Acronis

acronis.com

Cyber Protect service

Protecting Oracle Database

White Paper

REVISION: 1/26/2024

Table of contents

Copyright statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Introduction

More and more often, Oracle databases are used to run and support the most critical applications. An enterprise database may be complex and difficult to administrate and protect, while having little tolerance for downtime.

To address backup requirements for these databases, Oracle offers an integrated command-line backup solution named Recovery Manager (or RMAN). RMAN contains all backup and recovery functionality that is necessary for an Oracle environment of any complexity.

At the same time, RMAN lacks a GUI, has a steep learning curve, and requires an experienced database administrator to configure and use correctly. It may be a challenge for smaller companies that just have started using Oracle Database. RMAN is also limited in terms of storage that is supported out of the box (a local folder or SMB share only), does not support complex storage policies, and does not provide a simple disaster recovery scenario for the case when an entire Oracle server fails.

The Cyber Protection service offers a solution for protecting Oracle Database data. This solution combines the full power of the Cyber Protection service and RMAN in a package that is simple to use even for those who are not versed in Oracle Database intricacies.

Backup and recovery methods

Backup methods

The Cyber Protection service provides two methods of protecting Oracle data. Both methods allow you to utilize the backup management functionality: centralized management, replication, retention, email notifications, and more.

Server backup

Back up an entire Oracle server, using application-aware backup to ensure the application-consistent state of the Oracle database.

Benefits:

- Reduced RTO in case of the entire server failure.
- Backup is fully configured in the graphical user interface. Oracle Recovery Manager (RMAN) knowledge is not necessary.
- Having a backup of the entire server, you can easily create a virtual machine that needs only seconds to spin up and replace the original server.

Limitations:

- The database must be stored on a regular file system supported by the backup software. Raw partitions and Oracle Automatic Storage Management (ASM) volumes are not supported.

Database backup

Back up an Oracle database by using Oracle Recovery Manager (RMAN) to a local folder, and then back up the resulting files to a different location, keeping only the latest RMAN backups in the local folder. The solution provides RMAN scripts that can be automatically run before the file backup. Thus, the entire procedure can be set up and executed within a single workflow without prior knowledge of RMAN scripting.

Benefits:

- Support for databases stored on raw partitions or Oracle Automatic Storage Management (ASM) volumes.

Limitations:

- Longer RTO in case of entire server failure.

Comparison

	Server backup	Database backup
RTO in case of entire	Less	More

server failure		
The capability to run a virtual Oracle server	Yes, ESX or Hyper-V	No
Support for raw partitions/ASM	No	Yes
Support for databases spread over several volumes	Yes	Yes
Ease of use	Backup is fully configured in the graphical user interface. Knowledge of RMAN is not necessary.	Necessity to configure separate protection plans for full backup and backup of archived log.

Common limitations

- Oracle Real Application Clusters (RAC) are not supported.
- Only single-instance database configurations are supported.
- It is not possible to back up individual pluggable databases (PDB). They are backed up as part of the container database (CDB).
- The database must be in the ARCHIVELOG mode (the **NOARCHIVELOG** flag is disabled).

  A database in the NOARCHIVELOG mode can be backed up only in the closed state, while the backup solution is aimed at backing up databases without a downtime. Trying to create a disk-level backup will return a VSS error if an online database is in this mode, and RMAN cannot be used either.

  To avoid this error, stop and close the database with a pre-data capture command and restart the database with a post-data capture command. You will be able to recover the entire server but recovering via Oracle Explorer will not be available.
- With the application-aware backup, the Oracle archive logs are not truncated.

Recovery methods

Server recovery

Recover the entire server to the point in time of backup creation. If you recover the server to bare metal, Oracle Database will be recovered among other data and will be in a consistent state.

Benefits:

- The quickest and easiest disaster recovery method.
- Allows physical-to-virtual migration (P2V) and other methods of replication or migrating your Oracle server.
- Oracle Recovery Manager (RMAN) knowledge is not necessary.

Recovery by using Oracle Explorer

Recover datafiles to a point of time by using the Oracle Explorer tool provided with the solution. The tool employs RMAN and combines a number of useful RMAN options in a convenient UI. By using the tool, you can recover from both application-aware backups and database backups.

