

Database Backup and Disaster Planning

Kali Charan Sabat

NMIMS Global Access School for Continuing Education, V. L. Mehta Road,
Vile Parle (W), Mumbai 400056 Maharashtra India
kalicharan330@gmail.com

Abstract - A database is an anthology of related data structured in a way that facilitates data search. A database is a collection of entities, attributes, records and tables. The data within the database must be effectively organized so that the data storage and information retrieval should be completely seamless. Robust backup of databases is required to meet consequences of unforeseen disasters.

Keywords: Databases, Backups, Disaster Planning

I. INTRODUCTION

DATABASE often house a company's mission-critical strategic, tactical and operational data. Therefore proper design, management and backup of data is critical. If proper database backup is managed, the database can be used to transform any amount of raw data into useful information and knowledge that could help the managers, employees and other stakeholders to do their jobs faster, better, and most cost effectively. This will ultimately help the customers and assist the organization to achieve its ultimate goal of profit maximization [1].

A database is an anthology of related data structured in a way that facilitates data search. A database is a collection of entities, attributes, records, and tables. Entities are things about which we collect data, such as products, customers, courses and people. Attributes are the individual bit-by-bit pieces of information about an entity, such as a product's identification code number, a person's last name that are stored in a database backup or records. A record is the group of related attributes about any entity. A table is a set of related records about an entity type. Each row in the table is a record and each column is an attribute [2].

The data within the database must be effectively organized so that the data storage and information retrieval should be completely seamless. That's where the need of a robust database backup system arises [3].

II. DATABASE BACKUP MODELS

There are two types of database backup models:

1. Cold database backup
2. Hot database backup.

Cold Database Backup: Also many times referred as offline database backup is performed when the database is closed or

offline. The data and information from a cold backup system is always steady, and thus results in easier retrieval than data and information from a hot database backup. However, the database will be unavailable during the cold backup process. And, for large databases, the cost of downtime may be too high to perform backup operations quite frequently.

Hot Database Backup: Also many times referred as online database backup allows the database to be online and available while the backup operation is performed. This backup operation allows database backup in parallel so a database does not need to be shut down anytime. Contrasting with the cold database backup model, the data in hot database backups will be more inconsistent and therefore requires appropriate redo log files to be applied after the restore operation to make the data consistent. This process is also known as database recovery.

For enhancing the above discussed traditional backup models, nowadays Storage Checkpoint technology is most commonly used. The Storage Checkpoint technology helps the traditional backup models in reducing the time taken for backup, reducing the quantity of backup media needed to be managed, and allows for a overall faster recovery. The key benefit of a cold database backup system is its consistency of the backup image. Whereas the major disadvantage is the downtime it requires for backup.

Adding Storage Checkpoint technology to cold backups retains the key advantage while virtually eliminating the major disadvantage of downtime. The major benefit of the Storage Checkpoint technology for hot database backup is faster recovery from hot backup images. Adding Storage Checkpoints significantly reduces time in the hot backup mode [4].

III. DISASTER PLANNING

Whenever somebody does shopping on the internet, he will always interact with a database at some point, whether he is aware of it or not. Typically, e-commerce sites store product, customer, or order information in databases.

The major protocol of the internet is TCP/IP (Transmission Control Protocol/ Internet Protocol), which handles website requests and e-mail traffic.

Databases however make far-reaching use of UDP (Used Datagram Protocol) packages, which are smaller than TCP packages, for purpose such as finding the right database on a company's database server. While the use of such UDP packages enable us to interact with e-commerce sites such as Amazon.com, Gap.com, etc, malicious UDPs nearly caused the Internet to crash in early 2003 [5].

A worm called Slammer used a single UDP packet to attack a server running an SQL database by using a security hole in Microsoft's SQL Server software. At this server, the code instructed the computers to randomly generate IP addresses of other computers and send out new Slammer packets.

Likewise, the same security hole existed in other Microsoft products as well, making them vulnerable to the attack and thus helping the Slammer worm to replicate at an uncontrolled speed, as every infected computer immediately started reproducing the worm. A personal computer could send out hundreds of copies of the Slammer worm each second via a broadband internet connection.

Nevertheless the UDP packets are very small; the traffic created was more than large parts of the internet could hold. For companies, this number could be as high as millions of Slammer packages each second.

