Oracle Database 19c: Data Confidentiality

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

1. Course Overview

This course provides comprehensive knowledge on securing sensitive data in Oracle Database 19c. Participants will learn to implement encryption, masking, auditing, and access controls to ensure data confidentiality. The course emphasizes practical exercises and real-world scenarios to safeguard data from unauthorized access, both at rest and in transit.

2. What you'll learn?

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

- Understand data confidentiality concepts and compliance requirements
- Implement Transparent Data Encryption (TDE) for database files and columns
- Configure Data Redaction to hide sensitive information
- Apply Database Vault for fine-grained access control
- Implement Oracle Label Security (OLS) for classification-based access
- Configure auditing and monitoring to detect unauthorized access
- Follow best practices for securing sensitive data

3. Target Audience

- Database Administrators (DBAs)
- Security Administrators
- IT Professionals responsible for data privacy and compliance
- Developers implementing secure applications on Oracle Database

4. Pre-Requisites

Familiarity with:

- Oracle Database 19c architecture and administration
- Basic SQL and PL/SQL

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Security concepts and role-based access control

5. Course content

Module 1: Course Introduction

- Introduction
- Course Contents

Module 2: Introduction to Data Confidentiality

- Importance of Data Confidentiality
- Regulatory Compliance (GDPR, HIPAA, etc.)
- Threats to Data Security

Module 3: Transparent Data Encryption (TDE)

- Overview of TDE
- Configuring TDE for Tablespaces and Columns
- Managing Encryption Keys
- Best Practices and Performance Considerations

Module 4: Data Redaction

- Overview of Data Redaction
- Types of Redaction Policies
- Implementing and Testing Redaction Policies

Module 5: Oracle Database Vault

- Introduction to Database Vault
- Creating Realms and Command Rules
- Implementing Separation of Duties
- Monitoring and Managing Database Vault

Module 6: Oracle Label Security (OLS)

- Overview of OLS

- Defining Security Policies and Labels
- Label-Based Access Control
- Integration with Applications

Module 7: Auditing and Monitoring

- Standard and Fine-Grained Auditing
- Configuring Unified Auditing
- Monitoring Unauthorized Access Attempts
- Reporting and Compliance Checks

Module 8: Data Masking and Subsetting

- Overview of Data Masking Techniques
- Masking Sensitive Data in Non-Production Environments
- Tools and Best Practices

Module 9: Securing Data in Transit

- Network Encryption with Oracle Net
- SSL/TLS Configuration for Oracle Database
- Best Practices for Client-Server Security

Module 10: Security Best Practices

- Role-Based Access Control (RBAC)
- Password Policies and User Management
- Securing Backups and Exports

Module 11: Hands-On Labs and Exercises

- Implementing TDE and Redaction
- Configuring Database Vault and OLS
- Setting Up Auditing and Monitoring

Module 12: Wrap-Up and Next Steps

- Summary of Data Confidentiality Techniques

- Checklist for Secure Database Deployment
- Q&A and Further Learning Paths

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com