Contents

Preface

Audience l
Documentation Accessibility l
Diversity and Inclusion li
Related Documents li
Conventions lii

Changes in This Release for Oracle Database Security Guide

Changes in Oracle Database Security 23ai liii
Updates to Oracle Database Security 23ai lxiv

1 Introduction to Oracle Database Security

1.1 About Oracle Database Security 1-1
1.2 Additional Oracle Database Security Products 1-3

Part I Managing User Authentication and Authorization

2 Managing Security for Oracle Database Users

2.1 About User Security 2-1
2.2 Creating User Accounts 2-2
2.2.1 About Common Users and Local Users 2-2
2.2.1.1 About Common Users 2-3
2.2.1.2 How Plugging in PDBs Affects CDB Common Users 2-4
2.2.1.3 About Local Users 2-5
2.2.2 Who Can Create User Accounts? 2-6
2.2.3 Creating a New User Account That Has Minimum Database Privileges 2-6
2.2.4 Restrictions on Creating the User Name for a New Account 2-7
2.2.4.1 Uniqueness of User Names 2-8
2.2.4.2 User Names in a Multitenant Environment 2-8
2.2.4.3 Case Sensitivity for User Names 2-8

2.2.5 Assignment of User Passwords 2-9
2.2.6 Default Tablespace for the User 2-9
2.2.6.1 About Assigning a Default Tablespace for a User 2-9
2.2.6.2 DEFAULT TABLESPACE Clause for Assigning a Default Tablespace 2-10
2.2.7 Tablespace Quotas for a User 2-10
2.2.7.1 About Assigning a Tablespace Quota for a User 2-11
2.2.7.2 CREATE USER Statement for Assigning a Tablespace Quota 2-11
2.2.7.3 Restriction of the Quota Limits for User Objects in a Tablespace 2-11
2.2.7.4 Grants to Users for the UNLIMITED TABLESPACE System Privilege 2-12
2.2.8 Temporary Tablespaces for the User 2-12
2.2.8.1 About Assigning a Temporary Tablespace for a User 2-12
2.2.8.2 TEMPORARY TABLESPACE Clause for Assigning a Temporary Tablespace 2-13
2.2.9 Profiles for the User 2-13
2.2.10 Creation of a Common User or a Local User 2-14
2.2.10.1 About Creating Common User Accounts 2-14
2.2.10.2 CREATE USER Statement for Creating a Common User Account 2-15
2.2.10.3 About Creating Local User Accounts 2-16
2.2.10.4 CREATE USER Statement for Creating a Local User Account 2-17
2.2.11 Creating a Default Role for the User 2-17
2.3 Altering User Accounts 2-18
2.3.1 About Altering User Accounts 2-18
2.3.2 Methods of Altering Common or Local User Accounts 2-18
2.3.3 Changing Non-SYS User Passwords 2-19
2.3.3.1 About Changing Non-SYS User Passwords 2-19
2.3.3.2 Using the PASSWORD Command or ALTER USER Statement to Change a Password 2-20
2.3.4 Changing the SYS User Password 2-20
2.3.4.1 About Changing the SYS User Password 2-21
2.3.4.2 ORAPWD Utility for Changing the SYS User Password 2-22
2.4 Configuring User Resource Limits 2-22
2.4.1 About User Resource Limits 2-23
2.4.2 Types of System Resources and Limits 2-23
2.4.2.1 Limits to the User Session Level 2-24
2.4.2.2 Limits to Database Call Levels 2-24
2.4.2.3 Limits to CPU Time 2-24
2.4.2.4 Limits to Logical Reads 2-24
2.4.2.5 Limits to Other Resources 2-25
2.4.3 Values for Resource Limits of Profiles 2-25
2.4.4 Managing Resources with Profiles 2-26
2.4.4.1 About Profiles 2-26
2.4.4.2 ORA_CIS_PROFILE User Profile 2-27

2.4.4.3 ORA_STIG_PROFILE User Profile 2-27
2.4.4.4 Creating a Profile 2-28
2.4.4.5 Creating a CDB Profile or an Application Profile 2-29
2.4.4.6 Assigning a Profile to a User 2-29
2.4.4.7 Dropping Profiles 2-29
2.4.5 Common Mandatory Profiles in the CDB Root 2-30
2.4.5.1 About Common Mandatory Profiles in the CDB Root 2-30
2.4.5.2 Creating a Common Mandatory Profile in the CDB Root 2-31
2.4.5.3 Example: Function to Enforce Minimum Password Length 2-32
2.5 Dropping User Accounts 2-36
2.5.1 About Dropping User Accounts 2-37
2.5.2 Terminating a User Session 2-37
2.5.3 About Dropping a User After the User Is No Longer Connected to the Database 2-37
2.5.4 Dropping a User Whose Schema Contains Objects 2-38
2.6 Predefined Schema User Accounts Provided by Oracle Database 2-38
2.6.1 About the Predefined Schema User Accounts 2-38
2.6.2 Predefined Administrative Accounts 2-39
2.6.3 Predefined Non-Administrative User Accounts 2-42
2.6.4 Predefined Sample Schema User Accounts 2-42
2.7 Database User and Profile Data Dictionary Views 2-43
2.7.1 Data Dictionary Views That List Information About Users and Profiles 2-43
2.7.2 Query to Find All Users and Associated Information 2-44
2.7.3 Query to List All Tablespace Quotas 2-45
2.7.4 Query to List All Profiles and Assigned Limits 2-45
2.7.5 Query to View Memory Use for Each User Session 2-46

3 Configuring Authentication

3.1 About Authentication 3-1
3.2 Configuring Password Protection 3-2
3.2.1 What Are the Oracle Database Built-in Password Protections? 3-3
3.2.2 Minimum Requirements for Passwords 3-4
3.2.3 Creating a Password by Using the IDENTIFIED BY Clause 3-4
3.2.4 Using a Password Management Policy 3-4
3.2.4.1 About Managing Passwords 3-5
3.2.4.2 Finding User Accounts That Have Default Passwords 3-6
3.2.4.3 Password Settings in the Default Profile 3-7
3.2.4.4 Using the ALTER PROFILE Statement to Modify Profile Limits 3-8
3.2.4.5 Disabling and Enabling the Default Password Security Settings 3-9
3.2.4.6 Automatically Locking Inactive Database User Accounts 3-9
3.2.4.7 Automatically Locking User Accounts After a Specified Number of Failed Log-in Attempts 3-10

3.2.4.8 Example: Locking an Account with the CREATE PROFILE Statement 3-11
3.2.4.9 Explicitly Locking a User Account with the CREATE USER or ALTER USER Statement 3-11
3.2.4.10 Controlling the User Ability to Reuse Previous Passwords 3-11
3.2.4.11 About Controlling Password Aging and Expiration 3-12
3.2.4.12 Setting a Password Lifetime 3-13
3.2.4.13 Checking the Status of a User Account 3-13
3.2.4.14 Password Change Life Cycle 3-13
3.2.4.15 PASSWORD_LIFE_TIME Profile Parameter Low Value 3-15
3.2.5 Managing Gradual Database Password Rollover for Applications 3-16
3.2.5.1 About Managing Gradual Database Password Rollover for Applications 3-17
3.2.5.2 Password Change Life Cycle During a Gradual Database Password Rollover 3-18
3.2.5.3 Enabling the Gradual Database Password Rollover 3-19
3.2.5.4 Changing a Password to Begin the Gradual Database Password Rollover Period 3-20
3.2.5.5 Changing a Password During the Gradual Database Password Rollover Period 3-21
3.2.5.6 Ending the Password Rollover Period 3-22
3.2.5.7 Database Behavior During the Gradual Password Rollover Period 3-22
3.2.5.8 Database Server Behavior After the Password Rollover Period Ends 3-23
3.2.5.9 Guideline for Handling Compromised Passwords 3-23
3.2.5.10 How Gradual Database Password Rollover Works During Oracle Data Pump Exports 3-24
3.2.5.11 Using Gradual Database Password Rollover in an Oracle Data Guard Environment 3-24
3.2.5.12 Finding Users Who Still Use Their Old Passwords 3-24
3.2.6 Managing the Complexity of Passwords 3-25
3.2.6.1 About Password Complexity Verification 3-26
3.2.6.2 How Oracle Database Checks the Complexity of Passwords 3-26
3.2.6.3 Who Can Use the Password Complexity Functions? 3-26
3.2.6.4 ora12c_verify_function Password Requirements 3-26
3.2.6.5 ora12c_strong_verify_function Function Password Requirements 3-27
3.2.6.6 ora12c_stig_verify_function Password Requirements 3-27
3.2.6.7 About Customizing Password Complexity Verification 3-28
3.2.6.8 Enabling Password Complexity Verification 3-28
3.2.7 Managing Password Case Sensitivity 3-29
3.2.7.1 Management of Case Sensitivity for Secure Role Passwords 3-29
3.2.7.2 Management of Password Versions of Users 3-30
3.2.7.3 Finding and Resetting User Passwords That Use the 10G Password Version 3-30
3.2.7.4 How Case Sensitivity Affects Password Files 3-32
3.2.7.5 How Case Sensitivity Affects Passwords Used in Database Link Connections 3-33

3.2.8 Ensuring Against Password Security Threats by Using the 12C Password Version 3-33
3.2.8.1 About the 12C Version of the Password Hash 3-34
3.2.8.2 Oracle Database 12C Password Version Configuration Guidelines 3-35
3.2.8.3 Configuring Oracle Database to Use the 12C Password Version Exclusively 3-37
3.2.8.4 How Server and Client Logon Versions Affect Database Links 3-38
3.2.8.5 Configuring Oracle Database Clients to Use the 12C Password Version Exclusively 3-40
3.2.9 Managing the Secure External Password Store for Password Credentials 3-41
3.2.9.1 About the Secure External Password Store 3-41
3.2.9.2 How Does the Secure External Password Store Work? 3-42
3.2.9.3 About Configuring Clients to Use the Secure External Password Store 3-43
3.2.9.4 Configuring a Client to Use the Secure External Password Store 3-43
3.2.9.5 Example: Sample sqlnet.ora File with Wallet Parameters Set 3-45
3.2.9.6 Managing External Password Store Credentials 3-45
3.2.9.7 Creating SQL*Loader Object Store Credentials 3-47
3.2.10 Managing Passwords for Administrative Users 3-48
3.2.10.1 About Managing Passwords for Administrative Users 3-49
3.2.10.2 Setting the LOCK and EXPIRED Status of Administrative Users 3-49
3.2.10.3 Password Profile Settings for Administrative Users 3-49
3.2.10.4 Last Successful Login Time for Administrative Users 3-49
3.2.10.5 Management of the Password File of Administrative Users 3-49
3.2.10.6 Migration of the Password File of Administrative Users 3-50
3.2.10.7 How the Multitenant Option Affects Password Files for Administrative Users 3-51
3.2.10.8 Password Complexity Verification Functions for Administrative Users 3-51
3.3 Authentication of Database Administrators 3-51
3.3.1 About Authentication of Database Administrators 3-52
3.3.2 Strong Authentication, Centralized Management for Administrators 3-52
3.3.2.1 About Strong Authentication for Database Administrators 3-52
3.3.2.2 Configuring Directory Authentication for Administrative Users 3-53
3.3.2.3 Configuring Kerberos Authentication for Administrative Users 3-54
3.3.3 Authentication of Database Administrators by Using the Operating System 3-55
3.3.4 Authentication of Database Administrators by Using Their Passwords 3-55
3.3.5 Risks of Using Password Files for Database Administrator Authentication 3-56
3.4 Database Authentication of Users 3-57
3.4.1 About Database Authentication of Users 3-57
3.4.2 Advantages of Database Authentication 3-59
3.4.3 Creating Users Who Are Authenticated by the Database 3-59
3.5 Schema-Only Accounts 3-60
3.5.1 About Schema-Only Accounts 3-60
3.5.2 Creating a Schema-Only Account 3-61

3.5.3 Altering a Schema-Only Account 3-61
3.6 Configuring Operating System Users for a PDB 3-61
3.6.1 About Configuring Operating System Users for a PDB 3-62
3.6.2 PDB_OS_CREDENTIAL Initialization Parameter 3-62
3.6.3 Configuring an Operating System User for a PDB 3-62
3.6.4 Setting the Default Credential in a PDB 3-63
3.7 External (Non-Database) User Authentication and Access to the Database 3-64
3.7.1 External Authentication with Local Database Authorization 3-64
3.7.1.1 About External Authentication with Local Database Authorization 3-64
3.7.1.2 Operating System Authentication 3-65
3.7.1.3 Kerberos Authentication 3-66
3.7.1.4 Public Key Infrastructure Centificate Authentication 3-66
3.7.1.5 RADIUS Authentication 3-67
3.7.2 External Authentication with External Authorization 3-67
3.7.2.1 About External Authentication with External Authorization 3-68
3.7.2.2 Centrally Managed Users with Microsoft Active Directory 3-68
3.7.2.3 Microsoft Entra ID Integration 3-69
3.7.2.4 Oracle Cloud Infrastructure Identity and Access Management Integration 3-69
3.7.2.5 Oracle Enterprise User Security 3-69
3.8 Multitier Authentication and Authorization 3-69
3.9 Administration and Security in Clients, Application Servers, and Database Servers 3-70
3.10 Preserving User Identity in Multitiered Environments 3-71
3.10.1 Middle Tier Server Use for Proxy Authentication 3-72
3.10.1.1 About Proxy Authentication 3-73
3.10.1.2 Advantages of Proxy Authentication 3-73
3.10.1.3 Who Can Create Proxy User Accounts? 3-74
3.10.1.4 Guidelines for Creating Proxy User Accounts 3-74
3.10.1.5 Creating Proxy User Accounts and Authorizing Users to Connect Through Them 3-75
3.10.1.6 Proxy User Accounts and the Authorization of Users to Connect Through Them 3-76
3.10.1.7 Using Proxy Authentication with the Secure External Password Store 3-76
3.10.1.8 How the Identity of the Real User Is Passed with Proxy Authentication 3-77
3.10.1.9 Limits to the Privileges of the Middle Tier 3-78
3.10.1.10 Authorizing a Middle Tier to Proxy and Authenticate a User 3-79
3.10.1.11 Authorizing a Middle Tier to Proxy a User Authenticated by Other Means 3-79
3.10.1.12 Reauthenticating a User Through the Middle Tier to the Database 3-80
3.10.1.13 Using Password-Based Proxy Authentication 3-80
3.10.1.14 Using Proxy Authentication with Enterprise Users 3-81
3.10.2 Using Client Identifiers to Identify Application Users Unknown to the Database 3-82
3.10.2.1 About Client Identifiers 3-82
3.10.2.2 How Client Identifiers Work in Middle Tier Systems 3-82

3.10.2.3 Use of the CLIENT_IDENTIFIER Attribute to Preserve User Identity 3-83
3.10.2.4 Use of the CLIENT_IDENTIFIER Independent of Global Application Context 3-83
3.10.2.5 Setting the CLIENT_IDENTIFIER Independent of Global Application Context 3-84
3.10.2.6 Use of the DBMS_SESSION PL/SQL Package to Set and Clear the Client Identifier 3-85
3.10.2.7 Enabling the CLIENTID_OVERWRITE Event System-Wide 3-85
3.10.2.8 Enabling the CLIENTID_OVERWRITE Event for the Current Session 3-86
3.10.2.9 Disabling the CLIENTID_OVERWRITE Event 3-86
3.11 User Authentication Data Dictionary Views 3-86

