Design of Reliable Disaster Recovery System through Integrated Server Redundancy

Bong-Hyun Kim*

Professor, Department of Computer Engineering, Seowon University, 377-3 Musimseo-ro,Seowon-gu, Cheongju-si, Chungcheongbuk-do, 28674, Republic of Korea
Corresponding author: +80-10-2078-7808, bhkim@seowon.ac.kr

Article History:Received:11 november 2020; Accepted: 27 December 2020; Published online: 05 April 2021

Abstract: Even before the September 11 terrorist attacks in the United States in 2001, information systems prepared against disasters in Korea were extremely weak. However, as various domestic and foreign accident cases have occurred, it is recognized that preparations for this are necessary. Accordingly, at present, each institution has prepared and implemented various backup policies to protect the institution's information and data in case of disaster. Therefore, in this paper, we conducted a study to design a more stable and efficient disaster recovery system by building redundancy for server operating in integrated data center. To do this, we analyzed the redundancy design for the integrated disaster recovery server and designed the overall system configuration. Also, the design results were analyzed by testing web server redundancy and switch redundancy. In this paper, the proposed design method for stabilization and efficiency of disaster recovery system is the redundant construction of integrated server and switch. In other words, the disaster recovery system was composed of active storage and standby storage, and data stabilization was promoted through real-time replication of each other. In the existing disaster recovery system, there is a problem in stabilizing replication because there is no monitoring system for internal replication between storage arrays. To solve this problem, we designed a system that replicates all data in active storage to standby storage in real time and monitors the replication status. Therefore, introducing service conversion automation from the main system, which is the method designed in this paper, to the disaster recovery system, improves the stability and reliability of the service of the local governments, so that it is possible to operate a more efficient and advanced disaster recovery system.

Keywords: Server redundancy, Disaster recovery system, Data protection, Switch redundancy, Remote replication.

1. Introduction

In recent years, Korea has been suffering from various natural disasters such as earthquakes and typhoons. Since natural disasters have no solution for humans, there is a growing sense of crisis. In particular, the damage caused by natural disasters is gradually increasing, and the damage to them is also increasing. In the future, safeguarding information assets is of paramount importance[1]. Therefore, it is necessary to minimize the loss of information assets due to natural disasters. Recently, the importance of a disaster recovery system for protecting information assets from such natural disasters and for rapid disaster recovery has been highlighted. Disaster Recovery System (DRS) is a system that recovers quickly when a system problem occurs and performs its original function. In other words, if a company's IT infrastructure such as a data center fails to perform its function due to various disasters and disasters such as natural disasters or hacking, it means to replace or recover the system so that it can perform its original function[2-3]. Of course, since they have one more system with the same structure as the existing IT system, they are often reluctant to introduce them due to construction and operating costs. However, the dependence on IT of all industries is increasing and at the same time, threat factors of IT infrastructure such as hacking, terrorism and natural disaster are also becoming more complicated and diversified. In such a situation, if the IT infrastructure system is shut down, not only will there be a huge cost loss, but also the external credibility will fall, causing tremendous damage to the enterprise[4].

Except for disasters that are extremely unlikely to occur, such as a large earthquake, flooding or flooding of fires can be a threat at any time. If these incidents occur at the enterprise computer center, it can take up to several months to physically completely restore the infrastructure. In this way, even the ultimate restoration of infrastructure and services can be understood as disaster recovery in a broad sense[5-6]. However, from the standpoint of operating a corporate IT service, it is a top priority to restart the service quickly without considering the disaster. Therefore, building a disaster recovery system in terms of IT operations is to prepare for the normal operation so that the service can be replaced with another system as soon as possible in the event of a disaster. In 2000, Dongwon Securities was flooded with data centers and paralyzed stock trading for three days. As the September 11 terrorist attacks began, awareness of the disaster recovery system began to increase. The Financial Supervisory Service recommended that financial institutions establish and operate DR centers in 2001 to recover within three hours of a disaster. Financial companies have begun building DR systems in accordance with written regulations. However, problems actually emerged when actual incidents occurred in the data center. In 2010, Citibank incurred an accident in which all electronic financial transactions were suspended due to flooding of the system due to the freezing of the cooler of the Incheon Computer Center. As a result, service interruptions lasted more than six hours. In 2014, a fire broke out in the Samsung SDS Gwacheon data center and paralyzed all Samsung Group affiliates. Although back-up equipment has been restarted to a large

