

Zero Data Loss Recovery Appliance Protected Database Configuration Guide



Release 12.2

E88069-04

July 2018

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Zero Data Loss Recovery Appliance Protected Database Configuration Guide, Release 12.2

E88069-04

Copyright © 2014, 2017, Oracle and/or its affiliates. All rights reserved.

Contributing Authors: Glenn Maxey, Padmaja Potineni

Primary Author: Terence Buencamino

Contributors: Andrew Babb, Anand Beldalker, Jin-Jwei Chen, Tim Chien, Sean Connelly, Donna Cooksey, Sam Corso, Steve Fogel, Muthu Olagappan, Jony Safi, Daniel Sears, Lawrence To, Steve Wertheimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

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

Contents

Preface

Audience	xi
Documentation Accessibility	xi
Related Documents	xi
Conventions	xii

1 Getting Started with Recovery Appliance

1.1	Overview of Recovery Appliance	1-1
1.2	Overview of Protected Databases	1-2
1.2.1	Protected Databases and Recovery Appliance Architecture	1-2
1.2.2	Benefits of Using Recovery Appliance to Back Up Protected Databases	1-4
1.2.3	Tasks of Protected Database Administrators	1-5
1.2.4	Overview of Users and Privileges Required for Protected Databases	1-6
1.2.4.1	Protected Database Administrator	1-6
1.2.4.2	Recovery Appliance User	1-6
1.2.5	Overview of Protection Policies	1-7
1.2.6	Overview of Sending Protected Database Backups to Recovery Appliance	1-7
1.2.6.1	Overview of Backup Polling	1-8
1.2.7	Overview of Storing Protected Database Metadata	1-8
1.3	Backup and Recovery Concepts for Protected Databases	1-9
1.3.1	About RMAN SBT Channels and Protected Databases	1-9
1.3.2	About Backing Up Protected Databases to Recovery Appliance	1-10
1.3.2.1	About Backup Encryption and Recovery Appliance	1-10
1.3.3	About Restoring and Recovering Protected Databases Using Recovery Appliance	1-11
1.3.4	About the Recovery Appliance Incremental-Forever Backup Strategy	1-11
1.3.4.1	Difference Between RMAN Incrementally Updated and Recovery Appliance Incremental-Forever Backup Strategies	1-12
1.3.5	About Real-Time Redo Transport	1-12
1.3.5.1	How Real-Time Redo Transport Works	1-13
1.3.5.2	About Configuring Real-Time Redo Transport for Protected Databases	1-13

1.4	Tools for Protected Database Operations	1-14
1.5	Protected Database Administration Task Flow	1-14

2 Migration Considerations for Protected Database Administrators

2.1	Planning to Migrate Protected Databases to Recovery Appliance	2-1
2.2	Adapting an Existing Backup Strategy for Recovery Appliance	2-2
2.2.1	Modifying RMAN Channel Configurations	2-3
2.2.2	Modifying RMAN Backup and Recovery Scripts	2-3
2.2.3	Removing Unnecessary RMAN Commands	2-4
2.3	Migrating Backup Metadata to the Recovery Appliance Catalog	2-4
2.3.1	Connecting to the Protected Database and Recovery Appliance Using CLI	2-5
2.3.2	Importing Protected Database Metadata into the Recovery Appliance Catalog	2-6
2.3.2.1	Steps to Import Protected Database Metadata Into Recovery Appliance	2-6
2.3.2.2	Preparing to Import an RMAN Recovery Catalog into Recovery Appliance	2-7
2.3.2.3	Importing Protected Database Metadata Using the IMPORT CATALOG Command	2-9
2.4	Migrating Existing Backups to Recovery Appliance	2-10
2.4.1	Setting Up Backup Polling to Migrate Existing Backups to the Recovery Appliance	2-11
2.4.1.1	Mounting the NFS Storage for Backup Polling	2-12
2.4.2	Making Tape Backups Available to Recovery Appliance	2-12
2.4.3	Creating Local Backups	2-13
2.4.4	Recovering Protected Databases Using Local Backups	2-14

3 Configuring Protected Databases

3.1	Overview of Configuring Protected Databases for Recovery Appliance	3-1
3.1.1	Steps to Configure Protected Databases for Recovery Appliance	3-2
3.1.2	Overview of Recovery Appliance Backup Module	3-3
3.1.2.1	Install Location for the Recovery Appliance Backup Module	3-3
3.1.2.2	Recovery Appliance Backup Module Configuration File	3-3
3.1.2.3	Configuration Parameters for the Recovery Appliance Backup Module	3-4
3.1.3	Overview of Enrolling Protected Databases	3-5
3.1.4	Overview of Protected Database Backup Settings	3-6
3.1.5	Overview of Protected Database Recovery Settings	3-7
3.2	Enrolling the Protected Database with Recovery Appliance (Cloud Control)	3-8

3.2.1	Creating the Enterprise Manager Administrator to Manage Protected Database Operations	3-9
3.2.2	Enrolling a Protected Database with Recovery Appliance Using Cloud Control	3-10
3.2.3	Accessing the Protected Database Home Page Using Cloud Control	3-11
3.3	Enrolling the Protected Database with Recovery Appliance (Command Line)	3-12
3.3.1	Installing the Recovery Appliance Backup Module	3-14
3.3.1.1	Preparing to Install the Recovery Appliance Backup Module	3-14
3.3.1.2	Obtaining the Installer for the Recovery Appliance Backup Module	3-15
3.3.1.3	Running the Recovery Appliance Backup Module Installer	3-15
3.3.2	Enrolling Oracle 10g Protected Databases	3-16
3.3.3	Registering a Protected Database with the Recovery Appliance Catalog	3-17
3.4	Configuring Backup and Recovery Settings for Protected Databases (Cloud Control)	3-18
3.4.1	Configuring Backup Settings for Protected Databases Using Cloud Control	3-18
3.4.2	Configuring Recovery Settings for Protected Databases Using Cloud Control	3-21
3.4.3	Clearing the Backup Configuration of Protected Databases Using Cloud Control	3-23
3.5	Configuring Backup and Recovery Settings for Protected Databases (Command Line)	3-23
3.5.1	Configuring Backup Settings for Protected Databases Using the Command Line	3-24
3.5.1.1	Configuring Real-Time Redo Transport	3-24
3.5.1.2	Creating an Oracle Wallet on the Protected Database	3-27
3.5.2	Configuring Recovery Settings for Protected Databases Using the Command Line	3-28
3.5.3	Using RMAN Channels for Recovery Appliance Backup and Recovery Operations	3-29
3.5.3.1	Configuring RMAN SBT Channels for Recovery Appliance	3-29
3.5.3.2	Allocating RMAN SBT Channels for Recovery Appliance	3-30
3.6	Performing Test Backup and Recovery Operations	3-30
3.6.1	Running a Test Backup Using the Command Line	3-30
3.6.2	Running a Test Recovery Using the Command Line	3-31
3.6.3	Performing a Test Backup Using Cloud Control	3-31

4 Backing Up Protected Databases

4.1	Overview of Backing Up Protected Databases	4-1
4.2	Backing Up the Protected Database Using Cloud Control	4-2
4.2.1	Using the Oracle-Suggested Backup Strategy for Protected Databases	4-2
4.2.2	Backing Up the Whole Protected Database Using Cloud Control	4-4
4.3	Backing Up the Protected Database Using the Command Line	4-5

4.3.1	Creating the Initial Full Backup of the Protected Database	4-5
4.3.2	Creating Incremental Backups of the Protected Database	4-6
4.4	Monitoring Protected Database Backups Using Cloud Control	4-8
4.4.1	Viewing Backup Reports for Protected Databases	4-8
4.4.2	Viewing the Status of Protected Database Backup Jobs	4-9

5 Recovering Data from Recovery Appliance

5.1	Overview of Restoring and Recovering Data from Recovery Appliance	5-1
5.2	Recovering Protected Databases Using Cloud Control	5-1
5.2.1	Prerequisites for Recovering Protected Databases Using Cloud Control	5-2
5.2.2	Performing Block Media Recovery Using Cloud Control	5-2
5.2.3	Recovering an Entire Database Using Cloud Control	5-3
5.3	Restoring and Recovering Data from Recovery Appliance Using the Command Line	5-4
5.3.1	Prerequisites for Restoring and Recovering Data from Recovery Appliance	5-5
5.3.2	Restoring Protected Databases Using a Downstream Recovery Appliance	5-6
5.3.3	Example: Restoring and Recovering an Entire Database With the Existing Current Control File	5-7
5.3.4	Example: Recovering an Entire Database to a Specified Point-in-Time	5-7
5.3.5	Example: Restoring and Recovering the Control File	5-9
5.3.6	Example: Restoring and Recovering Tablespaces in the Protected Database	5-9
5.3.7	Example: Restoring and Recovering a Data File in the Protected Database	5-10
5.3.8	Example: Restoring and Recovering PDBs	5-11
5.3.8.1	Performing Complete Recovery of the Whole PDB	5-11
5.3.8.2	Performing Point-in-Time Recovery for the Whole PDB	5-12
5.3.8.3	Recovering Specific Data Files in a PDB	5-12
5.3.8.4	Recovering Specific Tablespaces in a PDB	5-13
5.3.9	Example: Recovering a PDB in an Oracle RAC Environment	5-14
5.3.10	Example: Restoring and Recovering One or Many Data Blocks in a PDB	5-14
5.3.11	Example: Recovering a Database Configured for Real-Time Redo Transport After a Severe Storage Failure	5-15
5.3.12	Example: Recovering the Control File and Database When Real-Time Redo Transport is Configured	5-17
5.4	Database Duplication from Recovery Appliance	5-18
5.4.1	Creating a Standby Database for a Protected Database	5-18
5.4.2	Cloning a Protected Database	5-19

A Differences in RMAN Commands

Index

List of Examples

3-1	Creating an Oracle Wallet on the Protected Database	3-28
3-2	Creating an Oracle Wallet with Multiple User Credentials	3-28
3-3	Configuring an RMAN Channel for Recovery Appliance	3-29
3-4	Allocating RMAN Channels for Recovery Appliance	3-30

List of Figures

1-1	Recovery Appliance Architecture and Protected Databases	1-3
3-1	Protected Database Home Page	3-12
3-2	Backup Settings Page for Protected Databases	3-19
3-3	Protected Database Recovery Settings	3-22
3-4	Recovery Appliance Settings Section of Backup Settings Page	3-32
4-1	Schedule Protected Database Backup	4-3
4-2	Protected Database Backup Report	4-9
4-3	Job Activity Report for Protected Database Backup Jobs	4-10

List of Tables

3-1	Recovery Appliance Backup Module Installer Parameters	3-4
3-2	Protected Database Backup Settings	3-6
3-3	Protected Database Recovery Settings	3-7
A-1	Modified RMAN Commands	A-1

Preface

Welcome to the *Zero Data Loss Recovery Appliance Protected Database Configuration Guide*.

This preface contains the following topics:

- [Audience](#) (page xi)
- [Documentation Accessibility](#) (page xi)
- [Related Documents](#) (page xi)
- [Conventions](#) (page xii)

Audience

This document is intended for a database backup administrator who will configure and administer a protected database to send backups to Zero Data Loss Recovery Appliance, commonly known as Recovery Appliance.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see the following documents:

- *Zero Data Loss Recovery Appliance Administrator's Guide*
- *Oracle Database Backup and Recovery User's Guide*
- *Oracle Database Backup and Recovery Reference*
- *Oracle Secure Backup Administrator's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Getting Started with Recovery Appliance

This chapter provides an overview of Zero Data Loss Recovery Appliance, commonly known as Recovery Appliance, and describes the high-level steps required to use Recovery Appliance for data protection.

This chapter contains the following topics:

- [Overview of Recovery Appliance](#) (page 1-1)
- [Overview of Protected Databases](#) (page 1-2)
- [Backup and Recovery Concepts for Protected Databases](#) (page 1-9)
- [Tools for Protected Database Operations](#) (page 1-14)
- [Protected Database Administration Task Flow](#) (page 1-14)

1.1 Overview of Recovery Appliance

Recovery Appliance is a cloud-scale Engineered System designed to protect all Oracle Databases in your enterprise. Built on a scalable architecture and integrated with Recovery Manager (RMAN), it uses a fully fault-tolerant and scalable hardware to provide a centralized, incremental-forever backup strategy for a large number of databases.

Recovery Appliance provides enhanced data protection and availability for the enterprise. Real-time redo transport enables data protection to the last sub-second, dramatically reducing recovery point objectives across the entire enterprise. Backup and restore processing is offloaded to the Recovery Appliance thus freeing production database resources and boosting their performance.

Backups are stored and managed in a centralized disk pool. An initial full backup followed by successive incremental backups is sufficient to protect your production databases. Incremental backups are indexed and stored as they are received by the appliance. Recovery Appliance provides **virtual full backups**, each of which is a complete database image as of one distinct point in time, to recover databases to any specified time within the recovery window. Virtual full backups are automatically created by Recovery Appliance for every incremental backup that it receives. Virtual backups enable the rapid reconstruction of a full backup to a point-in-time within the user's recovery window.

The Recovery Appliance metadata database manages the metadata for all backups stored on the Recovery Appliance and contains the Recovery Appliance catalog.

See Also:

Zero Data Loss Recovery Appliance Administrator's Guide for more information about Recovery Appliance architecture and features

1.2 Overview of Protected Databases

A client database whose backups are managed by a Recovery Appliance is called a **protected database**. Each protected database uses a specific Recovery Appliance as a destination for centralized backup and recovery. Protected databases use RMAN commands to perform backup and recovery operations. You must install the Zero Data Loss Recovery Appliance backup module (Recovery Appliance backup module), an Oracle-supplied SBT library, that enables RMAN to transfer protected database backups over the network to a Recovery Appliance.

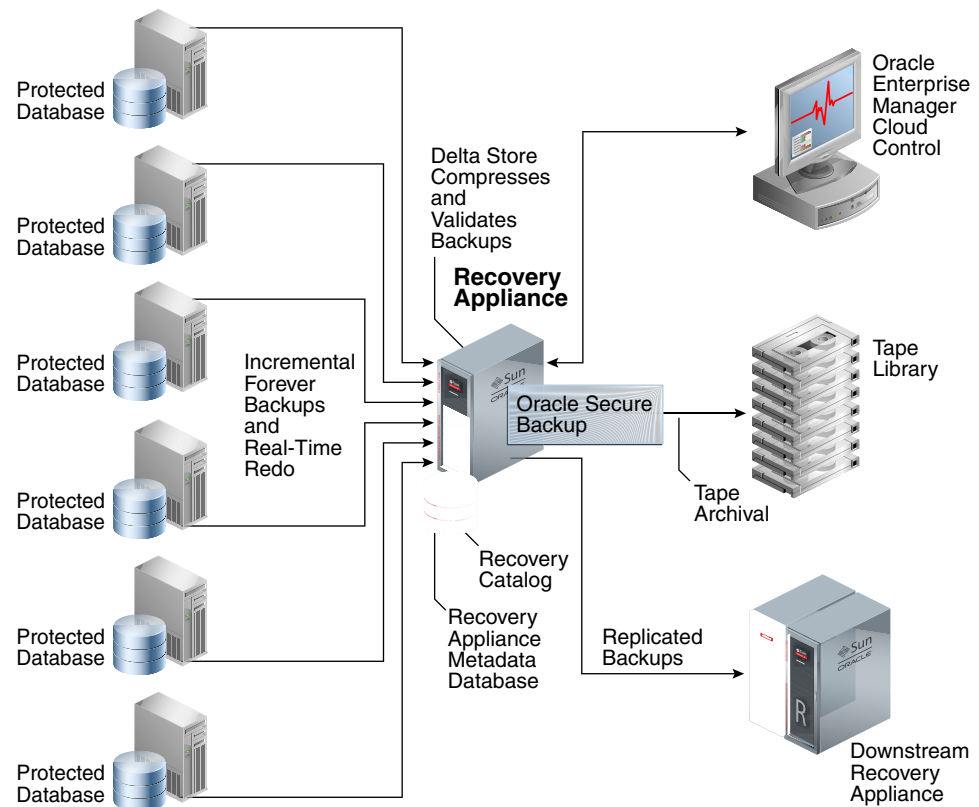
This section contains the following topics:

- [Protected Databases and Recovery Appliance Architecture](#) (page 1-2)
- [Benefits of Using Recovery Appliance to Back Up Protected Databases](#) (page 1-4)
- [Tasks of Protected Database Administrators](#) (page 1-5)
- [Overview of Users and Privileges Required for Protected Databases](#) (page 1-6)
- [Overview of Protection Policies](#) (page 1-7)
- [Overview of Sending Protected Database Backups to Recovery Appliance](#) (page 1-7)

1.2.1 Protected Databases and Recovery Appliance Architecture

[Figure 1-1](#) (page 1-3) illustrates the Recovery Appliance environment. Multiple protected databases are backed up to a Recovery Appliance using an incremental-forever backup strategy. You can also configure protected databases to transfer real-time redo data to the Recovery Appliance. The Recovery Appliance environment can include protected databases from Oracle Database 10g, Oracle Database 11g, and Oracle Database 12c. To enable protected databases to access and store backups to the Recovery Appliance, you must configure databases.

Figure 1-1 Recovery Appliance Architecture and Protected Databases



The Recovery Appliance receives incremental backups and redo data from multiple protected databases. It continuously validates backups at the Oracle block level thus assuring recoverability of data. Backups are compressed to optimize storage utilization before they are stored in the delta store. The delta store is the sum total of all Recovery Appliance storage that is used to store protected database backup data. All data file and archived redo log backups are stored in the delta store. Recovery Appliance creates virtual full backups of the protected database, which is a complete database image as of one distinct point in time.

The Recovery Appliance metadata database is the Oracle database that runs inside of the Recovery Appliance. It stores configuration data such as definitions, protection policy definitions, and client database definitions. The metadata database also stores backup metadata and contains the Recovery Appliance catalog.

Oracle Secure Backup, the tape management component of Recovery Appliance, is preinstalled on the Recovery Appliance and is used to archive backups to an attached tape library.

Oracle Enterprise Manager Cloud Control (Cloud Control) provides a unified backup management interface for the entire life cycle of backups. You can use Cloud Control to back up, recover, and report on protected databases.

As part of the disaster recovery strategy, Recovery Appliance can replicate protected database backups to other Recovery Appliances. When you configure replication, a Recovery Appliance (called the upstream Recovery Appliance) forwards backups to

another Recovery Appliance (called the downstream Recovery Appliance). Recovery Appliance supports a wide variety of replication topologies.

 **See Also:**

- ["Backup and Recovery Concepts for Protected Databases \(page 1-9\)"](#) for information about incremental-forever backup strategy and real-time redo transport
- ["Configuring Protected Databases \(page 3-1\)"](#)
- ["Overview of Storing Protected Database Metadata \(page 1-8\)"](#)
- *Zero Data Loss Recovery Appliance Administrator's Guide* for the supported Oracle Database releases
- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about replicating protected database backups

1.2.2 Benefits of Using Recovery Appliance to Back Up Protected Databases

- Minimizes the impact of backups on production servers
 - Minimizes backup windows

Recovery Appliance simplifies data protection for databases across the enterprise by reducing backup windows and providing a single repository for backups of multiple protected databases. Recovery Appliance uses an incremental-forever backup strategy in which only one level 0 backup is required for each protected database. Subsequently, protected databases send level 1 incremental backups to the Recovery Appliance.
 - Offloads backup processing from production servers

Most backup processing, including backup validation and backup maintenance operations are offloaded to the Recovery Appliance. Performance of production systems is improved because resources used for backup processing are freed up.
- Eliminates data loss
 - Transports redo data asynchronously to Recovery Appliance

Real-time redo transport enables protected databases to recover data to within a few subseconds of a database failure. It minimizes the window of potential data loss that exists between successive incremental archived log backups by writing redo data directly, as it is generated, from the protected database memory to the Recovery Appliance. See *Zero Data Loss Recovery Appliance Administrator's Guide* for information about the Oracle Database releases that support real-time redo transport.
 - Protects against data corruption

Backups created to Recovery Appliance are continuously validated to ensure that database backup integrity is maintained. With Oracle RMAN block checks, Automatic Storage Management (ASM) and Exadata data checks, Recovery

Appliance provides the best protection for Oracle databases far exceeding third-party solutions that rely mostly on hardware checksums.

- Integration with Oracle high availability technologies

Recovery Appliance is integrated with Oracle high availability technologies including Recovery Manager (RMAN), Oracle Real Application Clusters (Oracle RAC), Oracle Data Guard, and Oracle Secure Backup. You can use RMAN commands, with the exceptions noted in [Differences in RMAN Commands](#) (page A-1), to back up and recover protected databases.

- Reduced restore and recovery time

Recovery Appliance uses virtual full backups that are created on-demand to reduce the restore and recovery time. A virtual full backup is a complete database image as of a distinct point in time. Recovery Appliance efficiently maintains virtual full backups by indexing the incremental backups from protected databases.

- Optimizes storage requirements

Backup storage no longer needs to be distributed across all the protected databases. Recovery Appliance uses a shared disk backup pool to store backups for multiple protected databases.

Despite moving your backups to Recovery Appliance, you still need to configure a local fast recovery area on the protected databases to store control files, online redo log files, archived redo logs, and flashback logs. However, this fast recovery area can be considerably smaller because it does not need to store backups.

1.2.3 Tasks of Protected Database Administrators

In a conventional Oracle Database deployment, a DBA or team of DBAs would be responsible for database administration as well as for planning and performing backup and recovery activities. The storage administrator manages the storage requirements and database backups. By centralizing backup storage and management, Recovery Appliance provides DBAs with full visibility into the end-to-end enterprise backup lifecycle, from the protected database to Recovery Appliance to tape.

The protected database administrator is responsible for performing the following tasks:

- Planning backup and restore strategies for the protected database

Some of the considerations during the planning stage include deciding acceptable recovery window goals and retention policies for the protected database, estimating the storage space required to store protected database backups, and deciding on the method used to send backups to the Recovery Appliance.

When you move your protected database backups to Recovery Appliance for the first time, you must design a strategy to migrate to the Recovery Appliance.

- Configuring protected database access to the Recovery Appliance

Before using Recovery Appliance for data protection of your protected database, you must configure backup and recovery settings as per the protected database requirements.

- Performing backup and recovery operations

Backup jobs are used to perform protected database backup operations. Backup jobs can run immediately or be scheduled to run at a later time. Recovery operations are typically performed immediately in response to media or data loss incidents.

 **See Also:**

- ["Migration Considerations for Protected Database Administrators \(page 2-1\)"](#)
- ["Configuring Protected Databases \(page 3-1\)"](#)
- ["Backing Up Protected Databases \(page 4-1\)"](#)

1.2.4 Overview of Users and Privileges Required for Protected Databases

Backup operations to the Recovery Appliance require coordination between an RMAN client running on the protected database and the system software running on the Recovery Appliance. This section describes the users and privileges necessary for Recovery Appliance backup operations.

1.2.4.1 Protected Database Administrator

The protected database administrator is a user with `SYSDBA` or `SYSBACKUP` privileges on the protected database. This user connects to a Recovery Appliance to perform backup, restore, and recovery operations for the protected database.

With Oracle Database 12c, all RMAN backup and recovery operations can be performed with either `SYSBACKUP` or `SYSDBA` privileges. With releases of Oracle Database earlier than Oracle Database 12c, the protected database administrator must have `SYSDBA` privileges to perform RMAN backup and recovery operations.

To authenticate with a Recovery Appliance and perform backup and recovery operations, the protected database administrator must be associated with a Recovery Appliance user.

1.2.4.2 Recovery Appliance User

A Recovery Appliance user is a database user account, created in the Recovery Appliance metadata database by the Recovery Appliance administrator. This account has the privileges required to send and receive backups for one or more protected databases that are registered with the Recovery Appliance and to manipulate the Recovery Appliance catalog metadata for these protected databases. This is also the account to use to send redo data from a protected database to the Recovery Appliance.

The Recovery Appliance metadata database contains multiple Recovery Appliance user accounts. Each Recovery Appliance user owns a virtual private catalog and can access and modify only those rows in the Recovery Appliance catalog that pertain to databases to which it has been granted access. The authentication credentials of the Recovery Appliance user are stored securely in an Oracle Wallet on the protected database host. The protected database administrator connects to the Recovery Appliance user using the catalog role.