4 Configuring Privilege and Role Authorization

4.1 About Privileges and Roles 4-2
4.2 Privilege and Role Grants in a CDB 4-3
4.2.1 About Privilege and Role Grants in a CDB 4-4
4.2.2 Principles of Privilege and Role Grants in a CDB 4-4
4.2.3 Privileges and Roles Granted Locally in a CDB 4-5
4.2.4 What Makes a Privilege or Role Grant Local 4-5
4.2.5 Roles and Privileges Granted Locally 4-6
4.2.6 Roles and Privileges Granted Commonly in a CDB 4-6
4.2.7 What Makes a Grant Common 4-7
4.2.8 Roles and Privileges Granted Commonly 4-7
4.2.9 Grants to PUBLIC in a CDB 4-8
4.2.10 Grants of Privileges and Roles: Scenario 4-8
4.3 Who Should Be Granted Privileges? 4-11
4.4 How the Oracle Multitenant Option Affects Privileges 4-12
4.5 Managing Administrative Privileges 4-12
4.5.1 About Administrative Privileges 4-13
4.5.2 Grants of Administrative Privileges to Users 4-13
4.5.3 SYSDBA and SYSOPER Privileges for Standard Database Operations 4-13
4.5.4 Forcing oracle Users to Enter a Password When Logging in as SYSDBA 4-14
4.5.5 SYSBACKUP Administrative Privilege for Backup and Recovery Operations 4-14
4.5.6 SYSDG Administrative Privilege for Oracle Data Guard Operations 4-16
4.5.7 SYSKM Administrative Privilege for Transparent Data Encryption 4-17
4.5.8 SYSRAC Administrative Privilege for Oracle Real Application Clusters 4-17
4.6 Managing System Privileges 4-18
4.6.1 About System Privileges 4-19
4.6.2 Who Can Grant or Revoke System Privileges? 4-19
4.6.3 Why Is It Important to Restrict System Privileges? 4-20
4.6.3.1 About the Importance of Restricting System Privileges 4-20
4.6.3.2 User Access to Objects in the SYS Schema 4-20

4.6.4 Grants and Revokes of System Privileges 4-21
4.6.5 About ANY Privileges and the PUBLIC Role 4-21
4.7 Managing Schema Privileges 4-22
4.7.1 About Managing Schema Privileges 4-22
4.7.2 Privileges That Are Excluded from Schema Privilege Grants 4-23
4.7.3 Granting a Schema Privilege 4-25
4.7.4 Revoking a Schema Privilege 4-26
4.8 Administering Schema Security Policies 4-26
4.8.1 About Administering Schema System Security Policies 4-26
4.8.2 Granting an Administrator Schema Security Policy 4-27
4.8.3 Revoking an Administrator Security Policy 4-27
4.9 Managing Privileges to Enable Diagnostics 4-28
4.10 Managing Commonly and Locally Granted Privileges 4-29
4.10.1 About Commonly and Locally Granted Privileges 4-29
4.10.2 How Commonly Granted System Privileges Work 4-30
4.10.3 How Commonly Granted Object Privileges Work 4-30
4.10.4 Granting or Revoking Privileges to Access a PDB 4-31
4.10.5 Example: Granting a Privilege to a Common User 4-31
4.10.6 Enabling Common Users to View CONTAINER_DATA Object Information 4-31
4.10.6.1 Viewing Data About the Root, CDB, and PDBs While Connected to the Root 4-32
4.10.6.2 Enabling Common Users to Query Data in Specific PDBs 4-33
4.11 Managing User Roles 4-33
4.11.1 About User Roles 4-34
4.11.1.1 What Are User Roles? 4-35
4.11.1.2 The Functionality of Roles 4-35
4.11.1.3 Properties of Roles and Why They Are Advantageous 4-36
4.11.1.4 Typical Uses of Roles 4-36
4.11.1.5 Common Uses of Application Roles 4-38
4.11.1.6 Common Uses of User Roles 4-38
4.11.1.7 How Roles Affect the Scope of a User's Privileges 4-38
4.11.1.8 How Roles Work in PL/SQL Blocks 4-38
4.11.1.9 How Roles Aid or Restrict DDL Usage 4-39
4.11.1.10 How Operating Systems Can Aid Roles 4-40
4.11.1.11 How Roles Work in a Distributed Environment 4-40
4.11.2 Predefined Roles in an Oracle Database Installation 4-40
4.11.3 Creating a Role 4-48
4.11.3.1 About the Creation of Roles 4-48
4.11.3.2 Creating a Role That Is Authenticated With a Password 4-49
4.11.3.3 Creating a Role That Has No Password Authentication 4-50
4.11.3.4 Creating a Role That Is External or Global 4-50
4.11.3.5 Altering a Role 4-51

4.11.4 Specifying the Type of Role Authorization 4-51
4.11.4.1 Authorizing a Role by Using the Database 4-51
4.11.4.2 Authorizing a Role by Using an Application 4-52
4.11.4.3 Authorizing a Role by Using an External Source 4-52
4.11.4.4 Authorizing a Role by Using the Operating System 4-53
4.11.4.5 Authorizing a Role by Using a Network Client 4-53
4.11.4.6 Authorizing a Global Role by an Enterprise Directory Service 4-53
4.11.5 Granting and Revoking Roles 4-54
4.11.5.1 About Granting and Revoking Roles 4-54
4.11.5.2 Who Can Grant or Revoke Roles? 4-55
4.11.5.3 Granting and Revoking Roles to and from Program Units 4-55
4.11.6 Dropping Roles 4-55
4.11.7 Restricting SQL*Plus Users from Using Database Roles 4-56
4.11.7.1 Potential Security Problems of Using Ad Hoc Tools 4-56
4.11.7.2 How the PRODUCT_USER_PROFILE System Table Can Limit Roles 4-57
4.11.7.3 How Stored Procedures Can Encapsulate Business Logic 4-57
4.11.8 Role Privileges and Secure Application Roles 4-57
4.12 Managing Common Roles and Local Roles 4-58
4.12.1 About Common Roles and Local Roles 4-59
4.12.2 Common Roles in a CDB 4-59
4.12.3 How Common Roles Work 4-60
4.12.4 How the PUBLIC Role Works in a Multitenant Environment 4-60
4.12.5 Privileges Required to Create, Modify, or Drop a Common Role 4-60
4.12.6 Rules for Creating Common Roles 4-60
4.12.7 Creating a Common Role 4-61
4.12.8 Rules for Creating Local Roles 4-61
4.12.9 Local Roles in a CDB 4-62
4.12.10 Creating a Local Role 4-62
4.12.11 Role Grants and Revokes for Common Users and Local Users 4-62
4.13 Restricting Operations on PDBs Using PDB Lockdown Profiles 4-63
4.13.1 About PDB Lockdown Profiles 4-64
4.13.2 How PDB Lockdown Profiles Work 4-64
4.13.3 PDB_OS_CREDENTIAL Initialization Parameter 4-66
4.13.4 Features That Benefit from PDB Lockdown Profiles 4-66
4.13.5 PDB Lockdown Profile Inheritance 4-67
4.13.6 Default PDB Lockdown Profiles 4-67
4.13.7 Creating a PDB Lockdown Profile 4-68
4.13.8 Enabling or Disabling a PDB Lockdown Profile 4-69
4.13.9 Dropping a PDB Lockdown Profile 4-71
4.14 Managing Object Privileges 4-72
4.14.1 About Object Privileges 4-72
4.14.2 Who Can Grant Object Privileges? 4-73

4.14.3 Grants and Revokes of Object Privileges 4-73
4.14.3.1 About Granting and Revoking Object Privileges 4-73
4.14.3.2 How the ALL Clause Grants or Revokes All Available Object Privileges 4-74
4.14.4 READ and SELECT Object Privileges 4-74
4.14.4.1 About Managing READ and SELECT Object Privileges 4-74
4.14.4.2 Enabling Users to Use the READ Object Privilege to Query Any Table in the Database 4-75
4.14.4.3 Restrictions on the READ and READ ANY TABLE Privileges 4-75
4.14.5 Object Privilege Use with Synonyms 4-75
4.14.6 Sharing Application Common Objects 4-76
4.14.6.1 Metadata-Linked Application Common Objects 4-77
4.14.6.2 Data-Linked Application Common Objects 4-77
4.14.6.3 Extended Data-Linked Application Common Objects 4-78
4.15 Managing Dictionary Protection for Oracle-Maintained Schemas 4-79
4.15.1 About Managing Dictionary Protection for Oracle-Maintained Schemas 4-79
4.15.2 Enabling Dictionary Protection in an Oracle-Maintained Schema 4-80
4.15.3 Disabling Dictionary Protection in an Oracle-Maintained Schema 4-80
4.16 Table Privileges 4-81
4.16.1 How Table Privileges Affect Data Manipulation Language Operations 4-81
4.16.2 How Table Privileges Affect Data Definition Language Operations 4-81
4.17 View Privileges 4-82
4.17.1 Privileges Required to Create Views 4-82
4.17.2 Privileges to Query Views in Other Schemas 4-83
4.17.3 The Use of Views to Increase Table Security 4-83
4.18 Procedure Privileges 4-84
4.18.1 The Use of the EXECUTE Privilege for Procedure Privileges 4-84
4.18.2 Procedure Execution and Security Domains 4-84
4.18.3 System Privileges Required to Create or Replace a Procedure 4-84
4.18.4 System Privileges Required to Compile a Procedure 4-85
4.18.5 How Procedure Privileges Affect Packages and Package Objects 4-85
4.18.5.1 About the Effect of Procedure Privileges on Packages and Package Objects 4-85
4.18.5.2 Example: Procedure Privileges Used in One Package 4-86
4.18.5.3 Example: Procedure Privileges and Package Objects 4-86
4.19 Type Privileges 4-87
4.19.1 System Privileges for Named Types 4-88
4.19.2 Object Privileges for Named Types 4-88
4.19.3 Method Execution Model for Named Types 4-88
4.19.4 Privileges Required to Create Types and Tables Using Types 4-89
4.19.5 Example: Privileges for Creating Types and Tables Using Types 4-89
4.19.6 Privileges on Type Access and Object Access 4-90
4.19.7 Type Dependencies 4-91

4.20 Grants of User Privileges and Roles 4-92
4.20.1 Granting System Privileges and Roles to Users and Roles 4-92
4.20.1.1 Privileges for Grants of System Privileges and Roles to Users and Roles 4-92
4.20.1.2 Example: Granting a System Privilege and a Role to a User 4-93
4.20.1.3 Example: Granting the EXECUTE Privilege on a Directory Object 4-93
4.20.1.4 Use of the ADMIN Option to Enable Grantee Users to Grant the Privilege 4-93
4.20.1.5 Creating a New User with the GRANT Statement 4-93
4.20.2 Granting Object Privileges to Users and Roles 4-94
4.20.2.1 About Granting Object Privileges to Users and Roles 4-94
4.20.2.2 How the WITH GRANT OPTION Clause Works 4-95
4.20.2.3 Grants of Object Privileges on Behalf of the Object Owner 4-95
4.20.2.4 Grants of Privileges on Columns 4-97
4.20.2.5 Row-Level Access Control 4-97
4.21 Revokes of Privileges and Roles from a User 4-97
4.21.1 Revokes of System Privileges and Roles 4-98
4.21.2 Revokes of Object Privileges 4-98
4.21.2.1 About Revokes of Object Privileges 4-98
4.21.2.2 Revokes of Multiple Object Privileges 4-99
4.21.2.3 Revokes of Object Privileges on Behalf of the Object Owner 4-99
4.21.2.4 Revokes of Column-Selective Object Privileges 4-100
4.21.2.5 Revokes of the REFERENCES Object Privilege 4-100
4.21.3 Cascading Effects of Revoking Privileges 4-101
4.21.3.1 Cascading Effects When Revoking System Privileges 4-101
4.21.3.2 Cascading Effects When Revoking Object Privileges 4-101
4.22 Grants and Revokes of Privileges to and from the PUBLIC Role 4-102
4.23 Grants of Roles Using the Operating System or Network 4-102
4.23.1 About Granting Roles Using the Operating System or Network 4-103
4.23.2 Operating System Role Identification 4-104
4.23.3 Operating System Role Management 4-105
4.23.4 Role Grants and Revokes When OS_ROLES Is Set to TRUE 4-105
4.23.5 Role Enablements and Disablements When OS_ROLES Is Set to TRUE 4-105
4.23.6 Network Connections with Operating System Role Management 4-105
4.24 How Grants and Revokes Work with SET ROLE and Default Role Settings 4-106
4.24.1 When Grants and Revokes Take Effect 4-106
4.24.2 How the SET ROLE Statement Affects Grants and Revokes 4-106
4.24.3 Specifying the Default Role for a User 4-107
4.24.4 The Maximum Number of Roles That a User Can Have Enabled 4-107
4.25 Configuring Read-Only Users 4-108
4.26 User Privilege and Role Data Dictionary Views 4-109
4.26.1 Data Dictionary Views to Find Information about Privilege and Role Grants 4-110
4.26.2 Query to List All System Privilege Grants 4-112
4.26.3 Query to List Schema Privilege Grants 4-112

4.26.4 Query to List All Role Grants 4-112
4.26.5 Query to List Object Privileges Granted to a User 4-113
4.26.6 Query to List the Current Privilege Domain of Your Session 4-113
4.26.7 Query to List Roles of the Database 4-114
4.26.8 Query to List Information About the Privilege Domains of Roles 4-114

5 Performing Privilege Analysis to Identify Privilege Use

5.1 What Is Privilege Analysis? 5-1
5.1.1 About Privilege Analysis 5-2
5.1.2 Benefits and Use Cases of Privilege Analysis 5-2
5.1.2.1 Least Privileges Best Practice 5-2
5.1.2.2 Development of Secure Applications 5-3
5.1.3 Who Can Perform Privilege Analysis? 5-3
5.1.4 Types of Privilege Analysis 5-3
5.1.5 How Does a Multitenant Environment Affect Privilege Analysis? 5-4
5.1.6 How Privilege Analysis Works with Pre-Compiled Database Objects 5-4
5.2 Creating and Managing Privilege Analysis Policies 5-5
5.2.1 About Creating and Managing Privilege Analysis Policies 5-5
5.2.2 General Steps for Managing Privilege Analysis 5-6
5.2.3 Creating a Privilege Analysis Policy 5-6
5.2.4 Examples of Creating Privilege Analysis Policies 5-8
5.2.4.1 Example: Privilege Analysis of Database-Wide Privileges 5-8
5.2.4.2 Example: Privilege Analysis of Privilege Usage of Two Roles 5-8
5.2.4.3 Example: Privilege Analysis of Privileges During SQL*Plus Use 5-9
5.2.4.4 Example: Privilege Analysis of PSMITH Privileges During SQL*Plus Access 5-9
5.2.5 Enabling a Privilege Analysis Policy 5-9
5.2.6 Disabling a Privilege Analysis Policy 5-10
5.2.7 Generating a Privilege Analysis Report 5-10
5.2.7.1 About Generating a Privilege Analysis Report 5-11
5.2.7.2 General Process for Managing Multiple Named Capture Runs 5-11
5.2.7.3 Generating a Privilege Analysis Report Using DBMS_PRIVILEGE_CAPTURE 5-12
5.2.7.4 Generating a Privilege Analysis Report Using Cloud Control 5-13
5.2.7.5 Accessing Privilege Analysis Reports Using Cloud Control 5-13
5.2.8 Dropping a Privilege Analysis Policy 5-14
5.3 Creating Roles and Managing Privileges Using Cloud Control 5-14
5.3.1 Creating a Role from a Privilege Analysis Report in Cloud Control 5-15
5.3.2 Revoking and Regranting Roles and Privileges Using Cloud Control 5-15
5.3.3 Generating a Revoke or Regrant Script Using Cloud Control 5-16
5.3.3.1 About Generating Revoke and Regrant Scripts 5-16
5.3.3.2 Generating a Revoke Script 5-16

