Oracle Database 12c: Security

This Database 12c: Security training teaches you how to use Oracle Database features to meet the security, privacy and compliance requirements of your organization. Learn through interactive instruction and hands-on exercises.

Learn To

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.
- 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, 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.

Prerequisites

Suggested Prerequisite

- Perform RMAN backup and recovery
- Use Oracle Data Pump export and import
- Create and manage users, roles, and privileges
- Administer listeners

Required Prerequisite

- Good knowledge of Oracle Database

Audience

- Administrator
- Database Administrator
- Network Administrator
- Security Specialist
- Systems Administrator

Course Objectives

- 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
- Ensure data confidentiality using an encryption solution like Transparent Data Encryption, or Data Redaction or Oracle Data Masking
- Audit user actions using any of the auditing features like unified auditing
- Analyze any security risks of their organization
- Find appropriate Oracle solutions to meet the security, privacy and compliance requirements of their organization

Course Topics

- Introduction
- Understanding Security Requirements
- Choosing Security Solutions
- Implementing Basic Database Security
- Securing Data on the Network
- Using Basic and Strong User Authentication
- Configuring Global User Authentication
- Using Proxy Authentication
- Using Privileges and Roles
- Using Privilege Analysis
- Using Application Contexts
- Implementing Virtual Private Database
- Implementing Oracle Label Security
- Redacting Data
- Using Oracle Data Masking
- Using Transparent Sensitive Data Protection
- Encryption Concepts and Solutions
- Encrypting with DBMS_CRYPTO Package
- Using Transparent Data Encryption
- Database Storage Security
- Using Unified Audit
- Using Fine-Grained Audit

P C I T GmbH
Hohenlindener Straße 1, D- 81677 München
Geschäftsführung: Dipl.-Ing. Maik Pour
HRB 130684, UST-IDNR.: DE207255581

E-Mail: info@pcit.de
Internet: www.pcit.de

Telefon: +49 89 55 239 880
Telefax: +49 89 55 239 887