

Oracle Database Security: Preventive Controls Ed 1

Duration: 5 Days

What you will learn

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.

Benefits To You

This course discusses the following security features of the database: authentication, data access control including user authorizations by using privileges and roles, data confidentiality including Data Redaction, Oracle Data Masking and Subsetting, Transparent Sensitive Data Protection, encryption at the column, tablespace and file levels by using Transparent Data Encryption. This course discusses the use of the Oracle Key Vault to centrally manage keys across the enterprise. Oracle Database Vault is used to enforce Separation of Duties at the DBA level.

Hands-on practices and available demonstrations help students learn how to use most of the features of Oracle Database 12c to secure their data center, by using Oracle Enterprise Manager Cloud Control or other simple tools such as SQL*Plus.

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.

Related Training

Required Prerequisites

Create PL/SQL procedures

Create and manage tables and tablespaces

Create and manage users, roles, and privileges

Introduction to Oracle Database Security Ed 1

Suggested Prerequisites

Familiarity with Oracle Enterprise Manager Cloud Control

Familiarity with SQL*Plus, SQL*Developer

Use Flashback Data Archive and Create PL/SQL procedures

Use Oracle Data Pump export and import and Perform RMAN back

Course 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

Course Topics

Introduction

Course Objectives

Related courses and where this fits

Course Schedule and Appendices

Using Basic and Strong User Authentication

Basic Authentication

Strong Authentication

Database Link Passwords Protection

Security of Roles

Configuring Global User Authentication

About Enterprise User Management (EUS)

EUS and LDAP Integration

Using Proxy Authentication

Security Challenges of Three-Tier Computing

Proxy Authentication Solutions

Encryption Concepts and Solutions

Concepts

Solutions

Oracle Solutions

Using Built-In Encryption in Applications

Usage

Using Transparent Data Encryption (TDE)

Overview

The Master Keys and the Keystore

Hardware Keystore

Encryption

Database Storage Security

RMAN and OSB Backups

RMAN Encryption Modes

Data Pump Export and Import of Encrypted Data

Introduction to Oracle Key Vault

What is Oracle Key Vault?

Using Oracle Key Vault

Installing Oracle Key Vault

Installation

Endpoints

Using Oracle Key Vault

Reviewing or refreshing prerequisite knowledge

Contrasting Oracle Wallets and OKV Virtual Wallets

Administering Oracle Key Vault

Roles in detail

Best practice tips for Oracle Key Vault

Automated Sensitive Data Discovery

Overview

Application Data Modeling

Managing Application Data Models

Oracle Data Masking and Subsetting overview

Overview

Masking Sensitive Data in Non-Production Environments

Exploring Data Masking Format Library

Data Masking Transformations

Subsetting Data

Exploring Data Subsetting definitions

Managing Data Masking and Subsetting

Administering Data Masking and Subsetting

Heterogeneous masking and subsetting

Best Practices

Oracle Advanced Security - Data Redaction

Need to redact or dynamically mask data

Implementing Data Redaction

Data Redaction usage guidelines

Oracle Transparent Sensitive Data Protection (TSDP)

TSDP Implementation

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

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

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