ORACLE

Oracle Database Vault

Oracle Database Vault provides controls to prevent unauthorized privileged users from accessing sensitive data, prevent unauthorized database changes, and helps customers meet industry, regulatory, or corporate security standards.

March 23, 2020

Public

Purpose Statement

This document provides an overview of features and enhancements included in the latest releases of Oracle Database Vault. It is intended solely to help you assess the business benefits of using Oracle Database Vault preventive controls and to plan your Data Security / I.T. projects.

Disclaimer

Table of Contents

INTRODUCTION

Regulations, industry directives, and numerous breach disclosure laws require stronger security controls including separation of duties. Privacy and regulatory challenges are becoming increasingly complicated, as access to data be controlled based on laws spanning multiple countries. In parallel, attacks on databases are becoming increasingly common as hackers and even insiders target large data repositories to steal data, disrupt business, or gain economic advantage through industrial espionage. Data breaches resulting from unauthorized privileged users access or abuse of these accounts have accounted for a large percentage of the overall number of data breaches over the past few years. Protecting the database has become paramount and requires a defense-in-depth, multi-layered approach that encompasses preventive, detective, and administrative controls. Oracle Database 19c strengthens Oracle's industry-leading database security solution by providing important security controls in each of these areas.

"On our path towards EU GDPR compliance, we chose Oracle Database Security solutions including Oracle Advanced Security, Oracle Key Vault, Oracle Database Vault, Oracle Audit Vault and Oracle Database Firewall to streamline and simplify our Oracle deployment. With Oracle, we minimize risk and further enhance our overall security.

Henrique Zacarias
CIO
NOS

Oracle Database Vault with Oracle Database 19c provides the industry's most comprehensive access control capabilities for the Oracle Database. Oracle Database Vault provides essential safeguards against common threats, including:

- Threats that exploit stolen credentials obtained from social engineering, key-loggers, and other mechanisms to get access to privileged accounts in your database
- Threats from insiders that misuse privileged accounts to access sensitive data, or to create new accounts, and grant additional roles and privileges for future exploits
- Threats from insiders who bypass the organization's usage policies including IP address, date, and time of usage
- Threats from unintended mistakes from unauthorized SQL commands that change the database configuration and put the database in a vulnerable state
- Threats to sensitive data during maintenance window from the application administrators
- Threats that exploit weaknesses in the application to escalate privileges and attack other applications on the same database

CONTROLS FOR PRIVILEGED ACCOUNTS

Privileged user accounts are commonplace in all databases and are used by DBAs for daily tasks such as user management, performance tuning, replication, patching, backup and recovery, space management, startup, and shutdown. Many Oracle predefined system users and roles can access any application data in the database. Due to their wide-ranging access, most organizations enforce strict processes and internal rules regarding who can be granted privileged access to the database. These accounts and roles, however, have also been a prime target of hackers because of their unimpeded access inside the database. Privileged access can also be misused by insiders to gain access to confidential information.

PRIVILEGE USER ACCESS CONTROLS ON APPLICATION DATA WITH REALMS

Increasing controls on privileged and DBA accounts is vital to improving security. Oracle Database Vault creates a highly restricted application environment ("Realm") inside the Oracle Database that prevents access to application data from privileged accounts while continuing to allow authorized administrative activities on the database. Realms can be placed around all or specific application objects, such as tables or entire schemas, to protect them from unauthorized access while still allowing authorized users to access those tables and schemas. Database Vault Realms can allow access to those who have been granted direct access to the protected objects or limit access to only those who have been granted specific authorization through the Realm.

