

# Oracle Database Workshop

## (Real Application Clusters, Database Vault, Transparent Data Encryption)

---

### Workshop Overview

The purpose of this workshop is to configure Oracle Real Application Clusters (RAC) with Database Vault and Transparent Data Encryption (TDE). This workshop will cover many advanced topics, including:

- Installing Oracle 11.1.0.6 Clusterware Software (CRS)
- Installing Oracle 11.1.0.6 Automatic Storage Management (ASM) Software
- Installing Oracle 10.2.0.1 Base Software with Advanced Security Option (ASO)
- Creating an Oracle 10.2.0.1 Database
- Patching the Oracle Database to 10.2.0.3
- Setting up and administrating Oracle Advanced Security Option
- Installing Oracle Database Vault 10.2.0.3
- Setting up Oracle Database Vault Realms, Command Rules, and Rule Sets

The cluster is located in Oracle's Enterprise Technology Center (ETC) in Atlanta, Georgia. The cluster configuration for this workshop is as follows:

- Two SUN Fire V490's with Four Dual Core Processors
- Solaris 10 (5.10) on each node
- 32 GB RAM on each node
- 36 GB swap space on each node
- 114 GB internal disk free space on each node (stores Oracle binaries)
- EMC DMX with seven 69 GB LUNs generated using PowerPath (used as ASM disks)
- NFS storage with 160 GB free space (used for shared SQL scripts and startup / shutdown scripts)

Estimated times for completing most tasks are included in this document. Within four hours, you will be able to install the clusterware, configure ASM, create an Oracle database, patch it to the latest release, configure ASO, encrypt columns, install Database Vault and setup Database Vault realms, factors and command rules.

At the conclusion of this half day workshop, participants should fully understand the installation and configuration process for Oracle Clusterware, ASM, Oracle Database, ASO and Oracle Database Vault. Oracle Database Vault and Advanced Security Option should be installed on all Oracle servers (development, test and production) that contain sensitive data. These solutions dramatically reduce the liability of Oracle Database Administrators (DBA's) and minimize the possibility of unauthorized users accessing sensitive data. Practically any security policy or business rule can be enforced with Oracle Database Vault.

---

## Oracle “Defense in Depth” Security Solution

Oracle defines data protection in three different categories: Prevention, Encryption, and Detection.

- **Prevention** is the strongest form of security and should be the highest priority for an organization. Oracle strongly advocates this security best practice for achieving information assurance that places security in a preventive mode of operation. By doing so, this prevents access to sensitive data by unauthorized users.
- **Encryption** is an important strategy in regards to data protection. This practice uses cryptography to prevent anyone except the intended recipient from reading the data. There are many types of data encryption, and they are the basis of securing data at-rest and in-transit.
- **Detection** is an important component, which completes the enterprise security cycle. Detection mechanism allows organizations to meet and maintain regulatory compliance via monitoring. Additionally, detection creates an auditable log of critical activities.

Oracle Database Vault is the solution that handles prevention. A high level overview can be found in the next section. Oracle Transparent Database Encryption (which is a component of Oracle Advance Security Option) provides encryption capabilities. Oracle Audit Vault provides detection and has the capabilities to notify individuals when policies are violated.

To provide the maximum protection to any Oracle database environment, Oracle Database Vault, Oracle Advanced Security and Oracle Audit Vault is recommended.

---

### Data Protection – Prevention (Oracle Database Vault)

Under normal circumstances, highly privileged database users have access to sensitive data. How can companies prevent such users from accessing sensitive information? More importantly what are the consequences from compromising such information?

From a financial perspective, a single compromise due to an intrusion can be detrimental to an organization along with negative effects on branding, customer loyalty, and corporate image.

Oracle believes the best protection against such threats is prevention. Oracle Database Vault allows preventive controls by assigning appropriate responsibilities and enforcing true “separation of duty”.

## Business Value

With real financial risks associated with non-compliance, and market share risk in the event of a breach, Oracle strongly recommends a preventive approach with Oracle Database Vault to avoid the possibility of fines and lost revenue.

