

Name: Magboo, Matt Clemence C.	Date Performed: 08/08/2025
Course/Section: CPE212 - CPE31S2	Date Submitted: 08/08/2025
Instructor: Engr. Robin Valenzuela	Semester and SY: 2025-2026

Activity 1: Configure Network using Virtual Machines

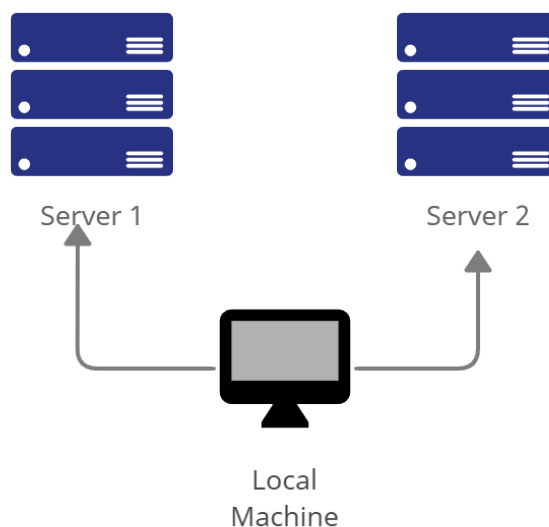
1. Objectives:

- 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:

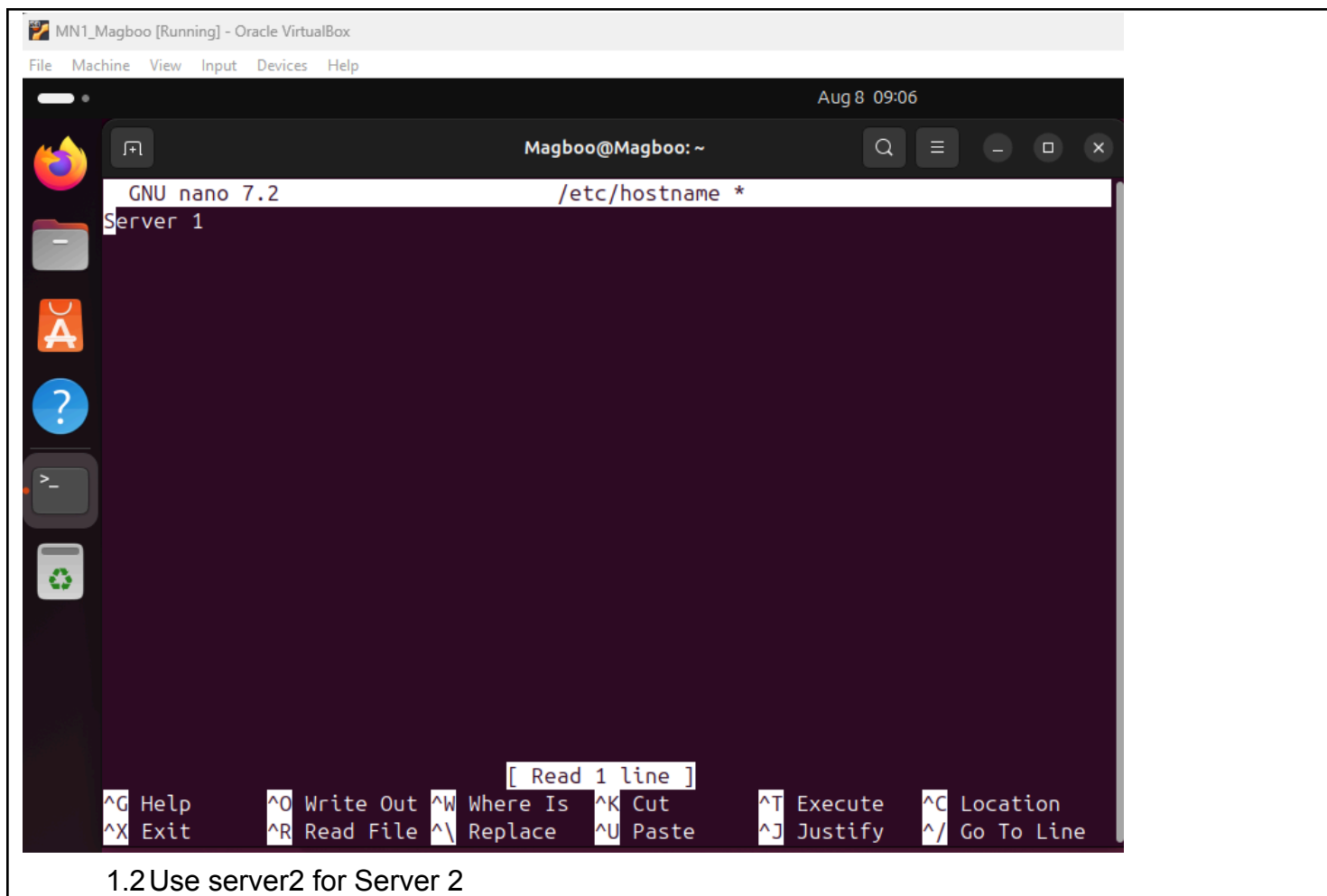
Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and*