Corresponding author: Bong-Hyun Kim
Professor, Department of Computer Engineering, Seowon University, 377-3 Musimseo-ro,Seowon-gu, Cheongju-si, Chungcheongbuk-do, 28674, Republic of Korea. bhkim@seowon.ac.kr

extent, the service has been suspended for more than a week. The damage increased further because the disaster recovery system for the area was not yet established.

In the face of these accidents, the domestic perception of the need for a disaster recovery system is improving significantly. In addition to the financial sector that must comply with regulations, the speed of recovery is different, but the willingness to build a disaster recovery system across the industry is fundamental. In recent years, DR systems are also being built in online shopping malls and electronic payments, where small obstacles lead directly to business losses, and in the medical field, which can threaten patient life in the event of system interruption. As a result, there is a growing recognition that disaster recovery systems are an essential element, and various information security laws recommend building a disaster recovery system.

Therefore, in this paper, we conducted a study to design a more stable and efficient disaster recovery system by building redundancy for server operating in integrated data center. To do this, we analyzed the redundancy design for the integrated disaster recovery server and designed the overall system configuration. Also, the design results were analyzed by testing web server redundancy and switch redundancy.

2. DR system current status

Disaster recovery(DR) system refers to a system for minimizing the failure of IT infrastructure such as data center due to various disasters such as natural disasters and hacking. In other words, when a system fails to perform its original function, a system for replacing or restoring it to perform its original function is called a disaster recovery system[7].

As we enter the digital age, computerization of work is accelerating and dependence on information systems is growing. Therefore, the ripple effect caused by information system failure, disaster and network interruption is also increasing. In particular, when R & D is carried out using national budgets and research outputs and related data are stored in the institution's information system, the loss of data or data causes a large loss of time and money nationally. Disaster recovery systems are categorized into independent, joint, and interdependence depending on the type of deployment. In the case of independent construction, it is easy to build and operate and has excellent security by establishing an independent disaster recovery center. However, there is a disadvantage that the construction and maintenance cost is the most expensive. Mainly adopted by large institutions. In the case of joint construction, two or more organizations use the disaster recovery system jointly. It costs less than a stand alone approach, but there are many things to consider, including consensus on security and operations between organizations that use it[8-9].

Lastly, in the case of mutual construction, instead of establishing a separate disaster recovery center, if two or more organizations act as mutual disaster recovery centers, or if one organization has a number of computer centers, disaster recovery centers among computer centers It is to play a role. In the case of mutual establishment of institutions or centers, it is a method of securing a system that is reserved through a contract or cooperation system and allocating a system for disaster recovery system to another organization (center) in the event of a disaster. This approach requires that institutions or centers have similar equipment and scale, and that there is room and compatibility in the system[10]. The cost of investment is low, but the security and reliability of disaster recovery are quite low and hardly feasible. Figure 1 shows the types of disaster recovery systems.

