

Application of Computer Room Management in Cloud Computing

Jianjun Wu

Hunan City University, Yiyang, 413000, China

Abstract: With the development of science and technology, there are more and more defects in the management of computer rooms in Colleges and universities. In order to solve these defects, this paper puts forward the application research of computer room management under cloud computing. Based on cloud computing theory and comparing with traditional computer room management, the information framework of computer room management under cloud computing is constructed. The system has important practical price. Value.

Keywords: Cloud computing; Computer room; System; Management

1. Introduction

Under the modern university teaching mode, it is becoming more and more common for college students to learn computer-related courses. Some professional courses in Colleges and universities also need to be arranged in the computer room to learn or carry out computer operation [1-2]. In addition, the large scale of university computer room, the large number of computers and the variety of computer models greatly increase the difficulty of computer room management, which requires the introduction of scientific and effective computer technology to strengthen the management of university computer room. Cloud computing technology is a technology that has been flourishing in recent years. In the management of university computer room, the use of Internet connection makes the computer in university computer room connect with Cloud Computing Center effectively. With the support of cloud computing technology, the management efficiency of university computer room can be effectively improved, and it also helps to reduce the cost of computer room management. Therefore, it is of great practical significance to study the application of cloud computing technology in the management of university computer rooms.

At present, only a few universities and enterprises in China have built cloud computing rooms, and most of them are used for research and development, while a few are used for teaching. At the end of 2014, our institute built five training rooms based on virtual cloud desktop technology, totaling 200 machines, and put them into use in 2015. As far as cloud computing security technology is concerned, various kinds of cloud computing security products and schemes are emerging at home and abroad, such as SUN, EMC, Intel, VMware and other companies have cloud computing security products, which are mature. Cloud computing security issues include cloud computing infrastructure security, data security in cloud

computing environment, IaaS, PaaS, SaaS service security, cloud computing security operation governance, cloud computing business continuity to ensure the legitimacy of cloud computing [3-5].

As far as the virtual cloud computing room is concerned, its security mainly refers to the security of cloud computing infrastructure, which needs to configure the security protection mechanism of cloud computing infrastructure system to improve the security performance of the system. So how to configure cloud computing infrastructure system security protection mechanism? The author thinks that the security performance of virtual cloud desktop computer room system can be improved from two aspects: 1) Using VM vSphere technology based on integrated VMsafe, configuring infrastructure security mechanism, including host security, network security, virtual machine security, storage security, etc., to ensure the internal security of the system. 2) Use advanced firewall technology and equipment to resist external attacks, improve defense capabilities and enhance the security performance of virtual cloud desktop system. This article is written in terms of VM vSphere 5.1.

2. Cloud Computing Theory

Cloud computing refers to a method of connecting multiple computers using virtual networks to establish a decentralized community, and dividing huge data programs into several small programs through calculation and processing, so that these programs can be processed at the same time, integrated after obtaining the data information needed by users, and then fed back to use. Household Distributed Computing Method. With the continuous development of cloud computing technology, a unique technology system has been formed, which mainly consists of virtualization technology, network computing technology, distributed technology and so on. Cloud computing technology platform includes LaaS

(Software Services) layer, PaaS (Platform Services) layer and SaaS (Infrastructure Services) layer. Its key technologies are also embodied in these three levels: first, IaaS layer security. IaaS layer is at the bottom of cloud computing platform. It can provide all kinds of resources for upper cloud applications, including computing, storage, network and so on. It is the foundation of cloud computing platform operation. Therefore, its security is very important. Second, PaaS layer security. The main responsibility of PaaS layer is to provide data support for the operation of upper platform applications. Thirdly, SaaS layer security. SaaS layer provides access services for users. The supplier deploys the corresponding service application software on the cloud server. Users can access related services through the Internet to enjoy the convenient experience brought by the development of information and network.

2.1. Traditional network security protection mechanism

In view of the traditional network security problems, the mainstream network security products in the current market are roughly divided into three categories:

Basic firewall classes based on packet filtering strategy;
Intrusion detection and defense;

Active security classes for special protocols, such as Web application firewall WAF and database application firewall DAF. The firewall adopted by our school is the next generation firewall NSFOCUS NF of Greenland League. NSFOCUS NF has the main functions and characteristics of the three traditional firewalls mentioned above, including routing, switching, access control, traffic management, SNAT/DNAT, ISP load balancing, DDoS protection, VPN, HA, log reports, etc., which make users have mature security solutions. The solution can be changed and smoothly transitioned to the next generation firewall security solution of NSFOCUS NF. The NSFOCUS NF firewall is deployed between the cloud computing room and the campus network.