5.3.3.3 Generating a Regrant Script 5-17
5.4 Tutorial: Using Capture Runs to Analyze ANY Privilege Use 5-18
5.4.1 Step 1: Create User Accounts 5-18
5.4.2 Step 2: Create and Enable a Privilege Analysis Policy 5-19
5.4.3 Step 3: Use the READ ANY TABLE System Privilege 5-20
5.4.4 Step 4: Disable the Privilege Analysis Policy 5-20
5.4.5 Step 5: Generate and View a Privilege Analysis Report 5-20
5.4.6 Step 6: Create a Second Capture Run 5-21
5.4.7 Step 7: Remove the Components for This Tutorial 5-22
5.5 Tutorial: Analyzing Privilege Use by a User Who Has the DBA Role 5-22
5.5.1 Step 1: Create User Accounts 5-23
5.5.2 Step 2: Create and Enable a Privilege Analysis Policy 5-24
5.5.3 Step 3: Perform the Database Tuning Operations 5-24
5.5.4 Step 4: Disable the Privilege Analysis Policy 5-25
5.5.5 Step 5: Generate and View Privilege Analysis Reports 5-25
5.5.6 Step 6: Remove the Components for This Tutorial 5-27
5.6 Tutorial: Capturing Schema Privilege Use 5-27
5.6.1 Step 1: Create User Accounts 5-27
5.6.2 Step 2: Create and Enable a Privilege Analysis Policy 5-28
5.6.3 Step 3: Use the READ ANY TABLE System Privilege 5-29
5.6.4 Step 4: Disable the Privilege Analysis Policy 5-29
5.6.5 Step 5: Generate and View Privilege Analysis Reports 5-29
5.6.6 Step 6: Remove the Components for This Tutorial 5-30
5.7 Privilege Analysis Policy and Report Data Dictionary Views 5-30

6 Configuring Centrally Managed Users with Microsoft Active Directory

6.1 Introduction to Centrally Managed Users with Microsoft Active Directory 6-1
6.1.1 About the Oracle Database-Microsoft Active Directory Integration 6-2
6.1.2 How Centrally Managed Users with Microsoft Active Directory Works 6-3
6.1.3 Centrally Managed User-Microsoft Active Directory Architecture 6-3
6.1.4 Supported Authentication Methods 6-4
6.1.5 Users Supported by Centrally Managed Users with Microsoft Active Directory 6-4
6.1.6 How the Oracle Multitenant Option Affects Centrally Managed Users 6-5
6.1.7 Centrally Managed Users with Database Links 6-5
6.2 Configuring the Oracle Database-Microsoft Active Directory Integration 6-6
6.2.1 About Configuring the Oracle Database-Microsoft Active Directory Connection 6-6
6.2.2 Connecting to Microsoft Active Directory 6-6
6.2.2.1 Step 1: Create an Oracle Service Directory User Account on Microsoft Active Directory and Grant Permissions 6-7
6.2.2.2 Step 2: For Password Authentication, Install the Password Filter and Extend the Microsoft Active Directory Schema 6-8
6.2.2.3 Step 3: If Necessary, Install the Oracle Database Software 6-10

6.2.2.4 Step 4: Create the dsi.ora or ldap.ora File 6-10
6.2.2.5 Step 5: Request an Active Directory Certificate for a Secure Connection 6-16
6.2.2.6 Step 6: Create the Wallet for a Secure Connection 6-17
6.2.2.7 Step 7: Configure the Microsoft Active Directory Connection 6-19
6.2.2.8 Step 8: Verify the Oracle Wallet 6-22
6.2.2.9 Step 9: Test the Integration 6-23
6.3 Configuring Authentication for Centrally Managed Users 6-24
6.3.1 Configuring Password Authentication for Centrally Managed Users 6-24
6.3.1.1 About Configuring Password Authentication for Centrally Managed Users 6-24
6.3.1.2 Configuring Password Authentication for a Centrally Managed User 6-25
6.3.1.3 Logging in to an Oracle Database Using Password Authentication 6-27
6.3.2 Configuring Proxy Authentication for Centrally Managed Users 6-27
6.3.2.1 About Configuring Proxy Authentication for Centrally Managed Users 6-28
6.3.2.2 Configuring Proxy Authentication for the Centrally Managed User 6-28
6.3.2.3 Validating the Centrally Managed User Proxy Authentication 6-29
6.3.3 Configuring Kerberos Authentication for Centrally Managed Users 6-29
6.3.4 Configuring Authentication Using PKI Certificates for Centrally Managed Users 6-30
6.4 Configuring Authorization for Centrally Managed Users 6-30
6.4.1 About Configuring Authorization for Centrally Managed Users 6-31
6.4.2 Mapping a Directory Group to a Shared Database Global User 6-32
6.4.3 Mapping a Directory Group to a Global Role 6-32
6.4.4 Exclusively Mapping a Directory User to a Database Global User 6-33
6.4.5 Altering or Migrating a User Mapping Definition 6-33
6.4.6 Configuring Administrative Users 6-34
6.4.6.1 Configuring Database Administrative Users with Shared Access Accounts 6-34
6.4.6.2 Configuring Database Administrative Users Using Exclusive Mapping 6-34
6.4.7 Verifying the Centrally Managed User Logon Information 6-35
6.5 Integration of Oracle Database with Microsoft Active Directory Account Policies 6-38
6.6 Configuring Centrally Managed Users with Oracle Autonomous Database 6-38
6.7 Troubleshooting Centrally Managed Users 6-38
6.7.1 ORA-01017 Connection Errors 6-39
6.7.2 ORA-28274 Connection Errors 6-39
6.7.3 ORA-28276 Connection Errors 6-40
6.7.4 ORA-28300 Connection Errors 6-41
6.7.5 Using Trace Files to Diagnose CMU Connection Errors 6-41

7 Authenticating and Authorizing IAM Users for Oracle DBaaS Databases

7.1 Introduction to Authenticating and Authorizing IAM Users for Oracle DBaaS 7-1
7.1.1 About Authenticating and Authorizing IAM Users for Oracle DBaaS 7-2
7.1.2 Architecture of the IAM Integration with Oracle DBaaS 7-4
7.1.3 IAM Users and Groups to Map with Oracle DBaaS 7-8

7.2 Configuring Oracle DBaaS for IAM 7-8
7.2.1 Enabling External Authentication for Oracle DBaaS 7-8
7.2.2 Configuring Authorization for IAM Users and Oracle Cloud Infrastructure Applications 7-9
7.2.2.1 About Configuring Authorization for IAM Users and Oracle Cloud Infrastructure Applications 7-10
7.2.2.2 Mapping an IAM Group to a Shared Oracle Database Global User 7-11
7.2.2.3 Mapping an IAM Group to an Oracle Database Global Role 7-12
7.2.2.4 Exclusively Mapping an IAM User to an Oracle Database Global User 7-12
7.2.2.5 Altering or Migrating an IAM User Mapping Definition 7-13
7.2.2.6 Mapping Instance and Resource Principals 7-13
7.2.2.7 Verifying the IAM User Logon Information 7-14
7.2.3 Configuring IAM Proxy Authentication 7-17
7.2.3.1 About Configuring IAM Proxy Authentication 7-17
7.2.3.2 Configuring Proxy Authentication for the IAM User 7-18
7.2.3.3 Validating the IAM User Proxy Authentication 7-18
7.3 Configuring IAM for Oracle DBaaS 7-19
7.3.1 Creating an IAM Policy to Authorize Users Authenticating with Tokens 7-19
7.3.2 Creating an IAM Database Password 7-20
7.4 Accessing the Database Using an Instance Principal or a Resource Principal 7-20
7.5 Configuring the Database Client Connection 7-21
7.5.1 About Connecting to an Autonomous Database Instance Using IAM 7-22
7.5.2 Supported Client Drivers for IAM Connections 7-22
7.5.3 Using Centralized Oracle Cloud Infrastructure Services for Net Naming and Secrets 7-22
7.5.4 Client Connections That Use an IAM Database Password Verifier 7-23
7.5.5 Client Connections That Use a Token Requested by an IAM User Name and Database Password 7-23
7.5.5.1 About Client Connections That Use a Token Requested by an IAM User Name and Database Password 7-23
7.5.5.2 Parameters to Set for Client Connections That Use a Token Requested by an IAM User Name and Database Password 7-24
7.5.5.3 Configuring the Database Client to Retrieve a Token Using an IAM User Name and Database Password 7-26
7.5.5.4 Configuring a Secure External Password Store Wallet to Retrieve an IAM Token 7-27
7.5.6 Client Connections That Use a Token Requested by a Client Application or Tool 7-27
7.5.7 TLS Connections without Client Wallets 7-28
7.5.8 Enabling Clients to Directly Retrieve IAM Tokens 7-28
7.5.9 Common Database Client Configurations 7-29
7.5.9.1 Configuring a Client Connection for SQL*Plus That Uses an IAM Database Password 7-29
7.5.9.2 Configuring a Client Connection for SQL*Plus That Uses an IAM Token 7-30
7.5.10 Using OCI Object Store for Network Service Configuration Information 7-32

7.6 Accessing a Database Cross-Tenancy Using an IAM Integration 7-32
7.6.1 About Cross-Tenancy Access for IAM Users to DBaaS Instances 7-32
7.6.2 Configuring Policies 7-33
7.6.2.1 Configuring the Source User Tenancy 7-34
7.6.2.2 Configuring the Target Database Resource Tenancy 7-34
7.6.2.3 Policy Examples for Cross-Tenancy Access 7-35
7.6.3 Mapping Database Schemas and Roles to Users and Groups in Another Tenancy 7-36
7.6.4 Configuring Database Clients for Cross-Tenancy Access 7-37
7.6.5 Requesting Cross-Tenancy Tokens Using the OCI Command-Line Interface 7-37
7.7 Database Links in an Oracle DBaaS-to-IAM Integration 7-37
7.8 Troubleshooting IAM Connections 7-38
7.8.1 Areas to Check on the Client-Side for ORA-01017 Errors 7-38
7.8.2 Database Client Trace Files 7-40
7.8.3 Check in the Oracle Cloud Infrastructure IAM and the Oracle Database for ORA-01017 Errors 7-41
7.8.4 ORA-01017 Errors Caused by Improperly Configured IAM Users 7-42
7.8.5 ORA-12599 and ORA-03114 Errors Caused When Trying to Access a Database Using a Token 7-43
7.8.6 Actions IAM Administrators Can Take to Address ORA-01017 Errors 7-43

8 Authenticating and Authorizing Microsoft Azure Users for Oracle Databases

8.1 Introduction to Oracle Database Integration with Microsoft Entra ID 8-1
8.1.1 About Integrating Oracle Database with Microsoft Entra ID 8-2
8.1.2 Architecture of Oracle Database Integration with Microsoft Entra ID 8-4
8.1.3 Azure Users Mapping to an Oracle Database Schema and Roles 8-5
8.1.4 Use Cases for Connecting to an Oracle Database Using Entra ID 8-6
8.1.5 General Process of Authenticating Microsoft Entra ID Identities with Oracle Database 8-7
8.2 Configuring the Oracle Database for Microsoft Entra ID Integration 8-8
8.2.1 Oracle Database Requirements for the Microsoft Entra ID Integration 8-8
8.2.2 Registering the Oracle Database Instance with a Microsoft Entra ID Tenancy 8-9
8.2.3 Enabling Microsoft Entra ID v2 Access Tokens 8-13
8.2.4 Managing App Roles in Microsoft Entra ID 8-13
8.2.4.1 Creating a Microsoft Entra ID App Role 8-14
8.2.4.2 Assigning Users and Groups to the Microsoft Entra ID App Role 8-15
8.2.4.3 Assigning an Application to an App Role 8-15
8.2.5 Enabling Entra ID External Authentication for Oracle Database 8-16
8.2.6 Disabling Entra ID External Authentication for Oracle Database 8-17
8.3 Mapping Oracle Database Schemas and Roles 8-18
8.3.1 Exclusively Mapping an Oracle Database Schema to a Microsoft Azure User 8-18

8.3.2 Mapping a Shared Oracle Schema to an App Role 8-18
8.3.3 Mapping an Oracle Database Global Role to an App Role 8-19
8.4 Configuring Entra ID Client Connections to the Oracle Database 8-19
8.4.1 About Configuring Client Connections to Entra ID 8-20
8.4.2 Operational Flow for SQL*Plus Client Connection to Oracle Database Using Microsoft Entra ID OAuth2 Token 8-21
8.4.3 Supported Client Drivers for Entra ID Connections 8-24
8.4.4 Registering a Client with Entra ID Application Registration 8-24
8.4.4.1 Confidential and Public Client Registration 8-25
8.4.4.2 Registering a Database Client App with Entra ID 8-25
8.4.5 Configuration of Clients to Work with Microsoft Entra ID Tokens 8-27
8.4.5.1 Configuring Clients to Work with Microsoft Entra ID Tokens 8-27
8.4.5.2 Enabling Clients to Directly Retrieve Entra ID Tokens 8-28
8.4.5.3 Client Credential Flow 8-30
8.4.5.4 Enabling Clients to Retrieve Entra ID Tokens from a File Location 8-33
8.4.5.5 Using Azure App Configuration Store for Network Service Configuration Information 8-34
8.4.6 Examples of Retrieving Entra ID OAuth2 Tokens Outside an Oracle Database Client 8-34
8.4.6.1 About Examples of Retrieving Microsoft Entra ID OAuth2 Tokens Outside of an Oracle Database Client 8-34
8.4.6.2 Example: Requesting a Token Using a Python Script for the Interactive (Authorization) Flow 8-35
8.4.6.3 Example: Requesting a Token Using Azure CLI for the Interactive (Authorization) Flow 8-35
8.4.6.4 Requesting a Token Using the Azure CLI for the Client Credential Flow 8-36
8.4.7 Creating a Network Proxy for the Database to Connect with the Internet 8-36
8.4.7.1 About Creating a Network Proxy for the Database to Connect with the Internet 8-37
8.4.7.2 Testing the Accessibility of the Entra ID Endpoint 8-37
8.4.7.3 Creating the Network Proxy for the Default Oracle Database Environment 8-39
8.4.7.4 Creating the Network Proxy for an Oracle Real Application Clusters Environment 8-39
8.4.7.5 Creating the Network Proxy in the Windows Registry Editor 8-40
8.4.8 Using Centralized Entra ID Services for Net Naming and Secrets 8-41
8.5 Configuring Microsoft Entra ID Proxy Authentication 8-41
8.5.1 About Configuring Microsoft Entra ID Proxy Authentication 8-41
8.5.2 Configuring Proxy Authentication for the Azure User 8-42
8.5.3 Validating the Azure User Proxy Authentication 8-42
8.6 Configuring Microsoft Power BI Single-Sign On 8-42
8.6.1 About Configuring Microsoft Power BI Single-Sign On 8-43
8.6.2 Configuring the Oracle Database 8-44
8.6.3 Authorizing the User 8-45
8.6.4 Connecting Power BI to Oracle Database using Microsoft Entra ID 8-45

8.7 Troubleshooting Microsoft Entra ID Connections 8-45
8.7.1 Trace Files for Troubleshooting Oracle Database Client Connections with Entra ID 8-46
8.7.1.1 About Trace Files Used for Troubleshooting Connections 8-46
8.7.1.2 Setting Client Tracing for Token Authentication 8-47
8.7.2 ORA-12599 and ORA-03114 Errors Caused When Trying to Access a Database Using a Token 8-47
8.7.3 Checking the Entra ID Access Token Version 8-48

