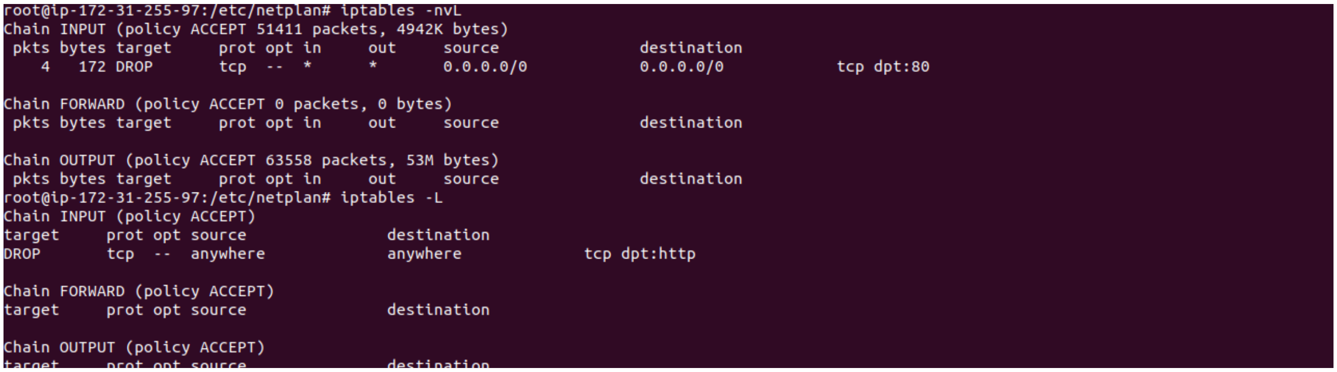
Task 1(install Apache and fix a broken EC2)

During the process of installing the needed dependencies for Apache server, The following issues has been discovered and corrected:

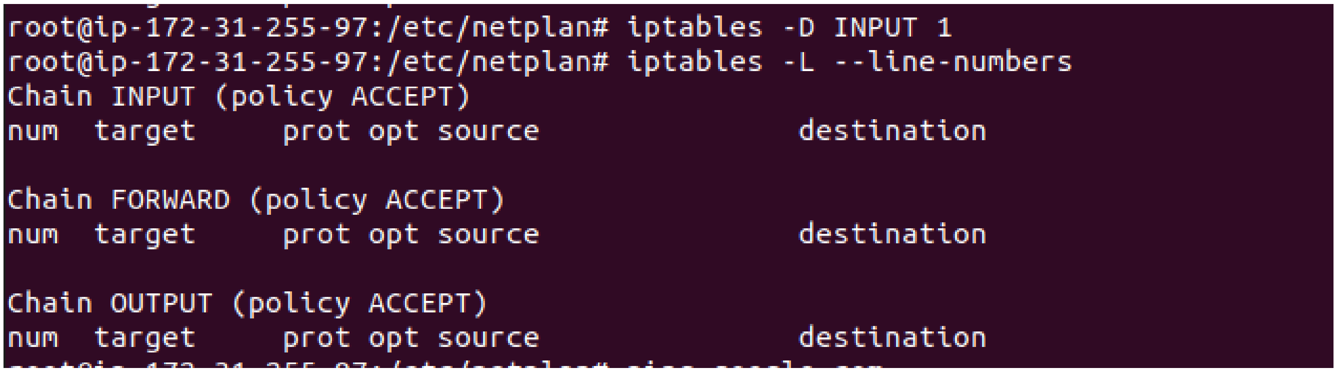
1. Iptables wrong configurations
2. Unable to solve the hostname due DNS mis-configurations
3. Full disk
4. Cannot resolve local hosts name issues
5. Unable to successfully start Apache2 due a an existing process listening to port 80

Iptables



```
root@ip-172-31-255-97:/etc/netplan# iptables -nvL
Chain INPUT (policy ACCEPT 51411 packets, 4942K bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   172 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 63558 packets, 53M bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ip-172-31-255-97:/etc/netplan# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

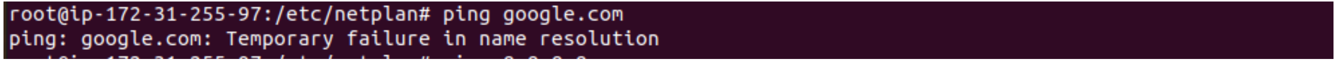
Now after I removed it



