Name: Reyes, Alexzander J.	**Date Performed: 08/08/2025**
Course/Section: CPE212-CPE31S2	**Date Submitted: 08/08/2025**
Instructor: Engr. Valenzuela	**Semester and SY: 1st Sem & 2025-2026**

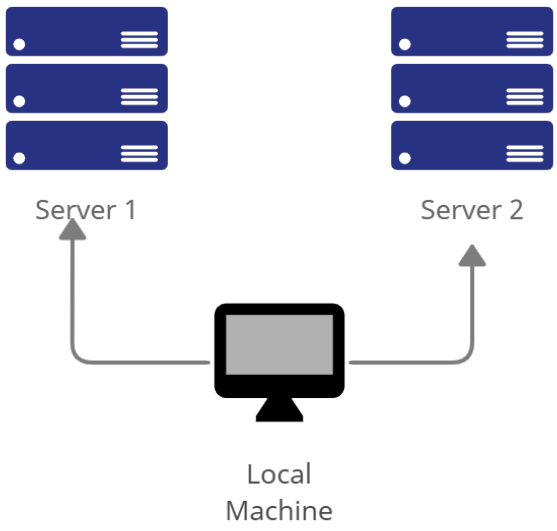
Activity 1: Configure Network using Virtual Machines

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*).

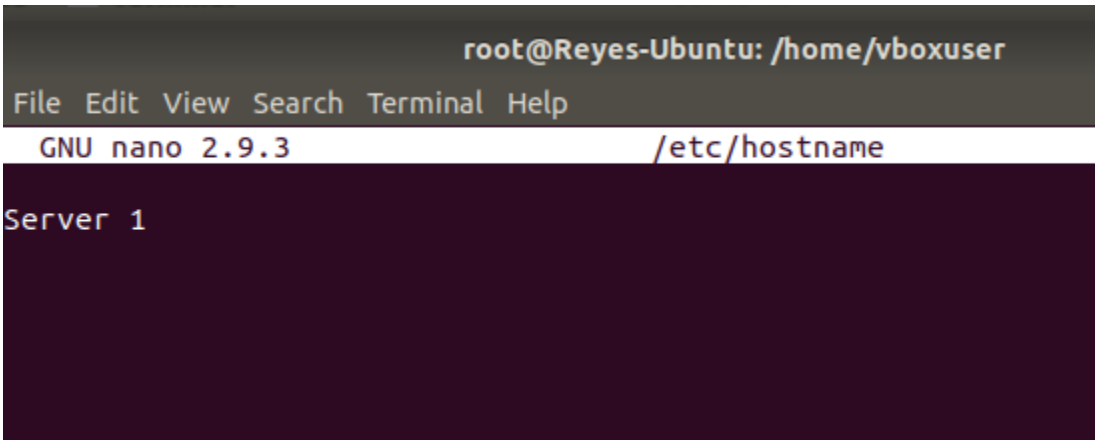


Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

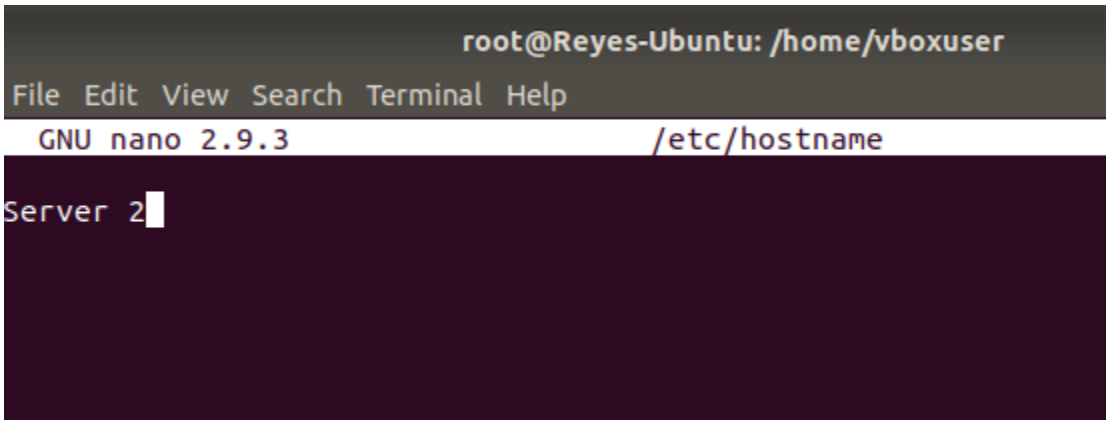
1. Change the hostname using the command *sudo nano /etc/hostname*
   1.1 Use server1 for Server 1
   1.2 Use server2 for Server 2
   1.3 Use workstation for the Local Machine

