Name: Frias, Abegail L.	**Date Performed: Aug 30, 2024**
Course/Section: CPE212 - CPE31S21	**Date Submitted: Aug 30, 2024**
Instructor: Engr. Robin Valenzuela	**Semester and SY: 1st Sem/2024-2025**

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

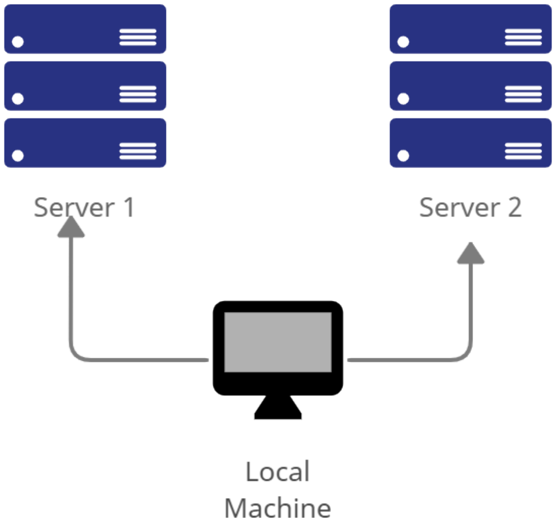
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

1.2. Set-up a Virtual Network and Test Connectivity of VMs

2. **Discussion:**

Network Topology:

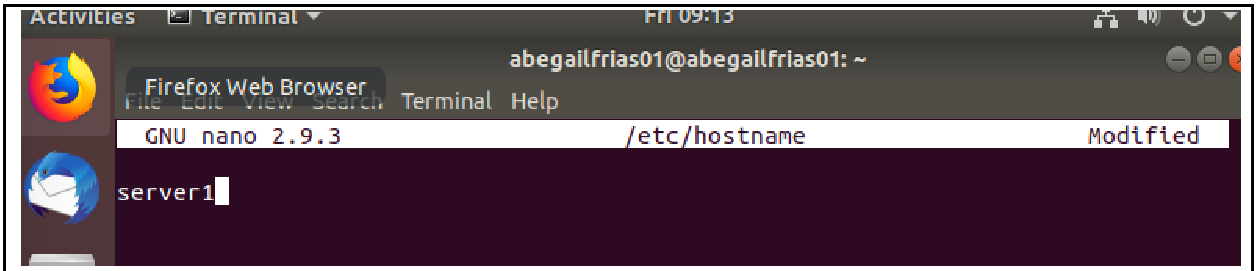
Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine*).



Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

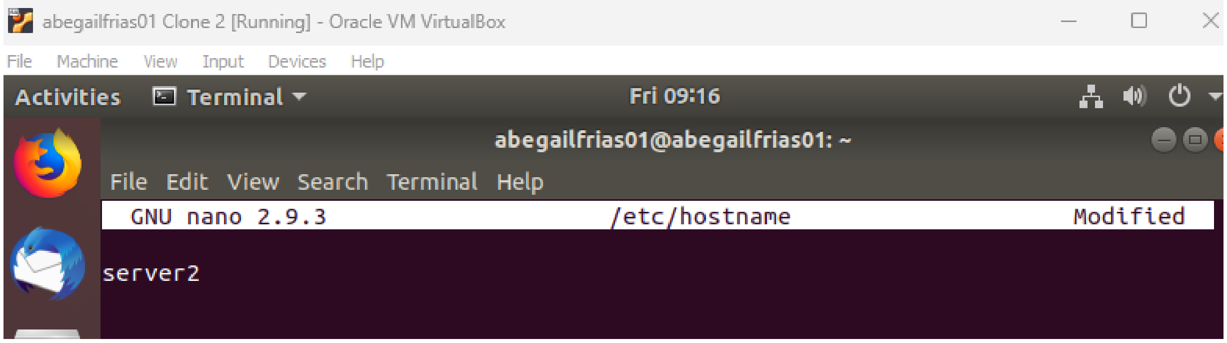
1. Change the hostname using the command *sudo nano /etc/hostname*

   1.1 Use server1 for Server 1


Activities
Terminal
Fri 09:13
abegailfrias01@abegailfrias01: ~
Firefox Web Browser
File Edit View Search Terminal Help

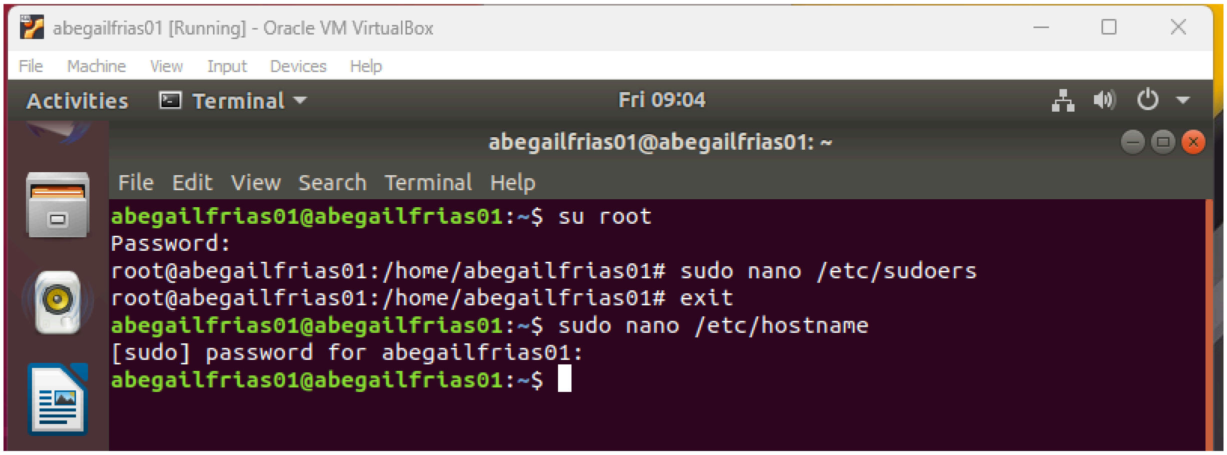
```
  GNU nano 2.9.3                 /etc/hostname                 Modified

server1
```

1.2 Use server2 for Server 2

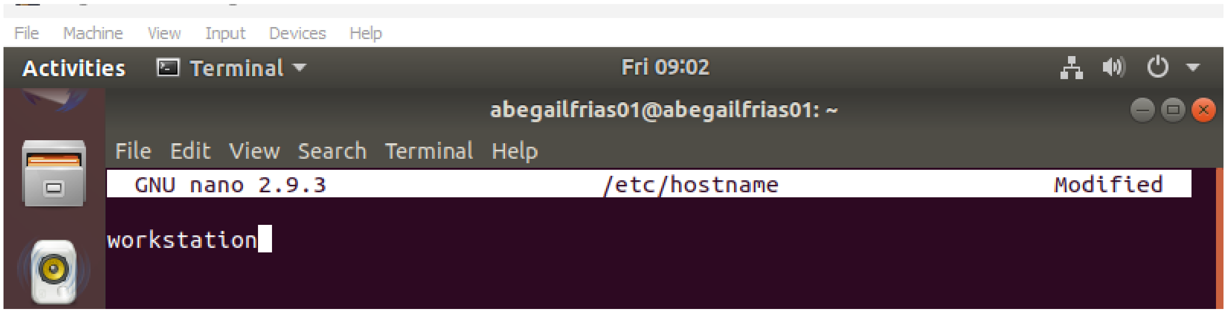

abegailfrias01 Clone 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Fri 09:16
abegailfrias01@abegailfrias01: ~
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                 /etc/hostname                 Modified