```
root@ip-172-31-255-97:/etc/netplan# iptables -D INPUT 1
root@ip-172-31-255-97:/etc/netplan# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

DNS mis-configurations

I tried to ping google.com



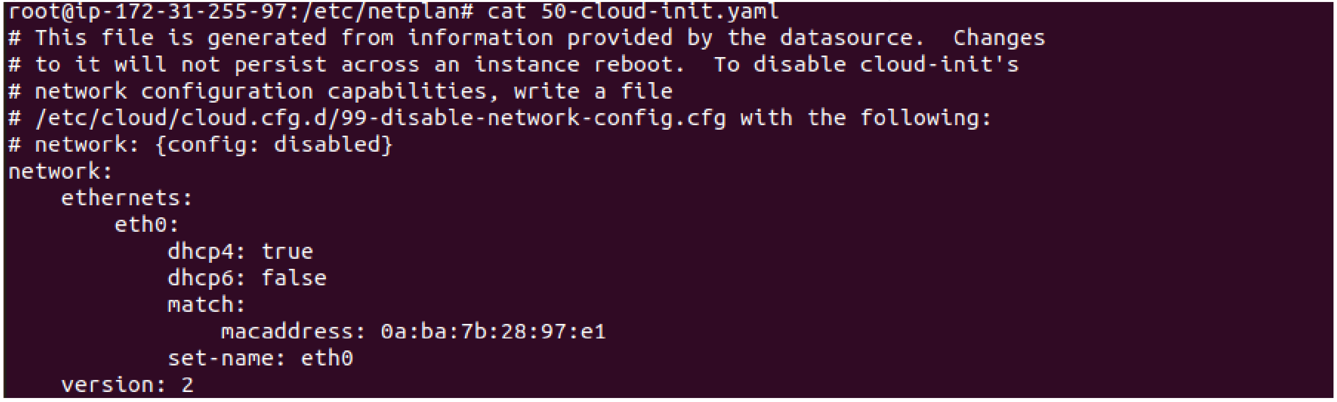
```
root@ip-172-31-255-97:/etc/netplan# ping google.com
ping: google.com: Temporary failure in name resolution
```

I decided to first check resolve.conf as start

```
root@ip-172-31-255-97:~# cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
```

```
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0
search ec2.internal
```

which is as follow with dhcp enables I decided to change that to have static ip/dns (instead of setting one for the scope of this exersize)



```
root@ip-172-31-255-97:/etc/netplan# cat 50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        eth0:
            dhcp4: true
            dhcp6: false
            match:
                macaddress: 0a:ba:7b:28:97:e1
            set-name: eth0
    version: 2
```

Note: while editing the file I found out I cannot save the file saying : "50-cloud-init.yaml" E514: write error (file system full?)
which I addressed below to complete this

Now that issue has been addressed I proceeded ahead

I ran that command to get my gateway and edit the file

```
root@ip-172-31-255-97:/etc/netplan# ip route
default via 172.31.255.1 dev eth0 proto dhcp src 172.31.255.97 metric 100
172.31.255.0/24 dev eth0 proto kernel scope link src 172.31.255.97
172.31.255.1 dev eth0 proto dhcp scope link src 172.31.255.97 metric 100
```

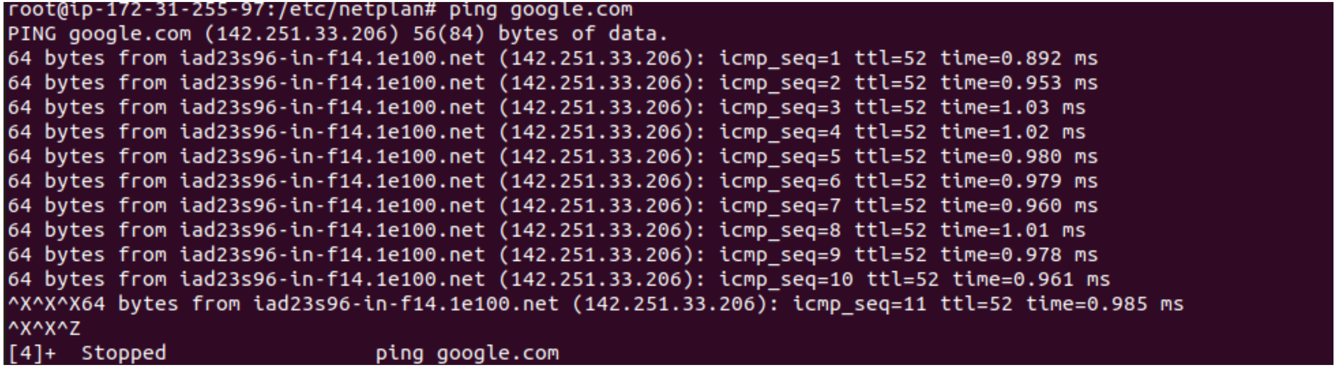
I created new file: **vi /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg and added network: {config: disabled}** to it so does not get overwritten

