Business Continuity Based on Backup

Ghazi K. AL-Abed
Middle East University Amman, Jordan
g8g@hotmail.it
Hebah H. O. Nasereddin
Middle East University Amman, Jordan
hebah66@hotmail.com

Abstract. This paper will be discussing Backup procedures and how crucial they are for business continuity. In addition discuss the different types of backups and go in depth in some of them. Furthermore refer to the importance of Data Backup and how companies who do backup their data are always on top of things and there business is never stopped. Data Backup has been a very important step throughout all the major global companies and is being implemented heavily which in return requires us to take it into consideration.

Keywords: Continuity of Business, COB, Backup, Protection, Off-site backup, Hardware & software backup, disaster.

1 INTRODUCTION

Business continuity is a plan which is structured to keep an organization up and running in case of a disaster occurring. This approach will help ensure the long-term survival of the organization. Business Continuity is essential to all companies, small companies as well as larger corporations. Plans need to be clear, concise and customized to the needs of the business. Business Continuity planning should become part of the structure that the organizations are built on. It is better to plan for incidents, which may affect your business, rather than having to "catch up" when a problem occurs.
The importance of having a business continuity plan in place: Survival, revealing inefficiency, Boosting staff morale, better communication, increased value, negotiation tool and relaxation:

- *Survival*
  The fact of putting together a plan and testing it just in case a disaster happens and coping with the disaster is better than going into a phase where the company might vanish completely.
- *Revealing inefficiency*
  A business under threat can be viewed like a patient on an operating table. The priorities are clear: maintain the cash flow, communication links and at all costs protect the staff and premises. Business continuity planning starts with a thorough analysis of the business to decide which parts are vital.
- *Boosting staff morale*
  To find and keep excellent staff you need to inspire confidence and maintain loyalty. When something goes wrong they expect the business to have a plan and to cope. In return they will give you their best efforts.
- *Better communication*
  Business continuity plan relies upon communication able to give the right person who can fix the problem the right info, at the right time to help in business survival in case of a disaster. Also, give the ability to keep talking to customers, suppliers and staff even when the company is in its worst condition.

- *Increased value*
  A business that will cope with whatever comes upon it at it is a more valuable and reliable investment than others. Ensure this is factored in when asking your bank manager for a loan, when selling some equity or dealing with the new owner when you have decided to sell up and relax.
- *Negotiation tool*
  Understanding the principles of business continuity means you can spot weaknesses in other businesses. If your main supplier is asking for a price increases ask about their business continuity plans.
- *Relaxation*
  While other business people lie awake at night, you can rest easy knowing your business continuity plan is ready.

2 BACKUP

Backing-up is a crucial process that everyone should do in order to have a fail-safe, when the inevitable happens. The principle is to make copies of particular data in order to use those copies for restoring the information if a failure occurs (a data loss event due to deletion, corruption, theft, viruses etc.). You can perform the backup manually by copying the data to a different location, or automatically using a backup program. [6]

2.1 Data backup

To schedule backup between servers, the servers must be able to connect to each other in order to update data. A connection needs to be setup between the machines in order for them to be able to communicate with each other replicate (Copy/mirror/sync) data. As users add, edit, and delete documents on a server, the data may contain slightly different information until the next time the servers replicate. Because replication transfers only changes to a database, the network traffic, server time, and connection costs are kept to a minimum.

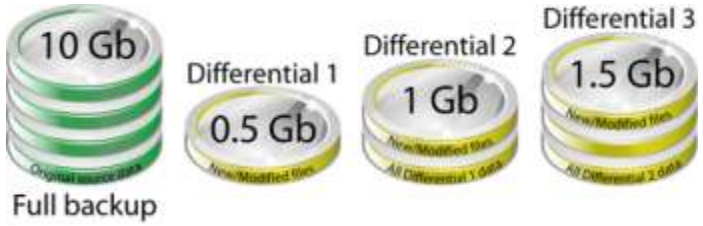
2.1.1 Types of data backup

Each program has its own approach in executing the backup, but there are four common backup types implemented and generally used in most of these programs:

- *Full backup*
  Full backup is the starting point for all other types of backup and contains all the data in the folders and files that are selected to be backed up. Because full backup stores all files and folders, frequent full backups result in faster and simpler restore operations. Remember that when you choose other backup types, restore jobs may take longer. As an example, for a full backup job that runs four times. Fig. 1 is conclusive on how the backed up data will grow with every run.

Full Backup, Fig. 1
Note: Full Backup will always back-up the entire source data. If you don't delete/exclude sources (only add/modified) it will always grow in size because it back up everything.

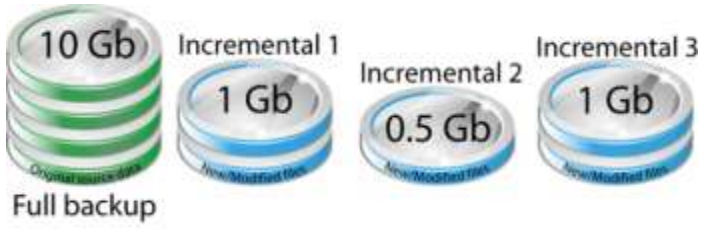
- *Differential backup*
  Differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup. Fig.2 shows an example on how a differential backup would look like for a backup job that runs four times.



Differential Backup, Fig. 2
Note: Each differential backup includes all new/modified files since the last full backup.

- *Incremental backup*

Incremental backup stores all files that have changed since the last FULL, DIFFERENTIAL OR INCREMENTAL backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup must be processed, which could result in a lengthy restore job. Fig. 3 shows how a backup job running four times would look like when using incremental.

