

Building Open Source Cloud for Organizations: An Deploy Using Eucalyptus

N.Nasurudeen Ahamed¹

S.Malathi², S.Naveena³, R.P.Rachana Ramachandran⁴

¹Assistant Professor, Department of Computer Science and Engineering,

Vivekanandha College of Engineering for Women (Autonomous), Namakkal-637205, India.

^{2, 3, 4} PG Scholar, Department of Computer Science and Engineering,

Vivekanandha College of Engineering for Women (Autonomous), Namakkal-637205, India.

Abstract

Cloud Computing is the huge era of IT consumption. Cloud services are supported both by Proprietary and Open Source Systems. As Proprietary products are very expensive, customers are not allowed to experiment on their product and security is a major issue in it, Open source systems help in solving out these problems. Cloud Computing motivated many academic and non academic members to develop Open Source Cloud Setup, here the users are allowed to study the source code and experiment it. This paper describes the configuration of a private cloud using Eucalyptus. Eucalyptus an open source system has been used to implement a private cloud using the hardware and software without making any modification to it and provide various types of services to the cloud computing environment.

Keywords: Cloud computing, private cloud, private cloud in educational institutions.

1. INTRODUCTION

Cloud computing is the delivery of computing services—servers, storage, databases, networking, Software, analytics and more-over the internet. Cloud computing is a big shift from the traditional way businesses think about IT resources. Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). These are sometimes called the cloud computing stack, because they build on top of one another

Cloud computing is mainly classified into three types based on the deployment model; Public cloud, Private cloud and Hybrid cloud. If the services are provided over the internet then it is public cloud or external cloud and if it is provided within an organization through intranet then it

is named as private cloud or internal cloud and Hybrid cloud is an internal/external cloud which allows a public cloud to interact with the clients but.

Cloud computing services all work a little differently, depending on the provider. But many provide a friendly, browser-based

dashboard that makes it easier for IT professionals and developers to order resources and manage their accounts. Some cloud computing services are also designed to work with REST APIs and a command-line interface (CLI), giving developers multiple options.

2. EUCALYPTUS

Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) was released in May 2008, creator of the leading Open-Source Private Cloud platform. They were incorporated as an organization in January 2009 Headquartered in Santa Barbara, California.

Eucalyptus software is available under GPL (General Public License) that helps in creating and managing a private or even a publicly accessible cloud. It provides an EC2 (Elastic Compute Cloud)-compatible cloud computing platform and S3 (Simple Storage Service)-compatible cloud storage platform.

This paper explains about EUCALYPTUS: an open-source system that enables the organization to establish its own cloud computing environment. Eucalyptus is structured by various components which interact with each other through well-defined interfaces. It is used for implementing on-premise private and hybrid clouds using the hardware and software infrastructure that is in place, without modification.

For implementing, managing and maintaining the virtual machines, network and storage Eucalyptus has variety of features.

- SSH Key Management
- Image Management
- Linux-based VM Management
- IP Address Management
- Security Group Management
- Volume and Snapshot Management

2.1 Components of Eucalyptus:

a. **Cluster Controller (CC)** Cluster Controller manages the one or more Node controller and responsible for deploying and managing instances on them. It communicates with Node

Controller and Cloud Controller simultaneously. CC also manages the networking for the running instances under certain types of networking modes available in Eucalyptus.

b. **Cloud Controller (CLC)** Cloud Controller is front end for the entire ecosystem. CLC provides an Amazon EC2/S3 compliant web services interface to the client tools on one side and interacts with the rest of the components of the Eucalyptus infrastructure on the other side.

c. **Node Controller (NC)** It is the basic component for Nodes. Node controller maintains the life cycle of the instances running on each nodes. Node Controller interacts with the OS, hypervisor and the Cluster Controller simultaneously.

d. **Walrus Storage Controller (WS3)** Walrus Storage Controller is a simple file storage system. WS3 stores the the machine images and snapshots. It also stores and serves files using S3 APIs.

