



Oracle AI Database: Data Guard Administration Workshop

Student Guide
D1111341GC10

Learn more from Oracle University at education.oracle.com



Copyright © 2025, Oracle and/or its affiliates.

Disclaimer

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

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Trademark Notice

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

This documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

1010312025

Contents

----- **Important Note** -----
Oracle AI Database 26ai has replaced **Oracle Database 23ai**. This change was announced at Oracle AI World in October 2025. The architecture, concepts, and features presented in this course remain fully relevant to 26ai.

Oracle AI Database: Data Guard Administration Workshop

1 Introduction to Oracle Data Guard

- Objectives 1-2
- What Is Oracle Data Guard? 1-3
- Types of Standby Databases 1-4
- Data Guard per PDB (DGPDB) 1-7
- Types of Data Guard Services 1-8
- Role Transitions: Switchover and Failover 1-9
- Oracle Data Guard Broker and OEMCC Framework 1-10
- Choosing an Interface for Administering a Data Guard Configuration 1-11
- Using Oracle Enterprise Manager Cloud Control 1-12
- Data Guard Overview Page 1-13
- Benefits of Using Enterprise Manager 1-14
- Oracle Data Guard: Architecture (Overview) 1-15
- Primary Database Processes 1-16
- Standby Database Processes 1-17
- Physical Standby Database: Redo Apply Architecture 1-18
- Logical Standby Database: SQL Apply Architecture 1-19
- Automatic Gap Detection and Resolution 1-20
- Data Protection Modes 1-21
- Hybrid Data Guard Configuration 1-23
- Hybrid DR Configurations: Challenges 1-24
- Hybrid DR Configurations: Possible Solutions 1-25
- Hybrid DR Configurations: Using Tablespace Encryption 1-26
- Data Guard Operational Requirements: Hardware and Operating System 1-27
- Data Guard Operational Requirements: Oracle Database Software 1-28
- Benefits of Implementing Oracle Data Guard 1-29
- Summary 1-30

2 Oracle Net Services in a Data Guard Environment

- Objectives 2-2
- Oracle Net Services Overview 2-3
- Configuring Oracle Net Services in a Data Guard Environment 2-4
- Understanding Name Resolution 2-5

- Local Naming Configuration Files 2-6
- Local Naming: tnsnames.ora 2-7
- Connect-Time Failover: Planning for Role Reversal 2-8
- Listener Configuration: listener.ora 2-9
- Dynamic Service Registration 2-10
- Static Listener Entries: listener.ora 2-11
- Optimizing Oracle Net for Data Guard 2-12
- Using the Broker Command: VALIDATE DGConnectIdentifier 2-14
- Summary 2-15

3 Oracle Data Guard Broker: Overview

- Objectives 3-2
- Oracle Data Guard Broker: Features 3-3
- Data Guard Broker: Components 3-4
- Data Guard Broker: Configurations 3-5
- Data Guard Broker: Management Model 3-6
- Data Guard Broker: Architecture 3-7
- Data Guard Monitor: DMON Process 3-8
- Benefits of Using the Data Guard Broker 3-10
- Comparing Configuration Management With and Without the Data Guard Broker 3-12
- Data Guard Broker Interfaces 3-13
- Broker Controlled Database Initialization Parameters 3-14
- Using the Command-Line Interface of the Data Guard Broker 3-15
- Summary 3-20

4 Creating a Data Guard Broker Configuration

- Objectives 4-2
- Data Guard Broker: Requirements 4-3
- Data Guard Broker and the SPFILE 4-5
- Data Guard Monitor: Configuration File 4-7
- Data Guard Monitor: Configuration File (continued) 4-8
- Data Guard Broker: Log Files 4-9
- Data Guard Broker: Automatic Primary Database Preparation 4-10
- Creating a Broker Configuration 4-13
- Clear Redo Transport Network Locations on Primary 4-14
- Connecting to the Primary Database with DGMGRL 4-15
- Defining the Broker Configuration and the Primary Database Profile 4-16
- Adding a Standby Database to the Configuration 4-17
- Adding a Far Sync to the Configuration 4-18
- Enabling the Configuration 4-19

