Oracle Database Vault for
Enterprise Tools 8.46 and higher
And Enterprise Tools 8.22
Table of Contents

Table of Contents ...................................................................................................................................................... 2

Chapter 1 - Introduction ........................................................................................................................................... 3
Structure of this Red Paper 3
Related Materials 3

Chapter 2 - Overview of how Oracle Database Vault protection works ............................................................. 4

Chapter 3 - PeopleTools with Oracle Database Vault release 10.2.0.3 ............................................................ 7

Chapter 4 - PeopleTools with Oracle Database Vault release 9.2.0.8 ............................................................ 8

Appendix A – Validation and Feedback .................................................................................................................. 9
Customer Validation 9
Field Validation 9

Appendix B – Revision History ............................................................................................................................ 11
Revision History ...................................................................................................................................................... 11

Appendix C – Known Limitations .......................................................................................................................... 11
Chapter 1 - Introduction

This Red Paper is a practical guide for technical users, installers, system administrators, Oracle Database Security Administrators, and programmers who implement, maintain, or develop applications for your PeopleSoft system. In this Red Paper, we discuss guidelines on how to implement Oracle Database Vault in a Peoples environment, including installation, configuration, and known limitations.

Much of the information contained in this document originated within PeopleSoft Development in collaboration with some of our big customers and is therefore based on "real-life" customer use cases encountered in the field. Although every conceivable problem that one could encounter in this document, the issues that appear are the problems that prove to be the most common.

Structure of this Red Paper

This Red Paper provides guidance for deploying Oracle Database Vault with PeopleTools 8.46 and higher and PeopleTools 8.22 on Oracle Database release 11g, Oracle Database release 10.2.0.3 and higher, and Oracle Database release 9.2.0.8.

Keep in mind that PeopleSoft updates this document as needed so that it reflects the most current feedback we receive from the field. Therefore, the structure, headings, content, and length of this document is likely to vary with each posted version. To see if the document has been updated since you last downloaded it, compare the date of your version to the date of the version posted on Customer Connection.

Related Materials

We assume that our readers are experienced IT professionals, with a good understanding of PeopleSoft’s Internet Architecture and Oracle Database administration. To take full advantage of the information covered in this document, we recommend that you have a basic understanding of system administration, basic Internet architecture, relational database concepts/SQL, and how to use PeopleSoft applications.

This document is not intended to replace the documentation delivered with the PeopleTools PeopleBooks. We recommend that before you read this document, you read the related information in the PeopleTools PeopleBooks as well as the Oracle Database Vault Installation Guide and the Oracle Database Vault Administrator’s Guide. Note: Much of the information in this document eventually gets incorporated into subsequent versions of the PeopleBooks.
Chapter 2 - Overview of how Oracle Database Vault protection works

Oracle Database Vault restricts highly privileged users’ access and enforces separation of duty for Oracle PeopleSoft environments. Regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Healthcare Insurance Portability and Accountability Act (HIPAA) require strong internal controls to protect sensitive information such as financial, healthcare, and credit cards records. Outsourcing, application consolidation, and increasing concerns over insider threats have resulted in an almost mandatory requirement for strong controls on access to sensitive application data. Oracle Database Vault provides protection for all Oracle PeopleSoft applications. Whether it is Human Resources application, Financial application, or Order Entry and CRM applications, Oracle Database Vault provides realms protections to protect them all.

Oracle Database Vault Protection for PeopleSoft Applications

Oracle Database Vault benefits Oracle PeopleSoft customers by restricting access to application data by highly privileged users, enforcing separation of duty, and enabling multi-factor authorization. Oracle Database Vault enforces security controls even when the application is bypassed. Oracle Database Vault validation with PeopleSoft applications benefits customers by:

- Restricting privileged users’ access to sensitive data.
- Enforcing separation of duty in the PeopleSoft Oracle Database environment.
- Providing PeopleSoft-specific Database Vault protection realms and command rules.
- Allowing seeded protections to be extendable.

Controlling Highly Privileged Users Access

PeopleSoft Application administrators and database administrators fill highly trusted positions within the enterprise. With Oracle Database Vault Realms and Command Rules, enterprises can restrict highly privileged users, even the powerful DBA, from accessing application data. Database Vault defines a PeopleSoft Realm and multiple Command Rules for Oracle PeopleSoft applications. Figure 2 describes this realm and command rules and who is authorized to access them.

