ODS-PC: Oracle Database Security: Preventive Controls

Course Code: ODS-PC
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

In the Oracle Database Security: Preventive Controls course, students learn how they can use Oracle Database Security products and technologies to meet the security, privacy and compliance requirements of their organization.

The current regulatory environment of the Sarbanes-Oxley Act, HIPAA, the UK Data Protection Act, and others, requires better security at the database level. Students learn how to secure the access to their databases and how to use the Oracle Database Security products and technologies that enhance data access and confidentiality. The course provides suggested Oracle solutions for common problems.

Learn To:

- Choose Oracle Database Security products and technologies to meet security requirements.
- Secure the database access by database or enterprise users with basic or strong authentication such as SSL, Kerberos and Radius.
- Protect against database bypass by using Transparent Database Encryption.
- Use Oracle Wallets and Oracle Key Vault to manage encryption keys.
- Discover sensitive columns such as Credit Card Numbers by using Application Data Modeling.
- Minimize sensitive data proliferation to test/dev environments by using Data Masking.
- Minimize storage costs in test/dev environments by using Data Subsetting.
- Reduce sensitive data exposure in applications by using Data Redaction.
- Understand and use Oracle Database Vault.

SKILLS COVERED

Upon completing this course, the learner will be able to meet these overall objectives:

- Configure and use Transparent Data Encryption
- Understand and use Oracle Key Vault
- Understand Oracle Data Redaction
- Understand and use Oracle Data Masking and Subsetting
- Understand security risks and identify appropriate Oracle solutions
- Configure general authentication and authorization
- Understand and implement Global Users
- Set up and maintain a simple wallet
- Install and use Oracle Database Vault
- Configure and use Transparent Sensitive Data Protection

WHO SHOULD ATTEND?

- Database Administrators
- System Analysts
- Support Engineer
- Security Administrators
- Network Administrator

PREREQUISITES

Suggested Prerequisite

- Use Oracle Data Pump export and import and Perform RMAN back

- Use Flashback Data Archive and Create PL/SQL procedures
- Familarity with SQL*Plus, SQL*Developer
- Familarity with Oracle Enterprise Manager Cloud Control

Required Prerequisite

- Introduction to Oracle Database Security Ed 1
- Create and manage users, roles, and privileges
- Create and manage tables and tablespaces
- Create PL/SQL procedures

MODULES

Module 1: Introduction

- Course Objectives
- Related courses and where this fits
- Course Schedule and Appendices

Module 2: Using Basic and Strong User Authentication

- Basic Authentication
- Strong Authentication
- Database Link Passwords Protection
- Security of Roles

Module 3: Configuring Global User Authentication

- About Enterprise User Management (EUS)
- EUS and LDAP Integration

Module 4: Using Proxy Authentication

- Security Challenges of Three-Tier Computing
- Proxy Authentication Solutions

Module 5: Encryption Concepts and Solutions

- Concepts
- Solutions
- Oracle Solutions

Module 6: Using Built-In Encryption in Applications

- Usage

Module 7: Using Transparent Data Encryption (TDE)

- Overview
- The Master Keys and the Keystore
- Hardware Keystore
- Encryption

Module 8: Database Storage Security

- RMAN and OSB Backups
- RMAN Encryption Modes
- Data Pump Export and Import of Encrypted Data

Module 9: Introduction to Oracle Key Vault

- What is Oracle Key Vault?
- Using Oracle Key Vault

Module 10: Installing Oracle Key Vault

- Installation
- Endpoints

Module 11: Using Oracle Key Vault

- Reviewing or refreshing prerequisite knowledge

- Contrasting Oracle Wallets and OKV Virtual Wallets

Module 12: Administering Oracle Key Vault

- Roles in detail
- Best practice tips for Oracle Key Vault

Module 13: Automated Sensitive Data Discovery

- Overview
- Application Data Modeling
- Managing Application Data Models

Module 14: Oracle Data Masking and Subsetting overview

- Overview

Module 15: Masking Sensitive Data in Non-Production Environments

- Exploring Data Masking Format Library
- Data Masking Transformations

Module 16: Subsetting Data

- Exploring Data Subsetting definitions

Module 17: Managing Data Masking and Subsetting

- Administering Data Masking and Subsetting
- Heterogeneous masking and subsetting
- Best Practices

Module 18: Oracle Advanced Security - Data Redaction

- Need to redact or dynamically mask data
- Implementing Data Redaction
- Data Redaction usage guidelines

Module 19: Oracle Transparent Sensitive Data Protection (TSDP)

- TSDP Implementation

Module 20: Oracle Database Vault Overview

- Understand Database Vault Controls
- What is a Realm? A Rule Set? A Command Rule? A Secure Application Role?
- What are Factors and Identities? Component Relationships and Evaluation?
- Database Vault Effects and Example
- Software Overview: API, Views, and Integration with Other Oracle Products

Module 21: Configuring Database Vault

- Configuring Database Vault
- Database Vault Roles and Schema
- What to Expect After You Enable Database Vault
- Securing Data in Multitenant Environments
- Configuring Database Vault Users in Cloud Control 12c

Module 22: Analyzing Privileges

- Privilege Analysis Overview and Features
- How Does it Work?
- What are The Types of Analysis, Tools, and Prerequisites?
- Managing Privilege Analysis Policies
- Use Cases

END OF PAGE