- Broker Support for Complex Redo Routing 4-20
- Defining RedoRoutes by Using DGMGRL 4-21
- RedoRoutes Usage Guidelines 4-22
- How to Read Redo Routing Rules 4-23
- Far Sync Example with RedoRoutes 4-24
- Changing Database Properties and States 4-25
- Managing Redo Transport Services by Using DGMGRL 4-26
- Managing the Redo Transport Service by Using the LogXptMode Property 4-30
- Setting LogXptMode to ASYNC 4-31
- Setting LogXptMode to SYNC 4-32
- Setting LogXptMode to FASTSYNC 4-33
- Commands to Set, Modify, and Display the Initialization Parameters: 4-34
 - The EDIT DATABASE SET PARAMETER Command 4-35
 - The EDIT DATABASE RESET PARAMETER Command 4-36
 - The EDIT DATABASE FAR_SYNC RESET PARAMETER Command 4-37
 - The EDIT RECOVERY_APPLIANCE SET PARAMETER Command 4-38
 - The EDIT RECOVERY_APPLIANCE RESET PARAMETER Command 4-39
 - The SET TRACE_LEVEL Command 4-40
 - Example: SET TRACE_LEVEL command 4-41
 - The EDIT FAR_SYNC SET PARAMETER Command 4-43
- Data Guard Broker Deprecated and Desupported Properties 4-44
- Export Broker Configuration 4-46
- Import Broker Configuration 4-47
- Disabling Broker Management of the Configuration or Standby Database 4-48
- Removing the Configuration or Standby Database 4-49
- Summary 4-50

5 Monitoring a Data Guard Broker Configuration

- Objectives 5-2
- Monitoring the Data Guard Configuration by Using Enterprise Manager Cloud Control 5-3
- Viewing the Data Guard Configuration Status 5-4
- Monitoring Data Guard Performance 5-5
- Viewing Log File Details 5-6
- Enterprise Manager Metrics and Alerts 5-7
- Data Guard Metrics 5-8
- Managing Data Guard Metrics 5-9
- Viewing Metric Value History 5-10
- Easier Checking of Data Guard Configurations Using the V\$DG_BROKER_PROPERTY Database View 5-11
- Viewing Data Guard Diagnostic Information 5-12

- Using Monitorable Database Properties to Identify a Failure 5-14
- Using the SHOW CONFIGURATION DGMGRL Command to Monitor the Configuration 5-15
- Using the SHOW DATABASE VERBOSE DGMGRL Command to Monitor the Configuration 5-16
- Using the SHOW|EDIT ALL MEMBERS Command to Show or Edit Properties and Parameters for all Members 5-18
- The VALIDATE DATABASE DATAFILE Command 5-19
- New Data Guard Broker Commands: VALIDATE DATABASE SPFILE 5-21
- New Data Guard Broker Commands: VALIDATE NETWORK CONFIGURATION 5-22
- New Data Guard Broker Commands: VALIDATE STATIC CONNECT IDENTIFIER 5-23
- Miscellaneous New Data Guard Broker Commands: SET ECHO and SHOW ALL 5-24
- PL/SQL API for Data Guard broker management 5-25
- Data Guard management from SQLcl 5-26
- ORDS REST API for Data Guard management 5-27
- Summary 5-28