Benefits:

- Allows granular, point-in-time recovery of your Oracle data directly from application-aware backups.
- Oracle Recovery Manager (RMAN) knowledge is not necessary.

Limitations:

- May require a two-step recovery process when used for database backups.

Recovery by using scripts

Recover a database to the point in time of the latest backup from the locally stored RMAN backups. The solution provides a RMAN script for this recovery. To recover to the point in time of a previous RMAN backup, first recover this RMAN backup from a file-level backup, and then use scripts to recover the database.

The same recovery operations can be performed with datafiles and the control file. The solution provides separate scripts for these recovery operations.

Also, the solution provides separate scripts for recovering to a custom point in time. This point in time can be specified by the exact date and time or by the System Change Number (SCN).

Benefits:

- It is possible to customize recovery for advanced scenarios.

Limitations:

- A customization requires RMAN knowledge.
- May require a two-step recovery operation.

Supported operating systems

Server backup

- Windows Server 2008R2 – Standard, Enterprise, Datacenter, and Web editions (x86, x64)
- Windows Server 2012R2 – Standard, Enterprise, Datacenter, and Web editions (x86, x64)
- Linux – any kernel and distribution supported by Agent for Linux (listed below)

Database backup

Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 and later – Standard and Enterprise editions (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Vista – all editions
- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation, and Web editions (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – all editions
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation, and Web editions
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – all editions
- Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions
- Windows Server 2012/2012 R2 – all editions
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise and LTSC (formerly LTSB) editions
- Windows Server 2016 – all installation options, except for Nano Server
- Windows Server 2019 – all installation options, except for Nano Server

Linux

Note
The following Linux distributions and kernel versions have been specifically tested. However, even if your Linux distribution or kernel version is not listed below, it may still work correctly in all required scenarios, due to the specifics of the Linux operating systems.

If you encounter issues while using Acronis Cyber Protection with your combination of Linux distribution and kernel version, contact the Support team for further investigation.

Linux with kernel from 2.6.9 to 5.19 and glibc 2.3.4 or later, including the following x86 and x86_64 distributions:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

Important
Configurations with Btrfs are not supported for SUSE Linux Enterprise Server 12 and SUSE Linux Enterprise Server 15.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*,9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3* – both Unbreakable Enterprise Kernel and Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

Before installing the product on a system that does not use RPM Package Manager, such as an Ubuntu system, you need to install this manager manually; for example, by running the following command (as the root user): `apt-get install rpm`

If your Linux distribution does not support the D-Bus mechanism (for example, Red Hat Enterprise Linux 6.x or CentOS 6.x) Acronis Cyber Protection will use the default location for storing secure keys because the operating system does not provide D-Bus compatible location.

* Starting from version 8.4, supported only with kernels from 4.18 to 5.19.

Supported Oracle Database versions

- Oracle Database version 11g, all editions
- Oracle Database version 12c, all editions
- Oracle Database version 19c, all editions
- Oracle Database version 21c, all editions

Only single-instance configurations are supported.

Prerequisites

Common prerequisites

- The Oracle backup functionality is not available in the Standard edition of the Cyber Protection service. You must be using a more powerful edition such as Advanced.

Prerequisites for application-aware backup of Windows machines

- Oracle VSS writer must be installed and working (this happens by default for supported Oracle versions).
- Other prerequisites are described in the "Protecting Microsoft applications" > "Prerequisites" section of the user documentation, under "Additional requirements for application-aware backups".

Installation

Backup software components

To protect Oracle data, you need the following software components:

- To protect a physical or virtual server running Oracle Database, install Agent for Oracle on this machine. Agent for Windows or Agent for Linux (depending on the server operating system) will be installed along with this agent.
- Oracle Explorer is designed for granular recovery of Oracle data. This component is part of Agent for Oracle.

To download the installation file, sign in to the Cyber Protection service and click the account icon in the top-right corner > Downloads. In Linux, Agent for Oracle shares the same installer with Agent for Linux (64-bit).

To install the agent, proceed as described in the "Installing the software" section of the user documentation.

Oracle RMAN integration scripts

The scripts are automatically installed with Agent for Oracle.

