Black Box Backup System

Iyad Aldasouqi *iyad@rss.gov.jo*
Information Technology Center
Royal Scientific Society
Amman, 11941, Jordan

Arafat Awajan *awajan@psut.edu.jo*
The King Hussein School for Information Technology
Princess Sumaya University for Technology
Amman, 11941, Jordan

Abstract

Modern organizations from different sizes (Small, , Medium and Large) consider information as one of the most important of their assets that need to be secured against increasing number of threats. The importance of the information comes from its impacts on the main tasks performed by the organization. The evolution of Information Technology and Information Systems is changing permanently the characteristics and the components of such systems and the ways needed to protect them against any security risk.

Periodic data backup is a system administration task that has changed as new technologies have altered the fundamental structure of networks. These changes encourage rethinking of modern backup strategies and techniques. In addition, standard backup programs and specialized tools are often needed.

This paper provides an overview of issues to be considered for a long term, stable and secure backup system. A new approach (Hardware) called Black Box backup system is proposed based on current risk management plans and procedures used mainly in the aerospace industry.

Keywords: Black Box, Backup, Network Backup System, Mirroring, RAID

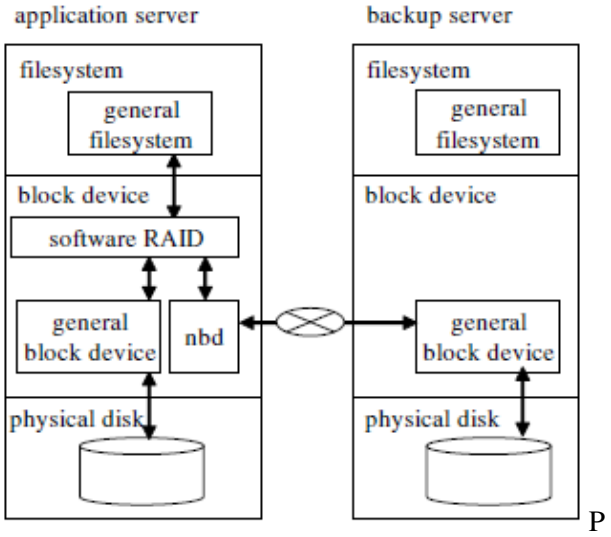
1. INTRODUCTION

Every organization tries to deliver value from information Technology (IT) while managing an increasingly complex range of IT-related risks. The best practice can help to avoid collisions, and reduce the occurrence of major IT risks, such as: project failures, security breaches, system crashes, and failures by service providers to meet the upon greed requirements. In addition, today's attacks aren't as likely threats never seen; therefore technologies which will be able to protect enterprise networks against these kinds of attacks should be chosen carefully and designed properly.

The purpose of this paper is to find and contribute in a stable secured back up system which can be resistant to any hazards, catastrophes, crises and natural disasters. The paper includes discussions on the features and limitations of the native backup and recovery available programs. It is hoped that the information presented here can help administrators consider tradeoffs in cost, performance, and reliability for different types of solutions. Furthermore, most of backing up techniques are utilizing for certain functions, such as the using of some techniques for backing up file-system e.g. In the snap shot backup, the technique which was LVM (Logical Volume Manager) and utilize the filesystem [1, 2].

Furthermore, backing up techniques have been used for the periodic backup, but cannot mirror data in real-time. In a real-time mirroring, RAID [3] has been frequently used to mirror data on a

local disk. The mirroring on a network has been often implemented as a function of the clustering system [4, 5]. Moreover, Network Block Device (NBD) makes a block device available on the network. The method to combine NBD with software RAID makes it possible to mirror on the network in real-time (Figure 1).



P

FIGURE 1: Conventional backup system with mirroring on device layer [20].

2. DATA BACKUPS SYSTEMS

Data backup is a necessary requirement for every organization. The well-known traditional reasons are system crash and disasters such as a flood and fire strike networks. Users may inadvertently delete files or overwrite existing files, hackers or disgruntled employees do the same purposely. Disk drives are inherently fragile devices. As a result, of that files become corrupted by bad disk sectors, magnetic fields, and improper system shutdown. In addition to the traditional threats, there are new threats such as thieves steal laptops, and the data contained on them. The threat posed by modern worms dwarfs those of older worms [6], and they are able to compromise every vulnerable machine on the Internet faster than any manual response can prevent [7].