server2
```

1.3 Use workstation for the Local Machine


abegailfrias01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Fri 09:04
abegailfrias01@abegailfrias01: ~
File Edit View Search Terminal Help

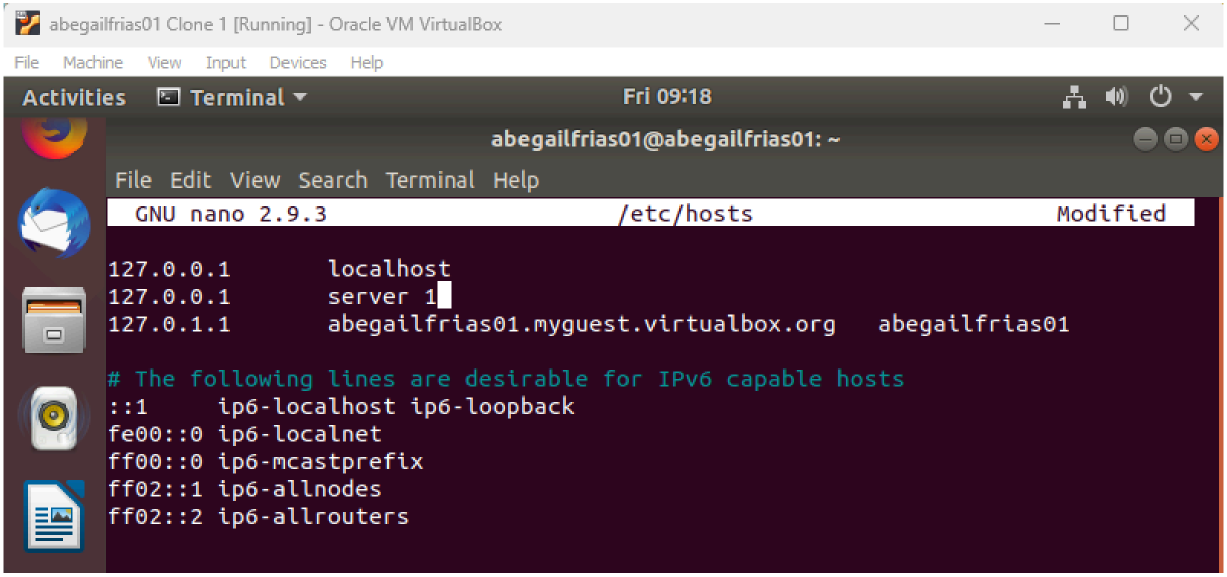
```
abegailfrias01@abegailfrias01:~$ su root
Password:
root@abegailfrias01:/home/abegailfrias01# sudo nano /etc/sudoers
root@abegailfrias01:/home/abegailfrias01# exit
abegailfrias01@abegailfrias01:~$ sudo nano /etc/hostname
[sudo] password for abegailfrias01:
abegailfrias01@abegailfrias01:~$ 
```


File Machine View Input Devices Help
Activities
Terminal
Fri 09:02
abegailfrias01@abegailfrias01: ~
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                 /etc/hostname                 Modified

workstation
```

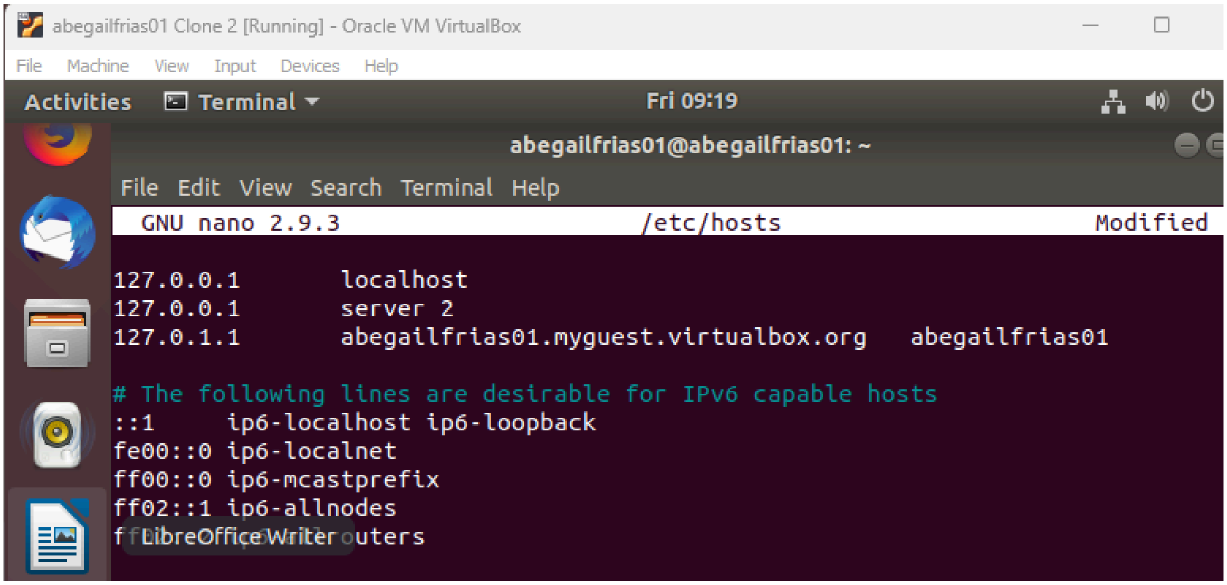
2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

2.1 Type 127.0.0.1 server 1 for Server 1


abegailfrias01 Clone 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Fri 09:18
abegailfrias01@abegailfrias01: ~
File Edit View Search Terminal Help

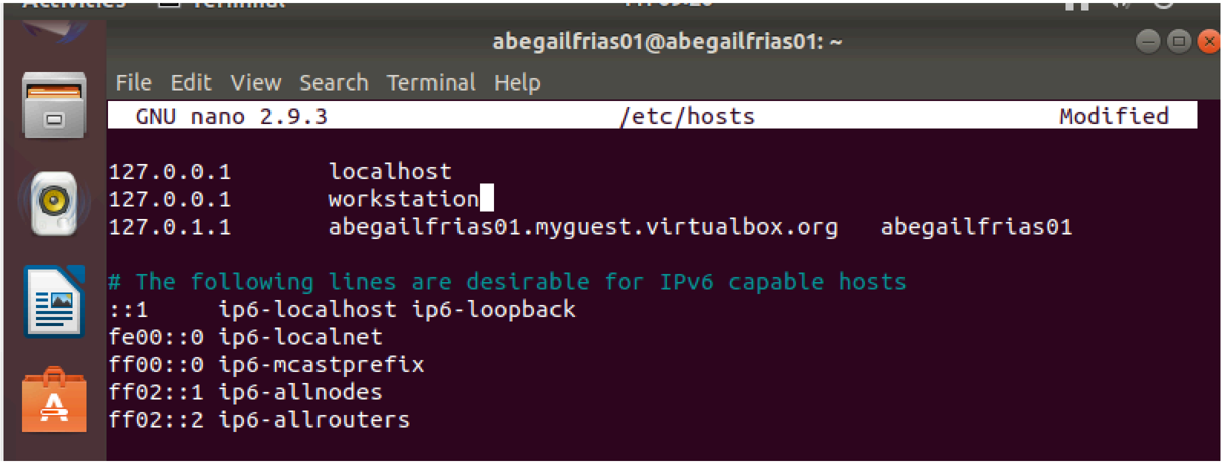
```
  GNU nano 2.9.3                  /etc/hosts                        Modified

127.0.0.1       localhost
127.0.0.1       server 1
127.0.1.1       abegailfrias01.myguest.virtualbox.org   abegailfrias01

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

2.2 Type 127.0.0.1 server 2 for Server 2


abegailfrias01 Clone 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Fri 09:19
abegailfrias01@abegailfrias01: ~
File Edit View Search Terminal Help
LibreOffice Writer

