Oracle Database 12c: Security

Duration: 5 Days

What you will learn

This Oracle Database 12c: Security training teaches you how you can use Oracle Database features to meet the security, privacy and compliance requirements of your organization. You'll get the chance to interact with expert Oracle University instructors through a combination of instruction and hands-on exercises that reinforce new concepts.

Learn To:
Understand Oracle security solutions and how they can help address your security requirements.
Configure strong authentication for database users using PKI and Kerberos.
Control data access using virtual private database and Oracle Label Security.
Analyze application privileges and reduce the attack surface using Oracle Database Vault Privilege Analysis.
Reduce risk of data exposure using Oracle Advanced Security Data Redaction, Transparent Data Encryption and Oracle Data Masking and Subsetting.
Audit activity inside the database using policy and condition based unified auditing.
Configure network encryption to protect information in transit.
Audit activity inside the database using policy and condition based unified auditing.
Protect against application bypass using Oracle Database Vault Realms.

Benefits to You
The current regulatory environment of the Sarbanes-Oxley Act, HIPAA, the UK Data Protection Act, and others requires better security at the database level. By investing in this course, you'll learn how to secure access to your databases and use database features that enhance data access and confidentiality. This course provides suggested Oracle solutions for common problems.

Deep Dive into Security Features
Expert Oracle University instructors discuss the following security features of the database: authentication, data access control including user authorizations using privileges and roles, Privilege Analysis, Virtual Private Database, Oracle Label Security as well as data confidentiality. This includes Data Redaction, Oracle Data Masking and Subsetting, Transparent Sensitive Data Protection and encryption at the column, tablespace and file levels using Transparent Data Encryption.

Auditing

Throughout this course, you'll also get a chance to discuss auditing using different features, including unified auditing and fine-grained auditing. You'll deep dive into some of the Oracle Network security topics, like securing the listener and restricting connections by IP address.

Gain Hands-On Experience
Hands-on practices and available demonstrations help you learn how to use most of the features of Oracle Database

12c to secure your data center. Develop an understanding of how to use Oracle Enterprise Manager Cloud Control and other tools like SQL*Plus.

Audience

Database Administrators
Network Administrator
Security Administrators
Security Compliance Auditors
Support Engineer
System Analysts

Related Training

Required Prerequisites

Good knowledge of Oracle Database

Suggested Prerequisites
Administer listeners

Create and manage users, roles, and privileges

Perform RMAN backup and recovery

Use Oracle Data Pump export and import

Course Objectives

Ensure data confidentiality using an encryption solution like Transparent Data Encryption, or Data Redaction or Oracle Data Masking and Subsetting

Audit user actions using any of the auditing features like unified auditing

Find appropriate Oracle solutions to meet the security, privacy and compliance requirements of their organization

Find solutions to secure database access through the network

Configure appropriate authentication for the database or enterprise users in the organization

Control data access and integrity in their organization using the appropriate feature or option or product like privileges or Oracle Label Security

Analyze any security risks of their organization

Course Topics

Introduction
Course Objectives

Course Schedule and Appendices

Understanding Security Requirements
Fundamental Data Security Requirements
Security Risks
Exploits
Techniques to Enforce Security

Choosing Security Solutions
Network Access Control
Database Access Control
Data Access Control
Data Confidentiality
Data Integrity
Audit
Compliance

Implementing Basic Database Security
Database Security Checklist
Reducing Administrative Effort
Principle of Least Privilege
Objects Protection

Securing Data on the Network
Network Access Control
Listener Security
Listener Usage Control

Using Basic and Strong User Authentication
Basic Authentication
Strong Authentication
Database Link Passwords Protection

Configuring Global User Authentication
About Enterprise User Management (EUS)
EUS and Oracle Internet Directory Integration

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

Using Privileges and Roles
Separation of Duties
Roles Management
Managing Security for Definer's Rights and Invoker's Rights
Managing RMAN Virtual Private Catalogs

Using Privilege Analysis
Privilege Analysis Flow
Privilege Analysis Implementation

Using Application Contexts

Description of Application Context
Application Context Implementation

Implementing Virtual Private Database
Fine-Grained Access Control and VPD
FGAC Policies Management
VPD Policies Management

Implementing Oracle Label Security
Access Control Overview
Oracle Label Security Registration
Oracle Label Security Policies Management

Redacting Data
Redacting Data
Masking Policies Implementation

Using Oracle Data Masking and Subsetting
Overview
Data Masking Definition Implementation
Data Masking Process
Data Subsetting Process

Using Transparent Sensitive Data Protection
TDPS Implementation

Encryption Concepts and Solutions
Concepts
Solutions
Oracle Solutions

Encrypting with DBMS_CRYPTO Package
Usage

Using Transparent Data Encryption
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

Using Unified Audit
Auditing Overview
Unified Audit Management
Specific Audit Situations

Using Fine-Grained Audit
Comparison with Unified Auditing

Overview
FGA Implementation