Oracle9*i*

Data Guard Broker

Release 2 (9.2)

March 2002

Part No. A96629-01

ORACLE

Oracle9*i* Data Guard Broker, Release 2 (9.2)

Part No. A96629-01

Contents

Send Us Your Comments xiii

Preface xv

Audience xv
Documentation Accessibility xv
Organization xvi
Related Documentation xvii
Conventions xviii

What's New in Data Guard Broker? xxiii

Oracle9*i* Release 2 (9.2) New Features in Data Guard Broker xxiv

1 Oracle9*i* Data Guard Broker Concepts

1.1 Oracle9*i* Data Guard Broker Overview 1-1
1.2 Benefits of Data Guard Broker 1-2
1.3 Data Guard Broker Management Model 1-4
1.4 Data Guard Broker Components 1-6
1.5 Data Guard Broker User Interfaces 1-7
1.5.1 Oracle9*i* Data Guard Manager 1-7
1.5.2 Data Guard Command-Line Interface (DGMGRL) 1-9
1.6 Data Guard Monitor 1-9
1.6.1 Data Guard Monitor (DMON) Process 1-10

1.6.2 Configuration Management 1-12
1.6.3 Database Property Management 1-13
1.7 Oracle9*i* Data Guard Installation, Upgrade, and First Use 1-13
1.7.1 Installation 1-14
1.7.2 Upgrade 1-14
1.7.3 Prerequisites for First Use 1-15

2 Managing Broker Configurations

2.1 Configuration Support 2-1
2.2 Starting the Data Guard Broker 2-6
2.3 Management Cycle of a Broker Configuration 2-6
2.4 Enable and Disable Operations 2-10
2.5 States 2-10
2.6 State Transitions 2-12
2.7 Status 2-14
2.8 Properties 2-15
2.9 Protection Modes 2-17
2.9.1 Setting the Protection Mode for Your Configuration 2-17
2.9.2 How Broker Operations Affect Protection Modes 2-20
2.9.2.1 Upgrading or Downgrading the Current Protection Mode 2-20
2.9.2.2 Switchover Operations 2-21
2.9.2.3 Failover Operations 2-21
2.9.2.4 Disable and Enable Operations 2-22
2.9.2.5 Requirements When Removing an Object in the Configuration 2-22
2.9.2.6 Requirements On Other Operations 2-23

3 Managing Site Objects

3.1 Site Objects 3-1
3.2 Role Management 3-2
3.2.1 Managing Switchover Operations 3-3
3.2.1.1 Before You Perform a Switchover Operation 3-4
3.2.1.2 Starting a Switchover Operation 3-5
3.2.1.3 How the Broker Performs a Switchover Operation 3-5
3.2.1.4 Troubleshooting Switchover Operations 3-6
3.2.2 Managing Failover Operations 3-8

3.2.2.1 Starting a Failover Operation 3-9
3.2.2.2 How the Broker Performs a Graceful Failover Operation 3-9
3.2.2.3 How the Broker Performs a Forced Failover Operation 3-10
3.2.2.4 Completing the Failover Operation 3-11
3.2.2.5 Troubleshooting Failover Operations 3-12

4 Managing Database Resources

4.1 Database Resources 4-1
4.2 Database Resource States 4-1
4.2.1 Offline State 4-2
4.2.2 Online State and Substates 4-2
4.2.3 Database State Transitions 4-3
4.3 Database Resource Properties 4-5
4.3.1 Monitorable (Read-Only) Properties 4-6
4.3.2 Configurable (Changeable) Database Resource Properties 4-6
4.3.2.1 Verifying and Updating Properties 4-8
4.3.2.2 Default Property Values 4-9
4.3.2.3 Preparing for Switchover Operations 4-9
4.3.2.4 Configuring Log Transport Services for Data Protection 4-10

5 Data Guard Manager Scenarios

5.1 Scenario 1: Starting Data Guard Manager 5-1
5.2 Scenario 2: Creating a Configuration 5-6
5.3 Scenario 3: Connecting to a Configuration 5-18
5.4 Scenario 4: Verifying the Configuration 5-20
5.5 Scenario 5: Adding Sites to a Broker Configuration 5-21
5.6 Scenario 6: Performing Routine Maintenance 5-26
5.6.1 Changing the State of a Database Resource 5-26
5.6.2 Changing the Database Protection Mode and LogXptMode Database Property 5-28
5.7 Scenario 7: Performing a Switchover Operation 5-32
5.8 Scenario 8: Performing a Failover Operation 5-34
5.9 Scenario 9: Monitoring a Data Guard Configuration 5-38
5.9.1 Verifying a Broker Configuration 5-39
5.9.2 Viewing Alert Log and Data Guard Log Information 5-40

5.9.3 Monitoring Configuration Performance 5-40
5.10 Scenario 10: Using Event Tests 5-45
5.10.1 Creating and Registering Data Guard Events 5-46
5.11 Scenario 11: Removing a Configuration and Exiting Data Guard Manager 5-52
5.11.1 Remove the Data Guard Configuration 5-52
5.11.2 Exit from Data Guard Manager 5-54
5.11.3 Stop the Data Guard Monitor 5-54
5.12 Scenario 12: Re-Creating a Configuration with Data Guard Manager 5-55

6 Data Guard Command-Line Interface Scenarios

6.1 Scenario 1: Creating a Physical Standby Database on a Remote Site 6-1
6.2 Scenario 2: Creating a Configuration 6-3
6.3 Scenario 3: Setting Database Properties 6-6
6.4 Scenario 4: Setting the Configuration Protection Mode 6-7
6.5 Scenario 5: Performing Routine Management Tasks 6-9
6.5.1 Changing States and Properties 6-9
6.5.1.1 Alter the State of the Broker Configuration 6-9
6.5.1.2 Alter a Database Resource Property 6-10
6.5.1.3 Alter the State of a Database Resource 6-10
6.5.1.4 Alter the State of a Site 6-10
6.5.2 Disabling the Configuration, Sites, and Database Resources 6-11
6.5.2.1 Disable a Configuration 6-11
6.5.2.2 Disable a Database Resource 6-12
6.5.2.3 Disable a Standby Site 6-12
6.5.3 Removing the Configuration or a Standby Site 6-13
6.6 Scenario 6: Enabling the Configuration, Sites, and Resources 6-14
6.7 Scenario 7: Performing a Switchover Operation 6-15
6.8 Scenario 8: Performing a Failover Operation 6-19
6.9 Scenario 9: Monitoring a Data Guard Configuration 6-20

7 Data Guard Command-Line Interface Reference

7.1 Starting the Data Guard Command-Line Interface 7-1
7.1.1 DGMGRL Optional Parameters 7-1
7.1.2 DGMGRL Command Format and Parameters 7-2
7.1.3 DGMGRL Command Usage Notes 7-4

7.2 Stopping the Data Guard Command-Line Interface 7-6
ALTER CONFIGURATION (protection mode) 7-7
ALTER CONFIGURATION (state) 7-10
ALTER RESOURCE (property) 7-11
ALTER RESOURCE (state) 7-14
ALTER SITE (state) 7-16
ALTER SITE (AUTO PFILE) 7-17
CONNECT 7-19
CREATE CONFIGURATION 7-21
CREATE SITE 7-24
DISABLE CONFIGURATION 7-27
DISABLE RESOURCE 7-28
DISABLE SITE 7-29
ENABLE CONFIGURATION 7-30
ENABLE RESOURCE 7-31
ENABLE SITE 7-33
EXIT 7-34
FAILOVER 7-35
HELP 7-37
QUIT 7-39
REMOVE CONFIGURATION 7-40
REMOVE SITE 7-41
SHOW CONFIGURATION 7-42
SHOW DEPENDENCY TREE 7-44
SHOW LOG 7-46
SHOW RESOURCE 7-49
SHOW SITE 7-52
SHUTDOWN 7-54
STARTUP 7-56
SWITCHOVER 7-60

8 Database Resource Properties

8.1 Monitorable (Read-Only) Properties for Database Resources 8-1
8.1.1 InconsistentLogXptProps (Inconsistent Log Transport Properties) 8-2
8.1.2 InconsistentProperties (Inconsistent Database Properties) 8-3
8.1.3 LogXptStatus (Log Transport Status) 8-4
8.1.4 LsbyFailedTxnInfo (Logical Standby Failed Transaction Information) 8-4
8.1.5 LsbyParameters (Logical Standby Parameters) 8-5
8.1.6 LsbySkipTable (Logical Standby Skip Table) 8-5
8.1.7 LsbySkipTxnTable (Logical Standby Skip Transaction Table) 8-5
8.1.8 SbyLogQueue (Standby Log Queue) 8-6
8.1.9 SendQEntries (Send Queue Entries) 8-6
8.2 Configurable Properties for Database Resources 8-7
Alternate 8-9
ApplyNext 8-10
ApplyNoDelay 8-10
ApplyParallel 8-11
ArchiveLagTarget 8-12
AsyncBlocks 8-12
Binding 8-13
DbFileNameConvert 8-14
DelayMins 8-14
Dependency 8-15
LogArchiveFormat 8-16
LogArchiveMaxProcesses 8-16
LogArchiveMinSucceedDest 8-16
LogArchiveTrace 8-17
LogFileNameConvert 8-18
LogShipping 8-18
LogXptMode 8-19
LsbyASkipCfgPr 8-21
LsbyASkipErrorCfgPr 8-21
LsbyASkipTxnCfgPr 8-22

LsbyDSkipCfgPr 8-23
LsbyDSkipErrorCfgPr 8-23
LsbyDSkipTxnCfgPr 8-24
LsbyMaxEventsRecorded 8-25
LsbyMaxSga 8-25
LsbyMaxServers 8-26
LsbyRecordAppliedDdl 8-26
LsbyRecordSkipDdl 8-27
LsbyRecordSkipErrors 8-28
LsbyTxnConsistency 8-28
MaxFailure 8-29
ReopenSecs 8-30
StandbyArchiveDest 8-30
StandbyFileManagement 8-31

Glossary

Index

List of Examples

2–1 Showing Default and Intended States with the CLI 2-13
6–1 Connecting to the Default Database on the Local System 6-4
6–2 Connecting to the Default Database on a Remote System 6-4
6–3 Altering the Broker Configuration 6-9
6–4 Altering a Database Resource Property 6-10
6–5 Altering a Database Resource State 6-10
6–6 Altering a Site State 6-10
6–7 Disabling the Configuration or the Primary Site 6-11
6–8 Disabling a Database Resource 6-12
6–9 Disabling a Standby Site 6-12

List of Figures

1–1 Hierarchy of Objects Managed by the Data Guard Broker 1-5
1–2 Components of Oracle9*i* Data Guard Broker 1-6
1–3 Oracle9*i* Data Guard Manager Main Window 1-8
1–4 Oracle9*i* Broker Background Process 1-11
2–1 Oracle9*i* Data Guard Broker Configuration 2-4
2–2 Life Cycle of a Broker Configuration 2-7
4–1 Database State Transition Diagrams 4-4
5–1 Starting Data Guard Manager 5-4
5–2 Oracle Data Guard Manager Welcome Window 5-5
5–3 Create Configuration Wizard - Welcome Page 5-7
5–4 Create Configuration Wizard - Configuration Name 5-8
5–5 Create Configuration Wizard - Choose Primary Database 5-9
5–6 Create Configuration Wizard - Standby Database Creation Method 5-10
5–7 Create Configuration Wizard - Select an Oracle Home 5-11
5–8 Create Configuration Wizard - Supplying the Datafile Copy Location 5-12
5–9 Create Configuration Wizard - Options 5-14
5–10 Create Configuration Wizard - Summary Page 5-16
5–11 Progress Dialog Box for Creating the Configuration 5-17
5–12 Configuration Connect Information Dialog Box 5-19
5–13 Verify Progress Dialog 5-21
5–14 Adding Standby Sites to an Existing Configuration 5-23
5–15 Logical Standby Support 5-24
5–16 Progress Dialog When Adding a Logical Standby Site 5-26
5–17 Verifying a State Change to a Physical Standby Database 5-28
5–18 Data Protection Mode Dialog 5-29
5–19 Standby Redo Log Assistant 5-30
5–20 Setting the LogXptMode Database Property 5-31
5–21 Choose a New Primary Site for the Switchover Operation 5-33
5–22 Failure Condition Indicates a Failover Operation May Be Necessary 5-34
5–23 Choosing a Target Standby Database for the Failover Operation 5-36
5–24 General Page After a Failover Operation Completes 5-37
5–25 Displaying General Information About a Configuration 5-39
5–26 Displaying the Performance Chart Page 5-41
5–27 Testing the Data Guard Configuration 5-44
5–28 Predefined Data Guard Event Tests 5-47
5–29 Viewing Registered Events 5-49
5–30 General Property Page of the Event Viewer 5-50
5–31 E-Mail Notification for the Actual Apply Delay Event 5-51
5–32 Removing a Data Guard Broker Configuration 5-53

List of Tables

2–1	Configuration Management With and Without the Broker	2-5
2–2	Common Properties	2-16
4–1	Database Substate Names and Descriptions	4-3
4–2	Data Guard Protection Modes and Log Transport modes	4-11
5–1	Optional Input to the Create Configuration Wizard	5-15
5–2	Data Guard Event Tests	5-45
7–1	Summary of DGMGRL Commands	7-2

Send Us Your Comments

Oracle9*i* Data Guard Broker, Release 2 (9.2)

Part No. A96629-01

Oracle Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, please indicate the document title and part number, and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: nedc-doc_us@oracle.com
- FAX: 603.897.3825 Attn: Oracle9*i* Data Guard
- Postal service:
- Oracle Corporation
- Oracle9*i* Data Guard
- One Oracle Drive
- Nashua, NH 03062-2804
- U.S.A.

If you would like a reply, please give your name, address, telephone number, and (optionally) electronic mail address.

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This document provides complete information about the Oracle9*i* Data Guard broker, a management and monitoring interface that helps you configure, monitor, and control an Oracle9*i* Data Guard configuration.

This preface contains these topics:

- Audience
- Documentation Accessibility
- Organization
- Related Documentation
- Conventions

Audience

Oracle9*i* Data Guard Broker is intended for database administrators (DBAs) and system administrators who want to use the Oracle9*i* Data Guard broker to automate many of the tasks involved in configuring and monitoring an Oracle9*i* Data Guard configuration.

The discussions herein assume that readers are already familiar with Oracle9*i* Data Guard, Oracle Enterprise Manager, and the network services provided by Oracle Net.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our

documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Standards will continue to evolve over time, and Oracle Corporation is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For additional information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation JAWS, a Windows screen reader, may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, JAWS may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation This documentation may contain links to Web sites of other companies or organizations that Oracle Corporation does not own or control. Oracle Corporation neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Organization

This document contains:

Chapter 1, "Oracle9i Data Guard Broker Concepts"

This chapter introduces Oracle9*i* Data Guard broker concepts and terminology.

Chapter 2, "Managing Broker Configurations"

This chapter helps you set up and install Oracle9*i* Data Guard and configure a Data Guard configuration. It also describes states, status, and properties of resources.

Chapter 3, "Managing Site Objects"

This chapter describes managing site resources, includes state changes, switchover operations, and failover operations.

Chapter 4, "Managing Database Resources"

This chapter describes configuring and managing database resource objects.

Chapter 5, "Data Guard Manager Scenarios"

This chapter shows how to use the Data Guard Manager graphical user interface to create, manage, and monitor a broker configuration.

Chapter 6, "Data Guard Command-Line Interface Scenarios"

This chapter describes how to use the Data Guard command-line interface to create, manage, and monitor a broker configuration.

Chapter 7, "Data Guard Command-Line Interface Reference"

This chapter provides reference information for the DGMGRL command-line interface.

Chapter 8, "Database Resource Properties"

This chapter provides reference information about database resource properties.

Glossary

Related Documentation

Refer to the following documentation for more information about Oracle9*i* Data Guard:

- *Oracle9i Data Guard Concepts and Administration*
- Oracle9*i* release notes specific to your operating system.
- Oracle9*i* installation guide specific to your operating system.
- For more information about Oracle9*i* Data Guard Manager, see the online help and quick tour available with this graphical user interface. To access the online help topics, click Help on the menu bar in Data Guard Manager.

Refer to the following documentation for information about related products:

- *Oracle9i Database Concepts.*
- *Oracle9i Net Services Administrator's Guide*
- Oracle Enterprise Manager product documentation set.

In North America, printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com/`

Customers in Europe, the Middle East, and Africa (EMEA) can purchase documentation from

`http://www.oraclebookshop.com/`

Other customers can contact their Oracle representative to purchase printed documentation.

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at

`http://otn.oracle.com/admin/account/membership.html`

If you already have a username and password for OTN, then you can go directly to the documentation section of the OTN Web site at

`http://otn.oracle.com/docs/index.htm`

To access the database documentation search engine directly, please visit

`http://tahiti.oracle.com`

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle9i Database Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.

Convention	Meaning	Example
UPPERCASE monospace (fixed-width font)	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a NUMBER column. You can back up the database by using the BACKUP command. Query the TABLE_NAME column in the USER_TABLES data dictionary view. Use the DBMS_STATS.GENERATE_STATS procedure.
lowercase monospace (fixed-width font)	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter sqlplus to open SQL*Plus. The password is specified in the orapwd file. Back up the datafiles and control files in the /disk1/oracle/dbs directory. The department_id, department_name, and location_id columns are in the hr.departments table. Set the QUERY_REWRITE_ENABLED initialization parameter to true. Connect as oe user. The JRepUtil class implements these methods.
lowercase monospace (fixed-width font) italic	Lowercase monospace italic font represents placeholders or variables.	You can specify the *parallel_clause*. Run U*old_release*.SQL where *old_release* refers to the release you installed prior to upgrading.
MixedCase monospace (fixed-width font)	Mixed-case monospace typeface indicates a Data Guard database property. The mixed case helps you visually differentiate a Data Guard property from its related database initialization parameter, which is always shown in uppercase typeface.	The StandbyFileManagement property corresponds to the STANDBY_FILE_MANAGEMENT initialization parameter.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[ ]	Brackets enclose one or more optional items. Do not enter the brackets.	`DECIMAL (`*`digits`*` [ , `*`precision`*` ])`
{ }	Braces enclose two or more items, one of which is required. Do not enter the braces.	`{ENABLE | DISABLE}`
|	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	`{ENABLE | DISABLE}` `[COMPRESS | NOCOMPRESS]`
...	Horizontal ellipsis points indicate either: ■ That we have omitted parts of the code that are not directly related to the example ■ That you can repeat a portion of the code	`CREATE TABLE ... AS `*`subquery`*`;` `SELECT `*`col1`*`, `*`col2`*`, ... , `*`coln`*` FROM employees;`
. . .	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	
Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	`acctbal NUMBER(11,2);` `acct CONSTANT NUMBER(4) := 3;`
Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	`CONNECT SYSTEM/`*`system_password`* `DB_NAME = `*`database_name`*

UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

Convention	Meaning	Example

`lowercase`	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files.
	
	Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.
		`SELECT last_name, employee_id FROM employees;`
		
		`sqlplus hr/hr`
		
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

`MixedCase monospace (fixed-width font)`	Mixed-case monospace typeface indicates a Data Guard database property. The mixed case helps you visually differentiate a Data Guard property from its related database initialization parameter, which is always shown in uppercase typeface.	The `StandbyFileManagement` property corresponds to the `STANDBY_FILE_MANAGEMENT` initialization parameter.

What's New in Data Guard Broker?

This section describes new features of Oracle9*i* Data Guard broker release 2 (9.2) and provides pointers to additional information.

Oracle9*i* Release 2 (9.2) New Features in Data Guard Broker

Oracle9*i* Data Guard Release 2 (9.2) provides several new features that enhance your ability to centrally control, manage, and monitor a broker configuration. In particular, release 2 introduces support for logical standby databases as well as providing significant enhancements to the existing support for physical standby databases and Data Guard broker components.

This release provides the following new features:

- **Support for logical standby databases**

  The Data Guard broker configures, controls, manages, and monitors a logical standby database in much the same way as is done for a physical standby database.

- **Support for multiple standby sites**

  A supported broker configuration in release 1 (9.0.1) supported a primary site and a single physical standby site. Now, there is support for up to nine standby sites for each broker configuration. Furthermore, support includes a mix of standby databases (both physical and logical standby databases) in a single broker configuration.

  Note: This release of Data Guard broker does not support Real Application Clusters environments. Data Guard broker cannot be enabled if the database instance is part of a Real Application Clusters configuration.

- **Support for switchover and failover operations**

  The Data Guard broker makes it very easy to switchover or failover the role of the primary site and database to one of the standby sites. The new Switchover and Failover wizards in Data Guard Manager and the new `SWITCHOVER` and `FAILOVER` commands available with the Data Guard command-line interface essentially reduce these complex tasks to push-button operations.

- **Support for data protection modes**

  You can dynamically tune the configuration to balance data protection levels and application performance to maximize data protection, maximize availability, or maximize performance.

- **Support for the following monitorable database properties:**

InconsistentLogXptProps (Inconsistent Log Transport Properties)

InconsistentProperties (Inconsistent Database Properties)

LogXptStatus (Log Transport Status)

LsbyFailedTxnInfo (Logical Standby Failed Transaction Information)

LsbyParameters (Logical Standby Parameters)

LsbySkipTable (Logical Standby Skip Table)

LsbySkipTxnTable (Logical Standby Skip Transaction Table)

SbyLogQueue (Standby Log Queue)

SendQEntries (Send Queue Entries)

- **Support for the following configurable database properties:**

  `Alternate`

  `ApplyNext`

  `ApplyNoDelay`

  `ApplyParallel`

  `ArchiveLagTarget`

  `AsyncBlocks`

  `Binding`

  `DbFileNameConvert`

  `DelayMins`

  `Dependency`

  `LogArchiveFormat`

  `LogArchiveMaxProcesses`

  `LogArchiveMinSucceedDest`

  `LogArchiveTrace`

  `LogFileNameConvert`

  `LogShipping`

  `LogXptMode`

  `LsbyASkipCfgPr`

LsbyASkipErrorCfgPr

LsbyASkipTxnCfgPr

LsbyDSkipCfgPr

LsbyDSkipErrorCfgPr

LsbyDSkipTxnCfgPr

LsbyMaxEventsRecorded

LsbyMaxSga

LsbyMaxServers

LsbyRecordAppliedDdl

LsbyRecordSkipDdl

LsbyRecordSkipErrors

LsbyTxnConsistency

MaxFailure

ReopenSecs

StandbyArchiveDest

StandbyFileManagement

- **Data Guard configuration file enhancements**

  In release 1, the Data Guard configuration file was named automatically for you using the operating system default name. Beginning with release 2, you can override the default name by setting the DG_BROKER_CONFIG_FILE*n* (where *n* is number 1 or 2) initialization parameters:

  ```
  DG_BROKER_CONFIG_FILE1
  DG_BROKER_CONFIG_FILE2
  ```

  See Also: Section 1.6.2, "Configuration Management"

- **Data Guard Manager enhancements**

  – Support for all of the new features for this release, including logical standby support, support for multiple standby sites, support for switchover and failover operations, support for new and changed database properties.

- New wizards to add a site, perform switchover operations, and to perform failover operations.
- View Log—The Data Guard Manager View Log feature allows remote viewing of database alert logs and Data Guard broker configuration logs.
- Performance monitoring and testing capabilities—A new Performance Chart page shows a graphical summary of how far behind and how much redo data is being generated and applied to the standby databases in the broker configuration. You can choose to display bar, line, grid, and pie charts.

Note: You must upgrade to Oracle Enterprise Manager Release 9.2 to manage a broker configuration running Oracle9*i* Data Guard Release 2 (9.2):

- Oracle9*i* Data Guard Release 2 (9.2) is incompatible with Data Guard Manager and the Data Guard command-line interface Release 1 (9.0.1).
- Oracle9*i* Data Guard Release 1 (9.0.1) is incompatible with Data Guard Manager and the Data Guard command-line interface Release 2 (9.2).

- **CLI enhancements**
  - Support for logical standby databases, multiple standby sites, switchover and failover operations, new and changed database properties.
  - New `SWITCHOVER` and `FAILOVER` commands for the Data Guard command-line interface.
  - Detects unfinished command lines and prompts you for more input. For example, the following command requires a semicolon to end the command:

```
DGMGRL> ALTER SITE 'Primary' SET STATE=OFFLINE
>;
```

This release provides the following changed or removed features:

- Renamed the ArchiveDestDependency property to Dependency property.
- Removed the `FAL_SERVER` and `FAL_CLIENT` properties; these are managed automatically by Data Guard broker.

- Renamed the DRS_START initialization parameter to DG_BROKER_START.
- Requires that you must use the persistent server initialization parameter file (SPFILE) to control static and dynamic initialization parameters.
- Removed the distinction between critical and noncritical properties.

1

Oracle9*i* Data Guard Broker Concepts

This chapter describes the Oracle9*i* Data Guard broker, its architecture and components, and how it automates and simplifies the creation, control, and monitoring of a Data Guard configuration. The assumption is that you already have an understanding of Oracle9i Data Guard terminology and concepts.

The following sections introduce Data Guard broker terminology and concepts:

- Section 1.1, "Oracle9i Data Guard Broker Overview"
- Section 1.2, "Benefits of Data Guard Broker"
- Section 1.3, "Data Guard Broker Management Model"
- Section 1.4, "Data Guard Broker Components"
- Section 1.5, "Data Guard Broker User Interfaces"
- Section 1.6, "Data Guard Monitor"
- Section 1.7, "Oracle9i Data Guard Installation, Upgrade, and First Use"

> **See Also:** *Oracle9i Data Guard Concepts and Administration* for complete information about Oracle9*i* Data Guard concepts and terminology

1.1 Oracle9*i* Data Guard Broker Overview

The Oracle9*i* Data Guard broker is a distributed management framework that automates and centralizes the creation, maintenance, and monitoring of Data Guard configurations. The following list describes some of the operations that the broker automates and simplifies:

- Creating and enabling one or more Data Guard configurations, with each configuration incorporating a primary site and database, a new or existing

standby site and (physical or logical) standby database, and configuring log transport services, and log apply services

- Adding up to 8 additional new or existing sites and (physical or logical) databases to each existing Data Guard configuration, for a total of one primary site and database, and from 1 to 9 standby sites and databases in the same configuration
- Managing an entire Data Guard configuration from any site in the configuration, including all sites and databases, log transport services, and log apply services
- Invoking switchover or failover operations with a single command to initiate and control complex role changes across all systems in the configuration
- Monitoring log apply rates, capturing diagnostic information, and detecting problems quickly with centralized monitoring, testing, and performance tools

You can perform all management operations locally or remotely through the broker's easy-to-use interfaces: Oracle9i Data Guard Manager, which is the broker's graphical user interface (GUI) and the Data Guard command-line interface (CLI).

Note: This release of the Data Guard broker does not support primary, logical, or physical standby databases configured in a Real Application Clusters environment. You must manage these Data Guard configurations without the broker.

1.2 Benefits of Data Guard Broker

The broker's easy-to-use interfaces improve usability and centralize management and monitoring of the Data Guard configuration, resulting in the following benefits:

Enhanced high availability and disaster protection: By automating the tasks required to configure and monitor a Data Guard configuration, the broker enhances the high availability and disaster protection capabilities that are inherent in Oracle9*i* Data Guard. Access is possible through any client on any system in the Data Guard configuration, eliminating any single point of failure. If the primary system fails, any of the standby databases can be used for production processing.

Automated creation of a Data Guard configuration: The broker helps you to logically define and create a Data Guard configuration consisting of a primary site and a local or remote (physical or logical) standby site. If you use Data Guard Manager, it also automatically configures the communication between the sites and

databases in a Data Guard configuration, which can be connected by a LAN and Oracle Network Services in the same data center, or—for maximum data protection—geographically dispersed over a WAN and connected by Oracle Network Services.

Data Guard Manager provides a wizard that automates the complex tasks involved in creating a broker configuration, including adding a new or existing standby database, and configuration of the standby control file, initialization parameter file, and datafiles. Although the CLI interface cannot automatically create a new standby database, the CLI can configure and monitor an existing standby database.

Easy configuration of additional standby databases: After you create a Data Guard configuration consisting of a primary and standby database, you can add up to eight new or existing, physical or logical standby databases to each Data Guard configuration. Data Guard Manager provides an Add Site wizard to guide you through the process of adding more sites and database resources. Data Guard Manager also makes all Oracle Net configuration changes necessary to support log transport services and log apply services across all sites in the configuration.

Simplified, centralized, and extended management: You can issue management commands from any system in the configuration to:

- Coordinate resource state transitions and modify resource properties while ensuring that changes are made to all of the sites in the configuration.
- Manage all components of the configuration, including the primary and standby sites and databases, log transport services, and log apply services.
- Update database properties dynamically with the broker recording the changes in a Data Guard configuration file that contains information about all of the objects in the configuration, and propagating the changes to the related databases and their SPFILEs in the Data Guard configuration.
- Dynamically tune the configuration protection modes (to maximize protection, to maximize availability, or to maximize performance) and balance the level of data protection against the impact on application performance.
- Use verify commands to ensure that log transport services and log apply services are configured and functioning properly.

Automated switchover and failover operations: Only one command is required to initiate complex role changes for switchover or failover operations across all systems in the configuration. Data Guard Manager provides switchover and failover wizards that automate switchover and failover to a specified standby site in

the broker configuration. Data Guard Manager prompts you to choose a new primary site from a list of viable standby sites (enabled and online, with normal status). The CLI `SWITCHOVER` and `FAILOVER` commands require you to specify only the target standby site before automatically initiating and completing the many steps in switchover or failover operations across the multiple sites in the configuration.

Built-in monitoring and alert and control mechanisms: The broker provides built-in validation that monitors the *health* of all of the sites in the configuration. From any system in the configuration, you can capture diagnostic information and detect obvious and subtle problems quickly with centralized monitoring, testing, and performance tools. Both Data Guard Manager and the CLI retrieve a complete configuration view of the primary log transport queue depth and the standby log apply queue depth, in addition to data specific to physical and logical standby databases.

Also, the ability to monitor local and remote databases and respond to events is significantly enhanced by the broker's health check mechanism and Data Guard Manager's interaction with the Oracle Enterprise Manager event management system.

Transparent application integration: Use of the broker is possible for any database because the broker works transparently with applications; no application code changes are required to accommodate a configuration that you manage with the broker. However, you will need to reconnect applications after a failover or switchover occurs.

> **See Also:** *Oracle9i Data Guard Concepts and Administration* for a complete description of the discrete steps that comprise the creation of standby databases and the other monitoring and control operations that have been automated or simplified by the broker.

1.3 Data Guard Broker Management Model

The broker simplifies the management of a Data Guard environment by performing operations against three logical objects:

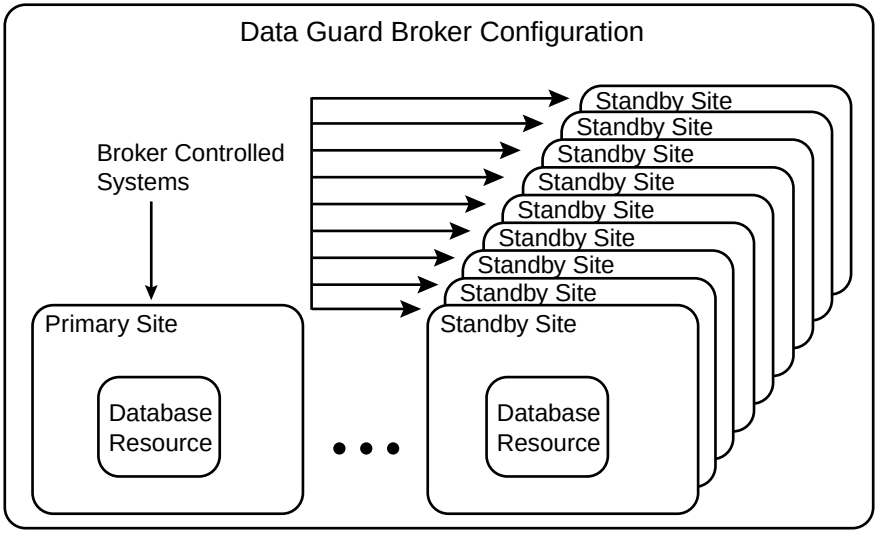
- Configuration
- Site
- Database resource

The broker supports one or more Data Guard configurations, each of which contains one primary site and database, and from one to nine physical or logical standby sites and databases. A supported broker configuration consists of:

- A **configuration** object, which is a named collection of sites and the resource objects that those sites contain. The configuration object contains one primary site object and up to nine standby site objects that can include a mix of both physical and logical standby databases. The site objects contained in a given configuration are typically distributed across multiple host systems.
- **Site** objects are named collections of resource objects with each site typically residing on a single host. The primary site object contains a database resource object that represents a primary database, and each standby site object contains a database resource object that represents either a physical or a logical standby database.
- **Database resource** objects, which are named objects, correspond to primary or standby database instances. The broker uses each database resource object to manage and control the state of a single database on a given site.

Figure 1–1 shows the hierarchy of these objects.

Figure 1–1 Hierarchy of Objects Managed by the Data Guard Broker



Because these objects are connected in a hierarchy, you can perform complex operations on a single object or on all objects in an entire configuration with a single mouse click or command. For example, you can bring each database resource and site in a configuration online one at a time, or bring them all online at the same time in a single step by bringing the configuration itself online.

> **See also:** Chapter 2, Chapter 3, and Chapter 4 for more information about managing configuration, site, and database resource objects

1.4 Data Guard Broker Components

The Oracle9*i* Data Guard broker consists of the following components:

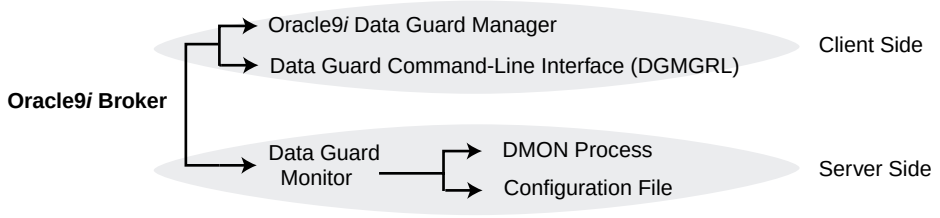
- Oracle9i Data Guard Manager
- Data Guard Command-Line Interface (DGMGRL)
- Data Guard Monitor

The Data Guard Manager graphical user interface and the Data Guard command-line interface are the broker client-side components that help you define a configuration consisting of a collection of primary and standby database sites. Section 1.5 describes these interfaces in more detail.

The Data Guard monitor is the broker server-side component that is integrated with the Oracle database server. Data Guard monitor is composed of the DMON process and Data Guard configuration files that allow you to control the objects of that configuration, modify object behavior at runtime, monitor the overall health of the configuration, and provide notification of other operational characteristics. Section 1.6 describes the Data Guard monitor in more detail.

Figure 1–2 shows these components of the broker.

Figure 1–2 Components of Oracle9i Data Guard Broker



1.5 Data Guard Broker User Interfaces

You can use either of the broker's user interfaces to create a broker configuration and to control and monitor the configuration from any host in the configuration. The following sections describe the broker's user interfaces:

- Oracle9i Data Guard Manager
- Data Guard Command-Line Interface (DGMGRL)

1.5.1 Oracle9*i* Data Guard Manager

The Data Guard Manager is a graphical user interface that works with the Data Guard monitor and Oracle Enterprise Manager to automate and simplify the management of a Data Guard configuration. Because it is integrated with Oracle Enterprise Manager, Data Guard Manager allows you to manage your configuration using a familiar interface and event management system.

With Data Guard Manager, the complex operations of creating and managing standby databases are simplified through wizards provided by Data Guard Manager. Data Guard Manager includes:

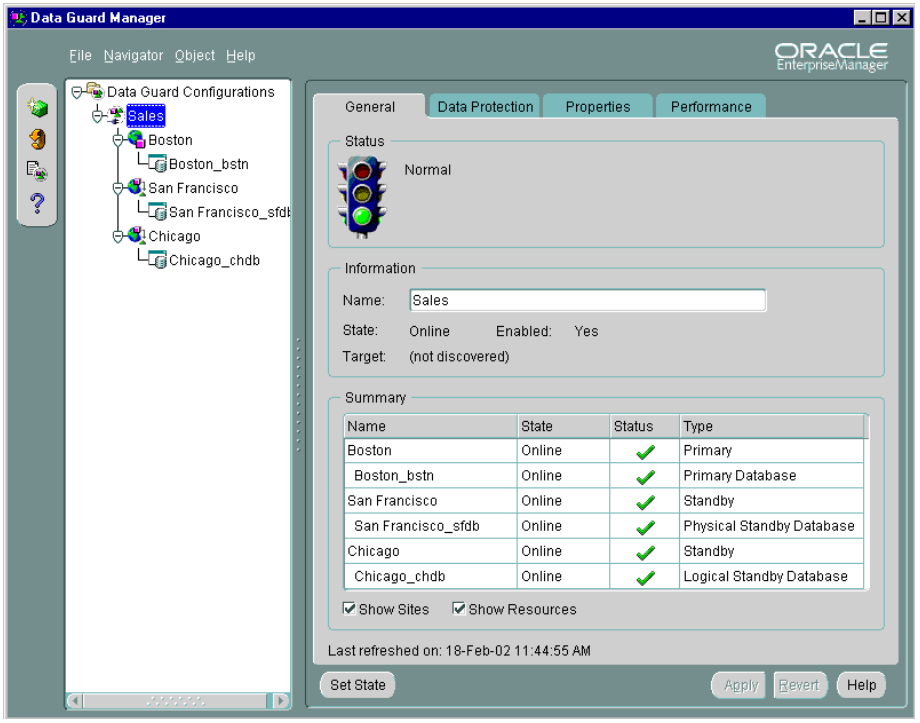
- A Create Configuration wizard that helps you to create a broker configuration having a primary site and a local or remote standby site. The wizard can create the standby site and either create its physical or logical standby database, or import an existing physical or logical standby database. If creating the physical or logical standby database, it also automates the creation of the standby control file, the standby initialization parameter file and SPFILE, log files, and the standby datafiles.
- An Add Site wizard that creates and adds new standby sites, and either creates its physical or logical standby database or imports an existing physical or logical standby database. or imports existing standby sites, into an existing broker configuration.
- A Switchover wizard that guides you through the steps to switch roles between the primary site and a standby site.
- A Failover wizard that changes one of the standby sites and its database into the role of a primary site and database.
- Performance tools and graphs that help you monitor and tune log transport services and log apply services.

- Property pages that allow you to set database properties on any site or database and, if applicable, the settings are immediately replicated to all other sites, databases, and server parameter files (SPFILE) in the configuration.
- Integration with Oracle Enterprise Manager to perform proactive event reporting through e-mail or pagers.

In addition, it makes all Oracle Net configuration changes necessary to support log transport services and log apply services

Figure 1–3 shows the general page from the Oracle9*i* Data Guard Manager main window.

Figure 1–3 Oracle9i Data Guard Manager Main Window



See Also: The Oracle9*i* Data Guard Manager online help and quick tour

1.5.2 Data Guard Command-Line Interface (DGMGRL)

The Data Guard command-line interface (CLI) allows you to control and monitor a Data Guard configuration from the CLI prompt or within scripts. You can perform most of the activities required to manage and monitor the objects in the configuration using the CLI.

The following example lists the available commands:

```
DGMGRL> HELP
The following commands are available:
quit
exit
show                See "help show" for syntax
enable              See "help enable" for syntax
disable             See "help disable" for syntax
help                 [<command>]
connect             <user>/<password> [@<connect>]
alter               See "help alter" for syntax
create              See "help create" for syntax
remove              See "help remove" for syntax
failover
shutdown
startup
switchover
```

This guide provides examples and reference information for the Data Guard command-line interface.

> **See Also:** Chapter 7 for complete reference information for the Data Guard command-line interface

1.6 Data Guard Monitor

The configuration, control, and monitoring functions of the broker are implemented by server-side software and configuration files that are maintained on each site that the broker manages. The software is called the Data Guard monitor.

The following sections describe how the Data Guard monitor interacts with the Oracle server and with remote Data Guard monitors to manage the sites in a broker configuration.

1.6.1 Data Guard Monitor (DMON) Process

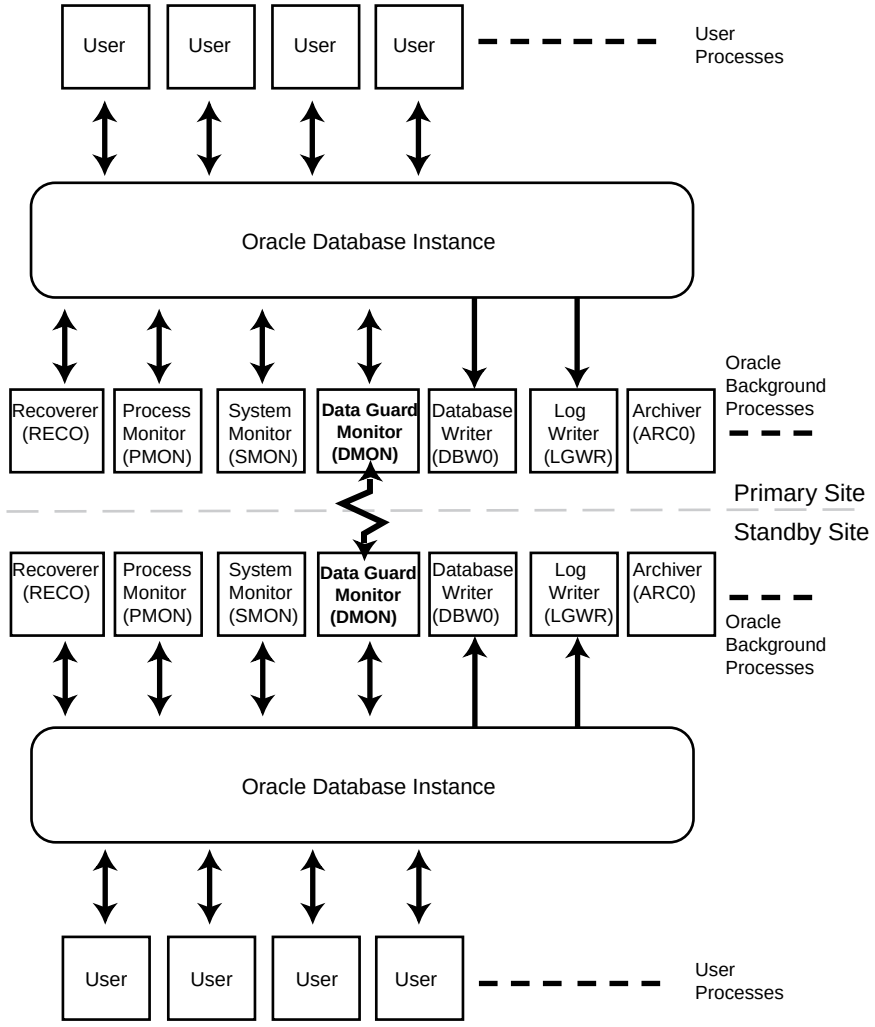
The Data Guard monitor process (DMON) is an Oracle background process that runs on every site that is managed by the broker. When you start the Data Guard monitor, a DMON process is created.

When you use Data Guard Manager or the CLI to manage an object, the DMON process is the server-side component that interacts with the local instance and the DMON processes running on other sites to perform the requested function. The DMON process is also responsible for monitoring the health of the broker configuration and for ensuring that every site has a consistent copy of the binary configuration files in which the DMON process stores its configuration data.

> **See Also:** *Oracle9i Database Concepts* for more information about the memory structures and processes that are used with an Oracle database instance

Figure 1–4 shows the DMON process among several background processes that perform maintenance work for the Oracle database server.

Figure 1–4 Oracle9i Broker Background Process



The zigzag arrow in the center of Figure 1–4 represents the two-way Oracle Net communication channel that exists between the DMON processes on sites in the same broker configuration.

This two-way communication channel is used to pass requests between sites, and to monitor the health of all of the sites in the broker configuration.

1.6.2 Configuration Management

The broker's DMON process maintains persistent configuration data about all objects in the broker configuration in a binary **configuration file.** A copy of this file is maintained by the DMON process on each of the sites that belong to the broker configuration. Changes to this file are made by the DMON process for all copies.

This configuration file contains entries that describe the states and properties of the objects in the configuration. For example, the file records the sites and databases that are part of the configuration, the roles and properties of each of the databases, and the state of each of the objects of the configuration.

The configuration data is managed transparently by the DMON process to ensure that the configuration information is kept consistent across all of the sites. The broker uses the data in the configuration file to configure and start the site and database resource objects, control each object's behavior, and provide information to the CLI and Data Guard Manager. (See Section 4.3.2 for more information.)

Whenever you add site or database resource objects to a broker configuration, or make a change to an existing object's properties, each DMON process records the new information in its copy of the configuration file.

Two copies of the file are maintained per site so as to always have a record of the last known *valid* state of the configuration. When the database instance is started, the configuration files are named automatically using a default name that is operating-system specific. You can override this default name on any given site by setting the following initialization parameters for that site:

```
DG_BROKER_CONFIG_FILE1
DG_BROKER_CONFIG_FILE2
```

You can also change the configuration file names dynamically by issuing the ALTER SYSTEM SQL statement. However, you cannot alter these parameters when the DMON process is running. To change the names of these configuration files on a given site, perform the following steps:

1. Disable the broker configuration using the CLI DISABLE command or the Disable operation in Data Guard Manager. See Section 2.4.
2. Stop the Data Guard broker DMON process using the following SQL statement:

   ```
   SQL> ALTER SYSTEM SET DG_BROKER_START=FALSE;
   ```

3. Change the configuration file names on the site:

   ```
   SQL> ALTER SYSTEM SET DG_BROKER_CONFIG_FILE1=filespec1
   SQL> ALTER SYSTEM SET DG_BROKER_CONFIG_FILE2=filespec2
   ```

4. Rename the existing files to *filespec1* and *filespec2*, respectively, at the operating system level to avoid losing the existing broker configuration information.
5. Restart the Data Guard broker DMON process on the site, as follows:

```
SQL> ALTER SYSTEM SET DG_BROKER_START=TRUE;
```

6. Enable the broker configuration using the CLI ENABLE command or the Enable operation in Data Guard Manager.

1.6.3 Database Property Management

Associated with each site and database resource object are various properties that the DMON process uses to control the object's behavior. The properties are recorded in the configuration file as a part of the object's definition that is stored there. In particular, many database resource properties are used to control database initialization parameters related to the Data Guard environment.

To ensure that the broker can update the values of parameters in both the database instance itself and in the configuration file, you must use a persistent server initialization parameter file (SPFILE) to control static and dynamic initialization parameters. The use of a SPFILE gives the broker a mechanism that allows it to reconcile property values selected by the DBA when using the broker with any related initialization parameter values recorded in the SPFILE.

Thus, when you set definitions or values for database properties in the broker configuration, the broker records the change in the configuration file and also propagates the changes to all of the sites in the Data Guard configuration.

Note: The broker supports both the default and non-default SPFILE filenames. If you use a non-default SPFILE name, the initialization parameter file (PFILE) must include the complete filename and location for the server parameter file (SPFILE).

See Also: Section 4.3.2 for more information.

1.7 Oracle9*i* Data Guard Installation, Upgrade, and First Use

Oracle9*i* Data Guard and the broker (including the CLI) are included with the Enterprise Edition or Personal Edition of the Oracle9*i* database server software.

The Oracle9*i* Data Guard Manager graphical user interface is included with the Oracle Enterprise Manager software.

1.7.1 Installation

To use the broker and the CLI, you must install the Oracle9*i* Enterprise Edition or Personal Edition database server on each site where you plan to manage broker configurations.

If you plan to use the Oracle9*i* Data Guard Manager graphical user interface to manage broker configurations, you must install it with the Oracle Enterprise Manager software.

