

Frequently Asked Questions

Oracle Database 12c – Database Vault

Introduction

Regulatory compliance, industrial espionage and insider threats are just few of the challenges facing organizations in today's global economy. At the same time, remaining competitive requires the flexibility to deploy IT systems in a cost effective manner through consolidation and off shoring. While problems such as insider threats are certainly not new, the concern over unauthorized access to sensitive information has never been greater. The cost of data theft from both a financial and public relations standpoint can be significant. At the same time compliance with regulations such as Sarbanes-Oxley (SOX), European Union Data Protection Directive, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and numerous breach disclosure laws requires strong controls on access to sensitive data. Oracle Database Vault provides a powerful and transparent security solution that helps organizations comply with regulations, deploy systems in a cost efficient manner, and prevent unauthorized access to sensitive data.

Table of Contents

Introduction..... 1
 Table of Contents 1
 Technical..... 1
 Manageability 2
 Business Use Cases 3
 Security and Compliance..... 3

Partners 4
 Application Certification and Protection..... 4
 Integration..... 5
 Training..... 7
 Packaging and Licensing 7

Technical

- Q:** What security controls does Oracle Database Vault provide?
- A:** Realms - A Realm is a "protection zone" inside the database that prevents privileged users such as DBAs from accessing any protected data inside it. The Oracle Database Vault administrator can create a Realm and add the sensitive database objects to be secured in it and authorize the users or roles that need access to it. A Realm can protect a single table, multiple tables, an entire application schema, or multiple applications schemas. There is also a second type of Realms called Mandatory Realms where protection is extended to block unauthorized access even by object owners. This is to provide an additional check before allowing object owner's access and to be able to lock down all access to sensitive data in the case of a cyber attack.

Command Controls - A Command Control or a Command Rule is a security policy that you create to control the conditions by which users can execute almost any SQL statements, including SELECT, ALTER SYSTEM, database definition language (DDL) statements, and data manipulation language (DML) statements. Command rules evaluate a security policy (Rule Set) to determine whether or not the statement is allowed.

Multi-Factor Authorization – Multi-factor authorization Rule Sets leverage multiple factors in their decision process and can be associated with Realm authorizations and Command Controls. Security administrators can define rules that are based on specific compliance requirements or security requirements. For example, limiting connections to a specific IP or to a range of IP addresses. Rule Sets use Factors such as time of the day, IP



address, host name, program name, or any number of identifiable attributes associated with the user. For example, a user can only access certain data if the Rule Set states that access to the application is restricted to working hours, from an internal IP address. These restrictions can be applied to all database users, including the DBAs.

Privilege Analysis – Privilege Analysis allows customers to see what privileges and roles applications and users actually use inside the database. It also provides a list of all unused privileges and roles that the application or user has. This helps customers make their applications more secure and reduce their attack surface by revoking all unused privileges and roles from users and applications.

- Q:** How does Privilege Analysis help make applications and users more secure?
- A:** Oracle Database Vault Privilege Analysis helps customers make their applications and users more secure by helping reduce attack surface and achieve least privilege model. Customers can use Privilege Analysis to create a policy that captures what privileges and roles applications or users actually use inside the database. The policy can be enabled for as long as needed to capture all the used privileges. Once this is done, customer can generate the captured results and get a report of all the unused roles, system and object privileges. Customers can then create a custom role for all used privileges, for example, and grant it to the user or application. Privilege Analysis can be used without enabling Oracle Database Vault controls.
- Q:** What is the performance overhead on the database with Oracle Database Vault Privilege Analysis?
- A:** Oracle's internal TPC-C benchmark testing showed that Oracle Database Vault Privilege Analysis has a minimal overhead of less than 2%. Privilege Analysis can be run as long as needed to capture all used privileges.
- Q:** What is the performance overhead on the database with Oracle Database Vault Realms and Command Controls?
- A:** Oracle's internal TPC-C benchmark testing showed that Oracle Database Vault Realms and Command Controls have a minimal overhead of less than 2%. Some of our large EBS and PeopleSoft customers have seen up to 3% CPU overhead with no impact on response time. Normal database tuning still applies when Oracle Database Vault is enabled.
- Q:** Has Oracle Database Vault been evaluated against any security standard?
- A:** Oracle Database Vault 11g Release 1 was evaluated against the international [Common Criteria Evaluation Assurance Level 4 Augmented \(EAL 4+\) certification](#). The Common Criteria for IT Security Evaluations is an internationally recognized standard (ISO 15408) to measure the security of IT products.

