Implementing Oracle Database Vault – Step By Step

Oded Raz
Oracle ACE Director, Brillix
Israel

Keywords:

Oracle Database Vault Security Separation of Duties, SOX, PCI, HIPPA

Introduction
Separation of duty has taken on increased importance over the past 10 years. For many organizations separation of duty is a new concept that continues to evolve. Database consolidation, regulatory compliance and outsourcing are just a few of the drivers for increased separation of duty. Database Vault separation of duty strengthens security by separating out security related administration from day to day DBA operations. Database Vault allows organizations to tailor their Database Vault separation of duty implementation to easily adapt to current and future business requirements. Small organizations, in particular, need flexibility as they attempt to increase their security profile with limited resources.

Before separation of duty can be successful, it is important to understand who performs basic administration tasks in your environment and what those administration tasks are. Even if a single DBA is responsible for managing both new database account provisioning and application patching, these individual tasks are important to document and plan for. Using separate administration accounts for these types of tasks provides increased accountability and reduces associated risks. In midsize to large organizations database administrators typically need to perform common administration tasks but they don't need access to business data managed by the application. Creating a matrix for your separation of duty can be a helpful exercise when planning your Database Vault deployment. Additional tasks and associated users can be added to this list. This information should become part of the overall enterprise security documentation for your organization. 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 who, when, where, and how application data can be accessed. Oracle Database Vault secures existing database environments transparently, eliminating costly and time consuming application changes.

Why – Oracle Database Vault
Up until now DBA's and other privileged database users could access sensitive data and there was almost nothing we could do about it. In the past few years organization data is rapidly growing holding sensitive business information such as financial data, customers data and more. As data grows so the amount of people handling the data and have a direct access to it such as DBA's, programmers, reports administrators and such. It became very hard controlling and preventing access to sensitive data from privileged users.

Oracle Database Vault helps organizations address regulatory mandates and increase the security of existing applications. Regulations such as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and similar global directives call for separation-of-duties and other

preventive controls to ensure data integrity and data privacy. With Oracle Database Vault, organizations can pro-actively safeguard application data stored in the Oracle database from being accessed by privileged database users.

Oracle database vault enables you to:

- Pro-actively safeguard application data stored in the Oracle database—Restrict access by unauthorized database users – even privileged users – by using powerful access controls built into the Oracle database.
- Address regulatory requirements—Implement separation-of-duty and other real-time preventive controls.
- Restrict ad-hoc access to application data— Prevent application-bypass with multi-factor policies that are enforced in the database for high security and performance.
- Deploy with confidence—Use certified default policies for Oracle E-Business Suite, Oracle PeopleSoft, and Oracle Siebel CRM applications.

Oracle Database Vault introduction

Oracle Database Vault restricts access to specific areas in an Oracle database from any user, including users who have administrative access. For example, you can restrict administrative access to employee salaries, customer medical records, or other sensitive information.

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

With Oracle Database Vault, you address the most difficult security problems remaining today: protecting against insider threats, meeting regulatory compliance requirements, and enforcing separation of duty.

Application data can be further protected using Oracle Database Vault’s multi-factor policies that control access based on built-in factors such as time of day, IP address, application name, and authentication method, preventing unauthorized ad-hoc access and application by-pass.

Let me give you a simple example how database vault can help us apply separation of duties in your database. Let's say we have 2 schema's in the database – HR and OE that hold HR sensitive data, when our regular DBA (who does not allow to see HR data) tries to query data related to HR database vault prevent it, when our HR DBA (who can access HR data, but not allowed to manage database users) try's creating a new database user database vault prevents it, and as seen on *Illustration 1: database vault separation of duties* database vault prevent accessing the database using "connect as sysdba" from every one.

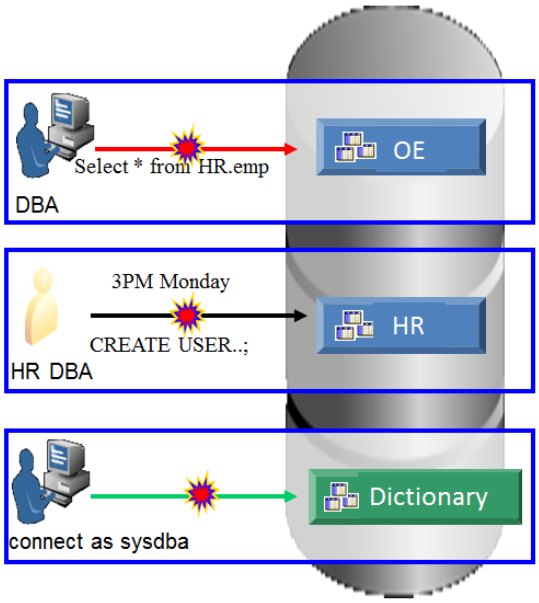

Illustration 1: database vault separation of duties.

Database Vault Building Blocks
Oracle database vault uses the following building block to implement security policies:

Realms:
Oracle Database Vault realms can protect a single object or an entire application schema. In most cases protecting the entire application provides a simplified yet robust protection model. Once a realm has been created, multiple users can be authorized to access the realm. Database objects (accounts, roles....) can be authorized in multiple realms.

