Oracle Database Vault

DBA Administrative Best Practices

Table of Contents

Introduction

Oracle Database Vault provides powerful security controls for protecting applications and sensitive data. Oracle Database Vault prevents privileged users from accessing application data, restricts ad hoc database changes and enforces controls over how, when and where application data can be accessed. Oracle Database Vault secures existing database environments transparently, eliminating costly and time consuming application changes.

With the increased sophistication and number of attacks on data, it is more important than ever to put more security controls inside the database. However, most customers have a small number of DBAs to manage their databases and cannot afford having dedicated people to manage their database security. Database consolidation and improved operational efficiencies make it possible to have even less people to manage the database. Oracle Database Vault controls are flexible and provide security benefits to customers even when they have a single DBA. For large and medium sized IT departments, Oracle Database Vault controls help enforce the necessary protections for outsourcing and off-shoring where outside DBAs can manage the database without having access to application data.

Oracle Applications and major partner applications have been certified with Oracle Database Vault. Oracle Database Vault protections are available for Oracle E-Business Suite, Oracle PeopleSoft, Oracle Siebel, Oracle JD Edwards EnterpriseOne, Oracle Retail, and Oracle Financial Services. Oracle Database Vault protections are also available for SAP and Infosys Finacle. For more information on this and on how to protect your custom applications with Oracle Database Vault, visit the Oracle Database Vault web page mentioned below.

This paper covers DBA best practices with Oracle Database Vault. The major topics covered in this paper are: General Database Administration Tasks, Administering Database Users, Database Backup and Recovery, Database Replication, Database Tuning, Database Patching and Upgrade, and Oracle Enterprise Manager. For each of these topics, DBA best practices with Oracle Database Vault and security considerations are described. This paper also covers Managing Oracle Database Vault and details various customers' scenarios.

After reading this paper, DBAs should understand how to manage Oracle Database with Oracle Database Vault.

This paper assumes the reader has basic knowledge of Oracle Database Vault. For an introduction on Oracle Database Vault, refer to the Oracle Database Vault web page at:

http://www.oracle.com/technetwork/database/options/database-vault/index-085211.html

Database Administration Tasks Summary

The following table lists the common database administration tasks and shows where Oracle Database Vault operational controls are required.

Administration Task	Oracle Database Vault operational controls required?	Comments
General Database Administration Tasks		
Starting up and shutting down the database	No	
Creating databases	No	
Configuring database network connectivity	No	
Database cloning	No	
Managing database initialization parameters	Yes	Some parameters are protected by the ALTER SYSTEM command rule.
Scheduling database jobs	Yes	Proper Oracle Database Vault authorization should be granted for this task.
Administering Database Users		
Managing users and roles	Yes	See relevant section in this paper.
Creating and modifying database objects	Yes	See relevant section in this paper.
Database Backup and recovery		
Oracle Data Pump	Yes	Proper Oracle Database Vault authorization should be granted before doing this task.
Oracle RMAN	No	See relevant section in this paper on Oracle RMAN security best practices.
Oracle SQL*Loader	No	
Flashback	Yes	Proper Oracle Database Vault authorization should be granted before doing this task.
Managing database storage structures	Yes	Requires authorization to the Oracle Data Dictionary realm.
Database Replication		
Oracle Data Guard	Yes	Support note number 754065.1 provides step-by-step instructions on this.
Oracle Streams	Yes	Proper Oracle Database Vault authorization should be granted before doing this task.
Database Tuning		
DBMS_STATS PL/SQL Package	No	
Modifying database instance memory	No	
Automatic database diagnostic monitor (ADDM)	No	
Active session history (ASH)	No	

Administration Task	Oracle Database Vault operational controls required?	Comments
Automatic workload repository (AWR)	No	
SQL Tuning Advisor	No	
EXPLAIN PLAN	Yes	PLAN_TABLE should be accessible to DBA.
ANALYZE TABLE	Yes	CHAINED_ROWS table should be accessible to DBA.
Maintaining indexes	Yes	See relevant section in this paper.
Database Patching and Upgrade		
Performing database patching	Yes	See relevant section in this paper.
Performing software upgrade	No	
Performing database upgrade	Yes	See relevant section in this paper.
Oracle Enterprise Manager		
Configuring Oracle Enterprise Manager settings	No	
Adding administrators in Oracle Enterprise Manager	Yes	See relevant section in this paper.

Table 1 Summary of common DBA activities with comments where operational controls are required

General Database Administration Tasks

This section discusses general database tasks that don't fall under the other main topics covered in this paper. In particular, this section covers Managing Database Initialization Parameters and Scheduling Database Jobs and what Oracle Database Vault controls are required to do these tasks.

Managing Database Initialization Parameters

Some Database initialization parameters are controlled and protected by the ALTER SYSTEM command rule. These parameters are listed in the Oracle Database Vault Administrator's Guide, in the Default Rule Sets section, under "Allow Fine Grained Control of System Parameters" rule set. For a DBA to be able to alter these parameters, the following requirements need to be satisfied:

1. DBA user should have ALTER SYSTEM privilege.

2. DBA user should be added to the rule set "Allow Fine Grained Control of System Parameters". This is done by editing the rule set and adding a new rule that allows that. In the example shown in the screen, we add a rule we call "Verify user is allowed on ALTER SYSTEM command". This rule verifies that the session user is DBA_JSMITH before allowing the user to change the protected initialization parameters. The rule expression we use is: SYS_CONTEXT ('USERENV','SESSION_USER') ='DBA_JSMITH'.