Manageability

- Q:** Can Oracle Database Vault be managed through Oracle Enterprise Manager?
- A:** Yes. Oracle Enterprise Manager Cloud Control 12c provides a complete management interface for all Oracle Database Vault features including Realms, Command Controls, Privilege Analysis, etc.
- Q:** Who can grant roles such as the DBA role in a database protected by Oracle Database Vault?
- A:** In an Oracle Database where Oracle Database Vault is enabled, if a realm protects a database role, then only a user who is authorized to the Realm as Owner can grant this role to others provided that user has been granted the role with admin option. Default database roles such as the DBA role are protected by the default Oracle System Privilege and Role Management Realm. Customers are recommended to create a named user account with the necessary privileges to grant the DBA role and authorize this named user as a Realm Owner to the Oracle System Privilege and Role Management Realm so he/she can grant the DBA role to other users.
- Q:** Who can create new users in an Oracle Database Vault environment?
- A:** In an Oracle Database Vault environment, the DV_ACCTMGR role is required to create new users. The DV_ACCTMGR role can be granted to a user to give that user the account management responsibility. This helps customers achieve strong operational controls inside the database by controlling who can create new users in their Oracle Database environment. It also helps customers avoid audit finding by preventing ad-hoc account creation.
- Q:** Can the Oracle Database Vault Administrator (owner) see data protected by a Realm?
- A:** No. The Database Vault Administrator can only setup security policies, such as Realms and Command Controls, but cannot see data protected by a Realm or a Command Control.

Q: How do you move Oracle Database Vault security Policies from a development system to a production system?

A: There are two ways to do this:

Oracle Enterprise Manager allows you to move Oracle Database Vault security policies from one Oracle database to multiple other Oracle Databases.

Oracle Enterprise Manager also allows you to generate Oracle Database Vault API script from existing security policies. You can then edit and run this API script on any number of target Oracle Databases to create the security policies there.

Q: How do you apply patches in a Database that is protected by Oracle Database Vault?

A: Oracle Database Vault allows for a patching mode where the database can be patched without disabling Oracle Database Vault protections. In this case, the Security Administrator grants the DV_PATCH_ADMIN role to a DBA so the DBA can patch the database. Once patching is done, the Security Administrator revokes the DV_PATCH_ADMIN role from the DBA. The DV_PATCH_ADMIN role allows a DBA to patch the database without having access to protected sensitive applications data.

Business Use Cases

Q: What are some of the example business use cases for Oracle Database Vault?

A: Some example business use cases for Oracle Database Vault include:

- Protecting against Advanced Persistent Threat and outside hackers who manage to compromise a privileged user account and use that account to steal sensitive data from the database. Oracle Database Vault controls privileged user's access to sensitive data such that when a DBA account gets compromised, the hacker would not be able to steal sensitive data.
- Compliance with regulations: Oracle Database Vault helps customers put in place controls to address compliance requirements resulting from privacy and corporate governance regulations. This includes regulations such as Sarbanes-Oxley, PCI, HIPAA, Gramm-Leach Bliley, the Japanese Privacy Act, BASEL II, and much more.
- Allowing customers to securely outsource / off-shore back end operations to cut costs and improve efficiency. This brings in the special security requirements where outsourced back end operators can do their work without

having access to sensitive data. Oracle Database Vault enables customers to achieve that.

- Allowing customers to securely consolidate data in a Cloud Computing environment. Customers want to take advantage of this modern cloud computing architecture without compromising their data security. Oracle Database Vault allows customers to achieve that.
- Protecting against the "insider threat": Oracle Database Vault enables customers to protect their sensitive data from insider attacks using features such as Realms and Command Rules.

Security and Compliance

Q: Can I use Oracle Database Vault to meet compliance requirements found in Sarbanes-Oxley, PCI, HIPAA, ITAR, and EU privacy laws?

