Oracle Database 19c: Security Fundamentals LVC

Oracle Database

DURATION	MODULES	COURSE CODE
1 Days	5 Lectures	—

Course Overview

The course covers the following topics: Security Overview Managing Database Users Securing Passwords Managing Authorization Securing Oracle Net

What You Will Learn

- I Module Overview
- Security Modules I-2
- Security Course 1 – Security Fundamentals I-3
- Security Course 2 – Data Confidentiality I-5
- Security Course 3 – Data Encryption I-7
- Security Course 4 – Monitoring and Maintaining a Secure Environment I-8

Security Overview

- Objectives
- The Value of Information
- Need for Security
- Security Risks
- Typical Attack Points for a Database
- Preventing Exploits
- Developing Your Security Policy
- Defining a Security Policy
- Implementing a Security Policy
- Maximum Security Architecture Overview
- Summary
- Practice 1: Overview

User Administration, Authentication, and Authorization

- Objectives

- Local Users
- Common Users Versus Local Users
- Profiles and Users
- Profile Parameters: Locking and Passwords
- Passwords and Password Verifiers
- Schema-Only Users
- Proxy Users
- Externally Authenticated Users
- OS Authentication
- Kerberos Authentication
- Radius Authentication
- PKI Certificate Authentication
- Certificates
- Enterprise User Security
- Oracle Identity Management Software
- Directory Structure: Overview
- Oracle Database: Enterprise User Security Architecture
- Authenticating Enterprise Users
- Enterprise Users
- Configuring Enterprise User Security
- Identifying the Enterprise User
- Enabling Current User Database Links
- Using Enterprise Roles
- User Migration Utility
- Enterprise-User Auditing
- Quiz
- Centrally Managed Users
- Account Management: Lock and Unlock Accounts
- Account Management: Expire Passwords
- Account Management: Identify Inactive Accounts
- Summary
- Practice 2: Overview

Securing Passwords

- Objectives
- Protecting Passwords
- Using a Secure External Password Store to Secure Passwords
- Designing Applications to Securely Handle Passwords
- Securely Handling Passwords in Scripts
- Managing the Database Password File
- Password File Improvements
- Password File Migration
- Password File Vulnerabilities
- Summary
- Practice 3: Overview

Authorization

- Objectives
- Concept of Least Privilege
- Privileges
- System Privileges
- Granting and Revoking System Privileges
- Object Privileges
- Granting and Revoking Object Privileges
- Administrative Privileges
- Roles
- Default and Non-Default Roles
- Secure Application Roles
- Implementing a Secure Application Role
- Privilege Analysis
- Privilege Analysis Flow
- Used Privileges Results
- Compare Used and Unused Privileges
- Listing Captures
- Dropping an Analysis
- PDB Lockdown Profiles
- Restricting Operations in a PDB Lockdown Profile
- PDB Lockdown Profiles Inheritance
- Static and Dynamic PDB Lockdown Profiles
- Summary
- Practice 4: Overview

Network Security

- Objectives
- Network Access Control for External Services
- How Do Network ACLs Relate to Microservice Deployments
- Using ACLs To Access Passwords in a Wallet
- Listener Valid Node Checking
- Network Service Profiles
- SEC_USER_UNAUTHORIZED_ACCESS_BANNER
- SEC_USER_AUDIT_ACTION_BANNER
- FALLBACK_AUTHENTICATION
- ALLOWED_LOGON_VERSION_CLIENT
- ALLOWED_LOGON_VERSION_SERVER
- Restricting Network IP Addresses: Valid Node Checking
- Enhancing Database Communication Security
- SEC_PROTOCOL_ERROR_TRACE_ACTION
- SEC_PROTOCOL_ERROR_FURTHER_ACTION
- SEC_MAX_FAILED_LOGIN_ATTEMPTS
- SEC_RETURN_SERVER_RELEASE_BANNER
- Summary

- Practice 5: Overview