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide for information about the different Recovery Appliance user accounts

1.2.5 Overview of Protection Policies

Recovery Appliance uses protection policies to simplify the management of protected database backups. A protection policy is a collection of attributes that defines recovery goals and storage space requirements for one or more protected databases. A Recovery Appliance contains multiple protection policies that define varied recovery goals. Each protected database is assigned exactly one protection policy that determines how the Recovery Appliance stores and maintains backup data for that protected database.

A protection policy defines the following attributes for each protected database that is associated with the protection policy:

- A Recovery Appliance storage location for storing the protected database backups
- The recovery window goal for disk backups
- (Optional) Whether backups protected by this policy must be replicated or written to tape before being considered for deletion
- (Optional) The recovery window for tape backups
- (Optional) A backup polling policy

Protection policies enable you to group protected databases by recovery service tier. For example, tier 1 databases require backups to be retained for 14 days on disk and 30 days on tape. You create a protection policy that defines these recovery window goals and then assign it to all tier 1 protected databases.

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide for information about creating and maintaining protection policies

1.2.6 Overview of Sending Protected Database Backups to Recovery Appliance

Protected database backups can be stored on Recovery Appliance using one of the following techniques:

- Protected databases send backups directly to a Recovery Appliance

The protected database administrator authenticates and connects to a Recovery Appliance and then backs up the protected database to the Recovery Appliance. The Recovery Appliance backup module is used to send backups over the network to the Recovery Appliance. The incremental-forever backup strategy is used to back up protected databases to the Recovery Appliance. If required, you

can configure real-time redo transport to transmit redo data directly to the Recovery Appliance.

Before you send protected database backups to a Recovery Appliance, you must enroll the protected database with the Recovery Appliance and configure settings.

- Recovery Appliance automatically picks up protected database backups from a shared location

Instead of directly interacting with a Recovery Appliance, the protected database writes backups to a configured shared storage location. The Recovery Appliance uses backup polling to periodically check the shared storage location and pick up new backups stored in this location.

See Also:

- ["Overview of Backup Polling \(page 1-8\)"](#)
- ["Configuring Protected Databases \(page 3-1\)"](#)
- ["Backing Up Protected Databases \(page 4-1\)"](#)

1.2.6.1 Overview of Backup Polling

Backup polling enables a Recovery Appliance to periodically poll a predefined shared disk directory, called the **backup polling location**, and pick up new protected database backups that are placed in this location. The protected database administrator does not interact with the Recovery Appliance to send backups. Instead, backups are placed in the backup polling location and the Recovery Appliance periodically checks and picks up these backups.

The backup polling location can store level 0, level 1, and archived redo log backup sets. It is accessible to the Recovery Appliance through Network File System (NFS).

A backup polling policy, created on the Recovery Appliance, defines a path to the backup polling location and the frequency at which the Recovery Appliance polls this location. The polling policy is associated with a protected database through a protection policy.

See Also:

- ["Setting Up Backup Polling to Migrate Existing Backups to the Recovery Appliance \(page 2-11\)"](#)
- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about creating and assigning backup polling policies

1.2.7 Overview of Storing Protected Database Metadata

The Recovery Appliance metadata database, which resides on the Recovery Appliance, manages the backup metadata for all protected databases registered with the Recovery Appliance and also contains the Recovery Appliance catalog. Every

protected database that stores backups on the Recovery Appliance must use the Recovery Appliance catalog. However, protected databases can use the Recovery Appliance catalog without also using the Recovery Appliance as a backup repository. Protected database administrators connect to the Recovery Appliance catalog using the same Recovery Appliance user that is used for backup and recovery operations.

After you enroll a protected database with a Recovery Appliance, you must register it with the Recovery Appliance catalog. Registering the protected database stores backup metadata for the protected database in the Recovery Appliance catalog. Existing backup metadata that is currently stored in the protected database's RMAN recovery catalog must be imported into the Recovery Appliance catalog.

See Also:

- ["Importing Protected Database Metadata into the Recovery Appliance Catalog \(page 2-6\)"](#)
- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about the Recovery Appliance metadata database

1.3 Backup and Recovery Concepts for Protected Databases

Each protected database that stores backups to a Recovery Appliance must have a globally unique database name (`DB_UNIQUE_NAME`). This global database name is used to identify the protected database to which a backup belongs. Backups for a protected database are written to the storage location that is specified in the protection policy associated with the protected database.

This section contains the following topics:

- [About RMAN SBT Channels and Protected Databases \(page 1-9\)](#)
- [About Backing Up Protected Databases to Recovery Appliance \(page 1-10\)](#)
- [About Restoring and Recovering Protected Databases Using Recovery Appliance \(page 1-11\)](#)
- [About the Recovery Appliance Incremental-Forever Backup Strategy \(page 1-11\)](#)
- [About Real-Time Redo Transport \(page 1-12\)](#)

1.3.1 About RMAN SBT Channels and Protected Databases

To perform protected database backup and recovery operations, you must use one or more RMAN SBT channels that correspond to the Recovery Appliance backup module. This backup module is the shared library that transfers backup data to and from the Recovery Appliance.

Protected database backups are sent over the network to a shared disk. Using a single RMAN channel may not provide optimal performance because of possible network latencies. It is recommended that you use between 2 and 4 RMAN channels for each backup client.

You can either configure an SBT channel that corresponds to the Recovery Appliance backup module or allocate RMAN SBT channels explicitly for each backup or recovery operation.

**See Also:**

["Using RMAN Channels for Recovery Appliance Backup and Recovery Operations \(page 3-29\)"](#)

1.3.2 About Backing Up Protected Databases to Recovery Appliance

Use the RMAN `BACKUP` command to back up protected databases to Recovery Appliance. When you back up a protected database to the Recovery Appliance for the first time, you must seed the repository by creating an initial level 0 backup of the entire database. A level 0 incremental backup must also be created when point-in-time recovery is performed on the protected database to a time before the oldest backup that exists on the Recovery Appliance.

After the first level 0 backup, your regular backup schedule will consist of creating periodic level 1 cumulative incremental backups of the protected database, the spfile, control files, and archived redo log files. Since archived logs hold records of all changes that occur in the database, these critical files must be backed up more frequently than data files. Frequent archived redo log backups reduce the potential data loss that is incurred, if the protected database is lost and backups need to be recovered.

You can either back up directly to the Recovery Appliance or first create backup sets in a local fast recovery area or disk directory and then copy them to the Recovery Appliance using the `BACKUP BACKUPSET` command.

A good backup strategy must ensure that backups created can actually be restored and used successfully. Because Recovery Appliance validates incoming backups for Oracle block correctness before storing them, you need not include a `RESTORE VALIDATE` command in your periodic full restore and recovery testing. Even virtual backups are periodically validated in-place by a background task running on the Recovery Appliance.

**See Also:**

["About the Recovery Appliance Incremental-Forever Backup Strategy \(page 1-11\)"](#)

1.3.2.1 About Backup Encryption and Recovery Appliance

You can configure protected databases to use backup encryption. If a backup is encrypted during an RMAN backup operation to Recovery Appliance, then the backup remains encrypted on the Recovery Appliance. A subsequent copy of this backup to tape will also remain in an encrypted format. However, Oracle recommends that you avoid using RMAN backup encryption when performing backups to Recovery Appliance. Encrypted backups are not ingested by Recovery Appliance and cannot be

used to construct virtual full backups or be part of an incremental-forever backup strategy.

Backups that are copied to tape from the Recovery Appliance can be encrypted using hardware-based encryption on tape drives or using Oracle Secure Backup.

 **See Also:**

Oracle Secure Backup Administrator's Guide for information about hardware-based encryption

1.3.3 About Restoring and Recovering Protected Databases Using Recovery Appliance

When restoring protected databases using backups stored on Recovery Appliance, a full backup is created from the corresponding virtual backup. The Recovery Appliance catalog is used to determine the most appropriate full virtual backup that can be used, based on the point-in-time specified for the recovery. The Recovery Appliance receives the restore request, constructs the physical backup sets from the appropriate virtual backups, and then sends these backup sets to the protected database through the SBT channels that was allocated earlier. On the protected database, RMAN validates the received backup sets and uses them to perform the restore operation. The RMAN `RESTORE` command enables you to restore protected databases using Recovery Appliance.

When the RMAN `RECOVER` command is used, the Recovery Appliance catalog is used to determine the appropriate archived log backups that are required to recover the restored data files to the desired point in time. Frequent level 1 incremental backups reduce the number of archived redo logs that need to be applied in case of a failure and this reduces recovery time. Recovery Appliance sends the required backups to the protected database which uses them to recover to a consistent point and to be subsequently opened. If real-time redo transport is configured for the protected database, then the most current archived redo logs are available and the database can be completely recovered with only sub-seconds worth of data loss.

1.3.4 About the Recovery Appliance Incremental-Forever Backup Strategy

While Recovery Appliance can support many different RMAN backup strategies, Oracle strongly recommends using the incremental-forever backup strategy to back up protected databases. This strategy is based on an initial level 0 incremental backup followed by successive level 1 cumulative incremental and archived redo log backups. Apart from the initial full backup, no regular full backups are required. This eliminates traditional backup windows and improves protected database performance.

For each protected database, Recovery Appliance regularly receives scheduled level 1 incremental backups consisting of only the data file block changes relative to the most recent virtual full backup (recorded as level 0 in the recovery catalog). The level 1 backups are validated to ensure that there are no corrupt data blocks, compressed using specialized block-level algorithms, and then written to a storage pool on the Recovery Appliance. Virtual full backups are created based on the incoming

incremental backups. When you need to recover the protected database, Recovery Appliance uses virtual full backups and archived log backups that together allow the recreation of all database changes until the specified recovery time.

You must include archived redo logs in both full and incremental backups. Oracle recommends that you take frequent backups of the archived redo log files and include them in your level 1 incremental backups. Backing up archived redo logs is not required if you configure the protected database to use real-time redo transport.



Note:

"[About Real-Time Redo Transport](#) (page 1-12)"

1.3.4.1 Difference Between RMAN Incrementally Updated and Recovery Appliance Incremental-Forever Backup Strategies

There are important differences between the incremental strategy used in a conventional RMAN setup and the incremental-forever backup strategy used with Recovery Appliance:

- The RMAN incrementally updated backup strategy uses an initial image copy, followed by successive level 1 incremental backups. The image copy is then updated by merging the level 1 incremental backups with the image copy.

Following is an example of a script that is used to implement the RMAN incrementally updated backup strategy:

```
run
{
  RECOVER COPY OF DATABASE
    WITH TAG 'incr_update';
  BACKUP
    INCREMENTAL LEVEL 1
    FOR RECOVER OF COPY WITH TAG 'incr_update'
    DATABASE;
}
```

- With the Recovery Appliance incremental-forever backup strategy, only one level 0 incremental backup is required. Subsequently, level 1 incremental backups are created and stored on the Recovery Appliance. A virtual full backup is created by referencing blocks from the initial level 0 and subsequent level 1 backups.

Following is an example of a script that implements the Recovery Appliance incremental-forever backup strategy:

```
BACKUP CUMULATIVE INCREMENTAL LEVEL 1
  DEVICE TYPE sbt FORMAT '%d_%U' TAG '%TAG'
  DATABASE;
BACKUP DEVICE TYPE sbt FORMAT '%d_%U' TAG '%TAG'
  ARCHIVELOG ALL NOT BACKED UP;
```

1.3.5 About Real-Time Redo Transport

Redo data contains records of all changes made to a database and is therefore critical to minimizing data loss in the event of data failures. Using real-time redo transport

substantially reduces the window of potential data loss that exists between successive archived redo log backups. When real-time redo transport is configured, archived redo log backups are transparent to the database administrator. The incoming redo stream from one or more protected databases is stored in the redo staging area on the Recovery Appliance. Protected databases can recover data up to the last change that the appliance received.

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide for information about Oracle Database releases for which real-time redo transport is supported

1.3.5.1 How Real-Time Redo Transport Works

With real-time redo transport enabled, Recovery Appliance becomes a remote destination for asynchronous redo transport services, similar to a standby database in an Oracle Data Guard environment. Redo data from the protected database is written asynchronously to the Recovery Appliance as it is generated. Load on production database servers is minimized because redo data is shipped directly from the memory to the Recovery Appliance without the involvement of disk I/O. As the redo stream is received, compressed archived log backups are created in the protected database's storage location every time a log switch occurs. The archived log backups generated by the Recovery Appliance are recorded in the Recovery Appliance catalog as normal backups and can be restored and applied to data files using the `RMAN RECOVER` command.

 **See Also:**

Oracle Data Guard Concepts and Administration for information about asynchronous redo transport services

If the protected database crashes, redo data received from the current redo log group until the time of the crash is backed up at the Recovery Appliance as a "partial" archived redo log. If the protected database is reopened, crash recovery of the protected database will complete the current redo log group at the time of the crash, and the completed redo log will be re-shipped to the Recovery Appliance through the automatic Data Guard Gap fetching feature. The "complete" archived redo log will be used in any future restore/recover operations instead of the previously backed up "partial" archived redo log.

During recovery of a protected database, partial and complete archived logs are automatically restored as required to completely recover the protected database.

1.3.5.2 About Configuring Real-Time Redo Transport for Protected Databases

Real-time redo transport requires setup on the Recovery Appliance and the protected database. You need a redo transport user that will be used to authenticate and then send redo data from the protected database to the Recovery Appliance. This user must be the same as the Recovery Appliance user that will be used to send protected

database backups to the Recovery Appliance. The credentials of this Recovery Appliance user are stored in an Oracle wallet on the protected database.

On the protected database, configure `ARCHIVELOG` mode and set up an archive destination for redo data (using the `LOG_ARCHIVE_DEST_n` parameter) that points to the service name of the Recovery Appliance.



See Also:

["Configuring Real-Time Redo Transport \(page 3-24\)"](#)

1.4 Tools for Protected Database Operations

Recovery Appliance provides multiple interfaces to manage backup and recovery operations for protected databases.

- Oracle Enterprise Manager Cloud Control (Cloud Control)
Cloud Control provides a GUI for administering, managing, and monitoring a Recovery Appliance environment. It also enables you to configure, back up, and recover protected databases.
Additional information about using Cloud Control is available in the Cloud Control online help.
- RMAN client
Recovery Appliance is integrated with RMAN and you can use the RMAN client installed on your protected database to configure, back up, and recover protected databases.
- SQL*Plus
SQL*Plus is a command-line tool that you can use to query the Recovery Appliance catalog and run the `DBMS_RA` PL/SQL package.

1.5 Protected Database Administration Task Flow

This section describes the high-level tasks in using Recovery Appliance to store and manage backups for multiple protected databases in the enterprise. These tasks can be performed using Cloud Control or RMAN. Depending on the management interface used, there may be minor variations in the steps to perform certain tasks.



See Also:

Zero Data Loss Recovery Appliance Administrator's Guide for the workflow to manage a Recovery Appliance environment

The task flow for setting up and using Recovery Appliance for enterprise data protection is as follows:

1. Decide on a strategy to migrate your protected database backups to Recovery Appliance as described in "[Migration Considerations for Protected Database Administrators](#) (page 2-1)".

2. Enroll the protected database with a Recovery Appliance.

This step only needs to be performed the first time you configure your protected database to use a Recovery Appliance.

 **See Also:**

- "[Enrolling the Protected Database with Recovery Appliance \(Cloud Control\)](#) (page 3-8)"
- "[Enrolling the Protected Database with Recovery Appliance \(Command Line\)](#) (page 3-12)"

3. Configure backup and recovery settings for the protected database.

This is typically a one-time task that you perform while enrolling a protected database with a Recovery Appliance. However, you can modify backup and recovery settings subsequently.

 **See Also:**

- "[Configuring Backup and Recovery Settings for Protected Databases \(Cloud Control\)](#) (page 3-18)"
- "[Configuring Backup and Recovery Settings for Protected Databases \(Command Line\)](#) (page 3-23)"

4. Perform a test backup to verify that your protected database configuration is accurate.

It is recommended that you perform a test backup when configuration settings are initially set or subsequently modified.

 **See Also:**

- "[Performing Test Backup and Recovery Operations](#) (page 3-30)"

5. Back up the protected database to the Recovery Appliance.

You can schedule protected database backups to be performed at a specified time.

 **See Also:**

- ["Backing Up the Protected Database Using Cloud Control \(page 4-2\)"](#)
- ["Backing Up the Protected Database Using the Command Line \(page 4-5\)"](#)

6. Perform test restore and recovery to assure yourself that the protected database can be recovered using the backups stored on the Recovery Appliance.

 **See Also:**

["Recovering Data from Recovery Appliance \(page 5-1\)"](#)

7. In the event of a failure (caused by a media failure or data corruption), recover the protected database using backups stored on the Recovery Appliance.

Depending on the type of failure, you can recover the entire protected database or just the affected database files.

 **See Also:**

- ["Restoring and Recovering Data from Recovery Appliance Using the Command Line \(page 5-4\)"](#)
- ["Recovering Protected Databases Using Cloud Control \(page 5-1\)"](#)

2

Migration Considerations for Protected Database Administrators

This chapter discusses strategies to migrate from an existing backup strategy to one that uses Recovery Appliance.

This chapter contains the following topics:

- [Planning to Migrate Protected Databases to Recovery Appliance](#) (page 2-1)
- [Adapting an Existing Backup Strategy for Recovery Appliance](#) (page 2-2)
- [Migrating Backup Metadata to the Recovery Appliance Catalog](#) (page 2-4)
- [Migrating Existing Backups to Recovery Appliance](#) (page 2-10)

2.1 Planning to Migrate Protected Databases to Recovery Appliance

A basic backup strategy involving Recovery Manager (RMAN) consists of a set of backup scripts that are scheduled to run at specified intervals. When you decide to use Recovery Appliance for data protection, you need to develop a plan to migrate your existing backup strategy to one that uses Recovery Appliance.

This section provides a high-level overview of the tasks involved in migrating your existing protected database backup strategy to Recovery Appliance. Details about how to perform each task are provided in the following sections.

If you are starting with Recovery Appliance for your protected database's data protection, then skip to [Configuring Protected Databases](#) (page 3-1).

Steps: Planning to Migrate Protected Databases to Recovery Appliance

1. Adapt the existing backup strategy for Recovery Appliance

All RMAN commands, with the exception of those listed in [Differences in RMAN Commands](#) (page A-1) will work with Recovery Appliance. You must make some changes to your existing RMAN backup strategy to adapt it for Recovery Appliance.

See Also:

["Adapting an Existing Backup Strategy for Recovery Appliance \(page 2-2\)"](#)

2. Migrate backup metadata to the Recovery Appliance catalog

Your existing backup strategy may be using an RMAN recovery catalog to store backup metadata for the protected database. You can migrate existing backup metadata for your protected database to the Recovery Appliance catalog.

 **See Also:**

["Migrating Backup Metadata to the Recovery Appliance Catalog \(page 2-4\)"](#)

3. Migrate existing protected database backups to the Recovery Appliance

You can migrate valid database backups that are within the configured recovery window goals to the Recovery Appliance. Alternately, you can start backing up to the Recovery Appliance without migrating existing protected database backups.

 **See Also:**

["Migrating Existing Backups to Recovery Appliance \(page 2-10\)"](#)

2.2 Adapting an Existing Backup Strategy for Recovery Appliance

When you decide to move from an existing backup strategy to one that uses Recovery Appliance for data protection, you need to make some modifications to your existing strategy. All RMAN backup and recovery scripts that you currently use will work in a Recovery Appliance environment with minor modifications.

The following modifications are required to adapt your existing RMAN backup and recovery scripts to work with Recovery Appliance:

- Modify RMAN channel configuration or channel allocations so that they use SBT channels corresponding to the Zero Data Loss Recovery Appliance backup module (Recovery Appliance backup module) instead of disk or tape channels.
- Modify RMAN backup scripts and remove commands whose behavior is modified in Recovery Appliance.
- Simplify existing RMAN scripts by removing commands that are not required in a Recovery Appliance environment.

 **See Also:**

- ["Modifying RMAN Channel Configurations \(page 2-3\)"](#)
- ["Modifying RMAN Backup and Recovery Scripts \(page 2-3\)"](#)
- ["Removing Unnecessary RMAN Commands \(page 2-4\)"](#)

2.2.1 Modifying RMAN Channel Configurations

An RMAN channel represents one stream of data to or from a backup device. The channel reads data from the input device, processes it, and then writes it to the output device. RMAN supports the following types of channel configurations:

- DISK (backups are stored on disk)
- SBT
Backups are stored on one of the following: tape using media management software such as Oracle Secure Backup, Recovery Appliance using the Recovery Appliance backup module, or on the Oracle Cloud.

Existing RMAN scripts will use either a DISK channel to backup to disk or an SBT channel to backup to tape. To back up to or restore from Recovery Appliance, you must configure use an SBT channel that corresponds to the Recovery Appliance backup module installed on the protected database host. In a Recovery Appliance environment, your backup and recovery scripts must allocate an SBT channel with the `SBT_LIBRARY` parameter pointing to the Recovery Appliance backup module.



See Also:

"[Using RMAN Channels for Recovery Appliance Backup and Recovery Operations](#) (page 3-29)" for examples of allocating or configuring RMAN channels for use with Recovery Appliance

2.2.2 Modifying RMAN Backup and Recovery Scripts

If your backup scripts use any RMAN commands whose functionality is slightly modified in Recovery Appliance (listed in [Differences in RMAN Commands](#) (page A-1)), then you must modify the scripts to replace these commands with the appropriate new commands. For example, the RMAN `UNREGISTER DATABASE` command functionality works differently with Recovery Appliance. Therefore, you must modify your existing RMAN scripts to replace the `UNREGISTER DATABASE` command. Note that the `DBMS_RA.DELETE_DB` procedure that must be used instead of `UNREGISTER DATABASE` can be used only from SQL*Plus, not RMAN.

If your existing backup strategy uses the RMAN incrementally updated backup strategy that merges successive level 1 incremental backups with the initial image copy backup, then modify the RMAN commands to use the Recovery Appliance incremental-forever backup strategy.



See Also:

- [Backing Up Protected Databases](#) (page 4-1)
- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about using the `DBMS_RA.DELETE_DB` procedure

2.2.3 Removing Unnecessary RMAN Commands

Typically RMAN backup and recovery scripts contain commands to validate backups. This includes commands such as `VALIDATE` and `CROSSCHECK`. Because Recovery Appliance automatically validates all backups from protected databases before writing them to the storage, these commands are no longer required after migrating your existing data protection strategy to use Recovery Appliance. While adapting your existing strategy to use Recovery Appliance, remove the `VALIDATE` and `CROSSCHECK` commands from your scripts.

From your existing backup strategy, you also need to remove those operations that will now be performed by Recovery Appliance, such as backing up to tape and deleting obsolete backups.

2.3 Migrating Backup Metadata to the Recovery Appliance Catalog

Your existing RMAN backup strategy typically involves storing backup metadata in an RMAN recovery catalog. When migrating to a data protection strategy that uses Recovery Appliance, you need a strategy to manage existing backup metadata that is stored in an RMAN recovery catalog.

See Also:

- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about the Recovery Appliance catalog
- *Oracle Database Backup and Recovery User's Guide* for more information about the RMAN recovery catalog

To manage existing backup metadata while moving to Recovery Appliance, use one of the following strategies:

- Import existing backup metadata for your protected database into the Recovery Appliance catalog

Importing backup metadata stored in an RMAN recovery catalog ensures that existing backup metadata for your protected databases is now contained in the Recovery Appliance catalog.

See Also:

["Importing Protected Database Metadata into the Recovery Appliance Catalog \(page 2-6\)"](#)

- Retain existing backup metadata in the RMAN recovery catalog and store metadata for backups created to Recovery Appliance in the Recovery Appliance catalog

You must manage the RMAN recovery catalog in conjunction with the Recovery Appliance catalog. To create local backups and store the backup metadata in the RMAN recovery catalog, use the steps described in "[Creating Local Backups](#) (page 2-13)". To create backups to a Recovery Appliance, configure the protected database and then back up to the Recovery Appliance.

 **See Also:**

- "[Configuring Protected Databases](#) (page 3-1)"
- "[Backing Up Protected Databases](#) (page 4-1)"

2.3.1 Connecting to the Protected Database and Recovery Appliance Using CLI

To perform protected database backup or recovery operations using a Recovery Appliance, you must connect to the protected database and to the Recovery Appliance catalog. The connection to the protected database is established as target using operating system authentication or password file authentication. The connection to the Recovery Appliance catalog must be established as catalog. If the protected database is a pluggable database (PDB), then you must connect to the root of the multitenant container database (CDB) as `TARGET`.

To connect to a protected database (non-CDB) and Recovery Appliance:

1. Start RMAN.

```
% rman
```

2. Use the `CONNECT` command to connect to the protected database as `TARGET` and to the Recovery Appliance catalog as `CATALOG`.