Rules Associated To The Rule Set

Select	Rule Name △	Rule Expression
○	Are System Security Parameters Allowed	DVSYS.DBMS_MACADM.check_sys_sec_parm_varchar = 'Y'
○	Are Dump or Dest Parameters Allowed	DVSYS.DBMS_MACADM.check_dump_dest_parm_varchar = 'Y'
○	Are Backup Restore Parameters Allowed	DVSYS.DBMS_MACADM.check_backup_parm_varchar = 'Y'
◉	Verify user is allowed on ALTER SYSTEM command	SYS_CONTEXT('USERENV', 'SESSION_USER') = 'DBA_JSMITH'
○	Are Optimizer Parameters Allowed	DVSYS.DBMS_MACADM.check_optimizer_parm_varchar = 'Y'
○	Are PL-SQL Parameters Allowed	DVSYS.DBMS_MACADM.check_plsql_parm_varchar = 'Y'
○	Are Security Parameters Allowed	DVSYS.DBMS_MACADM.check_security_parm_varchar = 'Y'
○	Are Database File Parameters Allowed	DVSYS.DBMS_MACADM.check_db_file_parm_varchar = 'Y'

Figure 1 An example of a rule added to the rule set controlling the ALTER SYSTEM Command Rule

Note that customers can add their own rule or rules to allow multiple users or roles in their environment to change the protected initialization parameters.

3. Change the rule set evaluation option from "All True" to "Any True" and click OK to save the changes.
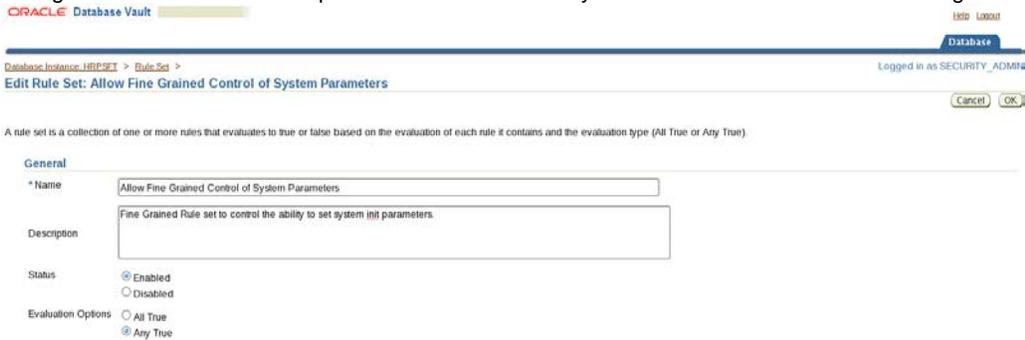
Figure 2 Change the Evaluation Type to "Any True" for the rule set of the ALTER SYSTEM Command Rule

Now the authorized DBA will be able to alter all database initialization parameters including the protected ones.

Scheduling Database Jobs

Scheduling a database job against a realm-protected schema requires Oracle Database Vault controls. This is to ensure proper authorization is in place. A DBA can be authorized to schedule database jobs on a schema by schema basis or on the entire database. Note that the DBA still needs the appropriate system privileges to run a database job such as CREATE JOB, CREATE ANY JOB, and MANAGE SCHEDULER.

In the following example, the DBA is authorized to schedule and run database jobs on the realm- protected HR application.
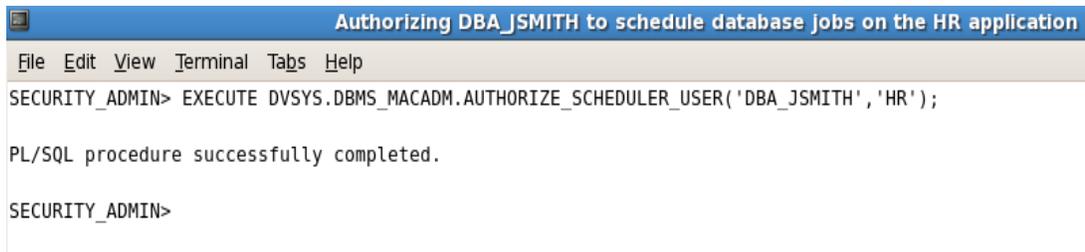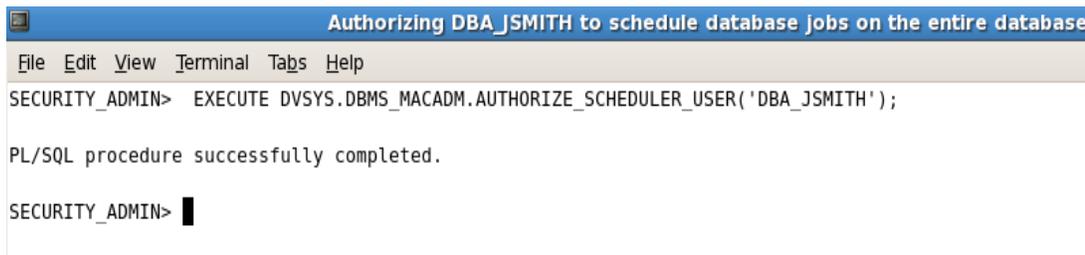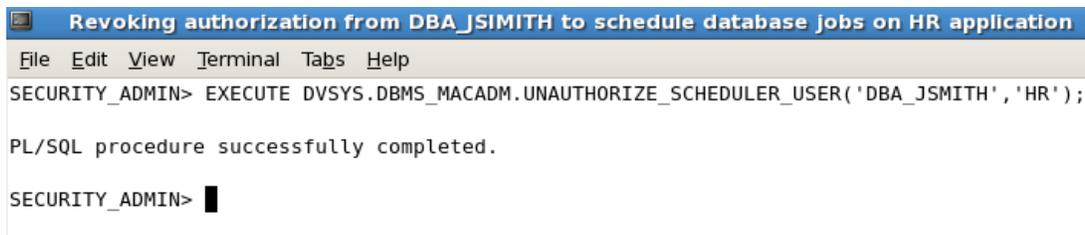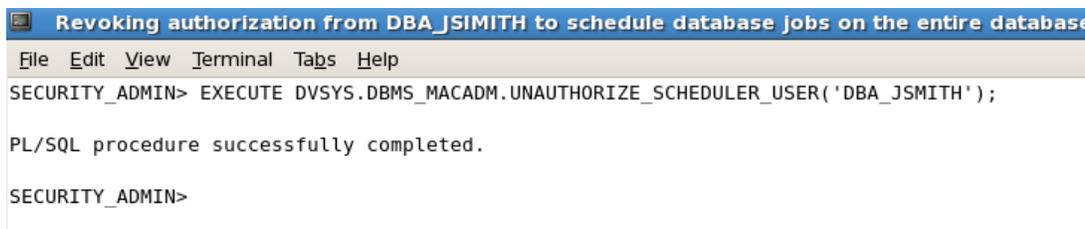

