Oracle Database 11g: Security Release 2

Duration: 5 Days

What you will learn

In this course, students learn how they can use Oracle Database features 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 their database and how to use the database features that enhance security. The course provides suggested architectures for common problems. This course discusses the following security features of the database: auditing, encryption for Payment Card Industry Data Security Standard (PCI DSS) including encryption at the column, tablespace and file levels, Virtual Private Database, Oracle Label Security and Enterprise User Security. Some of the Oracle Network security topics included are: securing the listener and restricting connections by IP address.

Learn To:
Implement Oracle Database security features to ensure the data is secure
Implement Oracle Database security features to ensure compliance with regulations
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.

Administrator
Database Administrators
Security Administrators
Support Engineer
System Analysts
Technical Administrator

Related Training

Required Prerequisites

Oracle Database 11g: Administration Workshop I
Oracle Database 11g: Administration Workshop I Release 2

Suggested Prerequisites

Oracle Database 11g: Administration Workshop II Release 2
Oracle Database 11g: Administration Workshop II

Course Objectives

Use basic Oracle Database security features
Choose a user authentication model

Secure the database and the listeners
Use the Enterprise Security Manager tool
Manage users using proxy authentication
Implement Enterprise User Security
Describe the benefits and requirements associated with the Oracle Advanced Security option
Manage secure application roles
Implement fine-grained access control
Manage Virtual Private Database
Implement fine-grained auditing
Use Transparent Data Encryption
Use file encryption
Encrypt and decrypt table columns
Set up Oracle Label Security policies

Course Topics

Introduction to Database Security
Fundamental Data Security Requirements
Data Security Concerns
Compliance Mandates
Security Risks
Developing Your Security Policy
Defining a Security Policy
Implementing a Security Policy
Techniques to Enforce Security

Choosing Security Solutions
Maintaining Data Integrity
Protecting Data
Controlling Data Access
Oracle Database Vault Overview
Oracle Audit Vault Overview
Combining Optional Security Features
Compliance Scanner
Enterprise Manager Database Control: Policy Trend

Basic Database Security
Database Security Checklist
Reducing Administrative Effort
Applying Security Patches
Default Security Settings
Secure Password Support
Enforcing Password Management

Protecting the Data Dictionary
System and Object Privileges

Auditing Database Users, Privileges, and Objects
Monitoring for Suspicious Activity
Standard Database Auditing
Setting the AUDIT_TRAIL
Specifying Audit Options
Viewing Auditing Options
Auditing the SYSDBA Users
Audit to XML Files
Value-Based Auditing

Auditing DML Statements
Fine-Grained Auditing (FGA)
Using the DBMS_FGA Package
FGA Policy
Triggering Audit Events
Data Dictionary Views
DBA_FGA_AUDIT_TRAIL
Enabling and Disabling an FGA Policy
Maintaining the Audit Trail

Using Basic User Authentication
User Authentication
Protecting Passwords
Creating Fixed Database Links
Encrypting Database Link Passwords
Using Database Links without Credentials
Using Database Links and Changing Passwords
Auditing with Database Links
Restricting a Database Link with Views

Using Strong Authentication
Strong Authentication
Single Sign-On
Public Key Infrastructure (PKI) Tools
Configuring SSL on the Server
Certificates
Using the orapki Utility
Using Kerberos for Authentication
Configuring the Wallet

Using Enterprise User Security
Enterprise User Security
Oracle Identity Management Infrastructure: Default Deployment
Oracle Database: Enterprise User security Architecture

Oracle Internet Directory Structure Overview
Installing Oracle Application Server Infrastructure
Managing Enterprise User Security
Creating a Schema Mapping Object in the Directory
Creating a Schema Mapping Object in the Directory

Using Proxy Authentication
Security Challenges of Three-Tier Computing
Common Implementations of Authentication
Restricting the Privileges of the Middle Tier
Authenticating Database and Enterprise Users
Using Proxy authentication for Database Users
Proxy Access through SQL*Plus
Revoking Proxy Authentication
Data Dictionary Views for Proxy Authentication

Using Privileges and Roles
Authorization
Privileges
Benefits of Roles
CONNECT Role Privileges
Using Proxy Authentication with Roles
Creating an Enterprise Role
Securing Objects with Procedures
Securing the Application Roles

Access Control
Description of Application Context
Using the Application Context
Setting the Application Context
Application Context Data Sources
Using the SYS_CONTEXT PL/SQL Function
PL/SQL Packages and Procedures
Implementing the Application Context Accessed Globally
Data Dictionary Views

Implementing Virtual Private Database
Understanding Fine-Grained Access Control
Virtual Private Database (VPD)
How Fine-Grained Access Control Works
Using DBMS_RLS
Exceptions to Fine-Grained Access Control Policies
Implementing a VPD Policy
Implementing Policy Groups
VPD Best Practices

Oracle Label Security Concepts
Access Control: Overview
Discretionary Access Control
Oracle Label Security
How Sensitivity Labels are used
Installing Oracle Label Security
Oracle Label Security Features
Comparing Oracle Label Security and VPD
Analyzing Application Needs

Implementing Oracle Label Security
Implementing the Oracle Label Security Policy
Creating Policies
Defining Labels Overview
Defining Compartments
Identifying Data Labels
Access Mediation
Adding Labels to Data
Assigning User Authorization Labels

Using the Data Masking Pack
Understanding Data Masking
Data Masking Pack Features
Identifying Sensitive Data for Masking
Types of Built-in Masking Primitives and Routines
Data Masking of the EMPLOYEES Table
Implementing a Post-Processing Function
Viewing the Data Masking Impact Report
Creating an Application Masking Template by Exporting Data Masking Definitions

Encryption Concepts
Understanding Encryption
Problems that Encryption Solves
Encryption is not Access Control
What to Encrypt
Data Encryption Challenges
Storing the Key in the Database
Letting the User Manage the Key
Storing the Key in the Operating System

Using Application-Based Encryption
DBMS_CRYPTO Package Overview
Using the DBMS_CRYPTO Package
Generating Keys Using RANDOMBYTES
Using ENCRYPT and DECRYPT
Enhanced Security Using the Cipher Block Modes
Hash and Message Authentication Code

Applying Transparent Data Encryption
Transparent Data Encryption (TDE)
Creating the Master Key
Opening the Wallet
Using Auto Login Wallet
Resetting (Rekeying) the Unified Master Encryption Key ** 11.2 **
Using Hardware Security Modules
TDE Column Encryption Support
Creating an Encrypted Tablespace

Applying File Encryption
RMAN Encrypted Backups
Oracle Secure Backup Encryption
Creating RMAN Encrypted Backups
Using Password Mode Encryption
Restoring Encrypted Backups
Data Pump Encryption
Using Dual Mode Encryption
Encrypting Dump Files

Oracle Net Services: Security Checklists
Overview of Security Checklists
Securing the Client Computer
Configuring the Browser
Network Security Checklist
Using a Firewall to Restrict Network Access
Restricting Network IP Addresses: Guidelines
Configuring IP Restrictions with Oracle Net Manager
Configuring Network Encryption

Securing the Listener
Listener Security Checklist
Restricting the Privileges of the Listener
Moving the Listener to a Non default Port
Preventing Online Administration of the Listener
Using the INBOUND_CONNECT_TIMEOUT Parameter
Analyzing Listener Log Files
Administering the Listener Using TCP/IP with SSL
Setting Listener Logging Parameters

Related Courses

Oracle Database 11g: Security