TASK 1

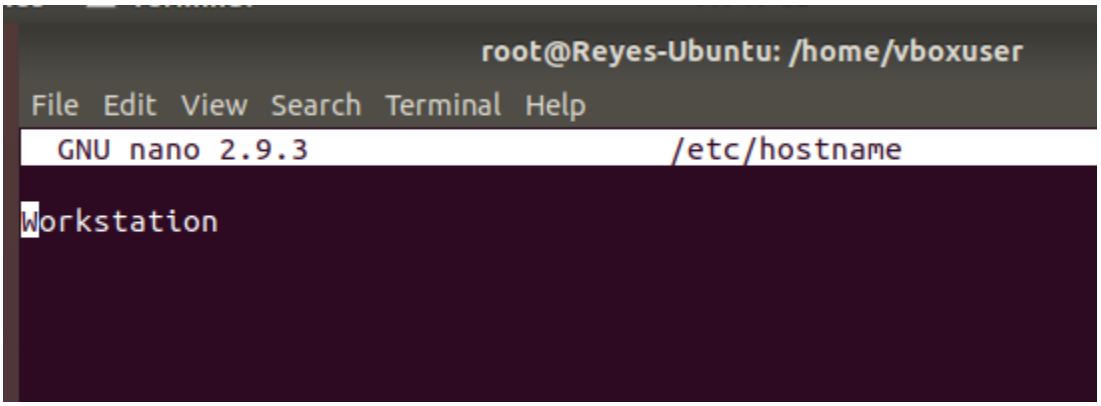
Server 1



Server 2

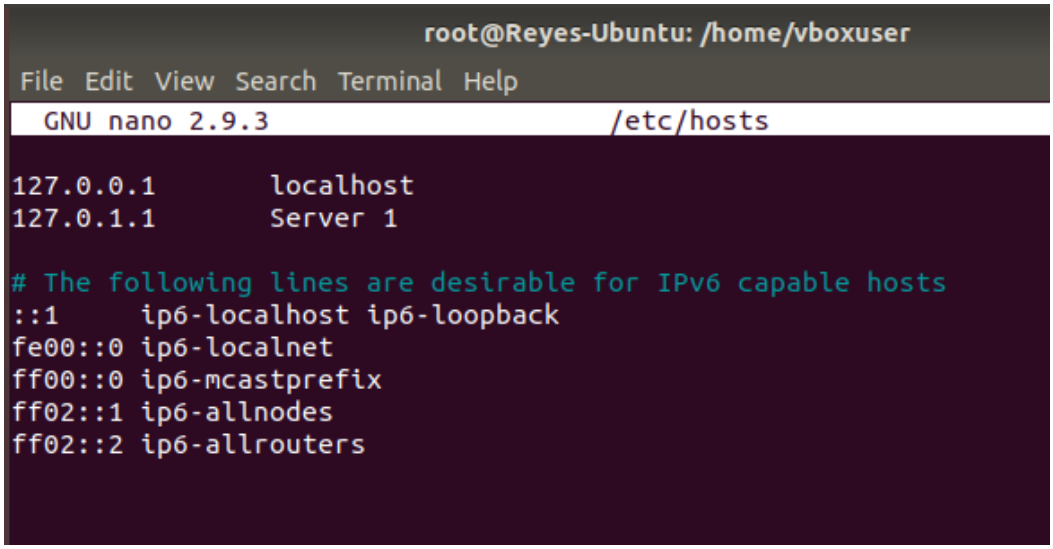


Local Machine

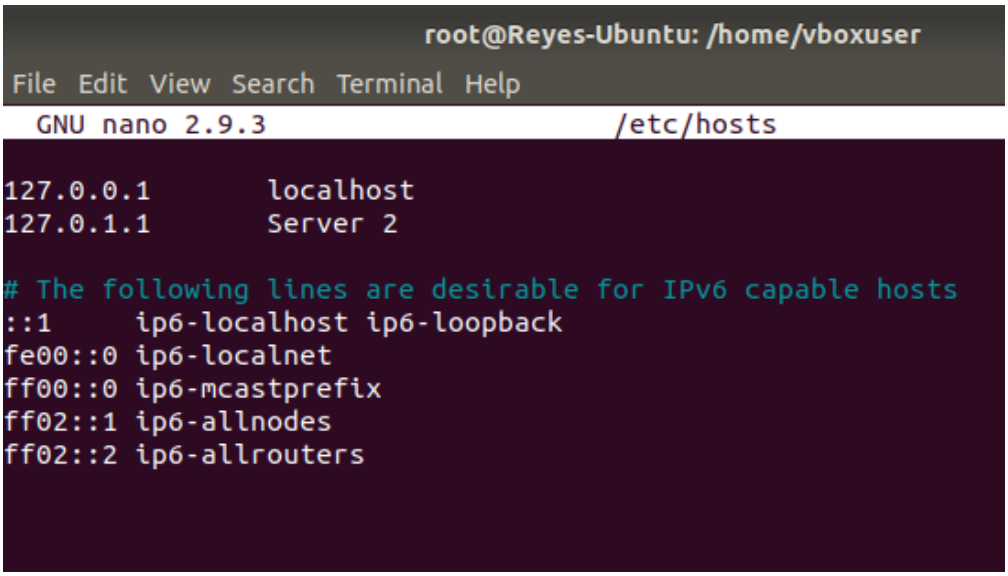


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.
   2.1 Type 127.0.0.1 server 1 for Server 1