Authorizing DBA_JSMITH to schedule database jobs on the HR application

File Edit View Terminal Tabs Help

```
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('DBA_JSMITH','HR');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

Figure 3 DBA_JSMITH is authorized to schedule database jobs on the realm-protected HR application

The following screen shows how to authorize the DBA to schedule jobs on the entire database:

Authorizing DBA_JSMITH to schedule database jobs on the entire database

File Edit View Terminal Tabs Help

```
SECURITY_ADMIN>  EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('DBA_JSMITH');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

Figure 4 DBA_JSMITH is authorized to schedule database jobs on the entire database

If the DBA no longer needs to run database jobs on the entire database or on realm-protected schemas, the authorizations can be revoked as shown in the screens below.

Revoking authorization from DBA_JSIMITH to schedule database jobs on HR application

File Edit View Terminal Tabs Help

```
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('DBA_JSMITH','HR');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

Figure 5 Revoking authorization from DBA_JSMITH to schedule database jobs on HR application

Revoking authorization from DBA_JSIMITH to schedule database jobs on the entire database

File Edit View Terminal Tabs Help

```
SECURITY_ADMIN> EXECUTE DVSYS.DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('DBA_JSMITH');

PL/SQL procedure successfully completed.

SECURITY_ADMIN>
```

Figure 6 Revoking authorization from DBA_JSMITH to schedule database jobs on the entire database

Administering Database Users

Oracle Database Vault, optionally, separates the user administration task into a different role called Database Accounts Management (DV_ACCTMGR). DBAs can no longer create or manage database users by default. This is to eliminate ad hoc accounts creation and to prevent audit findings.

Managing Users and Roles

A Database Accounts Manager is a user who has been granted the DV_ACCTMGR role. The first Database Accounts Manager is created during Oracle Database Vault installation. As a best practice, the customer should create additional dedicated Database Accounts Managers and grant them the DV_ACCTMGR role.

The Database Accounts Manager can: create new users, grant the CONNECT role, manage existing users, and create and manage Oracle Database profiles. Note that, for security reasons, database accounts manager is not allowed to change the password for the Oracle Database Vault administrators (security administrators). Each Oracle Database Vault administrator can change his/her own password only.

Once users are created, a dedicated senior DBA account can grant them system privileges and roles as needed. A senior DBA is a DBA who has been granted the necessary system privileges and roles with ADMIN OPTION. Oracle Database Vault controls require the senior DBA to be authorized as OWNER to the Oracle Data Dictionary realm before granting other users system privileges and roles.

Database roles can be protected by Oracle Database Vault realms. Therefore the grantor, in addition to having admin option on these roles, needs to be authorized as OWNER to the realm that protects these roles. Note that default database roles are protected by the Oracle Data Dictionary realm.

Oracle Database Vault related roles can only be granted by the Oracle Database Vault administrator's account that was created during Oracle Database Vault installation. Similarly, the DV_ACCTMGR role can only be granted by the Database Accounts Manager account that was created during Oracle Database Vault installation.

Managing Users using Oracle Enterprise Manager

Database users can be managed from Oracle Enterprise Manager. This provides the database accounts manager with a nice user interface. The database accounts manager needs to have the Oracle Database Vault DV_ACCTMGR role. In addition, a senior DBA should grant the database accounts manager the SELECT ANY DICTIONARY privilege. Once this is done, the database accounts manager can login to Oracle Enterprise Manager; click on Server tab, then on the Users link. This is where the user management screen is located. Note that the database accounts manager can manage database users and profiles but cannot grant system privileges.

