International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 587 - 590

A Model of Security Architecture on Private Cloud Using OpenStack

Venkatesan Balu
Research Scholar of St. Peter's University,
St.Peter's University
Avadi, Chennai
Tamilnadu, India.
Email:dropmail2venkat@gmail.com

Dr. L. Josephine Mary
Research Guide of St.Peter's University,
Avadi, Chennai,
Tamil Nadu, India
Email: josimgr@yahoo.co.in

Abstract*:-** Cloud computing is current trend and it is the best solution of the spending excessive budgeting for many organizations IT setup. With Cloud Computing becoming more widely utilized, it is important for organizations to understand ways to maximize benefits and minimize risks of a move to the cloud also to carefully consider its operating expenses essentially. Since most of the organization already has traditional IT setup by investing huge amount which they don't want to lose and also they like to have their IT setup to move into cloud model. The major share of the investment would be spent for having data center in any organization. The main objective of this paper "A MODEL OF SECURITY ARCHITECTURE ON PRIVATE CLOUD USING OPENSTACK***" is to provide the model architecture to move the organization's in-house data center to private cloud. Also this paper explains about the strategy for the migration from organization's on-premises IT setup to private cloud. This architecture is also used the open- source cloud computing software, called "**OpenStack**" platform. This technology consists of a series of interrelated projects that control pools of processing, storage, and networking resources throughout a data center-which users manage through a web-based dashboard, command-line tools, or a Restful API.

Keywords: Cloud computing, Private Cloud, OpenStack, Keystone, Security, Data Center.

*****

I. INTRODUCTION

The Private cloud[1] is a model or architecture and often presented as being the solution for all your computing issues in enterprises sector. It is distinct and secure cloud based environment which can be accessed and managed by the organization. It is very closer to the more traditional model of individual local access networks (LANs) that is used in the past by enterprise but having the added advantages of virtualization. This can be also called either "Internal" or "corporate" or "enterprise" cloud and it will be protected by firewall. The enterprise will have more control over its data and applications in this kind of setup. It also promises benefits such as energy savings, cost savings, rapid deployment and customer empowerment.

There could be additional security offered by ring fenced cloud model that could be ideal for any enterprises which needs to store and process private data or carry out some sensitive tasks. For instance, a private cloud service could be utilized by a financial company that is required by regulation to store sensitive data internally and who will still want to benefit from some of the advantages of cloud computing[2] within their business infrastructure, such as on demand resource allocation. On the other hand, technically the virtualization is not private cloud and private cloud is far beyond virtualization. Data Storage is the one of the important and primary resource enterprises wanted to keep with their control.

1.1. Objective of Private Cloud

The primary objective to have private cloud in the organization is that to achieve the below specification in their business services.

- Zero downtime in the system and service which is related to business requirements.
- Provision of self-service which enables access to information and applications at any time (24 hours in a day/7 days in a week) and from any location (worldwide).
- According to the business demand the system and service will be automated, rapid, and elastic provisioning and releasing. This can be also called as "Resource Pooling". This means that available service should appear to be unlimited to users and multiple users are served using a multi-tenant model.

1.2. Private Cloud vs. Standard Data Center

In general, Cloud never means to refer any hardware or physical resources. Cloud is a platform that could have API to provide access to all the physical resources virtually through API. It can also be an abstract layer for the physical resources.

Data Center refers to on-premise hardware like physical servers that stores data within the organization's local network. Data Center has limited capacity. Once we build a data center, it is difficult to change the amount of storage and workload and it can withstand without purchasing and installing more equipment.

1.3. Motivation for Migrate to Private Cloud

There are several kinds of reasons to move[3] the IT infrastructure to Cloud computing technology; for e.g., lower cost of entry, reduced risk of IT infrastructure failure, higher ROI, quick responses to changes in demand, rapid deployment, increased security, and ability to focus on an organization's core business.

On the economic side, there are need for processing large data volumes to grow strongly in both industry and research and that needs to conserve power by optimizing server utilization which is also thriving. Moreover, there is an increasing demand for consolidating IT resources due to economic conjuncture (recession). The market is on its way to on-demand computing power for both small businesses and research, which are increasingly exploring the option of having private cloud solutions.

Organizations are also looking at mobile applications as obvious candidates for implementing on cloud computing. Of course, that would not be possible if data were not available on-line. Organizations willing to streamline their office applications implementation are looking at Google Docs and Office 365.

