TELKOMNIKA, Vol. 11, No. 10, October 2013, pp. 6179 ~ 6186
ISSN: 2302-4046

The Design and Verification of Disaster Recovery Strategies in Cloud Disaster Recovery Center

Gang Li*[1,2], Qingpu Zhang [1], Wang Li [2], Zhengqian Feng [2]
[1]School of Management, Harbin Institute of Technology Harbin, 150006, China, +86-451-86403371
[2]Shandong Computer Science Center Jinan, 250014, China, +86-531-82605509
*Corresponding author, e-mail: lig@sdas.org

Abstract

Disaster recovery is an important means to ensure business continuity. However, the disaster recovery investment is so huge that the cloud disaster recovery becomes a best choice for enterprises, especially for SMEs. This paper discusses the necessity and importance of the cloud disaster recovery center and the vital indicators of disaster recovery by analyzing the classification and selecting principle of cloud disaster recovery strategy, developing disaster recovery strategy based on major disaster recovery strategy finally. In the end, this paper verifies the feasibility of the disaster recovery strategy by two specific cases of disaster recovery implementation.

Keywords: *cloud disaster recovery, disaster recovery strategy, design and verification*

1. Introduction

Informatization is an important driving force of social progress along with the progress of the society. Information is the core of informatization development and perfection as an important society strategic resource. Accordingly, the information data security and protection evolved into a major key issue to be solved in the national development strategies, moreover, which influence national overall situation and long-term interests. According to IDC, the disaster has happened to the company in the decade before 2000 in United States, 55% was closed down, and in the remaining 45%, there are 29% fail within two years because the data has been missed and to survive only 16% [1] [2]. Therefore, data security has become a key factor related to the smooth development of an enterprise or government. Similarly, information system has become a critical infrastructure of government agencies, enterprises and business development with the deepening of application of information technology in China. Security of business data plays a vital role in the operation of information systems [3]. The introduction of national standards “Disaster recovery specifications for information system"(GB/T 20988-2007) in 2007 provides that information systems disaster recovery should follow the basic requirements, marking the disaster recovery services towards standardization [4].

The construction of disaster center can be mainly divided into three patterns: First, self-built; second, cooperating with others; last, outsourcing mode. For most users, choosing the self-built or cooperating with others are just a desire, because of the construction of disaster recovery center has high demand for the financial and technical, and has huge one-time investment. The investment is prepared for small probability events, which are usually in an idle state, resulting in overall input costs and return on investment asymmetry, and low disaster recovery center resource utilization. Especially, self-built model is more than a good choice for small and medium-sized enterprises [5].

Establishing third-party disaster recovery center, and providing social, professional disaster recovery outsourcing services to various enterprises with emergency needs through the disaster recovery center, not only can save a lot of social costs, reduce repetitive construction investment, but also solve the lack of technology in disaster recovery for government and enterprises in a short time, thereby enhancing the industry-wide user disaster recovery capabilities [6]. With the development of cloud computing, cloud disaster recovery has become a trend. Cloud computing services are generally divided into SaaS, PaaS and IaaS [7].Cloud disaster recovery is a SaaS cloud computing service model, that is, the customer pay to use disaster recovery services, cloud computing center to provide disaster recovery [8]. Using this

Received April 19, 2013; Revised July 14, 2013; Accepted July 24, 2013

model, customers can take advantage of the superiority of technical resources, disaster recovery project experience and mature operational management process of the cloud computing center to achieve user's disaster recovery goals rapidly, reducing customer operation and maintenance costs and the intensity of work, while also reducing the total cost of the disaster recovery system [9].

Third-party cloud disaster recovery center construction is imperative, and its main task is to provide users with the choice of the disaster recovery strategy. The storage is the main carrier of the data, but storage vendors are differ in thousands ways. There is not only unified storage standard in the storage industry, but also each vendor's storage sui generis. Therefore, to be compatible with the user's storage is an important indicator for third-party cloud disaster recovery center and which needs to provide personalized services based on users. So the choice of disaster recovery strategy is particularly important.