Separation of Duty in the Database

Oracle Database Vault prevents ad-hoc creation of database accounts unless the administrator is explicitly assigned the Database Vault Account Management administrator role. This improves compliance in the Database for Oracle PeopleSoft environments. The Database Vault Security Administrator manages access to the PeopleSoft Realm and can create additional security rules to satisfy specific compliance requirements.
Vault prevents Database Administrators from granting powerful roles like the DBA role to other users, unless they are specifically authorized to do so in the Data Dictionary Realm.

<table>
<thead>
<tr>
<th>Authorized with Rule Set Type</th>
<th>SYSAADM</th>
<th>PSFTDBA</th>
<th>SYSTEM</th>
<th>DBA</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeopleSoft Realm</td>
<td>OWNER</td>
<td>OWNER</td>
<td>No. Access</td>
<td>No. Access</td>
</tr>
<tr>
<td>Select Command Rule</td>
<td>Not Restricted</td>
<td>Limit PSFTDBA Rule Set</td>
<td>No Access</td>
<td>No Access</td>
</tr>
<tr>
<td>Connect Command Rule</td>
<td>PeopleSoft Access Rule Set</td>
<td>Not Restricted</td>
<td>Not Restricted</td>
<td>Not Restricted</td>
</tr>
<tr>
<td>Drop Tablespace Command Rule</td>
<td>Disabled Rule Set</td>
<td>Disabled Rule Set</td>
<td>Disabled Rule Set</td>
<td>Disabled Rule Set</td>
</tr>
</tbody>
</table>

Figure 2: PeopleSoft Database Vault Realms and

Extending The Oracle-Supplied Security Settings

Customers are allowed to extend the Oracle-supplied security settings to accommodate their specific security requirements. Customers may add their own realms, authorize their own DBA accounts, and setup their own additional command rules for multi-factor authorizations. For example, customers can modify the CONNECT command rule to restrict connections to the database to a specific range of IP addresses.

Supported PeopleTools Releases

All PeopleSoft application modules and all PeopleSoft application releases running on PeopleTools release 8.46 and higher or PeopleTools release 8.22 are supported with Oracle Database Vault. Oracle Database release 9.2.0.8, Oracle Database release 10.2.0.3 and higher, and Oracle Database 11g are supported with this validation. Oracle Database Vault protection scripts can be downloaded from the Oracle Technology Network at the following link: [http://www.oracle.com/technology/software/products/database_vault/index.html](http://www.oracle.com/technology/software/products/database_vault/index.html)

PeopleSoft Applications Protection Use Cases

Our main goal is to validate that customers can ensure a DBA and other privileged users (system administrators) cannot view application data but can still perform necessary DBA and system administration functions such as application rollout and system maintenance. Several of the anticipated customer uses for DBV include:

- Limiting the system DBA’s access to PeopleSoft application data.
- Providing the application DBA proper access to the usual database objects such as tables, views, and indexes, for maintenance and deployment, without giving the ability to see any application business data.
- Allowing the application DBA to maintain the password for the accessid, which has full capability to run the PeopleSoft system, but preventing the DBA from using the accessid to view any application data.

- Ensuring the above policies are followed in a production environment as well as during any application maintenance or patching.

**Regulatory Compliance Snapshot**

Oracle Database Vault can be used to help fulfill various compliance related requirements, such as the following:

<table>
<thead>
<tr>
<th>Regulatory Legislation</th>
<th>Regulation Requirement</th>
<th>Does DBV Mitigate This Risk?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley Section 302</td>
<td>Unauthorized changes to data</td>
<td>Yes</td>
</tr>
<tr>
<td>Sarbanes-Oxley Section 404</td>
<td>Modification to data, Unauthorized access</td>
<td>Yes</td>
</tr>
<tr>
<td>Sarbanes-Oxley Section 409</td>
<td>Denial of service, Unauthorized access</td>
<td>Yes</td>
</tr>
<tr>
<td>Gramm-Leach-Bliley</td>
<td>Unauthorized access, modification and/or disclosure</td>
<td>Yes</td>
</tr>
<tr>
<td>HIPAA 164.306</td>
<td>Unauthorized access to data</td>
<td>Yes</td>
</tr>
<tr>
<td>HIPAA 164.312</td>
<td>Unauthorized access to data</td>
<td>Yes</td>
</tr>
<tr>
<td>Basel II – Internal Risk Management</td>
<td>Unauthorized access to data</td>
<td>Yes</td>
</tr>
<tr>
<td>CFR Part 11</td>
<td>Unauthorized access to data</td>
<td>Yes</td>
</tr>
<tr>
<td>Japan Privacy Law</td>
<td>Unauthorized access to data</td>
<td>Yes</td>
</tr>
<tr>
<td>PCI – Requirement 7</td>
<td>Restrict access to cardholder data by business need-to-know</td>
<td>Yes</td>
</tr>
<tr>
<td>PCI – Requirement 8.5.6</td>
<td>Enable accounts used by vendors for remote maintenance only during the time period needed</td>
<td>Yes</td>
</tr>
<tr>
<td>PCI – Compensating Controls for Requirement 3.4</td>
<td>Provide ability to restrict access to cardholder data or databases based on the following criteria: • IP address/Mac address • Application/service • User accounts/groups</td>
<td>Yes</td>
</tr>
<tr>
<td>PCI - Requirement A.1: Hosting providers protect cardholder data environment</td>
<td>Ensure that each entity only has access to own cardholder data environment</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Chapter 3 - PeopleTools with Oracle Database Vault release 10.2.0.3