Figure 7 Screen shows database accounts manager managing database users from Oracle Enterprise Manager

Creating and Modifying Database Objects

A database user with the proper system privileges can create and modify database objects in his/her schema. However, if the user's schema is protected by a realm, then the user needs to be authorized as owner in the realm. This allows the user is be able to execute Data Definition Language (DDL) SQL statements such as CREATE TABLE and TRUNCATE TABLE on his/her own objects. Note that Data Manipulation Language (DML) SQL statements such as SELECT and UPDATE are not affected in this case.

Oracle Database Vault Command Rules can also affect the database user's ability to create or modify database objects. For example, if needed and for added security, a command rule can be created to prevent a user from truncating a table he/she owns. Oracle Database Vault Command Rules can be applied to almost any of the Oracle Database SQL commands. A set of default Command Rules are created when Oracle Database Vault is installed. They are described in the Oracle Database Vault Administrator's Guide.

Database Backup and Recovery

This section discusses backup and recovery in an Oracle Database with Oracle Database Vault. It covers Oracle Data Pump and security best practices for using Oracle Recovery Manager (RMAN).

Oracle Data Pump

Using Oracle Data Pump in an Oracle Database with Oracle Database Vault requires additional operational controls. This prevents ad hoc export of data while allowing authorized users to do so.

For example, let us assume the HR application is protected by a realm, and a DBA needs to export a table or the entire HR application. In this case, Oracle Database Vault operational controls are required and the DBA needs to be authorized to export the particular table or the entire HR application. The following figure shows the Oracle Database Vault administrator (SECURITY_ADMIN) authorizing DBA_JSMITH to export the HR.EMPLOYEES table:
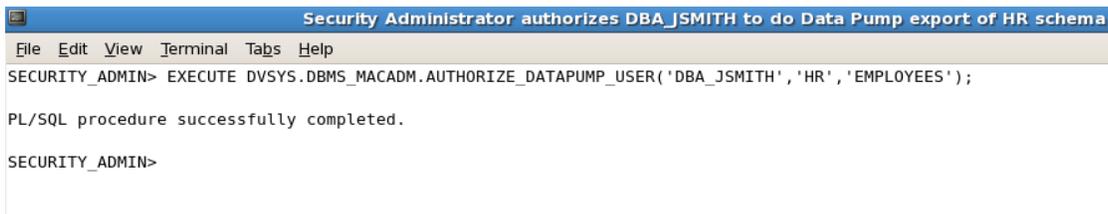
Figure 8 Authorize DBA_JSMITH to do Oracle Data Pump export on HR.EMPLOYEES

The DBA can be authorized to export the entire HR application:

Figure 9 Authorize DBA_JSMITH to do Oracle Data Pump export on the entire HR

Note: the DBA still needs the appropriate privileges such as EXP_FULL_DATABASE to be able to use Oracle Data Pump. Refer to the Oracle Database Utilities manual and the Oracle Database Vault Administrator's Guide for more information.

The DBA can be authorized to export the entire database. This would include Oracle Database Vault schemas DVSYS and DVF. The DBA, in this case, should be authorized to do so and should be granted the DV_OWNER role. The figure below shows how to authorize a DBA to export the entire database:

Figure 10 Authorize DBA_JSMITH to do Oracle Data Pump for the entire database

After the DBA finishes the Oracle Data Pump export operation, the Oracle Database Vault administrator can revoke the authorization as follows:
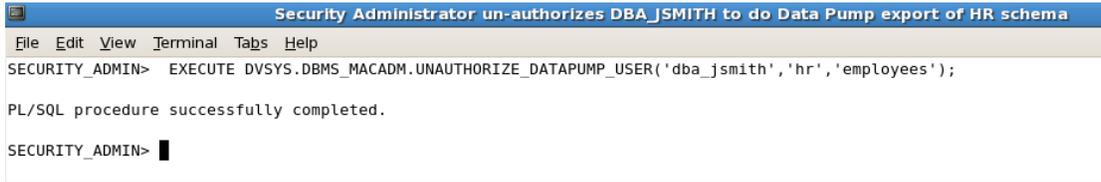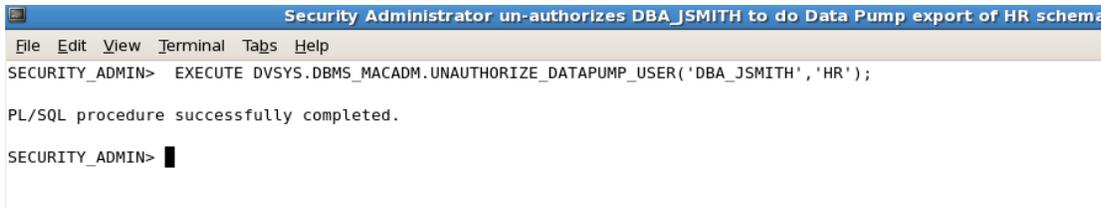

Figure 11 Revoke DBA_JSMITH privilege to do Oracle Data Pump export on HR.EMPLOYEES

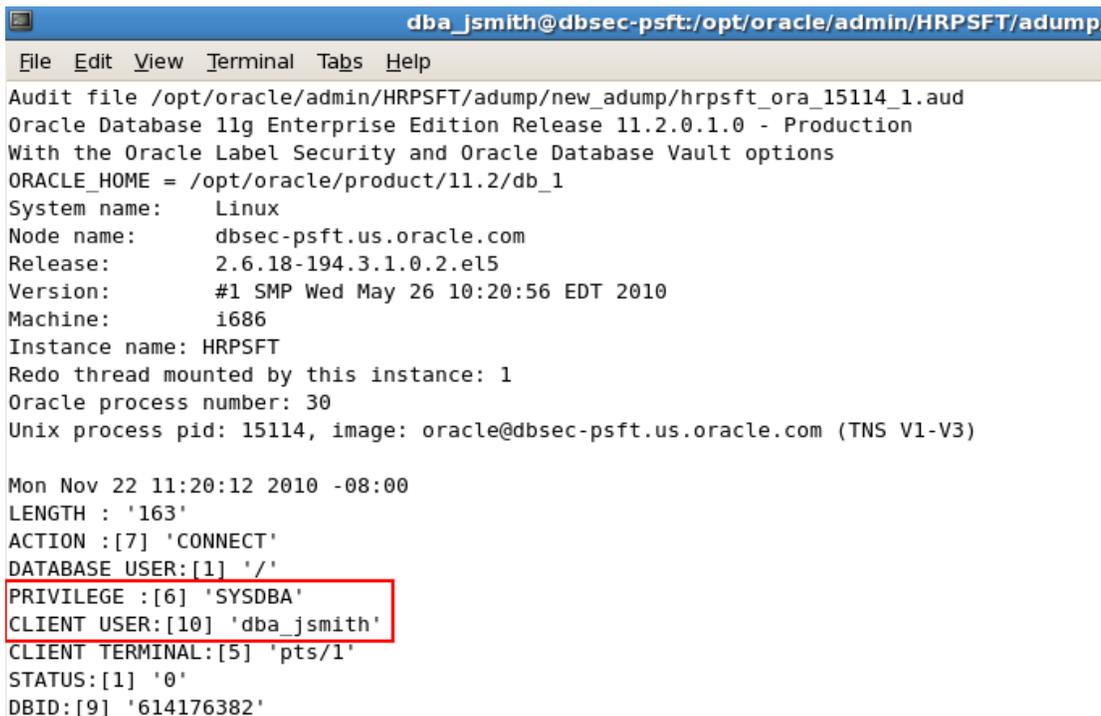Figure 12 Revoke DBA_JSMITH privilege to do Oracle Data Pump export on HR
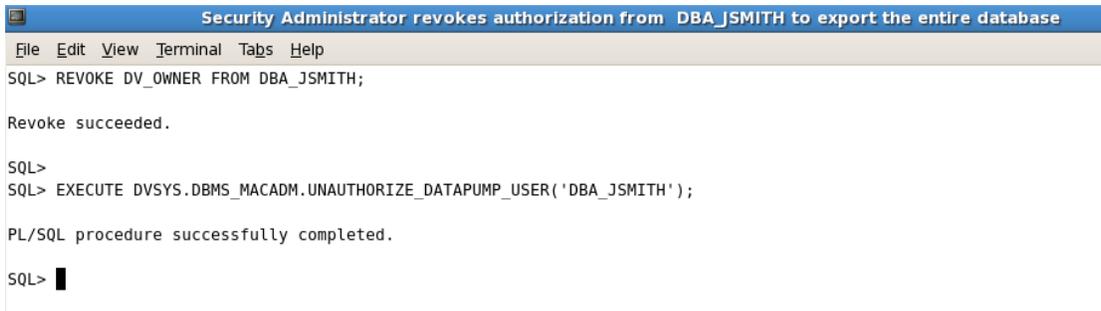
Figure 13 Revoke DBA_JSMITH privilege to do Oracle Data Pump export on the entire database

As a best practice, Oracle recommends encrypting Oracle Data Pump exports using Oracle Advanced Security. For more information on Oracle Data Pump, please refer to the Oracle Database Utilities manual.

Security Best Practices for using Oracle RMAN

Oracle RMAN requires the DBA to have operating system access to do backups and to login to the database with SYSDBA privilege. As a security best practice, Oracle recommends creating dedicated operating system accounts for DBAs who use Oracle RMAN. This enables customers to audit DBA operations using SYS AUDIT. It also alleviates the need for the DBA to login to the operating system as the Oracle software owner account. The following figure shows an audit record where DBA_JSMITH has logged in to the database using Oracle RMAN as SYSDBA to do database backup.