```
  GNU nano 2.9.3                  /etc/hosts                        Modified

127.0.0.1       localhost
127.0.0.1       server 2
127.0.1.1       abegailfrias01.myguest.virtualbox.org   abegailfrias01

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff                 outers
```

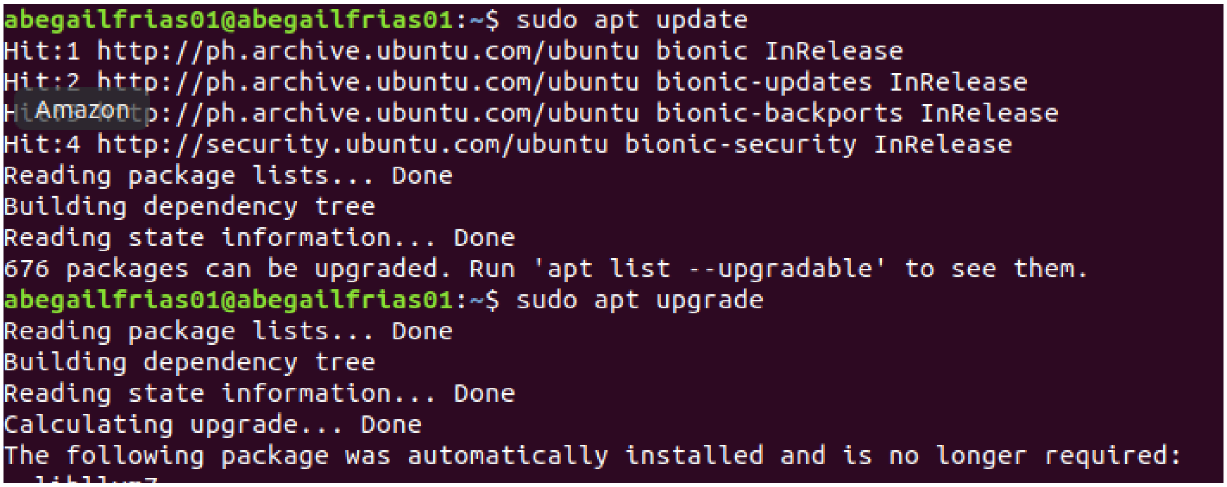
2.3 Type 127.0.0.1 workstation for the Local Machine


abegailfrias01@abegailfrias01: ~
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                    /etc/hosts                        Modified

127.0.0.1       localhost
127.0.0.1       workstation
127.0.1.1       abegailfrias01.myguest.virtualbox.org   abegailfrias01

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

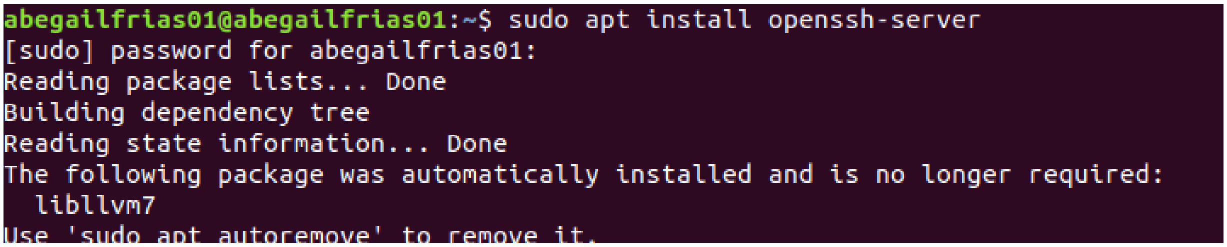
Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

1. Upgrade the packages by issuing the command *sudo apt update* and *sudo apt upgrade* respectively.



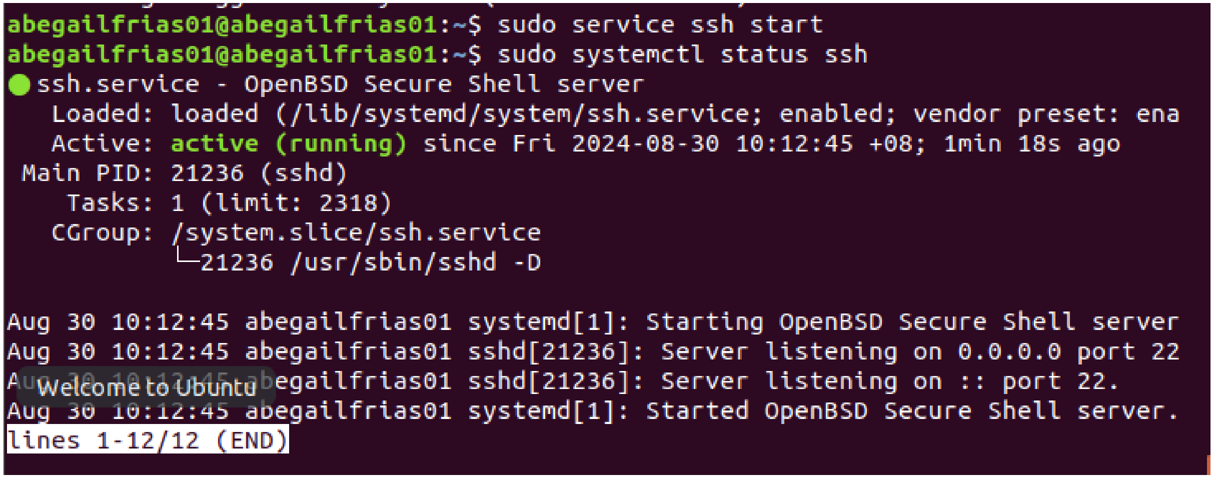
```
abegailfrias01@abegailfrias01:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.
abegailfrias01@abegailfrias01:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
  libllvm7
```

2. Install the SSH server using the command *sudo apt install openssh-server*.

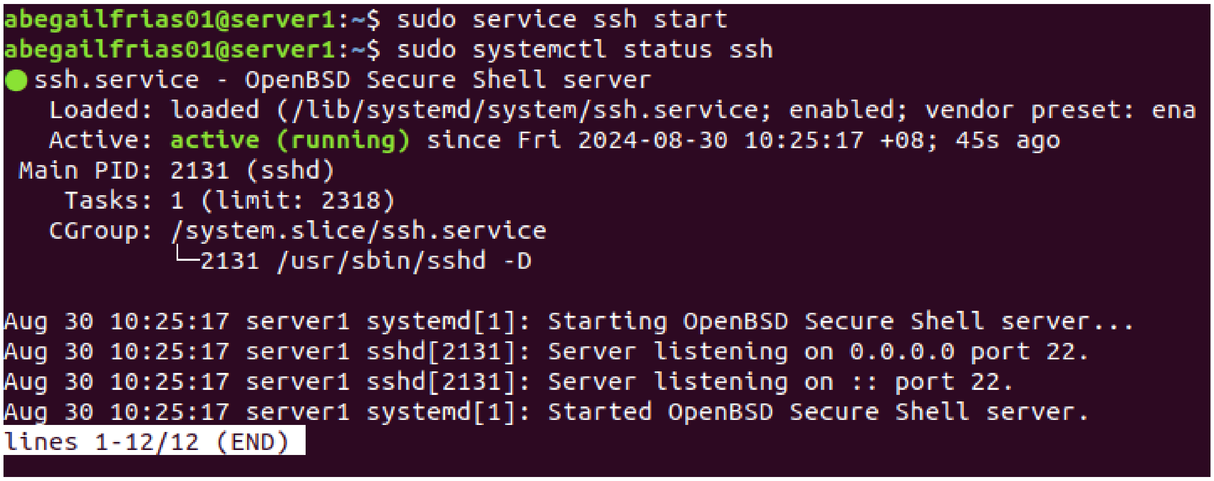


