

Oracle Database 11g: Implement Database Vault - LVC Release 2

Duration: 2 Days

What you will learn

Oracle Database Vault helps an organization meet their security goals. Many requirements are being put on systems regarding separation of duties and privacy and protection of data, including insider threats. DBAs and security administrators need to understand these requirements, and also the tools available for meeting them.

This course introduces the student to the Database Vault product, including installation, configuration, and how it affects activities in the database. New security concepts are introduced, illustrated, and clearly demonstrated by relevant practices.

Learn To:

How to use the various features of Oracle Database Vault

How to monitor and maintain an Oracle Database Vault environment

Install and configure Oracle Database Vault to meet your security compliance goals

How to use the various features of Oracle Database Vault

How to monitor and maintain an Oracle Database Vault environment

Install and configure Oracle Database Vault to meet your security compliance goals

A Live Virtual Class (LVC) is exclusively for registered students; unregistered individuals may not view an LVC at any time. Registered students must view the class from the country listed in the registration form. Unauthorized recording, copying, or transmission of LVC content may not be made.

Audience

Database Administrators

Security Administrators

Security Compliance Professionals

Support Engineer

Technical Consultant

Prerequisites

Required Prerequisites

Basic Oracle administration skills

SQL and PL/SQL skills

Suggested Prerequisites

Oracle Database 11g: Security

Oracle Database 11g: Administration Workshop I Release 2

Oracle Database 11g: Security - Online Course

Course Objectives

- Install and Configure Oracle Database Vault Audit Database Vault activities
- Configure Oracle Database Vault components (such as Realms, Identities, and Factors) to implement security
- Use attributes such as time of day and IP address to determine users' privileges
- Use the Database Vault administration browser interface
- Use PL/SQL APIs to perform Database Vault functionality
- Access Database Vault views to see security information
- Incorporate best practices into database vault configuration
- Identify the features and benefits of Oracle Database Vault

Course Topics

Introduction

Overview of Database Vault

- Overview of Database Vault elements and functionality
- Component relationships
- Database Vault example
- Database Vault effects
- Database Vault Administrator (DVA)
- Reporting and monitoring
- Database Vault API
- Managing Database Vault databases using Enterprise Manager

Configuring Database Vault

- Enabling Oracle Database Vault
- Configuring an Oracle database for Database Vault
- Database parameters altered during configuration
- Logging into DVA
- Database roles
- Database Vault accounts
- Database Vault schemas

Configuring Realms

- Realms: Concepts
- Creating and editing realms
- Deleting realms
- The realm algorithm
- Examples of realms
- Delivered realms
- Realm views
- Monitoring and reporting of realms

Defining Rule Sets

- Rule sets: Concepts
- Creating and editing rule sets
- Deleting rule sets
- Reusing rules
- Auditing rule sets
- Custom event handlers
- Using rule sets with realms

Rule set examples

Configuring Command Rules

Command Rules: Concepts
Creating and editing command Rules
Delivered command rules
DBA_DV_COMMAND_RULE view
Command rule report
Command rule API

Extending Rule Sets

Factors: Concepts
Factor scenarios
Creating and editing factors
Managing factors:
Identities: Concepts
Purpose of identities
Creating an identity
Managing identities

Configuring Secure Application Roles

Secure application roles: Concepts
Creating and editing secure application roles
Deleting secure application roles
Secure application roles: Examples
Managing secure application roles:

Viewing Database Vault Reports

Monitoring Database Vault
Configuration reports
Auditing reports
Security reports
Object privilege reports
Accounts and roles reports
Privilege summary reports
System privileges reports

Implementing Best Practices

Identifying your security requirements
Suggested naming conventions
Separation of duty best practices
Identifying your security requirements
Audit all violations
Connection pooling considerations
Enforcing connections from an application server
Performance considerations