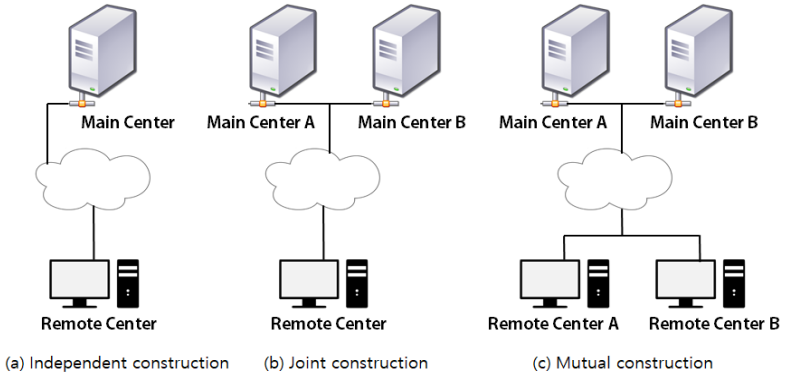

Figure 1. Types of disaster recovery system

The followings must be applied in the design and construction of a disaster recovery system. First, it is necessary to secure the continuity of external services according to the spread of web services of public services. Second, according to Article 56, Paragraph 2 of the Korean Electronic Information Act, the head of the agency has to establish and operate a stable disaster recovery system because it is obliged to operate the information system stably. Third, the latest technologies should be applied such as asynchronous data replication solution of less than 5 minutes, long distance data compression transmission technology over 100km, and remote automatic disaster recovery system solution[11-12]. Figure 2 illustrates the key strategic frameworks that should be

applied to the construction and implementation of a disaster recovery system.

Figure 2. Core strategic method of disaster recovery system

3. Experimental setup

In this paper, we conducted a study to design a more stable and efficient disaster recovery system by building redundancy for server operating in integrated data center. To do this, we analyzed the redundancy design for the integrated disaster recovery server and designed the overall system configuration. Also, the design results were analyzed by testing web server redundancy and switch redundancy.

In this paper, the proposed design method for stabilization and efficiency of disaster recovery system is the redundant construction of integrated server and switch. In other words, the disaster recovery system was composed of active storage and standby storage, and data stabilization was promoted through real-time replication of each other. In the existing disaster recovery system, there is a problem in stabilizing replication because there is no monitoring system for internal replication between storage arrays. To solve this problem, we designed a system that replicates all data in active storage to standby storage in real time and monitors the replication status. In addition, by providing a process that is stored in the disaster recovery system through asynchronous replication of information data, was promoted stabilization. Figure 3 shows the replication status real-time monitoring system proposed in this paper.

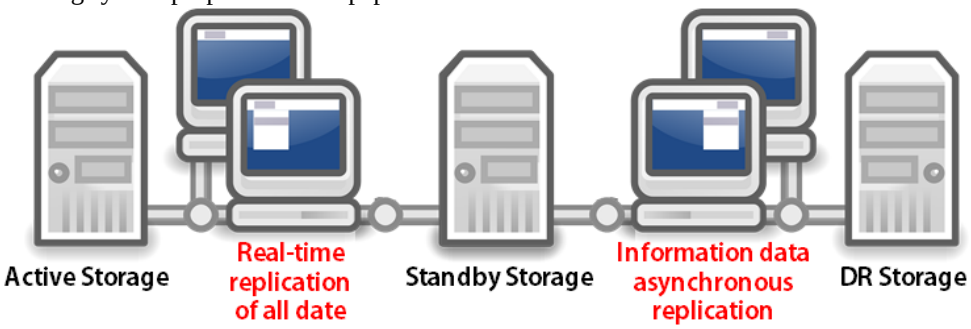

Figure 3. Real-time data replication monitoring system

In order to realize a stable environment of disaster recovery system, the redundant design of the integrated server and the redundant design of the switch are composed of network connection. In addition, data replication was carried out in connection with disaster recovery storage. Figure 4 shows the disaster recovery system server and switch configuration in the data center.