```
abegailfrias01@abegailfrias01:~$ sudo apt install openssh-server
[sudo] password for abegailfrias01:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
```

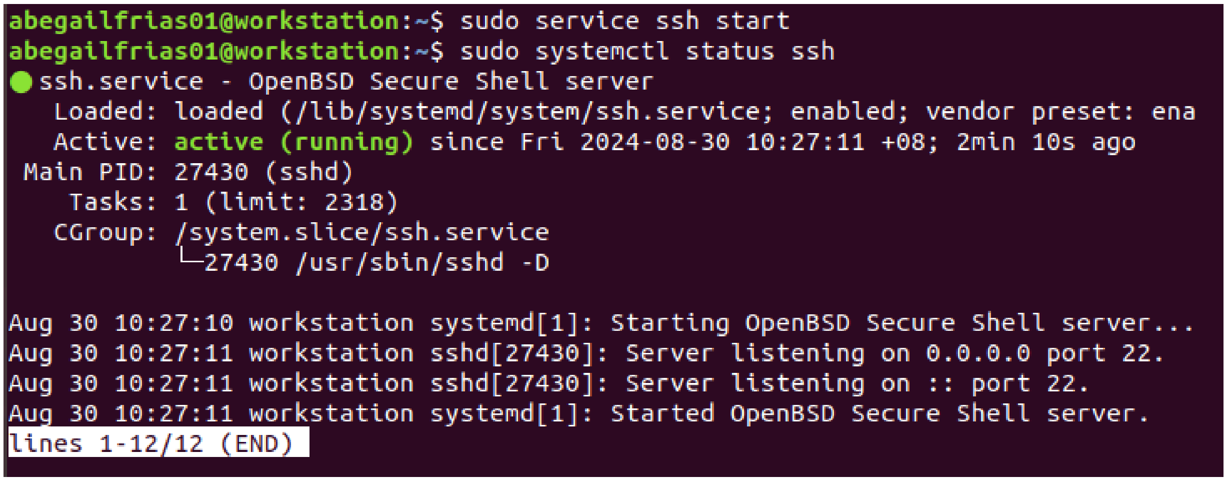
3. Verify if the SSH service has started by issuing the following commands:
   3.1 sudo service ssh start
   3.2 sudo systemctl status ssh



```
abegailfrias01@abegailfrias01:~$ sudo service ssh start
abegailfrias01@abegailfrias01:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2024-08-30 10:12:45 +08; 1min 18s ago
 Main PID: 21236 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─21236 /usr/sbin/sshd -D

Aug 30 10:12:45 abegailfrias01 systemd[1]: Starting OpenBSD Secure Shell server
Aug 30 10:12:45 abegailfrias01 sshd[21236]: Server listening on 0.0.0.0 port 22
Aug 30 10:12:45 abegailfrias01 sshd[21236]: Server listening on :: port 22.
Aug 30 10:12:45 abegailfrias01 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```



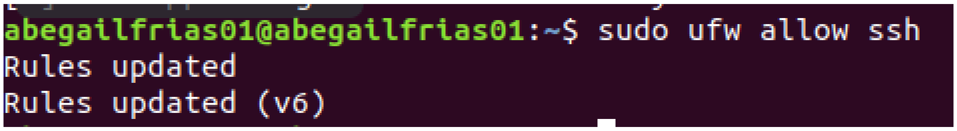
```
abegailfrias01@server1:~$ sudo service ssh start
abegailfrias01@server1:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2024-08-30 10:25:17 +08; 45s ago
 Main PID: 2131 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─2131 /usr/sbin/sshd -D

Aug 30 10:25:17 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 30 10:25:17 server1 sshd[2131]: Server listening on 0.0.0.0 port 22.
Aug 30 10:25:17 server1 sshd[2131]: Server listening on :: port 22.
Aug 30 10:25:17 server1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```



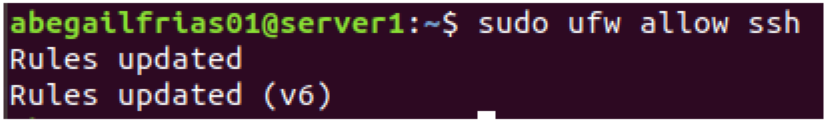
```
abegailfrias01@workstation:~$ sudo service ssh start
abegailfrias01@workstation:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2024-08-30 10:27:11 +08; 2min 10s ago
 Main PID: 27430 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─27430 /usr/sbin/sshd -D

Aug 30 10:27:10 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 30 10:27:11 workstation sshd[27430]: Server listening on 0.0.0.0 port 22.
Aug 30 10:27:11 workstation sshd[27430]: Server listening on :: port 22.
Aug 30 10:27:11 workstation systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

4. Configure the firewall to all port 22 by issuing the following commands:

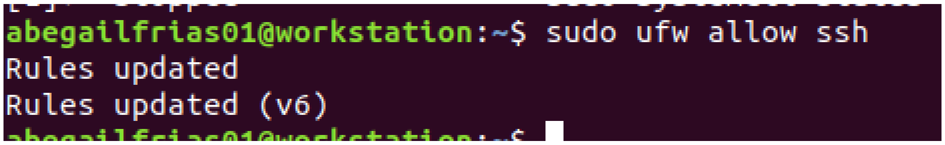
   4.1 sudo ufw allow ssh



```
abegailfrias01@abegailfrias01:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

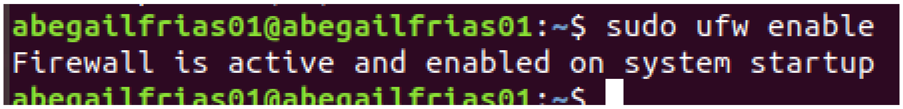


```
abegailfrias01@server1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

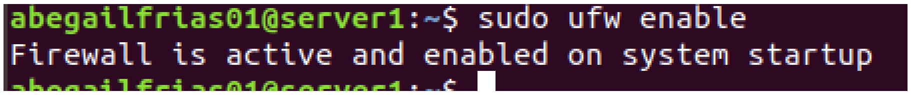


```
abegailfrias01@workstation:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
abegailfrias01@workstation:~$
```

