Secure Cloud Computing Infrastructure for K-12 Education

Dr. Connie Justice, Indiana University Purdue University, Indianapolis

Dr. Connie Justice is a Clinical Associate Professor in Computer and Information Technology (CIT) at the Purdue School of Engineering and Technology at Indiana University Purdue University Indianapolis (IUPUI) and a faculty member of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. Professor Justice has over 20 years experience in the computer and systems engineering field. Professor Justice is a Certified Information Systems Security Professional, CISSP. She created the networking option and security option for CIT majors and a Network Security Certificate Program. She has also designed and modified many courses in networking and networking security. Professor Justice is noted for her creation of the Living Lab, an experiential learning environment where students gain real world experience running an IT business.

Dr. Justice takes extreme pride and is a great innovator in the area of experiential learning and service. Experiential learning and service contributes to the integration of theory and application by creating an environment where the students learn by doing or apply their theory in service learning projects, practica, internships, games, and simulations. The Living Lab for CIT was created out of the need to provide a business environment for students to give them a taste of a ”real” IT environment. A secondary purpose is to provide service to internal and external clients. The Living Lab has served many internal and external clients.

Dr. Justice has consulted for and managed IT departments in small and medium sized businesses. Her areas of research include: experiential and service learning, information and security risk assessment, risk management, digital forensics, network security, network and systems engineering, network and systems administration, and networking and security course development.

Miss Nichole McFarland, Indiana University Purdue University, Indianapolis

I am a student at IUPUI perusing my Masters degree in Information Security.

Secure Cloud Infrastructure

Nichole McFarland, Dr. Connie Justice
Purdue School of Engineering and Technology, IUPUI
Indianapolis, IN 46202, USA
mcfarlini@iupui.edu, cjustice@iupui.edu

Abstract

With cloud computing becoming more and more popular among businesses, there has become a higher demand for security in the cloud. K-12 school systems have a lack of IT resources and support to securely store and share data, thus making cloud services an attractive option. Additionally, there is increasing pressure on school systems to provide information for students and parents that require access to the information stored on school networks. Therefore, cloud services are a viable option for K-12 school systems to alleviate the administrative overhead and to provide access to necessary information for students and parents. This applied research project is an experimental design for addressing the issues that the K-12 school systems face. The secure cloud project consisted of four databases and three nodes. The databases were Keystone, Glance, Nova, and Neutron. First, the Keystone database handled the identity service. The second database was the image client, Glance. Images were launched through this database following a correct authentication token. The third database was Nova. Nova handled all the compute services for the controller and compute node. Fourth was the Neutron database service, which handled all the networking agents that traveled through all three nodes. There were three nodes; a compute node; a controller node; and a networking node to run the cloud. The controller node is the first to be used by verifying identity of the user. It then travels through the management network to the compute node that operates the virtualized network. Traffic between will be monitored by the network node to assign DHCP to each session. Future work to the secure cloud include: a security node to filter through the traffic to alert when an issue arises; and another server to allow for more space to be allocated for virtual machines. These improvements will enhance performance by segmenting information on a different secure network.

Background

Lack of funding has traditionally been a problem in the K-12 educational systems. Therefore, advancing technology in the school systems has been a significant problem. The addition of Internet technologies brought the price point of high speed Internet connections within reach of K-12 schools Parents, educators, and students were demanding services to be delivered via the Internet whether they were onsite or remote and using mobile and/or desktop devices (Pierce and Cleary, 2016). With cloud computing becoming more and more popular, K-12 educational institutions were looking at ways to benefit from combined resources (Hartmann, Braae, Pedersen, & Khalid, 2016). These institutions, to get the most out of the small budgets they were dealt, felt pooling resources made good fiscal sense (Chandra & Malaya, 2012;Bennett & Weber, 2015; Hartmann, Braae et al., 2016; Pierce & Cleary 2016). As the demand for cloud computing increased, logically the need for security in the cloud became increasingly important

(Reidenberg, Russell, Kovnot, Norton, Cloutier, & Alvarado, 2013). Per Reidenberg, et al. cloud services were poorly understood, and clients didn't understand service level agreements (SLA's). Additionally, K-12 schools didn't understand how to address parental notices, consent, and access to student information, and protect personally identifiable information (PII). Schools with a lack of staff and smaller classrooms would benefit from virtualization. Classes could be taught remotely allowing for more students to attend. Collaboration with other teachers from other parts of the country or the world would allow for a greater spectrum of course content and global knowledge. Parents and students would be able to access grades and assignments portals respectively. The cloud would allow the school to run their environment to fit their exact needs. All applications and programs would be stored on a central location which would allow for less higher computing devices. These factors would save resources for the school.

