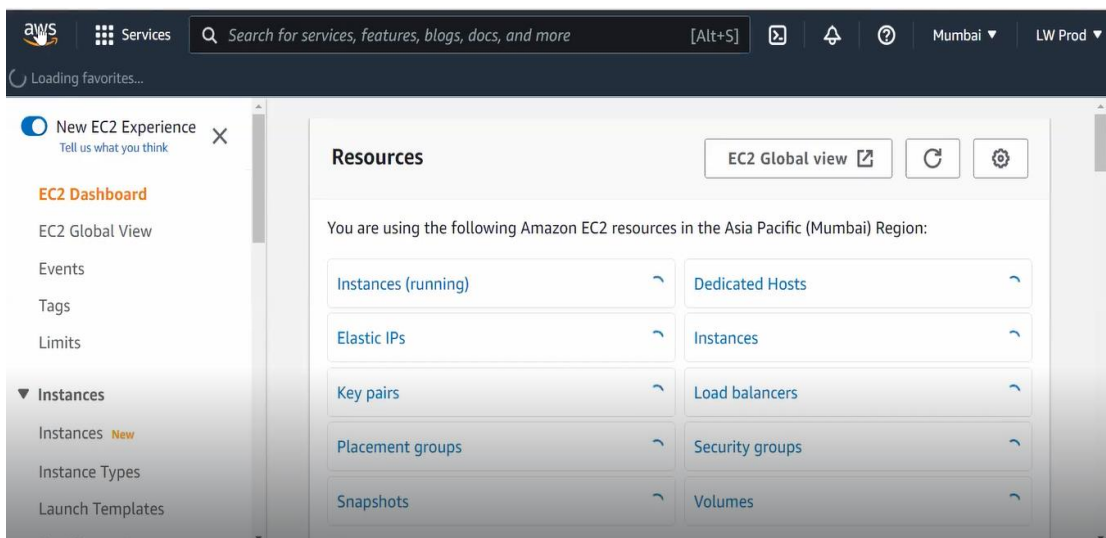


RHEL9

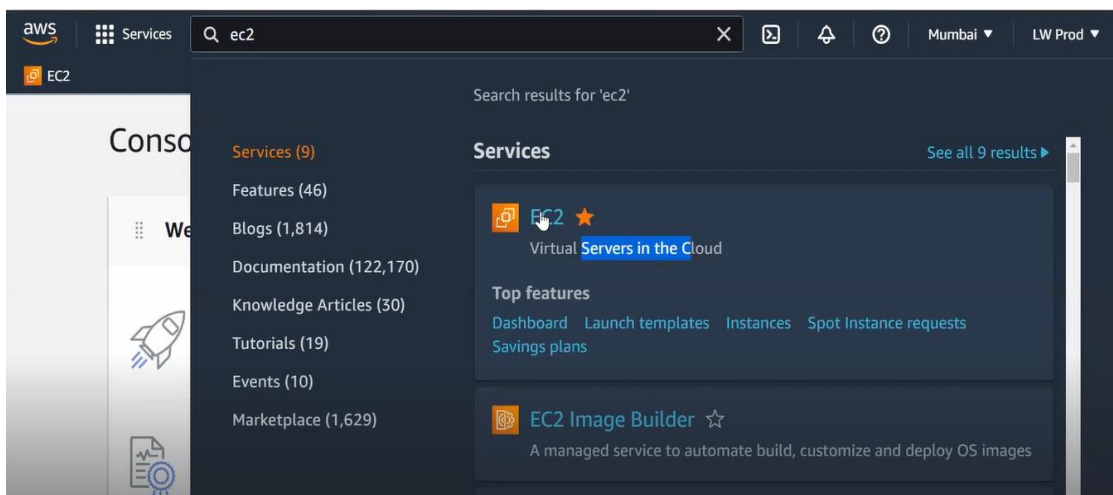


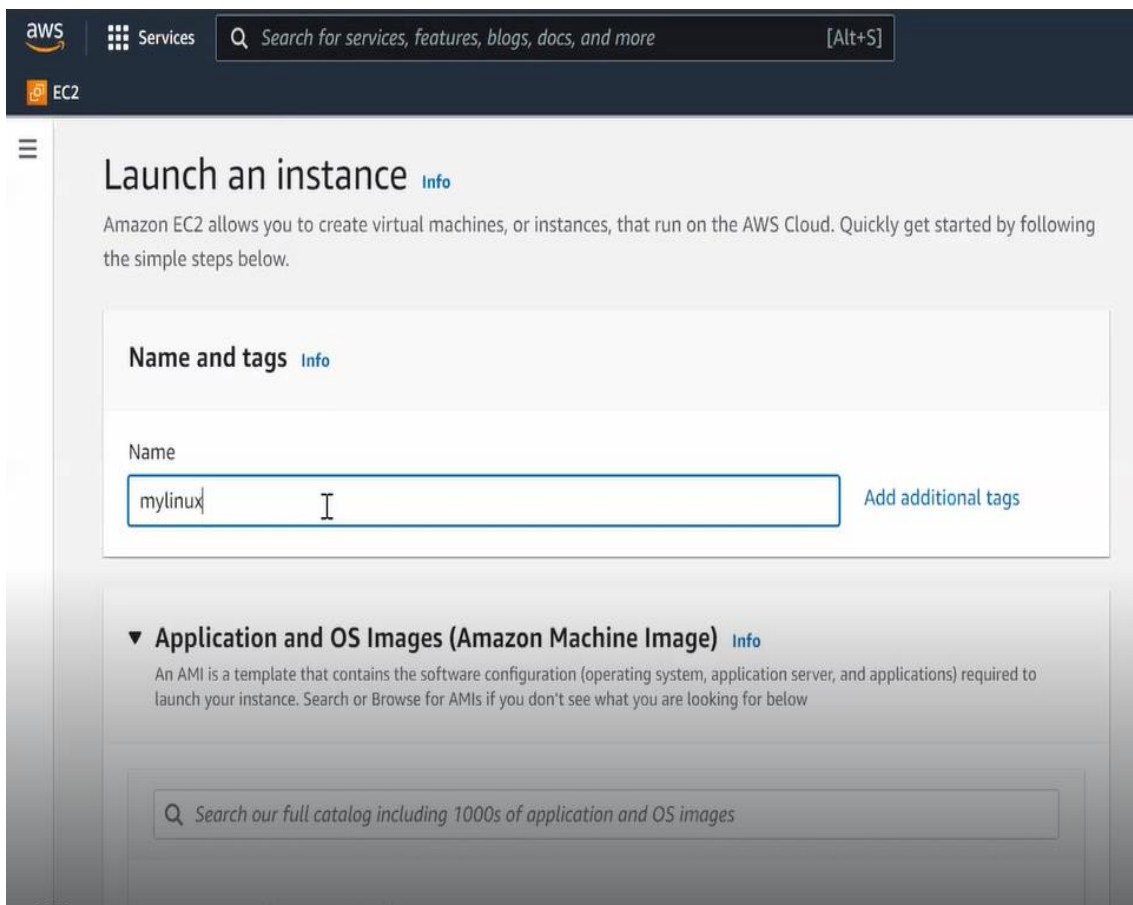
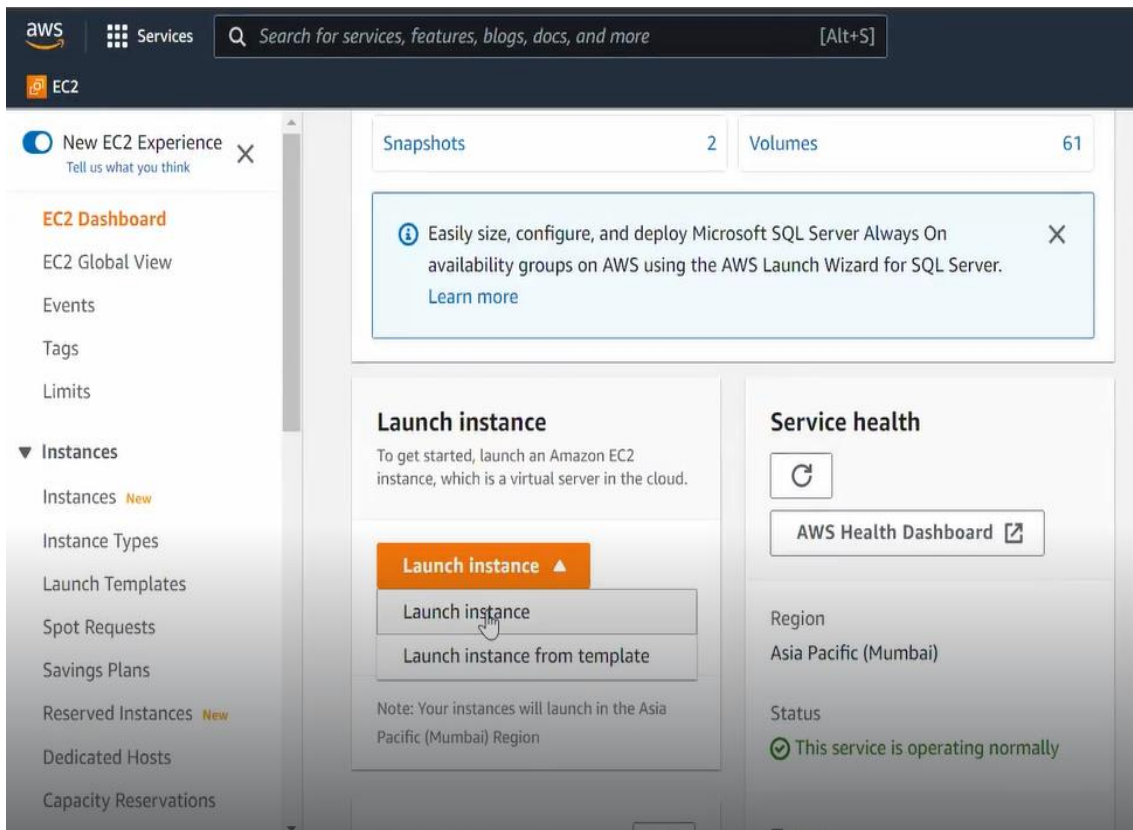
Session 3 – 16th October 2022 Summary

