Preventive Maintenance and Recovery Policy

Version 20

CONFIDENTIAL INFORMATION

DISCLAIMER

TRADEMARKS

Document released: August 26, 2010

Web address: http://www.exlibrisgroup.com

Table of Contents

1 Introduction

The purpose of this document is to define the maintenance activities that are necessary for the smooth running of Aleph. It is recommended that the system administrator and the DBA on site read this document thoroughly and carry out the tasks described within.

A summary of the various maintenance activities can be found in **Appendix A: Backup Strategy Guidelines** on page **5**. The following is a list of the activities that are described in this document:

- Ensure sufficient database space
- Ensure sufficient disk space for the archiving.
- Back up all system and application components
- Perform disk cleanup
- Review Oracle alert log

> **Note**:
> Whenever an online utility is mentioned in this document, refer to the relevant documentation (the *Aleph 20 System Administration Guide* for UTILs A and O, or the *System Administration Guide – System Overview* for all other UTILs) for complete details.

2 Sufficient Database Space

2.1 Tablespace Free Space

In order for the Oracle database to function properly, there must be free space in the various tablespaces. The Oracle tablespaces are logical storage units made up of physical datafiles. Use UTIL O to see free and utilized space. Make sure you have at least 10% free space in each tablespace or a minimum of 2 GB – the larger of the two. Use UTIL O in case you need to add datafiles to a tablespace.

Refer to the **UTIL O** chapter of the *Aleph 20 System Administration Guide* for complete details.

2.2 Database Temporary Tables

The Aleph application creates and uses Oracle tables for temporary data. Certain tables need to be cleaned periodically by using UTIL A.

See the UTIL A (util a/12 – a/16) chapter of the *Aleph 20 System Administration Guide* for complete details.

In addition, there is a temporary container library called `vir01`. Clean this library at least once a week by using the script `$aleph_proc/clear_vir01`. Many sites run the script as part of their post backup procedure or as part of their cleanup script. Run the script when the application is not active.

3 Archive Log Mode

In Oracle, all transaction made to the database are saved in special files called redo logs. These redo logs function in a cyclic manner. When all redo logs are full, the first one is reused and its original content is overwritten. Archive log mode is a mechanism designed to preserve all the redo log contents. When in archive log mode, all redo log files are saved to a designated directory. The purpose of saving these files is so that they can be applied to the database in case a recovery needs to be performed.

In order to ensure the smooth operation of the system, enough disk space must be available at all times for the archived redo logs. Make sure that the archive directory is on a disk with enough space for several days of work. The archived redo logs can be deleted only after they are backed up. By deleting the backed up archive files, free space is made available for the new files being created.

It is crucial to activate the archive mechanism prior to switching to production. If archive log mode is deactivated for some reason, you must immediately perform a full database backup when archive log mode is reactivated.

4 Backup

Sufficient backup of the application components is crucial for performing a database recovery. Customers are recommended to use third-party tools and/or custom-made scripts to handle their backups. It is important to understand the components of the application before dealing with backup methodology.

> **Note**:
>
> For Aleph 20, Ex Libris offers a backup package. Oracle – backups are now done with RMAN, an Oracle utility. The new Ex Libris Backup Package is intended for installations that do not have other backup methods in place for Aleph. In general, large installations tend to have robust backup infrastructure in place and do not need the new Ex Libris Backup Package.
>
> You do not need to use the Ex Libris Backup Package if you back up Aleph using other means.
>
> For further information, see the document *Ex Libris Backup Package*.

5 Components to Back Up

5.1 Database

Backing up the database datafiles is also known as a physical backup. There are two types of database backup: cold and hot.

5.1.1 Cold Backup

All the database files are backed up to tape or disk while the database is down. The list of database files to back up is taken from the database data dictionary before the database is shut down. The database (and Aleph) is down while the backup is being performed, thus no library activities can be held during this time.

> **Note**:
> Complete recovery of the database can always be done to the point the backup was done. In order to bring the database to the point prior to the failure, all archive files that were generated from the time of the backup until the time of the failure must be available.

5.1.2 Hot Backup

All database files (except redo log files) are backed up to tape or disk while the database continues running. Hot backups can be done only if the database is in archive log mode. The list of database files to back up is taken from the database data dictionary. The database (and Aleph) continues with normal operation while the backup is being performed, thus normal library activity can be held during this time. Do not run large batch jobs during the course of the hot backup.

> **Note**:
> Recovery from hot backups can only be done if archive files exist. Assuming all archive files are available and in sequence, the recovery is until the time prior to the failure.

5.2 Archive Files

Archived redo log files are backed up to tape or disk.

> **Note**:
> When recovering from hot backups, archive files must be used in order to enable the recovery. When recovering from cold backups, archive files may be used to minimize data loss and to affect a recovery until the point prior to the failure.

5.3 Data

Backing up the data of an Oracle database is also known as a logical backup.

Oracle tables contents are extracted to disk and are backed up to tape or disk. This can be done using Oracle export utility or via sequential dump.

5.4 Software

5.4.1 Aleph Software

Back up the Aleph application software to tape or disk.

5.4.2 Oracle Software

Back up the Oracle application software to tape or disk.

5.5 Site Configuration

Before the backup can be performed, the site must be configured.

To configure the site:

1. Back up the file structure of the libraries including exported data.
2. Back up the alephe directory that contains global configuration for all site specific libraries.

> **Note**:
> Aleph backup can be done with or without export (see below).

6 Backup Strategy

Once you understand the components of the database, how they are modified, and how often, you can set up a backup plan. With the exception of the Oracle database, the other components are basically directories and files. The more frequently they are backed up, the more up-to-date any data recovered is in the event of a crash. This reduces the chance of data loss to a minimum.

As mentioned above, there are two types of backup – physical and logical. Physical backup means backing up the database files. Logical backup means backing up the data extracted from the database tables. Physical backup can be done in one of two methods – cold and hot. Cold backup is done while the database is closed. Hot backup is done while the database is open. A hot backup can run only when the database is running in archive log mode.

Cold backup has an advantage over the hot backup in that a database can be recovered from a cold backup as it was at the time of the backup with no need for additional files. If there are archived redo logs after the time the cold backup was taken, they can be applied. By applying these archived redo logs, the database can be brought up to date with minimum data loss, if any at all. The hot backup must be restored together with the archived redo logs in order to synchronize the database. Recovery from a hot backup itself without archived redo logs is not possible.

The following backup policy is recommended:

- Cold – unless downtime is a major issue, this can run daily
- Hot – any day that cold is not run
- Archive – run daily
- Application configuration – run daily
- Export – as frequently as possible
- Aleph application – once every two months and after each upgrade or patch
- Oracle application – once every two months and after each upgrade or patch

See **Appendix A: Backup Strategy Guidelines** on page **12** for strategy guidelines.

7 Disk Cleanup

File systems tend to fill up with temporary files, logs, and various other material that can be deleted periodically. The system administrator should take precautions to avoid the file systems from reaching full or very high capacity.

Perform cleanup after backup and not before.

Refer to the **UTIL X** chapter of the *System Administrator's Guide – System Overview* for complete details.

7.1 Application

The following are a few areas that require cleanup: `$TMPDIR`, `$LOGDIR`, `$alephe_scratch`, and libraries' scratch/print directories.

7.2 Apache Logs

Large Apache logs can cause slowness in Web activity. The apache log directory has two basic log files: `error_log` and `access_log`. These files continually increase in size and need to be deleted periodically. There are two basic options:

- Stop the apache, delete the logs, and restart apache.
- Use the `rotatelogs` mechanism to limit the maximum file size or the time interval that the files are updated.

7.3 Oracle Logs

Trace files and the alert log are generated by Oracle under the directory `$ORACLE_BASE/diag/rdbms/$ORACLE_SID/$ORACLE_SID`. Under this directory, the following sub-directories can be found and may be cleaned from time to time:

- `alert` – a new alert directory for the plain text and XML versions of the alert log.
- `incident` – a directory for the incident packaging software.
- `incpkg` – A directory for packaging an incident into a bundle.
- `trace` – background processes traces and the alert log and user traces. (A replacement for the ancient background dump (`bdump`) and user dump (`udump`) destinations)
- `cdump` – core dump directory.

8 Review Oracle Alert Log

8.1 Oracle Trace Files and the Alert Log

When one of the server or background Oracle processes detects an error, it dumps information about the error to a trace file.

In Oracle Database 11*g*, the alert log is written in XML format. For the sake of compatibility with older tools, the traditional alert log is also available in the ADR Home directory under the trace directory mentioned in section 7.3 Oracle Logs on page 9 (See details in section 8.2 Oracle ADR on page 10 on ADR). The alert logs under the directory: `$ORACLE_BASE/diag/rdbms/$ORACLE_SID/$ORACLE_SID/alert` are in XML format.

As described above, for the sake of compatibility, each database also has an `alert_<sid>.log` file. The alert file of a database is a chronological log of messages and errors. Messages include information about administrative operations done on the database, tablespace, and rollback segments and errors such as a lack of database space. These traces are placed under the directory `$ORACLE_BASE/diag/rdbms/$ORACLE_SID/$ORACLE_SID/trace`. In addition UTIL O can be used to review the alert log.

Refer to the **UTIL O** chapter of the *Aleph 20 System Administration Guide* for complete details.

8.2 Oracle ADR

A special repository, named ADR (Automatic Diagnostic Repository) is automatically maintained by Oracle 11g to hold diagnostic information about critical error events. ADRCI Utility is a command line tool that enables you to view diagnostic data. To use the ADRCI Utility, go to the command prompt and type ADRCI. To see the alert, type SHOW ALERT.

For more information, see Chapter 8 *Managing Diagnostic Data* of the *Oracle Database Administration Guide.*

9 Recovery Policy

Recovery from system crashes is a very complex issue and requires deep knowledge and extensive expertise. As a policy, it is in the best interest of both the customer and Ex Libris for the customer to consult Ex Libris Support in any case involving database recovery. There are various reasons for this approach:

- Any given problem may have more than one solution. By consulting Ex Libris, the customer can expect to receive a wide range of solutions.
- Ex Libris has global support for Oracle and has a close relationship with Oracle. Ex Libris discusses and analyzes every crash scenario with Oracle before presenting the solution to the customer.

- Ex Libris has experienced DBAs who can offer suitable solutions taking into account application perspectives.

In case of a database crash, take the following steps:

1. Contact Ex Libris Support by CRM/PRB and by phone or mail.
2. If the crash is detected while the database is up, DO NOT shut down the database. This may cause the crash to be irreversible. In addition, although the database is corrupt, some critical information may be retrieved that is essential for recovery.
3. It is critical to backup the corrupt database "as is," while the database is inaccessible, to enable multiple solution attempts.
4. Discuss the crash and status with Ex Libris personnel. Make sure to review what backups were done, the symptoms of the crash, and any log or additional information relevant to the situation.
5. Send the Oracle alert log and trace files to Ex Libris Support.
6. Prepare any media that may be necessary for recovery (for example, backup tapes).

Appendix A: Backup Strategy Guidelines

As a rule, the more frequently that backups are made, the less the likelihood of data loss. As described in this document, we differentiate between backing up the database as files (physical backup) or as extracted data from the database tables (logical backup). In addition, there are directories and files that are not related to the database that require backup as well (for example, the library structure).

The ultimate backup strategy would be to run a cold backup of the database daily (including the archived redo logs) and a backup of the site configuration (alephe and libraries with their exported data) on a daily bases. This would mean that in case a recovery becomes necessary, it can be done from the previous night's backup.

For sites that cannot afford to run a cold backup each night for downtime reasons, hot backup should run each night that cold backup cannot be run. This also will enable recovery from the previous night's backup.

Sites that cannot run a full backup each night (cold nor hot) should do their utmost to set the time intervals between full backups to a minimum. For these sites, the role of the archived redo logs is critical for restoring a full backup done several nights before the crash and reapplying transactions to bring the database up-to-date. It is important to stress that to perform hot backups you MUST have archived redo logs regardless of the frequency that the hot backup is run.

Regarding the site configuration, the ability to restore an up-to-date file depends on the frequency the backup is taken. The library `tab` directory is probably the directory with the most modifications. Since the `tab` directory does not take up much disk space, a specific backup of this directory can be taken more often than others.

In addition to performing a backup, the backup tapes must be read to check their validity. Run a listing of a full backup tape at least once a week. Besides verifying that the tape is okay as far as the media is concerned, check the listing and make sure all expected directories and files are backed up. Do not take any backup mechanism for granted.

Backup Strategy Examples

Here is a chart with examples of backup strategies and their abbreviations. It is important to make sure you are familiar with all the components and that you have a comprehensive backup methodology.

C.A.S.E. – Cold + Archived redo logs + Site configuration + Export
H.A.S.E. - Hot + Archived redo logs + Site configuration + Export
A.S.E. - Archived redo logs + Site configuration + Export
T.V. – Tape Validity check
B.I. – Backup Integrity check

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Weekly
C.A.S.E.	C.A.S.E.	C.A.S.E.	C.A.S.E.	C.A.S.E.			T.V. + B.I.
C.A.S.E.	H.A.S.E.	C.A.S.E.	H.A.S.E.	C.A.S.E.			T.V. + B.I.
A.S.E.	H.A.S.E.	A.S.E.	A.S.E.	C.A.S.E.			T.V. + B.I.

Appendix B: Summary of Periodic Maintenance Activities

Activity	Recommended Time Interval	Method
Clean file system space	Weekly or more frequently (as needed).	Online using UTIL X or by script after backup.
Ensure free database space	Weekly.	UTIL O/14.
Delete temporary database tables	Weekly.	UTIL A.
Clear vir01 container.	Weekly.	Use the script $aleph_proc/clear_vir01
Backup database	Varies per site. See Appendix A for recommendations.	Third-party tool or customer's script.
Backup site configuration	Varies per site. See Appendix A for recommendations.	Third-party tool or customer's script.
Backup software	Once monthly or after each upgrade.	Third-party tool or customer's script.
Review backup media	Weekly.	Third-party tool or customer's script.