Oracle's Database Vault is the only solution in the market that allows changes by authorized users through its access control policies. In other words, companies can prevent users with super-privileges (DBAs) from accessing sensitive data. By instituting a control in this manner, companies can demonstrate Payment Card Industry (PCI) compliance. Additionally, Oracle Database Vault provides a set of pre-defined reports that show who is accessing what data and under what conditions. These reports offer a means to demonstrate proof of compliance for organizations to external auditors.

## Business Reasons:

1. Restrict privileged user access to sensitive data - This solution dramatically lowers the chances that employees entrusted with defining and enforcing access rights can unlawfully view or transfer confidential company data.
2. Allows organizations to establish security policies on who, when, where and how data can be accessed - This is extremely important for organizations that have undergone or is considering a database consolidation effort. Additionally, security policies can be created that adheres to the organizations business practices. Most database commands and SQL can be applied to a business practice to "lock down" your Oracle database.
3. Protect database structures from intentional or accidental harmful changes - Table and column modifications cannot be submitted without authorization. Administrators or table owners cannot mistakenly change a database object. Separation of Duty can be accomplished with Oracle Database Vault.
4. Prevent physical changes to the database from users that are not physically in the data center - This solution can force all physical database changes to occur within the data center and only during specific maintenance windows. An example of a physical database modification is adding or removing a file from the database.
5. Intuitive user interface - Database Vault administration is completely web based. Security personnel do not need to know SQL commands or database internals.
6. Transparent to existing applications - Existing applications do not require modifications when Database Vault is installed. This solution is transparent to applications which allow a relatively quick implementation.
7. Implement stringent account management policies - This solution prevents highly privileged users from creating new users. This prevents workarounds to access confidential data.



## Requirements for Oracle Database Vault:

Oracle Database 9.2.0.8 or  
Oracle Database 10gR2 and higher (including 11gR1)

---

## Data Protection – Encryption

Immediately following prevention, encryption is the next layer in data protection. Protecting data “at-rest” and “in-transit” from any security breach is not just a good practice, but it is a requirement for many compliances, including PCI.

The solution encrypts sensitive data in Oracle databases without writing a single line of code. This is accomplished by using Transparent Data Encryption (TDE) and Network Encryption. Both of these solutions are part of Oracle's Advanced Security Option (ASO).

### Business Reasons:

1. Protect sensitive data on the network – This solution encrypts data between the database server and the middle-tier or client. In addition to encrypting network data, checksums can be leveraged to minimize network security threats. Data package theft, disruption, modification or replay is not permissible for any network data packet.
2. Protect sensitive data on the server – Specific columns can be selected to encrypt. Not only is the data encrypted on disk, the data is encrypted anywhere on the server (memory, redo log, temporary segments, and undo structure).
3. Automatically encrypt backups – Because the data is encrypted on disk, all subsequent backups will be encrypted. This allows companies to select their backup utility of choice and guarantee all Oracle database backups with consumer data are protected.
4. Transparent to existing applications – Existing applications do not require modifications when ASO is installed. No triggers, views or application modifications are required when implementing ASO.
5. Minimal performance impact – ASO has been tested thoroughly and results have demonstrated that encrypted data access (update, delete, select) typically results in less than a 3% performance overhead. Additionally, inserts have been proven to generate less than 1% performance overhead.
6. Flexible configuration – ASO allows each table to leverage a different encryption algorithm. AES192, AES128, AES256, and 3DES168 encryption algorithms can be used in a single database. Additionally, ASO can be enabled on an existing column via a single Data Definition Language (DDL) command.

7. Fast and simple key management – ASO allows organizations to change their wallet key based on regulatory requirements with ease. Re-keying the master wallet does not force any disk input / output (I/O) and this task can be completed within seconds.

**Requirements for ASO:**

ASO Network Encryption: 9iR2 or higher

ASO Transparent Data Encryption: 10gR2 or higher (including 11gR1)

## Workshop Overview

This document can be leveraged as a quick reference guide to install Oracle Clusterware, Oracle Automatic Storage Management, Oracle Real Application Clusters RDBMS, Oracle Advanced Security Option and Oracle Database Vault. The clusterware and ASM versions used in this workshop are 11.1.0.6. The database version is 10.2.0.3. This approach allows companies to upgrade the databases to 11gR1 without upgrading the clusterware or ASM.