6 Creating a Physical Standby Database by Using DG Broker and RMAN Commands

- Objectives 6-2
- Steps to Create a Physical Standby Database 6-3
- Data Guard Broker: Automatic Primary Database Preparation 6-4
- Defining the Broker Configuration and the Primary Database Profile 6-7
- Using Data Guard Broker Automatic Primary Database Preparation 6-8
- Database Nologging Enhancements 6-10
- Configuring Standby Redo Logs 6-11
- Standby Redo Log Usage 6-12
- Using Data Guard Broker Automatic Primary Database Preparation 6-13
- Viewing Standby Redo Log Information 6-14
- Setting Initialization Parameters on the Primary Database to Control Redo Transport 6-16
- Using Data Guard Broker to Set LOG_ARCHIVE_CONFIG 6-17
- Using Data Guard Broker to set LOG_ARCHIVE_DEST_n 6-19
- Specifying Role-Based Destinations 6-20
- Combinations for VALID_FOR 6-22
- Defining the Redo Transport Mode 6-23
- Setting Initialization Parameters on the Primary Database 6-24
- Specifying Values for DB_FILE_NAME_CONVERT 6-25

- Specifying Values for LOG_FILE_NAME_CONVERT 6-26
- Specifying a Value for STANDBY_FILE_MANAGEMENT 6-27
- Specifying a Value for FAL_SERVER 6-28
- Example: Initialization Parameters on the Primary Database 6-29
- Creating an Oracle Net Service Name on Primary for Your Physical Standby Database 6-30
- Creating a Listener Entry for Your Standby Database 6-31
- Copying Your Primary Database Password File to the Physical Standby Database Host 6-32
- Creating an Initialization Parameter File for the Physical Standby Database 6-33
- Creating Directories for the Physical Standby Database 6-34
- Starting the Physical Standby Database 6-35
- Creating an RMAN Script to Create the Physical Standby Database 6-36
- Creating the Physical Standby Database 6-38
- Real-Time Apply (Default) 6-39
- Starting Redo Apply in Real Time 6-41
- Preventing Primary Database Data Corruption from Affecting the Standby Database 6-42
- Detecting Lost Writes with DBMS_DBCOMP.DBCOMP 6-44
- DBMS_DBCOMP.DBCOMP Usage Cases 6-45
- Creating a Physical Standby Database by Using Enterprise Manager 6-47
- Using the Add Standby Database Wizard 6-49
- Creating a Data Guard Standby by Using DBCA 6-50
- Example: Physical Standby Creation 6-51
- Creating a Physical Standby by Using SQL 6-52
- Standby Database on the Same System 6-53
- Summary 6-54

7 Managing Physical Standby Files After Structural Changes on the Primary Database

- Objectives 7-2
- Scenario 1: Adding a Data File or Creating a Tablespace 7-3
- Action Required on Physical Standby 7-4
- Scenario 2: Using Transportable Tablespaces with a Physical Standby Database 7-5
- Action Required on Physical Standby 7-6
- Automatic tempfile creation on the standby database 7-7
- Scenario 3: Renaming a Data File in the Primary Database 7-8
- Action Required on Physical Standby 7-9
- Scenario 4: Adding or Dropping a Redo File Group 7-11

Action Required on Physical Standby 7-12
Scenario 5: NOLOGGING or Unrecoverable Operations 7-13
Action Required on Physical Standby 7-14
Scenario 6: Resetting the TDE Master Encryption Key 7-18
Scenario 7: Refreshing the Password File 7-19
Scenario 8: Controlling PDB Replication 7-20
Example: ENABLED_PDBS_ON_STANDBY 7-21
Scenario 9: Instantiating a PDB on a Standby 7-22
Summary 7-24

8 Using Oracle Active Data Guard

Objectives 8-2
Oracle Active Data Guard 8-3
Using Real-Time Query 8-4
Enabling Real-Time Query 8-5
Disabling Real-Time Query 8-6
Checking the Standby's Open Mode 8-7
Understanding Lag in an Active Data Guard Configuration 8-8
Monitoring Apply Lag: V\$DATAGUARD_STATS 8-9
Monitoring Apply Lag: V\$STANDBY_EVENT_HISTOGRAM 8-10
Allowed Staleness of Standby Query Data 8-11
Configuring Zero Lag Between the Primary and Standby Databases 8-12
Setting STANDBY_MAX_DATA_DELAY by Using an AFTER LOGON Trigger 8-13
Example: Setting STANDBY_MAX_DATA_DELAY by Using an
AFTER LOGON Trigger 8-14
Forcing Redo Apply Synchronization 8-15
Creating an AFTER LOGON Trigger for Synchronization 8-16
DDL on Global Temporary Tables 8-17
DML on Global Temporary Tables 8-18
DML/DDI on Private Temporary Tables 8-19
Creating a Private Temporary Table 8-20
Support for Global Sequences 8-21
Support for Session Sequences 8-22
Benefits: Temporary Undo and Sequences 8-23
DML Operations on Active Data Guard Standby Databases 8-24
Configuring Automatic Redirection of DML operations 8-25
Example: Performing DML on a Physical Standby 8-26
PL/SQL Operations on Active Data Guard Standby Databases 8-27
IM Column Store in an Active Data Guard Standby Database 8-28
Summary 8-29