   2.2 Type 127.0.0.1 server 2 for Server 2
   2.3 Type 127.0.0.1 workstation for the Local Machine

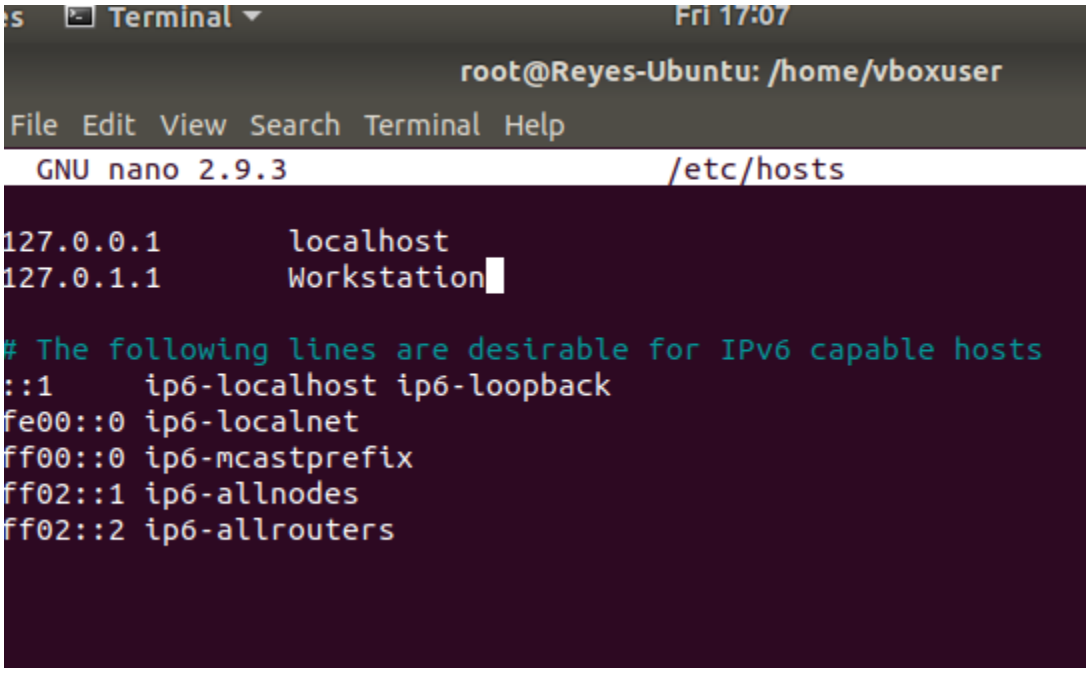
Server 1



Server 2



Local Machine



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.