the new file is with dhcp4 disabled and matching address and gateway

```
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        eth0:
            dhcp4: false
            dhcp6: false
            match:
                macaddress: 0a:ba:7b:28:97:e1
            addresses: [172.31.255.97/24]
            gateway4: 172.31.255.1
            nameservers:
                addresses: [1.1.1.1,8.8.8.8]
            set-name: eth0
    version: 2
```

then ran **netplan apply**

below see I can ping google.com



```
root@ip-172-31-255-97:/etc/netplan# ping google.com
PING google.com (142.251.33.206) 56(84) bytes of data.
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=1 ttl=52 time=0.892 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=2 ttl=52 time=0.953 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=3 ttl=52 time=1.03 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=4 ttl=52 time=1.02 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=5 ttl=52 time=0.980 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=6 ttl=52 time=0.979 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=7 ttl=52 time=0.960 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=8 ttl=52 time=1.01 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=9 ttl=52 time=0.978 ms
64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=10 ttl=52 time=0.961 ms
^X^X^X64 bytes from iad23s96-in-f14.1e100.net (142.251.33.206): icmp_seq=11 ttl=52 time=0.985 ms
^X^X^Z
[4]+  Stopped                 ping google.com
```

E514: write error (file system full?)

I first ran this command and noticed /dev/xvda1 is full

```
root@ip-172-31-255-97:/etc/netplan# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            224M     0  224M   0% /dev
tmpfs            48M  5.6M   43M  12% /run
/dev/xvda1      7.7G  7.7G     0 100% /
tmpfs           238M     0  238M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           238M     0  238M   0% /sys/fs/cgroup
/dev/loop0       98M   98M     0 100% /snap/core/9993
/dev/loop1       29M   29M     0 100% /snap/amazon-ssm-agent/2012
tmpfs            48M     0   48M   0% /run/user/0
```

then I ran **du -h -d 1**

```
431M ./snap
15M ./sbin
32K ./tmp
```

```
4.0K ./srv
0 ./sys
40M ./boot
4.0K ./opt
16K ./lost+found
111M ./lib
du: cannot access './proc/22332/task/22332/fd/4': No such file or directory
du: cannot access './proc/22332/task/22332/fdinfo/4': No such file or directory
du: cannot access './proc/22332/fd/3': No such file or directory
du: cannot access './proc/22332/fdinfo/3': No such file or directory
0 ./proc
15M ./bin
730M ./usr
4.0K ./mnt
4.0K ./media
4.0K ./lib64
5.5M ./etc
28K ./root
28K ./home
204M ./var
0 ./dev
5.6M ./run
1.6G .
```

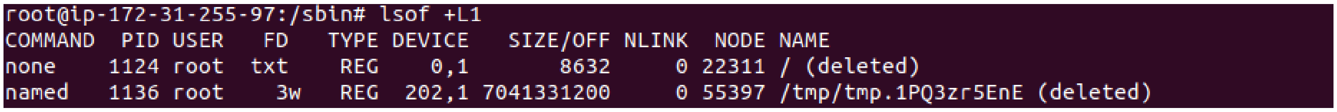
then I ran **fsck** to see if all mounted which seems like it is

```
root@ip-172-31-255-97:/# fsck /dev/xvda1
fsck from util-linux 2.31.1
e2fsck 1.44.1 (24-Mar-2018)
/dev/xvda1 is mounted.
e2fsck: Cannot continue, aborting.
```