- After Login to AWS Account -

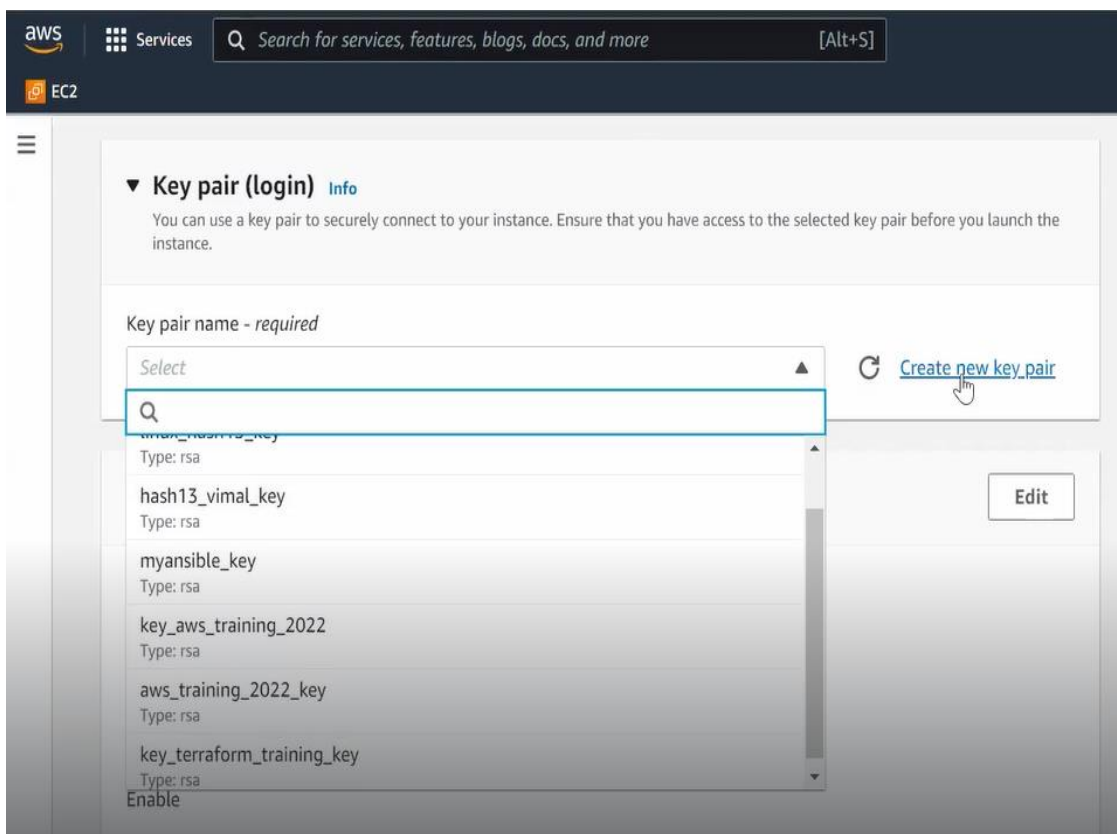
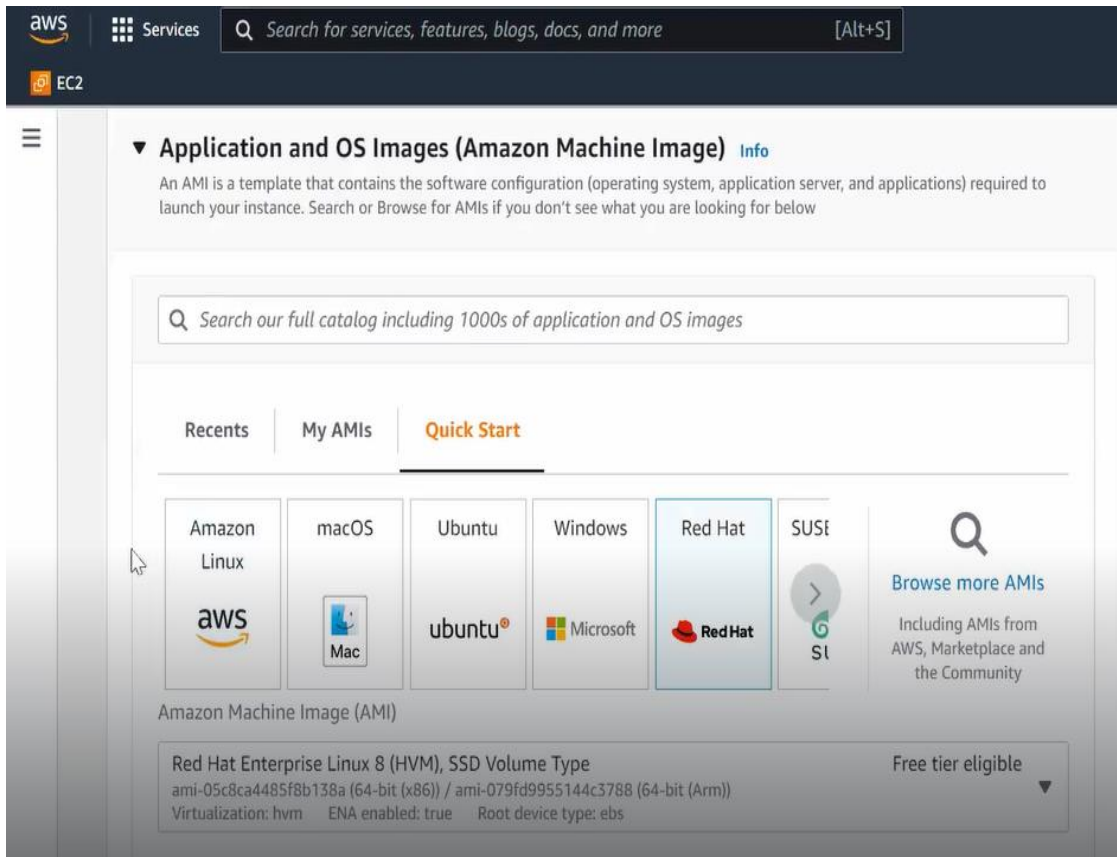


- Search for ec2 service—





➤ Select the RedHat Image



aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

EC2

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called 'launch-wizard-79' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☐ Allow HTTPs traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

EC2

▼ Summary

Number of instances Info

1

Software Image (AMI)

Provided by Red Hat, Inc.

ami-05c8ca4485f8b138a

Virtual server type (instance type)

t2.micro

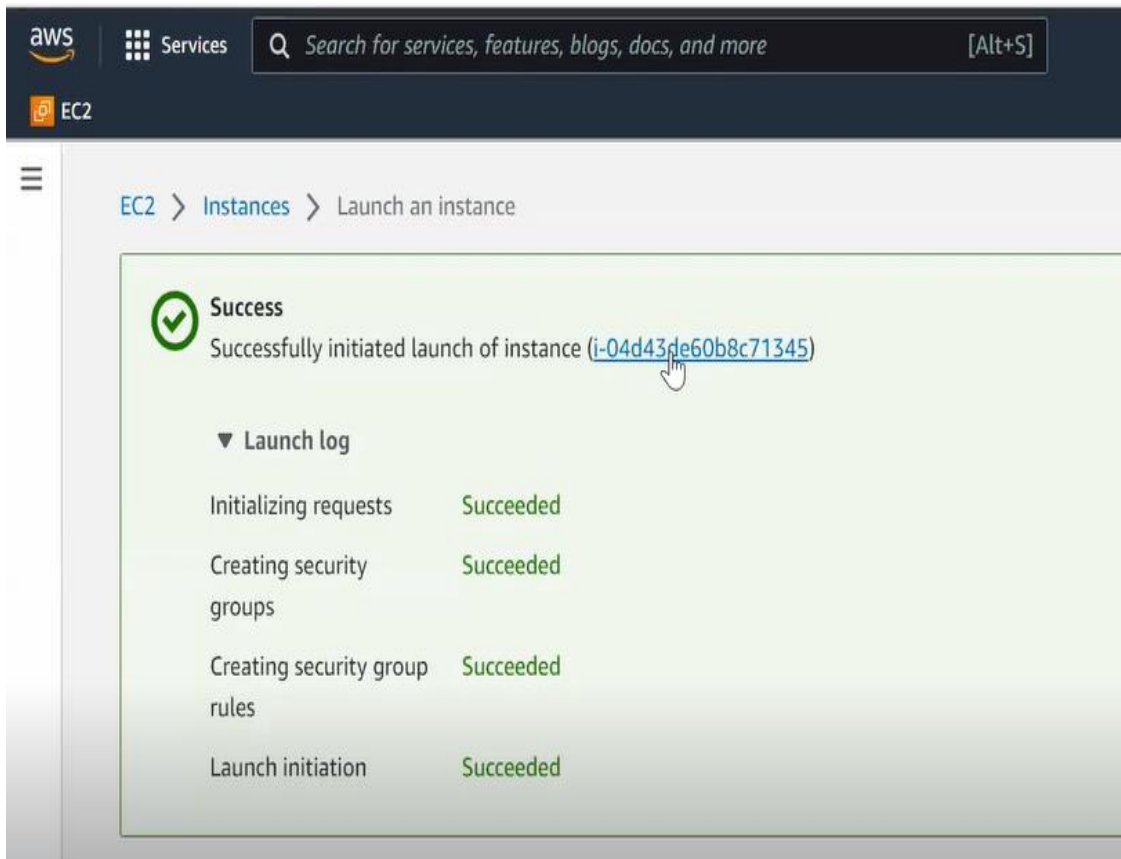
Firewall (security group)