1.7.2 Upgrade

If you are currently running an Oracle9*i* Data Guard Release 1 (9.0.1) configuration, you must upgrade to Oracle9*i* Release 2 (9.2) and recreate the broker configuration, as follows:

1. Delete the release 9.0.1 broker configuration using the Data Guard Manager or the CLI release 1 (9.0.1).
2. Upgrade the database server software to Oracle9*i*Release 2 (9.2). See the Oracle installation documentation that is appropriate for your operating system.
3. If you are using Oracle9*i* Enterprise Manager and Data Guard Manager Release 1 (9.0.1), you must upgrade to Oracle9*i* Enterprise Manager Release 2 (9.2) to manage a broker configuration running Oracle9*i* Data Guard Release 2 (9.2):
   - Data Guard Manager Release 1 (9.0.1) is not compatible with Oracle Data Guard Release 2 (9.2).
   - Data Guard Manager Release 2 (9.2) is not compatible with Oracle Data Guard Release 1 (9.0.1). You will receive an error message stating that the Oracle database is too old.
4. If you are using the CLI Release 1 (9.0.1), you must upgrade to Data Guard command-line interface Release 2 (9.2):
   - The CLI Release 1 (9.0.1) is not compatible with Oracle Data Guard Release 2 (9.2).
   - The CLI Release 2 (9.2) is not compatible with Oracle Data Guard Release 1 (9.0.1).
5. Invoke Data Guard Manager or the CLI and re-create the broker configuration.

See Also: *Oracle9i Database Migration* if you are upgrading from Oracle8*i* Data Guard to Oracle9*i* Data Guard

1.7.3 Prerequisites for First Use

The following conditions must be true before you can use the broker:

- The primary and standby databases must be running Oracle9*i* release 2 and installed in a single-instance environment (not an Oracle Real Applications Clusters environment). The database server must be licensed for Oracle9*i* Enterprise Edition or Personal Edition.
- You must use a persistent server initialization parameter file (SPFILE) to ensure the broker can persistently reconcile values between broker properties and any related initialization parameter values. See Section 1.6.3 for more information.
- The value of the `DG_BROKER_START` parameter must be set to `TRUE`. See Section 2.2 for more information. (Data Guard Manager sets this parameter for you automatically.)
- You may need to set up the `DG_BROKER_CONFIG_FILE`*n* initialization parameter. See Section 1.6.2 for more information.
- Oracle Net network files must be set up on the primary database site and on the the standby database site if you configure an existing standby database into the broker configuration. Otherwise, Data Guard Manager automatically sets up the network files when it creates a standby database.
- The primary instance must be opened in archivelog mode. (Data Guard Manager does this for you automatically.) If there is an existing standby instance, it must be mounted.
- You must also set the `COMPATIBLE` initialization parameter to 9.0.0.0.0 or higher for both the primary and standby databases.
- If you plan to configure an existing standby database into the broker configuration, you must set up a remote login password file to enable management of a remote standby database. Data Guard Manager automatically sets up the remote password file when it creates a standby database.

See Also: Section 2.2 for more information about preparing and starting Oracle9*i* Data Guard. See *Oracle9i Data Guard Concepts and Administration* for more information about setting up the network files.

2

Managing Broker Configurations

This chapter contains the following sections:

- Section 2.1, "Configuration Support"
- Section 2.2, "Starting the Data Guard Broker"
- Section 2.3, "Management Cycle of a Broker Configuration"
- Section 2.4, "Enable and Disable Operations"
- Section 2.5, "States"
- Section 2.6, "State Transitions"
- Section 2.7, "Status"
- Section 2.8, "Properties"
- Section 2.9, "Protection Modes"

2.1 Configuration Support

The broker allows you to logically define a Data Guard configuration, consisting of a primary site and physical and logical standby sites. With the broker, you define a **broker configuration** that is a *logical* grouping of the sites and database resources, including log transport services and log apply services. The broker controls the logical objects in the configuration, modifies their behavior at runtime, dynamically sets the protection mode across the configuration, monitors the overall health of the configuration, and reports any health and other operational characteristics up through the Enterprise Management notification mechanisms and the Data Guard Manager general property pages if you are using Data Guard Manager, or through `SHOW` commands if you are using the CLI.

The broker supports one or more Data Guard configurations, with each configuration consisting of a site containing a primary database, and up to nine standby databases on sites that are either local to, or, remote from, the primary site. This is the maximum number of standby databases allowed by the underlying Data Guard and standby database technology.

A supported Data Guard configuration contains the following components:

- A primary database, located on a primary site
- From one to nine physical or logical standby databases, each of which is located on a standby site.
- Physical systems that host the primary and standby database instances
- Oracle Net network configuration that defines a connection between the primary and standby database instances

> **Note:** For databases configured in a shared server configuration, the connect string or Oracle Net service name used for broker communications must specify a dedicated server process instead of the dispatcher process. This is because, during some database operations, the broker must perform database administration tasks that cannot be done over shared server connections. In addition, connections between the CLI or Data Guard Manager and the database instance must also use a dedicated server link.

- Archived redo log destination parameters and configuration properties
- Log transport services that archive the redo logs from the primary database to the standby databases
- Log apply services that apply the archived redo logs to the standby databases as they arrive from the primary database

The standby database is updated by archived redo logs that are shipped automatically from the primary database by means of log transport services. The archived redo logs contain a record of all of the database changes except for *unrecoverable* or *unlogged* changes. On the standby site, log apply services apply the archived redo logs to stay synchronized with the primary database. Thus, the standby database can take over operations if the primary database becomes unusable.

The broker's DMON process configures and maintains the broker configuration components as a unified group of objects that you can manage and monitor as a single unit. Thus, when you enter a command having a scope that affects multiple objects, the DMON process:

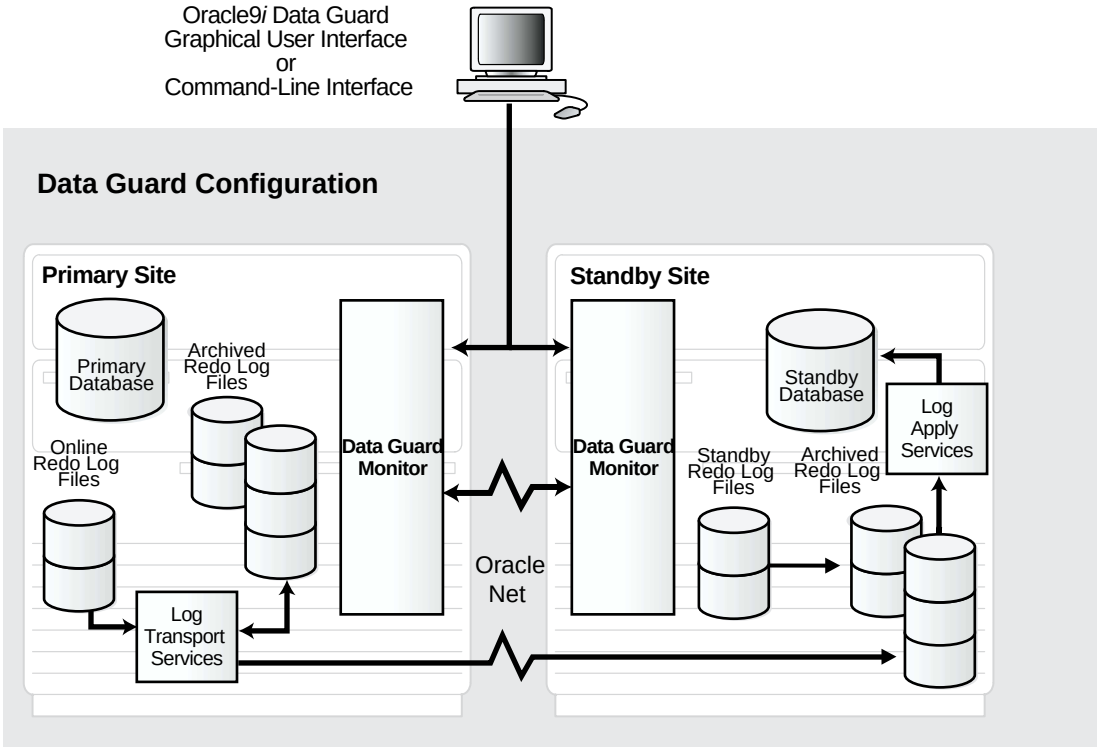
- Carries out your request on the primary site object
- Coordinates with the DMON process on the other sites as required for your request
- Updates its local configuration file
- Communicates with the DMON process on the other sites to update their copies of the configuration file

The broker carries out your requests against a hierarchy of objects that are dependent upon one another. For example, a database resource object is dependent upon the site object in which the resource resides, and the site object is dependent upon the configuration object. Thus, a site is the parent for a database resource and the configuration is the parent for a site.

This is important because when you request to take an object offline, its dependents will also be taken offline in dependency order. For example, if a site is put in an offline state, the database that is dependent on the site will also be put in an offline state first. Similarly, if the configuration is offline, all of the sites and resources in the configuration are also offline because all are dependent on the configuration. If you later request the configuration object to go online, the broker brings each site object to an online state, followed by bringing each resource object for the sites online as well. It is in this manner that the DMON process allows you to create, monitor, and control all aspects of the configuration together as a unit.

Figure 2–1 shows a two-site broker configuration with the Data Guard monitor (DMON) process running on each site. The standby site must contain a physical standby database to use the standby redo logs. Logical standby databases do not support standby redo logs.

Figure 2–1 Oracle9i Data Guard Broker Configuration



Note: This release of the Data Guard broker does not support primary or standby databases configured in a Real Application Clusters environment. You must manage these Data Guard configurations without the broker.

Table 2–1 provides a comparison of configuration management with and without the broker.

Table 2–1 Configuration Management With and Without the Broker

	Configuration Management	
	With the Broker	**Without the Broker**
General	Provides primary and standby database management as one unified configuration.	You must manage the primary and standby databases separately.
Standby Database Creation	Provides the Data Guard Manager wizards that automate and simplify the complex steps required to create a configuration with a single Oracle database instance on each site, including creating the standby control file, datafiles, and initialization parameter file.	You must manually: ■ Copy the database files to the standby site. ■ Create a control file on the standby site. ■ Create initialization parameter files on the standby site.
Configuration and Management	Allows you to configure and manage multiple sites from a single location and automatically unifies all of the sites and resources in the broker configuration.	You must manually: ■ Set up log transport services and log apply services on each site in the configuration. ■ Manage the primary database and standby databases individually.
Control	■ Automatically opens the primary database, mounts physical standby databases and opens logical standby databases, and starts log transport services and log apply services. ■ Automates switchover and failover operations. ■ Provides mouse-driven database state changes and a unified presentation of configuration and database status. ■ Provides mouse-driven property changes.	You must: ■ Use SQL*Plus commands to manage database states. ■ Coordinate sequences of multiple commands across multiple sites to execute operations.
Monitoring	■ Provides continuous monitoring of the configuration health, database health, and other runtime parameters. ■ Provides a unified updated status through the database alert log and Data Guard configuration log. ■ Provides an integrated tie-in to Oracle Enterprise Manager events.	You must: ■ Monitor the status and runtime parameters using fixed views on each site—there is no unified view of status for all of the sites and resources in the configuration. ■ Provide a custom method for monitoring events.

2.2 Starting the Data Guard Broker

After installing the Oracle9*i* release 2 database server on each site in the configuration, the DG_BROKER_START initialization parameter must be set to TRUE on each site to start the Data Guard monitor (DMON) processes.

By default, the DG_BROKER_START initialization parameter is set to FALSE. However, its runtime value is determined as follows:

- If you are using Data Guard Manager, it automatically sets the DG_BROKER_START initialization parameter to TRUE.
- If you are using the CLI, you must explicitly set the DG_BROKER_START initialization parameter to TRUE; otherwise, the DMON process will not start. You can set the DG_BROKER_START initialization parameter either before or after you start the Oracle instance:
  - Before starting the Oracle instance, add the DG_BROKER_START=TRUE record to the initialization parameter file.
  - After starting the Oracle instance, set DG_BROKER_START=TRUE using the SQL ALTER SYSTEM statement.

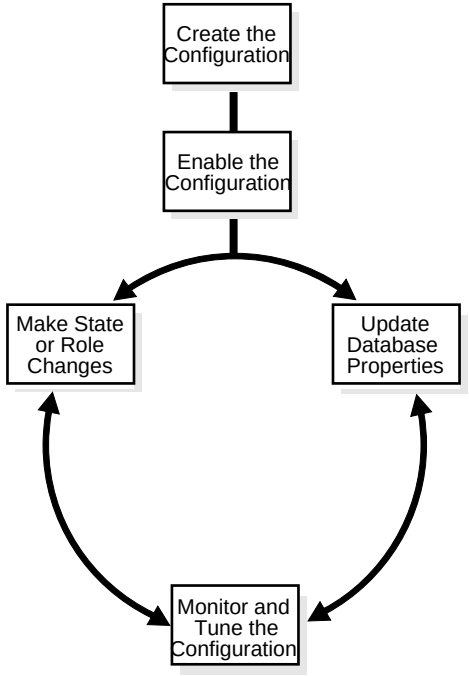
```
SQL> ALTER SYSTEM SET DG_BROKER_START=TRUE;

System altered.

SQL> SHOW PARAMETER DG_BROKER_START

NAME         TYPE      VALUE
-------------------------------------
dg_broker_start    boolean   TRUE
```

Whether you use Data Guard Manager or the CLI, Oracle Corporation recommends that you set the DG_BROKER_START=TRUE initialization parameter in the SPFILE on each primary and standby site. Doing so ensures that the DMON processes will start automatically the next time you start the database.

2.3 Management Cycle of a Broker Configuration

The broker helps you to create a new configuration or manage an existing configuration. Figure 2–2 shows the life cycle of a broker configuration.

Figure 2–2 Life Cycle of a Broker Configuration



Create the Broker Configuration

When using Data Guard Manager, the Create Configuration Wizard can either add an existing standby database into the configuration or create a new standby database and add it to the configuration. The standby database can be either a physical or logical database.

When using the CLI, the primary database and a standby database must already exist. You construct the standby database from backups of the primary database control files and datafiles, and then prepare it for recovery.

> **See Also:** Chapter 5 and Chapter 6 which describe the preparation requirements if you are using Data Guard Manager or the CLI, respectively

Enable the Broker Configuration

A Data Guard configuration must be enabled to be managed or monitored by the broker. Conversely, you disable a configuration when you no longer want to manage it with the broker. When you disable a configuration, broker management of all of its site objects and resource objects is also disabled.

A broker configuration, when first created using Data Guard Manager is automatically enabled as soon as the Create Configuration wizard completes.

A broker configuration, when first created using the CLI, is in a disabled condition. This means its constituent objects are not under active control of the Data Guard monitor. When you finish configuring the sites and resources into a broker configuration with the CLI, you must enable the configuration to allow the Data Guard monitor to manage the configuration.

You can enable:

- The entire configuration, including all of its sites and resources
- A standby site, including the standby database resource
- A database resource

The ability to enable and disable an entire configuration can be useful if you choose to use Data Guard Manager only to create a Data Guard configuration and then manage it using other interfaces (for example, using command-line interfaces and SQL statements). Also, you can easily disable a site (or a database resource on the site) if a problem has occurred and the site can no longer function properly in the broker configuration.

You may also want to disable a configuration temporarily, and then change some properties in the broker configuration without affecting the actual database properties. The changed properties will take effect when the configuration is enabled again for management by the broker.

Make State Changes or Role Changes to the Broker Configuration, As Needed

The Data Guard monitor transitions the configuration, sites, and database resources into an online state, by default, the first time that you enable the configuration.

At any time, you can issue a single command through Data Guard Manager or the CLI to change the state of the entire configuration, or of a single site or database resource. For example, you could bring the primary database resource into an online, paused state to temporarily stop archiving logs to the standby database. Then, you simply issue another command to return the database resource to a full online state (that is, online and archiving logs to the standby databases).

Similarly, at any time, you can issue a single command to change the roles of the objects in the configuration. If some event renders the primary database unusable, you can fail over one of the standby databases to become the new primary database.

In addition, planned downtime for maintenance can be reduced because you can quickly and easily switch over production processing from the current primary database to a standby database, and then back again.

> **See Also:** Chapter 3 for more information about site management and role changes

Update Database Properties, As Needed

The Data Guard monitor allows you to set database properties that map directly to several of the database initialization parameters. You can change these properties to dynamically control such things as log archival, file management, log switching, and to support the overall configuration protection mode. The broker records the changes in the Data Guard configuration file and also propagates the changes to the related initialization parameters in the server parameter files (SPFILE) to each site in the Data Guard configuration.

> **See Also:** Chapter 4 for complete information about database properties

Monitor and Tune the Configuration

You can check the health of the configuration, display and update the properties of the database resources, set Oracle Enterprise Manager events, and change the state to online or offline, as required. Moreover, the broker allows you to tune the configuration to balance data protection levels and application performance impact; you can configure the protection mode to maximize data protection, maximize availability, or maximize performance.

Data Guard Manager also provides a dynamic performance page that automatically and dynamically refreshes chart data and status at specified intervals. (The collection interval—the rate at which data is sampled from the primary—defaults to 60 seconds. You can change the collection interval.) The different performance charts include bar, line, grid, and pie show a graphical summary of how far behind and how much redo data is being generated and applied. You can also set up multiple test applications to quickly modify a table under a test schema to generate redo data and test the configuration setup.

> **See Also:** Chapter 5 and Chapter 6 for scenarios that show examples using Data Guard Manager and the CLI, respectively

2.4 Enable and Disable Operations

A key concept of management with the broker is the notion of enabling and disabling objects in a broker configuration. The enable and disable operations are relevant only to the (logical) objects in a broker configuration; you cannot perform these broker operations on the physical components of a Data Guard configuration. This is because when you enable or disable an object in the broker configuration, you are effectively enabling or disabling the ability of the Data Guard monitor (DMON) process to:

- Manage and monitor the specified configuration, site, or database resource object.
- Manage the configuration information in the Data Guard configuration file on each site.

However, disabling a broker configuration does not affect services and operations in the actual Data Guard configuration. For example, when you disable a *broker configuration*, log transport services and log apply services in the *Data Guard configuration* continue to function unchanged, but you can no longer manage them through the broker interfaces.

In addition, disabling an object *does not* remove or delete it from the Data Guard configuration file. You can re-enable your ability to manage with the broker using the CLI `ENABLE CONFIGURATION`, `ENABLE SITE`, or `ENABLE RESOURCE` commands, or the `Enable` and `Disable` options in Data Guard Manager.

Thus, it may be advantageous to disable a configuration temporarily and change one or more properties in the broker configuration all at the same time. When you change properties in a disabled configuration, it does not affect the actual database properties because the changes are not applied to the running database until you re-enable the configuration. For example, you might want to change the overall configuration protection mode and the log transport services properties on a disabled configuration so that all changes are applied to the configuration at the same time upon the next enable operation.

> **See Also:** Section 2.9.2, "How Broker Operations Affect Protection Modes"

2.5 States

While enabled, a broker configuration, site, or database resource can be in one of two states: offline or online. When disabled, the states of the objects in the configuration are left *as is*. The first time that the broker configuration is enabled[1],

each object is automatically entered into the following default runtime state known as a **default state**:

- The broker configuration is in an online state.
- The primary and standby sites are in online states.
- The primary database resource is in an online state, started and opened in read / write mode, but the replicated tables in the database are open read-only to queries.
- The physical standby database resource is in an online state, *started and mounted*. The logical standby database is opened in read / write mode.
- Log transport services and log apply services are online.

When the broker configuration is enabled for the first time, the configuration and all of the sites and database resources are also brought online automatically. In addition, note that the database resources' online states are further qualified by substates (for example, the primary database is opened in *read/write mode* with log transport services started).

The database resource substates are related to the role (primary or standby) in which the site is currently running. By default, the first time the configuration and all of the objects are enabled and brought online, the database resources are put into the following substates:

- For a primary database, the default is to start the database instance and open it in read / write mode with log transport services started (archiving redo logs to the standby database). This is referred to as the `READ-WRITE-XPTON` substate in the CLI. In Data Guard Manager, you can put the database in this state by selecting **Online** on the Set State dialog for the primary database resource.
- For a physical standby database, the database instance is *started and mounted*, while a logical standby database is open in read / write mode. Log apply services apply archived redo logs to the standby database. This is referred to as the `PHYSICAL-APPLY-ON` (for physical standby databases) or `LOGICAL-APPLY-ON` (for logical standby databases) substate in the CLI. In Data Guard Manager, you can put the database in this state by selecting **Online** on the Set State dialog for the standby database.

> **See Also:** Chapter 4 for complete information about the online substates for the primary and standby database resources

[1] Configurations are enabled automatically when created with Create Configuration wizard in Data Guard Manager, but you must enable a configuration that you create with the CLI.

Running the broker configuration using the *initial* default online states described in this section will be fine, most of the time. However, there may be times when you want to change the state of one or more objects in the broker configuration. Section 2.6 describes state transitions in more detail.

Note: Taking an object offline should be done only when absolutely necessary, because it will perform a `shutdown immediate` on the databases. If you take a configuration offline, the broker shuts down and restarts (nomount) all instances.

2.6 State Transitions

When enabled, you can transition any object in the broker configuration into another valid state (or substate if it is a database resource), provided such a transition is allowed for the object. When you change the state of an object, you are effectively changing its current runtime state, which is sometimes referred to as its **intended state**.

State transitions occur when:

- You explicitly cause a state change (by selecting the online or offline states in Data Guard Manager or by using the `CLI ALTER` command) to bring the configuration, sites, or resources online or take them offline as necessary.
- You enable the configuration, sites, or resources (using the Data Guard Manager `Enable` option or using the `CLI ENABLE` command).
- A failover or a switchover operation occurs.

When a state change occurs, it only affects the current (intended) runtime state for the object; the default state is not altered. (Section 2.5 described the default state, which is the initial runtime state of an object when the broker configuration is first enabled.)

State transitions may result in a state change to multiple objects. You can request a state transition that affects only one resource, or you can change the state of the broker configuration and affect all of the sites and resources in the configuration. For example, when you change the broker configuration into an offline state, the configuration and all of its dependent sites and resources are also taken offline. The databases in the configuration will be shut down and started (nomount), log transport services will stop sending archived redo logs, and log apply services will stop applying redo logs to the standby database.

Note: Taking the configuration, any site, or any database resource offline will perform an immediate shutdown and startup (nomount) of the database.

Although Data Guard Manager does not differentiate between states and substates, or default and intended states, the CLI does. You can see information about the default and intended (current runtime) states by issuing the CLI SHOW commands or viewing the General property page in Data Guard Manager. In Example 2–1, the SHOW RESOURCE VERBOSE command displays the default and intended states and other information for the Sales_db database resource on site Boston. Notice that although the configuration was initially enabled in the READ-WRITE-XPTON (default state), its current runtime (intended) state is READ-WRITE with log transport services stopped.

Example 2–1 Showing Default and Intended States with the CLI

```
DGMGRL> SHOW RESOURCE VERBOSE Sales_db ON SITE Boston;
```

The CLI returns the following information:

```
Resource
  Name:             Sales_db
  Manager Type:     internal
   Standby Type:     PHYSICAL
Online States:
  ONLINE
  PHYSICAL-APPLY-READY
  PHYSICAL-APPLY-ON
  READ-ONLY
  LOGICAL-APPLY-READY
  LOGICAL-APPLY-ON
  READ-WRITE
  READ-WRITE-XPTON
Properties:
  INTENDED_STATE                = 'READ-WRITE-XPTON'
  ENABLED                       = 'yes'
  IGNORE_STATUS                 = 'no'
  LogXptMode                    = 'ARCH'
  Dependency                    = ''
  Alternate                     = ''
  DelayMins                     = '0'
  Binding                       = 'OPTIONAL'
```

```
    MaxFailure                     = '0'
    ReopenSecs                     = '300'
    AsyncBlocks                    = '2048'
    LogShipping                    = 'ON'
    ApplyNext                      = '0'
    ApplyNoDelay                   = 'NO'
    ApplyParallel                  = '1'
    StandbyArchiveDest             = '/oracle/dbs/a1'
    LogArchiveTrace                = '4095'
    StandbyFileManagement          = 'AUTO'
    ArchiveLagTarget               = '0'
    LogArchiveMaxProcesses         = '5'
    LogArchiveMinSucceedDest       = '1'
    DbFileNameConvert              = 'dbs/s2t, dbs/t'
    LogFileNameConvert             = 'dbs/s2t, dbs/t'
    LogArchiveFormat               = 'r_%t_%s.arc'
    InconsistentProperties         = '(monitor)'
    InconsistentLogXptProps        = '(monitor)'
    SendQEntries                   = '(monitor)'
    LogXptStatus                   = '(monitor)'
    SbyLogQueue                    = '(monitor)'
  Properties for 'PRIMARY' state:
    DEFAULT_STATE    = 'READ-WRITE-XPTON'
    EXPLICIT_DISABLE = 'no'
    REQUIRED         = 'yes'
  Properties for 'STANDBY' state:
    DEFAULT_STATE    = 'PHYSICAL-APPLY-ON'
    EXPLICIT_DISABLE = 'no'
    REQUIRED         = 'yes'
  Current status for "db":
  SUCCESS
```

2.7 Status

A configuration status reveals the overall health of the configuration. In essence, the status indicates whether or not the configuration, site, or resource is in its intended state.

The following list describes the possible status modes for a configuration:

- Normal

  The configuration, including all of the database resources configured in it, is operating as specified by the user. All of the resources that are in the ONLINE state are operating properly without any warnings or errors.

- Warning

  One or more of the database resources in the configuration has failed and may no longer be operating as specified by the user. To obtain more information, locate each resource and examine its error status to reveal the source of the problem.

- Error

  One or more of the database resources in the configuration is not operating as specified by the user. To obtain more information, locate each resource and examine its error status to reveal the source of the problem.

- Permanently Disabled

  A database resource object is permanently disabled and can no longer be managed through Data Guard Manager or the CLI.

- Unknown

  Broker management of the configuration is disabled and not currently under the control of Data Guard Manager. Therefore the status is unknown.

2.8 Properties

There are two types of properties that can be associated with broker objects—configurable and monitorable:

- Configurable property values can be viewed and dynamically updated.

  Configurable properties affect the operation or configuration of the broker object. You can change the value of these properties using the Data Guard CLI or Data Guard Manager. You can edit properties if the configuration and its sites and database resources are enabled, disabled, online, or offline. However, if the state is offline, the new property value will not take effect until you enable the configuration, site, or resource, as appropriate.

- Monitorable property values can only be viewed when the associated object is enabled.

  Monitorable properties allow you to view information related to objects, but you cannot change the value of these properties.

  See Also: Chapter 4 for complete information about database resource properties.

There are a number of properties that are common to most of the objects in a broker configuration. Table 2–2 lists common properties for each.

Table 2–2 Common Properties

Property	Common to . . . .
DEFAULT_STATE	Configurations, sites, and resources
ENABLED	Configurations, sites, and resources
EXPLICIT_DISABLE	Configurations, sites, and resources
HEALTH_CHECK_INTERVAL[1]	Configuration (Default is 1 minute)
INTENDED_STATE	Configurations, sites, and resources
STATUS	Configurations, sites, and resources

[1] The health check interval is configurable with Data Guard Manager.

For example, to see these properties, you might use any of the SHOW commands. The following example uses the SHOW SITE VERBOSE command to display information about the Boston site.

```
DGMGRL> SHOW SITE VERBOSE 'Boston';
Site
  Name:                          'Boston'
  Hostname:                      'system1'
  Instance name:                 'bstn'
  Service Name:                  'primary'
  Standby Type:                  'physical'
  Number Built-in Processes:     '2'
  Enabled:                       'yes'
  Required:                      'yes'
  Default state:                 'PRIMARY'
  Intended state:                'PRIMARY'
  Number of resources:  1
  Resources:
    Name: Sales_db (default) (verbose name='Sales_db')
```

See Also: Chapter 7 for complete information about the Data Guard command-line interface

2.9 Protection Modes

The broker can simplify the process of setting up your configuration for any of the different grades of data protection: maximum protection, maximum availability, maximum performance.

This section contains the following topics to help you configure the proper protection for your configuration:

- Section 2.9.1, "Setting the Protection Mode for Your Configuration"
- Section 2.9.2, "How Broker Operations Affect Protection Modes"

2.9.1 Setting the Protection Mode for Your Configuration

To set the protection mode, perform the following steps:

Step 1 Determine which data protection mode you want to use.

Each data protection mode provides a different balance of data protection, data availability, and database performance. To select the data protection mode that meets the needs of your business, carefully consider your data protection requirements and the performance expectations of your users.

Maximum Protection

Maximum protection mode offers the highest level of data protection, but it may decrease the performance and availability of the primary database. The maximum protection mode:

- Guarantees there will be no data loss between the primary site and at least one physical standby site in the configuration.
- Shuts down the primary database instance if the primary database is unable to write the redo records to at least one physical standby database that is configured to use the SYNC log transport mode.
- Requires at least one physical standby database must be configured to use the SYNC log transport mode.

  You must set the LogXptMode property to SYNC for the physical standby database. (See Section 4.3.2.4 for more information about setting the log transport mode.)
- Requires that standby redo logs must be configured for at least one physical standby database.

- Does not support logical standby databases.

Maximum Availability

Maximum availability mode offers the next highest level of data protection possible while maximizing the availability of the primary database. The performance impact on the primary database is less than that of the maximum protection mode. The maximum availability mode:

- A transaction does not commit until all data needed to recover it has been written to at least one (physical or logical) standby database that is configured to use the SYNC log transport mode. This mode guarantees zero data loss unless a primary database failure occurs before recovery from a network outage.
- Makes a *best effort* to write the redo records to at least one physical or logical standby database that is configured to use the SYNC log transport mode.

  Unlike maximum protection mode, the maximum availability mode *does not* shut down the primary database instance if the primary database is unable to write the redo records to at least one physical standby database that is configured to use the SYNC log transport mode. Instead, the protection mode is downgraded temporarily to maximum performance mode until the fault has been corrected and the standby database has caught up with the primary database.
- Requires that at least one standby database must be configured to use the SYNC log transport mode.

  You must set the `LogXptMode` property to SYNC for the standby database. (See Section 4.3.2.4 for more information about setting the log transport mode.)
- Requires that standby redo logs must be configured for physical standby databases.
- Can be used with physical and logical standby databases.

Maximum Performance

Maximum performance mode is the default protection mode. This mode provides the highest level of data protection possible without affecting the performance of the primary database. This protection mode:

- Allows a transaction to commit on the primary database before the data needed to recover it has been written to a (physical or logical) standby database. Therefore, some transactions may be lost if the primary database fails and you are unable to recover the redo records from the primary database.

- You should set the LogXptMode property to ASYNC or ARCH for the standby database. (See Section 4.3.2.4 for more information about setting the log transport mode.)

  See Also: *Oracle9i Data Guard Concepts and Administration* for a complete discussion about the advantages and disadvantages of each data protection mode and for information about configuring log transport services for each protection mode

Step 2 Set up standby redo logs, if needed.

If the data protection mode that you need requires that one or more physical standby databases use the SYNC or ASYNC log transport mode, you may need to add standby redo logs to those physical standby sites. Logical standby database do not support standby redo logs. (Note that the maximum performance mode does not require standby redo logs.)

Data Guard Manager provides the Standby Redo Log Assistant that automatically sets up standby redo logs on one or more physical standby databases in your configuration, and on the primary database in preparation for a switchover operation.

Step 3 Set the LogXptMode property, if necessary.

If the data protection mode requires that you change the log transport mode used by any of the standby databases, change the setting of the LogXptMode database property appropriately on each standby database. See Section 4.3.2.4 for more information about setting the log transport mode.

Step 4 Set the protection mode.

Select the Protection Mode using the CLI or Data Guard Manager:

With Data Guard Manager:

1. Select the configuration in the navigator tree.
2. Click the **Data Protection** tab.
3. Select the Protection Mode you chose in step 1 and click **Apply**.

   After you change the protection mode, the primary site and database will automatically restart.

With the CLI:

1. If you plan to set the protection mode to either the MAXPROTECTION or MAXAVAILABILITY protection mode, ensure that standby redo logs are configured on the physical standby site.
2. Use the ALTER RESOURCE (property) command on the standby database to set the log transport mode that corresponds to the protection mode you plan to set. For example, if you plan to set the overall Data Guard configuration to the MAXAVAILABILITY mode, you must use the ALTER RESOURCE command to set the SYNC mode for log transport services. For example:

   ```
   SQL> ALTER RESOURCE 'Sales_db' ON SITE 'Boston' SET PROPERTY
   LogXptMode=SYNC;
   ```

3. Use the ALTER CONFIGURATION SET PROTECTION MODE AS *protection-mode*; command on the standby database to set the overall configuration protection mode. For example:

   ```
   SQL> ALTER CONFIGURATION SET PROTECTION MODE AS MAXAVAILABILITY;
   ```

After you change the protection mode, the primary site and database will automatically restart.

2.9.2 How Broker Operations Affect Protection Modes

This section describes how operations such as switchover, failover, disabling, or enabling the Data Guard configuration can have an affect on the configuration's protection mode and the log transport services. This section contains the following sections:

- Upgrading or Downgrading the Current Protection Mode
- Switchover Operations
- Failover Operations
- Disable and Enable Operations
- Requirements When Removing an Object in the Configuration
- Requirements On Other Operations

2.9.2.1 Upgrading or Downgrading the Current Protection Mode

When you change the current Data Guard protection mode to another protection mode (for example, you might want to upgrade from the maximum performance mode to the maximum availability mode), you must shut down and restart the

primary database. Follow these recommendations when upgrading or downgrading the Data Guard protection mode:

- When upgrading the protection mode, upgrade the log transport mode before you upgrade the overall protection mode. At the time when you change the protection mode or reset the log transport mode of a standby site, the broker verifies that there is at least one standby site in the configuration that can support the requested grade of protection. If not, then the broker does not change the protection mode and returns an error.
- When downgrading the protection mode, downgrade the protection mode first and then change the log transport mode (if necessary). The broker will not downgrade the log transport mode if doing so invalidates the current overall protection mode.

For example, if you reset the protection mode from the maximum performance mode to the maximum protection mode, the broker ensures that there is at least one physical standby database using standby redo logs, and whose log transport mode is set to SYNC. If there are no physical standby databases in the configuration that meet these requirements, the request to upgrade the protection mode is rejected with an error.

2.9.2.2 Switchover Operations

A switchover operation does not change the overall Data Guard protection mode. The protection mode remains the same as it was at prior to the switchover operation. However, before you start the switchover operation, you should verify that there will be at least one standby site in the configuration whose log transport mode can support the grade of protection after the switchover occurs.

Before you invoke a switchover operation, if necessary, you can pre-set the log transport mode on the current primary site to the SYNC, ASYNC, or ARCH mode that is required to support the Data Guard protection mode. Then, when the switchover operation begins, the broker verifies the log transport mode setting on each standby site including the log transport mode value that you preset for the current primary site. If the verification is successful, the switchover operation continues; otherwise the switchover operation fails, and the database roles and the Data Guard configuration files remain unchanged.

2.9.2.3 Failover Operations

After a failover, the Data Guard protection mode is always degraded to maximum performance mode. This is because there may not be a standby site in the configuration whose log transport mode can support a higher grade of protection

(maximum protection and maximum availability mode) after the failover occurs. You can upgrade the protection mode later, if necessary. During a failover operation, the log transport modes of the bystanders remain the same.

2.9.2.4 Disable and Enable Operations

When you disable a standby site or a standby database resource, the broker checks to see if the overall protection mode can still be satisfied by any of the remaining standby databases. If not, the broker rejects the disable operation. Otherwise, the broker allows the disable operation to proceed.

After a standby database resource object is successfully disabled, you can change the log transport mode of the resource and the broker will record the change only in the Data Guard configuration file. Thus, the change will not affect the overall protection mode because it is guaranteed that at least one of the enabled standby databases already satisfies the overall protection mode requirement. Once the database resource object is re-enabled, the broker will set the log transport mode of the database according to the value in the Data Guard configuration file.

When you disable the entire configuration, the broker always allows the operation to complete. This is because you may want to use the broker only to set up a Data Guard configuration, and then disable it from the broker's control and use other interfaces (for example, using command-line interfaces and SQL statements) for management.

If the entire configuration is disabled, you can change any broker settings, including the log transport modes of the standby databases and the protection mode of the configuration. The broker saves the changes in the Data Guard configuration file, but the changes will not be made to the database itself.

When enabling the entire configuration, the broker first checks to see if the protection mode will be satisfied by the log transport modes of the standby databases that will be enabled. If not, the enable operation fails and the configuration remains disabled. Otherwise, the enable operation successfully enables the configuration and the broker enables the database using the settings saved in the Data Guard configuration file.

2.9.2.5 Requirements When Removing an Object in the Configuration

When removing a standby database resource object or a standby site, the broker checks to see if the protection mode is still satisfied. If you want to remove the entire configuration, the broker always allows the operation.

2.9.2.6 Requirements On Other Operations

Some operations that take place in a broker configuration, especially operations related to log transport services, can affect the overall protection mode. These operations include:

- Setting the standby database into the offline state
- Stopping log transport services on the primary database
- Stopping log transport services on individual standby databases

Before any of these operations can proceed, the broker checks to see if the protection mode will be supported by the log transport mode settings on the standby sites after the operation completes. If not, the broker quits the operation and returns an error.

3

Managing Site Objects

This chapter describes site objects and how the broker manages them during switchover and failover operations.

This chapter includes the following sections:

- Section 3.1, "Site Objects"
- Section 3.2, "Role Management"

3.1 Site Objects

A site object is the middle level of the hierarchy of objects managed by the broker. A site object corresponds to a primary or standby site in a Data Guard configuration. Through site objects, you have the ability to centrally control the states and behavior of the primary and standby databases in the configuration, such as starting up and mounting the databases, starting and stopping log transport services and log apply services, performing a switchover or failover operation, dismounting and shutting down databases, and so on.

A site object may be enabled or disabled. When disabled, a site object is no longer managed and monitored by the broker. When enabled, a site object can be in an offline or an online state.

- Offline: If a site's state is offline, the site has been shut down. If you take a site offline, its database instance is put into a started, nomount state. If this is a primary database resource, then the log transport services will stop sending archived redo logs to the standby database. If this is a standby database resource, then the log apply services will stop accepting and applying the archived redo logs to the standby database.
- Online: If a site is online, the site is being managed by the broker and the database resource for the site will be put into its appropriate state:

- The primary database will be opened and the log transport services will ship archived redo log files to the standby databases.
- Physical standby databases will be mounted and the log apply services will apply archived redo logs to the databases.
- Logical standby databases will be opened (with the database guard set to on) and the log apply services will apply archived redo logs to the databases.

The state of a site object is dependent upon the state of the configuration containing the site, and the state of the database object is dependent upon that of the site. Thus, if a site is in an offline state, the database that is dependent on the site must also be in an offline state. Similarly, if the configuration is offline, all of the sites and resources in the configuration are also offline because all are logically dependent on the configuration object.

When in an online state and enabled, the broker manages the sites in a broker configuration in their mutually exclusive roles: primary or standby:

- Primary role: In this role, the primary site contains the primary database from which redo logs are transmitted to one or more standby sites
- Standby role: In this role, a standby site contains a standby database on which redo logs are received and applied to the standby database.

Thus, if a site is in an primary role, the database that is dependent on the site must also be in an primary role. With the broker, you can change these roles dynamically as a planned transition called a switchover operation, or you can change these roles as a result of a database failure through either a *graceful failover* or a *forced failover* operation. These are known as role transitions. The broker manages the steps involved in switchover and failover operations automatically for you by coordinating the role transitions for all of the affected sites and their dependent databases.

In configurations that include multiple standby sites, the standby sites that are not involved in the role transition are referred to as **bystanders**.

3.2 Role Management

When the primary site fails, such as when a system or software failure occurs, you may need to transition one of its corresponding standby sites to take over the primary role by performing a failover operation. Even in the absence of a disaster, you may have reason to perform a switchover operation to direct one of the standby

sites to assume the role of being the primary site, while the former primary site assumes the role of being a standby site.

Without the broker, failover and switchover operations are manual processes that can be automated only by using script-based solutions. For example, if a physical standby site is in read-only mode (log apply services are offline) when a failure occurs on the primary site, you must change the standby database to managed recovery mode, apply archived redo logs that have not yet been applied to the standby database, and fail over the standby database to the primary role.

The broker simplifies the switchover or failover operations by allowing you to invoke them through a single command and then coordinating role transitions on all sites in the configuration.

Note: If you are using Data Guard Manager and there are both physical and logical standby sites in the configuration, the broker will perform the switchover operation to a physical standby site. Data Guard Manager will switch over a logical standby site to the primary role only if there is no viable (enabled and online with NORMAL status) physical standby site. For failover operations, Data Guard Manager will switch over to the physical or logical standby database that you specify as the target of the failover.

3.2.1 Managing Switchover Operations

You can switch a site role from primary to standby, as well as from standby to primary, without resetting the online redo logs of the associated new primary database. This is known as a database switchover operation, because the standby database on the site that you specify becomes the primary database, and the original primary database becomes a standby database. There is no loss of application data, the data does not diverge between the original and the new primary database after the switchover operation completes, and there is no need to restart the bystander databases.

Whenever possible, you should always perform a switchover operation to a physical standby site:

- If the switchover operation transitions a physical standby site to the primary role, then the original primary site will be switched to a physical standby role. The redo logs are continuously shipped from the new primary database to all standby sites in the configuration.

- If the switchover operation transitions a logical standby site to the primary role, then the original primary site will be switched to a logical standby role. If there are physical bystanders in the configuration, they will not be able to serve as standby sites to the new primary site, because the new log stream is has become that of a logical standby site.
- If the switchover operation transitions a physical standby site to the primary role, then both the primary databaes and the target standby database will be restarted after the switchover operation completes.
- If the switchover operation transitions a logical standby site to the primary role, nothing needs to be restarted after the switchover operation completes. Neither the primary database nor the logical standby databases need to be restarted.

Warning: Switchover operations to a logical standby database will result in the physical standby databases being permanently disabled in the configuration.

3.2.1.1 Before You Perform a Switchover Operation

Consider the following points before you begin a switchover operation:

- When you start a switchover operation, the broker verifies that at least one standby database (including the new standby database that is about to be transitioned to the standby role) is configured to support the overall protection mode (maximum protection, maximum availability, or maximum performance).
- You should prepare the primary database in advance for its possible future role as a standby database. For example, if the primary site might be transitioned to a physical standby role and the LogXptMode property is set to SYNC or ASYNC, then you need to set up standby redo logs on the primary site. If you pre-set database properties for the standby database role, note that these properties are not verified by the broker until you actually switch over the primary database to the standby role.
- After a switchover operation completes, the overall Data Guard protection mode (maximum protection, maximum availability, or maximum performance) remains at the same protection level it was in prior to the switchover operation. Also, the log transport mode (SYNC, ASYNC, or ARCH) of bystanders does not change after a switchover operation. Log apply services for all bystanders automatically begin applying archived redo logs from the new primary database.

- If there are both logical and physical standby database in the configuration and the switchover operation occurs to a logical standby database, you will need to reinstantiate all physical bystanders in the new configuration after the switchover operation completes.

3.2.1.2 Starting a Switchover Operation

The act of switching roles should be a well-planned activity. The primary and standby databases involved in the site switchover operation should have as small a transactional lag as possible. Oracle Corporation highly recommends that you consider performing a full, consistent backup of the primary database prior to starting the switchover operation. (*Oracle9i Data Guard Concepts and Administration* provides detailed information about setting up the sites and databases in preparation of a switchover operation.)

To start a switchover operation using Data Guard Manager, select the Data Guard broker configuration and select **Switchover** from the right-click menu to invoke the Switchover wizard. When using the CLI, you need to issue only one `SWITCHOVER` command to specify the name of the standby site that you want to change into the primary role.

The broker controls the rest of the switchover operation, as described in Section 3.2.1.3.

3.2.1.3 How the Broker Performs a Switchover Operation

Once you start the switchover operation, the broker:

1. Verifies that the primary and the target standby sites and databases are in the following states:
   - The primary site and database must be enabled and online, with log transport services started. (For the CLI, this is the READ-WRITE-XPTON substate.)
   - A participating physical standby site and database must be enabled and online, with log apply services started. (For the CLI, this is the PHYSICAL-APPLY-ON substate)
   - A participating logical standby site and database must be enabled and online, with log apply services started. (For the CLI, this is the LOGICAL-APPLY-ON substate.)

   The broker allows the switchover operation to proceed as long as there are no errors for the primary site and standby site that you selected to participate in

the switchover operation. However, errors occurring for any bystanders will not stop the switchover operation.

2. Switches roles between the primary and standby sites.

   The broker first converts the original primary database to run in the standby role. Then, the broker transitions the target standby database to the primary role. If any errors occur during either conversion, the broker stops the switchover operation. See Section 3.2.1.4 for more information.

3. Updates the Data Guard configuration file to record the change in roles.

   Because the configuration file describes all site and resource objects in the configuration, this ensures that each object will run in the correct role.

4. Restarts the new primary database if the switchover operation occurs with a physical standby database, opening it in read / write mode, and starts log transport services shipping archived redo logs to the standby databases, including to the former primary database. If the switchover operation occurs to a logical standby database, then there is no need to restart any databases.

5. Restarts the new standby database if the switchover operation occurs with a physical standby database, and log apply services begin applying archived redo logs shipped from the new primary database.

The broker verifies the state and status of the database resources on each site to ensure that the switchover operation has successfully transitioned the sites to their new role correctly. Bystanders will continue operations in the state they were in before the switchover operation. For example, if a bystander physical standby database was in read-only mode, it will remain in that mode after switchover completes. Log apply services for all bystanders automatically begin applying archived redo logs from the new primary database.

3.2.1.4 Troubleshooting Switchover Operations

If the switchover operation fails due to problems with the configuration, the broker reports any problems it encounters. In general, you can choose another site for the switchover operation or fix the problem and then retry the switchover operation. The following subsections describe how to recover from the most common problems.

Problems Transitioning the Primary Site to the Standby Role

If the error messages returned indicate a problem when transitioning the original primary site and database to the standby role (including stopping log transport

services and starting log apply services), use these general guidelines to fix the problem:

1. Investigate the error message returned by the broker to find the source of the problem on the primary site and correct it. For example, you can look in the Data Guard Manager Viewlog for alert log information.
2. Reenable the configuration to refresh and restore the sites and database resources to their original roles and states.
3. Perform the switchover operation again.

Problems Transitioning the Standby Site to the Primary Role

If the error messages that have been returned indicate that a problem occurred when transitioning the original standby database to the primary role (including stopping log apply services and starting log transport services), use these general guidelines to fix the problem:

1. Disable the configuration.
2. Investigate the error messages returned by the broker to find the source of the problem on the standby site and correct it.
3. Restart the original primary database to run in the standby role. (You must restart this site as a standby site and database because the switchover operation has already successfully transitioned it to run in the standby role.)
4. Execute SQL*Plus commands to convert the *new* standby database back to running in the primary database role. To do this, perform the following steps:
   a. Locate the trace file in the log directory where you issued the SQL statements to create the control file for the original primary database.
   b. Extract the SQL commands from the trace file into a temporary file and execute the file from the SQL*Plus command line.
   c. Execute the `SHUTDOWN IMMEDIATE` command on the original primary database instance to restart it.
5. Restart the original primary database as the primary database.
6. Reenable the configuration.
7. Perform the switchover operation again.

3.2.2 Managing Failover Operations

Database failover transitions one of the standby sites to the role of primary site. You should perform a failover operation only when a catastrophic failure occurs on the primary site, and there is no possibility of recovering the primary site and database in a timely manner. The failed primary site is discarded and the target standby site and database assume the primary role.

The broker supports two grades of failover operations:

- Graceful failover

  This is the recommended failover option. Graceful failover automatically recovers some or all of the original primary database application data and attempts to bring along any bystander sites and databases to continue serving as standby databases to the new primary database:

  – After a graceful failover to a physical standby database, the original primary database must be re-created. In addition, some physical standby databases may be permanently disabled if the broker detects that the data has diverged from the new primary database. However, physical standby databases that were disabled during the failover operation may be salvaged if the required logs are available and can be recovered. Otherwise, you must re-create bystanders that were permanently disabled prior to the failover operation or required reinstantiation as a result of the failover operation before they can serve as standby sites to the new primary site.

  – After a graceful failover to a logical standby database, the broker attempts to reinstate logical standby bystanders. However, the failover operation may result in all logical standby databases being permanently disabled under some circumstances. For example, if there is a gap in the log sequence and the logical standby bystanders cannot finish applying all of the redo data that the target logical standby database had applied prior to the failover operation. All physical standby databases will be permanently disabled when the failover occurs to a logical standby database.

- Forced failover

  Do not perform a forced failover to a standby site except in an emergency. Forced failover may result in lost application data even when standby redo logs are configured on the (physical) standby database. A consequence of a forced failover operation is that you must re-create the original primary database and all bystanders before they can serve as standby sites to the new primary site. Another consequence is that there may be lost application data unless the standby and primary databases had been configured to run in maximum

protection mode prior to the failover, and all logs have been successfully applied to the standby database.