A: Oracle Database Vault is designed to help address technical security requirements found in various regulations such as Sarbanes-Oxley, PCI, HIPAA, ITAR, and EU privacy laws. Customers are also required to follow processes and procedures required by these regulations. Oracle Database Vault provides strong internal controls inside the database controlling who, when, where, and how applications data can accessed. In addition, Oracle Database Vault controls what changes can be made to the database helping keep the database available and secure.

Q: What are internal controls?

A: Internal controls are mechanisms put in place to enforce business best practices. They are generally closely associated with addressing regulatory compliance requirements. Internal controls can be preventive, detective or corrective in nature. Preventive controls are designed to discourage or pre-empt errors or irregularities from occurring. They are generally thought to be more cost-effective than detective controls. Oracle Database Vault serves as a database enforced preventive control—something highly desirable by the internal audit function of companies.

Q: How does Oracle Database Vault help address customer compliance requirements?

A: Oracle Database Vault can be used by organizations as a preventive control. In other words, organizations can configure Oracle Database Vault to prevent privileged users (DBAs) from accessing application data. By instituting a control in this manner, an organization can demonstrate compliance with specific regulations that require strong internal control on individuals who can

access or update financial information, for example. Such is a common requirement across a number of regulations and is specifically called out in Section 404 of Sarbanes-Oxley. Payment Card Industry regulations such as PCI – DSS Requirement 7 calls for restricting access to cardholder data to business need-to-know. This can be enforced with Oracle Database Vault. Additionally, Oracle Database Vault Privilege Analysis helps customers achieve least privilege model for applications and users which make them more compliant with regulations and more secure. Oracle Database Vault also comes with a set of pre-defined reports that show what security policies are in place and who is authorized to access protected data. These reports help demonstrate proof of compliance for organizations.

Partners

- Q:** Does Oracle work with partners to deploy and embed Oracle Database Vault?
- A:** Yes, Oracle works closely with partners including global System Integrators (SIs) and Independent Software Vendors (ISVs) such as Accenture, BearingPoint, SAP, Infosys, Deloitte LLP, and Price Waterhouse Coopers. These partners help to deploy Oracle Database Vault for customers and embed Oracle Database Vault within their solutions.

Application Certification and Protection

- Q:** Is Oracle Database Vault certified with major Oracle and partner enterprise applications?
- A:** Yes. Oracle Database Vault is certified with Oracle Applications including: Oracle Fusion Applications, Oracle E-Business Suite, Oracle PeopleSoft, Oracle Siebel, Oracle JD Edwards EnterpriseOne, Oracle Retail Applications (Retek), Oracle Financial Services (iFlex), Oracle Utilities Applications, and Oracle Enterprise Taxation Management. Major Partner applications have also been certified with Oracle Database Vault including: SAP, Banner, and Finacle from Infosys. You can find more information on this at the Oracle Database Vault OTN page:
<http://www.oracle.com/technetwork/database/options/database-vault/index-090593.html>
- Q:** Does Oracle Database Vault replace the security mechanisms in applications?
- A:** No, Oracle Database Vault protections complement applications security mechanisms. Oracle Database Vault secures the database and the applications by adding

security protections within the database kernel, preventing backend direct access to the applications data by privileged users (DBAs) that bypasses front end applications controls. This complements applications security controls and allows user access only through the application interface.

- Q:** What does it take to certify my custom application with Oracle Database Vault?
- A:** To protect and certify your custom applications with Oracle Database Vault, follow the recommendations mentioned in the Oracle Database Vault Best Practices white paper. Following are the main steps:
1. Create a Realm around your application schemas.
 2. Authorize the application owner to the realm.
 3. Optionally, create a connect command rule to verify application owner access to the database is coming from the middle tier.
 4. Run an application functional test to make sure the application works as expected.
 5. Use Enterprise Manager to save the protection policy to an API script so you can apply them to your production system.
- Q:** How to install an Application with Database Vault enabled?
- A:** When applications are installed, they normally use a default database account such as SYS or SYSTEM to perform the installation. The installation typically involves creating schemas, tables, indexes, etc and granting privileges. Before starting the installation, make sure the user performing the installation, such as SYS or SYSTEM, is authorized to all default Realms as owner. Then have the Database Vault administrator grant the DV_PATCH_ADMIN role to the user doing the installation. Once the Application installation is complete, the Database Vault administrator must revoke the DV_PATCH_ADMIN from this user.
- Q:** What versions of Oracle PeopleSoft applications are certified with Oracle Database Vault?
- A:** All modules and versions of Oracle PeopleSoft applications are supported to run with Oracle Database Vault provided they have a supported version of PeopleTools. For a list of supported PeopleTools versions, please visit the Oracle Support web site.