New security group

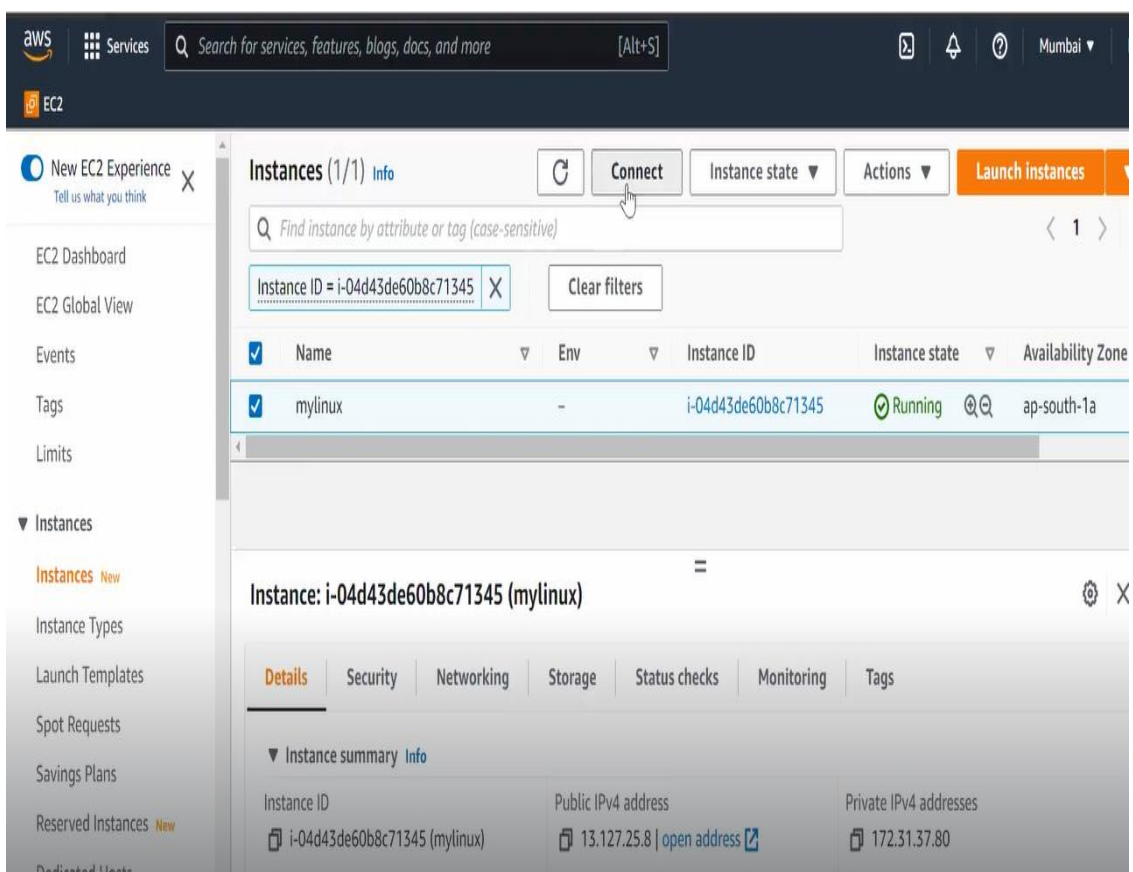
Storage (volumes)

Cancel

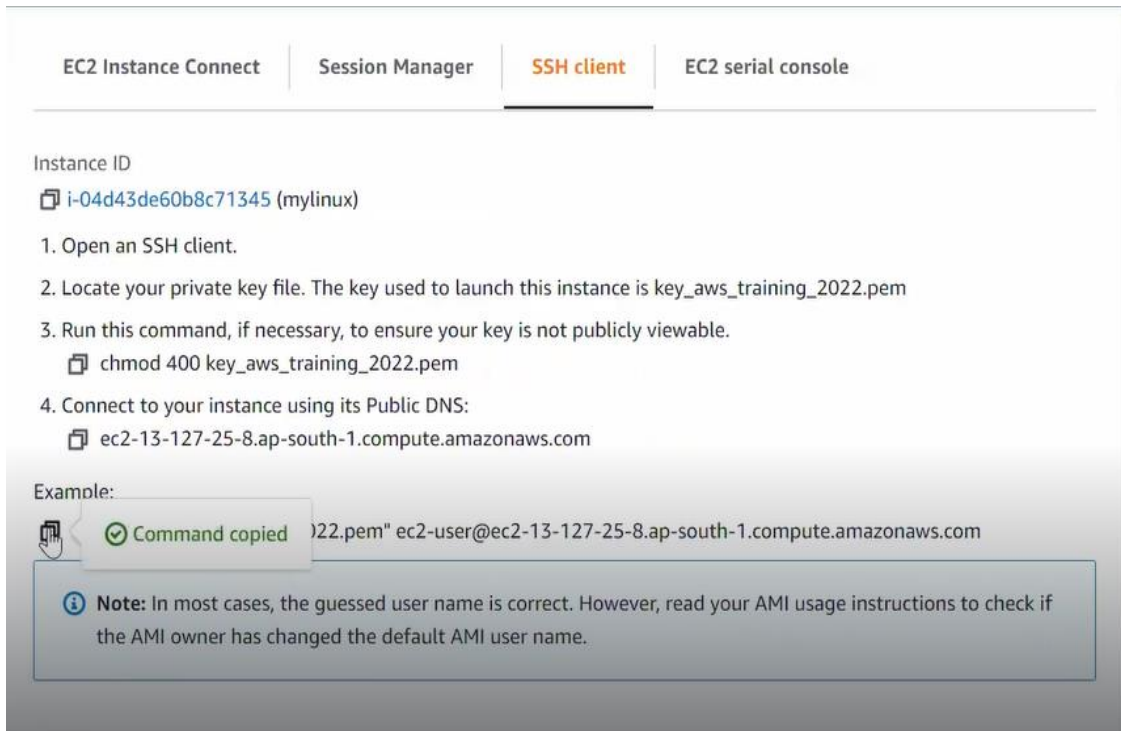
Launch instance



➤ After launching the OS – public IP Address is given



➤ Copy the command

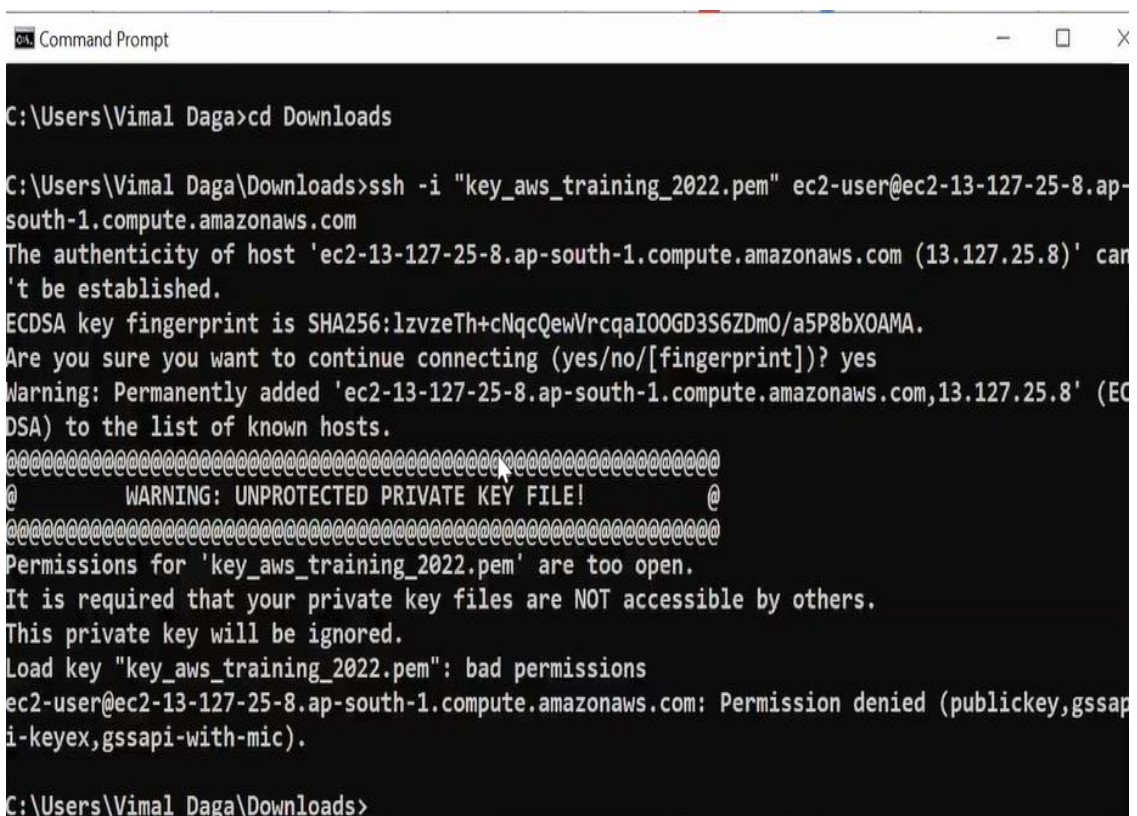


The screenshot shows the AWS Management Console interface for an EC2 instance. At the top, there are four tabs: "EC2 Instance Connect", "Session Manager", "SSH client" (which is selected and highlighted in orange), and "EC2 serial console". Below the tabs, the "Instance ID" is displayed as "i-04d43de60b8c71345 (mylinux)". A list of instructions is provided:

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is key_aws_training_2022.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
`chmod 400 key_aws_training_2022.pem`
4. Connect to your instance using its Public DNS:
`ec2-13-127-25-8.ap-south-1.compute.amazonaws.com`

An "Example:" section shows a terminal window with the command: `ssh -i "key_aws_training_2022.pem" ec2-user@ec2-13-127-25-8.ap-south-1.compute.amazonaws.com`. A green checkmark and the text "Command copied" are visible next to the command. Below this, a note states: "Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name."

