

PETROL PLUS SYSTEM BACKUP PROCEDURE FOR ORACLE 11G

*Administrator's Guide
Version 1.00*

REVISION LOG

CHANGED PART (section, page)	MODIFICATIONS (added and deleted items) and description	
Document publication	Date: 27.07.2012	Version: 1.00

TABLE OF CONTENTS

1 INTRODUCTION	4
1.1 BASIC CONCEPTS	4
1.2 BACKUP METHODS	5
1.3 COMPARISON OF BACKUP METHODS	5
1.4 BACKUP MODEL.....	6
1.5 COMPLYING WITH THE BACKUP PROCEDURE	7
2 COLD DATABASE BACKUP	8
2.1 DETERMINING THE LOCATION OF THE FILES.....	8
2.2 COPYING FILES.....	9
3 BACKUP USING THE EXP UTILITY	10
3.1 DETERMINING THE NAMES OF THE SCHEMAS FOR BACKING UP	10
3.2 EXPORTING DATA	11
3.2.1 <i>Database Export Using an Executable File</i>	11
3.2.1.1 Description of Export Parameters	12
3.2.2 <i>Database Export Using Built-In Tools</i>	12
3.2.2.1 Backup in the OC Module	12
3.2.2.2 Backup in the DPC/ROC Module	13
3.3 CHECKING THE BACKUP LOG FILE	13
4 BACKUP USING THE RMAN UTILITY	14
4.1 SETTING UP THE ARCHIVELOG MODE FOR THE TARGET DATABASE.....	15
4.1.1 <i>Setting Up the ARCHIVELOG Mode Using PFILE</i>	16
4.1.1.1 Setting the Maximum FRA Size	16
4.2 SETTING UP THE RMAN BACKUP SCRIPTS	17
4.3 SETTING UP AN AUTOMATIC BACKUP SCHEDULE.....	18
4.4 PERFORMING RMAN BACKUP	18
4.5 CHECKING THE BACKUP LOG FILES	18
4.5.1 <i>Deleting ARCHIVELOG and Backup Files Manually</i>	19
4.5.2 <i>Checking the Amount of Free Space in the FRA Folder</i>	19
5 DATABASE RECOVERY PROCEDURE	21
5.1 DATABASE RECOVERY CONDITIONS.....	21
5.2 ACTIONS TO PERFORM IF THE RECOMMENDED BACKUP PROCEDURE HAS BEEN FOLLOWED EXACTLY.....	21
5.3 ACTIONS TO PERFORM IF THE RECOMMENDED BACKUP PROCEDURE HAS NOT BEEN FOLLOWED.....	21

1 INTRODUCTION

The Petrol Plus system (the *System*) is a system for loyalty and non-cash payments that allows granting discounts and performing payments for goods and services using smart cards. All information within the *System* is stored in the Oracle database, which requires to be backed up on a regular basis to ensure data security.

Creating a database backup means creating a copy of the database on an accessible data storage medium to provide quick and timely data recovery in case the database is corrupted or deleted.

This document describes the recommended backup procedure and backup schedule, as well as the recommended methods for creating backups of the Oracle 11g database. The document also describes the database recovery procedure (see section 5, p. 21).

1.1 Basic Concepts

Archive log – backed up redo log files of the database. These files are created in the **FRA** (Flash Recovery Area) folder in the course of database operation and are necessary to restore the database to its up-to-date state;

FRA – Flash Recovery Area, the standard Oracle folder for storing backups. The default path to this folder is `C:\oracle\product\11.2.0\flash_recovery_area\MAGICASH\`. If the database is in the ARCHIVELOG mode, this folder is used for storing Archive log files;

Note.

Starting from Oracle 11.2.0.2, the FRA folder is named "Fast Recovery Area" and is located at the following path: `C:\oracle\product\11.2.0\fast_recovery_area\MAGICASH\`.

RMAN – Oracle Recovery Manager, a utility for automation and efficient management of Oracle database backup and recovery operations;

Up-to-date backup – a properly created backup with enough data to restore the database to its up-to-date state;

Up-to-date database state – the state of the database after recovery that does not require manual data input because no information from the database has been lost. The up-to-date database state after recovery is identical to the database state after the last successfully performed operation right before the crash;

Alert log – the database operation log, which contains records about all database events, including creation of Archive log files and errors occurring in the course of database operation. By default, the Alert log is recorded in `C:\oracle\product\11.2.0\admin\MAGICASH\bdump\alert_MAGICASH.log`;

Note.

Drive `C:` is used as an example in this document. The drive letter may vary depending on the installation path of the Oracle DBMS and database files. Also, `MAGICASH` is used as an example of the database name in all paths and scripts.

Dump – a backup file created by the EXP utility. A dump contains a compressed copy of the database data and its logical structure;

Differential backup – an additional partial copy of database files, which is used by the RMAN utility for database recovery. To restore the database successfully, a full backup, all the subsequent differential backups and Archive log files are required;

Log file – a text file that contains information about script execution results;

Backup method – a method for creating a backup of the *System* database;

Backup model – the recommended procedure and schedule for regular operations related to *System* database backup;

Full backup – a copy of all files of the target database at a particular moment in time;

ARCHIVELOG mode – a database operation mode that enables creation of Archive log files required for data recovery in case of failure;

Script – a set of instructions in the form of a command-line batch file. In general, scripts have the `*.bat` extension;

Schema – an element of the database logical structure synonymous with "database user". A schema owns a set of database objects, such as tables, indexes, etc. When installing any software module of the *System*, it is necessary to specify the schema to which the objects will belong. For the Operation Centre module, the default schema name is `MAGICASH5`. When creating a backup using the EXP utility, all schemas used by software modules of the *System* should be specified;

Target database – the database that is being backed up or recovered.

1.2 Backup Methods

This document describes the following database backup methods:

- cold database backup;
- database backup using the EXP utility;
- database backup using the RMAN utility;

The main method that should be used for daily database backup is backup using the RMAN utility. The other methods are secondary and provide additional security.

Database backup using the RMAN utility allows creating up-to-date backups, which are used in the recommended backup model (see subsection 1.4) and by the technical support staff for database recovery (see section 5, p. 21).

This method consists in performing database backup using RMAN, an internal Oracle utility. The method involves creating full database backups weekly and partial database backups daily, as well as storing Archive log files. Creation of backups is launched using executable files (scripts) and can be monitored by checking log files. This method is described in more detail in section 4 (p. 14).

The following additional backup methods are described in this document for the purposes of creating weekly/monthly additional backups (see subsection 1.4), as well as for emergency backup and for backup before performing database system operations that involve increased risks (deleting data, configuring parameters, moving files).

Cold database backup consists in copying all database files to another folder (preferably to an external data storage medium or another physical disk). This method requires the database to be shut down for successful backup creation. The cold database backup method is described in more detail in section 2 (p. 8).