The following documents should be reviewed prior to installing Real Application Clusters, Automatic Storage Management, Oracle RDBMS, Oracle Database Vault and Advanced Security.

- Oracle Clusterware 11gR1 Installation Guide
- Oracle Database 11gR1 Installation Guide (ASM Instructions)
- Oracle Database 10.2.0.1 Installation Guide
- Oracle Database 10.2.0.3 Patch Release Notes
- Oracle Database Vault 10.2.0.3 Installation Guide
- Oracle Database Vault 10.2.0.3 Administration Guide

Prior to starting the installation, confirm the physical memory, swap space and bit mode is set appropriately. SUN Solaris was leveraged for this workshop.

1. To check physical memory on a Solaris server:  

```
# /usr/sbin/prtconf | grep "Memory size"
Memory size: 32768 Megabytes
```
2. To determine swap space on a Solaris server:  

```
# /usr/sbin/swap -s
total: 60168k bytes allocated + 4944k reserved = 65112k used, 36718488k available
```
3. To confirm the server is running in 64 bit mode:  

```
# /bin/isainfo -kv
64-bit sparcv9 kernel modules
```
4. To confirm the processor cores:  

```
# psrinfo
0  on-line  since 07/17/2008 09:55:43
1  on-line  since 07/17/2008 09:55:43
2  on-line  since 07/17/2008 09:55:43
3  on-line  since 07/17/2008 09:55:19
16 on-line  since 07/17/2008 09:55:43
17 on-line  since 07/17/2008 09:55:43
18 on-line  since 07/17/2008 09:55:43
19 on-line  since 07/17/2008 09:55:43
```

## Workshop Exercises

Please follow the instructions in the Oracle 11gR1 Clusterware Installation Guide and the Oracle 11gR1 Database Installation Guide to install the Clusterware and Automatic Storage Management (ASM) software.

### GENERAL TIPS AND WORKAROUNDS DURING 11gR1 CRS and ASM INSTALLATION

1. As a best practice, install all software from one node. The hostname for all installations in this workshop is atl4903. The remote hostname is atl4904.
2. During the **11gR1 Clusterware** installation, the following issues may occur.
  - a. When inputting the public, private and VIP aliases in runInstaller, two error messages may appear stating an invalid IP address was inserted. Make sure you can ping the public and private aliases. Also make sure you can issue an nslookup on the VIP aliases. If the pings and nslookups are okay before installing 11gR1 Clusterware, ignore the error message by selecting 'Continue'.
  - b. If "Check failed" appears while 'Checking existence of VIP node application (required)' after running 'runcluvfy.sh stage -post crsinst...' in runInstaller, edit /etc/hosts and insert the VIP aliases and IP addresses, then manually run \$CRS\_HOME/crs/bin/vipca as root. Run 'olsnodes' as root to make sure your nodes are included in the cluster. Check the status of CRS by running 'crsctl check crs' and 'crs\_stat -t -v' as root. These files can be found in \$CRS\_HOME/crs/bin.
  - c. The 11gR1 Clusterware installation takes approximately fifteen minutes.
3. During the **11gR1 ASM** installation, perform the following:
  - a. Select 'Custom' in runInstaller. Do not select 'Enterprise' or 'Standard'.
  - b. The Oracle Base directory should be different than the Oracle Base directory for 11gR1 Clusterware.
  - c. When the 'Create Database' screen appears, select 'Configure Automatic Storage Management (ASM)'.
  - d. Since EMC PowerPath is handling the disk striping and mirroring, select 'External' redundancy. Create four ASM diskgroups using the 69 GB LUN candidates.
  - e. Consider using a non default listener and port for ASM.
  - f. To manage ASM at a later time, launch dbca from the ASM \$ORACLE\_HOME/bin directory.
  - g. The 11gR1 ASM installation takes approximately twenty minutes.