The following command connects to the protected database as the `sys` user. `ra_rman_user` is the Recovery Appliance user that the protected database uses to authenticate with the Recovery Appliance. `ra1` is the net service name of the target Recovery Appliance that is configured in the Oracle wallet. Enter the passwords for both users when prompted.

```
RMAN> CONNECT TARGET sys as sysdba;  
RMAN> CONNECT CATALOG ra_rman_user@ra1;
```

To connect to a protected database (CDB) and Recovery Appliance:

1. Start RMAN.

```
% rman
```

2. Use the `CONNECT` command to connect as `TARGET` to the root of the CDB and to the Recovery Appliance catalog as `CATALOG`.

 **Note:**

Connecting to the Recovery Appliance as `CATALOG` when connected to a PDB as `TARGET` is not supported. When using the Recovery Appliance catalog, RMAN must connect as `TARGET` to the root of the CDB for backup and recovery operations.

The following command, run from the CDB, connects to the root as the common user `c##bkuser` user. `my_cdb` is the net service name of the CDB. `ra_rman_user` is the Recovery Appliance user that the protected database uses to authenticate with the Recovery Appliance. `ra1` is the net service name of the target Recovery Appliance. Enter the passwords for both users when prompted.

```
RMAN> CONNECT TARGET c##bkuser@my_cdb;  
RMAN> CONNECT CATALOG ra_rman_user@ra1;
```

 **See Also:**

Oracle Database Backup and Recovery User's Guide for additional examples on connecting as `TARGET` to the root of a CDB

2.3.2 Importing Protected Database Metadata into the Recovery Appliance Catalog

To use Recovery Appliance for data protection of your protected databases, metadata for these protected databases must be stored in the Recovery Appliance catalog and not in an RMAN recovery catalog. Existing backup metadata that is currently stored in an RMAN recovery catalog can be imported into the Recovery Appliance catalog. It is recommended that you import your existing recovery catalogs into the Recovery Appliance catalog.

An RMAN recovery catalog can store metadata for one or more protected databases. While importing an RMAN recovery catalog into the Recovery Appliance catalog, you can import metadata related to only some databases or import all the metadata in the RMAN recovery catalog.

Note that importing your existing catalog to the Recovery Appliance catalog copies the backup metadata only. The existing backups themselves are not copied to the Recovery Appliance during catalog import. If required, you must separately copy existing backups as described in "[Migrating Existing Backups to Recovery Appliance](#) (page 2-10)".

2.3.2.1 Steps to Import Protected Database Metadata Into Recovery Appliance

1. Complete the preparation steps described in "[Preparing to Import an RMAN Recovery Catalog into Recovery Appliance](#) (page 2-7)".
2. Import the RMAN recovery catalog that stores metadata for the protected database that is being migrated to the Recovery Appliance as described in "[Importing Protected Database Metadata Using the IMPORT CATALOG Command](#) (page 2-9)".

2.3.2.2 Preparing to Import an RMAN Recovery Catalog into Recovery Appliance

Before importing a protected database's metadata from an RMAN recovery catalog into the Recovery Appliance catalog, some actions must be performed both on the protected database and on the Recovery Appliance.

1. Perform the following steps on the Recovery Appliance:
 - a. Create a Recovery Appliance user that will be used by the protected database whose metadata is being migrated. The protected database authenticates with the Recovery Appliance using this Recovery Appliance user.
 - b. Create a protection policy that will be used by the protected database whose metadata is being migrated.

You can also use an existing protection policy, if it meets the requirements for the protected database being migrated.
 - c. Enroll the protected database whose metadata is being migrated with the Recovery Appliance.

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide for more information about performing these steps

2. Perform the following steps on the protected database:
 - a. If the source RMAN recovery catalog is not contained in an Oracle 12c Release 1 database, then upgrade the recovery catalog database to Oracle 12c Release 1.

 **See Also:**

Oracle Database Upgrade Guide for information about upgrading a database to Oracle Database 12c Release 1 (12.1).

- b. Install the Recovery Appliance backup module that creates the shared library required to transfer backup data to the Recovery Appliance.

Installing the backup module will create the Oracle wallet that contains credentials used to authenticate the protected database with the Recovery Appliance.

 **See Also:**

["Installing the Recovery Appliance Backup Module \(page 3-14\)"](#)

- c. Connect as `TARGET` to the protected database and as `CATALOG` to the RMAN recovery catalog that stores metadata for the protected database.

The following example connects as `TARGET` to the protected database and as `CATALOG` to the source RMAN recovery catalog. The owner of the RMAN recovery catalog is `rman_cat11` and `dbrcat11` is the net service name of the RMAN recovery catalog database. Replace `rmancat11_pswd` with the password of the `rman_cat11` user.

```
$ rman target / catalog rman_cat11/rmancat11_pswd@dbrcat11
```

- d. Ensure that no backups from the protected database are being created to the RMAN recovery catalog.

The following commands connect to SQL*Plus as the owner of the source RMAN recovery catalog and query for backups that are being created to the RMAN recovery catalog `rman_cat11`.

```
$ sqlplus rman_cat11/rmancat11_pswd@dbrcat11
SQL> SELECT username, module
       FROM v$session
       WHERE username = 'RMAN_CAT11';
```

This query should not return any results. Rows returned indicate a connection for what could be an ongoing backup or restore operation. If rows are returned, verify that there are no connections, then retry the query.

- e. Determine the number of backup pieces contained in the catalog for the protected database.

The following example lists the number of backup pieces for the protected database `MY_PTDB`:

```
SQL> SELECT db_name, COUNT(*)
       FROM rc_backup_piece_details
       WHERE db_name='MY_PTDB';
```

- f. Exit SQL*Plus, and reconnect as `TARGET` to the protected database and as `CATALOG` to the source RMAN recovery catalog to verify that the backups in the recovery catalog are valid and can be used for a successful recovery operation.

```
$ rman target / catalog rman_cat11/rmancat11_pswd@dbrcat11
```

You can either verify the backups by restoring them or by using the `RESTORE ... VALIDATE` command.

See Also:

Oracle Database Backup and Recovery Reference for details about using the `RESTORE ... VALIDATE` command

- g. Connect to SQL*Plus as the owner of the source RMAN recovery catalog and run the `dbmsrmansys.sql` script. This script grants additional privileges that are required for the `RECOVERY_CATALOG_OWNER` role.

```
$ sqlplus rman_cat11/rmancat11_pswd@dbrcat11
SQL> $ORACLE_HOME/rdbms/admin/dbmsrmansys.sql
SQL> exit
```

The `rman_cat11` user owns the RMAN recovery catalog and the net service name of the recovery catalog database is `dbrcat11`. Replace `rmancat11_pswd` with the password of the `rman_cat11` user.

- h. On the Recovery Appliance, start an RMAN session and connect to the Recovery Appliance as `TARGET` using the `RASYS` user and to the source RMAN recovery catalog as `CATALOG`.

The following command connects as `TARGET` to the Recovery Appliance and as `CATALOG` to the source RMAN recovery catalog.

```
$ rman target rsys/rsys_pswd
RMAN> CONNECT CATALOG rman_cat11/rmancat11_pswd@dbrcat11
```

`RASYS` is the owner of the Recovery Appliance catalog. Replace `rsys_pswd` with the password of the `rsys` user. The owner of the source RMAN recovery catalog is `rman_cat11` and the service name of the recovery catalog database is `dbrcat11`. Replace `rmancat11_pswd` with the password of the `rman_cat11` user.

- i. Upgrade the source RMAN recovery catalog to Oracle Database 12c Release 1 (12.1.0.2). The `UPGRADE CATALOG` command needs to be entered twice for confirmation.
 - `UPGRADE CATALOG;`
`UPGRADE CATALOG;`
- j. Repeat Steps 2.d (page 2-8) through 2.f (page 2-8) on the upgraded source RMAN recovery catalog to verify that the upgraded catalog is fine and can be used to recover the protected database.

2.3.2.3 Importing Protected Database Metadata Using the `IMPORT CATALOG` Command

Use the RMAN `IMPORT CATALOG` command to import metadata from an RMAN recovery catalog into the Recovery Appliance catalog.

The version of the source RMAN recovery catalog schema must be equal to the current version of the Recovery Appliance recovery catalog schema (12.1.0.2). Upgrade the source recovery catalog schema to 12.1.0.2 if needed.

To import protected database metadata into the Recovery Appliance catalog:

1. Start RMAN and connect as `CATALOG` using the `rsys` user. Note that `rsys` is the owner of the Recovery Appliance catalog.

The following command (replace `ra_pswd` with the password of the `rsys` user) connects as `CATALOG` to the Recovery Appliance catalog. The Single Client Access Name (SCAN) of the Recovery Appliance is `ra-scan` and the service name of the Recovery Appliance metadata database is `zdlra5`. `rsys` is the Recovery Appliance catalog owner.

```
# rman CATALOG rsys/ra_pswd@ra-scan:1521/zdlra5
```

2. Import the source RMAN recovery catalog into the Recovery Appliance catalog. The credentials of the source RMAN recovery catalog are provided by the protected database administrator.

Use the `NO UNREGISTER` clause to specify that the protected database must not be unregistered from the source RMAN recovery catalog that it is currently using.

The following command imports all the metadata contained in the source RMAN recovery catalog that is owned by the user `rman_cat11` (replace `rmancat11_pswd` with the password of the `rman_cat11` user).

```
IMPORT CATALOG rman_cat11/rmancat11_pswd@dbrcat11 NO UNREGISTER;
```

The following command imports the metadata for the protected database with database name `MY_PTDB` contained in the source RMAN recovery catalog that is owned by the user `rman_cat11` (replace `rmancat11_pswd` with the password of the `rman_cat11` user).

```
IMPORT CATALOG rman_cat11/rmancat11_pswd@dbrcat11  
DB_NAME 'MY_PTDB' NO UNREGISTER;
```

3. Verify that all the backup pieces are included in the Recovery Appliance catalog by querying the `RC_BACKUP_PIECE_DETAILS` view.

Compare the number of rows returned by the query in Step 2.e (page 2-8) of "[Preparing to Import an RMAN Recovery Catalog into Recovery Appliance](#) (page 2-7)" with the output of this step. The number of backup pieces returned by both queries must be the same.

See Also:

Oracle Database Backup and Recovery Reference for information about the `IMPORT CATALOG` command

2.4 Migrating Existing Backups to Recovery Appliance

Your existing backup strategy may store protected database backups in a local disk location or on a shared disk. After you import the metadata for the protected database backups into the Recovery Appliance catalog, you must migrate existing backups that are within the recovery window goals to the Recovery Appliance storage. You can migrate backups for only a subset of the protected databases contained in the imported RMAN recovery catalog. However, for all the databases represented in the imported catalog, you can begin using the Recovery Appliance catalog as your recovery catalog.

Note:

To begin using an incremental-forever backup strategy with Recovery Appliance, you must first submit a level 0 incremental backup. If a recent level 0 incremental backup already exists for a particular protected database, it might be more convenient to migrate that backup into the Recovery Appliance, rather than take another level 0 backup from the database. After migrating the level 0 backup and any required existing level 1 backups and archived log files, you can then begin the incremental-forever strategy by sending level 1 incremental backups and archived log files.

The recommended strategy is to migrate all existing backups and switch immediately to Recovery Appliance. Any backups created after you migrate existing backups must be stored on the Recovery Appliance.

Use one of the following techniques to migrate existing protected database backups that are stored on disk to the Recovery Appliance:

- Configure a backup polling location where all the existing protected database backups can be placed. Next, set up the Recovery Appliance to poll this location and pick up the protected database backups.

See "[Setting Up Backup Polling to Migrate Existing Backups to the Recovery Appliance](#) (page 2-11)".

If you have existing backups that are stored on tape, then use the steps described in "[Making Tape Backups Available to Recovery Appliance](#) (page 2-12)".

- Back up image copies that are stored on local disk storage as backup sets to the Recovery Appliance using the `RMAN BACKUP AS BACKUPSET COPY OF DATABASE` command. You must configure an SBT channel that corresponds to the Recovery Appliance backup module, as described in "[Configuring RMAN SBT Channels for Recovery Appliance](#) (page 3-29)", before you run this command.

See Also:

- "[Importing Protected Database Metadata into the Recovery Appliance Catalog](#) (page 2-6)"
- *Oracle Database Backup and Recovery Reference* for details about the syntax of the `BACKUP AS BACKUPSET` command

2.4.1 Setting Up Backup Polling to Migrate Existing Backups to the Recovery Appliance

This section describes how to migrate protected database backups that are currently stored in a polling location to the Recovery Appliance storage. A polling location is a file system directory on shared storage, outside the Recovery Appliance, that stores backup pieces and archived redo log files for a protected database. The Recovery Appliance polls this location at specified intervals, retrieves any new backups, and stores them on the Recovery Appliance.

To import existing backup sets by configuring a polling location:

1. On the Recovery Appliance, create a polling policy corresponding to the polling location that contains the protected database backups to be migrated.

The following example, when connected as the `RASYS` user to SQL*Plus, creates a polling policy called `MIGRATION_LINUX` that polls the location `/polling/shared_backup_location` for backups.

```
BEGIN
    DBMS_RA.CREATE_POLLING_POLICY (
        polling_policy_name => 'MIGRATION_LINUX',
        polling_location => '/polling/shared_backup_location',
        polling_frequency => INTERVAL '1' MINUTE,
```

```
delete_input => FALSE);
END;
```

2. On the Recovery Appliance, use the `DBMS_RA.UPDATE_PROTECTION_POLICY` procedure to assign the polling policy created in Step 1 (page 2-11) to the protection policy that is associated with the protected database.

Set the `delete_input` parameter to `False` to indicate that the backups must not be deleted from the source location.

See Also:

Zero Data Loss Recovery Appliance Administrator's Guide

3. Mount the polling location directory on the Recovery Appliance database nodes as described in "[Mounting the NFS Storage for Backup Polling](#) (page 2-12)".
4. Verify that the backup sets have been imported by querying the `ra_task` view.

You can also query the `rc_backup_piece_details` view to display the backup pieces for protected databases that are being polled.

2.4.1.1 Mounting the NFS Storage for Backup Polling

When you use backup polling, you must mount the Network File System (NFS) directory that stores backups for this protected database. Ensure that the path is accessible

Use the following steps to mount the polling location directory on the Recovery Appliance database nodes:

1. As the `root`, create the directory that will be used as the polling location.

```
# mkdir /polling_import
```

2. As `root`, mount the polling location using the following command:

```
# mount -o options nfs_server_name:nfs_directory_name directory
```

where `options` represent the NFS mount options, `nfs_server_name` is the host name of the NFS server, `directory_name` is the directory on the NFS server, and `directory` is the mount point directory.

The following example attaches the `/backup/bkp_db_imp` directory on the NFS server `myNFShost` at the directory `polling_import`:

```
# mount -o rw,hard,rsize=32768,wspace=32768,tcp,vers=3,timeo=600,actimeo=0
myNFShost:/backup/bkp_db_imp/source_bkp_dir /polling_import
```

3. Ensure that the `oracle` user has read permission for the mounted directory.

2.4.2 Making Tape Backups Available to Recovery Appliance

If your current tape backup strategy uses third-party media management software, you can make these tape backups available to the Recovery Appliance. Note that you need to import the metadata for these tape backups into the Recovery Appliance catalog.

To make tape backups available to Recovery Appliance:

1. Allocate an SBT channel that corresponds to the Recovery Appliance backup module.
2. Allocate an SBT channel that corresponds to the media management library that manages the existing tape backups.
3. Maintain both these SBT channels until the retention period or recycling period of the tapes is reached.

During this period, if required, the protected database can be recovered using the backups stored on tape.

4. After the retention period or recycling period of the tapes is reached, release the channel configured in Step 2 (page 2-13).

 **See Also:**

["Importing Protected Database Metadata Using the IMPORT CATALOG Command \(page 2-9\)"](#)

2.4.3 Creating Local Backups

When you create protected database backups to local disk storage, metadata about these backups is stored in an RMAN recovery catalog. If an RMAN recovery catalog is not configured, or if you do not connect to the catalog, then the metadata is stored in the protected database control file.

To create local backups of the protected database:

1. Connect RMAN to the protected database as `TARGET` and connect to an RMAN recovery catalog as `CATALOG`.

The following command connects as `TARGET` to the protected database with service name `hr_ptdb` and as `CATALOG` to an RMAN recovery catalog database with net service name `catdb`. `rco` is the RMAN recovery catalog owner and `hradm` is a user with `SYSDG` privileges on the protected database. Enter the password for the `hradm` and `rco` users when prompted.

```
% rman TARGET hradm@hr_ptdb CATALOG rco@catdb
```

2. Create local backups of the protected database.

Depending on your backup strategy, you can create full or incremental backups. Include archived redo log files in all backups to minimize the time required to recover from a failure. Allocate an RMAN channel of device type `DISK` to store backups to the local disk.

The following example allocates a disk channel and creates a level 1 incremental backup of the entire database including the archived redo log files:

```
RUN
{
  ALLOCATE CHANNEL d1 DEVICE TYPE DISK;
  BACKUP INCREMENTAL LEVEL 1
    DATABASE
```

```

    PLUS ARCHIVELOG;
}

```

Because no location is specified in the command, the backups are stored in the local fast recovery area that is configured for the protected database. To store backups on locally configured tape devices, allocate an SBT channel that corresponds to the legacy media management software.

2.4.4 Recovering Protected Databases Using Local Backups

When you create protected database backups to a local disk location, you can use regular RMAN commands to perform recovery. You need to configure one of the following before you restore and recover the protected database:

- disk channels that corresponds to the disk location where the backups are stored
- SBT channels that correspond to backups on legacy media management environments where the backups are stored

To perform complete recovery of a protected database using local disk backups:

1. Connect RMAN to the protected database as `TARGET` and connect to the RMAN recovery catalog as `CATALOG`.

The following command connects as `TARGET` to the protected database with net service name `hr_ptdb` and as `CATALOG` to an RMAN recovery catalog database with net service name `rco`. `hradm` is a user with `SYSPBACKUP` privileges on the protected database and `rco` is the RMAN recovery catalog owner. Enter the passwords for the `hradm` and `rco` users when prompted.

```
% rman TARGET hradm@hr_ptdb CATALOG rco@catdb
```

2. Allocate an RMAN channel of device type `DISK` to use backups stored on local disk storage.

The following command allocates a disk channel that creates backups to the local disk storage.

```
RMAN> ALLOCATE CHANNEL d1 DEVICE TYPE DISK;
```

3. Restore and recover the protected database using the `RESTORE` and `RECOVER` commands respectively.

The following example performs complete recovery of the protected database:

```

RUN
{
  STARTUP MOUNT;
  ALLOCATE CHANNEL c1 DEVICE TYPE DISK;
  RESTORE DATABASE;
  RECOVER DATABASE;
  ALTER DATABASE OPEN;
}

```

3

Configuring Protected Databases

This chapter describes how to configure protected databases for backup and recovery operations with Recovery Appliance.

This chapter contains the following topics:

- [Overview of Configuring Protected Databases for Recovery Appliance](#) (page 3-1)
- [Enrolling the Protected Database with Recovery Appliance \(Cloud Control\)](#) (page 3-8)
- [Enrolling the Protected Database with Recovery Appliance \(Command Line\)](#) (page 3-12)
- [Configuring Backup and Recovery Settings for Protected Databases \(Cloud Control\)](#) (page 3-18)
- [Configuring Backup and Recovery Settings for Protected Databases \(Command Line\)](#) (page 3-23)
- [Performing Test Backup and Recovery Operations](#) (page 3-30)

3.1 Overview of Configuring Protected Databases for Recovery Appliance

To use Recovery Appliance as a centralized repository for your protected database backups, configuration is required both on the Recovery Appliance and on the protected database. You can use Enterprise Manager Cloud Control (Cloud Control) or RMAN to configure protected databases.

On the Recovery Appliance, the configuration steps include creating a protection policy that is assigned to the protected database, creating a Recovery Appliance user who owns the virtual private catalog, and granting access for the protected databases to a Recovery Appliance user. These steps are described in *Zero Data Loss Recovery Appliance Administrator's Guide*.

On the protected database, the configuration includes enabling the protected database to access the Recovery Appliance, adding protected database metadata to the Recovery Appliance, and specifying settings that will be used during backup and recovery operations.

 **Note:**

Oracle recommends that you use a server parameter file for your protected database.

 **Note:**

Oracle wallets created by Cloud Control support HTTP transport only. To use HTTPS transport, the wallet needs to be set up outside of Cloud Control.

3.1.1 Steps to Configure Protected Databases for Recovery Appliance

Configuring protected databases performs the set up tasks required to back up and recover protected databases using Recovery Appliance.

To configure a protected database for Recovery Appliance:

1. Enroll the protected database with a Recovery Appliance.

Enrolling is a one-time task that must be performed the first time you set up a protected database to use the Recovery Appliance.

 **See Also:**

- ["Enrolling the Protected Database with Recovery Appliance \(Cloud Control\) \(page 3-8\)"](#)
- ["Enrolling the Protected Database with Recovery Appliance \(Command Line\) \(page 3-12\)"](#)

2. Configure backup and recovery settings for the protected database.

These settings are used during backup and recovery operations for the protected database. The settings can be modified according to the backup or recovery task that is being performed.

 **See Also:**

- ["Configuring Backup and Recovery Settings for Protected Databases \(Cloud Control\) \(page 3-18\)"](#)
- ["Configuring Backup and Recovery Settings for Protected Databases \(Command Line\) \(page 3-23\)"](#)

3. Perform a test backup to verify that your protected database configuration is successful as described in ["Performing a Test Backup Using Cloud Control \(page 3-31\)"](#).

 **See Also:**

- ["Overview of Enrolling Protected Databases \(page 3-5\)"](#)
- ["Overview of Protected Database Backup Settings \(page 3-6\)"](#)
- ["Overview of Protected Database Recovery Settings \(page 3-7\)"](#)

3.1.2 Overview of Recovery Appliance Backup Module

The Recovery Appliance backup module is an Oracle-supplied SBT library that functions as a media management library. RMAN uses the Recovery Appliance backup module to transfer backup data over the network to the Recovery Appliance. The backup module is referenced when allocating or configuring an RMAN SBT channel for backup or recovery operations to the Recovery Appliance. All backups to the Recovery Appliance, and all restores of complete backup sets, are performed by means of this backup module.

3.1.2.1 Install Location for the Recovery Appliance Backup Module

The Recovery Appliance backup module must be installed in the following locations:

- In the Oracle home of every protected database that uses RMAN to backup protected databases to Recovery Appliance
If a particular Oracle home is used by more than one protected database, then the backup module must be installed only once in this Oracle home.
- On every upstream Recovery Appliance that sends backups to downstream Recovery Appliances in replication environments

The library for the Recovery Appliance backup module, `libra.so`, is preinstalled on Recovery Appliance. However, the Oracle wallet containing the replication user credentials must be created on the upstream Recovery Appliance.

 **See Also:**

- ["Installing the Recovery Appliance Backup Module \(page 3-14\)"](#)
- *Zero Data Loss Recovery Appliance Administrator's Guide*

3.1.2.2 Recovery Appliance Backup Module Configuration File

The Recovery Appliance backup module configuration file contains the configuration settings that are used when protected databases communicate with the Recovery Appliance. The configuration file is created automatically when the Recovery Appliance backup module is installed on the protected database host.

You can also set some Recovery Appliance backup module configuration parameters inline, while configuring or allocating RMAN SBT channels for the Recovery Appliance, as shown in [Example 3-3 \(page 3-29\)](#) and [Example 3-4 \(page 3-30\)](#).



See Also:

"[Configuration Parameters for the Recovery Appliance Backup Module](#) (page 3-4)" for the configuration parameters that can be specified while installing the Recovery Appliance backup module

3.1.2.3 Configuration Parameters for the Recovery Appliance Backup Module

Table 3-1 (page 3-4) describes the configuration parameters that are used when installing the Recovery Appliance backup module. These parameters are used by protected databases while backing up to and restoring from Recovery Appliance.

