Testing options.
      SQL> @apex_dv_setup_121.sql
   ```

3. To test the Oracle Database Vault – Oracle Application Express environment again, repeat Step 1 above. Now you notice that the Workspace is created successfully.

Oracle Database Vault in Oracle Database 12c Multitenant Environment

For the tasks discussed in this section, you should have already installed Oracle Database and Oracle Application Express. See the *Prerequisites* section.

In a multitenant environment, you must register Oracle Database Vault in the root first, then in the PDBs afterward. If you try to register in a PDB first, then you see an `ORA-47503: Database Vault is not enabled on CDB$ROOT` error. Depending upon the type of configuration you have, perform the specific steps required to integrate Oracle Application Express with Oracle Database Vault. For more information, see *[Oracle Database Vault Administrator's Guide](#)*.

This section covers steps to integrate Oracle Database Vault with Oracle Application Express installed in a CDB and also in a specific PDB.

Integrating Oracle Database Vault with Oracle APEX Installed in a CDB

If you are integrating Oracle Database Vault with Oracle Application Express installed in a CDB, then you should follow the steps explained in this section. If your environment involves APEX in a PDB, then first make sure you register Oracle Database in the root and then follow the steps discussed in *Integrating Oracle Database Vault with Oracle APEX Installed in a Specific PDB* section.

Registering Database Vault with a Common User to Manage the CDB Root

In SQL*Plus, you can register Oracle Database Vault with a common user who will manage the CDB root. Perform the following steps:

1. Log into the root of the database instance as a user who has privileges to create users and grant the `CREATE SESSION` and `SET CONTAINER` privileges.

   ```
   sqlplus sys as sysdba
   Enter password: password
   ```

2. Create two user accounts to be used as the Database Vault accounts and grant them the `CREATE SESSION` and `SET CONTAINER` privileges. One account will be the Database Vault Owner user and the second (optional) account will be the Database Vault Account Manager account. Prepend the names of these accounts with `c##` or `C##`.

   ```
   GRANT CREATE SESSION, SET CONTAINER TO c##dbv_owner_root IDENTIFIED BY
   password CONTAINER = ALL;
   GRANT CREATE SESSION, SET CONTAINER TO c##dbv_acctmgr_root IDENTIFIED
   BY password CONTAINER = ALL;
   ```

3. Connect to the root as `SYS` user with the `SYSDBA` administrative privilege

   ```
   CONNECT SYS AS SYSDBA
   Enter password: password
   ```

4. Configure the Database Vault user accounts.

```
BEGIN
 DVSYS.CONFIGURE_DV (
    dvowner_uname          => 'c##dbv_owner_root',
    dvacctmgr_uname        => 'c##dbv_acctmgr_root');
 END;
/
```

5. Run the `utlrp.sql` script to recompile invalidated objects.

```
@?/rdbms/admin/utlrp.sql
```

6. Connect to the root as the Database Vault Owner user that you just configured.

```
CONNECT c##dbv_owner_root
Enter password: password
```

7. Enable Oracle Database Vault.

```
EXEC DVSYS.DBMS_MACADM.ENABLE_DV;
```

8. Connect with the `SYSDBA` administrative privilege.

```
CONNECT / AS SYSDBA
```

9. Restart the database.

