Research on the Common Security Risks and Precautions of Server Virtualization

Yongxin Guo

The University of Arizona, Arizona 85721, USA.

Abstract: At present, with the rapid development of domestic network technology, the increasing use of virtual server in the computer system, especially in the field of cloud computing technology, such as big data, the application of server virtualization technology, greatly improved the big data running speed and integration performance, however, in the large-scale application, some common security problems were exposed. Therefore, this paper discusses some common security problems and corresponding prevention methods in the virtual environment.

Keywords: Server; Virtualization; Security Risks; Precautions

Foreword

Server virtualization, also known as network virtual architecture, refers to the computer software environment is divided into multiple independent partitions, which can simulate a complete set of computer operation system according to the requirements. Server virtualization, also known as network virtual architecture, refers to the computer software environment is divided into multiple independent partitions, which can simulate a complete set of computer operation system according to the requirements. At present, many domestic network systems have less than 15% of the load, its scale far exceeds the needs of the system, and because the IT structure inside the system is too complex, the performance of the system is not high. The virtualization of the server has many ways, it can virtual a server into multiple, multiple server virtual into one, can turn several virtual machine into a logic machine, and then expand it to multiple virtual scenarios, using "virtual", "virtual" virtualization, can ensure multiple different requirements, can increase the speed of the system, save space; in the realization of simple management of the network, load balancing, dynamic migration and automatic fault separation, greatly enhance the stability of the network. However, due to the virtualization of servers, many traditional servers do not have any security, and it has a strong concealment, once the damage to its maintenance cost is very high, so, the article will discuss some common server virtualization risks and preventive measures.

1. Common security risks for server virtualization

1.1 There is a risk of information leakage

At present, although the application scope of server virtualization is constantly expanding, providing users with a lot of work and life convenience, but the user use information also increases the risk of being stolen. Survey data shows that more than half of the virtual machines are lower than their other physical servers. Gartner suggests that not everyone focused on information security in the initial server virtualization project. Usually, because the business department focuses on the backup and restoration of the data, it ignores the control over the security of the information. This increases the security issues of the system, but also with its own features; its location and parsing programs are more difficult and complex than the regular servers.

1.2 Server virtualization is easily affected by the underlying virtualization platform

A physical server is a virtual server through a virtual platform. New technologies have brought some inevitable flaws, but technically is often difficult to detect. At present, many famous virtual applications have appeared some security problems, most of which are caused by their own defects. In this way, hackers can attack and escape through the weakness of the underlying virtual platform, and use the host server for malicious programs to control or attack the host related to the host server, resulting in the security problems of the host network access and confidential information leakage.

1.3 Virtuality between virtuators limits the effectiveness of security policies

Because the virtual network between virtual machines does not be visual and controllable, the current security management measures are difficult to achieve. At present, in the market, the interaction between the virtual hosts is based on establishing the network card and the virtual switch, and uses the simulated data exchange function and the network communication function to achieve the purpose of virtualization. Basic network security protection devices, such as: firewall, intrusion detection and defense system, and network traffic control and monitoring system, network security protection equipment has a certain protection range, the above three types of network security protection equipment protection range is called the physical server north and south traffic or in and out of the traffic.

1.4 No virtual device isolation with different levels of security

Currently, under the premise of ensuring high security, business systems deploy more key and important systems to high security virtual machines; while high-level virtual machines and low-level virtual machines are in the same physical environment, cannot be independent state, which will pose a certain threat to the security of the virtual machine, resulting in high-level virtual machine is constrained by the weak virtual machine.

1.5 Missing control over the secure access VM hypervisor

The role of virtual machine manager is to plan, deploy and manage virtual machines, optimize and manage the various functions of virtual machine terminal to terminal, so pay special attention to the strict control of secure access in the process of using virtual machine manager. In the absence of proper security access control, hackers can through the IP address to control the virtual host, at this time, even if it is difficult to break the virtual host login password, also can launch a distributed denial of service attack, at this time, if the virtual host management program all resources are out, it means that the virtual machine in the system can't run.