2. An Important Indicator of Cloud Disaster Recovery Center

We need to clear a few important concepts of disaster recovery first before we design disaster recovery technical solution.

Disaster recovery capability: It refers to the ability to recovery timely and continuing to operate using disaster recovery resources and disaster recovery plans after the disaster. Disaster recovery capability is divided into six levels according to the Chinese national standard GB/T20988-2007 definition. Therefore, it needs to be able to meet the demand of 1-6 when it selects disaster recovery strategy [10] [11].

Data backup strategy: Data backup strategy refers to the determination of steps and actions in order to achieve data recovery and reconstruction objectives. It can be divided into specific data backup and operating system backup. Data backup refers to information data backup generated by the system running. It is critical business data, and changes in real time. Data can be backed up by the backup software, database software or storage hardware and it is the key point of data disaster [12]. Operating system data backup refers to the backup of system operation environment. Data backup of the operating system is simple relatively because the system running environment is almost unchanged [13].

Replication technology: It is the core technology of disaster recovery and it is also the main technical of the stored. We can achieve data backup between the primary data center and disaster recovery center through it and it is the basis to maintain data synchronization and remote disaster recovery. Replication technology is divided into synchronous and asynchronous replication [14].Replication technology refers to copying the local data to an offsite synchronized fully by software. Moreover, every local I/O transactions are required to wait for the confirmation of remote copy completion and then released. Asynchronous replication technology makes sure that the completion of basic operation to the local storage system before the update remote storage view. I/O operation provided by the local storage system to request mirrored host completes the confirmation information.

Data snapshots: Snapshot is also one of the key technologies of storage, and storage establishes a snapshot logical unit number and snapshot cache for the backup data through software disk subsystem scanning the date to be backed up quickly. At the same time, the storage copies data block which is about to be modified during the backup process to the snapshot cache when rapid scanning. Snapshot can extract the current online business data in real-time in the case of the user's normal business is not affected [15] [16].

RTO and RPO: There are two key measures in the process of disaster recovery: one is the RTO, another is the RPO [17].RTO（ Recovery Time Objective）refers to the time requirement from information systems or business function standstill to recovery after the disaster. It is embodied that how long system downtime can users stand for [2]. RPO（ Recovery Point Objective） refers to the request of time point system and data must be restored after the disaster. It is embodied that how long the data loss can the users be tolerated [18].Misuse can causes data update error or configuration error. What we concern is which time point can restore to the correct data in the end by misuse treatment [19].

What we introduce above is the key technologies and indicators of disaster recovery. Cloud disaster recovery center should focus on the consideration of these technologies and indicators in the design of disaster recovery strategy.

3. The Design Principle and Classification of Disaster Preparedness Strategies

The main feature of the cloud disaster recovery center is the integration of resources, and it provides personalized disaster recovery needs for different users, so we should give full play to the characteristics of the cloud disaster recovery center in terms of disaster recovery strategy design.

The first problem of cloud disaster recovery meet is compatibility issues, because the storage of different brands are compatible hardly, and sometimes the same brand of equipment are not compatible, resulting a lot of self-built disaster recovery system restricted by equipment brands completely [20]. Cloud disaster recovery center need to deal with multiple users who have different storage brands, so we must solve the problem of compatibility with different storage brands, but also solve the problem of limited of ours own brand. Therefore, the first principle is compatible with mainstream brands in design of disaster recovery strategy.

Cloud disaster recovery center is a professional disaster recovery provider to provide service for multiple users and it should meet the disaster recovery demand of different users. Therefore, the second principle is disaster recovery capability should satisfy the demand of standard grade 1 to grade 6 in design of disaster recovery strategy.

The most important indicators of disaster recovery strategy are RPO and RTO. The smaller the RPO and RTO is, the less the customers loss, of course, the greater disaster recovery invest. Users have all kinds of requirements, so not the higher parameters disaster recovery solution is best suited to the users. We should take full account of the user's status and affordability. Therefore, the third principle is achieving the highest investment returns for users in technology in design of disaster recovery strategy.

