



Construction of Information Disaster Recovery for Hospitals

Juan Xu

School of Information, Yunnan University of Finance and Economics, Yunnan 650221, China

E-mail: Xujuan@ynufe.edu.cn

Abstract

When data disaster happens, the disaster recovery system (DRS) can respond automatically and real-time, and quickly restart the application system in the redundant device to keep the processing of the business. The construction principle of the disaster recovery system has been studied, and combining the base function and national standard of the hospital information system (HIS), the data disaster recovery mode in the hospital information system was analyzed systematically and the constructive project was proposed in the article.

Keywords: Hospital information system, Data disaster recovery, Business recovery, Remote backup

1. Introduction

With the quick development of the computer technology, the information technology has been extensively applied in the medial and health industry. On the one hand, China is actively pushing the requirement and standard of the hospital informationization construction. On the other hand, in the informationization construction of hospital, the management quality of hospital has been enhanced, and hospitals have benefited much. And hospitals have also been trying to push the informationization construction all along.

The medical information system has been applied in hospitals widely, which makes hospitals acquire notable management benefit and economic benefit. When hospitals enjoy quick service decision-making and convenient management because of informationization, they are in the danger of data loss (Dong, 2001, P.66-68).

Danger one: The deep development of hospital informationization, the patients continually added, and the business mode of 24×7 every weak make the data of HIS increase by the class of TB, and the explosive data need to continually add storage devices, and the storage and backup system in HIS is always approaching to breakdown.

Danger two: When the computer system encounters natural disasters, computer crime, computer virus, hardware/software error and man-made mistake operations, how to guarantee the security of users' data and the continual operation of the information management system.

Danger three: The upgrade of the old system will certainly bring the problem of data transfer, and how to ensure that the system doesn't lose key data in the transfer process?

Danger four: The invalidation of the key nodes in the network system will induce the stop of the data operation. How to quickly respond the faults and start the data recovery system to continue the business processing?

The virus attack and the loss of backup data will induce death warrant to the continual operation of hospital. The urgent problems how to guarantee the normal running of the system and prevent the data loss because of faults or disasters should be solved by HIS as soon as possible. If the security of the hospital data can not be guaranteed, the meanings of large numbers of network investment will be lost.

2. Hospital information disaster recovery system

2.1 Hospital information system

HIS (Informationization Work Lead Group Office of Chinese Ministry of Public Health, 2001) means to utilize modernization measures such as computer software and hardware technologies and network communication technology to comprehensively manage the patient flow, logistics and financial flow of the hospital and various departments, and collect, store, process, abstract, transport, gather and generation various information generated in various stages of the medial activity, and provide comprehensive and automatic management and the information system of various services for the whole running of hospital. HIS is the necessary infrastructure and support environment in the construction of modern hospital.

HIS belongs to the most complex type in the enterprise class information system, and it is decided by the objective, task and character of hospital. It can not only follow and manage the management information generating in the patient flow, financial flow and logistics with other management information systems (MIS) to enhance the running efficiency of the

whole system, but also support the whole medical, teaching and researching activity taking the patient medical information record as the center.

2.2 Disaster recovery system

Disaster recovery (DR) (Zhang, 2004) is a concept with extensive category, and generally, all contents relative to the operation continuity should be brought into the disaster recovery. DR is a systematic engineering, and it includes all aspects supporting the user operation. For IT, DR is the computer system to prevent that the user operation system suffers various disasters. And DR is also represented as a kind of initiative taking precautions, and it is not “taking precautions after suffering a loss” after disaster happens.

From the strict view, the DR usually talked by us means that when the production stations are destroyed by the disaster, other redundant stations established by the user can replace the normal operation and keep the continual operation. To achieve higher usability, many users even establish multiple redundant stations.

To prevent above possible disasters and reduce possible losses furthest, the disaster recovery system (DRS) is often established for pivotal operations (Xie, 2004). The establishment of DRS needs two parts, i.e. the data disaster recovery and the application disaster recovery. The data disaster recovery means to establish a distant data system which is a real-time copy of the local key application data. The application disaster recovery is to establish a set of complete copy application system corresponding with the local production system in the different place, and in the disaster, the remote system could quickly replace the local system. The data disaster recovery is the guarantee to fight disaster, and the application disaster recovery is the construction target of the disaster recovery system.

Technically, there are two main indexes, RPO (Recovery Point Object) and RTO (Recovery Time Object) to measure the disaster recovery system (IBM, 2005), and the RPO presents the data quantity allowed to be lost when the disaster happens, and RTO presents the recovery time of the system. When RPO and RTO are smaller, the usability of the system is higher and user's investments will be larger. Of course, the class of the disaster recovery system is also decided by the protection class and the significance of the operation application, and the construction should be based on the effective capital utilization and the existing system rebuilding. RPO and RTO must be confirmed by different operation demands after the risk analysis and operation influence analysis are performed. To different operations, the demands of RPO and RTO are also different.

3. Disaster recovery mode of HIS

Disasters can not be predicted basically, and the loss also can not be estimated exactly, but the influence of the disaster always is deathful for the subsequent works of the hospital which has begun the informationization construction. The hospital data disaster recovery is one part of the continual plan of hospital operation, and it is most important to establish HDDRS. When the data disaster happens, the disaster recovery system (DRS) can respond automatically and real-time, and quickly restart the application system in the redundant device to keep the processing of the business.

According to the actual situation of hospitals in China, the information system of hospital mainly includes HIS, LIS and PACA. And most hospitals only have HIS and LIS at present, and the data quantity they generates every year is not large, less than 10G. But the data generated by PACS are egregious, and it will generate more than 1TB data, so it is more important to protect the security of data.

For the hospital data recovery, the storage is the base, the backup is the core and the recovery is the key.

The data storage can not ensure the continual running of key business, and the data backup is necessary in the network of the enterprise class. The data backup can quickly recovery the back-up data, largely reduce the time of service interrupt, and provide good data service for users when the system is damaged or the data is lost.

Because the particularity of the hospital operation system, to ensure the continual running of the system, the server control center generally adopts the double-computer fault tolerance and the server cluster, or the cold backup computer to deal with the downtime to reduce the time of halt. The data backup in most hospitals is not perfect. For the hospitals without PACA, most of them only adopt the self-backup program of the database software to copy the data to the hard disk one time or two times one day, and only few of them adopt the magnetic tape backup and hard disk backup. For the large-sized hospitals which have used the PACS system, most of them adopt the LAN-free backup mode based on SAN to connect the LTO tape base in the fiber exchanger, and realize the automatic classified storage and backup by the backup software, which can completely release the bandwidth of the network. Both the magnetic tape (base) backup and the hard disk backup respectively have their corresponding advantages and disadvantages (He, 2004, P.41-45).

Only the local data backup can not fulfill the requirement of the hospital informationization construction. So the remote disaster recovery system must be established to protect the key data in the HIS. The key data will be copied to the remote disaster recovery center by means of the remote data backup technology. The remote disaster recovery center can monitor the activities in the production center and the local backup center real time, and once the faults occur in the local production center and the backup center, the operation process will be quickly replaced to the remote disaster

recovery center.

Combining present analysis, according to the operation demand and operation data scale of hospital, three-class modes are adopted to construct the hospital information data disaster recovery solution.

The first class: Establishing stable production data storage center.

The second class: Establishing safe local data backup system.

The third class: Establishing remote disaster recovery system with quick response.

3.1 System structure of the HIS disaster recovery mode

The system structure of the HIS disaster recovery mode is seen in Figure 1.

3.2 To establish stable production data storage center

According to the operation contents and data quantity processed in HIS, the storage solution of the production data storage center can be established. The information service is composed by the application system N+1 cluster system, and the storage part is composed by the storage solutions based on iSCSI. The solution project of the production data storage center is seen in Figure 2.

PACA is the comprehensive application system to collect, store, manage, diagnose and process the digital medical hospital image information generated by the digital medical equipments such as CT, MR, US, X-ray apparatus, DSA and CR in the hospital, and it is one of most important parts of HIS. For large numbers of image information and accumulated data generated every day, the N+1 cluster can provide all application information service of HIS. According to the types of the collected information, five applied information servers and one backup computer are designed. Five application information servers provide the services respectively for the PACS, outpatient service, being-in-hospital, medicine, and material equipment and financial information.

iSCSI (small-sized computer system interface of Internet SCSI) is a standard to transfer data mass on the Internet or Ethernet. It was initiated by Cisco and IBM, and largely supported by the people who advocated the IP storage technology. And it also is a SCSI instruction set which can be running on the IP and be used for hardware device. Simply speaking, iSCSI can realize the running of SCSI agreement in the IP network, which can make it select the route on the gigabit Ethernet with high speed. The main function of iSCSI is to perform the encapsulation and reliable transfer of large numbers of data between the master computer system (initiator) and the storage device (target) on the TCP/IP network. In addition, iSSCI also can provide the encapsulating SCSI order in IP network and run on the TCP. iSSCI is the technical standard based on IP, and it can realize the connection between SCSI and TCP/IP, and for the users taking the LAN as the network environment, a few investments can help them to realize convenient and quick interactive information and data transfer and management.