Pre-Installation Steps

1. Make sure PeopleSoft is installed on Oracle Database release 10.2.0.3.

2. PeopleTools does require interim patches 5128368, 5574966, and 5683652 for using Oracle 10.2.0.3. These required patches are documented on Customer Connection. Make sure you install these patches.

3. Make sure PeopleTools version is 8.22 or 8.46 and above. This translates to the following PeopleSoft application versions:
   a. PeopleSoft applications less than 8.4 (8.0, 8.1, 8.3) must be on PeopleTools 8.22.
   b. PeopleSoft applications 8.4 or greater (8.4, 8.8, 8.9, 9.0) must be on PeopleTools 8.46 or greater.

4. Make sure the database has the Tablespace “TEMP” as a temporary Tablespace.

5. Note, at this stage Oracle Database Vault is not installed yet.

Installation Steps

1. Download the Database Vault 10.2.0.3 security policies for PeopleSoft from the Oracle Technology Network at the following link:

2. Unzip the file psft_dbvault_sec_policies.zip into a temporary directory.

3. In your PeopleSoft installation, if PeopleSoft Access Id is not SYSADM then edit the script psft_dbagrants.sql and replace SYSADM with your PeopleSoft Access Id.

4. Login to the database as SYSDBA and run the script psftdba_grants.sql.

5. Install Oracle Database Vault release 10.2.0.3 as documented in the Database Vault Installation Guide.

6. Repeat step 3 for all scripts in the directories create_policies, delete_policies, enable_policies, and disable_policies.

7. Using Sqlplus, login to the database with the Database Vault Administrator (owner) account and run the script create_dbv_policies.sql. This script is located under the create_policies directory. While testing the security policies if you need to remove them you can run the delete_dbv_policies.sql script. It is under the delete_policies directory. To disable the security policies go to the directory disable_policies and run disable_dbv_policies.sql. To enable the security policies go to the directory enable_policies and run enable_dbv_policies.sql script.

Description of the PeopleSoft-Specific Protections

The script create_dbv_policies.sql creates the following PeopleSoft-specific protections:

**PeopleSoft Realm:** This realm protects against unauthorized access by privileged users to business data. It protects all objects owned the PeopleSoft Access Id in addition to some PeopleSoft database roles. Access to this Realm is granted to PeopleSoft Access Id as well as the user PSFTDBA.
The user PSFTDBA is a new user designed to do administration activities on the PeopleSoft applications (such as patching) but it is not allowed to access business data inside the PeopleSoft applications. This is enforced using a security policy defined in the Limit PSFTDBA Rule Set and attached to the Select Command Rule described below.

The PeopleSoft Access Id authorization is restricted to specific processes. This is enforced through the PeopleSoft Access Rule Set.

**Performance Statistics Realm:** This realm provides the PeopleSoft Access id the ability to gather table statistics to improve performance. Authorization is also given to the PSFTDBA.

**Select Command Rule:** This command restricts Select access to business data owned by the PeopleSoft Access Id. Only PeopleSoft Access Id is allowed Select access. It prevents PSFTDBA and other users from accessing business data.

**Connect Command Rule:** This command allows connection to the database by various users according to specific security policies. The PeopleSoft Access Id is allowed to connect to the database using pre-defined list of processes. These processes include middle tier processes, PeopleTools processes, and the Cobol processes. As a customer you can add rules that specify which IP address or hostname these processes should connect from. All other users are allowed to connect using any process.

