Zeus Cloud

Attempt to run Eucalyptus Cloud along with Rocks Cluster Management software

Submitted by

Roll No	Names of Students
B100312CS	Sudev A C
B100229CS	Sharath Hari N

Under the guidance of
Dr. Vineeth Paleri

Department of Computer Science and Engineering
National Institute of Technology Calicut
Calicut, Kerala, India – 673 601

Abstract

This project aims to study the Minix 3 microkernel and implement a support for immediate files which is currently unavailable. An immediate file is a file whose data is not stored in a data block, but directly inside the inode itself. With such an implementation, data fragmentation in the file system caused by small files can be solved and number of disk accesses can be reduced.

Contents

Chapter 1

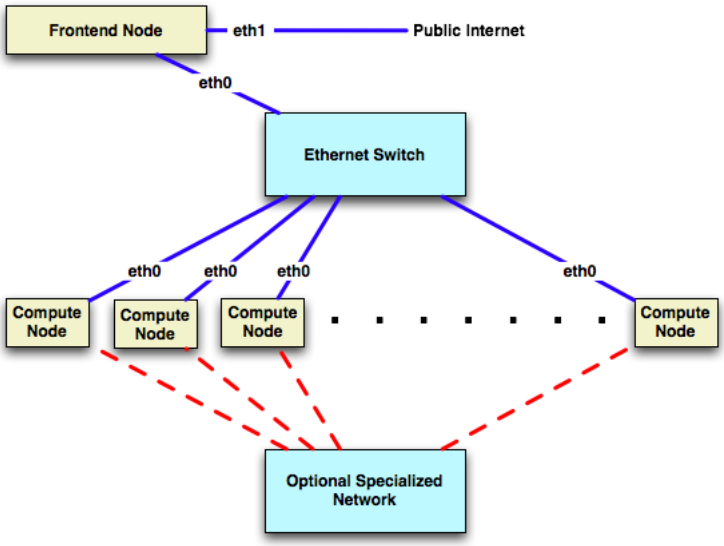
Installing Rocks

1.1 Rocks Installation

We advise you to go through the rocks official [1] documentation before the installation to understand the basic principles of clusters.

1.1.1 Physical Assembly

The first thing to manage is the physical deployment of a cluster.The following diagram shows how the frontend and compute nodes must be connected:



On the Compute nodes (Vm-container), the Ethernet interface that Linux maps to eth0 should be connected to the cluster's Ethernet switch. This

network is considered private, i.e, all traffic on this network is physically separated from the external public network (e.g., The Internet). On the Frontend, at least two Ethernet interfaces are required. The interface that Linux maps to eth0 should be connected to the same Ethernet network as the compute nodes. The interface that Linux maps to eth1 should be connected to the external network (Internet or your organization's intranet).

In our case the eth0 is connected to the switch placed within the rack and eth1 of the Frontend is connected to public network under Networks systems labâĂŹs subnet.

1.2 Frontend Installation

The installation on the Frontend is done using a disk image either by a DVD or a bootable USB drive.The Jumbo DVD has all the required rolls in one single disk image. The x86 64 version of Rocks 6.1 can be downloaded from here [2]

- Insert the DVD/USB Drive and restart the main node (Frontend). A boot screen will be displayed with a prompt. Enter the following command to start the installation:
- The next screen shows the list of all rolls in the DVD. Select the required rolls from the list. The Kernel, Base, OS and Web-Server rolls are mandatory. Additional rolls can be installed by using DVD based rolls. Hit next to proceed.
- The next screen is for entering Cluster Information. Enter the details for Host name, cluster name, organization, locality, state, country, contact, URL, latitude and longitude. The fully-qualified host name is mandatory and is important for several cluster services.
- The next screen has the option to set the eth1 (which is the interface to public network) IP address. This is the public IP of the cluster(connected to the internet). Enter the public IP as 192.168.41.203.
- The next screen has the option to set the private network eth0 IP address and netmask. This is the IP address of the private network between the Frontend and the nodes. The IP address used is 10.1.1.1 and the netmask is 255.255.0.0.

