Oracle Database 11g: Security

Duration: 5 Days

What you will learn

In Oracle Database 11g: Security 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 covers 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, label security and enterprise user security. Some of the Oracle Network security topics covered are: securing the listener and restricting connections by IP address.

Learn To:

- Identify business security requirements
- Set up security policies
- Implement access control
- Manage user authentication

Database Administrators
Security Administrators
Security Compliance Auditors
Security Compliance Professionals

Related Training

* Suggested Prerequisites
  Oracle Database 11g: Implement Database Vault

Oracle Database 11g: Implement Database Vault Release 2

Oracle Database 11g: Implementing Database Vault

Course Objectives

- Use database security features
- Secure the database and its listener
- Manage users using proxy authentication
Manage secure application roles
Implement fine-grain access control
Implement fine-grain auditing
Use Transparent Data Encryption

Course Topics

Security Requirements
Data Security Concerns
Fundamental Data Security Requirements
Components for enforcing security
Security Risks: Internal, External, Sabotage, Recovery
Principle of Least Privilege
Defining a Security policy
Implementing a Security Policy

Choosing Security Solutions
Maintaining data integrity
Controlling data access
Data Protection
Database Vault overview
Audit Vault overview
Combining Optional Security Features
Compliance Scanner
Database Control: Policy Trend

Basic Database Security
Database Security Checklist
Installing only what is required
Applying Security Patches
11g Default security settings
Enforcing Password Management
System and Object Privileges
Restricting the Directories Accessible by the User
Separation of Responsibilities

Database Auditing
Standard Database Auditing
Monitoring for Suspicious Activity
Audit Log Location Options
Viewing Auditing Results
Configure Auditing to syslog
Value-Based Auditing
Triggers and Autonomous Transactions

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

Basic User Authentication
User Authentication
User Identified by a Password
User Identified Externally
Protecting Passwords
Encrypted Database Link Passwords
Audit with Database Links

Using Strong Authentication
Strong User Authentication
Single Sign-On
How to Use Certificates for Authentication
Configuring SSL
orapki Utility
How to Use Kerberos for Authentication
RADIUS Authentication: Overview
External Secure Password Store

Enterprise User Security
Setting up Enterprise User Security
Oracle Identity Management Infrastructure: Default Deployment
Oracle Database: Enterprise User Security Architecture
Authenticating Enterprise Users
User Migration Utility
Enterprise-User Auditing

Proxy Authentication
Security Challenges of Three-Tier Computing
Common Implementations of Authentication
Restrict the Privileges of the Middle Tier
Using Proxy Authentication for Database Users
Using Proxy Authentication for Enterprise Users
Revoking Proxy Authentication
Data Dictionary Views for Proxy Authentication

Authorization Methods
Authorization
Assigning Privileges
Using Enterprise roles
Implementing a Secure Application Role

Using Application Context
Application Context Overview
Implementing a Local Context
Application Context Accessed Globally
Guidelines

Implementing Virtual Private Database
Understanding Fine Grain Access Control
Virtual Private Database
Implementing VPD Policies
Manage VPD Policies
Policy Performance
Checking for Policies Applied to SQL Statements

Oracle Label Security Concepts
Access Control: Overview
Discretionary Access Control
Oracle Label Security
Comparing Oracle Label Security and the VPD

Implementing Oracle Label Security
Policy Enforcement Options
Managing levels, groups, compartments
Administering Labels
Trusted Stored Package Units
Performance tips

Using the Data Masking Pack
Understanding Data Masking
Identifying Sensitive Data for Masking
Implementing Data Masking
Data Masking Impact Report

Encryption Concepts
Understanding encryption
Cost of encryption
Encryption is not Access Control
Data Encryption Challenges
Encryption Key Management
Solutions and examples

Using Application Based Encryption
Overview
The DBMS_CRYPTO Package
Generate 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 overview
Components of Data Encryption
Using Data Encryption
Using Hardware Security Modules
Tablespace Encryption
Use File Encryption
RMAN Encrypted Backups
Oracle Secure Backup Encryption
Using Transparent Mode Encryption
  Using Password Mode Encryption
Using Dual Mode Encryption
Restoring encrypted backups

Oracle Net Services Security Checklist
Security Checklists Overview
Client Checklist
Network Security Checklist
Restricting Network IP Addresses
Restricting Open Ports
Encrypting Network Traffic
Configure Checksumming
Oracle Net Services Log Files

Securing the Listener
Listener Security Checklist
Restricting the Privileges of the Listener
Password Protect the Listener
Administering the Listener Using TCP/IP with SSL
Analyzing Listener Log Files