Oracle Database 19c: Monitoring and Maintaining a Secure Environment

Titulo: Oracle Database 19c: Monitoring and Maintaining a Secure Environment

Clave: S106124GC10

Duración: 01 día /8hrs

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 Auditing

Learning Objectives 1-2
Default, Privileged User, and Standard Audit 1-3
Fine Grained Audit (FGA) 1-4
FGA Policy 1-5
Triggering Audit Events 1-7
Data Dictionary Views 1-8
Unified Audit Implementation 1-9
DBA_FGA_AUDIT_TRAIL/UNIFIED_AUDIT_TRAIL 1-10
Security and Performance: Audit Architecture 1-11
Tolerance Level for Loss of Audit Records 1-12
Consolidation: Unique Audit Trail 1-13
Basic Audit Versus Extended Audit Information 1-14
Extended Audit Information 1-15
Data Pump Audit Policy 1-16
Oracle RMAN Audit Information 1-17
Extending Unified Auditing with Context information 1-18
Introducing Oracle Audit Vault and Database Firewall 1-19
Database Auditing and Activity Monitoring 1-20
Oracle AVDF Components 1-22
Oracle Audit Vault and Database Firewall Architecture 1-23
Audit Collection: Supported Secured Target Types 1-24
Configuring Network Firewalls to Enable Audit Vault and Database Firewall Deployment 1-25

Oracle AVDF Administrator Tasks 1-26
Oracle AVDF Auditor Tasks 1-27
Summary 1-28
Practice 1: Overview 1-29

2 Database Vault
Learning Objectives 2-2
Database Vault 2-3
Default Separation of Duties with Database Vault 2-4
Privileges That Are Revoked from Existing Users and Roles 2-5
Privileges That Are Prevented for Existing Users and Roles 2-6
Oracle Database Vault Roles 2-7
What Is a Realm? 2-8
Benefits of Using Realms 2-9
Effect of Realms on Nonmembers 2-10
Mandatory Realms and Object Privileges 2-11
Protecting with a Mandatory Realm 2-12
Characteristics of Mandatory Realms 2-13
Benefits of Mandatory Realms 2-14
Database Vault Factors, Rules, and Rule Sets 2-15
What Is a Command Rule? 2-16
What Is a Rule Set? 2-17
Database Vault Command Rules 2-18
How Realms and Command Rules Work Together 2-19
Protecting Roles 2-20
Protecting Sensitive Data During Patching 2-22
Protecting Objects from DBAs 2-23
Protecting Sensitive Data During Run Time 2-24
Tasks Involving Realms 2-25
Realm Attributes 2-26
Realm Views 2-27
Oracle-Defined Realms 2-29
Predefined Reports 2-30
Evaluation of Rule Sets 2-31
Using Rule Sets 2-32
Oracle-Defined Rule Sets 2-33
Creating and Maintaining Rules 2-34
Rule Set Tasks 2-35

Auditing Rule Sets 2-36
Setting a Custom Event Handler 2-37
Using Rule Sets with Realms 2-38
Rule Set Reports 2-39
Rule Set Views 2-40
Rule Set API 2-41
Command Rules 2-42
Use Case 2-43
Scope of Command Rules 2-45
Disallowing ALTER TABLE in a Schema 2-46
Delivered Command Rules 2-47
Reports and Views 2-48
Command Rule API 2-49
Database Vault Operations Control 2-50
Database Vault Operations Control: Allowing Operations 2-51
Database Vault Operations Control: Granting the DV_OWNER Role 2-52
Database Vault Operations Control: Setting an Exception List 2-53
Summary 2-54
Practice 2: Overview 2-55

3 Database Security Assessment Tool
Learning Objectives 3-2
Database Security Assessment Tool (DBSAT) 3-3
DBSAT Components – Collector and Reporter 3-4
DBSAT Components – Discoverer 3-5
Install DBSAT 3-6
Collect Data Using Collector 3-7
Generate the Database Security Assessment Report Using Reporter 3-8
View the Database Security Assessment Report 3-9
View the Database Security Assessment Report – Basic Information 3-11
View the Database Security Assessment Report – Auditing 3-12
View the Database Security Assessment Report – Operating System 3-13
Discover Sensitive Data – Configure the Discoverer 3-14
Discover Sensitive Data – Define Search Patterns for the Discoverer 3-15
Discover Sensitive Data – Discover Sensitive Data 3-16
Database Sensitive Data Assessment Report – Summary 3-17
Database Sensitive Data Assessment Report – Sensitive Data 3-18
Database Sensitive Data Assessment Report – Tables Detected within Sensitive

Category 3-19
Database Sensitive Data Assessment Report – Schema View 3-20
Summary 3-21
Practice 3: Overview 3-22

4 Database Patching
Learning Objectives 4-2
Difference Between RU and RUR 4-3
Types of Patches 4-4
Critical Patch Updates (CPUs) 4-5
What is a CVE? 4-6
Decoding the CVSS Risk Scoring 4-7
Lifetime Support Policy 4-8
Overview of the Patch Process 4-9
Oracle Patching Tools: opatch 4-10
Oracle Patching Tools: OPatch Auto 4-11
OPatch Automation: Examples 4-12
Minimizing Down Times: Rolling Patching 4-13
Minimizing Down Times: Standby-First Patching 4-14
Minimizing Down Times: Patching a Cloned Home 4-15
Queryable Patch Inventory 4-16
Alternative Methods of Patching 4-17
Client Patching 4-18
Summary 4-19
Practice 4: Overview 4-20

5 Database Security in the Cloud
Learning Objectives 5-2
Autonomous Database "Self-Securing" 5-3
Self-securing Capabilities 5-4
Hybrid Cloud Scenarios 5-5
Shared Responsibility Model Between Oracle and You 5-6
Summary 5-7
Practice 5: Overview 5-8