Figure 14 Audit record of DBA_JSMITH When logged in to the database using Oracle RMAN as SYSDBA

The added benefit of having dedicated operating system accounts for DBAs is they would not be able to turn off Oracle Database Vault protections.

Another security best practice for using Oracle RMAN is to encrypt database backups with Oracle Advanced Security. For more information on Oracle RMAN, please refer to the Oracle Backup and Recovery Reference.

Flashback Table

Flashback of a table to an earlier SCN or timestamp works as usual. However, if the table is protected by an Oracle Database Vault realm, then the DBA needs to be authorized to the realm for the duration of the Flashback operation.

In addition, Flashback dropped tables requires RECYCLEBIN to be enabled. Oracle Database Vault installation turns RECYCLEBIN off. This is because if a table protected by a realm is dropped, it gets moved to the recycle bin where it is not protected. Therefore, unless the customer explicitly turns on RECYCLEBIN to be able to FLASHBACK dropped tables, Flashback dropped tables would not work. Note that this is being considered as enhancement for a future release.

Managing Database Storage Structures

For the DBA to be able to manage the database storage structures, the DBA is typically granted privileges such as CREATE TABLESPACE, DROP TABLESPACE, and ALTER TABLESPACE. In an Oracle Database Vault environment, the DBA also needs to be authorized as PARTICIPANT or OWNER to the Oracle Data Dictionary realm.

Database Replication

In an Oracle Database Vault environment, Oracle Database cloning works as before with no change. But the database should be always cloned to an Oracle Home where Oracle Database Vault is enabled. This is to ensure that Oracle Database Vault protections persist in the cloned database environment. For other replication activities, such as Streams and Data Guard, proper Oracle Database Vault authorizations should be granted at the source database. The target databases should also be enabled with Oracle Database Vault for the protections to persist there.

Oracle Data Guard

There are three types of Oracle Data Guard: Data Guard Logical Standby, Data Guard Physical Standby, and Oracle Active Data Guard. Data Guard Physical Standby and Oracle Active Data Guard are both supported with Oracle Database Vault. Support note number 754065.1 provides step-by-step instructions on how to configure Oracle Data Guard in an Oracle Database with Oracle Database Vault. Oracle Data Guard Logical Standby is currently not supported with Oracle Database Vault. Support for Oracle Data Guard Logical Standby is planned for a future release.

Oracle Streams

Oracle Streams can replicate data from a realm-protected schema. However, Oracle Database Vault control requires the DV_STREAMS_ADMIN role to be granted to the DBA who configures Oracle Streams. This enables the tight management of Oracle Streams' processes using Oracle Database Vault, but does not change the way a DBA would normally configure Oracle Streams.
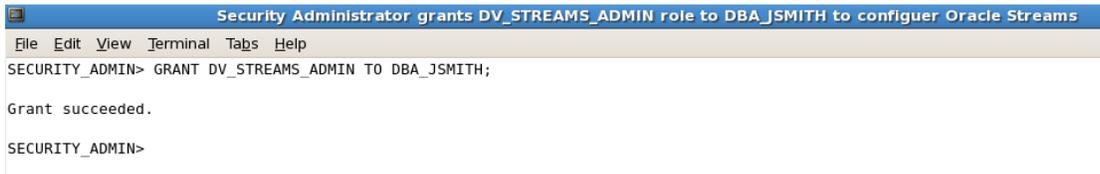
Figure 15 Grant DV_STREAMS_ADMIN role to a DBA to be able to configure Oracle Streams

Database Tuning

In this section, we will go over some of the tools and techniques DBAs use to tune the Oracle Database such as EXPLAIN PLAN and ANALYZE TABLE and what Oracle Database Vault operational controls are required. The goal is to protect sensitive application data while enabling the DBA to tune the database.

EXPLAIN PLAN

For a DBA to be able to run EXPLAIN PLAN on a realm protected table, the PLAN_TABLE needs to exist in a schema where the DBA has INSERT and SELECT privileges to it. The screen below shows how a DBA can run the

EXPLAIN PLAN command on a realm-protected table successfully. In this case, the PLAN_TABLE was created in the DBA_JSMITH schema. So, DBA_JSMITH has INSERT and SELECT privileges to the PLAN_TABLE.
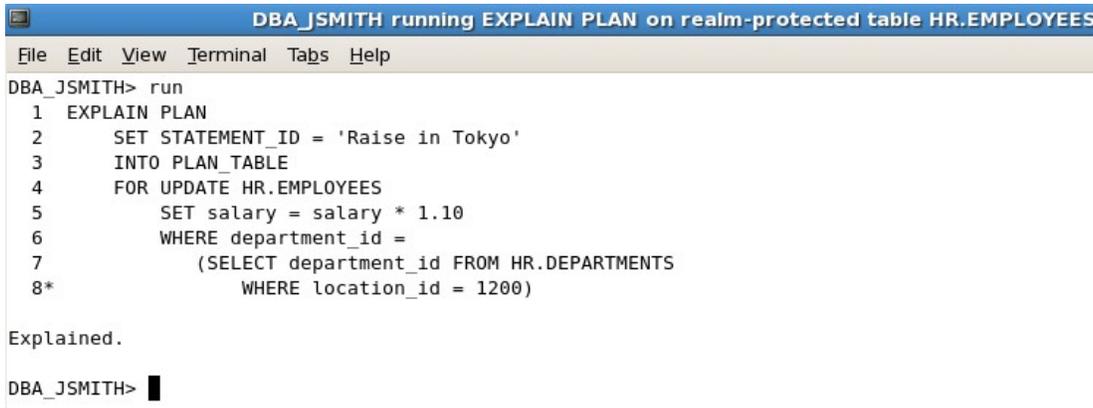
```
DBA_JSMITH running EXPLAIN PLAN on realm-protected table HR.EMPLOYEES
File  Edit  View  Terminal  Tabs  Help
DBA_JSMITH> run
  1  EXPLAIN PLAN
  2      SET STATEMENT_ID = 'Raise in Tokyo'
  3      INTO PLAN_TABLE
  4      FOR UPDATE HR.EMPLOYEES
  5          SET salary = salary * 1.10
  6          WHERE department_id =
  7              (SELECT department_id FROM HR.DEPARTMENTS
  8*                 WHERE location_id = 1200)