I tried df -i to see if I reached nodes num max which was not the case

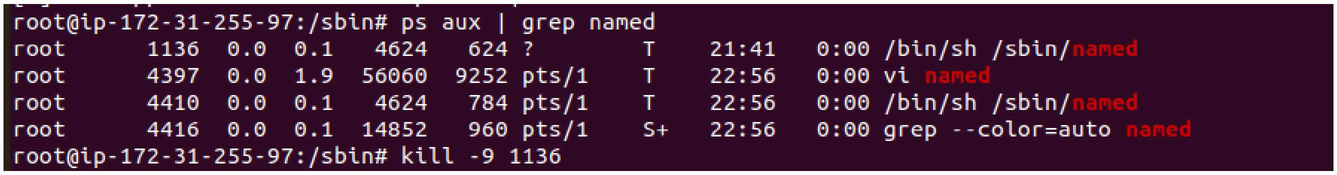
```
 root@ip-172-31-255-97:/# df -i
Filesystem      Inodes IUsed  IFree IUse% Mounted on
udev             57256   314  56942    1% /dev
tmpfs            60847   465  60382    1% /run
/dev/xvda1     1024000 64656 959344    7% /
tmpfs            60847     1  60846    1% /dev/shm
tmpfs            60847     3  60844    1% /run/lock
tmpfs            60847    18  60829    1% /sys/fs/cgroup
/dev/loop0          15    15      0  100% /snap/amazon-ssm-agent/2012
/dev/loop1       12804 12804      0  100% /snap/core/9993
tmpfs            60847    11  60836    1% /run/user/0
```

so it does not add up (my hunch said maybe a deleted file or some hidden file (since numbers do not add up) so I ran) lsof command (you can see named process

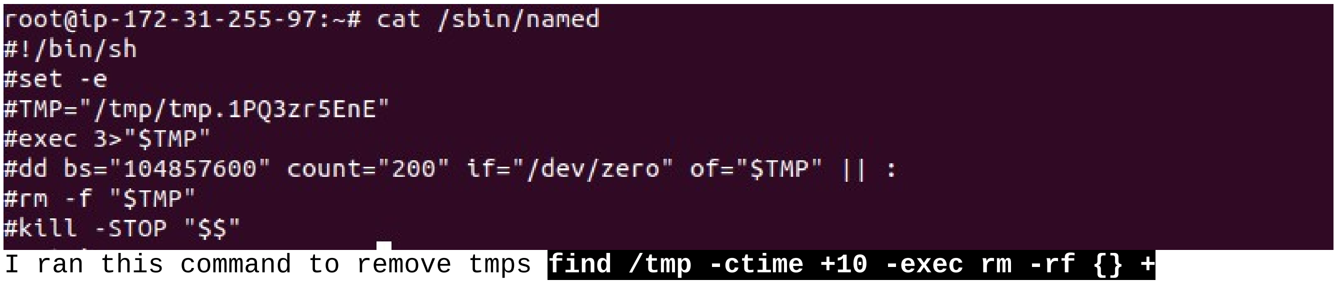


```
root@ip-172-31-255-97:/sbin# lsof +L1
COMMAND   PID USER   FD   TYPE DEVICE   SIZE/OFF NLINK  NODE NAME
none     1124 root  txt    REG    0,1       8632     0 22311 / (deleted)
named    1136 root   3w    REG  202,1 7041331200     0 55397 /tmp/tmp.1PQ3zr5EnE (deleted)
```

now I wanted to check that process named which you can see
I also commented the code which is the reason we have that issue ; named is creating a huge file then deleting it but keeping it open