Depending on the log transport services destination attributes, a graceful failover may provide no data loss or minimal data loss. A forced failover may result in data loss. Always try to perform a graceful failover operation; only when a graceful failover is unsuccessful should you perform a forced failover operation.

Note: After a failover operation, the overall Data Guard protection mode is always reset to the maximum performance mode. The log transport mode (SYNC, ASYNC, or ARCH) of the bystanders does not change.

3.2.2.1 Starting a Failover Operation

To start a failover operation using Data Guard Manager, select the Data Guard configuration in the navigator tree and then select **Failover** from the right-click menu to invoke the Failover wizard. The Failover wizard guides you through the steps necessary to transition one of the standby sites into the primary role. When using the CLI, you issue one FAILOVER command that specifies the name of the standby site that you want to change into the primary role, and the keyword GRACEFUL or FORCED to specify the type of failover operation.

The standby site that is the target of the failover operation should be a physical standby site in an enabled state. You can fail over to logical standby sites only if there are no enabled physical standby sites in the configuration.

After the failover operation, the overall protection mode of the new configuration (maximum protection, maximum availability, or maximum performance) is reset to the maximum performance mode, which is the default.

The broker controls the failover operation steps described in Section 3.2.2.2. However, you must perform the additional steps described in Section 3.2.2.4 after the failover operation completes.

3.2.2.2 How the Broker Performs a Graceful Failover Operation

Once you start the failover operation, the broker:

1. Verifies that the target standby site and database are in the enabled state. (For the CLI, this is the PHYSICAL-APPLY-ON substate for physical standby databases, or the LOGICAL-APPLY-ON substate for logical standby databases.)

If the database is not enabled, then you will not be able to perform a failover operation to this site.

2. Waits for the target standby site to finish applying any remaining archived redo logs before stopping log apply services on it.
3. Updates the Data Guard configuration file to record the change in roles.

   If a bystander was in an online state, then the bystander will be restarted in the state it was in before the failover operation. If a bystander was in the offline state, then it will be taken to its default online state during the failover operation. For example, if a physical standby database was operating in read-only mode, it will remain in read-only mode.

   Note: Standby bystanders may be permanently disabled during a graceful failover operation and they must be re-created in the configuration before they can serve as standby sites to the new primary site. A graceful failover to a logical standby database may result in all logical standby databases being permanently disabled, but it will result in all physical standby databases being permanently disabled.

4. Transitions the target standby site into the primary role, opens the new primary database in read/write mode, and starts log transport services that begin shipping archived redo logs to bystanders.

The broker allows the failover operation to proceed as long as there are no errors for the standby site that you selected to participate in the failover operation. However, errors occurring for any bystanders will not stop the failover operation. If you initiated a graceful failover operation and it fails, you might need to restart it as a forced failover operation.

3.2.2.3 How the Broker Performs a Forced Failover Operation

Once you start the failover operation, the broker:

1. Verifies that the target standby site and database are enabled. If the standby site is not enabled for management by the broker, then the failover operation cannot occur.
2. Stops log apply services on the standby site immediately, without waiting for log apply services to finish applying the available archived redo logs. Note that this may result in some data loss.

3. Updates the Data Guard configuration file to record the change in roles.
4. Transitions the target standby site into the primary role, opens the new primary database in read / write mode, and starts log transport services.

   Because a forced failover operation starts a new log stream from the new primary site, all bystanders are permanently disabled from the broker configuration. These standby sites are left in an online state, but they are no longer manageable by the broker.

The broker allows the failover operation to proceed as long as there are no errors for the standby site that you selected to participate in the failover operation.

3.2.2.4 Completing the Failover Operation

You must perform recovery steps after the failover operation completes:

- After a graceful or forced failover operation completes, the original, failed primary database and the new primary database have diverged. The original primary database is permanently disabled by the broker until such time as the database can be reinstantiated as a standby to the new primary database.
- After a graceful failover completes, any of the bystander standby sites that determine for themselves that they cannot continue as a viable standby for the new primary will be permanently disabled by the broker.

  For instance, this could happen if a bystander finds that it has applied more logs than the new primary itself has applied, hence diverging from the new primary. The bystander must be reinstantiated before it may serve as a standby for the new primary database.
- After a graceful failover to a logical standby completes, all physical bystander standby databases in the configuration have diverged from the new primary database. The broker permanently disables the physical bystanders. They must be reinstantiated before they can serve as standby to the new primary database.
- After a forced failover completes, the new primary database has diverged from all bystander standby sites regardless of their type. The broker permanently disables all of them. They must be reinstantiated before they can serve as standby to the new primary database.

A permanently disabled site is recovered for broker operation by:

- Removing the site object from the configuration. This also removes any dependent objects, i.e. the database object that depends upon that site.

- Reinstantiate the database itself from the new primary database using the procedures described in *Oracle9i Data Guard Concepts and Administration.*
- Restore the site and its database to the broker configuration.
- Enable the restored site. The newly reinstantiated standby database will begin serving as standby to the new primary database.

3.2.2.5 Troubleshooting Failover Operations

Although it is possible for a failover operation to stop, it is very unlikely. If an error occurs, it is likely to happen when the standby site is transitioning to the primary role. If the error messages that have been returned indicate that this is when the problem occurred, use these general guidelines to fix the problem:

1. Investigate the error message returned by the broker to find the source of the problem and correct it.
2. Perform the failover operation again.

4

Managing Database Resources

This chapter describes managing the states and properties that are specific to the database resource object in the following sections:

- Section 4.1, "Database Resources"
- Section 4.2, "Database Resource States"
- Section 4.3, "Database Resource Properties"

4.1 Database Resources

A database resource object is at the lowest level in the hierarchy of objects managed by the broker. A database resource object corresponds to a primary or standby database instance. The broker uses this object to manage and monitor the state of a single database.

The broker can distinguish between a physical and a logical standby database, and configures a physical standby site object and database resource object in a broker configuration, or a logical standby site and database resource object. These logical objects are configured with states, properties, and dependency relationships that are appropriate for their standby types.

4.2 Database Resource States

The state of a database resource is dependent upon the state of the site on which the resource resides. For example, if a site is in an offline state, the database that is dependent on the site must also be in an offline state.

When a site is in an online state and enabled, its database resource object can be in either an offline or an online state.

4.2.1 Offline State

When you first create and enable a configuration with the broker, the default state for database resources is online. Before setting the state to offline, you should carefully consider whether or not the interruption in access to data and the computing resources is necessary. The following list describes the actions the broker takes when you set a database resource to the offline state:

When you set the state of a primary or standby (logical or physical) database to offline, the broker automatically shuts down the database first and then restarts it (nomount).

- While the primary database is in the offline state, the database instance is started (nomount) and log transport services are stopped (archive redo logs are not being shipped to any standby databases).
- While the physical or logical standby database is in the offline state, the database instance is started, nomount and log apply services do not apply archived redo logs to the standby database. Furthermore, the standby site is incapable of receiving archived redo logs.

4.2.2 Online State and Substates

When the broker first starts a database resource in the online state, the database resource is started in one of several substates. For example:

- For a primary database, the default online state is to start the database resource and open it in read / write mode with log transport services started (archiving redo logs to the standby database).
- For a physical standby database, the database resource is started and mounted, with log apply services started and applying archived redo logs to the standby database.
- For a logical standby database, the database resource is started and opened in read / write mode, but the replicated tables in the database are open read-only to queries. The database guard is turned on and log apply services are started and applying archived redo logs to the standby database.

Table 4–1 describes all of the primary and standby database resource online states and substates. The first two columns of the table show the substate name if you are using Data Guard Manager and the corresponding name if you are using the CLI.

Table 4–1 Database Substate Names and Descriptions

Substate Name in CLI	Substate Name in Data Guard Manager	Description
LOGICAL-APPLY-READY	Apply Off	The logical standby database is open for read-only queries, but log apply services are not running. The logical standby database guard is on.
LOGICAL-APPLY-ON	Online	The logical standby database is open for read-only queries and log apply services are started. The logical standby database guard is on. This is the default state for a logical standby database.
PHYSICAL-APPLY-READY	Apply Off	The physical standby database is mounted, but log apply services are stopped. The standby database is not open for read-only queries.
PHYSICAL-APPLY-ON	Online	The physical standby database is mounted and log apply services are started. The standby database is not open for read-only queries. This is the default state for a physical standby database.
READ-ONLY	Read-only	The physical standby database is open for read-only queries, but log apply services are stopped. This substate is not applicable to logical standby databases.
READ-WRITE	Transport Off	The primary database is open for read / write access, but log transport services are not shipping logs to the standby databases.
READ-WRITE-XPTON	Online	The primary database is open for read / write access and log transport services are archiving redo logs to the standby databases. This is the default state for a primary database.

4.2.3 Database State Transitions

Figure 4–1 graphically shows the online states and substates that were described in Table 4–1. The double arrows indicate that you can transition from one state to any other state.

Figure 4–1 Database State Transition Diagrams

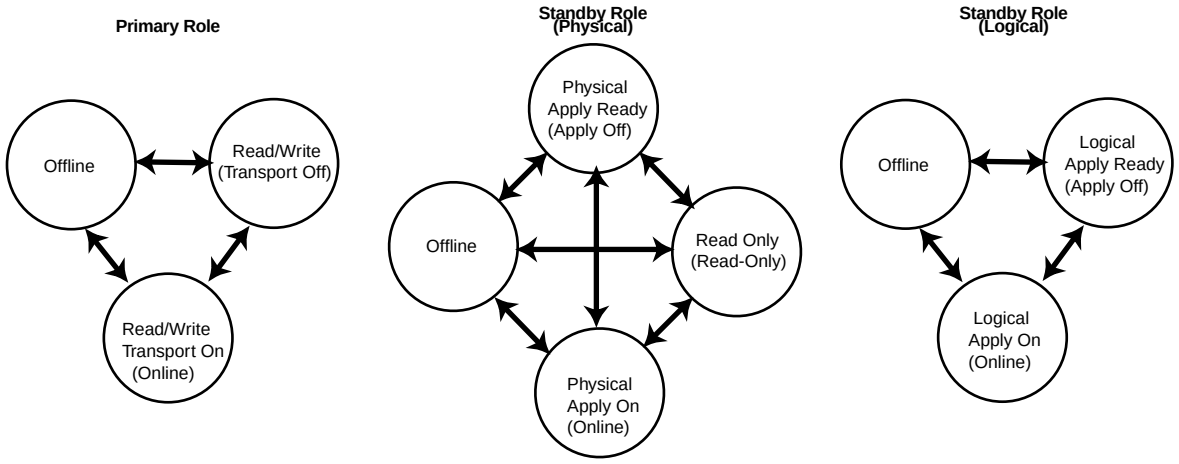


Figure 4–1 shows that the primary and standby databases can be in an offline state or, when online, can be in one of several substates:

- Primary database online substates:

  READ-WRITE
  READ-WRITE-XPTON

  For a primary database, the transition from any online state to an offline state includes shutting down and restarting the primary database in nomount mode.

- Logical standby database online substates:

  LOGICAL-APPLY-READY
  LOGICAL-APPLY-ON

  When a logical standby database is taken offline, it is shut down and restarted as is done for the primary database.

- Physical standby database online substates:

  PHYSICAL-APPLY-READY
  PHYSICAL-APPLY-ON
  READ-ONLY

  When a physical standby database is taken offline, it is shut down and restarted as is done for the primary database.

Note: Before you can transition a physical standby database from a READ-ONLY state to any other state, you must first close all of the open sessions to the standby database. If some of the sessions are not closed, the state transition will fail.

The physical standby database cannot have any user sessions connected when changing from the read-only state to any other state. The state change will fail and return the ORA-16727 error corresponding to the ORA-1093 error. You can resolve this error by performing the following steps:

1. Check the alert log for additional errors.

   If you see the ORA-1093 message in the alert log, it is likely that there are additional user sessions connected to the standby database that is in a read-only state.

2. Query V$SESSION view (specify the SELECT OSUSER, PROGRAM, TYPE statement) to see all active sessions.

3. If you see any sessions in the V$SESSION view other than your current broker (Data Guard Manager or command-line interface) session, ask the read-only users to disconnect before you perform the state transition.

With the CLI, you can use the ALTER RESOURCE command to explicitly change the state of a database resource. For example, the ALTER RESOURCE command in the following example changes the state of the Sales_db resource to read/write.

```
DGMGRL> ALTER RESOURCE 'Sales_db' ON SITE 'Boston' SET STATE='read-write';
Succeeded.
```

See Also: Chapter 7 for complete information about the ALTER RESOURCE command. See Chapter 5 for examples of performing state transitions using Data Guard Manager.

4.3 Database Resource Properties

The broker manages database initialization parameter values as **database resource properties** and stores them in the Data Guard configuration file.

There are two types of properties: configurable and monitorable:

- Monitorable property values can only be viewed.
- Configurable property values can be viewed and dynamically updated.

4.3.1 Monitorable (Read-Only) Properties

Monitorable properties allow you to view information related to database resources, but you cannot change the value of these properties. These properties can be very helpful when you are trying to diagnose problems in the broker configuration. For example, view the `InconsistentLogXptProps` property to determine where there is a discrepancy for log transport services properties whose values are inconsistent between the Data Guard configuration file and the actual value currently used by the database. You can view all of the monitorable properties using CLI `SHOW` commands. Data Guard Manager displays the information obtained from these properties on the Properties page.

The following monitorable properties can be seen only when you are using the CLI and the database resource is enabled:

`InconsistentLogXptProps`	(Inconsistent Log Transport Properties)
`InconsistentProperties`	(Inconsistent Database Properties)

The following monitorable properties can be seen only when the database resource is enabled and in an online state in the CLI, except for the `LsbySkipTable` and the `LsbySkipTxnTable` properties, which also can be seen in Data Guard Manager:

`LogXptStatus`	(Log Transport Status)
`LsbyFailedTxnInfo`	(Logical Standby Failed Transaction Information)
`LsbyParameters`	(Logical Standby Parameters)
`LsbySkipTable`	(Logical Standby Skip Table)
`LsbySkipTxnTable`	(Logical Standby `Skip Transaction Table`)
`SbyLogQueue`	(Standby Log Queue)
`SendQEntries`	(Send Queue Entries)

> **See Also:** Chapter 8 for more information about the database resource monitorable properties.

4.3.2 Configurable (Changeable) Database Resource Properties

Configurable properties affect the operation or configuration of the database resource objects. When you use the CLI or Data Guard Manager to create a primary site and import existing standby sites into a new broker configuration, the property values are imported from the database settings. Later, you can update many property values when the database is either disabled or enabled.

The following configurable properties are listed according to whether the property controls initialization parameters, log transport services, or log apply services.

- Properties that control initialization parameters:

  `ArchiveLagTarget`

  `DbFileNameConvert`

  `LogArchiveFormat`

  `LogArchiveMaxProcesses`

  `LogArchiveMinSucceedDest`

  `LogArchiveTrace`

  `LogFileNameConvert`

  `StandbyArchiveDest`

  `StandbyFileManagement`

- Properties that control log transport services:

  `Alternate`

  `AsyncBlocks`

  `Binding`

  `DelayMins`

  `Dependency`

  `LogShipping`

  `LogXptMode`

  `MaxFailure`

  `ReopenSecs`

  See Also: Section 4.3.2.4 for information about controlling the log transport services protection mode with the LogXptMode property

- Properties that control log apply services:

  The following properties control log apply services for physical standby databases:

  `ApplyNext`

ApplyNoDelay

ApplyParallel

The following properties control SQL apply services for logical standby databases:

LsbyASkipCfgPr

LsbyDSkipCfgPr

LsbyASkipErrorCfgPr

LsbyDSkipErrorCfgPr

LsbyASkipTxnCfgPr

LsbyDSkipTxnCfgPr

LsbyMaxEventsRecorded

LsbyMaxServers

LsbyMaxSga

LsbyRecordAppliedDdl

LsbyRecordSkipDdl

LsbyRecordSkipErrors

LsbyTxnConsistency

Note: Data Guard Manager uses the LsbySkipTable property to represent the LsbyASkipCfgPr, LsbyDSkipCfgPr, LsbyASkipErrorCfgPr, and LsbyDSkipErrorCfgPr properties. It uses the LsbySkipTxnTable property to represent the LsbyASkipTxnCfgPr and LsbyDSkipTxnCfgPr properties.

See Also: Chapter 8 for reference information for all of the database resource properties

4.3.2.1 Verifying and Updating Properties

When the configuration is enabled, the broker keeps the database property values in the Data Guard configuration file consistent with the values being used in the

database. For initialization parameter-related properties, the broker maintains the consistency between the value in the Data Guard configuration file, the current database value, and the initialization parameter value in the server parameter file (SPFILE), as follows:

- For dynamic parameters, the broker keeps the value of the database parameter consistent in the system global area (SGA) for the instance, in the Data Guard configuration file, and in the SPFILE.
- For static parameters and properties, the database parameter value in the system global area (SGA) for the instances may temporarily differ from what is in the Data Guard configuration file and in the SPFILE. Typically, the database value becomes the same as the SPFILE value and the Data Guard configuration file value the next time the database instance is stopped and restarted.

Even when the configuration is disabled, you can update database property values through the broker. The broker retains the property settings (without validating the values) and updates the database initialization parameters in the SPFILE and the in-memory settings the next time you enable the broker configuration.

Note: Although you can change a property whether the configuration is enabled or disabled, the change does not take effect on the database unless the configuration is enabled.

4.3.2.2 Default Property Values

If you do not explicitly set property values, the broker uses a default value for the database properties. For example, if you created a new standby database without specifying a log transport mode, the broker sets the `LogXptMode` property to `ARCH`, for physical standby databases and to `ASYNC` for logical standby databases.

4.3.2.3 Preparing for Switchover Operations

All of the properties are present for all of the databases that are a part of a broker configuration—the values for individual databases can be different. Some subset of properties and associated values are used only when the database is a standby database, while others are used when the database is a primary database.

Note: If you set up the database resource properties for the standby role on the primary database in preparation for it becoming a standby database, the broker cannot verify these properties, thus causing potential problems after the switchover operation completes. For example, if you do not set the `StandbyArchiveDest` resource property on the primary database prior to the switchover operation, this may cause a problem that only becomes apparent after the switchover operation is complete.

Therefore, prior to performing a switchover operation, consider setting properties on the standby database to prepare it for a future transition to the primary role. Similarly, you should set properties on the primary database to prepare it for a future transition to the standby role.

If you set properties related to log transport services, such as the `Alternate`, `AsyncBlocks`, `Binding`, `DelayMins`, `Dependency`, `LogShipping`, `LogXptMode`, `MaxFailure`, or `ReopenSecs` properties on a standby database, the values that you set will persist through role changes during switchover or failover operations. Also:

- If you set these properties on a standby database, the actual database values are set on the primary database through the `LOG_ARCHIVE_DEST_`*n* and `LOG_ARCHIVE_DEST_STATE_`*n* initialization parameters.
- No matter which site becomes the primary site after a switchover or failover operation, these properties of a standby are always used to set log transport of the current primary to this standby.

4.3.2.4 Configuring Log Transport Services for Data Protection

Section 2.9 described how the broker handles data protection modes. As a part of the overall configuration protection mode, you must ensure that the log transport services are also properly set up for the data protection mode that you have chosen.

You use the `LogXptMode` property to set the `SYNC`, `ASYNC`, or `ARCH` mode for log transport services. Table 4–2 shows the protection modes, the corresponding log transport mode, and the SQL statement that corresponds to the protection mode that you have chosen.

Table 4–2 Data Guard Protection Modes and Log Transport modes

Protection Mode	Log Transport Services	Equivalent to . . . .
MAXPROTECTION[1]	SYNC	ALTER DATABASE SET STANDBY TO MAXIMIZE PROTECTION
MAXAVAILABILITY	SYNC	ALTER DATABASE SET STANDBY TO MAXIMIZE AVAILABILITY
MAXPERFORMANCE	ASYNC or ARCH	ALTER DATABASE SET STANDBY TO MAXIMIZE PERFORMANCE

[1] The MAXPROTECTION mode requires physical standby database and standby redo logs. This mode is not supported by logical standby databases.

The values for the `LogXptMode` property are described in the following list:

SYNC

Configures the log transport services for this standby database using the `LGWR`, `SYNC`, and `AFFIRM` settings. If this is a physical standby database, standby redo logs are required. If this is a logical standby database, standby redo logs are not required because logical standby databases do not use them. This mode is required for the maximum protection or maximum availability data protection modes. This log transport mode provides the highest grade of data protection to the primary database, but also incurs the highest performance impact.

ASYNC

Configures the log transport services for this standby database using the `LGWR`, `ASYNC`, and `NOAFFIRM` settings. If this is a physical standby database, standby redo logs are required. If this is a logical standby database, standby redo logs are not required because logical standby databases do not use them. This log transport mode provides a moderate grade of data protection to the primary database, and low performance impact.

ARCH

Configures the log transport services for this standby database using the `ARCH` setting. Standby redo logs are not required. This log transport mode provides the lowest grade of data protection to the primary database, and the lowest performance impact.

Note: If the data protection mode that you choose requires that one or more physical standby databases use the SYNC or ASYNC log transport mode, you may need to add standby redo logs to one or more of the standby sites.

Data Guard Manager provides the Standby Redo Log Assistant that automatically sets up standby redo logs on one or more physical standby databases in your configuration, and on the primary database in preparation for a switchover operation

5

Data Guard Manager Scenarios

This chapter provides several scenarios that show how to use the Oracle9*i* Data Guard Manager graphical user interface (GUI) to create, manage, and monitor a broker configuration.

This chapter contains the following scenarios:

- Scenario 1: Starting Data Guard Manager
- Scenario 2: Creating a Configuration
- Scenario 3: Connecting to a Configuration
- Scenario 4: Verifying the Configuration
- Scenario 5: Adding Sites to a Broker Configuration
- Scenario 6: Performing Routine Maintenance
- Scenario 7: Performing a Switchover Operation
- Scenario 8: Performing a Failover Operation
- Scenario 9: Monitoring a Data Guard Configuration
- Scenario 10: Using Event Tests
- Scenario 11: Removing a Configuration and Exiting Data Guard Manager
- Scenario 12: Re-Creating a Configuration with Data Guard Manager

5.1 Scenario 1: Starting Data Guard Manager

Start Data Guard Manager through the Oracle Enterprise Manager Console by taking the following steps.

Step 1 Start Oracle Management Server.

Start the Oracle Management Server from the command-line prompt by entering the `oemctl start oms` command.

Step 2 Launch the Oracle Enterprise Manager Console.

Launch Oracle Enterprise Manager at the command-line prompt by entering the `oemapp console` command. When the Enterprise Manager Console login dialog displays, you must select **Login to the Oracle Management Server**. Do not select Launch standalone, because Data Guard Manager will not be available from the Enterprise Manager Console if you select this option.

Step 3 Start the Intelligent Agent on the primary and standby nodes.

The Intelligent Agent must be running for Data Guard Manager to discover nodes, execute jobs and monitor events. Follow the directions in the *Oracle Intelligent Agent User's Guide* to configure and use the Intelligent Agent on the primary and standby nodes.

Step 4 Discover the primary and standby nodes.

Run the Enterprise Manager Discovery wizard, also referred to as the Discovery wizard, to discover the primary and standby nodes and gain access to the databases that you want to configure and administer with Data Guard Manager. To invoke the Discovery wizard from the Enterprise Manager Console menu bar, select **Navigator > Discover Nodes**.

Follow the directions in the Discovery wizard. When finished, all discovered nodes and databases are displayed in the Enterprise Manager navigator tree:

- On the primary node, the wizard discovers the primary database that you want to configure and administer with Data Guard Manager.
- On the standby node, the wizard discovers the following:
  - If you discover a standby node on which a standby database exists, the wizard gains access to the standby database and displays it in the Enterprise Manager navigator tree. When you run the Create Configuration wizard to create a configuration, you can have Data Guard Manager automatically add the existing standby database to the configuration.
  - If you discover a standby node on which a standby database does not exist, the wizard finds the Oracle homes on the system including the one where you have installed Oracle9*i* Enterprise Edition or Personal Edition. When you run the Create Configuration wizard to create a configuration, you can

select this Oracle home as the location in which you want Data Guard Manager to create a new standby database.

Step 5 Set Preferred Node Credentials on the primary and standby nodes.

You should set Preferred Credentials on both the primary and standby nodes to ensure Data Guard Manager can run remote processes to create the configuration. To set Preferred Credentials from the Enterprise Manager Console menu bar, select: **Configuration > Preferences > Preferred Credentials.**

Although setting Preferred Credentials for the databases is not required, you might want to set Preferred Credentials for the primary database and for the standby database if you are adding an existing standby database.

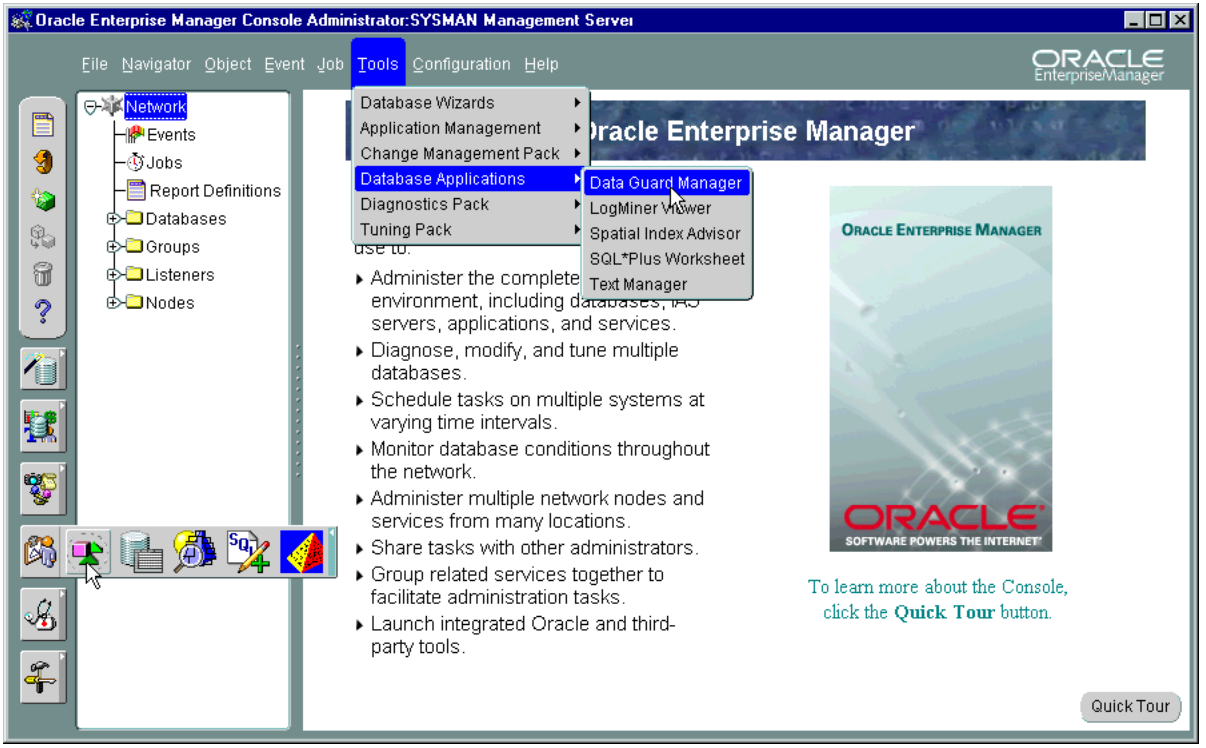
Step 6 Start Data Guard Manager.

You can start Data Guard Manager from the Enterprise Manager Console or at the command-line prompt:

- At the command-line prompt, enter the **`oemapp dataguard`** command.
- From the Enterprise Manager Console, use either of the following methods:
  - From the **Tools** menu in the Oracle Enterprise Manager Console, choose **Database Applications > Data Guard Manager**.
  - From the **Database Applications drawer** in the Oracle Enterprise Manager Console, move the cursor over the icons and select the **Data Guard Manager** icon.

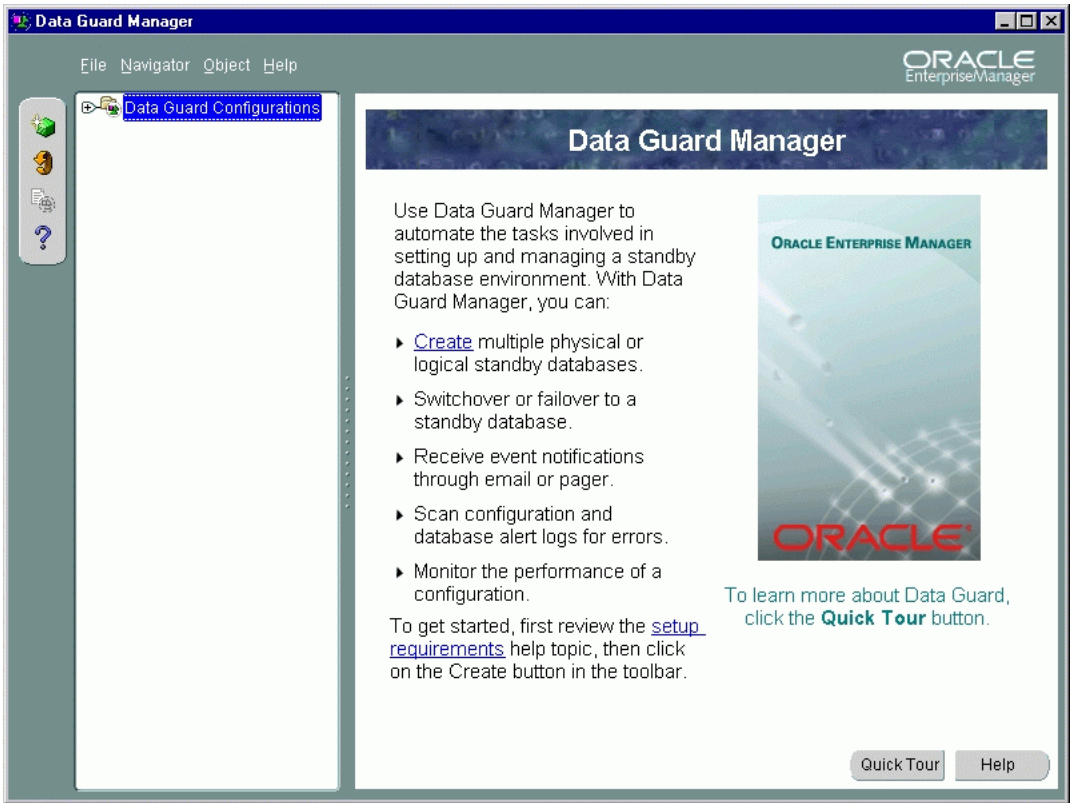
  Figure 5–1 shows both methods of starting Data Guard Manager from the Enterprise Manager Console.

Figure 5–1 Starting Data Guard Manager



When launched, Data Guard Manager displays the informational page shown in Figure 5–2.

Figure 5–2 Oracle Data Guard Manager Welcome Window



On this page, you can:

- Learn about Data Guard Manager: Click **Quick Tour** to call up the Data Guard Manager quick tour for an easy-to-follow product tour that describes Data Guard Manager concepts and operation.
- Search for information about any Data Guard Manager or Enterprise Manager topic—Click **Help** to display the Welcome to Oracle Data Guard Manager help topic. Once in the help system, you can use the Contents page or Search page to locate help topics of interest.
- Set up your environment to begin using Data Guard Manager: Click **setup requirements**.

- Create a broker configuration: Either right-click **Data Guard Configurations** in the navigator tree or click **Create** in the bulleted list on the right-hand window to start the Create Configuration wizard (described in Section 5.2).

5.2 Scenario 2: Creating a Configuration

Creating a broker configuration is the first thing you must do before you can manage and monitor the databases. Data Guard Manager provides the Create Configuration wizard to create a broker configuration that includes a primary database and one standby database. (You can use the Add Site wizard later to add more sites. See Section 5.5.) To start the Create Configuration wizard, right-click **Data Guard Configurations** in the navigator tree and choose **Create Configuration wizard**.

The wizard takes you through the following steps:

1. Ensure the Data Guard environment is set up properly.
2. Provide a configuration name.
3. Choose a primary database.
4. Choose how you want to add a standby database:
   - Import an existing standby database
   - Create a new physical or logical standby database
5. Verify the information you supplied to the wizard and make changes, if necessary.

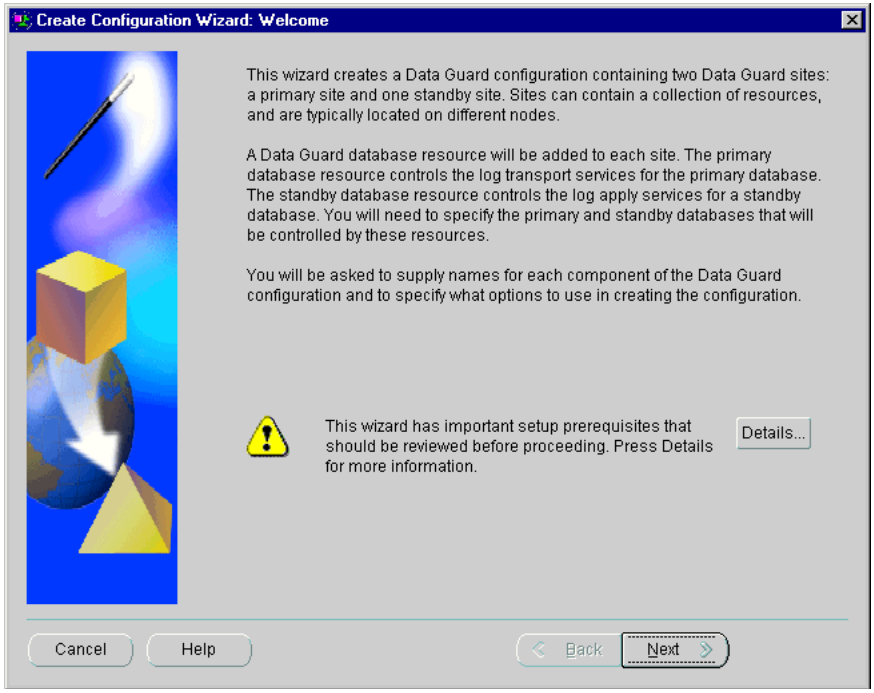
The following steps create a configuration and create a new physical standby database. It shows how the wizard takes you through additional steps to select the Oracle home for the database and to copy datafiles to the standby site.

Step 1 Ensure the Data Guard environment is set up properly.

Before the Create Configuration wizard steps you through the process of creating a broker configuration, you must ensure some basic configuration requirements have been met on the primary and standby nodes.

- When you click **Details** on the wizard welcome page shown in Figure 5–3, Data Guard Manager provides a handy checklist of setup requirements and information to help you ensure the environment is properly prepared.

Figure 5–3 Create Configuration Wizard - Welcome Page

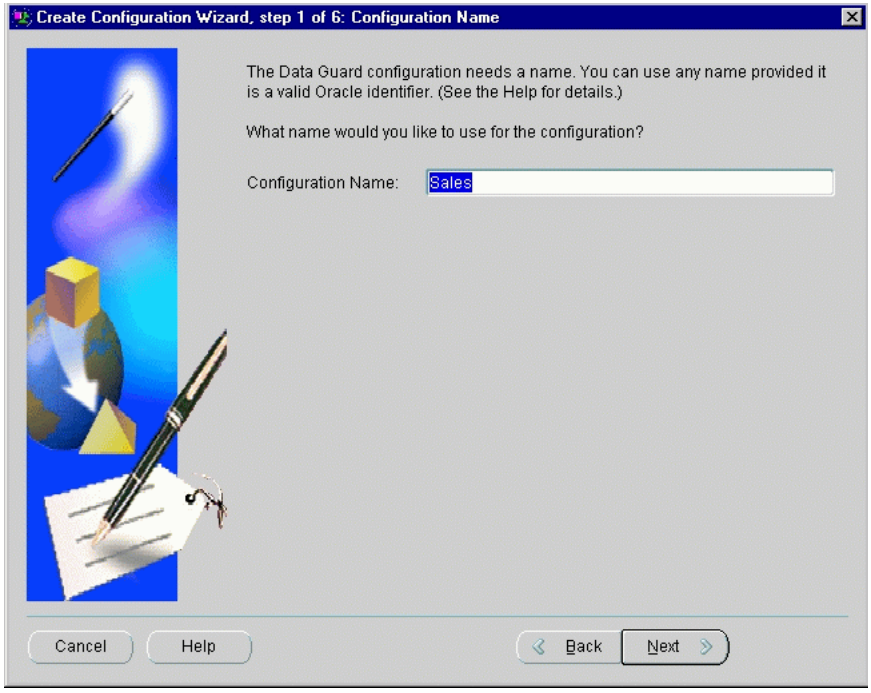


Step 2 Provide a configuration name.

The next dialog asks you to provide the name of the new broker configuration. Each configuration name must be an Oracle identifier that is unique among the configurations that you have created with Data Guard Manager.

Figure 5–4 shows the Configuration Name step in which a new configuration, Sales, is named.

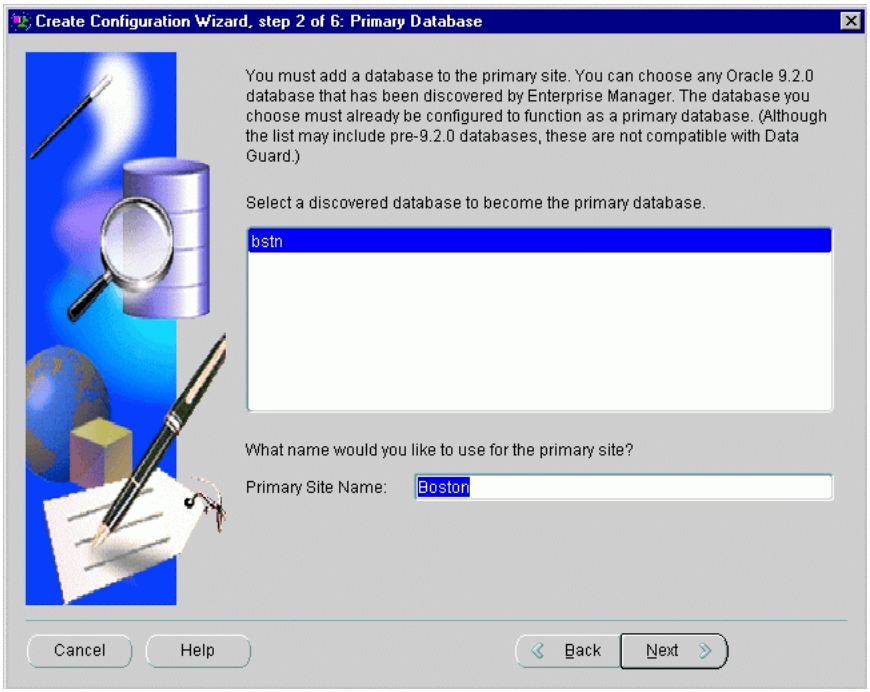
Figure 5–4 Create Configuration Wizard - Configuration Name



Step 3 Choose a primary database.

The list of discovered database instances listed on this page contains all of the instances that have been discovered through the Enterprise Manager Console Discovery wizard. (These instances were discovered during the setup work performed in Section 5.1 in the step titled, "Discover the primary and standby nodes.")

Figure 5–5 Create Configuration Wizard - Choose Primary Database



To select a primary database, select the Oracle9*i* database instance that you want to serve in the role of a primary database for this broker configuration. The database instance that you choose must be release 9.2 or greater, and it must be a primary database, such that the `CONTROLFILE_TYPE` in the V$DATABASE view is equal to `CURRENT`.

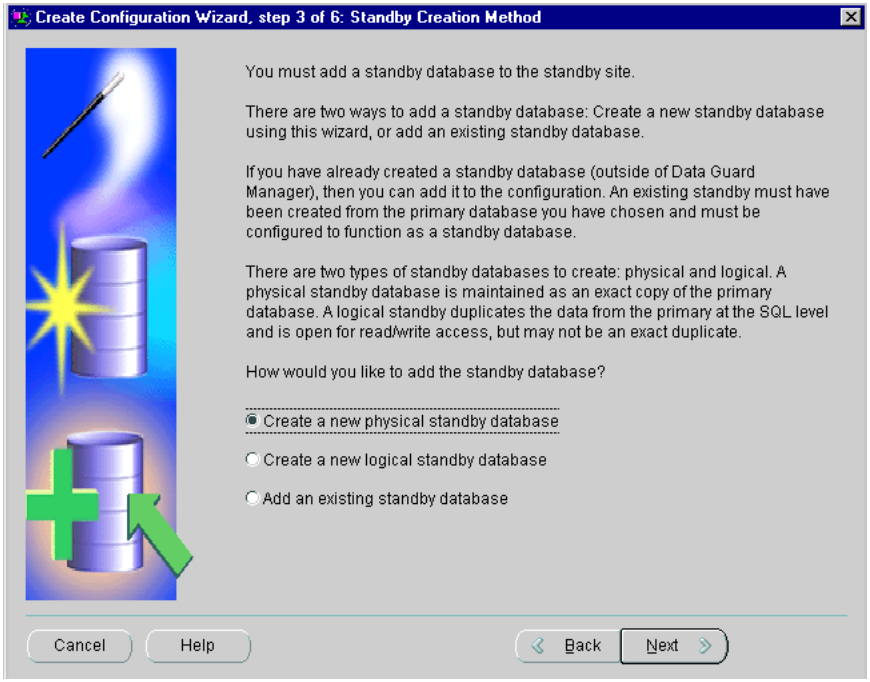
Note: The list of instances on this page may include both Oracle9*i* database instances and older instances (such as Oracle8*i*). For compatibility, you must select only Oracle9*i* release 2 (9.2) instances from the list.

Step 4 Choose how you want to add a standby database.

The wizard allows you to create a new physical or logical standby database or add an existing standby database.

This scenario will create a new physical standby database, as shown in Figure 5–6.

Figure 5–6 Create Configuration Wizard - Standby Database Creation Method



If you choose to add an existing standby database, the wizard displays a list of discovered database instances from which you select a physical or logical standby database to import into the broker configuration. The wizard connects to the database that you choose.

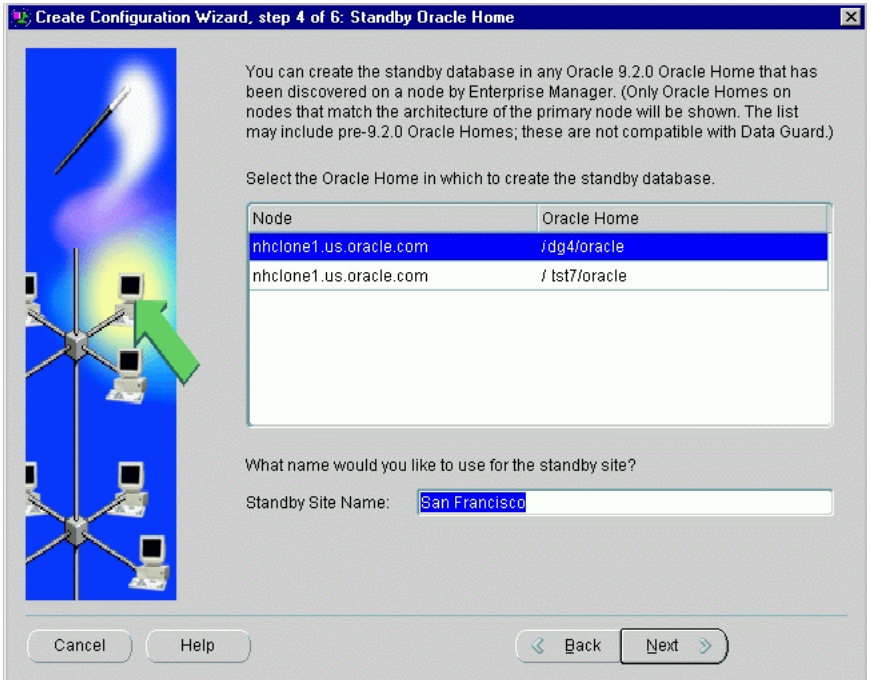
Step 5 Select an Oracle home, if necessary.

If you choose to create a new standby database, the wizard asks you to select the Oracle home on the standby node in which you want to create the standby database.

The wizard lists all of the Oracle homes that have been discovered through the Enterprise Manager Discovery wizard. You must select a discovered Oracle home and provide a unique name for the standby site.

Figure 5–7 shows this step of the configuration process.

Figure 5–7 Create Configuration Wizard - Select an Oracle Home



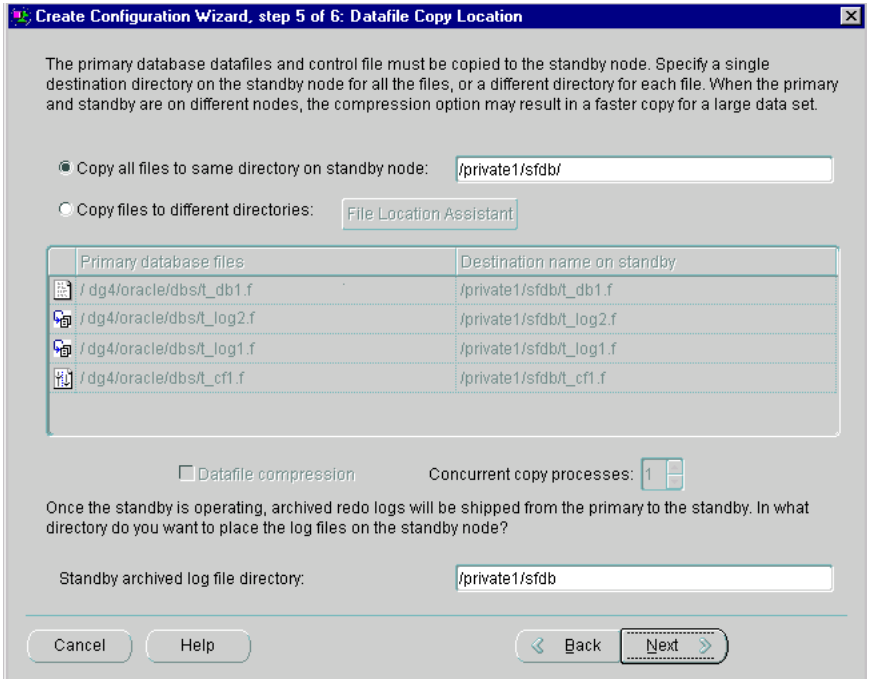
Step 6 Copy datafiles to the standby node.

If you choose to create a new standby database, part of the creation process involves copying the datafiles for the primary database to the standby node. Data Guard Manager uses the operating system (OS) method to copy the files.

- Select the location where you want the datafiles to be copied.

  As you enter the destination directory, the wizard assumes you want the archived redo logs in the same directory as the rest of the datafiles. and mirrors your input to the **Standby archived log file directory** field at the bottom of the page. Figure 5–8 shows this step of the configuration process.

Figure 5–8 Create Configuration Wizard - Supplying the Datafile Copy Location



Copy all files to the same directory on the standby node: Specify a single directory on the standby node. All files for the new standby instance will be copied to this directory. If the directory you specify does not exist on the standby database, Data Guard Manager will ask if you want to create the new directory and automatically

create it. (As you enter the destination directory, it is mirrored to the standby archived redo log file directory field at the bottom of the dialog.)

Copy files to different directories: You can specify individual destination directories on the standby node for each file. Enter each directory separately, or click **File Location Assistant** to automatically generate directory names. If a directory you specify does not exist on the standby database, Data Guard Manager will ask if you want to automatically create the directory.

Datafile compression: If the new standby database instance is located on a different node than the primary database, you can choose compression for the datafile copy. Depending on the composition of the datafiles, compression may result in a faster copy process, especially for large databases.

Concurrent copy processes: If the new standby database instance is located on a different node than the primary database, you can optionally specify up to 10 concurrent copy processes. Increasing the number of copy processes may result in a faster copy time for a large dataset. This option is available only on UNIX systems.

Standby archived log file directory: Specify a path name for the location on the standby node where you want log transport services to copy archived redo logs. Because archived redo logs sometimes require a large amount of space on the standby node, you might want to specify a different destination location from the datafiles. The default destination is the directory that you specified in the "Copy all files to the same directory on the standby node" text box at the top of this page.