9 Managing Security for Definer's Rights and Invoker's Rights

9.1 About Definer's Rights and Invoker's Rights 9-1
9.2 How Procedure Privileges Affect Definer's Rights 9-2
9.3 How Procedure Privileges Affect Invoker's Rights 9-3
9.4 When You Should Create Invoker's Rights Procedures 9-4
9.5 Controlling Invoker's Rights Privileges for Procedure Calls and View Access 9-4
9.5.1 How the Privileges of a Schema Affect the Use of Invoker's Rights Procedures 9-5
9.5.2 How the INHERIT [ANY] PRIVILEGES Privileges Control Privilege Access 9-6
9.5.3 Grants of the INHERIT PRIVILEGES Privilege to Other Users 9-6
9.5.4 Example: Granting INHERIT PRIVILEGES on an Invoking User 9-7
9.5.5 Example: Revoking INHERIT PRIVILEGES 9-7
9.5.6 Grants of the INHERIT ANY PRIVILEGES Privilege to Other Users 9-7
9.5.7 Example: Granting INHERIT ANY PRIVILEGES to a Trusted Procedure Owner 9-7
9.5.8 Managing INHERIT PRIVILEGES and INHERIT ANY PRIVILEGES 9-8
9.6 Definer's Rights and Invoker's Rights in Views 9-8
9.6.1 About Controlling Definer's Rights and Invoker's Rights in Views 9-9
9.6.2 Using the BEQUEATH Clause in the CREATE VIEW Statement 9-9
9.6.3 Finding the User Name or User ID of the Invoking User 9-10
9.6.4 Finding BEQUEATH DEFINER and BEQUEATH_CURRENT_USER Views 9-10
9.7 Using Code Based Access Control for Definer's Rights and Invoker's Rights 9-11
9.7.1 About Using Code Based Access Control for Applications 9-11
9.7.2 Who Can Grant Code Based Access Control Roles to a Program Unit? 9-12
9.7.3 How Code Based Access Control Works with Invoker's Rights Program Units 9-12
9.7.4 How Code Based Access Control Works with Definer's Rights Program Units 9-14
9.7.5 Grants of Database Roles to Users for Their CBAC Grants 9-15
9.7.6 Grants and Revokes of Database Roles to a Program Unit 9-16
9.7.7 Tutorial: Controlling Access to Sensitive Data Using Code Based Access Control 9-17
9.7.7.1 About This Tutorial 9-17
9.7.7.2 Step 1: Create the User and Grant HR the CREATE ROLE Privilege 9-18
9.7.7.3 Step 2: Create the print_employees Invoker's Rights Procedure 9-18
9.7.7.4 Step 3: Create the hr_clerk Role and Grant Privileges for It 9-19
9.7.7.5 Step 4: Test the Code Based Access Control HR.print_employees Procedure 9-19

9.7.7.6 Step 5: Create the view_emp_role Role and Grant Privileges for It 9-20
9.7.7.7 Step 6: Test the HR.print_employees Procedure Again 9-20
9.7.7.8 Step 7: Remove the Components of This Tutorial 9-21
9.8 Controlling Definer's Rights Privileges for Database Links 9-21
9.8.1 About Controlling Definer's Rights Privileges for Database Links 9-22
9.8.2 Grants of the INHERIT REMOTE PRIVILEGES Privilege to Other Users 9-23
9.8.3 Example: Granting INHERIT REMOTE PRIVILEGES on a Connected User 9-23
9.8.4 Grants of the INHERIT ANY REMOTE PRIVILEGES Privilege to Other Users 9-24
9.8.5 Revokes of the INHERIT [ANY] REMOTE PRIVILEGES Privilege 9-24
9.8.6 Example: Revoking the INHERIT REMOTE PRIVILEGES Privilege 9-25
9.8.7 Example: Revoking the INHERIT REMOTE PRIVILEGES Privilege from PUBLIC 9-25
9.8.8 Tutorial: Using a Database Link in a Definer's Rights Procedure 9-25
9.8.8.1 About This Tutorial 9-26
9.8.8.2 Step 1: Create User Accounts 9-26
9.8.8.3 Step 2: As User dbuser2, Create a Table to Store User IDs 9-26
9.8.8.4 Step 3: As User dbuser1, Create a Database Link and Definer's Rights Procedure 9-27
9.8.8.5 Step 4: Test the Definer's Rights Procedure 9-27
9.8.8.6 Step 5: Remove the Components of This Tutorial 9-28

10 Managing Fine-Grained Access in PL/SQL Packages and Types

10.1 About Managing Fine-Grained Access in PL/SQL Packages and Types 10-2
10.2 About Fine-Grained Access Control to External Network Services 10-2
10.3 About Access Control to Oracle Wallets 10-3
10.4 Upgraded Applications That Depend on Packages That Use External Network Services 10-3
10.5 Configuring Access Control for External Network Services 10-4
10.5.1 Syntax for Configuring Access Control for External Network Services 10-4
10.5.2 Enabling the Listener to Recognize Access Control for External Network Services 10-6
10.5.3 Example: Configuring Access Control for External Network Services 10-6
10.5.4 Revoking Access Control Privileges for External Network Services 10-7
10.5.5 Example: Revoking External Network Services Privileges 10-7
10.6 Configuring Access Control to an Oracle Wallet 10-7
10.6.1 About Configuring Access Control to an Oracle Wallet 10-8
10.6.2 Step 1: Configure the Operating System Certificate Store as the Default Wallet Path 10-8
10.6.3 Step 2: Configure Access Control Privileges for the Oracle Wallet 10-8
10.6.4 Step 3: Make the HTTP Request with the Passwords and Client Certificates 10-10
10.6.4.1 Making the HTTPS Request with the Passwords and Client Certificates 10-10
10.6.4.2 Using a Request Context to Hold the Wallet When Sharing the Session with Other Applications 10-11

10.6.4.3 Use of Only a Client Certificate to Authenticate 10-12
10.6.4.4 Use of a Password to Authenticate 10-12
10.6.5 Revoking Access Control Privileges for Oracle Wallets 10-13
10.6.6 Troubleshooting ORA-29024 Errors 10-13
10.7 Examples of Configuring Access Control for External Network Services 10-14
10.7.1 Example: Configuring Access Control for a Single Role and Network Connection 10-14
10.7.2 Example: Configuring Access Control for a User and Role 10-15
10.7.3 Example: Using the DBA_HOST_ACES View to Show Granted Privileges 10-15
10.7.4 Example: Configuring ACL Access Using Passwords in a Non-Shared Wallet 10-16
10.7.5 Example: Configuring ACL Access for a Wallet in a Shared Database Session 10-17
10.8 Specifying a Group of Network Host Computers 10-18
10.9 Precedence Order for a Host Computer in Multiple Access Control List Assignments 10-18
10.10 Precedence Order for a Host in Access Control List Assignments with Port Ranges 10-19
10.11 Checking Privilege Assignments That Affect User Access to Network Hosts 10-19
10.11.1 About Privilege Assignments that Affect User Access to Network Hosts 10-20
10.11.2 How to Check User Network Connection and Domain Privileges 10-20
10.11.3 Example: Administrator Checking User Network Access Control Permissions 10-21
10.11.4 How Users Can Check Their Network Connection and Domain Privileges 10-21
10.11.5 Example: User Checking Network Access Control Permissions 10-22
10.12 Configuring Network Access for Java Debug Wire Protocol Operations 10-22
10.13 Data Dictionary Views for Access Control Lists Configured for User Access 10-23

11 Managing Security for a Multitenant Environment in Enterprise Manager

11.1 About Managing Security for a Multitenant Environment in Enterprise Manager 11-1
11.2 Logging into a Multitenant Environment in Enterprise Manager 11-1
11.2.1 Logging into a CDB or a PDB 11-1
11.2.2 Switching to a Different PDB or to the Root 11-2
11.3 Managing Common and Local Users in Enterprise Manager 11-3
11.3.1 Creating a Common User Account in Enterprise Manager 11-3
11.3.2 Editing a Common User Account in Enterprise Manager 11-4
11.3.3 Dropping a Common User Account in Enterprise Manager 11-5
11.3.4 Creating a Local User Account in Enterprise Manager 11-5
11.3.5 Editing a Local User Account in Enterprise Manager 11-6
11.3.6 Dropping a Local User Account in Enterprise Manager 11-6
11.4 Managing Common and Local Roles and Privileges in Enterprise Manager 11-7
11.4.1 Creating a Common Role in Enterprise Manager 11-7
11.4.2 Editing a Common Role in Enterprise Manager 11-8
11.4.3 Dropping a Common Role in Enterprise Manager 11-9
11.4.4 Revoking Common Privilege Grants in Enterprise Manager 11-9
11.4.5 Creating a Local Role in Enterprise Manager 11-9

11.4.6 Editing a Local Role in Enterprise Manager 11-10
11.4.7 Dropping a Local Role in Enterprise Manager 11-10
11.4.8 Revoking Local Privilege Grants in Enterprise Manager 11-11

Part II Application Development Security

12 Managing Security for Application Developers

12.1 About Application Security Policies 12-2
12.2 Considerations for Using Application-Based Security 12-2
12.2.1 Are Application Users Also Database Users? 12-2
12.2.2 Is Security Better Enforced in the Application or in the Database? 12-3
12.3 Use of the DB_DEVELOPER_ROLE Role for Application Developers 12-4
12.4 Securing Passwords in Application Design 12-7
12.4.1 General Guidelines for Securing Passwords in Applications 12-7
12.4.1.1 Platform-Specific Security Threats 12-7
12.4.1.2 Guidelines for Designing Applications to Handle Password Input 12-8
12.4.1.3 Guidelines for Configuring Password Formats and Behavior 12-9
12.4.1.4 Guidelines for Handling Passwords in SQL Scripts 12-10
12.4.2 Use of an External Password Store to Secure Passwords 12-11
12.4.3 Securing Passwords Using the ORAPWD Utility 12-11
12.4.4 Example: Java Code for Reading Passwords 12-11
12.5 Securing External Procedures 12-16
12.5.1 About Securing External Procedures 12-16
12.5.2 General Process for Configuring extproc for a Credential Authentication 12-16
12.5.3 extproc Process Authentication and Impersonation Expected Behaviors 12-17
12.5.4 Configuring Authentication for External Procedures 12-18
12.5.5 External Procedures for Legacy Applications 12-19
12.6 Securing LOBs with LOB Locator Signatures 12-20
12.6.1 About Securing LOBs with LOB Locator Signatures 12-20
12.6.2 Managing the Encryption of a LOB Locator Signature Key 12-20
12.7 Managing Application Privileges 12-21
12.8 Advantages of Using Roles to Manage Application Privileges 12-22
12.9 Creating Secure Application Roles to Control Access to Applications 12-22
12.9.1 Step 1: Create the Secure Application Role 12-22
12.9.2 Step 2: Create a PL/SQL Package to Define the Access Policy for the Application 12-23
12.9.2.1 About Creating a PL/SQL Package to Define the Access Policy for an Application 12-23
12.9.2.2 Creating a PL/SQL Package or Procedure to Define the Access Policy for an Application 12-24
12.9.2.3 Testing the Secure Application Role 12-25

12.10 Association of Privileges with User Database Roles 12-25
12.10.1 Why Users Should Only Have the Privileges of the Current Database Role 12-25
12.10.2 Use of the SET ROLE Statement to Automatically Enable or Disable Roles 12-26
12.11 Protecting Database Objects by Using Schemas 12-26
12.11.1 Protecting Database Objects in a Unique Schema 12-26
12.11.2 Protection of Database Objects in a Shared Schema 12-27
12.12 Object Privileges in an Application 12-27
12.12.1 What Application Developers Must Know About Object Privileges 12-28
12.12.2 SQL Statements Permitted by Object Privileges 12-28
12.13 Parameters for Enhanced Security of Database Communication 12-29
12.13.1 Bad Packets Received on the Database from Protocol Errors 12-30
12.13.2 Controlling Server Execution After Receiving a Bad Packet 12-30
12.13.3 Configuration of the Maximum Number of Authentication Attempts 12-31
12.13.4 Configuring the Display of the Database Version Banner 12-32
12.13.5 Configuring Banners for Unauthorized Access and Auditing User Actions 12-32

Part III Controlling Access to Data

13 Using Application Contexts to Retrieve User Information

13.1 About Application Contexts 13-1
13.1.1 What Is an Application Context? 13-2
13.1.2 Components of the Application Context 13-2
13.1.3 Where Are the Application Context Values Stored? 13-2
13.1.4 Benefits of Using Application Contexts 13-3
13.1.5 How Editions Affects Application Context Values 13-3
13.1.6 Application Contexts in a Multitenant Environment 13-3
13.2 Types of Application Contexts 13-4
13.3 Using Database Session-Based Application Contexts 13-5
13.3.1 About Database Session-Based Application Contexts 13-6
13.3.2 Components of a Database Session-Based Application Context 13-7
13.3.3 Creating Database Session-Based Application Contexts 13-8
13.3.3.1 About Creating Database Session-Based Application Contexts 13-8
13.3.3.2 Creating a Database Session-Based Application Context 13-8
13.3.3.3 Database Session-Based Application Contexts for Multiple Applications 13-9
13.3.4 Creating a Package to Set a Database Session-Based Application Context 13-9
13.3.4.1 About the Package That Manages the Database Session-Based Application Context 13-10
13.3.4.2 Using the SYS_CONTEXT Function to Retrieve Session Information 13-11
13.3.4.3 Checking the SYS_CONTEXT Settings 13-12
13.3.4.4 Dynamic SQL with SYS_CONTEXT 13-12
13.3.4.5 SYS_CONTEXT in a Parallel Query 13-12

13.3.4.6 SYS_CONTEXT with Database Links 13-13
13.3.4.7 DBMS_SESSION.SET_CONTEXT for Setting Session Information 13-13
13.3.4.8 Example: Simple Procedure to Create an Application Context Value 13-14
13.3.5 Logon Triggers to Run a Database Session Application Context Package 13-15
13.3.6 Example: Creating a Simple Logon Trigger 13-15
13.3.7 Example: Creating a Logon Trigger for a Production Environment 13-16
13.3.8 Example: Creating a Logon Trigger for a Development Environment 13-16
13.3.9 Tutorial: Creating and Using a Database Session-Based Application Context 13-17
13.3.9.1 Step 1: Create User Accounts and Ensure the User SCOTT Is Active 13-17
13.3.9.2 Step 2: Create the Database Session-Based Application Context 13-18
13.3.9.3 Step 3: Create a Package to Retrieve Session Data and Set the Application Context 13-18
13.3.9.4 Step 4: Create a Logon Trigger for the Package 13-19
13.3.9.5 Step 5: Test the Application Context 13-20
13.3.9.6 Step 6: Remove the Components of This Tutorial 13-20
13.3.10 Initializing Database Session-Based Application Contexts Externally 13-21
13.3.10.1 About Initializing Database Session-Based Application Contexts Externally 13-21
13.3.10.2 Default Values from Users 13-21
13.3.10.3 Values from Other External Resources 13-22
13.3.10.4 Example: Creating an Externalized Database Session-based Application Context 13-22
13.3.10.5 Initialization of Application Context Values from a Middle-Tier Server 13-22
13.3.11 Initializing Database Session-Based Application Contexts Globally 13-23
13.3.11.1 About Initializing Database Session-Based Application Contexts Globally 13-23
13.3.11.2 Database Session-Based Application Contexts with LDAP 13-24
13.3.11.3 How Globally Initialized Database Session-Based Application Contexts Work 13-25
13.3.11.4 Initializing a Database Session-Based Application Context Globally 13-26
13.3.12 Externalized Database Session-Based Application Contexts 13-27
13.4 Global Application Contexts 13-28
13.4.1 About Global Application Contexts 13-28
13.4.2 Uses for Global Application Contexts 13-29
13.4.3 Components of a Global Application Context 13-29
13.4.4 Global Application Contexts in an Oracle Real Application Clusters Environment 13-30
13.4.5 Creating Global Application Contexts 13-30
13.4.5.1 Ownership of the Global Application Context 13-30
13.4.5.2 Creating a Global Application Context 13-30
13.4.6 PL/SQL Package to Manage a Global Application Context 13-31
13.4.6.1 About the Package That Manages the Global Application Context 13-31
13.4.6.2 How Editions Affects the Results of a Global Application Context PL/SQL Package 13-32