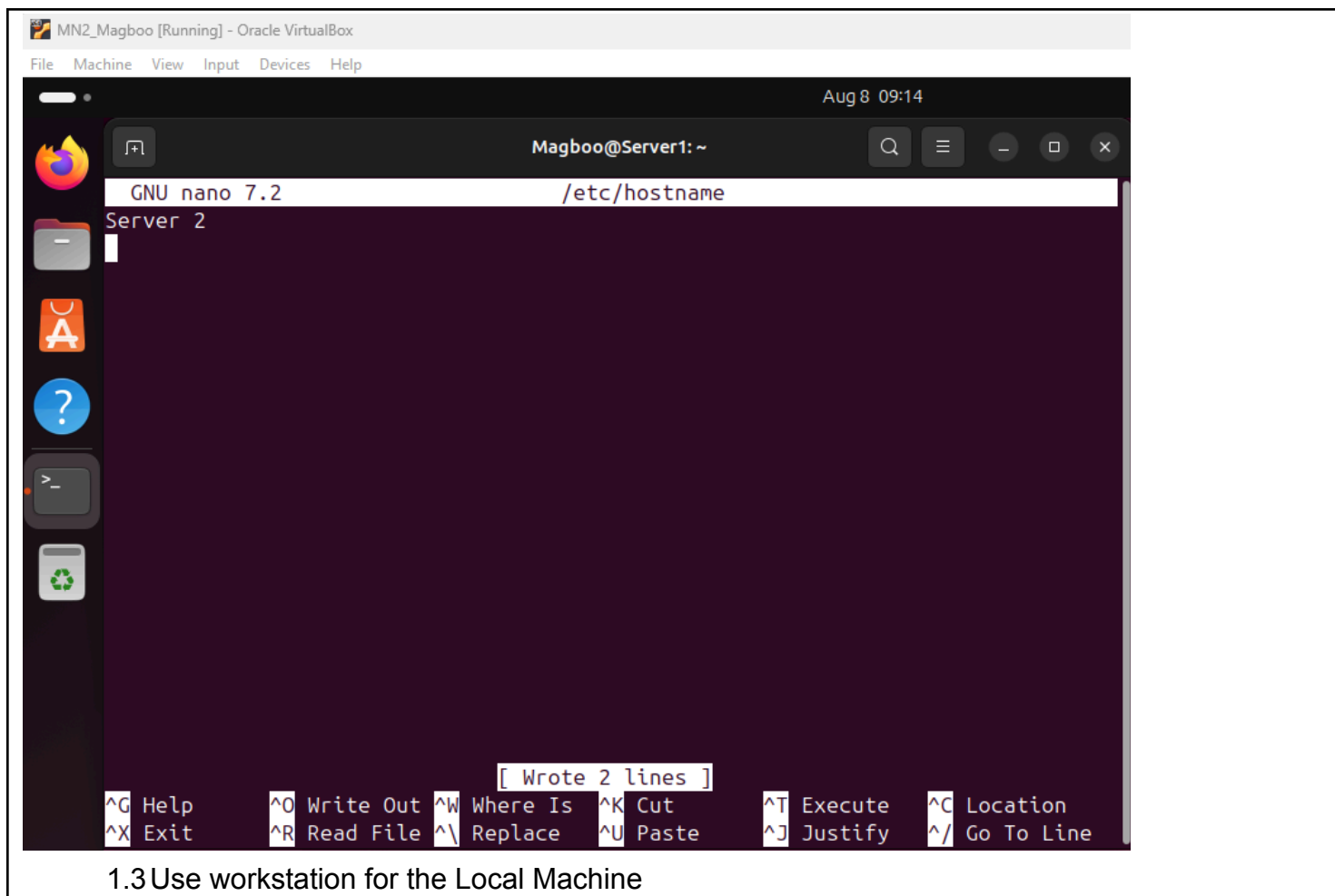
creating snapshots in a virtual machine).

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



1.2 Use server2 for Server 2



Control Node_Magboo [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 8 09:05

Magboo@Magboo: ~

GNU nano 7.2 /etc/hostname *

Local Machine

[Wrote 2 lines]

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^_\ Replace	^U Paste	^J Justify	^/ Go To Line

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

1.5 Type 127.0.0.1 server 1 for Server 1

MN1_Magboo [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 8 09:22

Magboo@LocalMachine: ~

GNU nano 7.2 /etc/hosts *

```
127.0.0.1 localhost
127.0.0.1 Server 1

# 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
```

[Wrote 9 lines]

^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute	^C Location
^X Exit	^R Read File	^_\ Replace	^U Paste	^J Justify	^/ Go To Line

1.6 Type 127.0.0.1 server 2 for Server 2

MN2_Magboo [Running] - Oracle VirtualBox

FileMachineViewInputDevicesHelp

Aug 8 09:23

Magboo@Server1: ~

GNU nano 7.2/etc/hosts

127.0.0.1 localhost
127.0.0.1 Server 2

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

[Wrote 9 lines]

