

Oracle Database 11g: Security

Volume I • Student Guide

D50323GC20

Edition 2.0

April 2010

D66808

ORACLE

Authors

Donna Keesling
James Spiller

Contributors and

Reviewers

Tammy Bednar
Tom Best
Maria Billings
Herbert Bradbury
Howard Bradley
Tomohiko Fukuda
Philip Garm
Joel Goodman
Naveen Gopal
Xander Heemskerck
Uwe Hesse
Magnus Isaksson
Tomoki Ishii
Chandrasekharan Iyer
Sushma Jagannath
Martin Jensen
Dominique Jeunot
Victor Lu
Yi L Lu
Tom Minella
Sabiha Miri
Pam Moutrie
Lynn Munsinger
Paul Needham
Roman Niehoff
Preetam Ramakrishna
Surya Rekha
Kevin Reardon
Wayne Reeser
Walter Romanski
Ron Soltani
Kar Srinivasan
Glenn Tripp
Branislav Valny
Peter Wahl
Andrew Webber
Anthony Woodell
Paul Youn

Editors

Aju Kumar
Amitha Narayan
Raj Kumar

Graphic Designer

Satish Bettgowda

Publishers

Jayanthi Keshavamurthy
Shaik Mahaboob Basha
Sujatha Nagendra

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Preface

I Introduction to Database Security

- Course Objectives 1-2
- Agenda 1-3
- Prerequisites 1-6

1 Understanding Security Requirements

- Objectives 1-2
- Fundamental Data Security Requirements 1-3
- Data Security Concerns 1-5
- Compliance Mandates 1-6
- Security Risks 1-8
- Security Standards 1-10
- Developing Your Security Policy 1-11
- Defining a Security Policy 1-12
- Implementing a Security Policy 1-14
- Quiz 1-15
- Techniques for Enforcing Security 1-16
- Principle of Least Privilege 1-17
- Defense in Depth 1-18
- Common Exploits 1-19
- Preventing Exploits 1-21
- Summary 1-22
- Case Study: Applying Security Practices 1-23
- Understanding SQL Injection 1-24
- Preventing SQL Injection 1-25
- Reducing the Attack Surface 1-26
- Using Invoker's Rights 1-27
- Avoiding Dynamic SQL 1-28
- Validating Input to Dynamic SQL 1-29
- Coding Review and Testing Strategy 1-30
- Mitigating the Scope of Exploits 1-31
- Avoiding Privilege Escalation 1-32
- Trapping and Handling Exceptions 1-33

2 Choosing Security Solutions

- Objectives 2-2
- Assuring Data Integrity 2-3
- Data Protection 2-5
- Authentication and Authorization 2-7
- Networkwide Authentication 2-9
- Access Control and Monitoring 2-10
- Quiz 2-11
- Oracle Database Vault 2-12
- Oracle Audit Vault 2-13
- Combining Optional Security Features 2-14
- Compliance Scanner 2-16
- Enterprise Manager Database Control: Policy Trend 2-17
- Security at a Glance: Details 2-18
- Enterprise Manager Grid Control Security Advisor 2-19
- Policy Library 2-20
- Summary 2-21
- Practice 2 Overview: Hardening Database Access 2-22

3 Basic Database Security

- Objectives 3-2
- Database Security: Checklist 3-3
- Reducing Administration Effort 3-4
- Installing Only What Is Required 3-5
- Applying Security Patches 3-6
- Secure Password Support 3-7
- Automatic Secure Configuration 3-8
- Password Configuration 3-9
- SYS and SYSTEM Accounts 3-10
- SYSDBA, SYSOPER, and SYSASM 3-11
- Allowing Remote Database Administration 3-12
- Locking and Expiring Default User Accounts 3-13
- Changing Default Account Passwords 3-15
- Enforcing Password Management 3-17
- Enabling Built-in Password Complexity Checker 3-19
- Quiz 3-20
- Protecting the Data Dictionary 3-21
- System and Object Privileges 3-22
- Restricting the Directories Accessible by the User 3-23
- Managing Fine-Grained Access to External Network Services 3-24
- Managing Scheduler Security 3-26

- External Jobs 3-27
- Limiting Users with Administrative Privileges 3-28
- Separation of Responsibilities 3-30
- Using Available Database Security Features 3-32
- Summary 3-33
- Practice 3 Overview: Hardening Database Access 3-34