13.4.6.3 DBMS_SESSION.SET_CONTEXT username and client_id Parameters 13-32
13.4.6.4 Sharing Global Application Context Values for All Database Users 13-33
13.4.6.5 Example: Package to Manage Global Application Values for All Database Users 13-34
13.4.6.6 Global Contexts for Database Users Who Move Between Applications 13-35
13.4.6.7 Global Application Context for Nondatabase Users 13-36
13.4.6.8 Example: Package to Manage Global Application Context Values for Nondatabase Users 13-37
13.4.6.9 Clearing Session Data When the Session Closes 13-39
13.4.7 Embedding Calls in Middle-Tier Applications to Manage the Client Session ID 13-40
13.4.7.1 About Managing Client Session IDs Using a Middle-Tier Application 13-40
13.4.7.2 Step 1: Retrieve the Client Session ID Using a Middle-Tier Application 13-40
13.4.7.3 Step 2: Set the Client Session ID Using a Middle-Tier Application 13-41
13.4.7.4 Step 3: Clear the Session Data Using a Middle-Tier Application 13-43
13.4.8 Tutorial: Creating a Global Application Context That Uses a Client Session ID 13-43
13.4.8.1 About This Tutorial 13-44
13.4.8.2 Step 1: Create User Accounts 13-44
13.4.8.3 Step 2: Create the Global Application Context 13-44
13.4.8.4 Step 3: Create a Package for the Global Application Context 13-45
13.4.8.5 Step 4: Test the Newly Created Global Application Context 13-46
13.4.8.6 Step 5: Modify the Session ID and Test the Global Application Context Again 13-47
13.4.8.7 Step 6: Remove the Components of This Tutorial 13-48
13.4.9 Global Application Context Processes 13-48
13.4.9.1 Simple Global Application Context Process 13-48
13.4.9.2 Global Application Context Process for Lightweight Users 13-49
13.5 Using Client Session-Based Application Contexts 13-51
13.5.1 About Client Session-Based Application Contexts 13-52
13.5.2 Setting a Value in the CLIENTCONTEXT Namespace 13-52
13.5.3 Retrieving the CLIENTCONTEXT Namespace 13-53
13.5.4 Example: Retrieving a Client Session ID Value for Client Session-Based Contexts 13-53
13.5.5 Clearing a Setting in the CLIENTCONTEXT Namespace 13-54
13.5.6 Clearing All Settings in the CLIENTCONTEXT Namespace 13-54
13.6 Application Context Data Dictionary Views 13-54

14 Using Oracle Virtual Private Database to Control Data Access

14.1 About Oracle Virtual Private Database 14-1
14.1.1 What Is Oracle Virtual Private Database? 14-2
14.1.2 Benefits of Using Oracle Virtual Private Database Policies 14-3
14.1.2.1 Security Policies Based on Database Objects Rather Than Applications 14-3
14.1.2.2 Control Over How Oracle Database Evaluates Policy Functions 14-3

14.1.3 Who Can Create Oracle Virtual Private Database Policies? 14-4
14.1.4 Privileges to Run Oracle Virtual Private Database Policy Functions 14-4
14.1.5 Oracle Virtual Private Database Use with an Application Context 14-4
14.1.6 Oracle Virtual Private Database in a Multitenant Environment 14-5
14.2 Components of an Oracle Virtual Private Database Policy 14-6
14.2.1 Function to Generate the Dynamic WHERE Clause 14-6
14.2.2 Policies to Attach the Function to the Objects You Want to Protect 14-8
14.3 Configuration of Oracle Virtual Private Database Policies 14-8
14.3.1 About Oracle Virtual Private Database Policies 14-9
14.3.2 Attaching a Policy to a Database Table, View, or Synonym 14-10
14.3.3 Example: Attaching a Simple Oracle Virtual Private Database Policy to a Table 14-11
14.3.4 Enforcing Policies on Specific SQL Statement Types 14-11
14.3.5 Example: Specifying SQL Statement Types with DBMS_RLS.ADD_POLICY 14-12
14.3.6 Control of the Display of Column Data with Policies 14-12
14.3.6.1 Policies for Column-Level Oracle Virtual Private Database 14-12
14.3.6.2 Example: Creating a Column-Level Oracle Virtual Private Database Policy 14-13
14.3.6.3 Display of Only the Column Rows Relevant to the Query 14-13
14.3.6.4 Column Masking to Display Sensitive Columns as NULL Values 14-14
14.3.6.5 Example: Adding Column Masking to an Oracle Virtual Private Database Policy 14-15
14.3.7 Oracle Virtual Private Database Policy Groups 14-16
14.3.7.1 About Oracle Virtual Private Database Policy Groups 14-16
14.3.7.2 Creation of a New Oracle Virtual Private Database Policy Group 14-17
14.3.7.3 Default Policy Group with the SYS_DEFAULT Policy Group 14-17
14.3.7.4 Multiple Policies for Each Table, View, or Synonym 14-18
14.3.7.5 Validation of the Application Used to Connect to the Database 14-18
14.3.8 Optimizing Performance by Using Oracle Virtual Private Database Policy Types 14-19
14.3.8.1 About Oracle Virtual Private Database Policy Types 14-20
14.3.8.2 Dynamic Policy Type to Automatically Rerun Policy Functions 14-20
14.3.8.3 Example: Creating a DYNAMIC Policy with DBMS_RLS.ADD_POLICY 14-21
14.3.8.4 Static Policy to Prevent Policy Functions from Rerunning for Each Query 14-21
14.3.8.5 Example: Creating a Static Policy with DBMS_RLS.ADD_POLICY 14-22
14.3.8.6 Example: Shared Static Policy to Share a Policy with Multiple Objects 14-22
14.3.8.7 When to Use Static and Shared Static Policies 14-23
14.3.8.8 Context-Sensitive Policy for Application Context Attributes That Change 14-23
14.3.8.9 Example: Creating a Context-Sensitive Policy with DBMS_RLS.ADD_POLICY 14-24
14.3.8.10 Example: Refreshing Cached Statements for a VPD Context-Sensitive Policy 14-24
14.3.8.11 Example: Altering an Existing Context-Sensitive Policy 14-25
14.3.8.12 Example: Using a Shared Context Sensitive Policy to Share a Policy with Multiple Objects 14-25

14.3.8.13 When to Use Context-Sensitive and Shared Context-Sensitive Policies 14-26
14.3.8.14 Summary of the Five Oracle Virtual Private Database Policy Types 14-26
14.4 Tutorials: Creating Oracle Virtual Private Database Policies 14-27
14.4.1 Tutorial: Creating a Simple Oracle Virtual Private Database Policy 14-27
14.4.1.1 About This Tutorial 14-28
14.4.1.2 Step 1: Ensure That the OE User Account Is Active 14-28
14.4.1.3 Step 2: Create a Policy Function 14-28
14.4.1.4 Step 3: Create the Oracle Virtual Private Database Policy 14-29
14.4.1.5 Step 4: Test the Policy 14-30
14.4.1.6 Step 5: Remove the Components of This Tutorial 14-30
14.4.2 Tutorial: Implementing a Session-Based Application Context Policy 14-31
14.4.2.1 About This Tutorial 14-31
14.4.2.2 Step 1: Create User Accounts and Sample Tables 14-31
14.4.2.3 Step 2: Create a Database Session-Based Application Context 14-33
14.4.2.4 Step 3: Create a PL/SQL Package to Set the Application Context 14-33
14.4.2.5 Step 4: Create a Logon Trigger to Run the Application Context PL/SQL Package 14-34
14.4.2.6 Step 5: Test the Logon Trigger 14-35
14.4.2.7 Step 6: Create a PL/SQL Policy Function to Limit User Access to Their Orders 14-35
14.4.2.8 Step 7: Create the New Security Policy 14-35
14.4.2.9 Step 8: Test the New Policy 14-36
14.4.2.10 Step 9: Remove the Components of This Tutorial 14-37
14.4.3 Tutorial: Implementing an Oracle Virtual Private Database Policy Group 14-37
14.4.3.1 About This Tutorial 14-38
14.4.3.2 Step 1: Create User Accounts and Other Components for This Tutorial 14-38
14.4.3.3 Step 2: Create the Two Policy Groups 14-39
14.4.3.4 Step 3: Create PL/SQL Functions to Control the Policy Groups 14-40
14.4.3.5 Step 4: Create the Driving Application Context 14-41
14.4.3.6 Step 5: Add the PL/SQL Functions to the Policy Groups 14-42
14.4.3.7 Step 6: Test the Policy Groups 14-42
14.4.3.8 Step 7: Remove the Components of This Tutorial 14-43
14.5 How Oracle Virtual Private Database Works with Other Oracle Features 14-44
14.5.1 Oracle Virtual Private Database Policies with Editions 14-44
14.5.2 SELECT FOR UPDATE Statement in User Queries on VPD-Protected Tables 14-45
14.5.3 Oracle Virtual Private Database Policies and Outer or ANSI Joins 14-45
14.5.4 Oracle Virtual Private Database Security Policies and Applications 14-45
14.5.5 Automatic Reparsing for Fine-Grained Access Control Policies Functions 14-46
14.5.6 Oracle Virtual Private Database Policies and Flashback Queries 14-46
14.5.7 Oracle Virtual Private Database and Oracle Label Security 14-46
14.5.7.1 Using Oracle Virtual Private Database to Enforce Oracle Label Security Policies 14-47
14.5.7.2 Oracle Virtual Private Database and Oracle Label Security Exceptions 14-47

14.5.8 Export of Data Using the EXPDP Utility access_method Parameter 14-48
14.5.9 Oracle Virtual Private Database Policies and Oracle Flashback Time Travel 14-49
14.5.10 User Models and Oracle Virtual Private Database 14-52
14.5.11 Oracle Virtual Private Database and JSON 14-53
14.6 Oracle Virtual Private Database Data Dictionary Views 14-53

15 Using Transparent Sensitive Data Protection

15.1 About Transparent Sensitive Data Protection 15-2
15.2 General Steps for Using Transparent Sensitive Data Protection 15-2
15.3 Benefits of Transparent Sensitive Data Protection Policies 15-3
15.4 Privileges Required for Using Transparent Sensitive Data Protection 15-4
15.5 How a Multitenant Environment Affects Transparent Sensitive Data Protection 15-4
15.6 Creating Transparent Sensitive Data Protection Policies 15-5
15.6.1 Step 1: Create a Sensitive Type 15-6
15.6.2 Step 2: Identify the Sensitive Columns to Protect 15-6
15.6.3 Step 3: Import the Sensitive Columns List from ADM into Your Database 15-7
15.6.4 Step 4: Create the Transparent Sensitive Data Protection Policy 15-7
15.6.4.1 About Creating the Transparent Sensitive Data Protection Policy 15-8
15.6.4.2 Creating the Transparent Sensitive Data Protection Policy 15-8
15.6.4.3 Setting the Oracle Data Redaction or Virtual Private Database Feature Options 15-9
15.6.4.4 Setting Conditions for the Transparent Sensitive Data Protection Policy 15-10
15.6.4.5 Specifying the DBMS_TSDP_PROTECT.ADD_POLICY Procedure 15-10
15.6.5 Step 5: Associate the Policy with a Sensitive Type 15-11
15.6.6 Step 6: Enable the Transparent Sensitive Data Protection Policy 15-12
15.6.6.1 Enabling Protection for the Current Database in a Protected Source 15-12
15.6.6.2 Enabling Protection for a Specific Table Column 15-12
15.6.6.3 Enabling Protection for a Specific Column Type 15-13
15.6.7 Step 7: Optionally, Export the Policy to Other Databases 15-13
15.7 Altering Transparent Sensitive Data Protection Policies 15-13
15.8 Disabling Transparent Sensitive Data Protection Policies 15-14
15.9 Dropping Transparent Sensitive Data Protection Policies 15-15
15.10 Using the Predefined REDACT_AUDIT Policy for Redaction 15-16
15.10.1 About the REDACT_AUDIT Policy 15-17
15.10.2 Variables Associated with Sensitive Columns 15-17
15.10.2.1 About Variables Associated with Sensitive Columns 15-17
15.10.2.2 Bind Variables and Sensitive Columns in the Expressions of Conditions 15-18
15.10.2.3 A Bind Variable and a Sensitive Column Appearing in the Same SELECT Item 15-19
15.10.2.4 Bind Variables in Expressions Assigned to Sensitive Columns in INSERT or UPDATE Operations 15-19
15.10.3 How Bind Variables on Sensitive Columns Behave with Views 15-20

15.10.4 Disabling the REDACT_AUDIT Policy 15-20
15.10.5 Enabling the REDACT_AUDIT Policy 15-20
15.11 Transparent Sensitive Data Protection Policies with Data Redaction 15-21
15.12 Using Transparent Sensitive Data Protection Policies with Oracle VPD Policies 15-21
15.12.1 About Using TSDP Policies with Oracle Virtual Private Database Policies 15-22
15.12.2 DBMS_RLS.ADD_POLICY Parameters That Are Used for TSDP Policies 15-22
15.12.3 Tutorial: Creating a TSDP Policy That Uses Virtual Private Database Protection 15-24
15.12.3.1 Step 1: Create the hr_appuser User Account 15-24
15.12.3.2 Step 2: Identify the Sensitive Columns 15-25
15.12.3.3 Step 3: Create an Oracle Virtual Private Database Function 15-25
15.12.3.4 Step 4: Create and Enable a Transparent Sensitive Data Protection Policy 15-25
15.12.3.5 Step 5: Test the Transparent Sensitive Data Protection Policy 15-26
15.12.3.6 Step 6: Remove the Components of This Tutorial 15-27
15.13 Using Transparent Sensitive Data Protection Policies with Unified Auditing 15-28
15.13.1 About Using TSDP Policies with Unified Audit Policies 15-28
15.13.2 Unified Audit Policy Settings That Are Used with TSDP Policies 15-29
15.14 Using Transparent Sensitive Data Protection Policies with Fine-Grained Auditing 15-30
15.14.1 About Using TSDP Policies with Fine-Grained Auditing 15-30
15.14.2 Fine-Grained Auditing Parameters That Are Used with TSDP Policies 15-31
15.15 Using Transparent Sensitive Data Protection Policies with TDE Column Encryption 15-32
15.15.1 About Using TSDP Policies with TDE Column Encryption 15-33
15.15.2 TDE Column Encryption ENCRYPT Clause Settings Used with TSDP Policies 15-34
15.16 Transparent Sensitive Data Protection Data Dictionary Views 15-35

16 Encryption of Sensitive Credential Data in the Data Dictionary

16.1 About Encrypting Sensitive Credential Data in the Data Dictionary 16-1
16.2 How the Multitenant Option Affects the Encryption of Sensitive Data 16-2
16.3 Encrypting Sensitive Credential Data in System Tables 16-2
16.4 Rekeying Sensitive Credential Data in the SYS.LINK$ System Table 16-3
16.5 Deleting Sensitive Credential Data in System Tables 16-4
16.6 Restoring the Functioning of Database Links After a Lost Keystore 16-5
16.7 Data Dictionary Views for Encrypted Data Dictionary Credentials 16-6

17 Securing and Isolating Resources Using DbNest

17.1 About DbNest 17-1
17.2 How DbNest Works 17-1
17.2.1 Purpose of DbNest 17-2
17.2.2 Linux Namespaces 17-2
17.2.3 DbNest Properties 17-3

17.2.4 DbNest Architecture 17-4
17.2.5 User Interface for DbNest 17-5
17.2.5.1 DbNest Initialization Parameters 17-5
17.2.5.2 DbNest Configuration File 17-5
17.2.6 How Oracle Database Manages a Nest 17-7
17.3 Enabling DbNest 17-7
17.4 Configuring File System Isolation for a Database Nest 17-8

18 On-Demand Encryption of Data

18.1 About On-Demand Encryption of Data 18-1
18.2 Security Problems That Encryption Does Not Solve 18-2
18.2.1 Principle 1: Encryption Does Not Solve Access Control Problems 18-2
18.2.2 Principle 2: Encryption Does Not Protect Against a Malicious Administrator 18-3
18.2.3 Principle 3: Encrypting Everything Does Not Make Data Secure 18-4
18.3 Data Encryption Challenges 18-4
18.3.1 Encrypted Indexed Data 18-4
18.3.2 Generated Encryption Keys 18-5
18.3.3 Transmitted Encryption Keys 18-5
18.3.4 Storing Encryption Keys 18-6
18.3.4.1 About Storing Encryption Keys 18-6
18.3.4.2 Storage of Encryption Keys in the Database 18-6
18.3.4.3 Storage of Encryption Keys in the Operating System 18-7
18.3.4.4 Users Managing Their Own Encryption Keys 18-8
18.3.4.5 Manual Encryption with Transparent Database Encryption and Tablespace Encryption 18-8
18.3.5 Importance of Changing Encryption Keys 18-8
18.3.6 Encryption of Binary Large Objects 18-8
18.4 Data Encryption Storage with the DBMS_CRYPTO Package 18-9
18.5 Asymmetric Key Operations with the DBMS_CRYPTO Package 18-15
18.6 Examples of Using the Data Encryption API 18-15
18.6.1 Example: Data Encryption Procedure 18-16
18.6.2 Example: AES 256-Bit Data Encryption and Decryption Procedures 18-17
18.6.3 Example: Encryption and Decryption Procedures for BLOB Data 18-17
18.6.4 Example: Encrypting or Decrypting a Number String 18-21