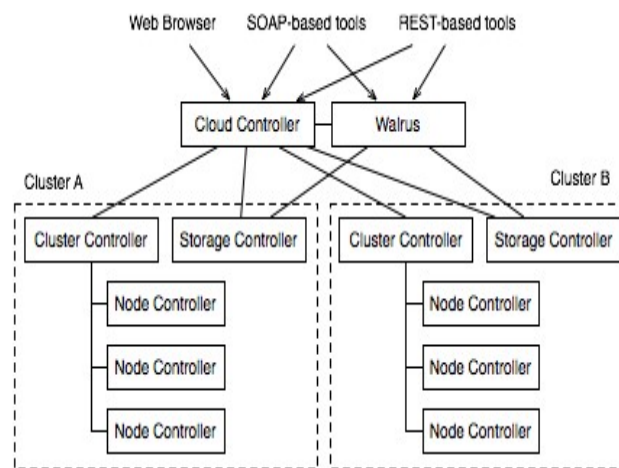


Fig:1. Eucalyptus Fundamental Architecture

e. **Storage Controller (SC)** allows the creation of snapshots of volumes. It provides persistent block storage over AoE or iSCSI to the instances.

Eucalyptus was developed to support the high performance computing (HPC). Eucalyptus can be deployed without modification on all major Linux OS distributions, including Ubuntu.

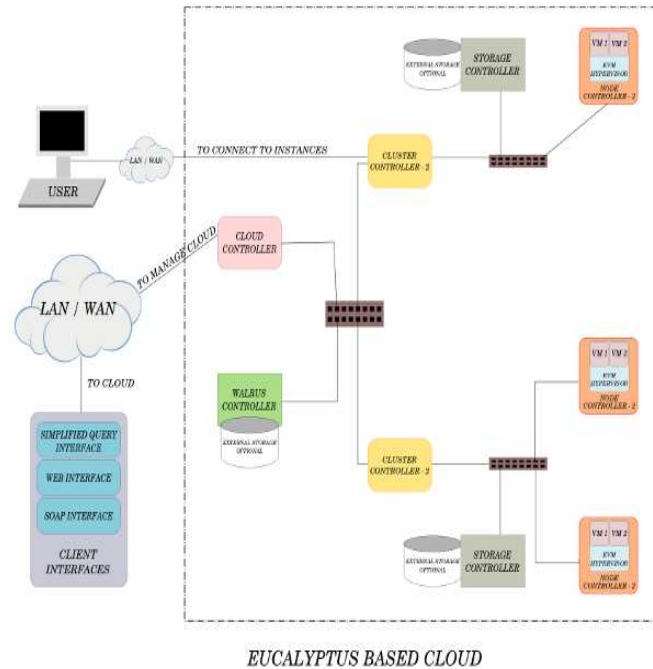


Fig: 2. Eucalyptus Architecture

3. Existing System:

Eucalyptus is an open source software framework for Cloud Computing that implements Infrastructure as a service (IaaS). It allows the users to run and control virtual machine instances, store and retrieve data using the WALRUS Data Storage Service and create and manage volumes and snapshots using Block Storage Service.

Cloud entities including cloud users, service providers and business partners share the available resources at different levels of technological operations. Hence, the Cloud Computing framework is inherently susceptible to a great number of security threats due to the amalgamation of different computing technologies that make it a complex architecture. Among all the potential threats, those targeting the users' data are significantly important and must be handled properly to facilitate effective cloud functionality.

Therefore, the preservation of cloud users' data privacy is one of the major challenges to be considered in a typical private cloud environment. It is very important that the users' data and metadata is protected and is available to authorized users only.

To identify some of the critical users' data privacy issues that could exist in a typical Private Cloud Computing environment.

One important fact about Cloud security is that the owner may not have control over his data or metadata. Private Clouds provide the facility of on-site virtualized data storage in order to maximize resource utilization which in turn raises the issue of users' data privacy.

3.1. Data Privacy Issues In Eucalyptus:

We can classify Eucalyptus cloud users' data into three major categories.

- Cloud users' personal information such as login names, passwords, and personal identification data requested by the cloud provider for users' subscription.
- Metadata of the cloud users' data residing in the cloud.
- Cloud users' cloud resident data (including user created VM images called EMIs).

