Proceedings of the 12th INDIACom; INDIACom-2018; IEEE Conference ID: 42835
2018 5th International Conference on "Computing for Sustainable Global Development", 14th - 16th March, 2018
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

A Collaborative Design for Securing IaaS in Clouds

Ahmad Raza Khan
Department of Information Technology
Majmaah University, Kingdom of Saudi Arabia
Email ID: ar.khan@mu.edu.sa

Suliman Alazmi
Department of Computer Science
Majmaah University, Kingdom of Saudi Arabia
Email ID: sa.alazmi@mu.edu.ss

***Abstract*— Cloud computing has revolutionised the provision of software software technologies and is still growing strong with new applications in many areas. As most of the businesses would like to switch over to the cloud but their primary concern is about the security of the cloud as the hardware resources are deployed at the location of the cloud service provider. Most hardware resources are virtualized on hardware servers, so it becomes a critical issue for the businesses to switch their project on to the cloud infrastructure and to deploy their projects on a virtualized environments, which are likely to break down if the physical hardware has any issues. In this research paper, we are focusing on how we can create a secure environment for the virtual machines which are deployed as virtual infrastructure by the cloud computing service provides. How they can configure their virtual machines securely and with reduction of most likely attacks which can cause a virtual machine to stop running on the network. We are also providing step by step deployment mechanism for firewall web service which are provided by some cloud computing service providers.**

Keywords—Virtual Machine, Virtual Infrastructure, Virtual environment security, firewalls, virtualization technology.

I. INTRODUCTION

As businesses are growing day in and out, it becomes essential to cater to the needs of hardware and software resources which are required by the organization so most of the companies are concerned about the capital expenditure and the return on the investment which they will be making on the capital. As businesses grow they require more computation power to serve the users who are using the business applications thus companies need to buy considerable servers to cater to the requirement of the users who are using the projects created by the companies. Infrastructure can be built physically on the premises of the company but this will involve a massive investment on the space which is required to deploy the hardware resources needed for the company and also maintenance of the hardware is a significant concern. Thus, companies are now trying to switch their IT infrastructure requirement to the cloud so that the deployment and the physical installation and configuration of the hardware is not required and no need to maintain the hardware on premises. Some of the major cloud computing services provide provide IAAS, SAAS and PAAS as a service to the customers who need to use any one or all of the services (1). Businesses require IAAS (Infrastructure as a service) service to scale development process on demand and also the programmers require good configuration machines to run the programs and deploy the project online so that the customers can use the business products without any latency in the application. As the demand of the application increases or the number of users using the application increases there is a requirement by business to increase their infrastructure to serve their client better and provide a flawless experience to the end users.

Cloud service providers provide IAAS as a package to organizations can consume infrastructure as an amenity and deploy VM's online on the cloud facilitators' physical infrastructure. Businesses can deploy virtual machines online and also scale their machines online when the demand of the end users increase this will reduce capital expenditure which is required to buy servers and other resource and deploy hardware on premises of the business. Major concern for most of the businesses using IAAS is security of the virtual machines of the virtual environment where their application is running (2). We are proposing a comprehensive architecture for securing the virtual environment which the companies would like to use by provisioning virtual machines online with minimum security configurations which will protect the virtual environment from getting attacked by the attackers.

II. SECURELY CREATING VIRTUAL MACHINE

Virtual machines are important part of the cloud computing environment all cloud service provider deploy virtual machine's to cater to the business needs some of the cloud service providers using virtualization as service to implement the IAAS as infrastructure.

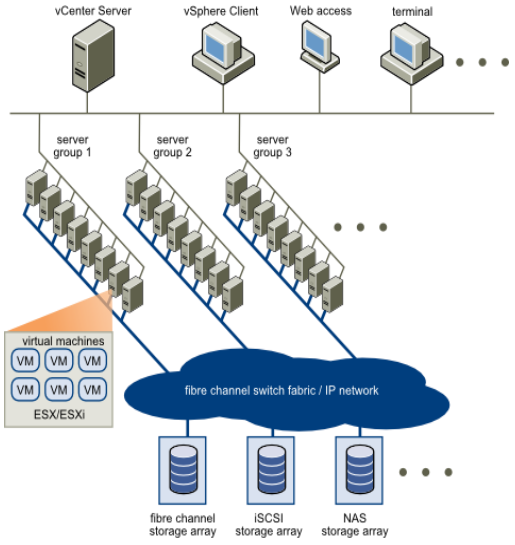

Fig. 1. Creation of virtual machine in cloud environment.