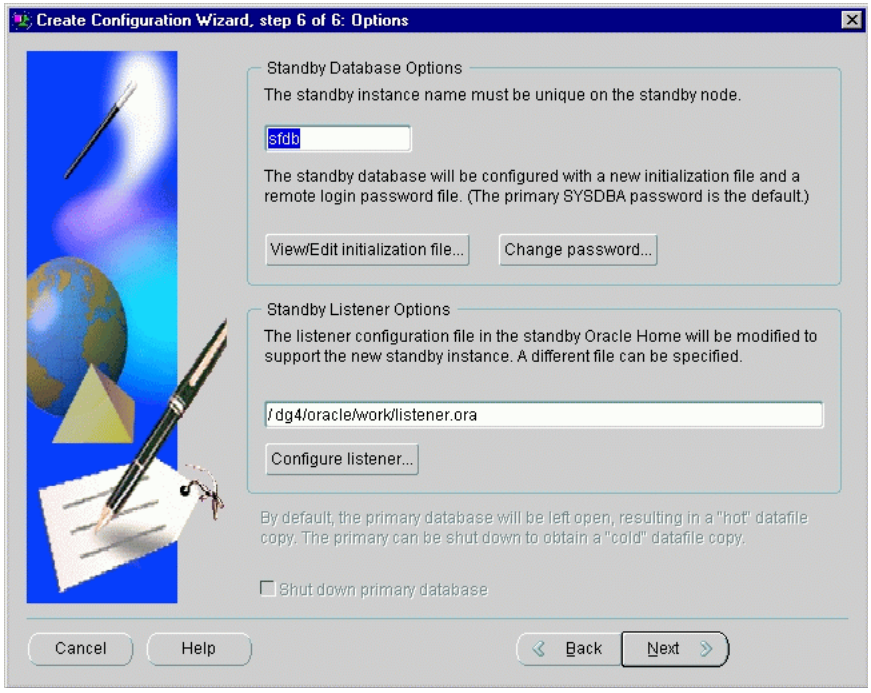
Step 7 Verify the information you supplied to the wizard and make changes, if necessary.

This page of the wizard provides several last-minute tuning opportunities. Normally, no input is necessary on this page because all parameters are set automatically. However, you can optionally change the following:

- Standby instance name
- Standby initialization file
- Standby database SYSDBA password
- Standby LISTENER.ORA file location and content

Figure 5–9 shows the Options dialog.

Figure 5–9 Create Configuration Wizard - Options



Although you do not have to provide any input, you can optionally make changes to any of the fields. Table 5–1 describes the default values for each field and includes comments about how the information is used.

Table 5–1 Optional Input to the Create Configuration Wizard

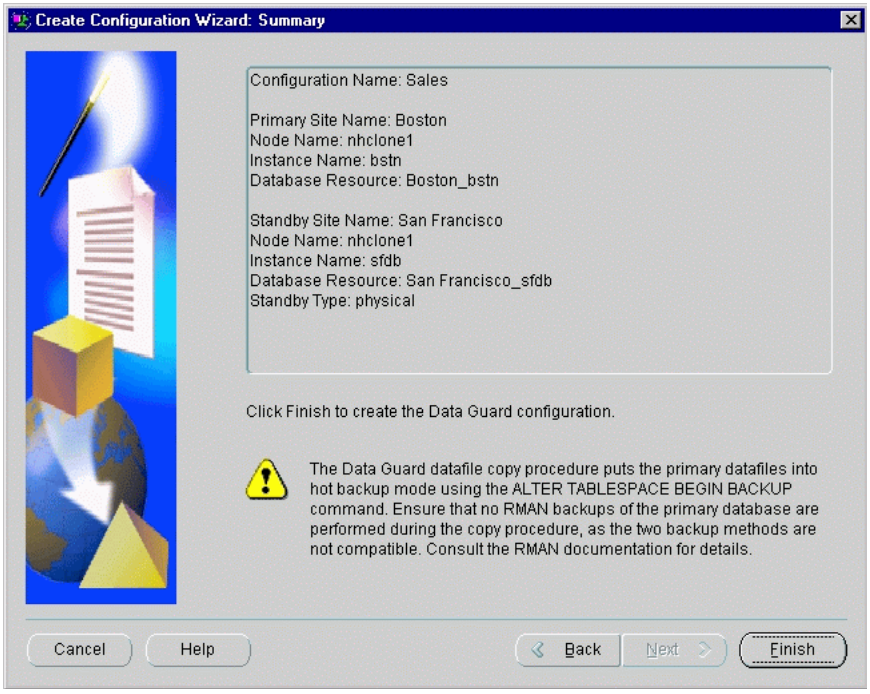
Field	By Default . . .	Comments
Standby instance name	This is the primary database name with a number appended to it. Typically, the number equals the number of sites in the configuration, plus 1.	If you edit the default name shown, ensure the new name is unique on the standby host and it must be 8 characters or less. Note that the name is case sensitive.
Standby initialization parameter file	This file is derived automatically from a combination of the current parameter settings for the primary database and additional standby database settings. You can edit the standby database parameter file to add or modify its contents.	The wizard creates the initialization parameter file for the standby instance in the platform-specific default Oracle home. (For example, on UNIX this would be `$ORACLE_HOME/dbs/init`*`instance_name`*`.ora`). In the Sales example, the generated filename would be `initsfdb.ora`. If a file with this name already exists, you will be prompted to change the instance name.
Standby database SYSDBA password	Although Data Guard Manager does not require a remote login password file for the standby database, this dialog box allows you to create one for the standby database to enable remote connections.	The wizard uses the orapwd utility to create the remote login password file in the default location in the Oracle home where you installed the standby database. For example, on a UNIX system the name of the file is `$ORACLE_HOME/dbs/orapwsfdb`.
Standby LISTENER.ORA file	A `LISTENER.ORA` file must already exist in the default location of the standby Oracle home (for example, `$ORACLE_HOME/network/admin/` on UNIX). Otherwise, the standby creation process will fail.	Whether or not you edit the file, the wizard: ▪ Installs the modified `LISTENER.ORA` file in the default location in the Oracle home. ▪ Starts the Oracle Net listener (or restarts it, if it is already running) that will listen for the new instance, using the `lsnrctl` utility.

Note: By default, the primary database remains open during the standby creation process, which results in a hot (inconsistent) backup of the datafiles. You can opt to shut down the primary database (with the immediate option) prior to creating the standby database instance. This will result in a cold (consistent) backup of the datafiles.

Next, the wizard displays a summary page on which you can verify the information that you provided to the wizard. If you find an error or decide to rename something, click **Back** to move backward through the screens in the wizard. Otherwise, click **Finish** to begin creating the configuration.

Figure 5–10 shows the summary page.

Figure 5–10 Create Configuration Wizard - Summary Page

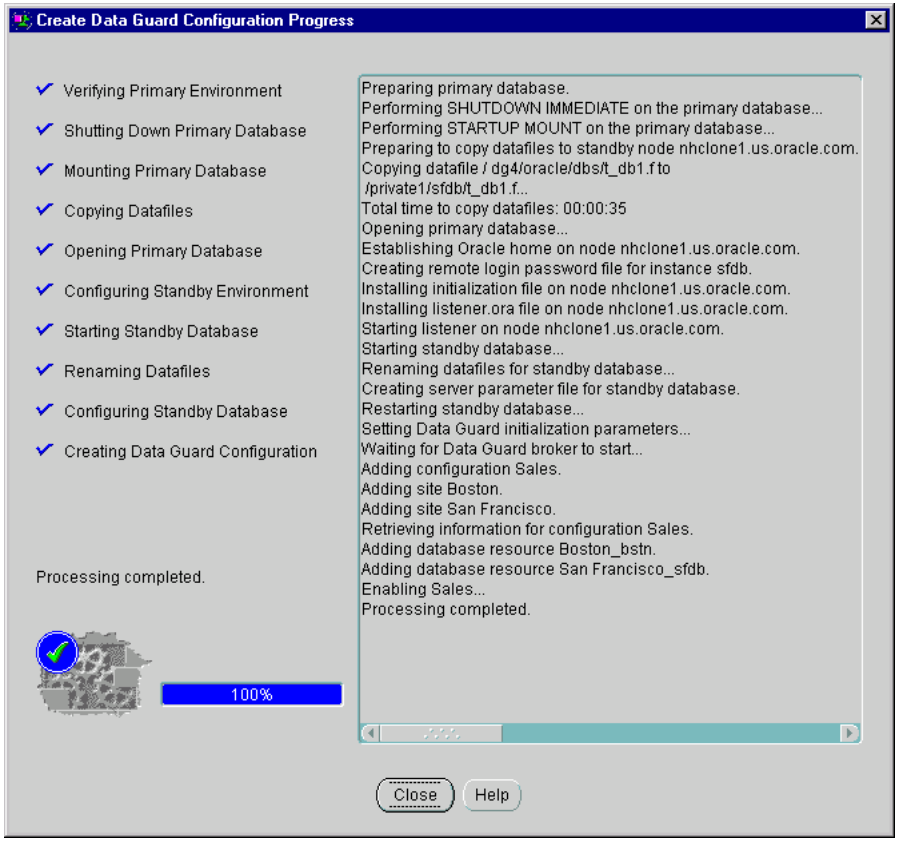


After you finish providing input to the wizard, Data Guard Manager opens a dialog box (shown in Figure 5–11) to display the wizard's progress as it creates the new configuration. The progress information that is displayed varies depending on if you are importing an existing standby database or creating a new standby database.

The progress dialog window displays the progress of the operation. Click **Close** when the create operation is done to close the progress dialog window and return control to the Data Guard Manager main window.

Figure 5–11 shows the progress dialog after the successful creation of the configuration named DGConfig.

Figure 5–11 Progress Dialog Box for Creating the Configuration



When the Create Configuration wizard completes, a To Do list is displayed describing a few tasks you must perform to finish configuring the broker configuration. Follow the instructions in the list to complete the tasks.

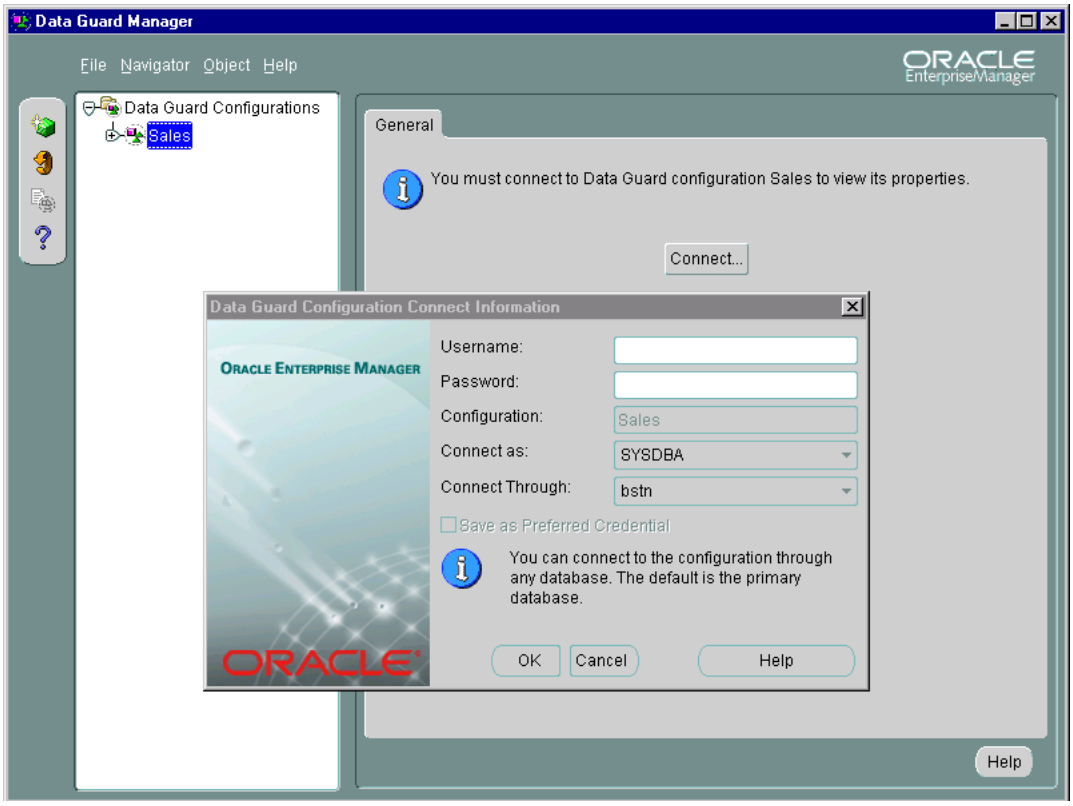
Note: If a problem occurs while creating the new configuration, Data Guard Manager prompts you to fix the problem and allows you to restart the creation process without having to rerun the wizard from the beginning. The restart option skips the step of copying the datafiles if they have already been copied from the primary site to the new standby site.

5.3 Scenario 3: Connecting to a Configuration

You must connect to the new configuration (created in Section 5.2) through the Data Guard Configuration Connect Information dialog box to manage and monitor the resources in it. You can connect through either the primary or a standby database.

To connect, double-click the configuration name in the navigator tree; this launches the Data Guard Connect Information dialog box shown in Figure 5–12.

Figure 5–12 Configuration Connect Information Dialog Box



If you require full management access (including the ability to add and remove sites and database resources, and to perform switchover and failover operations), connect using an Administrator account that has SYSDBA privileges. For read-only access to the configuration for monitoring purposes, you can connect as NORMAL. See the online help for more information about connecting to the configuration.

By default, the configuration, site, and resource objects are automatically enabled and the primary and standby database systems are online when you create a configuration. When the configuration is enabled, it means that you can manage and monitor all of the objects because they are under the control of Data Guard broker.

5.4 Scenario 4: Verifying the Configuration

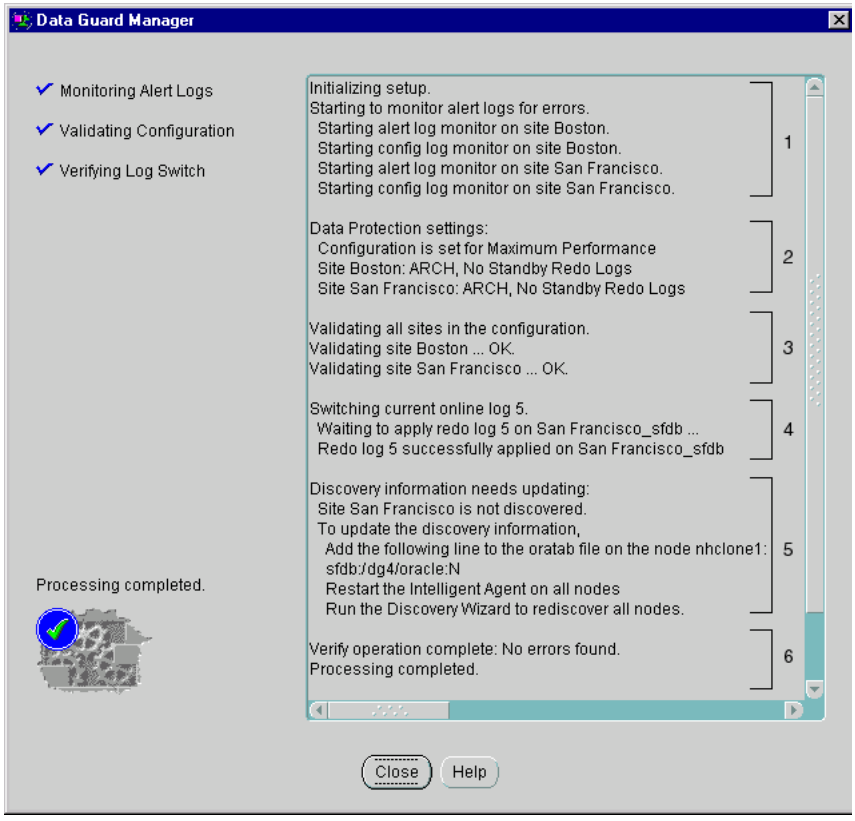
Use the Verify operation when you first create a configuration and at any time you want to perform a series of validation checks on the broker configuration, including a health check of each site and resource in the configuration.

Figure 5–13 shows how the Verify operation:

1. Starts monitoring the alert and configuration logs for any errors that may happen when switching logs. If any errors are found, they are reported at the end of the progress dialog (in step 6).
2. Shows current data protection mode settings, including the current log transport mode settings for each site and whether or not the standby redo logs are configured properly. In the figure, the value "No Standby Redo Logs" can indicate that no standby redo logs exist, there is an insufficient number of standby redo logs available, or the size of the standby redo logs is insufficient.
3. Validates each site for the current status.
4. Performs a log switch on the primary database and then verifies that the log was applied on each standby database.
5. Notifies you to run the Discovery wizard to rediscover nodes and update site information for the configuration
6. Shows the results of the Verify operation, including errors, if any. The Verify operation completes successfully if there are no errors and a redo log was successfully applied to at least one standby site.

Note: You can click **Cancel** at any time to stop the Verify operation.

Figure 5–13 Verify Progress Dialog



The Verify operation shown in Figure 5–13 was successful because the archived redo logs were applied on all standby databases. The progress dialog displays a blue check mark in the status area (left of the dialog) if the Verify operation is successful.

5.5 Scenario 5: Adding Sites to a Broker Configuration

You can use the Add Site wizard to add up to 8 additional standby sites, one at a time, to an existing broker configuration. You can choose to create or add existing (physical or logical) standby databases. Many of the tasks you perform with the Add Site wizard are similar to the steps you performed with the Create Configuration wizard in Section 5.2

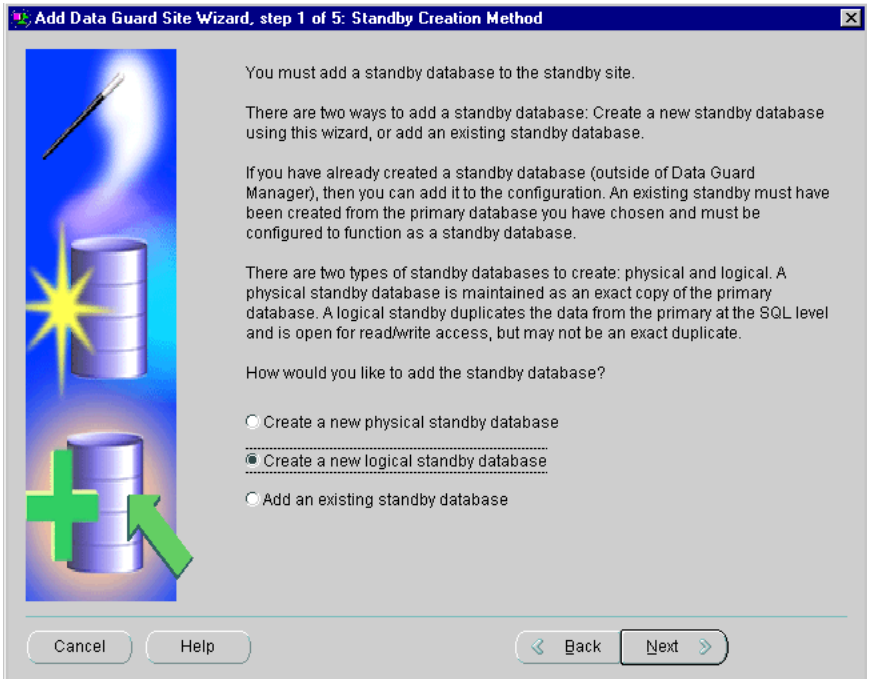
To start the Add Site wizard, right-click the **configuration** in the navigator tree and select **Add Site**. The Add Site wizard guides you through the following steps:

1. Ensure the Data Guard environment is set up properly.
2. Choose to create a new standby database or add an existing standby database. (If you choose to create a new standby database, the wizard also takes you through additional steps to select the Oracle home for the database and to copy datafiles to the standby site.)
3. Optionally, tune parameters such as the standby instance name, standby initialization file, LISTENER.ORA file location and content, SYSDBA password for the standby database, and more.
4. Verify the information you supplied to the wizard and make changes, if necessary.

   In addition, if there is no current connection to the primary database and you do not have Preferred Credentials set for the primary database in the current Enterprise Manager session, Data Guard Manager might prompt you to connect to the primary database.

The following figures highlight some of the pages you will see when you use the Add Site wizard. Figure 5–14 shows how you create a new logical standby database.

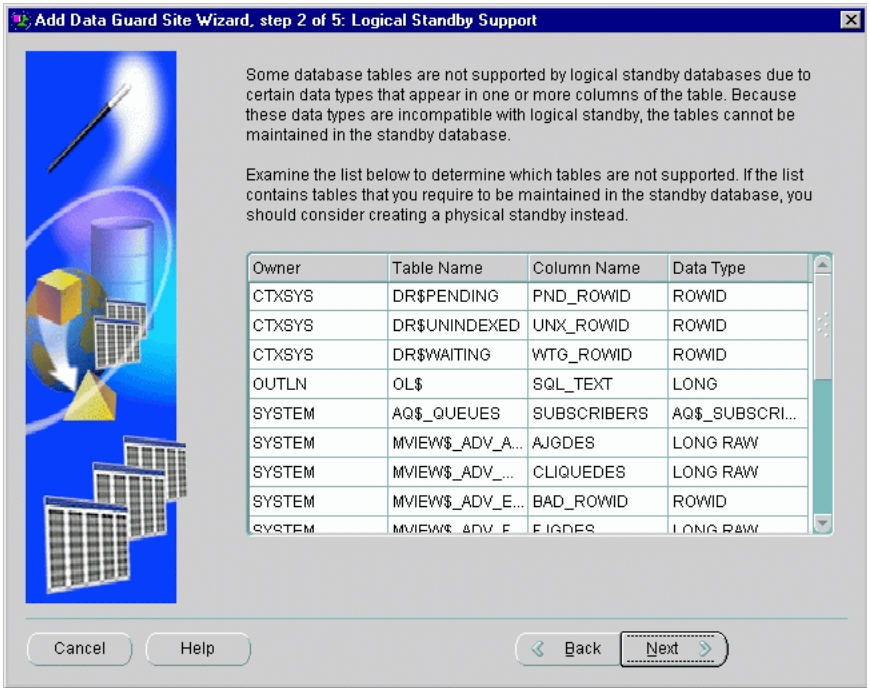
Figure 5–14 Adding Standby Sites to an Existing Configuration



When you create a logical standby database, the wizard lists datatypes and tables in the primary database that the logical standby database cannot support. Although log apply services will automatically exclude unsupported datatypes or tables when applying the archived redo logs to the logical standby database, you should examine the list to determine if any critical tables exist on the primary database that must be maintained on the logical standby database. If so, you should consider creating a physical standby database instead of a logical standby database. Otherwise, you can continue creating the logical standby database.

Figure 5–15 shows an example of many unsupported objects on the Logical Standby Support page.

Figure 5–15 Logical Standby Support

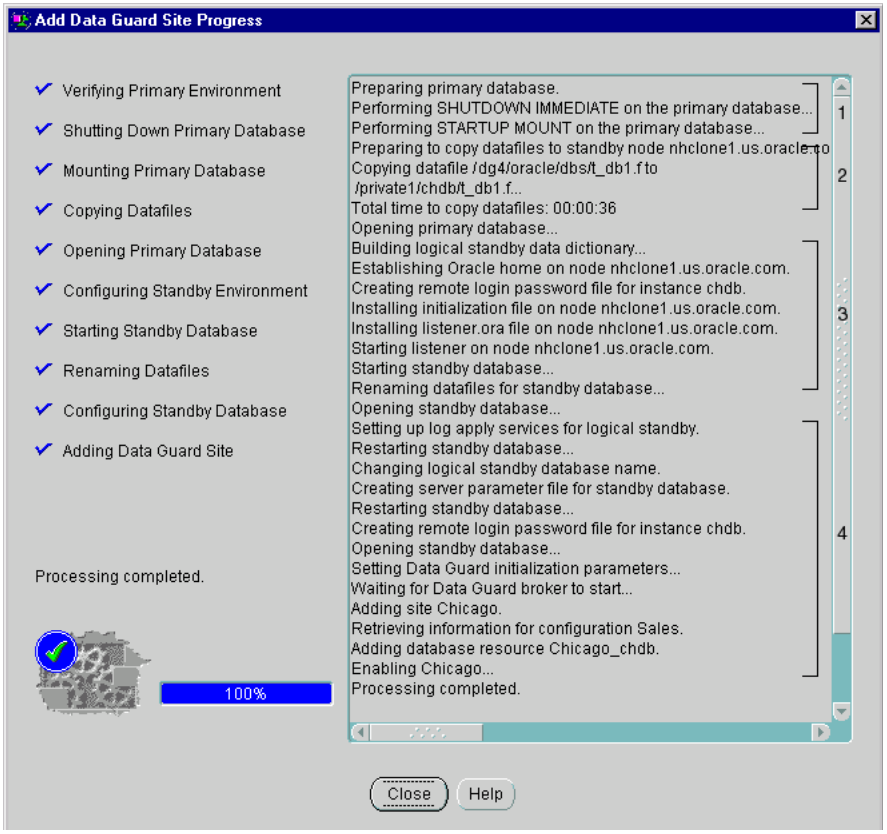


As with the Create Configuration wizard, you are prompted to select an Oracle home on the standby site, and specify a datafile copy location or locations. After you verify your input to the Add Site wizard on the Summary page, the wizard automatically creates the logical standby database, and adds it to the broker configuration.

The following list describes the progress dialog shown in Figure 5–16:

1. Shutting down and then starting and mounting the primary database, which is performed only when necessary or when requested by the user.
2. Copying the primary database datafiles and the standby control file to file locations on the standby site.
3. Setting up the new standby instance, which includes installing files, starting the listener, starting the standby database instance, and renaming datafiles on the standby site.
4. Building the broker configuration, which includes starting the broker on the standby site, and adding and enabling the new logical standby database.

Figure 5–16 Progress Dialog When Adding a Logical Standby Site



5.6 Scenario 6: Performing Routine Maintenance

Data Guard Manager can help simplify some of the routine maintenance tasks you must perform in the configuration. The following sections provide two examples: one shows how to take a site offline to replace a faulty disk drive.

5.6.1 Changing the State of a Database Resource

This section describes how to take the standby database resource offline for the purpose of replacing a faulty disk drive.

To change the state of the standby database to be offline, follow these steps:

1. In the navigator tree, select the **standby database resource**.
2. In the right-hand property sheet, click **Set State**.
3. Click **Offline**.
4. Click **OK**.

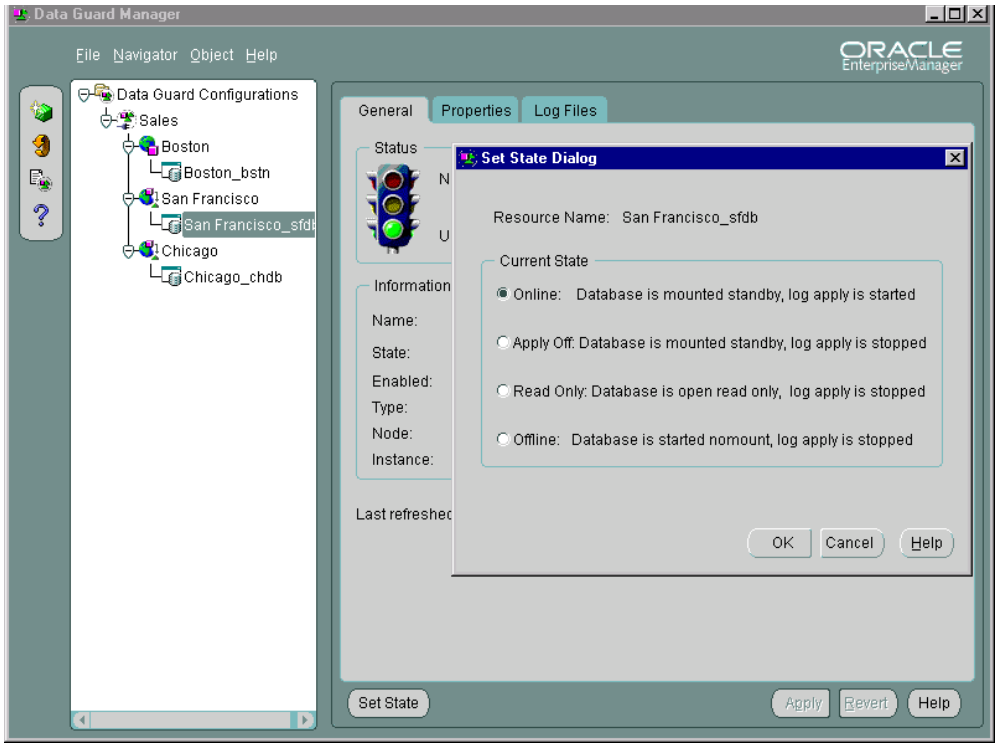
When changing the state of any database to offline, you also need to click **Yes** in the pop-up dialog box that displays to confirm that you want to change its state.

When you change the state of the standby database to offline, the standby database instance will be put into a started, nomount state and log apply services will be stopped. This temporarily pauses the transmission of redo logs to this site and also the application of the archived redo logs to the standby database while you replace the faulty disk drive. After completing your maintenance tasks, you can follow the same sequence of steps to bring the database online again.

Note: Taking any object offline should be done only when absolutely necessary, because it will perform a `shutdown immediate` and `startup nomount` on the databases.

Figure 5–17 shows the Set State dialog on which you will change the state of the standby database to offline.

Figure 5–17 Verifying a State Change to a Physical Standby Database



5.6.2 Changing the Database Protection Mode and LogXptMode Database Property

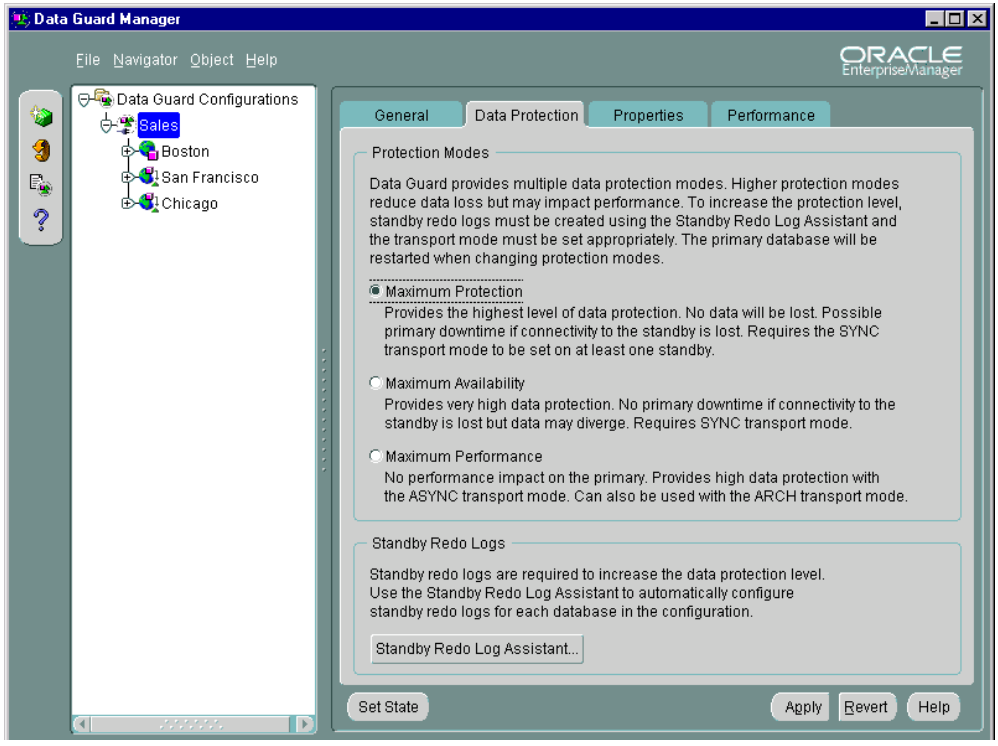
You can change the protection mode properties with Data Guard Manager at any time to modify and tune your current configuration.

When the configuration was first created it was placed in the maximum performance mode by default. This section describes the 4-step process for upgrading to the maximum protection mode. The maximum protection mode offers the highest level of data protection for the primary database because all data that has been committed on the primary database is guaranteed to be recoverable on properly configured physical standby sites in the event of a failure.

To set the maximum protection data protection mode:

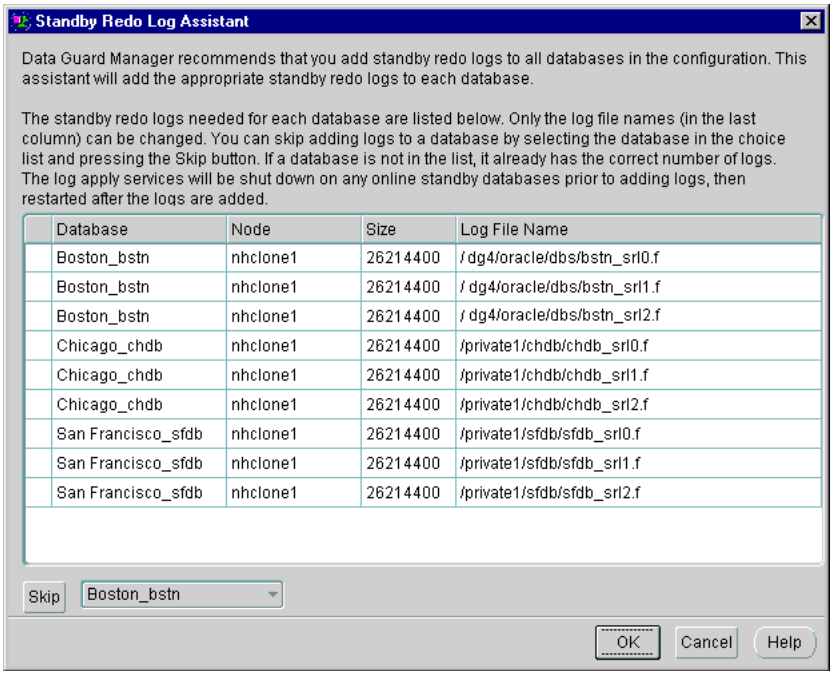
1. Select the **configuration** in the navigator tree and click the **Data Protection** tab.

Figure 5–18 Data Protection Mode Dialog



2. Click **Standby Redo Log Assistant** to configure standby redo logs. Standby redo logs are required for physical standby databases running in maximum protection or maximum availability mode.

Figure 5–19 Standby Redo Log Assistant



The Standby Redo Log Assistant automatically determines the correct number and size of standby redo logs needed for all databases in the configuration, and adds those logs using the directory locations you specify. You can optionally click Skip to avoid adding standby redo logs to one or more specific databases. See the Data Guard Manager help system for more information.

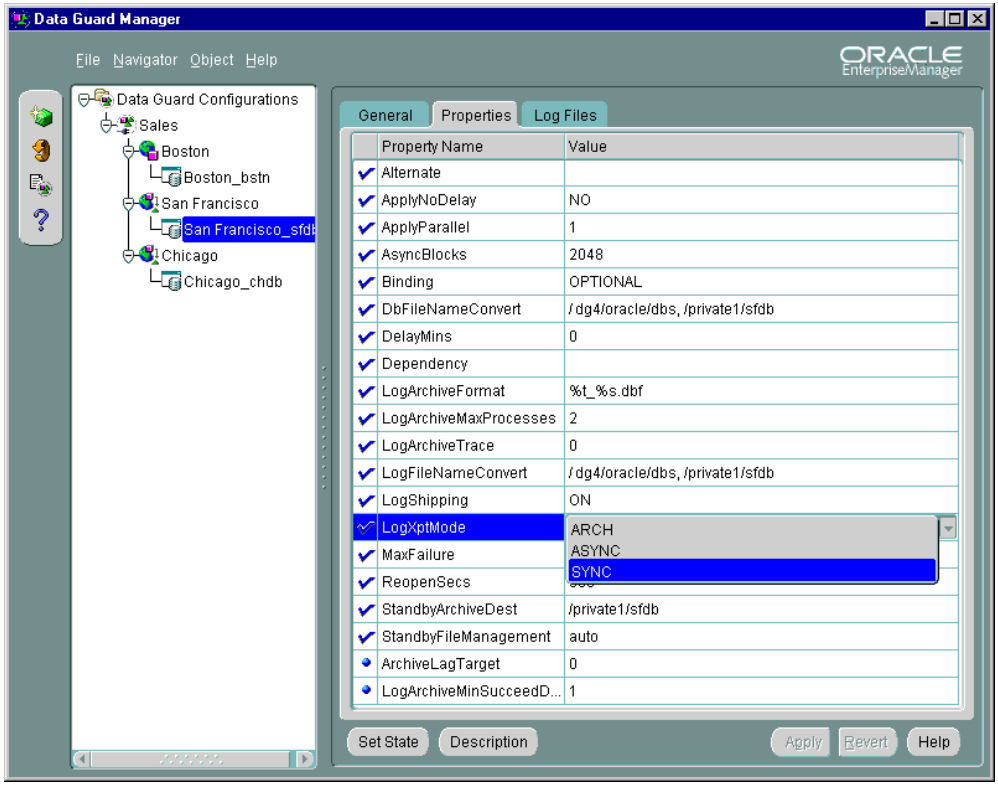
3. Set the `LogXptMode` property value appropriately for the data protection mode you chose in step 1. The maximum protection mode requires that you configure the value of the `LogXptMode` database property to SYNC on at least one physical standby site. To set the `LogXptMode`:

   a. In the navigator tree, select the **physical standby database resource**. (Logical standby databases do not support the maximum protection mode.)

   b. Click the **Properties** tab in the pane on the right side.

   c. Click the **LogXptMode** property and select **SYNC** from the choice box in the Value column, as shown in Figure 5–20.

Figure 5–20 Setting the LogXptMode Database Property



   d. Click **Apply**.

You can change database properties at any time in Data Guard Manager. Plus, when you set definitions or values for database properties in the broker configuration, the broker records the change in the configuration file and also propagates the changes to the related initialization parameters in the SPFILE files throughout the configuration.

4. Set the data protection mode to **maximum protection**:
   a. Select the **configuration** in the navigator tree.
   b. Click the **Data Protection** tab (see Figure 5–18).
   c. On the Data Protection page, select **Maximum Protection**. The primary database will be shut down and restarted.

      See Also: Section 4.3.2 for complete information about configurable database resource properties

5.7 Scenario 7: Performing a Switchover Operation

There may be occasions when you might want to perform a switchover operation between the primary database and standby databases. This scenario steps you through the process of using the Switchover wizard to switch roles between the primary site and a standby site.

To start the Switchover wizard, use either of the following methods:

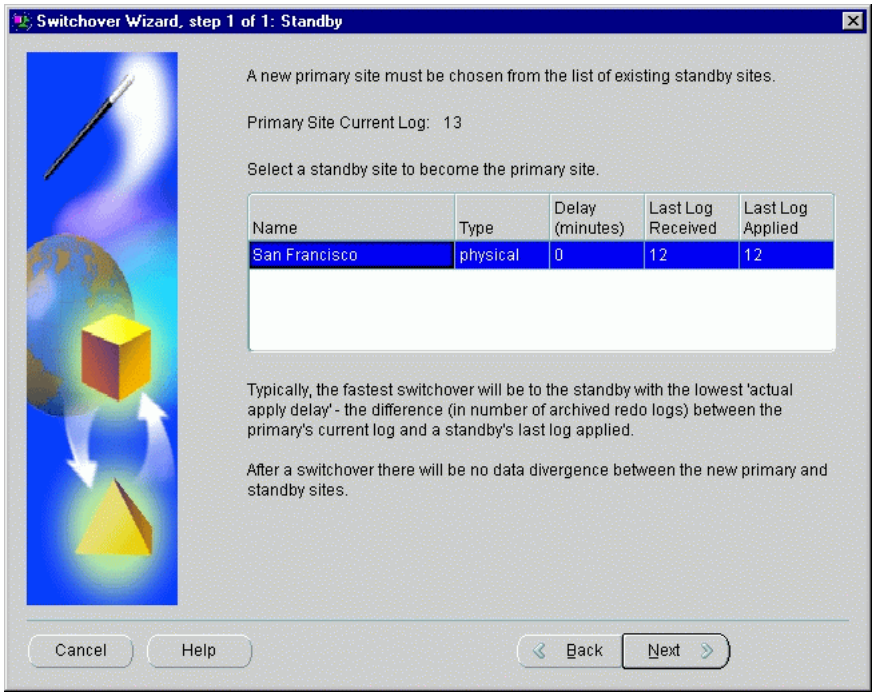
- In the tree view, right-click the **configuration** and select **Switchover**.
- On the Object menu, select **Switchover**.

The Switchover wizard displays a welcome screen and performs the following steps:

1. Ensures that the primary site and primary database are not currently in an error status condition, and verifies that the primary database resource is enabled and online.
2. Checks for, and notifies you of, any active user sessions connected to the primary database instance. The wizard closes these sessions in a manner similar to using the `SHUTDOWN IMMEDIATE` command if you do not shut them down yourself.

3. Lists existing standby sites that are viable (enabled and online) candidates for the switchover operation, and prompts you to choose a new primary site from the list. Figure 5–21 shows this dialog box.

Figure 5–21 Choose a New Primary Site for the Switchover Operation



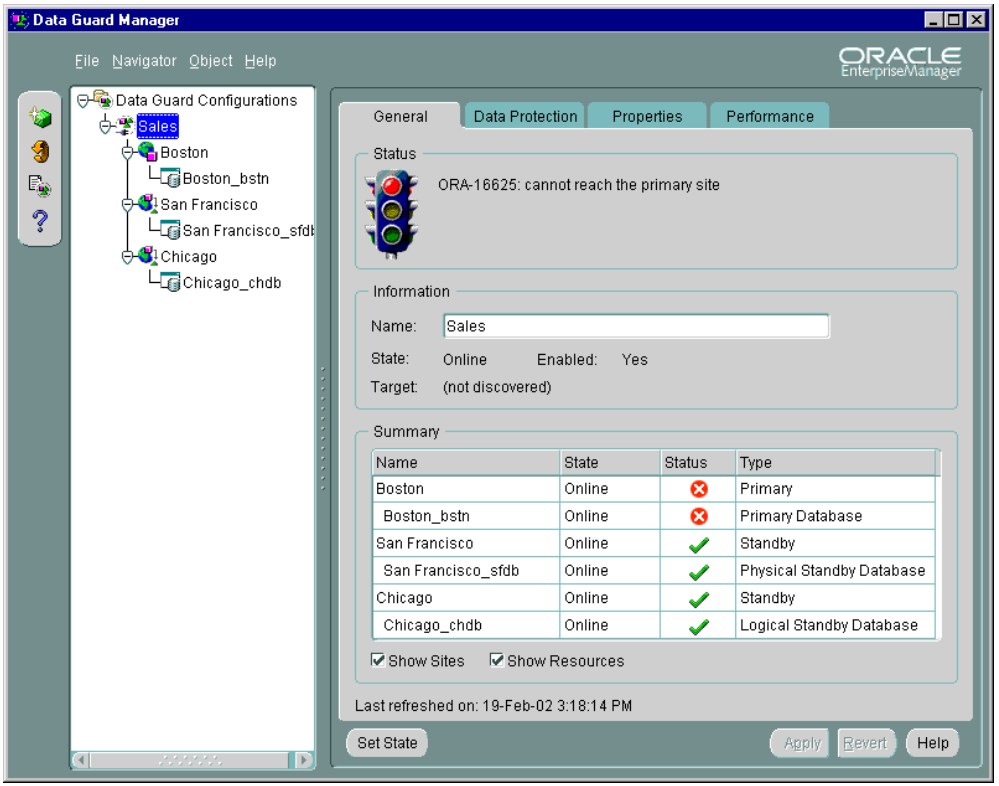
4. Notifies you of any active user sessions running against the chosen standby database instance. See the Check Open Sessions help topic for more information.
5. Verifies the information you supply to the wizard and prompts you to make changes, if necessary.
6. Performs the switchover operation by first changing the primary site to the standby role, and then the standby site to the primary role, displaying a progress dialog as the switchover operation progresses.
7. Restarts any physical standby instances.

5.8 Scenario 8: Performing a Failover Operation

This scenario steps you through the process of using the Failover wizard to transition one of the physical standby sites, San Francisco, into the primary role. You should perform a failover operation only in the event of a software or system failure that results in the loss of the primary database. The primary database is discarded and the standby database assumes the primary database role.

In Figure 5–22, the configuration General page shows the ORA-16625 status that indicates problems accessing the primary database.

Figure 5–22 Failure Condition Indicates a Failover Operation May Be Necessary



If you determine that a failure has occurred on the primary database and there is no possibility of recovering the primary database in a timely manner, you can start the Failover wizard by selecting **Failover** on the Object menu. Oracle Corporation

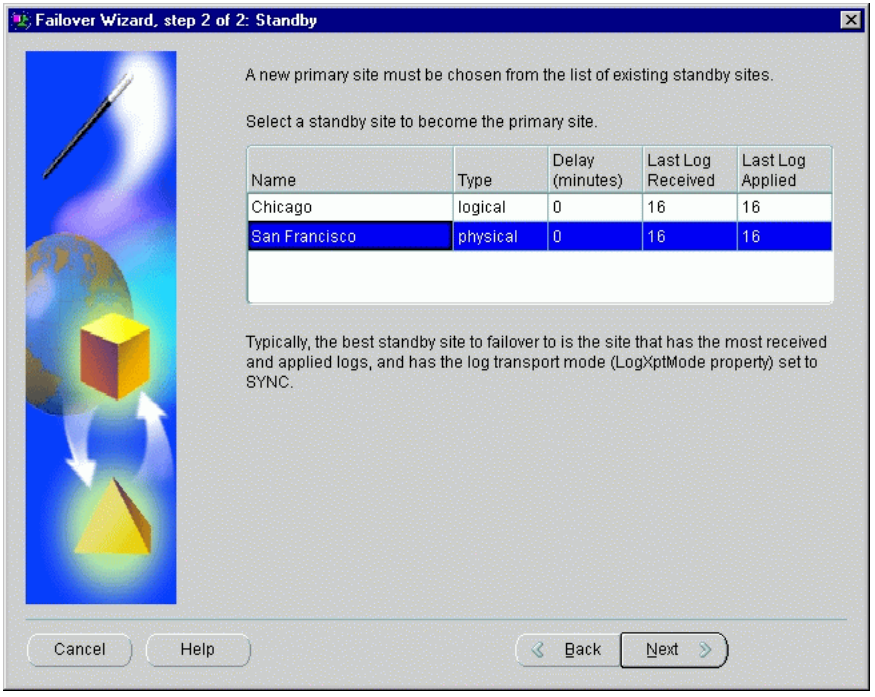
recommends that you always choose a physical standby database (over a logical standby database) as the target of a failover operation.

The Failover wizard displays a welcome screen and performs the following steps:

1. Prompts you to choose the type of failover: graceful or forced:
   - Graceful failover automatically recovers some or all of the original primary database application data and attempts to bring along any physical bystander standby databases.
   - Perform a forced failover to the standby database only in an emergency. Forced failover may result in lost application data even when standby redo logs are configured on a physical standby database.
2. Lists existing standby sites that contain an enabled standby database resource; standby sites that are not viable candidates for the transition to the primary role are not displayed on this page.
3. Notifies you of any active user sessions running against a standby database instance. See the Check Open Sessions help topic for more information.
4. Fails over to the San Francisco physical standby database.