^G Help

^O Write Out

^W Where Is

^K Cut

^T Execute

^C Location

^X Exit

^R Read File

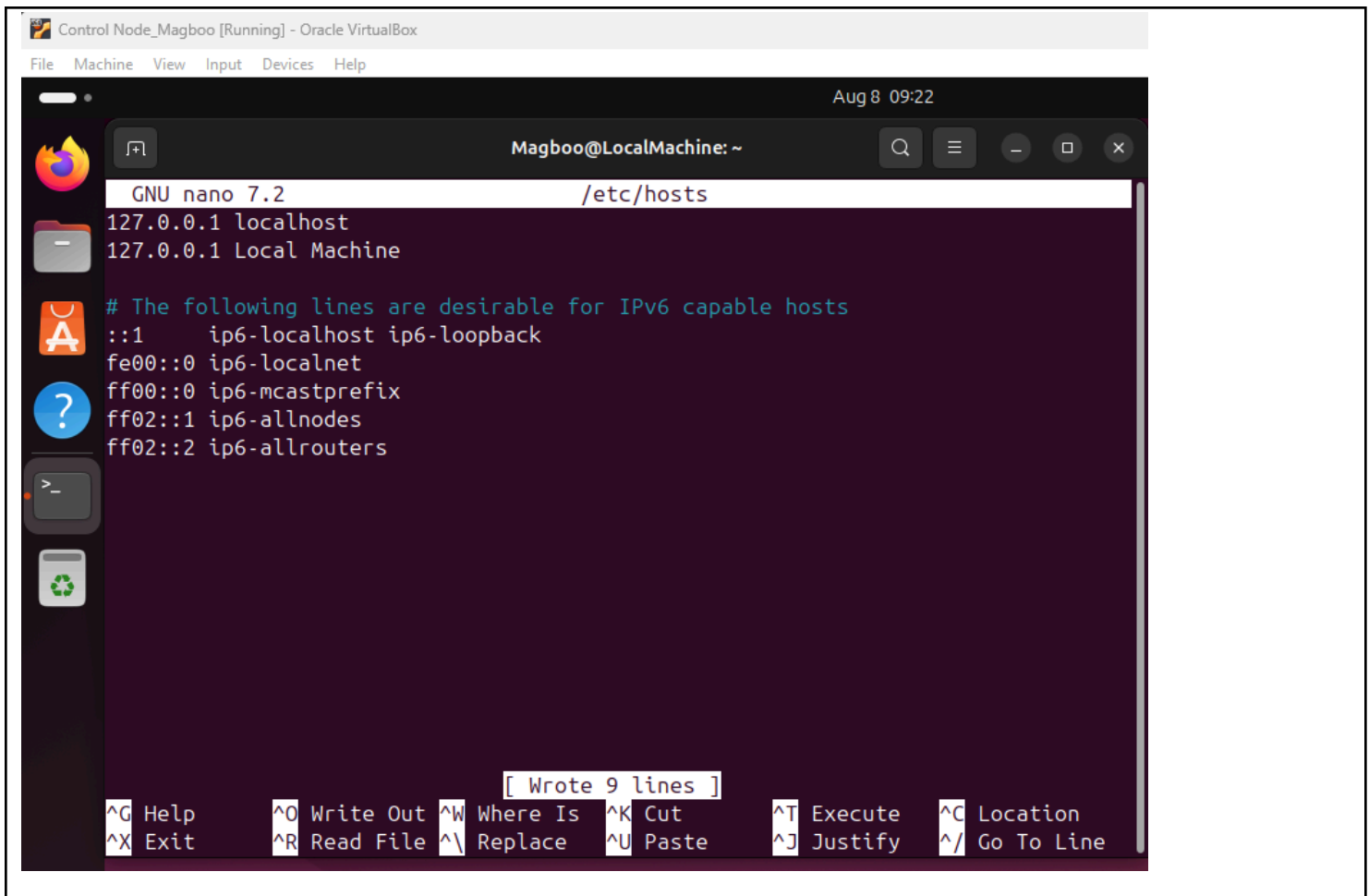
^_ Replace

^U Paste

^J Justify

^_ Go To Line

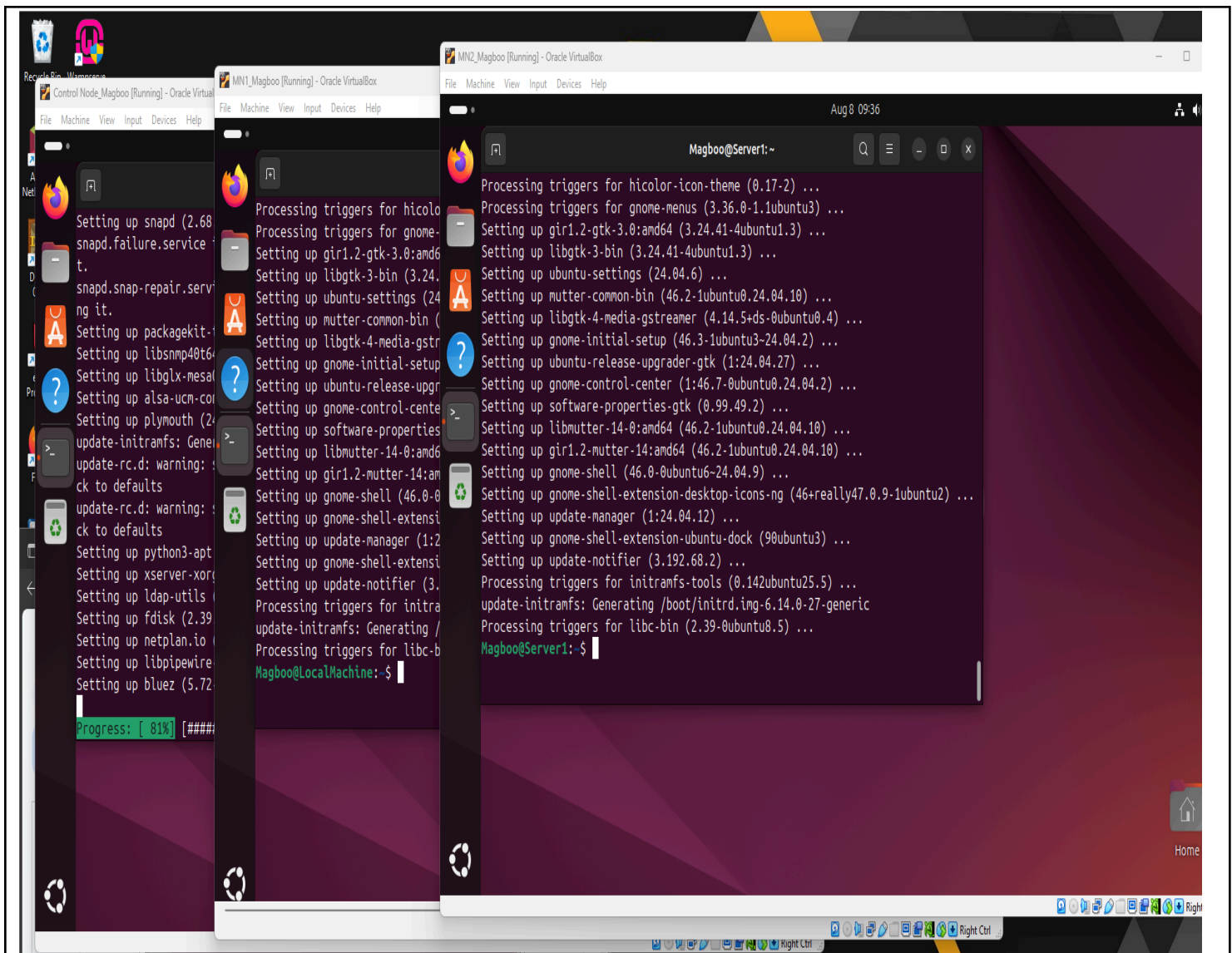
1.7 Type 127.0.0.1 workstation for the Local Machine