### INSTALL THE ORACLE SOFTWARE TO CREATE THE 10.2.0.1 DATABASE

4. Open two xterm windows (VNC, putty, etc.) and login as the oracle software owner
5. Unset the ORACLE\_HOME and ORACLE\_SID environment variable
  - a. unset ORACLE\_HOME; unset ORACLE\_SID
6. Setup the temporary directory environment variable
  - a. export TEMP=/tmp
7. Check environment variables associated with Oracle
  - a. env | grep -i oracle
  - b. Remove all Oracle related environment variables

8. Change directory to the location of the 10.2.0.1 database software
  - a. `cd /software/10gR2/db`
9. Start the Oracle Installer process (software will create instances on both nodes)
  - a. `./runInstaller` **(30 minutes)**
    - i. Select 'Enterprise Edition' when prompted for the "Select Installation Type"
    - ii. As a best practice, select an ORACLE\_BASE that is different than the 11g CRS and ASM ORACLE\_BASE.
    - iii. Please review Metalink note 578299.1. It explains the error message that specifically applies to using 11gR1 CRS and ASM with a 10gR2 RAC database. The workaround is to manually override the error message and proceed.
    - iv. Do not 'Upgrade an Existing Database' when prompted.
    - v. Select 'Create a Database' in the "Select Configuration Option" screen.
    - vi. Select 'Advanced' in the "Select Database Configuration" screen.
    - vii. Make sure all remote nodes are included on the "Summary" page.
    - viii. Select 'Custom Database' in the "Database Template" screen when DBCA is launched.
10. Capture the database control url from the installer process **(if Grid Control is not used)**
  - a. Bookmark it in your browser (<http://atlv4903:1158/em>)
  - b. Connect to database control and confirm it is operational
11. Set the Oracle environment variables (ORACLE\_SID, ORACLE\_HOME, ORACLE\_BASE)
12. If you wish to change the SQL\*Plus prompt to include the time and current service, perform the following:
  - a. Set an environment variable pointing to the directory for the login.sql file.
    - i. `SQLPATH=/u02/scripts; export SQLPATH`
  - b. The login.sql file in the SQLPATH directory should have the following lines:
    - i. `set time on`
    - ii. `set sqlprompt '_CONNECT_IDENTIFIER> '`
13. Connect to the database via the listener on both nodes to confirm it is operational
  - a. Connect to each instance and the service that was created with load balancing
  - b. `sqlplus system/password`
  - c. `sqlplus system/password@ORACLE_SERVICE`

## INSTALL ORACLE ADVANCED SECURITY OPTION

14. Confirm that ASO is not installed
  - a. Login to SQL\*Plus as sys and issue the following SQL statement
    - i. `select * from v$option where parameter like 'Transparent Data%';`
    - ii. The result should be 'FALSE'
    - iii. If the result is 'TRUE', go to step 20 (Review Metalink Note 567287.1)
15. Shutdown all Oracle processes (iSqlplus, dbconsole, database, and listener)
  - a. `cd; sh -x shutdown.sh` (script created to perform shutdown) **(3 minutes)**
    - i. `isqlplusctl stop`
    - ii. `emctl stop dbconsole` (*execute on both nodes*)
    - iii. `srvctl stop database -d prod -o immediate -c "sys/oracle1 as sysdba"`
      1. *Above command stops instances, database and services*
    - iv. *Issue 'srvctl config -n atlv4903' to determine listeners on a specific node*
    - v. `srvctl stop listener -n atlv4903 -l LISTENER_ATLV4903`
    - vi. `srvctl stop listener -n atlv4904 -l LISTENER_ATLV4904`

16. Change directory to the location of the 10.2.0.1 database software. This workshop takes this approach to demonstrate how to install ASO in an existing database.
  - a. `cd /software/10gR2/db`
  
17. Start the Oracle Installer process (software will modify binaries on both nodes)
  - a. `./runInstaller` **(10 minutes)**
    - i. Select 'Custom' when prompted for the "Select Installation Type"
    - ii. Select the 10gR2 destination in the "Specify Home Details" screen
    - iii. Select 'Advanced Security Option' and click 'Next'
    - iv. Complete the installation wizard.
  
