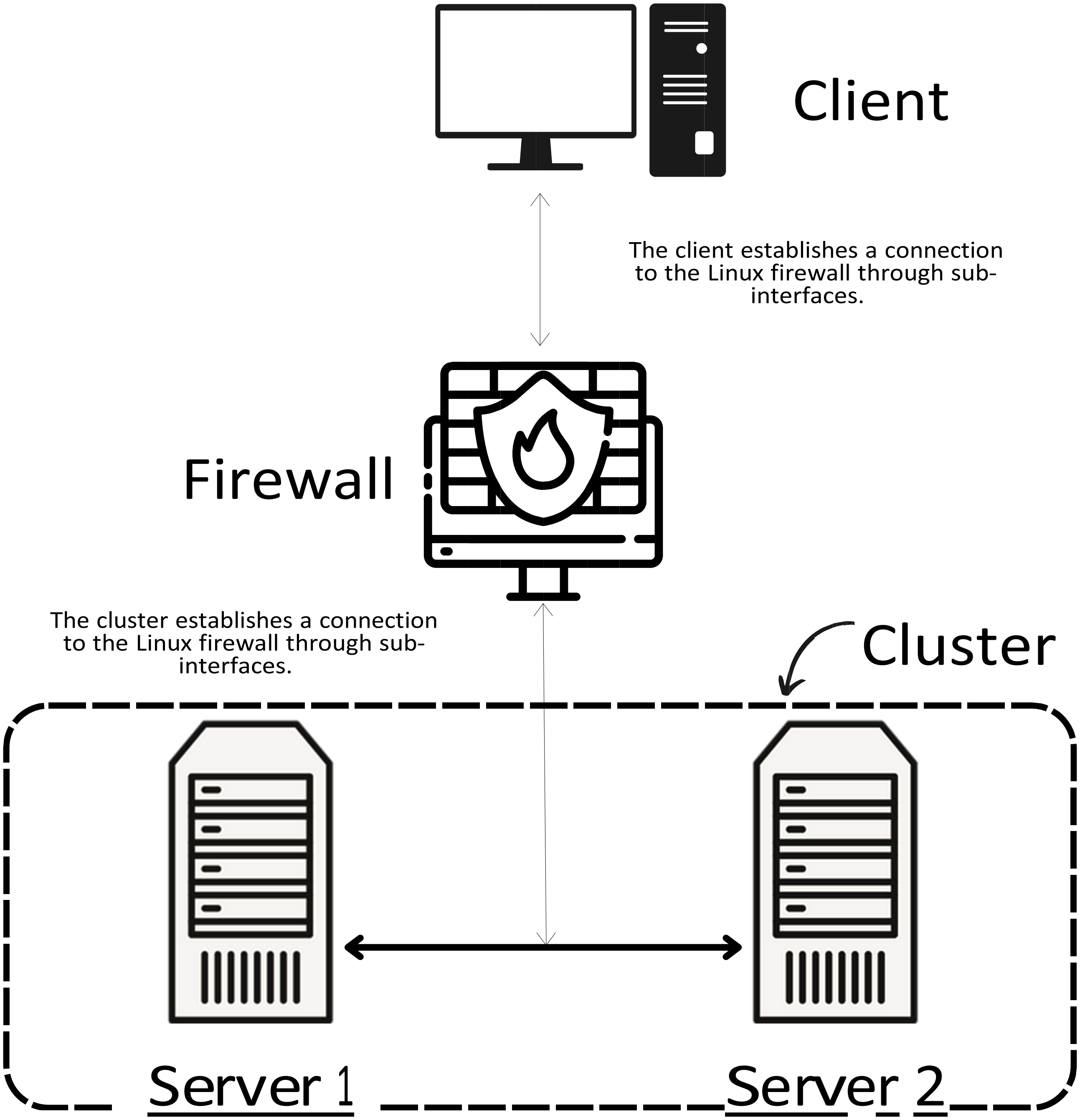
Name: Niyonkuru Valens
ID:25097

Linux Final Project Documentation


Client
The client establishes a connection to the Linux firewall through sub-interfaces.
Firewall
The cluster establishes a connection to the Linux firewall through sub-interfaces.
Cluster
Server 1
Server 2

This project requires us to implement 4 nodes infrastructure and configuring some services like bind* for DNS(Domain Name Service) , httpd* for Web configurations , and clustering servers . Clustering will help when one server goes down , the other one will immediately take a task . one will be master server then, other will be a slave server. We will also configuring firewall . firewall will be overall during communication between servers -> firewall->client . we will need to restriction for accessing websites so , we will configure iptables ,

I chose using Rhel 7.7 in this project , in order to be familiar with and being experienced with Redhat versions .

1 Machines Installations in VMWARE workstation 17 pro

I've installed 1 machine (master server) then I cloned it into 5 machines that I will use Slave, farewall, client . I followed all installing instruction in Rhel7.7 .

2. Configuring Repolist "a list of repo" **promotes efficiency, reliability, and security in software distribution and management.**

Steps for creating repo

Mkdir /valens

Load the cd into the vm and do cd /run/media/[hit tab] /Packages

cp * -v /valens

NB: note that in redhat 7 no need to install rpm createrepo delta python-delta because they are already there

createrepo -v /valens

vim

/etc/yum.repos.d/valens.repo Hit insert mode and put this in the above file

—-------------------------------

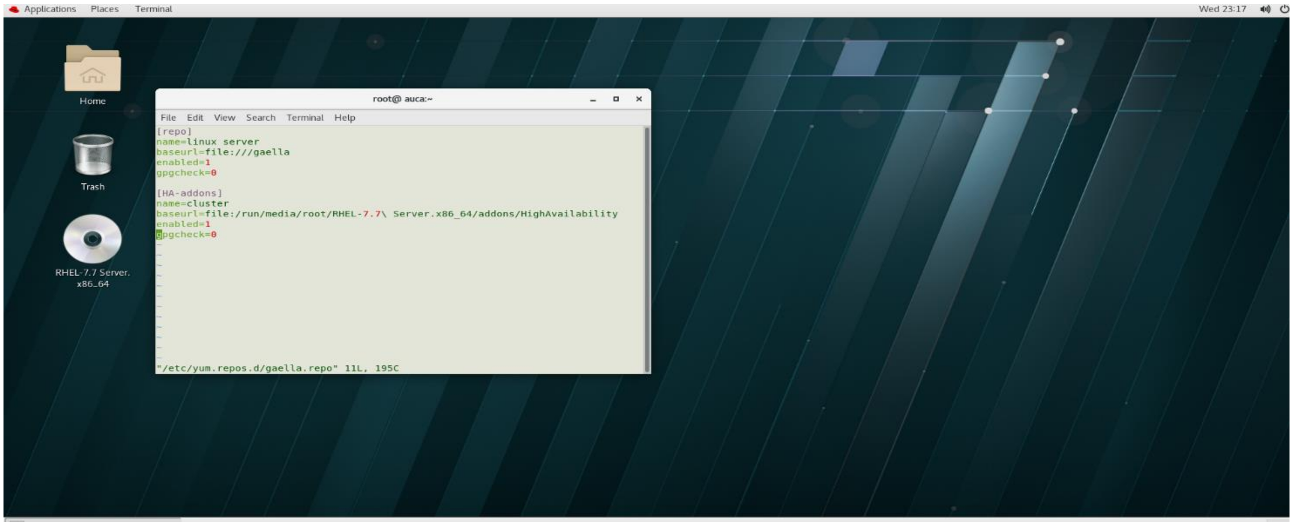
```
[server]
name= assign any name you like
baseurl=file:///valens
enabled=1
gpgcheck=0
```

the save (:wq)

Since we need the pacemaker we need to get it from addons so go back to the file above and add this.