Cloud disaster recovery center is different from the self-built disaster recovery center, so the responsibility of the parties that need to be more clearly. And many users of the system are in the running state, we should try to avoid the changes of the user's system. Therefore, the fourth principle is to try to ensure the integrity of the original system and have well defined power and responsibility in design of disaster recovery strategy.

We need to classify the disaster recovery strategy to adapt to the needs of different users when determine the four principles in design of disaster recovery strategy. Generally, disaster recovery strategy is usually divided into file-level disaster recovery, data-level disaster recovery and application-level disaster recovery [17].

Application-level disaster recovery is building a set of same application system in the disaster recovery site to ensure the consistency of the system and data by replication technology. When disaster occurs, the system can be switched to the disaster recovery site in a very short period of time to ensure business continuity [4]. Data-level disaster recovery is backing up data system environment to disaster recovery system in real-time by replication technology. As long as the user's operating system has no problem, they can remote access to the data system of the disaster recovery center directly when a disaster occurs. It guarantees data system recovery in real-time and data integrity, but the operating system level runs after recovery by certain means [21]. File-level disaster recovery is backing up data to disaster recovery system by means such as backup software. It needs to restore data and operating systems in order to complete the restoration of the system when a disaster occurs.

Overall, RPO tends to zero, RTO tends to zero, and misuse can be restored for application-level disaster recovery. RPO tends to zero, RTO is in hour’s level, and misuse can be restored for data-level disaster recovery. RPO is in minute’s level or higher, RTO is in hour’s level or higher, and misuse can’t be restored for file-level disaster recovery.

4. The Design of Disaster Recovery Strategy

According to the classification of the above disaster recovery strategy design principles and disaster recovery strategies in cloud disaster recovery center, we analysis and design the disaster recovery strategy of cloud disaster recovery center about China.

4.1. The Choice of Network Environment

Due to the disaster recovery taking up a larger bandwidth capacity, so we prefer to select the bare optical fiber transmission in the network environment. Bare fiber optic transmission which is different from the internet of a fiber-optic network cost higher and can reach more than 1Gb transmission speed. As long as the disaster recovery center and user

access e-government network, the cost is very low relatively because China has completed the construction of the e-government network basically.

For these users who not access to e-government extranet, they can connect to the internet if there is a demand for disaster recovery. After all, laying bare fiber cost higher indeed. We need the VPN network and IPSec hardware encryption in order to guarantee the basic environmental safety. We need more than 100Mb/s accesses bandwidth in order to ensure the transmission bandwidth.

4.2. Analysis and Design of Disaster Recovery Strategies

We mainly select a disaster recovery strategy by researching all the disaster recovery strategy currently on the market and finally determine the disaster recovery strategy according to analyzing the design principles of the disaster recovery strategy.

As shown in Figure 1, this is all of the current disaster recovery strategy, and we were sorting in accordance with the file-level disaster recovery, data-level disaster recovery and application-level disaster recovery. Application-level disaster recovery strategy includes hot standby and virtual machine migration. Data-level disaster recovery strategy includes storage replication, volume management software, virtual storage and virtual gateway. File-level disaster recovery strategy includes remote mount, virtual tape library, backup software, cloud storage. Following we will analyze each strategies [22].