- Now configure the gateway and DNS. Gateway used is 192.168.41.1 and DNS servers used are 192.168.254.2, 192.168.254.3.
- Enter the root password of the cluster when prompted.
- Configure the time by selecting the time zone for the cluster followed by inputting a Network Time Protocol(NTP) server that will keep the clock on the frontend in sync.
- The next screen shows the option for the partitioning of the hard disk of the Frontend. Select "Manual Partitioning" since the configuration of " Auto Partitioning provides insufficient space for the /var partition which is used by the Eucalyptus Cloud to upload Virtual Machine Images.
- The partition used for frontend is:

Partition Name	Size
/	170GB
/var	480GB
/export	170GB
swap	1GB

Chapter 2

Introduction to Eucalyptus

Eucalyptus is a Linux-based software architecture that implements scalable private and hybrid clouds within your existing IT infrastructure. Eucalyptus allows you to provision your own collections of resources (hardware, storage, and network) using a self-service interface on an as-needed basis.

You deploy a Eucalyptus cloud across your enterpriseâĂŹs on-premise data center. Users access Eucalyptus over your enterprise's intranet. This allows sensitive data to remain secure from external intrusion behind the enterprise firewall.

You can install Eucalyptus on the following Linux distributions:

- CentOS 6
- Red Hat Enterprise Linux 6

2.1 Overview

Eucalyptus was designed to be easy to install and as non-intrusive as possible. The software framework is modular, with industry-standard, language-agnostic communication. Eucalyptus provides a virtual network overlay that both isolates network traffic of different users and allows two or more clusters to appear to belong to the same Local Area Network (LAN). Also, Eucalyptus offers API compatibility with AmazonâĂŹs EC2, S3, and IAM services. This offers you the capability of a hybrid cloud.

2.2 Eucalyptus Components

Eucalyptus is comprised of six components: Cloud Controller (CLC), Walrus, Cluster Controller (CC), Storage Controller (SC), Node Controller (NC) and an optional VMware Broker (Broker or VB). Other than the VMware Broker, each component is a stand-alone web service. This architecture allows Eucalyptus both to expose each web service as a well-defined, language-agnostic API, and to support existing web service standards for secure communication between its components. A detailed description of each Eucalyptus component follows.

2.2.1 Cloud Controller

The Cloud Controller (CLC) is the entry-point into the cloud for administrators, developers, project managers, and end-users. The CLC queries other components for information about resources, makes high-level scheduling decisions, and makes requests to the Cluster Controllers (CCs). As the interface to the management platform, the CLC is responsible for exposing and managing the underlying virtualized resources (servers, network, and storage). You can access the CLC through command line tools that are compatible with AmazonâĂŹs Elastic Compute Cloud (EC2) and through a web-based Eucalyptus Administrator Console.

2.2.2 Walrus

Walrus allows users to store persistent data, organized as buckets and objects. You 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 AmazonâĂŹs 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.

2.2.3 Cluster Controller

The Cluster Controller (CC) generally executes on a machine that has network connectivity to both the machines running the Node Controllers (NCs) and to the machine running the CLC. CCs gather information about a set of NCs and schedules virtual machine (VM) execution on specific NCs. The

CC also manages the virtual machine networks. All NCs associated with a single CC must be in the same subnet.

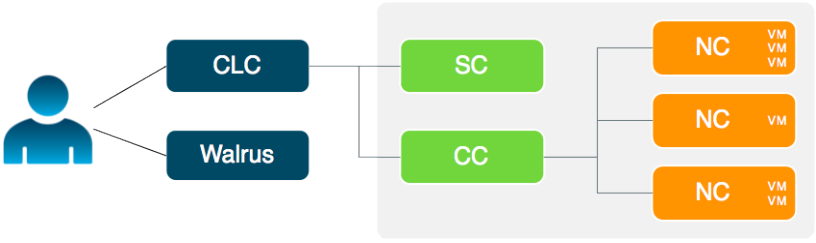
2.2.4 Storage Controller

The Storage Controller (SC) provides functionality similar to the Amazon Elastic Block Store (Amazon EBS). The SC is capable of interfacing with various storage systems. Elastic block storage exports storage volumes that can be attached by a VM and mounted or accessed as a raw block device. EBS volumes persist past VM termination and are commonly used to store persistent data. An EBS volume cannot be shared between VMs and can only be accessed within the same availability zone in which the VM is running. Users can create snapshots from EBS volumes. Snapshots are stored in Walrus and made available across availability zones. Eucalyptus with SAN support lets you use your enterprise-grade SAN devices to host EBS storage within a Eucalyptus cloud.

2.2.5 Node Controller

The Node Controller (NC) executes on any machine that hosts VM instances. The NC controls VM activities, including the execution, inspection, and termination of VM instances. It also fetches and maintains a local cache of instance images, and it queries and controls the system software (host OS and the hypervisor) in response to queries and control requests from the CC. The NC is also responsible for the management of the virtual network endpoint.

