

Research on Disaster Recovery and Application of College Data Center

Weihua Pu¹, Xiangyan Fu¹

¹ Shaanxi Fashing Engineering University, Xi 'an, Shaanxi, 712046

Keywords: data center; disaster recovery; application study

Abstract: With the increasing use of information technology in colleges and universities, especially the use of campus credit cards, the importance of data processing and production of information systems has gradually increased. The data center in colleges and universities needs a reliable protection, and can quickly restore its ability to work in the event of a disaster. The paper introduces several important disaster recovery tools, including data-level disaster recovery, application-level disaster recovery, and active-active data centers.

1. Introduction

With the in-depth application of information publishing platforms, mail systems, collaborative office and campus card services, more and more valuable information has been transformed into massive data, and the value of data has become higher and higher. Any loss of data will cause great loss to the user. A large amount of data needs to be based on a large number of hardware devices. The hardware runs all day round all day. It will inevitably cause various failures and hardware damage, and it may also be subject to fire and flood. All possible natural disasters, such as earthquakes, are as low as even a computer room crash. On the one hand, the increasing importance and dependence of data, and on the other hand, the decreasing security of data brought by the ever-expanding device groups, has caused increasingly sharp contradiction between the two. In order to reduce the damage caused by the failure and ensure the normal operation of the system, we can usually adopt two methods: One is to increase the availability of the system through redundancy, such as: disk RAID, two-machine fault tolerance, and so on. The second is to use data backup to export data to other storage media for recovery after a disaster. Therefore, establishing a complete and reliable data disaster recovery system within the university to ensure the stability and security of data is a problem to be considered when building a digital campus.

2. Disaster Recovery Technology

The main technologies for achieving data-level disaster recovery are virtual tape libraries and deduplication; virtual tape libraries are disk array hardware devices, but they emulate tape backup in terms of software functionality. The virtual tape library has the following advantages. (1) Compared to mechanical tapes, virtual tape libraries use compatible tape backup management software and traditional backup processes, which has greatly improved the availability of devices and the reliability of backups; (2) substantially improved performance and support for proximity disk arrays Extreme speed backup and recovery speed. And the immune virus, data security is equivalent to an ordinary tape library; (3) recovery work is extremely simple, if the required data exists in the VTL, it will not involve any mechanical work, recovery work is like the speed of disk backup; (4) virtual The tape library uses a disk array based on RAID protection, which increases the reliability of the backup by a few orders of magnitude compared to regular tape backups. The MTBF of the closed structure disk media itself is generally more than 5 times of the open structure tape media; (5) the compatibility is good, the standard FC, SCSI or iSCSI interface device is compatible with popular host devices and Operating system; (6) Good practicality, consistent with existing tape library application methods, without changing the management strategy of existing storage application software, protecting user investment; (7) Virtual tape library with electronic "robot" and tape "Driver" replaces exposed, fragile devices in a mechanical tape library.

RAID-based disk arrays have downgrading capabilities and have automatic alarm and online thermal recovery.

From the advantages of the above virtual tape library, it can be seen that the virtual tape library not only solves the problems of high maintenance burden, high backup failure efficiency, and poor backup and recovery capabilities of the traditional tape library, but also changes disk backups that are easily mistakenly deleted or infected by viruses. Infection and inconvenience in the unified management and optimization of the disadvantages in the SAN environment. Deduplication A data reduction technique commonly used for disk-based backup systems designed to reduce storage capacity used in storage systems. The way it works is to find repetitive variable size data blocks in different locations in different files within a certain period of time. Duplicate data blocks are replaced by indicators. Highly redundant data sets (such as backup data) benefit greatly from data deduplication; users can achieve a reduction ratio of 10:1 to 50:1. Deduplication technology allows users to efficiently and economically replicate backup data between different centers. The main technologies for implementing application-level disaster recovery are clustering technology and CDP (continuous data protection) technology. For off-site disaster recovery, CDP technology that can be implemented with low bandwidth is more common. In a low-bandwidth environment, Mi-croscan reduces the minimum data units transferred to 512 bytes (general software-level technology at 1 block of 4096 bytes, and hardware-level technology at block of 16,000 bytes). A very small bandwidth transmits a large amount of data. CDP automatic continuous snapshot technology can quickly restore current and historical data. Can greatly reduce the time for the system to resume production. Continuous I/O logging technology can restore data to any historical trace (seconds and I/O levels available). The data consistency guarantee technology generates a database checkpoint refresh at the specified snapshot point and copy point to ensure the consistency of the database log and data file, and achieve the goal of quickly starting the database. These technologies can make RPOs and RTOs that can be satisfied in remote disaster recovery centers to a relatively small extent. If you want to make RPO and RTO zero, you must adopt two-center active-active mode. In order to realize the dual livelihood of the production center and the disaster recovery center, to achieve a complete active-active architecture, it is necessary to carry out a live design at all levels of the information system. We divide the data center technology architecture of the data center into 7 layers: access layer, Web layer, application layer, database layer, system platform layer, storage layer, and network layer. In order to meet the requirements of the active-active center, the access access layer must make the client's request intelligently select between multiple centers to achieve business continuity (performance optimization/failover/on-demand connection). There are usually two ways to implement site selection: one is traditional site polling technology; the other is site load balancing technology.