18. Start the database, instances and services
  - a. `cd; sh -x startup.sh` (script created to perform startup) **(5 minutes)**
    - i. `svctl start listener -n atlv4903 -l LISTENER_ATLV4903`
    - ii. `svctl start listener -n atlv4904 -l LISTENER_ATLV4904`
    - iii. `svctl start database -d prod -c "sys/oracle1 as sysdba"`
      1. Above command starts the database and instances
    - iv. `svctl start service -d prod -c "sys/oracle1 as sysdba"`
      1. Above command starts the services on all nodes
    - v. `isqlplusctl start`
    - vi. `emctl start dbconsole` (execute on both nodes if not using Grid Control)
  
19. Confirm that ASO is installed
  - a. Login to SQL\*Plus as sys and issue the following SQL statement
    - i. `select * from v$option where parameter like 'Transparent Data%';`
    - ii. The result should be 'TRUE'
  
20. **Review Metalink Note 567287.1.** This note explains how to setup TDE in a RAC environment. Read the entire note (every line). Basically, the wallet should be managed from a single RAC node and the wallet should be pushed to the remote nodes using ``rcp``. If a wallet is created on each node, the encrypted columns will only be accessible via the first node that created the wallet. If a shared file system is preferred, only one wallet will exist and there is no need to copy wallets to remote nodes. However, if a shared file system is leveraged, this introduces a single point of failure for the wallet.
  
21. Create the TDE Wallet and push the wallet to the remote nodes
  - a. Modify the `sqlnet.ora` files on each node to specify the wallet location
    - i. Each node should maintain a copy of the wallet
    - ii. The following entry should be included in the `sqlnet.ora` file on each node (use the correct instance name instead of `prod1`)
 

```
"ENCRYPTION_WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /u04/app/oracle/admin/prod1/wallet/)
)
)"
```
  - b. Login to SQL\*Plus using 'sys as sysdba' on the node that installed the Oracle software
  - c. Create the wallet
    - i. Issue 'alter system set encryption key identified by "**wallet\_password**";'
  - d. Launch Oracle Wallet Manager (owm) and change "Auto Login" to true.

- e. Copy the wallet (ewallet.p12) and Single Sign-on file (cwallet.sso) the remote nodes using rcp

## 22. Create the DBVTEST user and two tables to test TDE

```
SQL> create user DBVTEST identified by DBVTEST default tablespace users;
SQL> grant connect,resource to DBVTEST;
SQL> connect DBVTEST/DBVTEST
SQL> create table DBVTEST.accounts (
            ssn          varchar2(9)          primary key,
            acc_no       number              not null,
            acc_name     varchar2(30)       not null);
SQL> insert into DBVTEST.accounts values ('123456780',101,'John Brown');
SQL> insert into DBVTEST.accounts values ('123456781',102,'Bill Jackson');
SQL> alter table DBVTEST.accounts modify (ssn encrypt no salt);
SQL> alter table DBVTEST.accounts modify (acc_no encrypt);
SQL> create table DBVTEST.customers (
            tax_id       varchar2(9)          encrypt using 'AES256' no salt primary key,
            cname        varchar2(30)       not null,
            cdesc        varchar2(30)       not null);
SQL> insert into DBVTEST.customers values ('987654322','Bed Bath and Beyond','Home Goods');
SQL> insert into DBVTEST.customers values ('987654321','Best Buy','Electronics');
SQL> select * from DBVTEST.accounts;
SQL> select * from DBVTEST.customers;
SQL> select * from user_encrypted_columns;
SQL> alter table DBVTEST.accounts rekey;
SQL> alter table DBVTEST.customers rekey using '3DES168';
SQL> select * from user_encrypted_columns;
SQL> alter table DBVTEST.accounts modify (acc_no decrypt);
SQL> select * from user_encrypted_columns;
```

## 23. Connect to the second instance and select data from the encrypted tables

24. If you would like to re-key the master key, perform the following
  - a. Change the key from node one (node that established the original key)
  - b. Close the wallet on the remote nodes
  - c. 'rcp' the wallet with the new master key to the remote nodes
  - d. Open the wallet on the remote nodes to load the master key into the SGA