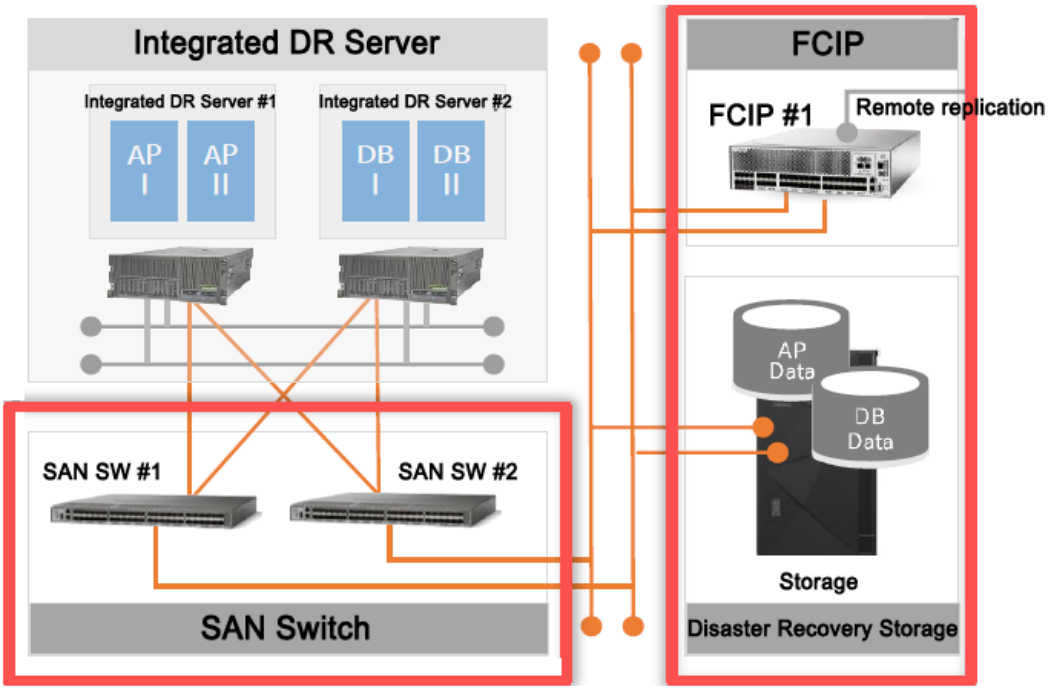

Figure 4. Integrated DR server and switch redundancy diagram

In addition, we designed an asynchronous storage environment that provides a recovery point objective (RPO) within 5 seconds for a long distance to construct a synchronization solution for disaster recovery systems. In other words, the mirror function was added to the data center and the disaster recovery system storage to replicate data in an asynchronous manner. This allows for quick resynchronization of the mirrored sites. Figure 5 shows the synchronization solution diagram of the disaster recovery system.