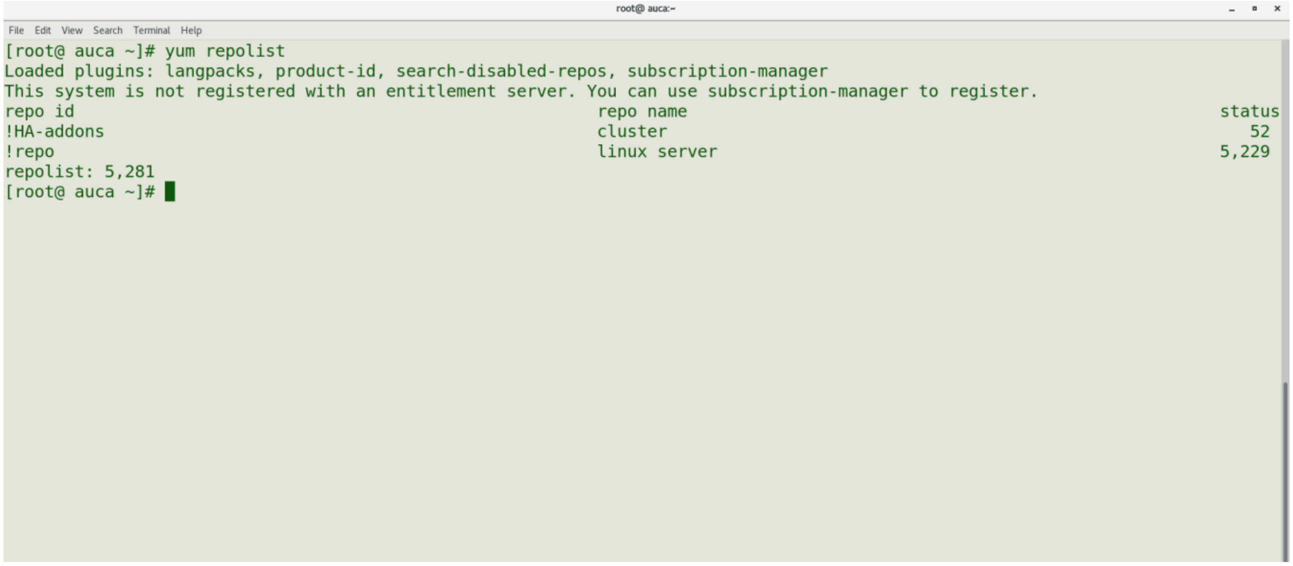
```
[HA]
name=HighAvailability
baseurl= file:/run/media/[hit tab]/addons/HighAvailablity
Enabled=1
gpgcheck=0
```

the save (:wq)



```
[repo]
name=linux server
baseurl=file:///gaella
enabled=1
gpgcheck=0

[HA-addons]
name=cluster
baseurl=file:/run/media/root/RHEL-7.7\ Server.x86_64/addons/HighAvailability
enabled=1
gpgcheck=0
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/yum.repos.d/gaella.repo" 11L, 195C
```

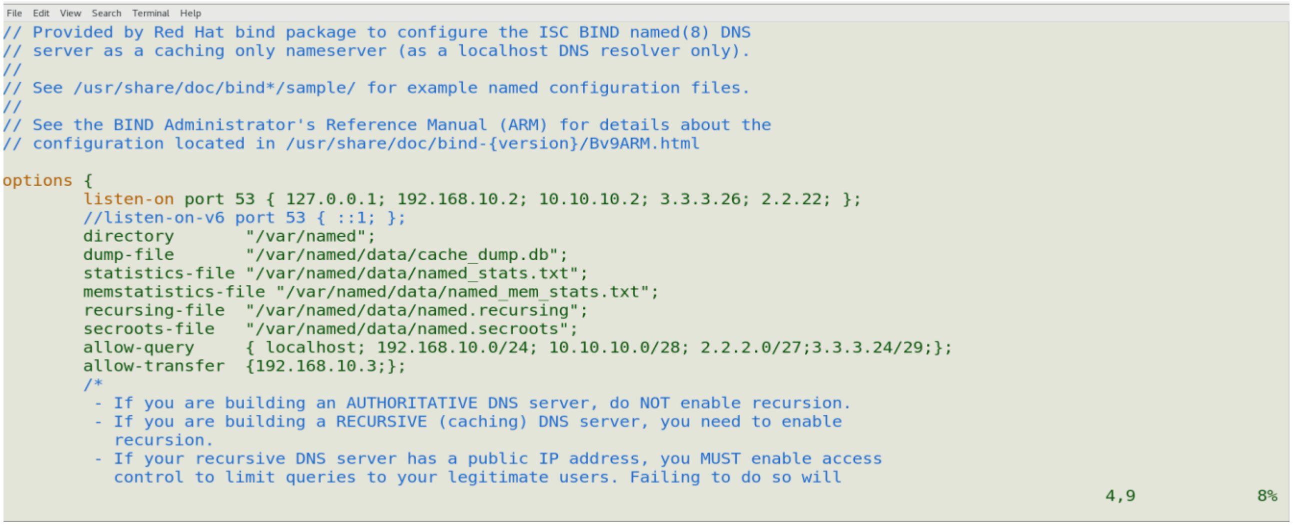
Then yum repolist then you get the following



```
[root@ auca ~]# yum repolist
Loaded plugins: langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.
repo id                                                     repo name                                                      status
!HA-addons                                                  cluster                                                            52
!repo                                                       linux server                                                    5,229
repolist: 5,281
[root@ auca ~]# 
```

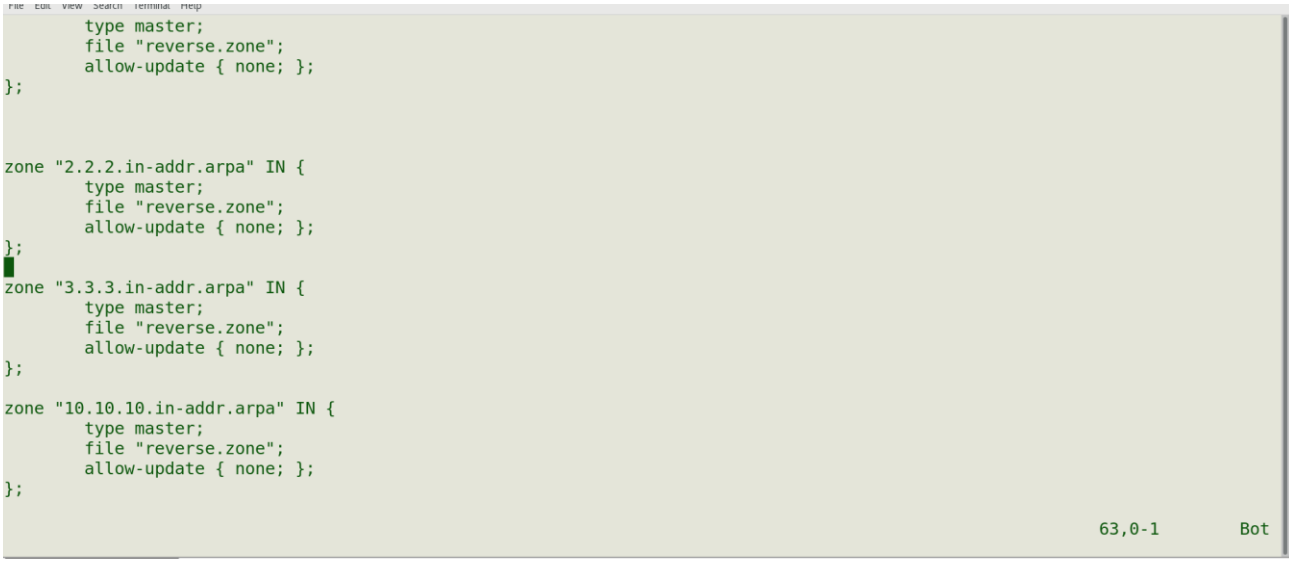
Bind* service(DNS)

BIND (Berkeley Internet Name Domain) is the most widely used DNS (Domain Name System) software on the internet It's installed on Linux systems for DNS resolution, translating domain names (auca.com) into IP addresses (2.2.2.2) vim /etc/named.conf



```
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 127.0.0.1; 192.168.10.2; 10.10.10.2; 3.3.3.26; 2.2.22; };
        //listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost; 192.168.10.0/24; 10.10.10.0/28; 2.2.2.0/27;3.3.3.24/29;};
        allow-transfer  {192.168.10.3;};
        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
                                                                                   4,9           8%
```

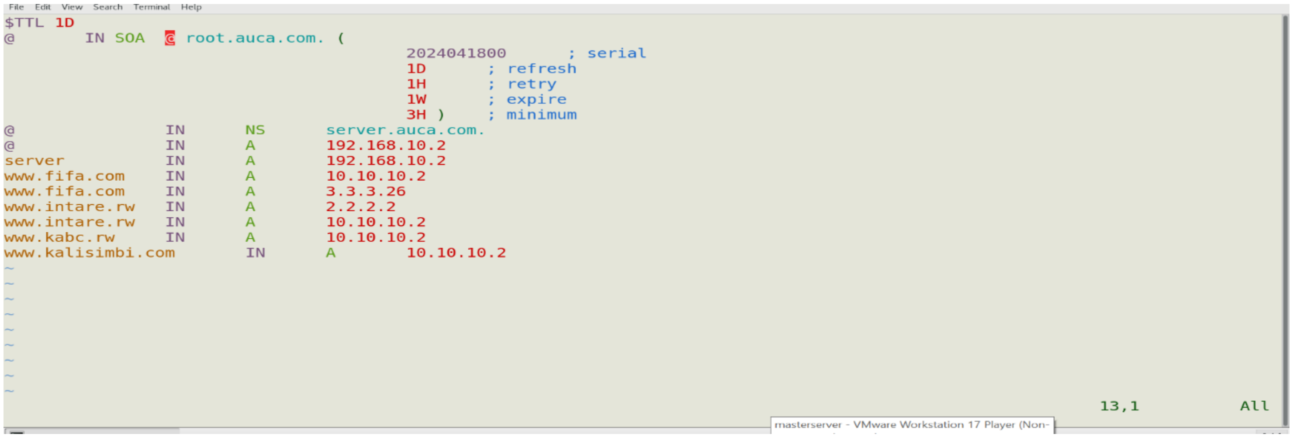
Add this at the bottom of the file /etc/named.rfc912.zones our domain will be auca.com



```
        type master;
        file "reverse.zone";
        allow-update { none; };
};



zone "2.2.2.in-addr.arpa" IN {
        type master;
        file "reverse.zone";
        allow-update { none; };
};

zone "3.3.3.in-addr.arpa" IN {
        type master;
        file "reverse.zone";
        allow-update { none; };
};

zone "10.10.10.in-addr.arpa" IN {
        type master;
        file "reverse.zone";
        allow-update { none; };
};

                                                                                63,0-1        Bot
```