Q: How does Oracle Database Vault help Oracle PeopleSoft customers with their compliance requirements?

A: Oracle Database Vault provides strong operational controls in the database, prevents privileged database users access to application's sensitive data, and provides multi-factor authorization to control who, when, where, and how application sensitive data can be accessed. These features help customers address common compliance requirements found in regulations, such as SOX, PCI and HIPAA, at the database layer. A special Oracle Database Vault protection policy has been developed for Oracle PeopleSoft applications. This policy protects all Oracle PeopleSoft applications including Financials, CRM, ERP, HR, and Campus solutions. This protection policy can be downloaded from OTN at: <http://www.oracle.com/technetwork/database/options/data-base-vault/index-090593.html>

Q: What versions of E-Business Suite are certified with Oracle Database Vault?

A: E-Business Suite version 11.5.10 CU2 and releases 12 and 12.1 and higher are all certified with Oracle Database Vault. For customer specific operating system support, please check the Oracle Customer Support site <http://support.oracle.com> and look for the relevant support note as follows:

- Note 1091086.1 - EBS 11.5.10.CU2 with 11g Release 2 Oracle Database Vault
- Note 1091083.1 - EBS 12.x with 11g Release 2 Oracle Database Vault
- Note 859399.1 - EBS 11.5.10.CU2 with 11g Release 1 Oracle Database Vault
- Note 859397.1 - EBS 12.x with 11g Release 1 Oracle Database Vault
- Note 428503.1 - EBS 11.5.10.CU2 with 10g Oracle Database Vault
- Note 1139798.1 - EBS 12.x with 10g Oracle Database Vault

Customers should also check the latest updates on Steven Chan's blog at: <http://blogs.oracle.com/stevenchan>

Q: What E-Business Suite modules are certified with Oracle Database Vault?

A: All E-Business Suite modules are certified to run with Oracle Database Vault including Financials, Manufacturing, HR and CRM. Oracle Clinical is not

certified yet. Once we certify Oracle Clinical we will announce it.

Q: What version of SAP is certified with Oracle Database Vault?

A: Oracle Database Vault is certified with SAP Kernel 7.0 or higher. This translates to SAP ERP 2005 and higher or SAP 6.1 and higher.

Oracle Database Vault releases 11.2 and higher or 10.2.0.5 are certified to run with SAP. For more information, refer to SAP Note 1355140.

Q: How can SAP customers purchase Oracle Database Vault?

A: SAP customers who have ASFU license for the Oracle Database can purchase license for Oracle Database Vault from their SAP sales representative.

SAP customers who have Full Use License for the Oracle Database can purchase license for Oracle Database Vault from their Oracle sales representative.

Q: What does it mean to certify Oracle Applications and SAP with Oracle Database Vault?

A: Certification means that Oracle Database Vault has been tested with the applications and out-of-the-box application-specific Oracle Database Vault protection policies are available. It also means that customers will be fully supported in using Oracle Database Vault with their applications by both the applications and the database support groups.

Integration

Q: Is it possible to use Oracle Database Vault with Oracle Database Appliance?

A: Yes, Oracle Database Vault can be installed and enabled on Oracle Database Appliance. Additional license fee will be required for Oracle Database Vault.

Q: Is it possible to use Oracle Database Vault with Oracle Exadata Database Machine?

A: Yes, Oracle Database Vault can be installed and enabled on Oracle Exadata Database Machine. We have many customers who are already using Oracle Database Vault to secure their sensitive data on Oracle Exadata Database Machine. Additional license fee will be required for Oracle Database Vault.

Q: Do other Oracle Database Security options and products work with Oracle Database Vault?

A: Yes. Oracle Advanced Security, Oracle Audit Vault and Database Firewall, and Oracle Label Security work with Oracle Database Vault.