Part IV Securing Data on the Network

19 Securing Data for Oracle Database Connections

20 Configuring Oracle Database Native Network Encryption and Data Integrity

20.1 About Oracle Database Native Network Encryption and Data Integrity 20-1
20.1.1 How Oracle Database Native Network Encryption and Integrity Works 20-2
20.1.2 Advanced Encryption Standard 20-2
20.1.3 Choosing Between Native Network Encryption and Transport Layer Security 20-2
20.2 Oracle Database Native Network Encryption Data Integrity 20-3
20.3 Data Encryption and Integrity sqlnet.ora Parameters 20-3
20.3.1 About the Data Encryption and Integrity Parameters 20-4
20.3.2 Sample sqlnet.ora File 20-5
20.4 Data Integrity Algorithms Support 20-6
20.5 Diffie-Hellman Based Key Negotiation 20-7
20.6 Configuration of Data Encryption and Integrity 20-7
20.6.1 About Activating Encryption and Integrity 20-8
20.6.2 About Negotiating Encryption and Integrity 20-8
20.6.2.1 About the Values for Negotiating Encryption and Integrity 20-9
20.6.2.2 REJECTED Configuration Parameter 20-10
20.6.2.3 ACCEPTED Configuration Parameter 20-10
20.6.2.4 REQUESTED Configuration Parameter 20-10
20.6.2.5 REQUIRED Configuration Parameter 20-11
20.6.3 Configuring Encryption and Integrity Parameters Using Oracle Net Manager 20-11
20.6.3.1 Configuring Encryption on the Client and the Server 20-11
20.6.3.2 Configuring Integrity on the Client and the Server 20-13
20.6.3.3 Enabling Both Oracle Native Encryption and SSL Authentication for Different Users Concurrently 20-14
20.7 Troubleshooting the Native Network Encryption Configuration 20-16
20.7.1 Checking if Native Network Encryption Is Enabled in the Current Session 20-16
20.7.2 ORA-12650 and ORA-12660 Errors in the Native Network Encryption Configuration 20-17

21 Configuring Transport Layer Security Encryption

21.1 Transport Layer Security (TLS) and the Oracle Database 21-1
21.1.1 Self-signed Certificate vs Public Certificate Authority (CA) Signed Certificate 21-2
21.1.2 One-way TLS vs Mutual TLS 21-2
21.1.3 TLS With or Without a Client Wallet 21-3
21.1.4 Certificate DN Matching 21-3
21.2 Configuring TLS for the Oracle Database and Client 21-4
21.2.1 About Configuring TLS for the Oracle Database 21-4
21.2.2 Configuring TLS Using a Public Certificate Authority Root of Trust for the Database Server Certificate 21-6
21.2.3 Configuring TLS with a Self-Signed Root Certificate 21-10

21.2.4 Configuring TLS Connection With a Client Wallet 21-16
21.2.5 Enabling Distinguished Name (DN) Matching 21-18
21.3 Advanced and Optional Configurations 21-20
21.3.1 Optional Parameters for Transport Layer Security 21-21
21.3.2 Mutual Transport Layer Security (mTLS) 21-23
21.3.2.1 Server Certificate DN Matching 21-27
21.3.3 Oracle Wallet Location 21-28
21.3.3.1 Configuring Wallet Location for the Client 21-28
21.3.3.2 Configuring Wallet Location for the Listener 21-29
21.3.3.3 Configuring PDB Wallet Location for server 21-30
21.3.3.4 Oracle Wallet Search Order 21-30
21.3.4 Enable Weak DN Matching 21-32
21.3.5 Private Key/Certificate Selection 21-33
21.3.5.1 Setting the SSL_CERTIFICATE_ALIAS Parameter 21-34
21.3.5.2 Setting the SSL_CERTIFICATE_THUMBPRINT Parameter 21-34
21.3.5.3 Setting the SSL_EXTENDED_KEY_USAGE Parameter 21-35
21.3.6 Transport Layer Security Encryption Combined with Authentication Methods 21-36
21.3.7 Specifying TLS Protocol and TLS Cipher Suites 21-37
21.3.7.1 Configuring TLS Protocol Versions 21-38
21.3.7.2 Configuring TLS Cipher Suites 21-39
21.3.7.3 Allowing Certificates from Earlier Algorithms 21-42
21.3.8 Certificate Validation with Certificate Revocation Lists 21-42
21.3.8.1 About Certificate Validation with Certificate Revocation Lists 21-43
21.3.8.2 What CRLs Should You Use? 21-43
21.3.8.3 How CRL Checking Works 21-43
21.3.8.4 Configuring Certificate Validation with Certificate Revocation Lists 21-44
21.3.8.5 Certificate Revocation List Management 21-46
21.3.8.6 Troubleshooting CRL Certificate Validation 21-51
21.3.8.7 Oracle Net Tracing File Error Messages Associated with Certificate Validation 21-52
21.4 TLS and Other Oracle Products 21-53
21.4.1 Transport Layer Security Connections in an Oracle Real Application Clusters Environment 21-53
21.4.1.1 Step 1: Configure TCPS Protocol Endpoints 21-54
21.4.1.2 Step 2: Ensure That the LOCAL_LISTENER Parameter Is Correctly Set on Each Node 21-55
21.4.1.3 Step 3: Create Transport Layer Security Wallets and Certificates 21-56
21.4.1.4 Step 4: Create a Wallet in Each Node of the Oracle RAC Cluster 21-59
21.4.1.5 Step 5: Define Wallet Locations in the listener.ora and sqlnet.ora Files 21-59
21.4.1.6 Step 6: Restart the Database Instances and Listeners 21-60
21.4.1.7 Step 7: Test the Cluster Node Configuration 21-60
21.4.1.8 Step 8: Test the Remote Client Configuration 21-60
21.5 Troubleshooting the Transport Layer Security Configuration 21-61

21.6 Migrating to and Configuring Transport Layer Security Version 1.3 21-64

Part V Managing Strong Authentication

22 Introduction to Strong Authentication

22.1 What Is Strong Authentication? 22-1
22.2 Centralized Authentication and Single Sign-On 22-2
22.3 How Centralized Network Authentication Works 22-2
22.4 Supported Strong Authentication Methods 22-3
22.4.1 About Kerberos 22-4
22.4.2 About Remote Authentication Dial-In User Service (RADIUS) 22-4
22.4.3 About Transport Layer Security 22-5
22.5 Oracle Database Native Network Encryption/Strong Authentication Architecture 22-6
22.6 System Requirements for Strong Authentication 22-7
22.7 Oracle Database Native Network Encryption and Strong Authentication Restrictions 22-8

23 Strong Authentication Administration Tools

23.1 About the Configuration and Administration Tools 23-1
23.2 Native Network Encryption and Strong Authentication Configuration Tools 23-1
23.2.1 About Oracle Net Manager 23-1
23.2.2 Kerberos Adapter Command-Line Utilities 23-2
23.3 orapki Utility for Public Key Infrastructure Credentials Management 23-3
23.4 Duties of Strong Authentication Administrators 23-3

24 Configuring Kerberos Authentication

24.1 Introduction to Kerberos on Oracle Database 24-1
24.1.1 Kerberos Components in a Typical Oracle Database Configuration 24-2
24.1.2 Tickets Used in the Kerberos Configuration 24-2
24.1.2.1 Kerberos Client Ticket Granting Ticket 24-3
24.1.2.2 Kerberos Client Service Ticket 24-4
24.1.3 Kerberos Server Key Distribution Center 24-4
24.1.4 How Oracle Database Works with Kerberos 24-5
24.1.5 Oracle Database Parameters Used in a Kerberos Configuration 24-6
24.1.6 How Authentication Works in an Oracle Database Kerberos Configuration 24-6
24.2 Enabling Kerberos Authentication 24-9
24.2.1 Step 1: Install Kerberos 24-9
24.2.2 Step 2: Configure a Service Principal for an Oracle Database Server 24-10
24.2.3 Step 3: Extract a Service Key Table from Kerberos 24-11
24.2.4 Step 4: Install an Oracle Database Server and an Oracle Client 24-12

24.2.5 Step 5: Configure Oracle Net Services and Oracle Database 24-12
24.2.6 Step 6: Configure Kerberos Authentication 24-12
24.2.6.1 Step 6A: Configure Kerberos on the Client and on the Database Server 24-12
24.2.6.2 Step 6B: Set the Initialization Parameters 24-14
24.2.6.3 Step 6C: Set sqlnet.ora Parameters (Optional) 24-14
24.2.6.4 Step 6D: Configure Kerberos to Use TCP or UDP (Optional) 24-16
24.2.7 Step 7: Create a Kerberos User 24-16
24.2.8 Step 8: Create an Externally Authenticated Oracle User 24-17
24.2.9 Step 9: Get an Initial Ticket for the Kerberos/Oracle User 24-17
24.3 Utilities for the Kerberos Authentication Adapter 24-18
24.3.1 okinit Utility Options for Obtaining the Initial Ticket 24-18
24.3.2 oklist Utility Options for Displaying Credentials 24-20
24.3.3 okdstry Utility Options for Removing Credentials from the Cache File 24-21
24.3.4 okcreate Utility Options for Automatic Keytab Creation 24-21
24.4 Connecting to an Oracle Database Server Authenticated by Kerberos 24-22
24.5 Configuring Interoperability with Microsoft Windows Server Domain Controller KDC 24-22
24.5.1 About Configuring Interoperability with a Microsoft Windows Server Domain Controller KDC 24-23
24.5.2 Step 1: Configure Oracle Kerberos Client for Microsoft Windows Server Domain Controller 24-23
24.5.2.1 Step 1A: Create the Client Kerberos Configuration Files 24-23
24.5.2.2 Step 1B: Specify the Oracle Configuration Parameters in the sqlnet.ora File 24-24
24.5.2.3 Step 1C: Optionally, Specify Additional Kerberos Principals Using tnsnames.ora 24-25
24.5.2.4 Step 1D: Specify the Listening Port Number 24-25
24.5.3 Step 2: Configure a Microsoft Windows Server Domain Controller KDC for the Oracle Client 24-26
24.5.3.1 Step 2A: Create the User Account 24-26
24.5.3.2 Step 2B: Create the Oracle Database Principal User Account and Keytab 24-26
24.5.4 Step 3: Configure Oracle Database for a Microsoft Windows Server Domain Controller KDC 24-27
24.5.4.1 Step 3A: Set Configuration Parameters in the sqlnet.ora File 24-27
24.5.4.2 Step 3B: Create an Externally Authenticated Oracle User 24-28
24.5.5 Step 4: Obtain an Initial Ticket for the Kerberos/Oracle User 24-28
24.6 Configuring Kerberos Authentication Fallback Behavior 24-28
24.7 Troubleshooting the Oracle Kerberos Authentication Configuration 24-29
24.7.1 Common Kerberos Configuration Problems 24-29
24.7.2 ORA-12631 Errors in the Kerberos Configuration 24-30
24.7.3 ORA-28575 Errors in the Kerberos Configuration 24-30
24.7.4 ORA-01017 Errors in the Kerberos Configuration 24-30
24.7.5 Enabling Tracing for Kerberos okinit Operations 24-32

25 Configuring PKI Certificate Authentication

25.1 How Oracle Database Uses Transport Layer Security for Authentication 25-1
25.2 Enabling Oracle Internet Directory to Use Transport Layer Security Authentication 25-2
25.3 Configuring User Authentication with Transport Layer Security 25-3
25.4 Configuring Transport Layer Security for Client Authentication and Encryption with X.509 Certificates 25-5
25.4.1 About Configuring TLS for Client Authentication and Encryption with X.509 Certificates 25-5
25.4.2 Configuring the Server for Authentication and Encryption with X.509 Certificates 25-5
25.4.2.1 Step 1: Create and Configure the Server Wallet for the X.509 Certificate 25-6
25.4.2.2 Step 2: Shut Down the Oracle Listener on the Server 25-7
25.4.2.3 Step 3: Configure the sqlnet.ora File on the Server 25-8
25.4.2.4 Step 4: For Logical Volume Management, Configure the Server listener.ora File 25-8
25.4.2.5 Step 5: For Grid Infrastructure, Configure the Server Listener Process 25-9
25.4.2.6 Step 6: Set Initialization Parameters on the Server 25-10
25.4.2.7 Step 7: Create an External Database User on the Server 25-10
25.4.2.8 Step 8: Restart and Check the Listener Process on the Server 25-10
25.4.3 Configuring the Client for Authentication and Encryption with X.509 Certificates 25-11
25.4.3.1 Step 1: Configure the sqlnet.ora File on the Client 25-11
25.4.3.2 Step 2: Configure the tnsnames.ora File on the Client 25-12
25.4.3.3 Step 3: Configure Microsoft Certificate Store on the Client 25-12
25.5 Configuring Email over Transport Layer Security with an Oracle Wallet 25-16
25.6 Troubleshooting Transport Layer Security Errors 25-22
25.6.1 Step 1: Check the TLS Connection with the tnsping Utility 25-22
25.6.2 Step 2: Check the SSL_VERSION Parameter 25-23
25.6.3 Step 3: Check the Wallet File Permissions 25-23
25.6.4 Step 4: Check the Wallet Settings in the sqlnet.ora and listener.ora Files 25-24
25.6.5 Step 5: Enable Tracing for the SQL*Net and Listener Connections 25-25

26 Configuring RADIUS Authentication

26.1 About Configuring RADIUS Authentication 26-1
26.2 RADIUS Components 26-3
26.3 RADIUS Authentication Modes 26-3
26.3.1 Synchronous Authentication Mode 26-3
26.3.1.1 Sequence for Synchronous Authentication Mode 26-4
26.3.1.2 Example: Synchronous Authentication with Tokens 26-4
26.3.2 Challenge-Response (Asynchronous) Authentication Mode 26-5
26.3.2.1 Sequence for Challenge-Response (Asynchronous) Authentication Mode 26-5
26.3.2.2 Example: Asynchronous Authentication with Tokens 26-7

26.4 RADIUS Parameters 26-7
26.4.1 RADIUS Parameters for Clients and Servers 26-7
26.4.2 Minimum RADIUS Parameters 26-8
26.4.3 Initialization File Parameter for RADIUS 26-8
26.5 Enabling RADIUS Authentication, Authorization, and Accounting 26-9
26.5.1 Step 1: Configure RADIUS Authentication 26-9
26.5.1.1 Step 1A: Configure RADIUS on the Oracle Client 26-9
26.5.1.2 Step 1B: Configure RADIUS on the Oracle Database Server 26-10
26.5.1.3 Step 1C: Configure Additional RADIUS Features 26-13
26.5.2 Step 2: Create a User and Grant Access 26-15
26.5.3 Step 3: Configure External RADIUS Authorization (Optional) 26-16
26.5.3.1 Step 3A: Configure the Oracle Server (RADIUS Client) 26-16
26.5.3.2 Step 3B: Configure the Oracle Client Where Users Log In 26-16
26.5.3.3 Step 3C: Configure the RADIUS Server 26-16
26.5.4 Step 4: Configure RADIUS Accounting 26-17
26.5.4.1 Step 4A: Set RADIUS Accounting on the Oracle Database Server 26-18
26.5.4.2 Step 4B: Configure the RADIUS Accounting Server 26-18
26.5.5 Step 5: Add the RADIUS Client Name to the RADIUS Server Database 26-18
26.5.6 Step 6: Configure the Authentication Server for Use with RADIUS 26-19
26.5.7 Step 7: Configure the RADIUS Server for Use with the Authentication Server 26-19
26.5.8 Step 8: Configure Mapping Roles 26-19
26.6 Using RADIUS to Log in to a Database 26-20
26.7 Integrating Authentication Devices Using RADIUS 26-20
26.7.1 About the RADIUS Challenge-Response User Interface 26-20
26.7.2 Customizing the RADIUS Challenge-Response User Interface 26-21
26.7.3 Example: Using the OracleRadiusInterface Interface 26-21