2. Preventive measures for server virtualization security risks

2.1 Strengthen the prevention and control awareness of server virtualization security risks

First, the platform supervisor in the virtual working environment must recognize the server virtualization security issues, and guarantee the security from its source; second, compared with the general traditional platform, the virtual platform pays more attention to the security issues, the virtual platform integrates storage, computing, network and other technical functions, so when introducing the virtual platform, the work managers must pay attention to the application of security technology, comprehensively think and study the potential security problems in the virtual environment, and make preventive measures.

2.2 Repair vulnerabilities in the virtualization platform

Currently, the platform weakness of virtualization requires a permission level, so an attacker can upgrade the permission to destroy the virtual machine that it supports. In order to enhance IT security and convenient management in virtual environment, vulnerabilities and deficiencies in the system can be found through testing and assistance by virtual equipment manufacturers. At the same time, it is necessary to fix the vulnerabilities of the virtualization platform; refine the hardware structure of the virtualization underlying platform with the authorization of changing parameters, making the virtualization platform simpler and changing its configuration parameters without permission.

2.3 Enhance the monitoring of virtual computer network traffic

Firstly, the virtual network traffic is used to analyze and process the data in the data of the virtual network, in the virtual network, monitor the traffic in the system, and accurately locate the fault traffic, and further check the server virtualization problem.

2.4 Isolate virtual machines with different security levels

When you deploy a virtual architecture, you must divide the virtual network into two parts, internal and external. Inside includes all virtual services, which enables VLAN to segment various services, while the virtual machine gateway can virtualize the service flow in mobile phone groups on VSG; and can also effectively separate various virtual machines in the corresponding security domain. In addition, all systems face the same safety hazard in the same safety zone, so both high and low safety zones should not be in the same safety zone; even if one safety zone is destroyed, it will not cause any damage to other safety zones.

2.5 Increase the diversified access restriction management procedures

Diversified access restriction management programs can be user passwords, ID authentication, etc. first, When adding the corresponding access restriction, HTTPS, TLS, or password VPN should be used to set administrator login virtual machine privileges, To prevent malicious source IP addresses from being invaded; next, In a managed virtual environment, In accordance with their respective management responsibilities, Provide the necessary access rights to the virtual platforms in a virtual environment; An account that requires a temporary account, After completing the work in question, Take Back the account, Convenient for reuse; in addition, Third-party software can also be used to conduct a real-time evaluation of management in a virtual environment, Ensure the evaluation effectiveness and security of the virtualization platform.

Peroration

At present, the domestic network technology is in the stage of rapid development, and server virtualization is a new technology emerging in recent years, it can greatly facilitate the work of various industries, improve work efficiency, but there are also a lot of security problems. To prevent problems and problem strategy improvement, need to start from many aspects, such as strengthening the virtual computer network traffic monitoring, strengthen the consciousness of server virtualization security, isolation set different security levels of virtual machine, increase diversified access restriction management program, etc., to promote the security construction of server virtualization technology in our country, so as to promote the development of national economy, science and technology.

References

[1] Han W. Common potential and preventive security risks of server virtualization [J]. China Management Informatization, 2017,20 (23).

[2] Tang Y, Xiao L. Analysis of the key technologies of server virtualization [J]. Digital Communications, 2012,39 (3).

[3] Nie YF. Server Virtualization Technology and Security [J]. Digital Technology and Application, 2022,40(04):229-231.

[4] Hong YL. Server Virtualization Technology and Security Research [J]. Computer Knowledge and Technology, 2022,18(08):34-35.

[5] Chen SQ. Research on the hidden risks and countermeasures of Server virtualization [J]. Fintech Era, 2020,28 (06): 79-81.

[6] Liu X, Zhao HY, Liu XY. Server virtualization security risks and prevention [J]. Information System Engineering, 2020 (04): 60-61.

[7]Wang Y. Server virtualization security risks and precautions [J]. Information Technology and Informatization, 2019 (04): 25-26.