Oracle Database 19c: Security Fundamentals

Course Duration: 8 Hours **Course code: 19cSFC**

1. Course Overview

This course introduces the fundamental concepts and practices of database security in Oracle Database 19c. Participants will learn how to implement user and privilege management, secure database objects, configure auditing, protect sensitive data with encryption, and enforce access control policies. It provides both theoretical and hands-on experience to help administrators understand threats, compliance requirements, and Oracle's security technologies. By the end of the course, learners will be able to apply best practices to secure an Oracle Database environment against internal and external risks.

2. What you'll learn?

By the end of this course, you should be able to:

- Describe Oracle Database 19c security architecture and features
- Implement user authentication, roles, and privilege management
- Secure database objects with authorization controls
- Configure database auditing for compliance and monitoring
- Use encryption technologies for data at rest and in transit
- Apply Virtual Private Database (VPD) and Label Security policies
- Implement Data Redaction and Transparent Data Encryption (TDE)
- Apply best practices for securing Oracle Database environments

3. Target Audience

- Database Administrators (DBAs)
- Security Administrators
- IT Professionals responsible for data protection and compliance
- Professionals preparing for Oracle Security certifications

4. Pre-Requisites

Familiarity with:

- Oracle Database Administration (basic to intermediate)
- SQL and PL/SQL
- General concepts of data security

5. Course content

Module 1: Course Introduction

- Introduction
- Course contents

Module 2: Oracle Database Security Overview

- Security threats and challenges
- Oracle security architecture
- Key Oracle Database 19c security features

Module 3: User and Privilege Management

- Creating and managing users
- System and object privileges
- Roles and role-based security
- Password policies and profiles

Module 4: Securing Database Objects

- Authorization and access control
- Schema object privileges
- Best practices for privilege assignment

Module 5: Auditing in Oracle Database 19c

- Unified auditing architecture
- Standard auditing vs. fine-grained auditing
- Configuring and managing audit policies

- Monitoring audit data

Module 6: Data Encryption and Protection

- Transparent Data Encryption (TDE) for data at rest
- Network encryption for data in transit
- Wallet and keystore management

Module 7: Advanced Access Controls

- Virtual Private Database (VPD)
- Oracle Label Security
- Row-level and column-level security

Module 8: Protecting Sensitive Data

- Data Redaction techniques
- Masking sensitive information
- Compliance use cases (GDPR, HIPAA, etc.)

Module 9: Database Security Best Practices

- Security assessments and baselines
- Least privilege principle
- Security patches and updates

Module 10: Case Studies and Wrap-Up

- Real-world security scenarios
- Troubleshooting common security issues
- Summary and Q&A