➤ Open the command prompt – go to downloads and paste the command – if you get such error – its due to permission issues



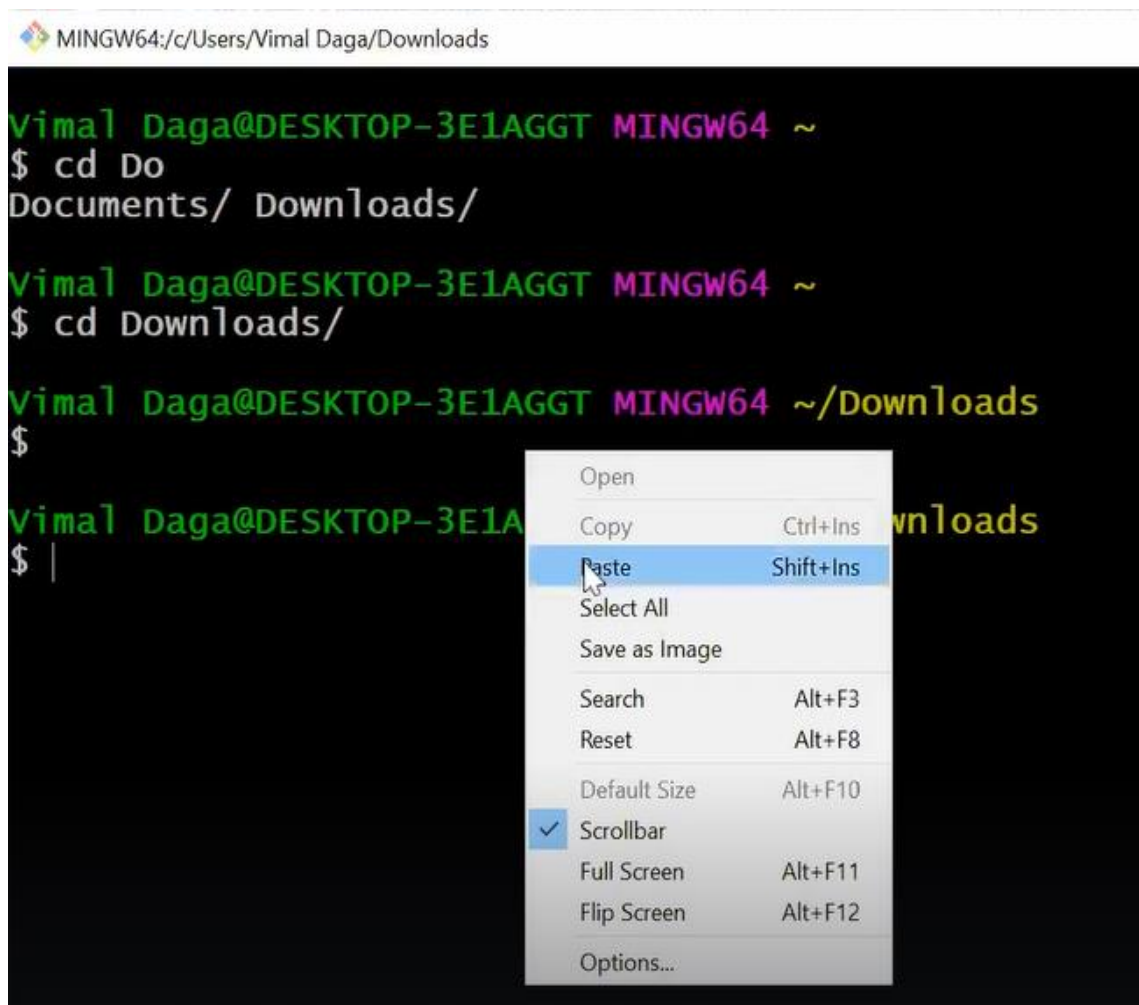
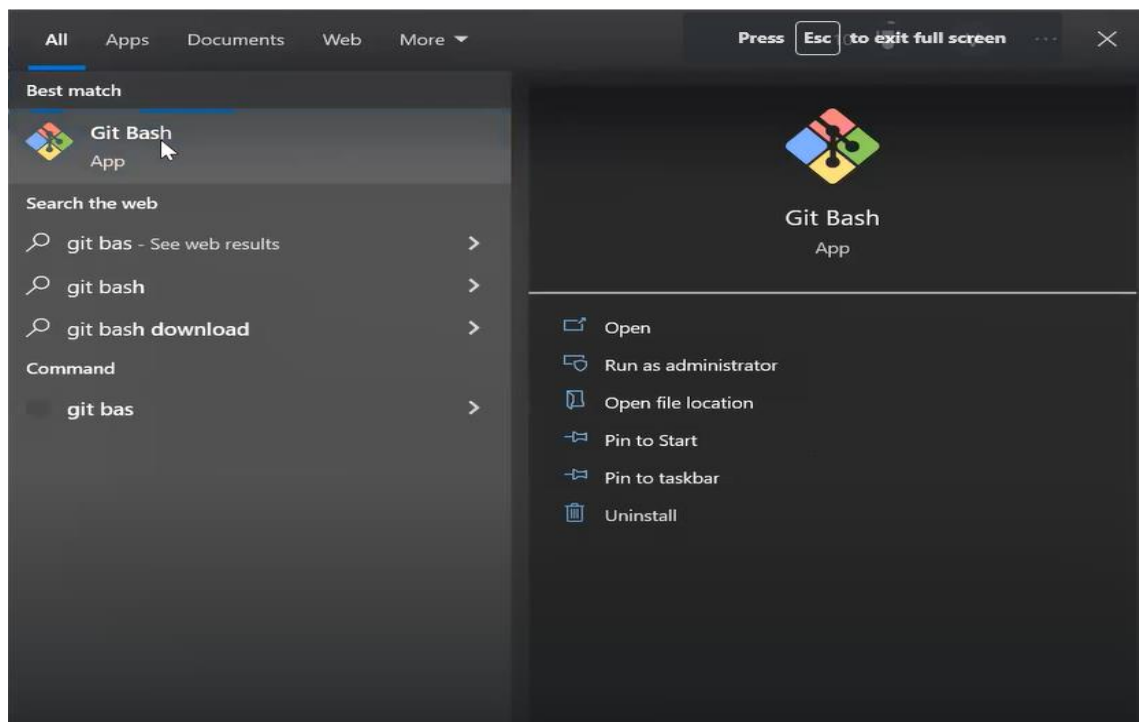
The screenshot shows a Windows Command Prompt window with the following text:

```
C:\Users\Vimal Daga>cd Downloads

C:\Users\Vimal Daga\Downloads>ssh -i "key_aws_training_2022.pem" ec2-user@ec2-13-127-25-8.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-127-25-8.ap-south-1.compute.amazonaws.com (13.127.25.8)' can't be established.
ECDSA key fingerprint is SHA256:1zvzeTh+cNqcQewVrcqaIO0GD3S6ZDmO/a5P8bXOAMA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-127-25-8.ap-south-1.compute.amazonaws.com,13.127.25.8' (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions for 'key_aws_training_2022.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key_aws_training_2022.pem": bad permissions
ec2-user@ec2-13-127-25-8.ap-south-1.compute.amazonaws.com: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

C:\Users\Vimal Daga\Downloads>
```

- We can resolve this by using Putty or Git Bash



- Finally logged in to the OS

```
ec2-user@ip-172-31-37-80:~  
Vimal Daga@DESKTOP-3E1AGGT MINGW64 ~  
$ cd Do  
Documents/ Downloads/  
Vimal Daga@DESKTOP-3E1AGGT MINGW64 ~  
$ cd Downloads/  
Vimal Daga@DESKTOP-3E1AGGT MINGW64 ~/Downloads  
$  
Vimal Daga@DESKTOP-3E1AGGT MINGW64 ~/Downloads  
$ ssh -i "key_aws_training_2022.pem" ec2-user@ec2-13-127-25-8.ap-south-1.compute  
.amazonaws.com  
[ec2-user@ip-172-31-37-80 ~]$  
[ec2-user@ip-172-31-37-80 ~]$  
[ec2-user@ip-172-31-37-80 ~]$
```

- Login to the root account

```
[ec2-user@ip-172-31-37-80 ~]$  
[ec2-user@ip-172-31-37-80 ~]$  
[ec2-user@ip-172-31-37-80 ~]$ sudo su - root  
[root@ip-172-31-37-80 ~]#  
[root@ip-172-31-37-80 ~]#  
[root@ip-172-31-37-80 ~]# whoami  
root  
[root@ip-172-31-37-80 ~]#
```

- When we launch RedHat OS on AWS Cloud – yum is pre-configured

```
[root@ip-172-31-37-80 ~]# yum install httpd  
Updating Subscription Management repositories.  
Unable to read consumer identity  
  
This system is not registered with an entitlement server. You can use subscrip  
on-manager to register.  
  
Red Hat Enterprise Linux 8 for x86_64 - AppStre 48 MB/s | 46 MB 00:00  
Red Hat Enterprise Linux 8 for x86_64 - BaseOS 69 MB/s | 52 MB 00:00
```


- Go into the configuration file and create a webpage

```
[root@ip-172-31-37-80 ~]#  
[root@ip-172-31-37-80 ~]#  
[root@ip-172-31-37-80 ~]# cd /var/www/html/  
[root@ip-172-31-37-80 html]# ls  
[root@ip-172-31-37-80 html]# cat > index.html  
i m vimal  
[root@ip-172-31-37-80 html]# ls  
index.html
```