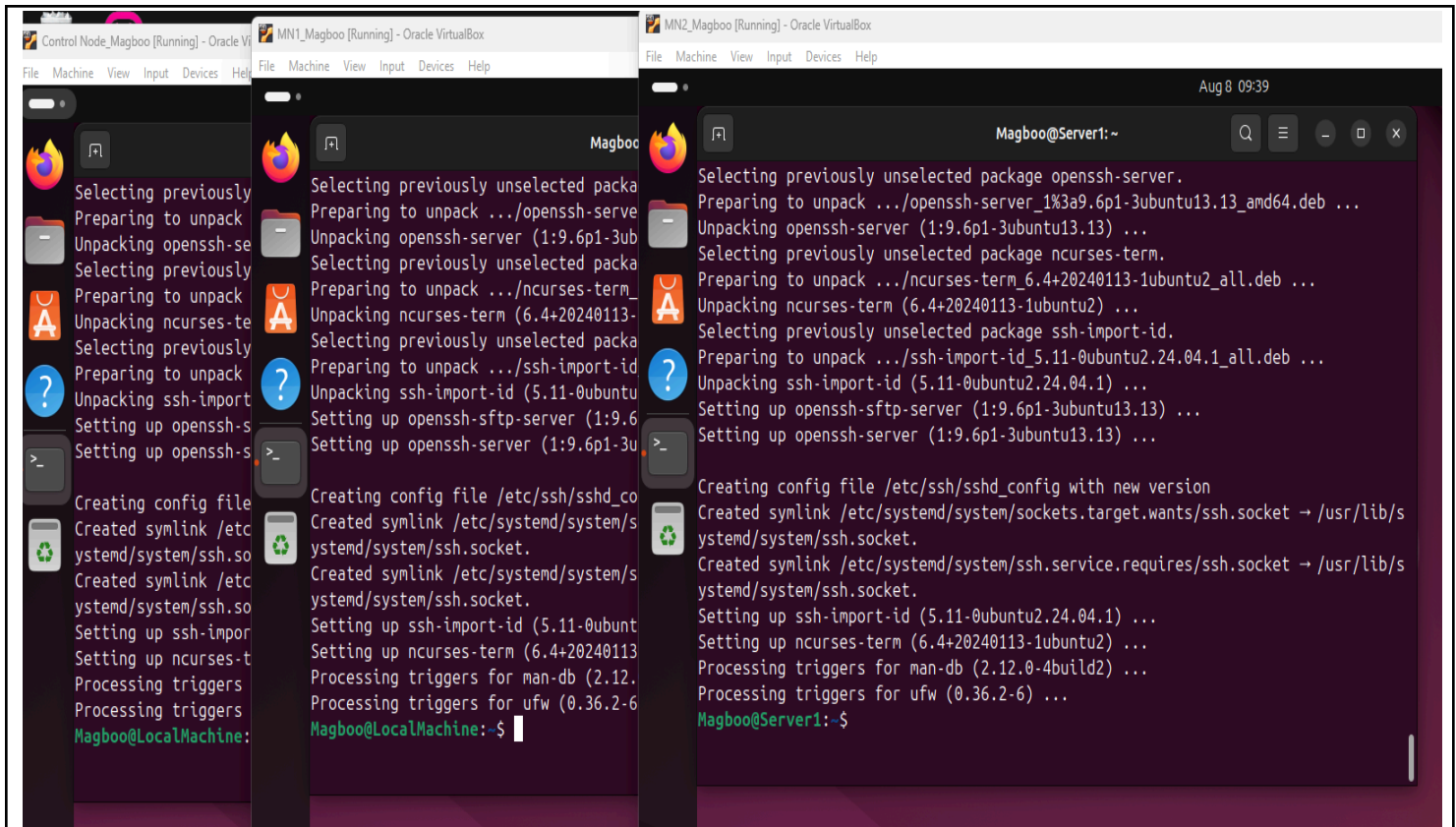
```
Control Node_Magboo [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 8 09:22
Magboo@LocalMachine: ~
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.0.1 Local Machine
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
[ Wrote 9 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

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.



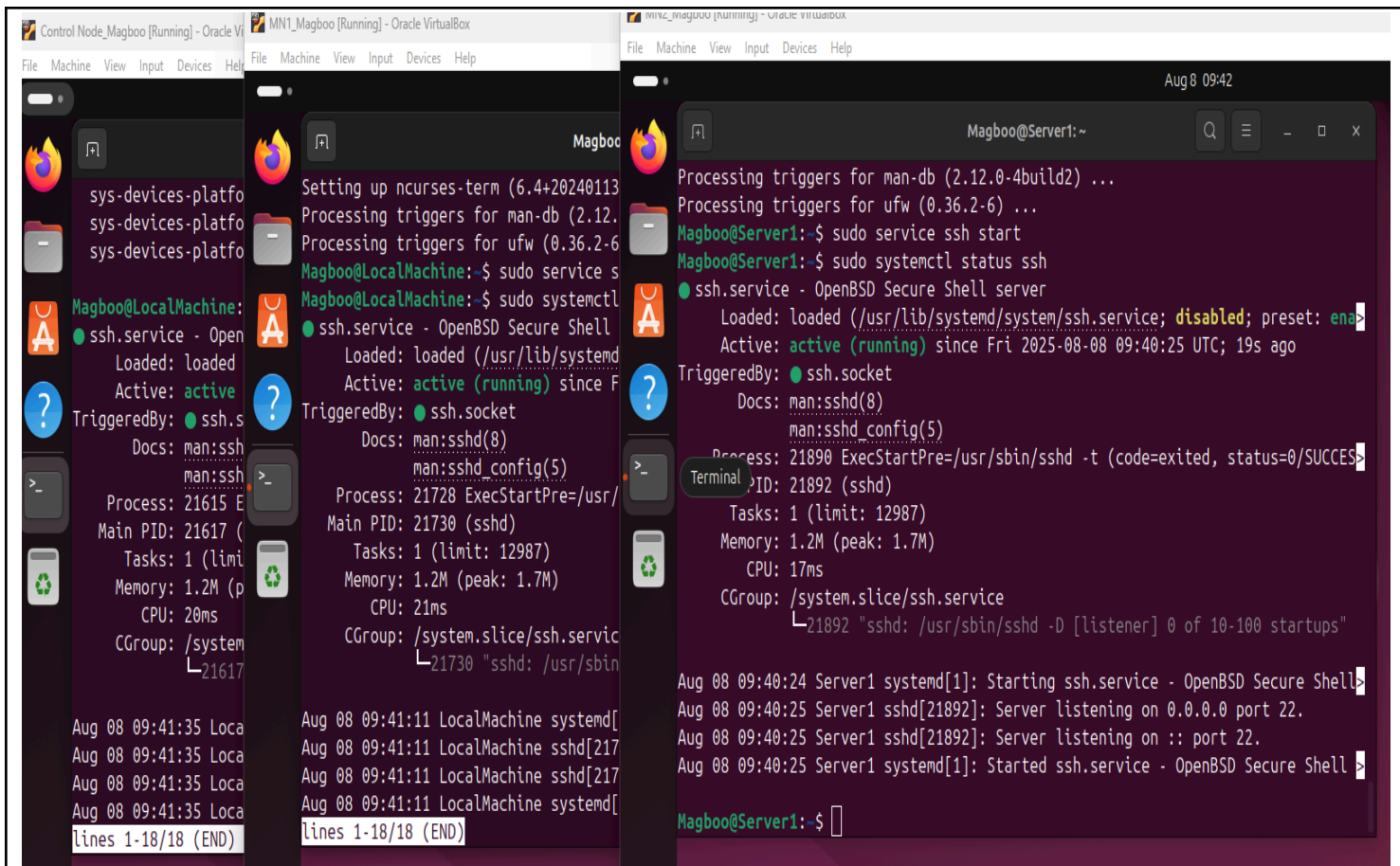
2. Install the SSH server using the command ***sudo apt install openssh-server***.



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*