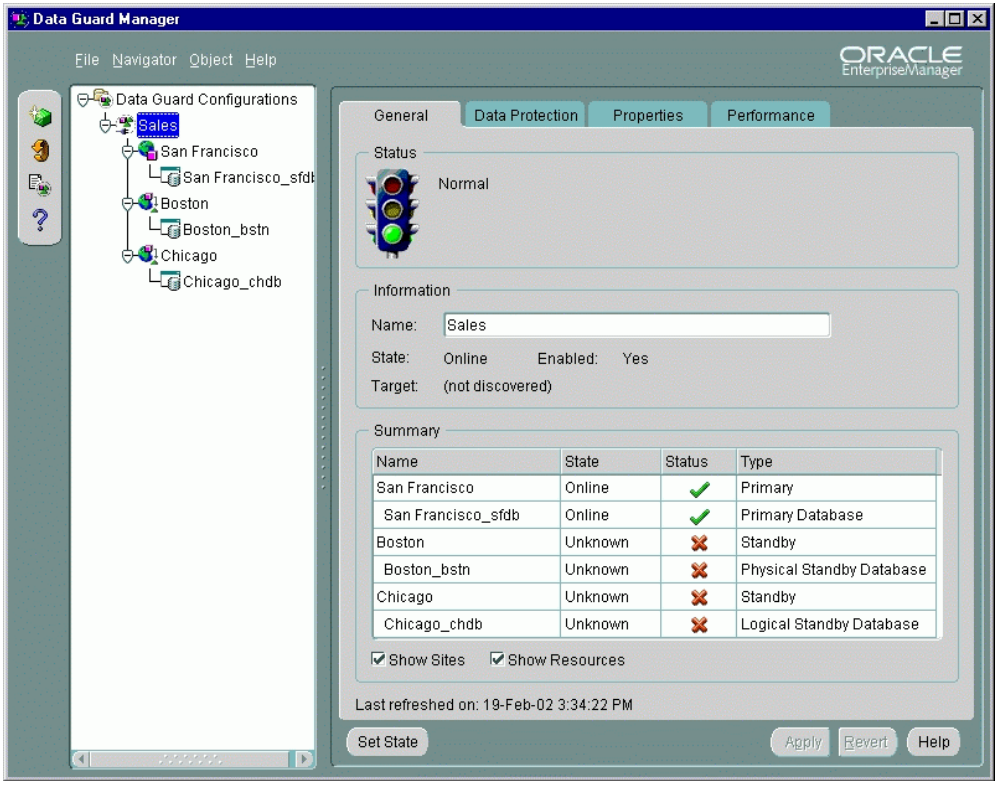
Figure 5–23 lists existing standby sites and prompts you to choose the one you would like to have serve as the new primary site.

Figure 5–23 Choosing a Target Standby Database for the Failover Operation



During the failover operation, the wizard opens a window to display the progress of the operation as it transitions the selected standby site into the primary role and restarts all online physical standby database instances involved in the failover operation. When completed, the configuration General page reflects the updated configuration, as shown in Figure 5–24.

Figure 5–24 General Page After a Failover Operation Completes



In the figure, a red X is displayed in the Status column to indicate that the original primary database (Boston) and the logical standby database (Chicago) are both permanently disabled and can no longer be managed through Data Guard Manager.

A graceful failover operation attempts to bring along any physical bystanders. However, when the graceful failover operation involves a logical standby database, you must re-create the original primary database and any logical bystanders. Also, you must stop and restart the Intelligent Agent and use the Discovery wizard from the Enterprise Manager Console to rediscover all nodes in the configuration.

> **See Also:** Chapter 3 for more information about failover operations

5.9 Scenario 9: Monitoring a Data Guard Configuration

Data Guard Manager provides several ways to monitor the status of a configuration as well as the redo log activity of the primary and standby databases. At the most basic level, the General tab for the configuration not only displays information about the configuration, but it also includes summary information about its sites and database resources.

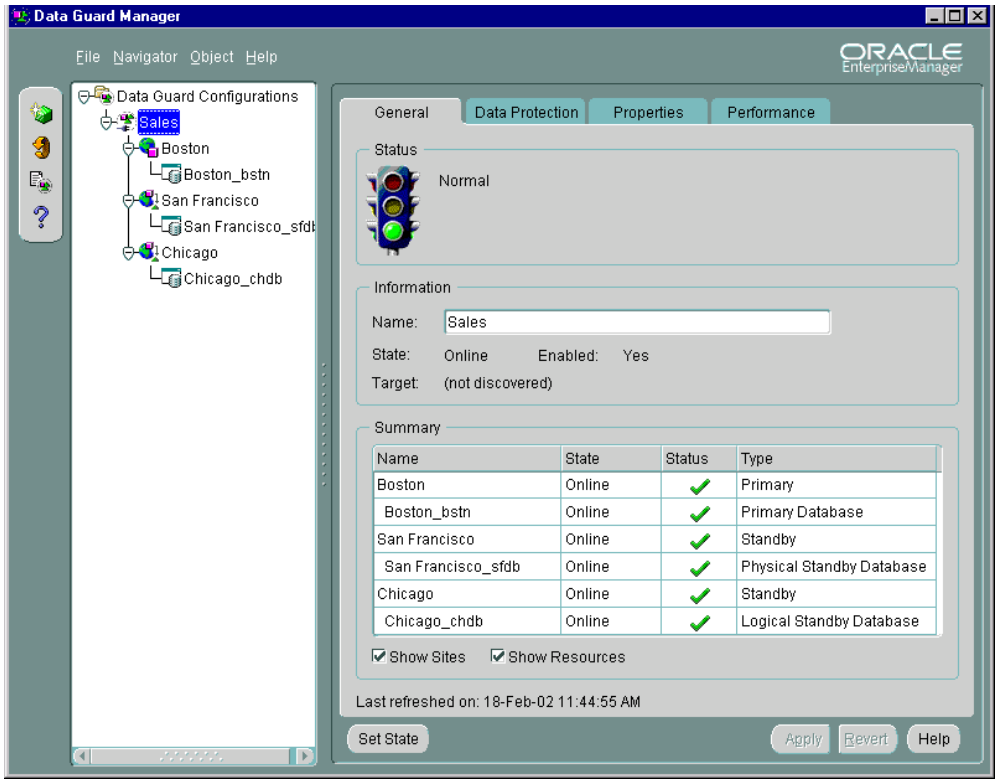
For example, the summary information on the General property page shows the states and status for all of the sites and databases in the configuration. If you want to find out more information about why a standby database resource is offline, select it in the navigator tree and view the database resource's property pages. Any Data Guard specific database properties that are incorrect, inconsistent or known to be in conflict with other parameters will be flagged with a warning in the Properties page for the database resource.

- To check the configuration status, select the configuration in the navigator view and look at the status information on the General page. The traffic light is green if the configuration is functioning normally, yellow if there is a warning, and red for an error condition. To see the status of individual site and database resource objects, hover the mouse over the Status field in the Summary area.
- To check a database resource object's status, in the navigator tree expand the configuration and the site, then select database resource that you want to check. Click the Properties tab to see a list of the database properties (reference the online help to get a brief description of each property). Hover the mouse over the icons in the first column for status information.

  For example, hovering over a yellow warning icon displays the message "A yellow warning indicates an inconsistent property has been detected. The value for this property is inconsistent between Data Guard and the database, Data Guard and the SPFILE, or Data Guard and both the database and SPFILE."

Figure 5–25 shows the General property page for the configuration.

Figure 5–25 Displaying General Information About a Configuration



5.9.1 Verifying a Broker Configuration

Another way to quickly check the overall health of a broker configuration is to run the Verify command. The Verify command performs a series of validation checks on the broker configuration, including a health check of each site and database resource object in the configuration. The checks include:

1. Monitoring the alert logs and Data Guard logs, reporting any errors.
2. Evaluating the configuration protection modes and identifying potential issues with switchover operations. For example, it checks that each site is enabled and online, and switches logs to make sure that the log was successfully archived and applied to the standby databases.

To verify the configuration, right-click the configuration in the navigator tree and select **Verify** from the drop-down list. The Verify command displays a progress dialog (see Section 5.4, "Scenario 4: Verifying the Configuration" for an example). When the verify operation completes successfully, the broker configuration is healthy, guarding the data and ready for a switchover or failover operation.

5.9.2 Viewing Alert Log and Data Guard Log Information

The View Log dialog allows you to display the database alert logs, the Data Guard configuration logs, or both logs for the primary and standby sites. Use it for rapid error searches and monitoring because you can obtain results quickly, if common Oracle errors or specific patterns.

To use the View Log dialog:

1. Click the **ViewLog icon** that is located above the Help icon on the far left-hand side of the Data Guard main window, or select **View Log** from the Object menu.
2. In the View Options dialog, select one or more **log files** that you want to view and choose your viewing preferences. For example, you can monitor the logs continuously or choose a time period to view them. Also, you can highlight errors to make them easier to find.
3. Use the Window menu option to arrange the resulting panes for the best view.

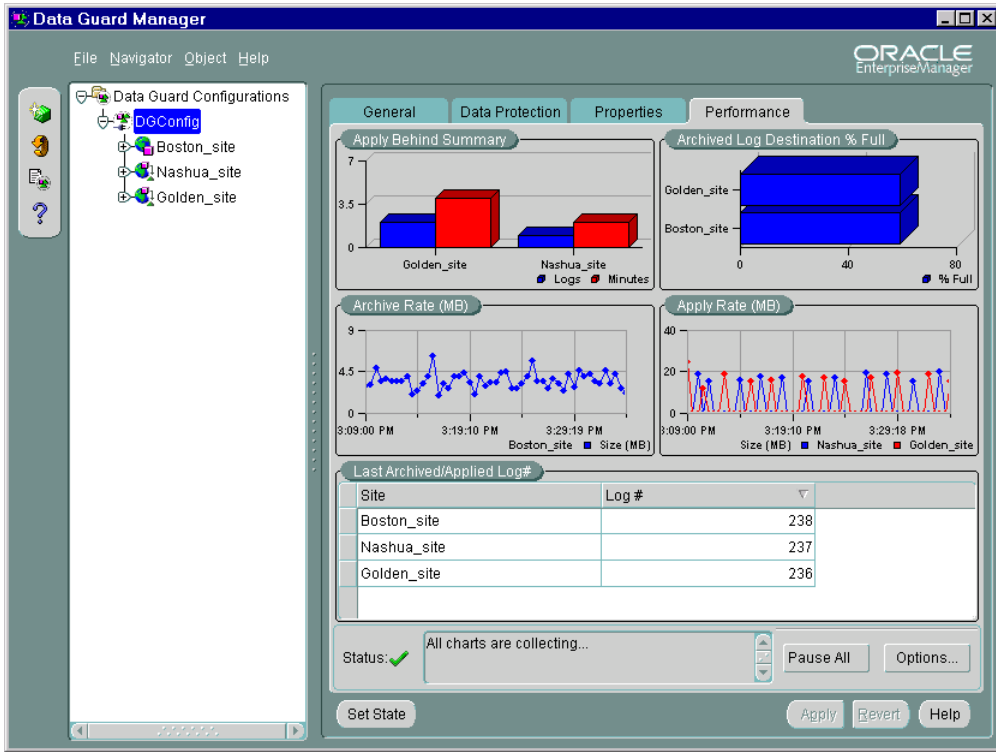
   In addition, you can use the F3, F7 and F8 keys for rapid searching in the logs. Choose **Matching common Oracle errors** to view a subset of errors discovered in the logs. Choose **Match Regular Expression** to perform a search on specific words in the logs. Click **OK**.

5.9.3 Monitoring Configuration Performance

For more in-depth performance and monitoring, you can display detailed performance statistics for a broker configuration using performance charts that provide a graphical summary of all redo log activity in the configuration. The charts are refreshed based on a collection interval (the rate at which data is sampled from the primary database) that you can specify. The default collection interval is 60 seconds, which can be changed. See the online Help for detailed information about performance sampling rates.

For example, Figure 5–26 shows performance information for all of the objects in the configuration.

Figure 5–26 Displaying the Performance Chart Page



The Performance page begins charting information as soon as the page is displayed. The charts run continuously while the configuration is selected in the navigator tree, even if you go to another page for the configuration. For example, if you click the General, Data Protection, or Properties tab, the charts continue collecting data and be up-to-date when you return to the Performance tab. The Performance page stops collecting data when you click Pause All at the bottom of the page, disconnect from the configuration, or select another object in the tree view. Also, data will not be collected for any offline or disabled sites. For example, if the primary site is offline, no charts will be displayed for it.

Note: To view the Performance page while also using other features of Data Guard Manager, right-click the configuration in the navigator tree and choose **Edit**. This displays the Performance information in a new window to provide you the flexibility to perform other functions in the Data Guard Manage main window. This is effective unless sessions used by the Performance page need to be terminated for some reason, such as a switchover operation.

From the Performance page, click **Options** to access the Performance Chart Options dialog that allows you to customize display settings on the Performance page or invoke a Test Application that modifies a test table and generates redo to test the configuration setup.

The Test Application is a good way to make sure that the configuration is set up and functioning properly before using live data and to test relative performance.

Running the Test Application

You use the Test Application dialog (shown in Figure 5–27) to help you evaluate the performance of your broker configuration by adding and deleting rows in a test schema on your primary database. To set up a Test Application, perform the following steps:

1. On the Performance Page, click **Options**.
2. Click **Start Test** and start a test on the primary database (the default). You can also select logical standby databases and physical standby databases that are in read-only mode.
3. Click **Setup** at the bottom of the page to create the test tables.
4. Choose **Single Update Mode** or **Continuous Update Mode**:

Single Update Mode Single Update Mode inserts one row of the value you specify into the Test Application. To use Single Update Mode:

On the primary database:

1. Enter a value (using a VARCHAR datatype) in the text box under Single Update Mode.
2. Click **Apply**.

On the physical standby databases:

3. Set the state of the physical standby database to read-only mode.
4. Click **Options** on the Performance Page and start another Test Application for each physical standby database.
5. View the **Value** field in the Test Application to see the inserted value.

On logical standby databases:

1. Click **Options** on the Performance Page and start another Test Application for each logical standby database.
2. View the **Value** field in the Test Application to see the inserted value.

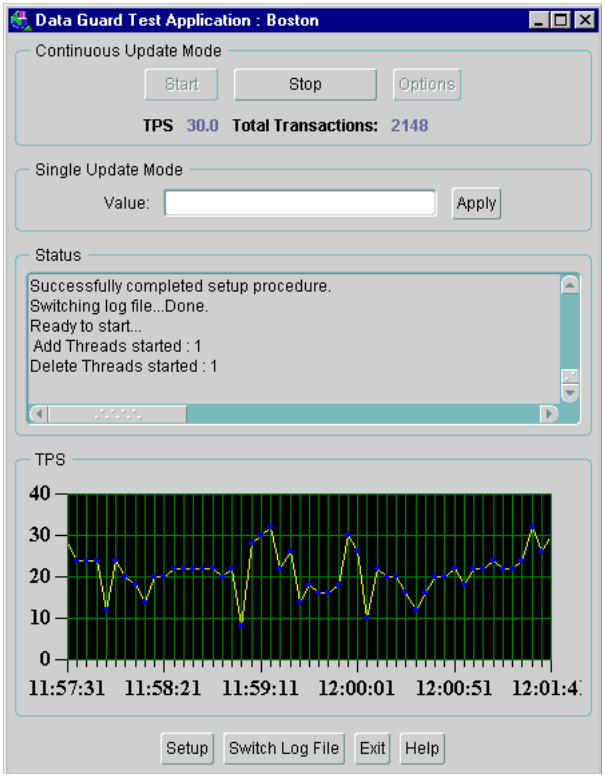
When the value from the primary database is inserted into the standby database, the value will appear in the Test Value text area of the Test Application started on the logical.

Continuous Update Mode Continuous Update Mode inserts a number of insert and delete threads in the Test Application. To set it up, select **Options** in the Continuous Update Mode section of the Test Application page and enter the number of Insert and Delete threads.

More threads will produce more transactions resulting in more log traffic. The Test Application will run until you click **Stop** or until there is a lack of resources. There are no restrictions on how many threads may be started and it is possible to exceed the hardware or database resource limits (which can also be a very useful test).

Figure 5–27 shows the Test Application dialog for setting up single or continuous update mode tests.

Figure 5–27 Testing the Data Guard Configuration



The test application plots the number of transactions per second (TPS) in a graph, providing a profile of the performance impact of the simulated archived redo log traffic. By using the Test Application, you can determine how different settings may affect overall performance. For example, you might want to test the effect of the different protection modes: maximum protection, maximum availability, and maximum performance.

Note: The performance information is for the Test Application only. You may see different results based on different applications and other factors when you run different tests.

5.10 Scenario 10: Using Event Tests

In addition to monitoring the status and log activity using Data Guard Manager, you can register event tests with Oracle Enterprise Manager to monitor the redo log activity on the primary and standby databases or monitor the status of the configuration as a whole.

You can create events using predefined event tests that are installed with Data Guard. Table 5–2 describes the six Data Guard event tests.

Table 5–2 Data Guard Event Tests

Event	Description
Actual Apply Delay	Measures the difference (in number of archived redo logs) between the current log at the primary database and the last log applied on the standby database.
Data Not Applied	Measures the time difference (in minutes) between the last archived redo log received and the last log applied on the standby database.
Logs Not Applied	Measures the difference (in number of archived redo logs) between the last log received and the last log applied on the standby database.
Logs Not Shipped	Measures the difference (in number of archived redo logs) between the current log on the primary database and the last log shipped to the standby database.
Potential Data Loss	Measures the time difference (in minutes) between the current redo log on the primary database and the last log received on the standby database.
Status	Checks the status of the broker configuration. **Note**: If the status is not SUCCESS, then this event test is triggered.

Using the Enterprise Manager Event System, you can register one or more Data Guard event tests against both the primary and standby databases. You can also set up the Paging /Email Services to notify you through your pager or e-mail if any of the event tests are triggered.

In addition to registering the Data Guard event tests, consider registering the Node UpDown event test against each node where the Oracle Intelligent Agent is running. This event test monitors the node and the Intelligent Agent. Because the UpDown event test is triggered if any problems occur with the node or agent, it can be very beneficial in detecting problems that may prevent other event tests, including Data Guard event tests, from running.

See Also: Oracle Enterprise Manager help and documentation for more information about registering event tests and using the Paging/Email Services

5.10.1 Creating and Registering Data Guard Events

The example in this section describes how to create and register Data Guard event tests and set up for notification through e-mail when an event occurs.

Step 1 Ensure Oracle Enterprise Manager is prepared.

To prepare the Enterprise Manager environment for events, it is essential that you have performed the following prerequisite tasks:

- Ensure the Oracle Intelligent Agent is running on all nodes in the configuration.
- Ensure the primary and standby nodes have been discovered (and therefore the primary and standby databases have been discovered).
- Set Preferred Credentials on all databases (requires the SYSDBA role).
- Invoke Data Guard Manager and connect to the broker configuration.

Note: These tasks were discussed in detail in Section 5.1.

Step 2 Set up to receive event notification by pager or e-mail.

If you want to receive event notification by pager or e-mail, invoke the Paging/Email Services to set up the SMTP mail gateway and mail address of the person who will receive the event notification. From the menu bar on the Enterprise Manager Console, invoke the Paging/Email Services by selecting: **Configuration > Configure Paging/Email.**

See Also: The Oracle Enterprise Manager documentation and help for a complete description of the Paging/Email Services

Step 3 Create the event tests.

From the menu bar on the Enterprise Manager Console, select:

Event > Create Event

Complete or modify the fields in the following Create Event property pages:

- General: Specifies a name for the event, target type, and monitored targets. To create one or more Data Guard event tests, enter a user-friendly name for the

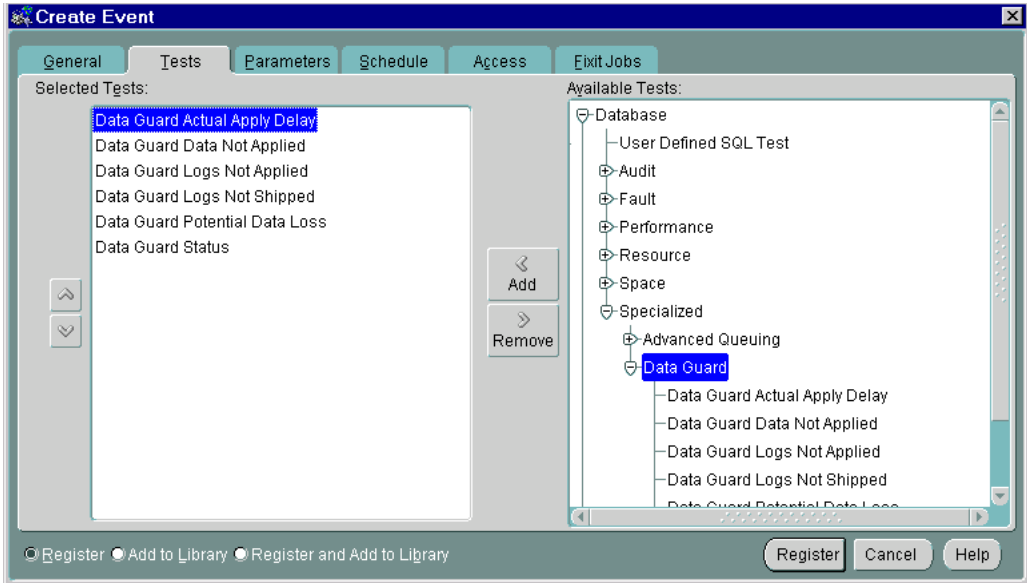
Event Name, select **Database** as the Target Type, and add the **primary and standby databases** as the targets you want to monitor.

- Tests: Specifies the event tests that you want to create. You can select any event listed in the Available Tests navigator tree, including any of the Data Guard event tests that were described in Table 5–2. To see the list of Data Guard event tests, select:

  Database > Specialized > Data Guard

  For each event test that you want to create, select the test from the Available Tests view and click **Add** to move it to the Selected Tests list. In Figure 5–28, all of the Data Guard event tests have been selected.

Figure 5–28 Predefined Data Guard Event Tests



- Parameters: Specifies settings, such as the number of occurrences and threshold values, that you can customize for each event test. Parameters vary according to the event test selected. The available parameters for an event test are displayed when the event test is selected in the Tests tab. Some event tests, such as Data Guard Status, do not have parameters.

- Schedule: Specifies how frequently you want the Oracle Intelligent Agent to run event tests. By default, all of the event tests run every 5 minutes (except for the Up / Down event test, which is checked at an interval set by the system itself).

  Note: You should experiment with the schedule setting because there is a trade-off between frequency of the test and the performance of your system. Running tests at a more frequent interval increases the workload on your system and may produce a noticeable effect on performance.

- Access: Specifies the access permissions that you want to assign for the event. You can allow other DBAs no access, full access, or restricted access so that other DBAs can only view the event or modify the event log. Because the example in this section is set up for e-mail notification, you should ensure that the Notify option is selected for each DBA who requires notification.
- Fixit Jobs: Specifies jobs that respond to specific error conditions. There are no fixit jobs for Data Guard event tests.

When you have completed all of the Create Event property sheets, select **Register & Add to Library** option on the bottom left side and then click **Register & Add** to send the event to the selected destinations. This adds the event to the Library and saves the event definitions.

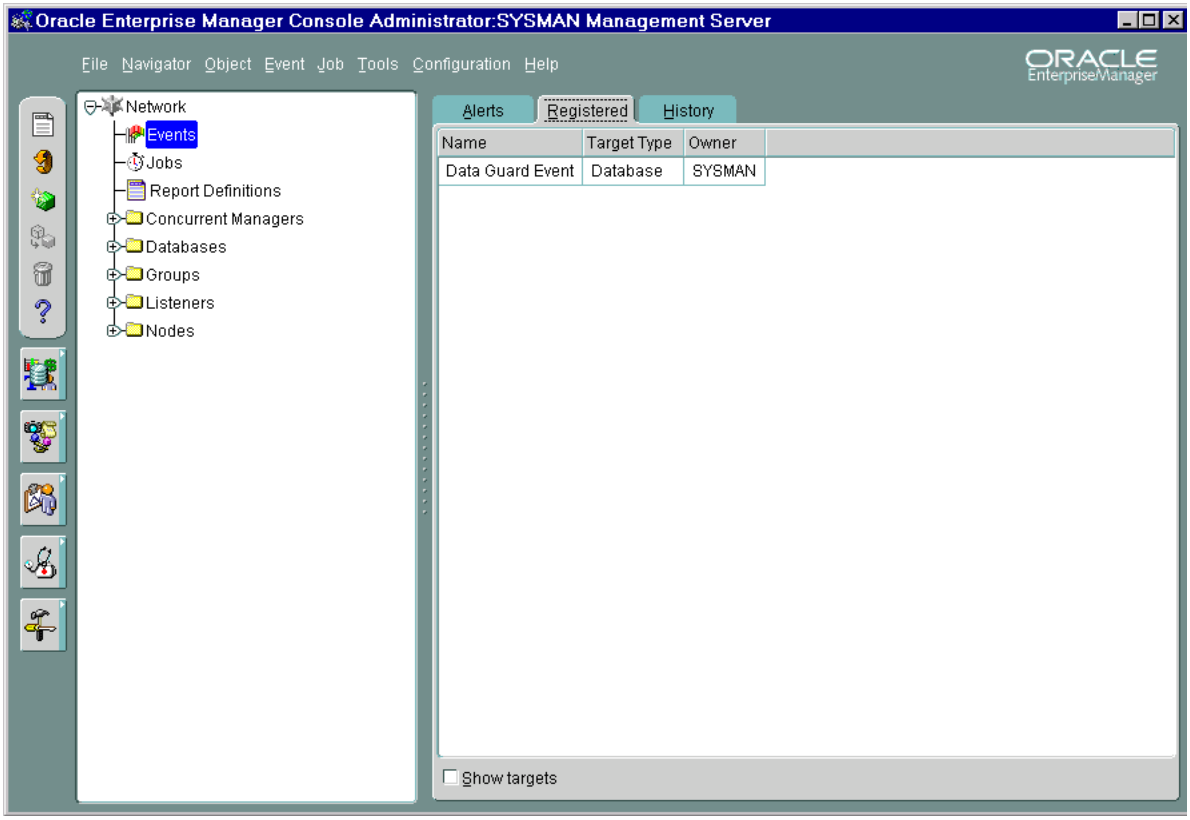
When the event is submitted, the primary and standby database destinations are validated and the Intelligent Agent for each destination processes the event.

Step 4 View registered events.

If the registration is successful, the event displays in the Registered page of the Events pane. For example, Figure 5–29 shows that the event named Data Guard Event was registered successfully.

Note: Remember, the primary and standby nodes must already be discovered, Preferred Credentials must be set, the Intelligent Agent must be running, and you must be connected to the broker configuration for the *registration to be successful*.

Figure 5–29 Viewing Registered Events

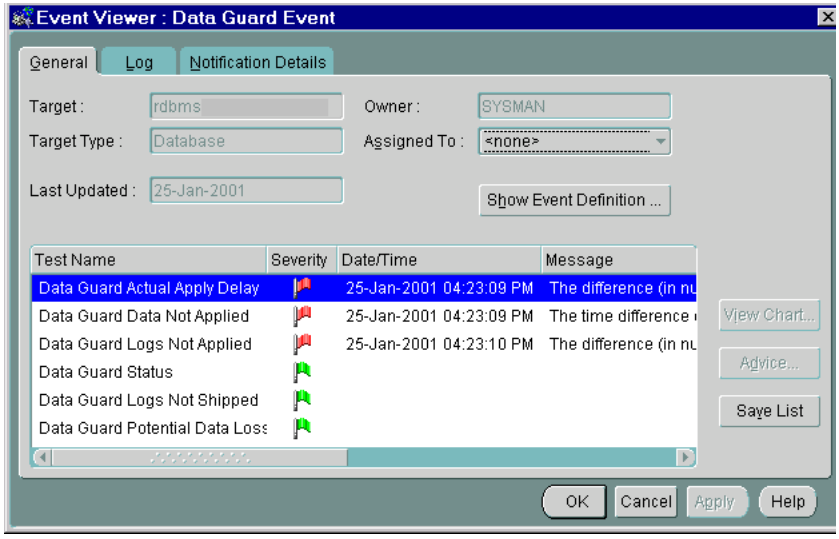


Step 5 View triggered events.

If an event condition is triggered or a threshold value is exceeded, it shows up in the Alerts pane. If you double-click on an event, the Event Viewer displays a property page showing the status of your events.

Figure 5–30 shows some Data Guard events that were triggered after log transport services and log apply services stopped between the primary and standby databases.

Figure 5–30 General Property Page of the Event Viewer



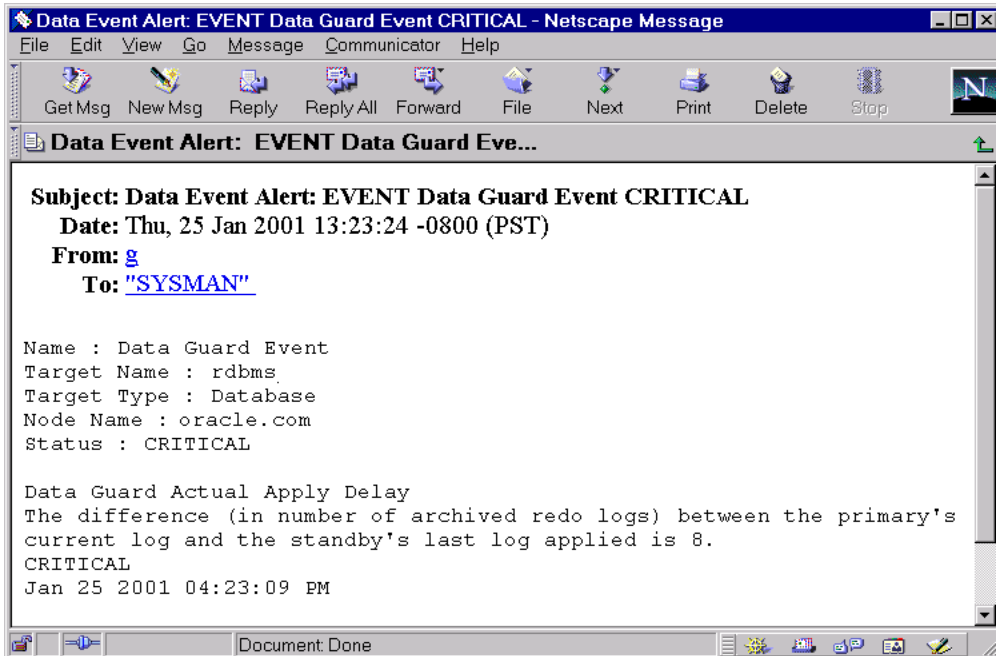
In Figure 5–30, notice how the events return a different flag symbol and message, depending on the severity of the event. The severity levels are determined by the parameters you set for the event tests when you created them. See the Oracle Enterprise Manager online help system for more information about the different symbols.

When running the Data Guard event tests, an error might occur for the following reasons:

- The event test fails to run.
- The event test cannot make requests of the Data Guard broker.

Because the Paging/Email Services was set up, DBAs are also notified by an e-mail message similar to the one shown in Figure 5–31.

Figure 5–31 E-Mail Notification for the Actual Apply Delay Event



After an event condition is fixed, the event is cleared automatically. You can also clear an event by acknowledging it and moving it to the Events History page.

5.11 Scenario 11: Removing a Configuration and Exiting Data Guard Manager

You can remove a configuration so that it is no longer visible from the navigator in the current Data Guard Manager window, or you can permanently delete the broker configuration.

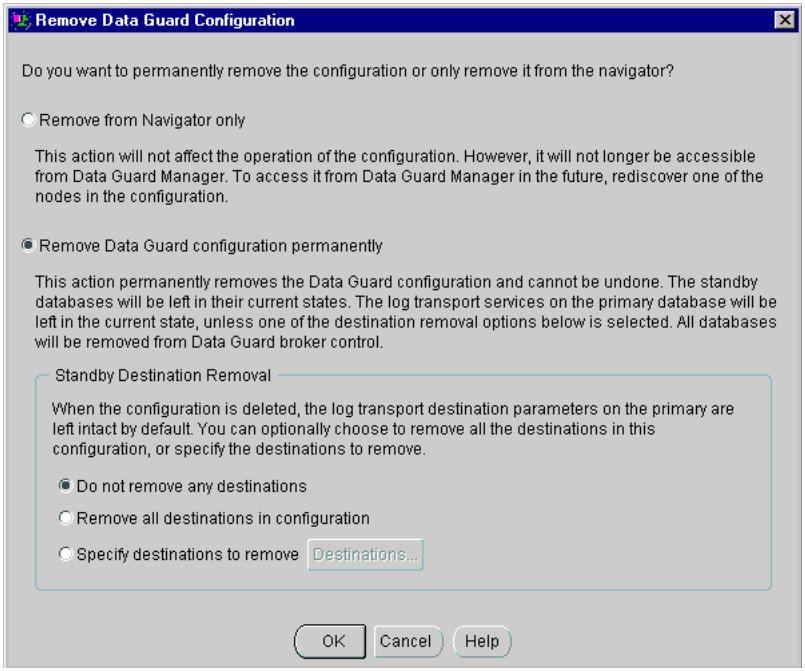
When you remove a configuration from Data Guard Manager, you remove all broker objects in the configuration from management and monitoring through the GUI. By default, it does not affect the underlying operations of the primary and standby databases, log transport services, or log apply services. Operations such as log shipping and log applying could continue to function. However, these services are no longer manageable through Data Guard Manager.

5.11.1 Remove the Data Guard Configuration

To remove the broker configuration, you must be connected to the configuration through the primary database. Perform the following steps:

1. In the navigator tree, select the **configuration**.
2. From the **Object** menu, select **Remove**. The Remove Data Guard Configuration dialog displays, as shown in Figure 5–32.

Figure 5–32 Removing a Data Guard Broker Configuration



3. Select Remove from Navigator only or Remove Data Guard configuration permanently and click OK.

   - **Remove from Navigator only**

     This option removes the configuration from the Data Guard Manager console without actually destroying it. When you choose this option, the actual Data Guard configuration, sites, and resources are still operational and the configuration still exists. You can make the configuration visible in Data Guard Manager once again by using the Enterprise Manager Discovery wizard to rediscover any one of the nodes on which one of the sites is located.

   - **Remove Data Guard configuration permanently**

     When you choose this option, Data Guard Manager removes (deletes) the selected broker configuration permanently. You must be connected to the broker configuration through the primary database to use this option. When you permanently remove a configuration, the remove operation:

* Does not affect the underlying operations of the standby databases or the log apply services. Operations such as log shipping and log applying continue to run; however, these services are no longer manageable through Data Guard Manager.
* Destroys all broker configuration information maintained on each site; the configuration is then unknown to the broker and can no longer be managed from Data Guard Manager.
* By default, does not stop or remove the log transport services. You can optionally choose to have Data Guard Manager automatically remove each of the standby sites in the configuration from the list of standby destinations currently in use by the primary database. In the Standby Destination Removal section, select from the following options: Do not remove any destinations, Remove all destinations in configuration, Specify destinations to remove. (Press the Destinations button to specify exactly which destinations to remove.)

Although the configuration information is not recoverable once you delete a broker configuration permanently, you can easily re-create the configuration with the Create Configuration wizard. See Section 5.12 for more information.

5.11.2 Exit from Data Guard Manager

To exit from Data Guard Manager, choose **File > Exit.**

5.11.3 Stop the Data Guard Monitor

On both the primary and standby sites, stop the Data Guard monitor by setting the DG_BROKER_START=FALSE parameter using the SQL ALTER SYSTEM statement.

```
SQL> ALTER SYSTEM SET DG_BROKER_START=FALSE;
System altered.

SQL> SHOW PARAMETER DG_BROKER_START;
NAME         TYPE      VALUE
-----------------------------------
dg_broker_start    boolean   FALSE
```

Note: After performing this step, you should stop and restart the Intelligent Agent on both nodes to rediscover the nodes and databases. See *Oracle Intelligent Agent User's Guide* for additional information.

5.12 Scenario 12: Re-Creating a Configuration with Data Guard Manager

Use the Create Configuration wizard and choose the Create Existing Standby option to create and enable the broker configuration based on the new primary and standby roles. (Follow the steps in Section 5.2 through Section 5.4.) Because the standby site is already created, you can use the Create Existing Standby method to create the standby database. This method takes only a few minutes to re-create the standby database.

6

Data Guard Command-Line Interface Scenarios

This chapter provides several scenarios that show how to use the Data Guard command-line interface (CLI) to create, manage, and monitor a broker configuration.

This chapter describes the following scenarios:

- Scenario 1: Creating a Physical Standby Database on a Remote Site
- Scenario 2: Creating a Configuration
- Scenario 3: Setting Database Properties
- Scenario 4: Setting the Configuration Protection Mode
- Scenario 5: Performing Routine Management Tasks
- Scenario 6: Enabling the Configuration, Sites, and Resources
- Scenario 7: Performing a Switchover Operation
- Scenario 8: Performing a Failover Operation
- Scenario 9: Monitoring a Data Guard Configuration

6.1 Scenario 1: Creating a Physical Standby Database on a Remote Site

- One of the prerequisites for using the CLI is that a primary database and any standby databases must already exist and the DG_BROKER_START initialization parameter must be set to TRUE for all instances in the configuration. You also need to use a server parameter file (SPFILE) with the broker (see Section 7.1.3, "DGMGRL Command Usage Notes").

After starting the Oracle instance, set the DG_BROKER_START=TRUE initialization parameter using the SQL ALTER SYSTEM statement. The parameter value will be saved in the server parameter file (SPFILE). Then, the next time that you start the Oracle instance, the broker is started automatically and you do not need to issue the SQL ALTER SYSTEM statement again.

This scenario describes the creation of a physical standby database on a remote site. The following assumptions are being made:

- You can perform a consistent backup.
- TCP/IP is used to connect to primary and standby databases.
- The primary database site name is Boston.
- The remote site name is San Francisco.

To create your Data Guard configuration, you must construct the standby database from backups of the primary database control files and datafiles, and then prepare it for recovery. *Oracle9i Data Guard Concepts and Administration* provides detailed information about creating standby databases. However, the following list summarizes the steps:

> **See Also:** *Oracle9i Data Guard Concepts and Administration* for detailed information about creating standby databases.

1. Make a backup of the primary database datafiles (or access a previous backup) and create the standby control file.
2. Transfer the datafiles and control file to the standby site.
3. Configure Oracle Net to enable communication between the primary and standby database instances. The procedure includes the configuration of the tnsnames.ora and the listener.ora files as well as the startup of listeners on both primary and standby sites.
4. Configure the standby initialization parameter files.
5. Start the standby database instance and mount it.
6. Convert the initialization parameter files (PFILES) on both primary and standby sites into server parameter files (SPFILES), if necessary. Use the following SQL*Plus command:

   ```
   CREATE SPFILE FROM PFILE='pfilename';
   ```

If an instance is not using a SPFILE, then you must shut down the instance and restart it using the SPFILE.

> **See Also:** *Oracle9i Database Administrator's Guide* for detailed information about creating server parameter files (SPFILE)

6.2 Scenario 2: Creating a Configuration

This section provides examples that create a broker configuration named Sales that includes a primary and standby site located in two different cities.

Each site in this configuration has a single database instance:

- The primary database is located in Boston.
- A standby database is located in San Francisco.

The following steps show how to create a configuration and add one physical standby site.

Step 1 Invoke the Data Guard CLI.

To start the CLI, enter DGMGRL at the command-line prompt on a system where Oracle9*i* Data Guard is installed:

```
% DGMGRL [options]
DGMGRL for Solaris:  Version 9.2.0.0.0 - Production.
(c) Copyright 2002 Oracle Corporation. All rights reserved.
Welcome to DGMGRL, type "help" for information.
DGMGRL>
```

Step 2 Connect to the primary database.

Before you specify any command (other than the HELP, EXIT, or QUIT command), you must first connect to the primary database using the DGMGRL CONNECT command.

The account from which you connect to the database (SYS in this example) must have SYSDBA privileges on the primary and standby sites. You do not have to include AS SYSDBA on the CONNECT command because SYSDBA is the default setting for this command.

The following examples show two variations of the CONNECT command. Example 6–1 shows how to connect to the default database on the local system and Example 6–2 includes the Oracle Net service name (prmy) to make a connection to a database located on a remote system.

Example 6–1 Connecting to the Default Database on the Local System

```
DGMGRL> CONNECT sys/change_on_install;
Connected.
```

Example 6–2 Connecting to the Default Database on a Remote System

```
DGMGRL> CONNECT sys/change_on_install@primary;
Connected.
```

Step 3 Create the broker configuration.

To create the broker configuration, you first define the configuration including the primary site, which in this case is called Boston. In a later command, you will add the standby site, San Francisco.

Use the CREATE CONFIGURATION command to create the Sales configuration and define the primary site, Boston. The Boston site hosts a database resource called Sales_db.

```
DGMGRL> CREATE CONFIGURATION 'Sales' AS
  PRIMARY SITE IS 'Boston'
  RESOURCE IS 'Sales_db'
  HOSTNAME IS 'prmyhost1'
  INSTANCE NAME IS 'bstn'
  SERVICE NAME IS 'primary'
    SITE IS MAINTAINED AS PHYSICAL;
```

The CLI returns the following information:

```
Configuration "Sales" added with primary site "Boston"
Database resource "Sales_db" added.
```

Step 4 Show the configuration information.

Use the SHOW CONFIGURATION command to display a brief summary of the configuration:

```
DGMGRL> SHOW CONFIGURATION;
```

The CLI returns the following information:

```
Configuration 'Sales' is
  Primary Site is 'Boston'
Current status for "Sales":
DISABLED
```

Use the SHOW CONFIGURATION VERBOSE command to display a detailed summary of the configuration:

```
DGMGRL> SHOW CONFIGURATION VERBOSE;
```

The CLI returns the following information that shows the broker configuration currently contains only the primary site:

```
Configuration
  Name:              'Sales'
  Enabled:           'no'
  Default state:     'ONLINE'
  Intended state:    'OFFLINE'
  Protection Mode:   'MaxPerformance'
  Number of sites:   1
  Sites:
    Primary site: Boston
Current status for "Sales":
SUCCESS
```

Note: Always fetch the database host and service name by querying the V$INSTANCE view.

Step 5 Add a standby site to the configuration.

To add a standby database site to the Sales configuration, use the CREATE SITE command.

The following command defines the San Francisco location as a standby site hosting a database resource called reportingdb, which is the standby database associated with the primary database called Salesdb.

```
DGMGRL> CREATE SITE 'San Francisco'
  RESOURCE IS 'reportingdb'
  HOSTNAME IS 'stdbyhost1'
  INSTANCE NAME IS 'sfdb'
  SERVICE NAME IS 'dest2'
    SITE IS MAINTAINED AS PHYSICAL;
```

The CLI returns the following information:

```
Site "San Francisco" added to configuration.
Database resource "reportingdb" added.
```

Then, use the SHOW SITE VERBOSE command to verify that the San Francisco site was added to the Sales configuration:

```
DGMGRL> SHOW SITE VERBOSE 'San Francisco';
```

The CLI returns the following information:

```
Site
  Name:                          'San Francisco'
  Hostname:                      'system2'
  Instance name:                 'sfdb'
  Service Name:                  'dest2'
  Standby Type:                  'physical'
  Number Built-in Processes:     '2'
  Number Generic Processes:      '0'
  Enabled:                       'no'
  Required:                      'yes'
  Default state:                 'STANDBY'
  Intended state:                'OFFLINE'
  Number of resources:  1
  Resources:
    Name: reportingdb (default) (verbose name='reportingdb')
```

6.3 Scenario 3: Setting Database Properties

After you create the configuration with the CLI, you can set database properties at any time. For example, the following SQL statement sets the LogArchiveFormat and StandbyArchiveDest properties for the reportingdb standby database resource:

```
DGMGRL> ALTER RESOURCE reportingdb ON SITE 'San Francisco' SET PROPERTY
LogArchiveFormat='log_%t_%s.arc';
DGMGRL> ALTER RESOURCE reportingdb ON SITE 'San Francisco' SET PROPERTY StandbyArchiveDest
= '/archfs/arch/';
```

These properties map directly to the LOG_ARCHIVE_FORMAT and STANDBY_ARCHIVE_DEST database initialization parameters. If the database resource is enabled, setting a database resource property value causes the underlying parameter value to be changed in the corresponding database and the value for the changed parameter is reflected in the SPFILE file. Thus, if the database is shut down and restarted outside of Data Guard Manager (such as from the SQL*Plus interface), the database uses the new parameter values from the updated SPFILE file when it starts. However, you should not make changes to the database dynamically through SQL statements. Doing so will cause an inconsistency between the database and the broker.

> **Note:** The database properties are always displayed in mixed-case typeface to help you visually differentiate database properties (from the corresponding initialization parameter, SQL statement, or PL/SQL procedure), which are typically documented in UPPERCASE typeface.

You can change a property if the database resource is enabled or disabled. However, if the database resource is disabled when you change a property, the change does not take effect until the database resource is enabled.

6.4 Scenario 4: Setting the Configuration Protection Mode

You can change the protection mode of the configuration at any time. However, it is best if you do this when there is no activity occurring in the configuration.

> **Note:** Sometimes the broker may need to restart instances within the configuration after the configuration is already enabled. For example, if the protection mode that is set on the database is different from what is set in the configuration. the broker will automatically restart the database instance. See Section 2.9 for information the steps required to change the protection mode for your configuration.

This scenario sets the protection mode of the configuration to the MAXPROTECTION mode. Note that this protection mode requires that the broker configuration has at least one physical standby site configured to use standby redo logs.

Step 1 Configure standby redo logs, if necessary.

Because we will be setting the protection mode to the MAXPROTECTION mode, it is important to ensure that sufficient standby redo logs are configured on the physical standby site.

Data Guard Manager provides the Standby Redo Log Assistant to configure standby redo logs automatically for you. If you are using the CLI, see *Oracle9i Data Guard Concepts and Administration* for information about creating standby redo logs.

Step 2 Set the LogXptMode property appropriately.

Use the ALTER RESOURCE (property) command on the standby database to set the log transport mode that corresponds to the protection mode you plan to set. For example:

```
DGMGRL> ALTER RESOURCE 'reportingdb' ON SITE 'San Francisco' SET PROPERTY
  > LogXptMode=SYNC;
```

The broker will not allow this command to succeed unless there is a physical standby database configured with standby redo logs in the configuration.

Step 3 Change the overall protection mode for the configuration.

Use the ALTER CONFIGURATION command to upgrade the broker configuration to the MAXPROTECTION protection mode.

```
DGMGRL> ALTER CONFIGURATION SET PROTECTION MODE AS MAXPROTECTION;
Operation requires restart of site "Boston"
Shutting down site Boston...
Database closed.
Database dismounted.
ORACLE instance shut down.
Restarting site Boston...
Started "Boston" as new primary
```

After you change the protection mode, the primary database will automatically restart.

Step 4 Verify the protection mode was changed.

Use the SHOW CONFIGURATION VERBOSE command to display the current protection mode for the configuration.

```
DGMGRL> SHOW CONFIGURATION VERBOSE;
Configuration
  Name:             'Sales'
  Enabled:          'yes'
  Default state:    'ONLINE'
  Intended state:   'ONLINE'
  Protection Mode:  'MaxProtection'
  Number of sites:  2
  Sites:
    Primary Site: Boston
    Standby Site: San Francisco
Current status for "Sales":
SUCCESS
```

If the configuration is disabled when you enter this command, the actual protection mode change is not applied until you enable the configuration with the ENABLE CONFIGURATION command. The broker will not allow you to enable the configuration if it does not find any standby database in the configuration that can support the requirements of the protection mode.

See Also: Section 2.9, "Protection Modes"

6.5 Scenario 5: Performing Routine Management Tasks

There may be situations in which you want to change the state or properties of the objects in a broker configuration to perform routine maintenance on one or more objects. You might also need to disable objects in a configuration when you want to transition the resources from a managed mode to a state of no longer being managed by the Data Guard broker.

6.5.1 Changing States and Properties

As you monitor the configuration, you might need to dynamically modify the states of the resource objects and database properties. The following sections show how to change the state or properties of the objects in the configuration.

6.5.1.1 Alter the State of the Broker Configuration

Taking an object offline should be done only when absolutely necessary, because it will perform a `shutdown immediate` and `startup nomount` on the database. If you take a configuration offline, all instances will be restarted when you bring the configuration online again. You can be connected through any database to change a Data Guard configuration to an offline state. You cannot change state of a configuration, site, or database resource object that is disabled.

Example 6–3 shows how to take all objects offline across the entire broker configuration.

Example 6–3 Altering the Broker Configuration

```
DGMGRL> ALTER CONFIGURATION SET STATE = 'OFFLINE';
```

6.5.1.2 Alter a Database Resource Property

Section 6.3 described the database properties that must be set before the configuration is enabled. You can modify the values of database properties at any time—if the database is enabled, disabled, online, or offline.

Example 6–4 shows how to use the ALTER RESOURCE command to change the LogArchiveTrace property to the value 127 for the Sales_db database resource

Example 6–4 Altering a Database Resource Property

```
DGMGRL> ALTER RESOURCE 'Sales_db' ON SITE 'Boston'
>  SET PROPERTY 'LogArchiveTrace'='127';
```

The CLI returns the following message to indicate that the LogArchiveTrace property was updated successfully in the Data Guard configuration file:

```
Property "LogArchiveTrace" updated
```

If the configuration is currently disabled, the database resource does not use the new property value until you enable the broker configuration with the ENABLE CONFIGURATION command.