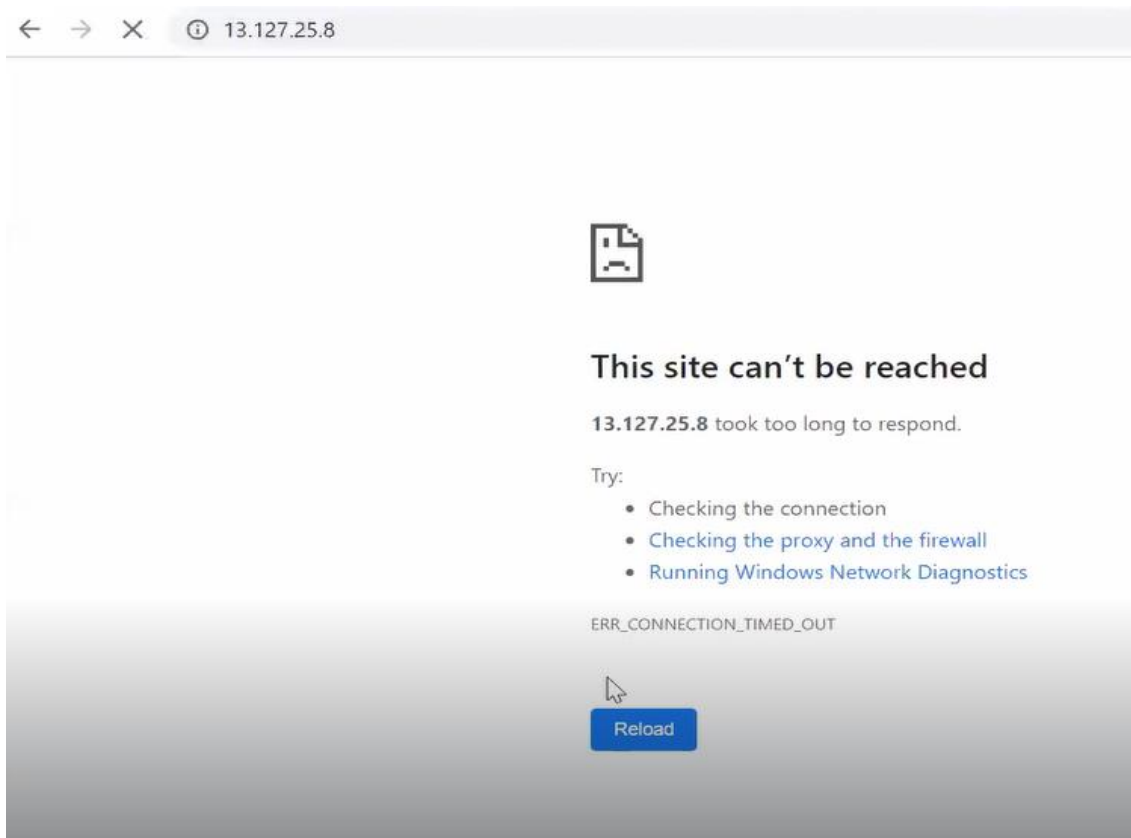
- Start the service

```
[root@ip-172-31-37-80 html]# systemctl start httpd  
[root@ip-172-31-37-80 html]# systemctl status httpd  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres>  
   Active: active (running) since Sun 2022-10-16 08:53:28 UTC; 6s ago  
     Docs: man:httpd.service(8)  
  Main PID: 13183 (httpd)  
    Status: "Started, listening on: port 80"  
   Tasks: 213 (limit: 4700)  
  Memory: 25.8M  
   CGroup: /system.slice/httpd.service  
           └─13183 /usr/sbin/httpd -DFOREGROUND  
             └─13184 /usr/sbin/httpd -DFOREGROUND  
               └─13185 /usr/sbin/httpd -DFOREGROUND  
                 └─13186 /usr/sbin/httpd -DFOREGROUND  
                   └─13187 /usr/sbin/httpd -DFOREGROUND  
  
Oct 16 08:53:27 ip-172-31-37-80.ap-south-1.compute.internal systemd[1]: Startin>  
Oct 16 08:53:28 ip-172-31-37-80.ap-south-1.compute.internal systemd[1]: Started>  
Oct 16 08:53:28 ip-172-31-37-80.ap-south-1.compute.internal httpd[13183]: Serve>  
[root@ip-172-31-37-80 html]#  
[root@ip-172-31-37-80 html]#
```

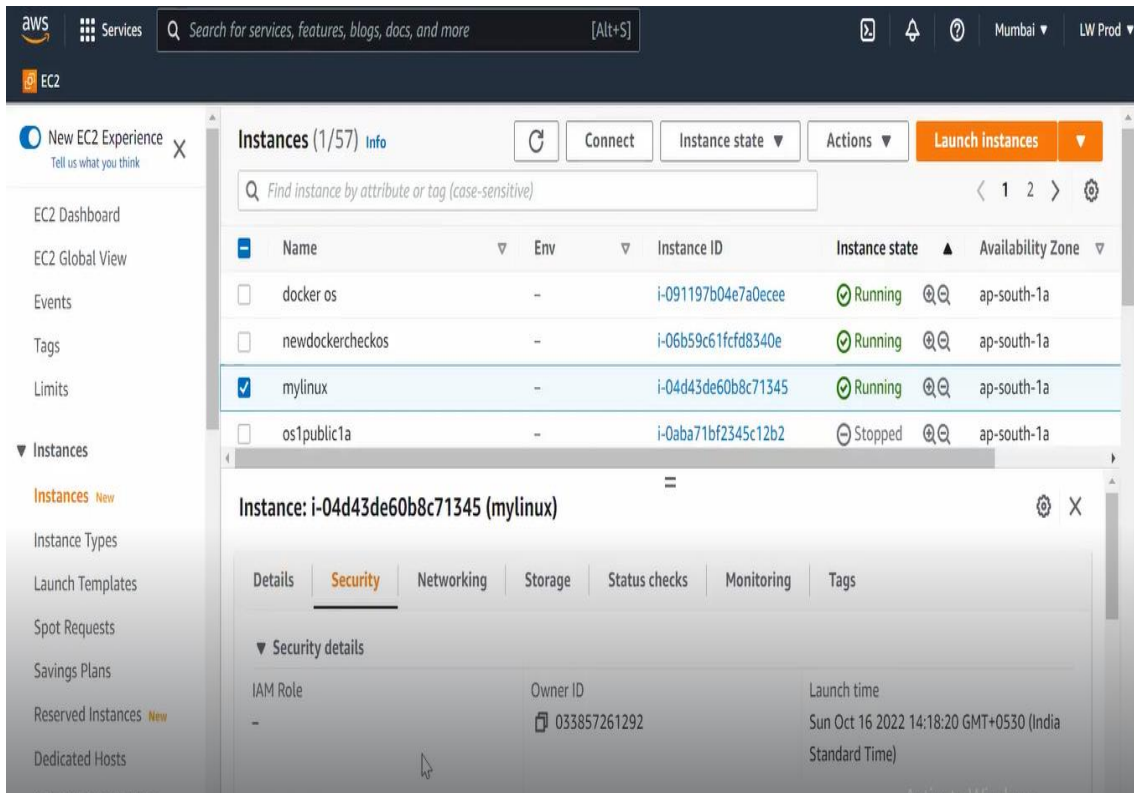
- Firewall disabled – there is no software installed

```
[root@ip-172-31-37-80 html]#  
[root@ip-172-31-37-80 html]#  
[root@ip-172-31-37-80 html]# systemctl status firewalld  
Unit firewalld.service could not be found.  
[root@ip-172-31-37-80 html]#
```

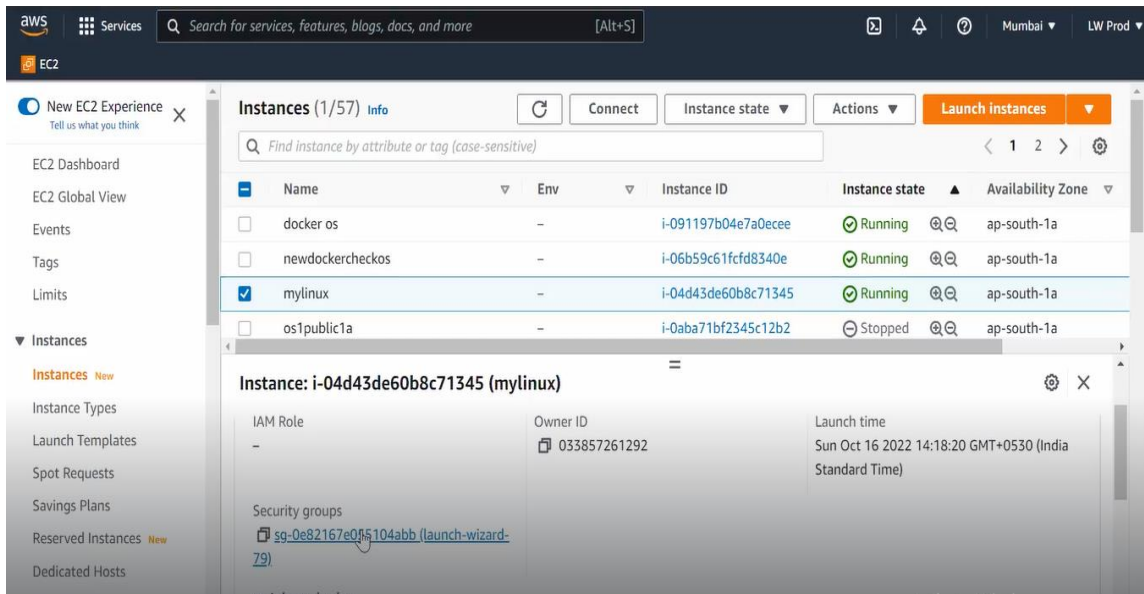
- But still not able to connect – this is because of internal firewall in cloud