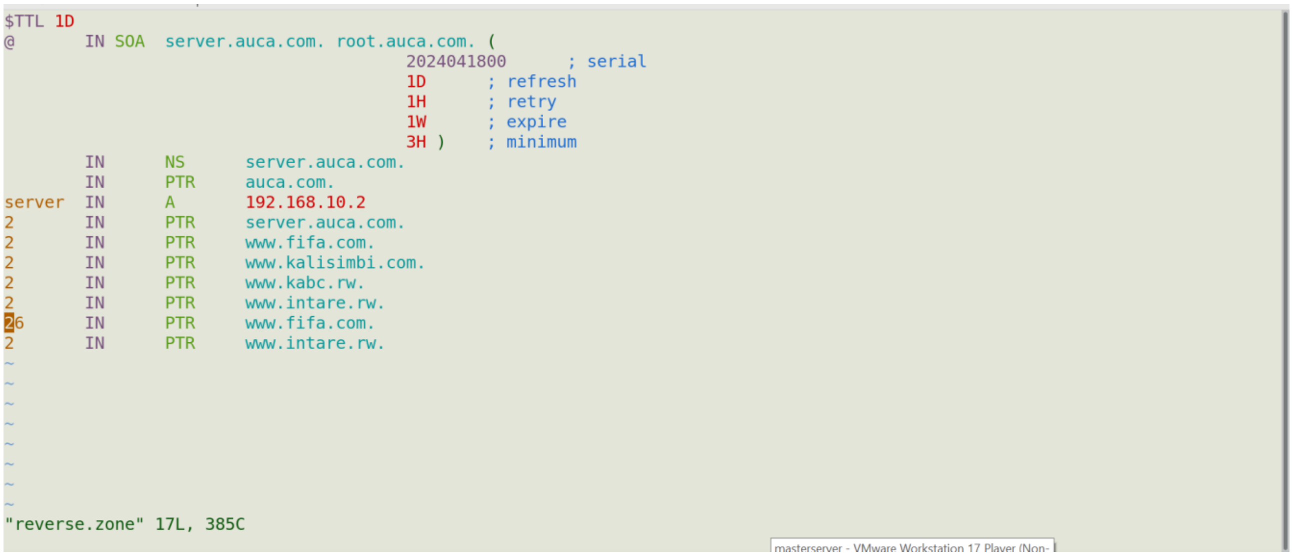
Create the forward.zone and reverse.zone because it is in the above folder the two files must be created under /var/named and edit them like this.

This is the forward.zone file


File Edit View Search Terminal Help
masterserver - VMware Workstation 17 Player (Non-

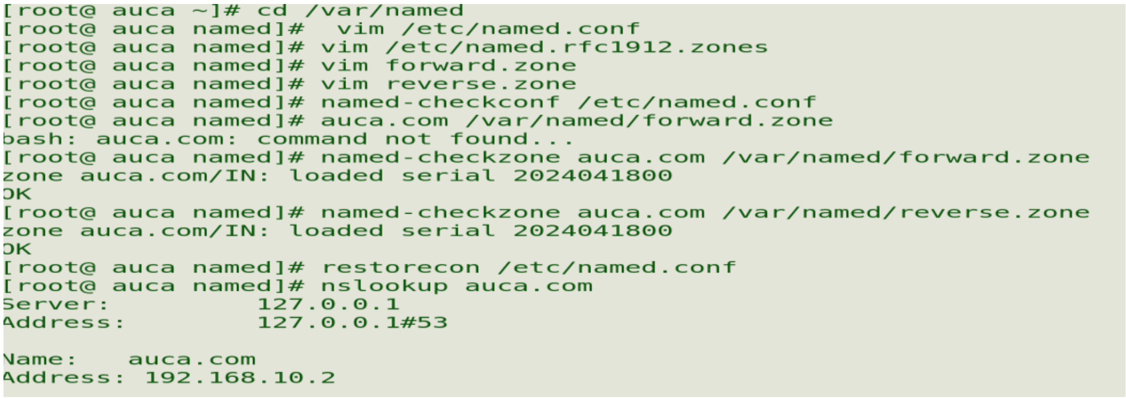
```
$TTL 1D
@       IN SOA  @ root.auca.com. (
                                        2024041800      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@               IN      NS      server.auca.com.
@               IN      A       192.168.10.2
server          IN      A       192.168.10.2
www.fifa.com    IN      A       10.10.10.2
www.fifa.com    IN      A       3.3.3.26
www.intare.rw   IN      A       2.2.2.2
www.intare.rw   IN      A       10.10.10.2
www.kabc.rw     IN      A       10.10.10.2
www.kalisimbi.com       IN      A       10.10.10.2
~
~
~
~
~
~
~
~
~
                                                                13,1          All
```

This is the forward.zone file

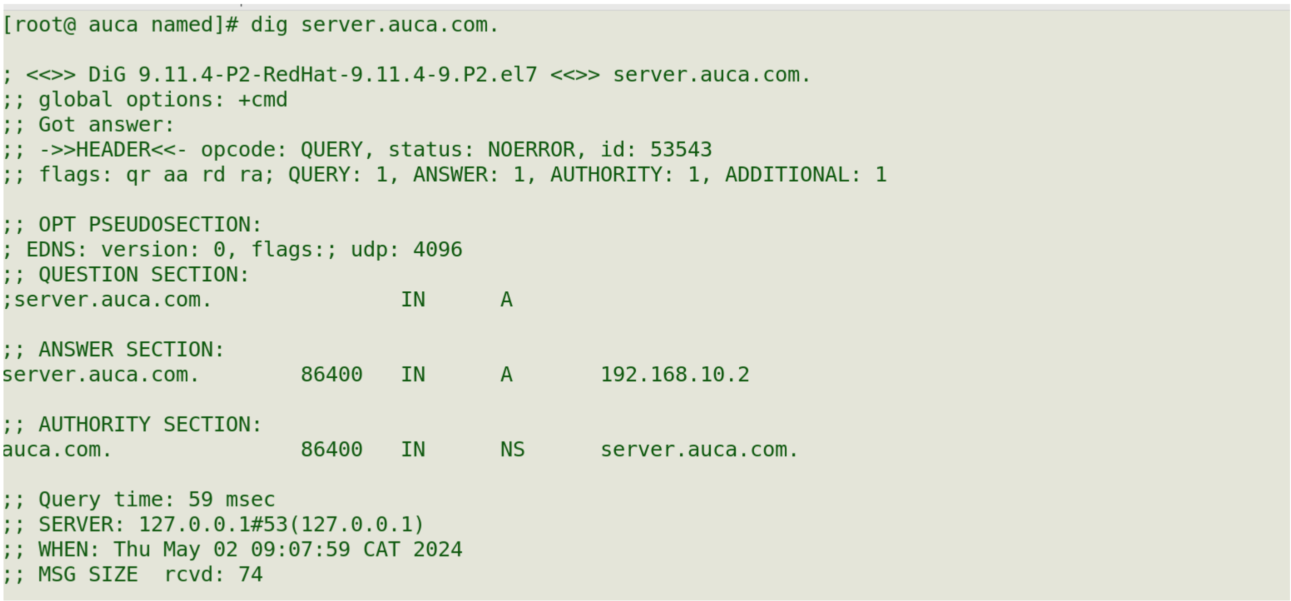


```
$TTL 1D
@       IN SOA  server.auca.com. root.auca.com. (
                                        2024041800      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      server.auca.com.
        IN      PTR     auca.com.
server  IN      A       192.168.10.2
2       IN      PTR     server.auca.com.
2       IN      PTR     www.fifa.com.
2       IN      PTR     www.kalisimbi.com.
2       IN      PTR     www.kabc.rw.
2       IN      PTR     www.intare.rw.
26      IN      PTR     www.fifa.com.
2       IN      PTR     www.intare.rw.
~
~
~
~
~
~
~
~
"reverse.zone" 17L, 385C
```

