Implementing Security Rules, Safeguards, and IDS tools for Private Cloud Infrastructures

Author: Aleksander Okonski – aleksander.oko@gmail.com
Supervisor: Salman Toor
Review: Bjorn Victor

Contents

1 Background

The cloud computing space has grown over the last several years. Business and Universities are looking at solutions to migrate their existing infrastructure to the cloud. There are several reasons for this type of business shift: costs, scalability, reliability [7]. The cloud offers some precedented advantages to a standardized computational model. One is able to pay for only the resources used, with more resources added/removed depending on the demand. Another advantage is the ability to spine up/destroy several machines with little overhead. Several companies are fronting the cloud revolution including Amazon, Google, Microsoft, and Digital Ocean.

1.1 Cloud Models

In the cloud computing space several computational models exist [1].

- Software as a Service (SaaS) allows for the user to utilize applications (I.E. Email, games, etc.) without the need to set up / worry about the underlying infrastructure.
- Platform as a Service (PaaS) give the user the ability to create applications (I.E. Web servers, databases, etc.) without the need to create the entire system from the ground up.
- Infrastructure as a Service (IaaS) gives the users a basic virtual machine with the user needing to set up all necessary functionality.

1.2 Cloud Infrastructure

At the most fundamental layer a cloud computer is a server running in a data-center that has a hypervisor which then contains and runs another operating system. These hypervisores are the backbone of cloud computing allowing several virtual environments to use the same hardware. There are several different hypervisors to choose from (Xen, Oracle VirtualBox, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V) with each having similar outcomes through different approach to the problem. To control the users and virtual machines many cloud providers (Amazon, Google, etc.) have created proprietary solutions. However, NASA and RackSpace Hosting [4] have created an open source version called OpenStack.

1.3 Cloud Roles

When cloud computing first started to take off, the main type of computing resource provided was IaaS in the public cloud [2]. This started to change in the recent years when two new types models for cloud computing emerged. Public and Hybrid clouds allowed for companies to utilize the power of the cloud while still having some or all of there resources located in their own data centers.

1.4 Cloud Computing vs Standard Models

Cloud computing has some distinct differences from regular computing.

- Systems do not usually stay active for long. Users will provision and destroy systems with a high turnover.
- Users may spin up several machines at once.
- There may not be a dedicated team used to ensure up time / health of systems.
- Users will usually have full control of the systems.

Cloud computing also has a different threat model compared to a normal dedicated server [12, 9, 8]. With normal server infrastructure the infrastructure and system are built once and then ran for extended periods of time. The systems themselves are not refreshed or rebuilt as happens in the cloud.

2 Related Work

In this work we will be looking at ways to protect VM clusters by ensuring proper configuration steps are setup and used with the addition of looking at ways to implement an IDS solution into the cloud environment. Before starting the work, we looked into previous work done in this field. Cloud security had been a hot topic in recent times therefor several papers have been written [12, 9, 8]. These particular papers focus on the different aspects and concerns that are present when running in a cloud environment. They are a nice starting point to look at how the threat landscape in the cloud differs from the slandered model. An important distinction of how information is

treated differently in a centralized and cloud environments is talked about in "Assessing Cloud Computer Security Issues" [12]. The three staples of information security are confidentiality, integrity, and availability. In the cloud new difficulties come up for each of these classifications as data in the cloud is now accessible to more individuals. The second set of articles looked at was about intrusion detection systems (IDS), more specifically how these can be used within the cloud [6, 10]. These articles did not focus so much on implementation as they were focused more on the theory. An interesting comparison that shows the advantages and disadvantages for different IDS systems is table 2 in [**?**, SurveyOfIDS] This is the basis for the types of IDS solutions that were chosen for this project. As this work was primarily focused on OpenStack, one particular IDS conference talk was used as a starting point for this research [5].

3 OpenStack

OpenStack is an open source platform for cloud computing [11]. OpenStack is built of many components that are designed to provide a different set of services (Nova, Neutron, etc.) the full list can be found on the open stack website located here. OpenStack is very scalable and diverse system that can be arranged to fit the needs of any cloud environment. For this project we ran OpenStack newton version 15.0.0.0.rc1. OpenStack is very modular with several core features running as the backbone of the software. The features that were used for this project were:Nova, Neutron, and Swift.

4 Security

The field of computer security is large and diverse [**?**]. The general focus of computer security is to ensure that computer systems follow the CIA model of confidentiality, integrity, and availability. "The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability and assurance." [3] The disciplines that are focused on in this paper include: intrusion detection systems, network security, and system security. Intrusion detection systems come in two main

forms, host based and network based. A host based system runs on the host and attempts to detect any security threats on the host machine. A network based IDS is connected on the network and inspects network traffic, trying to find threats by inspecting network traffic patterns. Both of these systems have advantages and disadvantages. With a host based system software must be installed and configured on each system. In a network IDS system the packets are monitored for unusual traffic patterns. There are disadvantages to this type of solution also, mainly network traffic can be encrypted and the overall volume of traffic encountered. Some examples of network based IDS tools are Snort.

5 User Recommendation

The first stage of this project involved setting up user recommendations for configuring a secure VM and understanding some security features in the OpenStack platform.

6 Design Implementation

References

[1] Cloud computing.

[2] Cloud history.

[3] It security architecture.

[4] Openstack.

[5] unobtrusive intrusion detection in openstack.

[6] Bhavesh Borisaniya Hiren Patel Avi Patel Muttukrishnan Rajarajan Chirag Modi, Dhiren Patel. A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 2013.

[7] Tharam Dillon, Chen Wu, and Elizabeth Chang. Cloud computing: Issues and challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference*.

[8] Ronald L Krutz and Russell Dean Vines. *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing, 2010.

[9] Ankur Mishra, Ruchita Mathur, Shishir Jain, and Jitendra Singh Rathore. Cloud computing security. *International Journal on Recent and Innovation Trends in Computing and Communication*, 1(1):36–39, 2013.

[10] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino JúNior. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications*, 36(1):25–41, 2013.

[11] Wikipedia. Openstack — wikipedia, the free encyclopedia, 2017. [Online; accessed 30-January-2017].

[12] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation computer systems*, 28(3):583–592, 2012.