```
Control Node_Magboo [Running] - Oracle VM
File Machine View Input Devices Help
Magboo
sys-devices-platfo
sys-devices-platfo
sys-devices-platfo
Magboo@LocalMachine:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: active (running) since Fri 2025-08-08 09:40:25 UTC; 19s ago
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 21615 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 21617 (sshd)
     Tasks: 1 (limit: 12987)
    Memory: 1.2M (peak: 1.7M)
       CPU: 20ms
      CGroup: /system.slice/ssh.service
              └─21617 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 08 09:41:35 LocalMachine systemd[1]: Starting ssh.service - OpenBSD Secure Shell server:
Aug 08 09:41:35 LocalMachine sshd[21617]: Server listening on 0.0.0.0 port 22.
Aug 08 09:41:35 LocalMachine sshd[21617]: Server listening on :: port 22.
Aug 08 09:41:35 LocalMachine systemd[1]: Started ssh.service - OpenBSD Secure Shell server:
lines 1-18/18 (END)

MN1_Magboo [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Magboo
Setting up ncurses-term (6.4+20240113) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for ufw (0.36.2-6) ...
Magboo@LocalMachine:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: active (running) since Fri 2025-08-08 09:40:25 UTC; 19s ago
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 21728 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 21730 (sshd)
     Tasks: 1 (limit: 12987)
    Memory: 1.2M (peak: 1.7M)
       CPU: 21ms
      CGroup: /system.slice/ssh.service
              └─21730 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 08 09:41:11 LocalMachine systemd[1]: Starting ssh.service - OpenBSD Secure Shell server:
Aug 08 09:41:11 LocalMachine sshd[21730]: Server listening on 0.0.0.0 port 22.
Aug 08 09:41:11 LocalMachine sshd[21730]: Server listening on :: port 22.
Aug 08 09:41:11 LocalMachine systemd[1]: Started ssh.service - OpenBSD Secure Shell server:
lines 1-18/18 (END)

mn1c_magboo [Running] - Oracle VM
File Machine View Input Devices Help
Magboo@Server1:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: active (running) since Fri 2025-08-08 09:40:25 UTC; 19s ago
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 21890 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 21892 (sshd)
     Tasks: 1 (limit: 12987)
    Memory: 1.2M (peak: 1.7M)
       CPU: 17ms
      CGroup: /system.slice/ssh.service
              └─21892 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