The prospective attacks in a private cloud environment include attacks from internal and external sources. External sources are business competitors, cloud's legitimate and illegitimate users and external computing systems. The internal sources include administrators and technical staff.

Among all possible attack sources, the cloud's administrators stand the greatest chance of violating the users' data privacy. Having physical access to the cloud machines, privileged cloud access rights and most importantly cloud administration expertise, the cloud administrators can deliberately compromise the cloud users' data privacy to their own advantages.

3.2. Walrus:

Walrus allows users to store persistent data, organized as buckets and objects. We can use Walrus to create, delete, and list buckets, or to put, get, and delete objects, or to set access control policies. Walrus is interface compatible with Amazon's Simple Storage Service (S3), providing a mechanism for storing and accessing virtual machine images and user data. Walrus can be accessed by end-users, whether the user is running a client from outside the cloud or from a virtual machine instance running inside the cloud. Walrus should be considered as a simple file storage system.

The WALRUS buckets can be accessed by the users for the following two services:

- For storing and managing Eucalyptus VM images (termed as 'EMIs'-Eucalyptus Machine Images).
- For storing and managing cloud users' data.

4. BUCKET RELATED ATTACKS:

It involves making use of the credential file 'eucarc' along with attribute values as extracted from the catalog eucalyptus_auth.script. Source this new eucarc file and run the s3curl commands to create a new bucket impersonating the user whose credentials are used. Once the attacker is in possession of the list of user owned buckets, by using the credentials he can interact with the Walrus buckets.

4.1. Object Related Attacks:

- The attacker needs to know the exact bucket name in which the target object is located. After getting hold of this information, the attacker needs to make a new eucarc file with the query interface credentials of his victim, source this file and run s3curl
- Commands to put an object into the victim's bucket, get the MD5 checksum, size and modification time of a victim's object, read the victim's object into a file or delete a victim's object.

4.2. Access Control List Related Attacks:

Each WALRUS bucket and object has an Access Control List (ACL) attached to it as a sub resource. To launch access control list related attacks on buckets/objects, the attacker first needs to get hold of their respective ACL sub resources. Then the attacker modifies the *.acl file or creates a new *.acl file containing his preferred access control rights.

4.3. User Password Related Attacks:

Eucalyptus enables the users to generate access log files for the buckets that they own. The access log files are objects of particular interest to the attackers since they provide the attackers with the opportunity to remove their attack traces. Another attack avenue for the attacker can be to read the 'logging' sub resources of the victim's buckets into *.logging files, make the desired modifications to the selected sub resource in order to forge the real information contained in the log files and finally set the modified file as the 'logging' sub resource of the target bucket.

4.4. S3Curl COMMANDS:

We are using s3curl for interacting with WALRUS. It adds security parameters as curl headers. Using s3curl, users can create/delete/list buckets, put/get/delete objects, set object/bucket access control policies, enable/disable object/bucket access logging and obtain MD5 checksums and last modification date and time for objects and buckets.

Ubuntu Enterprise Cloud (UEC) offers a promising solution to organizations aspiring to exploit their fullest infrastructural potential. A Eucalyptus based private cloud deployment, however,

must be weighed in the light of prospective benefits and imminent risks. Public clouds are normally considered to be incapable of providing reliable guarantees in relation to the preservation of their users' data privacy owing to the fact that they store users' data at multiple geographical locations and the users are themselves not aware of the physical location of their data, thus limiting users' control over their own data.

This project is concerned with the security analysis of cloud, pertinent to data privacy of users' cloud resident data and metadata. It identifies the potential attack sources and prospective attacks originating from these sources.