This research project started with the K –12 school systems having a lack of IT resources to safely and securely store and share data. The client requested a cloud server prototype that could serve the purpose. Additionally there was increasing pressure on school systems to provide information for students and parents that required access to their networks. The secure cloud was an experimental design for addressing the school systems' issues.

This project consisted of four databases and three nodes. The databases are Keystone, Glance, Nova, and Neutron. First, the Keystone database handled the identity service. Authentication is handled through Keystone with username/password or username/API key. After verification of identity, it issued an authentication token to approve requests. The second database was the image client, Glance. Images were launched through this database following a correct authentication token. The third database was Nova. Nova handled all the compute services for the controller and compute node. Fourth was the Neutron service, which handled all the networking agents that traveled through all three nodes. Neutron provides an API to request virtual machines and configure. It connected all interfaces including Virtual Machines and NICs. The second node, compute node, handled the kernel-based virtual machine (KVM) Hypervisor and the compute services. This node allowed deployment of Virtual Environments or instances. Third, the network node, handled all the networking for all three nodes as well as DHCP agents. The Network Node deployed several processes between all nodes. All nodes worked together to maintain the smooth operation of the secure cloud.

Problem

Due to the shortage of funding in K-12 school systems, most schools have a lack of IT resources to securely store and share information needed for students, parents, and teachers that require access to networks.

Purpose

The goal of this project was to create a secure cloud solution for K-12 school systems so that the school systems could store data in a central repository and make use of collaborative resources in a secure manner, and allow K-12 schools within the state to utilize the cloud storage solution.

Method

The method used in this project was to 1) meet with client and determine the needs of the secure cloud solution for the K-12 school system; 2) design the secure cloud solution; 3) implement the secure cloud design.

Client needs

Meetings were held with the client to discuss the scope of the project. The conversation centered on the storage of information and how the solution would be used within K-12 school systems state-wide. The issues of concern were the policies and procedures in storing sensitive information in the cloud. Each district that utilized the cloud solution would create appropriate policies and procedures on the use of the secure cloud. There were public and private cloud solutions. Public cloud solutions allowed a third party to handle storage. With the private cloud solutions, it allowed the school system to handle the data with less risk of data leakage. Security was a priority considering the sensitive student information that would be in the cloud. The budget for the cloud storage was minimal and required the cloud to use open source if possible. The state IT provider chose a private cloud solution prototype that was vendor neutral to not incur undo costs by popular third-party vendors. Openstack design software was selected by the client. Openstack had the scalability and was easy to integrate with any system. Openstack insured data replication and integrity of the data. Openstack was open source and offered a distributed architecture. Openstack had another very appealing feature, it had the ability to be configured as a public or private cloud service. The ability to be configured as either public or private opened the flexibility of Infrastructure-as-a-service (IaaS) solution for multiple school districts (Kumar, Gupta, Charu, Jain, & Jangir, 2014).

Secure cloud design

The secure cloud design included three core node components. The components were the controller, network, and compute node. The nodes and services allowed the students and administration to access the information provided by the school system in a secure manner. The controller node, which handled the image and database services, allowed the users to access the cloud. The network node handled the virtual machine traffic that launched the images. The compute node handled the virtual machines and resources needed to run applications through virtualization. The block and object storage nodes stored the information. The security node was added to inspect the packets that traveled over the network for any suspicious payloads. The management network was used to communicate between each of the nodes. The management node was integral for all communication and services to run on all nodes. Figure 1 below shows the secure cloud design.

