Creating a Technical Disaster Recovery Implementation Plan (TDRIP)

Arjen Visser
Avisit Solutions Limited
Creators of Dbvisit – Protection Recovery Continuity
Introducing myself – Arjen Visser
Founder and CEO of Avisit Solutions Limited in New Zealand.

The creators of:
**Dbvisit** – Standby Database Technology (Data Guard alternative)
*Leading software solution providing Oracle Disaster Recovery.*

Dbvisit is used world-wide. Customers and sectors include:
- Kellogg’s
- Alcatel-Lucent
- Oklahoma State Bureau of Investigation
- New York Blood Centre
- Banking/Financials industry
- Healthcare
- Government and City Councils
- Manufacturing

See [www.dbvisit.com](http://www.dbvisit.com) for more information.
How important is Disaster Recovery to your business?

43% of US businesses never reopen again after a disaster and a further 29% close within 2 years. (*)

93% of companies that suffer significant data loss are out of business within 5 years. (**) 

(* US Small Business administration)  
(** US Bureau of Labor)
What is it?
A Technical Disaster Recovery Implementation Plan (TDRIP) is a plan of the actual implementation of the hardware and software at the disaster recovery location.

Why?
This plan ensures there are no unforeseen surprises when building the disaster recovery solution and that all critical systems and their components have been accounted for.

How?
This paper will show how to create a TDRIP plan. This paper focuses mainly on Oracle centric applications in Unix/Linux environment.
Disaster Recovery project time line:

- Technical Disaster Recovery Implementation Plan comes at the end of the planning phase.
- Technical Disaster Recovery Implementation Plan is part of the Disaster Recovery plan.
What happens without a plan?

“And I did it without any technical plans.”
What is a Disaster?

- Complete or partial loss of a data center or service for an extended period of time.
  - Earthquake.
  - Flood (Global warming).
  - Tsunami.
  - Fire.
  - Power failure.
  - Hurricane.
  - Pandemics (Swine flu threats).
  - Disgruntled employee for getting back at you for firing them.
  - Human induced disaster (Newbie DBA meant backup not delete!).
What is Disaster Recovery (DR)?

- Is not High Availability
- Is not Business Continuity
- Is not operational recovery
- Is not an offsite backup

**Disaster Recovery** is:
- Process to restore operations critical to the resumption of business after a natural or human-induced disaster
What is the best location of the DR site?

- DR site could be your current primary site.
  This ensures staff are onsite when disaster strikes.

- What should be the distance between two sites?
  Should be geographically different locations.

- DR is not just about systems, also about people, buildings and processes.
  Will you or your staff be available when disaster strikes?
  Ensure you do not take things for granted like cell phones.
Prerequisites required for TDRIP:

- High level business disaster recovery plan
- Key metrics of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are defined
- Identified mission critical systems
- Standby hardware budget
- Standby location
- Top priority with backing from Senior Management

RTO – Maximum amount of time before systems are up and running again. How long before business is operational again.

RPO – Maximum amount of data loss (measured in time) acceptable in the event of a disaster. How much data can we afford to loose without serious impact to the business.
Mission critical systems:

DR systems and methodology identified by business needs.

<table>
<thead>
<tr>
<th>Tier</th>
<th>RPO</th>
<th>RTO</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>No dataloss</td>
<td>&lt;30 min</td>
<td>$$$$$$$$$$$</td>
</tr>
<tr>
<td>II</td>
<td>&lt; 30 min</td>
<td>&lt; 1 hour</td>
<td>$$$</td>
</tr>
<tr>
<td>III</td>
<td>24+ hours</td>
<td>48+ hours</td>
<td>$</td>
</tr>
<tr>
<td>IV</td>
<td>7+ days</td>
<td>3+ days</td>
<td>$</td>
</tr>
</tbody>
</table>

An RTO/RPO of more than 24 hours means that backup may be sufficient for DR. An RTO/RPO of less than 24 hours requires some kind of replication. Normal backups are not good enough anymore.
Assumptions for Disaster Recovery Implementation

1. Asynchronous replication (not synchronous)
2. Host based replication (not array or fabric based)
Technical Disaster Recovery Implementation Plan

8 Steps to creating the TDRIP:
1. Technical register of applications and servers
2. Application consistency groups
3. Server mapping
4. Configuration register for each primary server including OS, patches, firewall rules, etc.
5. Software licenses and media register
6. Oracle standby database implementation
7. Host Replication methodology
8. Best practice primary servers and standby servers
Step 1 - Technical register of applications and servers

What servers (and components) should be included in the disaster recovery plan?

Map the critical systems identified in the business disaster recovery plan to actual servers and components of servers

<table>
<thead>
<tr>
<th>System</th>
<th>Software component</th>
<th>Server</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Data Warehouse</td>
<td>Oracle database - SALESPP</td>
<td>avisit012</td>
<td>950G</td>
</tr>
<tr>
<td></td>
<td>Oracle Warehouse Builder Repository – OWBREP</td>
<td>avisit013</td>
<td>20G</td>
</tr>
<tr>
<td></td>
<td>Reporting application server</td>
<td>avisit022</td>
<td>2G</td>
</tr>
<tr>
<td></td>
<td>Web server</td>
<td>avisit034</td>
<td>3G</td>
</tr>
<tr>
<td></td>
<td>Source data system</td>
<td>avisit067</td>
<td>120G</td>
</tr>
<tr>
<td>CRM system</td>
<td>Oracle database – CRM01P</td>
<td>avisit320</td>
<td>550G</td>
</tr>
<tr>
<td></td>
<td>Web server</td>
<td>avisit034</td>
<td>15G</td>
</tr>
</tbody>
</table>
Step 2 - Application consistency groups

Application is not just one server and one database
• Feeds in and out
• Multiple servers

May need to replicate the systems at the exact same point in time to avoid inconsistencies and incomplete processes.

<table>
<thead>
<tr>
<th>System</th>
<th>Software component</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Data Warehouse</td>
<td>Oracle database - SALESP</td>
<td>avisit012</td>
</tr>
<tr>
<td></td>
<td>Oracle Warehouse Builder Repository – OWBREP</td>
<td>avisit013</td>
</tr>
<tr>
<td></td>
<td>Reporting application server</td>
<td>avisit022</td>
</tr>
<tr>
<td></td>
<td>Web server</td>
<td>avisit034</td>
</tr>
<tr>
<td>CRM system</td>
<td>Oracle database – CRM01P</td>
<td>avisit320</td>
</tr>
<tr>
<td></td>
<td>Web server</td>
<td>avisit034</td>
</tr>
</tbody>
</table>
Step 3 - Server Mapping (One to one mapping)

Each primary server has a corresponding standby server.
Step 3 - Server Mapping (Many to one mapping)

Primary servers are consolidated on the standby site
Step 3 - Server Mapping (One to one virtual mapping)

Each primary server has a corresponding virtual standby server.
### Step 3 – Comparing Server Mappings

<table>
<thead>
<tr>
<th>Mapping</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>One to one</td>
<td>• Easiest to implement</td>
<td>• Hardware cost is highest</td>
</tr>
<tr>
<td></td>
<td>• Easiest to administer</td>
<td>• More hardware to maintain</td>
</tr>
<tr>
<td>Many to one</td>
<td>Hardware can be consolidated</td>
<td>Conflicts may arise:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Software conflicts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User ID (UID) conflicts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Group ID (GID) conflicts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mount point conflicts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuration conflicts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Port conflicts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Patch conflicts</td>
</tr>
<tr>
<td>One to one virtual</td>
<td>Hardware can be consolidated</td>
<td>• Not all platforms can be virtualised together.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Introduces a new layer to the standby platform</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• New backup methods needed as VM are backuped</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtualisation not ideal for databases.</td>
</tr>
</tbody>
</table>
Step 4 – Configuration register

For all primary servers included in the disaster recovery plan.
Aim is to identify the components that are needed and to make a checklist to ensure nothing is left out when building the standby servers.
The configuration register should be split into the following categories:
• Servers
• Application Software
• Oracle Databases

This configuration register is a good starting point to get an idea of the scope involved in building the standby servers.
Step 4 – Configuration register (Servers)

List servers with all the following information for each server:

1. Operating Systems, version, level and patches
2. Server software installations that will be needed at the standby servers. This could be monitoring tools, utilities, etc.
3. User ID number (UID) of the Unix/Linux accounts that will be needed at the standby servers
4. Ports that are needed by the specific software
5. Printer configurations on the server that are needed at the disaster recovery site
6. Mount points that are used by the specific software
7. Important configuration files (smb.conf, sshd_config etc)
8. Firewall rules
Step 4 – Configuration register (Application Software)

List the application software that is needed at the standby site and for each software list the following:

1. Name of software, version, level and patches
2. Installation directory
3. Mount points used
4. Important configuration files
Step 4 – Configuration register (Oracle Databases)

List databases with the following information for each database:
1. Listener port(s) and network configurations
2. Oracle software installation directory
3. Location of Oracle networking files
4. Oracle version and patches
5. Mount points used by databases
6. Oracle admin/trace directories
7. Others (utl_file_dir etc)
Step 5 – Software licenses and media register

**Media:**
- Identify the software media needed to build the standby servers.
- Ensure all media and patches are available if software cannot be copied from primary server.

**Licenses:**
- Ensure standby servers software licenses have been purchased or are accounted for.
- Ensure standby databases are fully licensed.
Step 6 – Oracle standby database implementation

Oracle replication methods:
1. Physical standby database (using redo or archive logs)
2. Logical standby database (using SQL and LogMiner)
3. Oracle replication (using triggers or streams)

Methods to keep physical standby database up to date:
1. Dbvisit (used world-wide [www.dbvisit.com](http://www.dbvisit.com))
2. Data Guard (Enterprise Edition needed)
3. Home grown scripts (robust enough?)

Make sure your Oracle replication method is not your weakest link.
Step 7 – Host Replication methodology

Assume asynchronous and host based replication

**One Master:**

Ensure any changes to the primary servers are also replicated to the standby servers. This includes:

- New users and passwords
- Changes to configuration files
- New or updated printers
- User files

**Synchronising methods:**

- rsync
- rdist
- Commercial software
Step 8 – Best practice primary servers
(to avoid conflicts when standby servers are consolidated)

Primary servers:
1. Assign range of port numbers that only this server may use
2. Assign range of UID (and GID) that only this server may use. Or have global UID and GID.
3. Pre-fix all non standard mountpoints with a unique identifier for the server to ensure no conflicts when consolidated. (Example: /oradata01 should be /s23-oradata01)
4. Ensure you consider DR site on your change control
Step 8 (ii) – Best practice standby servers

Keep the same layout as on the primary servers – You will make your life a lot easier!

Standby servers:
1. Keep the user UID the same as on primary server.
2. Keep GID the same as on primary server.
3. Keep mount points the same as on the primary server.
4. Keep port numbers the same as on the primary server.
5. Keep the layout of database the same.
Summary Technical Disaster Recovery Implementation Plan

8 Steps of TDRIP:
1. Technical register of applications and servers
2. Application consistency groups
3. Server mapping
4. Configuration register for each primary server including OS, patches, firewall rules, etc.
5. Software licenses and media register
6. Oracle standby database implementation
7. Host Replication methodology
8. Best practice primary servers and standby servers
Conclusion

Create a plan to be prepared.

And finally….

>>Test your DR plan regularly<<
End of presentation

Thank you

www.dbvisit.com
At the heart of Oracle Disaster Recovery

Oracle is a registered trademark of Oracle Corporation. Dbvisit is a registered trademark of Avisit Solutions Limited.