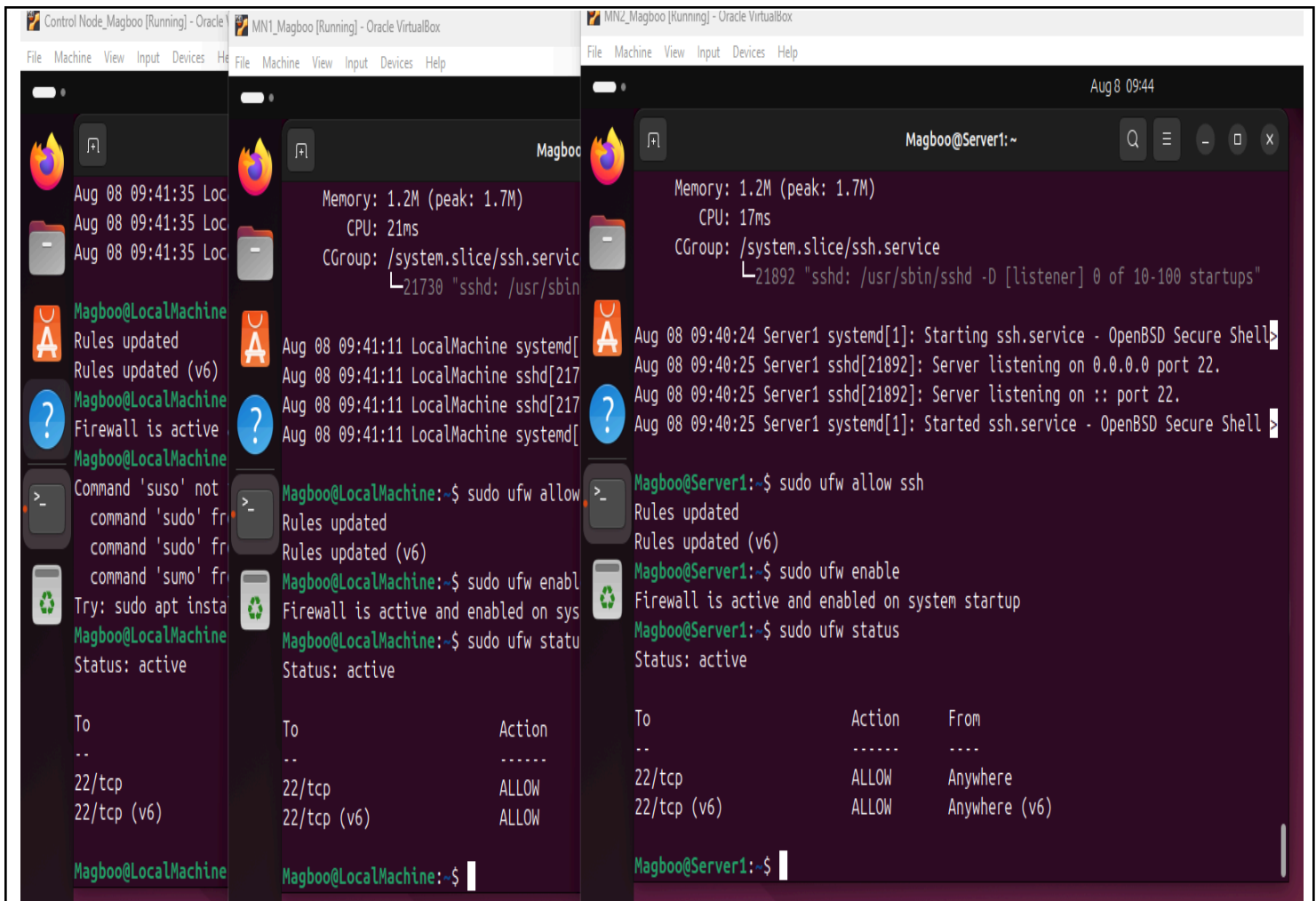
Aug 08 09:40:24 Server1 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server:
Aug 08 09:40:25 Server1 sshd[21892]: Server listening on 0.0.0.0 port 22.
Aug 08 09:40:25 Server1 sshd[21892]: Server listening on :: port 22.
Aug 08 09:40:25 Server1 systemd[1]: Started ssh.service - OpenBSD Secure Shell server:
Magboo@Server1:~$
```

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

4.1 *sudo ufw allow ssh*

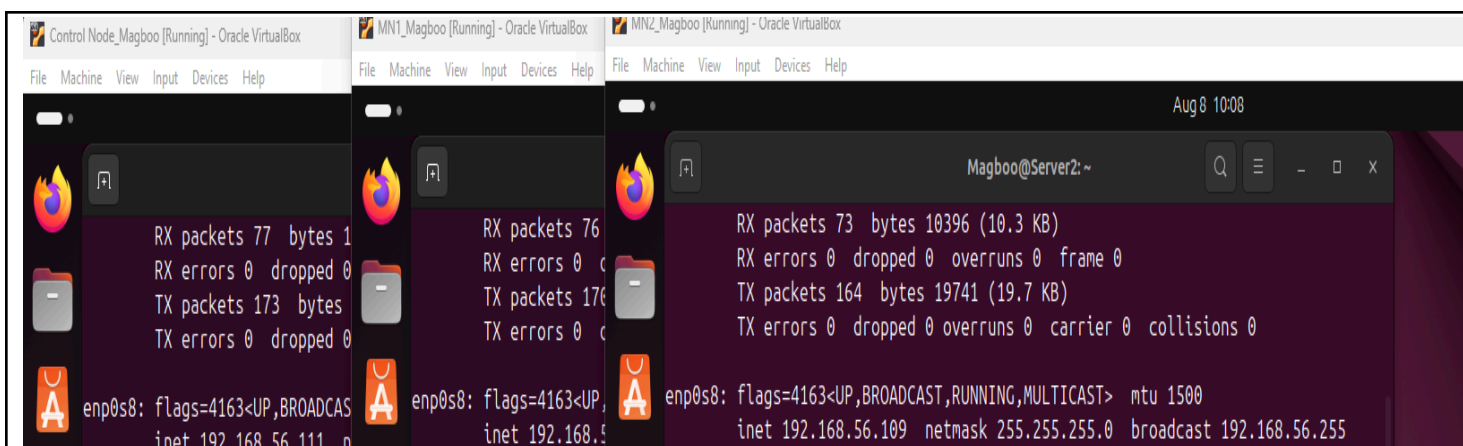
4.2 *sudo ufw enable*

4.3 *sudo ufw status*



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

- 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.
 - Server 1 IP address: 192.168.56.111
 - Server 2 IP address: 192.168.56.110
 - Server 3 IP address: 192.168.56.109



2. Make sure that they can ping each other.

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

