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 [5]. The cloud offers some precedented advantages to an standardized computational model. One is able to pay for only the resources used, with more recurses 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 different 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 he ground up.
- Infrastructure as a Service (IaaS) gives the users a basic virtual machine with the user needing to setup all nectary functionality.

1.2 Cloud Infrastructure

At the most fundamental layer a cloud computer is a server running in a datacenter that has a hypervisor which then contains and runs another operating system. These hypervisores are the backbone of cloud computing allowing several different 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 [3] 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 recourses located in there own datacenters.

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 uptime / 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 [8, 7, 6]. 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 [8, 7, 6]. A good starting article [4]

References

[1] Cloud computing.

[2] Cloud history.

[3] Openstack.

[4] 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.

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

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

[7] 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.

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