Roles set:
Rule sets can be created that restrict access based on time, specific hosts, subnets or any other Database Vault factors supplied out-of-the-box. In addition, custom factors can be created using the Oracle Application Context.

- Each authorized user can be associated with a different Database Vault Rule Set.
- Each authorized user can be associated with a different Rule Set that specifies conditions and restrictions on access to the objects protected by the realm.

Command Roles:
Oracle Database Vault Command Rules can be used to protect application objects from modification. For example, command rules can be used to place restrictions on the drop table command. Once created, the command rule can be associated with a Database Vault rule set that is called Disabled. For patching or maintenance operations the command rule can be edited and associated with a rule set called Enabled.

Rules Sets:
Rule sets provide an easy way to group individual rules together into a meaningful set. You can share rules among multiple rule sets. This lets you develop a library of reusable rule expressions. Oracle recommends that you design such rules to be discrete, single-purpose expressions. As a naming convention, name your rule starting with a verb and complete the name with the purpose of the rule.

For example, to create a rule that allows connections coming from certain IP addresses, name the rule: "Allow Connect from Middle Tier IP Addresses". Name Rule Sets starting with a noun and complete the name with the name of the Command Rule, Factor, or Realm authorization that it will be associated with. For example, the name for the rule set that will be associated with the SADM user's access to the Siebel Realm will be: "Siebel SADM Realm Access". In the Rule Set Description field, document the business requirements that are accomplished by this Rule Set.

Factors:
Oracle Database Vault factors can be leveraged in your rule expressions to provide powerful checks and also to increase overall security by eliminating the requirement to manually define context values inside Oracle. Quite simply, factors provide contextual information to use in your security rules expressions.

Database vault Installation
Database vault installation varies between versions; database vault is available from version 9.2.0.8 and 10.2.0.4 and up. In Oracle 9 and 10 database vault is installed as ad-on patch, starting Oracle 11.1 database vault is a database feature that can be enabled or disabled using DBCA.
Before installing database vault some pre-requisites must be met:

- Oracle Label Security must be installed.
- Oracle database control must be installed or Oracle Grid Control mast be available.
- When installing database vault on Oracle 10g ASM must not be installed in the same ORACLE_HOME as the database.

During the enablement process, DBCA provides the ability to create an account management responsibility. Oracle recommends creating this responsibility to provide enhanced separation of duties between Oracle Database Vault administration, database account management, and the DBA responsibilities. Customers can use Oracle Enterprise Manager Cloud Control 12c to manage Oracle Database Vault.

Starting with Oracle Database 12c, Oracle Database Vault is installed by default but not enabled. Customers can enable it using DBCA or from the command line using SQL*Plus in a matter of minutes. Oracle Database Vault can be enabled in existing environments where Oracle and third party applications are already installed. Subsequent installation of new applications or patching require Oracle Database Vault DV_PATCH_ADMIN role to be granted to the user doing the installation or patching.

When installing Oracle database vault on Oracle 10g please follow the following metalink note:
What to Check for a Successful Database Vault Installation in 10gR2 (Doc ID 793739.1).

For more information about Database Vault Installation please follow this video:
Database Vault Installation - Step By Step

Using Database vault
During my presentation, I will demonstrate how to use database vault to achieve separation of duties and protect sensitive data.
Please follow the following videos to see the demo's that will take place in the session:

Oracle Database Vault - 11g Installation and Realms

Database Vault - Factors & Role sets

Oracle Database Vault - Advanced Factors

Using Database Vault built-in packages
Although database vault administration is done mainly using the supplied GUI, oracle provides a set of build-in packages to manage database vault, these packages may become useful when we want to script database vault roles in order to spread them across several databases or when the GUI is not available for some reasons. The supplied database vault packages reside under DVSYS schema, there are 3 main packages you should now about:

- *DVSYS.DBMS_MACADM* - Configure Realms, Rules Sets, Command Roles and more.
- *DVSYS.DBMS_MACSEC_ROLES* – Setting Secure application roles
- *DVSYS.DBMS_MACUTL* – Contains pre-defined constants to use alongside DVSYS.DBMS_MACADM.

Documentation on the available functions and procedures in the above packages can be found here - http://docs.oracle.com/cd/B28359_01/server.111/b31222/apis_dbms_macadm.htm

Uninstall database vault
Once database vault is installed you should not try and uninstall it. Using DBCA to uninstall database vault will delete necessary files in ORACLE_HOME and you will need to reinstall the entire ORACLE_HOME, but all is not lost you can disable it as will.

Disable Oracle 10g:
How To Reconfigure Database Vault in 10g (Doc ID 744390.1)

Disable Oracle 11g:
How To Uninstall Or Reinstall Database Vault in 11g (Doc ID 803948.1)

Contact address:

Oded Raz
Brillix LTD
Moshe Sne 28
Petach Tikva, Israel

Phone: +972(54)4746926
Fax: +972(3)5472632
Email oded@brillix.co.il
Internet: www.dbsnaps.com