The scripts are installed to the following folder:

- In Windows: `%ProgramFiles%\Acronis\Oracle`.
- In Linux: `/usr/lib/Acronis/Oracle`.

Later in this document, this folder is referred to as `<scripts location folder>`.

List of the scripts

The following table lists the scripts provided with the solution.

Script name	For Windows or Linux?	Description
main.py	Windows, Linux	The main script that performs all operations related to Oracle backup and recovery. Not for independent use.
main.cfg	Windows, Linux	The configuration file contains the database access parameters and other parameters that are common for other scripts. This is the only file that you may need to edit. This file is located in the following folder: • In Windows: **%ProgramData%\Acronis\Oracle\Config** • In Linux: **/var/lib/Acronis/Oracle/Config**

backup_full_pre.bat	Windows	Calls the main script to perform a full database backup by RMAN.
backup_full_pre.sh	Linux	Calls the main script to perform an archived log backup by RMAN.
backup_incr_pre.bat	Windows	
backup_incr_pre.sh	Linux	Calls the main script to recover the entire database to the latest available state.
restore_disaster.bat	Windows	
restore_disaster.sh	Linux	Calls the main script to recover the datafiles to the latest available state (complete recovery).
restore_datafiles.bat	Windows	
restore_datafiles.sh	Linux	Calls the main script to recover the control file to the latest available state.
restore_controlfile.bat	Windows	
restore_controlfile.sh	Linux	Calls the main script to recover the database to a point in time in the past (incomplete recovery). Such point in time is specified by a date and time in the following format: yyyy-mm-dd:hh24:mi:ss.
restore_to-point-in-time.bat	Windows	
restore_to-point-in-time.sh	Linux	Calls the main script to recover the database to a point in time in the past (incomplete recovery). Such point in time is specified by a System Change Number.
restore_to-scn.bat	Windows	
restore_to-scn.sh	Linux	Calls the main script to show its latest log.
last_log.bat	Windows	
last_log.sh	Linux	RMAN scripts for various operations. Not for independent use.
***.rman**	Windows, Linux	
***.sql**	Windows, Linux	SQL*Plus scripts for various operations. Not for independent use.

Other	Windows, Linux	Auxiliary scripts. Not for independent use.

Configuration parameters

This section lists parameters that you can modify in the file **main.cfg**. These parameters influence only database backup. Server backup does not use these parameters.

- `BACKUP_DIR`: the local folder where RMAN backups will be stored.

  The disk where you want to store RMAN backups must have free space enough for two copies of the database.

  The default path is **C:\local_rman_backups** in Windows and **/tmp/local_rman_backups** in Linux.

  Note
  In Windows, use double backslash characters instead of single ones. For example, the default path is specified as **C:\\local_rman_backups**.

- `TARGET`: connection string for the database.

  The default value is `/`. With this value, the script will log on to Oracle by using the operating system authentication.

  Note
  Only operating system authentication is supported. In Windows, the script will use the account under which the agent service runs. In Linux, the script will use the `ORACLE_USER` variable value (see `ORACLE_USER` below). In both Windows and Linux, the account that you specify must have the SYSDBA system privilege in Oracle. To grant this privilege, add the user to the ORA_DBA group.

In Linux, you may need to additionally modify the following Oracle environment variables to reflect the actual Oracle Database settings:

- `ORACLE_BASE`: the root of the Oracle Database directory tree. The default value is `/u01/app/oracle`. To learn the actual value, run the `env | grep ORACLE_BASE` command under an account that has the SYSDBA system privilege in Oracle Database.
- `ORACLE_HOME`: the location of a specific Oracle Database installation. The default value looks like `/u01/app/oracle/product/12.1.0.2/db_1/`. To learn the actual value, run the `env | grep ORACLE_HOME` command under an account that has the SYSDBA system privilege in Oracle Database.
- `ORACLE_SID`: the system identifier of the database. The default value is `orcl`. To learn the actual value, run the `env | grep ORACLE_SID` command under an account that has the SYSDBA system privilege in Oracle Database.
- `ORACLE_USER`: the account that RMAN and SQL*Plus use to log on to Oracle when the `TARGET` parameter value is `/` (see the `TARGET` parameter above). The default value is `oracle`. The account that you specify here must have the SYSDBA system privilege in Oracle Database. Also, this account must be part of the **acronis** group. This group is automatically created during the

installation of Agent for Oracle and it is defined in `/etc/passwd` file. If the `ORACLE_USER` account is not a member of the **acronis** group, use the `groupadd` command to add it.