Then Checking errors by this command named-checkconf /etc/named.conf
if you get error ,
Then also check for the zone named-checkzone
for forward :auca.com /var/named/forward.zone : okay
[root@ auca named]# named-checkzone auca.com /var/named/forward.zone
zone auca.com/IN: loaded serial 2024041800
OK
[root@ auca named]#
for reverse :auca.com /var/named/reverse.zone : okay
[root@ auca named]# named-checkzone auca.com /var/named/reverse.zone
zone auca.com/IN: loaded serial 2024041800
OK
[root@ auca named]#
Then do restorecon /etc/named.conf for security enhancement
Then nslookup auca.com the get the ip address of auca.com



```
[root@ auca ~]# cd /var/named
[root@ auca named]#  vim /etc/named.conf
[root@ auca named]# vim /etc/named.rfc1912.zones
[root@ auca named]# vim forward.zone
[root@ auca named]# vim reverse.zone
[root@ auca named]# named-checkconf /etc/named.conf
[root@ auca named]# auca.com /var/named/forward.zone
bash: auca.com: command not found...
[root@ auca named]# named-checkzone auca.com /var/named/forward.zone
zone auca.com/IN: loaded serial 2024041800
OK
[root@ auca named]# named-checkzone auca.com /var/named/reverse.zone
zone auca.com/IN: loaded serial 2024041800
OK
[root@ auca named]# restorecon /etc/named.conf
[root@ auca named]# nslookup auca.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   auca.com
Address: 192.168.10.2
```

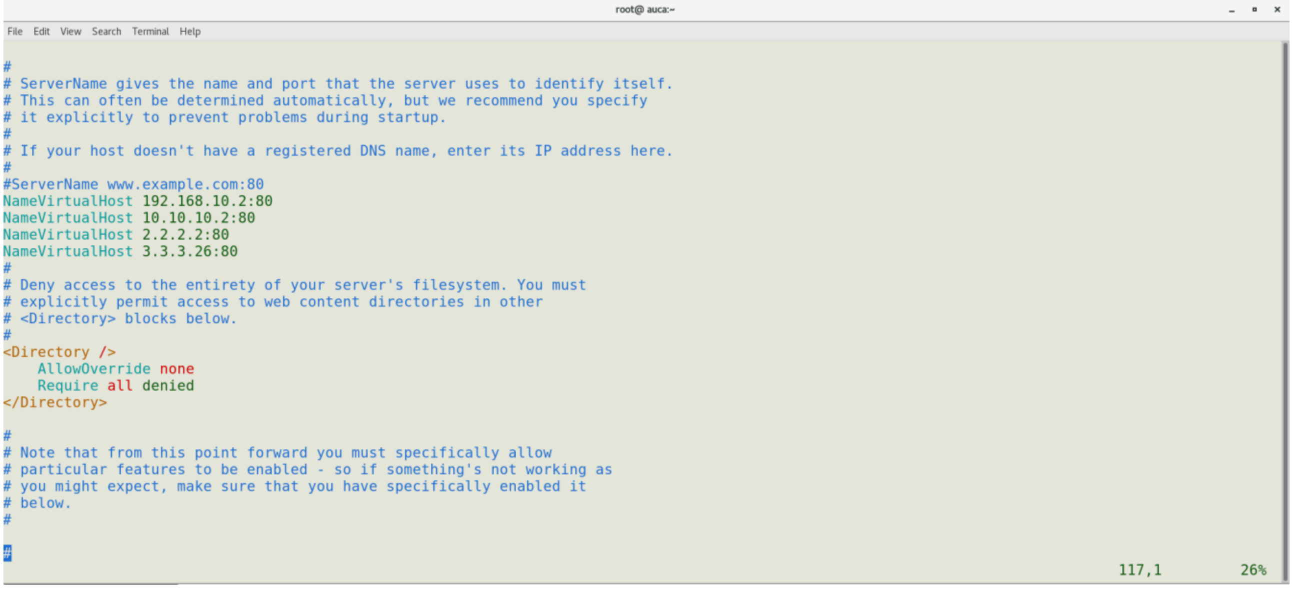


```
[root@ auca named]# dig server.auca.com.

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> server.auca.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53543
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;server.auca.com.               IN      A

;; ANSWER SECTION:
server.auca.com.        86400   IN      A       192.168.10.2

;; AUTHORITY SECTION:
auca.com.               86400   IN      NS      server.auca.com.

;; Query time: 59 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 02 09:07:59 CAT 2024
;; MSG SIZE  rcvd: 74
```

Httpd * service (web server)

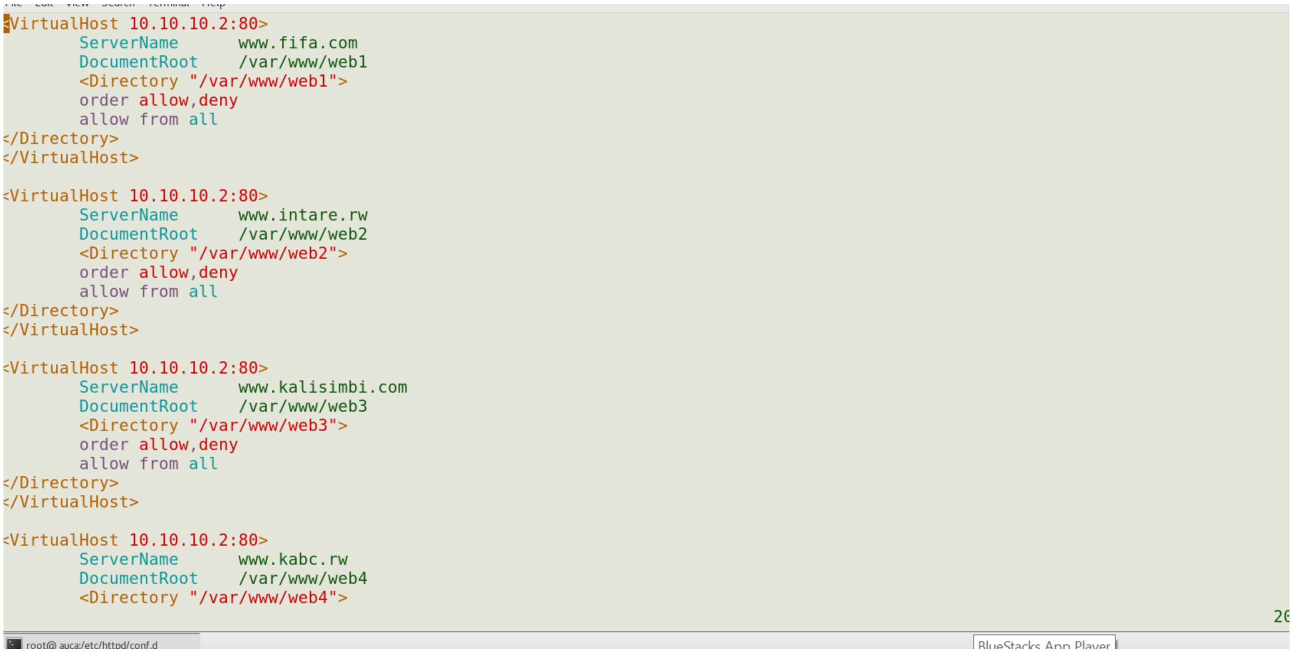
For web hosting HTTP servers like Apache HTTP Server are essential for hosting websites on Linux systems.

Do yum install httpd* -y to install the web server and all the additional packages
After go in the file /etc/httpd/conf/httpd.conf to add the NameVirtualHost and the port of httpd remember the sub-interfaces we created it will come in handy.



