ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2016 April 10(4): pages 78-84

Published BY **AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

Security Issues in Open Stack (Swift Storage)

[1]J. Anitha Ruth, [2]A.Meenakshi and [3]Dr. H Srimathi

[1]Department of Computer Applications, SRM University, Kanchipuram, TamilNadu, India.
[2]Department of Computer Applications, SRM Universit, Kanchipuram, TamilNadu, India.
[3]Department of Computer Applications, SRM University, Kanchipuram, TamilNadu, India.

Received 25 February 2016; Accepted 10 April 2016; Available 15 April 2016

Address For Correspondence:
J. Anitha Ruth, Department of Computer Applications, SRM University, Kanchipuram, TamilNadu, India .
E-mail: anitharuthj@gmail.com

ABSTRACT

Cloud Computing is a new technology that is adopted by the industry for building their business solutions. This technology is implemented in all categories which includes public and private sectors and education etc. As the usage of cloud computing technique is increased the security issues becomes an important challenge for the business. Another important issue in cloud computing is portability where cloud service provider (CSP) use different technologies for storing the data in cloud .It becomes difficult for the customers to switch between the cloud service provider. This problem can be eliminated by the open stack which is open source community product developed by companies like AMD,citrix,Dell,Redhat,Intel,Microsoft ,Cisco etc. The main purpose of this paper is to analyze how cloud security issues are handled in open stack platform and also how swift storage is better than other cloud storage components.

KEYWORDS: Cloud security, Openstack, Swift storage

INTRODUCTION

The National Institute Standards and Technology[NIST] defines cloud computing as a “model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort(or) service provider interaction”[1]. The cloud security alliance(CSA) builds cloud with five characteristics, three cloud service models and four cloud deployment models. The essential characteristics of cloud are Broad Network Access, Rapid Elasticity, Measured Services, On-Demand self service and Resource Pooling. The three service models of cloud are software as a service(Saas), Platform as a service(Paas) and Infrastructure as a service(Iaas).Further the cloud deployment models of cloud are public, private, hybrid and community. Cloud computing services are enabled by service models, operational models and technologies that make the organization involved cloud to be insecure. Security in an organization is characterized by effectiveness and completeness of the security controls that are implemented in various layers of the cloud from physical security, to the network infrastructure to the system security and to the application security. The security is also implemented at the people and process levels such as separation of duties and change management.

A. *Security issues in cloud:*

- Governance and Enterprise Risk management
- Legal Issues:Contracts and Electronic Discovery
- Compliance and Audit .
- Information management and Data Security
- Portability and Interoperability
- Traditional Security, Business continuity and Disaster Recovery

- Data Center operations
- Encryption and key management
- Identity and Access management

Table I: Security Issues Found in cloud.

Security issues	Sub Issues
Governance and Enterprise Risk management	Data location Compliance
Legal Issues: Contracts and Electronic Discovery	-
Compliance and Audit	Laws and Regulation compliance
Information management and Data Security	-
Portability and Interoperability	Data Portability VM Image Portability Application portability
Traditional Security, Business continuity and Disaster Recovery	-
Data Center operations	-
Encryption and key management	-
Identity and Acess management	Authentication Access control
Virtualization	VM Hypervisor protection Guest OS Protection Virtual Network protection

The paper is organized as follows section II presents the overview of Openstack .In section III ,we consider the security issues handled in Openstack. Section IV presents the Openstack swift storage . Section V gives the advantages of swift storage over cinder the block storage.Finally Section VI gives the conclusion.

Overview of Openstack:

Open stack[2] is a open source software for creating private and public clouds. It controls large pools of compute, storage and networking resources through out a datacenter, managed through a dashboard or via openstack API.

Openstack is ideal for heterogeneous infrastructure .Hundreds of business organization rely on Openstack to run their business with reduce cost and helping them to move faster. The software is built by various community developer in collaboration with users. The Openstack includes the following components

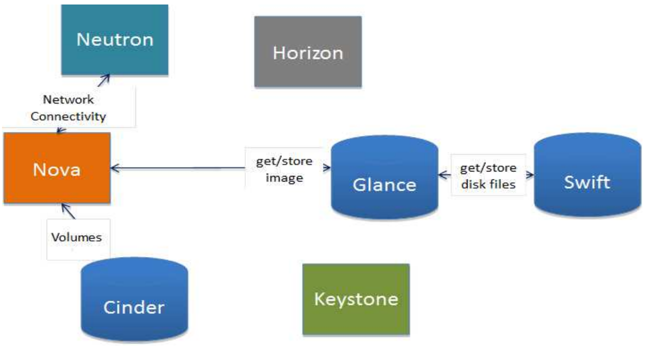

Fig. 1: Components of Openstack.

Nova(Compute) - A service that manages networks of virtual machines running on nodes, providing virtual machines on demand. Nova is a distributed component and interacts wi.th keystone for authentication, glance for images and horizon for web interface.

Glance (image) - A service that acts as a registry for virtual machine images, allowing users to copy server images for immediate storage .These images can be used as templates when setting up new instances.

Neutron(networking) -.It provides connectivity between the interfaces of other Open stack services such as Nova.

Cinder(Block Storage) -A service that manages storage volumes for virtual machines. This is persistent block storage for the instances running in Nova. Snapshots can be taken for backing up data, either for restoring data or to be used to create new block storage volumes.

Swift(object storage) -A service providing object storage which allows users to store and retrieve files. Swift architecture is distributed to allow for horizontal scaling and to provide redundancy as failure –proofing. Data replication is managed by software ,allowing greater scalability and redundancy than dedicated hardware.

Keystone(Identity) -A centralized identity service that provides authentication and authorization for other services. Keystone also provides a central catalog of services running in a particular Openstack cloud. It supports multiple forms of authentication, including username and password credentials, token-based systems. Keystone acts as a (SSO) authentication services for users and components.