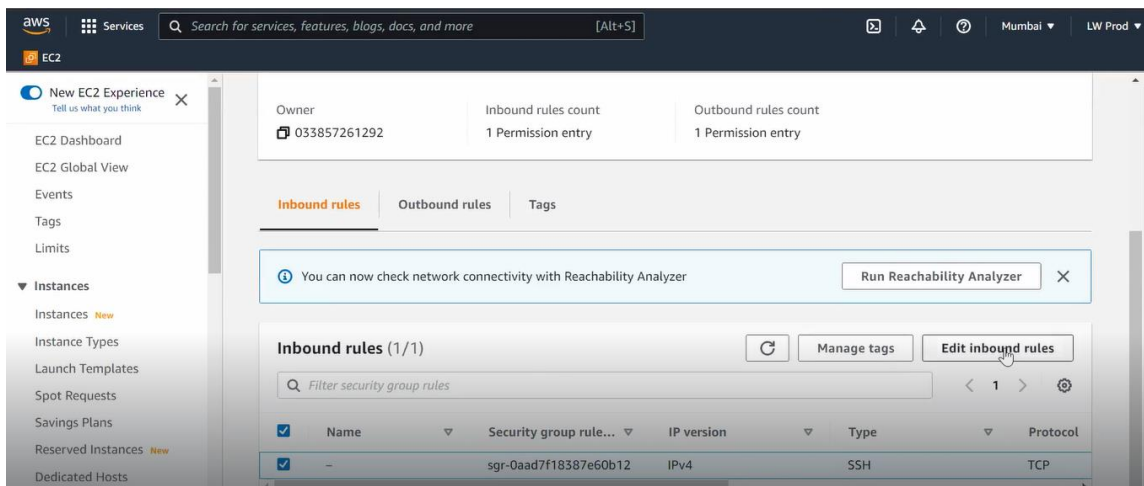
- Click on security



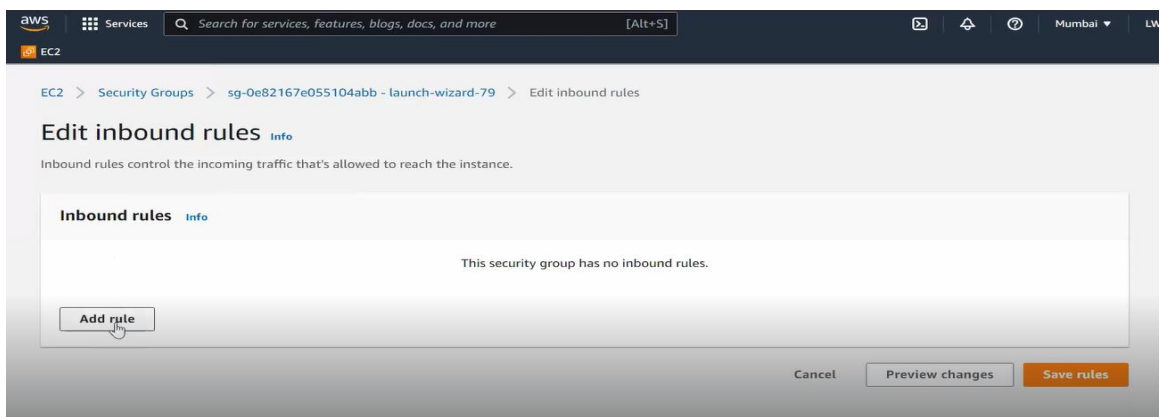
➤ Click on security groups

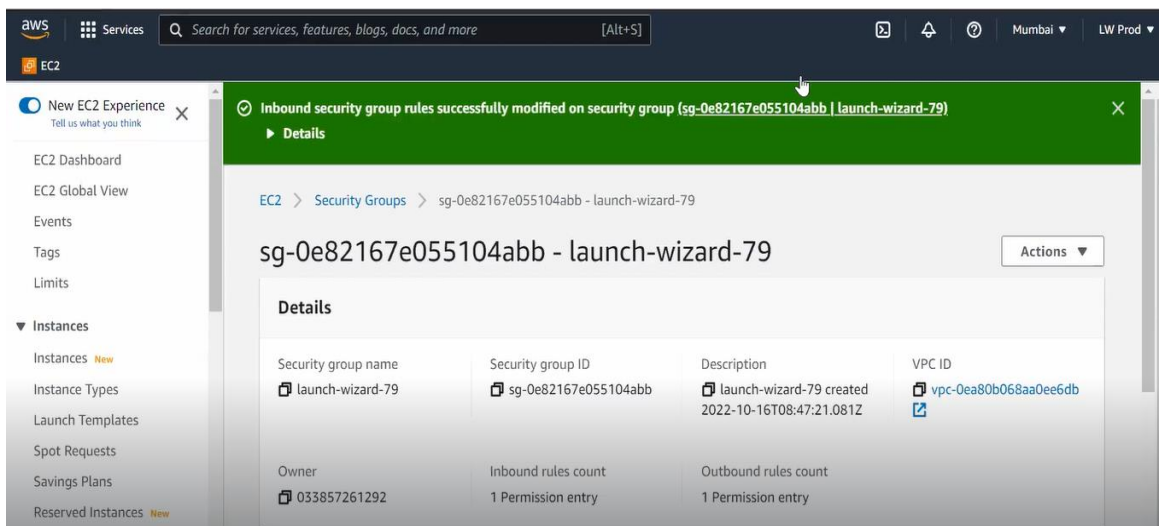
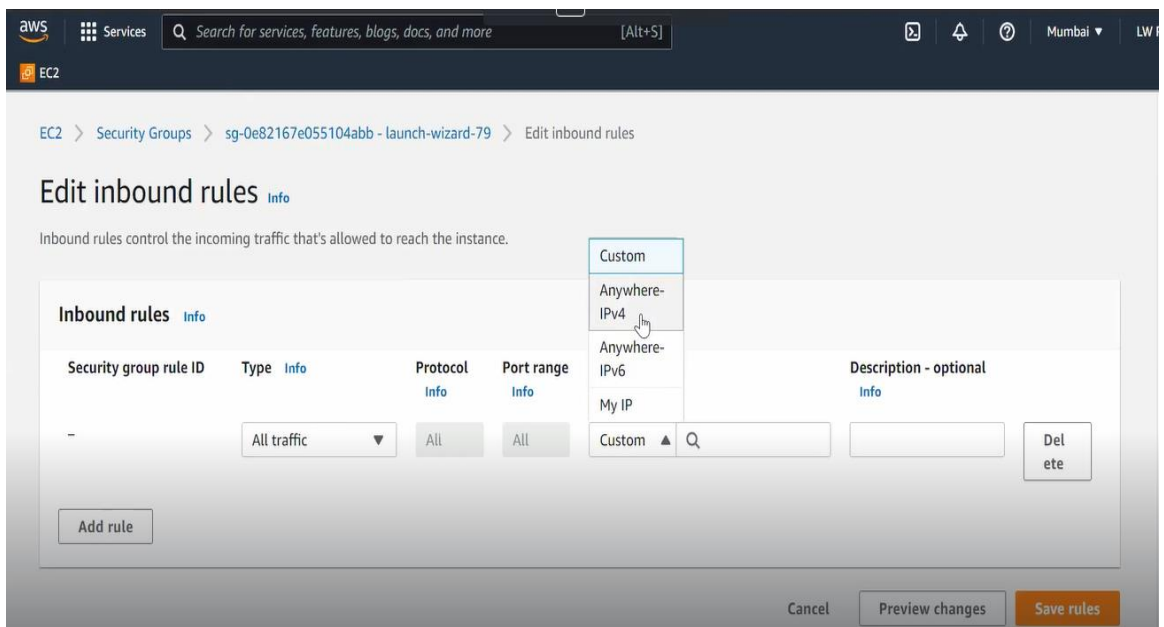
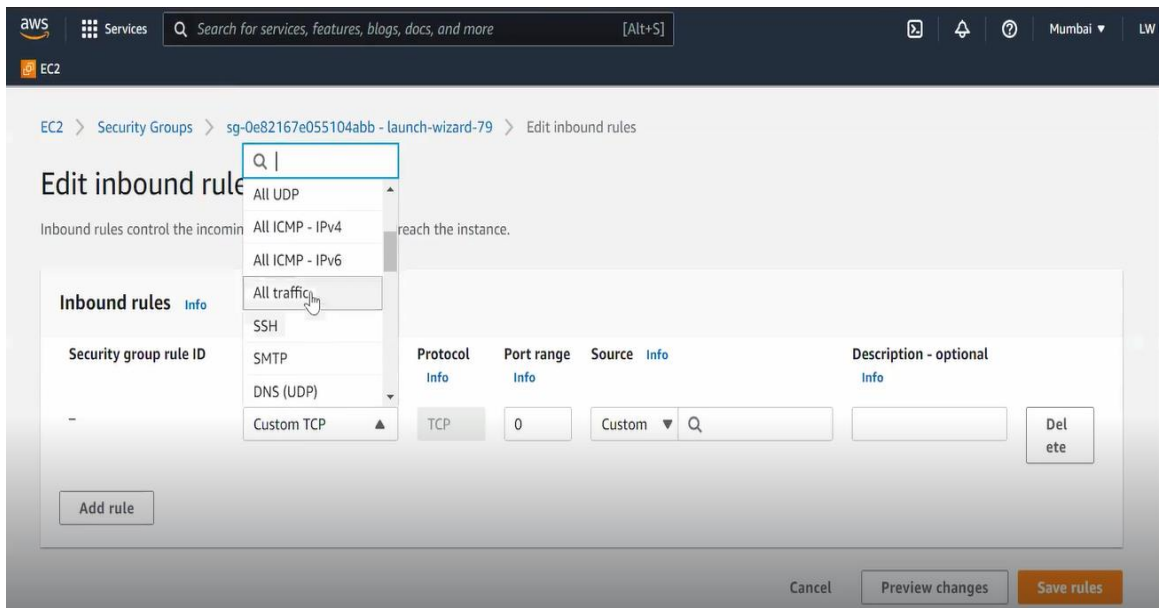


➤ Click on Edit Inbound Rules

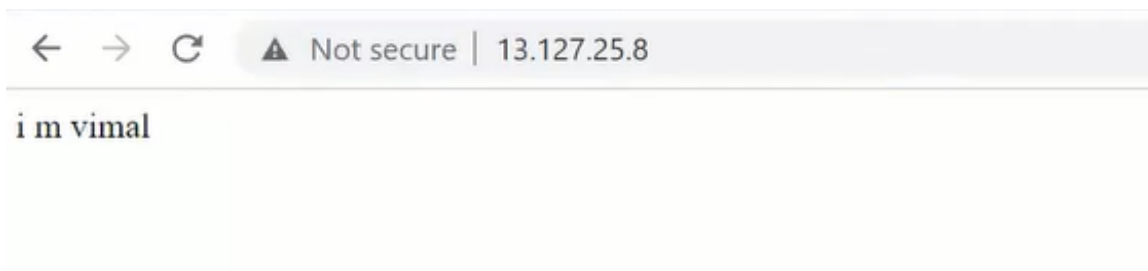


➤ Add a rule





- By using the public IP anyone can access the webpage



- Command to check the configuration file of the Apache HTTPD Webserver

```
[root@localhost ~]# rpm -q httpd
httpd-2.4.51-7.el9_0.x86_64
[root@localhost ~]# rpm -q -c httpd
/etc/httpd/conf.d/autoindex.conf
/etc/httpd/conf.d/userdir.conf
/etc/httpd/conf.d/welcome.conf
/etc/httpd/conf.modules.d/00-base.conf
/etc/httpd/conf.modules.d/00-dav.conf
/etc/httpd/conf.modules.d/00-mpm.conf
/etc/httpd/conf.modules.d/00-optional.conf
/etc/httpd/conf.modules.d/00-proxy.conf
/etc/httpd/conf.modules.d/00-systemd.conf
/etc/httpd/conf.modules.d/01-cgi.conf
/etc/httpd/conf/httpd.conf
/etc/httpd/conf/magic
/etc/logrotate.d/httpd
```

