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

Aleksander Okonski
aleksander.oko@gmail.com

1 Background

Cloud computing has revolutionized the way computational resources had been offered before. The philosophy of having dedicated in-house resources transformed into pay-as-you-go model for accessing large amount of computational and storage resources. Together with number of advantages, the technology also brings some serious challenges for the community. Security is one of the fundamental concerns both for the users and service providers.

UPPMAX is a local HPC centre at Uppsala University. Together with HPC setups, UPPMAX is also participating in national level cloud initiative called SNIC Science Cloud (SSC). SSC is an community cloud environment for Swedish academia, consists of three geographically distributed regions (HPC2N, C3SE and UPPMAX). The SNIC Science Cloud uses OpenStack as its underlying cloud framework. OpenStack is an open source cloud computing solution that focuses on Infrastructure-as-a-Service (IaaS). This service is now expanding to the classroom where students are using SNIC cloud for cloud computing courses. As the SNIC Science Cloud becomes more poplar among researchers and students the security surface gradually expands. As machines are provisioned, and deployed into this hybrid cloud they will be accessible from the Internet. This poses a security risk as these users may not be aware of security rules and proper guidelines to use when managing virtual machines (VMs) in the cloud. There have already been issues with several VMs being infected and joining bot-nets. It is therefor necessary to look into the ability to protect the SNIC Science Cloud and ensure users are following best practices.

2 Proposal

The proposal for this project is to assess and implement a three step solution to monitor and protect private cloud infrastructures based on Openstack solution. SSC will be the reference infrastructure. The first part will be to identify and write a set of recommendation for setting up and provisioning VMs. The second part will be to implement a watch dog VM that would monitor the other VMs in the cluster externally for misconfiguration. This VM would be part of the deployed OpenStack cluster. The final part would be to look into implementing a system that would allow the internal processes of a VM to be monitored for internal configuration problems and threats.

3 Tasks

1. Provide recommendations for secure VM provisioning on private cloud infrastructures.
2. Create the Watch Dog VM to aggregate logs and scan for misconfigduration.
3. Ensure that the Watch Dog VM is properly tested and can be extended.
4. Study and implement a way to view VM activities and internal configurations.

4 Time Line

1. Week 1-2 Literature survey and write documentation on different specifications that are needed in the cloud.
2. Week 3-6 Start building the Watch Dog server. Week 7 Finish up and test the Watch Dog server.
3. Week 7 Finish up and test the "Watch Dog" server.
4. Week 8-10 Start looking into ways of implementing a hypervisor based solution for viewing VM activities and configuration.

5. Week 10-17 Implement a method to view internal VM activities and configurations.

6. Week 17-19 Fix bugs and ensure that all created components are working as expected.

7. Week 20 Finish up the report and prepare for presentation.

References

[1] https://nmap.org/

[2] https://github.com/pyKun/openstack-systemtap-toolkit

[3] https://wiki.openstack.org/wiki/Successes

[4] https://openstack-in-production.blogspot.se/2015/09/ept-huge-pages-and-benchmarking.html

[5] https://www.openstack.org/summit/vancouver-2015/summit-videos/presentation/unobtrusive-intrusion-detection-in-openstack

[6] https://en.wikipedia.org/wiki/Security_information_and_event_management
https://www.splunk.com/en_us/download.html

[7] https://github.com/pyKun/openstack-systemtap-toolkit
https://wiki.openstack.org/wiki/Successes
https://openstack-in-production.blogspot.se/2015/09/ept-huge-pages-and-benchmarking.html