- `RMAN_PATH`: the directory where RMAN is located.

  The default value is `$ORACLE_HOME/bin`. To learn the actual value, run the `which rman` command under an account that has the SYSDBA system privilege in Oracle. For example, if the command output is `/u01/app/oracle/product/12.1.0.2/db_1/lib/rman`, set the `RMAN_PATH` value to `$ORACLE_HOME/lib`.

Backup

Backing up an entire server

When creating a protection plan for a server where Oracle Database is installed, follow the below guidelines:

- Select the entire machine. Otherwise, you will not be able to create application-aware backup.
- Click **Application backup** and enable the **Oracle Database** switch.
- In the backup options, do the following:
  - Ensure that the **Multi-volume snapshot** option is enabled.
  - [Only for Windows] Ensure that the **Volume Shadow Copy Service** option is enabled. Unless you have a reason to do otherwise, we recommend that you keep the default value **Automatically select snapshot provider**.

  These settings will guarantee that the database is correctly frozen and flushed during the snapshot creation. As a result, the backed-up application will be fully consistent.

For more information about how to back up, refer to the "Backup" section of the user documentation.

Backing up an Oracle database

Preparation

Select the local folder that will store RMAN backups. The disk allocated for storing RMAN backups must have free space enough for two copies of the database. Do not select the same disk as the one where the database is located.

The default path is **C:\local_rman_backups** in Windows and **/tmp/local_rman_backups** in Linux. To change this path, edit the `BACKUP_DIR` parameter value in the **main.cfg** file as described in "Configuration parameters".

If the folder does not exist, create it in advance. Ensure that the following users have the read permission for this folder:

1. The account under which the agent service runs.
2. The account under which Oracle instance service (`OracleService<Database ID>`) runs.
3. [Only in Linux] The root user.

If necessary, change other script configuration parameters.

Creating protection plans

To back up an Oracle database, create one or two protection plans. One of them is mandatory, it will first create a full RMAN backup, and then create a full backup of the resulting files to a different

location. The other one is optional, it will first create a RMAN backup of archived logs, and then create an incremental backup of the resulting files to the same location and with the same backup file name as the full backup. Use the second protection plan to back up archived logs more often than the database.

A full RMAN backup must be created before backups of archived logs. Otherwise, you will not be able to recover the database until the full backup is created. If, according to the schedule, the incremental backup will run first, run the full backup manually before that.

To create a protection plan for full backups

Follow the below guidelines:

- In **What to back up**, select **Files/folders**. Select the folder that will store the RMAN backups.
- In **Schedule** > **Backup scheme**, select **Always full** or **Custom**.
- Specify the backup schedule. If you have selected the **Custom** backup scheme, specify only the full backup schedule here.

  We recommend that you create full backups once a week.
- In the backup options, do the following:
  a. Click **Backup file name**, and then change the file name template. Do not use the `[Plan ID]` and `[Plan name]` variables.

     Memorize or write down the template you specified because you will need to set the same value in the second protection plan.
  b. Click **Pre/post commands**.
  c. Enable the **Execute a command before the backup** switch.
  d. Specify the following settings.

     [In Windows]
     - In **Command**, enter `<scripts location folder>\backup_full_pre.bat`.
     - In **Working directory**, enter `<scripts location folder>`.

     [In Linux]
     - In **Command**, enter `/<scripts location folder>/backup_full_pre.sh`.
     - In **Working directory**, enter `/<scripts location folder>/`.

For more information about how to back up, refer to the "Backup" section of the user documentation.

To create a protection plan for archived log backups

Follow the below guidelines:

- In **What to back up**, select **Files/folders**. Select the folder that will store the RMAN backups.
- In **Where to back up**, select the same backup location as for full backups.
- In **Schedule** > **Backup scheme**, select **Custom**.
- Change the backup schedule for full backups. Because full backups are not needed in this case, the schedule must guarantee that full backups will never be done.