9 Using Oracle Active Data Guard: Far Sync and Real-Time Cascading

- Objectives 9-2
- Oracle Active Data Guard 9-3
- Oracle Data Guard: Far Sync 9-4
- Far Sync: Redo Transport 9-5
- Far Sync: Alternate Redo Transport Routes 9-7
- Far Sync Instance Creation by Using RMAN 9-8
- Far Sync Instance Creation by Using SQL 9-10
- Benefits: Far Sync 9-11
- Far Sync: Alternate Design 9-12
- Real-Time Cascade 9-13
- Traditional Multi-Standby Database Architecture 9-14
- Benefits: Real-Time Cascade 9-15
- Summary 9-16

10 Creating and Managing a Snapshot Standby Database

- Objectives 10-2
- Snapshot Standby Databases: Overview 10-3
- Snapshot Standby Database: Architecture 10-4
- Converting a Physical Standby Database to a Snapshot Standby Database 10-5
- Activating a Snapshot Standby Database: Issues and Cautions 10-7
- Snapshot Standby Database: Target Restrictions 10-8
- Viewing Snapshot Standby Database Information 10-9
- Snapshot Standby Space Requirements 10-10
- Converting a Snapshot Standby Database to Physical Standby 10-11
- Activating a Snapshot Standby Database: Issues and Cautions 10-12
- Summary 10-13

11 Configuring Data Protection Modes

- Objectives 11-2
- Data Protection Modes and Redo Transport Modes 11-3
- Data Protection Modes 11-4
- Maximum Protection Mode 11-5
- Maximum Availability Mode 11-6
- Maximum Performance Mode 11-7
- Comparing Data Protection Modes 11-8
- Setting the Data Protection Mode by Using Enterprise Manager 11-9
- Setting the Data Protection Mode by Using DGMGRL 11-11
- Setting the Data Protection Mode by Using SQL 11-12
- Summary 11-13

12 Optimizing and Tuning a Data Guard Configuration

- Objectives 12-2
- Monitoring Configuration Performance by Using Enterprise Manager Cloud Control 12-3
- Optimizing Redo Transport Services 12-4
- Setting the ReopenSecs Database Property 12-5
- Setting the NetTimeout Database Property 12-6
- Setting the DataGuardSyncLatency Property 12-7
- Optimizing Redo Transmission by Using Redo Transport Compression 12-8
- Compressing Redo Data by Setting the RedoCompression Property 12-9
- Delaying the Application of Redo 12-10
- Setting the DelayMins Database Property to Delay the Application of Redo 12-11
- Using Enterprise Manager to Delay the Application of Redo 12-12
- Optimizing SQL Apply 12-13
- Adjusting the Number of APPLIER Processes 12-14
- Adjusting the Number of PREPARER Processes 12-15
- Tuning Automatic Outage Resolution 12-17
- Diagnostic Tools in Active Data Guard (Read-Only) Standby Databases 12-18
- Summary 12-19