3. Current Disaster Recovery Backup Mode Problems and Countermeasures

At present, many colleges and universities abroad have adopted a global enrollment strategy. Therefore, admissions agencies and teaching institutions are distributed throughout the world. Under such conditions, all teaching and enrollment tasks must be conducted continuously within 24 hours. This requires that business continuity is very high, and any interruption will result in irreparable loss. Since the enrollment and teaching of colleges and universities in China are mainly local, their continuous demand for admissions and teaching is not very strong. Therefore, the consciousness of disaster recovery is also relatively weak.

In terms of data security, China's domestic universities often have different extremes. Some colleges and universities do not pay attention to data security work. Once any data security emerges, disaster recovery is thought. In fact, data security is not just a part of disaster recovery. It is a complete system and a management issue. For example, first of all, we need to pay attention to personnel issues, management issues, data building security issues, network security issues, and so on. The second is the technical problem. For a disaster recovery system, the disaster recovery system mainly includes three levels. They are the host's available system, backup system, and overall system's fault tolerance. According to the author's investigation, many colleges and

universities often only pay attention to the construction of the third level when neglecting the construction of the first two levels. This makes the level not really play a role.

There are no unplanned disaster recovery safeguards. When formulating a school data security plan, we should first strengthen institutional development and manage personnel well to avoid human error. Secondly, tape and dual-system hot backups need to be strengthened so that local data can be effectively protected and potential threats can be reduced. Finally, there is a lack of remote disaster backup. Disaster recovery is a continuous task. It is necessary to ensure that planned downtime is not affected and that unplanned downtime is not affected. Only in this way can disaster recovery be implemented to avoid catastrophic consequences. However, at present, disaster recovery in universities in our country often refers only to planned downtime. There is no effective safeguard against unplanned disruptions.

Strengthen data security awareness. In terms of data security, we should strengthen the construction of safety awareness. We must not only strengthen technology, but also need to strengthen a series of related supporting facilities, such as good personnel training, good maintenance of the entire computer room, good supervision of network security, etc. Only in this way can the school data be truly secure. In carrying out capacity building in the backup system, we need to strengthen the construction of the host usable system and the backup system, and we cannot ignore the importance of these two systems.

Strengthen unplanned disaster recovery protection. For colleges and universities, colleges and universities should strengthen unplanned disaster recovery safeguard measures. In general, unplanned disasters generally include human factors, natural factors, and so on. For human factors, the training of personnel should be strengthened. Retraining should be available to staff in order to continuously improve the overall quality of personnel and reduce the probability of disasters. For natural disasters such as blackouts, earthquakes and other reasons, we should build a special plan to reduce the concentration of the host by dispersing the host in different regions so that the disaster can be minimized.

4. Conclusion

The adoption of disaster recovery technology in university data centers is a balance between the need for data protection and the economic cost of achieving this effect. When the application requires the requirement of uninterrupted work, the active-active center is the focus of consideration; when there are certain RPO and RTO requirements, application-level disaster recovery is the focus of consideration. Data-level disaster recovery is the last line of defense for high availability of data. It can only meet the data recovery objective of data loss and data destruction, and cannot provide real-time service takeover. The structure and technology of selecting and cooperating with itself need to be comprehensively analyzed according to the actual situation. In addition, building disaster-resilient data centers, technology is only one of them, and a great deal of research and deployment work is needed in terms of services, management, processes, personnel training, etc. Another important aspect is the application of transformation, and there are more difficulties. It also brings many challenges for researchers and constructors.

Acknowledgment

Item Number: 17JK0931

Title: Application of Unified Disaster Recovery Technology in University Data Security

References

- [1] Li Chunxi. Data Center Disaster Recovery System Classification [J]. Intelligent Building and City Information, 2010(11):31-33.
- [2] Wang Dejun, Wang Lina. Disaster Recovery System Research [J]. Computer Engineering, 2005, 31(6):43-45,113.

- [3] Yang Tianming. Research on Data Deduplication in Network Backup [J]. Journal of Huazhong University of Science and Technology, 2011(7):47-49.
- [4] Xiao Lianghua. Cloud data center active technology analysis [J]. Financial Electronics, 2012(2):59-61.
- [5] Huang Dachuan. Two new solutions for the data center disaster recovery architecture [J]. China Financial Computer, 2013(10): 88-88.