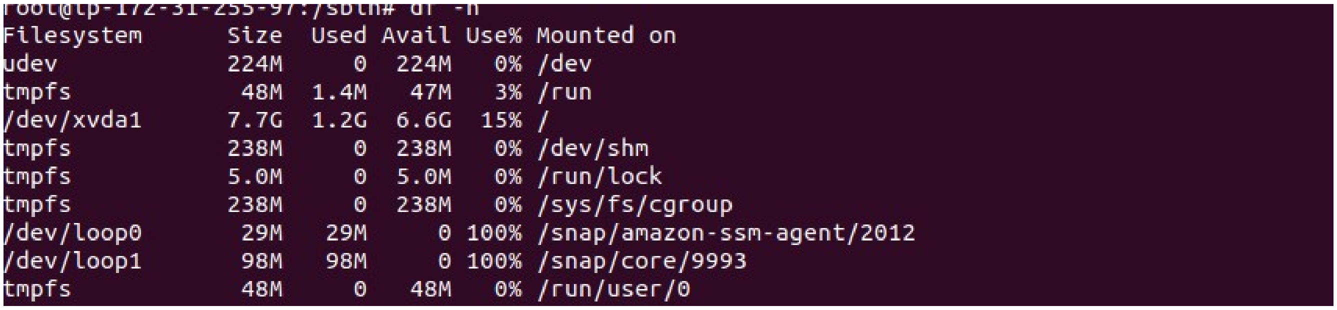
```
root@ip-172-31-255-97:/sbin# ps aux | grep named
root      1136  0.0  0.1   4624   624 ?        T    21:41   0:00 /bin/sh /sbin/named
root      4397  0.0  1.9  56060  9252 pts/1    T    22:56   0:00 vi named
root      4410  0.0  0.1   4624   784 pts/1    T    22:56   0:00 /bin/sh /sbin/named
root      4416  0.0  0.1  14852   960 pts/1    S+   22:56   0:00 grep --color=auto named
root@ip-172-31-255-97:/sbin# kill -9 1136
```



```
root@ip-172-31-255-97:~# cat /sbin/named
#!/bin/sh
#set -e
#TMP="/tmp/tmp.1PQ3zr5EnE"
#exec 3>"$TMP"
#dd bs="104857600" count="200" if="/dev/zero" of="$TMP" || :
#rm -f "$TMP"
#kill -STOP "$$"
```

I ran this command to remove tmps `find /tmp -ctime +10 -exec rm -rf {} +`

below you see we have space in disk :)



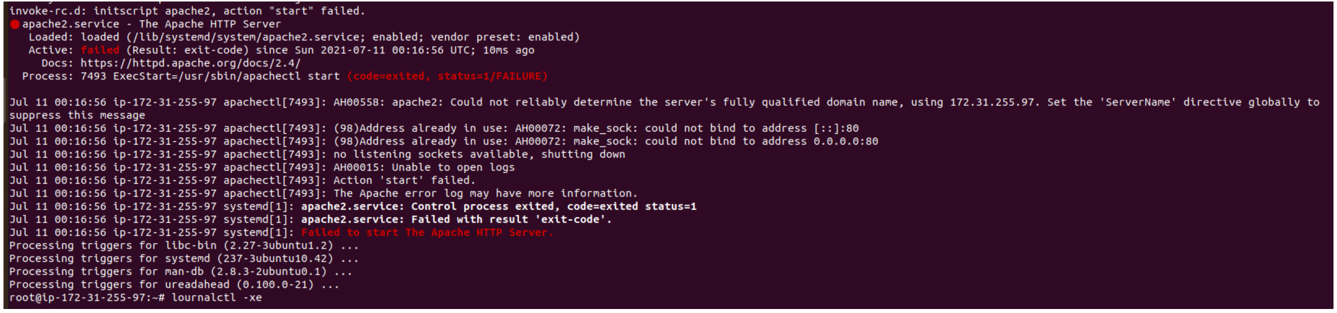
```
root@ip-172-31-255-97:/sbin# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            224M     0  224M   0% /dev
tmpfs            48M  1.4M   47M   3% /run
/dev/xvda1      7.7G  1.2G  6.6G  15% /
tmpfs           238M     0  238M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           238M     0  238M   0% /sys/fs/cgroup
/dev/loop0       29M   29M     0 100% /snap/amazon-ssm-agent/2012
/dev/loop1       98M   98M     0 100% /snap/core/9993
tmpfs            48M     0   48M   0% /run/user/0
```

Cannot resolve local hosts name issues

I decided add entry to /etc/hosts using this command after that issues been solved
`echo $(hostname -I | cut -d\  -f1) $(hostname) | sudo tee -a /etc/hosts`