```
SHUTDOWN IMMEDIATE
STARTUP
```

10. Test if Oracle Database Vault and Oracle Label Security are enabled. You should see a result of `TRUE` by running each of the following two commands:

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

Configuring and Testing the Database Vault – Application Express Environment

In this section, you perform the steps to configure Oracle Application Express with Oracle Database Vault in an Oracle Database 12c Multitenant environment.

1. Before configuring the Oracle Database Vault – Oracle Application Express environment, perform a quick test by manually creating a new Workspace in Oracle Application Express. You see an ORA-01031 error. Perform the following steps:

   a) In a web browser, navigate to Oracle Application Express Administration Services and sign in using the Instance Administrator credentials
   b) Click Manage Workspaces
   c) Under Workspace Actions, click Create Workspace

d) For Identify Workspace, enter a unique Workspace name and specify description. Leave Workspace ID blank and click Next.

e) For Identify Schema, select No for Re-use existing Schema, enter a unique name for Schema Name, specify the Schema Password, and then click Next

f) For Identify Administrator, enter the Workspace Administrator name, password, Email and click Next

g) Confirm your selections and click Create Workspace

2. Connect to SQL*Plus and run **apex_cdbdv_setup_121.sql**. You use *Database Vault Owner* and *Database Vault Account Manager* credentials.

   Note: You should have downloaded the **apex_cdbdv_setup_121.sql** script to your working directory in the Prerequisites section.

   ```
   sqlplus /nolog
   SQL*Plus: Release 12.1.0.2.0 Production on Thu May 21 10:09:15 2015
   Copyright (c) 1982, 2014, Oracle.  All rights reserved.
   Connected to:
   Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
   Production
   With the Partitioning, Oracle Label Security, OLAP, Advanced Analytics,
   Oracle Database Vault and Real Application Testing options.
   SQL> @apex_cdbdv_setup_121.sql
   ```

3. To test the Oracle Application Express – Oracle Database Vault environment again, repeat Step 1 above. Now you notice that the Workspace is created successfully.

Integrating Oracle Database Vault with Oracle APEX Installed in a Specific PDB

Registering Database Vault common users to manage specific PDBs

In a multitenant environment, you must register Oracle Database Vault in the root first, then in the PDBs afterward. If you try to register in a PDB first, then you see an ORA-47503: Database Vault is not enabled on CDB$ROOT error.

Note: If you have not already registered Oracle Database Vault in the root, first perform the steps as mentioned in the *Integrating Oracle Database Vault with Oracle APEX Installed in a CDB*section.

Perform the following steps:

1. Log into the root of the database instance as a user who has privileges to create users and grant the CREATE SESSION and SET CONTAINER privileges.

   ```
   sqlplus sys as sysdba
   Enter password: password
   ```

2. Ensure that Oracle Database Vault has been configured and enabled on the root. Run the following command in SQL*Plus and you should see the VALUE setting as TRUE.

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

3. If you have not already done, create two user accounts now to be used as the Database Vault accounts and grant them the CREATE SESSION and SET CONTAINER privileges.

4. Connect to the PDB to which the common users will need access. To check the current PDB, run the show con_name command.

```
CONNECT SYS@pdb_name AS SYSDBA
Enter password: password
```

5. While still in the PDB, configure the Database Vault user accounts.
   Note: See step 2 in *Registering Database Vault with a Common User to Manage the CDB Root* section.

```
BEGIN
 DVSYS.CONFIGURE_DV (
    dvowner_uname           => 'c##dbv_owner_root',
    dvacctmgr_uname         => 'c##dbv_acctmgr_root');
 END;
/
```

6. Run the utlrp.sql script to recompile invalidated objects.

```
@?/rdbms/admin/utlrp.sql
```

7. Connect to the PDB as the Database Vault Owner user that you just configured.

```
CONNECT c##dbv_owner_root@pdb_name
Enter password: password
```

8. Enable Oracle Database Vault.
```
EXEC DVSYS.DBMS_MACADM.ENABLE_DV;
```

9. Connect with the SYSDBA administrative privilege.
```
CONNECT / AS SYSDBA
```

10. Close and reopen the PDB.

```
ALTER PLUGGABLE DATABASE pdb_name CLOSE IMMEDIATE;