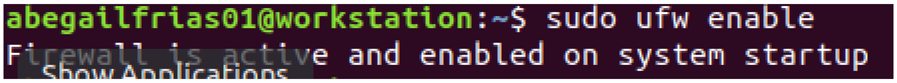
4.2 sudo ufw enable



```
abegailfrias01@abegailfrias01:~$ sudo ufw enable
Firewall is active and enabled on system startup
abegailfrias01@abegailfrias01:~$
```

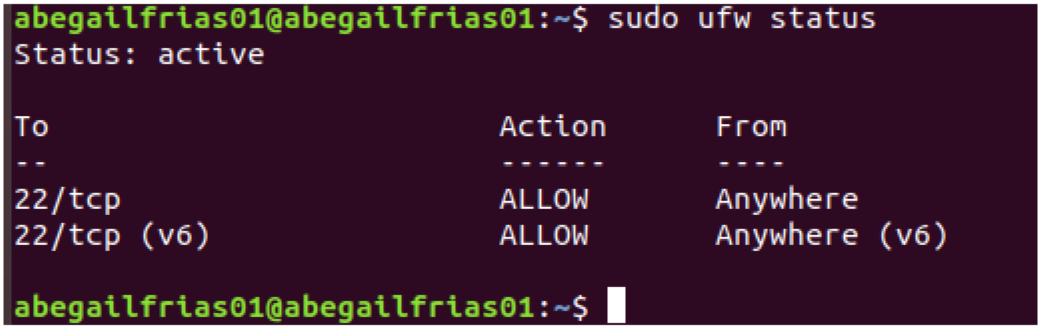


```
abegailfrias01@server1:~$ sudo ufw enable
Firewall is active and enabled on system startup
abegailfrias01@server1:~$
```

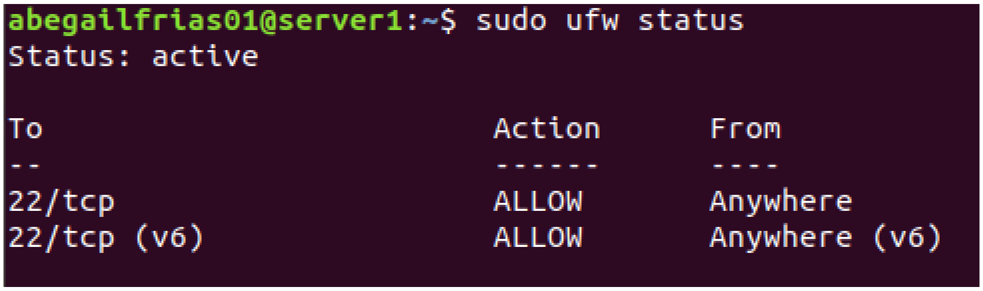


```
abegailfrias01@workstation:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

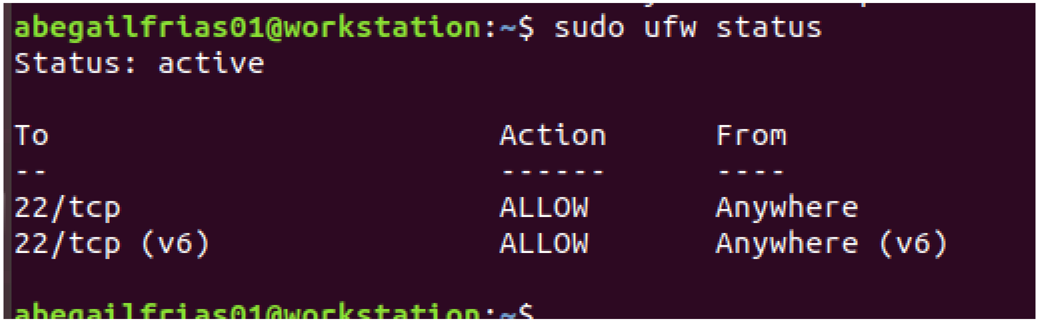
4.3 sudo ufw status



```
abegailfrias01@abegailfrias01:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

abegailfrias01@abegailfrias01:~$
```



```
abegailfrias01@server1:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
```

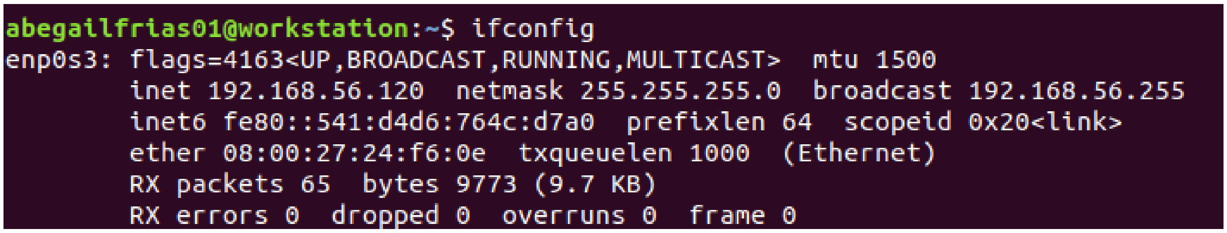


```
abegailfrias01@workstation:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

abegailfrias01@workstation:~$
```

Task 3: Verify network settings on Server 1, Server 2, and Local Machine. On each device, do the following:

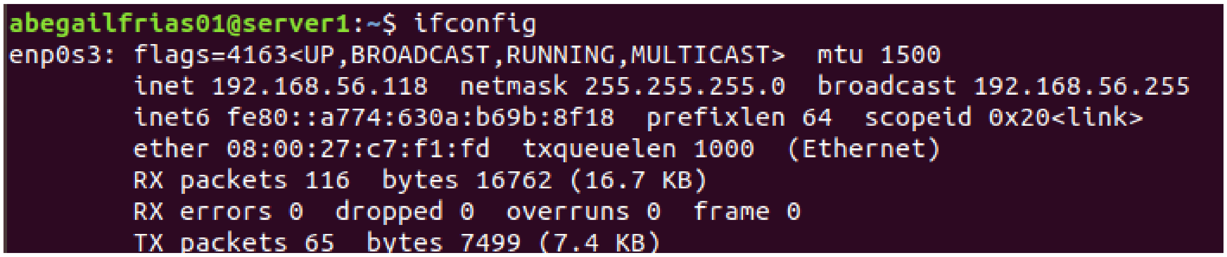
1. Record the ip address of Server 1, Server 2, and Local Machine. Issue the command *ifconfig* and check network settings. Note that the ip addresses of all the machines are in this network 192.168.56.XX.

   1.1 Server 1 IP address: 192.168.56.120



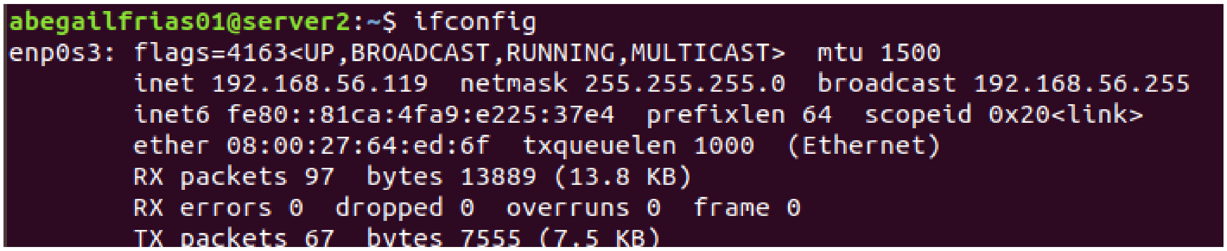
```
abegailfrias01@workstation:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.120  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::541:d4d6:764c:d7a0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:24:f6:0e  txqueuelen 1000  (Ethernet)
        RX packets 65  bytes 9773 (9.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