The internet was affected all over world, and the virus also destroyed Seattle's 911 dispatching systems and cell phone services in South Korea, causing a total damage of \$ 1 Billion [5].

While there are many technical solutions for making the databases fast and easy, but at the same time, just one UDP packet using a single personal computer can almost knock out the entire internet if hacker knows how to identify and utilize security holes in databases and software packages. Thus companies should always maintain their own disaster management plans, so as to prevent their databases from such disasters.

Another very important aspect of disaster planning process is handling of trans-border data security and privacy. Other than technical and human resource related challenges, sometimes cultural issues may pose significant challenges for the organizations. One of the most important issues is regarding the general rules and regulations existing across nations regarding the information systems and trans-border data flow. For example, rules and regulations on trans-border data flow in the European Union Data Protection Directive limits how personal data may be used within the European Union countries.

Despite the fact that European Union countries have data

protection laws for a long time, the laws passed by the directive are very stringent. Contrary to the regulations in the United States, the directive suggests that personal data collected in Europe may be used for only the purposes for which it has been collected. For all other purposes, a consent form must be obtained from the customer. This directive has had severe implication for the airline industry, as Article 25 of the directive argues that no personal data can be transferred from Europe to countries that have less stringent privacy policies, including the United States. After the terrorist attacks of September 11, 2001, the United States under its disaster management action plan started demanding for detailed information, such as credit card information and meal preferences, about all US bound air travelers. Airlines can be fined up to six thousand dollars for not providing this information. However, complying with US demands would mean to violate Article 25 of the EU directive. According to the EU, it would be illegal to force airlines to comply with the US regulations.

While currently the US and the EU are in the process of negotiating this aspect of data protection, international corporations in other industry sectors are still struggling to comply with Article 25. In a move to gain a competitive advantage, many European companies are trying to outsource business process outsourcing (BPO) operations to countries such as India and Philippines. But the lack of adequate data security laws in most non-EU countries limits this possibility. Even though the data stays within the company, the mere fact that the BPO is located in a non- EU country may make the transfer of customer data unlawful [5]. And, with different data theft and misuse issues are in news in recent years at the off-shoring countries like India, Disaster planning has become more critical to the companies outsourcing their BPO operations to third world countries.

The importance of integration of Database backups and Disaster planning, and the impact if both are not effectively executed.

According to Jessup and Valacich [5], benefits of integrating disaster planning with Database backups include:

1. Will boost innovation and creativity in the organization.
2. Improved customer service, shorter product development cycles, and streamlined operations.
3. Will enhance employee retention.
4. Improved organizational performance.

Some challenges an organization may face if Database backups and Disaster planning are not in place [5]:

1. Getting employee buy-in.
2. Focusing too much on technology.
3. Forgetting the company Mission and goals.
4. Dealing with knowledge overload and obsolescence.

IV. REFERENCES

- [1]. J.A. Hoffer, M. B. Prescott and F. R. McFadden.. *Modern DatabaseManagement*,.6th ed. Upper Saddle River, NJ: Pearson Education, 2005.
- [2]. Craig S. Mullins. *Database Administration*. 2nd ed. Addison-Wesley Professional, 2013.
- [3]. A.C. Boynton and R. W. Zmud. An Assessment of Critical Success Factors. *In Management Information Systems*, ed. Gray, King, McLean, and Watson. 2nd ed. Fort Worth, TX: Dryden Press, 1994.
- [4]. Dorian Cougias, E. L. Heiberger and Karsten Koop. *The Backup Book: Disaster Recovery from Desktop to Data Center*. 3rd ed. Schaser-Vartan Books, 2003.
- [5]. L.M. Jessup and J. S. Valacich. *Information Systems Today. Why IS Matters*. 2nd ed. Pearson Education. Prentice Hall, 2006.



Kalicharan Sabat is working as an Assistant Professor at NMIMS Global Access School for Continuing Education, NMIMS University, Mumbai. Worked in industry for about 8 years in the areas of Project Management, Business Analytics, Quality Assurance, Supply chain Management, Process improvement, Production planning and control at various organizations such as Bharat Electronics, Air India, Google Geo, etc.

Carries 5 years of academic experience in the areas of Six Sigma, Total Quality Management, Project Management, Purchase & Negotiations Management, Operation Management, Supply Chain Management and Business Statistics. My Research interests are Sustainability, IT security, Analytics, Social responsibility, and Green supply chain management.