6.5.1.3 Alter the State of a Database Resource

You might want to use the standby database temporarily for reporting applications. To change the state of the standby database to read-only, enter the ALTER RESOURCE command as shown in Example 6–5.

Example 6–5 Altering a Database Resource State

```
DGMGRL> ALTER RESOURCE 'reportingdb' ON SITE 'San Francisco'
>  SET STATE='READ-ONLY';
```

Remember that when you put the standby database in the read-only state, it stops log apply services from applying the archived redo logs to the standby database.

6.5.1.4 Alter the State of a Site

By default, a site is in the same state as the configuration. However, you can use the ALTER SITE command (shown in Example 6–6) to restrict a site and its dependent database resources from going online when its parent configuration goes online.

Example 6–6 Altering a Site State

```
DGMGRL> ALTER SITE 'Boston' SET STATE='Offline';
```

The CLI returns the following message to indicate that the command was successfully updated in the Data Guard configuration file:

```
Succeeded.
```

6.5.2 Disabling the Configuration, Sites, and Database Resources

When you disable the broker configuration or any of its sites or resources, you are disabling the broker's management of those objects and are effectively removing your ability to use the CLI to manage and monitor the disabled object. However, disabling the broker's management of a broker configuration does not affect the actual operation of the underlying Data Guard configuration, its sites, or the database resources. For example, the log transport services and log apply services in the Data Guard configuration continue to function unchanged, but you cannot manage them with the CLI.

In addition, disabling the broker's management of an object **does not** remove or delete it from the Data Guard configuration file. You can re-enable your ability to use the CLI (or Data Guard Manager) to manage the object by entering the appropriate ENABLE CONFIGURATION, ENABLE SITE, or ENABLE RESOURCE command.

After you enter a DISABLE CONFIGURATION, DISABLE SITE, or DISABLE RESOURCE command, the CLI returns the following message to indicate that the command successfully updated the Data Guard configuration file:

```
Disabled.
```

6.5.2.1 Disable a Configuration

You must use the DISABLE CONFIGURATION command to disable management of the entire broker configuration or that of the primary site as shown in Example 6–7.

Example 6–7 Disabling the Configuration or the Primary Site

```
DGMGRL> DISABLE CONFIGURATION;
```

The only way to disable broker management of the primary site is to use the DISABLE CONFIGURATION command; the DISABLE SITE command only disables management of a standby site.

Note: If you disable management of a configuration while connected to the standby database, you must connect to the primary database when you re-enable the configuration.

6.5.2.2 Disable a Database Resource

You use the `DISABLE RESOURCE` command on the primary database or standby database when you no longer want to use the CLI to manage and monitor it. The `DISABLE RESOURCE` command disables broker management of the database, but it does not stop or change actual database operations (for example, log apply services) occurring in the Data Guard configuration. The command shown in Example 6–8 disables management of the `reportingdb` standby database.

Example 6–8 Disabling a Database Resource

```
DGMGRL> DISABLE RESOURCE reportingdb ON SITE 'San Francisco';
```

6.5.2.3 Disable a Standby Site

You use the `DISABLE SITE` command when you no longer want to use the CLI to manage and monitor a standby site and a standby database resource.

You can explicitly disable broker management of a standby site to prevent it from being brought online when the rest of the configuration is brought online. Example 6–9 shows how to disable the San Francisco standby site.

Example 6–9 Disabling a Standby Site

```
DGMGRL> DISABLE SITE 'San Francisco';
```

Note: To disable management of a primary site, you must use the `DISABLE CONFIGURATION` command.

When running in either the maximum protection or maximum availability protection mode, the broker prevents you from disabling the last database resource or site that supports the protection mode.

6.5.3 Removing the Configuration or a Standby Site

When you use either the REMOVE CONFIGURATION or REMOVE SITE command, you effectively delete the configuration or standby site information from the Data Guard configuration file, removing the ability of the Data Guard broker to manage the configuration or the standby site, respectively.

A remove operation *does not* remove or delete the actual Data Guard configuration, nor does it affect the operation of the actual Data Guard configuration, its sites, or the database resources.

> **Caution: After you use the** REMOVE CONFIGURATION or REMOVE SITE **command, you cannot recover the configuration information that has been deleted from the Data Guard configuration file. You must go through the steps in Section 6.2, as necessary, to create a broker configuration that can be managed with the CLI (or Data Guard Manager).**

Step 1 Remove a standby site from the configuration.

When you use the REMOVE SITE command, you remove the standby site and standby database from management and monitoring by the broker.

```
DGMGRL> REMOVE SITE 'San Francisco';
```

The CLI returns the following message to indicate that the command successfully removed the San Francisco site information from the Data Guard configuration file:

```
Removed site "San Francisco" from configuration.
```

Step 2 Remove the broker configuration.

Use the following command to remove the entire configuration from management and monitoring by the broker:

```
DGMGRL> REMOVE CONFIGURATION;
```

The CLI returns the following message to indicate that the command successfully removed all of the configuration information from the Data Guard configuration file:

```
Removed configuration.
```

You cannot remove the primary site unless the configuration is disabled. To remove the primary site when the configuration is enabled, you must remove the entire

configuration. Also, when you remove a site, the broker verifies that it is the last site configured to meet the minimum requirements for the current protection mode. However, you can delete the configuration regardless of the protection mode.

> **See Also:** Section 2.9, "Protection Modes" for more information about the broker manages objects to ensure support for protection modes

6.6 Scenario 6: Enabling the Configuration, Sites, and Resources

So far, the Sales configuration has been disabled, which means it is not under the control of the Data Guard broker. When you finish configuring the sites and resources into a broker configuration and setting any necessary database properties (described in Section 6.3), you must enable the configuration to allow the Data Guard broker to manage the configuration, and so that you bring the primary and standby database systems online.

You can enable:

- The entire configuration, including all of its sites and resources
- A standby site, including the database resource on the standby site
- A database resource

Step 1 Enable the entire configuration.

You can enable the entire configuration, including all of the sites and resources, with the following command:

```
DGMGRL> ENABLE CONFIGURATION;
Enabled.
```

The configuration's default state is online.

Step 2 Show the configuration.

Use the SHOW command to verify that the configuration and its resources were successfully enabled and brought online.

```
DGMGRL> SHOW CONFIGURATION VERBOSE;
```

The CLI returns the following information:

```
Configuration
  Name:              'Sales'
  Enabled:           'yes'
```

```
  Default state:    'ONLINE'
  Intended state:   'ONLINE'
  Protection Mode:  'MaxProtection'
  Number of sites:  2
  Sites:
    Primary Site: Boston
    Standby Site: San Francisco
```

6.7 Scenario 7: Performing a Switchover Operation

You can switch the role of the primary site and a standby site using the SWITCHOVER command. Before you issue the SWITCHOVER command, you must make sure:

- The state of the primary resource is set to READ-WRITE-XPTON and the state of the target standby database resource is PHYSICAL-APPLY-ON for a physical standby database resource or LOGICAL-APPLY-ON for a logical standby database resource
- All participating site and database resource objects are in good health, without any errors or warnings present
- The standby database properties have been set on the primary database resource, so that the primary resource can function correctly when transitioning to a standby database resource

Perform the following steps:

Step 1 Check the primary database resource

Use the SHOW RESOURCE VERBOSE command to check the state and health of the primary database resource, as follows:

```
DGMGRL> SHOW RESOURCE VERBOSE 'Sales_db';
Resource
  Name:             Sales_db
  Manager Type:     internal
   Standby Type:     PHYSICAL
Online States:
  ONLINE
  PHYSICAL-APPLY-READY
  PHYSICAL-APPLY-ON
  READ-ONLY
  LOGICAL-APPLY-READY
  LOGICAL-APPLY-ON
  READ-WRITE
```

```
  READ-WRITE-XPTON
Properties:
  INTENDED_STATE                = 'READ-WRITE-XPTON'
  ENABLED                       = 'yes'
  IGNORE_STATUS                 = 'no'
  LogXptMode                    = 'ARCH'
  Dependency                    = ''
  Alternate                     = ''
  DelayMins                     = '0'
  Binding                       = 'OPTIONAL'
  MaxFailure                    = '0'
  ReopenSecs                    = '300'
  AsyncBlocks                   = '2048'
  LogShipping                   = 'ON'
  ApplyNext                     = '0'
  ApplyNoDelay                  = 'NO'
  ApplyParallel                 = '1'
  StandbyArchiveDest            = '/dbs/a1'
  LogArchiveTrace               = '4095'
  StandbyFileManagement         = 'AUTO'
  ArchiveLagTarget              = '0'
  LogArchiveMaxProcesses        = '5'
  LogArchiveMinSucceedDest      = '1'
  DbFileNameConvert             = 'dbs/s2t, dbs/t'
  LogFileNameConvert            = 'dbs/s2t, dbs/t'
  LogArchiveFormat              = 'r_%t_%s.arc'
  InconsistentProperties        = '(monitor)'
  InconsistentLogXptProps       = '(monitor)'
  SendQEntries                  = '(monitor)'
  LogXptStatus                  = '(monitor)'
  SbyLogQueue                   = '(monitor)'
Properties for 'PRIMARY' state:
  DEFAULT_STATE    = 'READ-WRITE-XPTON'
  EXPLICIT_DISABLE = 'no'
  REQUIRED         = 'yes'
Properties for 'STANDBY' state:
  DEFAULT_STATE    = 'PHYSICAL-APPLY-ON'
  EXPLICIT_DISABLE = 'no'
  REQUIRED         = 'yes'
Current status for "Sales_db":
SUCCESS
```

In particular, you should examine the `INTENDED_STATE` property and the current status item, and some of the standby properties such as `StandbyArchiveDest`,

DbFileNameConvert, and LogFileNameConvert. See Chapter 4 for information about managing database resources.

Step 2 Check the standby database resource that is the target of the switchover operation

Use the SHOW RESOURCE VERBOSE command to check the state and health of the standby database resource that is the target of the switchover operation. For example:

```
DGMGRL> SHOW RESOURCE VERBOSE reportingdb;
Resource
  Name:              reportingdb
  Manager Type:      internal
   Standby Type:      PHYSICAL
Online States:
  ONLINE
  PHYSICAL-APPLY-READY
  PHYSICAL-APPLY-ON
  READ-ONLY
  LOGICAL-APPLY-READY
  LOGICAL-APPLY-ON
  READ-WRITE
  READ-WRITE-XPTON
Properties:
  INTENDED_STATE                 = 'PHYSICAL-APPLY-ON'
  ENABLED                        = 'yes'
  IGNORE_STATUS                  = 'no'
  LogXptMode                     = 'ARCH'
  Dependency                     = ''
  Alternate                      = ''
  DelayMins                      = '0'
  Binding                        = 'OPTIONAL'
  MaxFailure                     = '0'
  ReopenSecs                     = '300'
  AsyncBlocks                    = '2048'
  LogShipping                    = 'ON'
  ApplyNext                      = '0'
  ApplyNoDelay                   = 'NO'
  ApplyParallel                  = '1'
  StandbyArchiveDest             = '/dbs/a2'
  LogArchiveTrace                = '4095'
  StandbyFileManagement          = 'AUTO'
  ArchiveLagTarget               = '0'
  LogArchiveMaxProcesses         = '5'
```

```
    LogArchiveMinSucceedDest        = '1'
    DbFileNameConvert               = 'dbs/t, dbs/s2t'
    LogFileNameConvert              = 'dbs/t, dbs/s2t'
    LogArchiveFormat                = 'r_%t_%s.arc'
    InconsistentProperties          = '(monitor)'
    InconsistentLogXptProps         = '(monitor)'
    SendQEntries                    = '(monitor)'
    LogXptStatus                    = '(monitor)'
    SbyLogQueue                     = '(monitor)'
  Properties for 'PRIMARY' state:
    DEFAULT_STATE    = 'READ-WRITE-XPTON'
    EXPLICIT_DISABLE = 'no'
    REQUIRED         = 'yes'
  Properties for 'STANDBY' state:
    DEFAULT_STATE    = 'PHYSICAL-APPLY-ON'
    EXPLICIT_DISABLE = 'no'
    REQUIRED         = 'yes'
  Current status for "reportdb2":
  SUCCESS
```

In particular, you should examine the INTENDED_STATE property and the current status of the resource.

Step 3 Issue the switchover command

Issue the SWITCHOVER command to swap the roles of the primary and standby sites. The following example shows how the broker automatically shuts down and restarts the two participating sites as a part of the switchover operation. (See the usage notes in Section 7.1.3 for information about how to set up the broker environment so that CLI can automatically restart the primary and standby sites for you.)

```
DGMGRL> SWITCHOVER TO 'San Francisco';
Performing switchover NOW. Please wait...
Operation requires restart of site "Boston"
Operation requires restart of site "San Francisco"
Shutting down site Boston...
database not mounted
ORACLE instance shut down.
Shutting down site San Francisco...
database not mounted
ORACLE instance shut down.
Restarting site Boston...
Restarting site San Francisco...
Started "Boston" as standby
```

```
Started "San Francisco" as new primary
Switchover succeeded. New primary is "San Francisco"
```

After the switchover operation completes, use SHOW CONFIGURATION, SHOW SITE and SHOW RESOURCE commands to verify that the switchover operation was successful.

6.8 Scenario 8: Performing a Failover Operation

You invoke a failover operation in response to an emergency situation; usually when the primary site cannot be accessed or connected. See Section 3.2.2, "Managing Failover Operations" before you fail over to decide which standby site should be the target of the failover operation and which type of failover operation (graceful or forced) you want to perform.

If you must perform a failover operation, Oracle Corporation recommends that you always perform a graceful failover operation. The following scenario describes a graceful failover operation to the remote site called “San Francisco.”

Step 1 Connect to the target standby site.

To perform the failover operation, you must connect to the standby site to which you want to fail over using the SYSDBA username and password of that site. For example:

```
DGMGRL> connect sys/change_on_install@dest2;
Connected.
```

Step 2 Issue the failover command.

Now you can issue the failover command to make the target standby site the new primary site for the configuration. Note that after the failover operation completes, the original primary site cannot be used as a viable standby site of the new primary site. The following example shows how the broker automatically shuts down and restarts the new primary site as a part of the failover operation. (See the usage notes in Section 7.1.3 for information about how to set up the broker environment so that the CLI can automatically restart the new primary site and database for you.)

```
DGMGRL> FAILOVER TO 'San Francisco' GRACEFUL;
Performing failover NOW. Please wait...
Operation requires restart of site "San Francisco"
Shutting down site San Francisco...
database not mounted
ORACLE instance shut down.
Restarting site San Francisco...
```

```
Started "San Francisco" as new primary
Failover succeeded. New primary is "San Francisco"
You have now finished failover. You can use SHOW CONFIGURATION, SHOW SITE and
SHOW RESOURCE commands to check if the failover operation is successful.
```

6.9 Scenario 9: Monitoring a Data Guard Configuration

The scenario in this section demonstrates how to use SHOW commands to view database monitorable properties, and identify and resolve a failure situation.

Step 1 Identify the failure.

Assume that a failure occurred when the primary database attempted to transport an archived redo log to the standby site. To identify the failure, examine the LogXptStatus (log transport status) property to see the error status of log transport services for the standby site. Use the following command at the DGMGRL command-line prompt:

```
DGMGRL> SHOW RESOURCE 'Sales_db' LogXptStatus;
LogXptStatus = 'San Francisco=ORA-16049: simulated error on archivelog write'
```

This LogXptStatus property indicates that the error ORA-16049 has been returned during a write operation to the standby site, San Francisco.

Step 2 Obtain additional information.

To obtain additional information, use the SHOW LOG ALERT LATEST command to view the database alert log on the primary site, Boston. For example:

```
DGMGRL> SHOW LOG ALERT LATEST ON SITE 'Boston';
```

The command returns the following output:

```
------------------------------------------------------------------------------
7590 Transmitting activation ID 1332649663 (4f6e9ebf)
7591 ARCH: Completed archiving  log# 1 thrd# 1 seq# 737
7592 Fri Jan 19 16:23:26 2001
7593 Completed checkpoint up to RBA [0x2e2.2.10], SCN: 0x0000.0000df8d
7594 Fri Jan 19 16:25:07 2001
7595 Beginning log switch checkpoint up to RBA [0x2e3.2.10], SCN:0x0000.0000df91
7596 Fri Jan 19 16:25:07 2001
7597 ARCH: Beginning to archive log# 2 thrd# 1 seq# 738
7598 Fri Jan 19 16:25:07 2001
7599 Thread 1 advanced to log sequence 739
7600   Current log# 1 seq# 739 mem# 0: /vobs/oracle/dbs/t_log1.f
7601 Fri Jan 19 16:25:07 2001
```

```
7602 ARC0: Beginning to archive log# 2 thrd# 1 seq# 738
7603 ARC0: Unable to archive log# 2 thrd# 1 seq# 738
7604       Log actively being archived by another process
7605 Fri Jan 19 16:25:07 2001
7606 Transmitting activation ID 1332649663 (4f6e9ebf)
7607 Transmitting activation ID 1332649663 (4f6e9ebf)
7608 ARCH: I/O error 16049 archiving log 2 to 'standby1'
7609 ARCH: Completed archiving  log# 2 thrd# 1 seq# 738
```

In the example, lines 7603 through 7609 (in boldface type) show that the archiver process (ARC*n*) failed to transmit log file 738 to the standby archive destination identified as standby1. This is probably because an I/O error occurred when archiving the redo log to the standby site.

Step 3 Examine the primary and standby queues for archived redo logs.

To determine the severity of this failure and its effect on the integrity of the Data Guard configuration, use the following commands to examine the state of the archived redo logs from the perspective of both the primary and standby sites.

1. Use the following command to examine the SendQEntries (send queue entries) property on the primary database, Sales_db. The SendQEntries property shows the archive status of all of the log files on the primary site:

```
DGMGRL> SHOW RESOURCE 'Sales_db' SendQEntries;
PRIMARY_SEND_QUEUE
           SITE_NAME        STATUS     LOG_SEQ          TIME_GENERATED          TIME_COMPLETED
       San Francisco      ARCHIVED         738      01/19/2001 16:23:23     01/19/2001 16:25:07
                           CURRENT         739      01/19/2001 16:25:07
```

The output shows that log 738 has been archived locally on the primary site but has not yet shipped to the San Francisco standby site.

2. Now, examine the SbyLogQueue (standby log queue) property to view the archived redo logs that have been received by the standby site, but have not been applied to the standby database, reportingdb:

```
DGMGRL> SHOW RESOURCE 'reportingdb' SbyLogQueue;
STANDBY_RECEIVE_QUEUE
           LOG_SEQ         TIME_GENERATED            TIME_COMPLETED
               738    01/19/2001 16:23:23        01/19/2001 16:25:07
```

3. Use the same commands again to monitor the problem:

```
DGMGRL> SHOW RESOURCE VERBOSE 'Sales_db' SendQEntries;
DGMGRL> PRIMARY_SEND_QUEUE
           SITE_NAME        STATUS     LOG_SEQ          TIME_GENERATED          TIME_COMPLETED
       San Francisco      ARCHIVED         738      01/19/2001 16:23:23     01/19/2001 16:25:07
```

```
       San Francisco      ARCHIVED         740      01/19/2001 16:31:26     01/19/2001 16:32:33
                           CURRENT         745      01/19/2001 16:51:55

DGMGRL> SHOW RESOURCE VERBOSE 'reportingdb' SbyLogQueue;
DGMGRL> STANDBY_RECEIVE_QUEUE
           LOG_SEQ         TIME_GENERATED            TIME_COMPLETED
               738    01/19/2001 16:23:23        01/19/2001 16:25:07
               739    01/19/2001 16:25:07        01/19/2001 16:31:26
               740    01/19/2001 16:31:26        01/19/2001 16:32:33
               741    01/19/2001 16:32:33        01/19/2001 16:36:28
               742    01/19/2001 16:36:28        01/19/2001 16:41:36
               743    01/19/2001 16:41:36        01/19/2001 16:46:41
               744    01/19/2001 16:46:41        01/19/2001 16:51:55
```

As you can see, the problem is not resolving itself. The primary send queue contents shown by the SendQEntries property show that logs 738 and 740 have not been successfully archived to the standby destination. The initial failure with transporting log 738 to the standby has caused log apply services on the standby database to fall behind the primary database. The output for the SbyLogQueue property shows that the standby database receive queue grows with every new archived redo log sent by the primary database.

The failure resulted in only a portion of log 738 being written to the standby database destination.

Step 4 Examine the database alert log on the standby site.

The final step in this process is to examine the database alert log on the standby site to determine a possible solution to the problem. The following command allows you to view the latest entries in the database alert log for the standby site.

```
DGMGRL> SHOW LOG ALERT LATEST ON SITE 'San Francisco';

------------------------------------------------------------------------------
 7571 Fri Jan 19 16:21:15 2001
 7572 Media Recovery Log /vobs/oracle/dbs/stdby_1_736.arc
 7573 Media Recovery Waiting for thread 1 seq# 737
 7574 Fri Jan 19 16:23:30 2001
 7575 Media Recovery Log /vobs/oracle/dbs/stdby_1_737.arc
 7576 Media Recovery Waiting for thread 1 seq# 738
 7577 Fri Jan 19 16:25:15 2001
 7578 Media Recovery Log /vobs/oracle/dbs/stdby_1_738.arc
 7579 Fri Jan 19 16:25:15 2001
 7580 Errors in file /vobs/oracle/rdbms/log/stdby1_mrp0_28842.trc:
 7581 ORA-00311: cannot read header from archived log
 7582 ORA-00334: archived log: '/vobs/oracle/dbs/stdby_1_738.arc'
 7583 ORA-27091: skgfqio: unable to queue I/O
 7584 ORA-27072: skgfdisp: I/O error
```

```
7585 SVR4 Error: 25: Inappropriate ioctl for device
7586 Additional information: 1
7587 MRP0: Background Media Recovery failed with error 311
7588 Recovery interrupted.
7589 Recovered data files restored to a consistent state at change 270314464672.
7590 MRP0: Background Media Recovery process is now terminated
```

This output from the database alert log shows that a fatal error reading log 738 (the corrupted log file) has resulted in the shutdown of the background Media Recovery Process. For this reason, no other archived redo logs have been applied to the standby database. The errors are shown in boldface type in the example.

Step 5 Fix the problem.

The solution is to manually copy logs 738 and 740 from the primary site to the standby site. Then, the next log file that is sent automatically to the standby site should trigger the application of all of the log files waiting in the standby queue to the standby database.

If this does not fix the problem, you might need to take the standby database resource offline and then put it back online again.

The `ALTER RESOURCE` command in the following example changes the state of the `reportingdb` database resource to `offline` and then back into an `online` state.

```
DGMGRL> ALTER RESOURCE 'reportingdb' ON SITE 'San Francisco' SET STATE='offline';
Succeeded.

DGMGRL> ALTER RESOURCE 'reportingdb' ON SITE 'San Francisco'
    SET STATE='PHYSICAL-APPLY-ON';
```

7

Data Guard Command-Line Interface Reference

The Data Guard command-line interface allows you to manage a Data Guard configuration and its site and database resource objects directly from the command line, or from batch programs or scripts. You can use the Data Guard command-line interface as an alternative to the Oracle9*i* Data Guard Manager graphical user interface for managing a Data Guard configuration.

This chapter provides reference information for the Data Guard command-line interface.

7.1 Starting the Data Guard Command-Line Interface

To run the Data Guard command-line interface, you must have SYSDBA privileges.

Start the command-line interface by entering `DGMGRL` at the command line prompt on a system where Oracle9*i* Data Guard is installed:

```
% DGMGRL [options]
DGMGRL for Solaris:  Version 9.2.0.0.0 - Production.
(c) Copyright 2002 Oracle Corporation. All rights reserved.
Welcome to DGMGRL, type "help" for information.
DGMGRL>
```

7.1.1 DGMGRL Optional Parameters

You can supply optional parameters on the command line to indicate how you want the Data Guard command-line interface to display output such as command prompts, banners, and messages.

Specify none, one, or all of the following keywords when you invoke the DGMGRL command-line interface:

- -echo

  Echoes command input and output to the default display device. If you do not use this parameter, only the output from the command is displayed.

- -silent

  Suppresses the display of the DGMGRL (DGMGRL>) command prompt on your default display device. This option is useful if you are directing the command output to a file or to another display tool.

The following subsections specify the command format that you enter at the DGMGRL> command prompt.

7.1.2 DGMGRL Command Format and Parameters

The DGMGRL commands allow you to create and maintain one broker configuration at a time. A broker configuration can consist of a primary site and from 1 to 9 standby sites.

After you invoke the command-line interface, you can enter any of the DGMGRL commands listed in Table 7–1. Each command and its associated parameters are described in detail in later sections of this chapter.

Table 7–1 Summary of DGMGRL Commands

Command	Effect
ALTER CONFIGURATION (protection mode)	Alters the protection mode of the overall Data Guard configuration.
ALTER CONFIGURATION (state)	Alters a broker configuration state from online to offline, or from offline to online.
ALTER RESOURCE (property)	Allows you to change the value of a property for the specified database resource object.
ALTER RESOURCE (state)	Allows you to change the state of the specified database resource object.
ALTER SITE (state)	Allows you to change the state of a site object from online to offline, or from offline to online.

Table 7–1 (Cont.) Summary of DGMGRL Commands

Command	Effect
ALTER SITE (AUTO PFILE)	Allows you to specify the initialization parameter file used to automatically restart the database of the site as needed by the client. The information you specify with this command is session specific; that is, it resets to the default initialization parameter file when you connect to a database using the `CONNECT` command.
CONNECT	Connects a given username to the specified database.
CREATE CONFIGURATION	Creates a broker configuration, a primary site object, and a database resource object on the primary site.
CREATE SITE	Creates a new standby site object and a database resource object, and adds them to the broker configuration.
DISABLE CONFIGURATION	Disables broker management of a configuration so that the configuration and all of its site objects and database resource objects are no longer managed by the broker.
DISABLE RESOURCE	Disables broker management of a database resource object in the broker configuration.
DISABLE SITE	Disables broker management of the specified standby site object in the broker configuration so that the standby site object and the database resource objects on the standby site are no longer managed by the broker.
ENABLE CONFIGURATION	Enables broker management of the broker configuration.
ENABLE RESOURCE	Enables broker management of a database resource object in the broker configuration.
ENABLE SITE	Enables broker management of a standby site object in the broker configuration.
EXIT	Exits the Data Guard command-line interface.
FAILOVER	Performs a database failover operation in which the standby site to which the CLI is currently connected fails over into the role of primary database. You issue the `FAILOVER` command as a result of an unplanned transition.
HELP	Displays online help for the Data Guard command-line interface.
QUIT	Quits the Data Guard command-line interface.
REMOVE CONFIGURATION	Removes the broker configuration including all of its site objects and database resource objects.

Table 7–1 (Cont.) Summary of DGMGRL Commands

Command	Effect
REMOVE SITE	Removes a standby site object from the broker configuration including the database resource object running on the standby site.
SHOW CONFIGURATION	Displays a information about the broker configuration.
SHOW DEPENDENCY TREE	Displays the dependency tree and default online states for the broker configuration.
SHOW LOG	Shows the Data Guard configuration log or the Oracle database alert log.
SHOW RESOURCE	Displays information about the named database resource object and its status.
SHOW SITE	Displays information about the site object in the broker configuration.
SHUTDOWN	Shuts down a currently running Oracle database instance.
STARTUP	Starts an Oracle instance with several options, including mounting and opening a database.
SWITCHOVER	Performs a switchover operation in which the current primary site becomes a standby site, and the standby site becomes the primary site.

7.1.3 DGMGRL Command Usage Notes

To use the Data Guard command-line interface, the following must be true:

- The DG_BROKER_START dynamic initialization parameter is set to TRUE.
- Oracle Net must be properly configured on the hosts that contain the primary and standby database sites. Specifically, the primary and standby database services must be properly registered with the listener, a net service name should have been created for the primary and standby database sites, and the listener must be started.

> **See Also:** Chapter 6 for more information about preparing and starting Oracle Data Guard. See the *Oracle9i Database Administrator's Guide* for more information about setting up the network files and listener on the standby database.

- You must have SYSDBA privileges to use the Data Guard command-line interface.
- For systems configured with shared servers, the connect string or Oracle Net service name used for broker communications must specify the use of a dedicated server (`SERVER=DEDICATED`) process instead of the shared server process. In addition, the connection between the CLI and the database instance must also use a dedicated server link.
- To connect to a remote standby database and manage it, you need to set up a remote login password file. You also need to set up a remote login password file for DGMGRL to be able to restart the database automatically.

  See Also: *Oracle9i Data Guard Concepts and Administration*, the *Oracle9i Database Administrator's Guide*, and your operating system-specific documentation to set up remote access using the `REMOTE_LOGIN_PASSWORDFILE` initialization parameter

- A semicolon is required at the end of each DGMGRL command.
- Characters specified in a DGMGRL command string value are interpreted as lowercase characters, unless enclosed in double (") or single (') quotation marks. For example, site and SiTe are equivalent, but "site" and "SiTe" are distinctive.
- You can use the backslash (\) as an escape character. This makes it possible to embed any character in a character string of a command prompt.
- Some operations on a broker configuration may require that one or more sites be shut down and restarted. In most cases, the CLI will automatically shut down and restart a given site for you if the following are true:
  - The broker must be able to connect to the site using the username and password given in the last `CONNECT` command, even if the last `CONNECT` command was used to connect to another site. Thus, the remote password file for the site must contain the username and password given in the last `CONNECT` command.
  - The PFILE of the site must be set by the `ALTER SITE (AUTO PFILE)` command, or the PFILE or the SPFILE for the site can be found at the default directory location.

    See Also: *Oracle9i Database Administrator's Guide* for more information about setting up remote password files and the default location of the PFILE and SPFILE initialization parameter files.

Command Examples

Example 1

This example demonstrates how to connect to the DGMGRL command-line interface on a local system.

```
% DGMGRL

Welcome to DGMGRL, type "help" for information.

DGMGRL> CONNECT sys/change_on_install;
Connected.
```

Example 2

This example demonstrates how to connect to the DGMGRL command-line interface on a remote system.

```
DGMGRL> CONNECT sys/change_on_install@remote-stby;
Connected.
```

7.2 Stopping the Data Guard Command-Line Interface

When you are done working with the command-line interface and want to return to the operating system, enter the `EXIT` or `QUIT` command at the DGMGRL command prompt. For example:

```
DGMGRL> EXIT;
```

You can use either the `EXIT` or the `QUIT` command to leave the DGMGRL command-line interface.

ALTER CONFIGURATION (protection mode)

Alters the current protection mode setting for broker configuration.

Format

ALTER CONFIGURATION SET PROTECTION MODE AS *protection-mode*;

Command Parameters

protection mode
The data protection mode in which you want the configuration to run when the configuration is enabled. The possible protection modes are:

MAXPROTECTION
MAXAVAILABILITY
MAXPERFORMANCE

Usage Notes

Perform the following steps before you use the `ALTER CONFIGURATION` command to set the protection mode:

- If you plan to set the protection mode to either the `MAXPROTECTION` or `MAXAVAILABILITY` protection mode, ensure that standby redo logs are configured on a standby site.
- Use the `ALTER RESOURCE (property)` command on a standby database of at least 1 site, to set the log transport mode that minimally corresponds to the protection mode you plan to set. For example, if you plan to set the overall Data Guard configuration to the `MAXAVAILABILITY` mode, you must use the `ALTER RESOURCE` command to set the `SYNC` mode for log transport services. For example:

  ```
  ALTER RESOURCE 'Sales_db' ON SITE 'Boston' SET PROPERTY LogXptMode=SYNC;
  ```

  The following table shows the configuration protection modes and the minimum corresponding settings for log transport services:

Protection Mode	Log Transport Mode	Require Physical Standby Database and Standby Redo Logs?
MAXPROTECTION	SYNC	Yes
MAXAVAILABILITY	SYNC	No
MAXPERFORMANCE	ARCH or ASYNC	No

See Also: Chapter 4 for more information about the protection modes and log transport modes

- After you change the protection mode, the primary site and database will automatically restart.
- Use the SHOW CONFIGURATION VERBOSE command to display the current protection mode for the configuration.

```
DGMGRL> SHOW CONFIGURATION VERBOSE;
Configuration
  Name:             'The SUPER cluster'
  Enabled:          'yes'
  Default state:    'ONLINE'
  Intended state:   'ONLINE'
  Protection Mode:  'MaxPerformance'
  Number of sites:  2
  Sites:
    Primary Site: Primary
    Standby Site: Standby2
Current status for "The SUPER cluster":
SUCCESS
```

If broker management of the configuration is disabled when you enter the ALTER CONFIGURATION command, the protection mode of the configuration does not take effect until the next time you enable the configuration with the ENABLE CONFIGURATION command.

Command Examples

Example 1

The following example shows how to upgrade the broker configuration to the MAXPROTECTION protection mode. The broker configuration will have the maximum amount of data protection after these commands complete.

After verifying that standby redo logs are configured on the standby site and that the LogXptMode is set properly to support the protection mode, enter the following commands:

```
DGMGRL> ALTER RESOURCE 'Sales_db' SET PROPERTY LogXptMode=SYNC;
Property "logxptmode" updated.

DGMGRL> ALTER CONFIGURATION SET PROTECTION MODE AS MAXPROTECTION;
Operation requires restart of site "Primary";
Shutting down site Primary...
Database closed.
Database dismounted.
ORACLE instance shut down.
Restarting site Primary...
Started "Primary" as new primary
```

The broker automatically stops and restarts the primary site and database.

ALTER CONFIGURATION (state)

Alters the intended (runtime) state of the broker configuration.

Format

ALTER CONFIGURATION SET STATE = *state*;

Command Parameters

state
The state in which you want the configuration to be running when management of the configuration is enabled. The possible states are:

OFFLINE
ONLINE

Usage Notes

- Use the `SHOW CONFIGURATION` command to display the current default and intended states for the configuration.
- This command changes only the intended (runtime) state for the configuration; the default state is not altered. If the configuration is set to offline, then all sites and database resources are set to the offline state. This means all databases will be shut down and restarted in nomount mode.
- The state of the configuration cannot be changed when the configuration is disabled.

Command Examples

Example 1

In the following example, the broker configuration will be in the online state the next time you enable the configuration.

```
DGMGRL> ALTER CONFIGURATION SET STATE = ONLINE;
Succeeded.
```

ALTER RESOURCE (property)

Allows you to change the value of a property for the specified database resource object.

Format

ALTER RESOURCE *resource-name* [ON SITE *site-name*]

SET PROPERTY *property-name* = *value*;

Command Parameters

resource-name
The name of the database resource object for which you want to set a property value.

site-name
The name of the site object where the database resource object is located.

property-name
The name of the property for which you want to set a new value. Section 2.8 describes the database resource properties in detail.

value
The new value for the property. Section 2.8 describes the values for each property.

Usage Notes

- You do not have to disable broker management of the configuration or database resource to change a database resource property. However, if the database resource is disabled when you use the ALTER RESOURCE command, the property change does not take effect until you enable broker management of the configuration.
- If some properties are set with the wrong values while the database resource is disabled, then when the database is later enabled the broker will not set the incorrect values in the database. This results in a health check (a warning saying some properties are inconsistent between the Data Guard configuration file or database, or saying some property values are invalid (for example, returned errors might include ORA-16792, ORA-16801, ORA-16804). When this happens, check which property has the problem by investigating monitorable

properties, InconsistentProperties, InconsistentLogXptProps, and by looking at the Data Guard console logs. Reset the property with the correct value.

- If multiple log transport properties are set incorrectly in the Data Guard configuration file, then resetting one property to correct its value will not work because all of the properties correspond to one attribute of the LOG_ARCHIVE_DEST_*n* initialization parameter to be successful. In this case, disable the database resource, correct all property values, and then re-enable the resource again.
- If you change the value of a property that corresponds to a static initialization parameter, you must shut down and start up the database for the change to take effect. For example, changing the DbFileNameConvert property (which corresponds to the DB_FILE_NAME_CONVERT initialization parameter) would require that you stop and start the database. See Chapter 8 for information about which properties are static and dynamic.
- If you do not specify a site, the broker searches each site for the specified database resource. If it finds more than one database resource with the specified name (for example, if the database resource name you specified is not unique within the broker configuration), the ALTER RESOURCE command returns an error message. You must re-issue the ALTER RESOURCE command and specify a site name with the ON SITE option.
- Use this command on the standby database to set the log transport mode that corresponds to the protection mode you set with the ALTER CONFIGURATION (protection mode)command. For example, if you plan to set the overall Data Guard configuration to the MAXAVAILABILITY protection mode, you must use the ALTER RESOURCE command to set the SYNC mode for log transport services. For example:

  ```
  ALTER RESOURCE 'Sales_db' ON SITE 'Boston' SET PROPERTY LogXptMode=SYNC;
  ```

  The following table shows the configuration protection modes and the corresponding settings for log transport services:

Protection Mode	Log Transport Mode	Require Physical Standby Database and Standby Redo Logs?
MAXPROTECTION	SYNC	Yes
MAXAVAILABILITY	SYNC	No
MAXPERFORMANCE	ARCH or ASYNC	No

- Use the SHOW RESOURCE command to display the current property values for the database resource object.
- See Section 2.8 for detailed information about each property.

Command Examples

Example 1

The ALTER RESOURCE command in the following example changes the value of the LogArchiveTrace property to be 127 for the database resource object named Sales_db.

```
DGMGRL> ALTER RESOURCE 'Sales_db' ON SITE 'Boston' SET PROPERTY 'LogArchiveTrace'='127';
Property "LogArchiveTrace" updated.
```

The command-line interface returns the following message to indicate that the LogArchiveTrace property was updated successfully in the Data Guard configuration file:

```
Property "LogArchiveTrace" updated
```

If broker management of the configuration is currently disabled, the property does not affect the actual database, until the next time you enable the broker configuration with the ENABLE CONFIGURATION command.

ALTER RESOURCE (state)

Allows you to change the state of the specified database resource object.

Format

ALTER RESOURCE *resource-name* [ON SITE *site-name*]

SET STATE = *state*;

Command Parameters

resource-name
The name of the database resource object for which you want to change the state.

site-name
The name of the site object that contains the database resource object that you want to alter.

state
The state to which the database resource will transition when it is enabled.

Usage Notes

- Use the SHOW RESOURCE command to display information, such as the current runtime state of a database resource object.
- If you do not specify a site, the broker searches each site for the specified database resource. If it finds more than one database resource with the specified name (for example, if the database resource name you specified is not unique within the broker configuration), the ALTER RESOURCE command returns an error message. You must issue the ALTER RESOURCE command again and specify a site name with the ON SITE option.
- The database can be in an ONLINE or OFFLINE state. The ONLINE state has the following substates:

```
PHYSICAL-APPLY-READY
PHYSICAL-APPLY-ON (default state for a physical standby database)
READ-ONLY
LOGICAL-APPLY-READY
LOGICAL-APPLY-ON (default state for a logical standby database)
READ-WRITE
```

```
READ-WRITE-XPTON (default state for a primary database)
```

Command Examples

Example 1

The ALTER RESOURCE command in the following example changes the state of the Sales_db database resource to read / write.

```
DGMGRL> ALTER RESOURCE 'Sales_db' ON SITE 'Boston' SET STATE='read-write';
Succeeded.
```

ALTER SITE (state)

Allows you to change the state of a site object.

Format

ALTER SITE *site-name*

SET STATE = *state*;

Command Parameters

site-name
The name of the site object for which you want to change state.

state
The state to which the site will transition when management of the site is enabled. The possible states are:

OFFLINE
ONLINE

Usage Notes

- Use the `SHOW SITE` command to display information about a site object.
- A site will operate either in the primary or standby role. When you change the state of the site to online, the site and its dependent database resource object begins operating in that role.

Command Examples

Example 1

```
DGMGRL> ALTER SITE 'Boston' SET STATE='online';
Succeeded.
```

ALTER SITE (AUTO PFILE)

Allows you to specify an initialization parameter file that will be used to automatically restart the database of the site.

Format

ALTER SITE *site-name*

SET AUTO PFILE= *initialization-file* | OFF ;

Command Parameters

site-name
The name of the site object for which you want to specify the automatic restart initialization parameter file.

initialization-file
The name of the PFILE initialization parameter file that will be used to automatically restart the database of the site.

Usage Notes

- The broker requires that you specify a server parameter file (SPFILE) in the initialization parameter file. See the *Oracle9i Database Administrator's Guide* for more information about creating and using the server parameter file (SPFILE).
- If you set the `SET AUTO PFILE=OFF` option and you receive a message telling you to restart a site, use the `SHUTDOWN` and `STARTUP` commands to restart your databases.
- The default mode is `SET AUTO PFILE=''`, which indicates using the default PFILE name to restart databases.
- The information you specify with this command is session specific; that is, it resets to the default initialization parameter file when you connect to a database using the `CONNECT` command.
- Use the `SHOW SITE` command with the VERBOSE option to display the current parameter file information for a site.

Command Examples

Example 1

```
DGMGRL> ALTER SITE 'Boston' SET AUTO PFILE='/oracle/dbs/initbs.ora';
Succeeded.
```

Example 2

```
DGMGRL> ALTER SITE 'Boston' SET AUTO PFILE=OFF;
Succeeded.
```

CONNECT

Connects a given username to the specified database.

Format

CONNECT *username/password*[*@net-service-name*];

Command Parameters

username/password
Represents the username and password with which you want to connect to the database.

net-service-name
Consists of the Oracle Net service name of the site to which you want to connect. The exact syntax depends upon the Oracle Net communications protocol your Oracle installation uses.

Usage Notes

- The username and password must be valid for the database to which you are trying to connect. The username you specify must have the SYSDBA privilege.
- If the `CONNECT` command returns an error, check to see that you specified a valid service name.
- The Data Guard broker communications must be configured over a dedicated server. (The connect string or the Oracle Net service name in the `LISTENER.ORA` file must specify the use of a dedicated server (`SERVER=DEDICATED`) process, not a shared (`SERVER=SHARED`) process.)

Command Examples

Example 1

This example connects to the default database on the local system.

```
DGMGRL> CONNECT sys/change_on_install;
Connected.
```

Example 2

This example connects to a remote database whose service name is prmy.

```
DGMGRL> CONNECT sys/change_on_install@prmy;
Connected.
```

CREATE CONFIGURATION

Creates a new broker configuration, and creates and adds a primary site object and a database resource object to the configuration.

Format

CREATE CONFIGURATION *configuration-name* AS

PRIMARY SITE IS *site-name*

RESOURCE IS *resource-name*

HOSTNAME IS *host-name*

INSTANCE NAME IS *instance-name*

SERVICE NAME IS *net-service-name*

SITE IS MAINTAINED AS *standby-type*;

Command Parameters

configuration-name
A user-friendly name for the configuration you are creating. Valid names contain any alphanumeric characters. If spaces are included in the name, the name must be enclosed in double or single quotation marks. The name must consist of 30 or fewer bytes.

site-name
A user-friendly name for the primary site object.

resource-name
A user-friendly name for the database resource object to be created for the primary site.

host-name
The host name of the primary site, as shown in the `V$INSTANCE` view.

instance-name
The instance name of the primary database, as shown in the `V$INSTANCE` view.

net-service-name
Consists of the Oracle Net service name for the primary site. The exact syntax depends upon the Oracle Net communications protocol your Oracle installation uses. For more information, refer to the Oracle Net documentation.

standby-type
Specify PHYSICAL or LOGICAL for this parameter to indicate the type of standby database that this site will contain as a result of a switchover operation.

Usage Notes

- A broker configuration is a named collection of one or more site objects and database resource objects that you want to manage as a group. You must specify a value for each of the parameters. There are no default values.
- To add more standby sites and databases after you create the broker configuration, use the CREATE SITE command.
- The Data Guard broker communications must be configured over a dedicated server. (The connect string or the net service name in the LISTENER.ORA file must specify the use of a dedicated server (SERVER=DEDICATED) process, not a shared (SERVER=SHARED) process.)
- The host-name and instance-name parameters specify information the broker requires to uniquely identify a site in the configuration. To obtain the proper values for the host-name and instance-name parameters, use the values returned from the V$INSTANCE fixed view.

  The following example shows a SQL*Plus statement that selects these values from the V$INSTANCE fixed view. In the example, the values boston and bstn should be supplied for the hostname and instance-name parameters in the CREATE CONFIGURATION command.

```
SQL> CONNECT sys/change_on_install AS SYSDBA;
SQL> SELECT HOST_NAME, INSTANCE_NAME FROM V$INSTANCE;
HOST_NAME                      INSTANCE_NAME
---------------------------------------------------------------
boston                         bstn
```

Command Examples

Example 1

The following example creates a new broker configuration named Sales with a database that will have the physical standby characteristics if the primary database transitions to the standby role in a future switchover operation.

```
DGMGRL> CREATE CONFIGURATION 'Sales' AS
  PRIMARY SITE IS 'Boston'
  RESOURCE IS 'Sales_db'
  HOSTNAME IS 'boston'
  INSTANCE NAME IS 'bstn'
  SERVICE NAME IS 'bstn'
    SITE IS MAINTAINED AS PHYSICAL;

Configuration "Sales" added with primary site "Boston"
Database resource "Sales_db" added.
```

CREATE SITE

Creates a new standby site object and database resource object and adds it to an existing broker configuration.

Format

CREATE SITE *site-name*

RESOURCE IS *resource-name*

HOSTNAME IS *host-name*

INSTANCE NAME IS *instance-name*

SERVICE NAME IS *net-service-name*

SITE IS MAINTAINED AS *standby-type*;

Command Parameters

site-name
A user-friendly name for the site object you are creating. Valid names contain any alphanumeric characters. If spaces are included in the name, the name must be enclosed in double or single quotation marks. The name must consist of 30 or fewer bytes.

resource-name
A user-friendly name for the database resource object to be created for the standby site.

host-name
The host name of the standby site.

instance-name
The instance name of the primary database.

net-service-name
Consists of the Oracle Net service name of the standby site that you want to add. The exact syntax depends upon the Oracle Net communications protocol your Oracle installation uses. For more information, see the Oracle Net documentation.

standby-type
Specify PHYSICAL or LOGICAL for this parameter to indicate the type of standby database that this site will contain.

Usage Notes

- The standby database must already exist on the site before you can add the site object to a broker configuration.

  See Also: *Oracle9i Data Guard Concepts and Administration* for information about creating a standby database

- Before you can add standby sites with the CREATE SITE command, you must create the broker configuration using the CREATE CONFIGURATION command.
- Use the CREATE SITE command after you have connected to the primary database using the CONNECT command.
- You can add up to nine standby sites to an existing configuration.
- The broker configuration can be in any state (online, offline) when you create a site.
- If management of the broker configuration is enabled when you issue the CREATE SITE command, the site object is created in a disabled state to allow you to change properties before the site goes online.
- A resource can be associated with only 1 broker configuration. Site names must be unique within the configuration
- The Data Guard broker communications must be configured over a dedicated server. (The connect string or the net service name in the LISTENER.ORA file must specify the use of a dedicated server (SERVER=DEDICATED) process, not a shared (SERVER=SHARED) process.)
- The host-name and instance-name parameters specify information the broker requires to uniquely identify a site in the configuration. To obtain the proper values for the host-name and instance-name parameters, use the values returned from the V$INSTANCE fixed view.

  The following example shows a sample SQL*Plus statement that selects these values from the V$INSTANCE fixed view. In the example, the values sf and sfdb should be supplied for the host-name and instance-name parameters in the CREATE SITE command.

```
SQL> CONNECT sys/change_on_install AS SYSDBA;
```

```
SQL> SELECT HOST_NAME, INSTANCE_NAME FROM V$INSTANCE;
HOST_NAME                      INSTANCE_NAME
---------------------------------------------------------------
sf                             sfdb
```

Command Examples

Example 1

The following example demonstrates how to add a standby site called San Francisco to the broker configuration.

```
DGMGRL> CREATE SITE 'San Francisco'
  RESOURCE IS 'reportingdb'
  HOSTNAME IS 'sf'
  INSTANCE NAME IS 'sfdb'
  SERVICE NAME IS 'dest2'
    SITE IS MAINTAINED AS PHYSICAL;

Site "San Francisco" added to configuration.
Database resource "reportingdb" added.
```

DISABLE CONFIGURATION

Disables broker management of a broker configuration and all of its site objects and database resource objects.

Format

DISABLE CONFIGURATION;

Command Parameters

None.