Nowadays, organizations' computer and information systems are the most important assets and organizations depend on them more than ever; therefore, loss of data is more expensive than ever in terms of efforts spent and downtime and with increasing threats and increasing costs, backups are more crucial than ever.

Therefore, developing a backup strategy is needed for specific network, data, and organizational objectives (different strategies for different purposes). A survey of factors to consider is presented in [8]. It provides an excellent planning tool for developing backup strategies.

2.1. Properties of Good Backups

In a well-managed network, backup operations are performed on a regular predefined basis. Additionally, a good recovery system is essential. During both normal use and recovery, backup operations should be transparent to users. Backup operations should be automatic and not be the responsibility of users. Instead, a system administrator should centrally manage backup and recovery operations. Since backups are of high priority, they should be managed by a person who understands their importance, rather than a new hired or intern one.

Finally, the scale of modern networks is beyond what can be manually managed. Good management requires human intelligence supported by automated information gathering and management.

2.2. Methods Available for Data Backup and Recovery

Backup solutions can be divided into two major categories. The first category includes the native backup and recovery programs which backup volume data from file servers, also it is providing a backup application that is needed by data to achieve the goal of backup process.

The second category relies on file system. These categories take data from a file server in the same way that users access their data, which is very helpful in 24/7 environment.

2.3. Information storage strategies.

Having a data-backup-recovery strategy requires answering two questions:

1. How quickly must you recover the data before your business experiences serious setbacks?
2. How much are you willing to pay to implement a data-backup plan?

An organizations data should be backed up regularly on some type of removable medium, and then delivered to another location for protection purpose.

Other questions may be asked:

- How safe is the information in your computer?
- If a fire, flood, earthquake or even sabotage struck your office, would your electronic data survive?
- If you could access your data, how long would it take to get your information system up and running again?

To answer above questions, and to start designing such a strategy, we have to take into consideration two important issues:

- Downtime: How quickly must you recover the information before your business experiences serious setbacks?

- Cost: How much are you willing to pay to implement a data-backup plan?

While the questions are often difficult to answer, it is clear that large and small organizations need to prepare disaster-preparation strategies. We can conclude that faster recovery times equal lower downtime costs. However, strategies that speed recovery also can be expensive. This paper focuses on one area of disaster preparedness which is data backup.

2.4. Back up Practice / Cost

Storing the backed-up data in a secure place is called vaulting process, in which organizations copy computer files regularly on removable medium (Magnetic tape, CD or hard disk), and then delivered them to an off-site location for safekeeping. The timing of backups can vary depending on the organization's needs.

The off-site location called the renting a bank, with cost depending on the amount of space needed and its location. Another but the more expensive strategy is the redundant computer hardware, where if one component fails, a backup device keep the system running. An example of this approach is to use a technology known as redundant array of independent disks (RAID). There are many kinds of RAID systems, all of them designed to provide different levels of error recovery and fault tolerance.

One RAID choice is disk mirroring—a process in which data are simultaneously duplicated on one or more disks within the same system. The only additional hardware you need to set up a mirroring system is an additional disk drive that is the same size as your current drive. A typical 60-Gb drive, for example, costs about $200. For additional protection you also might consider buying a separate disk controller card for the new drive for around $80. The dual disk drive/controller card option results in a special type of mirroring protection called disk duplexing [9].

Another choice is disk striping; while there are many variations of striping, the most common is to set up an array of at least three and usually five disk drives. Disk striping does not store redundant data across the disk array; rather, it uses a system of parity checks—or hash totals—to rebuild lost data should one drive in the array fail. If you are running Windows NT Server, Windows 2000 Server or Novell NetWare, your computer is capable of handling disk mirroring and striping.[9]

If you are running your business on a single computer, it's easy to add a RAID configuration. However, if your business runs on two or more networked computers, a network administrator will be the responsible person to maintain the system.