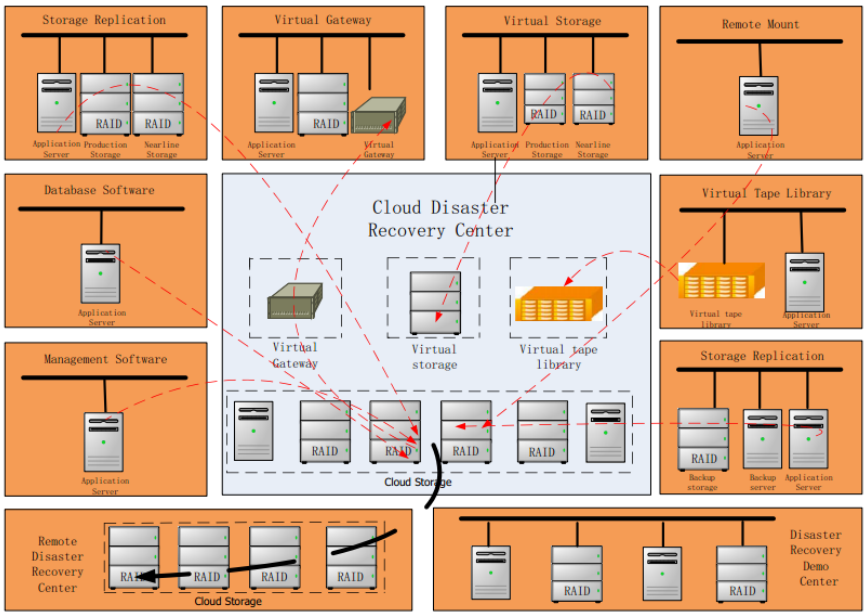

Figure 1. The disaster recovery strategy of disaster recovery center

4.2.1. The Selection of Application-Level Disaster Recovery Strategy

Hot Standby: It refers to hot standby based on two servers in the high availability system. In other words, configuring the same hardware and software environment in the disaster recovery center with production center to ensure the consistency of the system and data by synchronous or asynchronous replication technology [23] [24].This kind of disaster recovery strategy which requires a lot of investment is basically a double sets of equipment. However, there is certain market for high-end users. Consequently it can be used as one of disaster recovery strategy for cloud disaster recovery center.

Virtual Machine Migration: Virtual machine migration is a new technology in the development of cloud computing. Virtualization can guarantee the independence of the disaster recovery equipment. As a consequence virtual machine migration technology provides a convenient method for disaster recovery. Virtual machine migration which costs low will be the best disaster recovery strategy as long as the user using cloud computing technology. Therefore, the

migration of virtual machines can be used as one of the disaster recovery strategy for cloud disaster recovery center.

4.2.2. The Selection of Data-Level Disaster Recovery Strategy

Storage replication: Storage replication is directly implemented data disaster recovery using synchronous or asynchronous replication software. Storage replication is stability and high security despite the different storage brands are not compatible. Therefore, we strongly recommend using storage replication as disaster recovery strategy for users who use the same storage brand with disaster recovery center [25].

You can also use the storage replication backup strategy for the users of different brands of storage. The specific program is that client puts a low-end storage which is compatible with the storage of disaster recovery center, and realizes the storage replication between low-end of the storage and disaster recovery center. Production systems storage and low-end storage can use volume management software or backup software below-mentioned to achieve data synchronization because the transmission distance is relatively close. In this case, users only add a low-end storage which is relatively inexpensive (10T capacity needs about $ 10,000), and the user is relatively easy to accept. Specific disaster recovery strategy is shown in Figure 2.

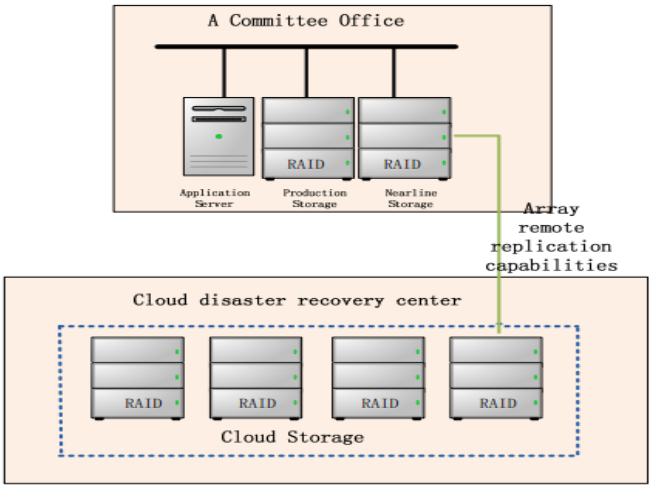

Figure 2. The disaster recovery strategy framework of storage replication

Volume management software: It is the real-time disk mirroring achieved by software shipped with the operating system. We use volume management software shipped with the operating system such as the LVM for Linux and Unix servers to achieve real-time the mirror of application data volume cloud disaster recovery array volume. And we recommend that achieving real-time mirroring use volume management software shipped with the operating system or dynamic disk management in windows platform for Windows servers. Volume management software is not suitable for remote disaster data transmission due to the high system requirements and taking up resources. So, volume management software is not suitable as a disaster recovery strategy alone. But it will be a good disaster recovery strategy if it combined with storage replication or remote mount.

