Backup and Recovery Procedure LAIS

Date
November 23, 2013

Author(s)
VAN DER KRIEKE, Piet; STALKNECHT, Wilko
# Table of contents

1. Introduction .......................................................................................................................... 3
2. Integrated Backup .................................................................................................................. 4
3. Integrated Backup Procedure .................................................................................................. 5
   3.1 Standard procedure ............................................................................................................. 5
   3.2 Procedure in case of a change of the content of one of the databases ........................................ 5
   3.3 Procedure in case of a change of the tables of the databases ................................................... 5
4. Back-up Schedule .................................................................................................................... 6
5. Continuity management .......................................................................................................... 7
6. Restore procedure ................................................................................................................... 8
1 Introduction

This document shows the required Backup and Restore procedures for the integrated LAIS system. The LAIS system has several components and where the components are integrated, based on the content of the different databases, it’s a requirement that the data will always be consistent.

Normally the software will take care for the consistency of the data but there are some cases that might cause that there is an inconsistency in one of the databases that requires the recovery of the database. This cause can be an error in the software or an error in the disks that contains the data.

Normally the hard disk should have the ability to restore the data by the redundancy in itself but there are cases in which this fails.

Starting point of view is that in the present situation, backups are already made from the data and that it’s also possible to restore these data.
2 Integrated Backup

Database backups

The Integrated LAIS system consists of an amount of components. First the component maintaining and using the data will be mentioned.

1. the Arc GIS database (SQL-server)
2. the LAIS Administrative database (postgresql)
3. the LAIS Administrative Documents Database (postgresql)
4. the Scanned Documents share environment
5. the Aero photo server

The first three environments should be always in sync. The three different environments communicate through web services and if a transaction in one of the systems can’t be done, the transaction will be rolled back in the other system. So in the daily use, the system parts will be in sync.

There is only a need for an integrated backup in the case that one of the databases becomes corrupt through whatever cause and there is a need for one of the databases to be restored. In that case, also the other databases have to be restored to the same situation.

System backup.

For the case that the hardware, on which the software is running, will crash, a system backup is needed and should be available for a restore, to make sure that a quick installation of the entire system can be done on new or repaired hardware.
3 Integrated Backup Procedure

3.1 Standard procedure
If a backup should be made, no user access is allowed to the systems. It will not be a problem if a user should still work but it will frustrate the users if the systems are stopped while they are still working.
Advised is to
- do the backup always on the same time (time has to be communicated)
- Do the backup after the normal office hours and warn the user half an hour before the closing of the systems
Procedure
- All three systems has to be stopped
- Backup has to be made according to the backup schedule
- Make systems available for use

3.2 Procedure in case of a change of the content of one of the databases
If the content of one the databases is made through a procedure that makes the changes straight in the database without a transaction mode, a backup should be made before the task is executed and also a backup should be made after the execution of the task.
The content of the database should be checked before the systems are made available for the users.

3.3 Procedure in case of a change of the tables of the databases
In the case that a change in the software, also requires a change in the database from one of the tables in the database and may be some of the data should be initially filled, there is a need for backups, but there is also a relation with the implemented software version.
It depends on how the software is developed how to handle.
- If the software is developed in the way that it can handle both versions of the database, the software has to be implemented first and if it works well, the database changes can be made (see 3.2)
- If the software is developed in the way that only the old version can work with the old version of the database and the new version of the software can only work with the new version of the database, the same procedure as mentioned in 3.1 and 3.2 has to be followed, but in case the system doesn’t work well, not only the backup of the database has to be restored, also the old version of the software has to be installed again.
4 Back-up Schedule

An industry standard for the backup schedules is the Grandfather, Father, Son schema. The servers perform back-ups in the Grandfather\(\text{}/\)Father\(\text{}/\)Son rotation schema:

<table>
<thead>
<tr>
<th>Set</th>
<th>Frequency</th>
<th>Type</th>
<th>Overwritten At</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grandfather</td>
<td>Monthly</td>
<td>Full Back-up</td>
<td>overwritten every 13th Month</td>
</tr>
<tr>
<td>Father</td>
<td>Weekly</td>
<td>Full Back-up</td>
<td>overwritten every 6th Week</td>
</tr>
<tr>
<td>Son</td>
<td>Daily</td>
<td>Full Back-up</td>
<td>overwritten every 8th day</td>
</tr>
</tbody>
</table>

Consequently the grandfather set consists of twelve (12) media devices, the father set consists of five (5) media devices and the Son set consists of four (4) media devices on each server. Twenty-one (21) tapes are employed in the schema on each backup server.

**Media Rotation**

Backup to disk volumes (B2D) from the Son set are used to perform back-ups every night Monday through Thursday. A tape from the Father set is used for the Weekly backup (Friday) and a tape from the Grandfather set is used on the first business day on or after the last business day of every month. A Grandfather back-up supersedes and replaces either a Son or Father back-up.

Example: The last day of the month falls on a Saturday. The grandfather tape is run on the next business day, Monday. The usually Monday DLT, a selection from the Son set, is skipped for that week.

This schema can be used as a basic, but there can be chosen for an incremental backup, that only keeps the changes from a day and the choice can be made to keep the monthly backups only for two months. The decisions are based on risk management.

**Media.**

Initially the backup can be done on a disk environment, that makes it easy and fast to recover, but older backups can be removed to tape.
5 Continuity management

If the backups are stored on the same hardware / disk as the databases are running, in case of a crash all information will be lost. The first requirement is;
- to separate the backup from the place where the original information is stored.

If the backup is stored in the same building as the original data, in case of a collapse of the building or a fire in the data centre, all information will be lost. The second requirement is
- to store the backups outside the building in a secured place.

Based on risk management has to be decided how often backups should be brought outside.

The most solid solution is the situation that a backup is made straight to disks in another building.
6 Restore procedure

If something is wrong with the data due to whatever reason, the users have to stop the data entry and all the systems should be stopped. The management of the RNRA should be involved in this kind of incidents, because it can have a big impact on the business side and they have to be one of the decision makers to select a solution.

An investigation should be done to find the reason.

- If it’s caused by a change of the application (software) first the software should be changed again, to make sure that it will not happen again.
- A risk evaluation should be made, to see if only a small part of the data is affected or if the whole database is corrupt. Based on the outcome of the risk evaluation, the next actions should be taken.
  - If only the data of a small amount of parcels is affected and the errors can be traced and solved, the software should be changed and the database should be changed for the affected parcels and the systems can be brought up again.
  - If it’s caused by a hardware failure it might be possible to solve it by adjustment or replacement of hardware.
  - If just one of the databases is corrupt and it’s not possible to solve it through the hardware, an investigation has to be done to figure out which backup has to be used to solve the issue.

Attention points for a restore.

It must be very clear that if the database has to be restored, all the transactions that have been done after the backup was made, should be done again by the users. It might even affect the printing of certificates, so that must be all taken into consideration when a decision should be made about restore.

For GIS, if the transactions have to be done again, it will not be sure that the numbers of the parcels will be given in the same order. Only if all the transactions in the same cell are handled in the same order and also in the transactions the parcels are created in the same order.

So a restore will only be done if there is no other way to get out of trouble. Required is that the business management knows about the complications for the business.

Restore in case of an incremental backup

If a database has to be restored from a point in time for which an incremental backup is available, first the original backup should be restored and then the following incremental backups.