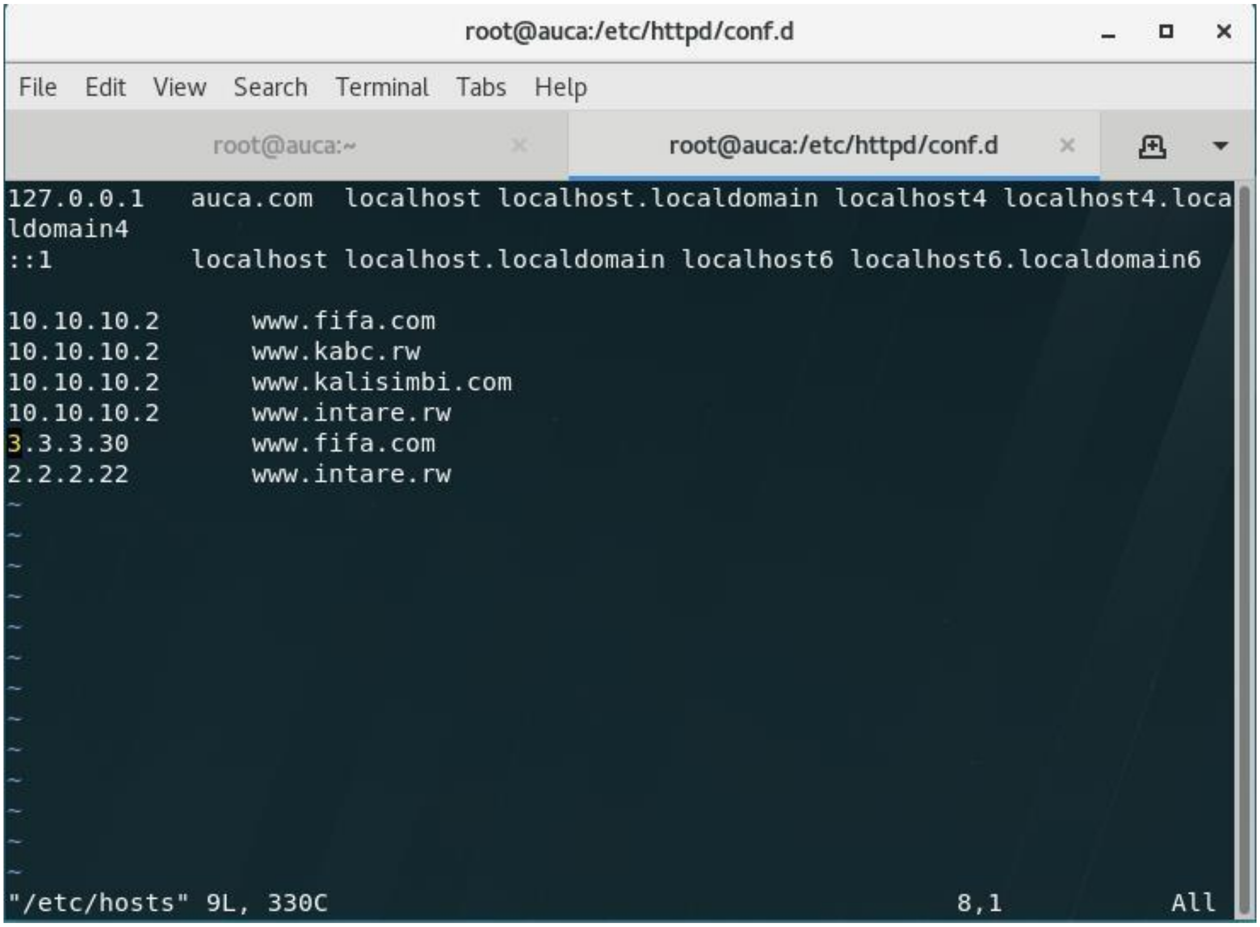
```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80
NameVirtualHost 192.168.10.2:80
NameVirtualHost 10.10.10.2:80
NameVirtualHost 2.2.2.2:80
NameVirtualHost 3.3.3.26:80
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
                                                                  117,1         26%
```

After this we will go to the directory of /etc/httpd/conf.d then we copy a file named welcome.conf to a file of our creation named www.conf then go inside www.conf and edit like this in this case you will see 10.10.10.2 more often cause it must get access to all site



```
<VirtualHost 10.10.10.2:80>
        ServerName      www.fifa.com
        DocumentRoot    /var/www/web1
        <Directory "/var/www/web1">
        order allow,deny
        allow from all
</Directory>
</VirtualHost>

<VirtualHost 10.10.10.2:80>
        ServerName      www.intare.rw
        DocumentRoot    /var/www/web2
        <Directory "/var/www/web2">
        order allow,deny
        allow from all
</Directory>
</VirtualHost>

<VirtualHost 10.10.10.2:80>
        ServerName      www.kalisimbi.com
        DocumentRoot    /var/www/web3
        <Directory "/var/www/web3">
        order allow,deny
        allow from all
</Directory>
</VirtualHost>

<VirtualHost 10.10.10.2:80>
        ServerName      www.kabc.rw
        DocumentRoot    /var/www/web4
        <Directory "/var/www/web4">
                                                                                  2(
```

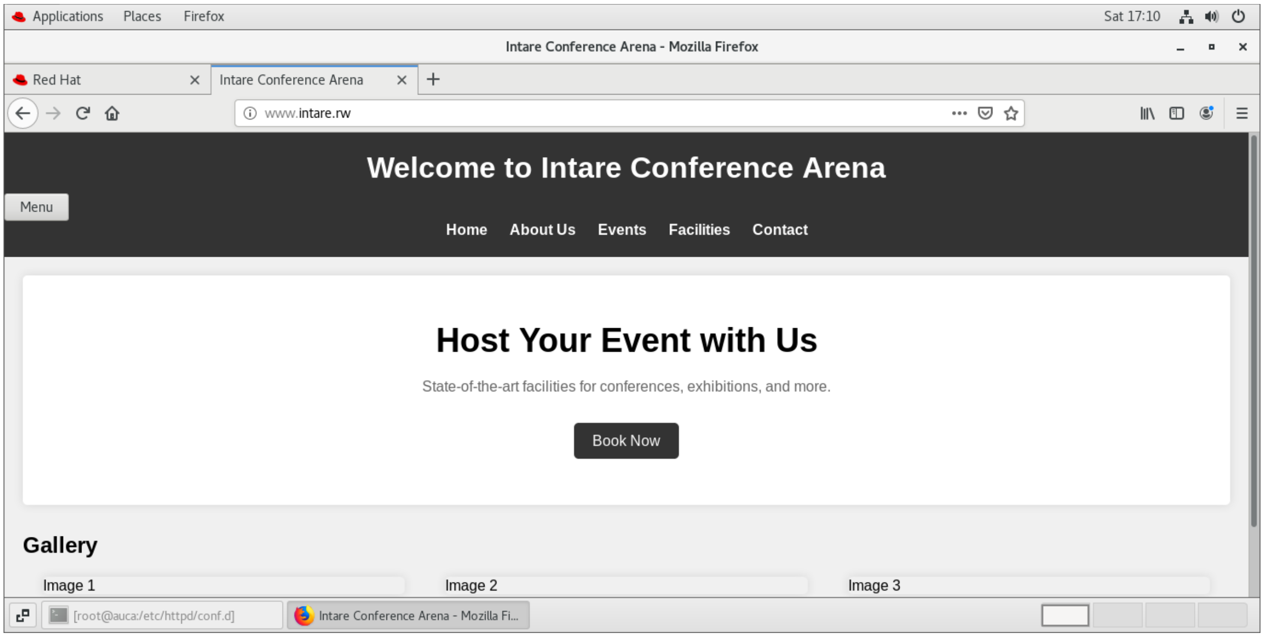
You follow this format and add the other Ip address depending on hostings then you add the site to the forward and reverse as shown before so lets move in the /etc/hosts so lets the edits we make.



root@auca:/etc/httpd/conf.d
File Edit View Search Terminal Tabs Help
root@auca:~
root@auca:/etc/httpd/conf.d

```
127.0.0.1   auca.com  localhost localhost.localdomain localhost4 localhost4.loca
ldomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

10.10.10.2      www.fifa.com
10.10.10.2      www.kabc.rw
10.10.10.2      www.kalisimbi.com
10.10.10.2      www.intare.rw
3.3.3.30        www.fifa.com
2.2.2.22        www.intare.rw
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 9L, 330C                                         8,1           All
```

This allows you not only to access it using an ip address I mean website but also by the name which is the responsibility of the DNS server.


Applications
Places
Firefox
Sat 17:10
Intare Conference Arena - Mozilla Firefox
Red Hat
Intare Conference Arena
www.intare.rw
Welcome to Intare Conference Arena
Menu
Home
About Us
Events
Facilities
Contact
Host Your Event with Us
State-of-the-art facilities for conferences, exhibitions, and more.
Book Now
Gallery
Image 1
Image 2
Image 3
[root@auca:/etc/httpd/conf.d]
Intare Conference Arena - Mozilla Fi...

