Discussion on Business Isolation Technology in the Cloud Computing Environment

Li zhiming[1,a], Guo jianbo[2,b], Ma jiang[3,c]

[1]Modern Education Technology Center, Hebei College of Finance, BaoDing,China

[2]Computing Center ,TangShan College, Tangshan,China

[3]Network&Education Center, TangShan College, Tangshan,China

[a]email: 13383328060@126.com, [b]email: jianboguo@qq.com, [c]email:majiang66@qq.com

Keywords: Cloud Computing, Network Security, Virtualization, Business Isolation

Abstract. Multi-businesses and multi-tenants are operating on a uniform cloud network when the concept of the cloud computing is popular today, the bearing network and key technology will be required to realize security isolation in the data from all variety of businesses.

Introduction

There are more and more successful business applications with the development of cloud computing today, Such as Google's Google APP. The Google APP provides more online office tools such as Gmail, calendar, documentation of enterprise version and cooperation platform and over two million enterprises have purchased the Google APP service. Sales force’s Force.com platform has provided a perfect development and environment for over 47000 enterprises to develop and test online application. Amazon EC2 product has leased different scale computing resources for users, and its revenue has exceeded over two hundred million yuan.

We have already known the three levels of service in the cloud computing, the picture shows below:

SoftWare as a Service
Platform as a Service
Infrastructure as a Service

Figure 1.The type of cloud computing services

In fact, these three levels have a certain dependent relationship from a technical perspective. A SaaS platform often depends on PaaS layers to complete development, testing and deployment, and it may be deployed in a IaaS computing resource platform.

Meanwhile, whether they are private clouds or public clouds, these clouds above are adopted as the design architecture of multi-tenants, the core of cloud computing platform has evolved into the delegation of many third-party application. A large number of different enterprise data are running in the same set of systems, on the platform or infrastructure. Therefore, the user's privacy and safety of different businesses is an important security challenges in the cloud computing environment.

New security challenges of virtualization

The use of resource order on the cloud computing platform is an important feature. Its CPU resource is often not fully utilized when a server is only running a kind of business, the CPU with big purchase is still sleeping in a rack, it does not work with huge consumption power.

Most customers want to deploy virtualization in order to maximize the efficiency of the original server CPU to some extent. Virtualization software (such as VMWarevsphere, XEN, KVM, etc.) is a good solution to this problem, a CPU can be assigned to more virtual machines for utilization simultaneously in the virtualization software. The server with deployment of virtualization software, its CPU utilization are often able to grow from less than 10% to 70%.

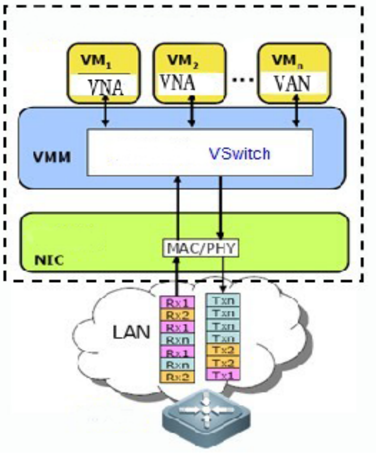

Figure 2. The Virtualization implementation

But in this environment, network virtualization has become the new bottleneck. As above shown, when more and more different types of virtual machines are running on a physical server, their input and output data will be crowded in an I / O channel, which is obviously unreasonable. Moreover, the traffic flow of different virtual machines come from the same physical network card, therefore, it is difficult for the switch to identify the flow, which results in the difficult implementation of QoS guarantee and security isolation.

Multi-services and multi-systems are running on a physical machine, security issues between the isolation are also an important challenge even though virtualization is so popular today.

The requirements of the bearing network for virtual machine migration

Another important feature for virtualization is the migration technology of virtual machine, the application services can be seamlessly migrated through technology from one virtual machine to another, and this technology can address the original problem which can not be met when the application needs were enhanced. Virtualization software can make two virtual machines dynamic migration not only within the same physical server but also within the different physical server. And it also maintains the operational status prior to migration (such as TCP session state), requiring another virtual machine to keep the original IP address, at the same time it keeps network gateway constant before and after migration. This requirement makes it more and more difficult to maintain a layer 2 network when facing enlarging data center.

It is hoped that there is a larger layer 2 network from the perspective of migration, but from the perspective of security there is not only layer 2 network but balancing between the two is also an important challenge.

The traditional security isolation

At present, many data centers on business and data isolation problem usually have no pressure, which can not be communicated to the network department. Business sector can solve this problem by using IP Tables, etc. on the server to control the IP packet filtering and firewall configuration. A single physical server will contain several virtual machines, and each virtual machine requires considerable security policy. Server performance will be consumed much by using this method. Therefore, the business sector begins to consider other ways, and then assign this work to the network department to complete when the server performance was influenced widely.

Rational VLAN and IP address design will be carried out when Networks department took over this network design. As the core of cloud computing platform is applied and delegated by many third-parties, business isolation is the first problem to solve, otherwise it is impossible to ensure security of third-party applications and data. The business isolation can be guaranteed that all variety of the business server can be separated from the access layer from the perspective of network.

