19c ORACLE Database

Oracle Database Vault

Oracle Database Vault prevents unauthorized privileged user access to sensitive data and unauthorized changes to the database through strong controls and enforced separation of duties. Database Vault uses trusted paths as additional controls to protect the database from unauthorized access. 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.

PRODUCT OVERVIEW

What is Oracle Database Vault?

Oracle Database Vault provides strong security controls to prevent unauthorized access to sensitive information by privileged users and protect against unintended changes to the database. This reduces the risk of malicious users using privileged accounts to attack the database.

Why do I need Oracle Database Vault if I already encrypt my database?

Most cyber attacks use various means to steal privileged user account information. Privileged user accounts give the keys to the kingdom and allow cyber attackers to jump to parallel systems or exfiltrate data from a system.

Encryption prevents database bypass attacks where sensitive data can be stolen from database files in OS level, storage devices, backup devices and export files.

With proper encryption, cyber attackers are forced to attack through the database privileged user accounts to steal sensitive data from a database. Enforcing strong controls with Oracle Database Vault minimizes the risk of a breach from the malicious use of privileged accounts.

ORACLE

Oracle Database Vault provides trusted paths to further restrict access to sensitive data using system factors such as IP address, program name, time of day and user name.

In addition to strong protection and access controls, Oracle Database Vault enforces and supports the Separation of Duty principle.

How does Oracle Database Vault improve security and improve compliance?

Oracle Database Vault improves security by minimizing risks from privileged user attacks, the most common form of cyber attack. Most compliance requirements include controls for separation of duty and preventing administrative access to sensitive data. Since Oracle Database Vault implements security in the engine of the database, these security controls are in place no matter what network or server the cyberattack originates from.

Has Oracle Database Vault been evaluated against any security standard?

Oracle Database Vault has been certified with Common Criteria. Please review the Oracle Technology Network website for the latest information regarding Oracle Database and Database Vault certifications. The Common Criteria for IT Security Evaluations is an internationally recognized standard (ISO 15408) to measure the security of IT products.

What security does Oracle Database Vault provide in the Cloud?

Oracle Database Vault protects sensitive data in a Cloud from attacks by cloud or customer administrators that have privileged user access to the database. The database is also protected from unauthorized changes by either cloud or customer administrators.

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

Oracle Database Vault is designed to help address technical security requirements found in various regulations such as Sarbanes-Oxley, PCI, HIPAA, ITAR, and EU GDPR. 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 be accessed. In addition, Oracle Database Vault controls what changes can be made to the database helping keep the database available and secure.

COMPONENTS AND FEATURES

What security controls does Oracle Database Vault provide?

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 security 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. Only the Oracle Database Vault security administrator is able to authorize access to the sensitive data.

Command Controls - A Command Control or a Command Rule controls the conditions by which users can execute 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, and under which conditions.

Trusted Path – Trusted Path Rule Sets leverage multiple factors in their decision process and can be associated with Realm access and Command Controls. Security administrators can define rules that are based on specific compliance requirements or security requirements. 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 or a range of internal IP addresses. These restrictions can be applied to all database users, including the DBAs.

Operations Control – Operations Control strengthens security for the popular database consolidation technology – Oracle Multitenant. Apart from using PDB lockdown profiles that prevent PDB users from impacting other PDBs and the database, Oracle Database Vault Operations Control transparently prevent Multitenant container administrators from accessing application sensitive data in pluggable databases.

ADMINISTRATION

What new roles are created for Database Vault?

Two primary roles are created and granted to users when Oracle Database Vault is created. They are DV_OWNER and DV_ACCTMGR roles. The DV_OWNER role allows the user to create security objects (realms, command rules..), add authorized users, enable/disable controls and other management tasks related to the Database Vault security objects. DV_ACCTMGR role is used to create and manage users and profiles. There are several other roles that are created that are subsets of these two roles. It is important to note that backup accounts are recommended for these two roles since the SYSDBA privilege will not be able to recover lost passwords for accounts with these roles. In other words, at least TWO database accounts should have the DV_OWNER role – one ore more used for day to day configuration and management of Database Vault, another as an emergency account stored in your organization's Privileged Account Management solution.

Do the new Oracle Database Vault roles change how my database administrators work today?

Most DBA tasks will not change. One area of change is in creating and managing users and profiles. This security related task can only be done by a user with the DV_ACCTMGR role. Additionally, tasks that can expose sensitive data like Datapump and Job Scheduling need a separate authorization from an account with the DV_OWNER role.