```
Magboo@LocalMachine:~$ ping 192.168.56.110
PING 192.168.56.110 (192.168.56.110) 56(84) bytes of data.
64 bytes from 192.168.56.110: icmp_seq=1 ttl=64 time=3.06 ms
ping: Warning: time of day goes back (-1 s), taking countermeasures
64 bytes from 192.168.56.110: icmp_seq=2 ttl=64 time=0.550 ms
64 bytes from 192.168.56.110: icmp_seq=3 ttl=64 time=1.56 ms
64 bytes from 192.168.56.110: icmp_seq=4 ttl=64 time=0.704 ms
^C
--- 192.168.56.110 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3101ms
rtt min/avg/max/mdev = 0.550/1.467/3.055/0.994 ms
```

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

```
Magboo@LocalMachine:~$ ping 192.168.56.109
PING 192.168.56.109 (192.168.56.109) 56(84) bytes of data.
64 bytes from 192.168.56.109: icmp_seq=1 ttl=64 time=0.483 ms
64 bytes from 192.168.56.109: icmp_seq=2 ttl=64 time=0.228 ms
64 bytes from 192.168.56.109: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 192.168.56.109: icmp_seq=4 ttl=64 time=0.076 ms
ping: Warning: time of day goes back (-1 s), taking countermeasures
64 bytes from 192.168.56.109: icmp_seq=5 ttl=64 time=0.510 ms
64 bytes from 192.168.56.109: icmp_seq=6 ttl=64 time=0.700 ms
64 bytes from 192.168.56.109: icmp_seq=7 ttl=64 time=2.20 ms
^C
--- 192.168.56.109 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6133ms
rtt min/avg/max/mdev = 0.028/0.604/2.203/0.690 ms
```

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

```
Magboo@Server1:~$ ping 192.168.56.109
PING 192.168.56.109 (192.168.56.109) 56(84) bytes of data.
64 bytes from 192.168.56.109: icmp_seq=1 ttl=64 time=0.998 ms
64 bytes from 192.168.56.109: icmp_seq=2 ttl=64 time=0.520 ms
64 bytes from 192.168.56.109: icmp_seq=3 ttl=64 time=1.02 ms
^C
--- 192.168.56.109 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2236ms
rtt min/avg/max/mdev = 0.520/0.844/1.015/0.229 ms
```

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 jvtaylor@192.168.56.120*
 - 1.2 Enter the password for server 1 when prompted
 - 1.3 Verify that you are in server 1. The user should be in this format user@server1. For example, *jvtaylor@server1*







Control Node_Magboo [Running] - Oracle VirtualBox

FileMachineViewInputDevicesHelp

Aug 8 10:15

Magboo@Server1: ~





```
Magboo@LocalMachine:~$ ssh Magboo@192.168.56.110
The authenticity of host '192.168.56.110 (192.168.56.110)' can't be established.
ED25519 key fingerprint is SHA256:r/DWcH5rjQ1BZjxVPAj1myNwc0dfycRR6wisGdz+F8k.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.110' (ED25519) to the list of known hosts.
Magboo@192.168.56.110's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

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.
```

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

3. Do the same for Server 2.

```
Magboo@LocalMachine:~$ ssh Magboo@192.168.56.109
The authenticity of host '192.168.56.109 (192.168.56.109)' can't be established.
ED25519 key fingerprint is SHA256:r/DWcH5rjQ1BZjxVPAj1myNwc0dfycRR6wisGdz+F8k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.109' (ED25519) to the list of known hosts.
Magboo@192.168.56.109's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

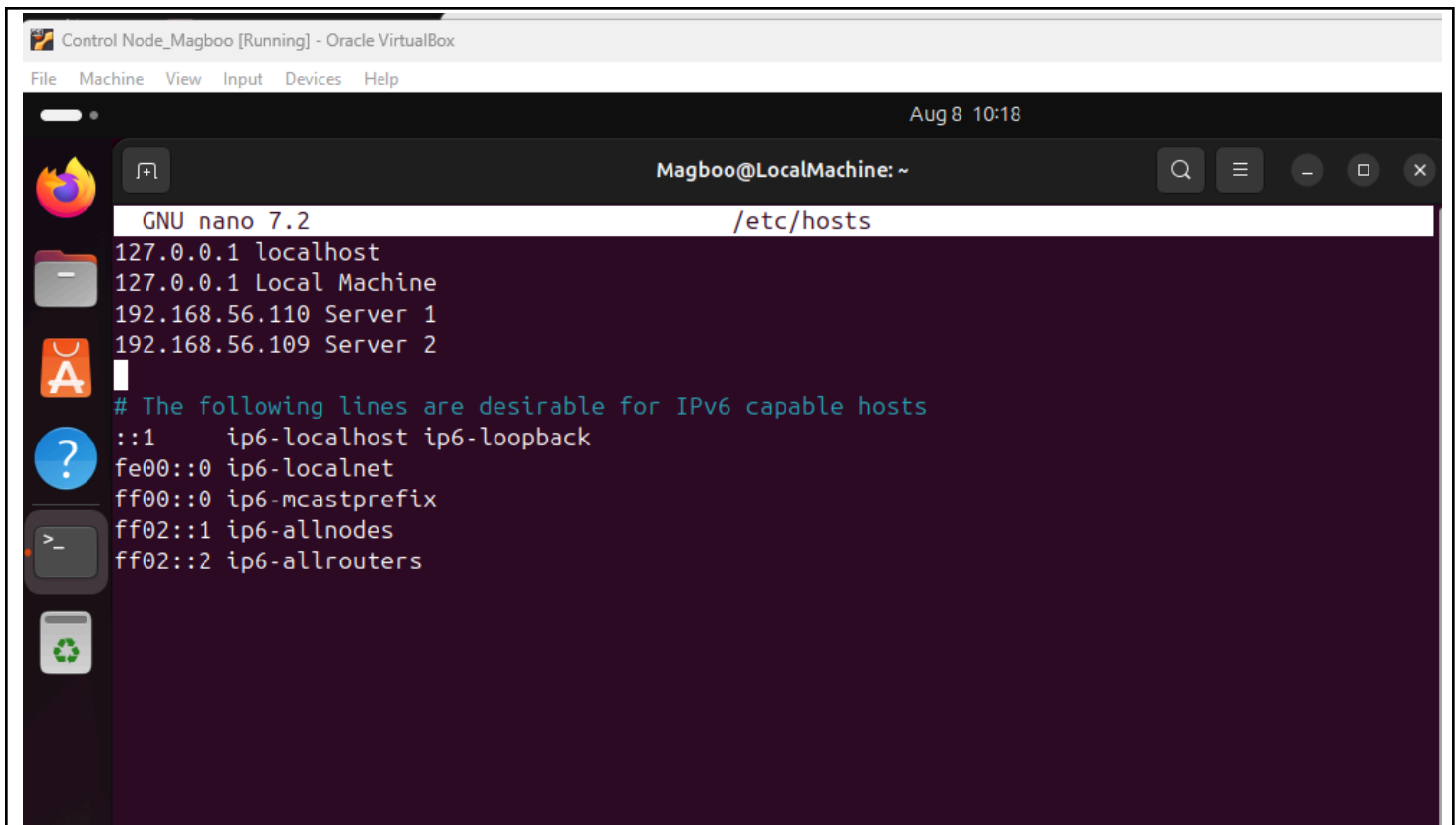
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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.

Magboo@Server2:~$
```

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)



Control Node_Magboo [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 8 10:18

Magboo@LocalMachine: ~

GNU nano 7.2 /etc/hosts

```
127.0.0.1 localhost
127.0.0.1 Local Machine
192.168.56.110 Server 1
192.168.56.109 Server 2
# 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 jvtaylor@server1**. Enter the password when prompted. Verify that you have entered Server 1. Do the same for Server 2.

Aug 8 10:20

Magboo@Server1: ~

Magboo@LocalMachine:~\$ ssh Magboo@Server 1

Magboo@server's password:

bash: line 1: 1: command not found

Magboo@LocalMachine:~\$ sudo nano /etc/hosts

[sudo] password for Magboo:

Magboo@LocalMachine:~\$ ssh Magboo@Server 1

ssh: Could not resolve hostname server: Temporary failure in name resolution

Magboo@LocalMachine:~\$ ssh Magboo@Server1

The authenticity of host 'server1 (192.168.56.110)' can't be established.

ED25519 key fingerprint is SHA256:r/DWcH5rjQ1BZjxVPAj1myNwc0dfycRR6wisGdz+F8k.

This host key is known by the following other names/addresses:

~/.ssh/known_hosts:1: [hashed name]

~/.ssh/known_hosts:4: [hashed name]

~/.ssh/known_hosts:5: [hashed name]

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added 'server1' (ED25519) to the list of known hosts.

Magboo@server1's password:

Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic x86_64)

* Documentation: <https://help.ubuntu.com>

* Management: <https://landscape.canonical.com>

* Support: <https://ubuntu.com/pro>

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.

See <https://ubuntu.com/esm> or run: `sudo pro status`

Last login: Fri Aug 8 10:15:34 2025 from 192.168.56.111

```
Magboo@LocalMachine:~$ ssh Magboo@Server2
The authenticity of host 'server2 (192.168.56.109)' can't be established.
ED25519 key fingerprint is SHA256:r/DWcH5rjQ1BZjxVPAj1myNwc0dfycRR6wisGdz+F8k.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server2' (ED25519) to the list of known hosts.
Magboo@server2's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

Last login: Fri Aug  8 10:14:26 2025 from 192.168.56.111
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
because on the hosts we applied the ip addresses and the hostnames of the server1 and server2
2. How secured is SSH?
it is very secure it has built in encryption that would make it very hard to get the password from the outside.