Now issues while installing apache2 on the ec2

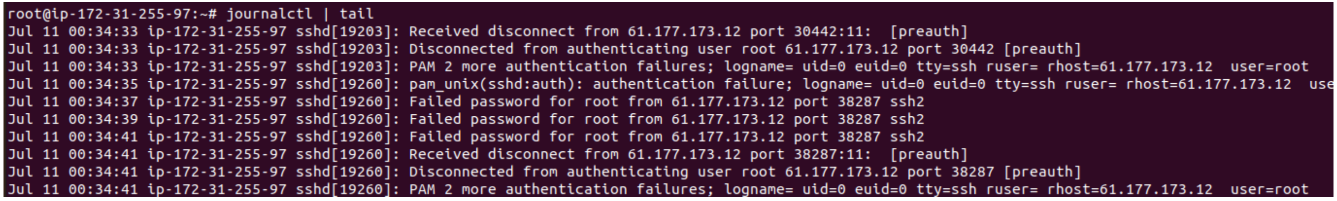
when I tried to install apache 2 I got this error



```
invoke-rc.d: initscript apache2, action "start" failed.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Sun 2021-07-11 00:16:56 UTC; 10ms ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 7493 ExecStart=/usr/sbin/apachectl start (code=exited, status=1/FAILURE)

Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.31.255.97. Set the 'ServerName' directive globally to
suppress this message
Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: (98)Address already in use: AH00072: make_sock: could not bind to address [::]:80
Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: (98)Address already in use: AH00072: make_sock: could not bind to address 0.0.0.0:80
Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: no listening sockets available, shutting down
Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: AH00015: Unable to open logs
Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: Action 'start' failed.
Jul 11 00:16:56 ip-172-31-255-97 apachectl[7493]: The Apache error log may have more information.
Jul 11 00:16:56 ip-172-31-255-97 systemd[1]: apache2.service: Control process exited, code=exited status=1
Jul 11 00:16:56 ip-172-31-255-97 systemd[1]: apache2.service: Failed with result 'exit-code'.
Jul 11 00:16:56 ip-172-31-255-97 systemd[1]: Failed to start The Apache HTTP Server.
Processing triggers for libc-bin (2.27-3ubuntu1.2) ...
Processing triggers for systemd (237-3ubuntu10.42) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
root@ip-172-31-255-97:~# lournalctl -xe
```

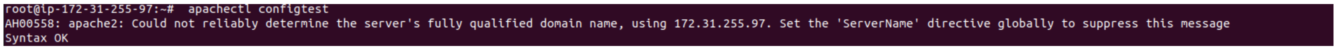
```
AH00558: apache2: Could not reliably determine the server's fully qualified domain
name, using 172.31.255.97. Set the 'ServerName' directive globally to
suppress this message
```

then I ran
journalctl -u apache2.service --since today –no-pager



```
root@ip-172-31-255-97:~# journalctl | tail
Jul 11 00:34:33 ip-172-31-255-97 sshd[19203]: Received disconnect from 61.177.173.12 port 30442:11:  [preauth]
Jul 11 00:34:33 ip-172-31-255-97 sshd[19203]: Disconnected from authenticating user root 61.177.173.12 port 30442 [preauth]
Jul 11 00:34:33 ip-172-31-255-97 sshd[19203]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.12  user=root
Jul 11 00:34:35 ip-172-31-255-97 sshd[19260]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.12  use
Jul 11 00:34:37 ip-172-31-255-97 sshd[19260]: Failed password for root from 61.177.173.12 port 38287 ssh2
Jul 11 00:34:39 ip-172-31-255-97 sshd[19260]: Failed password for root from 61.177.173.12 port 38287 ssh2
Jul 11 00:34:41 ip-172-31-255-97 sshd[19260]: Failed password for root from 61.177.173.12 port 38287 ssh2
Jul 11 00:34:41 ip-172-31-255-97 sshd[19260]: Received disconnect from 61.177.173.12 port 38287:11:  [preauth]
Jul 11 00:34:41 ip-172-31-255-97 sshd[19260]: Disconnected from authenticating user root 61.177.173.12 port 38287 [preauth]
Jul 11 00:34:41 ip-172-31-255-97 sshd[19260]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.12  user=root
```

apachectl configtest

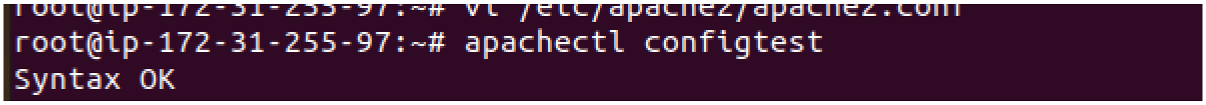


```
root@ip-172-31-255-97:~#  apachectl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.31.255.97. Set the 'ServerName' directive globally to suppress this message
Syntax OK
```