In addition, built-in database security features such as Virtual Private Database and Secure Application Roles work with Oracle Database Vault.

Q: Does Oracle Database Vault integrate with Oracle Label Security (OLS)? Can OLS leverage Oracle Database Vault Factors?

A: Yes, Oracle Database Vault integrates with Oracle Label Security (OLS). Oracle Database Vault factors can be leveraged by OLS to provide an additional dimension in deciding the security clearance of a user's session. For example, let us assume a user has been authorized to access sensitive data. However the security administrator wants to ensure the user accesses sensitive data only when he / she is in the office and connected to the trusted network. An Oracle Database Vault factor like Network Domain can be used to determine the security clearance of a user's database session. If the user is coming from the public Internet, he / she can see only non-sensitive data. If the user is coming from the trusted network, then the user is allowed access to sensitive data. Oracle Database Vault can also evaluate user security clearances assigned by Oracle Label Security before allowing access to Realms and Command Controls.

Q: Does Oracle Database Vault work with Oracle Advanced Security Data Redaction?

A: Yes, Oracle Database Vault works well with Oracle Advanced Security Data Redaction. Data Redaction reduces the exposure of sensitive data by fully or partially redacting sensitive data when certain conditions are satisfied. Oracle Database Vault Realms, Multi-Factor Authorization, and Command Rules provide security controls to prevent unauthorized users from accessing protected data. Oracle Database Vault and Oracle Advanced Security Data Redaction complement each other.

Q: Does Oracle Database Vault work with Oracle Advanced Security Transparent Data Encryption?

A: Yes, Oracle Database Vault works well with Oracle Advanced Security Transparent Data Encryption. Transparent Data Encryption protects sensitive data at

rest by encrypting it. This protects against direct operating system attacks that try to access the database files directly to steal data. Oracle Database Vault Realms, Multi-Factor Authorization, and Command Rules provide security controls inside the database. Oracle Database Vault and Oracle Advanced Security Transparent Data Encryption protections complement each other.

Q: Does Oracle Database Vault work with Oracle Data Guard?

A: Yes, Oracle Database Vault works with Oracle Active Data Guard and Oracle Data Guard Physical Standby. Refer to the white paper "DBA Administrative Best Practices with Oracle Database Vault" for more information.

Q: Does Oracle Database Vault work with Oracle Database Utilities such as Data Pump?

A: Yes, Oracle Database Vault works with Oracle Data Pump and other Oracle Database Utilities. Refer to the white paper "DBA Administrative Best Practices with Oracle Database Vault" for more information.

Q: How is Oracle Database Vault different from Oracle Audit Vault and Database Firewall? Do I need both to protect my Oracle Database?

A: As part of Oracle's defense in-depth solution, Oracle Audit Vault and Database Firewall provides the first line of defense by protecting from SQL injection attacks before they reach the database. In addition, Oracle Audit Vault and Database Firewall consolidates and secures audit data from multiple heterogeneous sources such as Oracle Database, IBM DB2, and Microsoft SQL Server. It also provides a rich set of compliance reports and allows customers to create custom reports if needed. Oracle Database Vault, on the other hand, provides strong operational controls inside the Oracle Database. Oracle Database Vault protections restrict privileged user access to sensitive data inside the Oracle Database. Customers need both Oracle Audit Vault and Database Firewall and Oracle Database Vault to implement defense in-depth protection for their applications and Databases.

Q: How is Oracle Database Vault different from Oracle Virtual Private Database?

A: Oracle Virtual Private Database provides a row-level security API within the Oracle Database. Oracle Database Vault, on the other hand, provides a security solution for the database and applications, by controlling privileged users (DBAs) access to sensitive data and enforcing strong operational controls inside the database.

Training

- Q:** Is there training available for Oracle Database Vault?
- A:** Yes. Oracle University offers training classes for Oracle Database Vault in different formats: Classroom Training, Live Virtual Class, and Self-Paced. For the latest schedule and to register, check the Oracle University

website at: <http://education.oracle.com> and search for Oracle Database Vault.

Packaging and Licensing



- Q:** How is Oracle Database Vault packaged?
- A:** Oracle Database Vault is a security option for the Oracle Database Enterprise Edition.



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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/blogs
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Hardware and Software, Engineered to Work Together

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0115