- Command to open the configuration file

```
[root@localhost ~]# vim /etc/httpd/conf/httpd.conf
```

- The Webserver running on Port Number 80

```
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
Listen 80
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
#
# If you wish httpd to run as a different user or group, you must run
```

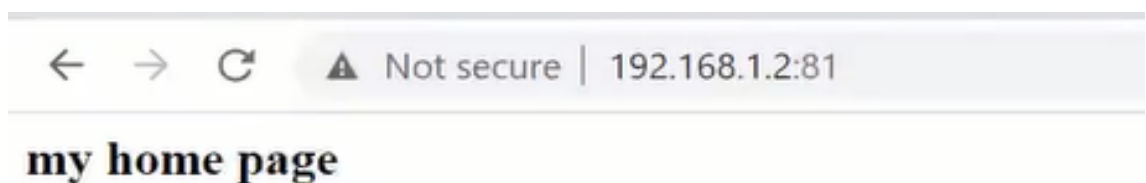


```
Command Prompt

C:\Users\Vimal Daga>curl http://192.168.1.2:81/index.html
<h2>my home page</h2>

C:\Users\Vimal Daga>curl http://192.168.1.2:80/index.html
curl: (7) Failed to connect to 192.168.1.2 port 80 after 2004 ms: Connection refused

C:\Users\Vimal Daga>
```



- If we change the port number out of range

```
root@localhost:~ — vim /etc/httpd/conf/httpd.conf

# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
# 2 bytes: 0-65535
Listen 70000

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
```

```
[root@localhost ~]# systemctl reload httpd
Job for httpd.service failed.
See "systemctl status httpd.service" and "journalctl -xeu httpd.service" for details.

[root@localhost ~]#
```

- Command to check if the service fails

```
[root@localhost ~]# journalctl -xeu httpd.service
```

```
root@localhost:~ — journalctl -xeu httpd.service

as begun execution.

tpd[2791]: AH00526: Syntax error on line 48 of /etc/httpd/conf/httpd.conf:
tpd[2791]: Invalid address or port
stemd[1]: httpd.service: Control process exited, code=exited, status=1/FAILURE

pport

nit httpd.service has exited.

d its exit status is 1.
stemd[1]: Reload failed for The Apache HTTP Server.
service has finished
```

- Two process cannot have same port no –

```
root@localhost:~ — vim /etc/httpd/conf/httpd.conf

# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#Listen 12.34.56.78:80
# 2 bytes: 0-65535
Listen 22

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
-- INSERT --

48,10 10%
```



```
C:\Users\Vimal Daga>curl http://192.168.1.2:80/index.html
<h2>my home page</h2>

C:\Users\Vimal Daga>curl http://192.168.1.2:81/index.html
<h2>my home page</h2>

C:\Users\Vimal Daga>curl http://192.168.1.2:8080/index.html
<h2>my home page</h2>
```

- Command to list the port numbers supported by httpd

```
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# semanage port -l
```

```
root@localhost:~
howl_port_t      tcp      5335
howl_port_t      udp      5353
hplip_port_t     tcp      1782, 2207, 2208, 8290, 8292, 9100, 9101
, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290, 9291, 50000, 50002
http_cache_port_t tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t udp      3130
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
i18n_input_port_t tcp      9010
ibm_dt_2_port_t  tcp      1792
ibm_dt_2_port_t  udp      1792
imaze_port_t     tcp      5323
imaze_port_t     udp      5323
inetd_child_port_t tcp      1, 9, 13, 19, 512, 544, 891, 892, 5666
inetd_child_port_t udp      1, 9, 13, 19, 891, 892
innd_port_t      tcp      119
intermapper_port_t tcp      8181
interwise_port_t tcp      7778
```

- The tool to scan the network

```
[root@localhost ~]# yum whatprovides nmap
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You
can use rhn_register to register with RH Subscription-
Manager.

Repository 'dvd1' is missing name in configuration, using i
Repository 'dvd2' is missing name in configuration, using i
Last metadata expiration check: 0:32:20 ago on Sun 16 Oct 2
nmap-3:7.91-10.el9.x86_64 : Network exploration tool and se
Repo      : dvd2
Matched from:
Provide   : nmap = 3:7.91-10.el9

[root@localhost ~]# yum install nmap
```


- Command to check IP is alive

```
[root@localhost ~]# nmap 192.168.1.2
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 15:09
Nmap scan report for 192.168.1.2
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
1234/tcp   open  hotline

Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
[root@localhost ~]#
```

- Command to check the ports open

```
[root@localhost ~]# nmap -p 1234 192.168.1.2
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 15:11
Nmap scan report for 192.168.1.2
Host is up (0.000040s latency).

PORT      STATE SERVICE
1234/tcp   open  hotline

Nmap done: 1 IP address (1 host up) scanned in 6.70 seconds
[root@localhost ~]#
```

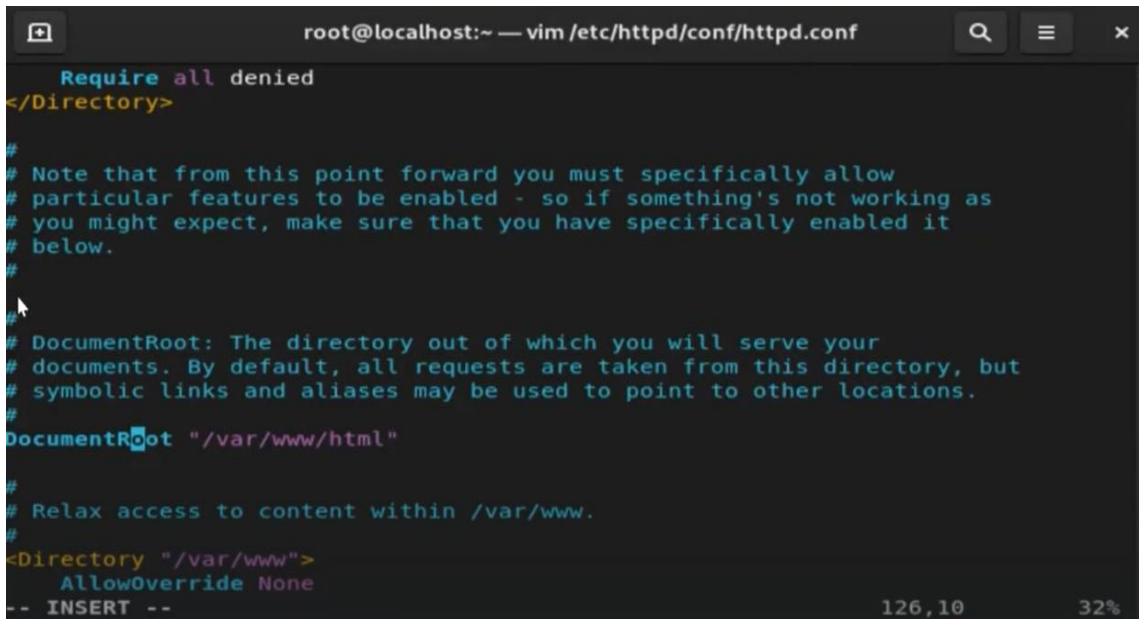
- Command to perform version scanning-

```
[root@localhost ~]# nmap -p 1234 -sV 192.168.1.2
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-16 15:11
Nmap scan report for 192.168.1.2
Host is up (0.000042s latency).

PORT      STATE SERVICE VERSION
1234/tcp   open  http      Apache httpd 2.4.51 ((Red Hat Enterprise Linux 7.9))

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
[root@localhost ~]#
```

- The document root of httpd – deploy the webpages in “/var/www/html”

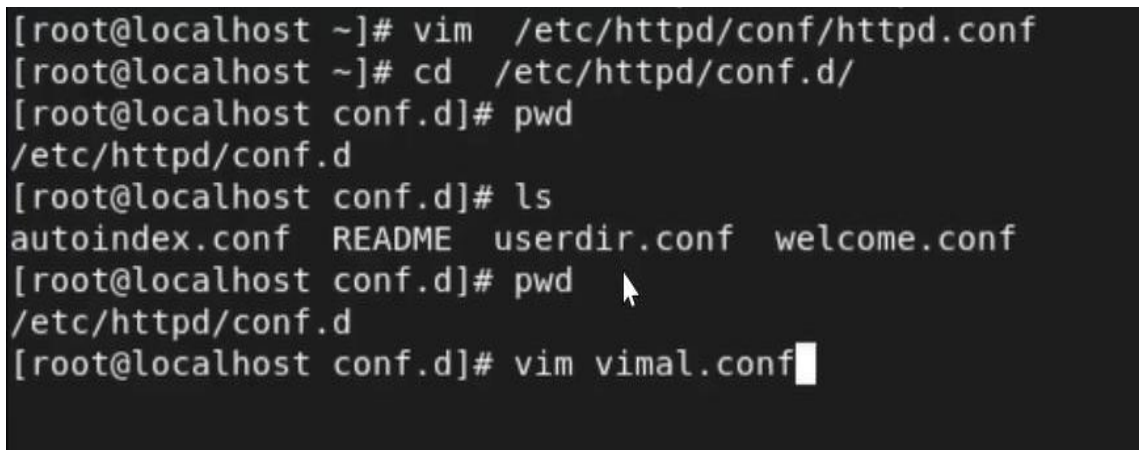


```
root@localhost:~ — vim /etc/httpd/conf/httpd.conf
Require all denied
</Directory>

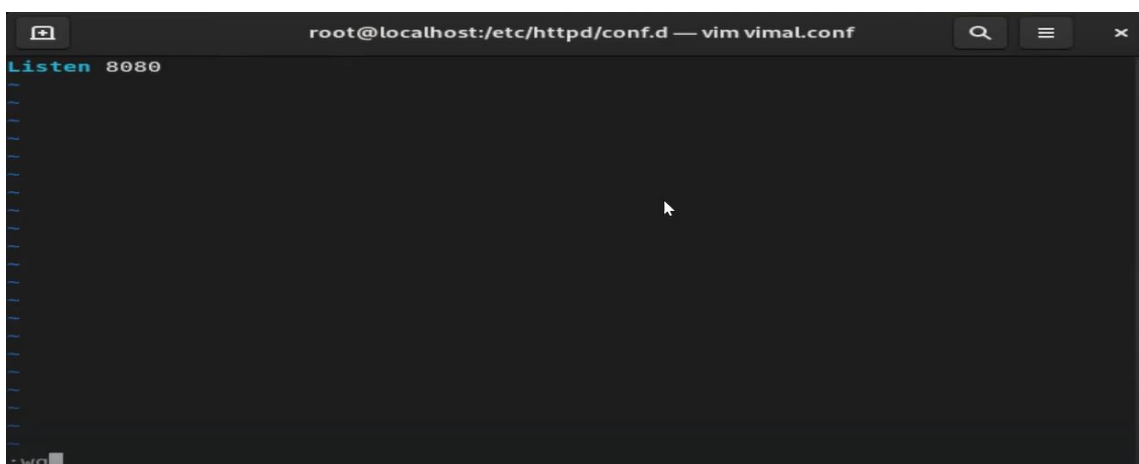
#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"

#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
-- INSERT --
126,10 32%
```