ALTER PLUGGABLE DATABASE pdb_name OPEN;
```

11. Test if Oracle Database Vault and Oracle Label Security are enabled. You should see show the VALUE setting as TRUE by running each the following two commands:

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

Configuring and Testing the Database Vault – Application Express Environment

Perform the following steps:

1. Before configuring the Oracle Database Vault – Oracle Application Express environment, perform a quick test by manually creating a new Workspace in Oracle Application Express. You see an ORA-01031 error. Perform the following steps:

    a) In a web browser, navigate to Oracle Application Express Administration Services and sign in using the Instance Administrator credentials
    b) Click Manage Workspaces
    c) Under Workspace Actions, click Create Workspace
    d) For Identify Workspace, enter a unique Workspace name and specify description. Leave Workspace ID blank and click Next.
    e) For Identify Schema, select No for Re-use existing Schema, enter a unique name for Schema Name, specify the Schema Password, and then click Next
    f) For Identify Administrator, enter the Workspace Administrator name, password, Email and click Next
    g) Confirm your selections and click Create Workspace

2. Connect to SQL*Plus and run **apex_pdbdv_setup_121.sql**. You use *Database Vault Owner* and *Database Vault Account Manager* credentials.

    Note: You should have downloaded the **apex_pdbdv_setup_121.sql** script to your working directory in the Prerequisites section.

    ```
    sqlplus /nolog
    SQL*Plus: Release 12.1.0.2.0 Production on Thu May 21 10:09:15 2015
    Copyright (c) 1982, 2014, Oracle.  All rights reserved.
    Connected to:
    Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit
    Production
    With the Partitioning, Oracle Label Security, OLAP, Advanced Analytics,
    Oracle Database Vault and Real Application Testing options.
    SQL> @apex_pdbdv_setup_121.sql
    ```

3. To test the Oracle Application Express – Oracle Database Vault environment again, repeat Step 1 above. Now you notice that the Workspace is created successfully.

Disabling and Enabling Oracle Database Vault

You must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features. If the Oracle Database Vault is registered with your Oracle Database and enabled before installing Oracle Application Express, you must first disable it before installing Oracle Application Express. After installing Oracle Application Express, you need to re-enable Oracle Database Vault.

The three steps involved in this process are:

1. Disable Oracle Database Vault
2. Perform the required tasks, for example, installing Oracle Application Express
3. Enable Oracle Database Vault

Note: After you disable Oracle Database Vault, Oracle Label Security, which is required to run Database Vault, is still enabled.

Oracle Database 11g Release 2

Perform the following steps if you are using Oracle Database11g Release 2:

1. First, check if Oracle Database Vault is enabled or disabled by querying the V$OPTION data dictionary view. Any user can query this view. If Oracle Database Vault is enabled, the query returns TRUE. Otherwise, it returns FALSE. Note that the PARAMETER column value is case sensitive.

   ```
   sqlplus sys as sysdba
   Enter password: password

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

2. Log in to SQL*Plus as SYS user with the SYSOPER privilege and shut down the database. Then from the command line, stop the Database Control console process and listener.

   ```
   sqlplus sys as sysoper
   Enter password: password

   SQL> SHUTDOWN IMMEDIATE
   SQL> EXIT

   $ emctl stop dbconsole
   $ lsnrctl stop [listener_name]
   ```

3. Disable the Oracle Database Vault by running the following command:

   ```
   $ cd $ORACLE_HOME/rdbms/lib
   $ make -f ins_rdbms.mk dv_off ioracle
   ```

4. Log in to SQL*Plus as SYS user with the SYSOPER privilege and restart the database. Then from the command line, restart the Database Control process and listener.

```
sqlplus sys as sysoper
Enter password: password
SQL> STARTUP
SQL> EXIT
$ emctl start dbconsole
$ lsnrctl start [listener_name]
```

5. Perform the required tasks, for example, install Oracle Application Express
6. Stop the database, Database Control console process, and listener. Repeat step 2.
7. You must enable Oracle Label Security before you can use Database Vault. The `make` command enables both Oracle Database Vault (dv_on) and Oracle Label Security (lbac_on). Run the following commands.

```
$ cd $ORACLE_HOME/rdbms/lib
$ make -f ins_rdbms.mk dv_on lbac_on ioracle
```

8. Now, restart the database, Database Control process and listener. Repeat step 4.

To learn more about disabling and enabling Oracle Database Vault in Oracle Database 11g Release 2, see *Oracle Database Vault Administrator's Guide 11g Release 2 (11.2)*.

Oracle Database 12c

Perform the following steps if you are using Oracle Database 12c:

1. First, check if Oracle Database Vault is enabled or disabled by querying the V$OPTION data dictionary view. Any user can query this view. If Oracle Database Vault is enabled, the query returns TRUE. Otherwise, it returns FALSE. Note that the PARAMETER column value is case sensitive.

```
sqlplus sys as sysdba
Enter password: password

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

2. In SQL*Plus, log in as the Oracle Database Owner account. In a multitenant environment, connect to the appropriate pluggable database (PDB). Then disable Oracle Database Vault.