Horizon (Dashboard) - A web-based interface for managing Openstack services.it provides a graphical user interface for operations such as launching instances, managing networking and setting access controls.

Security Issues In Open Stack:

Cloud technology[3] is implemented in Openstack through public, private and community deployment models. Openstack public clouds are handled by the service provider and it can be used by the individuals and organizations or by any customer. A public cloud provider is exposed to all the features such as software defined networking, block storage and multiple instance type. Public open stack cloud is exposed to high degree of risk. The user of the public cloud should validate whether the cloud provider has the necessary certification, attestation and other regulatory consideration. The cloud provider should ensure that there is tenant isolation and protect management infrastructure from external attacks. In the case of private cloud it is provisioned for single organization comprising multiple consumers.Similarly community cloud should be specific for a community of consumers from an organization that their information. Finally hybrid clouds are designed when there is a requirement of two or more distinct cloud infrastructure are needed.

Open stack security[4] is concerned with four domains namely the

- Public
- Guest
- Management
- Data

These areas are exposed to the trust within the openstack deployment model. The trust requirement in these domains depend upon whether the cloud instance is public , private or hybrid. The Openstack follows certain security guidelines such as

- Apply restrictive file permissions
- Avoid dangerous file parsing and object serialization libraries
- Un validated URL redirect
- Escape user input to prevent XSS attacks
- Use secure channels for transmitting data parameterize database queries
- Protect sensitive data in config files from disclosure
- Use strong and established Cryptographic elements
- Restrict path access to prevent path traversed.
- Create ,use and remove temporary files securely
- Python pipes to avoid shells
- Validate certificates on HTTPs connections to avoid man-in-the middle attacks
- Use subprocess securely

Swift storage:

The commonly used storage system in a enterprise are file system storage and block level storage. The file system storage[5] is deployed as Network Attached Storage(NAS) systems used for storing and sharing files over network. Block storage is implemented as storage area Network (SAN) systems is used to store database. The organization has to isolate both the storage and data from other application. Hence organization needs a scalable storage for storing its data which is not possible in file and block storage.

The drawbacks of file and block storage are as follows

- It does not efficiently scale to support new workloads
- It is logged down by operational overhead
- It is difficult to match storage to application requirements
- It is time consuming to adjust to workload changes and migrants
- It is manually managed or semi automated

Organization finds difficulty in managing the unstructured data. Moreover the organization needs scaling and availability of data which is difficulty to be maintained in file or block storage .The block storage system and file systems are strongly consistent but their limits scalability and may reduce availability to data when hardware failure occurs .Object Storage systems such as swift provides consistent and massive scalability.

A swift [6] is a high available ,distributed, eventually consistent object/blob store. Organizations use swift to store data efficiently, safely and cheaply. The components of swift storage are

- Proxy server

- Object server
- Container
- Account

The proxy server uses the object ring to decide where to store newly uploaded objects.it uses the object ring to decide where to store newly uploaded objects.it updates the relevant container database to reflect the presence of a new object.

Object server is responsible for storing data objects in partitions on disk devices .Container service maintains database of objects in containers. There is one database file for each container and they are replicated along the cluster.

Account service maintains databases of all containers accessible by any given account.

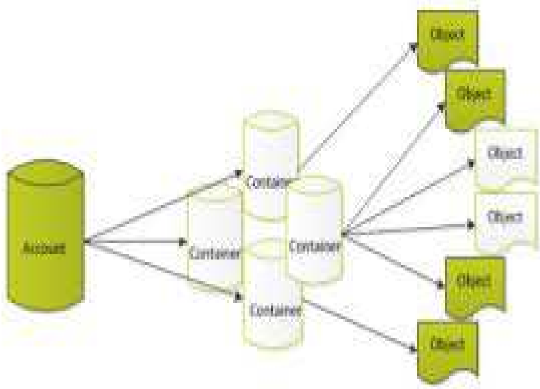

Fig. 2: Components of swift storage.

V. Advantages Of Swift Storage Over Cinder Block Storage Components

Swift is a object storage which provides same functions as Amazon S3.It provides a distributed scale-out object store across nodes in an openstack cluster. The object stores reference data as binary objects and referenced using HTTP(web based) protocols.

In swift objects are physically stored on object servers. swift uses the idea of eventual consistent when replicating data for resilience .The data is not replicated synchronously across the open stack cluster but rather duplicated as a background task.

Cinder is the open stack component that provides access to and manages, block storage. The storage appears as a block device that uses iSCSI, fiber channel and NFS .The Cinder interface specifies a number of discrete functions ,including basic functionality such as create volume, delete volume etc.

Conclusion

The paper discusses the open stack security issues and how the security concerns of cloud is handled in open stack and it gives a overview of swift storage and the advantages of swift storage over Cinder block storage.

ACKNOWLEDGEMENT

I would like to thank my supervisor Dr. H. Srimathi for her continuous support and encouragement in my research work

REFERENCES

1. http://www.cloudsecurityalliance.org/guidance/csaguide.v3-0pdf.
2. https://www.openstack.org
3. Ishan Gidwani, DasrathMane, 2015. “Security issues in openstack” International Journal of Computer Science and Information Technology research, 3(2): 1147-1158. Apirl-June 2015,ISSN, 2348-1196 .
4. HalaAlbaroodi, selvakumar manickam and Parminder Singh, 2014. “Critical review of OpenStack security issues and weakness”,Journal of Computer Science, 10: 23-22, 2014 ISSN: 1549-3636,doi:10.3844/jcssp.2014.23.33]
5. https://security.openstack.org
6. https://www.swiftstack.com/openstack-swift