Oracle Database Vault

by

Craig Moir

Of

MyDBA

May 2012
Oracle Database Vault

What is Oracle Database Vault?

Oracle Database Vault is a database security option that allows you to address the most pressing security problems facing organizations today, and that is:

- protecting sensitive data against insider threats;
- meeting regulatory compliance requirements; and
- enforcing Separation of Duties.
Oracle Database Vault

Oracle Database Vault in a nutshell

Database Vault provides real time preventive controls by restricting access to application data by highly privileged users and enabling control over who, when, where and how databases and application data can be accessed and/or changed.

In other words:

- **Nobody** can view **any data in any table** without authority.
- **Nobody** can make **any change** without authority and control.
Oracle Database Vault

Oracle Database Vault Architecture

- **Realms**: is the term used to identify a boundary that is set up around a set of objects in a schema that you want to protect. Specific conditions must exist to gain access to what is protected by the Realm.

- **Factors**: are attributes of a user or the system at any given time which contribute to the decision making process used to authorise access or not. A combination of several factors may be considered at once.

- **Identities**: are specific values that Factors may take on.

- **Rule Sets**: is a collection of one or more rules that are evaluated for the purpose of granting access.

- **Command Rules**: rules that determine the execution of ‘commands’ on an object/s.

- **Secure Application Roles**: A secure application role is a role that can be enabled dynamically based on the evaluation of an Oracle Database Vault rule set.
Oracle Database Vault

Oracle Database Vault Architecture

REALMS:

functional grouping of database schemas, objects, and roles that must be secured
Oracle Database Vault

Oracle Database Vault Architecture

FACTORS: A factor is a named variable or attribute

<table>
<thead>
<tr>
<th>USER</th>
<th>FACTOR</th>
<th>OBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR Clerk</td>
<td>Domain = Internet</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Update HR.EMPLOYEES set .....</td>
<td>Ault</td>
</tr>
<tr>
<td>HR Clerk</td>
<td>WorkHours = Weekend</td>
<td>Jones</td>
</tr>
<tr>
<td></td>
<td>Update HR.EMPLOYEES set .....</td>
<td>Smith</td>
</tr>
<tr>
<td>ASMITH</td>
<td>UserID=ASMITH</td>
<td>Tait</td>
</tr>
<tr>
<td></td>
<td>IP_ADDR=10.2.210.123</td>
<td>Zimmer</td>
</tr>
</tbody>
</table>

Update HR.EMPLOYEES set .....

Copyright © 2012 MyDBA CC
IDENTITIES: An Identity is a value associated with a FACTOR which have a TRUST level assigned.
RULE SETS: A collection of rules evaluated together to produce as result.

**RULE**

1. Is Machine Local?

2. Is Office Hours?

6. Is column <> sysdate?

**EVALUATION**

- TRUE or FALSE
- AND / OR
- TRUE or FALSE
- AND / OR
- TRUE or FALSE

**RULE SET RESULT**

- TRUE or FALSE
**Oracle Database Vault Architecture**

**COMMAND RULES**: Defines the rules that must be followed to perform a command on an object, typically DDL and DML.

**REQUEST**
- To perform this Command
- On this Object
- That is owned by this User
- This Rule Set must evaluate to TRUE

**COMMAND RULE**
- Command Type
- Object
- Owner
- Rule Set

**EXAMPLE**
- Alter Table
- SALARIES
- HR
- Is it HR_DBA & After_Hours?
SECURE APPLICATION ROLES: Roles that are enabled on User request by the Application, depending on the outcome of the evaluation of the associated rule set.
Oracle Database Vault

Oracle Database Vault Advantages

• Protects your data from ‘super-user’ access but still allows them to administer your Oracle Databases.
• Protects database and schema structures from unauthorized change.
• Defines when, where, what and who can make database, application and data changes.
• Enforces Separation of Duties.
• Meets Regulatory compliance such as POPI, King III and SOX.
• Enforces Internal Control measures.
• Transparent to Applications.
Oracle Database Vault

Oracle Database Vault Examples

- DBA’s can fully manage the database but cannot access (read) application data.
- Data structures can only be modified by specific personnel from specific PC’s at specific times.
- Data is only modified from within the Application.
- Applications can be individually secured within the same database using Realms therefore disallowing even ‘SELECT ANY TABLE’ or similar global database privileges.
- Multi-Factor authentication processes.
- Multiple Identity values.
- Data access Rule Sets – Logging in from a specific PC and a specific time.
- Command Rule Sets - covering DDL and DML restrictions.
- Secure Application Roles - enabled conditionally and dynamically.
Oracle Database Vault Scenario

At 15H00 on Tuesday

CREATE USER ...

SELECT * FROM HR.SALARIES;

CONNECT AS SYSDBA
Oracle Database Vault Operability

- Host installation and administration done through Database Vault Configuration Assistant (DVCA).
- Full security administration via web based Database Vault Administrator (DVA).
- Comprehensive reporting from 13 predefined Database Vault reports and 40 general database security reports.
- Detailed monitoring capabilities covering Policy Changes, Violation Attempts and Configuration and Structural changes.
- Database Vault API.
- Supports RAC and Data Guard.
Oracle Database Vault

Oracle Database Vault Summary

- Data is protected – even from the DBA and System Administrator.
- Fully POPI, King III and Sox compliant.
- Enforces Separation of Duties (SoD).
- Enforces Principle of Least Privilege.
- Monitoring and Reporting.
- Auditing.
Oracle Database Vault

MyDBA Security Credentials

- Oracle Database 11g Security Options Certified Implementation Specialists.
- Database Vault implementation experience.
- MyDBA Lectures Oracle Identity Manager at Oracle University SA.
- MyDBA Lectures Oracle Access Manager at Oracle University SA.
- MyDBA Lectures Oracle Database 10GR2 Security at Oracle University SA.
For more information on MyDBA’s security consulting services please contact us on:

security@mydba.co.za
0861 911 DBA
+27 11 027 9400
http://www.mydba.co.za

Disclaimer: This document is provided for information purposes only. While MyDBA has taken care to ensure that the content on this document is accurate, the information is provided "as is" and is not warranted to be error-free. Your use of and reliance on the information is entirely at your own risk.

This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the prior written permission of MyDBA.