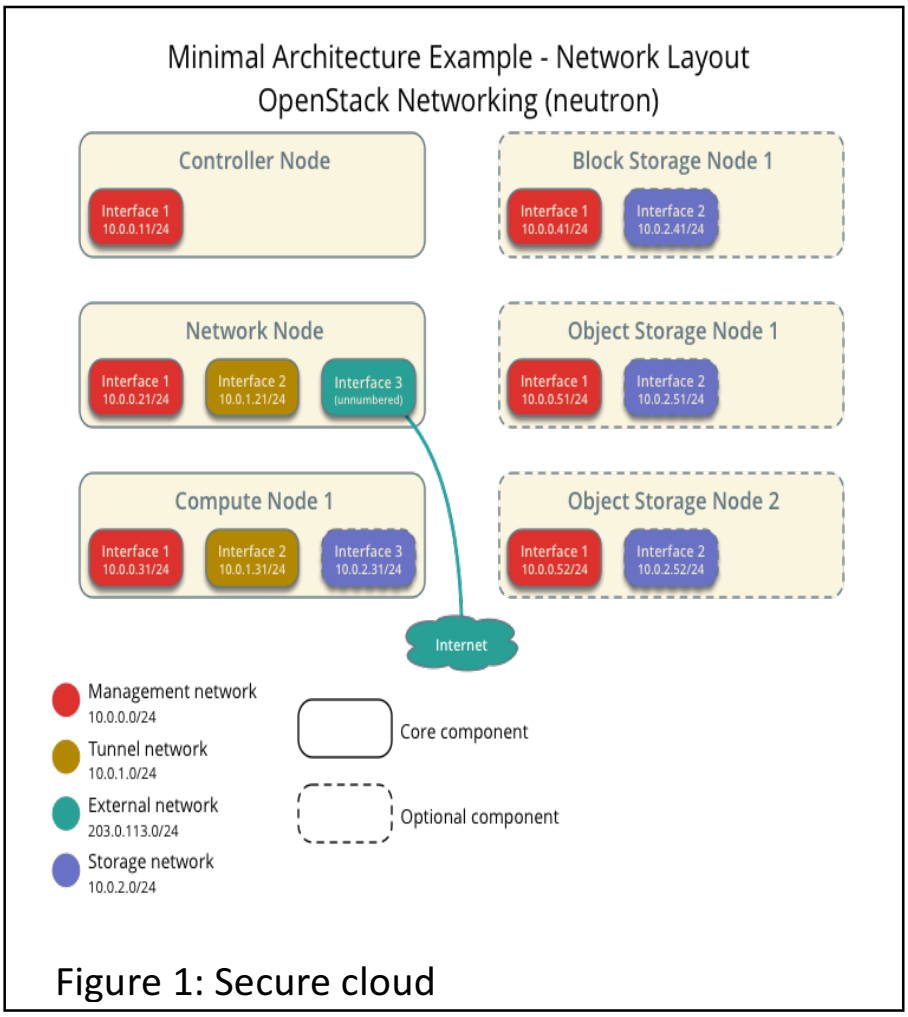

Figure 1: Secure cloud

Implementation of secure cloud design.

Implementation of the secure cloud design began with the acquisition of four physical servers. Ubuntu14.04 LTS operating system was installed on each server, then each server was configured as stated in the network layout.
The Controller node handled all the services informing the Network node and Compute node of what to do through these basic services. The supporting services provided storage for all the data and the basic services needed. Additionally, it allowed for communication over the management network. See figure 2.

Supporting services

- MySQL: A standard database service used to store information for Keystone, Glance, Nova, Neutron and Horizon.
- RabbitMQ: A message broker that coordinated operations and status information among services.
- NTP: Used to synchronize services among nodes.

Controller node basic services

- Keystone: The identity services which was responsible for tracking users and permissions. The Keystone was also responsible for maintaining a catalog of the available services and application program interface endpoints.
- Glance: Glance was the image service which allowed users to locate, register and retrieve virtual machine images. Images were pulled from files systems and object-storage systems.
- Nova: Nova was the compute service responsible for interacting with Keystone, Glance and Horizon allowing them to function together.
- Neutron: Allowed the creation and attachment of devices managed by other OpenStack services and networks.
- Horizon: Web interface that enabled administrators and users to manage various OpenStack resources and services.