Explained.

DBA_JSMITH>
```
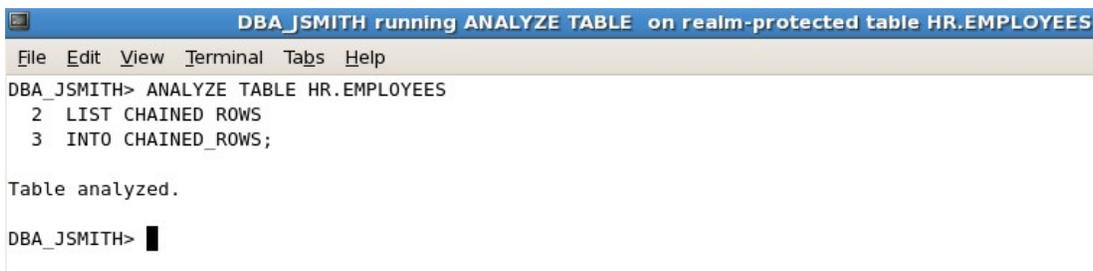
Figure 16 DBA running EXPLAIN PLAN successfully on a realm-protected table

In this case, the DBA running EXPLAIN PLAN does not need to be authorized to the realm and would not have access to realm-protected data.

ANALYZE TABLE

A DBA can run the ANALYZE TABLE command on a realm-protected table successfully without being authorized to the realm. However, to be able to LIST CHAINED ROWS, the DBA needs to create the table CHAINED_ROWS in a schema where he has INSERT and SELECT privileges. As shown in the screen below, DBA_JSMITH runs ANALYZE TABLE and lists the chained rows into the CHAINED_ROWS table that he created in his own schema. So, DBA_JSMITH has INSERT and SELECT privileges to the CHAINED_ROWS table.

```
DBA_JSMITH running ANALYZE TABLE  on realm-protected table HR.EMPLOYEES
File  Edit  View  Terminal  Tabs  Help
DBA_JSMITH> ANALYZE TABLE HR.EMPLOYEES
  2  LIST CHAINED ROWS
  3  INTO CHAINED_ROWS;

Table analyzed.