Usage Notes

- A disabled configuration is no longer managed by the broker.
- The only way to disable broker management of the primary site is to use the `DISABLE CONFIGURATION` command.
- This command does not remove or delete the broker configuration. See the `REMOVE CONFIGURATION` command for more information about removing the configuration.

Command Examples

Example 1

The following example disables management of the broker configuration and all of its sites and database resources.

```
DGMGRL> DISABLE CONFIGURATION;
Disabled.
```

DISABLE RESOURCE

Disables broker management of a database resource object.

Format

DISABLE RESOURCE *resource-name* [ON SITE *site-name*];

Command Parameters

resource-name
The name of the database resource object that you want to disable.

site-name
The name of the site containing the database resource that you want to disable.

Usage Notes

- A disabled database resource is no longer managed by the broker.
- If you do not specify a site, the broker searches each site for the specified database resource. If it finds more than one database resource with the specified name (for example, if the database resource name you specified is not unique within the configuration), the `DISABLE RESOURCE` command returns an error message. You must re-issue the `DISABLE RESOURCE` command and specify a site name with the `ON SITE` option.
- This command does not remove or delete the database resource from the broker configuration.

Command Examples

Example 1

The following example demonstrates how to disable management of the database resource `reportingdb` from the San Francisco site.

```
DGMGRL> DISABLE RESOURCE 'reportingdb' ON SITE 'San Francisco';
Disabled.
```

DISABLE SITE

Disables broker management of the specified standby site object in the broker configuration and any database resource objects on the site.

Format

DISABLE SITE *site-name*;

Command Parameters

site-name
The name of the standby site that you want to disable.

Usage Notes

- When you disable broker management of a standby site in the configuration, management of the database resource configured on the standby site is also disabled.
- You cannot disable the primary site with the `DISABLE SITE` command. Use the `DISABLE CONFIGURATION` command to disable the primary site.

Command Examples

Example 1

The following example demonstrates how to disable broker management of the San Francisco standby site.

```
DGMGRL> DISABLE SITE 'San Francisco';
Disabled.
```

ENABLE CONFIGURATION

Enables the broker to actively manage the broker configuration including all of its site objects and database resource objects.

Format

ENABLE CONFIGURATION;

Command Parameters

None.

Usage Notes

- This command enables the broker to manage the broker configuration including all of the sites and database resources in the configuration.
- Use this command to enable broker management of the primary site object.
- When you enable broker management of a broker configuration, its default state is online. To change the intended runtime state of the configuration, use the `ALTER CONFIGURATION (state)` command.
- By default, broker management of the primary database resource object is enabled in the online state with the log shipping turned on (`READ-WRITE-XPTON` state), a physical standby database resource object is enabled in the `PHYSICAL-APPLY-ON` state, and a logical standby database resource object is enabled in the `LOGICAL-APPLY-ON` state. You can change the state of the database resource using the `ALTER RESOURCE (state)` command, but not when the resource or a configuration is disabled.
- See the `SHOW CONFIGURATION` command to display information about the configuration.

Command Examples

Example 1

The following example enables management of a broker configuration.

```
DGMGRL> ENABLE CONFIGURATION;
Enabled.
```

ENABLE RESOURCE

Enables the broker to actively manage the specified database resource object.

Format

ENABLE RESOURCE *resource-name* [ON SITE *site-name*];

Command Parameters

resource-name
The name of the database resource object you want to manage with the broker.

site-name
The name of the site object containing the database resource object that you want to enable.

Usage Notes

- If broker management of the site where the database resource is located is disabled, the database resource you specify with the ENABLE RESOURCE command will remain disabled (and cannot be managed by the broker) until you enable the site. See the ENABLE SITE command.
- By default, broker management of the standby database resource object is enabled with log apply services started (a physical standby database is in the PHYSICAL-APPLY-ON state and a logical standby database resource object is enabled in the LOGICAL-APPLY-ON state). You can change the state of the database resource using the ALTER RESOURCE (state) command, but not when the database resource, site, or configuration is disabled.
- If you do not specify a site, the broker searches each site for the specified database resource. If it finds more than one database resource with the specified name (for example, if the database resource name you specified is not unique within the configuration), the ENABLE RESOURCE command returns an error message. You must re-issue the ENABLE RESOURCE command and specify a site name with the ON SITE option.
- Use the SHOW RESOURCE command to display information about the database resource, including its default and intended states, and the properties of the database resource.

Command Examples

Example 1

The following example enables broker management of the database resource object named Sales_db.

```
DGMGRL> ENABLE RESOURCE 'Sales_db';
Enabled.
```

ENABLE SITE

Enables the broker to actively manage the specified standby site object, including its database resource object.

Format

ENABLE SITE *site-name*;

Command Parameters

site-name
The name of the standby site object you want to manage with the broker.

Usage Notes

- This command enables the broker to actively manage the standby site object.
- To enable broker management of a primary site object, use the `ENABLE CONFIGURATION` command.
- When you enable broker management of a standby site object, the database resource object on the standby site is also enabled (unless it has been explicitly disabled with the `DISABLE` command).
- By default, management of the standby database resource object is enabled with log apply services started (in the `PHYSICAL-APPLY-ON` or `LOGICAL-APPLY-ON` state. You can change the state of the database resource using the `ALTER RESOURCE (state)` command.

Command Examples

Example 1

The following example enables management of the standby site named San Francisco.

```
DGMGRL> ENABLE SITE 'San Francisco';
Enabled.
```

EXIT

Exits the command-line interface.

Format

EXIT;

Usage Notes

- This command has the same effect as the QUIT command.
- A database connection is not required to execute this command. However, if you are connected, this command breaks the connection.

Command Examples

Example 1

The following example demonstrates how to exit (quit) the command-line interface.

```
DGMGRL> EXIT;
```

FAILOVER

A failover operation changes one of the standby sites and its database into the role of a primary site and database.

> **Note:** Because a failover operation results in a role transition that may result in the loss of application data, you should perform a failover operation *only* if the primary database has failed. If you want the current primary database and a standby database to switch roles, then use the SWITCHOVER command.

Format

FAILOVER TO *site-name* {GRACEFUL | FORCED};

Command Parameters

site-name
The name of the standby site object you want to fail over to the primary site role.

Usage Notes

- You must include one of the following options on the FAILOVER command:
  - GRACEFUL: A graceful failover automatically recovers some or all of the original primary database application data. A graceful failover allows the new primary database to communicate with the bystanders and attempt to keep the active (enabled) bystanders in the configuration. This is the recommended failover option.
  - FORCED: A forced failover may result in lost application data even when standby redo logs are configured on the standby database.
- To be considered as a viable candidate for the failover operation, the specified standby site and its database must be enabled before the failover operation can proceed.
- The failover operation operates on the site object, and its dependent database resource object. Thus, the failover operation changes one of the standby databases into the role of a primary database. Any other bystanders remain in the standby role.

- Before you issue the FAILOVER command, verify that you are connected to the standby site that will become the new primary site. If necessary, issue a CONNECT command to connect to the standby site.
- If the standby site that is transitioning into the role of primary site contains a physical standby database, then the instance will be restarted after the failover operation completes. If the site contains a logical standby database, the instance does not need to be restarted.
- Once you have failed over, you can only configure the original primary database to be a standby database; you cannot restart the original primary site or database to run in the primary role.

Command Examples

Example 1

The following example performs a graceful failover in which the standby site, Standby2, transitions to the primary role:

```
DGMGRL> FAILOVER TO 'Standby2' GRACEFUL;
Performing failover NOW. Please wait...
Operation requires restart of site "Standby2"
Shutting down site Standby2...
database not mounted
ORACLE instance shut down.
Restarting site Standby2...
Started "Standby2" as new primary
Failover succeeded. New primary is "Standby2"
```

Example 2

The following example performs a forced failover operation:

```
DGMGRL> FAILOVER TO 'Standby4' FORCED;
Performing failover NOW. Please wait...
Operation requires restart of site "Standby4"
Shutting down site Standby4...
database not mounted
ORACLE instance shut down.
Restarting site Standby4...
Started "Standby4" as new primary
Failover succeeded. New primary is "Standby4"
```

HELP

Displays online help for the Data Guard command-line interface.

Format

HELP [<*topic*>];

Command Parameters

topic
The topic for which you want to display help information. If you do not specify a topic, the command lists all of the topics and the format. Valid topics are:

ALTER
CONNECT
CREATE
DISABLE
ENABLE
EXIT
FAILOVER
HELP
QUIT
REMOVE
SHOW
SHUTDOWN
STARTUP
SWITCHOVER

Usage Notes

A database connection is not required to execute this command.

Command Examples

Example 1

The following examples get help on the HELP and CONNECT commands.

```
DGMGRL> HELP HELP;
Display the help for a given command
```

```
DGMGRL> HELP CONNECT;
Connect to a server
connect <user>/<password>@<connect>;
```

Example 2

```
DGMGRL> HELP ALTER;
edit a configuration, site or resource
alter configuration set state = '[ONLINE|OFFLINE]'

alter configuration set protection mode as
  '[MaxProtection|MaxAvailability|MaxPerformance]'

alter site '<site name>' set state = '[ONLINE|OFFLINE]'

alter site '<site name>' set auto pfile='<pfile>'

alter resource '<resource name>'
   [ on site '<site name>'] set state = '<state>'

alter resource '<resource name> [ on site <site name> ] '
   set property '<property name>' = '<value>';
```

QUIT

Exits the Data Guard command-line interface.

Format

QUIT;

Usage Notes

- This command has the same effect as the EXIT command.
- A database connection is not required to execute this command. However, if you are connected, this command breaks the connection.

Command Examples

Example 1

The following example shows how to quit (exit) the command-line interface.

```
DGMGRL> QUIT;
```

REMOVE CONFIGURATION

Removes all of the broker configuration information from the Data Guard configuration file, and removes management of all of the site and database resource objects associated with the broker configuration.

Caution: When you use the REMOVE CONFIGURATION command, all information is deleted from the Data Guard configuration file and cannot be recovered.

Format

REMOVE CONFIGURATION;

Command Parameters

None.

Usage Notes

- When you remove a broker configuration, management of all of the site objects and database resource objects associated with that configuration is removed.
- This command does not remove or affect the actual primary or standby database instances, databases, datafiles, or control files.

Command Examples

Example 1

The following example shows how to remove configuration information from the configuration file.

```
DGMGRL> REMOVE CONFIGURATION;
Removed configuration.
```

REMOVE SITE

Removes the specified standby site object from the broker configuration.

Caution: When you use the REMOVE SITE command, all of the information about the standby site and its database resource is deleted from the Data Guard configuration file and cannot be recovered.

Format

REMOVE SITE *site-name*;

Command Parameters

site-name
The name of the standby site that you want to remove.

Usage Notes

- When you remove a standby site, management of the database resource object associated with that standby site is removed. However, this command does not remove or affect the actual standby site and database.
- You cannot remove the primary site with this command. Use the REMOVE CONFIGURATION command to remove the primary site object.

Command Examples

Example 1

The following example shows how to remove information about the site object named San Francisco.

```
DGMGRL> REMOVE SITE 'San Francisco';
Removed site "San Francisco" from configuration.
```

SHOW CONFIGURATION

Displays a brief or a detailed summary about the broker configuration.

Format

SHOW CONFIGURATION [VERBOSE] [*property-name*];

Command Parameters

property-name
The name of the property for which you want to display summary information. Available properties are:

ENABLED
EXPLICIT_DISABLE
INTENDED_STATE
HEALTH_CHECK_INTERVAL
STATUS

See Section 2.8 for complete information about properties.

Usage Notes

- The default is to display a brief summary of the configuration. Use the VERBOSE option to display a detailed summary of the configuration.
- Use the `ALTER CONFIGURATION (state)` command to change the intended state of a configuration.
- Use the `SHOW DEPENDENCY TREE` command to display the dependency tree and default path information for the configuration.

Command Examples

Example 1

The following example provides a brief summary of the Sales configuration.

```
DGMGRL> SHOW CONFIGURATION;
Configuration 'Sales' is
  Primary Site is 'Boston'
  Standby Site is 'San Francisco'
```

```
Current status for "Sales":
SUCCESS
```

Example 2

The following example uses the VERBOSE option to show complete information about the Sales configuration.

```
DGMGRL> SHOW CONFIGURATION VERBOSE;
Configuration
  Name:              'The SUPER cluster'
  Enabled:           'yes'
  Default state:     'ONLINE'
  Intended state:    'ONLINE'
  Protection Mode:   'MaxPerformance'
  Number of sites:   2
  Sites:
    Primary Site is 'Primary'
    Standby Site is 'Standby2'
Current status for "The SUPER cluster":
SUCCESS
```

Example 3

The following example shows the STATUS property for the Sales configuration.

```
DGMGRL> SHOW CONFIGURATION STATUS;
  STATUS = 'SUCCESS'
```

SHOW DEPENDENCY TREE

Displays a dependency tree that shows a static map of the broker configuration and the default online states for each database resource in the configuration.

Format

SHOW DEPENDENCY TREE;

Usage Notes

For detailed information about the configuration, use the SHOW CONFIGURATION command.

Command Examples

Example 1

The following example shows a configuration named Sales with two sites (Boston and San Francisco) and database resource objects called Sales_db and reportingdb. The database resource object (Sales_db) is brought online in its default state of READ_WRITE_XPTON when Boston is running as the primary site. The other database resource object, reportingdb, is brought online in its default state of PHYSICAL_APPLY_ON when San Francisco is running as the standby site.

```
DGMGRL> SHOW DEPENDENCY TREE;
Sales
Sales[ONLINE]->Boston
Sales[ONLINE]->Boston[PRIMARY]->Sales_db
Sales[ONLINE]->Boston[STANDBY]->Sales_db
Sales[ONLINE]->San Francisco
Sales[ONLINE]->San Francisco[PRIMARY]->reportingdb
Sales[ONLINE]->San Francisco[STANDBY]->reportingdb

Default Path:
Sales[ONLINE]->Boston[PRIMARY]
Sales[ONLINE]->Boston[PRIMARY]->Sales_db[READ-WRITE-XPTON]
Sales[ONLINE]->San Francisco[STANDBY]
Sales[ONLINE]->San Francisco[STANDBY]->reportingdb[PHYSICAL-APPLY-ON]
```

In the example, the reportingdb database resource has a dependency on whether or not the San Francisco site is in the primary or the standby role. Furthermore, the

reportingdb database resource object will go to the PHYSICAL-APPLY-ON state when the San Francisco site is a standby site.

Example 2

The following example shows the dependency tree output for a configuration that has multiple standby sites.

```
DGMGRL> SHOW DEPENDENCY TREE;
The SUPER cluster
The SUPER cluster[ONLINE]->Primary
The SUPER cluster[ONLINE]->Primary[PRIMARY]->db
The SUPER cluster[ONLINE]->Primary[STANDBY]->db
The SUPER cluster[ONLINE]->Standby2
The SUPER cluster[ONLINE]->Standby2[PRIMARY]->reportdb2
The SUPER cluster[ONLINE]->Standby2[STANDBY]->reportdb2
The SUPER cluster[ONLINE]->Standby3
The SUPER cluster[ONLINE]->Standby3[PRIMARY]->reportdb3
The SUPER cluster[ONLINE]->Standby3[STANDBY]->reportdb3

Default Path:
The SUPER cluster[ONLINE]->Primary[PRIMARY]
The SUPER cluster[ONLINE]->Primary[PRIMARY]->db[READ-WRITE-XPTON]
The SUPER cluster[ONLINE]->Standby2[STANDBY]
The SUPER cluster[ONLINE]->Standby2[STANDBY]->reportdb2[PHYSICAL-APPLY-ON]
The SUPER cluster[ONLINE]->Standby3[STANDBY]
The SUPER cluster[ONLINE]->Standby3[STANDBY]->reportdb3[PHYSICAL-APPLY-ON]
```

SHOW LOG

Displays the Data Guard configuration log or database alert log from the named site object.

Format

SHOW LOG [ALERT] [LATEST] ON SITE *site-name*;

Command Parameters

ALERT
Displays the database alert log for the specified site object.

LATEST
Specifies the last 20 lines of the SHOW LOG command output.

site-name
The user-friendly name of the site for which you want to display the Data Guard configuration log or the database alert log.

Usage Notes

If you omit the ALERT parameter, then the Oracle Data Guard configuration log for the named site is displayed (if the site is enabled).

Command Examples

Example 1

The following example displays the last 20 lines of the SHOW LOG command output for the Boston site.

```
DGMGRL> SHOW LOG LATEST ON SITE 'Boston';
DRSLOG
LINE  OBJECT_ID DATE                LOG
--------------------------------------------------------------------------------
 2961       913 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=61)
 2962       914 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=61)
 2963       915 2000-11-02-09:29:33  Parent 33554433 child 33554690 vinst
33554690 state 5 (PRIMARY) name reportingdb
 2964       915 2000-11-02-09:29:33  Parent 33554433 child 33554691 vinst
```

```
33554691 state 6 (STANDBY) name reportingdb
 2965       915 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=219)
 2966       916 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=61)
 2967       917 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=61)
 2968       918 2000-11-02-09:29:33  Parent 1 child 16777217 vinst 16777217
state 1 (ONLINE) name Boston
 2969       918 2000-11-02-09:29:33  Parent 1 child 33554433 vinst 33554433
state 1 (ONLINE) name San Francisco
 2970       918 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=204)
 2971       920 2000-11-02-09:29:33  Parent 16777217 child 16777474 vinst
16777474 state 5 (PRIMARY) name Sales_db
 2972       920 2000-11-02-09:29:33  Parent 16777217 child 16777475 vinst
16777475 state 6 (STANDBY) name Sales_db
 2973       920 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=201)
 2974       922 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=61)
 2975       925 2000-11-02-09:29:33  Parent 33554433 child 33554690 vinst
33554690 state 5 (PRIMARY) name reportingdb
 2976       925 2000-11-02-09:29:33  Parent 33554433 child 33554691 vinst
33554691 state 6 (STANDBY) name reportingdb
 2977       925 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=219)
 2978       928 2000-11-02-09:29:33  DMON: DRS OP 204: success. (len=61)
 2979       929 2000-11-02-09:29:33  DMON: DRS OP 207: success. (len=79)
 2980       935 2000-11-02-09:29:34  DMON: DRS OP 207: success. (len=79)
```

Example 2

The following example displays the last 20 lines of the database alert log for the Boston site.

```
DGMGRL> SHOW LOG ALERT LATEST ON SITE 'Boston';
DRSLOG
LINE LOG
------------------------------------------------------------------------------
 1672 Thu Nov  2 09:28:07 2000
 1673 ALTER SYSTEM SET fal_server='' SCOPE=MEMORY SID='bstn';
 1674 ALTER SYSTEM SET fal_client='bstn' SCOPE=MEMORY SID='bstn';
 1675 Thu Nov  2 09:29:31 2000
 1676 ALTER SYSTEM SET fal_server='' SCOPE=MEMORY SID='bstn';
 1677 ALTER SYSTEM SET fal_client='bstn' SCOPE=MEMORY SID='bstn';
 1678 Thu Nov  2 09:29:31 2000
 1679 Beginning log switch checkpoint up to RBA [0x11.2.10], SCN:0x0000.00011b11
 1680 Thread 1 advanced to log sequence 17
 1681   Current log# 2 seq# 17 mem# 0: /ade/ctrezza_bstn/oracle/dbs/t_log2.f
 1682 Thu Nov  2 09:29:31 2000
 1683 ARC0: Beginning to archive log# 1 thread 1 seq# 16
 1684 ARC0: Completed archiving  log# 1 seq# 16 thrd# 1
```

```
1685 Thu Nov  2 09:29:32 2000
1686 ALTER SYSTEM SET fal_server='' SCOPE=MEMORY SID='bstn';
1687 ALTER SYSTEM SET fal_client='bstn' SCOPE=MEMORY SID='bstn';
1688 ALTER SYSTEM SET fal_server='' SCOPE=MEMORY SID='bstn';
1689 ALTER SYSTEM SET fal_client='bstn' SCOPE=MEMORY SID='bstn';
1690 Thu Nov  2 09:29:33 2000
1691 Completed checkpoint up to RBA [0x11.2.10], SCN: 0x0000.00
```

SHOW RESOURCE

Displays a brief or a detailed summary and status of the specified database resource object.

Format

SHOW RESOURCE [VERBOSE] *resource-name* [*property-name*] [ON SITE *site-name*];

Command Parameters

resource-name
The name of the database resource object for which you want to display information.

property-name
The name of the property for which you want to display summary information. See Section 4.3 for a list of database resource properties.

site-name
The name of the site object that has the database resource for which you want a brief summary.

Usage Notes

- The default is to display a brief summary of the database resource object. Specify the VERBOSE option to display a detailed summary.
- Use the `ALTER RESOURCE (property)` command to alter the properties of a database resource object, or use the `ALTER RESOURCE (state)` command to alter the state of a database resource object.
- If you do not specify a site, the broker searches each site for the specified database resource. If it finds more than one database resource with the specified name (for example, if the database resource name you specified is not unique within the configuration), the SHOW RESOURCE command returns an error message. You must re-issue the SHOW RESOURCE command and specify a site name with the ON SITE option.
- To display dependency information, use the `SHOW DEPENDENCY TREE` command.

- Use the SHOW RESOURCE *resource-name property-name* command to show monitorable properties.

Command Examples

Example 1

The following example shows a brief summary of the database resource object called Sales_db.

```
DGMGRL> SHOW RESOURCE 'Sales_db';
Resource 'Sales_db' on site 'Boston'
  depends on 'Boston'
Current status for "Sales_db":
SUCCESS
```

Example 2

The following example uses the VERBOSE option to show complete information about the database resource object called Sales_db on the Boston site.

```
DGMGRL> SHOW RESOURCE VERBOSE Sales_db;
Resource
  Name:              reportdb2
  Manager Type:      internal
   Standby Type:      PHYSICAL
Online States:
  ONLINE
  PHYSICAL-APPLY-READY
  PHYSICAL-APPLY-ON
  READ-ONLY
  LOGICAL-APPLY-READY
  LOGICAL-APPLY-ON
  READ-WRITE
  READ-WRITE-XPTON
Properties:
  INTENDED_STATE                 = 'PHYSICAL-APPLY-ON'
  ENABLED                        = 'yes'
  IGNORE_STATUS                  = 'no'
  LogXptMode                     = 'ARCH'
  Dependency                     = ''
  Alternate                      = ''
  DelayMins                      = '0'
  Binding                        = 'OPTIONAL'
  MaxFailure                     = '0'
  ReopenSecs                     = '300'
```

```
  AsyncBlocks                    = '2048'
  LogShipping                    = 'ON'
  ApplyNext                      = '0'
  ApplyNoDelay                   = 'no'
  ApplyParallel                  = '1'
  StandbyArchiveDest             = '/oracle/dbs/a2'
  LogArchiveTrace                = '4095'
  StandbyFileManagement          = 'AUTO'
  ArchiveLagTarget               = '0'
  LogArchiveMaxProcesses         = '5'
  LogArchiveMinSucceedDest       = '1'
  DbFileNameConvert              = 'dbs/t, dbs/s2t, dbs/s3t, dbs/s2t'
  LogFileNameConvert             = 'dbs/t, dbs/s2t, dbs/s3t, dbs/s2t'
  LogArchiveFormat               = 'r_%t_%s.arc'
  InconsistentProperties         = '(monitor)'
  InconsistentLogXptProps        = '(monitor)'
  SendQEntries                   = '(monitor)'
  LogXptStatus                   = '(monitor)'
  SbyLogQueue                    = '(monitor)'
Properties for 'PRIMARY' state:
  DEFAULT_STATE    = 'READ-WRITE-XPTON'
  EXPLICIT_DISABLE = 'no'
  REQUIRED         = 'yes'
Properties for 'STANDBY' state:
  DEFAULT_STATE    = 'PHYSICAL-APPLY-ON'
  EXPLICIT_DISABLE = 'no'
  REQUIRED         = 'yes'
Current status for "Sales_db":
SUCCESS
```

Example 3

If you see the ORA-16792 error message when you use the SHOW RESOURCE command, you can specify the "InconsistentProperties" property on the command to show a detailed report of the properties that are causing the error.

```
DGMGRL> SHOW RESOURCE db ;
Resource 'db' on site 'Primary'
  depends on 'Primary'
Current status for "db":
Warning: ORA-16792: Some configurable property value is inconsistent with the
database setting
DGMGRL> SHOW RESOURCE db 'InconsistentProperties' ;
INCONSISTENT PROPERTIES
       PROPERTY_NAME       DATABASE_VALUE         SPFILE_VALUE       METADATA_VALUE
    ArchiveLagTarget                  100                  100                   -1
```

SHOW SITE

Displays a brief or detailed summary of the specified site object.

Format

SHOW SITE [VERBOSE] *site-name* [property-name];

Command Parameters

site-name
The name of the site object for which you want to display information.

property-name
The name of the property for which you want to display summary information. Available properties are:

ENABLED
EXPLICIT_DISABLE
INTENDED_STATE
HEALTH_CHECK_INTERVAL
STATUS

See Section 2.8 for complete information about site properties.

Usage Notes

- The default is to display a brief summary of the site object. Specify the VERBOSE option to display a detailed summary.
- Use the `SHOW DEPENDENCY TREE` command to display dependency tree information about a site object.
- Use the `ALTER SITE (state)` command to change the state of a site object.

Command Examples

Example 1

The following example shows a brief summary of the site object called Boston.

```
DGMGRL> SHOW SITE 'Boston';
Site 'Boston' is
```

```
  Hostname is 'boston'
  Instance name is 'bstn'
  Service name is 'bstn'
  Standby is maintained as 'physical'
  Site has 1 resource
    Resource is 'Sales_db'
Current status for "Boston":
SUCCESS
```

Example 2

The following example uses the VERBOSE option to show complete information about the site object called Boston.

```
DGMGRL> SHOW SITE VERBOSE 'Boston';
Site
  Name:                          'Boston'
  Hostname:                      'boston'
  Instance name:                 'bstn'
  Service Name:                  'bstn'
  Standby Type:                  'physical'
  Number Built-in Processes:     '2'
  Number Generic  Processes:     '0'
  Enabled:                       'yes'
  Required:                      'yes'
  Default State:                 'PRIMARY'
  Intended State:                'PRIMARY'
  PFILE:
  Number of resources:  1
  Resources:
    Name: Sales_db (default) (verbose name='Sales_db')
```

Example 3

The following example shows the status property of the site object called Boston.

```
DGMGRL> SHOW SITE 'Boston' STATUS;
  STATUS = SUCCESS
```

SHUTDOWN

Shuts down a currently running Oracle instance.

Format

SHUTDOWN [ABORT | IMMEDIATE | NORMAL];

Command Parameters

None.

Usage Notes

- Before you shut down a database, disable the database resource object in the broker configuration first. When you later restart the database, use the STARTUP NOMOUNT command, then enable the database resource object and allow the broker bring the database to the correct state.
- Using the SHUTDOWN command with no arguments is equivalent to using the SHUTDOWN NORMAL command.
- You must be connected to a database as SYSOPER or SYSDBA. If connecting through an Oracle Net service name, it must be a dedicated server connection. For more information about connecting to a database, see the CONNECT command.
- The following list describes the options to the SHUTDOWN command:
  - ABORT

    Proceeds with the fastest possible shutdown of the database without waiting for calls to complete or for users to disconnect from the database. Uncommitted transactions are not rolled back. Client SQL statements currently being processed are terminated. All users currently connected to the database are implicitly disconnected, and the next database startup will require instance recovery. You must use this option if a background process terminates abnormally.
  - IMMEDIATE

    Does not wait for current calls to complete or users to disconnect from the database. Further connections are prohibited. The database is closed and

dismounted. The instance is shut down, and no instance recovery is required on the next database startup.

– NORMAL

  This is the default option which waits for users to disconnect from the database. Further connections are prohibited. The database is closed and dismounted. The instance is shut down, and no instance recovery is required on the next database startup.

Command Examples

Example 1

The following command shuts down the database in normal mode.

```
DGMGRL > SHUTDOWN;

Database closed.
Database dismounted.
Oracle instance shut down.
```

STARTUP

Starts an Oracle database instance with any of the following options:

- Force: shuts down the current Oracle instance in the `SHUTDOWN ABORT` mode before restarting it.
- Restrict: allows only Oracle users with the `RESTRICTED SESSION` system privilege to connect to the instance.
- Pfile: specifies the PFILE initialization parameter file to be used when the database instance is started.
- Mount: mounts the specified database without opening it. If you do not specify a database name, the database name is taken from the initialization parameter `DB_NAME`.
- Open: mounts and opens the specified database.
- Nomount: starts the specified database instance without mounting the database.

Format

STARTUP

[FORCE]

[RESTRICT]

[PFILE=*filename*]

[MOUNT [*database-name*] | OPEN [*open-options*] [*database-name*] | NOMOUNT];

Command Parameters

filename
The name of the initialization parameter file to be used when starting the database instance. If you do not specify the PFILE parameter option, then the default SPFILE startup parameter file (specific to your operating system) is used.

database-name
The name of the database to mount or open. If you do not specify the `database-name` parameter, the database name is taken from the initialization parameter `DB_NAME`.

open-options
The mode of access in which you want the specified database to start. The possible modes are:

READ ONLY
READ WRITE

Usage Notes

- Before you shut down a database, disable the database resource object in the broker configuration first. When you later restart the database, use the STARTUP NOMOUNT command, then enable the database resource object and allow the broker bring the database to the correct state.
- You cannot use the STARTUP command if the broker management of the configuration is enabled.
- You must be connected to the instance as SYSOPER or SYSDBA. If connecting through an Oracle Net service name, it must be a dedicated server connection. For more information about connecting to the instance, see the CONNECT command.
- Using the STARTUP command with no arguments is equivalent to using the STARTUP OPEN command.
- If you do not use the FORCE option when you use the STARTUP command and the current database instance is running, an error results. The FORCE option is useful when you are debugging and when error conditions are occurring. Otherwise, it should not be used.
- Use the RESTRICT option to allow only Oracle users with the RESTRICTED SESSION system privilege to connect to the instance. Later, you can use the ALTER SYSTEM command to disable the restricted session feature.
- If you do not use the PFILE option to specify the initialization parameter file, the STARTUP command uses the default SPFILE server parameter file, if it exists. Else, it uses the default initialization parameter file. The default files are platform specific. For example:
  - On a UNIX system, the default initialization parameter file might be similar to the following:

    $*oracle_home*/DBS/INIT$*oracle_sid*.ORA

  - On a Windows system, the default initialization parameter file might be similar to the following:

%oracle_home%\DATABASE\INIT*ORCL*.ORA

See your operating system-specific documentation for more information about the default parameter files.

- Use the MOUNT option to mount a primary database or a logical standby database without opening it. If you do not specify a database name, the database name is taken from the initialization parameter DB_NAME.
- Use the OPEN option to mount and open the specified database.
- The NOMOUNT option starts the database instance without mounting the database. You cannot use the NOMOUNT option with the MOUNT or OPEN options.

Command Examples

Example 1

The following examples show two different methods for starting a database instance. Each command starts a database instance using the standard parameter file, mounts the default database in exclusive mode, and opens the database.

```
DGMGRL> STARTUP;
DGMGRL> STARTUP OPEN database;
```

Example 2

The following command shuts down the current instance, immediately restarts it without mounting or opening the database, and allows only users with restricted session privileges to connect to it.

```
DGMGRL > STARTUP FORCE RESTRICT NOMOUNT;
```

Example 3

The following command starts an instance using the parameter file testparm without mounting the database.

```
DGMGRL > STARTUP PFILE=testparm NOMOUNT;
```

Example 4

The following command shuts down a particular database, immediately restarts and opens it in parallel mode, allows access only users with restricted session privileges, and uses the parameter file MYINIT.ORA.

```
DGMGRL > STARTUP FORCE RESTRICT PFILE=myinit.ora SHARED OPEN database;
```

Example 5

The following example starts and mounts a database instance, but does not open it.

```
DGMGRL> STARTUP MOUNT;
```

SWITCHOVER

A switchover operation is a planned transition in which the primary site changes roles with one of the standby sites. When you issue the switchover command, the current primary site becomes a standby site, and the selected target standby site becomes the primary site.

Format

SWITCHOVER TO *site-name*;

Command Parameters

site-name
The name of the standby site that you want to change to the primary role.

Usage Notes

- If the standby site that is assuming the primary role contains a physical standby database, then both the primary and standby databases will be restarted after the `SWITCHOVER` operation completes. If the standby site contains logical standby databases, then neither the primary database nor the logical standby database is restarted.
- The broker verifies that the primary and standby sites and databases are in the following states prior to starting the switchover operation:
  - The primary site and database must be enabled and online, with log transport services started (READ-WRITE-XPTON substate).
  - If switching to a physical standby site, the site and database must be enabled and online, with log apply services started (PHYSICAL-APPLY-ON substate).
  - If switching to a logical standby site, the site and database must be enabled and online, with log apply services started (LOGICAL-APPLY-ON substate).
- The broker allows the switchover operation to proceed as long as there are no log transport services errors for the standby site that you selected to participate in the switchover operation. However, errors occurring for any bystanders will not prevent the switchover operation from proceeding.

Command Examples

Example 1

The following example shows a successful switchover in which the standby site, Standby2, transitions into the primary role.

```
DGMGRL> SWITCHOVER TO 'Standby2'
Performing switchover NOW. Please wait...
Operation requires restart of site "Primary"
Operation requires restart of site "Standby2"
Shutting down site Primary...
database not mounted
ORACLE instance shut down.
Shutting down site Standby2...
database not mounted
ORACLE instance shut down.
Restarting site Primary...
Restarting site Standby2...
Started "Primary" as standby
Started "Standby2" as new primary
Switchover succeeded. New primary is "Standby2"
```

Example 2

This switchover example shows a switchover operation that succeeded but returns an error because the CLI cannot shut down and start up the primary and standby databases.

```
DGMGRL> SWITCHOVER TO 'Standby2';
Performing switchover NOW. Please wait...
Operation requires restart of site "Primary"
Operation requires restart of site "Standby2"
Shutting down site Primary...
ORA-01031: insufficient privileges

You are no longer connected to ORACLE
Please connect again.
Unable to shut down Primary
You must restart site "Primary" manually.
You must restart site "Standby2" manually.
Switchover succeeded. New primary is "Standby2"
```

Note: For the CLI to restart instances automatically, you must connect to the database as SYSDBA using the username and password you specified in the remote password file before you begin the switchover operation. The username and password must be the same on the primary and standby databases.

You must manually issue the `SHUTDOWN` and `STARTUP` commands to restart the new primary and standby database instances in this configuration.

8

Database Resource Properties

Database resource properties help you to view and control the behavior of database resource objects, log transport services, and log apply services in a broker configuration. This chapter provides the following sections about the monitorable and configurable properties:

Section 8.1, "Monitorable (Read-Only) Properties for Database Resources"

Section 8.2, "Configurable Properties for Database Resources"

8.1 Monitorable (Read-Only) Properties for Database Resources

Monitorable properties allow you to view information related to resources, but you cannot change the values of these properties. You can view all of the monitorable properties using CLI `SHOW` commands.

> **Note:** Information for monitorable properties can be seen only when broker management of the database resource is enabled and in an online state. Data Guard Manager displays the information obtained from these properties on the Properties page, except for the `LsbySkipTable` and the `LsbySkipTxnTable` properties, which can be seen on the Data Guard Manager Properties page.

The following sections describe the database resource monitorable properties:

- InconsistentLogXptProps (Inconsistent Log Transport Properties)
- InconsistentProperties (Inconsistent Database Properties)
- LogXptStatus (Log Transport Status)

- LsbyFailedTxnInfo (Logical Standby Failed Transaction Information)
- LsbyParameters (Logical Standby Parameters)
- LsbySkipTable (Logical Standby Skip Table)
- LsbySkipTxnTable (Logical Standby Skip Transaction Table)
- SbyLogQueue (Standby Log Queue)
- SendQEntries (Send Queue Entries)

8.1.1 InconsistentLogXptProps (Inconsistent Log Transport Properties)

The `InconsistentLogXptProps` monitorable property returns a table that shows all properties related to log transport services whose values are inconsistent between the Data Guard configuration file and the actual value in the database.

Query this property on the primary database resource. The table contains the following columns:

1. `STANDBY_SITE_NAME`

   The name of the standby site that contains the database resource to which this log transport services property pertains.

2. `PROPERTY_NAME`

   The name of the log transport services property with an inconsistent value.

3. `DATABASE_VALUE`

   The corresponding value saved in the database server parameter file.

4. `SPFILE_VALUE`

   The corresponding value saved in the server parameter file (SPFILE).

5. `METADATA_VALUE`

   The value of the log transport services property saved in the Data Guard configuration file.

Note: In Oracle9*i* Data Guard Manager, information from `InconsistentLogXptProps` monitorable property is displayed on the Properties page for the database resource. The first column of the Properties page contains icons indicating a normal, error, or warning status for each property. If a property has an inconsistent property value, the first column will contain a triangular (yellow) warning icon. You can obtain further details about the warning by placing the mouse cursor over the warning sign.

8.1.2 InconsistentProperties (Inconsistent Database Properties)

The `InconsistentProperties` monitorable property returns a table that shows all database properties whose values contained in the Data Guard configuration file are inconsistent with the actual values in the database, and the values in the corresponding server parameter file (SPFILE) or the runtime values in the database.

Query this property on the each individual database resource. The table contains the following columns:

1. `PROPERTY_NAME`

   The name of the database property with the inconsistent value.

2. `DATABASE_VALUE`

   The corresponding runtime value being used in the database.

3. `SPFILE_VALUE`

   The corresponding value saved in the server parameter file (SPFILE).

4. `METADATA_VALUE`

   The value of the database property saved in the Data Guard configuration file.

Note: In Oracle9*i* Data Guard Manager, information from the `InconsistentProperties` monitorable property is displayed on the Properties page for the database resource. The first column of the Properties page contains icons indicating a normal, error, or warning status for each property. If a property has an inconsistent property value, the first column will contain a triangular (yellow) warning icon. You can obtain further details about the warning by placing the mouse cursor over the warning sign.

8.1.3 LogXptStatus (Log Transport Status)

The LogXptStatus property contains the error status of log transport services for each of the currently enabled standby sites. You query this property on the primary database resource.

The format of the error status is as follows:

```
"standby1_sitename=error_status, standby2_sitename=error_status,..."
```

The error status can be an empty string, which indicates there is no error.

In the following example, the string for Standby1 is empty because there is no error for the Standby1 destination. The standby2 destination returned the ORA-01034 message.

```
DGMGRL> SHOW RESOURCE VERBOSE 'Sales_db' 'LogXptStatus';
  LogXptStatus ='Standby1=,standby2=ORA-01034: ORACLE not available'
```

Note: In Oracle9*i* Data Guard Manager, information from the LogXptStatus property is displayed in the Log Transport Summary section of the General property page for the primary database resource.

8.1.4 LsbyFailedTxnInfo (Logical Standby Failed Transaction Information)

The LsbyFailedTxnInfo property identifies a failed transaction that caused log apply services to stop. This property contains a string with the following values from the DBA_LOGSTDBY_EVENTS view:

- XIDUSN: Transaction ID undo segment number
- XIDSLT: Transaction ID slot number
- XIDSQN: Transaction ID sequence number
- STATUS_CODE: Status (or Oracle error code) belonging to the STATUS message
- STATUS: Description of the current activity of the process, or the reason why log apply services stopped

The transaction IDs and status information are separated by a string of pound (###) signs.

8.1.5 LsbyParameters (Logical Standby Parameters)

The `LsbyParameters` property contains a string that identifies the `MAX_SGA` (maximum system global area) and `MAX_SERVERS` (maximum number of parallel query servers) specifically reserved for log apply services. The value contains the following information, separated by the "###" string:

- `MAX_SGA`
- `MAX_SERVERS`

8.1.6 LsbySkipTable (Logical Standby Skip Table)

The `LsbySkipTable` property returns a table with following columns from the `DBA_LOGSTDBY_SKIP` view:

- `ERROR`

  Indicates if the statement should be skipped or if errors should be returned for the statement

- `STATEMENT_OPT`

  Indicates the type of statement that should be skipped

- `SCHEMA`

  The schema name under which this skip option should be used

- `NAME`

  Name of the object for which this skip option should be used

- `PROCEDURE`

  Name of the stored procedure to execute when processing the skip option

- `ACTIVE`

  The table separates the column information with the "###" string.

8.1.7 LsbySkipTxnTable (Logical Standby Skip Transaction Table)

The `LsbySkipTxnTable` property returns a table with following columns:

- `XIDUSN:` Transaction ID undo segment number
- `XIDSLT:` Transaction ID slot number
- `XIDSQN:` Transaction ID sequence number

- ACTIVE: Description of the current activity of the process, or the reason why log apply services stopped

8.1.8 SbyLogQueue (Standby Log Queue)

The SbyLogQueue property returns a table that indicates all logs that were received by the standby site, but have not yet been applied. If no rows are returned, it implies all logs received have been applied. The table contains the following columns in the order shown:

- LOG_SEQ

  The log sequence number

- TIME_GENERATED

  The time when the log was generated

- TIME_COMPLETED

  The time when the log was completed

For example:

```
DGMGRL> SHOW RESOURCE VERBOSE 'reportingdb' 'SbyLogQueue';
STANDBY_RECEIVE_QUEUE
             LOG_SEQ  TIME_GENERATED       TIME_COMPLETED
                   6  11/21/2000 10:57:16  11/21/2000 10:57:41
                   7  11/21/2000 10:57:41  11/21/2000 10:57:43
                   8  11/21/2000 10:57:43  11/21/2000 10:57:49
```

In Data Guard Manager, this information is displayed on the Log Files property page.

8.1.9 SendQEntries (Send Queue Entries)

The SendQEntries property returns a table that shows all log files on the primary site that have not yet been successfully shipped to one or more standby sites. Query this property on a standby database resource. Query this property on the primary database resource. The table contains the following columns:

- SITE_NAME

  The value can be empty or it can contain the name of the site. If empty, the STATUS column will contain a value of CURRENT or NOT_ARCHIVED.

- STATUS

The STATUS column is set to one of the following values:

- CURRENT: A log file to which online redo is being written currently.
- NOT_ARCHIVED: A completed online redo log file that has not been archived locally.
- ARCHIVED: A completed log file that has been archived locally but has not been shipped to the standby site specified in the SITE_NAME column.

The table contains exactly one row with the value of STATUS=CURRENT. There can be multiple rows with the value STATUS=ARCHIVED or STATUS=NOT_ARCHIVED.

- LOG_SEQ

  The log sequence number. Multiple rows may have the same LOG_SEQ value (for different SITE_NAME values).

- TIME_GENERATED

  The time when the log was generated.

- TIME_COMPLETED

  The time when the log was completed.

For example, the following shows output from a SHOW RESOURCE VERBOSE command:

```
DGMGRL> SHOW RESOURCE VERBOSE 'db' 'SendQEntries';
PRIMARY_SEND_QUEUE
SITE_NAME    STATUS              LOG_SEQ    TIME_GENERATED       TIME_COMPLETED
Standby      ARCHIVED             9         11/21/2001 10:57:49  11/21/2001 10:59:42
Standby      ARCHIVED            10         11/21/2001 10:59:42  11/21/2001 10:59:43
Standby      ARCHIVED            11         11/21/2001 10:59:43  11/21/2001 10:59:49
Standby      ARCHIVED            12         11/21/2001 10:59:49  11/21/2001 10:59:54
             CURRENT             13         11/21/2001 10:59:54
```

Note: In Oracle9*i* Data Guard Manager, information from the SendQEntries property is displayed on the Log Files property page for the primary database resource.

8.2 Configurable Properties for Database Resources

The configurable properties include the following:

Alternate

ApplyNext
ApplyNoDelay
ApplyParallel
ArchiveLagTarget
AsyncBlocks
Binding
DbFileNameConvert
DelayMins
Dependency
LogArchiveFormat
LogArchiveMaxProcesses
LogArchiveMinSucceedDest
LogArchiveTrace
LogFileNameConvert
LogShipping
LogXptMode
LsbyASkipCfgPr
LsbyASkipErrorCfgPr
LsbyASkipTxnCfgPr
LsbyDSkipCfgPr
LsbyDSkipErrorCfgPr
LsbyDSkipTxnCfgPr
LsbyMaxEventsRecorded
LsbyMaxSga
LsbyMaxServers
LsbyRecordAppliedDdl
LsbyRecordSkipDdl
LsbyRecordSkipErrors
LsbyTxnConsistency
MaxFailure
ReopenSecs
StandbyArchiveDest
StandbyFileManagement

See Also: Section 1.6.3 for more information about database property management

Note: When a broker configuration is created and standby sites are added to the configuration, the broker imports existing settings for the database to set many of the properties. If importing an existing setting fails, or if a property value is not imported, then the broker uses a broker default value. The default values and whether or not a property is imported is indicated within each property description.

Alternate

Updates the ALTERNATE attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter. With this property, you specify the name of the site to which log transport services should ship archived redo logs in case there is a problem shipping to the current site. The broker also updates the setting of the LOG_ARCHIVE_DEST_STATE_*n* initialization parameter to the specified ALTERNATE site.

Datatype	String
Valid Values	Site name (except for the primary site and the standby site itself)
Broker Default	Empty string
Imported?	No
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical and logical
Corresponds to	■ ALTERNATE attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter ■ ALTERNATE column of the V$ARCHIVE_DEST view

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* and LOG_ARCHIVE_DEST_STATE_*n* values in the initialization parameter file for the primary database.

For example, if you are managing a configuration with the CLI you would issue the following SQL statement to set the standby site 'Chicago' to be an alternate site for the standby site 'San Francisco' with database 'reportingdb':

```
SQL> ALTER RESOURCE 'reportingdb' ON SITE 'San Francisco' SET PROPERTY
```

```
> 'Alternate' = 'Chicago';
```

ApplyNext

Specifies the number of archived redo logs that log apply services should apply immediately to the physical standby database, temporarily overriding any previously specified apply delay interval. The `ApplyNext` property value is applied only at the point when you explicitly specify that value. Once the value is applied, the property no longer has any effect until the next time that its value is explicitly specified.

Specifying a value for this property has no effect and will be ignored if management of the standby database is disabled or if the log apply services are offline at the time that a value is specified.

Datatype	Integer
Valid Values	>=0 logs
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Physical
Corresponds to	`ALTER DATABASE RECOVER MANAGED STANDBY DATABASE NEXT 2`

Note: Oracle9*i* Data Guard Manager obtains information from the `ApplyNext` property and displays it on the Log Files property page for the standby database resource. The Log Files property page shows information about archived redo logs that have not been applied to the standby site.

ApplyNoDelay

Specifies whether or not to cancel the delay option that has been set on the primary database or on the standby database:

- If log apply services are online and you set `ApplyNoDelay=YES`, then log apply services apply the archived redo logs as soon as they have been archived

to the standby site. This property is equivalent to using the following SQL statement:

```
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE NODELAY;
```

- If log apply services are online and you set `ApplyNoDelay=NO`, then log apply services respect the delay settings specified by the DelayMins property of the standby database. This property is equivalent to using the following SQL statement:

  ```
  ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DEFAULT DELAY;
  ```

- If log apply services are offline, then setting the property has no immediate effect. However, when log apply services are online again, the value of the property is used to determine the mode of log apply services.

Datatype	String
Valid Values	YES or NO
Broker Default	NO
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Physical
Corresponds to	YES=ALTER DATABASE RECOVER MANAGED STANDBY DATABASE NODELAY NO=ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DEFAULT DELAY

The value of the `ApplyNoDelay` property persists through role changes. For example, if the `ApplyNoDelay` property is set to Yes and then the site undergoes a series of switchover operations, transitioning the database from the standby role to the primary role and then back again, the `ApplyNoDelay` property will continue to be set to Yes throughout all of the role changes.

ApplyParallel

Specifies the number of concurrent processes log apply services can use on the physical standby database for managed recovery. If log apply services are offline, then setting the property has no immediate effect. However, when log apply

services are online again, the value of the property is used to determine the mode of log apply services.

Datatype	Integer
Valid Values	>=1
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Physical
Corresponds to	`ALTER DATABASE RECOVER MANAGED STANDBY DATABASE PARALLEL...`

ArchiveLagTarget

Updates the ARCHIVE_LAG_TARGET initialization parameter setting. This property limits the amount of data that can be lost and effectively increases the availability of the standby database by forcing a log switch after the amount of time you specify (in seconds) elapses. That way, the standby database will not miss redo records generated from a time range longer than the value set for the ARCHIVE_LAG_TARGET initialization parameter.