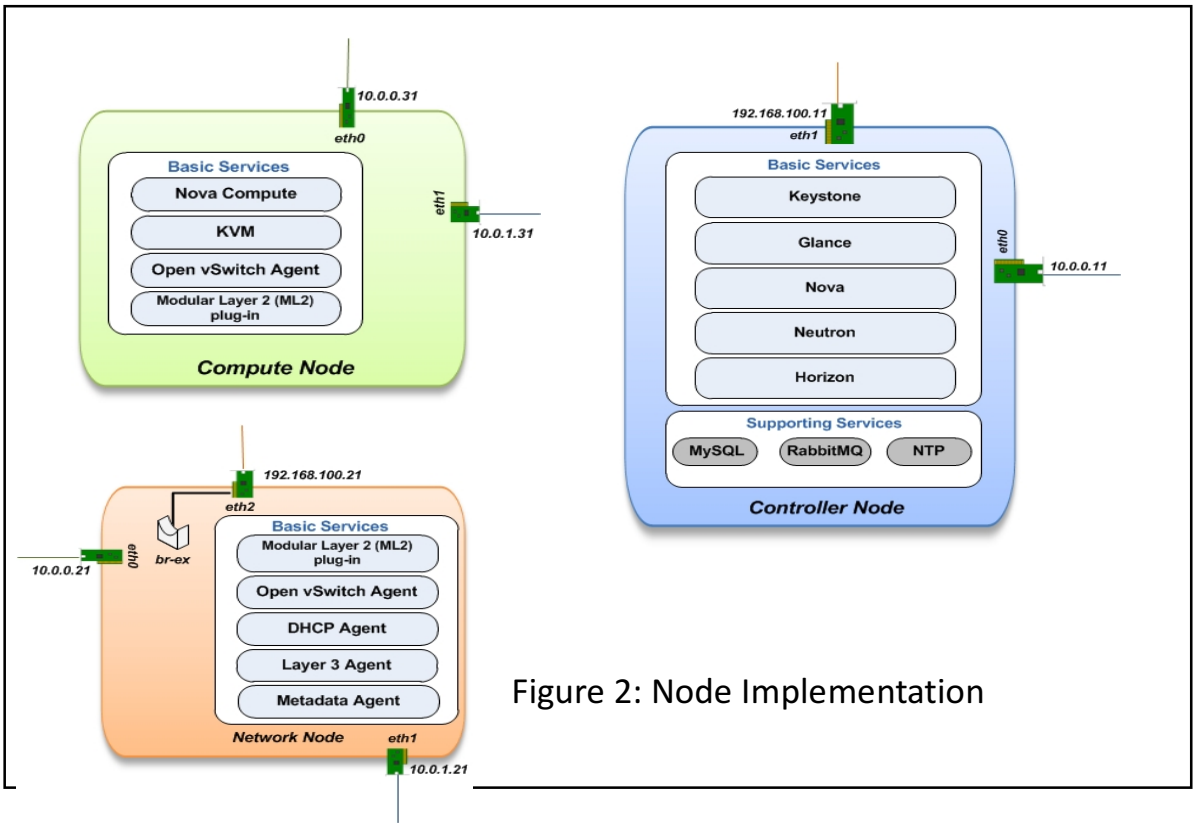

Figure 2: Node Implementation

Network node basic services

- Modular Layer 2: Used Open vSwitch Agent to build virtual networking frameworks for the instances
- Open vSwitch Agent: Provided virtual networking frameworks for instances, using the integration bridge to handle internal instance network traffic within OVS and the external bridge to handle external instance network traffic.
- DHCP Agent: Provided DHCP services for all the virtual networks.

- Layer 3 Agent: Provided routing services for virtual networks
- Metadata Agent: Provided configuration information with credentials to instances.

Compute node basic services

- Nova Compute: Used to create and terminate virtual machines and instances through the hyperviser API.
- KVM: Provided a hypervisor for operating virtual machines and instances.
- Open vSwitch Agent: Provided virtual networking frameworks for instances using the integration bridge to handle internal instance network traffic within OVS and the external bridge to handle external instance network traffic.
- Modular Layer 2: Used Open vSwitch Agent to build virtual networking frameworks for instances

In addition, a tunnel was added between the compute and network node, shown in Figure 1. The tunnel allowed traffic to be sent through the network node and eventually to the security node for analysis. Sans Investigative Forensics Toolkit (SIFT) was used for the operating system for the security node as it was open source and produced the desired log reports. If malicious activity was detected, the software would allow to parse packets and analyze to conclude results. SIFT is an incident response tool that includes memory analysis and other examination tools. If malicious activity went through the network to the cloud, the alerts would flag the event. Finally, Figure 3 depicts how the databases worked with the cloud.