4 Auditing Database Users, Privileges, and Objects

- Objectives 4-2
- Monitoring for Suspicious Activity 4-3
- Audit Tool Comparisons 4-5
- Standard Database Auditing: Overview 4-6
- Standard Database Auditing 4-7
- Setting the `AUDIT_TRAIL` Parameter 4-9
- Audit Log Location Options 4-10
- Moving the Database Audit Trail from the `SYSTEM` Tablespace 4-11
- Limiting the Size of the Operating System Audit Trail 4-13
- Limiting the Age of the Operating System Audit Trail 4-14
- Clearing the Size and Age Properties 4-15
- Specifying Audit Options 4-16
- Auditing Sessions 4-18
- Viewing Auditing Options 4-20
- Viewing Auditing Results 4-21
- Quiz 4-22
- Purging Audit Trail Records 4-23
- Initializing the Audit Trail for Purging 4-24
- Setting an Archive Timestamp for Audit Records 4-25
- Manually Purging the Audit Trail 4-26
- Scheduling an Automatic Purge Job for the Audit Trail 4-27
- Auditing the `SYSDBA` and `SYSOPER` Users 4-29
- Viewing the `SYSDBA` Audit Trails 4-30
- Audit to XML Files 4-32
- Writing Audit Records to `syslog` 4-33
- Configuring Auditing to `syslog` 4-34
- `syslog` Limitations 4-35
- Value-Based Auditing 4-37
- Triggers and Autonomous Transactions 4-39
- Summary 4-41
- Practice 4 Overview: Implementing Basic Auditing 4-42

5 Auditing DML Statements

- Objectives 5-2
- Fine-Grained Auditing (FGA) 5-3
- FGA Policy 5-4
- Triggering Audit Events 5-6
- Data Dictionary Views 5-7
- DBA_FGA_AUDIT_TRAIL 5-8
- Quiz 5-9
- DBMS_FGA Package 5-10
- Enabling and Disabling an FGA Policy 5-11
- Dropping an FGA Policy 5-12
- FGA Policy Guidelines 5-13
- FGA Policy Errors 5-14
- Maintaining the Audit Trail 5-15
- Summary 5-16
- Practice 5 Overview: Implementing Fine-Grained Auditing 5-17

6 Using Basic User Authentication

- Objectives 6-2
- User Authentication 6-3
- User Identified by a Password 6-4
- User Identified Externally 6-5
- Protecting Passwords 6-6
- Quiz 6-7
- Fixed User Database Links 6-8
- Encrypted Database Link Passwords 6-9
- Database Links Without Credentials 6-10
- Database Links and Changing Passwords 6-12
- Auditing with Database Links 6-13
- Restricting a Database Link with Views 6-14
- Summary 6-16
- Practice 6 Overview: Using Basic Authentication Methods 6-17

7 Using Strong Authentication

- Objectives 7-2
- User Authentication 7-3
- Strong User Authentication 7-4
- Single Sign-On 7-6
- Public Key Infrastructure (PKI) Tools 7-7
- Certificates 7-8
- How to Use Certificates for Authentication 7-9

- Configuring SSL on the Server 7-10
- Configuring Oracle Net Files on the Server 7-11
- Configuring SSL on the Client 7-12
- Configuring Oracle Net Files on the Client 7-13
- Creating a User Identified by a Certificate 7-15
- Connecting to the Database 7-16
- Quiz 7-17
- `orapki` Utility 7-18
- How to Use Kerberos for Authentication 7-19
- How to Use KDC with Windows 2000 for Authentication 7-21
- RADIUS Authentication: Overview 7-23
- Secure External Password Store 7-24
- Configuring the Wallet 7-25
- Configuring `sqlnet.ora` 7-26
- Managing the External Password Store 7-27
- Summary 7-28
- Practice 7 Overview: Configuring the External Secure Password Store 7-29

