

Oracle Database 19c: Data Encryption

Course Duration: 8 Hours

Course code:19c data Encryption

1. Course Overview

This course provides comprehensive training on encrypting data in Oracle Database 19c. Participants will learn to implement Transparent Data Encryption (TDE), column-level encryption, and network encryption to ensure data is secure both at rest and in transit. The course emphasizes hands-on exercises, real-world scenarios, and best practices for protecting sensitive information and meeting compliance requirements.

2. What you'll learn?

By the end of this course, participants will be able to:

- Explain the concepts and importance of data encryption
- Implement Transparent Data Encryption (TDE) for tablespaces and columns
- Manage encryption keys and wallets
- Encrypt data in transit using network encryption (SSL/TLS)
- Integrate encryption with Oracle Backup and Recovery strategies
- Monitor and troubleshoot encryption configurations
- Follow industry best practices for securing data

3. Target Audience

- Database Administrators (DBAs)
- Security Administrators
- IT Professionals responsible for data protection
- Developers designing secure Oracle Database applications

4. Pre-Requisites

Familiarity with:

- Oracle Database 19c architecture and administration

- Basic SQL and PL/SQL
- Security concepts and role-based access control

5. Course content

Module 1: Course Introduction

- Introduction
- Course Contents

Module 2: Introduction to Data Encryption

- Importance of Data Encryption
- Data Encryption at Rest vs. Data in Transit
- Regulatory Compliance Requirements (GDPR, HIPAA, etc.)

Module 3: Transparent Data Encryption (TDE)

- Overview of TDE
- Tablespace Encryption
- Column-Level Encryption
- Configuring and Managing TDE Wallets
- Key Management and Rotation

Module 4: Network Encryption

- Overview of Oracle Net Encryption
- Configuring SSL/TLS for Client-Server Communication
- Best Practices for Network Security

Module 5: Backup and Recovery with Encrypted Data

- Encrypted Backup Configurations
- RMAN and TDE Integration
- Restoring and Recovering Encrypted Data

Module 6: Monitoring and Troubleshooting Encryption

- Monitoring TDE and Network Encryption
- Common Errors and Solutions
- Performance Considerations

Module 7: Advanced Encryption Features

- Column-Level Encryption Best Practices
- Integration with Oracle Data Guard and RAC
- Multi-tenant Database Encryption Considerations

Module 8: Hands-On Labs and Exercises

- Implementing TDE for Tablespaces and Columns
- Configuring SSL/TLS Network Encryption
- Key Management and Rotation Scenarios
- Backup and Recovery with Encrypted Data

Module 9: Security Best Practices

- Data Encryption Strategy Checklist
- Integrating Encryption with Overall Database Security
- Compliance Reporting

Module 10: Wrap-Up and Next Steps

- Summary of Data Encryption Techniques
- Checklist for Secure Database Deployment
- Q&A and Further Learning Paths