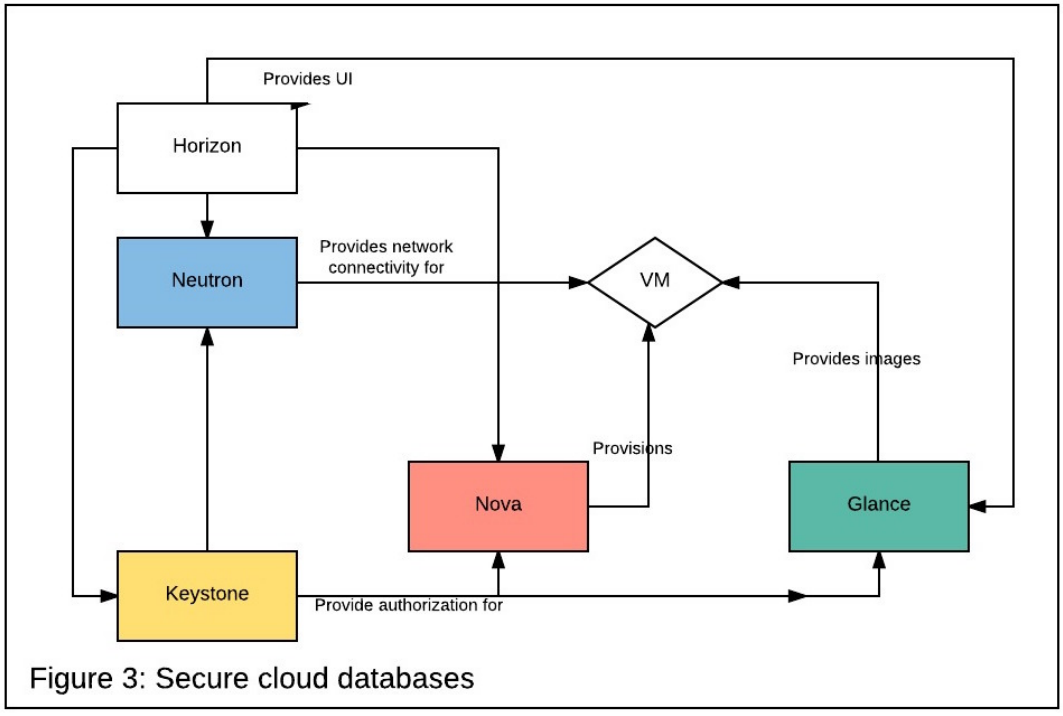

Figure 3: Secure cloud databases

Conclusions

With advancements in technology, it was imperative to come up with solutions to provide K-12 school systems with secure cloud infrastructure state-wide. The resolution chosen provided a cost effective, secure method to provide information to students, parents, administrators and educators.

Future work

The next step in the process is to implement the prototype for testing. The school would choose the applications necessary for the school environment to deploy from the controller node. After the prototype is completed, the necessary training for teachers and students would be to use their own devices within the cloud. The Security Node would be a prevention method for any misuse or malicious activity that someone younger might not be aware of. Additionally, OpenStack APIs can be used to build tools on top of the implemented system. Tools can be written to support scaling up or down of virtual machines based on the resources used.

References

Bennett, E. & A. Weber (2015). "Cloud computing in New York State education: Case study of failed technology adoption of a statewide longitudinal database for student data." QScience Connect: 2.

Chandra, D. G. & D. B. Malaya (2012). Role of cloud computing in education. Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on, IEEE.

Hartmann, S. B., Braae, L.Q.N., Pedersen, S., & Khalid, S. (2016). "The Potentials of Using Cloud Computing in Schools: A Systematic Literature Review." Turkish Online Journal of Educational Technology.

Kumar, R., Gupta, N., Charu, S., Jain, K., & Jangir, S.K. (2014). "Open source solution for cloud computing platform using OpenStack." International Journal of Computer Science and Mobile Computing **3**(5): 89-98.

Pierce, G. L. and P. F. Cleary (2016). "The K-12 educational technology value chain: Apps for kids, tools for teachers and levers for reform." Education and Information Technologies **21**(4): 863-880.

Reidenberg, J., Russell, N. C., Kovnot, J. Norton, T.B., Cloutier, R. & Alvarado, D. et al. (2013). "Privacy and cloud computing in public schools."