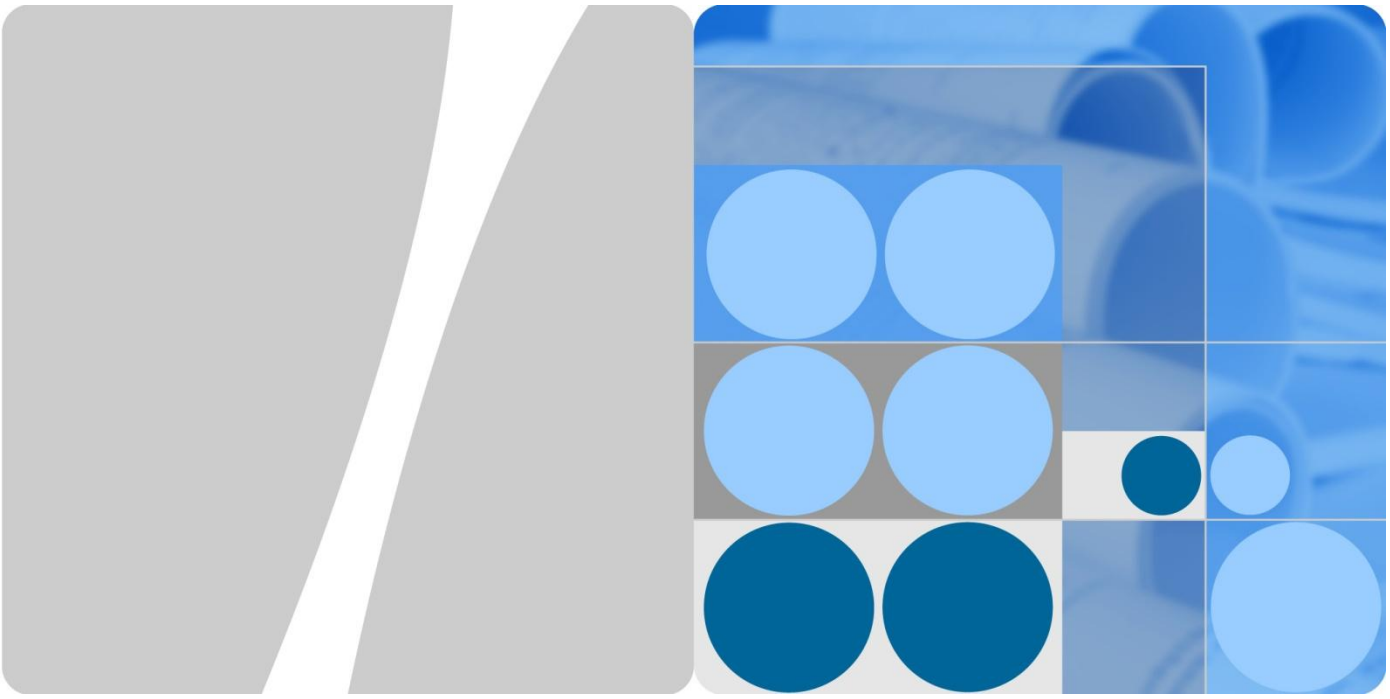


FusionCube V100R002C02 Database Infrastructure Backup Solution

Issue 2.02

Date 2014-02-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

Contents

1 Backup Overview 1
1.1 Database Backup Overview 1
1.1.1 Importance of Backups 1
1.1.2 Backup System Design Principle 1
1.1.3 Backup System Positioning 2
1.1.4 Backup System Components 3
1.2 Typical Backup Requirements 3
1.3 FusionCube Database Backup Solution Overview 4
2 FusionCube Database Backup Solution Description 5
2.1 FusionCube Database Backup Solution 5
2.1.1 Overview 5
2.1.2 Application Scenario 5
2.1.3 Networking 5
2.2 Backup Policy 6
2.3 Backup Check 7
2.3.1 Checking Whether User Oracle Is Granted the Rights to Execute crontab Commands 7
2.3.2 Checking Whether the Database Is in ARCHIVELOG Mode 7
2.3.3 Checking the Database Backup Directory and Space 7
2.3.4 Modifying the Data Backup Retention Policy 8
2.3.5 Enabling Automatic Backup for the Database Control File 8
2.4 Data Backup Process 9
2.4.1 Creating Directories for Storing Backup Scripts 9
2.4.2 Creating Database Full Backup Scripts 9
2.4.3 Creating Archive Log Backup Scripts 11
2.4.4 Configuring a Scheduled Task for Archive Log Backup 11
2.5 Database Restoration and Recovery 12
2.5.1 Searching for Control Files 12
2.5.2 Restoring and Recovering a Database Using Full Backup Files 12
2.5.3 Restoring and Recovering a Database Using Archive Log Backups 14
2.5.4 Verifying Database Restoration and Recovery 15
A Acronyms and Abbreviations 17

1 Backup Overview

1.1 Database Backup Overview

Databases support IT applications of modern enterprises and are the core of the enterprise IT infrastructure. Valuable data in the whole IT system is stored in the databases. Once data in an enterprise database is lost, the enterprise will suffer huge economic losses and high customer churn rate. Therefore, the key for an enterprise to succeed and win competitive edges in the fiercely competitive economic environment is to preserve data integrity. To achieve this goal, Huawei provides a database backup solution to ensure that key data will not lose in the event of a disaster and that system services can be restored as soon as possible.

1.1.1 Importance of Backups

Any system may be faulty. Therefore, it is important for enterprises to ensure that data in their core database will not lose even if the database is faulty.

Although the IT technology brings great conveniences to people's daily life, a lot of factors, such as misoperations, software bugs, hardware damages, viruses, attacks, and natural disasters, may cause data in computers to lose, which incurs tremendous losses for enterprises. To keep core data in the service system secure, we must effectively protect the data and support quick data restoration.

All data backups are used for data restoration in the event of a disaster. In addition to the backup mode and speed, data restorability is also another factor that users should take into consideration when evaluating an automatic backup system. Restorability is determined by restoration speed and operation simplicity.

1.1.2 Backup System Design Principle

Data backups ensure that data can be recovered in the event of a system failure or disaster, thereby relieving users and operators' worries. The backup solutions vary depending on different application scenarios. Typically, a well-defined backup system must comply with the following principles:

- Stability

  A backup system is used to provide data protection for the IT system. Therefore, the backup system must be stable and reliable. In addition to the complete compatibility with the OS, the backup system must be capable of recovering data in a quick and effective manner when a fault occurs.
- Comprehensiveness

In a complicated computer network environment, there may be various OSs, such as Linux and Windows, and different applications, such as the Enterprise resource planning (ERP), database, and Email system. Therefore, the backup software must support different OSs, databases, and typical applications.

- Automation

  Many systems have requirements on the backup start time and backup window. Backup operations are recommended to be performed at midnight when the service load is light, which, however, increases the workload of system administrators. Therefore, the backup system must provide automatic backup and automatic management for backup media devices. During the backup, the backup system must record logs and generate alarms for exceptions and faults.

- High performance

  To ensure optimal system performance, backup operations must be performed at non-working hours. However, with the development of services, massive data is generated and the data is updated at a higher speed. As a result, the non-working hours are insufficient to complete the backup. If the backup is performed during busy hours, the system performance is adversely affected. Therefore, the backup speed must be improved for the backup system to complete the backup within the specified backup window to ensure high system performance.

- Service system validity

  Backup may have great impact on service system performance. Therefore, proper technical measures must be taken to minimize the impact on service systems, such as server system, database system, and network system, and to ensure the integrity and validity of the recovered data.

- Ease of use

  Data backup is applied to different industries where the backup operators may not be professionals. A clear graphical user interface (GUI) featuring ease of use can help operators to quickly understand the backup operations and to perform and complete the backup with ease.

- Real time

  Some key tasks must run for 24 hours without service interruption, and some files may be opened during the backup. Therefore, measures must be taken to query the file size in real time and trace operations performed on the files during the backup so that all files in the system are correctly backed up in a real-time manner.

1.1.3 Backup System Positioning

Data backup aims to preserve data status of a system at one or multiple specific moments. The backed-up data is used to restore the original data after a data loss to enhance data security. The difference between backup and disaster recovery (DR) is that backup is used to ensure data security while DR is used to ensure service applications security. This means backup provides protection for data, while DR provides protection for service applications. Backup involves copying data using backup software over the storage medium, such as the tape library, compact disc, network-attached storage (NAS) device, and cloud storage device. DR involves connecting two sites using high availability (HA) solutions to achieve quick system recovery.

Although the backup and DR have different objectives, they do have some similarities. Both backup and DR involve data protection. In backup solutions, low-performance and low-cost storage devices are used, such as SATA hard disks and physical tape libraries. In DR solutions, high-performance and high-cost storage devices, such as SA hard disks, are used because DR has high requirements for data availability. Backup is an essential part in a complete DR

solution because it is the basis of storage functions. Moreover, backup is an effective supplement to the DR solution. In a DR solution, data must be always available, which may cause the storage system to break down. However, backup can be used to recover data from an earlier time even after a data loss event.

After all the factors are taken into consideration, the following two schemes are usually used to build a DR and backup system.

- Scheme 1: Only a backup system is built. Data is backed up using this system for future data recovery. The backup system can be built at a third place to store data in a remote server, which also provides certain DR functions.
- Scheme 2: A DR system and a backup system are built. Service continuity and data security are ensured using the two systems. If this scheme is used, only data in the DR system needs to be backed up.

1.1.4 Backup System Components

- Backup software

  Superior backup software can speed up data backup, implement automatic backup, and provide the DR function, which is of great importance to a secure and effective data backup.
- Backup network

  The backup network can be storage area network (SAN), local area network (LAN), metropolitan area network (MAN), wide area network (WAN), or a hybrid of SAN and LAN, MAN, or WAN. The backup network is the channel for data transmission and determines the backup efficiency.
- Backup medium

  The backup medium carries data. Therefore, the quality of the backup medium is important to data security.
- Backup management

  In addition to quality software and hardware, an optimal backup and recovery system must have reliable backup policies and management plans. For a complicated IT system, customized backup policies must be formulated based on application and service types. Generally speaking, various factors must be taken into consideration when you configure backup policies for the system.

1.2 Typical Backup Requirements

Backup mode

- Manual backup

  Each backup operation is manually triggered by users.
- Automatic backup

  The system automatically backs up data at the specified time after backup policies are configured.

Backup Type

- Full backup

It is a complete backup of everything you want to back up. The advantage is that data restoration is fast since you only need one set of backup set. The disadvantage is that large amount of data needs to be backed up, and the backup process is slow.

- Incremental differential backup

  Only new data in the files that have been changed since last full backup is backed up. The advantage is that it is faster to create a differential backup than a full backup because less data is backed up. The disadvantage is that the last full backup and the last differential backup are required to complete the data restoration.

- Cumulative incremental backup

  Only the data that have changed since the last backup is backed up. The advantage is that the backup process is fastest among the three. The disadvantage is that data restoration is the slowest because the last full backup and all the incremental backups are required to fully restore all the data.

Storage medium

- Disk backup: The storage media include internal storage devices, cloud storage, and external storage devices, such as network-attached storage (NAS), SAN devices, and disk arrays.
- Tape backup: The storage media include physical and virtual tape libraries.

Data backup storage location

- Local backup

  Data is backed up to local backup storage devices.

- Remote backup

  Data is backed up to both the local and the remote backup storage devices. When a disaster happens at the production site and data in both the system and the local backup storage device may be lost, data backups stored in the remote backup storage device can be used to recover data and avoid data loss.

1.3 FusionCube Database Backup Solution Overview

The FusionCube solution provides a backup solution based on the Oracle Recovery Manager (RMAN) for the highly available Oracle databases. RMAN supports various backup modes and types, such as hot backup, cold backup, full backup, and incremental backup. Users can choose the backup mode and type based on their service requirements.

2 FusionCube Database Backup Solution Description

2.1 FusionCube Database Backup Solution

2.1.1 Overview

Features:

Ease of use: The NAS or SAN devices can be attached to a directory of the Real Application Clusters (RAC) node. The database data can be directly backed up to a backup storage device by running the RMAN script or backed up to the local storage space of the RAC node and then store to a large-capacity storage devices.

Flexible backup policy configuration: The solution supports periodical full and incremental backup. Users can configure the backup interval, backup window, data backup retention period, and obsolete data backup deletion policies. Users can also allocate backup channels for data backup.

Restoration: Users can select objects to be restored based on service requirements and select proper restoration channels based on the volume of data to be restored.

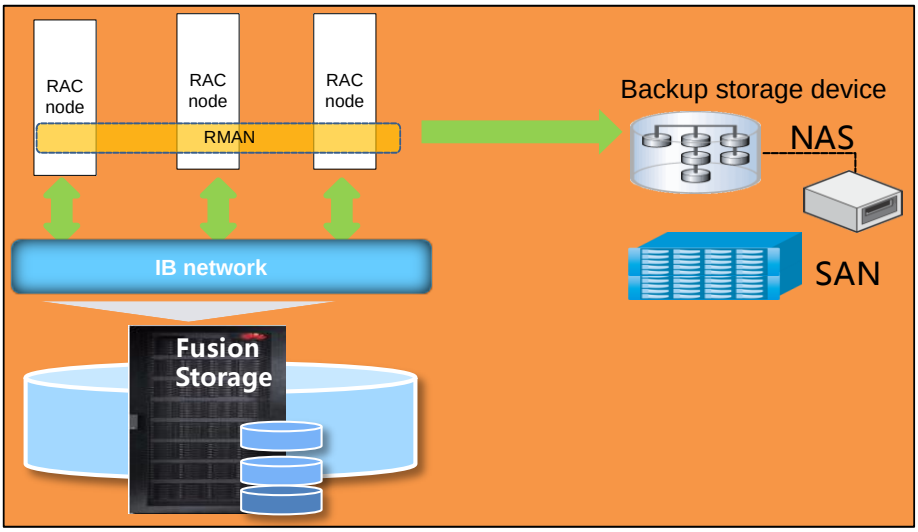
2.1.2 Application Scenario

This solution applies to the single-node databases with archive function enabled or the Oracle RAC databases.

2.1.3 Networking

Figure 2-1 shows the RMAN-based backup solution for Oracle databases.

Figure 2-1 RMAN-based backup solution for Oracle databases



New Software and Hardware Devices

Destination database (optional): When the RMAN is used to back database data, destination database information needs to be stored. If no destination database is configured, the RMAN will store the information to the control files of destination database.

Backup storage device: Data can be backed up to the Network File System (NFS) or Common Internet File System (CIFS) shared file systems. Huawei OceanStor N8500 clustered NAS system is recommended. The required size of backup storage space varies depending on the amount of data to be backed up and the backup policies.

2.2 Backup Policy

- Full backup and archive log mode are used.
- A full backup is performed for the database every day. The time for performing the full backup varies depending on actual requirements, usually at midnight or the early morning.
- Archive logs are backed up every 3 hours. The logs can be deleted only after the database is backed up.
- Store all data of a complete backup.

2.3 Backup Check

2.3.1 Checking Whether User Oracle Is Granted the Rights to Execute crontab Commands

Log in to the database server as user **oracle** and run the following command:

$crontab –l

If no error message is displayed, user oracle has been granted the rights to execute crontab commands.

If an error message is displayed, log in to the database as user **root** and grant user **oracle** the rights to execute crontab commands. The method to grant rights to user **oracle** varies depending on the operating systems (OSs) of the databases. For details, see the related guide.

2.3.2 Checking Whether the Database Is in ARCHIVELOG Mode

Ensure that the database is in ARCHIVELOG mode before backup. Otherwise, the database fails to be backed up.

Step 1 Log in to the database server as user **oracle**.

Step 2 Run the following command to log in to the database:

sqlplus "/as sysdba"

Step 3 Run the following command to check the archive log mode of the database:

SQL> ***select DBID,NAME,LOG_MODE from v$database;***

In the command output, if the value of **LOG_MODE** is **ARCHIVELOG**, the archive log mode is **ARCHIVELOG**. If the value of **LOG_MODE** is **NOARCHIVELOG**, change the value to **ARCHIVELOG**.

----End

2.3.3 Checking the Database Backup Directory and Space

Although RMAN and Oracle Secure Backup can be used to directly back up data in the Oracle database to tapes, the charges are high. This document describes how to back up data to disks. After the data is backed up to disks, a tape drive can be used to migrate the data backups from the disks to tapes. For details about how to migrate data to tapes, see the operation guide of tape drives.

Data backups are centrally stored in the file directory mounted to the logical volume. Therefore, ensure that the required file system has enough available space.

Step 1 Log in to the database server as user **root**.

Step 2 Run the following command to check whether the required file system has been mounted to the specified directory:

mount

Step 3 Run the following command to check the available space of the specified directory:

df –k

----End

2.3.4 Modifying the Data Backup Retention Policy

The recovery window (the maximum number of days into the past for which you can recover) depends on customer requirements. In the following operation, the recovery window is changed to one day.

Step 1 Log in to the database server as user **oracle**.

Step 2 Run the following command to log in to the RMAN:

% rman target / nocatalog

Step 3 Change the recovery window to one day on the RMAN.

Run the following command to check the default configuration of the RMAN:

RMAN> show all;

If **CONFIGURE RETENTION POLICY TO REDUNDANCY 1** is displayed in the command output, the recovery window is one day. If not, run the following command to change the recovery window to one day:

RMAN> CONFIGURE RETENTION POLICY TO REDUNDANCY 1;

Step 4 Run the following command to check whether the recovery window is successfully changed:

RMAN> show all;

----End

2.3.5 Enabling Automatic Backup for the Database Control File

The full backup is performed every day. To prevent key information loss, the database control file must be backed up in a timely manner. Therefore, the automatic backup function for the database control file must be enabled.

Step 1 Log in to the database server as user **oracle**.

Step 2 Run the following command to log in to the RMAN:

% rman target / nocatalog

Step 3 Enable automatic backup for the control file of the Oracle database.

Run the following command to check the default configuration of the RMAN:

RMAN> show all;

If **CONFIGURE CONTROLFILE AUTOBACKUP OFF** is displayed in the command output, the automatic backup function is disabled. Run the following commands to enable the function:

RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;

RMAN> CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/backup/data/controlfile_%F.cntl';

----End

2.4 Data Backup Process

Back up the database after all the preparations have been made. You are advised to back up the Oracle RAC database in dual-channel mode.

The operations in this chapter must be performed for all nodes.

2.4.1 Creating Directories for Storing Backup Scripts

Step 1 Log in to the database server as user **root**.

Run the following commands to create required directories for storing backup scripts:

$mkdir /backup/bin /backup/log /backup/data /backup/arch

- The **/backup/bin** directory stores the backup script program.
- The **/backup/log** directory stores backup logs.
- The **/backup/data** directory stores all data backups of the database.
- The **/backup/arch** directory stores data backups of the archived logs.
- The **/backup** directory stores the backed-up **pfile** file generated before the database starts. The **pfile** file must be backed up each time you want to restart the database.

Step 2 Run the following command to change the permissions for the **/backup** directory:

$chown -R oracle:dba /backup

----End

2.4.2 Creating Database Full Backup Scripts

Scheduled tasks are configured for the database OS to back up Oracle databases. The OS invokes the required scripts to complete the backup.

Step 1 Create a command line script for the database full backup.

Create the **backup_cldb.cmd** file in the **/backup/bin** directory. The file contains the following information:

```
run {
# Hot database level 0 whole backup

allocate channel t1 type disk connect 'sys/sys@ora11g1';
allocate channel t2 type disk connect 'sys/sys@ora11g2';
#allocate channel t1 type disk;
backup
  incremental level 0
 # skip inaccessible
  #filesperset 6
  # recommended format
 format '/backup/data/db_%s_%p_%T_%d'
```

```
 #AS COMPRESSED backupset
(database);
delete obsolete;
  sql 'alter system archive log current';
  # backup all archive logs
  backup
  # skip inaccessible
   #filesperset 10
  format '/backup/arch/arclogback_%s_%p_%t_%d'
#AS COMPRESSED backupset
   (archivelog all
delete input);
delete obsolete;
  release CHANNEL t1 ;
  release CHANNEL t2 ;
}
```

NOTE

format '/backup/data/db_%s_%p_%T_%d ' indicates the directory containing data to be backed up and the name of the files to be backed up. The directory varies depending on the actual condition.

%s specifies the backup set number.

%p specifies the piece number within the backup set. This value starts at 1 for each backup set and is incremented by 1 as each backup piece is created.

%t specifies the backup set time stamp.

%d specifies the database name.

The **delete obsolete** command can be used to delete all obsolete backups defined by the currently configured retention policy.

@ora11g1 and **@ora11g2** are the service names of **$ORACLE_HOME /network/admin/tnsnames.ora**.

NOTE

When backing up the whole database, you are advised to back up it in dual-channel mode. The Oracle Database 11g supports single-channel mode. However, dual-channel mode is used for non-RAC scenarios, such as the cold backup of databases working in active/standby mode. The following is the script for backing up non-RAC databases in single-channel mode:

```
run {
# Hot database level 0 whole backup
allocate channel t1 type disk;
backup
  incremental level 0
  skip inaccessible
  # filesperset 6
  # recommended format
 format '/backup/data/back_%s_%p_%T_%d'
 #AS COMPRESSED backupset
database plus archivelog
format '/backup/arch/arclogback_%s_%p_%t_%d'
delete input;
delete obsolete;
}
```

Step 2 Create an execution script for a database full backup.

Create the **backup_db.sh** file in the **/backup/bin** directory. The **backup_db.sh** file is the execution script for database full backup and contains the following information:

```
rman target / nocatalog cmdfile=/backup/bin/backup_cldb.cmd
1>>/backup/log/backup_db.log 2>&1
```

For cold backup of databases working in active/standby mode, automatic backup must be configured so that the databases are backed up once an active/standby switchover occurs.

----End

2.4.3 Creating Archive Log Backup Scripts

Scheduled tasks are configured for the database OS to back up Oracle databases. The OS invokes the required scripts to complete the backup.

Step 1 Create a command line script for the database archive log backup.

Create the **arch_back.cmd** file in the **/backup/bin** directory. The file contains the following information if the database to be backed up is the Oracle 11g RAC database:

```
run {

allocate channel t1 type disk;
  # sql 'alter system archive log current';
  # backup all archive logs
  backup
    skip inaccessible
   #filesperset 10
  format '/backup/arch/arclogback_%s_%p_%t_%d'
#AS COMPRESSED backupset
   (archivelog all
delete input);
delete obsolete;
  release CHANNEL t1 ;
}
```

Step 2 Create an execution script for the database archive log backup.

Create the **arch_back.sh** file in the **/backup/bin** directory. The **arch_back.sh** file is the execution script for database archive log backup and contains the following information:

```
rman target / nocatalog cmdfile=/backup/bin/arch_back.cmd
1>>/backup/log/backup_arch.log 2>&1
```

----End

2.4.4 Configuring a Scheduled Task for Archive Log Backup

Step 1 Run the following command as user **root**.

$chmod +x /backup/bin/ *

Step 2 Log in to the database server as user **root** again and run the following command to open a file:

$crontab -e

Step 3 Add the following information to the opened file:

```
#2:00 am erveryday
0 2 * * * su - oracle -c /backup/bin/backup_db.sh
#ervery 3 hours
0 0,3,6,9,12,15,18,21 * * * su - oracle -c /backup/bin/arch_back.sh
```

NOTE

The arch_back script must be added for both the active and standby database nodes at different time periods. However, the backup_db script only needs to be added for one node.

----End

2.5 Database Restoration and Recovery

The restoration and recovery functions provided by the RMAN have some differences. Restoration involves copying backup files from secondary storage (backup media) to disk. Recovery is the process of applying redo logs to the database to roll it forward. To correctly understand these two functions helps users to recover the database. Generally, a database is first restored and then recovered.

2.5.1 Searching for Control Files

Control file backup is used to back up a database. Therefore, the control files used to restore the database must be located before database restoration and recovery.

Step 1 Log in to the system as user **oracle**.

Step 2 Run the following command to log in to the RMAN:

% rman target / nocatalog

Step 3 Run the following command to search for the control file:

RMAN> ***list backup of controlfile;***

If the piece name of the backup control file and the date cannot be found out by running the **RMAN> list backup of controlfile;** command, you must restart the database. If the database fails to start, view information listed in the **backup.log** file in the **/backup/log** directory.

----End

2.5.2 Restoring and Recovering a Database Using Full Backup Files

Step 1 Run the following commands to stop the target database:

$sqlplus "/as sysdba"

SQL> shutdown immediate;

Step 2 Run the following command to start the database in nomount mode:

SQL> startup nomount;

Step 3 Run the following command to log in to the RMAN:

rman target / nocatalog

Step 4 Run the following command to restore the control file:

RMAN> restore controlfile from 'controlfile';

The control file must be the one generated at the time point to which the database is to be restored. ***'controlfile'*** indicates the directory containing the control file. For details about how to locate the control file, see section 2.1.1.

Step 5 Run the following command to mount the database:

RMAN> alter database mount;

Step 6 Execute the following scripts to recover the database to a specific time point:

The script for non-RAC databases:

```
Oracle 11g non-rac
RMAN> run
{
#set until time '07/26/2013 14:27:27';
restore database;
recover database;
}
Set the time based on actual requirements.
```

The script for RAC databases:

```
Oracle 11g rac
RMAN> run
{
#set until time '07/26/2013 14:27:27';
allocate channel t1 type disk connect 'sys/sys@ora11g1';
allocate channel t2 type disk connect 'sys/sys@ora11g2';
restore database;
recover database;
release CHANNEL t1 ;
release CHANNEL t2 ;
}
```

NOTE

@ora11g1 and **@ora11g2** are the service names of **$ORACLE_HOME /network/admin/tnsnames.ora**.

Step 7 Run the following command to open the database:

RMAN> alter database open resetlogs;

Step 8 Start databases on other nodes.

If the target database is an Oracle RAC database, perform this step. Otherwise, skip this step.

NOTE

Perform a full backup for the database after the database is recovered.

----End

2.5.3 Restoring and Recovering a Database Using Archive Log Backups

Step 1 Run the following commands to stop the target database:

$sqlplus "/as sysdba"

SQL> shutdown immediate;

NOTE
If the target database is the Oracle RAC database, stop databases on all nodes. However, the restoration and recovery only need to be performed for one node.

Step 2 Run the following command to start the database in nomount mode:

SQL> startup nomount;

Step 3 Run the following command to log in to the RMAN:

rman target / nocatalog

Step 4 Run the following command to restore the control file:

RMAN> restore controlfile from 'controlfile';

The control file must be the one generated at the time point to which the database is to be restored. ***'controlfile'*** indicates the directory containing the control file.

NOTE
The control file is not backed up during archive log backup. Therefore, the control file used is the one backed up in the previous full backup.

Step 5 Run the following command to mount the database:

RMAN> alter database mount;

Step 6 Run the following command to restore the archive logs.

RMAN> restore archivelog all;

Step 7 Run the following script to restore and recover the database:

```
RMAN> RUN
{
SET UNTIL TIME '07/25/2013 13:20:00';
RESTORE DATABASE;
RECOVER DATABASE;
}
```

NOTE
Time in the command indicates the time point to which the database is restored and can be changed based on actual requirements.

Step 8 Run the following command to open the database:

RMAN> alter database open resetlogs;

Step 9 Start databases on other nodes.

Restoration and recovery operations only need to be performed for one node. Before performing restoration and recovery operations for a node, stop other nodes. After the node is recovered, start the nodes.

NOTE
Perform a full backup for the database after the database is recovered.

----End

2.5.4 Verifying Database Restoration and Recovery

Perform verification operations after a database is recovered using full backup files.

Step 1 Run the following command to create table space for testing in the database:

SQL> *create tablespace test datafile '/oracle/db/datafile/test.dbf' size 10M;*

Step 2 Run the following command to check whether the table space is successfully created:

SQL> *select tablespace_name from dba_tablespaces;*

Step 3 Run the following commands to create test tables and insert required test data:

SQL> *create table test(*

id number(7)

3)tablespace test;

SQL> ***select TABLE_NAME from dba_tables where TABLESPACE_NAME='TEST';***

Step 4 Execute the **/backup/bin/backup_db.sh** script to perform a full backup for the database.

The script contains the following content:

% ***/backup/bin/backup_db.sh***

```
RMAN> run {
2> # Hot database level 0 whole backup
3> allocate channel t1 type disk;
4> backup
5>  incremental level 0
6>  skip inaccessible
7>  filesperset 6
8>  # recommended format
9>  format '+RAW_FLA/back_%s_%p_%T'
10>    (database);
11>  delete obsolete;
12>  sql 'alter system archive log current';
13>  # backup all archive logs
14>  backup
15>   skip inaccessible
16>   filesperset 10
17>  format '+RAW_FLA/arclogback_%s_%p_%t'
18>   (archivelog all
19>    delete input);
20>    delete obsolete;
21> }
```

If no error is displayed in the backup log, the full backup is successful. The log contains information about database location and name of files that are backed up. You can run the following commands to information about and location of the backed up files:

% rman target / nocatalog

RMAN> *list backup of controlfile;*

Step 5 Run the following command to delete the table space and related data:

SQL> *drop tablespace test including contents and datafiles;*

Step 6 Run the following commands to stop the database and then start it in nomount mode:

SQL> *shutdown immediate;*

SQL> startup nomount;

Step 7 Run the following commands to log in the RMAN and restore the control file:

% ***rman target / nocatalog***

RMAN> *restore controlfile from '+RAW_FLA/back_173_1_20081126';*

Step 8 Run the following command to mount the database:

RMAN> *alter database mount;*

Step 9 Run the following commands to recover the database to a specific time point:

RMAN> *run*

{

set until time '07/26/2013 14:27:27';

restore database;

recover database;

}

Step 10 Run the following command to open the database:

RMAN> *alter database open resetlogs;*

Step 11 Run the following command to check whether the database is successfully recovered:

SQL> *select TABLE_NAME from dba_tables where TABLESPACE_NAME='TEST';*

Step 12 Start databases on other nodes.

If the target database is an Oracle RAC database, perform this step. Otherwise, skip this step.

----End

A Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
RMAN	Recovery Manager