8 Using Enterprise User Security

- Objectives 8-2
- User Authentication 8-3
- Enterprise User Security 8-4
- Oracle Identity Management Infrastructure: Default Deployment 8-5
- Oracle Database: Enterprise User Security Architecture 8-6
- Authenticating Enterprise Users 8-7
- OID Structure Overview 8-9
- Quiz 8-10
- Setting Up Enterprise User Security 8-11
- Installing Oracle Application Server Infrastructure 8-12
- Registering the Database 8-13
- Managing Enterprise User Security 8-14
- Creating an Enterprise User 8-15
- Creating an Enterprise User in the Directory 8-16
- Creating a Schema Mapping Object in the Directory: Subtree 8-17
- Creating a Schema Mapping Object in the Directory: User Name 8-18
- Identifying the Enterprise User 8-19
- Enabling Current User Database Links 8-20
- User Migration Utility 8-21
- Enterprise-User Auditing 8-23
- Summary 8-24
- Practice 8 Overview: Implementing Enterprise User Security 8-25

9 Using Proxy Authentication

- Objectives 9-2
- User Authentication 9-3
- Security Challenges of Three-Tier Computing 9-4
- Identifying the Real User 9-5
- Common Implementations of Authentication 9-7
- User Reauthentication 9-9
- Restricting the Privileges of the Middle Tier 9-11
- Implementing Proxy Authentication Solutions 9-12
- Quiz 9-14
- Authenticating Database and Enterprise Users 9-15
- Using Proxy Authentication for Database Users 9-17
- Using Proxy Authentication for Enterprise Users 9-19
- Proxy Access Through SQL*Plus 9-21
- Enterprise User Proxy 9-22
- Enterprise User Proxy: Example 9-23
- Revoking Proxy Authentication 9-25
- Application-User Model 9-26
- Data Dictionary Views for Proxy Authentication 9-28
- Data Dictionary Views: DBA_PROXIES and USER_PROXIES 9-29
- Data Dictionary Views: V\$SESSION_CONNECT_INFO 9-30
- Auditing Actions Taken on Behalf of the Real User 9-31
- Data Dictionary Views: DBA_STMT_AUDIT_OPTS 9-33
- Data Dictionary Views: DBA_AUDIT_TRAIL 9-34
- Summary 9-35
- Practice 9 Overview: Implementing Proxy Authentication 9-36

10 Using Privileges and Roles

- Objectives 10-2
- Authorization 10-3
- Privileges 10-4
- Roles 10-5
- Benefits of Roles 10-6
- Predefined Roles 10-7
- CONNECT Role Privileges 10-8
- Using Proxy Authentication with Roles 10-9
- Quiz 10-10
- Using Enterprise Roles 10-11
- Creating an Enterprise Role 10-12

| | |
|--|-------|
| Assigning an Enterprise User to an Enterprise Role | 10-13 |
| Securing Objects with Procedures | 10-14 |
| Secure Application Role | 10-15 |
| Implementing a Secure Application Role | 10-16 |
| Step 1: Create the Role | 10-17 |
| Step 2.a: Create the Package Specification | 10-18 |
| Step 2.b: Create the Package Body | 10-19 |
| Step 3: Grant the EXECUTE Privilege on the Package | 10-21 |
| Step 4: Write the Application Server Code That Sets the Role | 10-22 |
| Viewing Dictionary Information for Secure Application Roles | 10-23 |
| Summary | 10-24 |
| Practice 10 Overview: Implementing the Secure Application Role | 10-25 |

11 Using Application Contexts

| | |
|--|-------|
| Objectives | 11-2 |
| Application Context: Description | 11-3 |
| Creating a Context in a Namespace | 11-4 |
| Using the Application Context | 11-5 |
| Setting the Application Context | 11-6 |
| Using the SYS_CONTEXT PL/SQL Function | 11-7 |
| Application Context Data Sources | 11-8 |
| Quiz | 11-10 |
| Implementing a Local Context | 11-11 |
| Step 1: Create an Application Context | 11-12 |
| Step 2: Create a PL/SQL Package That Sets the Context | 11-14 |
| Step 3: Call the Package | 11-15 |
| Step 4: Read the Context Attribute in the Application | 11-16 |
| Application Context Accessed Globally | 11-17 |
| Application Context Accessed Globally in Action | 11-19 |
| Using the DBMS_SESSION Package | 11-21 |
| Implementing the Application Context Accessed Globally | 11-24 |
| Step 1: Create the Application Context Accessed Globally | 11-25 |
| Step 2: Establish a Session | 11-26 |
| Step 3: Handle Subsequent Requests | 11-27 |
| Step 4: End a Session | 11-28 |
| Viewing Application Context Information | 11-29 |
| Application Context Usage Guidelines | 11-31 |
| Summary | 11-33 |
| Practice 11 Overview: Creating an Application Context | 11-34 |