27 Customizing the Use of Strong Authentication

27.1 Connecting to a Database Using Strong Authentication 27-1
27.2 Disabling Strong Authentication and Native Network Encryption 27-2
27.3 Configuring Multiple Authentication Methods 27-4
27.4 Configuring Oracle Database for External Authentication 27-5
27.4.1 Setting the SQLNET.AUTHENTICATION_SERVICES Parameter in sqlnet.ora 27-5
27.4.2 Setting OS_AUTHENT_PREFIX to a Null Value 27-6

Part VI Monitoring Database Activity with Auditing

28 Introduction to Auditing

28.1 What Is Auditing? 28-1
28.2 Why Is Auditing Used? 28-3

28.3 Best Practices for Auditing 28-4
28.4 Unified Auditing and Its Benefits 28-5
28.5 Who Can Perform Auditing? 28-6
28.6 Handling the Desupport of Traditional Auditing 28-8
28.7 Unified Auditing in a Multitenant Environment 28-9
28.8 Auditing in a Distributed Database 28-10

29 Provisioning Audit Policies

29.1 Getting Started with Auditing 29-1
29.2 About Audit Policies 29-2
29.3 Activities That Are Mandatorily Audited 29-3
29.4 Auditing Activities with the Predefined Unified Audit Policies 29-4
29.4.1 About Auditing Activities with the Predefined Unified Audit Policies 29-5
29.4.2 Secure Options Predefined Unified Audit Policy 29-6
29.4.3 Oracle Database Parameter Changes Predefined Unified Audit Policy 29-7
29.4.4 User Account and Privilege Management Predefined Unified Audit Policy 29-7
29.4.5 Center for Internet Security Recommendations Predefined Unified Audit Policy 29-8
29.4.6 Security Technical Implementation Guide Predefined Unified Audit Policies 29-9
29.4.6.1 STIG Recommendations Predefined Unified Audit Policy 29-9
29.4.6.2 All Top Level Actions Predefined Unified Audit Policy 29-10
29.4.6.3 Logon and Logout Predefined Unified Audit Policy 29-10
29.4.7 ORA_DICTIONARY Sensitive Column Queries Predefined Unified Audit Policy 29-11
29.4.8 Oracle Database Real Application Security Predefined Audit Policies 29-11
29.4.8.1 System Administrator Operations Predefined Unified Audit Policy 29-12
29.4.8.2 Session Operations Predefined Unified Audit Policy 29-12
29.4.9 Oracle Database Vault Predefined Unified Audit Policy for DVSYS and LBACSYS Schemas 29-13
29.4.10 Oracle Database Vault Predefined Unified Audit Policy for Default Realms and Command Rules 29-13
29.4.11 Oracle Label Security Predefined Unified Audit Policy for LBACSYS Objects 29-14
29.5 Steps to Provision Unified Audit Policies 29-14
29.5.1 Auditing Most Commonly Used Security-Relevant Activities 29-15
29.5.2 Auditing SQL Statements, Privileges, and Other Activities of Interest 29-15
29.5.3 Value-Based Fine-Grained Audit Activities 29-16
29.6 Common Audit Configurations Across All PDBs 29-16
29.7 General Audit Data Dictionary Views 29-17

30 Creating Custom Unified Audit Policies

30.1 About Custom Unified Audit Policies 30-1
30.2 Best Practices for Creating Custom Unified Audit Policies 30-2
30.3 Syntax for Creating a Custom Unified Audit Policy 30-2

30.4 Auditing Standard Oracle Database Components 30-4
30.4.1 Auditing Roles 30-5
30.4.1.1 About Role Auditing 30-5
30.4.1.2 Configuring Role Unified Audit Policies 30-5
30.4.1.3 Example: Auditing the Predefined Common DBA Role 30-6
30.4.2 Auditing System Privileges 30-6
30.4.2.1 About System Privilege Auditing 30-6
30.4.2.2 System Privileges That Can Be Audited 30-7
30.4.2.3 System Privileges That Cannot Be Audited 30-7
30.4.2.4 Configuring a Unified Audit Policy to Capture System Privilege Use 30-8
30.4.2.5 Example: Auditing a User Who Has ANY Privileges 30-8
30.4.2.6 Example: Using a Condition to Audit a System Privilege 30-8
30.4.2.7 How System Privilege Unified Audit Policies Appear in the Audit Trail 30-8
30.4.3 Auditing Administrative Users 30-9
30.4.3.1 Administrative User Accounts That Can Be Audited 30-9
30.4.3.2 Configuring a Unified Audit Policy to Capture Administrator Activities 30-10
30.4.3.3 Example: Auditing the SYS User 30-10
30.4.4 Auditing Object Actions 30-10
30.4.4.1 About Auditing Object Actions 30-11
30.4.4.2 Object Actions That Can Be Audited 30-11
30.4.4.3 Guidelines for Column Level Auditing and Virtual Columns 30-12
30.4.4.4 Configuring an Object Action Unified Audit Policy 30-13
30.4.4.5 Example: Auditing Actions on SYS Objects 30-13
30.4.4.6 Example: Auditing Multiple Actions on One Object 30-13
30.4.4.7 Example: Auditing GRANT and REVOKE Operations on an Object 30-13
30.4.4.8 Example: Auditing Both Actions and Privileges on an Object 30-14
30.4.4.9 Example: Auditing an Action on a Table Column 30-14
30.4.4.10 Example: Auditing All Actions on a Table 30-14
30.4.4.11 Example: Auditing All Actions in the Database 30-15
30.4.4.12 How Object Action Unified Audit Policies Appear in the Audit Trail 30-15
30.4.4.13 Auditing Functions, Procedures, Packages, and Triggers 30-16
30.4.4.14 Auditing of Oracle Virtual Private Database Predicates 30-16
30.4.4.15 Audit Policies for Oracle Virtual Private Database Policy Functions 30-18
30.4.4.16 Unified Auditing with Editioned Objects 30-18
30.4.5 Auditing the READ ANY TABLE and SELECT ANY TABLE Privileges 30-18
30.4.5.1 About Auditing the READ ANY TABLE and SELECT ANY TABLE Privileges 30-19
30.4.5.2 Creating a Unified Audit Policy to Capture READ Object Privilege Operations 30-19
30.4.5.3 How the Unified Audit Trail Captures READ ANY TABLE and SELECT ANY TABLE 30-19
30.4.6 Auditing Only Top-Level Statements 30-21
30.4.6.1 About Auditing Only Top-Level SQL Statements 30-22

30.4.6.2 Configuring a Unified Audit Policy to Capture Only Top-Level Statements 30-22
30.4.6.3 Example: Auditing Top-Level Statements 30-22
30.4.6.4 Example: Comparison of Top-Level SQL Statement Audits 30-23
30.4.6.5 How the Unified Audit Trail Captures Top-Level SQL Statements 30-28
30.5 Unified Auditing with Configurable Conditions 30-28
30.5.1 About Conditions in Unified Audit Policies 30-29
30.5.2 Configuring a Unified Audit Policy with a Condition 30-29
30.5.3 Example: Auditing Access to SQL*Plus 30-30
30.5.4 Example: Auditing Actions Not in Specific Hosts 30-31
30.5.5 Example: Auditing Both a System-Wide and a Schema-Specific Action 30-31
30.5.6 Example: Auditing a Condition Per Statement Occurrence 30-31
30.5.7 Example: Unified Audit Session ID of a Current Administrative User Session 30-32
30.5.8 Example: Unified Audit Session ID of a Current Non-Administrative User Session 30-32
30.5.9 How Audit Records from Conditions Appear in the Audit Trail 30-32
30.6 Auditing for Multitier or Multitenant Configurations 30-33
30.6.1 Auditing in a Multitier Deployment 30-33
30.6.2 Auditing in a Multitenant Deployment 30-35
30.6.2.1 About Local, CDB Common, and Application Common Audit Policies 30-36
30.6.2.2 Common Audit Configurations Across All PDBs 30-37
30.6.2.3 Unified Audit Policies in an Application Root 30-38
30.6.2.4 Configuring a Local Unified Audit Policy or Common Unified Audit Policy 30-38
30.6.2.5 Example: Local Unified Audit Policy 30-40
30.6.2.6 Example: CDB Common Unified Audit Policy 30-41
30.6.2.7 Example: Application Common Unified Audit Policy 30-41
30.6.2.8 How Local or Common Audit Policies or Settings Appear in the Audit Trail 30-42
30.7 Extending Unified Auditing to Capture Custom Attributes 30-42
30.7.1 About Auditing Application Context Values 30-43
30.7.2 Configuring Application Context Audit Settings 30-43
30.7.3 Disabling Application Context Audit Settings 30-44
30.7.4 Example: Auditing Application Context Values in a Default Database 30-44
30.7.5 Example: Auditing Application Context Values from Oracle Label Security 30-44
30.7.6 How Audited Application Contexts Appear in the Audit Trail 30-45
30.8 Auditing Components of Other Oracle Products and Features 30-45
30.8.1 Auditing Oracle SQL Firewall 30-46
30.8.1.1 About Auditing Oracle SQL Firewall 30-46
30.8.1.2 Example: Auditing Oracle SQL Firewall Violations 30-46
30.8.1.3 How Oracle SQL Firewall Events Appear in the Audit Trail 30-46
30.8.2 Auditing Oracle Database Vault Events 30-47
30.8.2.1 About Auditing Oracle Database Vault Events 30-48
30.8.2.2 Who Is Audited in Oracle Database Vault? 30-48
30.8.2.3 About Oracle Database Vault Unified Audit Trail Events 30-49

30.8.2.4 Oracle Database Vault Realm Audit Events 30-49
30.8.2.5 Oracle Database Vault Rule Set and Rule Audit Events 30-50
30.8.2.6 Oracle Database Vault Command Rule Audit Events 30-51
30.8.2.7 Oracle Database Vault Factor Audit Events 30-51
30.8.2.8 Oracle Database Vault Secure Application Role Audit Events 30-52
30.8.2.9 Oracle Database Vault Oracle Label Security Audit Events 30-53
30.8.2.10 Oracle Database Vault Oracle Data Pump Audit Events 30-53
30.8.2.11 Oracle Database Vault Enable and Disable Audit Events 30-54
30.8.2.12 Configuring a Unified Audit Policy for Oracle Database Vault 30-54
30.8.2.13 Example: Auditing an Oracle Database Vault Realm 30-55
30.8.2.14 Example: Auditing an Oracle Database Vault Rule Set 30-55
30.8.2.15 Example: Auditing Two Oracle Database Vault Events 30-55
30.8.2.16 Example: Auditing Oracle Database Vault Factors 30-55
30.8.2.17 How Oracle Database Vault Audited Events Appear in the Audit Trail 30-56
30.8.3 Auditing Oracle Database Real Application Security Events 30-56
30.8.3.1 About Auditing Oracle Database Real Application Security Events 30-57
30.8.3.2 Oracle Database Real Application Security Auditable Events 30-57
30.8.3.3 Oracle Database Real Application Security User, Privilege, and Role Audit Events 30-58
30.8.3.4 Oracle Database Real Application Security Security Class and ACL Audit Events 30-59
30.8.3.5 Oracle Database Real Application Security Session Audit Events 30-60
30.8.3.6 Oracle Database Real Application Security ALL Events 30-62
30.8.3.7 Configuring a Unified Audit Policy for Oracle Database Real Application Security 30-62
30.8.3.8 Example: Auditing Real Application Security User Account Modifications 30-62
30.8.3.9 Example: Using a Condition in a Real Application Security Unified Audit Policy 30-62
30.8.3.10 How Oracle Database Real Application Security Events Appear in the Audit Trail 30-63
30.8.4 Auditing Oracle Recovery Manager Events 30-63
30.8.4.1 About Auditing Oracle Recovery Manager Events 30-63
30.8.4.2 Oracle Recovery Manager Unified Audit Trail Events 30-64
30.8.4.3 How Oracle Recovery Manager Audited Events Appear in the Audit Trail 30-64
30.8.5 Auditing Oracle Label Security Events 30-65
30.8.5.1 About Auditing Oracle Label Security Events 30-65
30.8.5.2 Oracle Label Security Unified Audit Trail Events 30-66
30.8.5.3 Oracle Label Security Auditable User Session Labels 30-68
30.8.5.4 Configuring a Unified Audit Policy for Oracle Label Security 30-68
30.8.5.5 Example: Auditing Oracle Label Security Session Label Attributes 30-69
30.8.5.6 Example: Excluding a User from an Oracle Label Security Policy 30-69
30.8.5.7 Example: Auditing Oracle Label Security Policy Actions 30-69
30.8.5.8 Example: Querying for Audited OLS Session Labels 30-69

30.8.5.9 How Oracle Label Security Audit Events Appear in the Audit Trail 30-70
30.8.6 Auditing Oracle Data Pump Events 30-70
30.8.6.1 About Auditing Oracle Data Pump Events 30-71
30.8.6.2 Oracle Data Pump Unified Audit Trail Events 30-71
30.8.6.3 Configuring a Unified Audit Policy for Oracle Data Pump 30-71
30.8.6.4 Example: Auditing Oracle Data Pump Import Operations 30-71
30.8.6.5 Example: Auditing All Oracle Data Pump Operations 30-72
30.8.6.6 How Oracle Data Pump Audit Events Appear in the Audit Trail 30-72
30.8.7 Auditing Oracle SQL*Loader Direct Load Path Events 30-73
30.8.7.1 About Auditing in Oracle SQL*Loader Direct Path Load Events 30-73
30.8.7.2 Oracle SQL*Loader Direct Load Path Unified Audit Trail Events 30-73
30.8.7.3 Configuring a Unified Audit Trail Policy for Oracle SQL*Loader Direct Path Events 30-74
30.8.7.4 Example: Auditing Oracle SQL*Loader Direct Path Load Operations 30-74
30.8.7.5 How SQL*Loader Direct Path Load Audited Events Appear in the Audit Trail 30-74
30.8.8 Auditing Oracle XML DB HTTP and FTP Protocols 30-74
30.8.8.1 About Auditing Oracle XML DB HTTP and FTP Protocols 30-75
30.8.8.2 Configuring a Unified Audit Policy to Capture Oracle XML DB HTTP and FTP Protocols 30-75
30.8.8.3 Example: Auditing Failed Oracle XML DB HTTP Messages 30-75
30.8.8.4 Example: Auditing All Oracle XML DB FTP Messages 30-76
30.8.8.5 Example: Auditing Oracle XML DB HTTP Messages That Have 401 AUTH Errors 30-76
30.8.8.6 How the Unified Audit Trail Captures Oracle XML DB HTTP and FTP Protocol Messages 30-76
30.8.9 Auditing Oracle Machine Learning for SQL Events 30-77
30.8.9.1 About Auditing Oracle Machine Learning for SQL Events 30-77
30.8.9.2 Oracle Machine Learning for SQL Unified Audit Trail Events 30-77
30.8.9.3 Configuring a Unified Audit Policy for Oracle Machine Learning for SQL 30-78
30.8.9.4 Example: Auditing Multiple Oracle Machine Learning for SQL Operations by a User 30-78
30.8.9.5 Example: Auditing All Failed Oracle Machine Learning for SQL Operations by a User 30-78
30.8.9.6 How Oracle Machine Learning for SQL Events Appear in the Audit Trail 30-79
30.9 Managing Unified Audit Policies 30-80
30.9.1 Altering Unified Audit Policies 30-80
30.9.1.1 About Altering Unified Audit Policies 30-80
30.9.1.2 Altering a Unified Audit Policy 30-81
30.9.1.3 Example: Altering a Condition in a Unified Audit Policy 30-82
30.9.1.4 Example: Altering an Oracle Label Security Component in a Unified Audit Policy 30-82
30.9.1.5 Example: Altering Roles in a Unified Audit Policy 30-82
30.9.1.6 Example: Dropping a Condition from a Unified Audit Policy 30-83