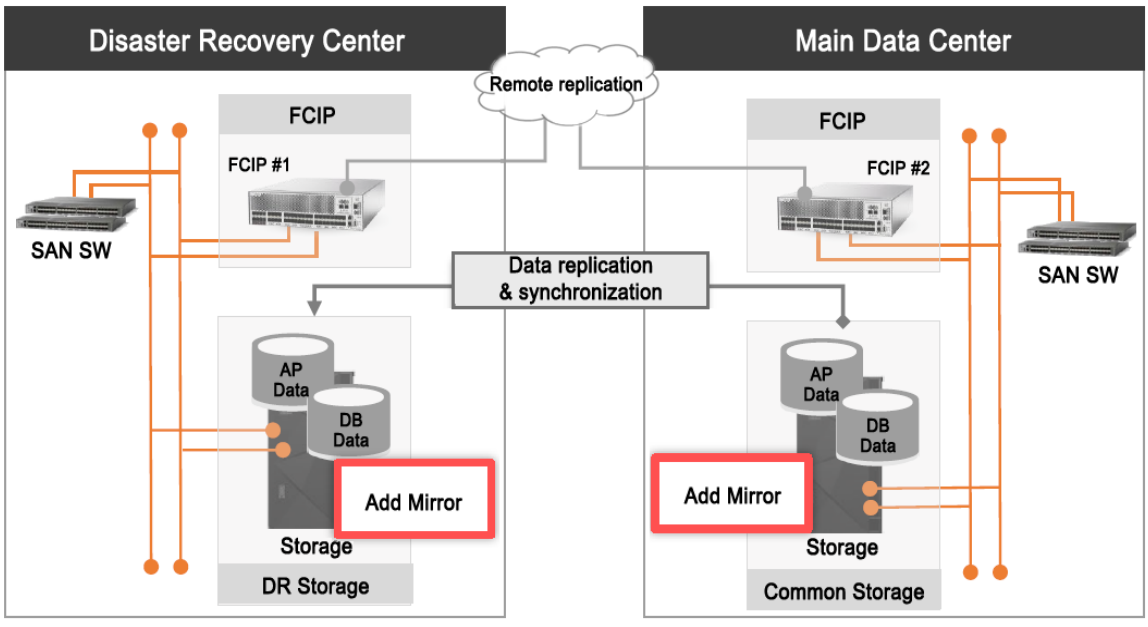

Figure 5. Disaster recovery system synchronization solution diagram

In conclusion, an asynchronous storage-based remote replication solution was applied to provide a 3 to 5 second recovery point objective (RPO) over a long distance. In addition, the mirroring function was added to provide perfect synchronization between the disaster recovery system and the common-based system. That is, the mirroring function was added to the storage for the main center and the disaster recovery system, and asynchronous data replication was performed. In addition, fast resynchronization of the mirrored site was

performed using only incremental changes. Finally, the redundancy test of the integrated DR server was conducted by removing any ports and cables among the two lines of the DR server service network. After removing any ports, the network service was tested for normality, and after removing any cables, the volume mount was tested for normalization. Figure 6 shows the screen to check the mount status after removing the port and cable.

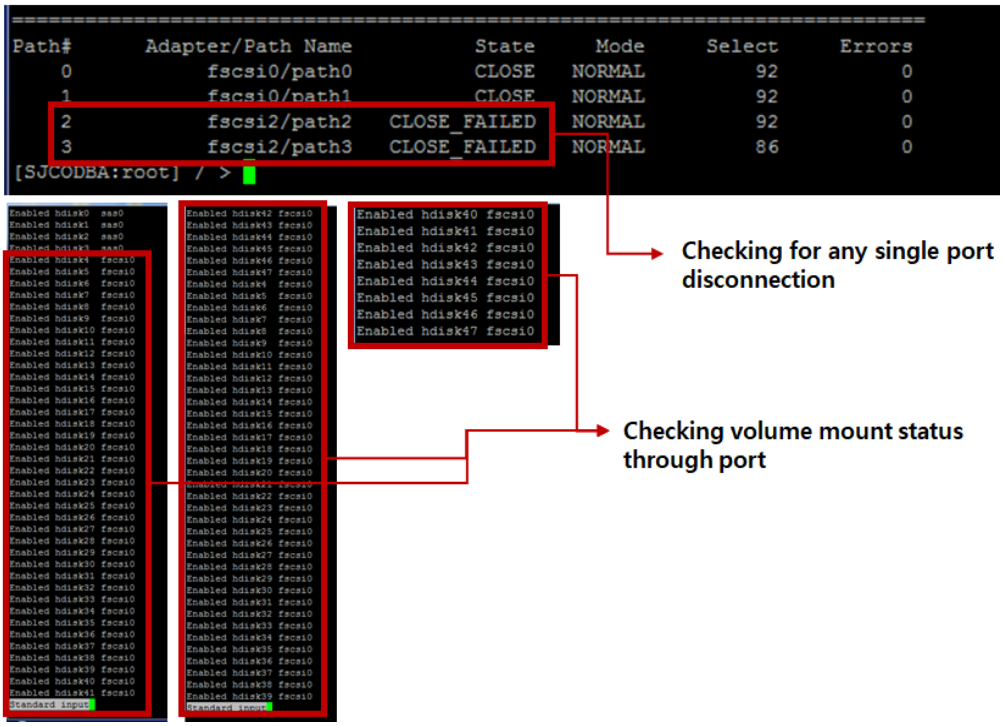

Figure 6. Result of checking the volume mount status after removing a single port

4. Conclusions

Currently, each institution has established and implemented various backup policies to protect the institution's information and data in case of disaster. This exists in a variety of ways, from a backup method that stores and stores data on a physical medium such as a tape or disk to a data recovery in real time by building a disaster recovery center. Instead of costly storage of physical backups, there is a risk of data loss from the time the backup is completed to before the disaster occurs. However, real-time backup does not have any loss of information in the event of a disaster, but has the disadvantage that it is expensive to build and operate. Therefore, it is important to select an appropriate disaster prevention and recovery method for each institution.

In this paper, we conducted a study to design a more stable and efficient disaster recovery system by building redundancy for server operating in integrated data center. To do this, we analyzed the redundancy design for the integrated disaster recovery server and designed the overall system configuration. Also, the design results were analyzed by testing web server redundancy and switch redundancy. Especially, in case of failure of integrated disaster recovery server network and HBA port part, it is designed to automatically switch over through server redundancy configuration and maintain service availability. In particular, we confirmed the redundancy of the Unified Disaster Recovery Server Network (UTP). In addition, we checked the HBA (SAN) redundancy of the integrated disaster recovery server.

By implementing web server redundancy and switch redundancy proposed in this paper, can be realized more stable disaster recovery system environment. In particular, through the service verification system of the information work system, it is possible to establish a defect-free system of the disaster recovery system. In addition, it is possible to secure reliability by considering compatibility with existing equipment, technology, and technology to be introduced.

References

1. Christopher W. Zobel. (2014) Quantitatively Representing Nonlinear Disaster Recovery. *Decision Sciences* 45(6), 1053-1082.
2. Shi Ling Chen, and Kai Ni. (2014) The Research on Data Disaster Recovery in Emergency Management System. *Applied Mechanics and Materials* 631, 222-225.

3. Bijan Khazai, Farnaz Mahdavian, and Stephen Platt. (2018) Tourism Recovery Scorecard (TOURS) – Benchmarking and monitoring progress on disaster recovery in tourism destinations. *International Journal of Disaster Risk Reduction* 27, 75-84.
4. Miao Liu, Eric Scheepbouwer, and Sonia Giovinazzi. (2016) Critical success factors for post-disaster infrastructure recovery. *Disaster Prevention and Management: An International Journal* 25(5), 685-700.
5. Razi J. Al-Azawi. (2017) Model of System Recovery in Periodic Disaster and Reproduction. *International Journal of Computation and Applied Sciences* 2(2), 57-61.
6. P. Petrantonakis, and J.-C. Panayiotopoulos. (2005) Using assignment model as an automated recovery system. *Disaster Prevention and Management: An International Journal* 14(1), 89-96.
7. Wei Chen, and Yu Ting Shang. (2017) Disaster Recovery of Online System Based on Cloud Computing. *Applied Mechanics and Materials* 865, 636-641.
8. Bryan Finch. (2016) Boston sport organizations and community disaster recovery. *Disaster Prevention and Management: An International Journal* 25(1), 91-103.
9. Yassar Alamri. (2017) Successful Post-disaster Recovery Requires Adequate Pre-disaster Preparedness: The Case of Gulf Countries. *Disaster Medicine and Public Health Preparedness* 11(4), 402.
10. Zhiyang Guo, and Yuanyuan Yang. (2015) On Nonblocking Multicast Fat-Tree Data Center Networks with Server Redundancy. *IEEE Transactions on Computers* 64(4), 1058-1073.
11. I. Peschansky. (2019) Stationary Characteristics of an Unreliable Multi-Server Queueing System with Losses and Time Redundancy. *Automation and Remote Control* 80(4), 648-665.
12. Haibo Jiang, Mingyu Fan, Xiaojing Wang, and Yilong Xiao. (2013) A Hybrid Redundancy Storage Scheme for Streaming Media Server Cluster. *International Journal of Advancements in Computing Technology* 5(8), 262-270.