 ISSN 0973-7529; ISBN 978-93-80544-28-1

A. Virtual Machines Creation

Many Cloud facilitators such as Amazon Cloud, Microsoft Azure, Google Cloud Platform and Digital Ocean provide IAAS as a web service business can use IAAS services and create virtual machines online and deploy applications within no time (3). Companies can select any cloud service provider and then follow the steps for creating virtual machine online. As most of the cloud service providers' offer to Pay as you go model so based on the usage of the device and the uptime of the machine the business need to pay online to the cloud services provider for the IAAS (Infrastructure as a service) which he is consuming.

B. Configuring VM with security

As security of the VM (Virtual Machine) is one of the most important concerns for the businesses who are using IAAS as a service offered by the cloud service providers. It's important to add a layer of security for the VM which is being created or deployed in the cloud environment. While configuring the VM online, it's essential to get a licensed copy of the operating system which the end user would like to use. In some cases, the cloud service provider may ask the end user to upload there. ISO image and configure the operating system using the. ISO image file. Once the operating system is installed on the infrastructure, it needs other security provisions such as setting up firewalls and the antivirus software. The end user can connect to the virtual machine by securely entering the two-factor authentication mechanism provided by the cloud facilitator (4). A remote connection can be established to the infrastructure created online by the business. It's easy to manage the online infrastructure and scale the IT infrastructure when required by the business. Some port blocking open source software solutions can be used while configuring the VM so that the attackers do not find ports to attack the virtual machine.

C. Scaling the IT infrastructure on the fly

It's important to select the option of scaling the IT infrastructure on the go so that the applications of the businesses which are running online need no downtime and scaling of the IT infrastructure can be done seamlessly businesses who are running Realtime systems on the VM need to configure the VM scalability option and securely scale the VM's based on the user's demand. As the number of users using VM's is increasing overtime then the scaling of the IT infrastructure should also automatically scale. It's essential that infrastructure changes and the VM's configuration change if any are notified to the business owner's so that action which is recommended by the cloud service provider to the business owner can be considered for action by the business representatives. Configuration Security of the VM's should be maintained such that when the scaling of the IAAS is going on the VM's will not stop running and the applications will not be affected when the scaling process is going on. Virtualization technology is one of the most secure methods for creating virtual machines online some of the cloud service providers are using VMWare solution for deploying the IT infrastructure online and Virtual machines online as the file product of the virtual machine created online is a file which has an extension of.VMware is a compressed file which is not easy to crack and requires specialized knowledge to run the configuration online, so it's not easy for the attackers to attack this file type and its system online. Thus, businesses can trust running and creating IT infrastructure online without worrying about the attacks on the application software.

III. Configuring and Deploying Virtual Firewall

Next layer of security is firewall which is also provided as a service by some cloud service providers firewall can be configured as one of the modules when deploying a virtual infrastructure on the cloud computing environment there are several components in the cloud infrastructure which can be configured to protect the privacy and security of the virtualization environment on which the cloud VM's are deployed. Virtual firewalls act as barriers and protect the VM's from getting attacked and also from various malicious viruses which may affect the VM's and their software's. Thus, firewalls can be configured on demand to protect the VM's which have been deployed by the businesses for running their applications in the cloud environment.

The virtual firewall has many configuration steps and also the businesses who are opting for a virtual firewall to protect their VM's need to pay constructed on the convention of the firewall. When the virtual environment running the applications are working and running, then the firewalls are protecting the VM's from getting attacked by intruders and malicious software (5). When the VM's are not up and running, then there is no need to run the firewall to protect a VM's file. Thus, businesses who are running Virtual firewalls as a service will charge others based on the runtime of the firewall.

A. Agreement between the company and the businesses (Service level Agreement SAL)

Most of the cloud service providers offer service level agreement which needs to be signed between the cloud computing company and the businesses who are consuming the cloud services. This agreement is called service level agreement (SLA) this document demonstrates that the cloud service providing company will give 99.99% uptime as some of the business have critical applications running on the cloud servers.