DBA_JSMITH>
```

Figure 17 DBA running ANALYZE TABLE successfully on a realm-protected table

In this case, the DBA running ANALYZE TABLE does not need to be authorized to the realm and would not have access to realm-protected data.

Maintaining Indexes

To allow a DBA to maintain indexes for realm-protected tables, a separate realm needs to be created for all their index types: Index, Index Partition, and Indextype. The DBA needs to be authorized as OWNER to this realm. The following shows an example of how to do this.

In our example, in addition to the "HR Application Protection Realm" that protects the entire HR schema, we create a second realm we call "Index Maintenance realm for HR Application" that protects all HR objects of types Index, Index Partition, and INDEXTYPE. Then we authorize DBA_JSMITH to this realm as OWNER.

* Name	Index Maintenance realm for HR Application
Description	This realm allows DBA_JSMITH to maintain indexes for the HR Application.

Status
- ◉ Enabled
- ○ Disabled

Audit Options
- ○ Audit Disabled
- ◉ Audit On Failure
- ○ Audit On Success or Failure

Realm Secured Objects

Create

Edit Remove

Select	Owner △	Object Type	Object Name
◉	HR	INDEX	%
○	HR	INDEX PARTITION	%
○	HR	INDEXTYPE	%

Edit Remove

Realm Authorizations

Create

Edit Remove

Select	Grantee △	Authorization Options	Authorization Rule Set Name
◉	DBA_JSMITH	Owner	

Figure 18 Indexes are separated in their own realm where DBAs can be authorized to maintain them

Now, as we see from the screen below, the DBA can rebuild an index for a protected table.


```
DBA_JSMITH rebuilding an index for the realm-protected table HR.DEPARTMENTS

File  Edit  View  Terminal  Tabs  Help

DBA_JSMITH> run
  1* ALTER INDEX HR.DEPT_ID_PK REBUILD

Index altered.