13 Performing Role Transitions

- Objectives 14-2
- Role Management Services 14-3
- Role Transitions: Switchover and Failover 14-4
- Buffer Cache Preservation During Role Change 14-5
- Keeping Physical Standby Sessions Connected During Role Transition 14-6
- Switchover 14-7
- Switchover: Before 14-8
- Switchover: After 14-9
- Performing a Switchover by Using Enterprise Manager 14-10
- Switchover and Failover Readiness 14-15
- Easier tracking of role transitions 14-16
- Validating Databases for Switchover by Using DGMGRL 14-17
- Strict validation of switchover readiness 14-20
- Performing a Switchover by Using DGMGRL 14-21
- Preparing for a Switchover Using SQL 14-22
- Performing a Switchover by Using SQL 14-23
- Considerations When Performing a Switchover to a Logical Standby Database 14-24
- Situations That Prevent a Switchover 14-25
- Tracking of role transitions Using SQL 14-26

Failover	14-27
Types of Failovers	14-28
Failover Considerations	14-29
Performing a Failover by Using Enterprise Manager	14-30
Performing a Failover to a Physical Standby Database	14-33
Performing a Manual Failover by Using DGMGRL	14-34
Re-enabling Disabled Databases by Using DGMGRL	14-35
Summary	14-36

14 Using Flashback Database in a Data Guard Configuration

Objectives	14-2
Using Flashback Database in a Data Guard Configuration	14-3
Overview of Flashback Database	14-4
Configuring Flashback Database	14-5
Configuring Flashback Database by Using Enterprise Manager	14-6
Using Flashback Database Instead of Apply Delay	14-8
Using Flashback Database and Real-Time Apply	14-9
Using Flashback Database After RESETLOGS	14-10
Flashback Through Standby Database Role Transitions	14-12
Using Flashback Database After Failover	14-13
Automatic Propagation of Restore Points to All Standby Databases	14-14
Automatic Flashback on Physical Standby Databases	14-15
Summary	14-17

15 Enabling Fast-Start Failover

Objectives	15-2
Fast-Start Failover: Overview	15-3
When Does Fast-Start Failover Occur?	15-4
Fast-start Failover and Protection Modes	15-5
Choose the Lag Type for Maximum Performance Mode	15-6
Installing the Observer Software	15-7
Fast-Start Failover Prerequisites	15-8
Configuring Fast-Start Failover	15-9
Step 1: Specify the Target Standby Databases	15-10
Dynamically Change Fast-start Failover Target	15-11
Setting a Fast Start Failover Target Using NOWAIT Mode	15-12
Step 2: Set the Protection Mode	15-14
Step 3: Set the Fast-Start Failover Threshold	15-15
Step 4: (Optional) Set Additional Fast-Start Failover Properties	15-16
Setting the Lag-Time Limit	15-17
Configuring the Primary Database to Shut Down Automatically	15-19

Automatic Reinstatement After Fast-Start Failover	15-20
Configuring Automatic Reinstatement of the Primary Database	15-21
Setting a Connect Identifier for the Observer	15-22
Setting an Observer Override	15-23
Setting Observer Reconnection Frequency	15-24
Step 5: Configure Additional Fast-Start Failover Conditions	15-25
Configuring Fast-Start Failover Conditions	15-27
Step 6: Enable Fast-Start Failover	15-28
Configuring Fast-Start Failover in Observe-only Mode	15-29
Step 7: Start the Observer	15-30
Data Guard Broker Property: ConfigurationWideServiceName	15-32
Multiple Observers Using a Single Configuration	15-33
Master Observer and Backup Observers	15-35
Starting Observers as Background Processes	15-36
Step 8: Verify the Configuration	15-37
Initiating Fast-Start Failover from an Application	15-38
Viewing Fast-Start Failover Information	15-40
Determining the Reason for a Fast-Start Failover	15-42
Prohibited Operations After Enabling Fast-Start Failover	15-43
Disabling Fast-Start Failover	15-44
Disabling Fast-Start Failover Conditions	15-46
Using the FORCE Option	15-47
Stopping the Observer	15-48
Performing Manual Role Changes	15-49
Manually Reinstating the Database	15-50
Using Enterprise Manager to Enable Fast-Start Failover	15-51
Changing the Protection Mode and Disabling Fast-Start Failover	15-56
Using Enterprise Manager to Disable Fast-Start Failover	15-57
Using Enterprise Manager to Suspend Fast-Start Failover	15-58
Moving the Observer to a New Host	15-59
Summary	15-60