sudo apt update

Server 1

```
root@Reyes-Ubuntu:/home/vboxuser# 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
687 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Server 2

```
root@Reyes-Ubuntu:/home/vboxuser# 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
687 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Local Machine

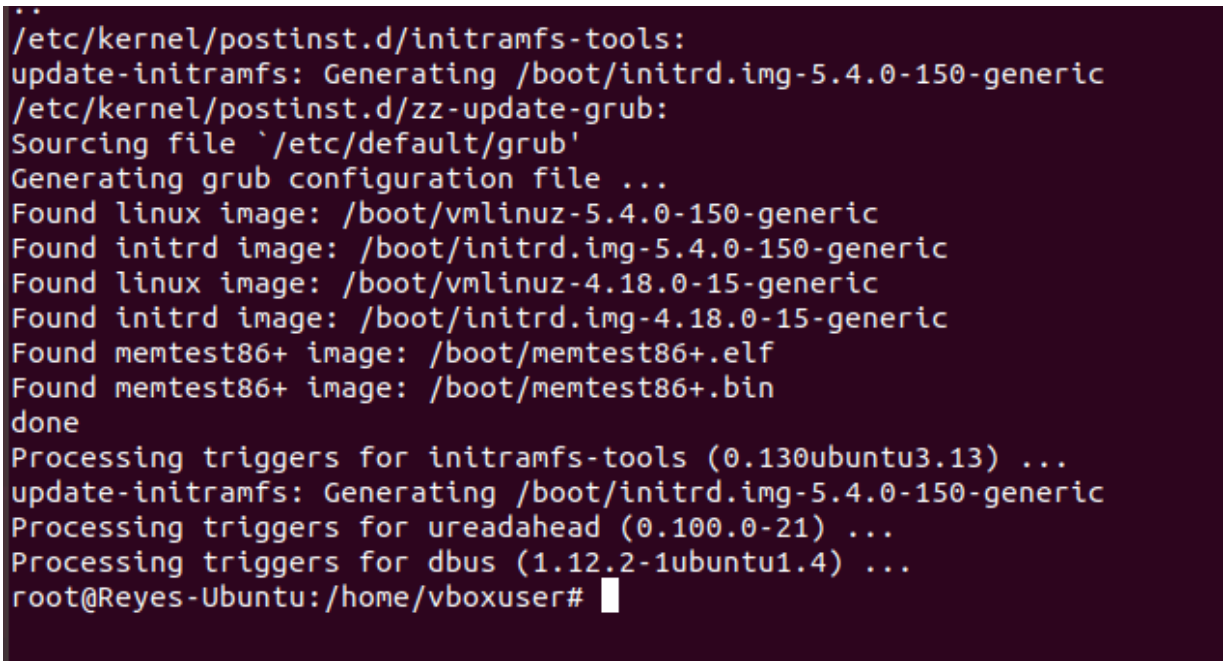
```
root@Reyes-Ubuntu:/home/vboxuser# sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
687 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

sudo apt upgrade

Server 1

Server 2

Local Host



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*
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*

Server 1

```
root@Reyes-Ubuntu:/home/vboxuser# sudo apt install openssh-server
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.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:hNaavu2wP/aIqSaEyT+F2+OqpSPReQtNVnLaOfP+Mw4 root@Reyes-Ubuntu (ED255
19)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.serv
ice.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/
systemd/system/ssh.service.
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.2) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
root@Reyes-Ubuntu:/home/vboxuser# sudo service ssh start
root@Reyes-Ubuntu:/home/vboxuser# 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 2025-08-08 17:44:11 +08; 1min 38s ago
 Main PID: 20015 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─20015 /usr/sbin/sshd -D

Aug 08 17:44:11 Reyes-Ubuntu systemd[1]: Starting OpenBSD Secure Shell server..
Aug 08 17:44:11 Reyes-Ubuntu sshd[20015]: Server listening on 0.0.0.0 port 22.
Aug 08 17:44:11 Reyes-Ubuntu sshd[20015]: Server listening on :: port 22.
Aug 08 17:44:11 Reyes-Ubuntu systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw enable
Firewall is active and enabled on system startup
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw status
Status: active