We recommend that you change the schedule to **On Windows Event Log event** and leave other parameters as they are.

- Specify the backup schedule for incremental backups.

  We recommend that you create incremental backups on each day of week except for the day you selected for full backups.
- In the backup options, do the following:
  a. Click **Backup file name**, and then specify the same file name template as for full backups.
  b. Click **Pre/post commands**.
  c. Enable the **Execute a command before the backup** switch.
  d. Specify the following settings.

     [In Windows]

     - In **Command**, enter `<scripts location folder>\backup_incr_pre.bat`.
     - In **Working directory**, enter `<scripts location folder>`.

     [In Linux]

     - In **Command**, enter `/<scripts location folder>/backup_incr_pre.sh`.
     - In **Working directory**, enter `/<scripts location folder>/`.

For more information about how to back up, refer to the "Backup" section of the user documentation.

Recovery

Recovering an entire server

To recover a server

1. Proceed as described in the "Recovering a machine" section of the user documentation.
2. If archived logs are available for the period after the backup from which you have recovered (for example, these logs can be stored on a separate undamaged volume or backed up separately), recover them to the latest state by using RMAN, after recovering the server.

Recovering Oracle databases by using Oracle Explorer

Oracle Explorer

Oracle Explorer can interact only with Agent for Oracle that is installed on the same server.

- In Windows, Oracle Explorer is located in the folder `%ProgramFiles%\BackupClient\OracleExplorer`. To run the tool, you can also use the shortcut created on the desktop after Agent for Oracle installation.
- In Linux, run `/usr/lib/Acronis/OracleExplorer/oracle_explorer.sh`.

Oracle Explorer recovers Oracle data in two steps. First, it restores the required Oracle files (datafiles, server parameter file, control file, and archived logs) from the application-aware backup or from the database backup. You can skip this step if these files are intact. Then, the tool calls an RMAN recovery command that applies redo logs and performs other operations to make the database consistent up to the desired state.

To recover Oracle data

1. Run Oracle Explorer.
2. Select the backup location. If prompted, specify the user name and password for the location.
3. Select the backup. If prompted, specify the password for the encrypted backup.
4. Select the recovery point and the database to be recovered.
5. Select the Oracle files to be restored from the backup. Skip this step if the files are intact.

   We recommend that you select tablespaces and archived logs. If you restore a control file, you will have to make a new incarnation of the database. If you restore a server parameter file, you will lose changes in the instance parameters that you have made after the backup.

   If you select to restore archive logs, select the specific logs to be restored.

   Oracle files will always be restored to the original location and will be overwritten.
6. [Optional] Select recovery options:
   - The point in time to which the database will be recovered.

     This can be either recovery to the latest available state (complete recovery) or recovery to a point in time in the past (incomplete recovery). Such point in time is specified either by the

date and time from the interval between the recovery point selected earlier and the current moment, or by a System Change Number.

- Whether to open the database after the recovery.

  Leave the database closed if you plan to perform manual recovery operations by using RMAN.
- Whether to reset logs.

  This option should be used with caution because resetting redo logs creates a new database incarnation, meaning that you might be limited in rolling back the database to the previous incarnation.
- The account under which the recovery will be performed.
- You can also restore the database files without running an RMAN recovery operation, if you plan to perform recovery later.

Later in this section, a number of basic recovery scenarios is described, with the recommended options you should select in each case.

Recovery to the latest state

Use this procedure if datafiles are lost or corrupted, or in case of another type of database failure. It is assumed that the control file and the server parameter file are intact.

You can also use this scenario to bring the database to the latest state after recovering the entire server from an older disk-level backup.

For this scenario, select **Tablespaces** and **Archive logs** as needed. In recovery options: select **Recover up to the latest available state**, keep the **Open database after recovery** check box selected, and keep the **Reset logs** check box cleared.

Recovery to an earlier point in time

Use this procedure when the database is operational but you want to roll it back to a previous state.

For this scenario, select **Tablespaces** and **Archive logs** as needed. In recovery options, select either **Recover to the point in time** or **Recover to System Change Number (SCN)**; specify the date and time or SCN to which the database should be recovered; keep the **Open database after recovery** check box selected; and select the **Reset logs** check box.