12 Implementing Virtual Private Database

- Objectives 12-2
- Fine-Grained Access Control: Overview 12-3
- Understanding Fine-Grained Access Control Policy Execution 12-5
- Benefits of Using Fine-Grained Access Control 12-7
- Virtual Private Database 12-8
- Examples of Virtual Private Database 12-9
- Quiz 12-11
- Tools to Implement Virtual Private Database 12-12
- Enterprise Manager 12-14
- Managing VPD Policies 12-15
- Using `DBMS_RLS` to Manage Policies 12-16
- Column-Level VPD 12-18
- Column-Level VPD: Example 12-19
- Policy Types: Overview 12-20
- Static Policies 12-21
- Context-Sensitive Policies 12-22
- Sharing Policy Functions 12-23
- Exceptions to VPD Policies 12-24
- Designing and Implementing a VPD Solution 12-25
- Implementing a VPD Policy 12-26
- Creating a Package and Context 12-27
- Writing the Function That Creates a Predicate 12-29
- Testing the Security Function 12-31
- Writing a Function That Returns Different Predicates 12-32
- Creating a Policy 12-34
- Quiz 12-35
- Implementing Policy Groups 12-36
- Grouping Policies 12-38
- Default Policy Group 12-39
- Creating a Driving Context 12-41
- Making the Context a Driving Context 12-43
- Creating a Policy Group 12-45
- Adding a Policy to a Group 12-46
- Best Practices for VPD 12-48
- Guidelines for Policies and Context 12-49
- Policy Performance 12-51
- Export and Import 12-53
- Policy Views 12-54
- Checking for Policies Applied to SQL Statements 12-55

Summary 12-56
 Practice 12 Overview: Implementing a Virtual Private Database Policy 12-57

13 Oracle Label Security Concepts

Objectives 13-2
 Access Control: Overview 13-3
 Discretionary Access Control 13-4
 Oracle Label Security 13-5
 How Sensitivity Labels Are Used 13-6
 Installing Oracle Label Security 13-7
 Quiz 13-8
 Oracle Label Security: Features 13-9
 Comparing Oracle Label Security and VPD 13-11
 Oracle Label Security and VPD Comparison 13-12
 Analyzing Application Requirements 13-13
 Summary 13-14

14 Implementing Oracle Label Security

Objectives 14-2
 Implementing an Oracle Label Security Solution 14-3
 Step 3: Create Policies 14-5
 Policy Enforcement Options 14-6
 Step 4: Define Labels: Overview 14-8
 Defining Levels by Using Enterprise Manager 14-9
 Creating Levels 14-10
 Defining Groups by Using Enterprise Manager 14-11
 Creating Groups 14-12
 Defining Compartments by Using Enterprise Manager 14-13
 Creating Compartments 14-14
 Identifying Data Labels 14-15
 Creating Data Labels 14-16
 Access Mediation 14-17
 Administering Labels 14-18
 Adding Labels to Data 14-19
 Step 5: Apply the Policy to a Table 14-20
 Step 6: Assign User Authorization Labels 14-21
 Quiz 14-23
 Oracle Label Security Special User Privileges 14-24
 Example: READ Privilege 14-25
 Example: FULL Privilege 14-26
 Example: COMPACCESS Privilege 14-27

| | |
|--|-------|
| Using the <code>PROFILE_ACCESS</code> Privilege | 14-28 |
| Trusted Stored Package Units | 14-30 |
| Exporting with Oracle Label Security | 14-31 |
| Importing with Oracle Label Security | 14-32 |
| Performance Tips | 14-33 |
| Summary | 14-35 |
| Practice 14 Overview: Implementing Oracle Label Security | 14-36 |