It is quite obvious question for many organizations that what approach to take for migrating to cloud computing? It seems that a "big bang" approach is not a feasible approach to migrating to cloud; rather the migration should be done in piecemeal manner. Such a migration can start with the data of low importance first, see how it goes, and then gradually move on, migrating the data of low importance.

1.4. Private Cloud Challenges

There are key challenges[4] that should be considered before the enterprises to build private cloud. So enterprises that

- Should think of bridging private cloud with the existing infrastructure or integrate with legacy systems and data.
- Should be able to have 24x7 support service for their end user when they experience any issue in private cloud.
- Have enough on-premises servers that can be virtualized and scaled for current and future demands.

There are some additional challenges that businesses need to consider on day-to-day business management.

- Managing the enterprise applications and responsible for updates and patches in the applications.
- Handling the security issues.
- Monitors and tests the system to ensure data and applications are properly backed up and readily retrievable.
- Managing the business critical deployment in the application and those activity tracking.

1.5. Private Cloud Key Benefits

To maximize the benefits of private cloud, to be sure that we implement these five private cloud automation tools and processes which can avoid unnecessary overhead to hire more system administration. The benefits are listed below:

- Infrastructure automation provisioning which can be achieved by using "Puppet" or "Chef" configuration management tools. These are called as "DevOps[5]" tools.
- Cloud management dashboard is essential and the infrastructure automation provisions are carried out behind the scenes by scripts. It presents an easy-to-use interface that allows users to provision and de-provision resources, track resource use, modify access controls to resources and view services available in the private cloud.
- Cloud automation monitoring will be useful for real-time monitoring (hardware failures or disrupted services) and long-term business support planning (aggregate information like use of cloud resources, demand for particular types of resources and costs of providing particular services).
- Resource tracking tools that will help to implement budget control for the users.

II. A MODEL OF SECURITY ARCHITECTURE FOR PRIVATE CLOUD USING OPENSTACK

2.1. OpenStack Architecture

OpenStack[6] is a free and open-source software cloud computing software platform. Users primarily deploy it as an infrastructure as a service (IaaS) solution. In Fig.1, we shows that OpenStack consists of a series of interrelated projects that control pools of processing, storage, and networking resources throughout a data center-which users manage through a web-based dashboard, command-line tools, or a RESTful API.

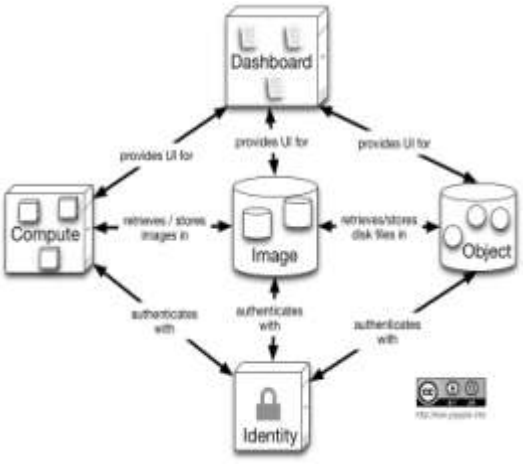

Fig 1: OpenStack Architecture

2.1.1. Key Elements of OpenStack Private Cloud

- Open Architecture – any component that can be adopted and used.
- Robust – there should be common or centralized administration to obtain best performance benchmarking.
- Scalability – automatic infrastructure creation when the server gets high load or downtime.
- Hybrid Cloud – bridge private and public cloud.
- No Downtime – environment should be always up and running.
- Client Support –there should be defined SLA and 24/7 support for the users.

2.2. A Model of Security Architecture for Private Cloud using OpenStack

OpenStack has combination of different component like compute, keystone[7] and storage which bundled with to build private and public cloud using this cloud platform. Keystone provides a single point of integration for OpenStack identity, token, catalog and Policy services for projects.

2.2.1. Security Architecture using Keystone Identity Service

Keystone has many components which help us model the secure architecture to build private cloud. Keystone ensures that

- User – incoming requests are from valid or approved from person, service or system
- Role – group of user assigned to set of privileges and perform specific operations.
- Credentials - specific user provides username and password or an authentication token.
- Authentication - identity service issues authentication token that user is allowed to make subsequent requests.
- Token - each token has a scope describing accessible resources. A token may be revoked at any time and is valid for a finite duration.
- Endpoint – network accessible address which usually described by URL for authenticated users.

There are two primary functions which can be achieved by using keystone.

