Best Practices for Installing, Configuring and Deploying Oracle Database Vault Release 10.2.0.4 in an SAP Environment
Introduction .................................................................................................................... 1
Overview of Oracle Database Vault .............................................................................. 3
Installation of Oracle Database Vault .......................................................................... 3
Pre-Installation Requirements ...................................................................................... 4
Installing the Oracle Database Vault protections for SAP ........................................ 35
Test the SAP system with the Database Vault protections enabled......................... 37
Customizing Database Vault protections for SAP ...................................................... 42
Overview of the Database Vault Protections for SAP ............................................... 42
Database Vault Integration with Other Oracle Technology ........................................ 47
Appendix ...................................................................................................................... 48
Introduction

As with any new technology, using a systematic approach is important. This is especially important when it comes to database security. Oracle Database Vault enables organizations to efficiently increase security without making changes to the (SAP) application code. Oracle Database Vault provides real time preventive controls by restricting access to (SAP) application data from highly privileged users. Oracle Database Vault enables control over who, when, where and how databases and application data can be accessed. This paper is intended to compliment the Oracle Database Vault documentation. Please refer to the Oracle Database Vault Installation Guide and the Oracle Database Vault Administration Guide for additional technical information and guidelines. You find these guides on the Oracle Technology network (Link http://www.oracle.com/technology/documentation/database.html).

This paper will cover the following topics in various level of detail. When a topic is not fully covered, a pointer to the appropriate documentation is provided. Here are the main topics this document will address:

- Overview of Oracle Database Vault
- Installation of Oracle Database Vault in an SAP environment: including Pre and Post installation steps
- The configuration of the Oracle Database Vault protections for SAP
- A description of the Oracle Database Vault protections for SAP
- Testing of the SAP system with Oracle Database Vault protections enabled
• Customizing Database Vault protections for SAP

• Integration with other Oracle technology

Target audience: This document is targeted for Oracle Database Administrators, Oracle Security Administrators, and SAP System Administrators who are familiar with the Oracle Database.

The content of this technical white paper (TWP) pertains to all Unix and Linux platforms. Windows platforms are not covered in this paper.

By the end of this document, you will be able to identify the requirements, perform the configuration, test, understand and describe the protections that Oracle Database Vault provides for the SAP environment for security and compliance with regulations.
Overview of Oracle Database Vault

Oracle Database Vault enables organizations to efficiently increase security without making changes to the (SAP) application code. Oracle Database Vault provides real time preventive controls by restricting access to (SAP) application data from highly privileged users and by enabling control over who, when, where and how databases and application data can be accessed.


**Oracle Database Vault Realms**

An Oracle Database Vault Realm is a firewall or a protection zone that the Database Vault security administrator can establish in the Oracle Database to protect an application schema from being accessed by unauthorized database users including highly privileged database users like DBAs.

**Oracle Database Vault Command Rules**

An Oracle Database Vault Command Rule is a security check that can be associated with a SQL command. Command Rules can be created by the Database Vault Administrator to protect SQL commands like CREATE, TRUNCATE, DROP and ALTER.

**Oracle Database Vault Factors**

An Oracle Database Vault Factor is a global database environment variable that the application or the Database Vault security administrator can set and depending on its value allow or block certain database operations based on the given security requirements.

**Oracle Database Vault Separation of Duty**

Separation of Duty is another important feature of Oracle Database Vault. It enforces the separation between Database Account Management, Database Security Administration, and the Database Administration Responsibility in a simple and secure way. This is designed to help customers with their regulatory compliance requirements, such as SOX, JSOX, HIPAA, Basel II, and the PCI Standard. It also helps with customers' internal security requirements to protect from insider threat.

For a complete reading of the Oracle Database Vault features, please refer to the Oracle Database Vault Administration Guide that comes as part of the standard Oracle Database Documentation (Link: [http://www.oracle.com/pls/db102/portal.portal_db?selected=22](http://www.oracle.com/pls/db102/portal.portal_db?selected=22)).

Installation of Oracle Database Vault

Oracle and 3rd party applications like SAP should be installed prior to installing Oracle Database Vault. Because Oracle Database Vault enforces separation of duty on account management and security administration, some installation and patching processes used by Oracle and 3rd party may fail (like SAP installation tool SAPINST). Therefore Oracle Database Vault should be installed into an already existing SAP system.
Subsequent installation of new software or patching may require Oracle Database Vault to be temporarily turned off. Instructions on how to turn off Oracle Database Vault can be found in the Oracle Database Vault Administration Guide (and are also mentioned briefly in this paper).

Pre-Installation Requirements

Perform the following pre-requisite steps to prepare your SAP system for Oracle Database Vault installation.

Check Prerequisites

The following prerequisites must be met to be able to use Oracle Database Vault 10.2 with SAP:

1. Oracle Database Release 10.2.0.4
2. Oracle Database Patches should be installed according to SAP note 1137346.
3. Database parameters should be set according to SAP note 830576.
4. Only one database is run from the Oracle Home. Do not install Database Vault into an Oracle Home that is used by more than one database.
5. SAP NetWeaver with SAP Kernel Release 7.00 or higher
6. SAP BR*Tools Release 7.10 PL 20 or higher
   Although Database Vault does not require any specific changes of the SAP BR*Tools, it is recommended to install at least version 7.10 PL 20 of SAP BR*Tools (see SAP note 12741 on how to upgrade SAP BR*Tools). ‘brtools –V’ command tells you the current version of SAP BR*Tools in your environment. Ensure that the permissions of these executables are set correctly (see SAP note 113747).
7. Oracle Enterprise Manager Database Control (dbconsole):
   This requirement must also be met even when your Oracle database is managed with Enterprise Manager Grid Control. By default, in an SAP environment, Oracle Enterprise Manager Database Control software is installed, but the Enterprise Manager repository (database user SYSMAN) is not created. Therefore, this paper describes the steps of how to configure this database component. Within this document ‘Enterprise Manager’ refers to ‘Enterprise Manager Database Control (dbconsole)’.
8. Oracle Database Vault License. Please refer to SAP note 740897 for questions on licensing Oracle Database Vault in an SAP environment.
9. Configure a Server Parameter File (SPFILE):
   Oracle Database Vault installation requires the database to be configured with an SPFILE. In order to ensure that the installation will run fine, check the following:
   
   SQL> show parameter spfile
   If an SPFILE is configured, this command shows the path of the file.
10. Test running of Database Configuration Assistant (DBCA):
   Check that the Database Configuration Assistant (DBCA) can be started to configure Enterprise Manager Database Control. As OS user ora<sid> do:
a. Set the DISPLAY environment variable accordingly.

b. Run dbca using the command: $ORACLE_HOME/bin/dbca &

If DBCA starts up fine, cancel it. You do not configure EM at this point.

11. Check Listener configuration:
   Check that the Listener name is LISTENER and that the listener runs from the same Oracle Home as the database. This is only an install-time requirement. You can revert to your preferred listener configuration after Oracle Database Vault installation is complete.

12. Check the Oracle Inventory pointer file oraInst.loc:
   Check that oraInst.loc in /etc or /var/opt/oracle points to the right Oracle Inventory location.

13. Check the oratab file:
   Check that /etc/oratab (or /var/opt/oracle/oratab) has an entry for the database (Oracle Home) you will be installing to. This is a requirement for DBCA and DVCA. The entry is case sensitive. Make sure it exactly matches your $ORACLE_SID.

14. Configure Flashback Database (optional):
   As a best practice, it is recommended to configure a Flash Recovery Area and create a Guaranteed Restore Point (GRP) before you install Oracle Database Vault. A GRP allows you to easily go back with your database to the restore point in case you run into an installation issue. This is easier than restoring a database backup. More details on how to accomplish this are described later in this document.


   To create a guaranteed restore point <GRP_NAME> with BRSPACE, use the command:
   $ brspace –u / -f mfback -a rpcreate -p <GRP_NAME> -g

   To get a list of restore points, run:
   $ brspace -u/ -f mfback -a rpshow

   To retrieve a complete status overview for flashback database run:
   $ brspace -u/ -f mfback -a fbshow

   To reset the database back to a given restore point <GRP_NAME>, use BRRECOVER:
   $brrecover –type reset –point <GRP_NAME>

15. Check OS requirements and OS kernel parameters:
   In general, installing Oracle Database Vault software into an existing 10.2.0.4 Oracle Home should not have other requirements than what Oracle Database has. Please refer to the Oracle Database Vault Installation Guide, specific to your platform, for more information on this.

16. Database Auditing:
   If you have Database auditing turned on, turn it off for the duration of the installation only. You
can turn it back on once the installation is complete. Take a note of your current AUDIT_TRAIL setting first:

SQL> SHOW PARAMETER AUDIT_TRAIL

Then run the following command as SYS to turn Database auditing off:

SQL> ALTER SYSTEM RESET AUDIT_TRAIL SCOPE=SPFILE;

The database needs to be restarted for this change to take effect.

17. Recyclebin should be always turned off in the Oracle Database Vault environment.

By default, the recyclebin feature is not enabled in SAP environments (see SAP note 830576). If you need to turn it off, run the following command as SYS:

SQL> ALTER SYSTEM SET RECYCLEBIN = OFF SCOPE=SPFILE;

18. Create Database Vault Base directory <dv_base>

On the database server where you install Oracle Database Vault, create a Database Vault base directory; example: oradbvault. Also, in <dv_base>, create sub directories <dv_soft> for Oracle Database Vault software, <dv_scripts> for Oracle Database Vault policy scripts and <dv_logs> for installation logs.

Example: $SAPDATA_HOME=/oracle/<SID>

Create <dv_base> directory:

$mkdir -p $SAPDATA_HOME/oradbvault

Create <dv_scripts> directory:

$mkdir -p $SAPDATA_HOME/oradbvault/dv_scripts

In this directory you will later extract the Database Vault Policy scripts.