syntax ok but I need to set globalname directive to take rid of that I did following below

vi /etc/apache2/apache2.conf and added **ServerName 127.0.0.1**

below result after fix

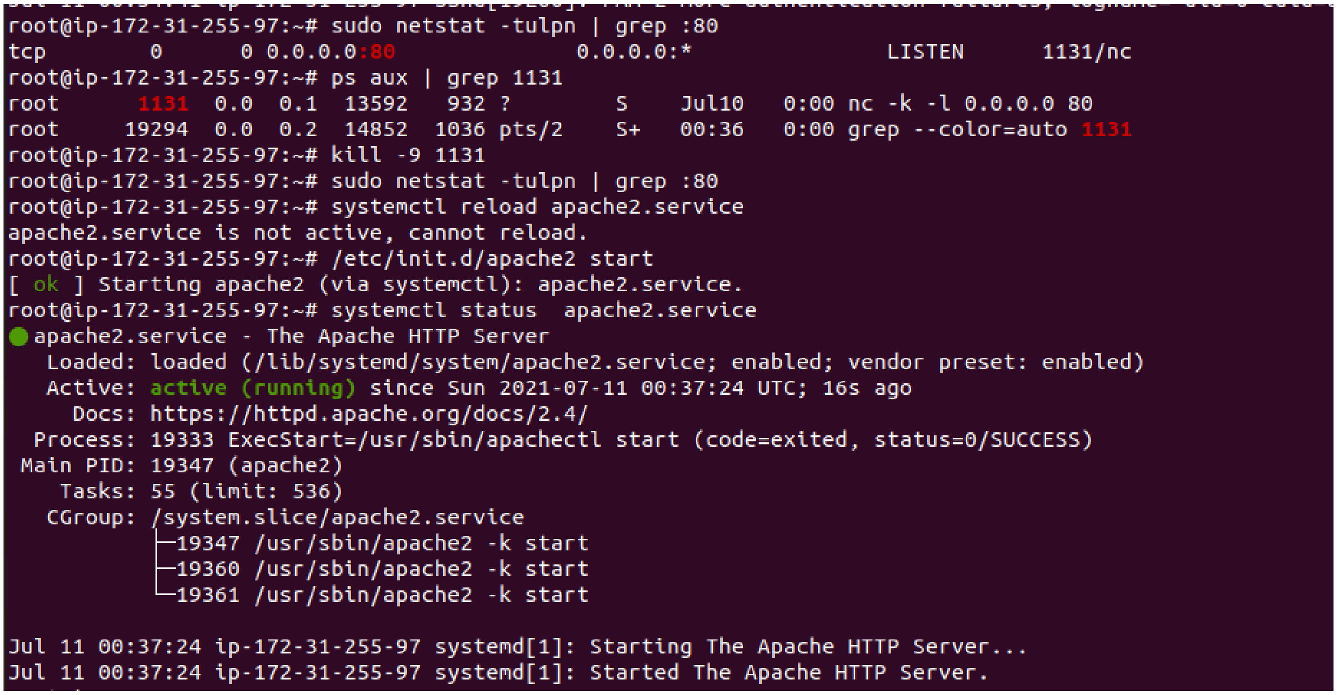


```
root@ip-172-31-255-97:~# vi /etc/apache2/apache2.conf
root@ip-172-31-255-97:~# apachectl configtest
Syntax OK
```