3. OUR CONTRIBUTION

The idea of using Black Box Backup System (BBBS) came from Black box (as in figure 2) system used in aircraft. It is a generic term used to describe the computerized flight data recorders carried by modern commercial aircraft. This device is typically used in conjunction with a second black box known as the Cockpit Voice Recorder (CVR), which documents radio transmissions and sounds in the cockpit, such as the pilots' voices and engine noises. In the event of a mishap, the information stored in these black boxes can be used to help determining the cause of the accident.

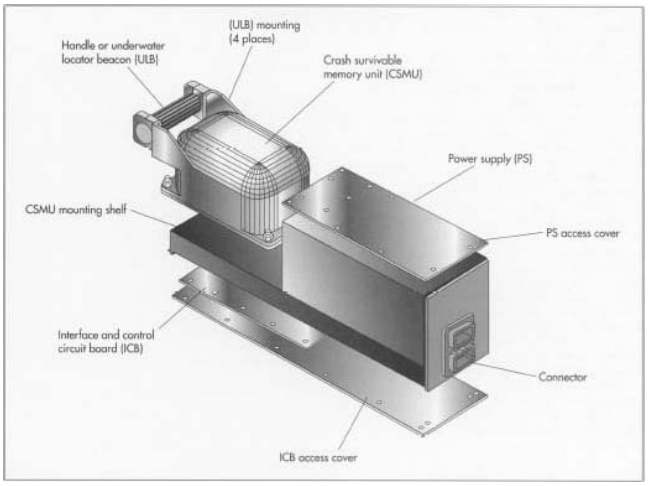


FIGURE 2: Black box model.

The proposed BBBS can be used in IT risk management plan, as a real time back up system which can be connected to a SCASI adapter or to Ethernet HUB, and it can depend on a separate processor (come up with processor) or used the server processor the most important feature is the possibility to use it against natural disasters (Like Earthquakes), water flood resistance and anti-fire. Therefore, we can be sure that availability, survivability and security issues are achieved, which can help saving all kinds of organization information assets with different sizes with reasonable cost.

3.1. Functionality

Storing data may uses several techniques such as a sniffer technique via the Ethernet adapter or regular backup technique with differential option and small time differences between backing up processes, or add sensing software to trigger the black box to start backup process. Therefore, when a crisis occurred (fire, earthquake or attack), the whole data can be recovered. This unit should be shielded and fixed to the ground. So this black box can be considered as a hybrid implementation technique; since it might be used for security and safety purposes.

Furthermore, early warning system can be used as an early warning system such as “Earthquake Monitoring System Using Ranger Seismometer Sensor” as in figure 3[10], which can forecast the occurrence of natural disasters 20 seconds in prior; so a small software program similar to the one used in Stream Processing Environmental Applications in Jordan Valley [11], that can receive the output of [10] and start shutdown the system before the disaster occurred as in figure 4.