Table 3-1 Recovery Appliance Backup Module Installer Parameters

Parameter Name	Mandatory/Optional	Description
dbUser	Mandatory	User name of the Recovery Appliance user who has the privileges required to connect to, send, and receive backups for the protected database
dbPass	Mandatory	Password for the dbUser user
host	Mandatory	SCAN host name of the Recovery Appliance
port	Mandatory	Listener port number of the Recovery Appliance metadata database
serviceName	Mandatory	Service name of the Recovery Appliance metadata database
walletDir	Mandatory	Location of the Oracle wallet that stores the Recovery Appliance user credentials and the proxy information used to connect to the Recovery Appliance. Note: If an Oracle wallet already exists in this directory, then the Recovery Appliance backup module installer overwrites the existing wallet.
proxyHost	Optional	Host name or IP address and TCP port of a proxy server through which to make an HTTP connection to the Recovery Appliance, in the form <i>host:port</i> .
configFile	Optional	Location of the configuration file that stores the configuration parameters for the Recovery Appliance backup module. The default location on Linux/UNIX is <code>\$ORACLE_HOME/dbs/raORACLE_SID.ora</code> . On Windows, the default location is <code>\$ORACLE_HOME\database\raORACLE_SID.ora</code> .

Table 3-1 (Cont.) Recovery Appliance Backup Module Installer Parameters

Parameter Name	Mandatory/Optional	Description
libDir	Optional	<p>Location where the shared library for the Recovery Appliance backup module is stored. This library is used to transfer backup data over the network to the Recovery Appliance.</p> <p>It is recommended that you store the shared library in <code>\$ORACLE_HOME/lib</code> on Linux/UNIX and in <code>\$ORACLE_HOME\database\lib</code> on Windows.</p> <p>When you omit this parameter, the installer does not download the shared library. Downloading the library is not required only when you regenerate the Oracle wallet and configuration file in an Oracle home where the backup module was previously installed.</p>
libPlatform	Optional	<p>Platform name of the protected database host on which the Recovery Appliance backup module needs to be installed.</p> <p>Typically, the Recovery Appliance backup module installer automatically determines the platform on which it is run. You need to set this parameter only if the installer displays an error indicating the platform cannot be determined.</p> <p>Valid values for platform name are: linux64, windows64, solaris_sparc64, solaris_sparcx64, zlinux64, aix_ppc64, and hpux_ia64.</p>
argFile	Optional	<p>File from which the remaining command-line parameters must be read during the Recovery Appliance backup module installation.</p>



See Also:

["Installing the Recovery Appliance Backup Module \(page 3-14\)"](#)

3.1.3 Overview of Enrolling Protected Databases

Enrolling a protected database enables a specific Recovery Appliance to receive backups from the protected database. This is a one-time task that must be performed the first time you set up a protected database to use Recovery Appliance. Enrolling requires steps to be performed on both the Recovery Appliance and the protected database.

Enrolling a protected database performs the following tasks:

- Configures credentials required for the protected database to access the Recovery Appliance

The protected database administrator requires credentials to authenticate with the Recovery Appliance and perform backup and recovery operations. This is done by associating a protected database administrator user with a Recovery Appliance

user (in the Recovery Appliance metadata database). These credentials are stored in an Oracle wallet that is created on the protected database.

- Defines recovery window goals and allocates reserved space on the Recovery Appliance by associating the protected database with an appropriate protection policy
- Grants access to the protected database to the Recovery Appliance user
- Registers the protected database with the Recovery Appliance catalog

Metadata for protected database backups must be stored in the Recovery Appliance catalog. There are multiple virtual private catalogs within the Recovery Appliance catalog. You must specify the virtual private catalog owner that will manipulate metadata for this protected database.

- When you use Cloud Control, an Enterprise Manager administrator must be provided access to the named credentials that are used to connect to a Recovery Appliance from Cloud Control. Enterprise Manager administrators that administer backup and restore operations for the protected database need access to these credentials in order to connect to the Recovery Appliance when configuring protected databases to backup to and restore from the Recovery Appliance.

 **See Also:**

- ["Enrolling the Protected Database with Recovery Appliance \(Cloud Control\) \(page 3-8\)"](#)
- ["Enrolling the Protected Database with Recovery Appliance \(Command Line\) \(page 3-12\)"](#)

3.1.4 Overview of Protected Database Backup Settings

Before you back up a protected database to Recovery Appliance, you must configure the protected database backup settings. These settings, described in [Table 3-2](#) (page 3-6), define the default behavior for your protected database backup environment. RMAN assigns default values for each backup setting. However, it is recommended that you configure settings according to the backup requirements of the protected database.

Table 3-2 Protected Database Backup Settings

Backup Setting	Description
Control file autobackup	Specifies that the control file and server parameter file must be automatically backed up whenever a backup record is added or database structure metadata in the control file changes.
Disk backup location	When configuring backups for the Recovery Appliance, if backup polling is required, then specify the backup polling location.
Backup optimization	Skips the backup of files when an identical file has already been backed up to the Recovery Appliance.

Table 3-2 (Cont.) Protected Database Backup Settings

Backup Setting	Description
Retention policy	Specifies which backups must be retained to meet your recovery goals. You can either specify a recovery window or a redundancy value. This setting needs to be specified when you use a parallel backup strategy and need to delete obsolete backups created by your existing (not Recovery Appliance) backup strategy.
Archived redo log deletion policy	Specifies when archived redo logs are eligible for deletion. This policy applies to all archiving destinations including the fast recovery area.

 **See Also:**

- *Oracle Database Backup and Recovery User's Guide*
- ["Configuring Backup Settings for Protected Databases Using Cloud Control \(page 3-18\)"](#)
- ["Configuring Backup Settings for Protected Databases Using the Command Line \(page 3-24\)"](#)

3.1.5 Overview of Protected Database Recovery Settings

Table 3-3 (page 3-7) describes the recovery settings for protected databases. The values of some settings (for example, fast recovery area), are assigned based on how the protected database is configured for the Recovery Appliance.

Table 3-3 Protected Database Recovery Settings

Recovery Setting	Description
Desired mean time to recover	The Mean Time to Recover (MTTR) is the time required to recover the protected database. Plan your backup strategy based on an MTTR that is acceptable for your protected database.

Table 3-3 (Cont.) Protected Database Recovery Settings

Recovery Setting	Description
ARCHIVELOG mode	<p>The ARCHIVELOG mode enables archiving of filled groups of online redo log files immediately after a redo log switch occurs. Optionally, configure the following additional properties for the protected database:</p> <ul style="list-style-type: none"> Log Archive File Name Format Specifies the default file name format for archived redo log files. Use a text string and variables to specify this value. Valid variables are described in <i>Oracle Database Reference</i>. Archived Redo Log Destination To use the fast recovery area as the redo log destination, set the Archived Redo Log Destination to <code>USE_DB_RECOVERY_FILE_DEST</code>. <p>Note: Running the protected database in ARCHIVELOG mode is mandatory if you want to send redo data to the Recovery Appliance.</p> <p>See Also: <i>Oracle Database Administrator's Guide</i> for information about configuring your database to run in ARCHIVELOG mode.</p>
Fast recovery area	<p>A fast recovery area is a disk location that stores backup-related files such as RMAN backups, archived redo log files, control file and online redo log file copies. The fast recovery area automates management of backup-related files and minimizes the need to manually manage disk space for backup-related files.</p> <p>See Also: <i>Oracle Database Backup and Recovery User's Guide</i> for more information about configuring a fast recovery area.</p>



See Also:

- *Oracle Database Backup and Recovery User's Guide*
- "[Configuring Recovery Settings for Protected Databases Using Cloud Control \(page 3-21\)](#)"
- "[Configuring Recovery Settings for Protected Databases Using the Command Line \(page 3-28\)](#)"

3.2 Enrolling the Protected Database with Recovery Appliance (Cloud Control)

Enrolling protected databases with a Recovery Appliance using Cloud Control includes the following high-level steps:

1. Create the Enterprise Manager administrator user who has the privileges required to back up and recover the protected database.

See "Creating the Enterprise Manager Administrator to Manage Protected Database Operations (page 3-9)".

2. Enroll the protected database with a Recovery Appliance.

See "Enrolling a Protected Database with Recovery Appliance Using Cloud Control (page 3-10)".

3.2.1 Creating the Enterprise Manager Administrator to Manage Protected Database Operations

The Enterprise Manager administrator is an Enterprise Manager user that has the roles and privileges required to manage the data protection of one or more protected databases.

To create an Enterprise Manager administrator named `protodb_admin`:

1. Log in to Cloud Control as an Enterprise Manager administrator who has the privileges to create other Enterprise Manager administrator accounts.

2. From the **Setup** menu, select **Security**, and then select **Administrators**.

The Administrators page is displayed.

3. Click **Create** to display the Create Administrator: Properties page.

4. Enter the credentials of the new Enterprise Manager administrator in the Name and Password fields. In this example, the name of the Enterprise Manager administrator is `protodb_admin`.

In the Password Profile field, **DEFAULT** is selected. This value need not be modified. Providing information in the other fields on this page is optional.

5. Click **Next** to display the Create Administrator `protodb_admin`: Roles page.

6. Move the **EM_USER** role from the Available Roles list to the Selected Roles list and click **Next**.

The Create Administrator `protodb_admin`: Target Privileges page is displayed.

7. In the Target Privileges section, add privileges for all the targets that the new Enterprise Manager administrator will require access to. The required target privileges for an administrator that will manage protected database operations are as follows:

- Targets corresponding to the protected databases that will be managed by this Enterprise Manager administrator user: Full privilege.
- Targets corresponding to the hosts of each protected database that will be managed by this Enterprise Manager administrator: Full privilege.
- Target corresponding to the Recovery Appliance to which the protected databases will be sending backups: View privilege.

To add privileges for these targets:

- a. Click **Add** to display the Search and Add: Targets dialog.
- b. Search for the target(s) using the Target Name, Target Type, and On Host filters. Choose the target(s) and click **Select**.

The selected protected database is added to the list of targets in the Target Privileges section.

- c. Privileges can be specified for all the targets in the list via the **Grant to All** button or by selecting individual targets and clicking the **Grant to Selected** button. Either way, in the subsequent **Assign Privileges** screen, select the appropriate privilege for the targets as specified above; then click **Continue** to return to the **Target Privileges** page.

Repeat these steps as needed for each target that will be managed by the new Enterprise Manager user.

8. Click **Next** to display the Create Administrator protdb_admin: EM Resource Privileges page.
9. Perform the following steps:
 - For the Job System privilege, click the Edit icon in the Manage Privilege Grants column. In the Resource Type Privileges section, select **Create** and then click **Continue**.
 - To provide the EM administrator user access to existing credentials, click the Edit icon in the Named Credential column. In the Resource Privileges section, click **Add** and select the named credentials that must be associated with this Enterprise Manager administrator.
10. Click **Review** to display the Create Administrator protdb_admin: Review page.

The properties, roles, and privileges for this new user are displayed. Review the settings and click **Back** to modify settings.
11. Click **Finish** to create the Enterprise Manager administrator.

3.2.2 Enrolling a Protected Database with Recovery Appliance Using Cloud Control

Cloud Control simplifies the process of enrolling protected databases by performing certain tasks automatically.



See Also:

["Overview of Enrolling Protected Databases \(page 3-5\)"](#)



Note:

The Recovery Appliance Settings section that is used to register the protected databases is displayed only for protected databases using Oracle Database 11g Release 2 (11.2) or later. If the protected database release is lower than 11.2, then use the command line to register the protected database and configure virtual private catalog user credentials.

To enroll a protected database with a Recovery Appliance:

1. Add the protected database to the Recovery Appliance.

This step must be performed by the Recovery Appliance administrator and is described in *Zero Data Loss Recovery Appliance Administrator's Guide*.

When adding a protected database, the Recovery Appliance administrator defines the following: protection policy associated with the protected database, minimum amount of disk space reserved for the protected database on the Recovery Appliance, and the Recovery Appliance user who has the privileges required to back up the protected database.

2. Access the home page of the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
3. From the Availability menu, select **Backup & Recovery**, and then **Backup Settings**.

The Backup Settings page is displayed.

4. In the Recovery Appliance Settings section, specify the following settings:
 - **Recovery Appliance:** Select the name of the Recovery Appliance with which the protected database is being enrolled. Protected database backups will be stored on this Recovery Appliance.
 - **Virtual Private Catalog User:** Select the virtual private catalog user (Recovery Appliance user) on the Recovery Appliance that has the privileges required to send backups for this protected database. This user must have already been created by the Recovery Appliance administrator as described in *Zero Data Loss Recovery Appliance Administrator's Guide*.

 **Note:**

You can asynchronously transport the protected database redo data directly to the Recovery Appliance by selecting **Enable Real-Time Redo Transport**. However, you can also enable real-time redo transport while configuring recovery settings for protected databases as described in "[Configuring Recovery Settings for Protected Databases Using Cloud Control](#) (page 3-21)".

5. Click **Apply** to save the settings.

After the protected database is enrolled with a Recovery Appliance, you can use the home page for the protected database (shown in [Figure 3-1](#) (page 3-12)) to perform configuration, backup, and recovery operations for the protected database.

3.2.3 Accessing the Protected Database Home Page Using Cloud Control

The home page of a protected database in Cloud Control provides a centralized interface to manage configuration, backup, and recovery tasks for the protected database.

To access the protected database home page:

1. Open the Cloud Control interface for Recovery Appliance and log in as the Enterprise Manager administrator of your protected database.

See "Creating the Enterprise Manager Administrator to Manage Protected Database Operations (page 3-9)".

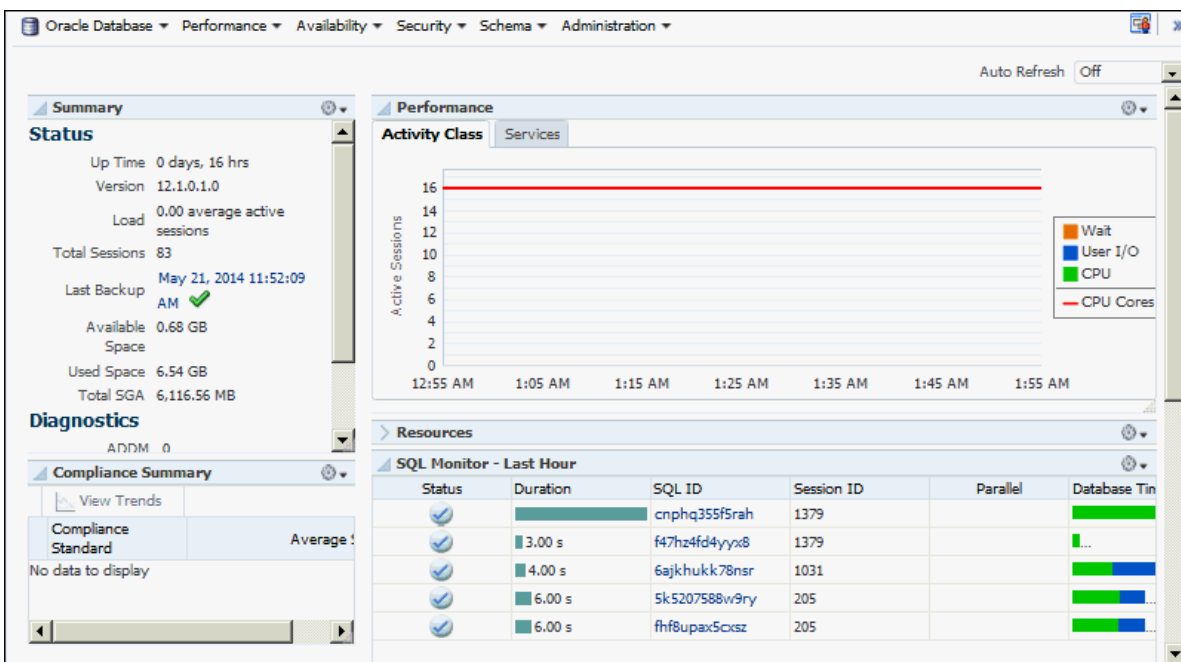
- From the Targets menu, select **Databases**.

The Databases page is displayed. All the protected databases for which you have privileges are listed.

- In the Name column, click the name of the protected database for which you want to perform backup and recovery operations.

The home page for the selected protected database is displayed as shown in [Figure 3-1](#) (page 3-12). Use the menu options on this page to perform configuration, backup, and recovery tasks for the protected database.

Figure 3-1 Protected Database Home Page



3.3 Enrolling the Protected Database with Recovery Appliance (Command Line)

The enrollment steps on the Recovery Appliance are performed using procedures in the `DBMS_RA` package. The steps performed on the protected databases use RMAN or operating system commands.

To enroll a protected database with a Recovery Appliance using RMAN:

- Install the Recovery Appliance backup module.

This creates the Oracle wallet that stores the credentials required to access the Recovery Appliance and installs the shared library that transfers backup data to the Recovery Appliance.

 **Note:**

Oracle 10g protected databases require alternate manual steps for installing the library and creating the wallet. See "[Enrolling Oracle 10g Protected Databases](#) (page 3-16)" for instructions on how to complete these tasks.

 **See Also:**

"[Installing the Recovery Appliance Backup Module](#) (page 3-14)"

2. Add the protected database to the Recovery Appliance.

The Recovery Appliance administrator, who has `sys` privileges on the Recovery Appliance metadata database, is responsible for adding protected databases. You must provide the following information to enable the Recovery Appliance administrator to decide which protection policy must be assigned to the protected database:

- recovery window goal for the protected database
- estimated space required to store backups for this protected database

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide

3. Grant the privileges required for performing backup and recovery operations to the Recovery Appliance user that the protected database will use for authentication. This Recovery Appliance user owns the virtual private catalog that stores metadata for the protected database.

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide

4. Register the protected database with the Recovery Appliance catalog.
"[Registering a Protected Database with the Recovery Appliance Catalog](#) (page 3-17)" describes this task.
5. After the registration process is complete, execute a test backup to ensure that the configuration is correct.
"[Running a Test Backup Using the Command Line](#) (page 3-30)" describes this task.

3.3.1 Installing the Recovery Appliance Backup Module

Protected databases communicate with the Recovery Appliance through the Recovery Appliance backup module. You must install the backup module on the protected database host before you enroll the protected database with Recovery Appliance.

During the Recovery Appliance backup module installation, an Oracle wallet that contains credentials required to authenticate the protected database with Recovery Appliance is created. Additional Oracle wallets can be created.

Note:

Oracle 10g protected databases require alternate manual steps for installing the library and creating the wallet. See "[Enrolling Oracle 10g Protected Databases](#) (page 3-16)" for instructions on how to complete these tasks.

To install the Recovery Appliance backup module:

1. Complete the preparation tasks described in "[Preparing to Install the Recovery Appliance Backup Module](#) (page 3-14)".
2. Download the Recovery Appliance backup module installer as described in "[Obtaining the Installer for the Recovery Appliance Backup Module](#) (page 3-15)".
3. In each Oracle home that contains one or more protected databases, install the Recovery Appliance backup module as described in "[Running the Recovery Appliance Backup Module Installer](#) (page 3-15)".

See Also:

- "[Overview of Recovery Appliance Backup Module](#) (page 3-3)" for the location where the Recovery Appliance backup module must be installed
- "[Creating an Oracle Wallet on the Protected Database](#) (page 3-27)"

3.3.1.1 Preparing to Install the Recovery Appliance Backup Module

Complete the following steps before you install the Recovery Appliance backup module:

- Verify that you have Java version 1.5 or higher
- Contact the Recovery Appliance administrator and obtain the following information:
 - Recovery Appliance host name and port number
 - Credentials of the Recovery Appliance user that will be used to authenticate the protected database with the Recovery Appliance

The permissions required to perform protected database backup and recovery operations need to be assigned to this Recovery Appliance user.

- Ensure that the release of the protected database is Oracle Database 10g Release 2 or later.

3.3.1.2 Obtaining the Installer for the Recovery Appliance Backup Module

You can either download the Recovery Appliance backup module installer from the Oracle Technology Network (OTN) or obtain it from the Recovery Appliance.

On the Recovery Appliance, the installer is called `ra_installer.zip` and is available in the `ORACLE_HOME/lib` directory. During the installation, the Recovery Appliance backup module first attempts to download the modules required for your platform from OTN. If OTN access is unavailable, then the installer obtains the required libraries from the Recovery Appliance.

To download the Recovery Appliance backup module installer from OTN:

1. Access the following URL on OTN:
<http://www.oracle.com/technetwork/database/availability/oracle-zdlra-backup-module-2279224.html>
2. Sign in using your OTN account credentials.
3. Select **Accept License Agreement** to accept the OTN license agreement.
4. Click **All Supported Platforms** to download the Recovery Appliance backup module for your platform.

The Recovery Appliance installer is named `ra_installer.zip`.

3.3.1.3 Running the Recovery Appliance Backup Module Installer

Install the Recovery Appliance backup module in the host file system of the protected database. Since the Recovery Appliance backup module is a shared library, it must be installed into a location within the shared library search path that is visible to every protected database instance. For example, `$ORACLE_HOME/lib` is the default location for shared libraries for the Oracle database.

The Recovery Appliance backup module location is used with the `SBT_LIBRARY` parameter in the `ALLOCATE CHANNEL` or `CONFIGURE CHANNEL` commands.

To run the Recovery Appliance backup module installer:

1. Unzip the installer downloaded in "Obtaining the Installer for the Recovery Appliance Backup Module (page 3-15)" into a local directory.
The installer contains the following files: `ra_install.jar` and `ra_readme.txt`.
2. Ensure that the `ORACLE_HOME` environment variable is set to the Oracle home of the protected database.
3. Run the installer `ra_install.jar` by providing the mandatory parameters. [Table 3-1](#) (page 3-4) describes the parameters required to install the Recovery Appliance backup module.

For example, the following command runs the Recovery Appliance installer with the VPC user name `rauser11` and password `raulpswd`. The Oracle wallet containing the Recovery Appliance credentials is stored in `$ORACLE_HOME/dbs/ra_wallet` and the SBT library for the Recovery Appliance backup module is stored in `$ORACLE_HOME/lib`. The Single Client Access Name (SCAN) of the Recovery

Appliance is `ra-scan`, the listener port number of the Recovery Appliance metadata database is `1521`, and the service name of the Recovery Appliance metadata database is `myzdlra`.

```
% java -jar ra_install.jar -dbUser rauser11 -dbPass raullpswd -host ra-scan -
port 1521
-serviceName myzdlra -walletDir $ORACLE_HOME/dba/ra_wallet -libDir $ORACLE_HOME/
lib
-proxyHost www-proxy.mycompany.com
```

See Also:

- ["Creating an Oracle Wallet on the Protected Database \(page 3-27\)"](#) for steps to manually create an Oracle wallet
- ["Using RMAN Channels for Recovery Appliance Backup and Recovery Operations \(page 3-29\)"](#)

3.3.2 Enrolling Oracle 10g Protected Databases

Oracle 10g protected database enrollment requires alternate manual configuration steps for the first part of the enrollment process.

Perform the following tasks on the protected database server:

1. Add a connect descriptor for the Recovery Appliance to the `tnsnames.ora` file.

This descriptor is required because Oracle 10g does not support the Easy Connect naming method.

The following example shows how an entry for Recovery Appliance should appear in the file:

```
ZDLRA9=
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = scaz15ingest-scan1)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = zdlra9)
    )
  )
```

2. Create a directory for an Oracle wallet in the `$ORACLE_HOME/dbs` directory.
3. Create a wallet in the subdirectory you created in the previous step.

The following example creates a wallet in a subdirectory named `ra_wallet`:

```
$ /u01/app/oracle/product/10.2.0/db_1/bin/mkstore -wrl
/u01/app/oracle/product/10.2.0/db_1/dbs/ra_wallet/ -create
```

4. Add the credentials for the Recovery Appliance user (virtual private catalog user) to the wallet.

The following example creates a credential with the user name `rauser10` and the password `welcome1` for the `zdlra9` Recovery Appliance:

```
$ /u01/app/oracle/product/10.2.0/db_1/bin/mkstore -wrl
/u01/app/oracle/product/10.2.0/db_1/dbs/ra_wallet/ -createCredential "zdlra9"
"rauser10" "welcome1"
```

5. Ensure that the `sqlnet.ora` file contains the location of the Oracle wallet.

The following example shows how the entry should appear:

```
$ cat /u01/app/oracle/product/10.2.0/db_1/network/admin/sqlnet.ora
# sqlnet.ora Network Configuration File:
/u01/app/oracle/product/10.2.0/db_1/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
SQLNET.WALLET_OVERRIDE = true
WALLET_LOCATION =
(SOURCE =
  (METHOD = FILE)
  (METHOD_DATA =
    (DIRECTORY = /u01/app/oracle/product/10.2.0/db_1/dbs/ra_wallet)
  )
)
```

6. Copy the `libra.so` file from the `ORACLE_HOME/lib` directory of the Recovery Appliance to the `ORACLE_HOME/lib` directory of the protected database.

3.3.3 Registering a Protected Database with the Recovery Appliance Catalog

All protected databases must use the Recovery Appliance catalog on the target Recovery Appliance to store protected database backup metadata. Registering the protected database with the Recovery Appliance catalog ensures that metadata for the protected database and its backups is stored in the Recovery Appliance catalog. However, any existing backup metadata stored in an RMAN recovery catalog is not available in the Recovery Appliance catalog unless you import the RMAN recovery catalog into the Recovery Appliance catalog.

Use the `REGISTER DATABASE` command to register protected databases with the Recovery Appliance.

To register a protected database with the Recovery Appliance:

1. Obtain the name and password of the Recovery Appliance catalog owner that will store backup metadata for this protected database. Contact the Recovery Appliance administrator for these credentials.
2. Connect to the protected database as `TARGET` and to the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Register the protected database using the `REGISTER DATABASE` command.

The following command registers the protected database with the Recovery Appliance:

```
REGISTER DATABASE;

database registered in recovery catalog
starting full resync of recover catalog
full resync complete
```

 **See Also:**

- ["Importing Protected Database Metadata into the Recovery Appliance Catalog \(page 2-6\)"](#)
- *Oracle Database Backup and Recovery Reference* for more information about the `REGISTER DATABASE` command
- *Oracle Database Backup and Recovery User's Guide* for information about the RMAN recovery catalog
- *Oracle Database Net Services Administrator's Guide* for more information about net service names

3.4 Configuring Backup and Recovery Settings for Protected Databases (Cloud Control)

Before you back up a protected database to the Recovery Appliance, you must configure backup and recovery settings for the protected database. These configured settings are used in subsequent backup and recovery operations.

 **Note:**

You can use Cloud Control to enroll protected databases with Oracle Database 11g Release 2 (11.2) or later. For Oracle Database releases earlier than 11.2, use the command line to configure backup and recovery settings.

3.4.1 Configuring Backup Settings for Protected Databases Using Cloud Control

Backup settings define the default backup environment for the protected database. The settings that configure real-time redo transport and polling locations define how backups are created to the Recovery Appliance. Other settings, such as control file autobackups or backup optimization, define best practices and performance improvements for protected database backups. These settings may be configured based on your requirements.

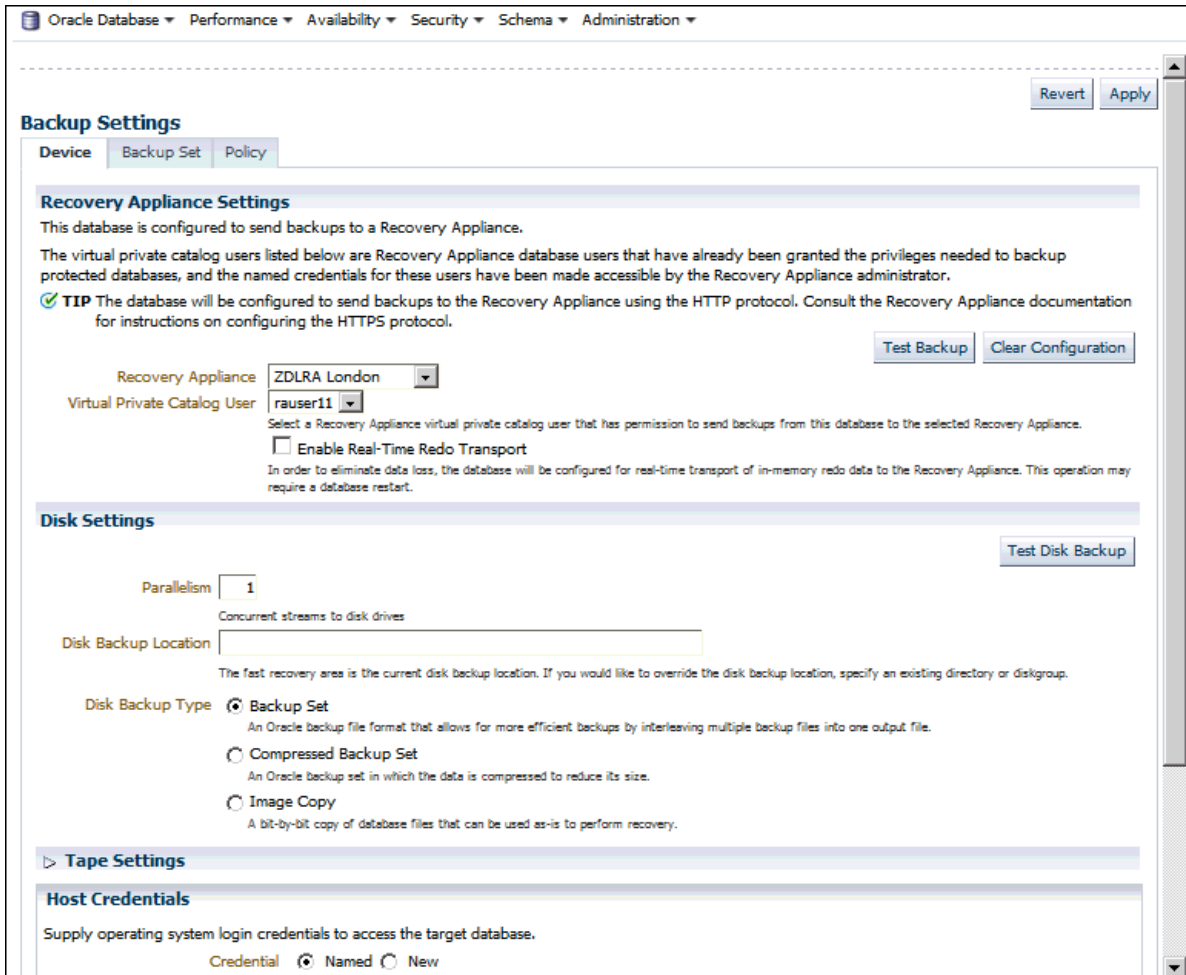
To configure backup settings for a protected database using Cloud Control:

1. Access the home page for the protected database as described in ["Accessing the Protected Database Home Page Using Cloud Control \(page 3-11\)"](#).
2. From the **Availability** menu, select **Backup & Recovery**, and then select **Backup Settings**.

The Backup Settings page for the protected database is displayed. [Figure 3-2 \(page 3-19\)](#) displays the Device tab of the Backup Settings page. The Recovery Appliance Settings section displays the Recovery Appliance and the Recovery

Appliance user that you configured in "Enrolling a Protected Database with Recovery Appliance Using Cloud Control (page 3-10)".

Figure 3-2 Backup Settings Page for Protected Databases



3. In the Device tab, configure the following optional settings:
 - To write redo data asynchronously from the protected database to the Recovery Appliance, in the Recovery Appliance Settings section, select **Enable Real-Time Redo Transport**.

 **See Also:**

["About Real-Time Redo Transport \(page 1-12\)"](#)

- If you want to configure backup polling for the protected database, then specify the polling location in the Disk Backup Location setting of the Disk Settings section.

Disk backups created to this location will then be automatically picked up by the Recovery Appliance if the protected database is assigned to a protection policy that specifies this location as a polling location. Polling policies are created by the Recovery Appliance administrator.

 **See Also:**

- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about backup polling policies
- "[Mounting the NFS Storage for Backup Polling](#) (page 2-12)"

4. In the Policy tab, configure settings that define the objects that must be backed up.

Although it is not mandatory to configure the settings in this section, it is strongly recommended that you configure automatic backups for the control file and server parameter file. [Table 3-2](#) (page 3-6) describes these configuration settings.

- To configure control file and server parameter file autobackups:
 - Select **Automatically backup the control file and server parameter file (SPFILE) with every backup and database structural change**.
 - In the Autobackup Disk Location field, specify an existing directory or Automatic Storage Management (ASM) disk group name to which the control file and server parameter file autobackups must be stored. If no location is specified, then the autobackups are stored in the local fast recovery area.
- To enable backup optimization, select **Optimize the whole database backup by skipping unchanged files such as read-only and offline datafiles that have been backed up**.
- To enable block change tracking, select **Enable block change tracking for faster incremental backups** and specify the name of the block change tracking file in the Block Change Tracking File field.
- In the Tablespaces Excluded from Whole Database Backup section, ensure that you do not add any tablespaces.

 **Note:**

When backing up to Recovery Appliance, the initial full backup of the protected database must contain all the tablespaces.

- In the Archived Redo Log Deletion Policy section, select one of the following options to specify how RMAN must handle redo log file deletion for the local backups stored on the protected database host:
 - None

Archived redo logs in the fast recovery area are eligible for deletion if they have been backed up at least once or if they are obsolete according to the backup retention policy.
 - Delete archived redo log files after they have been backed up the specified number of times

Deletes archived redo log files that have been backed up the number of times specified in the **Backups** field.

 **Note:**

In the Retention Policy section, you need not specify any values. The settings in the Retention Policy section are not used for backups to Recovery Appliance, as the retention policy is inherited from the protection policy that is associated with the protected database when it is enrolled with the Recovery Appliance.

5. Click **Apply** to save the backup settings.

 **See Also:**

["Overview of Protected Database Backup Settings \(page 3-6\)"](#)

3.4.2 Configuring Recovery Settings for Protected Databases Using Cloud Control

Recovery settings define the default recovery environment for the protected database. The only mandatory setting for Recovery Appliance is the Log Archive Filename Format. Configuring the remaining recovery settings is optional.

To configure recovery settings for a protected database using Cloud Control:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control \(page 3-11\)](#)".
2. From the Availability menu, select **Backup & Recovery**, then select **Recovery Settings**.

The Recovery Settings page for the protected database is displayed as shown in [Figure 3-3 \(page 3-22\)](#).

Figure 3-3 Protected Database Recovery Settings

Oracle Database ▾ Performance ▾ Availability ▾ Security ▾ Schema ▾ Administration ▾

Recovery Settings

Show SQL Revert Apply

Instance Recovery

The fast-start checkpointing feature is enabled by specifying a non-zero desired mean-time to recover (MTTR) value, which will be used to set the FAST_START_MTTR_TARGET initialization parameter. This parameter controls the amount of time the database takes to perform crash recovery for a single instance. When fast-start checkpointing is enabled, Oracle automatically maintains the speed of checkpointing so that the requested MTTR is achieved. Setting the value to 0 will disable this functionality.

Current Estimated Mean Time To Recover (seconds) 13

Desired Mean Time To Recover 0 Minutes

Media Recovery

The database is currently in ARCHIVELOG mode. In ARCHIVELOG mode, hot backups and recovery to the latest time are possible, but you must provide space for archived redo log files. If you change the database to ARCHIVELOG mode, you should perform a backup immediately. In NOARCHIVELOG mode, only cold backups are possible and data may be lost in the event of database corruption.

ARCHIVELOG Mode*

Log Archive Filename Format* %t_%s_%r.dbf

Number	Archived Redo Log Destination	Status	Type
1	USE_DB_RECOVERY_FILE_DEST	VALID	Local

Add Another Row

TIP It is recommended that archived redo log files be written to multiple locations spread across the different disks.
 TIP You can specify up to 10 archived redo log destinations.

Enable Minimal Supplemental Logging

Minimal supplemental logging logs the minimal amount of information needed for LogMiner (and any product building on LogMiner technology) to identify, group, and merge the redo operations associated with DML changes.

Fast Recovery

This database is using a fast recovery area. The chart shows space used by each file type that is not reclaimable by Oracle. Performing backups to tertiary storage is one way to make space reclaimable. Usable Fast Recovery Area includes free and reclaimable space.

Fast Recovery Area Location +RECO

Fast Recovery Area Size 4800 MB

Fast Recovery Area Size must be set when the location is set.

Fast Recovery Area Usage

3. In the Instance Recovery section, specify the Desired Mean Time To Recover.
4. In the Media Recovery section, perform the following steps:
 - (Optional) Select **ARCHIVELOG Mode**.
 - (Optional) In the Log Archive Filename Format field, specify the format used for archived redo log file names.
 - In the Archived Redo Log Destination field, provide a destination to store archived redo log files or specify `USE_DB_RECOVERY_FILE_DEST` to indicate that the redo log files must be stored in the local fast recovery area.

If you selected **Enable Real-Time Redo Transport** in the Backup settings for this protected database, then the archived redo log destination is automatically set.
5. Configure a local fast recovery area for the protected database by specifying the following in the Fast Recovery section:
 - In the Fast Recovery Area Location field, specify the file-system or ASM location where backup-related files are stored. Oracle recommends that you configure a fast recovery area for the protected database. Local backups of the protected database are stored in the fast recovery area.
 - In the Fast Recovery Area Size field, specify the disk space quota allocated to the fast recovery area. This is the maximum storage that can be used by the

recovery area for this protected database. Specifying a size is mandatory when you configure a fast recovery area.

6. Click **Apply** to save the recovery settings.

 **See Also:**

- [Table 3-3](#) (page 3-7) for a brief description of the recovery settings
- ["Overview of Protected Database Recovery Settings](#) (page 3-7)"

3.4.3 Clearing the Backup Configuration of Protected Databases Using Cloud Control

You can clear the backup configuration of a protected database and remove its existing Recovery Appliance settings. Clearing the backup configuration removes the currently-configured Recovery Appliance and virtual private catalog user, any configured RMAN channels, and the real-time redo transport configuration.

To clear the backup configuration for a protected database using Cloud Control:

1. Access the home page for the protected database as described in ["Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. From the **Availability** menu, select **Backup & Recovery**, and then select **Backup Settings**.

The Backup Settings page for the protected database is displayed as shown in [Figure 3-2](#) (page 3-19).

3. In the Recovery Appliance Settings section, click **Clear Configuration**.

 **Note:**

If real-time redo transport was configured for the protected database, then you must manually force a redo log switch to maintain an accurate state for the Redo Shipping column of this protected database in Cloud Control.

3.5 Configuring Backup and Recovery Settings for Protected Databases (Command Line)

You can use the regular RMAN commands to configure backup and recovery settings for protected databases. These configured settings are used in subsequent backup and recovery operations.

This section contains the following topics:

- [Configuring Backup Settings for Protected Databases Using the Command Line](#) (page 3-24)

- [Configuring Recovery Settings for Protected Databases Using the Command Line \(page 3-28\)](#)
- [Using RMAN Channels for Recovery Appliance Backup and Recovery Operations \(page 3-29\)](#)

3.5.1 Configuring Backup Settings for Protected Databases Using the Command Line

RMAN assigns default values for protected database backup settings. You can use the `CONFIGURE` command to modify these settings according to the backup requirements of your protected database.

To configure backup settings for a protected database using the command line:

1. Use RMAN to connect to the protected database as `TARGET` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)](#)".

The following command starts RMAN and connects to the protected database as target using operating system authentication:

```
% rman target /
```

2. Use the `CONFIGURE` command to configure the required backup settings.

The backup settings that you can configure are:

- Fast recovery area
- Media manager for the Recovery Appliance
Configure an RMAN SBT channel that points to the Recovery Appliance backup module.
- Backup optimization

3. (Optional) To set up redo transport services for the protected database, configure real-time redo transport as described in "[Configuring Real-Time Redo Transport \(page 3-24\)](#)".

See Also:

- "[Overview of Protected Database Backup Settings \(page 3-6\)](#)"
- "[Configuring RMAN SBT Channels for Recovery Appliance \(page 3-29\)](#)"
- *Oracle Database Backup and Recovery User's Guide* for information about configuring backup optimization

3.5.1.1 Configuring Real-Time Redo Transport

When you configure real-time redo transport, redo data from the protected database is directly transported and stored on the Recovery Appliance. This reduces the window of potential data loss that exists between successive archived log backups.

Configuring real-time redo transport for a protected database is a one-time step. After you set it up, the protected database asynchronously transports redo data to the Recovery Appliance.

 **Note:**

- The user you use for redo transport must be the same user you configured to send backups to the Recovery Appliance.
- When you clear the real-time redo transport configuration for a protected database, you must manually force a redo log switch to maintain an accurate state for the protected database. The log switch forces the remote file server process (RFS) to stop sending redo data to Recovery Appliance.

To enable real-time redo transport for a protected database:

1. Ensure that the Recovery Appliance user that the protected database uses to send backups to the Recovery Appliance is configured. This same user will be used for redo transport.

Also ensure that an Oracle wallet is created on the protected database that contains credentials for the Recovery Appliance (and redo transport) user. This process is described in "[Creating an Oracle Wallet on the Protected Database](#) (page 3-27)".

 **See Also:**

Zero Data Loss Recovery Appliance Administrator's Guide for information about creating the virtual private catalog account that is used by the Recovery Appliance user

2. Ensure that the following conditions are met for the protected database:

- ARCHIVELOG mode is enabled
- DB_UNIQUE_NAME parameter is set

3. Ensure that the REMOTE_LOGIN_PASSWORDFILE and LOG_ARCHIVE_FORMAT initialization parameters are set for the protected database:

```
REMOTE_LOGIN_PASSWORDFILE=exclusive
LOG_ARCHIVE_FORMAT='log_%d_%t_%s_%r.arc'
```

REMOTE_LOGIN_PASSWORDFILE can be set to `exclusive` or `shared`.

4. Start SQL*Plus and connect to the protected database as a user with the SYSDBA or SYSBACKUP privilege.

The following command uses operating system authentication to connect to the protected database using SYSDBA privileges:

```
% sqlplus / as sysdba
```

5. Set the LOG_ARCHIVE_CONFIG initialization parameter to include a DG_CONFIG list. Also set the DB_UNIQUE_NAME for the protected database.

The following SQL commands, when connected to the protected database as a user with SYSDBA privilege, set the `DB_UNIQUE_NAME` and `LOG_ARCHIVE_CONFIG` parameters for a protected database whose `db_unique_name` is `hr_ptdb` and `db_name` is `hr_ptdb`:

```
ALTER SYSTEM SET DB_UNIQUE_NAME=hr_ptdb SCOPE=BOTH;
ALTER SYSTEM SET LOG_ARCHIVE_CONFIG='DG_CONFIG=(zdlra2,hr_ptdb)' SCOPE=BOTH;
```

The `DB_NAME` and the `DB_UNIQUE_NAME` of the Recovery Appliance database is `zdlra2`.

See Also:

Oracle Data Guard Concepts and Administration for information about setting a `DG_CONFIG` list

6. Configure an archived log destination that points to the redo staging area on the Recovery Appliance.

You configure an archived log destination by setting one of the `LOG_ARCHIVE_DEST_n` parameters, where `n` is any number between 1 and 31. You must include the `SERVICE` attribute to specify where to store the redo data. Set this attribute to the net service name of the Recovery Appliance database that stores the redo stream from the protected database.

The following example configures the protected database to transport redo data asynchronously to a Recovery Appliance whose net service name is `boston`.

```
ALTER SYSTEM SET LOG_ARCHIVE_DEST_3='SERVICE=boston
VALID_FOR=(ALL_LOGFILES, ALL_ROLES) ASYNC DB_UNIQUE_NAME=zdlra2' SCOPE=BOTH;
```

See Also:

Oracle Database Reference for information about setting the `LOG_ARCHIVE_DEST_n` parameter

7. Enable logging for the archived redo log destination configured in Step 6 (page 3-26) by setting the `LOG_ARCHIVE_DEST_STATE_n` parameter, where `n` matches the value used for the `LOG_ARCHIVE_DEST_n` parameter specified in Step 6 (page 3-26).

The following command enables archived redo logging for the destination set using the `LOG_ARCHIVE_DEST_3` parameter:

```
ALTER SYSTEM SET LOG_ARCHIVE_DEST_STATE_3='ENABLE' SCOPE=BOTH;
```

See Also:

Oracle Database Reference for information about setting the `LOG_ARCHIVE_DEST_STATE_n` parameter

8. Set the redo transport user to the Recovery Appliance user that was created for this protected database (see Step 1 (page 3-25)).

The following example sets the redo transport user to `ravpcl`:

```
ALTER SYSTEM SET REDO_TRANSPORT_USER=ravpcl SCOPE=BOTH;
```

9. Shut down the protected database and restart it.

```
SHUTDOWN IMMEDIATE;
STARTUP;
```

If the protected database uses a parameter file instead of a server parameter file, then add the parameters that were set in Steps 5 (page 3-25) to 8 (page 3-26) to the parameter file before you start up the protected database.

See Also:

- ["About Configuring Real-Time Redo Transport for Protected Databases \(page 1-13\)"](#)
- *Zero Data Loss Recovery Appliance Administrator's Guide* for information about Oracle Database releases for which redo transport is supported
- [Deploying Zero Data Loss Recovery Appliance in a Data Guard Configuration](#) for instructions on how to configure redo transport for Recovery Appliance with Oracle Data Guard

3.5.1.2 Creating an Oracle Wallet on the Protected Database

An Oracle wallet stores the credentials of the Recovery Appliance user that will be used by the protected database to authenticate with the Recovery Appliance. These same credentials are used for sending backups and redo, if configured. When you install the Recovery Appliance backup module, an Oracle wallet is automatically created. You can also create the wallet and add required entries manually.

Note:

The `sqlnet.ora` file in the protected database must contain the location of the Oracle wallet. Typically, the wallet location is automatically added to this file when you install the Recovery Appliance backup module.

In the case of multiple ZDLRAs, store a single wallet in a centralized location and have the `sqlnet.ora` file on each ZDLRA reference that centralized wallet location.

If the wallet cannot be stored in a centralized location for multiple ZDLRAs, then it needs to be copied to all instances. Create the wallet and master key on the first instance, and then copy the wallet to the other instances. Further, set up the environment variable `ORACLE_UNQNAME` to separate your database wallets. Then you can refer to them dynamically from the `sqlnet.ora` as follows for Unix / Linux:

```
WALLET_LOCATION =
(SOURCE=(METHOD=FILE)
(METHOD_DATA =
(DIRECTORY=/etc/oracle/wallets/${ORACLE_UNQNAME/})))
```

On Windows-based systems, you can refer to a database dynamically with:

```
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = E:\oracle\%ORACLE_UNQNAME%)))
```

In addition on Windows, establish a Windows registry key for the database `ORACLE_UNQNAME=<dbname>`. However, this registry key can only be set for one database on Windows, so this approach is currently restricted to environments where there is only one database running on the Windows server.

Example 3-1 Creating an Oracle Wallet on the Protected Database

The following command creates an Oracle wallet that stores the credentials of the Recovery Appliance user named `ravpc1`:

```
$ mkstore                               \
-wrl $ORACLE_HOME/oracle/wallet \
-createALO                               \
-createCredential zdlra01ingest-scan.acme.com:1521/zdlra01:dedicated ravpc1
```

Enter the password for the `ravpc1` user when prompted. Here, `zdlra01` is the net service name of the Recovery Appliance database. The directory `$ORACLE_HOME/oracle/wallet` must be created before the `mkstore` command is run.

Example 3-2 Creating an Oracle Wallet with Multiple User Credentials

The following command creates two sets of credentials in the Oracle wallet of a protected database. In this scenario, `ra_user` is used both by the Recovery Appliance for normal backup and recovery operations (and real-time redo transport, if enabled) and by the Data Guard standby database for data synchronization. The service name of the Recovery Appliance is `zdlra2` and that of the primary database in the Data Guard set up is `chicago`.

```
$ mkstore                               \
-wrl $ORACLE_HOME/oracle/wallet \
-createALO                               \
-createCredential chicagoingest-scan.acme.com:1521/chicago:dedicated
ra_user \
-createCredential zdlra02ingest-scan.acme.com:1521/zdlra02:dedicated ra_user
```

Enter the password for `ra_user` when prompted. The directory `$ORACLE_HOME/oracle/wallet` must be created before the `mkstore` command is run.

3.5.2 Configuring Recovery Settings for Protected Databases Using the Command Line

Use the `CONFIGURE` command to modify the default values assigned by RMAN for the protected database recovery settings.

To configure recovery settings for a protected database using the command line:

1. Use RMAN to connect to the protected database as `TARGET`.

The following command starts RMAN and connects to the protected database as target using operating system authentication:

```
% rman target /
```

2. Use the `CONFIGURE` command to configure the required recovery settings described in ["Overview of Protected Database Recovery Settings \(page 3-7\)"](#).

 **See Also:**

Oracle Database Backup and Recovery User's Guide

3.5.3 Using RMAN Channels for Recovery Appliance Backup and Recovery Operations

To transfer backups to and from the Recovery Appliance, you must use an RMAN SBT (System Backup to Tape) channel that corresponds to the Recovery Appliance backup module.

The following techniques are available to use RMAN channels for protected database operations:

- [Configuring RMAN SBT Channels for Recovery Appliance \(page 3-29\)](#)
- [Allocating RMAN SBT Channels for Recovery Appliance \(page 3-30\)](#)

 **See Also:**

- ["About RMAN SBT Channels and Protected Databases \(page 1-9\)"](#)
- ["Installing the Recovery Appliance Backup Module \(page 3-14\)"](#)

3.5.3.1 Configuring RMAN SBT Channels for Recovery Appliance

You configure RMAN SBT channels for Recovery Appliance using the RMAN `CONFIGURE` command. Configuring channels for a protected database creates persistent settings that are applicable to all backup, restore, and maintenance operations on that protected database. Configured settings remain in effect until they are explicitly cleared, changed, or overridden in a particular operation using an `ALLOCATE` command.

[Example 3-3 \(page 3-29\)](#) configures an RMAN SBT channel for a Recovery Appliance. After this configuration, you need not explicitly allocate SBT channels that correspond to the Recovery Appliance backup module for each backup or recovery operation.

Example 3-3 Configuring an RMAN Channel for Recovery Appliance

In this example, an RMAN SBT channel is configured with the `SBT_LIBRARY` parameter pointing to the Recovery Appliance backup module. The complete path of the shared library `libra.so` is specified. The `RA_WALLET` parameter represents the location of the Oracle wallet that stores the credentials used to authenticate this protected database with the Recovery Appliance. `ra-scan` is the SCAN of the Recovery Appliance and `zdlra5` is the service name of the Recovery Appliance metadata database.

```
CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE'
PARMS 'SBT_LIBRARY=/u01/app/oracle/product/11.2.0.4.0/dbhome_1/lib/libra.so,
ENV=(RA_WALLET=location=file:/u01/app/oracle/product/11.2.0.4.0/dbhome_1/dbs/zdlra
credential_alias=ra-scan:1521/zdlra5:dedicated)' FORMAT '%U_%d';
```

3.5.3.2 Allocating RMAN SBT Channels for Recovery Appliance

Use the RMAN `ALLOCATE` command to allocate RMAN SBT channels that will be used to back up to or recover from the Recovery Appliance. For a particular operation, you can override the persistent configuration that was set using the `CONFIGURE` command by explicitly allocating an RMAN SBT channel before the operation. Enclose the `ALLOCATE` command and the other commands in a `RUN` block.

Example 3-4 (page 3-30) allocates an RMAN SBT channel for the Recovery Appliance and then creates a full backup of the protected database including archived redo logs.

Example 3-4 Allocating RMAN Channels for Recovery Appliance

This example allocates an RMAN SBT channel with the `SBT_LIBRARY` parameter specifying the complete path of the Recovery Appliance backup module. The `ENV` setting is used to specify the configuration parameters used by the Recovery Appliance backup module. `ra-scan` is the SCAN of the Recovery Appliance and `zdlra5` is the service name of the Recovery Appliance metadata database.

```
RUN
{
ALLOCATE CHANNEL c1 DEVICE TYPE sbt_tape
PARMS='SBT_LIBRARY=/u01/app/oracle/product/12.1.0.2/dbhome_1/lib/libra.so,
ENV=(RA_WALLET=location=file:/u01/app/oracle/product/12.1.0.2/dbhome_1/dbs
credential_alias=ra-scan:1521/zdlra5:dedicated)' FORMAT '%U_%d';
BACKUP INCREMENTAL LEVEL 1 DATABASE PLUS ARCHIVELOG;
}
```

3.6 Performing Test Backup and Recovery Operations

After you enroll the protected database with a Recovery Appliance, it is recommended that you perform a test backup and recovery operation. This testing helps confirm that your configuration settings are accurate and that the backup to and recovery from the Recovery Appliance are performed successfully. If you encounter any problem with the test backup or recovery, you may correct your settings and reconfigure your protected database.

3.6.1 Running a Test Backup Using the Command Line

After configuring a protected database for Recovery Appliance, you can test the connection to the Recovery Appliance by attempting a test backup.

To create a test backup of the protected database:

1. Connect to the protected database as `TARGET` and to the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
2. Configure an RMAN SBT channel for the Recovery Appliance as described in "[Configuring RMAN SBT Channels for Recovery Appliance](#) (page 3-29)".

A good guideline for choosing the number of channels is to start with the number of channels that are currently used for incremental backups or a default of 2 or 4 channels per node depending on the number of cores or CPUs.

3. Use the following RMAN command to perform a full backup:

```
BACKUP DEVICE TYPE SBT CUMULATIVE INCREMENTAL LEVEL 1 DATABASE  
PLUS ARCHIVELOG FORMAT %d_%U;
```

This `BACKUP` command creates a new level 0 backup, if one does not already exist, when it is run for the first time.

 **Note:**

Archive redo logs can be included with regular backups because the Recovery Appliance keeps track of which logs may need to be backed up and avoids backing up the same archived redo logs twice. The benefit of including archived redo logs is in the case where there is a gap. Without archived redo logs, gap detection may be delayed.

3.6.2 Running a Test Recovery Using the Command Line

After creating a test backup of the protected database to Recovery Appliance, you can test this backup by performing a test recovery.

To perform a test recovery of the protected database:

1. Shutdown and restart the protected database in `NOMOUNT` mode.
2. Connect to the protected database as `TARGET` and to the Recovery Appliance catalog as `CATALOG`.

See "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".

3. Configure an RMAN SBT channel for the Recovery Appliance as described in "[Configuring RMAN SBT Channels for Recovery Appliance](#) (page 3-29)".
4. Use the following RMAN command to restore the previously created test backup from the Recovery Appliance. Because the `VALIDATE` option is used, this can be done without interfering with the production database.

```
RESTORE VALIDATE DATABASE;
```

If these backup and recovery procedures succeed, then the client database is ready to perform regular backups to the Recovery Appliance.

3.6.3 Performing a Test Backup Using Cloud Control

After configuring the protected database, verify that the configuration is accurate by performing a test backup.

To perform a test backup using Cloud Control:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".

- From the Availability menu, select **Backup & Recovery**, then **Backup Settings**.
The Device tab of the Backup Settings page is displayed. [Figure 3-4](#) (page 3-32) displays the Recovery Appliance Settings section of this page.

Figure 3-4 Recovery Appliance Settings Section of Backup Settings Page

Recovery Appliance Settings
This database is configured to send backups to a Recovery Appliance.
The virtual private catalog users listed below are Recovery Appliance database users that have already been granted the privileges needed to backup protected databases, and the named credentials for these users have been made accessible by the Recovery Appliance administrator.
TIP The database will be configured to send backups to the Recovery Appliance using the HTTP protocol. Consult the Recovery Appliance documentation for instructions on configuring the HTTPS protocol.

Recovery Appliance: ZDLRA London
Virtual Private Catalog User: rauser11

Enable Real-Time Redo Transport
In order to eliminate data loss, the database will be configured for real-time transport of in-memory redo data to the Recovery Appliance. This operation may require a database restart.

Test Backup Clear Configuration

- In the Recovery Appliance Settings section, click **Test Backup**.
A test backup is initiated by Cloud Control and the Processing: Test Recovery Appliance Backup page is displayed.
If the backup is successful, the following message is displayed: Recovery Appliance backup test successful.
If there is an error when performing the backup, then an error message stating "Recovery Appliance backup test failed" is displayed. Click **View Error Details** to display the View Error Details page containing detailed information about the cause of the error. Rectify the problem and then perform a test backup.

4

Backing Up Protected Databases

This chapter describes how to back up protected databases to Recovery Appliance.

This chapter contains the following topics:

- [Overview of Backing Up Protected Databases](#) (page 4-1)
- [Backing Up the Protected Database Using Cloud Control](#) (page 4-2)
- [Backing Up the Protected Database Using the Command Line](#) (page 4-5)
- [Monitoring Protected Database Backups Using Cloud Control](#) (page 4-8)

4.1 Overview of Backing Up Protected Databases

After you configure the protected database, you can create and schedule protected database backups. Recovery Appliance uses the incremental-forever backup strategy for protected database backups. In this strategy, an initial level 0 incremental backup is followed by successive level 1 incremental backups.

To ensure that you can perform complete recovery for the protected database, include archived redo log files in all backups except when using real-time redo transport. While real-time redo transport sends archive logs to the Recovery Appliance, archive log backup operations of *"not backed up"* files is still recommended.

Enterprise Manager Cloud Control (Cloud Control) provides a GUI for creating and scheduling backup jobs. When using the command line, create a script containing the RMAN backup commands required to implement your backup strategy and then schedule this script using any scheduling utility.

Note:

If the protected database is running in `NOARCHIVELOG` mode, then you must perform consistent backups which requires shutting down the protected database.

See Also:

- ["Configuring Protected Databases](#) (page 3-1)"
- ["About the Recovery Appliance Incremental-Forever Backup Strategy](#) (page 1-11)"

4.2 Backing Up the Protected Database Using Cloud Control

Cloud Control provides a preconfigured Oracle-Suggested Recovery Appliance Backup that implements the incremental-forever backup strategy for your protected database. Alternately, you can create and schedule full backups, incremental backups, backups of selected tablespaces or data files, or backups of archived redo logs files and control files.

This section contains the following tasks:

- [Using the Oracle-Suggested Backup Strategy for Protected Databases](#) (page 4-2)
- [Backing Up the Whole Protected Database Using Cloud Control](#) (page 4-4)

4.2.1 Using the Oracle-Suggested Backup Strategy for Protected Databases

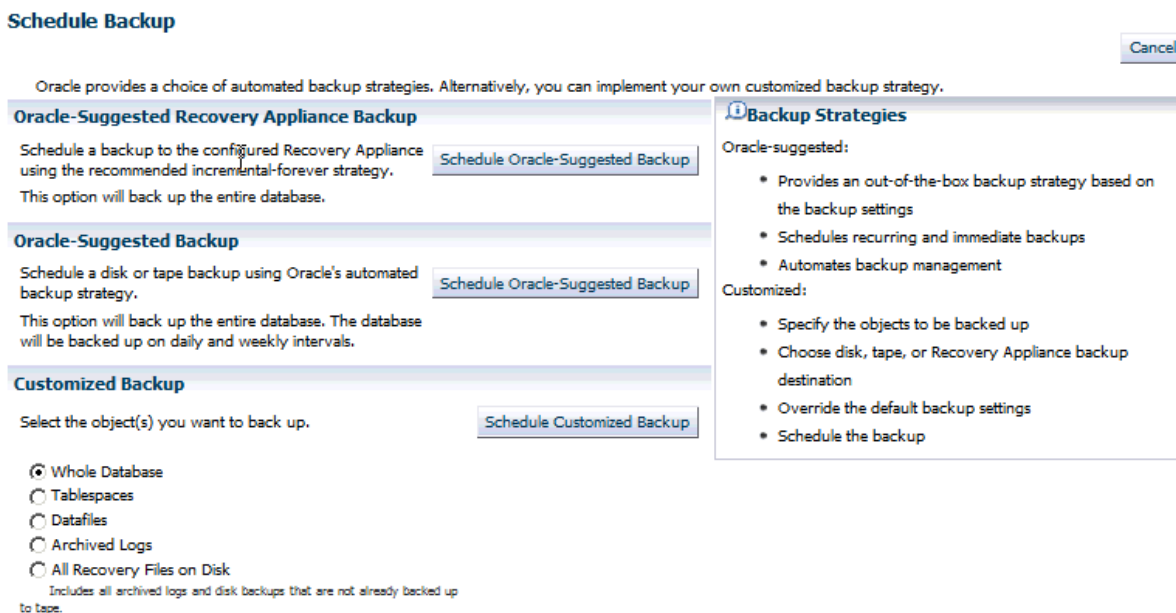
The Oracle-Suggested Recovery Appliance Backup strategy is a regularly scheduled, incremental-forever backup strategy that backs up your protected database.

To implement the Oracle-Suggested Recovery Appliance Backup strategy:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. Ensure that the configuration steps described in "[Enrolling the Protected Database with Recovery Appliance \(Cloud Control\)](#) (page 3-8)" and "[Configuring Backup and Recovery Settings for Protected Databases \(Cloud Control\)](#) (page 3-18)" are completed.
3. From the Availability menu, select **Backup & Recovery**, and then **Schedule Backup**.

The Schedule Backup page is displayed as shown in [Figure 4-1](#) (page 4-3).

Figure 4-1 Schedule Protected Database Backup



4. In the Oracle-Suggested Recovery Appliance Backup section, select **Schedule Oracle-Suggested Backup**.

The Schedule Oracle-Suggested Recovery Appliance Backup: Options page is displayed.

5. Specify the method used to back up redo data.
 - If real-time redo transport is not configured for the protected database, select **Also back up all archived logs on disk**.
 - If required, select **Delete all archive logs from disk after they are successfully backed up**.
6. Click **Next** to display the Schedule Oracle-Suggested Recovery Appliance Backup: Schedule page.
7. (Optional) Modify the default values provided in the Job Name and Job Description fields.
8. Schedule the backup job.

In the Schedule section, select **Repeating**, then set the frequency to repeat daily, and then select **Indefinite**.

9. Click **Next** to display the Schedule Oracle-Suggested Recovery Appliance Backup: Review page.

The Settings section displays the settings that will be used to create this backup. Cloud Control generates the RMAN script required to create and schedule this backup. You can view this script in the RMAN Script section.

10. Click **Submit Job**.

A backup job is created based on the settings in the Schedule section. The following message is displayed: The job has been successfully submitted.

11. Click **View Job** to display the status of the backup job.

The Summary section displays a job summary that includes the status, type of backup, database name, Recovery Appliance catalog user name, and other details.

Click **Job Report** to display a detailed report of the backup steps performed.

4.2.2 Backing Up the Whole Protected Database Using Cloud Control

Cloud Control can be used to create and schedule backup jobs that can be run immediately or at a later time. Oracle recommends that you include archived redo logs in all full and incremental backups. Backing up redo data ensures that the recovery time is reduced.

This section describes how to schedule a backup job that creates a full backup of the protected database with archived redo log files. The backup job repeats every day for an indefinite period of time.

To backup the whole protected database along with archived redo logs:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. Ensure that the configuration steps described in "[Enrolling the Protected Database with Recovery Appliance \(Cloud Control\)](#) (page 3-8)" and "[Configuring Backup and Recovery Settings for Protected Databases \(Cloud Control\)](#) (page 3-18)" are completed.

3. From the Availability menu, select **Backup & Recovery**, and then **Schedule Backup**.

The Schedule Backup page is displayed as shown in [Figure 4-1](#) (page 4-3).

4. In the Customized Backup section, select **Schedule Customized Backup**.

The Schedule Customized Backup: Options page is displayed.

5. In the Backup Type section, select **Full Backup**.

If you want to use this backup as the base of an incremental backup strategy, then select **Use as the base of an incremental backup strategy**.

6. In the Backup Mode section, select **Online Backup**.

7. In the Advanced section, select **Also back up all archived logs on disk** to back up the redo logs along with the protected database.

8. Click **Next** to display the Schedule Customized Backup: Settings page.

9. Select **Recovery Appliance** to store protected database backups on the Recovery Appliance with which the protected database is enrolled.

10. Click **Next** to display the Schedule Customized Backup: Schedule page is displayed.

11. (Optional) Edit the job name and description to provide user-defined names.

12. In the Schedule section, click **Repeating** and enter the following information:

- Frequency Type: By Weeks
- Repeat Every: 1
- Start Time: 1:00 am
- Repeat Until: Indefinite

13. Click **Next** to display the Schedule Customized Backup: Review page.

The Settings section displays the settings that will be used to create this backup. Cloud Control generates the RMAN script required to perform this backup job. The RMAN Script section displays the generated script.

14. Click **Submit Job** to create a backup job based on the settings provided in the Schedule section.

The following message is displayed: The job has been successfully submitted.

15. Click **View Job** to display the status of the backup job.

The Summary section displays a job summary that includes the status, type of backup, protected database name, Recovery Appliance catalog user name, and so on.

Click **Job Report** to display a detailed report of the backup steps performed.

4.3 Backing Up the Protected Database Using the Command Line

Use regular RMAN commands to create backups of your protected database. To schedule protected database backups, create a script that contains the required backup commands and then use any scheduling utility to schedule backups. You can create full backups, incremental backups, archived redo log backups, control file backups, or backups of specific data files and tablespaces. To implement the incremental-forever backup strategy, you need one level 0 incremental database backup and successive periodic level 1 incremental backups.

Because multiple protected databases are backed up to the same Recovery Appliance, backup piece names must be unique across all protected databases. Use the substitution variables `%d_%U` in the `FORMAT` string of `BACKUP` commands to ensure that backup piece names are unique.

See Also:

Oracle Database Backup and Recovery Reference for information about the substitution variables

To implement the incremental-forever backup strategy using the command line:

1. Create a full backup of the protected database that will form the basis of the incremental-forever backup strategy as described in "[Creating the Initial Full Backup of the Protected Database](#) (page 4-5)".
2. Create and schedule regular level 1 incremental backups that include archived redo logs as described in "[Creating Incremental Backups of the Protected Database](#) (page 4-6)".

4.3.1 Creating the Initial Full Backup of the Protected Database

This section describes how to create a one-time full backup of the whole protected database that includes archived redo logs. Assume that the protected database is in

ARCHIVELOG mode and is configured to automatically back up the control file and server parameter file.

To create a full backup of the whole protected database:

1. Connect RMAN to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG`.
See ["Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)"](#).
2. Ensure that the configuration steps described in ["Enrolling the Protected Database with Recovery Appliance \(Command Line\) \(page 3-12\)"](#) and ["Configuring Backup and Recovery Settings for Protected Databases \(Command Line\) \(page 3-23\)"](#) are completed.
3. Run the following command to allocate three SBT channels for the Recovery Appliance and then create a full backup of the protected database including archived redo log files:

```
RUN
{
  ALLOCATE CHANNEL c1 DEVICE TYPE sbt_tape
    PARMS='SBT_LIBRARY=/u01/oracle/product/11.2.0.4/dbhome_1/lib/libra.so,
    ENV=(RA_WALLET=location=file:/u01/oracle/product/11.2.0.4/dbhome_1/dbs/ra
    credential_alias=ra-scan:1521/zdlra5:dedicated)'
    FORMAT'%U_%d';
  ALLOCATE CHANNEL c2 DEVICE TYPE sbt_tape
    PARMS='SBT_LIBRARY=/u01/oracle/product/11.2.0.4/dbhome_1/lib/libra.so,
    ENV=(RA_WALLET=location=file:/u01/oracle/product/11.2.0.4/dbhome_1/dbs/ra
    credential_alias=ra-scan:1521/zdlra5:dedicated)'
    FORMAT'%U_%d';
  ALLOCATE CHANNEL c3 DEVICE TYPE sbt_tape
    PARMS='SBT_LIBRARY=/u01/oracle/product/11.2.0.4/dbhome_1/lib/libra.so,
    ENV=(RA_WALLET=location=file:/u01/oracle/product/11.2.0.4/dbhome_1/dbs/ra
    credential_alias=ra-scan:1521/zdlra5:dedicated)'
    FORMAT'%U_%d';
  BACKUP DEVICE TYPE sbt
    TAG 'db_full_incr'
    CUMULATIVE INCREMENTAL LEVEL 1
    DATABASE FORMAT '%d_%U'
    PLUS ARCHIVELOG FORMAT '%d_%U' NOT BACKED UP;
}
```

The `BACKUP ... INCREMENTAL LEVEL 1` command automatically creates a level 0 backup if no level 0 backup already exists.

4.3.2 Creating Incremental Backups of the Protected Database

This section describes how to create a script that performs level 1 incremental backups of the whole protected database and schedule this script to be run at 1 am every day. The backup includes archived redo log files. You can use any job scheduler, including adding your customized RMAN script in an RMAN job in Cloud Control, to schedule the RMAN script to be run at a specified time every day.

To create and schedule a level 1 incremental backup that includes archived redo log files:

1. Ensure that the configuration steps described in ["Enrolling the Protected Database with Recovery Appliance \(Command Line\) \(page 3-12\)"](#) and ["Configuring Backup](#)

and Recovery Settings for Protected Databases (Command Line) (page 3-23)" are completed.

2. Ensure that at least one RMAN SBT channel that corresponds to the Recovery Appliance is configured as described in "Using RMAN Channels for Recovery Appliance Backup and Recovery Operations (page 3-29)".

3.  **Note:**

The backup command in this sections applies when the ZDLRA is the only backup destination. However, if implementing a dual backup strategy, follow either:

- [Implementing a Dual Backup Strategy with Backups to Disk and Recovery Appliance \(Doc ID 2154461.1\)](#)
- [Implementing a Dual Backup Strategy with Backups to Tape and Recovery Appliance \(Doc ID 2154471.1\)](#)

Open a text editor and create and save a file with the following contents.

Save the file in a directory that is accessible to the Oracle Database software and on which the Oracle software owner has the read permission. This script file is saved as `/u01/app/oracle/product/11.2.0.4/db_home1/db_incr_daily.sh`.

```
export ORACLE_HOME=/u01/app/oracle/product/11.2.0.4/dbhome_1
export ORACLE_SID=db1124sm
export PATH=$PATH:$HOME/bin:$ORACLE_HOME/bin:$ORACLE_HOME/Opatch
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/rdbms/lib:/lib:/usr/lib;
export LD_LIBRARY_PATH
export LOG_TRACE_DIR=$HOME/RA_TEST/RMAN_SCRIPTS/LOG
dt=`date +%y%m%d%H%M%S`
$ORACLE_HOME/bin/rman log=$LOG_TRACE_DIR/rman_bkincr_log_db1124sm_$dt.log <<EOF
CONNECT TARGET /
CONNECT CATALOG rauser/welcome1@ra-scan:1521/zdlra5:dedicated

BACKUP DEVICE TYPE SBT
TAG 'db_full_incr'
CUMULATIVE INCREMENTAL LEVEL 1
DATABASE FORMAT '%d_%U'
PLUS ARCHIVELOG FORMAT '%d_%U' NOT BACKED UP;
EOF
```

4. Log in to the protected database host as a user who is a member of the OSBACKUPDBA operating system group.

 **See Also:**

Oracle Database Administrator's Guide for information about the OSBACKUPDBA group

5. Open a text editor, create a file with the following contents, and save the file using the name `.crontab` into your home directory. This example uses the crontab utility to schedule the RMAN script.

```
MAILTO=first.last@example.com
# MI HH DD MM DAY CMD
00 1 * * * /u01/app/oracle/product/11.2.0.4/db_home1/db_incr_daily.sh
```

6. In a command window, change directory to your home directory and enter the following command to create a crontab file for this user from the contents of `.crontab`.

```
# crontab .crontab
```

4.4 Monitoring Protected Database Backups Using Cloud Control

Cloud Control provides reporting capabilities and also enables you to monitor and change the status of protected database backup and recovery jobs.

4.4.1 Viewing Backup Reports for Protected Databases

Cloud Control provides a Backup Report that displays the details of all backup and recovery jobs that were run for a particular protected database. You can filter the data displayed in this report depending on the time period for which you want to see the reports.

To display the Backup Report for a protected database:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. From the Availability menu, select **Backup & Recovery**, then select **Backup Reports**.

The View Backup Report page is displayed.

3. Filter the data displayed in the backup report using the fields in the Search section. You can filter by job status, type of backup job, or start time.
4. Click **Go** to display the backup report.

[Figure 4-2](#) (page 4-9) displays a Backup Report of incremental backup jobs that completed with warnings within the last one week. You can view additional details about a particular job by clicking a backup name in the Backup Name column.

Figure 4-2 Protected Database Backup Report

Logged in as SYS

View Backup Report
The following backup jobs are known to the database. The data is retrieved from the recovery catalog. [View Backup Sets And Image Copies](#)


Search

Status: Start Time: Type:

Results

Total 2 (! 2)

Backup Name	Status	Start Time	Time Taken	Type	Output Devices	Input Size	Output Size	Output Rate (Per Sec)
2014-06-12T10:12:38	COMPLETED WITH WARNINGS	Jun 12, 2014 10:12:44 AM PDT	00:06:33	DB INCR	SBT_TAPE	14.85G	9.75G	25.40M
2014-06-12T10:04:40	COMPLETED WITH WARNINGS	Jun 12, 2014 10:04:45 AM PDT	00:07:20	DB INCR	SBT_TAPE	14.85G	14.17G	32.98M

 **TIP** * in Output Devices column indicates that backups from this job are on DISK and SBT_TAPE

4.4.2 Viewing the Status of Protected Database Backup Jobs

The Job Activity report displays details about the active, completed, and failed jobs for the protected database.