Datatype	Number
Valid Values	Seconds (either 0 seconds, or any number from 60 to 7200 seconds)
Broker Default	0
Imported?	Yes, from the ARCHIVE_LAG_TARGET initialization parameter
Parameter Class	Dynamic
Role	Primary
Standby Type	Not applicable
Corresponds to	ARCHIVE_LAG_TARGET=*seconds* initialization parameter

AsyncBlocks

Specifies the size of the SGA buffer to be used when network I/O operations are to be done asynchronously using the log writer process (LGWR). The value you set for

AsyncBlocks property takes effect only when the LogXptMode property is set to ASYNC.

Datatype	Integer
Valid Values	0 to 20,480 blocks
Broker Default	2048
Imported?	Yes, from the ASYNCH_BLOCKS column of the V$ARCHIVE_DEST view
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical and logical
Corresponds to	■ ASYNC attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter ■ ASYNCH_BLOCKS column of the V$ARCHIVE_DEST view

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

Binding

Specifies whether or not the standby destination is mandatory or optional.

Datatype	String
Valid Values	MANDATORY or OPTIONAL
Broker Default	OPTIONAL
Imported?	Yes, from the BINDING column of the V$ARCHIVE_DEST view
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical and logical
Corresponds to	■ MANDATORY and OPTIONAL attributes for the LOG_ARCHIVE_DEST_*n* initialization parameter ■ BINDING column of the V$ARCHIVE_DEST view

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

DbFileNameConvert

Distinguishes standby datafile filenames from primary datafile filenames. You must set this property on all standby databases. If you add a datafile to the primary database, you must add a corresponding file to the standby database. When the standby database is updated, this property converts the datafile name on the primary database to the datafile name on the standby database. The file on the standby database must exist and be writable, or the recovery process will halt with an error.

Datatype	String
Valid Values	Set the value of this parameter to two strings: 1. The pattern found in the datafile names on the primary database 2. The pattern found in the datafile names on the standby database DB_FILE_NAME_CONVERT = [(]'string1', 'string2', 'string3', 'string4',...[)] Where: ■ string1 is the pattern of the primary database filename. ■ string2 is the pattern of the standby database filename. ■ string3 is the pattern of the primary database filename. ■ string4 is the pattern of the standby database filename.
Broker Default	' ',' '
Imported?	Yes, from the DB_FILE_NAME_CONVERT initialization parameter
Parameter Class	Static
Role	Standby
Standby Type	Physical
Corresponds to	DB_FILE_NAME_CONVERT initialization parameter

DelayMins

Specifies the number of minutes log apply services will delay applying the archived redo logs on the standby database.

Datatype	Integer
Valid Values	>= 0
Broker Default	0
Imported?	Yes, from the DELAY_MINS column of the V$ARCHIVE_DEST view
Parameter Class	Dynamic
Role	Standby
Standby Type	Physical and logical
Corresponds to	■ DELAY attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter ■ DELAY_MINS column of the V$ARCHIVE_DEST view

Dependency

Specifies the dependency attribute for the LOG_ARCHIVE_DEST_*n* parameter. The site name (can be the primary or a standby site name) on which this site depends for receiving archived redo logs.

Datatype	String
Valid Values	Site name, except for the standby site itself or you can set this property to null.
Broker Default	Empty string
Imported?	No
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical or logical
Corresponds to	Dependency attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

LogArchiveFormat

Specifies the format for filenames of archived redo log files.

Datatype	String
Valid Values	Same as for the LOG_ARCHIVE_FORMAT initialization parameter.
Broker Default	Empty string
Imported?	Yes, from the LOG_ARCHIVE_FORMAT initialization parameter
Parameter Class	Static
Role	Primary and standby
Standby Type	Physical and logical
Corresponds to	LOG_ARCHIVE_FORMAT initialization parameter

LogArchiveMaxProcesses

Specifies the number of archiver background processes (ARC0 through ARC9) the Oracle database server initially invokes. The actual number of archiver processes in use may vary subsequently based on archive workload.

Datatype	Integer
Valid Values	1 to 10
Broker Default	2
Imported?	Yes, from the LOG_ARCHIVE_MAX_PROCESSES initialization parameter
Parameter Class	Dynamic
Role	Primary and standby
Standby Type	Physical and logical
Corresponds to	LOG_ARCHIVE_MAX_PROCESSES initialization parameter

LogArchiveMinSucceedDest

Defines the minimum number of destinations that must succeed for the online log file to be available for reuse.

Datatype	Integer

Valid Values	1 to 10
Broker Default	1
Imported?	Yes, from the LOG_ARCHIVE_MIN_SUCCEED_DEST initialization parameter
Parameter Class	Dynamic
Role	Primary
Standby Type	Not applicable
Corresponds to	LOG_ARCHIVE_MIN_SUCCEED_DEST initialization parameter

LogArchiveTrace

Set this parameter to an integer value to see the progression of the archiving of redo logs on the primary and the standby sites. Oracle database server writes an audit trail of the archived logs received from the primary database into a trace file.

Datatype	Integer
Valid Values	The valid values have the following meanings: 0: Disable archivelog tracing 1: Track archival of redo log file 2: Track archival status of each archivelog destination 4: Track archival operational phase 8: Track archivelog destination activity 16: Track detailed archivelog destination activity 32: Track archivelog destination parameter modifications 64: Track ARCn process state activity 128: Track FAL (fetch archived log) server related activities 256: Supported in a future release 512: Tracks asynchronous LGWR activity 1024 RFS physical client tracking 2048 ARC*n* / RFS heartbeat tracking
Broker Default	255
Imported?	Yes, from the LOG_ARCHIVE_TRACE initialization parameter

Parameter Class	Dynamic
Role	Primary and standby
Standby Type	Physical and logical
Corresponds to	LOG_ARCHIVE_TRACE initialization parameter

LogFileNameConvert

Converts the filename of a new log file on the primary database to the filename of a log file on the standby database. If you add a log file to the primary database, you must add a corresponding file to the standby database.

Datatype	String
Valid Values	A list of an even number of strings, separated by commas. `LOG_FILE_NAME_CONVERT = [(]'string1', 'string2', 'string3', 'string4',...[)]` Where: ■ `string1` is the pattern of the primary database filename ■ `string2` is the pattern of the standby database filename ■ `string3` is the pattern of the primary database filename ■ `string4` is the pattern of the standby database filename
Broker Default	' ',' '
Imported?	Yes, from the LOG_FILE_NAME_CONVERT initialization parameter
Parameter Class	Static
Role	Standby
Standby Type	Physical standby
Corresponds to	LOG_FILE_NAME_CONVERT initialization parameter

LogShipping

Specifies whether or not log transport services can send archived redo logs to the particular standby database. The broker uses the value of the LogShipping property only when the primary database is in READ-WRITE-XPTON state:

- If the primary database is in the READ-WRITE state, then log transport services are offline to all standby sites, regardless of whether or not the LogShipping property is set to on or off.
- If the primary database is in READ-WRITE-XPTON state and the value of the LogShipping property is ON, then log transport services are enabled to send archived redo logs to the particular standby site. If the LogShipping property is OFF, then log transport services are disabled to send archived redo logs to the particular standby site.

Datatype	String
Valid Values	ON or OFF
Broker Default	ON
Imported?	No
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical and logical
Corresponds to	The ENABLE and DEFER values for the LOG_ARCHIVE_DEST_ STATE_n initialization parameter

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

LogXptMode

Allows you to set the data protection mode for log transport services. You set the log transport services on each standby database to one of the following modes:

- SYNC

  Configures the log transport services to this standby using the LGWR, SYNC, AFFIRM settings. If this is a physical standby database, standby redo logs are required. If this is a logical standby database, standby redo logs are not required because logical standby databases do not use them. This mode provides the highest grade of data protection and potentially a correspondingly high impact on primary database performance.

- ASYNC

Configures the log transport services to this standby using the LGWR, ASYNC, NOAFFIRM settings. Also, standby redo logs are required for physical standby databases; they are not required for logical standby databases. This mode provides the next highest grade of data protection with a correspondingly lower impact on primary database performance.

- ARCH

  Configures the log transport services to this standby database using the ARCH setting. Standby redo logs are not required. This is the default setting.

  This mode provides the lowest grade of data protection and the least impact on primary database performance of the 3 options.

Datatype	String
Valid Values	SYNC or ASYNC or ARCH
Broker Default	■ ASYNC for logical standby databases ■ ASYNC for physical standby databases with standby redo logs ■ ARCH for physical standby databases without standby redo logs
Imported?	Yes, from the ARCHIVER, TRANSMIT_MODE, AFFIRM column of V$ARCHIVE_DEST view
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical or logical
Corresponds to	ARCH, LGWR, SYNC, ASYNC, AFFIRM, NOAFFIRM attributes for the LOG_ARCHIVE_DEST_*n* initialization parameter. ARCHIVER, TRANSMIT_MODE, AFFIRM column of V$ARCHIVE_DEST view

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

See Also: Chapter 4 for more information about setting data protection modes for log transport services

LsbyASkipCfgPr

Provides a way to apply specific SQL statements and *skip* (ignore) SQL statements that you do not want applied to the logical standby database. The SKIP procedure:

- Sets the criteria for identifying the SQL statements that will not be applied to the standby database
- Specifies any additional processing that will be done, if necessary

This property is used only when you explicitly update its value. The property will not be reused when you enable the database for management by the broker.

Datatype	String
Valid Values	A valid set of arguments to the DBMS_LOGSTDBY.SKIP procedure.
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.SKIP procedure

Note: Data Guard Manager uses the LsbySkipTable property to represent the LsbyASkipCfgPr, LsbyDSkipCfgPr, LsbyASkipErrorCfgPr, and LsbyDSkipErrorCfgPr properties.

LsbyASkipErrorCfgPr

Provides criteria to determine if an error should cause log apply services to stop. All errors to be skipped are stored in system tables that describe how exceptions should be handled. This property is used only when you explicitly update its value. The property will not be reused when you enable the database for management by the broker.

Datatype	String

Valid Values	A valid set of arguments to the DBMS_LOGSTDBY.SKIP_ERROR procedure. The string must contain comma separators between the arguments.
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.SKIP_ERROR procedure

Note: Data Guard Manager uses the LsbySkipTable property to represent the LsbyASkipCfgPr, LsbyDSkipCfgPr, LsbyASkipErrorCfgPr, and LsbyDSkipErrorCfgPr properties.

LsbyASkipTxnCfgPr

Skips over a transaction that caused the log apply services to stop applying transactions to the logical standby database. This property allows you to specify the transaction ID (XIDSQN NUMBER) of the problematic transaction that you want log apply services to ignore. Before you restart log apply services, you should take some corrective action, such as providing a compensating transaction. This will help avoid data divergence between the primary and logical standby databases that might result from skipping the problematic transaction. This property is used only when you explicitly update its value. The property will not be reused when you enable the database for management by the broker.

Datatype	String
Valid Values	A valid set of arguments to the DBMS_LOGSTDBY.SKIP_ TRANSACTION procedure. Use comma separators between the arguments.
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby

Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.SKIP_TRANSACTION procedure

Note: Data Guard Manager uses the LsbySkipTxnTable property to represent the LsbyASkipTxnCfgPr and LsbyDSkipTxnCfgPr properties.

LsbyDSkipCfgPr

Reverses the actions of the LsbyASkipCfgPr property by finding the record, matching all the parameters, and removing the record from the system table. The match must be exact, and multiple *skip* actions can be undone only by a matching number of *unskip* actions. You cannot undo multiple skip actions using wildcard characters. The property will not be reused when you enable the database for management by the broker.

Datatype	String
Valid Values	A valid set of arguments to the DBMS_LOGSTDBY.UNSKIP procedure
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.UNSKIP procedure

Note: Data Guard Manager uses the LsbySkipTable property to represent the LsbyASkipCfgPr, LsbyDSkipCfgPr, LsbyASkipErrorCfgPr, and LsbyDSkipErrorCfgPr properties.

LsbyDSkipErrorCfgPr

Reverses or undoes the actions of the LsbyASkipErrorCfgPr property by finding the record, matching all of the parameters, and removing the record from the

system table. The match must be exact, and multiple *skip* actions can be undone only by a matching number of *unskip* actions. You cannot undo multiple skip actions with just one unskip procedure call. The property will not be reused when you enable the database for management by the broker.

Datatype	String
Valid Values	A valid set of arguments to the DBMS_LOGSTDBY.UNSKIP_ERROR procedure. The string must contain comma separators between the arguments.
Broker Default	Not applicable
Imported?	No
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.UNSKIP_ERROR procedure

Note: Data Guard Manager uses the LsbySkipTable property to represent the LsbyASkipCfgPr, LsbyDSkipCfgPr, LsbyASkipErrorCfgPr, and LsbyDSkipErrorCfgPr properties.

LsbyDSkipTxnCfgPr

Reverses the actions of the LsbyASkipTxnCfgPr property. The transaction IDs must match exactly, and multiple *skip transaction* actions can be undone only by a matching number of *unskip transaction* actions. You cannot undo multiple skip transaction actions with just one unskip transaction procedure call. The property will not be reused when you enable the database for management by the broker.

Datatype	String
Valid Values	A valid set of arguments to the DBMS_LOGSTDBY.UNSKIP_TRANSACTION procedure
Broker Default	Not applicable
Imported?	No

Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.UNSKIP_TRANSACTION procedure

Note: Data Guard Manager uses the LsbySkipTxnTable property to represent the LsbyASkipTxnCfgPr and LsbyDSkipTxnCfgPr properties.

LsbyMaxEventsRecorded

Specifies the number of events that will be stored in the DBA_LOGSTDBY_EVENTS table, which stores logical standby event information.

Datatype	Integer
Valid Values	>=0
Broker Default	0
Imported?	Yes, from the MAX_EVENTS_RECORDED row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('MAX_EVENTS_RECORDED') and the DBMS_LOGSTDBY.APPLY_UNSET('MAX_EVENTS_RECORDED') procedures

LsbyMaxSga

Specifies the number of megabytes for the system global area (SGA) allocation for log apply services cache. The default value is one quarter of the value set for the SHARED_POOL_SIZE initialization parameter.

Datatype	Integer
Valid Values	>=0

Broker Default	0
Imported?	Yes, from the MAX_SGA row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('MAX_SGA') and the DBMS_LOGSTDBY.APPLY_UNSET('MAX_SGA') procedures

LsbyMaxServers

Specifies the number of parallel query servers specifically reserved for log apply services. By default, log apply services use all available parallel query servers to read the log files and apply changes.

Datatype	Integer
Valid Values	>=0
Broker Default	0
Imported?	Yes, from the MAX_SERVERS row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('MAX_SERVERS') and the DBMS_LOGSTDBY.APPLY_UNSET('MAX_SERVERS') procedures

LsbyRecordAppliedDdl

Controls whether or not DDL statements that have been applied to the logical standby database are recorded in the DBA_LOGSTDBY_EVENTS table. Specify one of the following values:

- TRUE: Indicates that DDL statements applied to the logical standby database are recorded in the DBA_LOGSTDBY_EVENTS table. This is the default parameter setting.

- FALSE: Indicates that applied DDL statements are not recorded.

Datatype	String
Valid Values	TRUE or FALSE or NULL
Broker Default	NULL
Imported?	Yes, from the RECORD_APPLIED_DDL row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('RECORD_APPLIED_DDL') and the DBMS_LOGSTDBY.APPLY_UNSET('RECORD_APPLIED_DDL') procedures

LsbyRecordSkipDdl

Controls whether or not skipped DDL statements are recorded in the DBA_LOGSTDBY_EVENTS table. Specify one of the following values:

- TRUE: Skipped DDL statements are recorded in the DBA_LOGSTDBY_EVENTS table. This is the default parameter setting.
- FALSE: Skipped DDL statements are not recorded in the DBA_LOGSTDBY_EVENTS table.

Datatype	String
Valid Values	TRUE or FALSE or NULL
Broker Default	NULL
Imported?	Yes, from the RECORD_SKIP_DDL row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('RECORD_SKIP_DDL') and the DBMS_LOGSTDBY.APPLY_UNSET('RECORD_SKIP_DDL') procedures

LsbyRecordSkipErrors

Controls whether skipped errors (as described by the DBMS_LOGSTDBY.SKIP_ERROR procedure) are recorded in the DBA_LOGSTDBY_EVENTS table. Specify one of the following values:

- TRUE—Skipped errors are recorded in the DBA_LOGSTDBY_EVENTS table.
- FALSE—Skipped errors are not recorded in the DBA_LOGSTDBY_EVENTS table.

Datatype	String
Valid Values	TRUE or FALSE or NULL
Broker Default	NULL
Imported?	Yes, from the RECORD_SKIP_ERRORS row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('RECORD_SKIP_ERRORS') and the DBMS_LOGSTDBY.APPLY_UNSET('RECORD_SKIP_ERRORS') procedures

LsbyTxnConsistency

Level of transaction consistency maintained between the primary and standby databases. Specify one of the following values:

- FULL: Transactions are applied to the logical standby database in the exact order in which they were committed on the primary database. This option results in the lowest performance.
- READ_ONLY: Transactions are committed out of order (which provides better performance), SQL SELECT statements return read-consistent results. This is particularly beneficial when the logical standby database is being used to generate reports. **Note:** DML statements involving standby tables are not allowed in this mode.
- NONE: Transactions are committed out of order, and no attempt is made to provide read-consistent results. This results in the best performance of the three modes. If applications that are reading the logical standby database make no assumptions about transaction order, this option works well.

Datatype	String
Valid Values	FULL or READ_ONLY or NONE
Broker Default	None
Imported?	Yes, from the TRANSACTION_CONSISTENCY row of system.LOGSTDBY$PARAMETERS
Parameter Class	Not applicable
Role	Standby
Standby Type	Logical standby
Corresponds to	DBMS_LOGSTDBY.APPLY_SET('TRANSACTION_CONSISTENCY') and the DBMS_LOGSTDBY.APPLY_UNSET('TRANSACTION_CONSISTENCY') procedures

MaxFailure

Specifies the maximum number of contiguous archival failures before the log transport services stop trying to transport archived redo logs to the standby database. A value of zero indicates that an unlimited number of failures are allowed.

Datatype	Integer
Valid Values	>=0
Broker Default	0
Imported?	Yes, from the MAX_FAILURE column of V$ARCHIVE_DEST view
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical and logical
Corresponds to	■ MAX_FAILURE attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter ■ MAX_FAILURE column of the V$ARCHIVE_DEST view

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

ReopenSecs

Specifies the minimum number of seconds before the archiver process (ARC*n*, foreground, or log writer process) should try again to access a previously failed destination.

Datatype	Integer
Valid Values	>=0 seconds
Broker Default	0
Imported?	Yes, from the REOPEN_SECS column of V$ARCHIVE_DEST view
Parameter Class	Dynamic
Role	Standby[1]
Standby Type	Physical and logical
Corresponds to	■ REOPEN attribute for the LOG_ARCHIVE_DEST_*n* initialization parameter ■ REOPEN_SECS column of the V$ARCHIVE_DEST view

[1] Although this property is set for the standby database, it is indirectly related to the log transport services for the primary database. The broker reconciles the setting you specify on the standby database with the LOG_ARCHIVE_DEST_*n* value in the initialization parameter file for the primary database.

StandbyArchiveDest

Updates the file specification for the STANDBY_ARCHIVE_DEST initialization parameter. Specifies the location of archived redo logs arriving from a primary database. You can set this property to null.

Datatype	String
Valid Values	File specification of the location of archived redo logs on the standby site
Broker Default	0
Imported?	Yes, from the STANDBY_ARCHIVE_DEST initialization parameter
Parameter Class	Dynamic
Role	Standby
Standby Type	Physical or logical

Corresponds to	STANDBY_ARCHIVE_DEST initialization parameter

StandbyFileManagement

Updates the STANDBY_FILE_MANAGEMENT initialization parameter setting. Set this property on each standby site to indicate whether or not the filenames on the standby database are the same as those used on the primary database. Set this parameter to AUTO only if the COMPATIBILITY parameter is set to 9.0.*n* or higher.

Datatype	String
Valid Values	AUTO or MANUAL
Broker Default	MANUAL
Imported?	Yes, from the STANDBY_FILE_MANAGEMENT initialization parameter
Parameter Class	Dynamic
Role	Standby
Standby Type	Physical or logical
Corresponds to	STANDBY_FILE_MANAGEMENT initialization parameter

Glossary

broker

A distributed management framework that automates and simplifies most of the complex operations required to create, control, and monitor a Data Guard configuration.

broker configuration

A hierarchical and logical grouping of the sites and database resources (including log transport services and log apply services) in a Data Guard configuration.

See also Data Guard configuration.

bystander

A standby site including its database that is configured in a Data Guard configuration when a failover or switchover operation occurs, but is not involved in the role transition. That is, a bystander retains its standby role throughout the failover or switchover operation. Management of a bystander and its associated standby database can be enabled or disabled, and its state can be set to online or offline.

configuration object

A named collection of sites and the resource objects that those sites contain. It is an abstraction of an actual Data Guard configuration.

database resource object

A named object that corresponds to a primary or standby database instance. The broker uses this object to manage and control the state of a single database and to associate properties with the database.

Data Guard configuration

A distributed computing system that prevents or minimizes losses due to unplanned events (for example, human errors, environmental disasters, or data corruption) as well as to planned downtime (such as for routine maintenance tasks).

See also broker configuration.

Data Guard environment

The physical configuration of the primary and standby databases. The environment depends on many factors, including the:

- Number of standby databases associated with a primary database
- Number of host machines used by the databases
- Directory structures of the machines used by the databases
- Network configuration
- Log transport services
- Log apply services

The standby database environment can be managed manually by a DBA, automatically using Data Guard Manager or the Data Guard CLI, or a combination of all of these.

default state

The initial runtime state in which the object will run when you enable management of the configuration. For a database resource, the actual default state can vary depending on the role (primary or standby) in which the database resource is currently running.

See also intended state.

failover

Failover changes one of the standby sites and its databases into the role of primary site and primary database.

intended state

The runtime state of an object while it is enabled for management by the broker.

See also default state.

logical standby database

A logical standby database takes standard Oracle archived redo logs, transforms them back into SQL transactions, and then applies them to an open standby database. Although changes can be applied concurrently with end user access, the tables being maintained through regenerated SQL transactions allow read-only access to users of the logical standby database. Because the database is open, it is physically different from the primary database. The database tables can have different indexes, and physical characteristics from their primary database peers, but must maintain logical consistency from an application access perspective, to fulfill their role as a standby data source.

physical standby database

A physical standby database is physically identical to the primary database. While the primary database is open and active, a physical standby database is either performing recovery (by applying logs), or open for reporting access. A physical standby database can be queried read-only when not performing recovery while the production database continues to ship redo data.

primary database

A production database from which one or more standby databases is created and maintained. Every standby database is associated with one and only one primary database. A single primary database can, however, support multiple standby databases.

primary site

The location of the primary database. This is the site in a Data Guard configuration from which the database is available to applications and from where the data is shipped.

read-only mode

A physical standby database mode that is initiated using the following SQL statement:

```
ALTER DATABASE OPEN READ ONLY;
```

The read-only mode allows you to query a physical standby database, but does not allow you to make changes to it. While in this mode, redo logs are archived but are not applied until the physical standby database reenters managed recovery mode.

resource

A physical or logical component that is available to a computing system. Most commonly, a resource is an Oracle database server.

These resources are categorized by type and can include an Oracle database server resource and other services upon which these items depend. The various resource types are each separately managed on a given Data Guard configuration by a resource guard. Resource guards are registered with Data Guard broker during configuration.

resource guard

A component that acts as an interface between Data Guard broker and resources in a Data Guard configuration. Its jobs include registering resources with Data Guard broker, taking resources online and offline, reporting status for resources, translating parameter changes that affect resources, and conveying messages to resources.

site

A managed unit of failover in a Data Guard configuration. A database is replicated across a set of sites, one replicant per site. Dependent applications are instantiated on a site. When a site holding a primary role fails, another site holding the standby role transitions to the primary role and provides the desired service to users. Sites may be one of several types of nodes, which vary from one another in the degree of hardware complexity and software management.

site object

A named collection of database resource objects that reside on a single host.

standby database

A copy of a production database created using a backup of your primary database. Standby databases are kept synchronized with the primary database by applying archived redo logs over time from the primary database to each standby database. The standby database can take over processing from the primary database, providing nearly continuous database availability. A standby database has its own initialization parameter file, control file, and datafiles.

See also logical standby database and physical standby database.

standby site

The location of the standby database. One or more server systems can serve as hosts for standby databases. The standby systems accept redo logs shipped from the

primary site and apply changes to local copies of the database. The standby site can be on the same host system as the primary database or on a separate host system.

Index

A

Add Site wizard, 1-7, 5-21
adding
  existing standby database to a broker configuration, 5-10
  standby site to the broker configuration, 6-5
alert logs
  displaying, 7-46
ALTER CONFIGURATION command, 7-7, 7-10
  example, 6-9
ALTER RESOURCE (property) command, 7-11
  example, 6-10
ALTER RESOURCE (state) command, 7-14
  example, 6-10
ALTER SITE command, 7-16
  example, 6-10
ALTER SYSTEM statement
  starting the broker, 2-6, 6-2
altering
  properties
    database resource, 6-10, 7-11
  protection modes
    configuration, 7-7
  states
    configuration, 6-9, 7-7, 7-10
    resource, 6-10, 7-14
    site, 6-10
  See also each ALTER command
Alternate property, 8-9
application integration, 1-4
Apply Off substate
  logical standby databases, 4-3
  physical standby databases, 4-3
ApplyNext property, 8-10
ApplyNoDelay property, 8-10
ApplyParallel property, 8-11
ARCH log transport mode, 4-11
architecture
  Data Guard broker, 1-6
ARCHIVE_LAG_TARGET initialization parameter
  setting in a broker configuration, 8-12
archived redo logs
  default database resource substates, 2-11, 4-2
  destination and configuration parameters, 2-2
  in a Data Guard configuration, 2-2
  primary database setup, 1-15
ASYNC log transport mode, 4-11
AsyncBlocks property, 8-12

B

background processes
  DMON, 1-10
banners
  suppressing from DGMGRL command-line interface output, 7-1
before you perform a switchover operation, 3-4
benefits
  Data Guard broker, 1-2
binary configuration file, 1-10, 1-12
Binding property, 8-13
broker
  components, 1-6
  configuration dependencies, 3-2
  Data Guard configuration file, 1-12
  forced failover operations, 3-10
  graceful failover operations, 3-9

installation, 1-15
introduction, 1-1
log transport services verification, 1-3
managing database resources, 4-1
managing site resources, 3-1
performing failover operations, 3-9
performing switchover operations, 3-5
user interfaces, 1-2, 1-7
broker configurations, 2-22
benefits, 1-2
components, 2-1
creating, 5-6 to 5-17, 5-18, 6-3, 7-21
Data Guard configuration file, 1-10
dependencies, 1-5, 4-1
disabling a database resource, 7-27, 7-28, 7-29
displaying dependencies, 7-44
enabling, 2-8, 6-14, 7-30, 7-31, 7-33
health, 1-10, 2-15
importing standby databases, 1-7
life cycle, 2-6
management, 1-4, 1-7, 1-9, 1-12
objects, 1-4, 2-3
Oracle Net configuration, 1-3, 1-8
overview, 2-1
properties, 2-12, 2-15
protection modes, 7-7
state transitions, 2-12, 7-10
states, 7-10, 7-25
status modes, 2-14
supported, 1-5, 2-1

C

changing
properties
database resources in a broker configuration, 4-6
states
database resources in a broker configuration, 4-3, 7-11, 7-14
of a standby site in a broker configuration, 5-26
of objects in a broker configuration, 6-9
See also altering
command prompts
suppressing from DGMGRL command-line interface output, 7-1
common properties, 2-16
COMPATIBLE initialization parameter
requirements for setting, 1-15
components
broker, 1-6
Data Guard configuration, 2-2
configurable properties, 2-15
database, 4-6, 8-7
related to initilaization parameters, 4-7
related to log apply services, 4-7
related to log transport services, 4-7
related to SQL apply services, 4-8
configuration file
See Data Guard configuration file
configurations
dedicated server process, 7-5
types of objects, 1-5
configuring
database resource properties, 7-11
Oracle Net for a broker configuration, 6-2
properties, 2-15
CONNECT command, 6-3
connecting
privileges required for Data Guard broker configurations, 7-5
to the primary database, 6-3
console log
displaying, 7-46
controlling
configuring log transport services for data protection, 4-10
CREATE CONFIGURATION command, 6-4, 7-21
Create Configuration wizard
definition, 1-7
introduction, 1-7
CREATE SITE command, 7-24
creating
a broker configuration, 5-6, 5-18, 6-3, 6-4, 7-21
a standby database, 2-7, 5-6, 6-1
standby sites, 5-10, 7-24

D

Data Guard broker
  See broker
Data Guard command-line interface
  banners from output, 7-1
  commands
    ALTER RESOURCE (property), 7-11
    ALTER RESOURCE (state), 7-14
    ALTER SITE, 7-16
    CREATE CONFIGURATION, 7-21
    CREATE SITE, 7-24
    DISABLE CONFIGURATION, 7-27
    DISABLE RESOURCE, 7-28
    DISABLE SITE, 7-29
    ENABLE CONFIGURATION, 7-30
    ENABLE RESOURCE, 7-31
    ENABLE SITE, 7-33
    EXIT, 7-34
    HELP, 7-37
    QUIT, 7-39
    REMOVE CONFIGURATION, 7-40
    REMOVE SITE, 7-41
    SHOW CONFIGURATION, 7-42
    SHOW DEPENDENCY TREE, 7-44
    SHOW LOG, 7-46
    SHOW RESOURCE, 7-49
    SHOW SITE, 7-52
  creating
    a standby database, 5-6, 6-1
    and adding a primary database resource object, 7-21
  database resource substates, 2-11, 7-14, 7-31
  DG_BROKER_START initialization parameter, 1-15, 7-4
  introduction, 1-2, 1-9
  sample help output, 1-9
  setting critical database properties, 6-6
  starting, 6-3, 7-1
  string values, 7-5
  summary of commands, 7-2
  suppressing command prompts, 7-1
Data Guard configuration file
  deleting, 7-41
  inconsistent values from SPFILE parameter file, 8-3
  relationship to DMON process, 1-10
  renaming, 1-12
Data Guard configurations
  background, 2-2
  supported, 2-2
Data Guard Manager, 1-7
  Add Site wizard, 1-7
  console, 1-8
  Create Configuration wizard, 1-7
  database property pages, 1-8
  discovering primary and standby nodes, 5-2
  integration with Oracle Enterprise Manager, 1-7, 5-1
  introduction, 1-2, 1-6
  making Oracle Net configuration changes, 1-3, 1-8
  performance tools and graphs, 1-7
  quick tour, 5-5
  setting Preferred Credentials, 5-3
  starting, 5-3
  upgrading, 1-14
  wizards
    automate standby database creation, 2-5
    creating standby databases, 1-7
Data Guard monitor (DMON), 1-9
  in a broker configuration, 2-3
  in a Data Guard configuration, 2-3
  interaction with the Oracle database server, 1-10
  maintaining configuration data, 1-12
  managing objects, 2-3, 2-8, 5-19, 6-14
  Oracle database server background processes, 1-10
  overview, 1-10
  removing objects, 6-13
  running on each site, 2-3
  starting with the DG_BROKER_START parameter, 2-6
  two-way network communication, 1-11
data protection modes
  See protection modes
database resource properties
  definition, 4-5
  setting values for switchover operations, 4-10

database resources
connecting to, 6-3
creating and adding to a broker configuration, 1-7
dependencies, 4-1
discovering, 5-2
installation for broker management, 1-15
logical object, 1-4
monitoring, 1-4
objects
definition, 1-5
in a broker configuration, 1-5
overview, 4-1
prerequisites for broker configurations, 1-15
properties
configurable, 4-6
definition, 4-5
property management, 1-13
property pages, 1-8
restarting after a failover, 7-36
starting the standby database instance, 6-2
states, 4-1
dependencies, 4-1
online substates, 2-11
transitions, 2-12, 4-3
substates, 4-2
database sites
See sites
DB_FILE_NAME_CONVERT initialization parameter
initialization parameters
setting DB_FILE_NAME_CONVERT in a broker configuration, 8-14
DbFileNameConvert property, 8-14
dedicated server link, 7-5
dedicated server process, 7-5
default values
database resource substates, 2-11
properties, 4-9
See also states
DelayMins property, 8-14
dependencies
displaying for a configuration, 7-44
hierarchy of objects in a broker configuration, 3-2, 4-1
object, 2-3
dependency tree, 7-44
destinations
archived redo log parameters, 2-2
viewing the LogXptStatus property, 8-4
DG_BROKER_CONFIG_FILEn file, 1-12
DG_BROKER_CONFIG_FILEn initialization parameter, 1-15
DG_BROKER_START initialization parameter, 1-13, 1-15, 2-6, 7-4
DGMGRL commands
FAILOVER, 7-35
SWITCHOVER, 7-60
diagrams of database state transitions, 4-4
DISABLE CONFIGURATION command, 7-27
example, 6-11
DISABLE RESOURCE command, 7-28
example, 6-12
DISABLE SITE command, 7-29
example, 6-12
disabling
broker configuration, 6-11, 7-27
database resources, 6-12, 7-28
sites, 6-11, 6-12, 7-29
See also each DISABLE command
disaster protection
benefits, 1-2
discovering
primary and standby nodes, 5-2
discovering primary and standby nodes, 5-2
Discovery wizard, 5-2
displaying
alert log, 7-46
Data Guard configuration log, 7-46
Data Guard Manager quick tour, 5-5
help for CLI commands, 7-37
help for Data Guard Manager, 5-5
properties, 2-16
states, 2-13
summary information
configuration, 7-42
database resource, 7-49
site, 7-52
distributed management framework, 1-1
DMON

See Data Guard monitor (DMON)
downgrading
protection mode, 2-21

E

e-mail
reporting events, 1-8
ENABLE CONFIGURATION command, 6-14, 7-30, 7-31, 7-33
enabling
broker configuration, 2-8, 6-14
See also each ENABLE command
Enterprise Edition database server
installation, 1-13
error status, 2-15
event management system, 1-7
events
monitoring with Oracle Enterprise Manager, 2-5
Oracle Enterprise Manager, 1-4, 1-7
reporting, 1-8
responding to, 1-4
starting Oracle Intelligent Agent, 5-2
EXIT command, 7-34
See also QUIT command

F

failover
database restarts and, 7-36
FAILOVER command
DGMGRL command-line interface, 7-35
failover operations
affect on data protection mode, 3-9
benefits, 1-3
broker tasks, 3-9
completing, 3-11
failing over to a standby database, 7-35
forced, 3-8
graceful, 3-9
managing, 3-8
role management overview, 3-2
scenario, 5-34
starting, 3-9
troubleshooting, 3-12
using Data Guard Manager, 1-7
using the FAILOVER command, 7-35
Failover wizard, 1-7, 5-34
failures
primary site, 3-2
files
naming SPFILE, 1-13
forced failover operations
broker tasks, 3-10
overview, 3-8

G

graceful failover operations
broker tasks, 3-9
overview, 3-8

H

health check, 1-4
monitoring, 1-10, 1-11
revealed by configuration status, 2-14
HELP command, 7-37
sample, 1-9
hierarchy
objects in a broker configuration, 1-5, 2-3, 3-1, 4-1
high availability
benefits, 1-2
grades of data protection, 2-17, 8-19
log transport services
ARCH mode, 8-20
ASYNC mode, 8-20
SYNC mode, 8-19
LogXptMode property, 8-19

I

InconsistentProperties property, 8-3
initial default online states
See states
initialization parameters
COMPATIBLE, 1-15
database configurable properties, 4-6

DG_BROKER_CONFIG_FILEn, 1-15
DG_BROKER_START, 1-15
dynamic, 4-9
inconsistent, 8-3
LOG_ARCHIVE_DEST_STATE_n, 8-9
static, 4-9
See also SPFILE, 1-15
installation
archivelog mode setup, 1-15
Data Guard, 1-13
Data Guard Manager, 1-14
prerequisites, 1-13
remote login password file, 1-15
intended state
configuration health check, 2-14
definition, 2-12
invoking
the Data Guard command-line interface, 6-3

L

life cycle of a broker configuration, 2-6
log apply services
configuring, 1-3, 1-8, 4-7
configuring for logical standby databases, 4-8
Data Guard configuration, 2-2
delaying, 8-14
standby database online mode, 2-11, 4-2
verifying, 1-3
log transport services
ARCH mode, 4-11, 8-20
ASYNC mode, 4-11, 8-19
configuring, 1-3, 1-8, 4-7
data protection modes, 4-10, 8-19
Data Guard configuration, 2-2
LogShipping property, 8-18
primary database online mode, 2-11, 4-2
SYNC mode, 4-11, 8-19
verifying, 1-3
LOG_ARCHIVE_DEST_n initialization parameter
setting the ALTERNATE attribute, 8-9
setting the ASYNC attribute, 8-12
setting the DELAY attribute, 8-14
setting the DEPENDENCY attribute, 8-15
setting the ENABLE and DEFER attributes, 8-18
setting the MANDATORY or OPTIONAL attributes, 8-13
LOG_ARCHIVE_DEST_STATE_n initialization parameter
automatic update, 8-9
LOG_ARCHIVE_FORMAT initialization parameter, 8-16
LOG_ARCHIVE_MAX_PROCESSES initialization parameter, 8-16
LOG_ARCHIVE_MIN_SUCCEED initialization parameter, 8-16
LOG_ARCHIVE_TRACE initialization parameter
setting LogArchiveTrace property, 8-17
LOG_FILE_NAME_CONVERT initialization parameter
setting LogFileNameConvert property, 8-18
LogArchiveFormat property, 8-16
LogArchiveMaxProcesses property, 8-16
LogArchiveMinSucceedDest property, 8-16
LogArchiveTrace property, 8-17
LogFileNameConvert property, 8-18
logical standby databases
default online state, 2-11
online state, 4-2
LOGICAL-APPLY-ON substate, 2-11, 4-3
LOGICAL-APPLY-READY substate, 4-3
login password file, 1-15
LogShipping property, 8-18
LogXptMode property, 4-10
LogXptStatus property, 8-4
LsbyASkipCfgPr property, 8-21
LsbyASkipErrorCfgPr property, 8-21
LsbyASkipTxnCfgPr property, 8-22, 8-24
LsbyDSkipCfgPr property, 8-23
LsbyDSkipErrorCfgPr property, 8-23
LsbyFailedTxnInfo property, 8-4, 8-5
LsbyMaxEventsRecorded property, 8-25
LsbyMaxServers property, 8-26
LsbyMaxSga property, 8-25
LsbyRecordAppliedDdl property, 8-26
LsbyRecordSkipDdl property, 8-27
LsbyRecordSkipErrors property, 8-28
LsbyTxnConsistency property, 8-28

M

management
  benefits, 1-3
  Data Guard Manager, 1-7
  model, 1-4
managing
  a broker configuration, 2-1, 6-1
  a remote standby database, 1-15
  database resources, 4-1
  failover operations, 3-8
  local operations, 1-2
  objects in a broker configuration, 1-5
  remote operations, 1-2
  site objects, 3-1
  site resources, 3-1
  switchover operations, 3-3
MANDATORY attribute
  set with the Binding property, 8-13
MaxFailure property, 8-29
maximize availability, 1-3, 2-9, 8-19
maximize data protection, 1-3, 2-9, 8-19
maximize performance, 1-3, 2-9, 8-19
Maximum Availability data protection mode, 2-18
Maximum Performance data protection mode, 2-18
Maximum Protection data protection mode, 2-17
monitorable properties, 2-15
  database, 4-6
  InconsistentProperties, 8-3
  LogXptStatus, 8-4
  LsbyFailedTxnInfo, 8-4, 8-5
  SbyLogQueue, 8-6
  SendQEntries, 8-4, 8-5, 8-6
monitoring
  broker configurations, 1-10, 6-1
  Data Guard Manager performance page, 2-9
  local and remote databases, 1-4
  through the command-line interface, 1-9

N

networks
  Data Guard configuration, 2-2
  setting up files, 1-15
  two-way communication, 1-11
normal status, 2-14

O

objects
  broker configuration, 1-4, 2-3
  changing the state of, 6-9
  connected in a hierarchy, 1-6
  default online database resource substates, 2-11
  dependencies, 2-3, 3-2, 4-1
  disabling, 6-11
  enabling, 6-14
  hierarchy, 1-5
  properties for database resources, 1-13
  state transitions, 2-12
  states, 2-10
  taking offline, 6-9
oemapp console command, 5-2
oemapp dataguard command, 5-3
oemctl start oms command, 5-2
offline state
  transitioning objects, 6-9
online paths
  displaying for a broker configuration, 7-44
online states
  database resource, 4-2
  substates, 4-2
online substate
  logical standby database, 4-3
  physical standby database, 4-3
operations
  performing on broker objects, 1-6
OPTIONAL attribute
  set with the Binding property, 8-13
Oracle Enterprise Manager
  Discovery wizard, 5-2
  event management system, 1-4
  integration, 1-7
  monitoring events, 2-5
  setting Preferred Credentials, 5-3
  starting, 5-2
  starting Data Guard Manager, 5-3
Oracle Intelligent Agent
  starting, 5-2

Oracle Management Server
starting, 5-2
Oracle Net networks
configuration changes, 1-3, 1-8
configuring, 6-2
installation prerequisites, 1-15
service name, 7-5
supported configuration, 2-2
two-way communication, 1-11

P

pagers
reporting events, 1-8
password file
remote, 1-15, 7-5
performance
Data Guard Manager tools, 1-7, 2-9
log transport services
ARCH mode, 8-20
ASYNC mode, 8-20
SYNC mode, 8-19
Personal Edition database server
installation, 1-13
physical standby databases
online state, 4-2
PHYSICAL-APPLY-ON substate, 4-3
default online state, 2-11
state transitions, 4-4
PHYSICAL-APPLY-READY substate, 4-3
state transitions, 4-4
planned transitions
sites, 3-2
Preferred Credentials, 5-3
prerequisites
installation, 1-13
switchover operation, 3-4
primary database
archivelog mode, 1-15
connecting to, 6-3
constructing a standby database, 2-7, 6-2
Data Guard configuration, 2-2
default online state, 2-11
online state, 4-2
online substate, 4-3
online substates, 4-3
READ-WRITE-XPTON substate, 4-3
state transitions, 4-4
transport off substate, 4-3
primary site
configuration, 2-2
during failover operations, 1-7, 7-35
role, 3-2
switching over to the standby role, 7-60
processes
DMON, 1-10
Oracle database server, 1-10
properties
common, 2-16
configurable, 2-15
configuration, 2-12
database resource, 4-5
default values, 4-9
managing, 1-13
monitorable, 2-15
overview, 2-15
updating in SPFILE, 1-13, 1-15
property pages
configuration, 1-8
database resource, 1-8
protection modes
after a failover operation, 3-9
benefits, 1-3
configuration, 7-7
configuring log transport services, 4-10
downgrading, 2-21
log transport services setup, 8-19
setting for a broker configuration, 2-17
updating, 2-9
upgrading, 2-21

Q

quick tour, 5-5
QUIT command, 7-39
See also EXIT command

R

READ-ONLY substate

physical standby database, 4-3
state transitions, 4-4
read / write mode, 2-11, 4-2
READ-WRITE substate, 4-3
LogShipping property setting, 8-19
state transitions, 4-4
READ-WRITE-XPTON substate, 4-3
CLI default value, 2-11
setting LogShipping property, 8-19
state transitions, 4-4
remote login password file, 1-15, 7-5
REMOVE CONFIGURATION command, 7-40
example, 6-13
REMOVE SITE command, 7-41
example, 6-13
removing, 2-22
a standby database resource object, 2-22
broker configuration, 2-22
See each REMOVE command
ReopenSecs property, 8-30
requests
passing between sites, 1-11
resources
altering properties for, 7-11
altering states for, 7-14
configurable database properties, 4-6, 8-7 to 8-31
disabling management of objects, 7-27, 7-28, 7-29
displaying summary information for, 7-49
enabling, 6-14, 7-30, 7-31, 7-33
monitorable database properties, 4-6, 8-1 to 8-7
roles
effect on database resource substates, 2-11
managing during failover operations, 3-2

S

SbyLogQueue property, 8-6
scripts
using Data Guard command-line interface, 7-1
SendQEntries property, 8-6
server initialization parameter file
See SPFILE
server-side software, 1-9
setting
database properties, 6-6
SHOW CONFIGURATION command, 6-4, 7-42
SHOW CONFIGURATION VERBOSE command, 6-5, 6-14
SHOW DEPENDENCY TREE command, 7-44
SHOW LOG command, 7-46
SHOW RESOURCE command, 7-49
SHOW SITE command, 7-52
SHOW SITE VERBOSE command, 6-6
displaying properties, 2-16
showing
See each SHOW command
sites
adding with Add Site wizard, 1-7
creating, 7-24
deleting
Data Guard configuration file, 7-41
dependencies, 3-2, 4-1
during failover operations, 3-8
during switchover operations, 3-3
effects of removing metadata from, 7-40, 7-41
enabling, 6-14
logical object, 1-4
network setup, 1-11, 1-15
object
definition, 1-5
overview, 3-1
removing
from a broker configuration, 6-13
roles, 3-2
showing summary information, 7-52
states
online and offline, 3-1
transitions, 2-12
SPFILE
broker property management, 1-13, 1-15, 4-8
filenames, 1-13
inconsistent values from Data Guard configuration file, 8-3
standby databases
Apply Off substate, 4-3
constructing from backups, 2-7, 6-2
copying datafiles, 5-12
creating, 1-7, 5-6, 5-11, 6-1

Data Guard configuration, 2-2
discovering, 5-2
management, 1-15
online state, 2-11
online substate, 4-3
online substates, 4-3
read-only mode substate, 4-3
READ-ONLY substate, 4-3
removing from a broker configuration, 2-22
starting, 6-2
state transitions, 4-4
standby sites
changing the state of, 5-26
creating, 7-24
roles, 3-2
switching over to the primary role, 7-60
STANDBY_ARCHIVE_DEST initialization parameter
setting in a broker configuration, 8-30
STANDBY_FILE_MANAGEMENT initialization parameter
setting in a broker configuration, 8-31
StandbyArchiveDest property, 8-30
StandbyFileManagement property, 8-31
starting
Create Configuration wizard, 5-6
Data Guard command-line interface, 6-3, 7-1
Data Guard Manager, 5-3
Data Guard monitor (DMON), 2-6
failover operations, 3-9
Oracle Enterprise Manager Console, 5-2
Oracle Intelligent Agent, 5-2
Oracle Management Server, 5-2
standby databases, 6-2
switchover operations, 3-5
state transitions, 2-12
effect on database resource substates, 4-3
overview, 2-12
states, 2-10
changing, 6-9
configuration, 2-12, 7-10
database, 4-1
database transitions, 4-3
displaying, 2-13
initial default online, 2-12
transitioning, 2-12
status
configuration, 2-14
intended state of a configuration, 2-14
string values
Data Guard command-line interface, 7-5
substates
database resource, 4-2, 7-31
default, 2-11
effect on archived redo logs, 2-11
primary database, 4-4
standby databases, 4-4
supported broker configuration, 1-5
SWITCHOVER command
DGMGRL command-line interface, 7-60
switchover operations, 3-2
benefits, 1-3
broker tasks, 3-5
effect on database startup, 7-60
managing, 3-3
prerequisites, 3-4
setting up database property values, 4-10
starting, 3-5
troubleshooting, 3-6
using Data Guard Manager, 1-7
using the SWITCHOVER command, 7-60
Switchover wizard, 1-7, 5-32
SYNC log transport mode, 4-11
SYSDBA privileges, 6-3
to connect to the database, 7-5

T

test applications
tuning the broker configuration, 2-9
transport off substate, 4-3
troubleshooting
failover operations, 3-12
switchover operations, 3-6
tuning
using the Data Guard Manager, 2-9
two-way communication channel, 1-11

U

updating configuration properties, 2-15
upgrading
  Data Guard, 1-14
  Data Guard Manager, 1-14
  protection mode, 2-21
user interfaces
  overview, 1-7

V

viewing property information about database
    resources, 4-6, 8-1

W

warning status, 2-15
wizards
  Add Site, 1-7, 5-21
  Create Configuration, 1-7, 5-2, 5-6
  Discovery, 5-2, 5-9
  Failover, 1-7, 5-34
  Switchover, 1-7, 5-32