Database backup using the EXP utility is performed using an internal Oracle utility. Data export from the database involves creating a dump, a single file that essentially is the backup. Depending on the export parameters, this operation can copy either the entire database or particular schemas. When it becomes necessary to recover data from the backup, an import operation is performed. This method is also accessible through standard tools of the OC and DPC/ROC modules of the *System*. The details of this backup method are described in section 3 (p. 10).

1.3 Comparison of Backup Methods

The table below offers a comparison of all database backup methods (see Table 1). A "+" symbol indicates that the backup method has a certain advantage. A "-" symbol indicates the absence of such an advantage. A "++" pair indicates a marked superiority of the method over the other methods.

Table 1. Comparison of backup methods

Backup method	Criterion					
	High security	High backup speed	High recovery speed	Minimal loss of the most recent data	Small backup size	Ease of administration
EXP utility	–	–	–	–	+	+
Built-in export tools (OC, DPC)	–	–	–	–	+	++
Cold backup	+	+	+	–	–	+
RMAN utility	++*	+	+	+	–	–

* RMAN provides advanced security because it does not allow creating a backup if any database files are corrupted.

High security means that there is a high probability of database recovery.

High backup speed means that the speed is limited only by the read/write speed of the server hard disk drives.

High recovery speed is the maximum speed with which the data can be recovered and the database functionality can be restored. Recovery that does not involve using a full backup is usually faster.

Minimal loss of the most recent data means that the database can be restored to its up-to-date state.

Small backup size is a size that is significantly smaller than the size of the entire database.

Ease of administration means that the administrative procedures do not require time-consuming manual backup configuration.

1.4 Backup Model

The backup model described in this subsection is optimal in terms of administrative convenience, data security, and flexibility. The model is a specific procedure that should be performed on a regular basis (daily, weekly and monthly).

Complying with the requirements of this model increases the probability of successful data recovery to the up-to-date state after a database failure.

Note.

Since in most cases the amount of free disk space does not allow storing all backups recommended by this model, the *System* administrator may reduce the number of stored backups or increase the time period between creating backups. However, these measures increase the risk of data loss.

This model includes one main backup method (using the RMAN utility; for the configuration description, see section 4, p. 14) and two additional backup methods for increasing data security. When it is not possible to recover data from RMAN backups (for example, if the backups are corrupted), backups created using the other methods can be used.

The following general rules should be observed when using the backup model:

- the result of creating any of the database backups should be checked by viewing the backup log files and looking for errors. The means for checking the backup result are described in the corresponding section for each method. If any errors occur, contact the Technical Support Department;
- the created backups should be stored on a hard disk drive other than the drive containing the database;
- constant monitoring of the amount of free disk space is required for both the drives with the backups and the drive with the FRA folder.

The following operations should be performed to comply with the backup model:

- **Daily:**
 - **creating a daily partial database backup using RMAN** by executing the "rm_backup_daily_compress.bat" script;
 - **checking whether the partial database backup has been created successfully** (see subsection 4.5, p. 18) by checking the backup log file;
 - **checking the size of the FRA folder** (see subsection 4.5.2, p. 19). Checking the amount of free space available in the FRA folder and, if necessary, launching unscheduled backup creation using the "rm_backup_daily_compress.bat" script (during backup creation, the script deletes all current Archive log files from the FRA folder);

Note.

For more convenient creation of daily backups using RMAN, it is recommended to set up the "rm_backup_daily_compress.bat" script to be executed automatically (see subsection 4.3, p. 18).

- **Weekly:**
 - **creating a weekly full database backup using RMAN** by executing the "rm_backup_weekly_compress.bat" script;
 - **checking whether the full database backup has been created successfully** (see subsection 4.5, p. 18) by checking the backup log file;
 - **creating a database backup using EXP** (see section 3, p. 10). Executing the "exp_backup.bat" script;
 - **checking the consistency of the database dump** by checking the backup log file (see subsection 3.3, p. 13);

Notes:

1. For more convenient creation of weekly backups using RMAN, it is recommended to set up the "rm_backup_weekly_compress.bat" script to be executed automatically (see subsection 4.3, p. 18).
2. Weekly EXP backups can be created either manually or using the built-in export tools of the OC or DPC/ROC module. It is recommended to store these backups for one month (i.e., keeping 4-5 backups). After a backup is stored for one month, it should be deleted and replaced by a new one.

- **Monthly:**
 - **creating a cold database backup** (see section 2, p. 8) by obtaining the list of all database files and copying them into a separate folder;
 - **deleting database backups that are no longer needed.** Checking the folders for old weekly and monthly database backups.

Note.

It is recommended to create monthly backups manually after completing a reporting period. Monthly backups should be stored for 2 months (i.e., keeping 2 backups). After a backup is stored for two months, it should be deleted and replaced by a new one.

1.5 Complying with the Backup Procedure

Complying with the backup procedure requires at least one properly created, intact and up-to-date set of *System* database backups. This document outlines the recommendations and descriptions required for successful creation and management of such set of backups.

In order to comply with the procedure for creating and storing up-to-date database backups, the following is required:

1. Read the description of the backup model (see subsection 1.4, p. 6);
2. Set up the main RMAN backup method (see section 4) in accordance with the backup model;
3. Set up the additional backup methods (see subsections 2, p. 8; 3, p. 10) in accordance with the backup model;
4. Monitor and check successful creation of backups and observe the correct backup schedule in accordance with the backup model;
5. Read the database recovery conditions (see section 5, p. 21).

2 COLD DATABASE BACKUP

Cold database backup consists in copying all database files (by default, the files are located in C:\oracle\product\11.2.0\oradata\MAGICASH) to another folder (preferably to an external data storage medium or at least to another system drive). This method is universal because it can be applied to any database irrespective of its size. However, this method requires the amount of additional storage space equal to the database size.

The advantages of this method include high speed, high security, and simplicity of creating a database backup. This method is also characterized by high speed of database recovery.

A disadvantage of this method is large backup size, equal to the total size of all database files. However, the database files can be copied to another computer to reduce the load on the database server hardware.

To create a cold database backup, do the following:

1. Determine the location of all files of the target database (see subsection 2.1);
2. Copy all files of the target database (see subsection 2.2).

2.1 Determining the Location of the Files

Before creating a cold database backup, the list of database files to be copied should be created. This can be done either by making a number of requests to the target database, or by executing the "db_files.bat" script, which comes with this document and contains all these requests. The script does not require any preparatory steps before execution. It is recommended to run the script on the database server.

After the script is launched, it will display a number of requests, which should be answered:

- *Enter DATABASE name (default – MAGICASH):* – in reply to this request, enter the name of the target database that should be backed up. If you press , the default value (MAGICASH) will be used;
- *Enter SYS password:* – in reply to this request, enter the password of the SYS user in the target database. If you press , the default value (NCTSYS) will be used.

As a result of executing the script, the list of database files will be created in the "db_files.log" file in the folder containing the script. This list of files is used for creating a backup (see subsection 2.2, p. 9).

ATTENTION!

All files included in this list should be copied. If any of the database files are missing in the backup, this backup cannot be used, and database recovery is not possible. If the "db_files.log" file contains errors (they are marked by lines of the following type: "ORA-*sequence of digits*:*error text*"), this file should not be used. In this case, contact the Technical Support Department.

2.2 Copying Files

To copy the target database properly, do the following:

1. **Stop the target database.** To do this, stop the OracleServiceMAGICASH service by selecting Start\Settings\Control Panel\Administrative Tools\Services, and then selecting "Stop" in the context menu of the service (see Fig. 1).

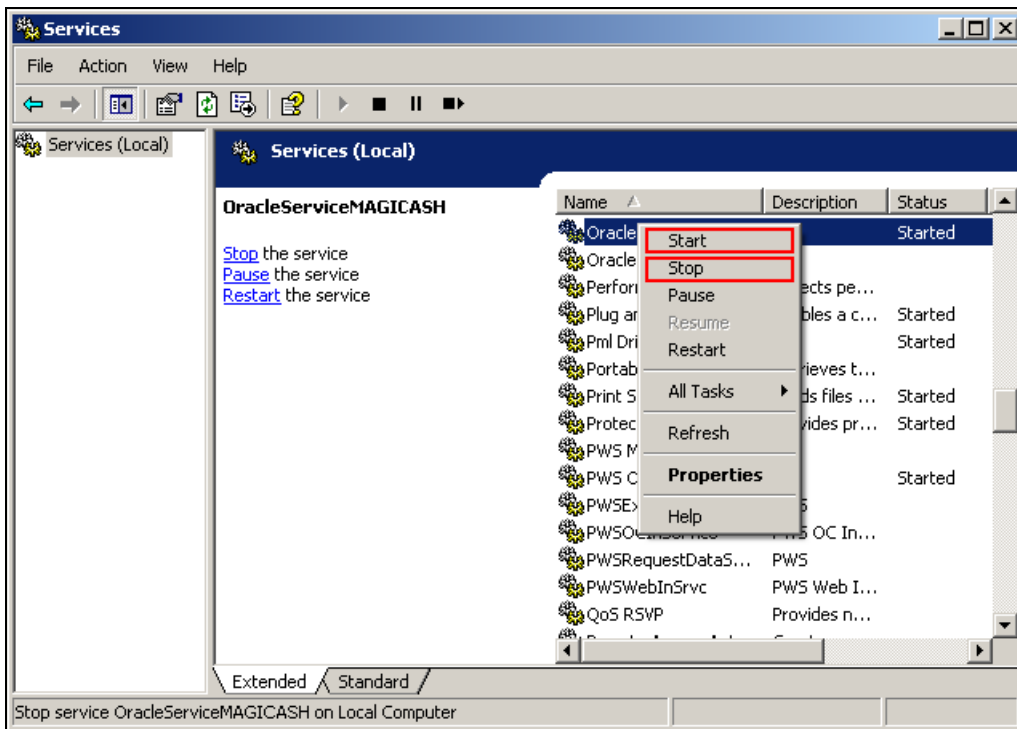


Fig. 1. Stopping the OracleServiceMAGICASH service

2. **Copy all files of the target database** that are listed in the db_files.log file. It is recommended to store cold backups of the target database on an external data storage medium or at least on another physical disk.
3. **Start the target database.** To do this, start the OracleServiceMAGICASH service by selecting Start\Settings\Control Panel\Administrative Tools\Services, and then selecting "Start" in the context menu of the service (see Fig. 1).

3 BACKUP USING THE EXP UTILITY

The Oracle DBMS includes utilities for exporting data from the database and importing data to the database. The EXP utility allows creating a database backup by copying data to a compressed file (dump). The backup procedure consists in creating dump files (*.dmp) by launching executable batch files (*.bat). The EXP utility copies data at logic level. Therefore, backups can be created only if the database is open and functional.

The advantages of this method include simplicity of backup creation, relatively low load on the database server hardware, and small backup size.

A disadvantage of this method is considerable amount of time required both for creating a backup and for recovering data. If the database size is greater than 30 GB, creating a backup may require several hours.

To create a database backup using the EXP utility, do the following:

1. Determine the names of all schemas of the target database that should be backed up (see subsection 3.1);
2. Export these database schemas to a *.dmp file (see subsection 3.2);
3. Check the export log file (see subsection 3.3).

3.1 Determining the Names of the Schemas for Backing Up

Exporting database data involves specifying the list of database schemas that should be backed up. Although the EXP utility allows creating a full database dump using the "FULL=Y" parameter, it is recommended to specify particular schemas for exporting in order to increase reliability during copying and recovery.

To determine the accurate list of schemas used by various software modules of the *System*, execute the "nct_info.bat" script, which comes with this document. The script does not require any preparatory steps before execution. It is recommended to run the script on the database server.

After the script is launched, it will display a number of requests, which should be answered:

- *Enter DATABASE name (default – MAGICASH):* – in reply to this request, enter the name of the target database that should be backed up. If you press Enter, the default value (MAGICASH) will be used;
- *Enter SYS password:* – in reply to this request, enter the password of the SYS user in the target database. If you press Enter, the default value (NCTSYS) will be used.

As a result of executing the script, the "nct_info.log" file will be created in the folder containing the script. This file has the following format:

```
*****
***** Users/Schemas with OC and LNR(LFC) *****
*****
MAGICASH5 - OC 4000,0 version: 5.12.0.0; LNR version: 5.4.2.0
--- D-Reports OC version: 6.0.7.0
--- D-Reports LNR version: 3.0.6.1.4306
--- D-Reports MCS version: 6.0.2.1
-----
*
*
*****
***** Users/Schemas with ROC and PC(DPC) *****
*****
MAGICASH5 - PC 5001 version: 5.35.0.0
--- D-Reports PC/ROC version: 6.0.3.0.5275
-----
*
```

In the log file example above, the name of the schema is displayed at the beginning of each paragraph in uppercase letters (MAGICASH5). As shown in this example, all software modules of the *System* use the same database schema (MAGICASH5). After the list of schemas is created, specify these schemas in the executable export file (for details, see subsection 3.2.1).

ATTENTION!

To successfully create a backup using the EXP utility (see subsection 3.2.1), all schemas used by software modules of the *System* should be specified. Schemas that have not been specified cannot be recovered. If the "nct_info.log" file contains errors (they are marked by lines of the following type: "ORA-*<sequence of digits>*:*<error text>*"), this file should not be used. In this case, contact the Technical Support Department.

3.2 Exporting Data

Correct database export can be performed using two different methods, which are not mutually exclusive. Database export using built-in tools (see subsection 3.2.2) allows avoiding manual backup configuration, while using an executable file (script) allows exporting several database schemas simultaneously.

3.2.1 Database Export Using an Executable File

To create a database backup using this method, do the following:

1. Create the backup folder (for example, "ExpImp") and place the export and import script files into this folder.
2. Launch the export script file.
3. Wait while the backup (*.dmp file) is being created. Do not interrupt the operation.

The backup is created using a *.bat executable file. This file is in plain text format and contains DOS commands. Each command with its parameters is placed on a separate line. The name of the executable file should not be identical to any of the commands in this file (for example, "exp.bat" is not a valid name).

An example of a line from the executable file for exporting a user (where the schema/user is MAGICASH5 and the database name is MAGICASH) is given below:

```
<EXP USERID=magicash5/nctmagicash5@magicash FILE=exp_magicash5.dmp
LOG=exp_magicash5.log OWNER=magicash5 GRANTS=y INDEXES=y ROWS=y
CONSTRAINTS=y>
```

You can also use the provided export file "exp_backup.bat", which comes with this document. This file contains the set of parameters required for successful backup creation. To configure the parameters, open the file using a text editor and edit the following lines:

```
rem ***Define database SERVICE NAME***
Set _TargetName=MAGICASH
```

Specify the name of the target database to be backed up after the "=" character (default name: MAGICASH).

```
rem ***Define SYS user PASSWORD***
Set _SysPsw=NCTSYS
```

Specify the password of the SYS user of the target database after the "=" character (default password: NCTSYS).

```
rem ***Define BACKUP FOLDER***
Set _BackupDir=.
```

Specify the full path to the folder to which backups and execution logs will be saved after the "=" character. The default value is ".", which means that backups will be placed in the folder containing the script. It is recommended to specify a path to a physically separate local disk and not to use network paths, because local paths are invariant with respect to changes of network settings and user privileges, and a separate physical disk drive ensures safety of the backup in case of failure of the database disk drive.

ATTENTION!

The EXP utility cannot use a mapped network drive as network path. If you use network paths, specify them in the following format: "\\Server\Folder\".

```
rem ***Define USERS dividing them by commas - MAGICASH5,MAGICASH6,TMS***
Set _Users=MAGICASH5
```

Specify the list of schemas that should be copied from the target database after the "=" character. The names of schemas should be separated by commas. The procedure for determining the list of schemas that are used by the *System* in the target database is described in subsection 3.1 (p. 10).

After the executable file has been configured and checked, it can be launched automatically using Windows Task Scheduler for creating weekly database backups. The backup schedule is set up in the same way as for backup using the RMAN utility (see subsection 4.3, p. 18).

3.2.1.1 Description of Export Parameters

This subsection contains a description of the parameters that are used in the backup executable file. If the "exp_backup.bat" export file is used, it is not necessary to modify or add these parameters. The parameters have been already pre-configured in this file in accordance with the recommended values.

Parameters used for backup using the EXP utility:

- **USERID** – parameter for connecting to the database server (in the following format: user/password@database name);
- **FILE** – parameter containing the full path to the file to which data will be exported;
- **LOG** – parameter containing the full path to the log file to which the export report will be recorded;
- a group of mutually exclusive parameters defining what should be exported:
 - **OWNER** – the database user for which all owned objects will be exported. If several users should be exported, specify their names in brackets, separated by commas;
 - **FULL** – full database export. Possible values: "y" – YES and "n" – NO;
- **GRANTS** – parameter responsible for exporting access rights to objects. Possible values: "y" – YES and "n" – NO;
- **INDEXES** – parameter responsible for exporting table indexes. Possible values: "y" – YES and "n" – NO;
- **ROWS** – parameter responsible for exporting table data. Possible values: "y" – YES and "n" – NO;
- **CONSTRAINTS** – parameter responsible for exporting constraints. Possible values: "y" – YES and "n" – NO.

3.2.2 Database Export Using Built-In Tools

To ensure the possibility of data recovery in case of software failure, the *System* provides the functionality of data backup. This functionality is available only in the OC module (see subsection 3.2.2.1) and the DPC/ROC module (see subsection 3.2.2.2).

ATTENTION!

Data export using built-in tools consists in copying only the schema used by the software module in which the export operation is performed. If the database contains several schemas with *System* software, data export should be performed using the executable file (see subsection 3.2.1).

3.2.2.1 Backup in the OC Module

To create a backup of the OC database, select "**Service / Backup**" in the OC main menu. The window shown below will appear (see Fig. 2).

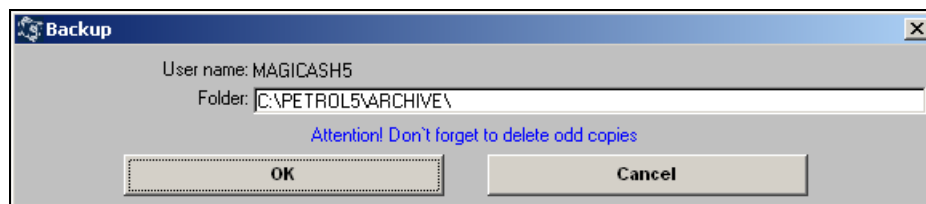


Fig. 2. "Backup" window

The "Folder:" field displays the path to the archive folder specified during configuration of the *System* (the default backup folder). If necessary, you can edit this path directly in the backup window.

This backup method also ensures creating a backup of the OC system files from the <Program_installation_folder>\DATA folder.

The database dump is saved as a file with the name in the following format:

ExpMG5_YYYYMMDDHHMMSS_full.dmp, where:

- YYYYMMDD stands for the year, month, and day of the beginning of the operation;
- HHMMSS stands for the time of the beginning of the operation (hours, minutes, and seconds).

Note.

The "**General**" tab of the "**System configuration**" window ("**System / Configuration / Settings**" menu item) contains the "Suggest backup when exiting the program" check box. If this check box is marked, the "**Backup**" window (see Fig. 2) will be displayed automatically each time the OC module is closed.

3.2.2.2 Backup in the DPC/ROC Module

To create a backup, do the following:

1. Select **"System / Database backup"** in the main menu. The following message will be displayed: *"Creating the database backup. Please wait..."*. When the operation is completed, a message confirming successful creation of a database backup will be displayed.
2. Click **OK**.

The backup is saved to the export folder in the form of two dump files (ExpUS_PC_YYYYMMDD.dmp and ExpDB_PC_YYYYMMDD.dmp) accompanied by two log files (ExpUS_PC_YYYYMMDD.txt and ExpDB_PC_YYYYMMDD.txt).

Note.

The export folder is configured in the **"System / Configuration / Settings"** window.

If the export folder contains backup files for the current date (i.e., files with the same names as the files to be created), the following message will be displayed: *"Outdated backups of files were found in the export folder. To backup, empty the folder. Transfer the files to the other folder or delete them."*

Move the files to another folder or delete them. Then repeat the backup procedure.

ATTENTION!

If error messages are displayed at any stage of the backup procedure, contact the Technical Support Department.

3.3 Checking the Backup Log File

Creation of a database backup using the EXP utility is successful if the "Export terminated successfully without warnings." line appears at the end of the log file created during the backup procedure.

The "Export terminated successfully with warnings." message means that the database backup has been created incorrectly and cannot be used for data recovery. If this message appears, create a new backup. If the message persists, contact the Technical Support Department.

4 BACKUP USING THE RMAN UTILITY

The Oracle Database 11g installation package includes the RMAN utility, which is designed for regular database backup and provides flexible backup configuration. This utility has its own command interpreter and allows using different backup strategies depending on the database size, the devices being used and other parameters. Backups are created at the physical level (i.e., database blocks are copied, rather than logical entities).

This section describes creating differential incremental backups (i.e., daily backups of all recent changes to database data) using RMAN.

This backup method can be used only if the database is in the ARCHIVELOG mode. In this mode, database redo logs, which are required for database recovery in case of failure, are continuously saved to the FRA folder as Archive log files.

The advantages of this method include high security, high speed of backup creation and the possibility to restore the database to its up-to-date state.

A disadvantage of this method is large backup size.

This document describes only one recommended method for using the RMAN utility. This method is characterized by the following features:

- the Recovery Catalog is not used;
- backup information is stored for 45 days;
- differential incremental backups are created (i.e., one full backup of the database and daily partial backups of changes to the database);
- controlfiles copies are created each time backup scripts are launched;
- Archive log copies are created each time backup scripts are launched; old Archive log files are deleted from the FRA folder.

The described backup method consists in the following: the "rm_backup_weekly_compress.bat" weekly script (for example, launched every Sunday) creates a full backup of the database (level 0 backup). In the course of the week, the "rm_backup_daily_compress.bat" script, launched every day, creates additional backups that contain only new and changed database data (level 1 backup).

Thus, the complete backup set will consist of the full (weekly) backup and several additional daily backups (see Fig. 3).

During recovery, RMAN restores data from the full (level 0) backup and then adds new and changed data from the daily (level 1) backups. After this, information from the Archive log files is added to the restored database. This backup algorithm allows restoring the database to its up-to-date state, i.e., the most recent state prior to the crash.

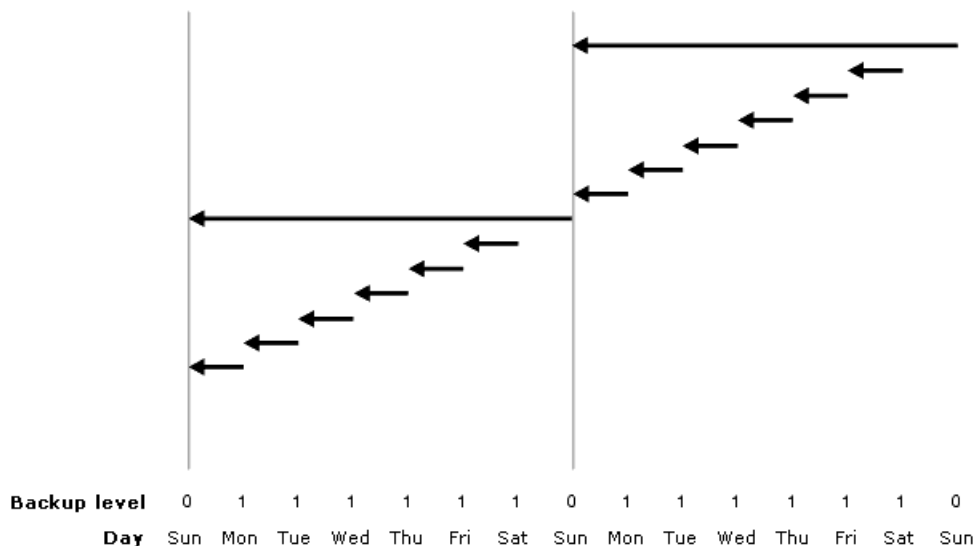


Fig. 3. Differential incremental backup using RMAN

To create a database backup using RMAN, do the following:

1. Set up the ARCHIVELOG mode for the target database (see subsection 4.1).
2. Set up the RMAN backup scripts (see subsection 4.2, p. 17).
3. Set up the schedule for automatic script launching (see subsection 4.3, p. 18).
4. Perform a manual backup using RMAN (see subsection 4.4, p. 18).
5. Check the RMAN backup log files (see subsection 4.5, p. 18).

4.1 Setting Up the ARCHIVELOG Mode for the Target Database

To enable the ARCHIVELOG mode for the database and to prepare for RMAN backup, execute the "rm_install.bat" script. It is designed for changing database parameters, setting the folder for Archive log files and enabling the ARCHIVELOG mode. During the execution of the script, the database will be restarted. The script does not require any preparatory steps before execution. It is recommended to run the script on the database server.

After the script is launched, it will display a number of requests, which should be answered:

Enter DATABASE name (default - MAGICASH):

In reply to this request, enter the name of the target database that should be backed up. If you press , the default value (MAGICASH) will be used.

Enter SYS password:

In reply to this request, enter the password of the SYS user in the target database. If you press , the default value (NCTSYS) will be used.

Enter PATH to FRA (default - C:\oracle\product\11.2.0\flash_recovery_area):

In reply to this request, enter the path to the FRA folder, where Archive log files of the target database will be stored. If you press , the default value (C:\oracle\product\11.2.0\flash_recovery_area) will be used.

ATTENTION!

Make sure that the path to the FRA folder specified at this step actually exists. If the specified folder does not exist, database failure may occur. Starting from Oracle 11.2.0.2, the FRA folder is named "Fast Recovery Area" and is located at the following path: C:\oracle\product\11.2.0\fast_recovery_area\MAGICASH\.

Recommended MAX size of FRA - 126G

Enter MAX size of FRA (default - 100G):

In reply to this request, enter the maximum total size that Archive log files can take up in the FRA folder specified at the previous step. You can specify either an exact value in bytes (for example, 100888666222), or a value in gigabytes (for example, 100G). If you press , the default value (100G) will be used. The recommended value of this parameter, calculated by the script for your database, is shown above the request:

Recommended MAX size of FRA - 126G

Use this value to reply to the request. You can also calculate the value manually by using the formula (see subsection 4.1.1.1, p. 16).

ATTENTION!

The size of the folder should be sufficient for storing all Archive log files that are being accumulated. If new Archive log files cannot be saved to the folder, database failure may occur.

After answers to all requests have been entered, the script will implement the required changes. After the script finishes running, check the log file ("rm_install.log" in the folder containing the script) for errors. Make sure that the log file contains the "SPFILE - OK." string.

Note.

If the log file contains the "ERROR!!! - PFILE" string instead of "SPFILE - OK.", perform the instructions given in subsection 4.1.1 instead of using the script.

ATTENTION!

If, despite the presence of the "SPFILE - OK." string, the "rm_install.log" file contains any errors (they are marked by lines of the following type: "ORA-<sequence of digits>:<error text>"), the script cannot be used. In this case, contact the Technical Support Department.

As a result of successful script execution, the ARCHIVELOG mode will be enabled in the database. You can check whether the mode has been enabled successfully by going to the specified FRA folder and checking the presence of Archive log files with the *.arc extension. If these files are present, you can start configuring the RMAN scripts and the backup schedule (see subsection 4.2).

4.1.1 Setting Up the ARCHIVELOG Mode Using PFILE

The procedure described in this subsection should be performed only if the "rm_install.log" script log contains the "ERROR!!! – PFILE" string (see subsection 4.1) or if you have found out, by any other means, that PFILE is used in the target database.

If PFILE is used, you should first find out which text initialization file on the database server is used for starting the database. To do this, find and open (using any text editor) the following file: C:\oracle\product\11.2.0\db_1\database\INITmagicash.ora. If the file contains a list of parameters, you will need to edit this file. If the file contains only the "IFILE=<path to the parameter file>" line, then the value in this line is the path to the initialization file (usually, the path is C:\oracle\product\11.2.0\admin\MAGICASH\pfile\init.ora), which should be edited. To set up the ARCHIVELOG mode using PFILE, do the following:

1. Add or edit the following parameters in the file:

```
db_recovery_file_dest='C:\oracle\product\11.2.0\flash_recovery_area';
```

// specifying the folder to which archive copies of database redo logs will be saved

ATTENTION!

Make sure that the path to the FRA folder actually exists. If the specified folder does not exist, database failure may occur. Starting from Oracle 11.2.0.2, the FRA folder is named "Fast Recovery Area" and is located at the following path:
C:\oracle\product\11.2.0\fast_recovery_area\MAGICASH\.

```
db_recovery_file_dest_size=100G; // specifying the maximum size of the FRA folder
```

(see subsection 4.1.1.1)

```
control_file_record_keep_time=45; // specifying the period for keeping information related to backups and Archive log files
```

2. After the parameters have been edited, save the PFILE file.

3. Using the command line ("Start / Run..."), launch "sqlplus.exe" with the /nolog parameter:

```
C:\oracle\product\11.2.0\db_1\BIN>sqlplus.exe /nolog
```

4. Enter the commands listed below in the Sqlplus command line. During execution of these commands, the database will be restarted:

```
SQL> spool C:\rm_install_pfile.log; // enabling the operation log
```

```
SQL> connect sys/NCTSYS@magicash as sysdba; // connecting to the database with sysdba privileges
```

```
SQL> shutdown immediate; // shutting down the database to update parameters
```

```
SQL> startup mount; // starting the database in the mount mode, which allows editing system information
```

```
SQL> alter database archivelog; // enabling log archiving
```

```
SQL> alter database open; // starting the database in the normal working mode
```

```
SQL> archive log start; // starting the log archiving process (in case it has not been started automatically)
```

```
SQL> alter system switch logfile; // several switches of redo logs to check successful creation of Archive log files
```

```
SQL> alter system switch logfile;
```

```
SQL> alter system switch logfile;
```

```
SQL> alter system switch logfile;
```

```
SQL> spool off // disabling the operation log
```

```
SQL> exit // exiting sqlplus
```

If no errors have appeared when executing the commands, the ARCHIVELOG mode has been enabled successfully. You can check whether the operation has been successful by going to the specified FRA folder and checking the presence of Archive log files with the *.arc extension. If these files are present, you can start configuring the RMAN scripts and the backup schedule (see subsection 4.2).

4.1.1.1 Setting the Maximum FRA Size

The procedure described in this subsection should be performed only if PFILE is used (see subsection 4.1.1) or if you have other reasons to calculate the FRA size manually.

The maximum size of the FRA folder, in which Archive log files are stored, is specified by the "db_recovery_file_dest_size" parameter.

The maximum size of the FRA folder should be specified depending on the database use dynamics (daily amount of changes). You can specify a greater FRA size value, but the size of the folder should not exceed the amount of free space in the disk partition; otherwise, the files may occupy all free disk space.

You can estimate the creation dynamics for Archive log files and the amount of disk space these files can take up after a certain period of time by viewing the database Alert log. To do this, open the alert_MAGICASH.log file (C:\oracle\product\11.2.0\admin\MAGICASH\bdump\ folder), then go to the end of the file and view the logs for the last few days (for example, for 3 days).

Pay attention to records of the following type:

```
Mon Mar 27 00:18:45 2012
```

```
Thread 1 advanced to log sequence 125 (LGWR switch)
```

Such messages are added to the Alert log when Oracle switches the process of recording changes to the next redo log group. This event means that, if the ARCHIVELOG mode is enabled, the previous redo log is added to the archiving queue. By counting the number of switch records for a certain period (one day, two days, etc.), you can approximately estimate the frequency of creation of new archived redo logs.

The overall size of Archive log files can be calculated using the following formula:

Size of Archive log files for period X = (Number of redo log switches for period X) * (Size of one redo log file)

In case of the recommended daily backup schedule, period X is equal to 2 days. Set the value of the "db_recovery_file_dest_size" parameter according to the result obtained using the formula.

4.2 Setting Up the RMAN Backup Scripts

Daily and weekly backups using RMAN are performed using a package of scripts, which comes with this document. The package includes the following 3 scripts:

- rm_backup_weekly_compress.bat – script for creating a weekly full database backup;
- rm_backup_daily_compress.bat – script for creating a partial differential incremental database backup;
- rm_archlog_crosscheck.bat – script for checking and cleaning up after backup deletion.

To set up one of the scripts, open the script file using a text editor and edit the following lines (all these scripts have the same structure):

```
rem ***Define database SERVICE NAME***
```

```
Set _TargetName=MAGICASH
```

Specify the name of the target database to be backed up after the "=" character (default name: MAGICASH).

```
rem ***Define SYS user PASSWORD***
```

```
Set _SysPsw=NCTSYS
```

Specify the password of the SYS user of the target database after the "=" character (default password: NCTSYS).

```
rem ***Define BACKUP FOLDER***
```

```
Set _BackupDir=C:\oracle\backuprman\
```

Specify the full path to the folder to which backups and execution logs will be saved after the "=" character. The default value is ".", which means that backups will be placed in the folder containing the script. It is recommended to specify a path to a physically separate local disk and not to use network paths, because local paths are invariant with respect to changes of network settings and user privileges, and a separate physical disk drive ensures safety of the backup in case of failure of the database disk drive.

ATTENTION!

The RMAN utility cannot use a mapped network drive as network path. If you use network paths, specify them in the following format: "\\Server\Folder\".

```
rem ***Define number of stored backup sets (1 - only latest backup set is stored)***
```

```
Set _red_int=2
```

Specify the number of backup sets (weekly full backup + daily partial backups) that will be stored after the "=" character. If the value of this parameter is "1", only the most recent backup set, which is required for recovery, will be stored. If the value is greater, older backup sets will be stored; these may be required if the more recent backups are damaged. The amount of disk space available for storing backups should be taken into account, since a greater number of backups will require more disk space. The recommended value is "2" (one set of the most recent backups + one older set of backups).

It is recommended to leave all the other lines, parameters, and values in the script unchanged. Make sure that the changed parameters are changed in all scripts.

To check the parameters, perform a manual backup (see subsection 4.4) and then check the log files (see subsection 4.5). If necessary, set up an automatic backup schedule (see subsection 4.3).

4.3 Setting Up an Automatic Backup Schedule

Automatic launching of scripts can be set up using Windows Task Scheduler as follows:

1. Select **"Start / Programs / Accessories / System Tools"**.
2. Select **"Scheduled Tasks"**.
3. In the main menu, select **"File / New / Scheduled Task"**.
4. Enter the name for the new scheduled task (for example, "RMAN – Weekly").
5. Right-click on the newly created task in the list, then select **"Properties"** in the context menu.
6. In the **"Task"** tab of the task properties window, specify the full path to the "rm_backup_weekly_compress.bat" script in the "Run" field (for convenience, you can use the **Browse...** button).
7. In the **"Schedule"** tab, specify the schedule for launching the script, for example: Schedule Task – "Weekly", Start time – "00:01", Schedule Task Weekly – Every "1" week on "Sun".
8. Confirm the changes.
9. In the main menu, select **"File / New / Scheduled Task"**.
10. Enter the name for the new scheduled task (for example, "RMAN – Daily").
11. Right-click on the newly created task in the list, then select **"Properties"** in the context menu.
12. In the **"Task"** tab of the task properties window, specify the full path to the "rm_backup_daily_compress.bat" script in the "Run" field (for convenience, you can use the **Browse...** button).
13. In the **"Schedule"** tab, specify the schedule for launching the script, for example: Schedule Task – "Daily", Start time – "00:01", Schedule Task Daily – Every "1" day.
14. Confirm the changes.

Note.

RMAN allows backing up the database and Archive log files when the database is in use. However, it is recommended to schedule the scripts for launching when no database connections are active (for example, during night hours and on weekends) to prevent the database from slowing down and to increase the backup speed.

The "rm_archlog_crosscheck.bat" script should not be scheduled for automatic launching. This script is used only in certain cases (see subsection 4.5.1).

The log files created during automatic backup procedures should be checked in the same way as for manual backup (see subsection 4.5).

4.4 Performing RMAN Backup

The backup scripts should be launched automatically according to the recommended database backup model (see subsection 1.4, p. 6). The procedure for setting up automatic execution of the model is described in subsection 4.3.

If you need to launch a script manually for checking or performing an unscheduled backup, no additional parameters are required.

The backup process can take from several minutes to several hours, depending on the database size.

ATTENTION!

The database administrator is responsible for monitoring script execution on a regular basis (checking the log files and monitoring the amount of free disk space for storing backups and Archive log files).

4.5 Checking the Backup Log Files

The log files of all executed scripts should be analyzed on a regular basis, according to the recommended database backup model (see subsection 1.4, p. 6).

Detecting script errors in time allows preventing creation of invalid backups, which might lead to data loss.

If the backup scripts ("rm_backup_weekly_compress.bat" and "rm_backup_daily_compress.bat") are completed correctly, the following files will be created in the backup folder specified during script configuration (see subsection 4.2):

1. Full database backup or partial database backup. The path to the file and the file name will have the following format:

```
<Backup folder>\backups_<Backup date>\
DB0_XXXXX_MAGICASH_XXXX.RM // "DB0" stands for level 0 backup, i.e., a full database backup. "DB1" files are created as a result of daily backup scripts;
```
2. Archive log backup. The path to the file and the file name will have the following format:

```
<Backup folder>\backups_<Backup date>\
ARC_XXXXX_MAGICASH_XXXX.RM;
```

3. Backup log file. The path to the file and the file name will have the following format:

```
<Backup folder>\logs_<Backup date>\
rm_backup_weekly_compress_MAGICASH_XXXXX.log // The name of the log file
may be different depending on the launched script.
```

If some of these files are missing after script execution is completed, check the log file for errors.

ATTENTION!

If the "rm_backup_weekly_compress_MAGICASH_XXXXX.log" or the "rm_backup_daily_compress_MAGICASH_XXXXX.log" log files contain errors (marked by lines of the following type: "RMAN-<sequence of digits>: <error text>"), this means that the backup failed. In this case, contact the Technical Support Department.

You can also resolve some of the RMAN backup errors using the table below.

Table 2. List of common RMAN error messages

Error text	Solution
<i>RMAN-03002: failure of configure command</i> <i>RMAN-06403: could not obtain a fully authorized session</i> <i>ORA-01034: ORACLE not available</i> <i>ORA-27101: shared memory realm does not exist</i>	The database is not started up. Restart the database service (the restart procedure is described in subsection 2.2, p. 9)
<i>RMAN-03009: failure of backup command</i> <i>ORA-19504: failed to create file "DB0_xxxx.RM"</i> <i>ORA-27040: skgfrcre: create error, unable to create file</i> <i>OSD-04002: unable to open file</i>	The database backup folder does not exist or is not accessible. Check the existence of the folder and the user access rights. Check whether a connected network drive is specified as backup folder (see subsection 4.2, p. 17)
<i>RMAN-06059: expected archived log not found</i> <i>ORA-19625: error identifying file xxx.ARC</i> <i>ORA-27041: unable to open file</i> <i>OSD-04002: unable to open file</i>	One of the Archive log files is missing. Use the "rm_archlog_crosscheck.bat" script. For details, see subsection 4.5.1
<i>RMAN-06207: WARNING: 4 objects could not be deleted for DISK channel(s)</i> <i>RMAN-06208: to mismatched status. Use CROSSCHECK command to fix status</i>	One of the database backup files is missing. Use the "rm_archlog_crosscheck.bat" script. For details, see subsection 4.5.1

Note.

If the script log file contains unknown errors or suspicious messages, contact the Technical Support Department.

4.5.1 Deleting ARCHIVELOG and Backup Files Manually

If, for any reason (for example, lack of disk space), some of the Archive log files have been deleted from the corresponding folder manually (without using RMAN), the backup script log file will contain errors if you attempt to create a backup (see Table 2).

To enable correct backup in such cases, run the "rm_archlog_crosscheck.bat" script (script configuration is described in subsection 4.2, p. 17).

ATTENTION!

It is not recommended to intentionally delete Archive log or backup files, since this may result in storing an incomplete backup set. If files have been deleted, run the "rm_archlog_crosscheck.bat" script and then create a full backup (using the "rm_backup_weekly_compress.bat" script).

4.5.2 Checking the Amount of Free Space in the FRA Folder

For successful RMAN backup, Archive log files are required. They are stored in the FRA folder specified during the initial RMAN configuration (see subsection 4.1, p. 15). Archive log files are created continuously during database operation. Thus, the total size of the Archive log files created during one day may be significant. If the total size of the Archive log files reaches the maximum FRA size, Archive log files

are no longer created, and the database operation is stopped until the FRA folder is cleaned manually (see subsection 4.5.1).

To check the amount of free space in the FRA folder, launch the "rm_check_fra.bat" script. The script does not require any preparatory steps before execution. It is recommended to run the script on the database server.

After the script is launched, it will display a number of requests, which should be answered:

Enter DATABASE name (default - MAGICASH) :

In reply to this request, enter the name of the target database that should be backed up. If you press **Enter**, the default value (MAGICASH) will be used.

Enter SYS password:

In reply to this request, enter the password of the SYS user in the target database. If you press **Enter**, the default value (NCTSYS) will be used.

As a result of executing the script, the "rm_check_fra.log" file will be created in the folder containing the script. This file has the following format (see Table 3):

Table 3. Results of executing the "rm_check_fra.bat" script

Path to the FRA folder	Size limit	Currently used	Free space in %	Number of files
D:\oracle\fast_recovery_area\	135 Gb	1.1 Gb	99.2%	8

Path to the FRA folder displays the current path to the FRA folder.

ATTENTION!

This path must exist. If the specified folder does not exist, database failure may occur.

Size limit means the current maximum size of the FRA folder.

Currently used displays the total size of the Archive log files stored in the FRA folder.

Free space in % displays the percentage of free space available in the FRA folder.

Number of files displays the number of the Archive log files stored in the FRA folder.

If the "Free space in %" value is less than 10%, the FRA folder will soon be completely used up. In this case, perform one of the following operations:

1. Perform unscheduled backup using the "rm_backup_weekly_compress.bat" or the "rm_backup_daily_compress.bat" script. During unscheduled backup, all Archive log files will be deleted from the FRA folder, and the amount of free space will increase.
2. Increase the maximum size of the FRA folder by specifying a greater value. To select the new value, analyze the dynamics of occupied space in the FRA folder or use the recommended calculation method (see subsection 4.1.1.1, p. 16).
To change the maximum FRA size, do the following:
3. Using the command line ("Start / Run..."), launch "sqlplus.exe" with the /nolog parameter:

```
C:\oracle\product\11.2.0\db_1\BIN>sqlplus.exe /nolog
```

Enter the commands listed below in the Sqlplus command line:

```
SQL> spool C:\rm_frasize.log // enabling the operation log
```

```
SQL> connect sys/NCTSYS@magicash as sysdba; // connecting to the database with sysdba privileges
```

```
SQL> alter system set db_recovery_file_dest_size=100G; // changing the FRA size
```

```
SQL> spool off // disabling the operation log
```

```
SQL> exit // exiting sqlplus
```

You can check whether the FRA size has been changed successfully by running the "rm_check_fra.bat" script again. The log file should contain the new FRA size. If you were unable to change the maximum FRA size, contact the Technical Support Department.

5 DATABASE RECOVERY PROCEDURE

5.1 Database Recovery Conditions

The backup procedure described in this document ensures the presence of up-to-date database backups required for successful data recovery. Up-to-date backups allow performing database recovery after any kind of failure and preserving *System* data. In case of data corruption or complete data loss, database recovery is performed by the Technical Support Department. Other recovery methods are not recommended. In case of physical hardware (hard disk drive) failure, it is not recommended to use the following recovery methods, which can lead to database corruption:

- the Chkdsk utility and other utilities for correcting bad blocks;
- the Acronis utility and other utilities for restoring the disk image.

If up-to-date backups (created using any of the recommended methods) are available, database recovery is performed by the Technical Support Department as part of the Support contract.

If the recommended procedure has not been followed, or if up-to-date backups are not available for any other reason, database recovery is paid for separately; the payment is decided upon agreement with the NCT Sales Department.

In addition, failure to comply with the recommended procedure may lead to the following problems:

- *System* operation stopping for a considerable period of time;
- loss of *System* data.

ATTENTION!

Each database failure is unique. A great number of errors may indicate that the database is corrupted. Thus, there is no universal procedure for identifying the database state or for recovering database data. In case of any database failure, contact the Technical Support Department.

The time required for database recovery will depend on:

- the nature of failure of the database and the operating system;
- the completeness/incompleteness of the available data;
- the existence and the up-to-date/not-up-to-date state of database backups and Archive log files;
- the possibility of remote access for the Technical Support staff to the server with the corrupted database.

The actions that should be performed, both if up-to-date database backups are available and if such backups are not available, are described below.

5.2 Actions to Perform if the Recommended Backup Procedure Has Been Followed Exactly

To recover the database with an existing up-to-date backup of the *System* database, the Technical Support Department will need the following information for analyzing the problem:

- the contents of the "C:\oracle\product\11.2.0\admin\MAGICASH" folder;
- the contents of the "C:\oracle\product\11.2.0\db_1\network\admin\MAGICASH" folder;
- the contents of the "C:\oracle\product\11.2.0\db_1\network\log\MAGICASH" folder;
- the path to the folder in which the up-to-date database backup is stored;
- the method and the date of the last successful database backup;
- the log files of the last successful backup;
- a description of the circumstances under which the database failure occurred;
- the version of the database server operating system;
- information about the possibility of remote access to the database server (using a remote desktop, TeamViewer, AMMY Admin or other applications for remote access).

The Technical Support Department will inform you about the subsequent actions to perform.

5.3 Actions to Perform if the Recommended Backup Procedure Has Not Been Followed

NCT cannot guarantee complete database recovery if up-to-date backups of the *System* database are not available.

To recover the database if the recommended backup procedure has not been followed, the Technical Support Department will need the following information:

- the contents of the "C:\oracle\product\11.2.0\admin\MAGICASH" folder;
- the contents of the "C:\oracle\product\11.2.0\db_1\network\admin\MAGICASH" folder;
- the contents of the "C:\oracle\product\11.2.0\db_1\network\log\MAGICASH" folder;

- a description of the circumstances under which the database failure occurred;
- information about the possibility of remote access to the database server (using a remote desktop, TeamViewer, AMMY Admin or other applications for remote access) or the possibility of sending a cold database backup (see section 2) to the NCT office (using FTP, e-mail, or an external data storage device);
- the path to the folder in which backups were stored (if backups were created);
- the method and the date of the last successful database backup, if it was performed;
- the log files of the last successful backup;
- the version of the database server operating system;
- the list of the NCT software modules installed (DPC/ROC, OC/branch, TMS, PWS, etc.), names of the databases and names of the database schemas in which the software modules are installed.

The Technical Support Department will inform you about the subsequent actions to perform.