### Chapter 4 - PeopleTools with Oracle Database Vault release 9.2.0.8

**Pre-Installation Steps**

1. PeopleTools does require interim patches 5128368, 5574966, and 5683652 for using Oracle 10.2.0.3. These required patches are documented on Customer Connection. Make sure you install these patches.

2. Make sure PeopleSoft is installed on Oracle Database release 9.2.0.8.

3. Make sure PeopleTools version is 8.22 or 8.46 and above. This translates to the following PeopleSoft application versions:
   - PeopleSoft applications less than 8.4 (8.0, 8.1, 8.3) must be on PeopleTools 8.22.
   - PeopleSoft applications 8.4 or greater (8.4, 8.8, 8.9, 9.0) must be on PeopleTools 8.46 or greater.

4. Make sure the database has the Tablespace “TEMP” as a temporary Tablespace.

5. Make sure your database has an `spfile`. Refer to the Oracle Database Administrator Guide for more information on how to create an `spfile`.

6. Note, at this stage Oracle Database Vault is not installed yet.

**Installation Steps**


2. Unzip the file `psft_dbvault_sec_policies.zip` into a temporary directory.

3. In your PeopleSoft installation, if PeopleSoft Access Id is not SYSADM then edit the script `psft_dbagrants.sql` and replace SYSADM with your PeopleSoft Access Id.

4. Login to the database as SYSDBA and run the script `psftdba_grants.sql`. 
5. Install Oracle Database Vault release 10.2.0.3 as documented in the Database Vault Installation Guide.

6. Repeat step 3 for all scripts in the directories create_policies, delete_policies, enable_policies, and disable_policies.

7. Using Sqlplus, login to the database with the Database Vault Administrator (owner) account and run the script create_dbv_policies.sql. This script is located under the create_policies directory. While testing the security policies if you need to remove them you can run the delete_dbv_policies.sql script. It is under the delete_policies directory. To disable the security policies go to the directory disable_policies and run disable_dbv_policies.sql. To enable the security policies go to the directory enable_policies and run enable_dbv_policies.sql script.

**Description of the PeopleSoft-Specific Protections**

The script create_dbv_policies.sql creates the following PeopleSoft-specific protections:

**PeopleSoft Realm:** This realm protects against unauthorized access by privileged users to business data. It protects all objects owned the PeopleSoft Access Id in addition to some PeopleSoft database roles. Access to this Realm is granted to PeopleSoft Access Id as well as the user PSFTDBA.

The user PSFTDBA is a new user designed to do administration activities on the PeopleSoft applications (such as patching) but it is not allowed to access business data inside the PeopleSoft applications. This is enforced using a security policy defined in the Limit PSFTDBA Rule Set and attached to the Select Command Rule described below.

The PeopleSoft Access Id authorization is restricted to specific processes. This is enforced through the PeopleSoft Access Rule Set.

**Select Command Rule:** This command restricts Select access to business data owned by the PeopleSoft Access Id. Only PeopleSoft Access Id is allowed Select access. It prevents PSFTDBA and other users from accessing business data.

**Connect Command Rule:** This command allows connection to the database by various users according to specific security policies. The PeopleSoft Access Id is allowed to connect to the database using pre-defined list of processes. These processes include middle tier processes, PeopleTools processes, and the Cobol processes. As a customer you can add rules that specify which IP address or hostname these processes should connect from. All other users are allowed to connect using any process.

**Appendix A – Validation and Feedback**

This section documents that real-world validation that this Red Paper has received.

**CUSTOMER VALIDATION**

PeopleSoft is working with PeopleSoft customers to get feedback and validation on this document. Lessons learned from these customer experiences will be posted here.

**FIELD VALIDATION**
PeopleSoft Consulting has provided feedback and validation on this document. Additional lessons learned from field experience will be posted here.
Appendix B – Revision History

Revision History


Appendix C – Known Limitations

When you try to create a database trigger, you might get an ORA-00604 error. This is due to bug number 5630439. The workaround is as follows:

1. Login to Sqlplus as the Database Vault Administrator and do:
   SQL>alter trigger dvsys.dv_before_ddl_trg disable;

2. Login as the user who needs to create the trigger and create it.

3. Login to Sqlplus as Database Vault Administrator and do:
   SQL>alter trigger dvsys.dv_before_ddl_trg enable;