An Oracle White Paper
March 2010

Oracle Database Vault for SAP
Introduction

International laws and regulations have been introduced for the financial sector in response to the falsification of balance sheets and misuse of data uncovered over the last few years. This legislation includes the Sarbanes-Oxley (SOX) Act, EuroSOX and Basel II. Companies which are subject to these regulations must therefore run internal inspection measures to allow them to guarantee and document that their published financial data is correct and reliable.

This in turn meant that additional monitoring measures needed to be implemented to raise the bar as far as overall data security is concerned.

It is most often the authorization concept of SAP applications that companies currently deploy to control and/or prevent access to application data stored in an SAP system.

However, Oracle database administrators can also access the content of all SAP tables and therefore all application data stored in the system even though this is not needed for their remit or responsibility. The data accessed by Oracle administrators is only rarely monitored or logged if at all.

With Oracle Database 11.2 Oracle Database Vault (hereinafter: DV) is a fully integrated database security option. It has been developed to prevent database administrators from accessing tables of application data.

Oracle Database Vault is also being implemented for SAP customers since Oracle Database 10.2.0.4. Since July 2009 Oracle Database Vault is for SAP in status of controlled availability (CA).
The Database Vault concept

DV is basically based on the idea of splitting and sharing administrative database tasks (SOD = "Separation of Duty"). This is done by introducing additional database roles and users and re-allocating tasks and responsibilities which previously were solely allocated to the role of the database administrator.

The main objective is thereby achieved: only those authorized to access sensitive SAP data requiring protection as a result of their role and function can do so. Database administrators only need to be able to access application data in order to carry out their tasks in a very small number of clearly exceptional cases.

Without Oracle Database Vault, the following central users have existed to date in SAP-Oracle databases:

- `sys` (DBA, owner of Oracle internal tables)
- `system` (DBA, is used by the BR*Tools)
- `sap<sid>` (owner of SAP tables)
- `sapr3` (owner of SAP tables in older SAP versions)
- `ops$<sid>adm` (used by SAP logon mechanism at database level)

With Oracle Database Vault, the following new users are also created:

- `secadmin` (owner of DV relevant tables and objects, security administrator)
- `secacctmgr` (DV account manager, security user manager)
- `sapacctmgr` (SAP account manager: user who manages the SAP password, …)
- `secanalyst` (User for monitoring and reporting purposes) - optional

The names of these users have been laid down by Oracle and SAP. (For support purposes it is recommended not to change these names.)
Changes resulting from Database Vault

As previously mentioned, the introduction of DV results in changes to the allocation of database user tasks:

<table>
<thead>
<tr>
<th>TASK</th>
<th>USER WITHOUT DV</th>
<th>NEW USER USING DV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database user administration</td>
<td>sys</td>
<td>secacctmgr</td>
</tr>
<tr>
<td>Password administration of SAP user sap&lt;sid&gt;</td>
<td>system or sys</td>
<td>sapacctmgr</td>
</tr>
</tbody>
</table>

Database Vault components

- Database Vault uses its own components to control and/or prevent access to data:
  - Realms
  - Command Rules
  - Rule Sets
  - Factors

Realm

A realm is a kind of "protective zone". Individual database objects like tables, all objects from a database schema or even database roles are assigned to a realm. A realm also includes dedicated access rights.

In the SAP environment for example a realm is used to protect the ABAP Stack, i.e. all tables belonging to the sap<sid> user. One subset of these are tables which are used by the BR*Tools. These are also protected by another realm, which does however permit the BR*Tools' access to these tables.

Command Rule

A Command Rule determines how DDL, DML or other database operations are performed. For example, a Command Rule can define the SELECT for tables in the SAP schema. Every Command Rule forms part of a Rule Set.
Rule Set

A Rule Set consists of one or more rules. The rules in a Rule Set define whether a Command Rule may be executed or not. One example of a rule is who can execute the Command Rule and who cannot. Another rule may be which programs can execute the Command Rule or which are excluded from it.

The final decision can be defined in a Rule Set on the basis of the associated rules in two ways:

1. Each individual rule has to be satisfied for the Rule Set as a whole to be satisfied.

or

2. At least one of the rules has to be satisfied for the Rule Set as a whole to be satisfied.

Factor

A Factor is one potential part of a rule. For example, this may be the IP address, network protocol, a program or even the time. A factor can be used to refine the access rules.

These DV components can now be used to control access to database objects in a dedicated and detailed way.
Licensing of TDE

TDE is part of the Advanced Security Option (ASO), which is contained in the Oracle database license offered by SAP. If the database license is bought directly from Oracle it has to be in the license scope prior using TDE.

Installing Database Vault

Requirements

Oracle DV for 11g is supported in the SAP environment with the same restrictions as an 11g database. The DV Option must be enabled during the Oracle database 11g installation. And also the Oracle Enterprise Manager Console (Database Control) for this database must be installed.

Installing software for Database Vault

With Oracle 11g DV is installed when selected in the Oracle Installer as one of the database options in the Oracle Database Home with the Oracle Installer and as an additional component in the database. The Oracle Installer then launches the Database Vault Configuration Assistant (DVCA). The users secadmin and secacctmgr and other DV users, tables and procedures are also created in the process. These DV objects are automatically protected by internal realms and rules to prevent unauthorized access.

Uninstalling Database Vault

Database Vault cannot be uninstalled! However, users may deactivate DV to return to the original state before having installed DV.

SAP-specific activation

The Database Vault configuration for SAP systems is undertaken once the DV software has been installed. This is done by running certain predefined SQL scripts. The DV policy for SAP installed thereby creates DV components such as Realms, Command Rules and Rule Sets adapted to SAP and activates them. Functions of the DVSYS.DBMS_MACADM package, which is only available to users with a DV_ADMIN or DV_OWNER role, e.g. secadmin, are used for this purpose in the SQL scripts.
Access rights

Once DV has been activated for a SAP system, as is shown below the access rights for SAP data are very restricted for the sys database administrator. SELECT and DML operations are blocked, but DDL operations are permitted.

**EXAMPLES AS SYS USER (SQLPLUS / AS SYSDBA):**

<table>
<thead>
<tr>
<th>QUERY</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>select * from &quot;SAPSR3&quot;.&quot;T100&quot;;</td>
<td>ORA-01031: insufficient privileges</td>
</tr>
<tr>
<td>select count(*) from &quot;SAPSR3&quot;.&quot;T100&quot;;</td>
<td>ORA-01031: insufficient privileges</td>
</tr>
<tr>
<td>create table sys.sapsr3_T100 as select * from sapsr3.t100;</td>
<td>ORA-01031: insufficient privileges</td>
</tr>
<tr>
<td>create table sapsr3.dv_test (c1 number);</td>
<td>OK</td>
</tr>
<tr>
<td>create index sapsr3.i_dv_test on sapsr3.dv_test (c1);</td>
<td>OK</td>
</tr>
<tr>
<td>analyze table sapsr3.dv_test validate structure;</td>
<td>OK</td>
</tr>
<tr>
<td>analyze table sapsr3.dv_test validate structure cascade;</td>
<td>OK</td>
</tr>
<tr>
<td>desc sapsr3.dv_test</td>
<td>OK</td>
</tr>
<tr>
<td>insert into sapsr3.dv_test values (1);</td>
<td>ORA-01031: insufficient privileges</td>
</tr>
<tr>
<td>delete from sapsr3.dv_test;</td>
<td>ORA-01031: insufficient privileges</td>
</tr>
<tr>
<td>truncate table sapsr3.dv_test;</td>
<td>OK</td>
</tr>
<tr>
<td>drop table sapsr3.dv_test;</td>
<td>OK</td>
</tr>
</tbody>
</table>

As a further security feature, the SAP user sap<sid> (or sapr3) can no longer be connected to the database using sqlplus:

Example – restricting the SAP user:

```
sqlplus /nolog
SQL> connect SAPSR3/
Enter password:
ERROR: ORA-47400: Command Rule violation for CONNECT on LOGON
```
Other database users are also refused access to SAP application data just as DV administrators are! The latter also cannot grant themselves access!

Only the SAP user sap<sid> can access the SAP data – but as part of the SAP work processes only.

