CCSE Computer and Information Science
www.ccsenet.org/journal.html

Vol. 2, No. 3
August 2009

Study on the Design Principles of Data Disaster Recovery System for Hospitals

Ping Xiao
Yunnan University of Finance and Economics, Kunming 650221, China
E-mail: Xiaoping@ynufe.edu.cn

Abstract

The medical information system has been applied in hospitals widely, which makes hospitals acquire notable management benefit and economic benefit. When hospitals enjoy the quick service decision and convenient management because of informationization, they are also in the danger of data loss. Data disaster recovery is the guarantee of the hospital informationization construction, and the base to ensure the normal medical service of hospital. In the article, the data disaster recovery mode in the medical information system is studied and the design principles of hospital data disaster recovery system are systematically analyzed.

Keywords: Hospital information system, Disaster recovery system, Design principles

1. Introduction

The medical information system has been applied in hospitals widely, which makes hospitals acquire notable management benefit and economic benefit. With the deeply using of the system, the data quantity in the server increases several-fold. At the same time, the downtime also occurs in the operation of the system, and though the system can be recovered depending on daily copy, and the loss is limited, but the normal work is influenced. So in the system, not various network equipments but data stored in the server are most precious. The urgent problem of the medical information system is to ensure the healthy running of the system and prevent the data loss because of default or disaster. If the data security of the hospital can not be guaranteed, large numbers of network investments should lose meanings. When hospitals enjoy the quick service decision and convenient management because of informationization, they are also in the danger of data loss. Because of virus attack, loss of data copy will seriously influence the sustainable works of hospitals.

2. Disaster recovery system

To prevent above possible disasters and reduce possible losses furthest, the disaster recovery system (DRS) is often established for pivotal operations. 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.

There are different definitions for the disaster recovery system in the world, but the total standards are same, i.e. first, the local data is copied, then the copy tape is stored at the remote place, and the remote copy system which can replace the local system in time is established, and the recovery time can be from several days to hour class, minute class, second class or zero data loss.

3. Measurement indexes 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, and the RPO presents the data quantity allowed to be lost when the disaster happens, and RTO presents the recovery time of the system.

To reduce data loss as much as possibly, a remote data storage system needs to be established, and it can perform the image copy of data with the production system. To reduce the recovery time of the system, a set of complete copy application system matching with the production system needs to be established in the disaster recovery center based on the data disaster recovery system. When the disaster happens, the disaster copy center could quickly replace the operation running, which can not only reduce the data loss and the system recovery time to the largest extent, but also largely enhance the continual usability of the hospital operation system.

If the construction investments are available, the ideal construction of the disaster recovery system is to achieve RTO=0 and RPO=0. The realization of RTO=0 is mainly decided by the concrete construction mode of the application system, such as the concrete applications of the system disaster examination technology and the data migration technology in the system. And the realization of RPO=0 is mainly decided by the concrete applications of data storage and copy technology and the data fault-tolerant technology. The synchronous replication of system and data can be adopted, but how to realize the synchronous replication and ensure the integrality of data will directly influence the investment cost of the system.

When the disaster recovery system is established, RPO and RTO should be reasonably selected according to users' demands. 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.

4. Design principles of hospital data disaster recovery system

4.1 Principle of operation demand

First of all, according to the operation contents of the hospital information system, the problem which application systems need disaster recovery should be confirmed. The operation flow of each subsystem should be known in detail, and RTO and RPO are defined in advance, and the problem which application system needs which disaster recovery structure should be confirmed.

The work mode and the data acquirement contents of each subsystem in the hospital information system are analyzed first, and the requirements of each subsystem are established in Table 1.

4.2 Principle of physical demand

The differences between the disaster recovery center and the operation production center are more, the variety of disaster which can be resisted is more, and the difference is embodied by the physical distance to the large extent.

According to the demand of application, the local copy center and the remote disaster recovery center can be selected and established. The cost of the local copy center is less, and the technology is relatively simple. But once destructive disasters such as earthquake, flood, fire and electric deficiency happens in the local place, all local copy data will be lost and the operation cannot be recovered.

When the main computer, storage and network structure which can be started at any moment in the remote place, and the copy station is not only a separate copy system, but it should be in the running state, can provide the production application service and quick operation replace. Generally, both the data center system and the copy center system are in the running state, but the operation processing system only runs in the production center. Any amendments to the data by the operation system will be copied to the copy center synchronously. When the faults happen in some parts of the production center, the application system on the fault machine will be automatically replaced by other machines in the production center by the copy software. When the whole system of the production center breaks down because of accidents, the copy server port software will start the whole operation application system in the copy center according to the appointed rules. After the system is recovered, the application system will be replaced to the production center from the copy center, and the copy center system returns to the copying state.

4.3 Principle of software demand

Physical defaults will make the system break down, which can be found easily. But the logical default is hard to be found, but only if the original data exist, the data can be recovered, so it is necessary to copy the historical data for long term. Therefore, good "data protection system" and "data protection project" will reduce the disaster loss to the minimum degree.

The disaster recovery software can automatically discover the default, and give clues to help deciding whether to perform the switch, and automatically perform data interview, application online and reorientation of the network. The disaster recovery software can often nondestructively test the disaster recovery fame with low costs, fully embody existing IT frame, be one part of DR plan, automatically perform necessary approaches, test and claim the happening of disaster, decide the default switch point, test the loss quantity of data and decide the acceptable data loss quantity.

The disaster recovery center must support the operation replacement (i.e. all operation flows are implemented in the system of the disaster recovery center) and the switch (i.e. after the operation replacement completes and the original data center could support the operation, and the operation will be switched to the original data center from the disaster recovery center). According to the design requirements of the disaster recovery center, the operation switch should be performed in the time of RTO value. By the support of the disaster recovery software, enterprise can effectively protect, interview, store and manage important information data at any time, which can help enterprise to enhance the information usability to large extent and relieve the fear of trouble in the rear of the enterprise.

4.4 Input and output analysis of the disaster recovery system

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. TCO and ROT are main indexes to measure the investment and return of the disaster recovery system, and the cost and benefit analysis (CBA) of the disaster recovery system emphasizes the analysis of the benefit of investment, and considers the rationality of the investment from the view of the development of the operation system.

First, the disaster recovery system which is prepared to be constructed and the continuality of the operation system which is running should be considered. To protect the former investments, the large-scale reconstruction of the original operation system should be avoided to the best. Second, the influence of the operation system extension to the disaster recovery system, especially the influences of the added storage capability and communication line load should be considered.

As viewed from the economy, the optimal disaster recovery solution is not certainly the disaster solution with the best performance, and TCO and ROI of the disaster recovery system are very important design indexes for many users. TCO includes the total investments of establishing system, maintaining system and extending system, and because of low starting probability of the disaster recovery system, the development of new technology and the enhancement of the cost performance of new product will certainly induce the depreciation of the disaster recovery equipments. Therefore, for the disaster recovery system, TCO is higher, ROI is lower.

According to the statistics of relative institutions, for the bank industry which requires the key operations highly, each downtime of the computer system will lose 10 million dollars averagely, and immaterial asset loss which can not be measured to the reputation of the company, but the cost of the disaster recovery project only needs one million dollars averagely. And the return ratios of investments will be relatively lower for the medical industry.

5. Conclusions

The data disaster recovery is the guarantee of the information-based construction for hospitals, and the base to ensure normal medical service of the hospital. Good works and bases will help to future construction and development. In this aspect, long-term thinking and investment will exert important functions for future online running of more application management systems.

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.

References

Chen, Qiang, Ma, Liya & Zhao, Wei. (2006). Digitized Hospital Standard System Construction and Question. *Medical Information*. No.19(1). P.27-29.

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).

Table 1. Operation analysis of hospital information system

Application system	Significance	Real time	Recovery time
Outpatient doctor work station subsystem	Pivotal	High	Less than 10 minutes
Hospital doctor work station subsystem	Pivotal	High	Less than 2 hours
Nurse work station subsystem	Pivotal	High	Less than 2 hours
Clinical examination subsystem	Pivotal	High	Less than 2 hours
Blood transfusion management system	Important	Middle	Less than 6 hours
Medical image system	Pivotal	High	Less than 2 hours
Surgery anesthesia subsystem	Important	Middle	Less than 6 hours
Drug management subsystem	Important	Middle	Less than 6 hours
Clinical and emergency register subsystem	Important	Middle	Less than 6 hours
Clinical and emergency pricing and charge subsystem	Pivotal	High	Less than 10 minutes
Inpatient in, out and transfer management subsystem	Important	Middle	Less than 6 hours
Hospitalization charge subsystem	Pivotal	High	Less than 2 hours
Material management subsystem	Important	Middle	Less than 6 hours
Equipment management subsystem	Important	Middle	Less than 6 hours
Financial management subsystem and economic accounting management subsystem	Pivotal	High	Less than 2 hours
Disease case management subsystem	Pivotal	High	Less than 2 hours
Medical statistical subsystem	Secondary	Low	In one day
Hospital director comprehensive inquiry and analysis subsystem	Pivotal	High	Less than 2 hours
Patient consultation service subsystem	Secondary	Low	In one day
Medical insurance system interface	Important	Middle	Less than 6 hours
Community medical system interface	Important	Middle	Less than 6 hours
Remote medical consultation service interface	Important	Middle	Less than 6 hours