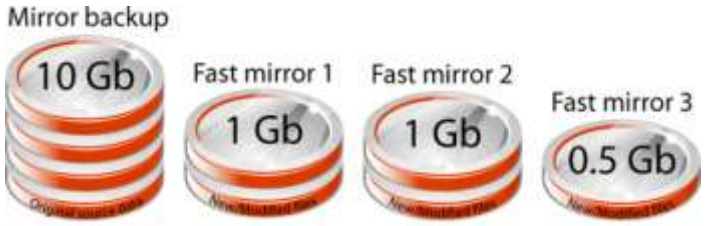


Incremental Backup, Fig. 3
Note: Each incremental contains only the new/modified files since the last backup (no matter what type).

- *Mirror backup*

Mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the source data. It has the benefit that the

backup files can also be readily accessed using tools like Windows Explorer. Fig. 4 shows how a mirror backup job would look after four times (first mirror will back-up everything, subsequent fast mirror backups will back-up only new/modified files).



Mirror Backup, Fig. 4
Note: First time when it runs, mirror backup will back-up everything without archiving. After that only new/modified files.

Table 1. Provides an overview comparison between these backup types

Table 1. Data backup types.

Backup type	Data backed up	Backup time	Restore time	Storage space
Full backup	All data	Slowest	Fast	High
Incremental backup (Recommended)	Only new/modified files/folders	Fast	Moderate	Lowest
Differential backup	All data since last full	Moderate	Fast	Moderate
Mirror backup	Only new/modified files/folders	Fastest	Fastest	Fastest

2.1.2 Data and file Protection

Data and file protection is another aspect that has to be taken into consideration. There are several sequences of procedure that need to be conducted based on the type data which requires protection.

Paper records and files containing personal data should be handled in such a way as to restrict access only to those persons with business reasons to access them. This should involve the operation of a policy whereby paper files containing such data are locked away when not required. Consideration should also be given to logging access to paper files containing such data and information items. Personal and sensitive information held on paper must be kept hidden from callers to offices.

Secure disposal of confidential waste should be in place and properly used. If third parties are employed to carry out such disposal, they must contractually agree to the Department's data protection procedures and ensure that the confidentiality of all personal data is protected.

Standard unencrypted email should never be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a secure email facility which will encrypt the data being sent. The strongest encryption methods available should be used. Departments should also ensure that such email is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key

management costs, particular attention should be paid to any central solutions put in place for this purpose.

2.3 Hardware and Software backup

Furthermore it is very crucial to identify which software applications and the hardware is required in case of disaster recovery. An offsite location needs to be prepared in case something happens and it needs to be ready to function at anytime. The primary hardware which is located in the main site needs to be reimaged at the offsite location in order to keep the daily/weekly functions running no matter what happens.
Ensuring that copies of program software are available to enable re-installation on replacement equipment is also crucial. Prioritize hardware and software restoration is a must.
Also another aspect that concerns this topic is having backup internet links. After investigation it is recommended that an organization must have different internet links from a couple of vendors. Of course these links will not be active at once, one of them will stay on standby and will run automatically if the primary link goes down. It often happens that the vendor is upgrading, running maintenance or even having technical difficulties. It is a recommended step in business continuity if the financial part is approved and if the data is highly critical to the organization.

2.4 Off-Site Backup

Off-site backup and data protection is sometimes required due to the fact that a huge catastrophe occurs. At times an offsite location is recommended to be located on different shores and in a peaceful location. What is meant by peaceful is a location where no political or economical problems are forecasted to happen. The important files from the servers and computers are securely uploaded to a data center and can be retrieved if needed to restore them. It's critical to backup important information to an off-site location in case of disaster. Disaster can come in many forms such as a natural disaster, a hard drive crash, electrical surge or accidental deletion. With your data being backed up in an offsite, they will be protected from any disaster that could damage or destroy the information.

3 CONCLUSION

Business Continuity is an essential part of any business. Planning it should occur as soon as the business is assembled. This paper discusses plenty of details regarding a lot of topics but not all of them are required to be implemented in the plan. A lot of the steps above can be simplified depending on the size of the organization and the amount of data available and how critical it is. The required is only what's needs to be implemented and also keep an eye out from a financial perspective. But at the end, our data needs to be protected, backed up and have it on hand no matter what happens. Because business is built on data and without it business won't continue.

References

F. D. Mu˜noz, H. Decker, (October 2007)
J. E. Armend´ariz, J. R. Gonz´alez de Mend´ıvil Rui Fan and Nancy Lynch ,(August 2003)
200 Technology Square, Cambridge, MA USA 02139
Somerset Local Authorities' (March 2009) Civil Contingencies Partnership.

Greater Manchester Local Authority Business Continuity Group (December). http://www.salford.gov.uk/d/gm-bc-leaflet1.pdf
CMOD Department of Finance (December 2008).
Stephen Belshaw (8 SEPTEMBER 2008).
Roland DuBeau (Apr 10, 2011)
IBM Corporation (August 14, 2008)
FEMA (October 2012)
Microsoft article ID: 136621 – (November, 2006) - Revision: 1.1 , published under Q136621
Softland, achieved (August 2007) the Microsoft Certified Partner status with an ISV/Software Solutions Competency.
IBM Tivoli Storage Manager (Augest 2010) Version 6.1 information center.
Derek Slater (December 13, 2012) CSO , http://www.csoonline.com/article/204450/business-continuity-and-disaster-recovery-planning-the-basics