Virtual storage: Virtual storage is concentrating multiple storage modules (such as disks, disk arrays) in a storage pool by certain means and unified management [26]. Although it is compatible with different brands of storage and ensures that the technical of the disaster recovery is feasible, it has two disadvantages. One is that it cost much more than the previously described near-line storage, the other one is that it needs the business system of users shut down and re-initialize. So it basically goes against the principle of selecting disaster recovery strategy in our cloud disaster recovery center and we would not adopt it.

Virtual Gateway: It transmits through VG bridging voice and corresponding signals among

multiple endpoints which are behind the same or different NAT or firewalls. It can be compatible with different brands of storage [27]. But there are also two disadvantages same as virtual storage. So we would not adopt it.

4.2.3. The Selection of File-Level Disaster Recovery Strategy

Remote mount: Remote mount is directly attaching disk of disaster recovery center to the production host at the system level using software shipped with the operating system. But remote mount is not usually using as a disaster recovery strategy alone because of higher requirements on the network and lower overall security. Typically, remote mount is used in conjunction with volume management software and disaster recovery software and provides service for the cloud disaster recovery center in common.

Virtual tape library: Virtual tape library is using hard disk to imitate the tape library functions when the hard disk storage cost drops to a certain extent. We don't accept it due to the high cost, limited security and less effective than other backup strategy.

Backup Software: It is directly backing up data to disaster recovery center using third-party software. Generally it is used in combination with remote mounted and remote storage replication, etc. in the cloud disaster recovery center rather than individual. Backup software is usually not used as disaster recovery strategy due to backup software provided by the user rather than the cloud disaster recovery center for the requirement of responsibilities clear[28].

Cloud storage: Cloud storage is a new technology developed from cloud computing technology. It is a system which collects a large number of different types of storage devices in the network through the application software to work together and to provide data storage and service access function in common. Cloud storage can be very good as a disaster recovery strategy for cloud disaster center combined with other strategy [9].

We can conclude that cloud disaster recovery center can use file-level backup strategy in allusion to the need of disaster recovery capacity of 1-2 grade in the national standard , that is, the remote mount and cloud storage technology based on IP storage meet the business applications which has less demanding business continuity. Cloud disaster recovery center can use data-grade-level backup strategy in allusion to the need of disaster recovery capacity of 3-5 grade, that is, it can provides a variety of solutions such as the storage layer replication, volume management software through replication, mirroring, virtualization technology. These solutions provide disaster recovery for critical data while ensuring the business continuity. Cloud disaster recovery center can use application-level backup strategy when the user puts forward business disaster recovery requirements that critical data loss tends to zero and business operation without interruption, that is, cloud disaster recovery center provides venues and assists the user to realize the request of level 6 with the solution of hot standby or virtual machine migration.

Therefore, cloud disaster recovery center can simplify the choice of disaster recovery technology for the user in a greater extent and meet the different disaster recovery level requirements to ensure grade 1 to grade 6 data recovery ability through mature, flexible and standardized solution.

5. Verification of Disaster Recovery Strategies

The data disaster recovery center is located in Jinan, Shandong, China, which is the professional third-party cloud disaster recovery center supported by provincial government and fully meets the requirements of disaster recovery. Verification of disaster recovery strategy is mainly in real environment validated of disaster recovery center.

5.1. Disaster Recovery Implementation of Rongcheng Education Department

Rongcheng is located in the east end of Shandong and the linear distance is 500 km with Jinan. The main is that Rongcheng education department has no access to the e-government network. So this test is mainly to verify the feasibility of disaster recovery software & remote mounts disaster recovery backup strategy and long-distance network environment. We finally choose the disaster recovery scheme based on IPsec &VPN as shown in figure 3.

Rongcheng department of education backs up data to the disaster recovery storage of professional disaster recovery center in Shandong province by VPN & Ipsec using Acronis Backup & Recover 11 software and restores data from the storage of professional disaster recovery center of Shandong province to itself using backup software after the disaster.