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

Server 2

```
root@Reyes-Ubuntu:/home/vboxuser# sudo apt install openssh-server
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.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/
systemd/system/ssh.service.
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.2) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
root@Reyes-Ubuntu:/home/vboxuser# sudo service ssh start
root@Reyes-Ubuntu:/home/vboxuser# 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 2025-08-08 17:51:23 +08; 21s ago
 Main PID: 19890 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─19890 /usr/sbin/sshd -D

Aug 08 17:51:23 Reyes-Ubuntu systemd[1]: Starting OpenBSD Secure Shell server..
Aug 08 17:51:23 Reyes-Ubuntu sshd[19890]: Server listening on 0.0.0.0 port 22.
Aug 08 17:51:23 Reyes-Ubuntu sshd[19890]: Server listening on :: port 22.
Aug 08 17:51:23 Reyes-Ubuntu systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw enable
Firewall is active and enabled on system startup
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw status
Status: active

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

Local Host

```
root@Reyes-Ubuntu:/home/vboxuser# sudo apt install openssh-server
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.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

```
256 SHA256:9zGcFT05r/NDlRmxwMk7GuzT7F9LotieGOB+AqQ9UJs root@Reyes-Ubuntu (ECDSA
)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:2s19yvLItkRBsqM49pnBY1KGi25znGWvqlON6kb9/lA root@Reyes-Ubuntu (ED255
19)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.serv
ice.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/
systemd/system/ssh.service.
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.2) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
root@Reyes-Ubuntu:/home/vboxuser# sudo service ssh start
root@Reyes-Ubuntu:/home/vboxuser# 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 2025-08-08 17:37:23 +08; 1min 17s ago
 Main PID: 20987 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─20987 /usr/sbin/sshd -D

Aug 08 17:37:23 Reyes-Ubuntu systemd[1]: Starting OpenBSD Secure Shell server..
Aug 08 17:37:23 Reyes-Ubuntu sshd[20987]: Server listening on 0.0.0.0 port 22.
Aug 08 17:37:23 Reyes-Ubuntu sshd[20987]: Server listening on :: port 22.
Aug 08 17:37:23 Reyes-Ubuntu systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw enable
Firewall is active and enabled on system startup
root@Reyes-Ubuntu:/home/vboxuser# sudo ufw status
Status: active

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

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: 192.168.56.105

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.105  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::b89d:f659:2e49:6f37  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ff:7a:a6  txqueuelen 1000  (Ethernet)
        RX packets 591  bytes 122757 (122.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 157  bytes 21209 (21.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.2 Server 2 IP address: 192.168.56.106

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.106  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::5d54:dedb:e5c:e165  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:55:5e:bf  txqueuelen 1000  (Ethernet)
        RX packets 540  bytes 112953 (112.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161  bytes 21769 (21.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.3 Server 3 IP address: 192.168.56.107

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.107  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::b74a:baae:6b59:6e98  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b7:2f:9b  txqueuelen 1000  (Ethernet)
        RX packets 14  bytes 3992 (3.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62  bytes 7130 (7.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Make sure that they can ping each other.

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

- **Successful**

```
vboxuser@Workstation:~$ ping 192.168.56.105
PING 192.168.56.105 (192.168.56.105) 56(84) bytes of data.
64 bytes from 192.168.56.105: icmp_seq=1 ttl=64 time=0.864 ms
64 bytes from 192.168.56.105: icmp_seq=2 ttl=64 time=0.400 ms
64 bytes from 192.168.56.105: icmp_seq=3 ttl=64 time=0.490 ms
64 bytes from 192.168.56.105: icmp_seq=4 ttl=64 time=0.404 ms
64 bytes from 192.168.56.105: icmp_seq=5 ttl=64 time=0.394 ms
64 bytes from 192.168.56.105: icmp_seq=6 ttl=64 time=0.435 ms
```

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

- **Successful**

```
vboxuser@Workstation:~$ ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=0.783 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=0.381 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=0.392 ms
```

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

- **Successful**

