

Oracle Database 19c: Data Confidentiality LVC

Oracle Database

DURATION

1 Days

MODULES

6 Lectures

COURSE CODE

—

Course Overview

The course covers the following topics: Application Contexts Virtual Private Database Oracle Label Security Data Masking Data Redaction Real Application Security

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

Application Contexts

- Learning Objectives
- Using the Application Context
- Creating Application Contexts
- Application Context Data Sources
- Viewing Application Context Information
- USERENV Namespace
- Using SYS_CONTEXT Function
- Application Context Accessed Globally
- SYS_LDAP_USER_DEFAULT Namespace
- Set Client Identifier to Identify the User of a Session
- APEX\$SESSION Namespace
- Extending Unified Auditing with Context information
- Application Context Usage Guidelines
- Summary
- Practice 1: Overview

Virtual Private Database

- Learning Objectives
- Access Control: Overview
- Fine-Grained Access Control: Overview
- Understanding FGAC Policy Execution
- Benefits of Using Fine-Grained Access Control
- Virtual Private Database
- Examples of VPD
- Using DBMS_RLS to Manage Policies
- Column-Level VPD
- Policy Types: Overview
- Designing and Implementing a VPD Solution
- Implementing a VPD Policy
- Writing a Function That Returns Different Predicates
- Exceptions to VPD Policies
- Quiz
- Guidelines for Policies and Context
- Policy Performance
- Export and Import
- Policy Views
- Summary
- Practice 2: Overview

Oracle Label Security

- Learning Objectives
- Access Control: Overview
- OLS: Overview
- Oracle Label Security
- Enabling and Managing OLS
- Quiz
- OLS and VPD Comparison
- Analyzing Application Requirements
- Implementing an OLS Solution
- Creating Policies with Enforcement Options
- Define Labels
- Assign User Authorization Labels
- Apply the Policy to a Table
- Adding Labels to Data
- Access Mediation
- Quiz
- OLS Special User Privileges
- Example: READ Privilege
- Example: FULL Privilege
- Example: COMPACCESS Privilege

- Using the PROFILE_ACCESS Privilege
- Trusted Stored Package Units
- Exporting and Importing with OLS
- Performance Tips
- Summary
- Practice 3: Overview

Data Masking

- Learning Objectives
- Data Masking: Dynamic Data Masking Vs. Static Data Masking
- Enterprise Manager Data Masking Pack (Static Data Masking)
- Inside the Application Data Model
- Starting an ADM job
- Viewing ADM Content
- Discovering Sensitive Columns
- Create the Sensitive Column Discovery Job
- Marking Sensitive Columns
- ADM Maintenance
- Inside Data Masking Format Library
- Creating or Using Masking Formats
- Using Oracle-Supplied Mask Formats and Built-in Masking Routines
- Creating a Masking Format Using a User Defined Function
- Example: Data Masking of the EMPLOYEES Table
- Inside the Data Masking Definition
- Creating Data Masking Definitions
- Importing Formats and Modifying Properties
- Using Condition-Based Masking
- Using Compound Masking
- Using a User-Defined Masking Function and Post-Processing Masking Function
- Generating the Data Masking Script
- Creating an Application Masking Template
- Controlling Data Masking Operations
- Data Masking Definition Maintenance
- In-Database versus At-Source Execution
- Automating Masking Operations with EMCLI
- Benefits of TSDP
- TSDP
- Audit Vault and Database Firewall: Data Privacy Reports
- Summary
- Practice 4: Overview

Data Redaction

- Learning Objectives
- Data Masking: Dynamic Data Masking Vs. Static Data Masking
- Oracle Data Redaction (Dynamic Data Masking)

- Oracle Data Redaction and Operational Activities
- Available Redaction Methods
- Oracle Data Redaction: Examples
- What Is a Redaction Policy?
- Managing Redaction Policies
- Defining a Redaction Policy
- Adding a Redaction Policy to a Table or View
- Full Redaction: Examples
- Partial Redaction: Examples
- Regular Expression
- Modifying the Redaction Policy
- Exempting Users from Redaction Policies
- Summary
- Practice 5: Overview

Real Application Security

- Learning Objectives
- Access Control: Overview
- Real Application Security: Overview
- Traditional Database Security
- Advantages of Real Application Security
- Oracle Database Real Application Security
- Architecture of Real Application Security Model
- Components of Real Application Security
- User and Role Model
- Application Session
- Authorization Service
- Data Realms
- Data Security
- Data Security Policy
- Access Control
- Analyzing Application Needs
- Using XS Packages
- RASADM Tool
- Summary
- Practice 6: Overview