16 Backup and Recovery Considerations in an Oracle Data Guard Configuration

Objectives	16-2
Using RMAN to Back Up and Restore Files in a Data Guard Configuration	16-3
Offloading Backups to a Physical Standby	16-4
Restrictions and Usage Notes	16-5
Association and Accessibility of RMAN Backups	16-6
Backup and Recovery of a Logical Standby Database	16-7
Using the RMAN Recovery Catalog in a Data Guard Configuration	16-8
Creating the Recovery Catalog	16-9

Registering a Database in the Recovery Catalog	16-10
Setting Persistent Configuration Settings	16-11
Setting RMAN Persistent Configuration Parameters on the Primary Database	16-13
Setting RMAN Persistent Configuration Parameters on the Physical Standby Database	16-14
Setting RMAN Persistent Configuration Parameters on the Other Standby Databases	16-15
Enabling Block Change Tracking on a Physical Standby Database	16-16
Configuring Daily Incremental Backups	16-17
Recovering from the Loss of a Data File on the Primary Database	16-19
Using a Backup to Recover a Data File on the Primary Database	16-20
Restoring and Recovering a Data File on the Primary Database Over the Network	16-21
Automated Standby Synchronization from Primary Database	16-22
Enhancements to Block Media Recovery	16-24
Executing the RECOVER BLOCK Command	16-26
Excluding the Standby Database	16-27
Summary	16-28

17 Enhanced Client Connectivity in a Data Guard Environment

Objectives	17-2
Connecting to the Appropriate Environment	17-3
Understanding Client Connectivity in a Data Guard Configuration	17-4
Preventing Clients from Connecting to the Wrong Database	17-5
Managing Services	17-6
Creating Services for the Data Guard Configuration Databases	17-7
Connecting Clients to the Correct Database	17-8
Creating the AFTER DB_ROLE_CHANGE Trigger for Role-Based Services	17-9
Configuring Service Names in the tnsnames.ora File	17-10
Configuring Role-Based Services Using Oracle Clusterware	17-11
Adding Standby Databases to Oracle Restart Configuration	17-13
Example: Configuring Role-Based Services	17-14
Automatic Failover of Applications to a New Primary Database	17-15
Client Failover: Components	17-16
Data Guard Broker and Fast Application Notification (FAN)	17-17
Automating Client Failover by Using Transaction Guard and Application Continuity	17-18
What Is Transaction Guard?	17-19
What Is Application Continuity?	17-20
Data Guard and Application Continuity	17-21
Using Application Continuity	17-22

- Configure Services on Single Instance Databases to Use Application Continuity 17-24
- Configuring Client: JDBC-Thin Driver 17-25
- Configuring Client: OCI Driver 17-27
- Configuring Client: ODP.NET Unmanaged Provider Driver 17-28
- Summary 17-29