```
root@Reyes-Ubuntu:/home/vboxuser# ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=0.610 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=0.416 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=0.531 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=0.438 ms
64 bytes from 192.168.56.106: icmp_seq=5 ttl=64 time=0.524 ms
```

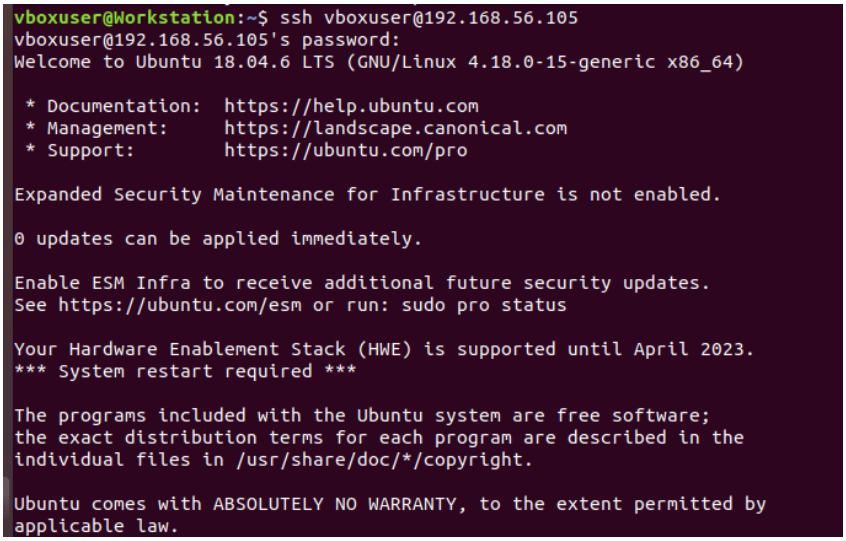
Task 4: Verify SSH connectivity on Server 1, Server 2, and Local Machine.

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

