

## Oracle Database Security (Hardening, Detective and Audit Control)

---

### Course Summary

#### Description

In this course, you will learn how to use features of Oracle Database 12c to secure the databases in your own organization. You'll begin by implementing basic database and network security and build on this knowledge throughout the course.

#### Objectives

At the end of this course, students will be able to:

- Choose Oracle security solutions to meet security requirements.
- Implement basic database security.
- Configure network security.
- Discover basic security configuration issues.

#### Topics

- Introduction
- Types of Auditing
- Using Fine-Grained Audit
- Introduction to Oracle Audit Vault and Database Firewall
- Planning the Oracle Audit Vault and Database Firewall Implementation
- Installing the Audit Vault Server
- Configuring the Audit Vault Server
- Configuring Oracle AVDF and Deploying the Audit Vault Agent
- OSI Seven-Layer Network Model: Overview
- Installing a Database Firewall
- Using Host Monitoring
- Managing the Audit Vault Server
- Managing the Database Firewall
- Performing Administrative Tasks
- Audit Policies and Audit Data Collection
- Oracle AVDF Reports
- Creating Alerts
- Customizing Rules for Your Database

#### Audience

The targeted audience for this course is Developers, Architects and Database administrators.

#### Prerequisites

Students should be familiar with

- Familiarity with Oracle database basics
- Some knowledge of computers
- Basic familiarity with programming

#### Duration

Four days

## Oracle Database Security (Hardening, Detective and Audit Control)

---

### Course Outline

- I. *Introduction*
  - A. Overview
  - B. Environment Familiarization
  - D. Verifying the Audit Vault Server Services
  - E. Configuring syslog Messages
  - F. Defining an Archiving Location
  - G. Creating Archive Policies
- II. *Types of Auditing*
  - A. Roles
  - B. Enabling Unified Auditing
  - C. Creating and Enabling Audit Policies?.Part 1
  - D. Creating and Enabling Audit Policies?.Part 2
  - E. Cleaning Up Audit Policies and Data
  - F. Auditing RMAN Backups
- III. *Using Fine-Grained Audit*
  - A. Implementing Fine-Grained Auditing
  - B. Viewing the FGA Trail
  - C. Using an Event Handler
- IV. *Introduction to Oracle Audit Vault and Database Firewall*
  - A. Identifying Audit Vault and Database Firewall Components
  - B. Identifying Supported Secured Targets
  - C. Identifying Third-Party Product Integration
  - D. Distinguishing Typical Tasks of Oracle AVDF Administrators and Auditors
- V. *Planning the Oracle Audit Vault and Database Firewall Implementation*
  - A. Implementing Oracle AVDF
  - B. Configuring Oracle AVDF and Deploying the Audit Vault Agent
  - C. Configuring Oracle AVDF and Deploying the Database Firewall
- VI. *Installing the Audit Vault Server*
  - A. Introduction
  - B. Performing Audit Vault Server Post-Installation Tasks
- VII. *Configuring the Audit Vault Server*
  - A. Creating Audit Vault Server Administrative Users
  - B. Verifying the Server Date and Time Settings
  - C. Verifying the Audit Vault Server Network Configuration
- VIII. *Configuring Oracle AVDF and Deploying the Audit Vault Agent*
  - A. Registering the Host
  - B. Deploying the Audit Vault Agent on the Host
  - C. Activating the Audit Vault Agent
  - D. Creating User Accounts on the Secured Target
  - E. Registering the Secured Target
  - F. Configuring an Audit Trail for the Secured Target
  - G. Configuring Stored Procedure Auditing
- IX. *OSI Seven-Layer Network Model: Overview*
  - A. Networking and Oracle AVDF
  - B. OSI Networking Model Layer
  - C. AVDF Supported Protocols
  - D. Configuring Database Firewall
  - E. Using Network Diagnostic Tools
- X. *Installing a Database Firewall*
  - A. Introduction
  - B. Performing Database Firewall Post-Installation Tasks
- XI. *Using Host Monitoring*
  - A. Reviewing Sample Configurations
  - B. Installing the Host Monitor
  - C. Configuring an Audit Trail
  - D. Starting the Host Monitor
- XII. *Managing the Audit Vault Server*
  - A. Verifying an Archived Location Definition
  - B. Starting an Archive Job
  - C. Restoring Archived Datafiles
- XIII. *Managing the Database Firewall*
  - A. Viewing Live Network Traffic
  - B. Capturing Network Traffic
  - C. Viewing the Database Firewall Status Report
  - D. Viewing a Database Firewall Diagnostic Report

## Oracle Database Security (Hardening, Detective and Audit Control)

---

### Course Outline (cont'd)

#### *XIV. Performing Administrative Tasks*

- A. Using Secured Target Groups
- B. Monitoring a Job
- C. Creating Auditor Accounts
- D. Viewing Audit Trails
- E. Viewing Enforcement Points
- F. Creating an Email Template

#### *XV. Audit Policies and Audit Data Collection*

- A. Oracle Database Traditional Auditing
- B. Retrieving Audit Settings
- C. Creating Audit Policy Settings
- D. Provisioning Audit Policies

#### *XVI. Oracle AVDF Reports*

- A. Viewing Audit Reports
- B. Customizing Reports
- C. Viewing Compliance Reports
- D. Viewing Firewall Reports
- E. Creating and Scheduling PDF Reports

#### *XVII. Creating Alerts*

- A. Creating an Alert
- B. Viewing the Triggered Alert
- C. Updating the Alert Status
- D. Viewing the Alert Report
- E. Scheduling an Alert Report

#### *XVIII. Customizing Rules for Your Database*

- A. Creating a Configuration Extension
- B. Creating an Agent-Side Compliance Standard Rule
- C. Creating a Manual Rule
- D. Creating a Compliance Standard
- E. Suppressing Violations
- F. Clearing Violations