5. FUTURE ENHANCEMENT:

In Eucalyptus Cloud Architecture, Disk Image Storage belongs to Walrus. Walrus Disk Storage attack by attackers and data which kept in the disk storage lost. So, we proposed the new parameter to overcome the disadvantages in existing system in this paper. Hackers don't even need your password anymore to get access to your cloud data

First, we need to be sure that local backups can be secured from unauthorized access in case someone gains access to your desktop, laptop, or mobile device. By using the industry-grade AES-256 algorithm, you can be sure that your data is safe. It is very hard to decrypt data secured by this algorithm. AES-256 is not that fast in terms of time and performance during the encryption process, so you may consider using shorter key lengths (AES-256 means that encryption key length is 256 bit) like 128 or 192 bits, in order to improve performance when protecting data that is not that sensitive.

Users can set the encryption algorithm and password that is used for encryption, and the Acronis agent handles key creation. The password you assign for backup can't be retrieved, so you need to memorize it. This is actually done on purpose, as this is a proper security approach. In case of a targeted or malware attack, your password won't be found in the agent/program files, and thus there will be no way to decrypt the backup file(s).

Secondly, the same goes for cloud storage: To encrypt and decrypt your data, the program needs the password, that you specify when you configure the online backup. The process and approach is the same as with a local backup – you need to memorize your password. Alternatively, you can use password manager software, like SafeinCloud and Enpass. Its, exponentially stronger than DES.

6. CONCLUSION:

We have presented the Eucalyptus open-source cloud computing software framework.

The EUCALYPTUS system provides the ability to deploy an infrastructure for user-controlled virtual machine creation and control atop existing resources.

We have shown that Eucalyptus is distinctive among other cloud computing IaaS systems in that it supports an industry standard interface (Amazon EC2), deploys as an overlay atop existing commonly encountered resource configurations (small clusters, workstation pools, etc), and has been designed as a modular system where components may be replaced or enhanced in order to promote future cloud computing research efforts.

There are various security issues in the cloud computing to overcome in this proposed system. By, using the industry grade AES-256 algorithm, you can be sure that your data is safe. It is very hard to decrypt data secured by this algorithm. Ensure that your data goes to secured cloud storage; via a secure channel.

EUCALYPTUS hierarchical design targets resources that are commonly found in academic and laboratory settings for the Research and Student Teacher communities in the Universities or Higher Educational Institutions.

REFERENCES:

[1] P.Uma Maheshwari, M.Ratna Sirisha and V.Sreenivas ,“ a panoramic design of cloudcomputing implementation elastic utility computing architecture,” *International journal of modern trends in engineering and research(IJMTER)*,ISSN(online)-2349-9745,ISSN(print)-2393-8161.

[2] Daniel Nurmi, Rich Wolski, Chris Grzegorzcyk, Graziano Obertelli, Sunil Soman, Lamia Youseff And Dmitrii Zagorodnov, “Eucalyptus: an open-source cloud computing infrastructure,” *Journal of Physics: Conference Series 180 (2009) 012051* doi:10.1088/1742-6596/180/1/012051 *SciDAC 2009 IOP Publishing*.

[3] Dr.G.R.Karpagam, J.Parkavi, “Setting up of an Open Source based Private Cloud,” *IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011*,ISSN (Online): 1694-0814 . www.IJCSI.org.

[4]D.SudhaDevi,P.Aruna, K.Thilagavathy,Ph.D, N.Priya, “Private Cloud in Educational Institutions: An Implementation using UEC,” *International Journal of Computer Applications (0975 – 8887) Volume78– No.1, September 2013*.

[5] P Aruna, L Yamuna Devi, D Sudha Devi, N Priya, Dr. S.Vasantha and Dr. K.Thilagavathy, "Private Cloud for Organizations: An Implementation using OpenStack," *International Journal of Scientific & Engineering Research*, Volume 4, Issue 10, October-2013 82 ISSN 2229-5518 IJSER 2013 <http://www.ijser.org>

[6] N. Ram Ganga Charan, S. Tirupati Rao, Dr .P.V.S Srinivas, "Advanced Computer Science and Applications," *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 2, No. 5, 2011 www.ijacsa.thesai.org

[7] Amita, Rajender Nath, "A Comparative Study of Open Source IaaS Cloud Computing Platforms," *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper* , Volume 5, Issue 5, May 2015 ISSN: 2277 128X www.ijarcsse.com