Oracle Audit Vault and Database Firewall: Install & Configure

Duration: 2 Days

What you will learn

Note: No hands-on lab environment for the Training On Demand course format

In the Oracle Audit Vault and Database Firewall: Install & Configure course, students will learn how to deploy Oracle Audit Vault and Database Firewall.

Learn To:
Install, configure, and manage the Audit Vault Server.
Deploy the Audit Vault Agent.
Describe Database Firewall Networking.
Install, deploy, and manage a Database Firewall.
Install and enable Host Monitoring.

Benefits To You

Oracle Audit Vault and Database Firewall provides comprehensive and flexible monitoring through the consolidation of audit data from Oracle and non-Oracle databases, operating systems, directory, and file systems. Dozens of built-in reports combined with powerful alerting assists auditors and information security personnel. Database Firewall can also be deployed as a first line of defense on the network, enforcing expected application behavior, helping prevent SQL injection, application bypass, and other malicious activity from reaching the database.

In this course, students will benefit by learning how to configure Audit Vault Server and deploy Audit Vault Agents to collect audit data, so the data can be viewed in built-in, customizable activity and compliance reports. Students will also learn how to deploy a Database Firewall that can monitor activity and block SQL statements on the network based on a firewall policy.

Audience

Database Administrators
Security Administrators
System Administrator

Related Training

Required Prerequisites

Oracle Database 12c: Security

Suggested Prerequisites
Networking knowledge and experience

Oracle Database administration experience

Course Objectives

Install and configure a Database Firewall

Install and enable host monitoring

Configure high availability mode (resilient pairs)

Create custom collection plug-ins

Explain the Oracle AVDF architecture and process flow

Deploy an Audit Vault Agent

Install and configure an Audit Vault Server

Describe the AVDF auditing features

Course Topics

Introduction to Oracle Audit Vault and Database Firewall
Oracle Audit Vault and Database Firewall Features
Oracle Audit Vault and Database Firewall Components
Oracle Audit Vault and Database Firewall Architecture
Supported Secured Targets
Integrating Oracle AVDF with Third-party Products
Oracle AVDF Administrator Tasks
Oracle AVDF Auditor Tasks

Planning the Oracle Audit Vault and Database Firewall Implementation
Evaluating Oracle AVDF Configuration Requirements
Configuring Oracle AVDF and Deploying the Audit Vault Agent
Configuring Oracle AVDF and Deploying the Database Firewall

Installing the Audit Vault Server
Requirements for Installation of Oracle AVDF
Network Interface Card Requirements
Installing an Audit Vault Server
Performing Audit Vault Server Post-Installation Tasks

Configuring the Audit Vault Server
Specifying the Server Date and Time
Setting or Changing the Audit Vault Server Network Settings
Configuring or Changing the Audit Vault Server Services

Configuring the Audit Vault Server Syslog Destinations
Defining Datafile Archiving Locations
Creating Archiving Policies
Configuring the Email Notification Service
Configuring Administrative Accounts for the Audit Vault Server

Configuring Oracle AVDF and Deploying the Audit Vault Agent
Understanding Network Requirements for AV Server and AV Agent
Registering Hosts in the Audit Vault Server
Deploying and Activating the Audit Vault Agent on Host Computers
Registering the Audit Vault Agent as a Windows Service
Creating User Accounts for Oracle AVDF
Registering Secured Targets
Configuring Audit Trails for Secured Targets
Configuring Stored Procedure Auditing

Networking and Oracle AVDF
Overview of the OSI 7-level Network Model
Overview of IPv4 Addressing and Routing
Overview of MAC Addressing
Overview of Virtual LANs (VLANs)
Overview of Spanning Tree Protocol (STP)
Oracle AVDF Deployment Models (inline, out of band, and proxy)
Best Practices for Database Policy Enforcement (DPE) and Database Activity Monitoring (DAM) Modes

Installing a Database Firewall
Requirements for Installation of a Database Firewall
Network Interface Card (NIC) Requirements
Installing a Database Firewall
Performing Database Firewall Post-Installation Tasks

Configuring Oracle AVDF and Deploying Database Firewall
Configuring Basic Settings for Database Firewall
Configuring a Database Firewall on Your Network
Associating a Database Firewall with the Audit Vault Server
Registering Secured Targets
Configuring Enforcement Points
Configuring and Using Database Interrogation
Configuring and Using Database Response Monitoring

Using Host Monitoring
Overview of Host Monitoring
Installing and Enabling Host Monitoring
Checking the Status of the Host Monitor
Stopping the Host Monitor

Configuring High Availability
Overview of Oracle AVDF High Availability Architecture (resilient pairs)
Configuring a Resilient Pair of Audit Vault Servers
Configuring a Resilient Pair of Database Firewalls

Creating Custom Collection Plug-ins

Overview of Audit Collection Plug-ins
General Procedure for Writing Audit Collection Plug-ins
Setting Up Your Development Environment (downloading the SDK)
Creating Audit Collection Plug-ins
Packaging Audit Collection Plug-ins

Managing the Audit Vault Server
Starting an Archive Job
Restoring Audit Data
Monitoring Jobs

Managing the Database Firewalls
Viewing and Capturing Network Traffic in a Database Firewall
Viewing the Status and Diagnostics Report for a Database Firewall
Removing a Database Firewall from the Audit Vault Server

Overview of the Auditing and Reporting Features
Overview of Database Firewall Policies
Overview of Oracle Database Audit Policies
Overview of Reports and Report Schedules
Overview of Oracle Database Entitlement Auditing
Overview of Oracle Database Stored Procedure Auditing
Overview of Alerts and Email Notifications