3.3 To establish safe local data backup system

The local data backup can adopt the three-class backup. The first class backup is the hot backup of data, i.e. adopting the copy software to realize the synchronization of source-data and objective data. Each data updating operation is implemented on the production center and the local backup center at the same time. The second class backup is the code backup of data. Any technology has its own limitation. Though the copy software can realize high-level data protection, and it can protect data and realize the re-synchronization in time when the chain is in fault, or the main-array/assistant array is in the unattainable state or suffers natural or mechanical damage, but if the legal operation of source-data will induce the invalidation of database, the database of the objective data will be invalidated in the same way. So the cold backup of data can be adopted for the data source, for example, performing time added backup in the night of every Saturday. This project can provide the data protection to the man-made and application mistakes. The third class backup is the warm backup of data, i.e. the database copy technology. The complete data copy is reserved in the local backup center, and the updating log is transferred periodically to the local backup center by the production center through the network.

Generally, the disaster recovery system needs much investment, but the use probability is low, so the total cost of ownership (TCO) and the return on investment (ROT) should be seriously analyzed and computed, and in the local data backup system, one backup server is adopted as the backup system connecting with the tape base.

3.4 To establish remote disaster recovery system with quick response

In the various IT systems of enterprise, the production center is very important, and it always matches with a remote backup center. In the interior of the production center, various data protections have been implemented. When the fire or earthquake happens and the production center is in paralysis, the backup center will replace the production and continue to provide the network service. In the remote disaster recovery solution project, the remote disaster recovery center is established based on the iSCSI cluster system and it can actualize the uniform backup and system disaster recovery of the operation system.

Simply speaking, iSCSI is to encapsulate SCSI by TCP/IP and transfer it in the Ethernet. The high-speed gigabit iSCSI combines SCSI, Ethernet and TCP/IP.

The technology of iSCSI is mainly used to solve the remote storage problem (He, 2004, P.41-45).

3.4.1 To realize the data exchange among different places

Both different places have their own storage networks based on fiber (SAN), and the cost that two networks are connected by the fiber to realize the data exchange between two different places is too expensive. iSCSI is based on IP, and it can contain all parts in IP network, and if FC is converted into the data of IP, these data can be transferred by the traditional IP network, which will solve the problem of remote transfer, and when the data arrive at the other end, the data of IP are converted to the local FC storage network, so two fiber networks can be connect under low cost investment by iSCSI to realize the data exchange among different places.

3.4.2 To realize the data backup and disaster recovery among different places

By iSCSI, users can span standard Ethernet cable to establish actual SAN network at any place, and they need not to require special fiber channel network to transfer data between the server and the storage devices. iSCSI makes the remote mirroring and backup become possible, because without the distance limitation of fiber channel, the standard TCP/IP can make the data to transfer in the Ethernet. But from the view of data transfer, most iSCSI network transfer bandwidths are 1Gbit at present, and if the FDX is realized, the bandwidth can achieve 2Gbit, and the bandwidth of the second generation product can also achieve 2Gbit, and in the future third generation general iSCSI standard, the bandwidth will achieve 10Gb, and to establish the remote disaster system by iSCSI will be easily realized.

4. Conclusions and expectations

By the disaster recovery system, the medical information system can achieve high usability, high security, high efficiency, high expansibility and high management property. As viewed from the operation and application layers, the disaster recovery processing and high usability of the data center can enhance the efficiency of service and increase users' satisfactions and competitive forces through ensuring continual 24-hours key operations.

The disaster backup has gradually turned from original tape-backup technology to the disk mirroring technology and from single-computer backup to the network backup, and the backup data center has gradually turned to the hot backup from cold backup, and the requirements of disaster recovery class are high and higher. At present, to construct continually useful system and ensure the sustainable operation of the operation system, and better provide services to users is the objective pursued by the hospital informationization construction, and it is the development direction of future disaster recovery to establish the data center without data loss, which can automatically perform the switch when the disaster happens to ensure the continual usability of the operation system through the disaster recovery, especially the remote application class disaster recovery. But the research about the remote application class disaster recovery is still in the start stage, and relative technology and documents are rare, and the implementation is very difficult. But its importance can not be ignored, and it is the base to construct the usability system with continual operation, and the development direction of future disaster recovery, and a set of complete technical theory is needed to support it at present.

References

- Chen, Qiang, Ma, Liya & Zhao, Wei. (2006). Digitized Hospital Standard System Construction and Question. *Medical Information*. No.19(1). P.27-29.
- Dong, Weiyuan & Wang, Mingbao. (2001). Enterprise Disaster Recovery from "911". *PC World China*. No.6(1). P.66-68.
- He, Suining. (2004). Study on the Disaster Recovery Technology. *Modern Electronic Engineering*. No.4. P.41-45.
- IBM. (2005). White Book of Disaster Recovery. [Online] Available: <http://www.ibm.com>.
- Informationization Work Lead Group Office of Chinese Ministry of Public Health. (2001). *Basic Function Standard of Hospital Information System*. March of 2001.
- Xie, Changsheng, Han, Desheng, Li, Huaiyang & Cao, Qiang. (2004). Grade and Technology of Data Disaster Recovery and Copy. [Online] Available: www.csip.cn/new/st/al/2004/0730/342.htm. (July 30, 2007).
- Zhang, Feng. (2004). Expert Talking of Storage Technology: Disaster Recovery Builds a Port. [Online] Available: www.dostor.com/info/netstor/2004-10-29/0001921045. (Oct 29, 2004).

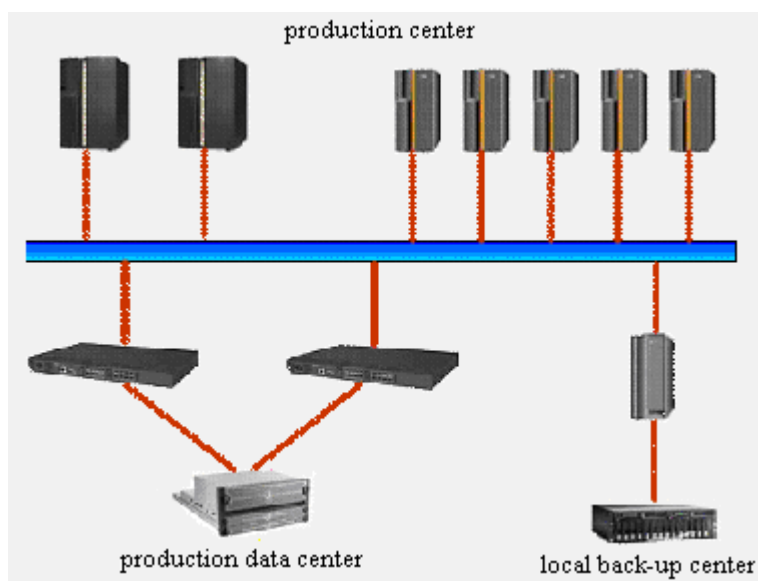


Figure 1. System Structure of the Hospital Data Disaster Recovery Mode

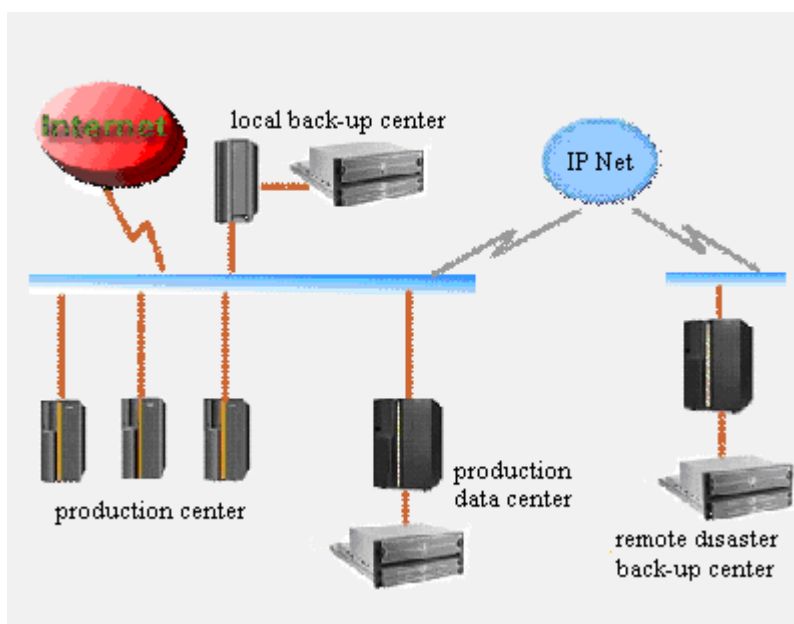


Figure 2. Solution Project of Production Data Storage Center