So after deployment of the website we cloned the server and changed the ip address and all the aspects related in order to configure the cluster of two nodes because I used redhat 7 I consulted the redhat site and the following is the code to configure the cluster

codes

```
yum install pcs pacemaker fence-agents-all.
firewall-cmd --permanent --add-service=high-availability
firewall-cmd --add-service=high-availability
passwd hacluster
systemctl start pcsd.service
systemctl enable pcsd.service
pcs cluster auth z1.example.com z2.example.com (replace with ip address of servers)
```

Creating a cluster

—-----------------------

```
pcs cluster setup --start --name my_cluster \
z1.example.com z2.example.com
pcs cluster enable --all
pcs cluster status
```

Fencing

—-------------------------

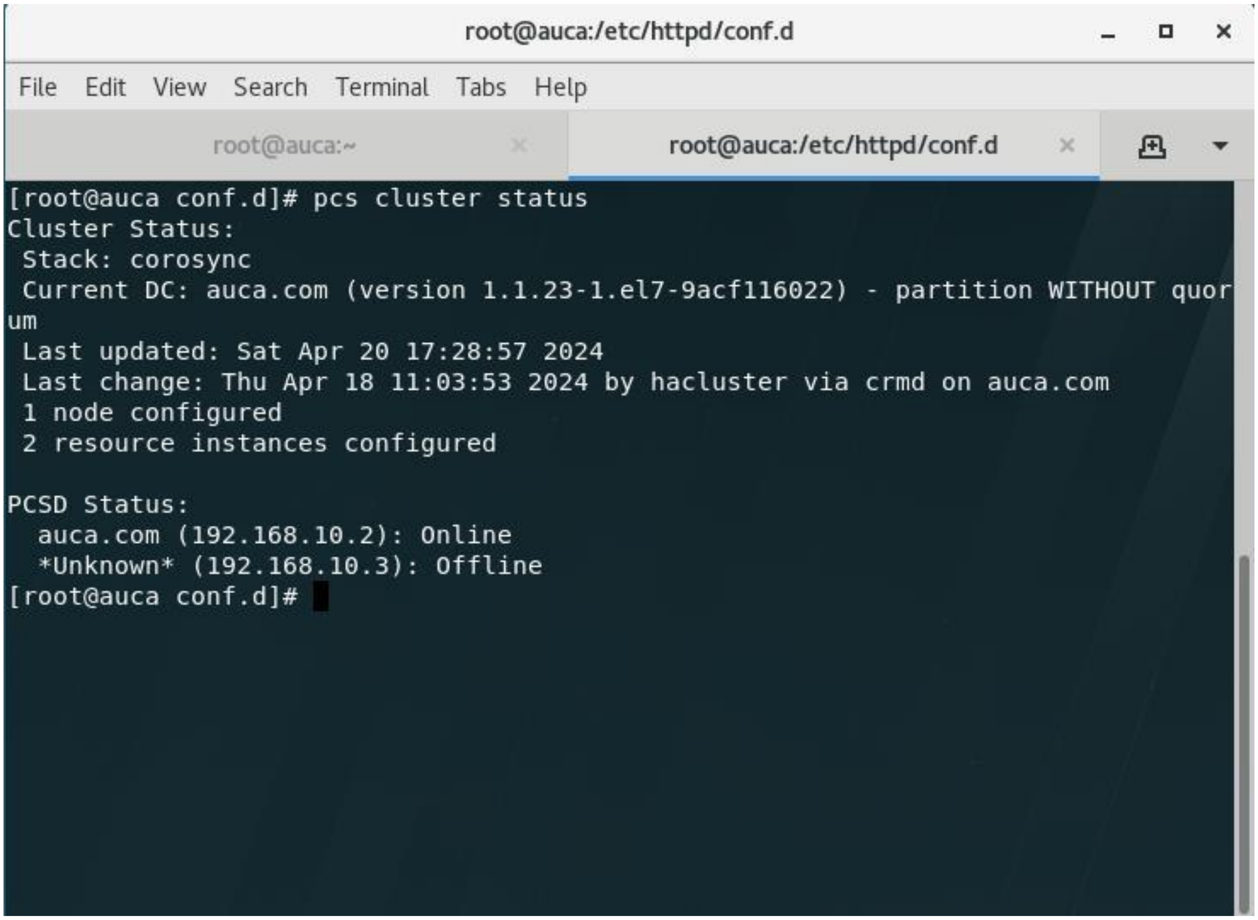
```
pcs stonith create myapc fence_apc_snmp \
ipaddr="zapc.example.com" pcmk_host_map="z1.example.com:1;z2.example.com:2" \
pcmk_host_check="static-list" pcmk_host_list="z1.example.com,z2.example.com" \
login="apc" passwd="apc"
(here we used a fencing agent named stonith)
pcs stonith show myapc
```

We add in httpd resource

—---

```
pcs resource create WebSite ocf:heartbeat:apache  \
      configfile=/etc/httpd/conf/httpd.conf \
      statusurl="http://localhost/server-status"  \

      op monitor interval=1min
```

For attest run since my pc can’t handle 4 pc up all together one server will be online for now and its the master server

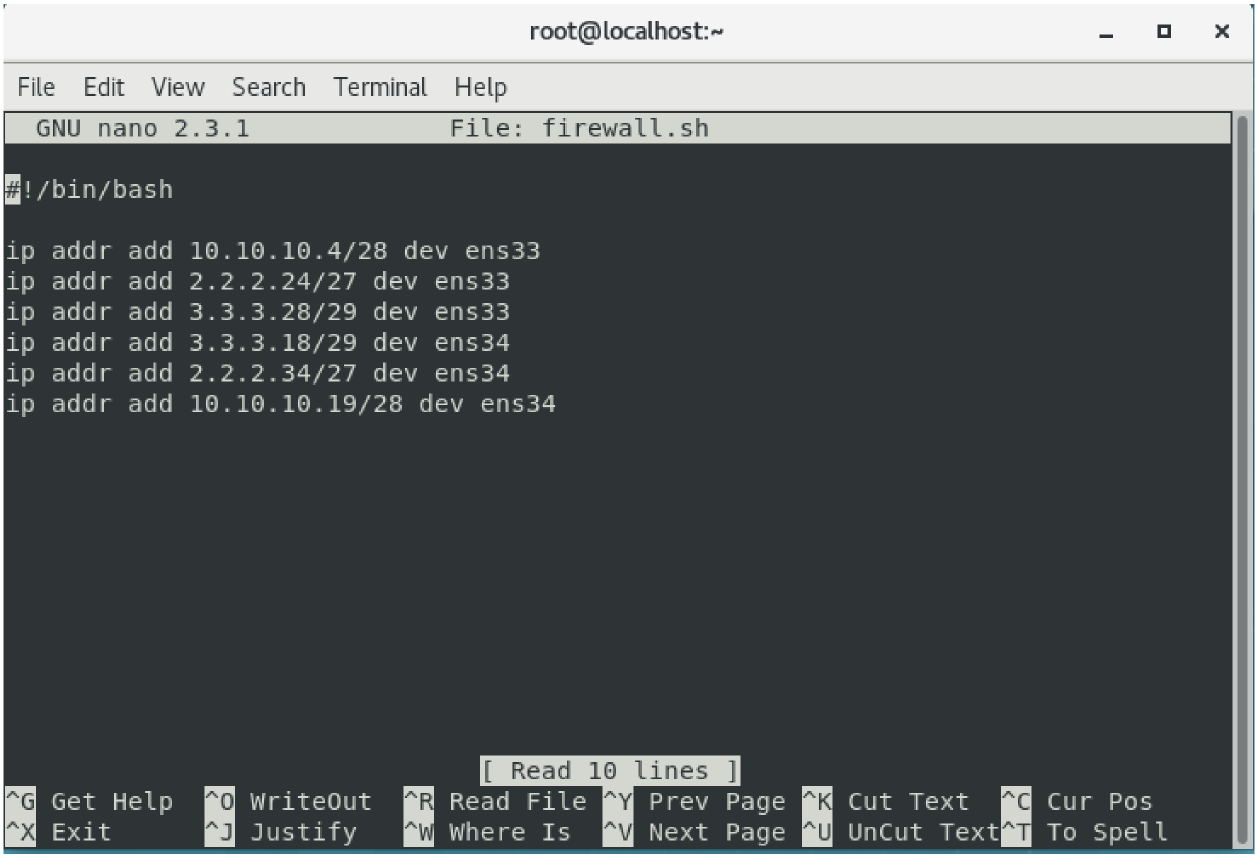

root@auca:/etc/httpd/conf.d
File Edit View Search Terminal Tabs Help
root@auca:~
root@auca:/etc/httpd/conf.d

```
[root@auca conf.d]# pcs cluster status
Cluster Status:
 Stack: corosync
 Current DC: auca.com (version 1.1.23-1.el7-9acf116022) - partition WITHOUT quor
um
 Last updated: Sat Apr 20 17:28:57 2024
 Last change: Thu Apr 18 11:03:53 2024 by hacluster via crmd on auca.com
 1 node configured
 2 resource instances configured

PCSD Status:
  auca.com (192.168.10.2): Online
  *Unknown* (192.168.10.3): Offline
[root@auca conf.d]# 
```

The two resources are webserver and stonith after the verification that cluster works we move to firewall configuration
In redhat7 to start a service you need to type systemctl start named.service and do the same on httpd.
In the fire you need to a script since ip routes disappear at reboot so the scripts are to assign the firewall with ip address to communicate with the machines server and client