2.2. Network virtualization network security protection mechanism

Whether horizontal integration or vertical segmentation of network virtualization technology, it improves the security, reliability, and availability of network services, but also brings new challenges to the cloud computing environment network deployed based on this technology, which requires the correct configuration and management of virtual switches and virtual firewalls. For network virtualization using VMware virtualization technology, virtual firewalls can be deployed and configured in the following three situations in a virtualized network environment managed by VM vSphere technology based on integrated VMsafe:

between the physical machine and the physical machine (e.g. between the vCenter Server system and the ESXi host);

between the virtual machine and the virtual machine (e.g. between the virtual machine as an external Web server and the virtual machine connecting the internal network of the company);

Between the physical machine and the virtual machine (e.g. between the physical network adapter card and the virtual machine). The way virtual firewalls are used in ESXi configurations depends on how the system administrator intends to use the network and how to provide the required security for a given component. For example, if each virtual machine in a virtual network is dedicated to running different benchmark Suites for the same department, the risk of adverse access from one virtual machine to another is minimal. Therefore, the configuration of virtual firewalls between virtual machines is not necessary. However, in order to prevent interference with the test run of external hosts, configurations can be set up to provide firewalls at the entry points of virtual networks to protect the entire set of virtual machines. In order to protect the security of the virtual host, our school adopts the third way to configure the virtual firewall according to the actual situation. Virtual networks are connected by virtual switches. Like physical networks, they also need security protection. The whole virtual network can be divided into several segments by dividing VLAN.

In order to ensure network security, the communication mode between network segments should minimize the interference between network segments. According to the actual situation, our school divides the 200 virtual machines into five network segments and allocates them to five computer rooms, which are independent of each other.

3. The Practical Application of Cloud Computing Technology in University Computer Room Management

3.1. Formulation of management scheme of computer room in colleges and universities based on cloud computing technology

Cloud computing technology in university computer room management should be combined with the actual situation of universities, and then redesign the overall framework of university computer room. In the process of building server cluster data center in university computer room, we should deal with the following technical problems: first, compatibility. Build various driver libraries of client PC. In this way, in the early deployment stage or extensive replacement of old aging equipment links, we can ensure the convenience and speed of terminal settings, reduce a large amount of time and cost investment. Second, the problem of virtual terminal data.

On the one hand, each terminal is an independent desktop experience, on the other hand, each terminal can access and apply various software and data information in the mirror file. Third, the server storage problem. Internal and external network isolation, provide security. Firstly, even if the physical isolation card partitions the physical hard disk, all kinds of drive-level Trojans can still read the hidden information data, that is, intercept the relevant file information and screen capture the terminal screen, in order to achieve the purpose of stealing information data. Secondly, if the information data is stored in the local PC hard disk, if the PC fails and has to send out the information, in this process, it is still possible to make the information data face the risk of leakage. Finally, the Trojan horse will infect other PCs on the network after the system is restored.

4. Framework of Cloud Computing Room

To build a unified resource sharing cloud for University laser network and server, intensive management is carried out based on B/S architecture. According to the latest teaching plan of each semester, the virtual image is modified and perfected in real time. Servers should take effective precautions against a series of potential risks to ensure that the mirror

In order to ensure the orderly development of teaching work, the complete integrity of image data transmission process is ensured, and the mirror letter is also given.

Information data storage management, server cluster can be real-time dynamic monitoring, etc^[3].

5. Conclusions

The rapid development of cloud computing has brought a lot of convenience to university teaching and computer room management. This technology has entered a new wave of development. The traditional computer room management system cannot meet the development of the times. The computer room management under cloud computing can greatly save costs, improve the utilization of resources, and realize the computer room of colleges and universities. There are cross effect management.

References

- [1] Telecommunications and Information Exchange between Systems–Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments,” IEEE Standard for Information Technology, 2010
- [2] Borgonovo F., Capone A., Cesana M., Fratta L. ADHOC MAC:New MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services. Wireless Netw., 2014, (10) ,359–366.
- [3] Hassan M., Vu H., Sakurai T. Performance analysis of the IEEE 802.11 MAC protocol for DSRC safety applications. IEEE Trans. Veh.Technol., 2011, 60(8), 3882–3896.
- [4] OmarH. Zhuang W., Li L. VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs.to be published.
- [5] Borgonovo F., Campelli L., Cesana M. Fratta L. Impact of user mobility on the broadcast service efficiency of the ADHOC MAC protocol. in Proc. IEEE VTC Spring,2005, (4).