Backup restore best practices

Technology

A backup practice is the process of creating new copies of data which serve to restore the original important ones in an event of data loss. A best practice is a technique or methodology of achieving a certain objective, which through practice and experience, has reliably proven to generate the desired results. A redundant hardware is one in which the primary system is guarded from failures and errors by the provision of multiple components which are used interchangeably.

This paper will therefore focus on some of the best backup practices in use and also determine whether a good backup strategy is better than a redundant hardware. A number of backup practices are employed to ensure a reliable way of recovering data some of which are elucidated below. Developing backup and restore plans and testing them is a major milestone in ensuring that all the stored data is secure. Planning on when, where, and how data is stored and backups performed is critical in quick recovery after a disaster strikes (Amini, Peiris, & Khnaser, 2006).

Training of personnel on backup and restore procedures can never be overlooked. Basically, this depends on the level of security of the network system in which such roles are assigned to members of the Administrator’s group for high security networks while for minimum and medium security situations, other staff members can be thoroughly trained. Both the storage devices such as tape drives and storage media such as tapes and disks should be highly secured so as to use them together with computer backups in case of data loss as long as one has administrative privileges for their access.

One should always opt to create a backup log, print it and store it in order to assist in locating specific files if the drive or system fails (Amini, Peiris, & Khnaser, 2006). A good backup strategy is only reliable if the knowledge of data recovery is not held by only a single person since this can lead to trouble in case of breakdown of the IT system and the person is not available.

According to Schonig & Geschwinde, if the people working with a system have redundant knowledge about how it works and what should be done in case offailure, it does not help no matter how redundant and reliable the IT system is (2002). A redundant hardware still does not save the situation in case of fire or any other disaster and especially if both the backup and the original data are all stored in the same location. In such as case everything ends up being destroyed in which case the data is lost and cannot be retrieved.

Where only the most recent backup is available, something might go amiss in the system unnoticed resulting in errors and difficulties in data recovery. Therefore, a redundant hardware is greatly advantageous only if a good backup strategy is constantly adopted by ensuring that the best backup or restore practices are in place. References Amini, R. , Peiris, C. , & Khnaser, E. N. (2006). How to Cheat at Designing Security for a Windows Server 2003 Network. Boston: Syngress. Schonig, H. , & Geschwinde, E. (2002). PostgreSQL develloper's handbook. St. Louis: Sams Publishing.