B. Unified Computing

- Most of the computing resources are scattered over the cloud services providers and these services which are consumed by the businesses need to be unified billed together as one system.
- Cloud service providers can collaborate together and share some common function so that the end users or consumers of their services find one center point for billing all the products which are being consumed by the businesses. All computing resources will be available at one point to the businesses and their applications.
- Aggregation of all subsystems can be done using the virtualization technology and security can be

maintained so that the business applications running online do not face any issues related to data breaching and security flaws. Information will flow between various virtualization servers. Security of information is an important point to consider while deploying the virtual machines on the cloud premises.

- Zero downtime for applications is also important as some businesses have Real-time data collection and transactions going on. These businesses need their applications to run without any downtime and critical issues in the infrastructure provided by the cloud service providers.

IV. Virtualization Platform and Its Security

Virtualization technology is a collaboration of many sub-technologies most of the cloud service providers deploy virtualization environment to create cloud computing resources available as web services to the businesses. Virtualization combines many standalone subsystems into one composite system this computing resource which is created using the virtualization technology includes (networking, computing, storage and compute power) into one system so that the businesses can comprehensively use all the technologies together for deploying their applications online on the cloud computing servers. Physical hardware construct skins the complexity of deploying and managing physical space and physical servers on the premises of the business thus this will provide simplicity for the consumer to scale the computing resources without worrying about the physical deployment issues and concerns (6). Also, the security layers which are required to maintain the physical space and the servers on premises.

Most of the virtualization technologies use hypervisor's which are responsible to host the virtual machines. VM's are isolated from each other and their components are isolated from other VM's. Virtual machines are running on the hypervisors and virtual machines are configured with security rights to be accessed by the users. The system administrators is responsible to configure the virtual machines and to create accessibility rights for the users of the virtual machine the rights create by the system admin will be deployed on all the virtual machines and users can access the virtual environment online when required by providing credentials provided by the system administrator for accessing the IAAS over the cloud.

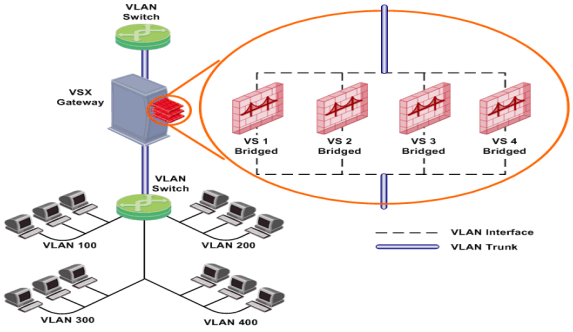

Fig. 2. VSX firewall gateway.

A. *Virtualization environment monitoring and control*

Most of the virtualization environment created by the cloud service providers need to be monitored by the company as businesses consuming the cloud environment need their IAAS to be running 24x7 and without any issues it's important for the cloud service provider to monitor the VM's environment and the uptime of the VM's sometimes physical server issues can bringdown an enterprise server this may case loss to the enterprise as they may totally rely on the cloud environment to run their business. The service provider needs to keep track of the start time of the virtual configuration and the running state of virtually configured machines and if the virtual machine needs scaling based on the resources which are being consumed by the business. The service provider will scale the virtual machine and inform the business consuming the virtual machine about the scaling this scaling of resources should be done without shutting down the virtual machine and the end user should not get any latency in their work. It's important to maintain security using virtual firewalls and gateways which help protect the virtual machines from getting attacked by the intruders and other malicious software's all the VM's should be constantly scanned for any malicious activities and security issues.

B. *Secure Virtual Networks and Virtual gateways*

Virtualization technology provide virtual networks which can be accessed online. Configuring virtual networks is also an important task which can be done by the system administrator. VLANs can provide isolation between virtual machines and thus improve security in a hypervisor environment. The VMWare VLAN setup helps the administrator to configure virtual machines on different VLANs and also businesses are isolated over the VLANs this will enhance the security level of the virtualization environment. Logs can be generated which describe which VLANs have been create and which have been used recently by the businesses. A configuration summary is also generated by the system administrator to keep track of what issues were faced while configuring a secure VLAN and how they were resolved. Integrity of the virtual machines and its components is also important and the service provider is responsible to integrate all the components of the virtual environment.