Create <dv_soft> directory:

$mkdir -p $SAPDATA_HOME/oradbvault/dv_soft

Create <dv_patches> directory:

$mkdir -p $SAPDATA_HOME/oradbvault/dv_patches

Create <dv_logs> directory:

$mkdir -p $SAPDATA_HOME/oradbvault/dv_logs

19. Download DV Software, patches and scripts:

Go to SAP Service market place (Link [http://service.sap.com/oracle-download](http://service.sap.com/oracle-download)). On the left side, click on 'Database Patches', then on 'Oracle', then on 'Oracle 10.2.0.4', and finally on 'Database Vault - DV'. Download Oracle Database Vault Software, patches and policy scripts and extract these in the corresponding directories <dv_soft>, <dv_patches> and <dv_scripts>.

When you extract the Oracle Database Vault scripts in <dv_scripts> with the command `unzip–d <dv_scripts>/SAP_DV_Policy-<version>.zip`, the scripts are extracted into a new subdirectory ‘SAP_DV_Policy’. When running scripts from this directory, we will refer to this directory as `<SAP_DV_Policy>`.

20. Configure glogin.sql for SQL*Plus (optional):

This is a best practice recommendation. If you configure Oracle Database Vault for the first time, it might be a little confusing because of all the new database users that are created and their duties. Therefore, it is a little helpful if you always see in the SQL prompt of SQL*Plus which database user you are currently connected as. The custom SQL prompt will look like (where SID=QO1):

SYS AS SYSDBA @ QO1>
PUBLIC AS SYSOPER @ QO1>
SECADMIN @ QO1>
SECACCTMGR @ QO1>
SAPSR3 @ QO1>
SAPSR3DB @ QO1>
OPS$ORAQO1 @ QO1>
OPSSQO1ADM @ QO1>

To get this kind of customized SQL prompt, just edit the SQL*Plus configuration file in $ORACLE_HOME/sqlplus/admin/glogin.sql and add the following line:
SET sqlprompt "_user _privilege '@' _connect_identifier> "

Note: A sample glogin.sql file is also provided in the scripts (subdirectory administration). You can just copy it to $ORACLE_HOME/sqlplus/admin.

Caution: Do not configure the SQL prompt using ‘_date’ or any other token containing or expanding to ‘0’ or ‘1’. Such a prompt could cause a parsing issue during DV installation and the DV installation would fail (Oracle Bug 8324012). To avoid any installation issues caused by a custom SQL prompt, you might choose to configure SQL prompt in glogin.sql after you finish the DV installation.

21. Check the database password file:
During an SAP installation with Oracle Database Release 10.2, a password file orapw<SID> is configured by default. During Oracle Database Vault installation, a new password file will be created. Check the current password file contents before installing Oracle Database Vault:
$ cd <dv_logs>
$sqlplus / as sysdba
SQL>set pagesize 100
SQL>spool pwfile_users_before_DV_install.log
SQL>select * from v$pwfile_users;
SQL>spool off
SQL>exit

Make a backup of the original password file before the installation.

22. Check existing database users:
The installation of Oracle Database Vault creates new database users in the database. To easily identify which users are new, get a list of all database users as they exist now in the database before you start the installation.
$ cd <dv_logs>
$sqlplus / as sysdba
SQL>set pagesize 100
SQL>spool dbusers_before_dv_install.log
SQL>select username, account_status, created from dba_users order by username;
SQL>spool off
23. Verify that the following database users are able to connect to the database before the installation. <SID> means Oracle System ID ($ORACLE_SID):

$ cd <dv_logs>
$ sqlplus /nolog

Now, connect as OPS$ORA<SID> / OPS$<SID>ADM:
SQL> connect /

Connect as SYSDBA:
SQL> connect / as sysdba

Connect as SYS using a password:
SQL> connect sys@<SID> as SYSDBA

Connect as SAP account for ABAP-Stack (example: SAPSR3):
SQL> connect sapsr3

Connect as SAP account for ABAP-Stack (example: SAPSR3) through listener (remote):
SQL> connect sapsr3@SID

Connect as SAP account for Java-Stack (example: SAPSR3DB):
SQL> connect sapsr3db

Connect as SAP account for Java-Stack (example: SAPSR3DB) through listener (remote):
SQL> connect sapsr3db@SID

Test the database connection from the SAP application server side as <sid>adm user:
$ R3trans –d
R3trans finished (0000).

24. Check the environment variables:

Ensure that the following environment variables are set correctly: ORACLE_BASE, ORACLE_HOME, ORACLE_SID, LD_LIBRARY_PATH. In an SAP environment, these environment variables should always be set automatically when you log on to the database server as ora<sid> user.

25. Create a temporary tablespace named TEMP (size ~200MB).
Oracle Database Vault release 10.2.0.4 requires that a temporary tablespace named TEMP exists. This is a mandatory requirement not only for initial Database Vault installation but also for patching Database Vault thereafter. This issue (Oracle bug numbers 7191113, 5679271) will be fixed in a future release of Oracle Database Vault.

You can create the TEMP tablespace either manually (CREATE TEMPORARY TABLESPACE TEMP TEMPFILE '<tempfile>' size <size> AUTOEXTEND OFF) or use BRSPACE for this task. Because of SAP naming conventions for tablespaces, BRSPACE does not allow you to create a tablespace named TEMP. Therefore, with BRSPACE, first create a temporary tablespace with a name that follows the SAP naming conventions like PSAPTEMPDV:

Note: If you run BRSPACE in interactive mode, do not set this tablespace as default temporary tablespace of the database when asked by BRSPACE. So ignore the following messages:

BR1094I The default temporary tablespace of database QO1 can be set to PSAPTEMPDV now.

BR1224I The temporary tablespace of owner SAPSR3 can be set to PSAPTEMPDV now

After that, rename tablespace PSAPTEMPDV to TEMP:

$brspace –u / –f tsalter –action rename –tablespace PSAPTEMPDV –name TEMP

You only need to rename the tablespace. You do not necessarily need to rename the data files associated with it. So just skip this action when asked by BRSPACE.

26. Take a backup your database, Oracle Home, and Oracle Inventory. In addition, make a backup copy of the spfile:

$sqlplus / as sysdba

SQL> create pfile = '*/dbs/init<SID>.ora.before_DV_install' from spfile;

Optionally, backup the complete dbs directory:

$cp -r $ORACLE_HOME/dbs <dv_base>/dbs.SV.before_DV_install

27. If you run your database in an advanced configuration like Oracle RAC, physical standby (Oracle Data Guard), or SAP MCOD, then please refer to the corresponding section further down in this document.
Configure the database with Oracle Enterprise Manager Database Control (dbconsole)

Note: This step is required even if your database is managed by Oracle Enterprise Manager Grid Control.

Note: Although, it is technically possible to manually deploy the Database Vault Administrator (DVA) application to the Oracle Containers for Java (OC4j) home $ORACLE_HOME/oc4j/j2ee/home – see procedure described in Oracle Database Vault Release Notes 10g Release 2 (10.2.0.4) --, it is recommended to automatically deploy the DVA during Oracle Database Vault installation which requires pre-installing Enterprise Manager Database Control (dbconsole) in the database. Manual deployment of DVA is error prone.

If you already have Oracle Enterprise Manager Database Control installed, then you can skip this section after you verify that you can start it up and login using SYSMAN user.

To create a guaranteed restore point before you configure Enterprise Manager, run the following SQL commands or use BRSPACE:
sqlplus / as sysdba
SQL> startup mount
SQL> CREATE RESTORE POINT GRP BEFORE EM INSTALL
   GUARANTEE FLASHBACK DATABASE;

To create this restore point with BRSPACE, run BRSPACE with the following command line:
$ brspace -u/-f mfback -a rpcreate -p GRP BEFORE EM INSTANL -g

Here are the steps to install Oracle Enterprise Manager Database Control:

1. Check that oratab (platform-dependent: /etc/oratab or /var/opt/oracle/oratab) contains an entry for the database <SID>:
   
   <SID>:/oracle/<SID>/102_64:[N | Y]
   
   As an example, for SID=C11, the entry will look like:

   C11:/oracle/C11/102_64:N

2. Check that the DISPLAY environment variable is set correctly:
   
   $ echo $DISPLAY
   $ xclock &

3. Make sure the database listener and the database are up, then run the Database Configuration Assistant:
   
   $ dbca &
On the ‘Welcome page’: select Next.

Select ‘Configure Database Options’ then click Next.
Select the database you want to configure then click Next.

Select 'Configure the Database with Enterprise Manager', leave both the 'Enable Email Notifications' and 'Enable Daily Backup' unchecked, and then click Next.
Verify that 'Enterprise Manager Repository' is selected and select SYSAUX for 'Enterprise Manager Repository' then click Next.

Provide the password for database users SYSMAN and DBSNMP then click Next.
Click ‘Finish’, then ‘OK’ to start the installation.
The installation will start.

Once the installation is complete, click on 'No' then exit dbca.

You can check the install logs in $ORACLE_HOME/configtoollogs/dbca/<SID>.
Alternatively, you could provide the necessary arguments for DBCA on the command line. For a list of DBCA command line options, run ‘dbca –help’.

Note: DBCA creates an empty directory under $ORACLE_BASE called ORACLE_BASE/oradata/<DBSID>. In an SAP environment this directory is not used to store Oracle database files. This directory can be deleted after the installation of Enterprise Manager is complete.

You can now logon as SYSMAN to Oracle Enterprise Manager Database Control using the link shown at the end of the installation: [https://<hostname>:<port>/em](https://<hostname>:<port>/em)

Note: if you do not intend to use Oracle Enterprise Manager Database Control (dbconsole) to manage or monitor your database, we recommend, from a security perspective, that you lock the SYSMAN account:

```bash
$ sqlplus / as sysdba
SQL> alter user SYSMAN account lock;
```

Edit the script ‘define_sap_user’ for the Oracle Database Vault protections for SAP

Before you can run the configuration scripts for the Oracle Database Vault protections for SAP, you must edit the input file `input_scripts/define_sap_user.sql` and define the database user names of your SAP system.

The following is an example of the values you have to provide. Please enter your environment’s corresponding values for the scripts to run successfully.