This report enables you to perform the following tasks:

- view additional details for each job
- suspend, resume, or stop currently active jobs
- modify the status of scheduled jobs

To view that status of protected database jobs:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. From the Oracle Database menu, select **Job Activity**.
The Job Activity page is displayed.
3. Use the Advanced Search section to provide criteria that filter the jobs displayed in the report.

The following fields specify criteria that filter the jobs displayed in the report:

- **Owner:** Select the owner of the job.
 - **Start:** Select the start time. Backup jobs scheduled to start during or after the selected time period are displayed. For example, select Last 7 Days to display jobs scheduled to start in the last 7 days.
 - **Job Type:** Select the type of job. For example, to display backup jobs select Database Backup.
 - **Status:** Select the status of the job. For example, to display the currently running jobs select Running.
4. Click **Go** to generate the report according to the specified criteria. [Figure 4-3](#) (page 4-10) shows the Job Activity Report for database backup jobs.

Figure 4-3 Job Activity Report for Protected Database Backup Jobs

Oracle Database Performance Availability Security Schema Administration

db12102 > Job Activity Page Refreshed Jun 12, 2014 10:05:23 PM PDT Auto Refresh Off

Job Activity

Advanced Search

Name:
 Owner: All
 Start: Last 31 days
Show jobs scheduled to start during or after the selected period.

Job Type: Database Backup
 Status: Succeeded
 Go Simple Search

View Results Edit Create Like Copy To Library Suspend Resume Stop Delete View Runs Create Job OS Command

Select	Name	Status (Executions)	Scheduled
<input checked="" type="radio"/>	BACKUP_DB1123ME_000021	1 Succeeded	May 26, 2014 10:41:57 AM GMT-07:00
<input type="radio"/>	BACKUP_DB12ORCL_000022	1 Succeeded	May 26, 2014 2:13:41 PM GMT-07:00
<input type="radio"/>	BACKUP_DB1211ZS_000051	1 Succeeded	May 29, 2014 10:38:00 AM GMT-07:00
<input type="radio"/>	BACKUP_DB1211ZS_000056	1 Succeeded	May 29, 2014 12:35:50 PM GMT-07:00
<input type="radio"/>	BACKUP_DB12CDB_000083	1 Succeeded	Jun 12, 2014 7:25:15 PM GMT-07:00

- To view the details of a particular job execution, select the job and click **View Results**.

To stop the execution of a particular job, select the job and click **Stop**. Similarly, you can use options to suspend, resume, or delete a job.

5

Recovering Data from Recovery Appliance

This chapter explains how to use backups stored on Recovery Appliance to recover your protected database after a failure.

This chapter contains the following sections:

- [Overview of Restoring and Recovering Data from Recovery Appliance](#) (page 5-1)
- [Recovering Protected Databases Using Cloud Control](#) (page 5-1)
- [Restoring and Recovering Data from Recovery Appliance Using the Command Line](#) (page 5-4)
- [Database Duplication from Recovery Appliance](#) (page 5-18)

5.1 Overview of Restoring and Recovering Data from Recovery Appliance

You can recover the entire protected database, one or more data files, or one or more tablespaces. If only certain data blocks in the protected database are corrupt, then you can perform block recovery to repair only the corrupted blocks. The recovery procedures using Recovery Appliance are identical to those used to recover a database within a conventional RMAN environment. The major difference is the use of a Recovery Appliance as the source for recovery data by configuring or allocating an RMAN channel that corresponds to the Recovery Appliance backup module.

You can use Enterprise Manager Cloud Control (Cloud Control) or RMAN to restore and recover protected databases.

5.2 Recovering Protected Databases Using Cloud Control

Cloud Control provides the following techniques to recover protected databases:

- Oracle Advised Recovery

Oracle Advised Recovery enables you to recover the protected database by using the automatic repair actions recommended by Data Recovery Advisor. The Data Recovery Advisor automatically diagnoses data failures, assesses their impact, reports these failures to the user, determines appropriate repair options, and executes repairs at the user's request.

See Also:

Oracle Database Backup and Recovery User's Guide for more information about performing Oracle advised recovery

- User Directed Recovery

This technique performs manual recovery based on the specified criteria. You must provide information such as the objects that must be recovered (database, data files, tablespaces, archived redo logs), whether to perform complete recovery or point-in-time recovery, location to which database files must be recovered, and so on.

 **See Also:**

Oracle Database Backup and Recovery User's Guide for more information about performing user-directed recovery

5.2.1 Prerequisites for Recovering Protected Databases Using Cloud Control

- The protected database must be enrolled and registered with the target Recovery Appliance.
- Backups required for the recovery process must be stored on the Recovery Appliance. When performing point-in-time recovery, you can recover to any point within the recovery window defined for a protected database.

5.2.2 Performing Block Media Recovery Using Cloud Control

This section describes how to recover corrupted data blocks by using Oracle Advised Recovery.

To recover from a failure caused by corrupted data blocks:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. Ensure that the prerequisites described in "[Prerequisites for Recovering Protected Databases Using Cloud Control](#) (page 5-2)" are met.
3. From the Availability menu, select **Backup & Recovery**, and then select **Perform Recovery**.

The Perform Recovery page is displayed. Any failures diagnosed by the Data Recovery Advisor are displayed in the Oracle Advised Recovery section.

4. Click **Advise and Recover**.

The failures detected by Data Recovery Advisor are listed.

5. In the User Directed Recovery section, select the following options:

- In Recovery Scope, select **Datfiles**.
- In Operation Type, select **Block Recovery**.

6. Click **Recover** to display the Perform Object Level Recovery: Block Recovery page.
7. Select **Corruption List** and click **Next**.

The Perform Object Level Recovery: Corrupted Blocks page is displayed. The Datafile Name section displays the data file name and the block IDs of the corrupt blocks.

8. Review the data file name and list of corrupt blocks and click **Next**.

The Perform Object Level Recovery: Schedule page is displayed. A default name and description are entered for the recovery job.

9. If required, edit the name and description of the recovery job and click **Next**.

The Perform Object Level Recovery: Review page is displayed.

10. (Optional) View and edit the RMAN script generated for this recovery job by clicking **Edit RMAN Script**.

11. Click **Submit Job**.

A message is displayed indicating that the job is submitted successfully.

12. Click **View Job**.

The Job page containing the job execution details is displayed. The Summary section provides information such as the type of job, protected database name, SID, and Recovery Appliance catalog user name. The table at the bottom of this page displays the execution steps and their status.

5.2.3 Recovering an Entire Database Using Cloud Control

This section describes how to recover the entire protected database to the current time using the user-directed recovery process in Cloud Control.

To perform complete recovery of the protected database:

1. Access the home page for the protected database as described in "[Accessing the Protected Database Home Page Using Cloud Control](#) (page 3-11)".
2. Ensure that the prerequisites described in "[Prerequisites for Recovering Protected Databases Using Cloud Control](#) (page 5-2)" are met.
3. From the Availability menu, select **Backup & Recovery**, and then select **Perform Recovery**.

The Perform Recovery page is displayed.

4. In the User Directed Recovery section, select the following options:
 - In Recovery Scope, select **Whole Database**.
 - In Operation Type, select **Recover to the current time or a previous point-in-time**.
5. Click **Recover** to display the Perform Whole Database Recovery: Point-in-time page.
6. Select **Recover to the current time** and click **Next**.

The Perform Whole Database Recovery: Rename page is displayed.

7. Select **No. Restore the files to the default location** and click **Next**.

The Perform Whole Database Recovery: Schedule page is displayed.
8. (Optional) Modify the default names provided for the Job Name and Job Description.

9. Click **Next** to display the Perform Whole Database Recovery: Review page.
10. (Optional) To edit the RMAN script generated for this recovery job, click **Edit RMAN Script**.
11. Click **Submit Job**.

A message is displayed indicating that the job is submitted successfully.

12. Click **View Job**.

The Job page containing the job execution details is displayed. The Summary section provides information such as the type of job, protected database name, SID, and Recovery Appliance catalog user name. The table at the bottom of the Summary page displays the execution steps and their status.

5.3 Restoring and Recovering Data from Recovery Appliance Using the Command Line

The examples in this section contain procedures that represent typical restore and recovery scenarios. If a protected database has been correctly configured for backup operations with a Recovery Appliance as described in "[Configuring Backup and Recovery Settings for Protected Databases \(Command Line\)](#) (page 3-23)", it can use the same configuration for recovery operations.

When using Recovery Appliance for restore and recovery operations, the RMAN connection syntax used is the same as with a regular RMAN recovery catalog connection. The only difference is that you connect to the Recovery Appliance catalog and configure RMAN channels as described in "[Using RMAN Channels for Recovery Appliance Backup and Recovery Operations](#) (page 3-29)".



See Also:

Oracle Database Backup and Recovery User's Guide for a complete description of how to recover databases

This section contains the following examples:

- [Example: Restoring and Recovering an Entire Database With the Existing Current Control File](#) (page 5-7)
- [Example: Recovering an Entire Database to a Specified Point-in-Time](#) (page 5-7)
- [Example: Restoring and Recovering the Control File](#) (page 5-9)
- [Example: Restoring and Recovering Tablespaces in the Protected Database](#) (page 5-9)
- [Example: Restoring and Recovering a Data File in the Protected Database](#) (page 5-10)
- [Example: Restoring and Recovering PDBs](#) (page 5-11)
- [Example: Recovering a PDB in an Oracle RAC Environment](#) (page 5-14)

- [Example: Restoring and Recovering One or Many Data Blocks in a PDB \(page 5-14\)](#)
- [Example: Recovering a Database Configured for Real-Time Redo Transport After a Severe Storage Failure \(page 5-15\)](#)
- [Example: Recovering the Control File and Database When Real-Time Redo Transport is Configured \(page 5-17\)](#)

5.3.1 Prerequisites for Restoring and Recovering Data from Recovery Appliance

Ensure that the following prerequisites are met before you use backups stored on Recovery Appliance to restore and recover your protected database:

- The protected database must be enrolled and registered with the target Recovery Appliance.

This is important if you have multiple Recovery Appliances or a Data Guard environment where primary and standby backs up to different Recovery Appliances.

- Backups required to restore and recover the protected database must be stored on the Recovery Appliance. When performing point-in-time recovery, you can recover to any point within the recovery window defined for the protected database.
- The Oracle wallet containing credentials used to authenticate with the Recovery Appliance must be configured on the protected database.
- Configure or allocate RMAN SBT channels that correspond to the Recovery Appliance backup module. The examples in this chapter assume that an SBT channel is configured for Recovery Appliance.

It is recommended that you configure channels using the `RMAN CONFIGURE` command because these settings are persistent settings. However, you can override the configured channel settings by using the `ALLOCATE CHANNEL` command within the `RUN` block that performs the backup or recovery operation.

See Also:

- ["Enrolling the Protected Database with Recovery Appliance \(Command Line\) \(page 3-12\)"](#)
- ["Installing the Recovery Appliance Backup Module \(page 3-14\)"](#)
- ["Creating an Oracle Wallet on the Protected Database \(page 3-27\)"](#)
- ["Using RMAN Channels for Recovery Appliance Backup and Recovery Operations \(page 3-29\)"](#)

5.3.2 Restoring Protected Databases Using a Downstream Recovery Appliance

When Recovery Appliance replication is configured, the protected database sends backups to the upstream Recovery Appliance. The upstream Recovery Appliance then forwards these backups to the downstream Recovery Appliance. In the event of a failure, if the upstream Recovery Appliance is unavailable, then you can perform restore operations using the downstream Recovery Appliance.

 **See Also:**

"[Protected Databases and Recovery Appliance Architecture](#) (page 1-2)" for a brief overview of replication

Use the following high-level steps to restore a protected database directly from a downstream Recovery Appliance:

1. Create an Oracle wallet that contains the credentials of the VPC user with which the protected database will authenticate with the downstream Recovery Appliance.

 **See Also:**

"[Creating an Oracle Wallet on the Protected Database](#) (page 3-27)"

 **Note:**

The protected database need not be explicitly added to or registered with the downstream Recovery Appliance before performing restore operations. When replication is configured between the upstream and downstream Recovery Appliance, the protected databases enrolled with the upstream Recovery Appliance are registered with the downstream Recovery Appliance.

2. Connect to the protected database as `TARGET` and to the downstream Recovery Appliance catalog as `CATALOG`.

 **See Also:**

"[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)"

3. Allocate an RMAN SBT channel that corresponds to the downstream Recovery Appliance, place the protected database in `MOUNT` mode, and restore the protected database.

All these statements must be enclosed within a `RUN` block as shown in "Example: Restoring and Recovering an Entire Database With the Existing Current Control File (page 5-7)".



See Also:

"Allocating RMAN SBT Channels for Recovery Appliance (page 3-30)"

5.3.3 Example: Restoring and Recovering an Entire Database With the Existing Current Control File

This example assumes that some or all the data files in the protected database are lost or damaged. However, the control file is available.

To restore and recover all the data files in a protected database:

1. Ensure that the prerequisites described in "Prerequisites for Restoring and Recovering Data from Recovery Appliance (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG`.



See Also:

"Connecting to the Protected Database and Recovery Appliance Using CLI (page 2-5)"

3. Restore and recover all the data files using the following command:

```
STARTUP MOUNT;  
RUN  
{  
  RESTORE DATABASE;  
  RECOVER DATABASE;  
  ALTER DATABASE OPEN;  
}
```

5.3.4 Example: Recovering an Entire Database to a Specified Point-in-Time

This example demonstrates how to perform point-in-time recovery (PITR) for a protected database. PITR may be required to revert the protected database to a prior date to recover from user errors (accidentally dropping tables or updating the wrong tables), media failure, or a failed database upgrade. You need to restore the control file only if there has been a structural change to the control file (such as creating or dropping tablespaces). Use the `SET UNTIL` clause to specify the time, SCN, or log sequence to which the protected database must be recovered.

If Flashback Database is enabled for the protected database, you can also use this feature to recover to a prior point-in-time.

 **See Also:**

- *Oracle Database Backup and Recovery User's Guide*
- *Oracle Database Backup and Recovery Reference*

To restore and recover the entire protected database, including the control file, to a specific point-in-time:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG`.

 **See Also:**

["Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)"](#)

3. Determine the point-in-time to which the protected database must be recovered. You can use an SCN, a time, or log sequence number to specify the point-in-time.

Use the following query to translate between timestamp and SCN:

```
SQL> set linesize 222
SQL> select name, current_scn, scn_to_timestamp(current_scn) "Time"
       from v$database;
```

NAME	CURRENT_SCN	TIME
ORA121	122019556	22-APR-14 12.30.15.000000000 PM

If the protected database is not available, you can query the Recovery Appliance catalog views to obtain the SCN number. You must provide the range date and time for your recovery window and the `db_unique_name` of the protected database. The following query (sample output included) is run when connected to the Recovery Appliance catalog:

```
SELECT a.db_key,
       a.db_name,
       a.sequence#,
       a.first_change#,
       a.next_change#,
       a.completion_time
FROM rc_archived_log a, db b
WHERE b.reg_db_unique_name = 'PTDB2' AND a.db_key = db.db_key
      AND to_date('16-Jul-2014 06:55:23', 'DD-Mon-YYYY HH24:MI:SS') BETWEEN
          a.first_time AND a.next_time;
```

DB_KEY	DB_NAME	SEQUENCE#	FIRST_CHANGE#	NEXT_CHANGE#	COMPLETION_TIME
24201	PTDB2	9911	288402086	288430116	14/07/2014 5:27:49 PM

The `FIRST_CHANGE#` corresponds to the first SCN number in the archive redo log and the `NEXT_CHANGE#` is the last SCN number in the archive redo log.

4. Restore and recover the control file and the protected database.

```
STARTUP NOMOUNT;
RUN
{
  SET UNTIL TIME "TO_DATE('2014-14-07:17:27:49','yyyy-dd-mm:hh24:mi:ss')";
  RESTORE CONTROLFILE;
  ALTER DATABASE MOUNT;
  RESTORE DATABASE;
  RECOVER DATABASE;
  ALTER DATABASE OPEN RESETLOGS;
}
```

5.3.5 Example: Restoring and Recovering the Control File

This example demonstrates how to recover a protected database after the loss of all control file copies. It is strongly recommended that you create multiple copies of your control files in separate disk locations.

To restore and recover the control file in a protected database:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG`.



See Also:

["Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)"](#)

3. Restore the control file and then mount the database using the following command:

```
STARTUP NOMOUNT;
RUN
{
  RESTORE CONTROLFILE;
  ALTER DATABASE MOUNT;
}
```

5.3.6 Example: Restoring and Recovering Tablespaces in the Protected Database

This example demonstrates how to restore and recover one or more tablespaces in the protected database after they are accidentally dropped or corrupted. The example assumes that the database is up and running and that you will restore only the affected tablespaces.

To restore and recover one or more tablespaces:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG`.

 **See Also:**

["Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)"](#)

3. Restore and recover the affected tablespaces.

The following command restores and recovers the `USERS` tablespace:

```
RUN
{
  SQL 'ALTER TABLESPACE users OFFLINE';
  RESTORE TABLESPACE users;
  RECOVER TABLESPACE users;
  SQL 'ALTER TABLESPACE users ONLINE';
}
```

5.3.7 Example: Restoring and Recovering a Data File in the Protected Database

This example demonstrates how to restore and recover a data file that was accidentally deleted or corrupted.

To restore and recover a data file in a protected database:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG`.

 **See Also:**

["Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)"](#)

3. Restore and recover the affected data file in the protected database using the following command:

The following command restores and recovers data file 3 in the protected database:

```
RUN
{
  SQL 'ALTER DATABASE DATAFILE 3 OFFLINE';
  RESTORE DATAFILE 3;
```

```
RECOVER DATAFILE 3;
SQL 'ALTER DATABASE DATAFILE 3 ONLINE';
}
```

5.3.8 Example: Restoring and Recovering PDBs

The multitenant architecture, introduced in Oracle Database 12c Release 1, enables an Oracle Database to function as a multitenant container database (CDB) that includes zero, one, or many customer-created pluggable databases (PDBs). All Oracle databases before Oracle Database 12c are non-CDBs.

A CDB includes the following components: root, seed, and user-created PDBs. The root stores the common users and Oracle-supplied metadata such as the source code for Oracle-supplied packages. The seed is a template that can be used to create new PDBs. A PDB is a portable collection of schemas, schema objects, and nonschema objects that appears to an Oracle Net client as a non-CDB.

This section demonstrates various restore and recovery scenarios for PDBs. The steps to restore and recover a PDB are similar to those used for restore and recover operations on non-CDBs. This section contains the following examples:

- [Performing Complete Recovery of the Whole PDB](#) (page 5-11)
- [Performing Point-in-Time Recovery for the Whole PDB](#) (page 5-12)
- [Recovering Specific Data Files in a PDB](#) (page 5-12)
- [Recovering Specific Tablespaces in a PDB](#) (page 5-13)

5.3.8.1 Performing Complete Recovery of the Whole PDB

This example demonstrates how to perform complete recovery for a PDB in the protected database.

To restore and recover a whole PDB:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the root of the CDB as `TARGET` and the Recovery Appliance catalog as `CATALOG`.



See Also:

["Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)"

3. Identify the PDB that needs to be restored by running the following query in the CDB:

```
SELECT name FROM v$pdb;
```

4. Restore and recover the required PDB in your protected database.

The following command restores and recovers the PDB `hr_pdb`:

```
RUN
{
```

```

ALTER PLUGGABLE DATABASE "hr_pdb" CLOSE IMMEDIATE;
RESTORE PLUGGABLE DATABASE 'hr_pdb';
RECOVER PLUGGABLE DATABASE 'hr_pdb';
ALTER PLUGGABLE DATABASE "hr_pdb" OPEN;
}

```

5.3.8.2 Performing Point-in-Time Recovery for the Whole PDB

This example demonstrates how to perform point-in-time recovery for one or more PDBs in your protected database. Specify the `SET UNTIL` clause to indicate the point to which the PDB must be recovered.

To restore and recover a PDB to a specific point-in-time:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the root of the CDB as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Identify the PDB that needs to be restored by running the following query in the CDB:

```
SELECT name FROM v$pdb;
```

4. Restore and recover the affected PDB to the specified point in time.

The following command restores and recovers the PDB `hr_pdb` to the point in time specified by the `SET UNTIL` clause.

```

RUN
{
  SET UNTIL TIME "to_date('2014-08-16 09:00:00','YYYY-MM-DD HH24:MI:SS')";
  ALTER PLUGGABLE DATABASE "hr_pdb" CLOSE IMMEDIATE;
  RESTORE PLUGGABLE DATABASE 'hr_pdb';
  RECOVER PLUGGABLE DATABASE 'hr_pdb';
  ALTER PLUGGABLE DATABASE hr_pdb OPEN RESETLOGS;
}

```

5.3.8.3 Recovering Specific Data Files in a PDB

Restoring and recovering data files in a PDB is similar to restoring and recovering any data file using RMAN. This example demonstrates how to restore and recover a data file in a PDB.

To restore and recover a specific data file in a PDB:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the root of the CDB as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Identify the PDB that needs to be restored by running the following query in the CDB:

```
SELECT name FROM v$pdb;
```


4. Identify the number of the data file in the PDB that needs to be recovered using the following query:

```
SELECT p.PDB_ID, p.PDB_NAME, d.FILE_ID, d.TABLESPACE_NAME, d.FILE_NAME
FROM DBA_PDBS p, CDB_DATA_FILES d
WHERE p.PDB_ID = d.CON_ID
ORDER BY p.PDB_ID;
```

5. Restore and recover the affected data files in the PDB.

The following example restores and recovers data file number 10 in the PDB.

```
RUN
{
  SQL 'ALTER DATABASE DATAFILE 10 OFFLINE';
  RESTORE DATAFILE 10;
  RECOVER DATAFILE 10;
  SQL 'ALTER DATABASE DATAFILE 10 ONLINE';
}
```

5.3.8.4 Recovering Specific Tablespaces in a PDB

This example demonstrates how to restore and recover the tablespace `USR_TBS` contained in the PDB `SH_PDB` in your protected database.

Restoring and recovering a tablespace in a PDB is similar to a normal tablespace restore and recovery. The difference is that you need to map the tablespace to the pluggable database (`pdb_name:tablespace_name`).

To restore and recover specific tablespaces in a PDB:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the root of the CDB as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Place the affected tablespace in offline mode.

The following example places the tablespace `use_tbs` in the PDB `sh_pdb` in offline mode.

```
ALTER TABLESPACE sh_pdb:usr_tbs OFFLINE;
```

4. Restore and recover the affected tablespaces contained in the PDB within your protected database.

The following example restore and recovers the tablespace `usr_tbs` in the PDB `sh_pdb`.

```
RUN
{
  RESTORE TABLESPACE sh_pdb:usr_tbs;
  RECOVER TABLESPACE sh_pdb:usr_tbs;
}
```

5. Make the restored and recovered tablespace online.

The following example brings the tablespace `usr_tbs` in the PDB `sh_pdb` online.

```
ALTER TABLESPACE sh_pdb:usr_tbs ONLINE;
```

5.3.9 Example: Recovering a PDB in an Oracle RAC Environment

The process to restore and recover a PDB in an Oracle Real Application Clusters (Oracle RAC) environment has some slight additions to the non-Oracle RAC process. This example demonstrates how to recover a PDB in an Oracle RAC environment.

To restore and recover a PDB in an Oracle RAC environment:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the root of the CDB as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Ensure that all instances of the affected PDB are closed.

The following command closes all instances of the PDB `hr_pdb`.

```
ALTER PLUGGABLE DATABASE "hr_pdb" CLOSE IMMEDIATE INSTANCES=all;
```

4. Restore and recover the affected PDB in your protected database.

The following command restores and recovers the `hr_pdb`.

```
RUN
{
  ALTER PLUGGABLE DATABASE "hr_pdb" CLOSE IMMEDIATE;
  RESTORE PLUGGABLE DATABASE 'hr_pdb';
  RECOVER PLUGGABLE DATABASE 'hr_pdb';
  ALTER PLUGGABLE DATABASE "hr_pdb" OPEN RESETLOGS;
  ALTER PLUGGABLE DATABASE "hr_pdb" OPEN INSTANCES=all;
}
```

5.3.10 Example: Restoring and Recovering One or Many Data Blocks in a PDB

Block media recovery enables you to recover one more corrupt data blocks while the data file is still online. This example demonstrates how to perform block media recovery to recover one or more corrupt data blocks.