This project was implemented in April 2012 and completed after a week. The test time was end in October 2012. Rongcheng education department and data disaster recovery center of Shandong province realized data transmission through VPN ,and made transmission speed reached to 3 MB / s using IPsec protocol, and ultimately backed up data to off-site storage by the backup software. After testing, data was security available. Specifically, the remote transmission rate was 3.3M/s in average for these files (such as video files) which occupy a larger space and connect better. The remote transmission rate was 2.5M/s in average for these files (such as installation files) which occupy small space and has poor continuity.

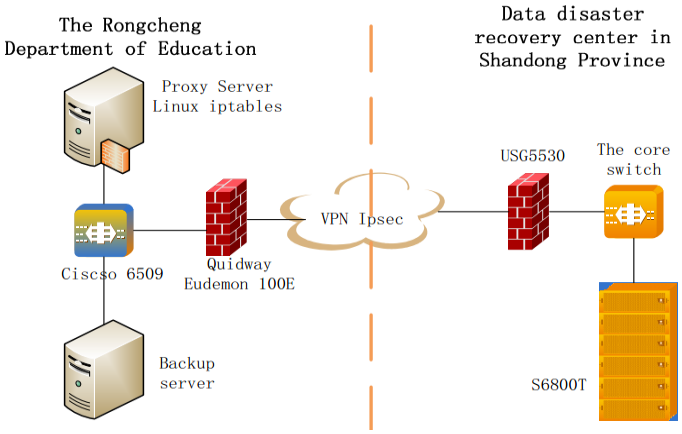

Figure 3. Rongcheng disaster recovery scheme

5.2. Disaster recovery implementation of Lixia education department

Lixia district is located in Jinan, Shandong and the linear distance is only 10 km with disaster recovery center. The user has access to e-government network and what is more, the series storage of user is same with storage of disaster recovery center. So this test is mainly to verify the disaster recovery backup strategy of storage replication and the feasibility of fiber-optic network disaster recovery.

We chose storage replication as disaster recovery scheme. Lixia education department lays bare fiber with data disaster recovery center through the e-government network and the linear distance is 10km; Lixia education department purchases switches and matching of single-mode optical modules and connects to the SAN network of professional disaster recovery center; Lixia education department backs up data stored to professional disaster recovery center through asynchronous remote replication.

This project was implemented in May 2012 and completed after a week. The test time was end in November 2012. This scheme realizes the interworking between Lixia education department and data disaster recovery center by using E-government network optical fiber. Its copy speeds is up to138MB/s in average, and fully meet the demand of the asynchronous remote replication. We have verified the effectiveness of the disaster recovery scheme and the security of data through nearly six months operation.

6. Conclusions and Outlook

This paper analyses cloud disaster recovery technology and the major existing disaster recovery strategies, combining with the selecting principle of cloud disaster recovery strategy, developing disaster recovery strategy for cloud disaster recovery center according to the needs of users. This paper verified the feasibility of a disaster recovery strategy developed by specific cases. Next, we will further analysis and improve disaster recovery strategy have developed to promote the development of third-party cloud disaster recovery center in China.

References

[1] Xie jun. Network Date Back Technology Research. *NETWORK AND COMMUNICATION.* 2012; (22): 63-64.
[2] Zhang hua, Xu juan. A Survey on Disaster Backup and Recovery Techniques. *Journal of YiBin University.* 2012; 12(6): 88-96.
[3] Liang Hailing. Building Disaster Recovery Backup System and Ensuring the Enterprise's Date Security. *Applied Technology*. 2010; (16): 94-95.
[4] Wu Qibin, Zhou Chunlei & Liu Yandong & Jia Wenjue. Review of Disaster Backup and Recovery Technology for Information Systems. *Land and Resources Informatization*. 2011; (1): 12-15.
[5] Dennis C Guster, Olivia F Lee. Enhancing the Disaster Recovery Plan through Virtualization. *Journal of Information Technology Research*. 2011: 18-40.
[6] Zhang Yan, Li Zhoujun & He Dequan. A Survey on Disaster Backup and Recovery Techniques. *COMPUTER ENGENEERING & SCIENCE.* 2005; 27(2): 107-110.
[7] Vijaykumar Javaraiah. ANTS2011-Backup for cloud and disaster recovery for consumers and SMBs.
[8] Kang Dongming, Wu Jianguo & Yu Weiwei. Design and Implementation of a Service Oriented Disaster Backup and Recovery Platform. *COMPUTER ENGINEERING & SCIENCE*. 2011; 33(4): 145-149.
[9] Yao Wenbin. System-Level Management Problems in Cloud Disaster Backup and Recovery. *ZTE TECHNOLOGY JOURNAL*. 2012; 18(6): 22-25.
[10] Wang yue. Building Disaster Backup Center to Ensure the Safety of E-Government System. *Information System Engineering*. 2010; 8: 60-61.
[11] Zhou zhou, Zhang ya. Construction and Application Research of Government Data Disaster Recovey Center. *Network Security Technology & Application.* 2012; (7): 21-27.
[12] Ge feng, Huang Liping. Discussion on Date Backup System and Its Hardware, Software Technologies and Products. *Information Technology*. 2012; (5): 56-61.
[13] Wu xin. Disaster Backup System Construction and Development. *Science and technology information*. 2010; (22): 112-113.
[14] Wu Ruiqing. Several Points of Consideration for Building Date and Disaster System Backup Center. *Modern computer.* 2012; (5): 55-57.
[15] Tian tao. Research on Data Backup and Remote Disaster Recovery Technology in SAN Environment. *China Computer & Communication.* 2012; (5): 93-94.
[16] Ma ling, Li Xianyu & Liu feng & He hui. Study of Snapshot in Disk Data Copy. *Computer Engineering and Design.* 2007; 27(22): 4285-4287.
[17] Yang Yixian, Yao Wenbin & Chen zhao. Review of Disaster Backup and Recovery Technology of Information System. *Journal of Beijing University of Posts and Telecommunications.* 2010; 33(2): 1-6.
[18] Timothy Wood, H Andrés Lagar-Cavilla & KK & Prashant Shenoy. PipeCloud: Using Causality to Overcome Speed-of-Light Delays in Cloud-Based Disaster Recovery. 2011.
[19] Li li. Date Backup Strategy and Method for Enterprise Information System. *Nonferrous Metals Engineering & Research.* 2012; 33(4): 47-49.
[20] Yang Ping, Kong Bo & Li Jinping & Lu Mengxia. Remote Disaster Recovery System Architecture Based on Database Replication Technology. *Computer and Communication Technologies in Agriculture Engineering*. 2010: 254-257.
[21] Chen Xiaojia, Zhang Junrui. Disaster Recovery Backup System Research. *Computer Knowledge and Technology.* 2009; 5(18): 4673-4674.
[22] Zhuang Qianman. Design of Massive Date Disaster Recovery System Based on SAN. *Information Security.* 2013; (1): 35-37.
[23] Qiu Jinlong, Liu Xiaojie & Zhao kui. Safe disaster backup system. *Computer Engineering and Design.* 2011; 32(10): 3258-3261.
[24] Zhang Xiaofei. The Application of Data backup in the digital library data security. *Information Research.* 2011; 6(6): 93-95.
[25] Bai yong. The theory and practice of data-level disaster recovery technology. *Financial Technology Time.* 2012; (11): 82-83.
[26] Kang Xiaowen, Yang Jieying & Du xin. Research of key technologies for data disaster tolerance based on virtual storage. *Application Research of Computers.* 2009; 26(7): 2603-2606.
[27] Zhu Jianfeng, Zhou Jingli & Zeng Dong & Qin Leihua. Design and implementation of data disaster recovery system based on storage-virtualization. *Eighth International Symposium on Optical Storage and 2008 International Workshop on Information Data Storage*. 2009; 712518-1-18.
[28] Huang bin, Xiao jian. Introduce Enterprise Data Backup Technology Briefly. *Computer CD Software and Applications.* 2012; (20):164.