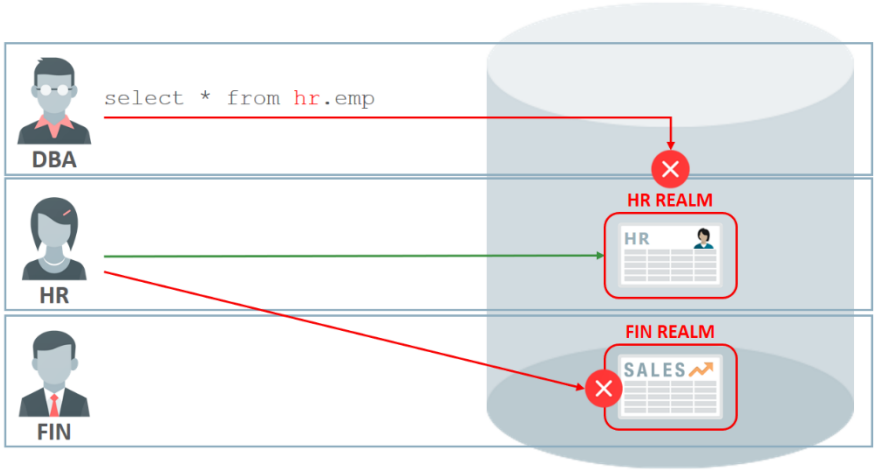

Figure 1. Oracle Database Vault for privileged accounts

Oracle Database Vault Realms use cases

USE CASE	DESCRIPTION
Prevent unauthorized access to application data	Realms help customers comply with data access regulations and protect from outsider attacks exploiting compromised DBA accounts and insider threats as well as.
Enable secure consolidation	Realms allow customers to consolidate multiple applications into a single database while preventing highly privileged application accounts from accessing each other's data. This helps customers secure their consolidated applications in their private clouds and helps cloud providers maintain higher level of security assurance for their customers.
Enable secure outsourcing	By controlling access to sensitive data even by administrative staff, Realms allow customers to take advantage of the cost benefits of outsourcing backend operations.

Oracle Database Vault Realms also place controls on powerful system privileges, roles, and account management. In addition, Oracle Database Vault Realms restrict access to security related packages commonly used by applications, such as the Virtual Private Database (VPD) and Oracle Labael

Security (OLS) packages. For example, Oracle Database Vault limits who can manage VPD and Label Security policies, increasing the overall security of applications that use these features.

STRONGER AUTHORIZATION CONTROLS WITH MANDATORY REALMS

While regular Database Vault Realms protect access to sensitive data from broad system privileges like SELECT ANY TABLE, a Database Vault Mandatory Realm also protects against direct object privileges. While schema owners and others with direct object grants can still access data allowed by their direct object privileges when data is protected by a regular realm, they would be blocked by a Database Vault Mandatory Realm. Even schema owners would be blocked from accessing their objects unless authorized to the Database Vault Mandatory Realm. This simplifies finding the list of users that are authorized to the realm protected data so the security officer doesn't have to worry about schema owners and others with direct object privileges from granting these same privileges to other users.

Database Vault Mandatory Realms can also be used during maintenance operations. Periodic access to production environments by IT support staff or application DBAs is a common requirement and is typically associated with patching activity or diagnosing a performance issue. Tasks may involve recreating indexes and triggers, compiling or recompiling PL/SQL packages, or adding new tables, views, and other objects. During such maintenance windows, organizations need the ability to seal off access to tables and views containing highly sensitive data, even to those with direct object grants or the application owner. This is an increasingly common security need driven by data governance requirements and multi-country privacy regulations. Mandatory Realms can be enabled during maintenance operations to protect just the sensitive data while other schema objects are updated. The table below shows how Oracle Database Vault Mandatory Realms enforces additional authorization check on the application owner before allowing access to application data.

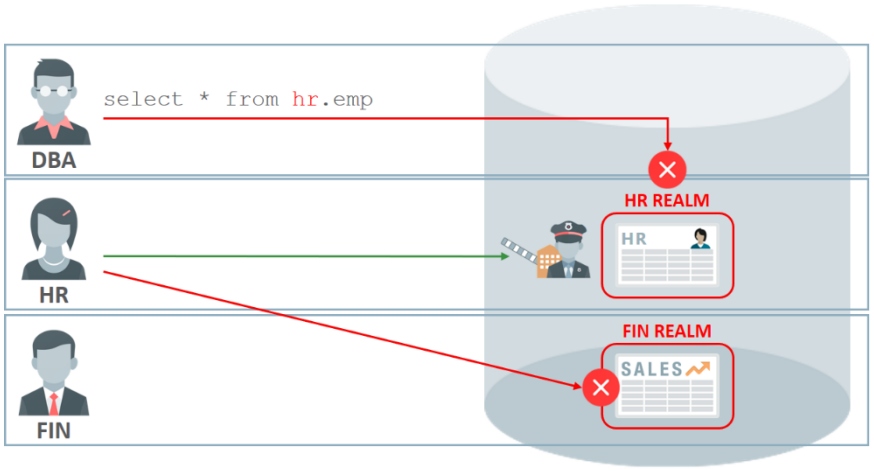

Figure 2. Oracle Database Vault Mandatory Realms for maintenance

Oracle Database Vault Mandatory Realms use cases

USE CASE	DESCRIPTION
Support and Development Access	Mandatory Realms are placed around all or specific application tables, blocking both the application owner as well as those with direct object grants from accessing the data. For patching and support access, stored procedures and application metadata can still be accessed and patched, but application sensitive data will be protected by the Mandatory Realm.

Entitlement Controls	Mandatory Realms freeze the entitlements granted to a database role so that no privileged user can change them. Only realm-authorized users will be able to grant these roles and change their entitlements.
Application Protection	Mandatory Realms are used to protect applications just like regular realms. In this case, all users who rely on direct grants for access should be added to realm authorizations. This makes it easier for auditors to identify all who have access to data and verify compliance.
Incident Response	In the event of a breach or other failure, data may need to be sealed off by Mandatory Realms irrespective of the direct grants and ownership until authorities can analyze the situation.
Threat Response	If an organization becomes aware of a threat, Mandatory Realms can be turned on quickly to stop all access until the threat has been evaluated.

CONTROLS FOR DATABASE CONFIGURATION

Technical controls can prevent changes that could lead to an insecure database configuration, prevent configuration drift, reduce the possibility of audit findings, and improve compliance. Changes to database structures such as application tables and roles, privileged role grants, and ad hoc creation of new database accounts are just a few examples of configuration drift that can have serious consequences. To prevent these audit findings and to comply with regulations, customers need to put in place strong operational controls inside the database. Oracle Database Vault allows customers to prevent configuration drift by controlling the use of commands such as ALTER SYSTEM, ALTER USER, CREATE USER, DROP USER, etc.

SQL COMMAND CONTROLS WITH ORACLE DATABASE VAULT

Oracle Database Vault can be used to control SQL commands that can impact the security and availability of the application and the database. Oracle Database Vault Command Rules introduce an additional layer of rules and checks before any SQL command is executed including CONNECT to the database, DROP TABLE, TRUNCATE TABLE, and DROP TABLESPACE, to name a few. The Command Rules can be used to restrict access to databases to a specific subnet, application server, and program, creating a trusted path from the application to the database. Built-in factors such as IP address, host name, and session user name can be used to enforce SQL command controls inside the database. Oracle Label Security factors can also be used to control activity based on the security clearance of the user's session. In addition, Oracle APEX includes native functions and factors can be used with Oracle Database Vault Command Rules to determine whether to allow access to specific DML or DDL statements.

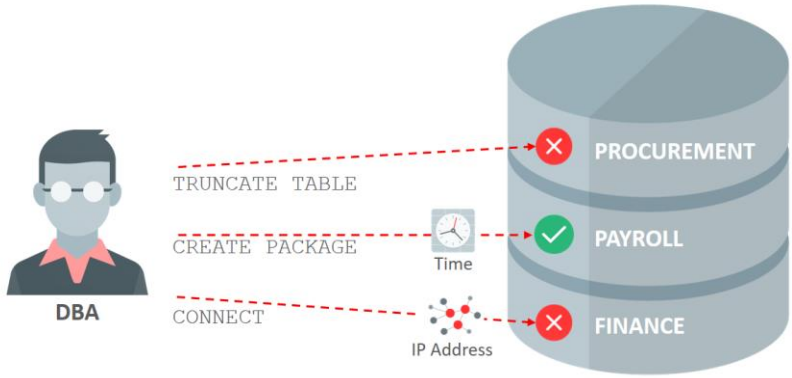

Figure 3. Oracle Database Vault Command Rules & Trusted Paths

ACCOUNT MANAGEMENT CONTROLS WITH ORACLE DATABASE VAULT

Oracle Database Vault places controls over who can create and manage database accounts and roles inside the database. By default, the ability to create database accounts is removed from existing DBAs and assigned to a new "Database Account Manager" role. This makes it possible to implement separation of duty (SOD) between regular database operations and account managers who are responsible for operations such as create user, change password, and alter user. This SOD enforcement control serves as an important safeguard against misuse and the proliferation of powerful database privileges and roles whether granted to users or applications. Organizations can provision the database account management role at their discretion. However, Oracle recommends trusted paths be used to increase security on account management by looking at factors such as IP address, program name and time. In addition, account management activity should be audited and may be alerted on, if needed.

DATABASE ROLE CONTROLS WITH ORACLE DATABASE VAULT

As roles aggregate privileges, there are two ways in which they can be misused: granting or revoking roles without authorization or changing the contents of role itself. Realms protect database roles from being granted by privileged but unauthorized users. If a role is protected by a realm, only the realm owner can grant the protected role to other users or roles.

In addition, Realms allow customers to freeze the settings of database roles by preventing any privilege grant or revoke from roles. This ensures that there is no drift in the roles and entitlements configurations inside the database.

CONTROLS FOR CONSOLIDATION AND CLOUD ENVIRONMENTS

Consolidation and cloud environments provide numerous cost and operational efficiencies but also dramatically increase the potential impact of a data breach due to the massive amount of data, applications, and users on the same database. Consolidation intrinsically brings new risks that were not present in single application databases. To manage such consolidated systems, there may be multiple teams of administrators to manage the system, database, and the application, requiring almost unimpeded access by many privileged users managing the environment. In addition, a simple administrative error on a single application may bring down the entire system or jeopardize the security of all applications and accounts on that server.

Oracle Database Vault can defend such high value targets through defense-in-depth approach by controlling database commands, restricting account management, and protecting sensitive application data. All Oracle Database Vault controls can be configured and deployed transparently on the Oracle Exadata Database Machine, including the pre-configured out-of-the-box control policies for Oracle and non-Oracle enterprise applications. Oracle Database Vault can be used and deployed with Oracle Advanced Security, and Oracle Audit Vault and Database Firewall to enable a Maximum Security Architecture for the Oracle Exadata Database Machine.

CONTROLS FOR ORACLE MULTITENANT

Oracle Database Vault secures pluggable databases (PDBs) by allowing customers to create realms around the sensitive application data inside a PDB which prevents access to their sensitive data by the common DBA in the multitenant container database (CDB), the local PDB DBA, and by other PDBs DBAs residing within the same CDB. Oracle Database Vault Command Rules can enforce from within a PDB from where and how the PDB is accessed as well as what operations can be performed within that PDB.

Operations Control, introduced in Oracle Database Vault 19c, prevents common user access to local PDB data, transparently, without having to configure and enable Database Vault in every PDB. This control is suited for cloud operations and consolidated customer multitenant databases where an infrastructure DBA team manages the fleet of PDBs from the CDB using common user accounts. This allows sensitive local PDB data to be protected without the PDB administrator having to enable Database Vault in the PDB and configure realms to protect local data.

APPLICATION PROTECTION POLICIES

The process of creating Oracle Database Vault controls for custom or commercial applications is a straightforward process. Oracle Enterprise Manager Cloud Control can be used to create a Database Vault Realm around the full application schema or around specific tables with sensitive data based on your security and application design. Alternately, a set of PL/SQL packages can also be used to create Realms and Command Rules.

Oracle Database Vault has been certified or supported with numerous Oracle and partner applications. Certifications include out-of-the-box security policies specific for applications taking into consideration their install, run-time, and maintenance requirements. These security policies protect application data from unauthorized privileged users and provide real-time preventive controls that prevent ad hoc changes to application's data structures.

Enterprise Applications supporting Oracle Database Vault

Application
Oracle Fusion Applications
Oracle E-Business Suite
Oracle Peoplesoft
Oracle JD Edwards Enterprise One
Oracle Siebel
Oracle Retail Applications
Oracle Financial Services
Oracle Utilities Applications
Oracle Primavera
Oracle Enterprise Taxation Management
SAP Applications
Infosys Finacle

Policies and guidelines for Oracle Applications are available through Oracle Support and the partner support portals. The policies can also be used as blueprints for designing policies to protect custom applications. The Oracle Database Security team continues to work with Oracle Application groups as well as with partners to provide policies and guidelines for additional applications.

MONITORING ORACLE DATABASE VAULT

Oracle Database Vault Audit shows SQL statements blocked by Oracle Database Vault, and any security policy changes made by an Oracle Database Vault administrator. For example, if a DBA attempts to access data in an application table protected by a Realm or Command Rule, Oracle Database Vault prevents that access and creates an audit record for the incident that can be viewed using the Realm Audit Report. Oracle Database Vault reports can also be used to track security administrators' actions and show any changes to Oracle Database Vault configuration.

Oracle Database Vault specific reports are available out-of-the-box through Oracle Enterprise Manager Cloud Control, or through Oracle Audit Vault and Database Firewall. In addition to aggregating and reporting on Oracle Database Vault audit events, Oracle Audit Vault and Database Firewall provides a comprehensive overview of activity that includes SQL statements on the network, as well as audit data generated by Oracle and non-Oracle databases, operating systems, and directories.

DEPLOYMENT AND OPERATIONAL SIMPLICITY

Oracle Database Vault is part of the core Database and can be enabled using the command line. Once enabled, the Oracle Database needs to be restarted for Oracle Database Vault controls to be in effect. No installation of additional software or re-linking of the Oracle database executable is needed.

Oracle Database Vault enforcement remains with the database even when the database files are exported or restored to a different Oracle home environment. Oracle Database Vault can be deployed with Oracle's Maximum Availability Architecture, including Oracle RAC and Oracle Data Guard.

Oracle Database Vault protects applications data while keeping the DBA fully operational. DBAs can perform their regular duties like tuning, diagnostics, backup and recovery as usual. However, Oracle Database Vault does enforce discipline when it comes to administering protected sensitive data. DBAs need authorization before they can export, import or move protected sensitive data. For more details, please refer to the Oracle Documentation for Database Vault.

Oracle Database Vault policies are enforced inside the Oracle Database kernel, providing unparalleled security and very low performance overhead, providing transparency to the performance profile of existing applications. Production customers running Oracle Database Vault on major applications have reported no change in their application response time.

Simulation Mode reduces risk when enabling new Database Vault controls in the production environment. Instead of enabling the controls, the controls are put into simulation mode to capture command rule and realm violations in a simulation log instead of blocking the SQL statement. This allows users to quickly certify an application with new Database Vault controls since the application will be able to complete its regression test without being blocked. New applications can also use simulation mode to identify authorized users, trusted paths and command rules to deploy with the application into production.

CONCLUSION

Oracle Database Vault creates a robust foundation for secure database operations and application deployment. It protects sensitive data like intellectual property, privacy data, and application data from external attackers and the insider threat. Controls can be pre-configured and enabled to meet increased security requirements. Oracle Database Vault provides support for consolidation and cloud computing and can be deployed seamlessly with Oracle Exadata and the Oracle Multitenant Database option. Oracle Database Vault preventive controls are designed to be transparent to existing applications and adaptive to existing database administration processes.

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 facebook.com/oracle twitter.com/oracle

Oracle Database Vault White Paper
June, 2020