C. *Virtual machine deployment threats and collaboration issues*

Virtual machines are deployed on physical hardware systems which are running virtualization software's such as hypervisors and other supporting sub-systems. Its important to correctly deploy the virtual machine and configure it properly so that the correct resources are accessed over the network all sub-components of the virtual machine need to be configured and communication between the sub-systems need to be established so that an effective and efficient virtual machine can be created which can be used by the businesses around the globe most of the IAAS service providers have all the hardware components in place and the system administrator is required to configure the hardware resources virtually over the physical system to generate a virtual environment which is requested by the business user. The cloud service provider will

configure the VM's based on the requirement of the business some time it's also important to share resources between VM's this will be a crucial point of contact where the attacks can be targeted so when VM's communicate with each other a secure channel for communication should be open so that information flow can be encrypted and no attacker can hack into the VM and steal information.

V. Security Architecture for IAAS

The security architecture compromises of three major components which need to be integrated while deploying the IAAS as a service by the cloud computing companies this model will enhance affirmation in the cloud security environment and will help business build they trust in switching to the cloud environment easily the three major components which need to be employed by the cloud service providers include.

A. Secure Configuration of Virtual Components

The configuration of various sub-components should be done securely if the loose coupling is there between the components then the system will have many flaws which the attackers can target and thus break into the system very easily. IAAS components from various vendors need to be tested and then integrated into the cloud environment if the any component is found not functioning as desired then that component must be easily replaced with other working component and the component which is removed due to some issue needs to be tested for possible issues (7). All components when deployed need to be monitored carefully so that if any component is not working as desired can be brought down and thus will not affect the functioning of the virtual environment. Sometime the virtual components may not function accurately due to the failure of some physical component in the physical servers this also needs to be monitored carefully and logs files should be maintained to monitor the activities of the physical server and the virtual configuration.

B. Security restrictions for the end users

System administrators are responsible for giving user rights to the virtual environment that is provided by the cloud facilitator. The administrators are solely responsible for the access rights and configuration changes if any by the consumer of the Virtual machines and about the virtual environment which is assigned by cloud facilitators thus most of the companies should focus on the end user licenses which is an important contract between the business consuming the virtual machines and the service provider giving access to virtual machines. The VM's should be kept isolated from other business users VM's so that the malicious software's if any in one VM will not affect the other VM's.

Acknowledgment

This research would not have been possible without the support of various hardware and software resources which have been provided by the Dean "Dr. Hisham Al" we would like to express out science thanks to all department members who have kept us motivated and guided us in the right direction to accomplish this research work.

References

[1] Wesam Dawoud, Ibrahim Takouna, and Christoph Meinel, "Infrastructure as a Service Security: Challenges and Solutions, " The 7th International Conference on Informatics and Systems (INFOS), pp. 1-8, March 2010.

[2] Mohamed Firdhous, "A Comprehensive Taxonomy for the Infrastructure as a Service in Cloud Computing," Fourth International Conference on Advances in Computing and Communications, pp.158-161, Aug 2014.

[3] Dan Gonzales, Jeremy M. Kaplan, Evan Saltzman, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds" IEEE Transactions on Cloud Computing, Volume: 5, Issue: 3, pp.523-536, July-Sept 2017.

[4] Sarika Jain, Prachi Tyagi, Siddharth Kalra, "A Novel Approach to Cloud Computing: Infrastructure as a Service Security," 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 501-504, Sept 2016.

[5] S. Berger, R. C´aceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "TVDc: Managing security in the trusted virtual datacenter," ACM SIGOPS Operating Systems Review, vol. 42, no. 1, p. 7, 2008.

[6] W. Mao, A. Martin, H. Jin, and H. Zhang, Security Protocols, ser. LectureNotesinComputerScience. Berlin,Heidelberg:SpringerBerlin Heidelberg, 2009, vol. 5087.

D. G. Murray, G. Milos, and S. Hand, "Improving Xen security through disaggregation," ACM/Usenix International Conference On Virtual Execution Environments, p. 9, 2008