15 Using the Data Masking Pack

| | |
|---|-------|
| Objectives | 15-2 |
| Data Masking: Overview | 15-3 |
| Understanding Data Masking | 15-4 |
| Using the Data Masking Pack | 15-5 |
| Accessing the Data Masking Pack | 15-6 |
| Data Masking Pack: Features | 15-7 |
| Data Masking: Best Practices | 15-8 |
| Implementing Data Masking | 15-9 |
| Identifying Sensitive Data for Masking | 15-11 |
| Quiz | 15-12 |
| Determining How to Mask the Data | 15-13 |
| Managing the Data Mask Format Library | 15-14 |
| Using Oracle-Supplied Mask Formats | 15-15 |
| Types of Built-in Masking Primitives and Routines | 15-16 |
| Example: Data Masking of the <code>EMPLOYEES</code> Table | 15-18 |
| Creating Data Mask Formats | 15-19 |
| Creating a User-Defined Data Mask Format | 15-20 |
| Creating a Masking Format Using a User-Defined Function | 15-21 |
| Creating Data Masking Definitions | 15-22 |
| Using Masking Formats | 15-23 |
| Automatic Identification of Related Columns | 15-24 |
| Adding Dependent Columns | 15-25 |
| Importing Formats | 15-26 |
| Importing Formats and Modifying Properties | 15-27 |
| Using Condition-Based Masking | 15-28 |
| Using Compound Masking | 15-29 |
| Using a User-Defined Masking Function | 15-30 |
| Creating a Post-Processing Function | 15-31 |
| Implementing a Post-Processing Function | 15-32 |
| Generating the Data Masking Script | 15-33 |
| Viewing the Data Masking Impact Report | 15-34 |
| Viewing the Data Masking Script | 15-35 |

| | |
|---|-------|
| Scheduling the Data Masking Job | 15-36 |
| Specifying Automatic Masking After Cloning | 15-37 |
| Understanding the Data Masking Process | 15-38 |
| Creating an Application Masking Template | 15-39 |
| Importing Data Masking Definitions | 15-40 |
| Controlling Data Masking Operations | 15-41 |
| Creating Custom Reports for Auditors | 15-42 |
| Summary | 15-45 |
| Practice 15 Overview: Implementing Data Masking | 15-46 |

16 Encryption Concepts

| | |
|--|-------|
| Objectives | 16-2 |
| Understanding Encryption | 16-3 |
| What Problems Does Encryption Solve? | 16-4 |
| Cost of Encryption | 16-5 |
| Encryption Is Not Access Control | 16-6 |
| Access by Privileged Users | 16-7 |
| What to Encrypt | 16-9 |
| Quiz | 16-10 |
| Data Encryption: Challenges | 16-11 |
| Encryption Key Management: Key Generation | 16-12 |
| Encryption Key Management: Key Modification and Transmission | 16-13 |
| Encryption Key Management: Storage | 16-14 |
| Storing the Key in the Database | 16-15 |
| Storing the Key in the Operating System | 16-17 |
| Letting the User Manage the Key | 16-18 |
| Solutions | 16-19 |
| Summary | 16-20 |

17 Using Application-Based Encryption

| | |
|--|-------|
| Objectives | 17-2 |
| Overview | 17-3 |
| DBMS_CRYPTO Package | 17-4 |
| Generating Keys Using RANDOMBYTES | 17-6 |
| Quiz | 17-9 |
| Using ENCRYPT and DECRYPT | 17-10 |
| Enhanced Security Using Cipher Block Modes | 17-13 |
| Hash and Message Authentication Code | 17-14 |
| Summary | 17-17 |
| Practice 17 Overview: Using DBMS_CRYPTO for Encryption | 17-18 |

18 Applying Transparent Data Encryption

- Objectives 18-2
- Transparent Data Encryption 18-3
- Benefits of TDE 18-4
- Components of TDE 18-5
- Using TDE 18-6
- Creating the Master Key 18-7
- Opening the Wallet 18-9
- Using Auto Login Wallet 18-11
- Backup and Recovery of the Wallet 18-12
- Quiz 18-13
- Master Key Re-Key Concepts 18-14
- Re-Keying Table Keys 18-15
- Using Hardware Security Modules 18-16
- Configuring for Hardware Security Modules 18-17
- Creating an Encrypted Column 18-20
- Encrypt Clause Syntax 18-21
- Creating an Index on an Encrypted Column 18-22
- Altering an Encrypted Column 18-23
- TDE Column Encryption Support 18-24
- TDE Column-Level Storage Requirements 18-26
- TDE Column Encryption: Restrictions 18-27
- Tablespace Encryption: Advantages 18-28
- Creating an Encrypted Tablespace 18-29
- Tablespace Encryption: Restrictions 18-30
- Exporting and Importing with TDE 18-31
- SECUREFILE LOB Encryption 18-32
- Summary 18-33
- Practice 18 Overview: Implementing TDE 18-34