```
CONNECT dbv_owner
Enter password: password
EXEC DBMS_MACADM.DISABLE_DV;
```

3. Restart the database.
```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@pdb1 AS SYSOPER
Enter password: password
SHUTDOWN IMMEDIATE
STARTUP
```

4. Perform the required tasks, for example, install Oracle Application Express

5. In SQL*Plus, connect as the Oracle Database Owner account. In a multitenant environment, connect to the appropriate pluggable database (PDB). Then, enable Oracle Database Vault.

```
CONNECT dbv_owner
Enter password: password

EXEC DBMS_MACADM.ENABLE_DV;
```

6. Verify if Oracle Label Security is enabled. If it is not enabled, then this query returns FALSE.

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Oracle Label Security';
```

7. If Oracle Label Security is not enabled, then enable it.

```
CONNECT SYS AS SYSDBA
Enter password: password

EXEC LBACSYS.CONFIGURE_OLS;
EXEC LBACSYS.OLS_ENFORCEMENT.ENABLE_OLS;
```

8. Restart the database.
```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@pdb1 AS SYSOPER
Enter password: password

SHUTDOWN IMMEDIATE
STARTUP
```

To learn more about disabling and enabling Oracle Database Vault in Oracle Database 12c, see *Oracle Database Vault Administrator's Guide 12c Release 1 (12.1)*).

Performing Other Upgrade Tasks

Patching Oracle Application Express when Oracle Database Vault is Enabled

If you want to upgrade Oracle Application Express to a later patch set, then you perform the following three steps:

1. First, disable Oracle Database Vault
2. Download the relevant patch set from My Oracle Support using the Patch Number provided on the Oracle Application Express Downloads page. Follow the instructions provided within the Patch Set Notes on the same page.
3. Enable Oracle Database Vault again.

Upgrading Oracle Database with Application Express and Database Vault Configured

If you have an Oracle Database 11.2.x with Oracle Database Vault configured, Oracle Application Express installed, and you want to upgrade the database to Oracle Database 12.1.x, perform the following steps:

1. Log in to SQL*Plus as Database Vault Owner user and run the following two commands. This step will update Oracle Database Vault default rules that were overwritten while upgrading to 12.1.x.

```
exec dbms_macadm.update_rule('Is User Manager',
'DVSYS.DBMS_MACUTL.USER_HAS_ROLE_VARCHAR(''DV_ACCTMGR'',SYS_CONTEXT(''u
serenv'',''current_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''');
```

2. Log in to SQL*Plus as Database Vault Owner user and run the following command:

```
exec dvsys.dbms_macadm.authorize_proxy_user('%','%');
```

Summary

Oracle Database Vault enables you to apply fine-grained access control to your sensitive data in a variety of ways. It hardens your Oracle Database instance and enforces industry standard best practices in terms of separating duties from traditionally powerful users. Most importantly, it protects your data from super-privileged users but still allows them to maintain your Oracle databases.

Oracle Application Express is a web-based development and deployment tool that is available with Oracle database. It enables you to create database-centric web applications that are reliable, scalable, and secure. Oracle Application Express includes number of built-in features and wizards that quicken your development process.

The following are a few examples of how Oracle Database Vault provides additional security capabilities to Oracle Application Express applications:
- Protecting database dictionary objects
- Enabling administrators to create Realms on schemas that are associated with Oracle Application Express Workspaces
- Separating duties to restrict the administrators from accessing application data and
- Restricting Oracle Application Express developers and the applications they develop from executing specific SQL commands or accessing specific data

By integrating Oracle Database Vault with Oracle Application Express, developers can take advantage of the completely built-in security implementation and controls provided by Oracle Database Vault. This will ensure avoiding the costly and time consuming application changes that would otherwise be required to implement the same security benefits.

ORACLE

Integrating Oracle Database Vault
with Oracle Application Express

August 2015
Authors: Chaitanya Koratamaddi
Contributors: Joel Kallman, Sarma Namuduri
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

Hardware and Software, Engineered to Work Together