ORACLE

Oracle Database 19c: Data Confidentiality

Titulo: Oracle Database 19c: Data Confidentiality

Clave: D11011118GC10

Duración: 01 día 8/hrs

Temario:

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

1 Application Contexts
Learning Objectives 1-2
Using the Application Context 1-3
Creating Application Contexts 1-4
Application Context Data Sources 1-5
Viewing Application Context Information 1-7
USERENV Namespace 1-8
Using SYS_CONTEXT Function 1-9
Application Context Accessed Globally 1-10
SYS_LDAP_USER_DEFAULT Namespace 1-12
Set Client Identifier to Identify the User of a Session 1-13
APEX$SESSION Namespace 1-14
Extending Unified Auditing with Context information 1-15
Application Context Usage Guidelines 1-16
Summary 1-18
Practice 1: Overview 1-19

2 Virtual Private Database
Learning Objectives 2-2
Access Control: Overview 2-3
Fine-Grained Access Control: Overview 2-4
Understanding FGAC Policy Execution 2-5
Benefits of Using Fine-Grained Access Control 2-7
Virtual Private Database 2-8

Examples of VPD 2-9
Using DBMS_RLS to Manage Policies 2-10
Column-Level VPD 2-11
Policy Types: Overview 2-12
Designing and Implementing a VPD Solution 2-13
Implementing a VPD Policy 2-14
Writing a Function That Returns Different Predicates 2-15
Exceptions to VPD Policies 2-16
Quiz 2-17
Guidelines for Policies and Context 2-18
Policy Performance 2-20
Export and Import 2-22
Policy Views 2-23
Summary 2-24
Practice 2: Overview 2-25

3 Oracle Label Security
Learning Objectives 3-2
Access Control: Overview 3-3
OLS: Overview 3-4
Oracle Label Security 3-6
Enabling and Managing OLS 3-7
Quiz 3-8
OLS and VPD Comparison 3-9
Analyzing Application Requirements 3-10
Implementing an OLS Solution 3-11
Creating Policies with Enforcement Options 3-13
Define Labels 3-15
Assign User Authorization Labels 3-17
Apply the Policy to a Table 3-19
Adding Labels to Data 3-20
Access Mediation 3-21
Quiz 3-22
OLS Special User Privileges 3-23
Example: READ Privilege 3-24
Example: FULL Privilege 3-25
Example: COMPACCESS Privilege 3-26
Using the PROFILE_ACCESS Privilege 3-27
Trusted Stored Package Units 3-28
Exporting and Importing with OLS 3-29

Performance Tips 3-30
Summary 3-31
Practice 3: Overview 3-32
4 **Data Masking**
Learning Objectives 4-2
Data Masking: Dynamic Data Masking Vs. Static Data Masking 4-3
Enterprise Manager Data Masking Pack (Static Data Masking) 4-4
Inside the Application Data Model 4-5
Starting an ADM job 4-6
Viewing ADM Content 4-7
Discovering Sensitive Columns 4-8
Create the Sensitive Column Discovery Job 4-9
Marking Sensitive Columns 4-10
ADM Maintenance 4-11
Inside Data Masking Format Library 4-12
Creating or Using Masking Formats 4-13
Using Oracle-Supplied Mask Formats and Built-in Masking Routines 4-14
Creating a Masking Format Using a User Defined Function 4-15
Example: Data Masking of the EMPLOYEES Table 4-16
Inside the Data Masking Definition 4-17
Creating Data Masking Definitions 4-18
Importing Formats and Modifying Properties 4-19
Using Condition-Based Masking 4-20
Using Compound Masking 4-21
Using a User-Defined Masking Function and Post-Processing Masking Function 4-22
Generating the Data Masking Script 4-23
Creating an Application Masking Template 4-24
Controlling Data Masking Operations 4-25
Data Masking Definition Maintenance 4-26
In-Database versus At-Source Execution 4-27
Automating Masking Operations with EMCLI 4-28
Benefits of TSDP 4-29
TSDP 4-30
Audit Vault and Database Firewall: Data Privacy Reports 4-31
Summary 4-32
Practice 4: Overview 4-33

5 Data Redaction
Learning Objectives 5-2
Data Masking: Dynamic Data Masking Vs. Static Data Masking 5-3
Oracle Data Redaction (Dynamic Data Masking) 5-4
Oracle Data Redaction and Operational Activities 5-5
Available Redaction Methods 5-6
Oracle Data Redaction: Examples 5-7
What Is a Redaction Policy? 5-8
Managing Redaction Policies 5-9
Defining a Redaction Policy 5-10
Adding a Redaction Policy to a Table or View 5-11
Full Redaction: Examples 5-12
Partial Redaction: Examples 5-13
Regular Expression 5-15
Modifying the Redaction Policy 5-16
Exempting Users from Redaction Policies 5-17
Summary 5-18
Practice 5: Overview 5-19

6 Real Application Security
Learning Objectives 6-2
Access Control: Overview 6-3
Real Application Security: Overview 6-4
Traditional Database Security 6-5
Advantages of Real Application Security 6-6
Oracle Database Real Application Security 6-7
Architecture of Real Application Security Model 6-8
Components of Real Application Security 6-9
User and Role Model 6-10
Application Session 6-12
Authorization Service 6-13
Data Realms 6-14
Data Security 6-15
Data Security Policy 6-16
Access Control 6-17
Analyzing Application Needs 6-18
Using XS Packages 6-19
RASADM Tool 6-21
Summary 6-22
Practice 6: Overview 6-23