Oracle Database 19c: Monitoring and Maintaining a Secure Environment LVC

Oracle Database

DURATION	MODULES	COURSE CODE
1 Days	**5 Lectures**	**—**

Course Overview

The course covers the following topics: Auditing Database Vault Database Security Assessment Tool Database Patching

What You Will Learn

- I Module Overview
- Security Modules I-2
- Security Course 1 – Security Fundamentals I-3
- Security Course 2 – Data Confidentiality I-5
- Security Course 3 – Data Encryption I-7
- Security Course 4 – Monitoring and Maintaining a Secure Environment I-8

Auditing

- Learning Objectives
- Default, Privileged User, and Standard Audit
- Fine Grained Audit (FGA)
- FGA Policy
- Triggering Audit Events
- Data Dictionary Views
- Unified Audit Implementation
- DBA_FGA_AUDIT_TRAIL/UNIFIED_AUDIT_TRAIL
- Security and Performance: Audit Architecture
- Tolerance Level for Loss of Audit Records
- Consolidation: Unique Audit Trail
- Basic Audit Versus Extended Audit Information
- Extended Audit Information
- Data Pump Audit Policy
- Oracle RMAN Audit Information
- Extending Unified Auditing with Context information

- Introducing Oracle Audit Vault and Database Firewall
- Database Auditing and Activity Monitoring
- Oracle AVDF Components
- Oracle Audit Vault and Database Firewall Architecture
- Audit Collection: Supported Secured Target Types
- Configuring Network Firewalls to Enable Audit Vault and Database Firewall
- Deployment
- Oracle AVDF Administrator Tasks
- Oracle AVDF Auditor Tasks
- Summary
- Practice 1: Overview

Database Vault

- Learning Objectives
- Database Vault
- Default Separation of Duties with Database Vault
- Privileges That Are Revoked from Existing Users and Roles
- Privileges That Are Prevented for Existing Users and Roles
- Oracle Database Vault Roles
- What Is a Realm?
- Benefits of Using Realms
- Effect of Realms on Nonmembers
- Mandatory Realms and Object Privileges
- Protecting with a Mandatory Realm
- Characteristics of Mandatory Realms
- Benefits of Mandatory Realms
- Database Vault Factors, Rules, and Rule Sets
- What Is a Command Rule?
- What Is a Rule Set?
- Database Vault Command Rules
- How Realms and Command Rules Work Together
- Protecting Roles
- Protecting Sensitive Data During Patching
- Protecting Objects from DBAs
- Protecting Sensitive Data During Run Time
- Tasks Involving Realms
- Realm Attributes
- Realm Views
- Oracle-Defined Realms
- Predefined Reports
- Evaluation of Rule Sets
- Using Rule Sets
- Oracle-Defined Rule Sets
- Creating and Maintaining Rules
- Rule Set Tasks

- Auditing Rule Sets
- Setting a Custom Event Handler
- Using Rule Sets with Realms
- Rule Set Reports
- Rule Set Views
- Rule Set API
- Command Rules
- Use Case
- Scope of Command Rules
- Disallowing ALTER TABLE in a Schema
- Delivered Command Rules
- Reports and Views
- Command Rule API
- Database Vault Operations Control
- Database Vault Operations Control: Allowing Operations
- Database Vault Operations Control: Granting the DV_OWNER Role
- Database Vault Operations Control: Setting an Exception List
- Summary
- Practice 2: Overview

Database Security Assessment Tool

- Learning Objectives
- Database Security Assessment Tool (DBSAT)
- DBSAT Components – Collector and Reporter
- DBSAT Components – Discoverer
- Install DBSAT
- Collect Data Using Collector
- Generate the Database Security Assessment Report Using Reporter
- View the Database Security Assessment Report
- View the Database Security Assessment Report – Basic Information
- View the Database Security Assessment Report – Auditing
- View the Database Security Assessment Report – Operating System
- Discover Sensitive Data – Configure the Discoverer
- Discover Sensitive Data – Define Search Patterns for the Discoverer
- Discover Sensitive Data – Discover Sensitive Data
- Database Sensitive Data Assessment Report – Summary
- Database Sensitive Data Assessment Report – Sensitive Data
- Database Sensitive Data Assessment Report – Tables Detected within Sensitive
- Category
- Database Sensitive Data Assessment Report – Schema View
- Summary
- Practice 3: Overview

Database Patching

- Learning Objectives

- Difference Between RU and RUR
- Types of Patches
- Critical Patch Updates (CPUs)
- What is a CVE?
- Decoding the CVSS Risk Scoring
- Lifetime Support Policy
- Overview of the Patch Process
- Oracle Patching Tools: opatch
- Oracle Patching Tools: OPatch Auto
- OPatch Automation: Examples
- Minimizing Down Times: Rolling Patching
- Minimizing Down Times: Standby-First Patching
- Minimizing Down Times: Patching a Cloned Home
- Queryable Patch Inventory
- Alternative Methods of Patching
- Client Patching
- Summary
- Practice 4: Overview

Database Security in the Cloud

- Learning Objectives
- Autonomous Database "Self-Securing"
- Self-securing Capabilities
- Hybrid Cloud Scenarios
- Shared Responsibility Model Between Oracle and You
- Summary
- Practice 5: Overview