- The main configuration file of httpd is “/etc/httpd/conf/httpd.conf” – if any changes to be made – we can create a file with extension “.conf”



```
[root@localhost ~]# vim /etc/httpd/conf/httpd.conf
[root@localhost ~]# cd /etc/httpd/conf.d/
[root@localhost conf.d]# pwd
/etc/httpd/conf.d
[root@localhost conf.d]# ls
autoindex.conf  README  userdir.conf  welcome.conf
[root@localhost conf.d]# pwd
/etc/httpd/conf.d
[root@localhost conf.d]# vim vimal.conf
```



```
root@localhost:/etc/httpd/conf.d — vim vimal.conf
Listen 8080
: wq
```

```
[root@localhost conf.d]# systemctl reload httpd
[root@localhost conf.d]# netstat -tnlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
1/systemd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
816/sshd: /usr/sbin
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
813/cupsd
tcp6       0      0 :::111                  :::*                     LISTEN
1/systemd
tcp6       0      0 :::8080                 :::*                     LISTEN
3580/httpd
tcp6       0      0 :::80                   :::*                     LISTEN
3580/httpd
tcp6       0      0 :::22                   :::*                     LISTEN
816/sshd: /usr/sbin
tcp6       0      0 :::1:631                :::*                     LISTEN
813/cupsd
[root@localhost conf.d]#
```

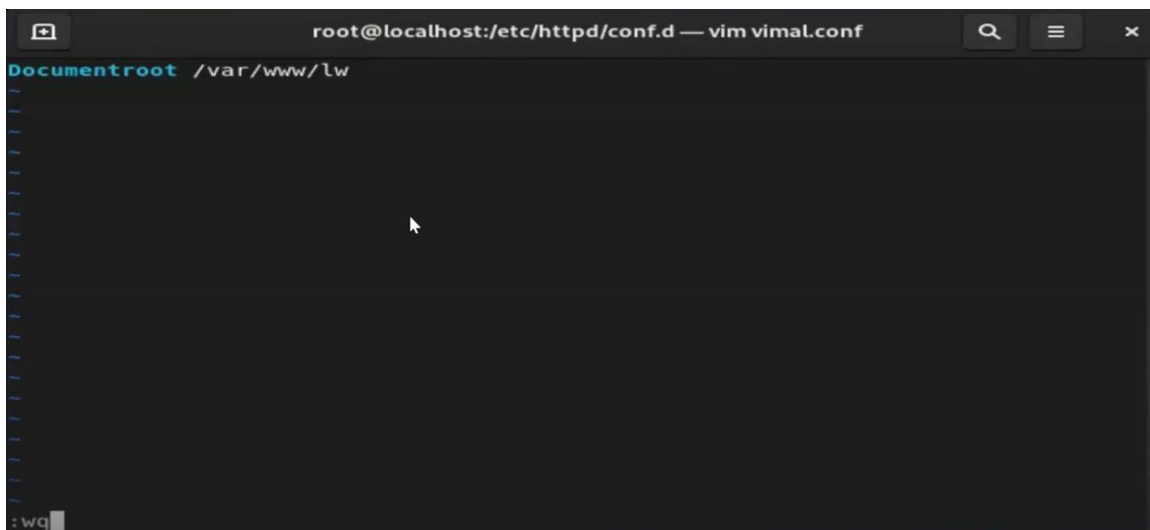
- Command to go back to the previous folder

```
[root@localhost lw]# cd -
/etc/httpd/conf.d
```

- To change the document root – first we have to create the folder

```
[root@localhost conf.d]# mkdir /var/www/lw
[root@localhost conf.d]# cd /var/www/lw
[root@localhost lw]# ls
[root@localhost lw]#
```

```
[root@localhost conf.d]# vim vimal.conf
```



The screenshot shows a vim editor window with the title bar "root@localhost:/etc/httpd/conf.d — vim vimal.conf". The editor content shows the "DocumentRoot" directive set to "/var/www/lw". The status bar at the bottom indicates the current line is 1 and the column is 11, with the text ":wq" followed by a cursor.

- Host a webpage –

```
[root@localhost html]# cd /var/www/lw/
[root@localhost lw]# ls
[root@localhost lw]# cat > index.html
new location ...
[root@localhost lw]# ls
index.html
[root@localhost lw]# pwd
/var/www/lw
[root@localhost lw]#
```

- When the client hits the server – the server records all the information of client –

```
[root@localhost conf.d]# cd /var/log/
[root@localhost log]# ls
anaconda      dnf.librepo.log  maillog        secure-20221016
audit         dnf.log          maillog-20221016 speech-dispatcher
boot.log      dnf.rpm.log      messages       spooler
boot.log-20221015 firewalld        messages-20221016 spooler-20221016
boot.log-20221016 gdm             private        sssd
btmptmp      hawkey.log       qemu-ga        tallylog
chrony        hawkey.log-20221016 README         wtmp
cron          httpd            rhsm
cron-20221016 insights-client samba
cups          lastlog          secure
```

```
[root@localhost log]# cd httpd/
[root@localhost httpd]# pwd
/var/log/httpd
[root@localhost httpd]# ls
access_log  error_log
[root@localhost httpd]# vim error_log
```



```

[Sun Oct 16 14:53:22.414208 2022] [mpm_event:notice] [pid 2968:tid 2968] AH00489:
: Apache/2.4.51 (Red Hat Enterprise Linux) configured -- resuming normal operations
[Sun Oct 16 14:53:22.414225 2022] [core:notice] [pid 2968:tid 2968] AH00094: Com
mand line: '/usr/sbin/httpd -D FOREGROUND'
[Sun Oct 16 14:55:56.496213 2022] [mpm_event:notice] [pid 2968:tid 2968] AH00493
: SIGUSR1 received. Doing graceful restart
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using localhost.localdomain. Set the 'ServerName' directive globally to s
uppress this message
(13)Permission denied: AH00072: make_sock: could not bind to address [::]:1234
(13)Permission denied: AH00072: make_sock: could not bind to address 0.0.0.0:123
4
[Sun Oct 16 14:55:56.573816 2022] [mpm_event:alert] [pid 2968:tid 2968] no liste
ning sockets available, shutting down
[Sun Oct 16 14:55:56.573822 2022] [:emerg] [pid 2968:tid 2968] AH00019: Unable t
o open logs, exiting
[Sun Oct 16 15:01:24.651830 2022] [core:notice] [pid 3580:tid 3580] SELinux poli
cy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sun Oct 16 15:01:24.653392 2022] [suexec:notice] [pid 3580:tid 3580] AH01232: s
uEXEC mechanism enabled (wrapper: /usr/sbin/suexec)

```

58,1 61%

```

[root@localhost httpd]#
[root@localhost httpd]# pwd
/var/log/httpd
[root@localhost httpd]# ls
access_log  error_log
[root@localhost httpd]# cat access_log

```

```

192.168.1.12 - - [16/Oct/2022:15:37:43 +0530] "GET /index.html HTTP/1.1" 404 196
 "-" "curl/7.83.1"
192.168.1.12 - - [16/Oct/2022:15:38:15 +0530] "GET /index.html HTTP/1.1" 200 17
 "-" "curl/7.83.1"
192.168.1.12 - - [16/Oct/2022:15:41:26 +0530] "GET /vimal.html HTTP/1.1" 200 6 "
 "-" "curl/7.83.1"
192.168.1.12 - - [16/Oct/2022:15:41:31 +0530] "GET / HTTP/1.1" 200 17 "-" "curl/
7.83.1"
192.168.1.12 - - [16/Oct/2022:15:41:36 +0530] "GET / HTTP/1.1" 200 17 "-" "curl/
7.83.1"
192.168.1.12 - - [16/Oct/2022:15:41:39 +0530] "GET /vimal.html HTTP/1.1" 200 6 "
 "-" "curl/7.83.1"
192.168.1.12 - - [16/Oct/2022:15:43:24 +0530] "GET /vimal.html HTTP/1.1" 200 6 "
 "-" "curl/7.83.1"
192.168.1.12 - - [16/Oct/2022:15:43:26 +0530] "GET / HTTP/1.1" 200 6 "-" "curl/7
.83.1"
192.168.1.12 - - [16/Oct/2022:15:43:33 +0530] "GET / HTTP/1.1" 200 6 "-" "curl/7
.83.1"
192.168.1.12 - - [16/Oct/2022:15:43:39 +0530] "GET /index.html HTTP/1.1" 200 17
 "-" "curl/7.83.1"
[root@localhost httpd]#
[root@localhost httpd]#

```