Script firewall

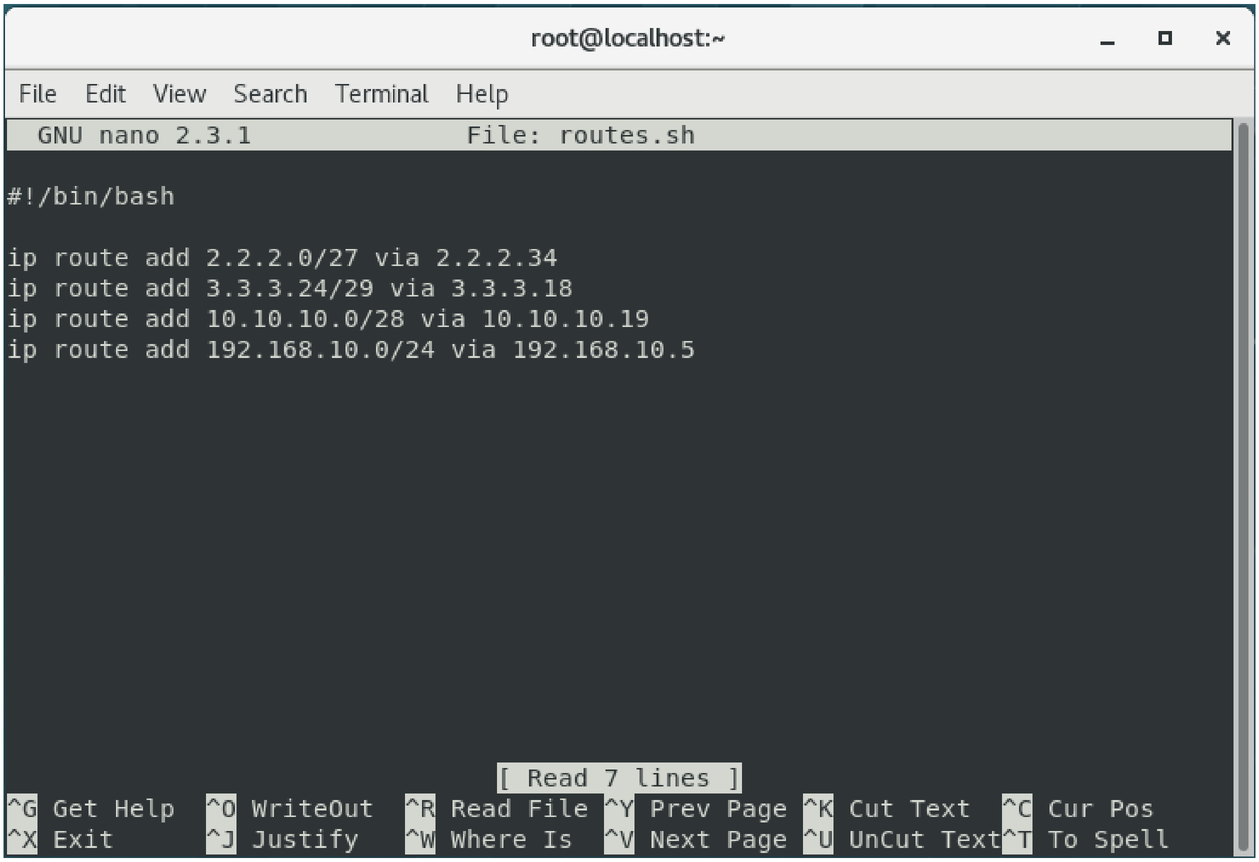
We can also use sub-interface to maintain the loss of information while on reboot



```
  GNU nano 2.3.1             File: firewall.sh

#!/bin/bash

ip addr add 10.10.10.4/28 dev ens33
ip addr add 2.2.2.24/27 dev ens33
ip addr add 3.3.3.28/29 dev ens33
ip addr add 3.3.3.18/29 dev ens34
ip addr add 2.2.2.34/27 dev ens34
ip addr add 10.10.10.19/28 dev ens34

                              [ Read 10 lines ]
^G Get Help   ^O WriteOut   ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Client script to communicate with the server

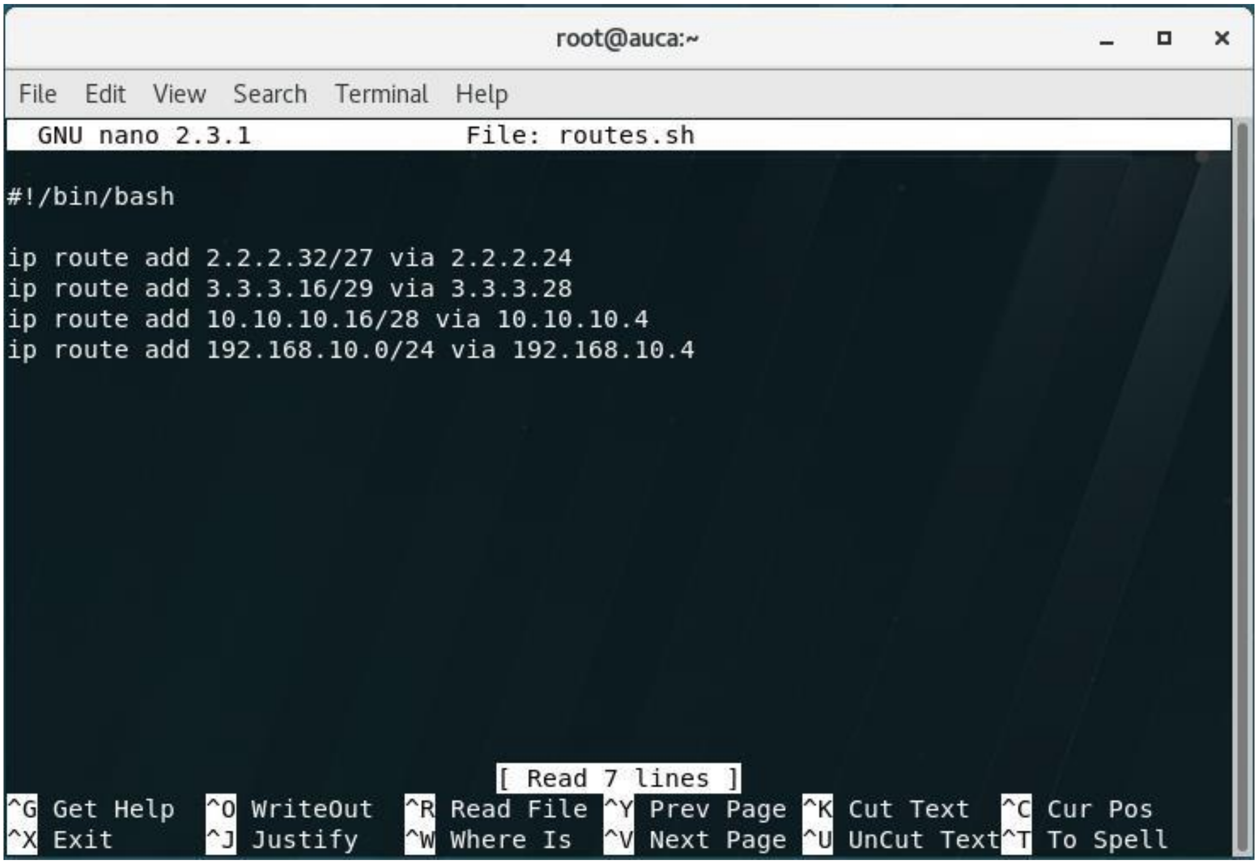
—--



```
  GNU nano 2.3.1             File: routes.sh

#!/bin/bash

ip route add 2.2.2.0/27 via 2.2.2.34
ip route add 3.3.3.24/29 via 3.3.3.18
ip route add 10.10.10.0/28 via 10.10.10.19
ip route add 192.168.10.0/24 via 192.168.10.5

                                [ Read 7 lines ]
```

Server-side script

—---

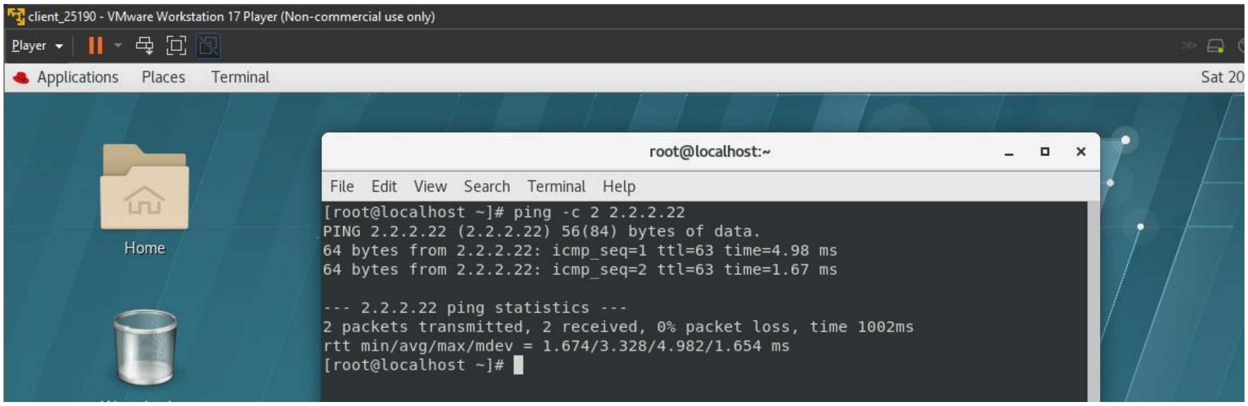

root@auca:~
File Edit View Search Terminal Help
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