2.3 Understanding the Eucalyptus Architecture



The cloud components, Cloud Controller (CLC) and Walrus, communicate with cluster components, the Cluster Controllers (CCs) and Storage Controllers (SCs). The CCs and SCs, in turn, communicate with the Node Controllers (NCs). The networks between machines hosting these components must be able to allow TCP connections between them.

However, if the CCs are on separate network interfaces (one for the network on which the cloud components are hosted and another for the network that NCs use) the CCs will act as software routers between these networks in some networking configurations. So each cluster can use an internal private network for its NCs and the CCs will route traffic from that network to a network shared by the cloud components.

Virtual machines (VMs) run on the machines that host NCs. You can use the CCs as software routers for traffic between clients outside Eucalyptus and VMs. Or the VMs can use the routing framework already in place without CC software routers. However, depending on the layer-2 isolation characteristics of your existing network, you might not be able to implement all of the security features supported by Eucalyptus.

Note : In our cluster we have installed CC, Walrus, CLC, SC in the frontend and the NCâĂŹs in the nodes.

Chapter 3

Network Configuration

3.1 Introduction

This is the most intriguing part of cloud installation, where we will have to decide upon a networking mode available in Eucalyptus. For Zeus cloud we are using Managed (No VLAN) Mode. Read more about managed no vlan here[3].

3.1.1 Enabling Public Web Access to Your Frontend

To permanently enable selected web access to the cluster from other machines on the public network, follow the steps below. Apache's access control directives will provide protection for the most sensitive parts of the cluster web site, however some effort will be necessary to make effective use of them.

To open port 80 (the 'www' service) for the public network of frontend, execute:

```
rocks open host firewall localhost \
network=public protocol=tcp service=www
```

Now you can try accessing the ip `192.168.41.203` or uri `zeus.nitc.ac.in`over network to view the rocks cluster web frontend.

3.1.2 Configuring Firewall

Eucalyptus components use a variety of ports to communicate. The following table lists the all of the important ports used by Eucalyptus.

Port
TCP 8443
TCP 8772
: JMX port. This is disabled by default, and can be enabled with the debug or jmx options for
TCP 8773
TCP 8774
TCP 8775
TCP 8776
TCP 8777
TCP 8080
UDP 7500
UDP 8773
TCP/UDP 53

3.1.3 To open the required ports,run the following commands

Here we are trying to open ports for Eucalyptus to communicate between its components, rocks command *rocks add firewall* can be used to add firewall rules.

Read the following rocks manual to understand more Managing firewall through Rocks [4].

3.1.4 Opening ports in Frontend

```
rocks add firewall host=frontend network=public protocol=tcp service=8443 \ chain=INPUT action=ACCEPT
      rulename=E10-PORT-8443

rocks add firewall host=frontend network=public protocol=tcp service=8772 \
chain=INPUT action=ACCEPT rulename=E10-PORT-8772

rocks add firewall host=frontend network=public protocol=tcp service=8773 \
 chain=INPUT action=ACCEPT rulename=E10-PORT-8773

rocks add firewall host=frontend network=public protocol=tcp service=8774 \
chain=INPUT action=ACCEPT rulename=E10-PORT-8774

rocks add firewall host=frontend network=public protocol=tcp service=8776 \
chain=INPUT action=ACCEPT rulename=E10-PORT-8776

rocks add firewall host=frontend network=public protocol=tcp service=8777 \
chain=INPUT action=ACCEPT rulename=E10-PORT-8777

rocks add firewall host=frontend network=public protocol=tcp service=8080 \
chain=INPUT action=ACCEPT rulename=E10-PORT-8080

rocks add firewall host=frontend network=public protocol=tcp service=5005 \
chain=INPUT action=ACCEPT rulename=E10-PORT-5005

rocks add firewall host=frontend network=public protocol=udp service=7500 \
chain=INPUT action=ACCEPT rulename=E10-PORT-7500
```

Before synchronising the firewall rules we need to remove two rules from the existing firewall. The command to remove the rules are

```
rocks remove firewall global rulename=R900-PRIVILEGED-TCP
rocks remove firewall global rulename=R900-PRIVILEGED-UDP
```

3.1.5 Opening Web Access to Public

Remove the rule which restrict the web access only to subnet 192.168.41.0/24

```
rocks remove firewall host=localhost rulename=A40-WWW-PUBLIC-LAN
```

3.1.6 Now, make it available to public

```
rocks add firewall host=frontend network=public protocol=tcp \
service=www chain=INPUT action=ACCEPT \
flags="-m␣state␣--state␣NEW␣--source␣0.0.0.0/0.0.0.0" \
rulename=A40-WWW-PUBLIC-NEW
```

3.1.7 Sync the above firewall rules to rocks frontend using

```
rocks sync host firewall frontend
```

3.1.8 Accepting everything from TCP and UDP

```
iptables -A INPUT -p udp --dport 0:1023 -j ACCEPT
iptables -A INPUT -p tcp --dport 0:1023 -j ACCEPT
/sbin/service iptables save
```

3.1.9 Opening ports required for DNS functioning

```
iptables -A INPUT -p tcp -m tcp --sport 53 --dport 1024:65535 -m state \ --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m udp --sport 53 --dport 1024:65535 -m state \ --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --sport 1024:65535 --dport 53 -m state \ --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m udp --sport 1024:65535 --dport 53 -m state \ --state NEW,ESTABLISHED -j ACCEPT
/sbin/service iptables save
```

3.1.10 Opening ports in nodes

Opening the web service in nodes

```
rocks add firewall appliance=vm-container protocol=tcp \
service=8775 network=all chain=INPUT action=ACCEPT \
rulename=E10-PORT-8775
```

3.1.11 Sync the firewall rules to all the nodes using

```
rocks sync host firewall vm-container
```

3.2 Verify TCP/IP Connectivity

Verify connectivity between the machines youâĂŹll be installing Eucalyptus on. Some Linux distributions provide default TCP/IP firewalling rules that limit network access to machines. Disable these default firewall settings

before you install Eucalyptus components to ensure that the components can communicate with one another. Verify component connectivity by performing the following checks on the machines that will be running the listed Eucalyptus components.

1. Verify connection from and end-user to the CLC on ports 8773 and 8443
2. Verify connection from an end-user to Walrus on port 8773
3. Verify connection from the CLC, SC, and NC to Walrus on port 8773
4. Verify connection from Walrus, SC, and VB to CLC on port 8777
5. Verify connection from CLC to CC on port 8774
6. Verify connection from CC to VB on port 8773
7. Verify connection from CC to NC on port 8775
8. Verify connection from NC (or VB) to Walrus on port 8773 or you can verify the connection from the CC to Walrus on port 8773, and from an NC to the CC on port 8776
9. Verify connection from public IP addresses of Eucalyptus instances (meta data) and CC to CLC on port 8773
10. Verify TCP connectivity between CLC, Walrus, SC and VB
11. Verify connection between CLC, Walrus, SC, and VB on UDP ports 7500 and 8773

We will use the program given below as socket which will listen to specified a port (as a server), run this program and telnet to the server's ip (where you ran the program) along with port number and check the connection.

```
import java.net.*;
import java.io.*;
public class PortMonitor {
    public static void main(String[] args) throws Exception {
         //Port to monitor
        final int myPort = Integer.parseInt(args[0]);
        ServerSocket ssock = new ServerSocket(myPort);
        System.out.println("port " + myPort + " opened");
         Socket sock = ssock.accept();
        System.out.println("Someone has made socket connection");
         OneConnection client = new OneConnection(sock);
        String s = client.getRequest();
     }
 }
class OneConnection {
    Socket sock;
    BufferedReader in = null;
    DataOutputStream out = null;
OneConnection(Socket sock) throws Exception {
```

```
        this.sock = sock;
        in = new BufferedReader(new InputStreamReader(sock.getInputStream()));
        out = new DataOutputStream(sock.getOutputStream());
    }
String getRequest() throws Exception {
        String s = null;
        while ((s = in.readLine()) != null) {
            System.out.println("got: " + s);
        }
        return s;
    }
}
```

Example (1) Verify connection from and end-user to the CLC on ports 8773
Now run the program in frontend with argument 8773

```
javac Portmonitor.java
java Portmonitor 8773
```

From any other system telnet into frontend with port 8773

```
telnet 192.168.41.203 8773
Trying 192.168.41.203...
Connected to 192.168.41.203.
Escape character is '^]'.
hello
```

Output @ frontend when connection is established

```
port 8773 opened
Someone has made socket connection
got: hello
```

Understand the scenario for each of the verification step given above using the program and telnet.

3.3 Configure SELinux

SELinux is not supported by Eucalyptus

1. Open /etc/selinux/config and edit the line SELINUX=enforcing to SELINUX=permissive.
2. Save the file.
3. Run the following command:
   setenforce 0

3.4 Configure NTP

Eucalyptus requires that each machine have the Network Time Protocol (NTP) daemon started and configured to run automatically on reboot.
NTP in Frontend
Check the status of ntpd daemon *service ntpd status*
Update the time using any server ntpdate -u 0.pool.ntp.org

Sync the time with the hardware clock *hwclock –systohc NTP in Nodes* rocks run host vm-container "ntpd -u 0.pool.ntp.org ; hwclock –systohc"

Chapter 4

Installing Eucalyptus

4.0.1 Enable Centos Repo in frontend

```
sed i.backup 's/enabled = 0/enabled = 1/' /etc/yum.repos.d/CentOS-Base.repo
```

4.0.2 Enable Centos Repo in Nodes

```
for i in {0..4}; do scp /etc/yum.repos.d/CentOS-Base.repo root@vm-container-0-$i:/etc/yum.repos.d/CentOS-
    Base.repo; done
```

4.0.3 Configure the Eucalyptus package repository

On Frontend:

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.3/centos/6/x86_64/eucalyptus-release-3.3.
    noarch.rpm

sed -i.backup 's/enabled = 0/enabled = 1/' eucalyptus-release.repo
```

On the Nodes:

```
for i in {0..4}; do scp /etc/yum.repos.d/euca2ools-release.repo root@vm-container-0-$i:/etc/yum.repos.d/
    euca2ools-release.repo ; done
```

4.0.4 Configure the EPEL package repository

On Frontend:

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.3/centos/6/x86_64/epel-release-6.noarch.
    rpm

sed -i.backup 's/enabled = 0/enabled = 1/' epel.repo
```

On the nodes:

```
for i in {0..4}; do scp /etc/yum.repos.d/epel.repo root@vm-container-0-$i:/etc/yum.repos.d/epel.repo ; done
```

4.0.5 Configure the ELRepo repository on frontend

```
yum install http://downloads.eucalyptus.com/software/eucalyptus/3.3/centos/6/x86_64/elrepo-release-6.noarch.
    rpm
sed -i.backup 's/enabled = 0/enabled = 1/' elrepo.repo
```

4.0.6 Install the Eucalyptus node controller software on each planned NC host

```
rocks run host vm-container "yum install eucalyptus-nc"
```

Check that the KVM device node has proper permissions. Run the following command:

```
rocks run host vm-container "ls -l /dev/kvm"
```

Verify the output shows that the device node is owned by user root and group kvm.

```
crw-rw-rw- 1 root kvm 10, 232 Nov 30 10:27 /dev/kvm
```

If your kvm device node does not have proper permissions, you need to reboot your node and change settings in BIOS to enable KVM.

4.0.7 Install the Eucalyptus cloud controller software on each planned CLC host

```
yum install eucalyptus-cloud
```

4.0.8 Install the software for the remaining Eucalyptus components in the frontend

```
yum install eucalyptus-cc eucalyptus-sc eucalyptus-walrus
```

If you would like Load Balancer support enabled in your Cloud, you will need to install the Load Balancer image package on the frontend:

```
yum install eucalyptus-load-balancer-image
```

After you have installed Eucalyptus, test multicast connectivity between each CLC and Walrus, and SC.

Run the following receiver command on the CLC:

```
java -classpath /usr/share/eucalyptus/jgroups-2.11.1.Final.jar\
 org.jgroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555
```

Once the receiver command blocks, simultaneously run the following sender command on each Walrus host:

```
java -classpath /usr/share/eucalyptus/jgroups-2.11.1.Final.jar\
 org.jgroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555
```

The two applications should be able to connect and arbitrary lines entered on the sender should appear on the receiver.

Chapter 5

Configuring Eucalyptus

5.1 Introduction

This section describes the parameters that need to be set in order to launch Eucalyptus for the first time. The first launch of Eucalyptus is different than a restart of a previously running Eucalyptus deployment in that it sets up the security mechanisms that will be used by the installation to ensure system integrity. Eucalyptus configuration is stored in a text file, /etc/eucalyptus/eucalyptus.conf, that contains key-value pairs specifying various configuration parameters. Eucalyptus reads this file when it launches and when various forms of reset commands are sent it the Eucalyptus components. Perform the following tasks after you install Eucalyptus software, but before you start the Eucalyptus services.

5.2 Configuring network modes

This section provides detailed configuration instructions for each of the four Eucalyptus networking modes. Eucalyptus requires network connectivity between its clients (end-users) and the cloud components (CC, CLC, and Walrus). In Managed (No VLAN) modes, traffic to instances pass through the CC. So, in this modes clients must be able to connect to the CC. In System and Static modes, clients need to connect directly to the NC. The CC does not act as a router in these two modes. The /etc/eucalyptus/eucalyptus.conf file contains all network-related options in in the âĂIJNetworking ConfigurationâĂİ section. These options use the prefix VNET_. The most commonly used VNET options are described in the following table. The set of networking settings that apply to a cloud varies based on its networking mode. Each setting in this section lists the modes in which it applies.

Unless otherwise noted, all of these settings apply only to CCs. The /etc/eucalyptus/eucalyptus.conf file contains all network-related options in in the Networking Configuration section. These options use the prefix VNET_. The most commonly used VNET options are described in the following table. We are using Managed-NoVLAN mode, below he have described the parameters to be for set for our network.

5.3 Frontend Configuration

Make the required changes in the file /etc/eucalyptus/eucalyptus.conf Given below is the Networking Configuration part of the eucalyptus.conf file after editing it as required.

```
# NETWORKING CONFIGURATION
##########################################################################
VNET_MODE="MANAGED-NOVLAN"
VNET_PRIVINTERFACE="eth0"
VNET_PUBINTERFACE="eth1"
VNET_BRIDGE="br0"
#VNET_MACMAP="AA:DD:11:CE:FF:ED=192.168.1.2 AA:DD:11:CE:FF:EE=192.168.1.3"
VNET_PUBLICIPS="192.168.41.215-192.168.41.240"
VNET_SUBNET="10.1.0.0"
VNET_NETMASK="255.255.0.0"
VNET_ADDRSPERNET="32"
VNET_DNS="192.168.254.2"
#VNET_DOMAINNAME="eucalyptus.internal"
#VNET_BROADCAST="192.168.1.255"
#VNET_ROUTER="192.168.1.1"
#VNET_LOCALIP="your-public-interface's-ip"
VNET_DHCPDAEMON="/usr/sbin/dhcpd41"
VNET_DHCPUSER="dhcpd"
```

5.4 Nodes Configuration

Get the eucalyptus.conf file from any of the nodes, edit it as per requirement and copy it back to all nodes Copy one file

```
scp root@vm-container-0-0:/etc/eucalyptus/eucalyptus.conf ~
```

Edit the file

```
# NETWORKING CONFIGURATION
##########################################################################
VNET_MODE="MANAGED-NOVLAN"
VNET_PRIVINTERFACE="eth0"
VNET_PUBINTERFACE="eth0"
VNET_BRIDGE="eth0"
#VNET_MACMAP="AA:DD:11:CE:FF:ED=192.168.1.2 AA:DD:11:CE:FF:EE=192.168.1.3"
#VNET_PUBLICIPS="your-free-public-ip-1 your-free-public-ip-2 ..."
#VNET_SUBNET="192.168.0.0"
#VNET_NETMASK="255.255.0.0"
#VNET_ADDRSPERNET="32"
#VNET_DNS="your-dns-server-ip"
#VNET_DOMAINNAME="eucalyptus.internal"
#VNET_BROADCAST="192.168.1.255"
#VNET_ROUTER="192.168.1.1"
#VNET_LOCALIP="your-public-interface's-ip"
VNET_DHCPDAEMON="/usr/sbin/dhcpd41"
```

Chapter 6

Configuring The Runtime Environment

6.1 INTRODUCTION

After Eucalyptus is installed and registered, perform the tasks in this section to configure the runtime environment.

6.2 GENERATE ADMINISTRATOR CREDENTIALS

Now that you have installed and configured Eucalyptus, you're ready to start using it. To do so, you must generate credentials.

NOTE: When you run the euca_conf –get-credentials command, you are requesting the access and secret keys and an X.509 certificate and key. You cannot retrieve an existing X.509 certificate and key. You can only generate a new pair.

To generate a set of credentials :

```
/usr/sbin/euca_conf --get-credentials admin.zip
unzip admin.zip
```

Source the eucarc file.

```
source eucarc
```

You are now able to run Eucalyptus commands. Tip : When you source something remember not to change the present working directory since bash environment variable won't be available after you cd into another.

6.3 CONFIGURING THE STORAGE CONTROLLER (SC)

The Eucalyptus Storage Controller must be configured explicitly upon registration. This is a change from previous versions (pre-3.2) of Eucalyptus, which would configure themselves to a default configuration using a tgtd-based filesystem-backed storage controller to provide volumes and snapshots directly from the Storage Controller. As of version 3.2, Eucalyptus Storage Controllers automatically go to the BROKEN state after being registered with the CLC and will remain in that state until the administrator explicitly configures the SC by telling it which backend storage provider to use.

Configuring the SC to use the local filesystem (Overlay):

```
euca-modify-property -p zeus.storage.blockstoragemanager=overlay
```

Possible Output: PROPERTY PARTI00.storage.blockstoragemanager overlay was <unset> You can check if it has been modified by executing the command :

```
euca-describe-properties | grep blockstoragemanager
```

6.4 CONFIGURING THE DNS AND THE SUBDOMAIN

Eucalyptus provides a DNS service that you can configure to:

1. Map instance IPs and Walrus bucket names to DNS host names
2. Enable DNS delegation to support transparent failover in HA mode

The DNS service will automatically try to bind to port 53. If port 53 cannot be used, DNS will be disabled. Typically, other system services like dnsmasq are configured to run on port 53. To use the Eucalyptus DNS service, you will need to disable these services. Before using the DNS service, configure the DNS subdomain name that you want Eucalyptus to handle as follows after the Eucalyptus Cloud Controller (CLC) has been started.

Log in to the CLC (the primary CLC in an HA setup) and enter the following:

```
euca-modify-property -p system.dns.dnsdomain=192.168.41.203
```

6.5 TURN ON IP MAPPING

To turn on mapping of instance IPs to DNS host names: Enter the following command on the CLC (the primary CLC in an HA setup):

```
euca-modify-property -p bootstrap.webservices.use_instance_dns=true
```

6.6 CONFIGURE THE MASTER DNS SERVER

Note : Please read for DNS and creating a zone file before attempting to the steps given below.

1. A good wiki article is available for understanding dns `http://en.wikipedia.org/wiki/Zone_file.`

2. A you should always look @ the original documentation provided by eucalyptus `http://www.eucalyptus.com/docs/eucalyptus/3.2/ig/setting_up_dns.html#setting_up_dns`

Set up your master DNS server to forward the Eucalyptus subdomain to the primary and secondary CLC servers, which act as name servers.

1. Open /etc/named.conf and set up the eucadomain.yourdomain zone. Add the following piece of code to the named.conf file.

```
zone "zeus.nitc.ac.in" {
        type master;
        file "/etc/named/db.zeus.nitc.ac.in";
};
#forward to master dns

zone "eucalyptus.zeus.nitc.ac.in"{
        type forward;
        forward only;
        forwarders { 192.168.41.203; };
};
```

2. Create a file /etc/bind/db.zeus.nitc.ac.in and write the following code into that file.

```
$TTL 604800
@ IN SOA zeus.nitc.ac.in. root.zeus.nitc.ac.in. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@ IN NS ns.zeus.nitc.ac.in.
@ IN A 192.168.41.203
;Assuming the master dns being the local campus dns 192.168.254.2
ns.zeus.nitc.ac.in. IN A 192.168.41.203

eucalyptus.zeus.nitc.ac.in. IN A 192.168.41.203
```

6.7 CONFIGURING THE NODE CONTROLLER

To alleviate potential problems, we recommend performing the following steps on each NC:

- Log in to an NC server and open the /etc/eucalyptus/eucalyptus.conf file.
- Change the CONCURRENT_DISK_OPS parameter to the number of disk-intensive operations you want the NC to perform at once. On some Linux installations, a sufficiently large amount of local disk activity can slow down process scheduling. This can cause other operations (e.g., network communication and instance provisioning) appear to stall. Examples of disk-intensive operations include preparing disk images for launch and creating ephemeral storage. Set this value to 1 to serialize all disk-intensive operations. Set to a higher number to increase the amount of disk-intensive operations the NC will perform in parallel.
- Set DISABLE_KEY_INJECTION=1 to disable key injection. By default, the node controller uses the filesystem to perform key injection. This is potentially an unsafe practice. Copy one file, edit it and spread it to all other nodes. Copy

```
scp root@vm-container-0-0:/etc/eucalyptus/eucalyptus.conf ~
```

Spread

```
for i in {0..4}; do scp ~/eucalyptus.conf root@vm-container-0-$i:/etc/eucalyptus/eucalyptus.conf ;
    done
```

Uncomment

```
#CONCURRENT_DISK_OPS =4
#DISABLE_KEY_INJECTION="0"
```

and change their values to

```
CONCURRENT_DISK_OPS =1
DISABLE_KEY_INJECTION="1"
```

6.8 INCREASE WALRUS DISK SPACE

The size of Walrus storage must be larger than the sum of all the uploaded images. Each uploaded image requires additional space to accommodate image decryption and the creation of temporary working files. **We recommend that the Walrus storage size be three times the size of all uploaded images.** To increase the image cache size in Walrus:

1. Log in to the Eucalyptus Administrator Console `https://zeus.nitc.ac.in:8443`.
2. Click Service Components in the Quick Links section.
3. The Service Components page displays.
4. Click walrus.
5. The Properties section displays.
6. Enter the new size 80 000 MB (80GB) in the space reserved for unbundling images field.
7. Click Save.

6.9 Set up security roups

In Managed and Managed (No VLAN) networking modes, you must configure the system with parameters that define how Eucalyptus will allocate and manage virtual machine networks. These virtual machine networks are known as security groups. The relevant parameters are set in the eucalyptus.conf on all machines running a CC. These parameters are:

- VNET_SUBNET
- VNET_NETMASK
- VNET_ADDRSPERNET

The CC will read VNET_SUBNET and VNET_NETMASK to construct a range of IP addresses that are available to all security groups. This range will then be further divided into smaller networks based on the size specified in VNET_ADDRSPERNET. Note that Eucalyptus reserves eleven addresses per security group, so these networks will be smaller than the value specified in VNET_ADDRSPERNET.

To configure Eucalyptus to use VLANs within a specified range:

1. Choose your range (a contiguous range of VLANs between 2 and 4095).
2. Configure your cluster controllers with a VNET_SUBNET, VNET_NETMASK, VNET_ADDRSPERNET that is large enough to encapsulate your desired range.
3. We have VNET_NETMASK as 255.255.0.0 and VNET_SUBNET 10.1.0.0

4. We should have distinct VLAN Tags for each security group.

5. No of Security Groups is calculated by dividing VNET_NETMASK, VNET_ADDRSPERNET i.e (2î6 -2)/32=2048.
   Refer `https://engage.eucalyptus.com/customer/portal/articles/256617-calculating-security-groups`

6. Configure your cloud controller to work within that range. Use the following commands to verify that the range is now set to be 2-2048, a superset of the desired range.

```
euca-describe-properties | grep cluster.maxnetworktag
euca-describe-properties | grep cluster.minnetworktag
```

7. Constrict the range to be within the range that the CC can support as follows:

```
euca-modify-property -p cloud.network.global_max_network_tag=2050
euca-modify-property -p cloud.network.global_min_network_tag=2
```

8. Make sure that the difference between the max and min value should be equal to 2048 (ie the no of security groups).

6.10 Configure the load balancer

Installing and Registering the Load Balancer Image : Eucalyptus provides a tools for installing and registering the Load Balancer image. Once you have run the tool, your Load Balancer will be ready to use. Run the following command on the machine where you installed the eucalyptus-load-balancer-image package:

```
euca-install-load-balancer --install-default
```

6.11 Verify the load balancer configuration

If you would like to verify that Load Balancer support is enabled you can list installed Load Balancers. The currently active Load Balancer will be listed as enabled. If no Load Balancers are listed, or none are marked as enabled, then your Load Balancer support has not been configured properly.

Run the following command to list installed Load Balancer images:

```
euca-install-load-balancer --list
```

You can also check the enabled Load Balancer EMI with:

```
euca-describe-properties loadbalancing.loadbalancer_emi
```

```
If you need to manually set the enabled Load Balancer EMI use:
euca-modify-property -p loadbalancing.loadbalancer_emi=emi-12345678
```

If you need to manually set the enabled Load Balancer EMI use: euca-modify-property -p loadbalancing.loadbalancer_emi=emi-12345678

6.12 Change the administrative path

Change the default password for the administration user. You can do this using the euare-usermodloginprofile or by logging in to the Eucalyptus Administrator Console `https://zeus.nitc.ac.in:8443`. The first time you log in to the console, you are prompted for a new password.

References

[1] Rocks official documentation
http://central6.rocksclusters.org/roll-documentation/base/6.1/

[2] Rocks official documentation
http://www.rocksclusters.org/wordpress/?page_id=449.

[3] Eucalyptus Managed No VLan
https://www.eucalyptus.com/docs/eucalyptus/3.2/ig/planning_managed_novlan.html#planning_managed_novlan

[4] Manage firewall using rocks
hhttp://central6.rocksclusters.org/roll-documentation/base/6.1/firewall.html