Recovering Oracle data by using scripts

Recovering a RMAN backup from a file-level backup

Perform this operation in the following cases:

- The latest RMAN backup has been lost or corrupted.
- You need to recover the database to a previous point in time.

To recover a RMAN backup from a file-level backup

Proceed as described in the "Recovering files by using the web interface" section of the user documentation.

Recovering Oracle data from a RMAN backup

Oracle database disaster recovery

Use this method if you need to recover the entire server or the disk where Oracle Database is installed but you do not have a disk-level backup of it. This method makes the database consistent up to the state of the RMAN backup.

To recover a database in case of disaster

1. Reinstall the operating system or take another server that is up and running. If the operating system is intact, skip this step.
2. Reinstall Oracle Database.
3. Create a new database with the same name and in the same location as the one that you need to recover.
4. Recover the required RMAN backup from the file-level backup, as described earlier in this section.
   If you recover from the latest RMAN backup and it is intact, skip this step.
5. [In Windows] At the command prompt, type `cd <scripts location folder>`.
   [In Linux] In the terminal, type `cd /<scripts location folder>`.
6. Run **restore_disaster.bat** (in Windows) or **restore_disaster.sh** (in Linux).

Complete database recovery

Use this method if a database has failed or has been corrupted after the latest backup. This method presumes that the control file and the server parameter file are intact.

To recover a database

1. Recover the required RMAN backup from the file-level backup, as described earlier in this section.
   If you recover from the latest RMAN backup and it is intact, skip this step.
2. [In Windows] At the command prompt, type `cd <scripts location folder>`.
   [In Linux] In the terminal, type `cd /<scripts location folder>`.
3. Run **restore_datafiles.bat** (in Windows) or **restore_datafiles.sh** (in Linux).

Control file recovery

Use this method if a control file has been lost or corrupted after the latest backup.

To recover a control file

1. Recover the required RMAN backup from the file-level backup, as described earlier in this section.

If you recover from the latest RMAN backup and it is intact, skip this step.

2. [In Windows] At the command prompt, type `cd <scripts location folder>`.
   [In Linux] In the terminal, type `cd /<scripts location folder>`.
3. Run **restore_controlfile.bat** (in Windows) or **restore_controlfile.sh** (in Linux).
4. Run a full backup.
   Recovering a control file resets logs, therefore the next backup must be full.

Recovery to a custom point in time (incomplete recovery)

Use this method to recover the database to a custom point in time. This point in time can be specified in the following ways:

- By the exact date and time. The available range is between the moment of the RMAN backup and the current moment.
- By the System Change Number (SCN). The available range is between the value written in file **scn.in** and the latest value available in archived logs.
  File **scn.in** is stored in the folder where RMAN backups are located. Normally, the SCN in this file reflects the point in time of the latest backup.
  To learn the latest SCN value from archived logs:
  a. At the command prompt (in Windows) or in the terminal (in Linux), type `sqlplus / as sysdba` to log in to Oracle.
  b. Type `select max(next_change#)-1 from v$archived_log;`

To recover to a custom point in time

1. Recover the required RMAN backup from the file-level backup, as described earlier in this section. This will overwrite file **scn.in**.
   If you recover from the latest RMAN backup and it is intact, skip this step.
2. [In Windows] At the command prompt, type `cd <scripts location folder>`.
   [In Linux] In the terminal, type `cd /<scripts location folder>`.
3. Do any of the following:
   - To recover to a certain point in time, run `restore_to-point-in-time.bat <point in time>` (in Windows) or `restore_to-point-in-time.sh<point in time>` (in Linux).
     Here, `<point in time>` should be specified in the following format: `yyyy-mm-dd:hh24:mi:ss`.
   - To recover to a certain SCN, run `restore_to-scn.bat <SCN>` (in Windows) or `restore_to-scn.sh <SCN>` (in Linux).

   If the date and time (the SCN) is not specified, the recovery will be performed to the moment of time determined by the SCN specified in the file **scn.in**.
4. Run a full backup.
   Incomplete recovery resets logs, therefore the next backup must be full.

Index

S

W