Database user of your SAP system (ABAP Stack):
DEFINE SAP_SCHEMA_ABAP='SAPSR3'

Database user of your SAP system (JAVA Stack):
DEFINE SAP_SCHEMA_JAVA='SAPSR3DB'
DEFINE SAP_SCHEMA_JAVA='' (if there is no JAVA-Stack)
OPS$ Database Users:
DEFINE SAP_SCHEMA_ORASID='OPS$ORA<SID>'
DEFINE SAP_SCHEMA_SIDADM='OPS$<SID>ADM'

OPS$ Database Users for SAP Application Servers on Windows:
DEFINE SAP_SCHEMA_SAPSERVICESID='OPS$SAPSERVICE<SID>'
DEFINE SAP_SCHEMA_SAPSERVICESID='OPS$<HOSTNAME>\SAPSERVICE<SID>'
DEFINE SAP_SCHEMA_SAPSERVICESID='OPS$<DOMAINNAME>\SAPSERVICE<SID>'

Save your changes and close the file.

Run Oracle Database Vault Prerequisite Script for SAP

Before we install Oracle Database Vault we need to create certain database accounts and also new database roles (SAPSYS, SAPCRED). This is achieved by running the script 'dv_sap_prerequisite_script.sql'.

Accounts created by this script are:

- **SAPACCTMGR**: This user is used to change the passwords of the SAP application (ABAP stack and Java stack). He is the only user allowed to do that. This is for separation of duty purposes. This account belongs in the Database Account Management responsibility.

- **SUPPORT_DBA**: This account is for SAP and Oracle Support use only. When enabled, it would work across responsibilities for SAP Support to be able to solve issues. Do not enable this user unless asked to do so by SAP and Oracle Support.

Login to SQL*Plus then run the script.

```
$ cd <SAP_DV_Policy>
sqlplus / as sysdba
SQL> @pre_dv_install/dv_sap_prerequisite_script.sql
SQL> exit
```

Verify that the script ran without errors.

Create guaranteed restore point before DV installation

Create a guaranteed restore point (GRP) before you continue with the installation. Start the instance in mount state:

```
$ sqlplus / as sysdba
SQL> startup mount
SQL> CREATE RESTORE POINT GRP_BEFORE_DV_INSTALL
    GUARANTEE FLASHBACK DATABASE;
```

Alternatively, you can use BRSPACE to create this guaranteed restore point (see SAP note 1125923):

```
Create restore point:
$ brspace -u/ -f mback -a rpcreate -p GRP_BEFORE_DV_INSTALL -g
```
Show restore point(s):
$ brspace –u/ -f mfback –a rpshow

Show flashback status:
$ brspace –u/ -f mfback –a fbshow

In case of an installation issue during the following DV installation - or if you would like to rerun the installation/configuration, you can reset the database to the restore point by running the following SQL commands without restoring a backup (see SAP note 966117):

SQL> CONNECT / AS SYSDBA
SQL> STARTUP MOUNT
SQL> FLASHBACK DATABASE TO RESTORE POINT GRP_BEFORE_DV_INSTALL;
SQL> ALTER DATABASE OPEN RESETLOGS;

Alternatively, you can use BRRECOVER to do that:
$ brrecover –type reset –point GRP_BEFORE_DV_INSTALL

Backup
At this point, it is good time to take another backup of your Oracle Database, Oracle Home, and Oracle Inventory. This is because de-installing Oracle Database Vault is not supported and the next step will be to install Oracle Database Vault.

De-Installation of Oracle Database Vault is not supported
Before you install the software please note that you cannot de-install Oracle Database Vault. That’s why you should backup your Oracle Database, Oracle Home, and Oracle Inventory now before you start the Oracle Database Vault installation. Do not de-install the Database Vault Software from your Oracle Home using Oracle Universal Installer. This would corrupt the Oracle Home.

If you need to back out of your Oracle Database Vault then restore your Oracle Home and inventory and flash back your database to your restore point as described above.

It is recommended to carefully read Oracle Database Vault Installation Guide and Release notes before you start the installation (http://www.oracle.com/pls/db102/portal.portal_db?selected=22)

Install Oracle Database Vault
Oracle Database Vault 10.2.0.4 gets installed as an additional Oracle Database option that consists of a software and a database components. Oracle Database Vault installer first installs the DV software into the Oracle Home, then starts the Database Vault Configuration Assistant (DVCA) to configure the DV component in the database. Within this step, DVCA creates the database users for the security administrator (SECADMIN) and for the account manager (SECACCTMGR). DVCA will also create the DV dictionary accounts (DV_SYS, DV_F), tables, and procedures. These DV objects are automatically protected from unauthorized access by default seeded realms and rules.

Stop the SAP application
As <sapsid>adm user, stop the SAP system:
Best Practices installing and Configuring Oracle Database Vault in an SAP Environment

$ stopsap r3
Note: Do not start the SAP system again before the Oracle Database Vault installation and configuration is complete.

Stop all Oracle processes
Stop the Oracle database, listener, and Enterprise Manager Database Control (dbconsole):
$ emctl stop dbconsole
$ lsnrctl stop
$ sqlplus / as sysdba
SQL> shutdown immediate
Verify that all Oracle processes from the Oracle Home are stopped:
$ ps -ef | grep –i ora

Install and Configure Oracle Database Vault
Note: you need the current SYS password for this step! If you are not sure, verify the SYS password with 'connect SYS/<pwd>@<SID>'.

There are 2 ways how you can install and configure Database Vault:
1. Have the installer run through both the software installation part and the database configuration in a single run. This is the default and recommended way.
2. Configure the installer to run only the software installation part, and then run the database configuration part manually using DVCA.

Install Oracle Database Vault (Software and Database) in one step
Here are the steps to go through the first way of installation (software and database in one step):
As ora<sid> user, run the Oracle Database Vault installer in interactive mode (no silent) from Oracle Database Vault software stage directory:
$ cd <dv_soft>/<stage directory>
$ ./runInstaller
Page1: Specify Installation Details:
On this page, Oracle Database Vault installer provides the option to create an account management responsibility. Oracle recommends creating the account management responsibility to provide enhanced separation of duties between the security administrator (owner), account management, and other DBA responsibilities. For SAP environments, we will follow this recommendation by creating the user SECACCTMGR.
On the 'Specify Installation Details' page, you need to provide the following accounts and their passwords:

Database Vault Owner: SECADMIN

Database Vault Account Manager: SECACCTMGR

Please note that the password policy requires that the passwords must contain characters, numbers and special characters. For special characters, only use the underscore "_" as there is a bug in using other special characters that can lead to unsuccessful installation. You can change the password of these accounts after the installation is done.
Page 2: Select Existing Database

On page 'Select Existing Database' you need to select the database. If you do not see your database here, check your oratab file and make sure it has an entry for the database you want to install to.

Enter and confirm the SYS password, then click Next:
The installer validates the provided input and verifies database requirements:

Confirm the following warning by clicking ‘OK’:
The installation continues with product-specific pre-requisite checks, once finished click Next:

On the summary page you can review what you have selected, then continue by clicking 'Install'. During the installation, a new sub-directory is created $ORACLE_HOME/dv. DV Installation log files are written...
to `$ORACLE_HOME/cfgtoollogs/` and `$ORACLE_HOME/cfgtoollogs/dv` directories. In case of installation errors, check these log files first. Install progress can be checked while the installation is running by checking the log `$ORACLE_HOME/cfgtoollogs/dvca_install.log`.

---

**Install**

*Installing Oracle Database Vault 10.2.0.4.8*

- Installation in progress
  - Link pending...
  - Setup pending...
  - Configuration pending...

Extracting files to `/oracle/Q01/102_64`

- 72%

Stop installation...

You can find a log of this install session at:

/`oracle/orainventory/logs/installsession2009-07-03_04-55-31PM.log`

---

**Install**

*Installing Oracle Database Vault 10.2.0.4.8*

- Install successful
- Link successful
- Setup successful
- Configuration pending...

- 24%

Stop installation...

You can find a log of this install session at:

/`oracle/orainventory/logs/installsession2009-07-03_04-55-31PM.log`
After successful install, link and setup of Oracle Database Vault software, the installer starts the Database Vault Configuration Assistant DVCA in the background to configure Database component of the install:
The End of Installation screen shows the URL to the Oracle Enterprise Manager Database Control. You replace the last two characters in this link (“em”) with “dva” to connect to the Database Vault Administrator (DVA) using the SECADMIN account.

Note: If the installation fails during the software install phase, restore Oracle Home and Inventory that you backed up before.

Note: If the installation fails during the database configuration phase, restore Oracle Home and Inventory and reset your database to the restore point GRP_Before_DV_INSTALL.

Now that the installation is complete, you continue with the Post-Installation Tasks.

The following section describes how to install Oracle Database Vault software and how to configure the database component in two separate steps.

Install Oracle Database Vault in two separate steps using OUI and DVCA

Here are the steps to go through the second way of installation:

Install the DV software part first:

Go to directory <dv_soft> where you extracted and staged the DV software and edit the response file dv_inplace.rsp located in directory <dv_stage>/install/response. Change the following line as follows and save the file:

```
#b_launchDVCA=true
b_launchDVCA=false
```

With this setting the Database Vault Configuration Assistant (dvca) will not be started from the DV installer. As a result, only the DV software will be installed.
As ora<sid> user, start the Database Vault installation:

$ cd <dv_soft>/<stage directory>

$ ./runInstaller

Go through the installation as described before; specify usernames and passwords for SECADMIN, SECACCTMGR and SYS.

Note: Although the account information will not be used by the dvca at this point, you still need to enter it.

If the installation of the software fails for some reason, just restore the Oracle Home and Oracle Inventory that you backed up before. When finished, exit the DV installer.

Now that you are done with the software install, you can run Database Vault Configuration Assistant (DVCA) as follows:

Start the database listener and the database then create a shell script called run_dvca.sh with the following content:


Replace SYS_password with your SYS password and do the same for other passwords. Replace sid_name with your $ORACLE_SID environment variable value, and <dv_logs> with your logs directory.

Note: the passwords for SECADMIN, SECACCTMGR must contain alphabetical characters, numerical characters, and special characters. Please do not use special characters other than the underscore '_' (Oracle Bug 7606995, Metalink Note 579308.1).

Note: for a complete description of the dvca command parameters, refer to the Oracle Database Vault Installation Guide.