Database Vault monitoring

An extension to the Oracle Enterprise Manager Console, the Database Vault Administrator (DVA), is available for DV monitoring. Users can log on to this console with a DV_OWNER or DV_ADMIN role. In the configuration for SAP this dedicated user is secanalyst.

Alongside Database Vault Administration, there are plenty of other ways of monitoring DV. One such option is for example displaying security infringements.

Various reports can also be run.

The above access error messages are for example logged in the Database Vault Realm Audit Report:

<table>
<thead>
<tr>
<th>Violation Attempt</th>
<th>Timestamp</th>
<th>Return Code</th>
<th>Account/Role</th>
<th>Instance/Number</th>
<th>Realm Name</th>
<th>Role Set</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm Violation</td>
<td>29-Jan-09 02:44:19 PM</td>
<td>1031</td>
<td>SYS</td>
<td>1</td>
<td>SAP Application Protection Realm for ABAP stack</td>
<td></td>
<td>insert into sapv109 dy_test values (1)</td>
</tr>
<tr>
<td>Realm Violation</td>
<td>29-Jan-09 02:48:12 PM</td>
<td>1031</td>
<td>SYS</td>
<td>1</td>
<td>SAP Application Protection Realm for ABAP stack</td>
<td></td>
<td>create table sys.sapv109 as select * from sapv109</td>
</tr>
<tr>
<td>Realm Violation</td>
<td>29-Jan-09 02:42:51 PM</td>
<td>1031</td>
<td>SYS</td>
<td>1</td>
<td>SAP Application Protection Realm for ABAP stack</td>
<td></td>
<td>delete from sapv109 dy_test</td>
</tr>
<tr>
<td>Realm Violation</td>
<td>29-Jan-09 02:42:20 PM</td>
<td>1031</td>
<td>SYS</td>
<td>1</td>
<td>SAP Application Protection Realm for ABAP stack</td>
<td></td>
<td>delete from sapv109 dy_test where c1 &gt; 100</td>
</tr>
<tr>
<td>Realm Violation</td>
<td>29-Jan-09 02:40:19 PM</td>
<td>1031</td>
<td>SYS</td>
<td>1</td>
<td>SAP Application Protection Realm for ABAP stack</td>
<td></td>
<td>insert into sapv109 dy_test values (1)</td>
</tr>
<tr>
<td>Realm Violation</td>
<td>29-Jan-09 02:40:06 PM</td>
<td>1031</td>
<td>SYS</td>
<td>1</td>
<td>SAP Application Protection Realm for ABAP stack</td>
<td></td>
<td>select * from sapv109 dy_test</td>
</tr>
</tbody>
</table>

Screenshot: sample extract from a Realm Audit Report

Amongst other things this allows for a retrospective analysis of access infringements
Performance

Based on past experience, we would assume a performance overhead of less than 5% for Oracle Database Vault.

More information about Database Vault

The Oracle Database Vault documentation (http://www.oracle.com/pls/db102/portal.portal_db?selected=22) contains more details about this subject.

The following SAP notes in particular apply to the Oracle Database Vault in the SAP environment:

1. Note 105047 - Support for Oracle functions in the SAP environment
2. Note 740897 - Info about the Oracle license scope; required Oracle options
3. Note 828268 - Oracle Database 10g: New functions
4. Note 1355140 - Using Oracle Database Vault in an SAP environment
5. Note 1361080 - Database Vault Policy Scripts for SAP
6. Note 1358126 - Oracle 10.2.0: Oracle database vault patches

Also see the "Oracle for SAP Technical Newsletter" http://www.oracle.com/newsletters/sap/volumes/volume17-en.pdf

and the “Best Practices for Installing, Configuring and Deploying Oracle Database Vault Release 10.2.0.4 in an SAP Environment". which is available at https://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/c008b8e2-b758-2c10-d188-98204c3daf3f&overridelayout=true


Oracle Database Vault – current status

As per July 2009, the introduction of Database Vault for Oracle databases in the SAP environment is status controlled availability (CA) for UNIX and LINUX. It is not yet released for systems on WINDOWS.