How do the Oracle Database Vault separation of duty controls work for smaller organizations?

Oracle recommends separate administrators for the additional roles that Oracle Database Vault provides (Oracle Database Vault owner –the security administrator responsible for the security controls and the Oracle Database Account Manager – the security administrator that is responsible for creating and managing new users and profiles.) These are separate and distinct from the database administrators. However in smaller organizations, this may not be possible. In these cases, one or more of these roles may be assigned to the same person. But even though the same person may have more than one database security role, Oracle recommends each role be granted to a separate user account for this person. This helps minimize the impact from an attack by a malicious user who steals one of these accounts.

Can the Oracle Database Vault owner view data protected by a Realm?

No. The Oracle Database Vault owner can only setup security policies, such as Realms and Command Controls, but cannot see data protected by a Realm or a Command Control. They cannot grant this access right to themselves.

Can security responsibilities of the Oracle Database Vault owner be delegated?

A Database Vault Policy can group related Realms and Command Rules and be delegated to a Policy Owner. The Policy Owner can make changes to the Policy without having the full role and privileges of an Oracle Database Vault Administrator. The Policy Owner needs the DV_POLICY_OWNER role to make changes to the Policy they are delegated.

How are changes made by Oracle Database Vault owner to the security objects audited?

All changes made to security objects (enable, disable, add objects, add authorization….) are audited. This cannot be disabled.

Can Oracle Database Vault block common users from accessing sensitive data in Pluggable Databases?

Starting in Oracle Database 19c Release, Oracle Database Vault Operations Control can block common users (infrastructure DBAs, for example) from accessing local data in pluggable databases (PDBs) in autonomous, regular Cloud, or on-premises environments. Common users and applications that must access PDB local data can be added to an exception list.

How complex is to enable Oracle Database Vault Operations Control?

It is simple to enable and transparent for PDB users. To enable Database Vault operations control, use the DBMS_MACADM.ENABLE_APP_PROTECTION PL/SQL procedure.

Can Oracle Database Vault be managed through Oracle Enterprise Manager?

Yes. Oracle Enterprise Manger Cloud Control provides a management interface for most Oracle Database Vault features including realms, rules and rule sets, command rules, etc.

How do Oracle DBA tasks change with Oracle Database Vault?

Most DBA tasks remain unchanged with Oracle Database Vault. One area of change is in creating and managing users and profiles. This security related task can only be done by a user with the DV_ACCTMGR role. Additionally, tasks that can expose sensitive data like Datapump and Job Scheduling need a separate authorization from an account with the DV_OWNER role. Please refer to the white paper “DBA Administrative Best Practices with Oracle Database Vault” available on Oracle Technology Network (OTN) for more information.

DEPLOYMENT

What is the performance overhead on the database with Oracle Database Vault Realms and Command Rules?

Testing with Oracle E-Business Suite shows Oracle Database Vault Realms and Command Controls have a minimal overhead of less than 2%. Normal database tuning still applies when Oracle Database Vault is enabled.

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

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.

How are applications certified and then deployed with Oracle Database Vault?

Starting from Oracle Database 12c Release 2, Oracle Database Vault has a simulation mode where the Oracle Database Vault security controls are checked, but instead of preventing access, it logs policy violations to a simulation log. This allows the customer to run a regression test end-to-end without interruptions from Oracle Database Vault. The simulation log is analyzed at the end of the regression test to see if any adjustments are required in the Oracle Database Vault security controls. Simulation mode is used again when the application is put into production to do a final check in production before the Oracle Database Vault protections are enabled.

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

Oracle Database Vault allows for a database patching mode where the database can be patched without disabling Oracle Database Vault. In this case, the Security Administrator (user with the DV_OWNER role) 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 application data.

How are DBAs prevented from making unauthorized system and session changes in the database?

Command Rules allow customers to limit what commands can be run in the database. ALTER SYSTEM and ALTER SESSION are powerful commands and their fine-grained use can be limited by Command Rules and the use of trusted paths.

MORE INFORMATION

Where can I find more information on Oracle Database Vault?

For more information, please see the Oracle Database Vault page on Oracle Technology Network (OTN). A variety of helpful information is available online including data sheet, white paper, customer references, end-user documentation, and a discussion forum. Oracle University offers a training course on Oracle Database Vault.

https://www.oracle.com/database/technologies/security/db-vault.html

19c ORACLE Database

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/cloudsecurity/db-sec facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE