Running Head: DATABASE DR

Database Disaster Recovery Planning

Jered McClure
Walden University

Database Disaster Recovery Planning

Ensuring database uptime is the primary concern for a DBA, and as such, disaster recovery (DR) planning should be taken quite seriously when it comes to protecting systems data integrity. Therefore, appropriate planning and implementation of a full scale DR solution should be readily available and up-to-date at all times. This solution should outline every aspect of restoring the database and data to full operational state, from scratch. Additionally, it should be written in such a way that any staff member should be able to implement it in the event of no IT personnel being available.

Systems availability begins with localized recovery methods and expands outwards into offsite and backup site recovery options. Localized recovery is those methods which utilize readily available hardware and software in the database’s physical location. These can be backed up SAN storage sitting in RAID 10, shadow copies of current data for constant data protection, on site tape libraries for “day-of” restores, physical copies of all software installation files on optical disks, and physical copies of all licensing keys (Klebanoff, 2009). Additionally, all database control files and tablespaces should be multiplexed across multiple directories with archiving turned on (Poweel & McCullough-Dieter, 2010). This will ensure that in the event of a single, or even multiple, hard disk failures, the database can be restored on site with very little down time.

Offsite backups start with storage of all backup tapes in a remote location. This is usually done through a security agency whose job is to protect valuable sensitive information and/or capital. In Australia, Chubb security offer a backup tape storage and retrieval service, along with IT networking security consultation and/or installation (Chubb, 2013). Because these tapes are taken every 24 hours, it ensures that in the event of a disaster that destroys all local data, only 24 hours will be lost on the overall system. While this may not be a perfect solution, it is better than a total failure without restoration capabilities.

The next level of offsite storage is backing up the database through a cloud storage service, such as that offered by TAS Managed Services (TAS Managed Services, 2013). Essentially, the database and all systems are hosted on the TAS systems. TAS then manages and maintains a localized disaster recovery procedure for all hardware and hosted applications. The database would still need to be backed up and maintained at an organizational access point (e.g. the main company headquarters), if only to ensure data availability in the event of the hosted solution going under. Alternatively to hosting the database through TAS is to simply host the DR solution through their cloud, thereby having a readily available fully functional solution running in a 2N capacity (e.g. local and remote).

Finally, an offsite secondary backup facility can be maintained as a last resort all-or-nothing approach. If localized restores and offsite restores completely fail, then the backup site becomes the new primary facility in the event of a disaster. This secondary facility should be located far enough away that environmental disasters do not have a sweep effect taking out both facilities. This secondary facility will have just enough hardware and software resources to bring the database and/or systems back to operational capability, although usually in a limited function. At this point, systems operation is the key focus over any other concern.

Once all the above is decided upon, documentation of the entire DR solution must be managed and maintained. The individuals responsible for this document should also be part of the change advisory board so as to be aware of any alterations to systems which would require a change to the DR plan. All information pertaining to the DR plan will be kept in this document, such that, any individual who is available to identify and report a disaster is able to follow all procedures, in full. This necessitates basic language and/or pictures to facilitate an expedient recovery.

Database Restore from Cloud Backup

The following is an example to outline how the database can be recovered from scratch. It is assumed that a localized disaster has forced data to be taken from cloud-backup, to restore at n minus one hour, since backups are synced at hourly intervals. Hardware is still functional, only data is lost. Additionally, this is more generalized than what is required for a full DR plan. Finally, the restore will be done using Oracle’s Recovery Manager (RMAN) application (Poweel & McCullough-Dieter, 2010) (Vembu Technologies Pvt. Ltd, 2012):

1. Reinstall Oracle database using offsite application software and licensing, following standardized install procedures from the DR plan.
2. Once the database is installed and operational, ensure that the SID of the database is correct.
	1. SET ORACLE\_SID = ORCL
		1. Note that the database SID may be different than ORCL
3. Connect RMAN to the target database where the restore will be loaded.
	1. RMAN TARGET /
4. The database will now need to be restarted from inside RMAN in order to mount the backed up control file.
	1. SHUTDOWN IMMEDIATE;
	2. STARTUP NOMOUNT
	3. RESTORE CONTROLFILE FROM ‘<<NETWORK DRIVE>>\<<ORACLE\_BACKUP>>\control\CONTROL\_nn.ctl’
		1. Note that all bracketed fields will be specific to the backup location for each DR solution.
		2. The “nn” in the CONTROL\_nn.ctl stands for the control file number from which the database will be restored.
5. The new/old control file will contain the information needed to mount the database from backup. Therefore, RMAN can now mount the database.
	1. SQL “ALTER DATABASE MOUNT”;
6. It is now time to restore and recover the database from the backed up data files located in the cloud backup solution.
	1. RESTORE DATABASE;
	2. RECOVER DATABASE;

Notes about this restore methodology. This requires that RMAN be setup, scheduled, and running. There is no sense in having a database without its primary recovery solution in operational capacity. Additionally, all backup files should themselves be backed up in redundancy. This ensures that while RMAN is doing its job, the hard files are still available in the event of a total disaster.

Reference

Chubb. (2013). *IT Network.* Retrieved July 11, 2013, from Chubb Security: http://www.chubb.com.au/utcfs/Templates/Pages/Template-54/0,8063,pageId%3D7045%26siteId%3D582,00.html

Klebanoff, J. (2009, September). End-to-End High Availability and Disaster Recovery. *System iNews*, 35-40.

Poweel, G., & McCullough-Dieter, C. (2010). *Oracle 10G: database Administrator: Implementation & Administration.* Boston: Cengage Learning.

TAS Managed Services. (2013). *Home*. Retrieved May 10, 2013, from TAS Managed Services: http://www.tasol.com.au/index.html

Vembu Technologies Pvt. Ltd. (2012). *Restore Oracle Database*. Retrieved July 11, 2013, from Storegrid: http://storegrid.vembu.com/online-backup/help/PageHelp/oracle-restore-config.html