30.9.1.7 Example: Altering an Existing Unified Audit Policy Top-Level Statement Audits 30-83
30.9.2 Enabling and Applying Unified Audit Policies to Users and Roles 30-83
30.9.2.1 About Enabling Unified Audit Policies 30-83
30.9.2.2 Enabling a Unified Audit Policy 30-85
30.9.2.3 Example: Enabling a Unified Audit Policy 30-85
30.9.3 Disabling Unified Audit Policies 30-86
30.9.3.1 About Disabling Unified Audit Policies 30-86
30.9.3.2 Disabling a Unified Audit Policy 30-86
30.9.3.3 Example: Disabling a Unified Audit Policy 30-87
30.9.4 Dropping Unified Audit Policies 30-87
30.9.4.1 About Dropping Unified Audit Policies 30-87
30.9.4.2 Dropping a Unified Audit Policy 30-88
30.9.4.3 Example: Disabling and Dropping a Unified Audit Policy 30-88
30.10 Tutorial: Auditing Nondatabase Users 30-88
30.10.1 Step 1: Create the User Accounts and Ensure the User OE Is Active 30-88
30.10.2 Step 2: Create the Unified Audit Policy 30-89
30.10.3 Step 3: Test the Policy 30-90
30.10.4 Step 4: Remove the Components of This Tutorial 30-91
30.11 Unified Audit Policy Data Dictionary Views 30-91

31 Value-Based Auditing with Fine-Grained Audit Policies

31.1 Overview of Fine-Grained Auditing 31-1
31.1.1 About Fine-Grained Auditing 31-2
31.1.2 Where Are Fine-Grained Audit Records Stored? 31-3
31.1.3 Who Can Perform Fine-Grained Auditing? 31-3
31.1.4 Fine-Grained Auditing on Tables or Views That Have Oracle VPD Policies 31-4
31.1.5 Fine-Grained Auditing in a Multitenant Environment 31-4
31.1.6 Fine-Grained Audit Policies with Editions 31-5
31.2 Creating Fine-Grained Audit Policies 31-6
31.2.1 About Creating a Fine-Grained Audit Policy 31-6
31.2.2 Syntax for Creating a Fine-Grained Audit Policy 31-7
31.2.3 Example: Using DBMS_FGA.ADD_POLICY to Create a Fine-Grained Audit Policy 31-9
31.2.4 Audits of Specific Columns and Rows 31-10
31.3 Managing Fine-Grained Audit Policies 31-10
31.3.1 Enabling a Fine-Grained Audit Policy 31-10
31.3.2 Disabling a Fine-Grained Audit Policy 31-11
31.3.3 Dropping a Fine-Grained Audit Policy 31-11
31.4 Tutorial: Adding an Email Alert to a Fine-Grained Audit Policy 31-12
31.4.1 About This Tutorial 31-12
31.4.2 Step 1: Install and Configure the UTL_MAIL PL/SQL Package 31-13

31.4.3 Step 2: Create User Accounts 31-14
31.4.4 Step 3: Configure an Access Control List File for Network Services 31-15
31.4.5 Step 4: Create the Email Security Alert PL/SQL Procedure 31-16
31.4.6 Step 5: Create and Test the Fine-Grained Audit Policy Settings 31-16
31.4.7 Step 6: Test the Alert 31-17
31.4.8 Step 7: Remove the Components of This Tutorial 31-18
31.5 Fine-Grained Audit Policy Data Dictionary Views 31-18

32 Administering the Audit Trail

32.1 Managing the Unified Audit Trail 32-1
32.1.1 How and Where Unified Audit Records Are Created 32-2
32.1.2 Sizing Recommendations for Unified Auditing 32-3
32.1.3 How Audit Trail Records Are Written to the AUDSYS Schema 32-3
32.1.4 Writing the Unified Audit Trail Records to SYSLOG or the Windows Event Viewer 32-4
32.1.4.1 About Writing the Unified Audit Trail Records to SYSLOG or the Windows Event Viewer 32-4
32.1.4.2 Enabling SYSLOG and Windows Event Viewer Captures for the Unified Audit Trail 32-5
32.1.5 How Unified Audit Records are Written to the Operating System 32-7
32.1.6 Moving Operating System Audit Records into the Unified Audit Trail 32-7
32.1.7 Improving the Performance of Queries and Purge Operations 32-8
32.1.8 Using Oracle Data Pump to Export and Import Unified Audit Trail Records 32-9
32.1.9 How Do Cursors Affect Auditing? 32-10
32.2 Archiving the Audit Trail 32-10
32.2.1 Archiving the Traditional Operating System Audit Trail 32-10
32.2.2 Archiving the Unified and Traditional Database Audit Trails 32-11
32.3 Purging Audit Trail Records 32-11
32.3.1 About Purging Audit Trail Records 32-12
32.3.2 Selecting an Audit Trail Purge Method 32-13
32.3.2.1 Purging the Audit Trail on a Regularly Scheduled Basis 32-13
32.3.2.2 Purging the Audit Trail on Demand 32-13
32.3.3 Scheduling an Automatic Purge Job for the Audit Trail 32-14
32.3.3.1 About Scheduling an Automatic Purge Job 32-14
32.3.3.2 Step 1: Ensure Online and Archive redo Log Sizes Are Tuned Appropriately 32-14
32.3.3.3 Step 2: Optionally, Set an Archive Timestamp for Audit Records 32-15
32.3.3.4 Step 3: Create and Schedule the Purge Job 32-17
32.3.4 Manually Purging the Audit Trail 32-18
32.3.4.1 About Manually Purging the Audit Trail 32-18
32.3.4.2 Using DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL to Manually Purge the Audit Trail 32-19

32.3.5 Other Audit Trail Purge Operations 32-21
32.3.5.1 Enabling or Disabling an Audit Trail Purge Job 32-21
32.3.5.2 Setting the Default Audit Trail Purge Job Interval for a Specified Purge Job 32-22
32.3.5.3 Deleting an Audit Trail Purge Job 32-22
32.3.5.4 Clearing the Archive Timestamp Setting 32-23
32.3.6 Example: Directly Calling a Unified Audit Trail Purge Operation 32-24
32.3.7 Purge CLI Records in Databases Upgraded from Oracle Database 12.1 or Earlier 32-24
32.4 Audit Trail Management Data Dictionary Views 32-25

Part VII Appendixes

A Keeping Your Oracle Database Secure

A.1 About the Oracle Database Security Guidelines A-2
A.2 Downloading Security Patches and Contacting Oracle Regarding Vulnerabilities A-2
A.2.1 Downloading Security Patches and Workaround Solutions A-2
A.2.2 Contacting Oracle Security Regarding Vulnerabilities in Oracle Database A-2
A.3 Guidelines for Securing User Accounts and Privileges A-3
A.4 Guidelines for Securing Passwords A-7
A.5 Securing Authentication for Oracle Database Microsoft Windows Installations A-10
A.6 Guidelines for Securing Roles A-10
A.7 Guidelines for Securing Data A-11
A.8 Guidelines for Securing the ORACLE_LOADER Access Driver A-12
A.9 Guidelines for Securing a Database Installation and Configuration A-13
A.10 Guideline for Securing Multitenant PDBs from the Root in a Linux Environment A-14
A.11 Guidelines for Securing the Network A-14
A.11.1 Client Connection Security A-15
A.11.2 Network Connection Security A-15
A.11.3 Transport Layer Security Connection Security A-19
A.12 Guideline for Securing External Procedures A-20
A.13 Guidelines for Auditing A-20
A.13.1 Manageability of Audited Information A-21
A.13.2 Audits of Typical Database Activity A-21
A.13.3 Audits of Suspicious Database Activity A-22
A.13.4 Audits of Sensitive Data A-23
A.13.5 Recommended Audit Settings A-23
A.13.6 Best Practices for Querying the UNIFIED_AUDIT_TRAIL Data Dictionary View A-24
A.14 Addressing the CONNECT Role Change A-25
A.14.1 Why Was the CONNECT Role Changed? A-25
A.14.2 How the CONNNECT Role Change Affects Applications A-25

A.14.2.1 How the CONNECT Role Change Affects Database Upgrades A-26
A.14.2.2 How the CONNECT Role Change Affects Account Provisioning A-26
A.14.2.3 How the CONNECT Role Change Affects Applications Using New Databases A-26
A.14.3 How the CONNECT Role Change Affects Users A-26
A.14.3.1 How the CONNECT Role Change Affects General Users A-27
A.14.3.2 How the CONNECT Role Change Affects Application Developers A-27
A.14.3.3 How the CONNECT Role Change Affects Client Server Applications A-27
A.14.4 Approaches to Addressing the CONNECT Role Change A-27
A.14.4.1 Creating a New Database Role A-28
A.14.4.2 Restoring the CONNECT Privilege A-29
A.14.4.3 Data Dictionary View to Show CONNECT Grantees A-29
A.14.4.4 Least Privilege Analysis Studies A-30

B Managing Oracle Database Wallets and Certificates

B.1 Introduction to Oracle Database Wallets and Certificates B-1
B.1.1 About Oracle Database Wallets B-2
B.1.2 About Oracle Database Certificates B-4
B.1.3 About Certificate Authority (CA) B-5
B.1.4 Tools Used to Manage Oracle Database Wallets and Certificates B-6
B.1.5 General Process of Managing Oracle Database Wallets and Certificates B-6
B.1.6 Oracle Database Wallet Search Order B-7
B.2 Managing Oracle Database Wallets and Certificates with the orapki Utility B-8
B.2.1 About Managing Oracle Database Wallets and Certificates with the orapki Utility B-8
B.2.2 orapki Utility Syntax B-9
B.3 Managing Oracle Database Wallets B-9
B.3.1 Creating a PKCS#12 Wallet B-10
B.3.2 Importing a PKCS#12 Wallet B-10
B.3.3 Creating an Auto-Login-Only Wallet B-11
B.3.4 Creating a Local Auto-Login Wallet B-11
B.3.5 Creating an Auto-Login Wallet That Is Associated with a PKCS#12 Wallet B-11
B.3.6 Viewing a Wallet B-12
B.3.7 Modifying the Password for a Wallet B-12
B.3.8 Converting an Oracle Wallet to Use the AES256 Algorithm B-13
B.3.9 Deleting a Wallet B-13
B.4 Managing Oracle Database Certificates B-14
B.4.1 Certificate Store Location for System Wallets B-15
B.4.2 Adding a Certificate Request to an Oracle Wallet B-15
B.4.3 Creating Signed Certificates B-16
B.4.4 Creating a Signed Certificate Using a Self-Signed Root B-17
B.4.5 Adding a Trusted Certificate to an Oracle Wallet B-19

B.4.6 Adding a Root Certificate to an Oracle Wallet B-19
B.4.7 Adding Root Certificate Authority That Requires an Intermediate Certificate Using Microsoft Internet Explorer B-20
B.4.8 Adding a User Certificate to an Oracle Wallet B-20
B.4.9 Verifying Credentials on the Hardware Device That Uses a PKCS#11 Wallet B-20
B.4.10 Adding PKCS#11 Information to an Oracle Wallet B-21
B.4.11 Viewing a Certificate B-21
B.4.12 Controlling MD5 and SHA-1 Certificate Use B-21
B.4.13 Certificate Import and Export Operations B-22
B.4.13.1 Importing a User-Supplied or Trusted Certificate into an Oracle Wallet B-22
B.4.13.2 Exporting Certificates and Certificate Requests from an Oracle Wallet B-22
B.4.14 Management of Certificate Revocation Lists (CRLs) with orapki Utility B-23
B.5 Examples of Creating Wallets and Certificates Using orapki B-23
B.5.1 Example: Wallet with a Self-Signed Certificate and Export of the Certificate B-24
B.5.2 Example: Creating a Wallet and a User Certificate B-24
B.6 orapki Utility Commands Summary B-25
B.6.1 orapki cert create B-28
B.6.2 orapki cert display B-28
B.6.3 orapki crl delete B-29
B.6.4 orapki crl display B-29
B.6.5 orapki crl hash B-30
B.6.6 orapki crl list B-31
B.6.7 orapki crl upload B-31
B.6.8 orapki secretstore create_credential B-32
B.6.9 orapki secretstore create_entry B-33
B.6.10 orapki secretstore create_user_credential B-33
B.6.11 orapki secretstore delete_credential B-34
B.6.12 orapki secretstore delete_entry B-34
B.6.13 orapki secretstore delete_user_credential B-35
B.6.14 orapki secretstore list_credentials B-35
B.6.15 orapki secretstore list_entries B-35
B.6.16 orapki secretstore list_entries_unsorted B-36
B.6.17 orapki secretstore modify_credential B-36
B.6.18 orapki secretstore modify_entry B-37
B.6.19 orapki secretstore modify_user_credential B-37
B.6.20 orapki secretstore view_entry B-38
B.6.21 orapki wallet add B-38
B.6.22 orapki wallet change_pwd B-41
B.6.23 orapki wallet convert B-41
B.6.24 orapki wallet create B-42
B.6.25 orapki wallet delete B-42
B.6.26 orapki wallet display B-43

B.6.27 orapki wallet export B-44
B.6.28 orapki wallet export_private_key B-44
B.6.29 orapki wallet import_pkcs12 B-45
B.6.30 orapki wallet import_private_key B-45
B.6.31 orapki wallet jks_to_pkcs12 B-46
B.6.32 orapki wallet pkcs12_to_jks B-46
B.6.33 orapki wallet remove B-47
B.7 mkstore Utility Commands Summary B-47
B.7.1 mkstore create B-48
B.7.2 mkstore createALO B-49
B.7.3 mkstore createCredential B-49
B.7.4 mkstore createEntry B-50
B.7.5 mkstore createUserCredential B-50
B.7.6 mkstore delete B-51
B.7.7 mkstore deleteCredential B-51
B.7.8 mkstore deleteEntry B-52
B.7.9 mkstore deleteSSO B-52
B.7.10 mkstore deleteUserCredential B-53
B.7.11 mkstore list B-53
B.7.12 mkstore listCredential B-54
B.7.13 mkstore modifyCredential B-54
B.7.14 mkstore modifyEntry B-55
B.7.15 mkstore modifyUserCredential B-55
B.7.16 mkstore viewEntry B-56

C Oracle Database FIPS 140-2 Settings

C.1 About the Oracle Database FIPS 140-2 Settings C-1
C.2 Configuration of FIPS 140-2 Using the Consolidated FIPS_140 Parameter C-2
C.2.1 About Configuration of FIPS 140-2 Using the FIPS_140 Parameter C-3
C.2.2 Configuring the FIPS_140 Parameter C-3
C.2.3 Running orapki in FIPS Mode C-3
C.2.4 Configuring Standalone Java FIPS for Running Java Client Applications in FIPS Mode C-4
C.2.5 Enabling FIPS by Running the enable_fips.py Python Script C-4
C.2.6 FIPS-Supported Algorithms for Transparent Data Encryption C-4
C.2.7 FIPS-Supported Cipher Suites for DBMS_CRYPTO C-5
C.2.8 FIPS-Supported Cipher Suites for Transport Layer Security C-6
C.2.9 FIPS-Supported Algorithms for Network Native Encryption C-7
C.3 Legacy FIPS 140-2 Configurations C-7
C.3.1 About Legacy FIPS 140-2 Configurations C-8
C.3.2 Configuring FIPS 140-2 for Transparent Data Encryption and DBMS_CRYPTO C-8

C.3.3 Configuring FIPS 140-2 for Transport Layer Security C-9
C.3.4 Configuring FIPS 140-2 for Native Network Encryption C-9
C.4 Postinstallation Checks for FIPS 140-2 C-10
C.5 Verifying FIPS 140-2 Connections C-10
C.5.1 Verifying FIPS 140-2 Connections When Using the FIPS_140 Parameter C-10
C.5.2 Verifying FIPS 140-2 Connections for Transport Layer Security C-11
C.5.3 Verifying FIPS 140-2 Connections for Network Native Encryption C-11
C.5.4 Verifying FIPS 140-2 Connections for Transparent Data Encryption and DBMS_CRYPTO C-11
C.6 Managing Deprecated Weaker Algorithm Keys C-12

D Considerations for Transitioning from Traditional to Unified Auditing

Glossary

Index