DBA_JSMITH>
```

Figure 19 DBA is able to alter the HR index once authorized to the "Index Maintenance realm for HR Application"

This allows the DBA to maintain indexes without having access to application data and gives control over who can maintain indexes. A database role can also be authorized to the index realm to manage the maintenance of the application indexes.

Database Patching and Upgrade

A DBA can patch the database without turning off Oracle Database Vault protection. However, the Oracle Database Vault role DV_PATCH_ADMIN needs to be granted to the DBA before the DBA can patch the database.

Figure 20 Grant DV_PATCH_ADMIN role to DBA_JSMITH to patch the database

The DBA then logs in to the database as SYS with the SYSDBA privilege to patch the database. Oracle Database Vault protections continue to be effective during database patching.

Figure 21 DBA can patch the database without having access to realm-protected application data

Once patching is complete, the DV_PATCH_ADMIN role should be revoked from the DBA.

Figure 22 Revoke DV_PATCH_ADMIN role from DBA after database patching is completed

E-Business Suite patching can be done without turning off Oracle Database Vault protection. For more information on patching E-Business Suite and other certified applications with Oracle Database Vault, refer to the relevant certification notes on the Oracle Support site.

Database upgrade, however, requires Oracle Database Vault protection to be turned off for the duration of the upgrade. During that process, Oracle recommends customers monitor all protected data using database audit. Once upgrade is done, Oracle Database Vault protection can be turned back on and database monitoring can go back to normal. Future release of Oracle Database will allow database upgrade without turning off Oracle Database Vault protection.

Oracle Enterprise Manager

Most of the tasks in Oracle Enterprise Manager do not require Oracle Database Vault controls. In this section we will cover adding Administrators to Oracle Enterprise Manager.

Adding administrators to Oracle Enterprise Manager

Adding an administrator to Oracle Enterprise Manager Database Control involves granting SELECT_CATALOG_ROLE to the new administrator. Oracle Data Dictionary realm protects this role and unless the user performing the task is authorized as OWNER to the realm, an error will occur. In the screen below user SYSMAN tries to add DBA_JSMITH as an administrator but gets an error.

Figure 23 Screen shows an error when SYSMAN tries to add an administrator in Database Control

In the Database Vault Administration screen below, SYSMAN is authorized as OWNER to the Oracle Data Dictionary realm:

Figure 24 SYSMAN is added as OWNER to the Oracle Data Dictionary realm

Now, SYSMAN can login to Oracle Enterprise Manager add a new administrator to the Oracle Enterprise Manager Administrators:

Figure 25 SYSMAN is able to add DBA_JSMITH as an administrator to Oracle Enterprise Manager Administrators

Managing Oracle Database Vault

With the increased sophistication of attacks on data, the need to put more operational controls on the database is greater than ever. Given the fact that most customers have a small number of DBAs to manage their databases, it is very important to keep database security related tasks separate in their own dedicated database accounts. Creating dedicated database accounts to manage database security helps customers prevent privileged DBA accounts from accessing application data, restricts ad hoc database changes, and enforces controls over how, when and where

application data can be accessed. Oracle Database Vault provides security benefits to customers even when they have a single DBA by:

1. Preventing hackers from using privileged users' accounts to steal application data
2. Protecting database structures from unauthorized and/or harmful changes
3. Enforcing controls over how, when and where application data can be accessed
4. Securing existing database environments transparently and without any application changes

In this section, we address managing Oracle Database Vault in different customer scenarios. These scenarios show how different customers, depending on how large they are and on the number of people available to manage their databases, have integrated Oracle Database Vault into their IT operation. The following diagram shows an outline of the main duties of a typical IT department and where Oracle Database Vault management and governance fit in the overall IT structure.
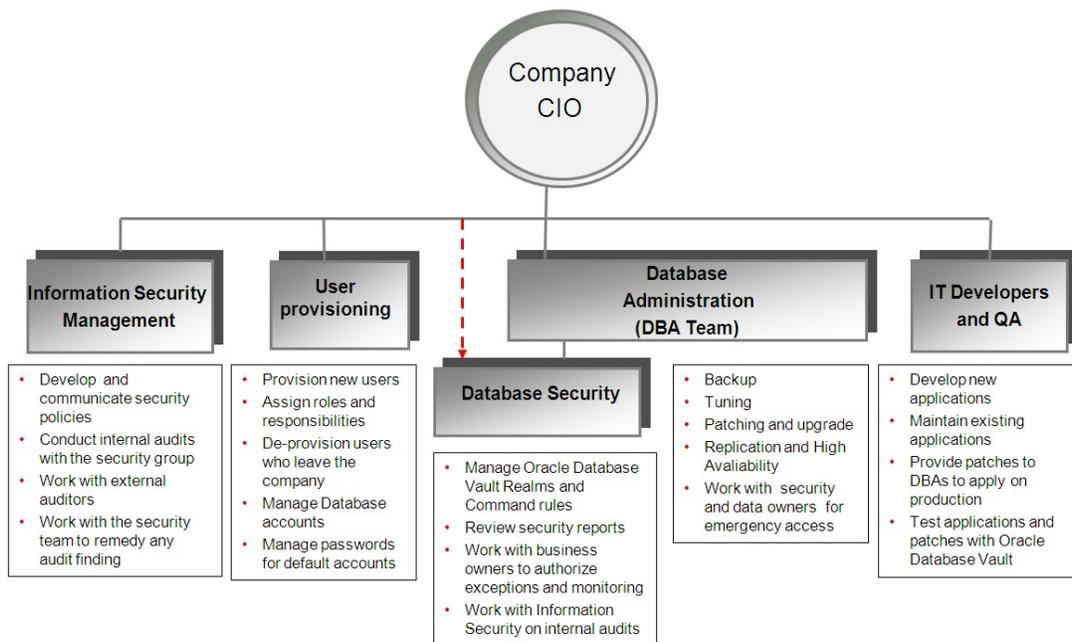

Figure 26 This diagram shows the main IT duties integrated with managing Oracle Database Vault

As we can see from the diagram above, the main IT duties are: Information Security Management, User Provisioning, Database Administration and Database Security, and Development and QA. Given the fact that most customers have a small IT department, most IT personnel have overlapping responsibilities. Let's first look at each of these IT duties:

» Information Security Management:
  » Develop and communicate company-wide internal security policies
  » Conduct internal audits periodically in conjunction with security to ensure compliance with internal security policies and industry regulations
  » Work with external auditors
  » Work with security to remedy any audit finding

» User Provisioning:
   » Provision new users
   » Assign roles and responsibilities to new and existing users
   » De-provision users who are no longer with the company
   » Manage database accounts
   » Manage passwords for default accounts including default Oracle Database Vault Accounts Administrator and Security Administrator

» Database Security:
   » Manage Oracle Database Vault: create realms, command rules, and factors and manage their authorizations
   » Review database security reports
   » Work with business owners to authorize exceptions and enable monitoring
   » Work closely with Information Security Management to conduct internal audits and to remedy any audit finding

» Database Administration:
   » Database backup
   » Database tuning
   » Database patching and upgrade
   » Database replication and high availability
   » Work closely with security and data owners to address exceptions and get emergency access

» IT development and Quality Assurance (QA):
   » Develop and test applications
   » Maintain existing applications
   » Provide patches to DBAs to apply on production environments
   » Test applications and patches with Oracle Database Vault

Now, let's cover three customer scenarios for small, medium, and large IT departments and see how they manage Oracle Database Vault.

In small sized IT departments where security procedures are evolving, the same person might be required to handle different responsibilities. For example, the same IT person might be administering the database and doing development and QA, or this person might be managing security and administering the database at the same time. In this case, we recommend that customers create separate dedicated accounts for each responsibility. For example, if John Smith is required to manage security and administer the database at the same time, then John Smith should have two separate database accounts with two different passwords: DBA_JSMITH for administering the database and SEC_ADMIN_JSMITH for managing database security. This is in addition to his dedicated operating system account. This helps the customer keep track of each account's actions for compliance and auditing purposes. This also prevents outside hackers from having access to application data if they manage to hijack a privileged database account.

In medium sized IT departments, a small number of people can be dedicated to security and they would typically handle more than one responsibility. For example, people who handle security might also be responsible for user provisioning. DBAs may be doing some development and system management. Developers might be doing

database administration in addition to their development and testing activities. With Oracle Database Vault, customers are able to protect sensitive data from hackers' attacks that hijack privileged database accounts. Customers are also able to protect production environments from any harmful and/or unauthorized changes.

In large IT departments, different people can be assigned to different responsibilities and each main area mentioned in the diagram might have its own dedicated staff. In this case, database accounts management is part of user provisioning and database security works closely with both information security and the DBAs. With Oracle Database Vault, Database Security is able to control what activities DBAs are allowed to do inside the Oracle Database. This is especially useful in outsourcing situations where outside DBAs need to have privileged database accounts but are prohibited from accessing sensitive data.

Conclusion

With the increased sophistication and number of attacks on data, it is more important than ever to enable strong security controls inside the database. Oracle Database Vault provides powerful and flexible security controls to protect applications and sensitive data. Oracle Database Vault realms, multi-factor authorization and command rules can be used individually or in combination to enforce operational controls and prevent data breaches. Oracle Database Vault control provides security benefits to customers even when they have a single DBA. As IT organizations and data governance models evolve, Oracle Database Vault controls can be customized to match new policies and procedures. Oracle Database Vault polices are available for major Oracle and partner applications, including Oracle PeopleSoft, Oracle E-Business Suite, Oracle Siebel and SAP.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE®

Hardware and Software, Engineered to Work Together

Oracle Database Vault DBA Administrative Best Practices
May 2015

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