See Also:

Oracle Database Backup and Recovery User's Guide

The existence of corrupt data blocks can be indicated by one of the following methods:

- The protected database alert log contains the following message indicating that one or more blocks are corrupt:

```
Sun Aug 17 09:34:48 2014
Hex dump of (file 2, block 16385) in trace file /u01/app/oracle/diag/rdbms/
dbstress/dbstress/trace/dbstress_ora_9732.trc
```

```
Corrupt block relative dba: 0x00004001 (file 2, block 16385)
Fractured block found during backing up datafile
```

```
Data in bad block:
type: 6 format: 2 rdba: 0x00004001
last change scn: 0x0000.00a564c0 seq: 0x1 flg: 0x06
spare1: 0x0 spare2: 0x0 spare3: 0x0
consistency value in tail: 0x00000000
check value in block header: 0xd6dd
computed block checksum: 0x58f7
```

- During an RMAN backup, the block corruption is detected and a message similar to the following will be displayed.

```
RMAN-08038: channel c3: starting piece 1 at 2014/08/17 09:34:43
RMAN-03009: failure of backup command on c1 channel at 08/17/2014 09:34:50
ORA-19566: exceeded limit of 0 corrupt blocks for file /SHARED1/ORADATA/DBF/
dbstress/soe.dbf
.
.
RMAN-03002: failure of backup plus archivelog command at 08/17/2014 09:35:55
RMAN-03009: failure of backup command on c1 channel at 08/17/2014 09:34:50
ORA-19566: exceeded limit of 0 corrupt blocks for file /SHARED1/ORADATA/DBF/
dbstress/soe.dbf
```

To restore and recover corrupt data blocks in the protected database:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Identify the corrupt blocks that need to be recovered.

Use the entries in the protected database alert log to identify corrupt blocks and the data files that contain these corrupt blocks. Or, query the `V$DATABASE_BLOCK_CORRUPTION` view to identify corrupt blocks.

4. Use the `BLOCKRECOVER` command to recover the corrupt data blocks.

The following example recovers the data blocks 46, 56, and 84 in data file 4.

```
RUN
{
  BLOCKRECOVER CORRUPTION LIST;
  BLOCKRECOVER DATAFILE 4 BLOCK 46,56,84;
}
```

5.3.11 Example: Recovering a Database Configured for Real-Time Redo Transport After a Severe Storage Failure

Real-time redo transport, when enabled, guarantees the lowest recovery downtime for protected database. When restoring and recovering a protected database immediately after a storage failure, the necessary complete and partial archived log files are restored and recovered so that media recovery can return the database state to the closest state from when the storage failure occurred.

The following example recovers a protected database that was configured to use real-time redo transport after a storage failure that results in the loss of all data files and online redo log files. To recover the protected database to the highest SCN using the backups and redo logs available at the Recovery Appliance, use the `FINAL_CHANGE#`

column of the `RC_DATABASE` view. The `FINAL_CHANGE#` column contains the highest SCN to which the protected database must be recovered. Use this SCN value in the `SET UNTIL SCN` command prior to performing a recovery. The recovery is performed using only the backups and redo logs available at the Recovery Appliance.

 **Note:**

In the following scenarios, `RC_DATABASE.FINAL_CHANGE#` will contain the value -1 and cannot be used in the `SET UNTIL SCN` command:

- version of the protected database is Oracle Database 11g (Release 11.1) or lower
- `COMPATIBLE` parameter of the protected database was set to 10.0 or lower while sending real-time redo log data to the Recovery Appliance

Instead, use the `NEXT_CHANGE#` column in the `V$ARCHIVED_LOG` view to determine the SCN to which the protected database needs to be recovered.

See My Oracle Support note 243760.1 for additional information. My Oracle Support is available at: <https://support.oracle.com>.

To restore and recover a protected database that is configured to use real-time redo transport:

1. Ensure that the prerequisites described in "[Prerequisites for Restoring and Recovering Data from Recovery Appliance](#) (page 5-5)" are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in "[Connecting to the Protected Database and Recovery Appliance Using CLI](#) (page 2-5)".
3. Determine the SCN to which the protected database must be recovered by querying the `RC_DATABASE` view. This SCN is the highest SCN at the time the database crashed.

```
SELECT final_change# FROM rc_database WHERE name='MY_DB';
```

4. Restore and recover the protected database.

This example assumes that the control file is available. If the control file is lost, then you need to first recover the control file before performing the steps listed here.

```
STARTUP NOMOUNT;
RUN
{
  SET UNTIL SCN 23098;
  RESTORE DATABASE;
  RECOVER DATABASE;
  ALTER DATABASE OPEN RESETLOGS;
}
```

 **Note:**

The `UNTIL SCN` clause is required. Unless a specific SCN value is chosen, the log containing the partial redo is not applied by recovery.

 **See Also:**

- ["About Real-Time Redo Transport \(page 1-12\)"](#)
- *Oracle Database Backup and Recovery Reference* for a description of the `FINAL_CHANGE#` column

5.3.12 Example: Recovering the Control File and Database When Real-Time Redo Transport is Configured

This example recovers a protected database that is configured to use real-time redo transport from the loss of all database files. Since the control file too is lost, you need to first restore the control file and then perform recovery of the protected database.

To restore and recover a protected database, including the control file, that is configured to use real-time redo transport:

1. Ensure that the prerequisites described in ["Prerequisites for Restoring and Recovering Data from Recovery Appliance \(page 5-5\)"](#) are met.
2. Use RMAN to connect to the protected database as `TARGET` and the Recovery Appliance catalog as `CATALOG` as described in ["Connecting to the Protected Database and Recovery Appliance Using CLI \(page 2-5\)"](#).
3. Determine the SCN to which the protected database must be recovered by querying the `RC_DATABASE` view. This SCN is the highest SCN at the time the database crashed.

```
SELECT final_change# FROM rc_database WHERE name='PTDB1';
```

4. Restore and recover the protected database.

This example assumes that the control file is available. If the control file is lost, then you need to first recover the control file before performing the steps listed here.

```
STARTUP FORCE NOMOUNT;
SET DBID=ptdbl;
RESTORE CONTROLFILE;
ALTER DATABASE MOUNT;
RUN
{
  SET UNTIL SCN 34568;
  RESTORE DATABASE;
  RECOVER DATABASE;
}
ALTER DATABASE OPEN RESETLOGS;
```

5.4 Database Duplication from Recovery Appliance

If you need to duplicate a protected database to create a standby database or to clone a protected database to a target host, you can do so by connecting to the Recovery Appliance catalog and using backup-based duplication. By using the catalog, there is no need to connect to the source database. Creating a standby database or a clone both involve running the `RMAN DUPLICATE` command.

See Also:

- *Oracle Database Backup and Recovery User's Guide* for additional information about duplicating databases
- *Oracle Database Backup and Recovery Reference* for the syntax of the `DUPLICATE` command

5.4.1 Creating a Standby Database for a Protected Database

When you create a standby database from Recovery Appliance, you connect to the standby (auxiliary instance) and to the Recovery Appliance catalog, and run the `RMAN DUPLICATE` command with the `FOR STANDBY` option.

Note:

Because the primary database is already registered with the Recovery Appliance catalog, you should not register the standby database with the Recovery Appliance catalog.

To create a standby database for a protected database:

1. On the target host, prepare the auxiliary instance by performing the following tasks:
 - Create the directories in which the standby database files will be stored.
 - Create an initialization parameter file for the auxiliary instance.
The mandatory parameters are `DB_NAME` and `DB_CREATE_FILE_DEST`.
 - Create a password file for the auxiliary database. This password file will be overwritten during the duplicate operation in step 3.
 - Establish Oracle Net connectivity between the protected database and the auxiliary instance.
 - Start the auxiliary instance in `NOMOUNT` mode.
2. Start `RMAN` and connect as `CATALOG` to the Recovery Appliance catalog and as `AUXILIARY` to the auxiliary instance.

In the following example, `ra_rman_user` is the Recovery Appliance user that the protected database `my_ptdb` uses to authenticate with the Recovery Appliance. `ra1`

is the net service name of the target Recovery Appliance that is configured in the Oracle wallet. `stdby` is the net service name of the auxiliary instance.

```
%rman
RMAN> CONNECT CATALOG ra_rman_user@ral;
RMAN> CONNECT AUXILIARY "sys@stdby AS SYSDBA";
```

3. Create the standby database using the `DUPLICATE` command. Configure one or more auxiliary channels that correspond to the Recovery Appliance backup module.

The following example configures three auxiliary channels and creates a standby database for the protected database `my_ptdb`.

```
RUN
{
  ALLOCATE AUXILIARY CHANNEL c1 DEVICE TYPE sbt_tape
  PARS='SBT_LIBRARY=/u01/oracle/product/12.1.0.2/dbhome_1/lib/libra.so,
  ENV=(RA_WALLET=location=file:/u01/oracle/product/12.1.0.2/dbhome_1/dbs/ra
  credential_alias=ra-scan:1521/zdlra5:dedicated)' FORMAT'%U_%d';
  ALLOCATE AUXILIARY CHANNEL c2 DEVICE TYPE sbt_tape
  PARS='SBT_LIBRARY=/u01/oracle/product/12.1.0.2/dbhome_1/lib/libra.so,
  ENV=(RA_WALLET=location=file:/u01/oracle/product/12.1.0.2/dbhome_1/dbs/ra
  credential_alias=ra-scan:1521/zdlra5:dedicated)' FORMAT'%U_%d';
  ALLOCATE AUXILIARY CHANNEL c3 DEVICE TYPE sbt_tape
  PARS='SBT_LIBRARY=/u01/oracle/product/12.1.0.2/dbhome_1/lib/libra.so,
  ENV=(RA_WALLET=location=file:/u01/oracle/product/12.1.0.2/dbhome_1/dbs/ra
  credential_alias=ra-scan:1521/zdlra5:dedicated)' FORMAT'%U_%d';
  DUPLICATE DATABASE my_ptdb FOR STANDBY DORECOVER;
}
```

5.4.2 Cloning a Protected Database

You can clone a protected database to a target host by using backup-based duplication. The Oracle-recommended method, covered in this section, connects to the Recovery Appliance catalog. By using a catalog for the duplicate operation, a connection to the source database is not required.

The example that follows represents the Oracle best practice for cloning a protected database and includes a sample script that you can customize for your scenario.

This example assumes the following:

- backups of the target database exist on the Recovery Appliance and are available to the auxiliary instance
- RMAN connection from the auxiliary database to the Recovery Appliance that contains metadata and backups for the target database is available
- both source and duplicate database use Oracle Managed Files (OMF)
- operating system used is Linux or UNIX
- the audit directory is created on the auxiliary database host
- prerequisites for backup-based duplication are met

The script provided in this example performs the following tasks:

- drops an existing auxiliary database
- backs up the target database
- creates a dummy auxiliary instance and opens it in `NOMOUNT` mode

- duplicates the target database using the target database backups and metadata available on the Recovery Appliance

The duplicate database control file is stored as `+REDO/ORACLE_SID/CONTROLFILE/cf3.ctl` and the data files are stored in the `+DATA` directory.

- verifies that the required objects are created in the duplicate database

To clone a protected database using backup-based duplication without a target connection:

1. Create a parameter file (pfile) for the auxiliary instance. The pfile contains only the `DB_NAME` initialization parameter which is set to the SID of the duplicate database.

The following pfile, called `init_dup.ora` and located in the `/home/oracle` directory, sets the `DB_NAME` parameter. Replace `dup_db` with the SID of your duplicate database:

```
*.db_name = 'dup_db'
```

2. Use a text editor and create a Shell script (called `dup_db.sh` in this example) with the contents shown below and with the following modifications:

- Replace the value of the `ORACLE_HOME` variable with the Oracle home directory of your auxiliary instance.
- Replace the value of the `logdir` variable with the directory in which you want to store log files.
- Replace the following placeholders (shown in Italics) with values appropriate to your duplication scenario:

dup_db: system identifier (SID) and service name of the auxiliary instance

tgt_db: SID and service name of the target database

sys_pwd: password for the `sys` user of the target database

vpc_user: name of the VPC user

vpc_user_pwd: password for the VPC user `vpc_user`

ra_scan: Single Client Access Name (SCAN) of the Recovery Appliance

ra_servicename: service name of the Recovery Appliance metadata database

system_pwd: password for the `SYSTEM` user in the target database

- If you want to store the duplicate database control file using a name and location that is different from `+REDO/ORACLE_SID/CONTROLFILE/cf3.ctl`, then replace the value of `control_files` in the `dup_aux_db` function with a value that is appropriate for your duplication scenario.
- If you want to store the duplicate data files in a directory that is different from `+DATA`, then replace the value of `db_create_file_dest` in the `dup_aux_db` function with a value that is appropriate for your duplication scenario.

```
#!/bin/bash
export ORACLE_HOME=/u01/app/oracle/product/11.2.0.4/dbhome_2
export ORACLE_BASE=/u01/app/oracle
export ORACLE_SID=dup_db
export PATH=$PATH:$HOME/bin:$ORACLE_HOME/bin:$ORACLE_HOME/Opatch
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/rdbms/lib:/lib:/usr/lib;
export LD_LIBRARY_PATH
export logdir=/home/oracle/log
```



```
export dt='date +%y%m%d%H%M%S'
export NLS_DATE_FORMAT='DD-MM-YYYY HH24:MI:SS'

function drop_aux_db {
export ORACLE_SID=dup_db
$ORACLE_HOME/bin/sqlplus -s '/ as sysdba' <<EOF2
set pagesize 999 linesize 999 heading off feedback off
select name, open_mode from v\${database};
shutdown immediate;
startup mount exclusive restrict;
drop database;
exit;
EOF2
}

echo "Backup the target database"
function backup_source_db {
$ORACLE_HOME/bin/rman target sys/sys_pswd@tgt_db catalog
vpc_user/vpc_user_pswd@ra_scan:1521/ra_serivcename:dedicated <<EOF
RUN {
backup as backupset cumulative incremental level 1 database include current
controlfile plus archivelog not backed up delete input;}
exit;
EOF
}

sleep 120

echo "List the backup of the target database"
function check_source_db_backup {
$ORACLE_HOME/bin/rman target sys/sys_pswd@tgt_db catalog vpc_user/
vpc_user_pswd@ra_scan:1521/ra_serivcename:dedicated <<EOF
LIST BACKUP OF DATABASE COMPLETED AFTER '(SYSDATE-1/24)';
EOF
}

echo "Start the auxiliary database in FORCE NOMOUNT mode"
function nomount_aux_db {
export ORACLE_SID=dup_db
$ORACLE_HOME/bin/rman target / <<EOF2
startup force nomount pfile='/home/oracle/init_dup.ora';
exit;
EOF2
}

echo "Duplicate the target database"
function dup_aux_db {
export ORACLE_SID=dup_db
$ORACLE_HOME/bin/rman catalog vpc_user/vpc_user_pswd@ra_scan:1521/
ra_serivcename:dedicated AUXILIARY /
<<EOF
duplicate database tgt_db to dup_db spfile
set control_files '+REDO/${ORACLE_SID}/CONTROLFILE/cf3.ctl'
set db_create_file_dest '+DATA/' ;
exit;
EOF
}

echo "Check schema objects on the target"
function check_source_db {
$ORACLE_HOME/bin/sqlplus -s system/system_pswd@tgt_db <<EOF2
```

```
set pagesize 999 linesize 999 heading off feedback off
select name, open_mode from v\${database};
select table_name, num_rows from dba_tables where owner='SOE';
exit;
EOF2
}

echo "Check schema objects on the auxiliary"
function check_aux_db {
export ORACLE_SID=dup_db
${ORACLE_HOME}/bin/sqlplus -s '/' as sysdba' <<EOF2
set pagesize 999 linesize 999 heading off feedback off
select name, open_mode from v\${database};
select table_name, num_rows from dba_tables where owner='SOE';
exit;
EOF2
}

drop_aux_db
backup_source_db
check_source_db_backup
nomount_aux_db
dup_aux_db
check_source_db
check_aux_db
```

3. Set execute permissions on the script `dup_db.sh` using the `chmod` command.

```
$ chmod +x dup_db.sh
```

4. On the duplicate host (that hosts the duplicate database), run the `dup_db.sh` script.

The following command runs the `dup_db.sh` script that is stored in the `/home/my_scripts/duplication` directory:

```
$ ./home/my_scripts/duplication/dup_db.sh
```

A

Differences in RMAN Commands

This appendix describes changes and limitations to standard RMAN commands when using Recovery Appliance.

Table A-1 Modified RMAN Commands

RMAN Command	Notes
CHANGE BACKUP ... UNAVAILABLE	This command should not be used with virtual backups.
CHANGE BACKUP ... UNCATALOG	This command should not be used with virtual backups.
CONFIGURE ... RETENTION POLICY	If <code>RETENTION POLICY</code> is set to <code>NONE</code> , then it is recommended that you configure a fast recovery area for local archived logs. The fast recovery area automatically manages its storage. As long as the fast recovery area has been sized appropriately for maintaining local logs, the fast recovery area will purge its storage space when necessary. Note: You can also store archived redo log backups to any disk directory when using a parallel backup strategy.
DELETE	DO NOT USE. Unlike normal backups, Recovery Appliance backup sets can include virtual backup and SBT pieces that are critical for successful recovery operations. In addition, missing backup pieces can interfere with indexing operations, tying up system resources and affecting the ingestion of new backups.
DROP DATABASE	Use the <code>DBMS_RA.DELETE_DB</code> procedure to unregister the protected database from the Recovery Appliance and then use the <code>DROP DATABASE</code> command.
MAXPIECESIZE clause	The <code>MAXPIECESIZE</code> clause of the <code>CONFIGURE</code> or <code>ALLOCATE</code> command is not supported for Recovery Appliance.
UNREGISTER DATABASE	Use the <code>DBMS_RA.DELETE_DB</code> procedure, instead of <code>UNREGISTER DATABASE</code> , to unregister a protected database from the Recovery Appliance. Note: See <i>Zero Data Loss Recovery Appliance Administrator's Guide</i> for information about the <code>DELETE_DB</code> procedure.

Index

A

administration tasks
protected databases, [1-5](#)

B

backing up
incremental-forever backup strategy, [4-5](#)
Oracle-suggested backup strategy, [4-2](#)
using Enterprise Manager, [4-4](#)
using RMAN, [4-5](#)
backup polling, [1-8](#)
backup reports
for protected databases, [4-8](#)
backup settings
about, [3-6](#)
using Enterprise Manager, [3-18](#)
using RMAN, [3-24](#)
block media recovery
using Enterprise Manager, [5-2](#), [5-3](#)

C

clone databases
from Recovery Appliance, [5-19](#)
configuration parameters
for Recovery Appliance backup module, [3-4](#)
configuring
protected database backup settings
using Enterprise Manager, [3-18](#)
using RMAN, [3-24](#)
protected database recovery settings
using Enterprise Manager, [3-21](#)
using RMAN, [3-28](#)
protected databases
high-level steps, [3-2](#)
overview, [3-1](#)
real-time redo transport
using Enterprise Manager, [3-11](#)
using RMAN, [3-24](#)
creating
clone databases from Recovery Appliance,
[5-19](#)
Enterprise Manager administrator, [3-9](#)

creating (*continued*)
standby databases from Recovery Appliance,
[5-18](#)
test backup
using Enterprise Manager, [3-31](#)
using RMAN, [3-30](#)

E

enrolling protected databases
about, [3-5](#)
using Enterprise Manager, [3-8](#), [3-10](#)
using RMAN, [3-12](#)
Enterprise Manager
accessing protected database home page,
[3-11](#)
examples
recovering protected databases, [5-4](#)
restoring protected databases, [5-4](#)

I

incremental-forever backup strategy, [1-11](#)
using with RMAN, [4-5](#)
installing
Recovery Appliance backup module, [3-14](#)
interfaces
protected database operations, [1-14](#)

O

Oracle Advised recovery
about, [5-1](#)
Oracle-suggested backup strategy
using Enterprise Manager, [4-2](#)

P

PDBs, [5-12](#)
performing complete recovery, [5-11](#)
performing point-in-time recovery, [5-12](#)
recovering data files, [5-12](#)
recovering tablespaces, [5-13](#)
pluggable databases
See PDBs

protected databases

- accessing Enterprise Manager home page, [3-11](#)
- administrator, [1-6](#)
- administrator tasks, [1-5](#)
- backing up
 - using Enterprise Manager, [4-4](#)
 - using RMAN, [4-5](#)
- backup polling, [1-8](#)
- backup reports, [4-8](#)
- backup settings, [3-6](#)
- configuring
 - high-level steps, [3-2](#)
 - overview, [3-1](#)
- configuring backup settings
 - using Enterprise Manager, [3-18](#)
 - using RMAN, [3-24](#)
- configuring real-time redo transport
 - using Enterprise Manager, [3-11](#)
 - using RMAN, [3-24](#)
- configuring recovery settings
 - using Enterprise Manager, [3-21](#)
 - using RMAN, [3-28](#)
- creating Enterprise Manager administrator, [3-9](#)
- enrolling
 - about, [3-5](#)
 - using Enterprise Manager, [3-8](#), [3-10](#)
 - using RMAN, [3-12](#)
- incremental-forever backup strategy, [1-11](#)
- interfaces, [1-14](#)
- metadata on Recovery Appliance, [1-8](#)
- modify scheduled job status, [4-9](#)
- Oracle Advised recovery, [5-1](#)
- overview, [1-2](#)
- performing user-directed recovery, [5-4](#)
- recovering, [5-1](#)
 - all data files, [5-7](#)
 - control file, [5-9](#)
 - corrupt blocks, [5-14](#)
 - data file, [5-10](#)
 - in Oracle RAC environment, [5-14](#)
 - prerequisites, [5-5](#)
 - tablespaces, [5-9](#)
 - using PITR, [5-7](#)
 - with real-time redo transport, [5-15](#)
- recovery settings overview, [3-7](#)
- registering with Recovery Appliance, [3-17](#)
- required privileges, [1-6](#)
- restoring, [5-1](#)
 - examples, [5-4](#)
 - prerequisites, [5-5](#)
- resume jobs, [4-9](#)
- stop running jobs, [4-9](#)
- suspend jobs, [4-9](#)

protected databases (*continued*)

- task flow, [1-14](#)
- techniques for sending backups, [1-7](#)
- test backup
 - using Enterprise Manager, [3-31](#)
 - using RMAN, [3-30](#)
- test recovery
 - using RMAN, [3-31](#)
- user directed recovery, [5-2](#)
- users, [1-6](#)
- using incremental-forever backup strategy, [4-5](#)
- view job details, [4-9](#)

protection policies, [1-7](#)

R

real-time redo transport

- about, [1-12](#)
- configuring
 - using Enterprise Manager, [3-11](#)
 - using RMAN, [3-24](#)
- recovering protected databases, [5-15](#)

recovering

- all data files in a protected database, [5-7](#)
- corrupt blocks
 - using Enterprise Manager, [5-2](#), [5-3](#)
- data files in a PDB, [5-12](#)
- PDBs
 - complete recovery, [5-11](#)
 - point-in-time recovery, [5-12](#)
- protected databases
 - to specific time, [5-7](#)
- tablespaces
 - in a PDB, [5-13](#)
 - using Oracle Advised recovery, [5-1](#)
 - using user directed recovery, [5-2](#)

recovering protected database

- tablespaces, [5-9](#)

recovering protected databases, [5-1](#)

- control file, [5-9](#)
- corrupt blocks, [5-14](#)
- data files, [5-10](#)
- in Oracle RAC, [5-14](#)
- prerequisites, [5-5](#)

Recovery Appliance

- benefits for protected databases, [1-4](#)
- modified RMAN commands, [A-1](#)
- overview, [1-1](#)
- registering protected databases, [3-17](#)

Recovery Appliance backup module

- about, [3-3](#)
- configuration parameters, [3-4](#)
- installing, [3-14](#)

Recovery Appliance users, [1-6](#)

recovery settings
protected databases overview, [3-7](#)
using Enterprise Manager, [3-21](#)
using RMAN, [3-28](#)

restoring
protected databases
examples, [5-4](#)
prerequisites, [5-5](#)

restoring protected databases, [5-1](#)

RMAN commands
modified in Recovery Appliance, [A-1](#)

S

SBT library
for transferring backups, [3-3](#)

sending to Recovery Appliance
protected database backups, [1-7](#)

standby databases
from Recovery Appliance, [5-18](#)

standby databases (*continued*)

T

tasks
for protected databases administrator, [1-14](#)

test recovery
running
using RMAN, [3-31](#)

transferring backups
using SBT library, [3-3](#)

U

user directed recovery
about, [5-2](#)

users
protected databases administrator, [1-6](#)
Recovery Appliance, [1-6](#)