## PATCH THE DATABASE TO 10.2.0.3

### 25. Change directory to the location of the 10.2.0.3 patch database software

- a. `cd /software/10.2.0.3/Disk1`

### 26. Shutdown all Oracle processes (iSqlplus, dbconsole, database, and listener)

- a. `cd; sh -x shutdown.sh` (script created to perform shutdown) **(3 minutes)**
  - i. `isqlplusctl stop`
  - ii. `emctl stop dbconsole` (*execute on both nodes*)
  - iii. `svrctl stop database -d prod -o immediate -c "sys/oracle1 as sysdba"`
  - iv. `svrctl stop listener -n atlv4903 -l LISTENER_ATLV4903`
  - v. `svrctl stop listener -n atlv4904 -l LISTENER_ATLV4904`

### 27. Start the Oracle Installer process (software will upgrade software on both nodes)

- a. `./runInstaller` **(10 minutes)**
  - i. Select the 10gR2 destination in the "Specify Home Details" screen
  - ii. Make sure all remote nodes are included on the "Summary" page.

28. Start the database listeners (all other oracle processes are stopped)
  - a. `srvctl start listener -n atlv4903 -l LISTENER_ATLV4903`
  - b. `srvctl start listener -n atlv4904 -l LISTENER_ATLV4904`
  
29. Change directory to the ORACLE\_HOME binary location
  - a. `cd $ORACLE_HOME/bin`
  
30. Start the Database Upgrade Assistant process
  - a. `dbua` **(35 minutes)**
    - i. Only upgrade the database, do not select 'Upgrade ASM'
    - ii. Confirm all instances and nodes are selected in the 'Summary' page
    - iii. `dbua` will start the database, instances and services
  
31. Connect to the database via the listener to confirm it is operational
  - a. Connect to each instance and the service that was created with load balancing
  - b. `sqlplus system/password`
  - c. `sqlplus system/password@ORACLE_SERVICE`
  
32. Test database control as a result of the upgrade process (if using DB Control)
  - a. This is the same url used earlier (<http://atlv4903:1158/em>)
  - b. Connect to database control and confirm it is operational
  
33. Shutdown all Oracle processes (iSqlplus, dbconsole, database, and listener)
  - a. `cd; sh -x shutdown.sh` (script created to perform shutdown) **(3 minutes)**
    - i. `isqlplusctl stop`
    - ii. `emctl stop dbconsole` (*execute on both nodes*)
    - iii. `srvctl stop database -d prod -o immediate -c "sys/oracle1 as sysdba"`
    - iv. `srvctl stop listener -n atlv4903 -l LISTENER_ATLV4903`
    - v. `srvctl stop listener -n atlv4904 -l LISTENER_ATLV4904`

## INSTALL ORACLE DATABASE VAULT

34. Set the ORACLE\_SID environment variable
  
35. Unset the ORACLE\_HOME environment variable
  - a. `unset ORACLE_HOME`
  
36. Set the ORACLE\_BASE environment variable
  - a. `export ORACLE_BASE=/u04/app/oracle`
  
37. Change directory to the location of the Database Vault software
  - a. `cd /software/DBV_Solaris64bit_stage`
  
38. Start the Oracle Installer process (will install DB Vault binaries on both nodes)
  - a. `./runInstaller` **(10 minutes)**
    - i. Confirm the correct ORACLE\_HOME is listed
    - ii. Create a database vault owner and database vault manager
    - iii. Make sure all remote nodes are included on the "Summary" page
  
39. Reset all Oracle environment variables on the node that executed runInstaller
  
40. Connect to the database from the node that executed runInstaller
  - a. `sqlplus system/password` (should see 'Database Vault' listed as installed option)