```
  GNU nano 2.3.1              File: routes.sh

#!/bin/bash

ip route add 2.2.2.32/27 via 2.2.2.24
ip route add 3.3.3.16/29 via 3.3.3.28
ip route add 10.10.10.16/28 via 10.10.10.4
ip route add 192.168.10.0/24 via 192.168.10.4
```

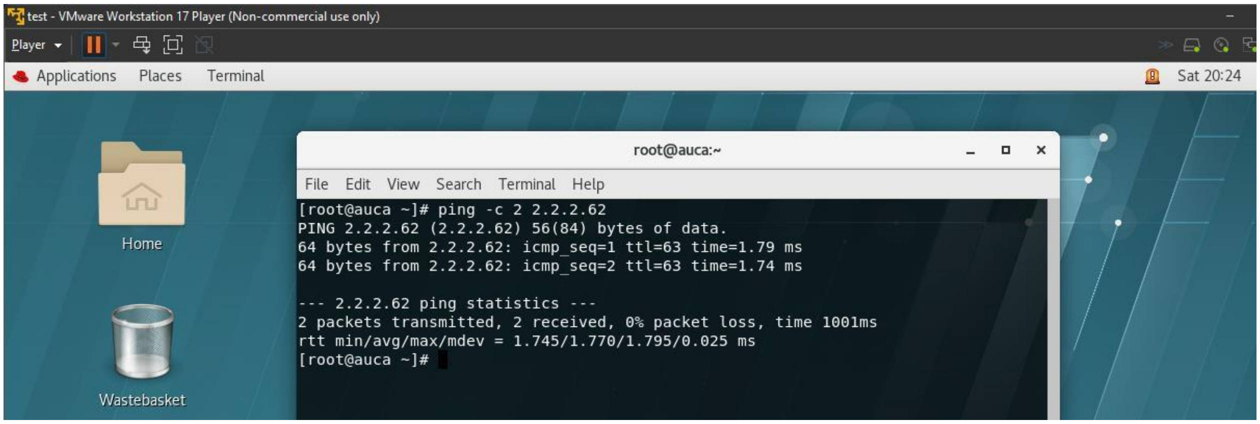
```
                                [ Read 7 lines ]
```

Lets if the client and the server could ping effectively

—---


client_25190 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places Terminal
Sat 20
Home
root@localhost:~
File Edit View Search Terminal Help

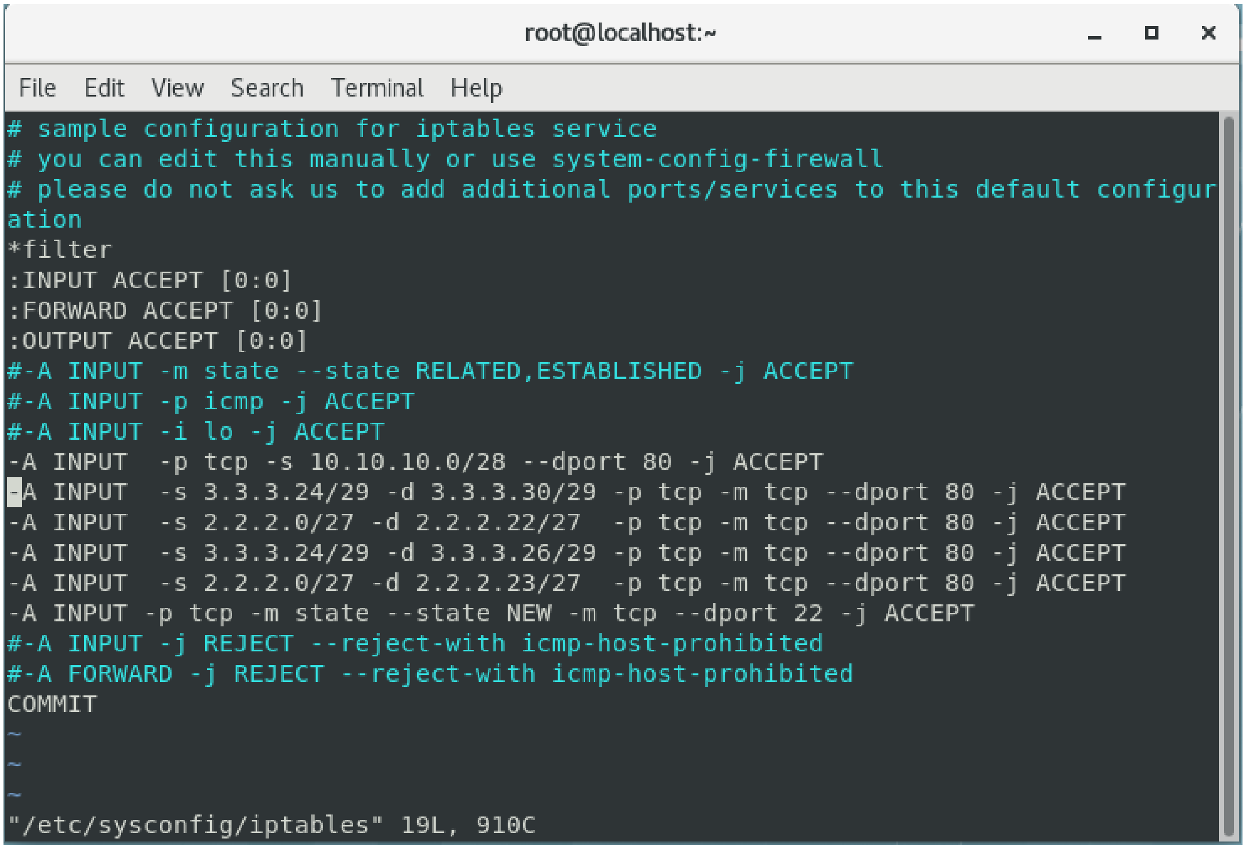
```
[root@localhost ~]# ping -c 2 2.2.2.22
PING 2.2.2.22 (2.2.2.22) 56(84) bytes of data.
64 bytes from 2.2.2.22: icmp_seq=1 ttl=63 time=4.98 ms
64 bytes from 2.2.2.22: icmp_seq=2 ttl=63 time=1.67 ms

--- 2.2.2.22 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.674/3.328/4.982/1.654 ms
[root@localhost ~]#
```



```
[root@auca ~]# ping -c 2 2.2.2.62
PING 2.2.2.62 (2.2.2.62) 56(84) bytes of data.
64 bytes from 2.2.2.62: icmp_seq=1 ttl=63 time=1.79 ms
64 bytes from 2.2.2.62: icmp_seq=2 ttl=63 time=1.74 ms

--- 2.2.2.62 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.745/1.770/1.795/0.025 ms
[root@auca ~]#
```

In order to get iptables in firewall redhat7 you need to install iptables by the command yum install iptables once the repolist have been installed

Then enter in vim /etc/sysconfig/iptables and edit the restrictions in order to edit iptables and restrictions to take effect you need to disable the firewall and stop it else the client will not be able to ping the server take a note that the iptables is different from firewall.



```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# please do not ask us to add additional ports/services to this default configur
ation
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
#-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
#-A INPUT -p icmp -j ACCEPT
#-A INPUT -i lo -j ACCEPT
-A INPUT  -p tcp -s 10.10.10.0/28 --dport 80 -j ACCEPT
-A INPUT  -s 3.3.3.24/29 -d 3.3.3.30/29 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT  -s 2.2.2.0/27 -d 2.2.2.22/27  -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT  -s 3.3.3.24/29 -d 3.3.3.26/29 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT  -s 2.2.2.0/27 -d 2.2.2.23/27  -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
#-A INPUT -j REJECT --reject-with icmp-host-prohibited
#-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
~
~
"/etc/sysconfig/iptables" 19L, 910C
```

After we have the configuration of iptables lets talk a little about tcp wrappers it has to files one called allow.conf another named deny.conf the ip address in allow.conf can access specific service another in deny can’t example of how its lets say in case of ssh Sshd: 192.168.10.2 if this was in allow file that means the ip address can use ssh else not in both files the order is the same.
But you can’t use tcp wrapper in restrictions.

Script to set ip and sub interface what you should know is that redhat has enss3 instead of eth0 so if you want GUI configuration pane type nmtiu
Then if not you can move to vim /etc/sysconfig/network-scripts
Then:

Vim ifcfg-ens33
:wq [to save]
cp ifcfg-ens33 ifcfg-ens:33:1 then what is in ifcfg-ens33 is copied to ens33:1
then use vim to edit.
After we check if our client can access website.

Done on 22/01/2024