

## Oracle Database 10g: Security Release 2

**Duration:** 4 Days

### What you will learn

In this course, the students learn how they can use Oracle database features to meet the security and compliance requirements of their organization. The current regulatory environment of the Sarbanes-Oxley Act, HIPPA, the UK Data Protection Act, and others requires better security at the database level. Students learn how to secure their database and how to use the database features that enhance security. The course provides suggested architectures for common problems.

This course explains the security features of the database like auditing, column and file encryption, virtual private database, label security and enterprise user security. Some of the Oracle Network security topics like securing the listener and restricting connections by IP address are also covered.

**Learn To:**

Explain the fundamental security requirements

Manage Wallet manager

Protect sensitive data

Install Label Security

Describe group Policies

### Audience

Database Administrators

Support Engineer

System Analysts

Technical Consultant

### Prerequisites

*Required Prerequisites*

Oracle Database 10g: Administration Workshop I Release 2

*Suggested Prerequisites*

Oracle Database 10g: Administration Workshop I

### Course Objectives

Use basic database security features

Choose a user authentication model

Secure the database and its listener

Use the Enterprise Security Manager tool

Manage users using proxy authentication

Implement Enterprise User Security

Describe the benefits and requirements associated with the Advanced Security Option

- Manage secure application roles
- Implement fine-grain access control
- Manage the Virtual Private Database (VPD)
- Implement fine-grain auditing
- Use Transparent Data Encryption
- Use file encryption
- Encrypting and Decrypt table columns
- Setup a simple Label Security policy

## Course Topics

### Security Requirements

- Security requirements
- Basic Requirements
- Components for enforcing security
- Define Least Privilege
- Enforce Security Policies
- Security in Depth(OS/database/network) Hardening each level

### Security Solutions

- Preventing Exploits (Industry standard practices)
- Data Protection California Breach Law
- Data Access Control HIPPA, UK Data Protection
- Middle-Tier Authentication/Authorization
- Consistent checklist
- Network Wide Authentication

### Internal Database Security

- Installation and patching
- Privileged accounts
- Manage user accounts and privileges

### Database Auditing

- Auditing Users that have Access
- Managing the Audit Trail
- Privileged user auditing (10g NF for 8i DBAs)
- DML and DDL auditing with triggers (Wayne Reeser brown bag) Include autonomous transaction
- Auditing with SYSLOG
- Audit Vault

### Fine-Grained Auditing

- Concepts
- Implementation
- Data dictionary views
- XML Format FGA logs

### Basic User Authentication

- Basic authentication
- Protecting Passwords
- Restricting Remote Database Authentication
- Database Links

## **Strong Authentication**

Example of Strong Authentication

Oracle provided tools

Enable Strong Authentication

Authentication adapters to Kerberos, Radius, et al

Secure External Password Store

External Security Module

## **Enterprise User Security**

Enterprise User Security (EUS) requirements

EUS architecture

EUS vs. version of database

Authenticating enterpriser users

Setup Enterprise User Security

Authorizing Enterprise users

Create Enterprise roles

Creating Enterpriser users using Migration Utility

## **Proxy Authentication**

Security Challenges of Three-tier Computing

Oracle 10g Proxy Authentication Solutions

Proxy Authentication

Data Dictionary Views

Auditing Actions Taken on Behalf of the Real User

Auditing the Real User

## **Authorization Methods**

Discretionary access control

Securing Objects

Secure Application Roles

Data Dictionary Views: APPLICATION\_ROLES

## **Using Application Context**

Tools: PL/SQL Packages

Implementing a Local Context

Accessing the Application Context Globally

Guidelines

Data Dictionary views: \*\_CONTEXT

## **Fine-Grained Access Control**

How Fine-Grained Access Control Works

EXEMPT ACCESS POLICY

Partitioned Fine Grained Access Control

Static vs. Dynamic Policies for Performance

FGAC: Creating a Virtual Private Database Policy: Tools

Implementation

Data Dictionary Views: \*\_POLICIES

## **Installing Label Security**

Label Security: Overview

Access Control

VPD vs. Label Security

How Sensitivity Labels Are Used

Access Mediation

Installing Label Security

Configuring Label Security

Installing Policy Manager

### **Implementing Label Security**

Implement Label Security

Analyze the Needs

Create policies

Create compartments

Setting user authorizations

Administering labels with Policy Manager

Add Labels to Data

Policy Special Privileges

### **Encrypting Data: Concepts**

Principles of Data Encryption

Data Encryption Challenges

Solutions

### **Use Application Based Encryption**

DBMS\_CRYPTO Package (New)

Encrypt

Decrypt

Using MD5, SHA

Guidelines

### **Use Transparent Data Encryption**

Transparent Data Encryption

Benefits of TDE

Using the External security Module

Using TDE

Export and Import with TDE

TDE Restrictions

### **Use File Encryption**

RMAN Encrypted Backups

Encrypted Export Files

Oracle Secure Backup

### **Oracle Net Services Security Checklist**

Overview of Net Services

Overview of firewalls

Network Security Checklist

Authenticate the Client

### **Securing the Listener**

Restrict Network IP addresses

Limit Resource Usage by Unauthorized Connections

Restrict the Privileges of the Listener

Prevent unauthorized administration of the Oracle Listener

- Prevent on-line administration
- Secure External Procedures
- Set listener log and trace file
- Restrict CREATE LIBRARY privileges

### **Using Connection Manager as a Firewall**

- Oracle Connection Manager Overview
- Oracle Connection Manager Architecture and processes
- Starting and stopping Connection Manager
- Access Control with Connection Manager
- Monitor Connection Events Using the CMAN Log File
- Prevent remote administration of the Oracle Connection Manager

### **Securing SQL\*Plus and iSQL\*Plus**

- SQL\*Plus
- iSQL\*plus