Application may be split in a different VLAN and network when it becomes larger if the VLAN and IP address planning are set relatively smaller. Therefore, the requirements such as clustering, virtual machine migration must cross-VLAN and layer 3 network. Furthermore, if the virtual machine is designed according to physical server, it will soon be exceed the scope of the original line scope with a larger proportion of the virtual machine, which make the application not expand.

At present the size of new data centers are built larger and larger, and the number of applications born becomes more and more although most of the scale is still small, but no one can predict which number of users will increase, which requires the elasticity of computing resources.

Since the above problems brought by the controlling business through the VLAN and IP address design, then a larger Layer 2 will be set up and this data center is placed in this Layer 2 network. Therefore the special requirements such as larger business and migration will no longer be a problem. business isolation can be achieved through the switch PVLAN technology and ACL technology. But the subsequent issues will bring more troubles.

Firstly, to what extent a Layer 2 network can bear. Technically speaking, the larger layer 2 will test the core network equipment, a large number of broadcast packets and spanning tree packets will impact on the CPU of   the layer 3 core equipment. In theory, the size of a Layer 2 network hosts will be controlled in 2000 or less, of course, including the number of virtual machines, because the size is not enough for data centers in cloud computing.

Secondly, the switches actually do not know where the servers are when they are virtualized,. In server virtualization environment, the switch can not distinguish virtual machine from port directly. The server virtualization platform must support PVLAN TRUNK, or virtual switch built-in a physical a server must support PVLAN TRUNK if virtual machine is isolated by the PVLAN. The ACL policy above the switch will no longer work if virtual machines visit each other on the same physical machine.

The new technology of cloud computing era

International standards organizations and equipment suppliers are actively put forward a solution in response to the challenges of the network with this new application and new cloud computing environment.

The most typical techniques are: TRILL technology proposed and developed by the IETF and the 802.1Qbg technology in the bridge virtualization technology operated in early 2010 by the IEEE organization. TRILL technology has solved how a large data center network maintains a Layer 2 network. The 802.1Qbg has solved the communication problem between virtual machine traffic aggregation in virtual server and the external physical switch

Equipment suppliers represented by Cisco also put forward a similar solution actively, such as Fabric Path technology which owns a technical feature on the Cisco Nexus switch. Its goal is to solve more path and address space issue in the context of the Layer 2 environment. The Cisco's 802.1Qbh technology also solves the same problem just like Qbg technology. Although FabricPath and TRILL are compatible, 802.1Qbh and 802.1Qbg compatible too, an equipment supplier can not be bound by a large data center networks. Therefore, a unified standard technology is adopted to avoid possible compatibility problem to the maximal extent.

Layer 2 network is made bigger by TRILL technology in a larger Layer 2 network because simplifying IS-IS protocol data by TRILL equipment can make “routing” transfer, therefore, it is not necessary to worry about the core equipment CPU; Certainly it is also not necessary to worry about the size of MAC table because the TRILL equipment can select the learning object of MAC. And it is not necessary to worry about the actual link issue under the multi-path because TRILL technology combines ECMP technology.

Meanwhile, the 802.1Qbg technology can distinguish traffic flow issues of the virtual machine, develop a ACL policy configuration server and components of virtualization management platform, and also achieve dynamic migration of security policy when the virtual machine is migrating.

Conclusion

Cloud computing has been flourishing which can not be prevented. At present, all variety of security isolation technologies will be prevalent in a certain period of time in order to facilitate the efficient completion of the isolation of data and business within all types of cloud computing applications and cloud computing data centers.

But with further expansion of the application and scale, the 802.1Qbg, TRILL as new technology representatives will be the new safe, isolated application force rapidly and widely in the cloud computing environment.

Acknowledgement

In this paper, the work was supported by the Research Program of Hebei Education Department under Grant No. 2011218.

References

[1] Qinlu He, Zhanhuai Li, Xiao Zhang. Analysis on the key Technology of Cloud Computing . 2010 International Conference on Future Information Technology and Management Engineering. October 9-10, 2010:426-429

[2] LIANG Shuang.Design and realization of cloud computing framework model based on SOA.Computer Engineering and Applications，2011，47（35）：92-94.

[3] Buyya R，Yeo C S，Venugopal S.Market-oriented cloud computing：vision，hype，and reality for delivering IT services as computing utilities[C]//10th IEEE International Coference on High Performance Computing and Communications，2008，9：25-27

[4] Wang Long Wan Zhenkai. Research on Service-oriented Ar chitecture Cloud Computing and its Implementat ion. Computer & Digital Engineering.

[5] LI Zhen, DU Zhong-jun. Improved Map-Reduce Model in Cloud Computing Environment. Computer Engineering. Vol.38 No.11- June 2012:27-29.

[6] Youseff, L, Butr ico, M, Da Silva.Toward a Unified Ontology of Cloud Computing[C].2008 Grid Computing Environments Workshop.