Save the shell script run_dvca.sh then change the file permissions to make it executable:

$ chmod u+x run_dvca.sh

As ora<sid>, run the shell script run_dvca.sh as follows:

$ ./run_dvca.sh &

Ensure that dvca finishes successfully. The output should look similar to the following and can be viewed in the $ORACLE_HOME/configtoollogs/dvca_install.log:

`01/29/09 12:04:49 DVCA started
01/29/09 12:04:49 Executing task LOCKOUT_OFF
01/29/09 12:04:49 Executing task RESTART_SERVICES_PATCH
01/29/09 12:04:49 MANAGE_INSTANCE stop isqlplus
01/29/09 12:04:49 MANAGE_INSTANCE stop OC4J
01/29/09 12:04:53 MANAGE_LISTENER start listener
01/29/09 12:04:53 MANAGE_INSTANCE start RDBMS`
01/29/09 12:05:09 Executing task SQLPLUS_CATOLS
01/29/09 12:06:30 Executing task RESTART_SERVICESROLS
01/29/09 12:06:30 MANAGE_INSTANCE stop isqlplus
01/29/09 12:06:30 MANAGE_INSTANCE stop OC4J
01/29/09 12:06:34 MANAGE_LISTENER start listener
01/29/09 12:06:34 MANAGE_LISTENER start listener
result=/oracle/QO1/102_64/bin/dvca_start_listener.sh,1,
01/29/09 12:06:34 MANAGE_LISTENER start listener log=LSNRCTL for
HPUX: Version 10.2.0.4.0 - Production on 29-JAN-2009 12:06:34
Copyright (c) 1991, 2007, Oracle. All rights reserved.
TNS-01106: Listener using listener name LISTENER has already been started
01/29/09 12:06:34 MANAGE_INSTANCE start RDBMS
01/29/09 12:06:45 Executing task SQLPLUS_CATMAC
01/29/09 12:08:14 Executing task UNLOCK_DVSYS
01/29/09 12:08:14 Executing task LOAD_NLS_FILES
01/29/09 12:08:16 Executing task ACCOUNT_CREATE_OWNER
01/29/09 12:08:16 Executing task GRANT_CONNECT_OWNER
01/29/09 12:08:16 Executing task GRANT_ADMIN_DB_TRIG
01/29/09 12:08:16 Executing task GRANT_ALTER_ANY_TRIG
01/29/09 12:08:16 Executing task ACCOUNT_CREATE_MANAGER
01/29/09 12:08:16 Executing task GRANT_CONNECT_MANAGER
01/29/09 12:08:16 Executing task PASSWORD_CHANGE_DVSYS
01/29/09 12:08:16 Executing task PASSWORD_CHANGE_DVF
01/29/09 12:08:17 RULE_SYNC:TRUE
01/29/09 12:08:17 Executing task GRANT_DV_OWNER_OWNER
01/29/09 12:08:17 Executing task GRANT_DBMS_RLS_OWNER
01/29/09 12:08:17 Executing task GRANT_AUDIT_TRAIL
01/29/09 12:08:17 Executing task GRANT_DV_ACCTMGR_MANAGER
01/29/09 12:08:17 COMMAND_RULES:9
01/29/09 12:08:17 Executing task ALTER_TRIGGER_BEFORE_DDL
01/29/09 12:08:17 Executing task ALTER_TRIGGER_AFTER_DDL
01/29/09 12:08:17 Executing task REVOKE_CONNECT_DVSYS
01/29/09 12:08:17 Executing task REVOKE_CONNECT_DVF
01/29/09 12:08:17 Executing task LOCK_DVSY
01/29/09 12:08:17 Executing task LOCK_DVF
01/29/09 12:08:17 Executing task ALTER_TRIGGER_LBACSYS1
01/29/09 12:08:17 Executing task ALTER_TRIGGER_LBACSYS2
01/29/09 12:08:17 Executing task ALTER_TRIGGER_LBACSYS3
01/29/09 12:08:18 Executing task DEPLOY_DVA
01/29/09 12:08:18 DEPLOY_DVA,validate
01/29/09 12:08:18 DEPLOY_DVA get EM home
01/29/09 12:08:20 DEPLOY_DVA get EM home instance=hsi016_QO1
01/29/09 12:08:20 DEPLOY_DVA stop isqlplus
01/29/09 12:08:20 DEPLOY_DVA stop OC4J
01/29/09 12:08:24 DEPLOY_DVA,modify
/oracle/QO1/102_64/oc4j/j2ee/OC4J_DBConsole_hsi016_QO1/config/server.xml
01/29/09 12:08:24 DEPLOY_DVA,modify
/oracle/QO1/102_64/oc4j/j2ee/OC4J_DBConsole_hsi016_QO1/config/http-web-site.xml
01/29/09 12:08:24 Executing task SQLPLUS_UTLRP
01/29/09 12:08:30 Executing task INIT_AUDIT_SYS_OPERATIONS
01/29/09 12:08:30 Executing task INIT_REMOTE_OS_AUTHENT
01/29/09 12:08:30 Executing task INIT_REMOTE_OS_ROLES
01/29/09 12:08:30 Executing task INIT_OB_ROLES
01/29/09 12:08:30 Executing task INIT_SQL92_SECURITY
01/29/09 12:08:30 Executing task INIT_OB_AUTHENT_PREFIX
01/29/09 12:08:30 Executing task INIT_REMOTE_LOGIN_PASSWORDFILE
01/29/09 12:08:30 Executing task INIT_RECYCLEBIN
01/29/09 12:08:30 Executing task RESTART_SERVICES
01/29/09 12:08:30 MANAGE_INSTANCE stop isqlplus
01/29/09 12:08:30 MANAGE_INSTANCE stop OC4J
01/29/09 12:08:34 MANAGE_INSTANCE stop RDBMS
01/29/09 12:08:54 MANAGE_LISTENER stop listener
01/29/09 12:08:58 MANAGE_LISTENER start listener
Now the database part of the installation is complete, you can continue with the Post Installation Tasks.

**Post Installation Tasks**

Make sure your SAP system is still down and go through the following steps.

**Configure glogin.sql**

If you decided to postpone SQL prompt customization in glogin.sql to after DV installation, you can now do that as described in the prerequisites section.

**Create another guaranteed restore point after DV installation**

This Guaranteed Restore Point (GRP) helps you reset your database to this point in time in case of an issue in the coming remaining configuration steps.

```
SQL> STARTUP MOUNT;
SQL> CREATE RESTORE POINT GRP_AFTER_DV_INSTALL
       GUARANTEE FLASHBACK DATABASE;
SQL> SELECT * from V$RESTORE_POINT
       WHERE guarantee_flashback_database = 'YES';
```

Alternatively, use BRSPACE:

```
$ brspace –u/ -f mfback –a rpcreate –p GRP_AFTER_DV_INSTALL –g
$ brspace –u/ -f mfback –a rpshow
```

**Download the latest Oracle Database Vault recommended patch**

Please check SAP note 1355140 for the current recommended Database Vault patch that has to be installed and download it from SAP Service Marketplace.

**Install the latest Oracle Database Vault recommended patch**

To install the patch, stop all processes running from this Oracle Home:

1. Stop Enterprise Manager Database Control
2. Stop the database
3. Stop the listener

Extract the patch in the <dv_patches> directory. Follow the instructions of the patch readme file to install the patch. See also ‘Installation Steps for Oracle Database Vault Patches’ in the appendix of this document.

Note: MOPatch cannot be used for Oracle Database Vault patches.

After the patch has been applied, start Oracle processes again:
1. Start the listener
2. Start the database
3. Start Enterprise Manager Database Control

Remove Database Audit configurations set by Oracle Database Vault

Upon Oracle Database Vault installation or patching, DV configures a list of DV specific database audit settings. For database performance reasons, we recommend that you turn off these audit settings. To do so, you need to run the noaudit.sql script. This script is part of the SAP policy scripts and located under noaudit directory. Here are the steps:

1. Disable Database Vault Realm (as SECADMIN = DVOWNER) from SQL*Plus using the following script, then exit:
   ```bash
   cd <SAP_DV_Policy>
   sqlplus secadmin
   SQL> @noaudit/disable_dv_realm.sql
   ```
2. Run noaudit.sql as SYSDBA:
   ```bash
   sqlplus / as sysdba
   SQL> @noaudit/noaudit.sql
   SQL> exit
   ```
3. Enable Database Vault Realm again (as SECADMIN = DVOWNER), then exit:
   ```bash
   sqlplus secadmin
   SQL> @noaudit/enable_dv_realm.sql
   ```

These steps should run after the DV installation and every time a DV patch is applied.

Perform the following sanity checks

In this section, we will perform some sanity checks and modify some database initialization parameters.

Test SAP connection to the Database

Check the database connection by running ‘R3trans –d’ as <sapsid>adm OS user.

At this point, this will result in the output message ’R3trans finished (0012)’. Also, ‘sqlplus /’ will return with an ’ORA-01017: invalid username/password; login denied’ error.

This means, that the SAP application cannot connect to the database at the moment. This is because Oracle parameters os_authent_prefix and remote_os_authent were changed by the DV installation. The next step will fix the connection.

Check and modify Oracle parameters

DV installation affects certain security-related Oracle database parameters like OS_AUTHENT_PREFIX (set to null string) and REMOTE_OS_AUTHENT (set to FALSE). In an SAP environment we have to restore these parameters back to their previous state, because the SAP application and also SAP BR*Tools use the OPS$-user to connect to the database.

```bash
sqlplus / as sysdba
```
SQL> show parameter os_authent_prefix
SQL> alter system reset os_authent_prefix scope = spfile sid = '*';
Note: If you set the parameter os_authent_prefix to a non-default value in your system, then you must set it back to the value you had before.
SQL> show parameter remote_os_authent
SQL> alter system set remote_os_authent=true scope = spfile;
Restart the database for the changes to take effect:
SQL> shutdown immediate
SQL> startup
SQL> show parameter os_authent_prefix
SQL> show parameter remote_os_authent
Now R3trans should be able to connect successfully. Run the following command as <sapsid>adm:
$ R3trans -d
R3trans finished (0000).
‘sqlplus /’ as <sid>adm should connect successfully, too.

Check and correct contents of new password file
After installing DV, if you login to the database as SYS AS SYSDBA and check the password file contents:
SQL> select * from v$pwfile_users;
USERNAME SYSDB SYSOP
------------------------------ ----- ----- 
SYS FALSE TRUE
SYS is not allowed to connect with SYSDBA privilege from remote. As a result, if you try to do:
SQL> connect SYS@<SID> as sysdba
You will get the following error:
ERROR:
ORA-01031: insufficient privileges
To correct this, as SYSDBA do the following:
SQL> grant sysdba to sys;
Now test the connect command again:
SQL> connect SYS@<SID> as sysdba
This should work now.
Test Database connections

On the database server, as operating system user ora<sid>, test the following database connections:

$ sqlplus /nolog
Connect as OPS$ORA<SID>:
SQL>connect /

Connect as SYSDBA:
SQL>connect / as sysdba
SQL>connect SYS@<SID> as sysdba

Connect as SAP account for ABAP-Stack:
SQL>connect sapsr3

Connect as SAP account for ABAP-Stack (remote):
SQL> connect sapsr3@<SID>

Connect as SAP account for Java-Stack:
SQL> connect sapsr3db

Connect as SAP account for Java-Stack (remote):
SQL> connect sapsr3db@<SID>

From the SAP application server (<sid>adm) check the following:

$ sqlplus /nolog
Connect as OPS$<SID>ADM:
SQL>connect /

Connect as SAP account for ABAP-Stack (remote):
SQL> connect sapsr3@<SID>

Connect as SAP account for Java-Stack (remote):
SQL> connect sapsr3db@<SID>

Save a list of after-install Database users (optional)

Get a list of all database users in the database after DV is installed.

$cd <dv_logs>
$sqlplus / as sysdba
SQL> set pagesize 100
SQL>spool dbusers_after_dv_install.log
SQL>select username, account_status, created from dba_users order by username;
SQL>spool off
The output can be compared with the list of users in dbusers_before_dv_install.log that was created before the DV install.

Check Oracle Database Vault Option is enabled (V$OPTION)

To check whether the Oracle Database Vault option is enabled or not run the following query:

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

This should return ‘TRUE’.

Test login to DVA as SECADMIN

Check whether Oracle Enterprise Manager Database Control (dbconsole) is running (‘emctl status dbconsole’). If not, start it ‘emctl start dbconsole’ (note: database and listener must also be started).

Login to the Database Vault Administrator web interface (DVA) using the SECADMIN account using the following URL format: http://<your_host_name>:<em_port>/dva.

Logon as SECADMIN user:

After logon, you will be shown the Database Vault Administration page:
Click on Realms link. On the Realms page, you will see the four Oracle default realms created upon DV installation:

![Oracle Realms Image]

Database Vault realms provide a capability to classify database schema and database roles into functional groups in order to provide fine-grained access control of ability to use system level privileges against these types of database objects.

### Installing the Oracle Database Vault protections for SAP

In this section, we show how to install the Oracle Database Vault protections for SAP and provide a description of these protections.

Note: the Oracle Database Vault protections for SAP has been tested and certified with SAP Applications and SAP BR*Tools. **It is mandatory for every SAP customer that uses Oracle Database Vault to install these protections.** Customers are allowed to add their own additional Oracle Database Vault custom settings after they apply the Oracle Database Vault protections for SAP.

Create another guaranteed restore point (optional)

Before you install the Oracle Database Vault protections for SAP, create another restore point as follows:

```sql
SQL> CREATE RESTORE POINT GRP_BEFORE_DV_CONFIG GUARANTEE FLASHBACK DATABASE;
Alternatively with BRSPACE:
$ brspace –u/ -f mbackup –a rprecreate –p GRP_BEFORE_DV_CONFIG –g
```

Run DV post-installation scripts

Go to `<SAP_DV_Policy>` directory and run the following scripts:

As SECACCTMGR:

```
$ sqlplus SECACCTMGR @post_dv_install/post_dv_install_secacctmgr.sql
```

As SYS:

```
$ sqlplus / as sysdba @post_dv_install/post_dv_install_sys.sql
```

Verify that the scripts ran without errors. Logs are written to `<SAP_DV_policy>/logs`
Run the scripts for the Oracle Database Vault protections for SAP

In this step, you configure the SAP specific Oracle Database Vault protection policy. Go to directory `<SAP_DV_policy>`. As SECADMIN, login to the database and run the following script:

```
$ cd <SAP_DV_Policy>
SQL> @create_policies/create_dv_sap_policies.sql
```

Verify that the script ran without errors by checking the log. By running this script, the Oracle Database Vault protections for SAP are created and automatically enabled.

From the DVA interface, you can see that there are additional SAP specific realms created:

![Database Vault interface showing SAP realms](image)

Configuring the Oracle Database Vault protections for SAP MCOD Installations

If you have an SAP MCOD environment (MCOD=Multiple SAP Components in One Database), you need to modify the DV realm definitions in the scripts before you run them. There is multiple approaches how one can configure database vault for such an MCOD scenario: One possible solution for this is to define additional separate SAP realms for each ABAP and each Java Stack. Another, easier way to do this, is to simply add all SAP ABAP stack schemas to the SAP ABAP stack realm and all SAP Java stack schemas to the SAP Java stack realm. As a result, the number of DV realms in an SAP MCOD would remain the same. Refer to the Customer Customizations Consideration section for a detailed description on the needed changes to the scripts to accommodate an SAP MCOD system. The scripts package contains a folder named administration/MCOD_configuration that contains templates for the SQL scripts to be adapted.

Create another guaranteed restore point (optional)

After you install the Oracle Database Vault protections for SAP, create another restore point as follows:

```
SQL> CREATE RESTORE POINT GRP_AFTER_DV_CONFIG
   GUARANTEE FLASHBACK DATABASE;
```
Alternatively with BRSPACE:

$ brspace -u/ -f mfback -a rpcreate -p GRP_AFTER_DV_CONFIG -g

Perform a backup

We recommend that you perform a complete (cold) backup at this stage. Backup your Oracle Database, Oracle Home, and Oracle Inventory.

Test the SAP system with the Database Vault protections enabled

Run the following tests to check that the SAP system is working as expected and that the Oracle Database Vault protections work as expected.

Test Oracle Database Vault Protections

The primary goal of Oracle Database Vault is to protect SAP application data. A highly privileged database user (database administrator with DBA role privilege like SYSDBA or SYSTEM) should not be allowed to access data stored in SAP application tables.

Try to access SAP table data as SYSDBA or as SYSTEM user:

sqlplus / as sysdba
SQL> select * from "SAPSR3"."T100";
→ORA-01031: insufficient privileges
SQL> select count(*) from sapsr3.t100;
→ORA-01031: insufficient privileges
SQL> create table sapsr3_T100 as select * from sapsr3.t100;
→ORA-01031: insufficient privileges
SQL> create table sapsr3.dv_test (c1 number);
→OK
Insert into sapsr3.dv_test values (1);
→ORA-01031
SQL> drop table sapsr3.dv_test;
→OK
SQL> truncate table sapsr3.dv_test;
→OK
SQL> delete from sapsr3.dv_test;
→ORA-01031
SQL> analyze table sapsr3.dv_test validate structure;
→OK
SQL> analyze table sapsr3.dv_test validate structure cascade;
→OK
SQL> create index sapsr3.i_dv_test on sapsr3.dv_test (c1);
→OK
SQL> describe sapsr3.dv_test;
→OK
After DV has been installed and SAP DV policy has been activated, access to SAP Application data by highly privileged users like SYS or SYSTEM is restricted. SELECT and DML operations are blocked, DDL operations and administrative tasks are still allowed.

NOTE: It is important to understand that Oracle Database Vault protection is real-time. This means that changes to the Database Vault Security policy have immediate effect without restarting the instance and without reconnecting to the database and without restarting the SAP application.

**Oracle Database Vault’s Performance Impact**

Oracle internal benchmark tests have shown an overhead on CPU of less than 5% (typically less than 2%) on the database server.

**Test SAP BR*Tools**

The Oracle Database Vault protections for SAP have been designed to accommodate running all database administration tasks offered by SAP BR*Tools.

Note: If you do not use SAP BR*Tools for administration of your Oracle database, you need to run the corresponding administration tasks from your DBA Tool/program/environment.

SAP BR*Tools connect as OPS$ account, SYSOPER, or SYSDBA depending on the task to perform. BRARCHIVE, BRBACKUP and BRCONNECT must have the correct file permissions, to function properly (see SAP note 113747 ([https://service.sap.com/sap/support/notes/113747](https://service.sap.com/sap/support/notes/113747)):

$ chmod 4775 brarchive brbackup brconnect

$ ls -l brarchive brbackup brconnect

-rwsrwxr-x ora<sid> sapsys brarchive

-rwsrwxr-x ora<sid> sapsys brbackup

-rwsrwxr-x ora<sid> sapsys brconnect

Some of the following BR*Tools tasks can also be started from the SAP application in the DB13 Planning calendar. Some of the following administration tests use certain SAP schema names like SAPSR3 or SAPSR3DB, tablespace names like PSAPSR3. You might need to replace these names according to your system.

Run the following administration tasks using SAP BR*Tools on your Oracle database:

**Test BRTOOLS**

$ brtools
Start the “Show instance status” function.
Run this test as ora<sid> user.

**Test BRCONNECT (Update Table Statistics)**

Run this test as <sid>adm user or from DB13 Planning calendar.

Gather table statistics for all “DBA*” tables:

$ brconnect -u / -c -f stats -t "DBA*" -f collect
Update statistics for tables of SAPSR3 user (ABAP):
$ brconnect -u / -c -f stats -o SAPSR3 -t all

Update statistics for tables of SAPSR3DB user (JAVA):
$ brconnect -u / -c -f stats -o SAPSR3DB -t all

Test BRCONNECT (Dictionary Statistics)
Run this test as <sid>adm user or ora<sid> user.
Gather dictionary statistics and system statistics:
$ brconnect -u / -c -f stats -t oradict_stats
$ brconnect -u / -c -f stats -t system_stats
Gather system statistics in NOWORKLOAD mode (recommended):
$ brconnect -u / -c -f stats -t system_stats
Gather system statistics in WORKLOAD mode:
$ brconnect -u system -c -f stats -t system_stats –i 5

Test BRCONNECT (Database Check)
Run this test as <sid>adm user or from DB13 Planning calendar.
$ brconnect -u / -c -f check

Test BRCONNECT (Other functions)
Recreate Synonyms for BR*Tools tables:
$ brconnect -u / -c -f crsyn -o sapsr3
Change password of ABAP realm SAP user (SAPSR3):
For this task you must use the SAPACCTMGR. This is the only account that has the required privileges (SAPCRED database role) to change the SAP database user password.
$ brconnect -u SAPACCTMGR -c -f chpass -o sapsr3 -p <newpwd>

Test BRCONNECT (Validate Structure)
You can run this test as <sid>adm user or ora<sid> user.
$ brconnect -u / -c -f stats -t <tables> -v cascade

Test BRBACKUP and BRARCHIVE (Database Backup)
You can run this test as <sid>adm user, from DB13 Planning calendar or as ora<sid>.
$ brbackup -u / -c –m all …
$ brbackup -u / -c –m <tablespace name>
$ brarchive -u / -c …

Test BRSPACE (Table and Index Reorganization)
Run tests with BRSPACE as ora<sid>.
Table Online Reorganization:
$ brspace -u / -f tbreorg -t <table> -m online

Table Reorganization (offline):
$ brspace -u / -f tbreorg -t <table> -m offline

Index Rebuild:
$ brspace –u / -f idrebuild –t <table> -i allsel

Test BRSPACE (Export/Import)
By default, export/import of an SAP table is protected by Database Vault. Therefore the following tests should not be able to perform successfully.

BRSPACE Table export/import with exp/imp:
$ brspace -u / -f tbexport -t T100
$ brspace -u / -f tbimport -t T100

BRSPACE Table export/import with Data Pump expdp/impdp:
$ brspace -u / -f tbexport -l expdp -t T100
$ brspace -u / -f tbimport -l impdp -t T100

Note: How to export a table from an Oracle Database Vault enabled database is described below.

Test BRSPACE (Tablespace Management)
Test Create tablespace:
$ brspace -u / -f tscreate -c data -f sapdata2 -t psaptestdv
Test Drop tablespace:
$ brspace -u / -f tsdrop -t psaptestdv

Test BRSPACE (Instance Management)
Run tests with BRSPACE as ora<sid>.
$ brspace -f dbstart -m normal -s open
$ brspace -f dbshut -m immediate

Test Export/Import
Oracle Database Vault protections policy for SAP prevents the use of exp/imp utilities for data export/import. If you try to export with exp, you will encounter the following error message:
EXP-00056: ORACLE error 47400 encountered
ORA-47400: Command Rule violation for CONNECT on LOGON

If there is a need to export or import data, you have to use Oracle datapump (expdp/impdp).

Test Oracle Data Pump Export/Import
By default, exporting SAP application data is protected by Oracle Database Vault. In case you need to export data, the Security Administrator needs to authorize it. Please follow the instructions described in Metalink note 822048.1: How To Export / Import Objects In Database Vault Environment.
Here’s an example on how to authorize SYS to export (or import) table T100 of user SAPSR3:

First, the Security Administrator SECADMIN must allow SYS to export this table.

```sql
$ sqlplus SECADMIN
SQL> EXEC DVSYS.DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('SYS','SAPSR3','T100');
```

Note that SYS is authorized for datapump operations only on table SAPSR3.T100, in this example.

```sql
$ sqlplus / as sysdba
SQL> create or replace directory dp_dir as '<path_name>'; 
Export the table using Data Pump:
$ expdp directory=dp_dir tables=sapsr3.t100 dumpfile=expdp_sapsr3_t100.dmp
You can also use brspace to perform this operation:
$ brspace -u / -f tbexport -l expdp -t T100
$ brspace -u / -f tbimport -l impdp -t T100
After the export (or import) is done, SECADMIN must revoke the authorization for Data Pump operations from SYS again:
$ sqlplus SECADMIN
SQL> EXEC DVSYS.DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('SYS','SAPSR3','T100');
```

Please note that Oracle Database Vault does not protect data in export dump files outside the database, it only protects data that is inside the database. Therefore you should encrypt export dump files when you export SAP application data to keep the data protected against unauthorized access. You can do that using BRSPACE, as well. For more information, see SAP note 1324684 (Link [https://service.sap.com/sap/support/notes/1324684](https://service.sap.com/sap/support/notes/1324684)).

**DV Installation Cleanup Tasks**

Oracle Database Vault installation and configuration is complete now. All tests have been run successfully, you are confident with the configuration and you have performed another backup of Oracle Home, Oracle Inventory and the database.

**Drop Restore Points**

You must drop all guaranteed restore points created previously before you continue using the SAP system for production operations. You do not need them any more. If you do not drop them the database will hang as soon as the flash recovery area is filled up with flashback logs.

```sql
SQL> SELECT NAME FROM V$RESTORE_POINT;
SQL> DROP RESTORE POINT <name of GRP>;
```

Alternatively you can use SAP BR*Tools BRSPACE to list and drop the restore points (see SAP note 1125923: ‘brspace -f mbackup –a rpdrop’, ‘brspace –f mbackup –a rpshow’).
Change Passwords

As a best practice you should now change the passwords of the newly created accounts SECADMIN and SECACCTMGR. This is especially important if the passwords have been stored in scripts or have been used on command lines. SECADMIN should change its own password while SECACCTMGR can change its own as well as other user passwords (except the SECADMIN one). This is for security reasons.

Customizing Database Vault protections for SAP

Customers must have the Oracle Database Vault protections for SAP installed and enabled before they can create additional custom Database Vault protections in the SAP environment.

In this section we will describe how customers can add their own custom Database Vault Realms, allow additional third party programs to access the SAP applications, and add their own IP addresses or subnets to the CONNECT Command Rule.

Restricting Access using the CONNECT Command Rule

Oracle Database Vault protections for SAP contains a template file called sap_rule_ip_template.sql located in folder administration/ip_based_access_configuration that shows how to configure the CONNECT command rule to restrict database connections to known IP addresses only.

When creating the CONNECT rule, the following SQL expression must be added to the rule expression (with AND):

\[(\text{UPPER(SYS\_CONTEXT("USERENV","IP\_ADDRESS")}) \text{ IS NULL OR}
\text{UPPER(SYS\_CONTEXT("USERENV","IP\_ADDRESS")}) \text{ in (\text{<ip\_address\_list>})}\]

\(<\text{ip\_address\_list}>\) is the placeholder for the list of IP addresses of those hosts from which database connections you want it to be allowed.

Example:

\[(\text{UPPER(SYS\_CONTEXT("USERENV","IP\_ADDRESS")}) \text{ IS NULL OR}
\text{UPPER(SYS\_CONTEXT("USERENV","IP\_ADDRESS")}) \text{ in ("127.0.0.5", "127.0.0.6")}\]

Overview of the Database Vault Protections for SAP

In this section we describe the pre-configured DV security protections provided specifically for SAP.

Database Accounts

**SECADMIN** (DV_OWNER role) – Security Administrator: The SECADMIN account is created during the installation of Oracle Database Vault. Do not change the name of this account. This account is the Oracle Database Vault Security Administrator.

The purpose of this account is to manage Database Vault Security policies. It can create, enable, disable, and delete Database Vault realms, Factors, rule sets, and command rules, for example.

With SECADMIN, you can logon to DVA and manage Oracle Database Vault protection as well as run DV security reports and monitor any attempted security policy violation. SECADMIN can also login to the SQL*Plus command line and do all DV security administration tasks using the DV API (Application Programming Interface). For separation of duty purposes, this account does not have any DBA or database account management privileges. As SECADMIN, you cannot create database accounts, create or drop
tables, access SAP application data, nor start or stop the database or SAP instances. SECADMIN is granted the DV_OWNER role. SECADMIN can grant the DV_OWNER role to other personalized security administrators’ accounts, if needed.

SECACCTMGR (DV_ACCTMGR role) – Security Account Manager: The SECACCTMGR account is created during the installation of Oracle Database Vault. Do not change the name of this account. The purpose of SECACCTMGR (Database Vault Account Manager) is to manage (create, drop, lock, unlock, and change password) database accounts. This account is granted the DV_ACCTMGR role. SECACCTMGR can grant the DV_ACCTMGR role to other personalized accounts of security account managers, if needed.

This account does not have any DBA privileges. As SECACCTMGR, you cannot create or drop tables, access SAP application data, or start or stop the database or the SAP instances.

SECACCTMGR cannot manage Database Vault Security, because it does not have the DV_OWNER role. This is to enforce separation of duty.

SECACCTMGR should not be used to change the password of the SAP application schema. Use SAPACCTMGR instead for this purpose.

SECANALYST (DV_SECANALYST role) – Security Monitor: This account is not installed by default. You can optionally create it afterwards if there is a need for it. SECANALYST is granted the role DV_SECANALYST. The script to create this user is in the file create_secanalyst.sql under <SAP_DV_policy>/dv_security_accounts directory.

The purpose of this account is to monitor the security configuration and to create security reports and run DV security reports either from the DVA or from the command line.

This account does not have any DBA privileges. As SECANALYST, you cannot create or drop tables, access SAP application data, or start or stop the database or the SAP instances.

LBACSYS: This account belongs to Oracle Label Security. Oracle Label Security (OLS) is implicitly installed during DV installation. Oracle Database Vault uses OLS internally. For SAP applications, this account is transparent. Do not touch this account or any of its objects.

SUPPORT_DBA: This account is created for Oracle Support. It can be used in an emergency or support situation. Oracle support needs access to SAP application data with DBA privilege. By default, this account is locked. This account should always be locked and only unlocked and enabled in a support or an emergency situation. It should be then locked back. Oracle Database Vault will audit all commands run by this user. The scripts to unlock / lock and to enable / disable this account are in the <SAP_DV_policy>/customer_support_access directory.

SAPACCTMGR (DV_ACCTMGR and SAPCRED roles): In an SAP environment, SAPACCTMGR user is allowed to change the password of the SAP application.

SYSTEM – Oracle Database default DBA: The Oracle built-in default database administration account is SYSTEM. It is recommended to lock this generic DBA account and create personalized DBA accounts instead. For SAP BR*Tools, the SYSTEM account is not required.

Database Accounts in SAP and their Separation of Duty Map

The purpose of this section is to provide an overview of database accounts that (typically) exist in an SAP environment and their corresponding responsibilities, after Oracle Database Vault is installed. Here, you
also find recommendations whether these accounts can be locked or whether they are essential for the SAP system.

### DATABASE USERS

<table>
<thead>
<tr>
<th>USER NAME</th>
<th>ACCOUNT STATUS</th>
<th>DESCRIPTION, RESPONSIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVF</td>
<td>LOCKED</td>
<td>Database Vault Repository; created by DVCA.</td>
</tr>
<tr>
<td>DVSYS</td>
<td>LOCKED</td>
<td>Database Vault Repository; created by DVCA. This account needs to be temporarily unlocked for the installation of a DV patch.</td>
</tr>
<tr>
<td>LBACSYS</td>
<td>OPEN / LOCKED</td>
<td>Oracle Label Security (OLS); created by DVCA during Database Vault Installation. DV uses OLS internally. This account can be locked.</td>
</tr>
<tr>
<td>SYSMAN</td>
<td>OPEN / LOCKED</td>
<td>Enterprise Manager Database Control (dbconsole) Administrator account; created by EMCA during installation of EM; can be locked if EM is not used</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>OPEN / LOCKED</td>
<td>Oracle Built-in Default DBA account; by default this account is not used by SAP BRT*Tools; can be locked.</td>
</tr>
</tbody>
</table>
| SYS       | OPEN           | Oracle Dictionary Account; SYSDBA used for certain administrative tasks; can not be locked; responsibilities include for example:  
  - RMAN Backup / Recovery  
  - Tablespace Management  
  - Segment Management (export/import, reorganization, SAPSYS)  
  - Instance management (start/stop, manage profile parameter)  
  - Update database roles (SAPDBA, SAPCONN) |
| SAPSR3    | OPEN           | SAP application account for ABAP stack; created by SAP install; cannot be locked. |
| SAP<SAPSID> | OPEN           | SAP application account for Java stack; created by SAP install; cannot be locked. |
| SAPSR3DB  | OPEN           | Account created by SAP installation; used for database administration. |
| OPS$ORA<SID> | OPEN           | Account created by SAP installation:  
  - Used for SAP application to connect  
  - Has SAPDBA role  
  - Used for database administration (backup database, backup archive logs, update statistics, check database, backup verification) |
| OPS$<SID>ADM | OPEN           | Purpose / Responsibility: see the definition of account OPS$<SID>ADM |
| SECDATA    | OPEN           | DV Security Administrator (DV_DV_OWNER role); created by DVCA during Database Vault installation; responsibilities:  
  - DV Security Administration (DV realms, DV rules, …etc)  
  - DV Policy for SAP (install, update, modify) |
Best Practices installing and Configuring Oracle Database Vault in an SAP Environment

- Grant DV_ADMIN / DV_OWNER role to additional Security Administrators

**SECACCTMGR** OPEN  
DV Account Manager (DV_ACCTMGR role); created by DVCA during DV installation; responsibility:
- Account Management (ALTER USER / CREATE USER)
- Grant CONNECT role to new accounts
- Can not change password of SAP application accounts
- Responsible for locking / unlocking SUPPORT_DBA account

**SAPACCTMGR** OPEN  
SAP Account Manager (SAPCRED role); created by SAP DV Policy scripts; responsibility:
- Password management for SAP accounts (ABAP and Java Stacks)
- Account Management
- Can grant SAP specific database roles (SAPDBA, SAPCONN, SAPCRED, SAPSYS)

**SECANALYST** OPEN  
Database Vault Reporting and Monitoring Manager (DV_SECANALYST role); not created by default; can be created on demand using create_secanalyst.sql script; responsibilities:
- Monitor DV Security violations in DVA
- Run DV security reports from DVA or command line

**SUPPORT_DBA** LOCKED  
Database Administrator for Oracle Support. SAP DV Policy scripts create this account during configuration. By default this account is locked. This account should only be unlocked by SECACCTMGR in an emergency or a support situation where Oracle support needs access to SAP application data.

---

**SAP Database Roles Overview**

**SAPCONN**: This role contains all database roles, system privileges, and object privileges that are needed by the SAP application, i.e. SAP database user (SAPR3, SAPS3, …etc).

**SAPDBA**: This role contains all database roles, system privileges, and object privileges that are needed by the OPS$-users. This role is used for initial database connection of the SAP application and also for database administration tasks.

**SAPSYS**: This is a new SAP-specific database role created only in a Database Vault environment. This role is used for database administration to allow segment management tasks like online redefinition of SAP application tables. It is created in the preparation step for installing and configuring Oracle Database Vault.

**SAPCRED**: This is a new SAP-specific database role. This role comprises of all database roles and privileges that are required to manage the SAP credentials. Example: Change the password of the database user of the SAP application (i.e. SAPS3).

**Oracle Database Vault Default Realms**

During the installation of DV, the following Oracle default realms are created:

- Database Vault Account Management
Best Practices installing and Configuring Oracle Database Vault in an SAP Environment

- Oracle Data Dictionary
- Oracle Database Vault
- Oracle Enterprise Manager

These realms are fully described in the Oracle Database Vault Administrator’s Guide.

SAP-Specific Oracle Database Vault Realms and Command Rule

The Oracle Database Vault protections for SAP create the following realms:

- SAP Application Administration Realm for SAP BR*Tools
- SAP Application Credential Protection Realm
- SAP Application Protection Realm for ABAP stack
- SAP Application Protection Realm for Java stack (if Java schema exists)
- SAP Application Protection Realm for SAP Admin Roles

Following is a description of these realms:

**SAP Application Administration Realm for SAP BR*Tools**: This realm protects all objects (tables, indexes, ...etc) that are needed by the SAP BR*Tools. This realm facilitates backend operations of SAP BR*Tools. SAP business data is protected against unauthorized access from the backend privileged users. SAPDBA role is authorized to this realm as OWNER.

**SAP Application Credential Protection Realm**: This realm protects SAP data responsible for credential management. The SAPCRED role is authorized to this realm as owner.

**SAP Application Protection Realm for ABAP stack**: This realm protects SAP business data against unauthorized access from the backend by privileged users and any non-authorized user. This Realm Protection is for the ABAP stack. SAP business users are allowed access through the SAP application. The SAP Application account is authorized to this realm as OWNER.

**SAP Application Protection Realm for Java stack** (only if Java schema exists): This Realm Protection is for the Java platform. SAP business users are allowed access through SAP application. The SAP Application account is authorized to this realm as OWNER.

**SAP Application Protection Realm for SAP Admin Roles**: This realm protects the SAP administration roles: SAPCONN, SAPDBA, SAPCRED, SAPSYS. SAPACCTMGR will be managing granting of these roles.

**CONNECT Command Rule**: After DV installation, you can no longer connect with the SAP account from sqlplus:

sqlplus /nolog
SQL> CONNECT SAPS3/

Enter password:
ERROR:
ORA-47400: Command Rule violation for CONNECT on LOGON
This is by design, because only the SAP application should be allowed to connect to the database with this account.

Database Vault Integration with Other Oracle Technology

In this section, we will cover how Oracle Database Vault integrates with some of the Oracle Database technology. The Oracle Database Vault Administrator’s Guide has a full section on the integration topic as well.

Transparent Data Encryption (TDE)

If you have Transparent Data Encryption enabled in your Oracle Database environment, you don’t need to do any additional configuration for DV to work with it. Oracle Database Vault works with it seamlessly and without any additional configuration. For TDE configuration with SAP, see SAP note 974876 (https://service.sap.com/sap/support/notes/974876).

Network Encryption (ASO)

Oracle Database Vault and Oracle Network Encryption (SAP note 973450) are completely independent and can be enabled or disabled independently from each other. For information on Oracle Network Encryption with SAP see SAP note 973450.

Oracle Enterprise Manager Grid Control (EMGC)

As of Oracle Enterprise Manager Grid Control release 10.2.0.5, Oracle Database Vault can be managed using the EMGC. See Oracle Metalink note 760748.1: Managing Database Vault from Grid Control 10.2.0.5.

Oracle LogMiner

With Oracle LogMiner, a database administrator can access data in the redo logs to analyze or fix some specific issue like data corruptions. Upon installation of Oracle Database Vault, access to the LogMiner packages is removed. If you need to access LogMiner packages again, please follow Metalink note 417601.1.

SAP on Oracle RAC

The same DV installation and configuration steps apply if you run your SAP system on Oracle Real Applications Cluster (RAC).

Oracle Data Guard Physical Standby

Oracle Database Vault works with Data Guard Physical Standby (Logical standby is not supported yet). For more information on configuring Data Guard Physical Standby with DV, refer Oracle Metalink note 754065.1.
# Appendix

## Terms and Abbreviations used in this document

<table>
<thead>
<tr>
<th>ABBREVIATION</th>
<th>MEANING/EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>EM</td>
<td>Enterprise Manager</td>
</tr>
<tr>
<td>EMGC</td>
<td>Enterprise Manager Grid Control</td>
</tr>
<tr>
<td>EMDB</td>
<td>Enterprise Manager Database Control (dbconsole)</td>
</tr>
<tr>
<td>DBCA</td>
<td>Database Configuration Assistant</td>
</tr>
<tr>
<td>DV</td>
<td>Database Vault</td>
</tr>
<tr>
<td>DVA</td>
<td>Database Vault Administrator</td>
</tr>
<tr>
<td>DVA is a graphical interface for DV administration</td>
<td></td>
</tr>
<tr>
<td>DVCA</td>
<td>Database Vault Configuration Assistant</td>
</tr>
<tr>
<td>RAC</td>
<td>Real Application Clusters (see SI)</td>
</tr>
<tr>
<td>SI</td>
<td>Single Instance (see RAC)</td>
</tr>
<tr>
<td>TWP</td>
<td>Technical White Paper</td>
</tr>
<tr>
<td>OUI</td>
<td>Oracle Universal Installer (runInstaller)</td>
</tr>
<tr>
<td>&lt;dv_base&gt;</td>
<td>Database Vault Base Directory</td>
</tr>
<tr>
<td>example: $SAPDATA_HOME/dbvault</td>
<td></td>
</tr>
<tr>
<td>&lt;dv_scripts&gt;</td>
<td>Base directory for Database Vault Policy Scripts for SAP</td>
</tr>
<tr>
<td>Example: &lt;dv_base&gt;/dv_scripts</td>
<td></td>
</tr>
<tr>
<td>&lt;dv_patches&gt;</td>
<td>Base directory for DV patches</td>
</tr>
<tr>
<td>Example: &lt;dv_base&gt;/dv_patches</td>
<td></td>
</tr>
<tr>
<td>&lt;dv_soft&gt;</td>
<td>Base directory for Database Vault Software Stage</td>
</tr>
<tr>
<td>Example: &lt;dv_base&gt;/dv_soft</td>
<td></td>
</tr>
<tr>
<td>&lt;SAP_DV_Policy&gt;</td>
<td>Directory that contains the Database Vault Policy scripts / Database Vault Protections for SAP. Scripts are run from this directory.</td>
</tr>
<tr>
<td>Example: &lt;dv_scripts&gt;/SAP_DV_Policy</td>
<td></td>
</tr>
<tr>
<td>Example: /oracle/&lt;SID&gt;/oradbvault/dv_scripts/SAP_DV_Policy</td>
<td></td>
</tr>
<tr>
<td>&lt;dv_logs&gt;</td>
<td>Base directory for log files and backup files created during DV installation</td>
</tr>
<tr>
<td>SoD</td>
<td>Separation of Duty</td>
</tr>
</tbody>
</table>
Installation Steps for Oracle Database Vault Patches

The procedure described here is for Non-RAC installations (Single Instance). For RAC, follow the steps described in Metalink note 731466.1: How to Install Database Vault Patches on top of 10.2.0.4.

Prepare DV Patch installation

1. Check that Database Vault is enabled:
   ```sql
   SQL> SELECT * FROM V$OPTION
   WHERE PARAMETER = 'Oracle Database Vault';
   ```
   This should return TRUE.

2. Make sure all instances running under the ORACLE_HOME being patched are cleanly shut down before installing this patch:
   a) Stop Enterprise Manager Database Control (dbconsole):
      ```
      $ emctl stop dbconsole
      ```
   b) Shut down the database:
      ```
      $ sqlplus /nolog
      SQL> conn / as sysoper
      SQL> shutdown immediate
      SQL> exit
      ```
   c) Stop the listener:
      ```
      $ lsnrctl stop
      ```

3. Back up Oracle Home:
   You should back up the database, Oracle Home and Oracle Inventory before you apply the patch.

4. Disable Database Vault:
   Re-link the Oracle database software with dv_off:
   ```
   $ cd $ORACLE_HOME/rdbms/lib
   $ make -f ins_rdbms.mk dv_off
   $ cd $ORACLE_HOME/bin
   $ relink oracle
   ```
   Successful relinking ends with:
   ```
   mv -f $ORACLE_HOME/bin/oracle $ORACLE_HOME/bin/oracleO
   mv $ORACLE_HOME/rdbms/lib/oracle $ORACLE_HOME/bin/oracle
   chmod 6751 $ORACLE_HOME/bin/oracle
   ```

5. Start the database instance:
   ```
   $ sqlplus /nolog
   SQL> connect / as sysoper
   SQL> startup
   ```

6. Verify that the Database Vault option has been linked off:
   ```
   SQL> SELECT * FROM V$OPTION
   WHERE PARAMETER = 'Oracle Database Vault';
   ```
   This should return FALSE.

7. Unlock the DVSYS account:
   ```
   sqlplus /nolog
   SQL> connect / as sysdba
   ```
SQL> ALTER USER DVSYS ACCOUNT UNLOCK;
SQL> SELECT ACCOUNT_STATUS FROM DBA_USERS
         WHERE USERNAME = 'DVSYS';

8. Set password for DVSYS account:
   This is necessary if you have forgotten the password. You need to provide the password when
   applying the patch later.
   Note: the DVSYS password is the same as that of the DV Owner, unless it was changed after
   Database Vault installation.
SQL> ALTER USER DVSYS IDENTIFIED BY <new password>;

9. Disable the Oracle Database Vault triggers:
   $sqlplus /nolog
   SQL> connect / as sysdba
   Check DV trigger status:
   SQL> SELECT TRIGGER_NAME, STATUS FROM DBA_TRIGGERS
           WHERE TRIGGER_NAME LIKE 'DV_%';
   Disable DV triggers:
   SQL> ALTER TRIGGER DVSYS.DV_BEFORE_DDL_TRG DISABLE;
   SQL> ALTER TRIGGER DVSYS.DV_AFTER_DDL_TRG DISABLE;
   Check DV trigger status:
   SQL> SELECT TRIGGER_NAME, STATUS FROM DBA_TRIGGERS
           WHERE TRIGGER_NAME LIKE 'DV_%';

10. Shut down the database instance:
    sqlplus /nolog
    SQL> connect / as sysoper
    SQL> shutdown immediate
    SQL> exit

11. Check Oracle inventory:
    Before you apply the patch, get a list of the installed patches:
    $ORACLE_HOME/OPatch/opatch lsinventory

12. Extract the PSE container file:
    $ unzip <patch file>

13. Set your current working directory to the directory where the patch is located:
    $ cd <patch directory>

14. Apply the patch with opatch:
    $ORACLE_HOME/OPatch/opatch apply

15. Check Oracle inventory again:
    $ORACLE_HOME/OPatch/opatch lsinventory

16. Back up Oracle Home:
    You should back up the new Oracle Home and Oracle Inventory after the patch is installed.

17. Relink the Oracle database software:
    Note: In a single instance environment, you can skip this step.
18. Start the database instance:
   sqlplus /nolog
   SQL> connect / as sysoper
   SQL> startup

19. Prepare to run catmac.sql:
   To run catmac.sql, you need the DVSYS and SYS passwords. Also, ensure that there is a
tablespace named TEMP. This is a requirement for release 10.2.0.4.
   Verify the password of DVSYS:
   SQL> connect dvsys/<pwd>
   Verify the password of SYS:
   SQL> connect SYS@<SID> as sysdba
   Check TEMP tablespace:
   SQL> select count(*) from dba_tablespaces where tablespace_name = 'TEMP';

20. Check the PATCH README.
   There might be additional steps mentioned to run before or after catmac.sql. In that case, follow
the instructions given there before you run catmac.sql in the next step.

21. Run catmac.sql as SYSDBA:
   $ sqlplus /nolog
   SQL> connect / as sysdba
   SQL> spool patch.log
   SQL> @?/rdbms/admin/catmac.sql SYSTEM TEMP <SYS_password> <DVSYS_password>
   SQL> spool off
   Check the spool file for errors.

22. Lock the DVSYS account:
   sqlplus /nolog
   SQL> connect / as sysdba
   SQL> ALTER USER DVSYS ACCOUNT LOCK;
   SQL> SELECT ACCOUNT_STATUS FROM DBA_USERS
   WHERE USERNAME = 'DVSYS';

23. Run the following command as the SYS user:
   sqlplus /nolog
   SQL> connect / as sysdba
   SQL> @?/rdbms/admin/utlrp.sql

24. Enable the Database Vault triggers (as Database Vault Owner/SECADMIN):
   sqlplus /nolog
   SQL> connect secadmin
   Check DV trigger status:
   SQL> SELECT TRIGGER_NAME, STATUS FROM DBA_TRIGGERS WHERE
   TRIGGER_NAME LIKE 'DV_%';
   Enable DV triggers:
   SQL> ALTER TRIGGER DVSYS.DV_BEFORE_DDL_TRG ENABLE;
Best Practices Installing and Configuring Oracle Database Vault in an SAP Environment

SQL> ALTER TRIGGER DV_SYS.DV_AFTER_DDL_TRG ENABLE;

Check DV trigger status:

SQL> SELECT TRIGGER_NAME, STATUS FROM DBA_TRIGGERS WHERE TRIGGER_NAME LIKE 'DV_%';

25. Shut down the database:

sqlplus /nolog
SQL> connect / as sysoper
SQL> SHUTDOWN IMMEDIATE

26. Enable Database Vault by re-linking Oracle with dv_on:

$ cd $ORACLE_HOME/rdbms/lib
$ make -f ins_rdbms.mk dv_on
$ cd $ORACLE_HOME/bin
$ relink oracle

27. Restart the database:

sqlplus /nolog
SQL> connect / as sysoper
SQL> startup

28. Check that Database Vault is enabled:

SQL> SELECT * FROM V$OPTION WHERE PARAMETER = 'Oracle Database Vault';
This should return TRUE.

29. Restart the listener:

$ lsnrctl start

30. Restart Oracle Enterprise Manager Database Control:

$ emctl start dbconsole

31. Connect as DV_OWNER (SECADMIN) and execute:

sqlplus /nolog
SQL> connect secadmin
SQL> exec dvsys.dbms_macadm.sync_rules;
SQL> exit

32. Disable database auditing

Installing a Database Vault patch reconfigures Database Auditing, which might cause performance issues. Therefore, you should run the noaudit.sql script after installing a DV patch. The noaudit.sql script is shipped together with the DV policy scripts for SAP.

Do the following to run the noaudit.sql script:

a) Disable Database Vault Realm (as SECADMIN)
b) Run noaudit.sql (as SYSDBA)
c) Enable Database Vault Realm (as SECADMIN)

33. Disable Database Vault Realm (as SECADMIN)

You can do this either via DVA interface or by running the following script:

sqlplus /nolog
SQL> connect secadmin
34. Run `noaudit.sql` (as SYSDBA):
   This script is part of the DV policy scripts for SAP.
   ```
   SQL> @noaudit/disable_dv_realm.sql
   SQL> exit
   ```
Verify that the script ran without errors.

35. Enable Database Vault Realm (as SECADMIN)
   You can do this either via DVA interface or by running the following script:
   ```
   sqlplus /nolog
   SQL> connect secadmin
   SQL> @noaudit/enable_dv_realm.sql
   SQL> exit
   ```
The patch installation is finished.