Unable to successfully start Apache2

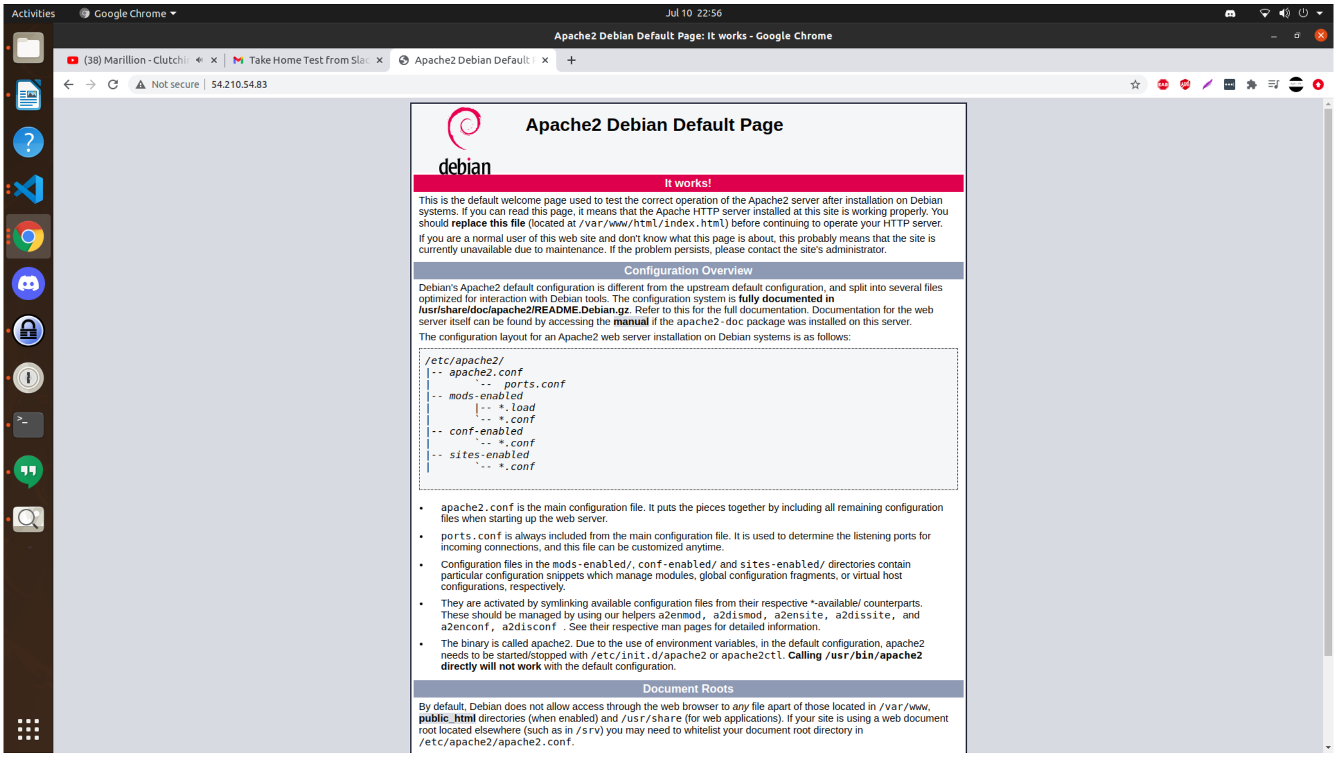
now for apache2 service non starting I decided to check if some other process listening to port 80

I had to kill process 1131 and checked what start it and start service and all good



```
root@ip-172-31-255-97:~# sudo netstat -tulpn | grep :80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1131/nc
root@ip-172-31-255-97:~# ps aux | grep 1131
root      1131  0.0  0.1  13592   932 ?        S    Jul10   0:00 nc -k -l 0.0.0.0 80
root     19294  0.0  0.2  14852  1036 pts/2    S+   00:36   0:00 grep --color=auto 1131
root@ip-172-31-255-97:~# kill -9 1131
root@ip-172-31-255-97:~# sudo netstat -tulpn | grep :80
root@ip-172-31-255-97:~# systemctl reload apache2.service
apache2.service is not active, cannot reload.
root@ip-172-31-255-97:~# /etc/init.d/apache2 start
[ ok ] Starting apache2 (via systemctl): apache2.service.
root@ip-172-31-255-97:~# systemctl status  apache2.service
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-07-11 00:37:24 UTC; 16s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 19333 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 19347 (apache2)
    Tasks: 55 (limit: 536)
   CGroup: /system.slice/apache2.service
           ├─19347 /usr/sbin/apache2 -k start
           ├─19360 /usr/sbin/apache2 -k start
           └─19361 /usr/sbin/apache2 -k start

Jul 11 00:37:24 ip-172-31-255-97 systemd[1]: Starting The Apache HTTP Server...
Jul 11 00:37:24 ip-172-31-255-97 systemd[1]: Started The Apache HTTP Server.
```

now I can access apache below screenshot of my browser you can notice vm ip in browser :)



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod, a2dismod, a2ensite, a2dissite,` and `a2enconf, a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Debian does not allow access through the web browser to *any* file apart of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.