- b. runInstaller does not start the instances and services on the remote nodes
41. If you would like to connect as sysdba to the RAC instances, create a password file on each node to accomplish this. Otherwise, "sqlplus sys/oracle1 as sysdba" will fail. By default, Database Vault disables this functionality. "sqlplus / as sysdba" will still fail after the password file is created when Database Vault is enabled.
  - a. Execute the following command on each node
    - i. `orapwd file=$ORACLE_HOME/dbs/orapwSID password=sys_password force=y nosysdba=n`
  - b. NOTE: Executing "srvctl start database" using the -c option with 'sys/oracle1 as sysoper' will result in the following error messages after Database Vault is installed.
 

```
PRKP-1001 : Error starting instance prod1 on node atlv4903
CRS-0215: Could not start resource 'ora.prod.prod1.inst'.
PRKP-1001 : Error starting instance prod2 on node atlv4904
CRS-0215: Could not start resource 'ora.prod.prod2.inst'.
PRKP-1030 : Failed to start the service prod1.
CRS-0215: Could not start resource 'ora.prod.prod1.cs'.
PRKP-1030 : Failed to start the service prod2.
CRS-0215: Could not start resource 'ora.prod.prod2.cs'.
```
42. Start the listener and services on the remote nodes
  - a. `srvctl start instance -d prod -i prod2 -c "sys/oracle1 as sysdba"`
43. Run dvca on all remote nodes to set the correct instance parameters
  - a. The command below must be executed as root.
    - i. `dvca -action optionrac -racnode atlv4904 -oh /u04/app/oracle/product/10.2.0/dbs -jdbc_str jdbc:oracle:oci:@prod2 -silent`
      1. Enter the password for sys when prompted
      2. Enter the password for the database owner account when prompted
  - b. After this command is executed, re-enable SYSDBA access on the remote nodes. Make sure this is done via the oracle userid.
    - i. `orapwd file=$ORACLE_HOME/dbs/orapwSID password=sys_password force=y nosysdba=n`
44. Connect to the database via the listener to confirm it is operational
  - a. Connect to each instance and the service that was created with load balancing
  - b. `sqlplus system/password`
  - c. `sqlplus system/password@ORACLE_SERVICE`
45. Test database control as a result of the upgrade process (if using DB Control)
  - a. This is the same url used earlier (`http://atlv4903:1158/em`)
  - b. Connect to database control and confirm it is operational
46. Connect to the Database Vault url to confirm it is operational
  - a. The url is on the same port as OEM database control
  - b. The url is `http://atlv4903:1158/dva`
47. Connect to the iSQL\*Plus url to confirm it is operational
  - a. The url is `http://atlv4903:5560/isqlplus`
  - b. 5560 is the default port for iSQL\*Plus
48. Determine if any additional patches have been released for Database Vault 10.2.0.3

## **CREATE A DATABASE VAULT REALM ON THE "DBVTEST" SCHEMA**

49. Login to SQL\*Plus using dbvnmgr and create an account (NEWUSR)
  - a. NOTE: This must be executed using the Database Vault Manager id. SYS and SYSTEM no longer has privileges to create users with Database Vault enabled.
  - b. "create user NEWUSR identified by NEWUSR default tablespace users temporary tablespace temp;"
  - c. "grant connect, resource to NEWUSR;"
50. Login as SYSTEM or SYS and select data from the DBVTEST tables (customers and accounts)
51. Create a Database Vault Realm on the DBVTEST schema via the Database Vault GUI and list DBVTEST as the only participant.
52. Attempt to select data in the DBVTEST tables as SYSTEM and SYS
  - a. This operation should failed due to the realm that was just created
53. Create rule sets, command rules and factors to:
  - a. Restrict access from tools that are not included in a list
  - b. Restrict access from IP addresses that are not in a list
  - c. Restrict the DBVTEST user from altering and dropping a DBVTEST table
  - d. Restrict a user from selecting data from a table during a specific day and time
54. Remove the DBVTEST Realm and the DBVTEST related Command Rules
55. Drop the DBVTEST and NEWUSR users (make sure you connect as the Database Vault Manager)
56. Database Vault and Advanced Security Option is now ready for your application.

---

## **Summary**

We strongly believe we have proven solutions that directly address security requirements.

By leveraging best practices, Oracle is uniquely suited to address the urgent security needs, while taking a preventive approach toward enterprise security.

On behalf of the Oracle Team, we thank you for the opportunity to work with you and look forward to moving ahead in support of your initiatives.