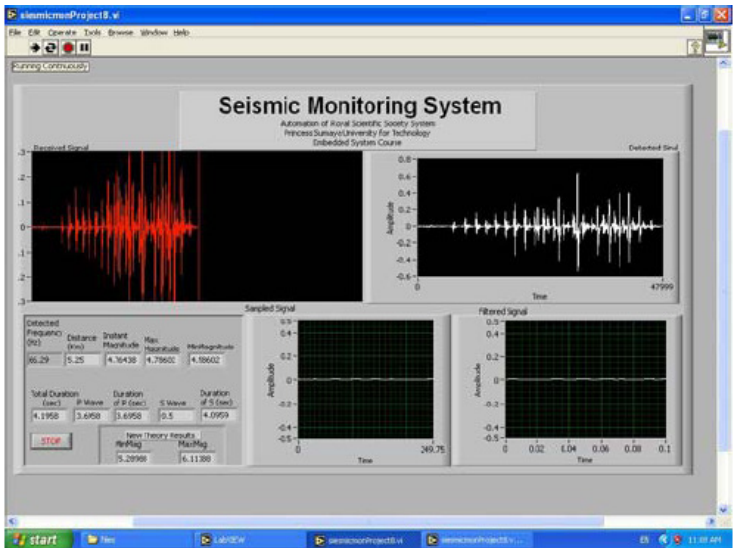


FIGURE 3: Early warning system

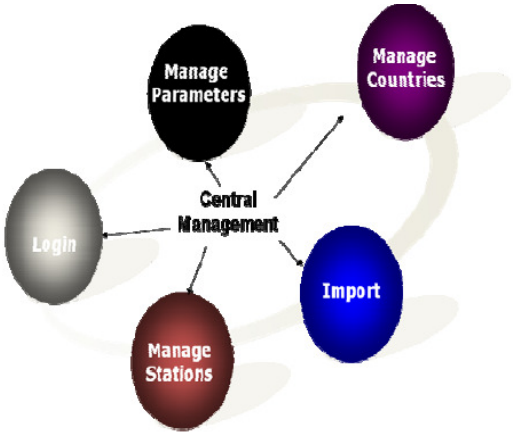


FIGURE 4: Stream processing architecture

In addition, the system used in Cluster-based scalable network services [4], can be send a statues update of the log files in addition to the control function to turn off services and shutdown the servers since it can talk with the hardware.

3.2. System block diagram

Figure 5 shows a general overview of the BBBS diagram and its position in the overall information security system.

The interior proposed black box consists of the eight following components [figure 6]:

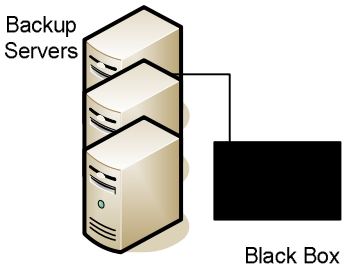


FIGURE 5: Black-Box overview.

a) Computer Interface Board (Data Acquisitions Card): it is a translator between the computer and machines or hardware as National Instruments products [19].
b) Audio Compressor Board: it is an audio recording system that is used to record any voice or movements around BBBS such as operators' discussion or thieves' talks.
c) High Temperature Insulation: it is a protection layer that can protect BBBS in case of fire occurred.
d) Stainless Steel Shell: it is another layer of protection to secure BBBS internal component from damage and tampering.
e) Under construction Locator Beacon: it is a device that gives a specific sound (like a buzzer or siren) to tell the rescue team about BBBS in case of a disaster occurred.
f) Stacked Memory Boards: it is the place where the data saved.
g) Memory Interface Cable: it is a cable that is used as a media between the storage area and the computer.
h) Acquisition Processor Board: it is a board similar to computer's motherboard that has different kind of interfaces to connect all BBBS components together.

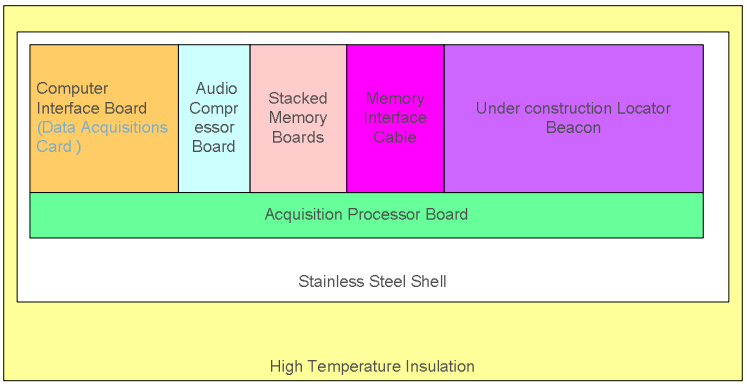


FIGURE 6: Suggested Black box block diagram

4. RELATED WORK

Backup and recovery systems are hot topics covered by many researches in the past and represent one of the most important security issues in the present. Theses research are based on different approaches varying from performance oriented, security oriented to accessibility oriented research. Our approach considers mainly the disaster recovery factor in addition to all other prospective.

A more comprehensive description of backup system issues and examples are in as in [12, 13]. Amanda (Advanced Maryland Automated Network Disk Archiver) is an early example of freely available backup management software [14, 15]. It uses a combination of full and incremental backups to concurrently backup networked clients to a single designated backup server and uses configuration files to determine the type of backup to perform. Multiple commercial systems [16,17, 18] now provide Amanda-like functionality; however, none deal gracefully with wireless hosts.