19 Applying File Encryption

- Objectives 19-2
- RMAN-Encrypted Backups 19-3
- Oracle Secure Backup Encryption 19-4
- Encrypted Backups to Tape 19-6
- Creating RMAN-Encrypted Backups 19-7
- Using Transparent-Mode Encryption 19-8
- Using Password-Mode Encryption 19-10
- Using Dual-Mode Encryption 19-11
- Quiz 19-12
- Restoring Encrypted Backups 19-13

- RMAN-Encrypted Backups: Considerations 19-14
- Data Pump Encryption 19-15
- ENCRYPTION Parameter 19-16
- ENCRYPTION_PASSWORD Parameter 19-17
- ENCRYPTION_MODE Parameter 19-18
- Encrypting Dump Files 19-19
- Summary 19-20
- Practice 19 Overview: Using RMAN Backup File Encryption 19-21

20 Oracle Net Services: Security Checklists

- Objectives 20-2
- Overview: Security Checklists 20-3
- Client Checklist 20-4
- Issues with Securing the Client Computer 20-5
- Configuring the Browser 20-6
- Network Security: Checklist 20-7
- Using a Firewall to Restrict Network Access 20-8
- Restricting Network IP Addresses: Valid Node Checking 20-9
- Restricting Network IP Addresses: Guidelines 20-11
- Configuring IP Restrictions with Net Manager 20-12
- Quiz 20-13
- Restricting Open Ports 20-14
- Encrypting Network Traffic 20-15
- End-to-End Encryption 20-17
- Configuring Network Encryption 20-18
- Checksumming 20-19
- Configuring Checksumming 20-20
- Oracle Net Services Log Files 20-21
- Summary 20-23
- Practice 20 Overview: Configuring Net Security 20-24

21 Securing the Listener

- Objectives 21-2
- Listener Security: Checklist 21-3
- Moving the Listener to a Nondefault Port 21-4
- Password-Protecting the Listener 21-5
- Preventing Online Administration of the Listener 21-7
- Quiz 21-8
- Administering the Listener Using TCP/IP for SSL 21-9
- INBOUND_CONNECT_TIMEOUT 21-10
- Setting Listener-Logging Parameters 21-12

Analyzing Listener Log Files 21-14
Listener Log Connect: Examples 21-16
Listener Log Command: Examples 21-18
Summary 21-20
Practice 21 Overview: Securing the Listener 21-21

Appendix A: Practices and Solutions

Appendix B: Using Oracle Connection Manager as a Firewall

Objectives B-2
Overview of Firewalls B-3
Network Architecture Regions B-4
Guidelines for Positioning Servers Within Firewalls B-5
Using a Firewall to Restrict Database Access B-6
Types of Firewalls B-7
Control Traffic from the Internet B-8
Using Oracle Connection Manager as a Firewall B-10
Oracle Connection Manager: Overview B-11
Oracle Connection Manager Processes B-12
Oracle Connection Manager Architecture B-13
Access Control with Oracle Connection Manager B-14
Configuring Oracle Connection Manager B-15
Configuring the `cman.ora` File B-16
Preventing Remote Administration of Oracle Connection Manager B-18
Allowing or Denying Access B-19
Configuring Clients to Use CMAN B-21
Configuring Database Servers to Use CMAN B-22
Oracle Connection Manager Control Utility B-23
Starting and Shutting Down Oracle Connection Manager B-24
Additional Commands B-26
Monitoring Connection Events Using the `CMAN` Log File B-28
Analyzing Oracle Connection Manager Log Files B-30
Summary B-31
Practice 22 Overview: Implementing CMAN as a Firewall B-32

Appendix C: Securing SQL*Plus

Objectives C-2
Limiting Commands Available in SQL*Plus C-3
Creating the PUP Table C-4

- Commands That Can Be Disabled C-6
- Example: Disabling a Command C-7
- Disabling a Role C-8
- Example: Disabling a Role C-9
- Using `SET ROLE` to Enable a Disabled Role C-11
- Example: Disabling `SET ROLE` C-12
- `PRODUCT_USER_PROFILE`: Guidelines C-13
- Summary C-14
- Practice 23 Overview: Securing SQL*Plus C-15

Appendix D: Source Code

Appendix E: `USERENV` Context

THESE eKIT MATERIALS ARE FOR YOUR USE IN THIS CLASSROOM ONLY. COPYING eKIT MATERIALS FROM THIS COMPUTER IS STRICTLY PROHIBITED