   1.2 Server 2 IP address: 192.168.56.118



```
abegailfrias01@server1:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.118  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a774:630a:b69b:8f18  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:f1:fd  txqueuelen 1000  (Ethernet)
        RX packets 116  bytes 16762 (16.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 65  bytes 7499 (7.4 KB)
```

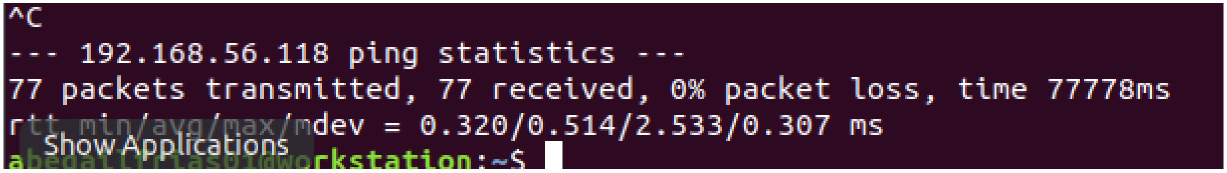
   1.3 Server 3 IP address: 192.168.56.119



```
abegailfrias01@server2:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.119  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::81ca:4fa9:e225:37e4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:64:ed:6f  txqueuelen 1000  (Ethernet)
        RX packets 97  bytes 13889 (13.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 67  bytes 7555 (7.5 KB)
```

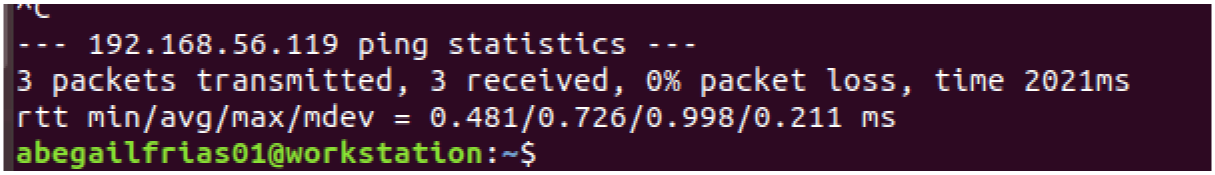
2. Make sure that they can ping each other.

   2.1 Connectivity test for Local Machine 1 to Server 1: □ Successful □ Not Successful



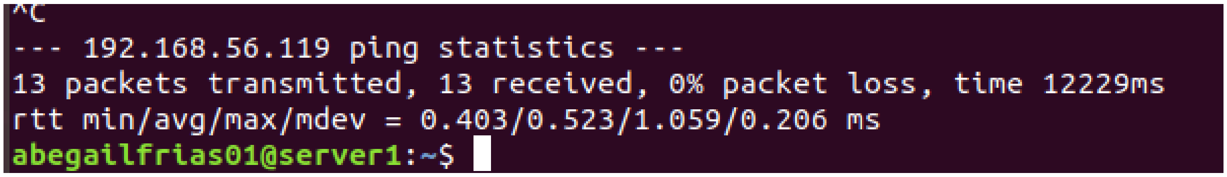
```
^C
--- 192.168.56.118 ping statistics ---
77 packets transmitted, 77 received, 0% packet loss, time 77778ms
rtt min/avg/max/mdev = 0.320/0.514/2.533/0.307 ms
abegailfrias01@workstation:~$
```

2.2 Connectivity test for Local Machine 1 to Server 2: □ Successful □ Not Successful



```
^C
--- 192.168.56.119 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2021ms
rtt min/avg/max/mdev = 0.481/0.726/0.998/0.211 ms
abegailfrias01@workstation:~$
```

2.3 Connectivity test for Server 1 to Server 2: □ Successful □ Not Successful



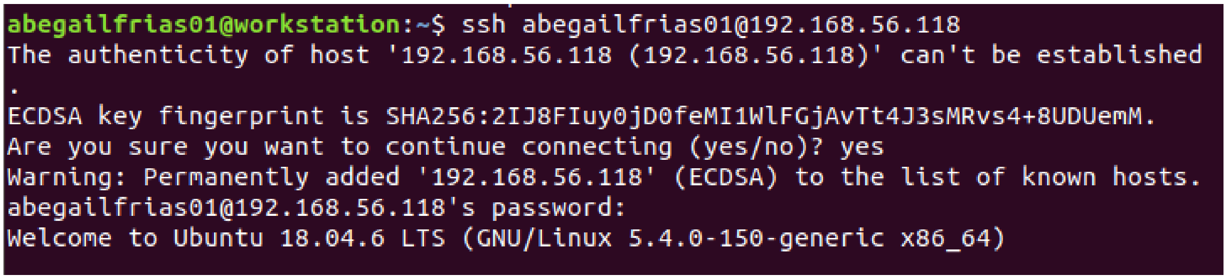
```
^C
--- 192.168.56.119 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12229ms
rtt min/avg/max/mdev = 0.403/0.523/1.059/0.206 ms
abegailfrias01@server1:~$
```

Task 4: Verify SSH connectivity on Server 1, Server 2, and Local Machine.

1. On the Local Machine, issue the following commands:

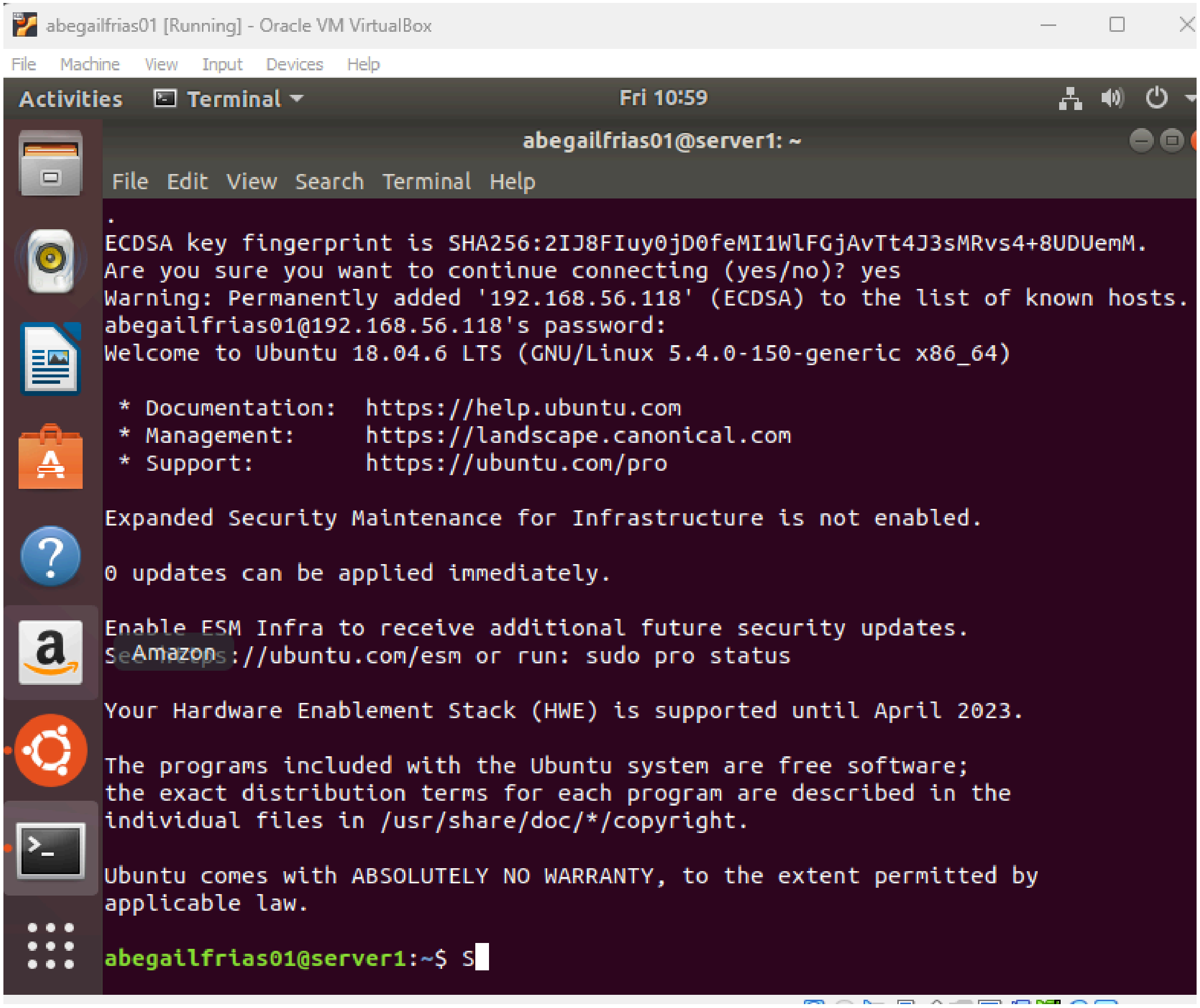
1.1 ssh username@ip_address_server1 for example, *ssh jvtaylar@192.168.56.120*

1.2 Enter the password for server 1 when prompted



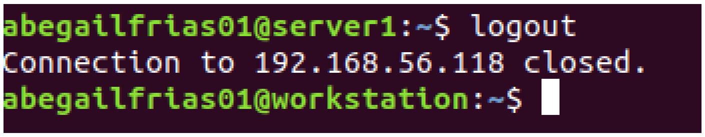
```
abegailfrias01@workstation:~$ ssh abegailfrias01@192.168.56.118
The authenticity of host '192.168.56.118 (192.168.56.118)' can't be established
.
ECDSA key fingerprint is SHA256:2IJ8FIuy0jD0feMI1WlFGjAvTt4J3sMRvs4+8UDUemM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.118' (ECDSA) to the list of known hosts.
abegailfrias01@192.168.56.118's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)
```

1.3 Verify that you are in server 1. The user should be in this format user@server1. For example, *jvtaylar@server1*


abegailfrias01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Fri 10:59
abegailfrias01@server1: ~
File Edit View Search Terminal Help
Amazon

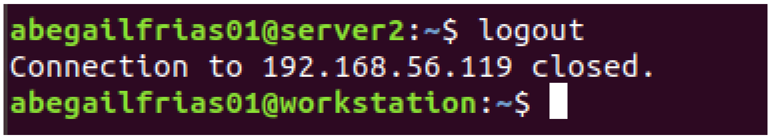
```
.
ECDSA key fingerprint is SHA256:2IJ8FIuy0jD0feMI1WlFGjAvTt4J3sMRvs4+8UDUemM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.118' (ECDSA) to the list of known hosts.
abegailfrias01@192.168.56.118's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

abegailfrias01@server1:~$ S
```

2. Logout of Server 1 by issuing the command *control + D.*



```
abegailfrias01@server1:~$ logout
Connection to 192.168.56.118 closed.
abegailfrias01@workstation:~$
```

3. Do the same for Server 2.

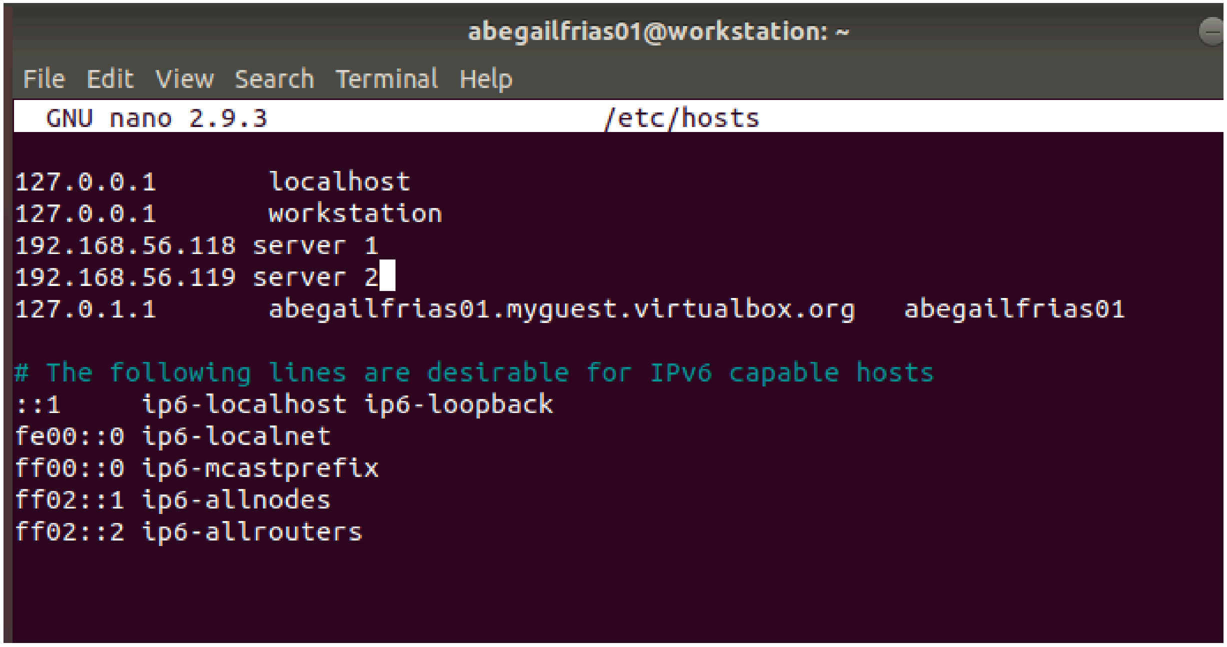


```
abegailfrias01@server2:~$ logout
Connection to 192.168.56.119 closed.
abegailfrias01@workstation:~$
```

4. Edit the hosts of the Local Machine by issuing the command *sudo nano /etc/hosts.* Below all texts type the following:

4.1 IP_address server 1 (provide the ip address of server 1 followed by the hostname)

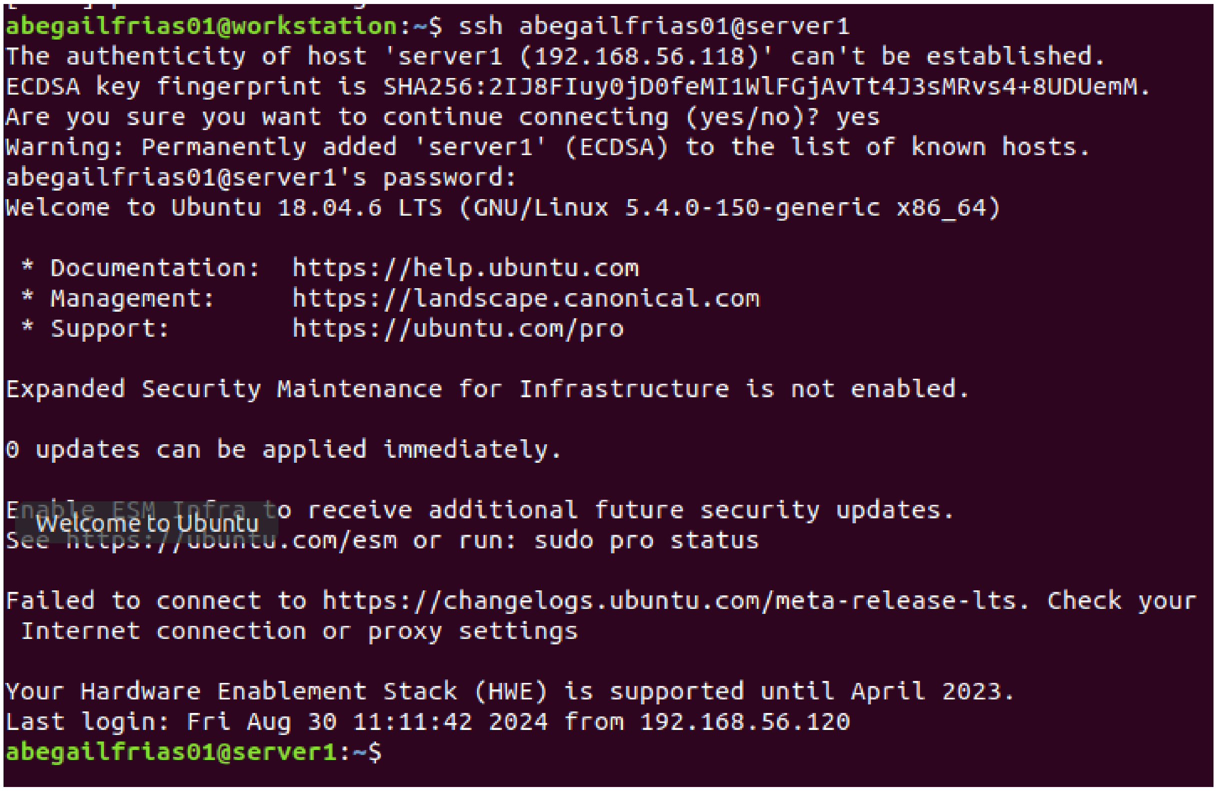
4.2 IP_address server 2 (provide the ip address of server 2 followed by the hostname)


abegailfrias01@workstation: ~
File Edit View Search Terminal Help

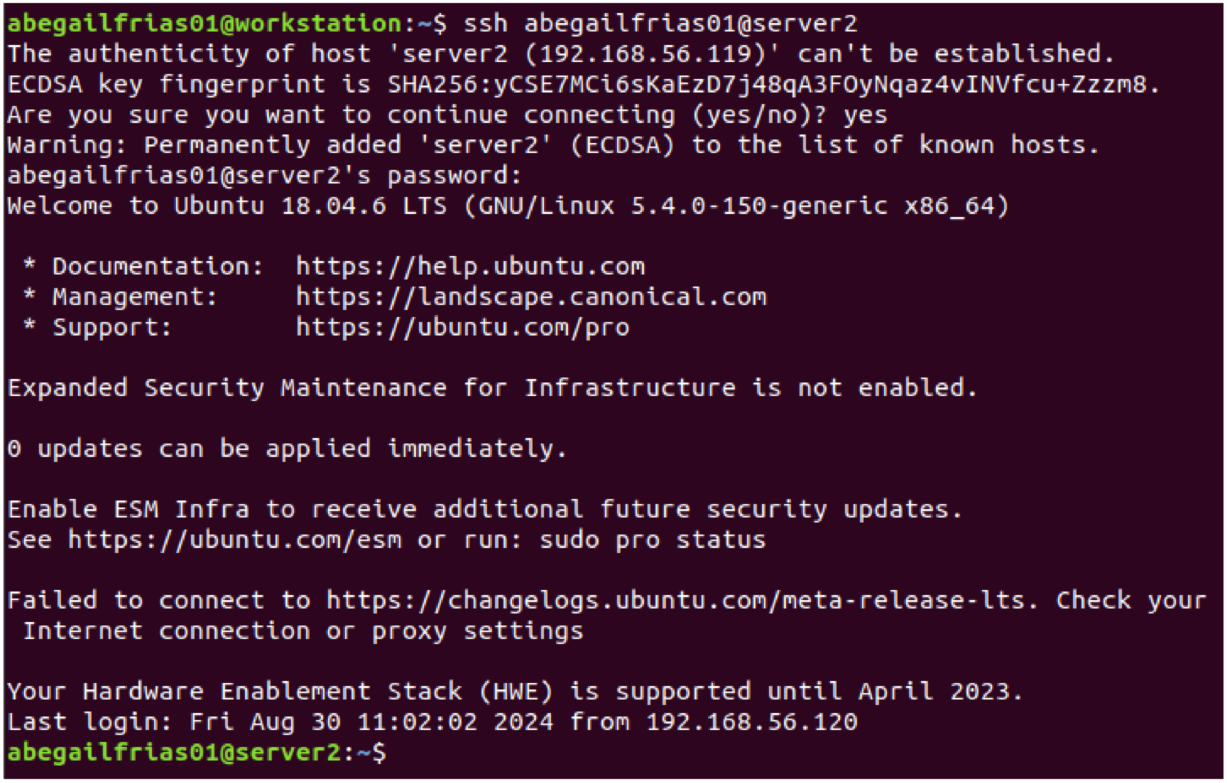
```
  GNU nano 2.9.3                          /etc/hosts

127.0.0.1       localhost
127.0.0.1       workstation
192.168.56.118 server 1
192.168.56.119 server 2
127.0.1.1       abegailfrias01.myguest.virtualbox.org   abegailfrias01

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

4.3 Save the file and exit.

5. On the local machine, verify that you can do the SSH command but this time, use the hostname instead of typing the IP address of the servers. For example, try to do *ssh jvtaylar@server1*. Enter the password when prompted. Verify that you have entered Server 1. Do the same for Server 2.



```
abegailfrias01@workstation:~$ ssh abegailfrias01@server1
The authenticity of host 'server1 (192.168.56.118)' can't be established.
ECDSA key fingerprint is SHA256:2IJ8FIuy0jD0feMI1WlFGjAvTt4J3sMRvs4+8UDUemM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1' (ECDSA) to the list of known hosts.
abegailfrias01@server1's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
 Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 11:11:42 2024 from 192.168.56.120
abegailfrias01@server1:~$
```



```
abegailfrias01@workstation:~$ ssh abegailfrias01@server2
The authenticity of host 'server2 (192.168.56.119)' can't be established.
ECDSA key fingerprint is SHA256:yCSE7MCi6sKaEzD7j48qA3FOyNqaz4vINVfcu+Zzzm8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
abegailfrias01@server2's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
 Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 11:02:02 2024 from 192.168.56.120
abegailfrias01@server2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   - By using the DNS editing the /etc/hosts or config the SSH I can change the ip address with the hostname in my SSH command and it's easier to remember.

2. How secured is SSH?
   - SSH is secured because of its encrypted data, authenticates users in its user key and ensures us in its data integrity. teh security also depends on the proper config and management.