



Oracle Database 19c: Security Fundamentals

Titulo: Oracle Database 19c: Security Fundamentals

Clave: D1101117GC10

Duración: 01 día 8/hrs

I Module Overview

Security Modules 1-2

Security Course 1 – Security Fundamentals 1-3

Security Course 2 – Data Confidentiality 1-5

Security Course 3 – Data Encryption 1-7

Security Course 4 – Monitoring and Maintaining a Secure Environment 1-8

1 Security Overview

Objectives 1-2

The Value of Information 1-3

Need for Security 1-4

Security Risks 1-6

Typical Attack Points for a Database 1-8

Preventing Exploits 1-10

Developing Your Security Policy 1-11

Defining a Security Policy 1-12

Implementing a Security Policy 1-14

Maximum Security Architecture Overview 1-15

Summary 1-16

Practice 1: Overview 1-17

2 User Administration, Authentication, and Authorization

Objectives 2-2

Local Users 2-3

Common Users Versus Local Users 2-4

Profiles and Users 2-5

Profile Parameters: Locking and Passwords 2-6

Passwords and Password Verifiers 2-8

Schema-Only Users 2-10

Proxy Users 2-11

Externally Authenticated Users 2-13

OS Authentication 2-15

Kerberos Authentication 2-16

Radius Authentication 2-18

- PKI Certificate Authentication 2-20
- Certificates 2-21
- Enterprise User Security 2-22
- Oracle Identity Management Software 2-23
- Directory Structure: Overview 2-24
- Oracle Database: Enterprise User Security Architecture 2-25
- Authenticating Enterprise Users 2-26
- Enterprise Users 2-28
- Configuring Enterprise User Security 2-29
- Identifying the Enterprise User 2-30
- Enabling Current User Database Links 2-31
- Using Enterprise Roles 2-32
- User Migration Utility 2-33
- Enterprise-User Auditing 2-35
- Quiz 2-36
- Centrally Managed Users 2-37
- Account Management: Lock and Unlock Accounts 2-38
- Account Management: Expire Passwords 2-40
- Account Management: Identify Inactive Accounts 2-41
- Summary 2-42
- Practice 2: Overview 2-43

3 Securing Passwords

- Objectives 3-2
- Protecting Passwords 3-3
- Using a Secure External Password Store to Secure Passwords 3-4
- Designing Applications to Securely Handle Passwords 3-5
- Securely Handling Passwords in Scripts 3-7
- Managing the Database Password File 3-9
- Password File Improvements 3-10
- Password File Migration 3-11
- Password File Vulnerabilities 3-12
- Summary 3-13
- Practice 3: Overview 3-14

4 Authorization

- Objectives 4-2
- Concept of Least Privilege 4-3
- Privileges 4-4
- System Privileges 4-5

- Granting and Revoking System Privileges 4-6
- Object Privileges 4-7
- Granting and Revoking Object Privileges 4-8
- Administrative Privileges 4-9
- Roles 4-10
- Default and Non-Default Roles 4-11
- Secure Application Roles 4-12
- Implementing a Secure Application Role 4-13
- Privilege Analysis 4-14
- Privilege Analysis Flow 4-15
- Used Privileges Results 4-16
- Compare Used and Unused Privileges 4-17
- Listing Captures 4-18
- Dropping an Analysis 4-19
- PDB Lockdown Profiles 4-20
- Restricting Operations in a PDB Lockdown Profile 4-21
- PDB Lockdown Profiles Inheritance 4-22
- Static and Dynamic PDB Lockdown Profiles 4-23
- Summary 4-24
- Practice 4: Overview 4-25

5 Network Security

- Objectives 5-2
- Network Access Control for External Services 5-3
- How Do Network ACLs Relate to Microservice Deployments 5-4
- Using ACLs To Access Passwords in a Wallet 5-5
- Listener Valid Node Checking 5-7
- Network Service Profiles 5-8
- SEC_USER_UNAUTHORIZED_ACCESS_BANNER 5-9
- SEC_USER_AUDIT_ACTION_BANNER 5-10
- FALLBACK_AUTHENTICATION 5-11
- ALLOWED_LOGON_VERSION_CLIENT 5-12
- ALLOWED_LOGON_VERSION_SERVER 5-13
- Restricting Network IP Addresses: Valid Node Checking 5-14
- Enhancing Database Communication Security 5-15
- SEC_PROTOCOL_ERROR_TRACE_ACTION 5-16
- SEC_PROTOCOL_ERROR_FURTHER_ACTION 5-17
- SEC_MAX_FAILED_LOGIN_ATTEMPTS 5-18
- SEC_RETURN_SERVER_RELEASE_BANNER 5-19
- Summary 5-20
- Practice 5: Overview 5-21