18 Creating a Logical Standby Database

- Objectives 18-2
- Benefits of Implementing a Logical Standby Database 18-3
- Logical Standby Database: SQL Apply Architecture 18-5
- SQL Apply Process: Architecture 18-6
- Preparing to Create a Logical Standby Database 18-7
- Unsupported Objects 18-8
- Unsupported Data Types 18-9
- Identifying Internal Schemas 18-10
- Checking for Unsupported Tables 18-11
- Checking for Tables with Unsupported Data Types 18-12
- SQL Commands That Do Not Execute on the Standby Database 18-13
- Unsupported PL/SQL-Supplied Packages 18-14
- Ensuring Unique Row Identifiers 18-15
- Adding a Disabled Primary Key RELY Constraint 18-17
- Creating a Logical Standby Database by Using SQL Commands 18-18
 - Step 1: Create a Physical Standby Database 18-19
 - Step 2: Stop Redo Apply on the Physical Standby Database 18-20
 - Step 3: Prepare the Primary Database to Support Role Transitions 18-21
 - Step 4: Build a LogMiner Dictionary in the Redo Data 18-22
 - Step 5: Transition to a Logical Standby Database 18-23
 - Step 6: Open the Logical Standby Database 18-24
 - Step 7: Verify That the Logical Standby Database Is Performing Properly 18-25
- Creating a Logical Standby Database by Using Enterprise Manager 18-27
 - Using the Add Standby Database Wizard 18-28
- Securing Your Logical Standby Database 18-31
- Automatic Deletion of Redo Log Files by SQL Apply 18-32
- Managing Remote Archived Log File Retention 18-33
- Creating SQL Apply Filtering Rules 18-34
- Deleting SQL Apply Filtering Rules 18-35
- Viewing SQL Apply Filtering Settings 18-36
- Using DBMS_SCHEDULER to Create Jobs on a Logical Standby Database 18-37
- Summary 18-38

19 Patching and Upgrading Databases in a Data Guard Configuration

- Objectives 19-2
- Data Guard Standby-First Patch Apply 19-3
- Upgrading an Oracle Data Guard Broker Configuration 19-6
- Upgrading Oracle Database in a Data Guard Configuration with a Physical Standby Database 19-7
- Upgrading Oracle Database in a Data Guard Configuration with a Logical Standby Database 19-9
- Using SQL Apply to Upgrade the Oracle Database 19-10
- Requirements for Using SQL Apply to Perform a Rolling Upgrade 19-11
- Performing a Rolling Upgrade by Using SQL Apply 19-12
- Identifying Unsupported Data Types 19-13
- Case 1: Performing a Rolling Upgrade by Using an Existing Logical Standby Database 19-14
- Performing a Rolling Upgrade by Using an Existing Logical Standby Database 19-15
- Case 2: Performing a Rolling Upgrade by Creating a New Logical Standby Database 19-20
- Case 3: Performing a Rolling Upgrade by Using a Physical Standby Database 19-21
- Performing a Rolling Upgrade by Using a Physical Standby Database 19-22
- Rolling Upgrades Using DBMS_ROLLING and Active Data Guard 19-27
- DBMS_ROLLING: Concepts 19-28
- DBMS_ROLLING: Overview 19-30
- Database Rolling Upgrade: Specification and Compilation Stages 19-32
- Example: Specification Stage 19-33
- Example: Compilation Stage 19-34
- Database Rolling Upgrade: Execution Stage 19-35
- Rolling Upgrade Support for Multitenant Databases 19-36
- Zero Application Downtime for Database Release Upgrades 19-37
- Summary 19-38

20 Oracle Data Guard Per Pluggable Database (DGPDB)

- Objectives 20-2
- Traditional per-CDB Data Guard architecture 20-3
- Oracle Data Guard for Container Databases 20-4
- Data Guard per PDB (DGPDB) 20-5
- 23ai DGPDB Integration Enhancements 20-6
- Current Limitations in DGPDB 20-7
- DGPDB Implementation: Overview 20-8
- Two Primary CDBs 20-9

Prepare both CDBs for Data Guard 20-10
Setup the passwords in the wallet 20-11
Two Data Guard Configurations 20-12
Add the Broker Configurations 20-13
Internal communication between CDBs 20-15
Prepare the configuration for DGPDB 20-16
Add target Pluggable Databases to Data Guard 20-17
Check the PDBs before adding them 20-18
Add the PDBs to DGPDB 20-19
Target Pluggable Databases require manual copy 20-20
Manual copy: example with scp on filesystem 20-21
Manual copy: example with RMAN and ASM 20-22
Transport Architecture 20-23
Add the Standby Redo Logs to the Target PDBs 20-24
The Apply Architecture 20-25
Start the Redo Apply 20-26
Show the status of the PDBs 20-27
PDB Switchover 20-28
DGPDB and Transparent Data Encryption 20-29
Summary 20-31