RAID [3] can protect systems against the failure of individual components. It provides no protection against unintentional/unauthorized modification of data, nor from catastrophic failure. Traditional RAID systems are impractical to field for mobile systems.

5. CONCLUSION AND FUTURE WORK

Most of backup strategies so far assume company data are located in easily identifiable and accessible places, but more of data are being stored on personal desktops, laptops and personal digital assistants, therefore dispersing important information into disparate isolated pockets. There are three basic users of data to be considered in this work: the central office worker, remote office staff member and the traveler. Office users and remote office should back up their files to local storage devices such as a CD, Zip or tape drives as well as to a network frequently.

The most important data are the organization databases and applications, which should be backed up almost every day or every moment; since it is the most important asset. Furthermore theses data should be located in at least in two different locations, and should be proceed and treated carefully using up to date secured techniques and technologies.

The strategy discussed in this paper is based on the use of a “Black box” model for conducting the backup activities and improving the disaster recovery planning in the organization. From that prospective, and since the components of the original black box were build based on IT technology, we suggest to implement this strategy in to save all kind of data and transactions including human being data.

As a future work, we suggest to start implementing and testing this system at Small Medium Enterprise (SME) organizations and to simulate via accepted estimating of the results comparing with traditional systems.

6. REFERENCES

[1] M. Rosenblum and J. K. Ousterhout. The design and implementation of a log-structured file system. ACM Trans. Comput. Syst., pages 26–52, 1992.

[2] S. Shim, W. Lee, and C. Park. An efficient snapshot technique for ext3 file system in linux 2.6. realtime linux foundation(RTLW), Nov. 2005.

[3] D. A. Patterson, G. Gibson, and R. H. Katz. A case for redundant arrays of inexpensive disks (raid). Proceedings of the 1988 ACM SIGMOD international conference on Management of data, pages 109–116, jun 1988.

[4] A. Fox, S. D. Gribble, Y. Chawathe, E. A. Brewer, and P. Gauthier. Cluster-based scalable network services. Symposium on Operating Systems Principles, pages 78–91, 1997.

[5] V. S. Pai, M. Aron, G. Banga, M. Svendsen, P. Druschel, W. Zwaenepoel, and E. Nahum. Locality-aware request distribution in cluster-based network servers. SIGOPS Oper. Syst. Rev., pages 205–216, 1998.

[6] Spafford, Eugene H., ‘‘An Analysis of the Internet Worm,’’ Proc. European Software Engineering Conference, September 1989.

[7] Staniford, Stuart, Vern Paxson, and Nicholas Weaver, "How to Own the Internet in Your Spare Time," USENIX Security Symposium, August 2002.

[8] Frisch, Æleen, Essential System Administration Third Edition, O'Reilly & Associates, 2002.

[9] www.adaptec.com

[10] Iyad Aldasouqi, Adnan Shaout, Earthquake Monitoring System Using Ranger Seismometer Sensor, INTERNATIONAL JOURNAL of GEOLOGY, Issue 1, Volume 3, 2009

[11] Iyad Aldasouqi, Jalal Atoum, Stream Processing Environmental Applications in Jordan Valley, Computer Science Journals, 2010.

[12] Preston, W. Curtis, Unix Backup and Recovery, O'Reilly and Associates, 1999.

[13] Frisch, Æleen, Essential System Administration Third Edition, O'Reilly & Associates, 2002.

[14] The AMANDA Homepage, http://www.amanda.org .

[15] da Silva, J., and O. Guomundsson, "The Amanda Network Backup Manager," Proceedings of the Seventh Large Installation Systems Administration Conference (LISA), November 1993.

[16] Dantz, Dantz Retrospect – Intelligent Backup and Restore, http://www.nwfusion.com/whitepapers/dantz/whitepaper.html , June 2004.

[17] IBM Software, IBM Storage Management Solutions, http://www.nasi.com/tivoli_backuprecovery.htm , 2004.

[18] Legato Software, Legato Networker, http://www. legato.com/products/networker/

[19] www.ni.com/dataacquisition/

[20] NISHIMURA Satoshi, SANO Mutsuo, IKEDA Katsuo, The design and implementation of an extensible network backup system in real-time, Proceeding ICUIMC '09 Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication