Chapter Three

Network Configuration

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 [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 website.

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	Description
TCP 8443	SSL port for the administrative web user interface. Configurable with euca-modify-property.
TCP 8772	DEBUG ONLY: JMX port. This is disabled by default, and can be enabled with the --debug or --jmx options for CLOUD_OPTS.

TCP 8773	Web services port for the CLC, Walrus, SC, and VB; also used for external and internal communications by the CLC and Walrus. Configurable with euca-modify-property.
TCP 8774	Web services port on the CC. Configured in the eucalyptus.conf configuration file.
TCP 8775	Web services port on the NC. Configured in the eucalyptus.conf configuration file.
TCP 8776	Used by the image cacher on the CC. Configured in the eucalyptus.conf configuration file.
TCP 8777	Database port on the CLC.
TCP 8080	Port for the administrative web user interface. Forwards to 8443. Configurable with euca-modify-property.
UDP 7500	Distributed cache port on the CLC, Walrus, SC, and VB.
UDP 8773	HA membership port.
TCP/UDP 53	DNS port on the CLC.

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 [2] .

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
```

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
```

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
```

Sync the above firewall rules to rocks frontend using

```
rocks sync host firewall frontend
```

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
```

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
```

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
```

Sync the firewall rules to all the nodes using

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

Verify TCP/IP Connectivity

Verify connectivity between the machines you'll 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 (metadata) 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 etablished

```
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.

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:
4. setenforce 0

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”
```

External Links [1] http://www.eucalyptus.com/docs/eucalyptus/3.2/ig/planning_managed_novlan.html#planning_managed_novlan

[2]http://central6.rocksclusters.org/roll-documentation/base/6.1/firewall.html