- User Management - tracks of user and their security[8] scope in which they are permitted to do.
- Service Catalog - provides a catalog of what services can be available for the user.

In Fig.2, we have shown the model architecture[9] to build secure private cloud using OpenStack's "Keystone".

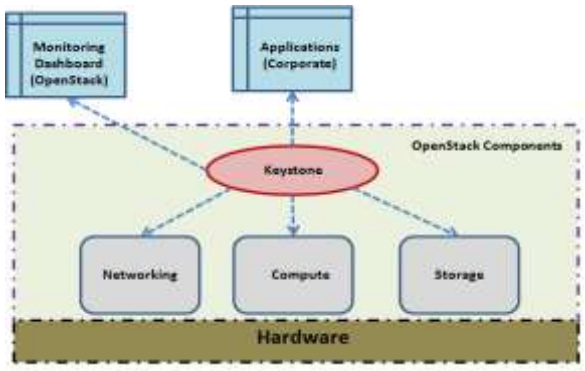

Fig 2: A Model of Security Architecture for Private Cloud using OpenStack

2.2.2. Private Cloud - Planning

Organization has to build a strategy or roadmap for the private cloud planning. The Fig.3 shows the model for the planning and each will be described below. Since the model should be a reiterate process, it can have more repetition.

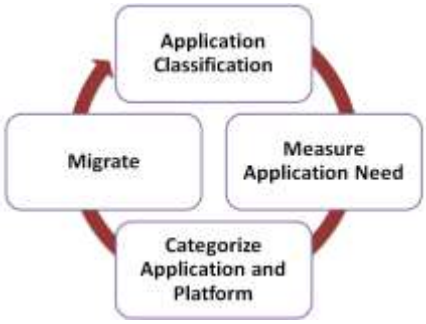

Fig 3: Roadmap of private cloud planning

- Application Classification - need to classify the list of application that can be moved to private cloud.
- Measure Application – need to measure the impact or importance of the application and make it in the proper queue then this can be taken with the order.
- Categorize Application and Platform – most of the enterprises should be having heterogeneous application and platform, need to categorize by platform.
- Migrate – need to start migrate the application with the respective platform and also has to think about the support services for the platform that we build.

2.2.3. Post Private Cloud Migration

Once the private cloud is up and running, then the enterprises has to provide the right tools[10] to help users to maintain and get maximum benefit out of cloud services. There are few important pointes highlighted below.

- Implement automation for the actual private cloud benefits. This can be done by using some famous DevOps tools like "Puppet" or "Chef".

- Meter the private cloud usage on “Bill for the usage or infrastructure” basis.
- Security tools are essential for the private cloud and it can be done by using self-service model.
- Maintaining a private cloud which means that server failover and downtime must not lead any problem.
- Determines that it is cost-effective with “Return on Investment (ROI)” software or tools.

III. CONCLUSION AND FUTURE WORK

In this paper, we studied the key points for the private cloud demand, motivation, challenges and the strategies to build the private cloud. Also it explained the post private cloud migration steps that should be taken care for the end users perspective.

The future topic and experiment should be to find out the implementation of the effective disaster recovery (DR) strategy and the security model in private cloud which is mandatory for any other IT setup environment. The implementation of the approach is commonly very complicated and expensive to organization. The future enhancement would find the optimal way of implementing the disaster recovery strategy and security.

REFERENCES

[1] Private Cloud Computing, Stephen R. Smoot,Nam K. Tan, Stephen R. Smoot,Nam K.Tan, 2012.
[2] Armbrust, M., et al., 2010, A View of Cloud Computing, ACM, 53(4), pp. 50-58.
[3] Ali Babar, M.; Chauhan M.A.; , A tale of migration to cloud computing for sharing experiences and observations, SECLOUD '11, ACM.
[4] Zhang, Q., Cheng, L., Boutaba, R., Cloud Computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, 2010, 1:7-18.
[5] OpenStack Manuals, docs.openstack.org, May 2012. and “Deploying OpenStack”, Ken Pepple, Oreilly, July 2011.
[6] DevOps for Developers, Apress, 2012 edition.
[7] Keystone, OpenStack Identity Service. http://docs.openstack.org/developer/keystone/
[8] S. King and P. Chen, “Subvirt: implementing malware with virtual machines,” in IEEE Symposium on Security and Privacy, May 2006.
[9] Cloud Enterprise Architecture, Auerbach Publications, 2012
[10] Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS), 2014 by Michael J. Kavis.