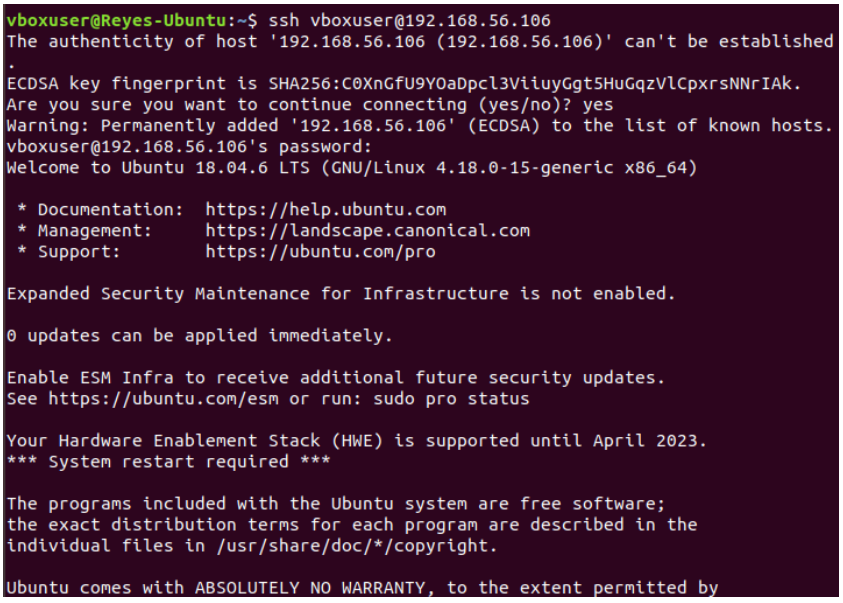
1.1 ssh username@ip_address_server1 for example, *ssh jvtaylar@192.168.56.120*

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, *jvtaylar@server1*



2. Logout of Server 1 by issuing the command *control + D.*
3. Do the same for Server 2.

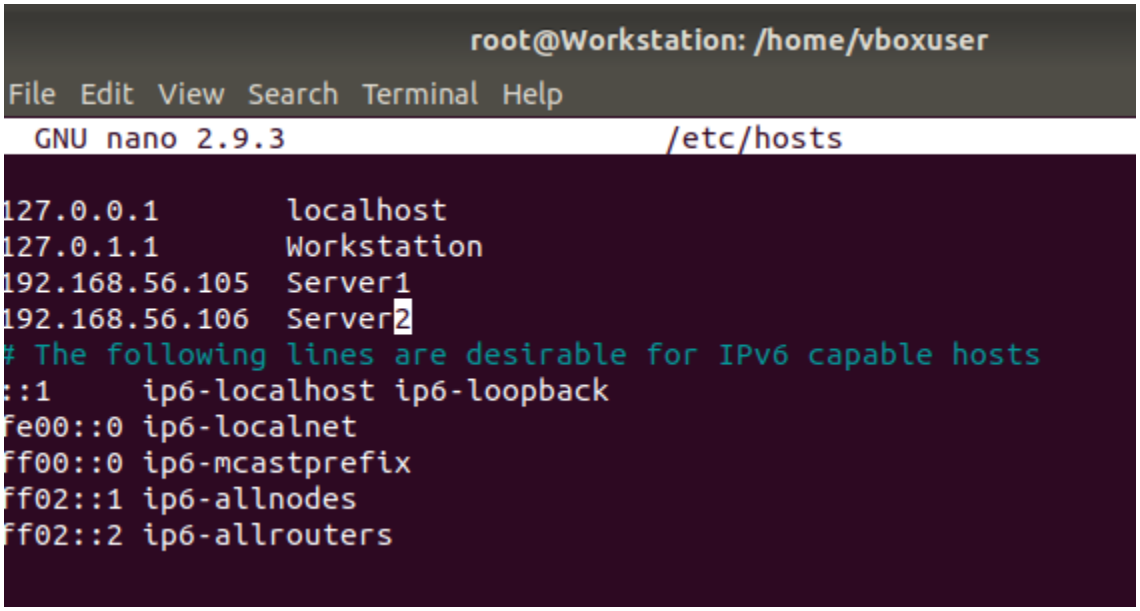


4. Edit the hosts of the Local Machine by issuing the command *sudo nano /etc/hosts.* Below all texts type the following:

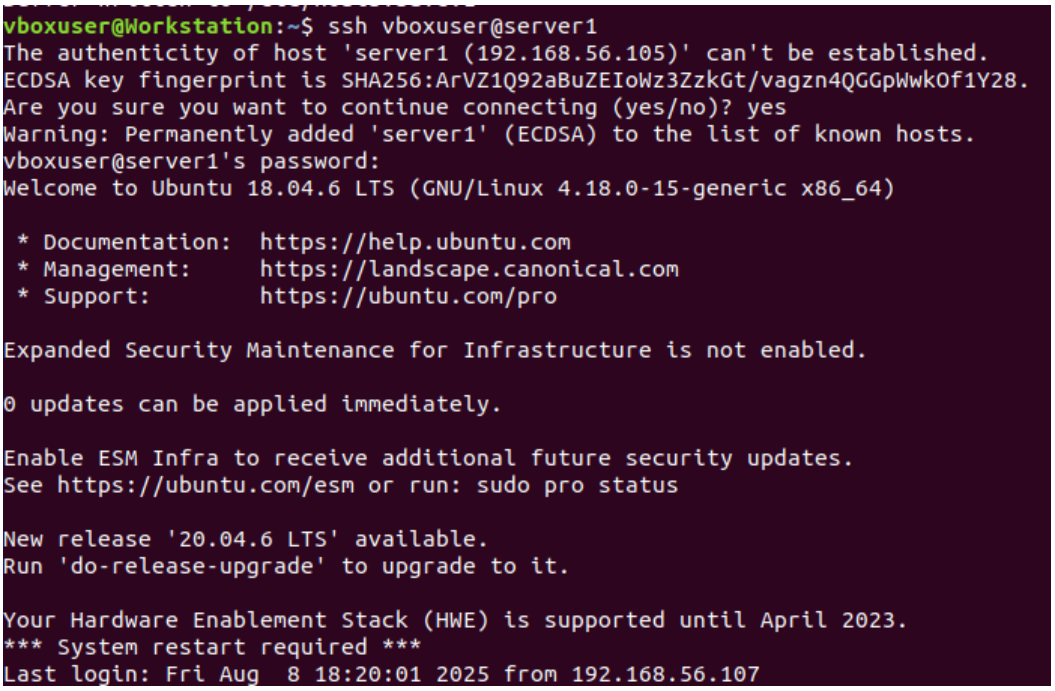
4.1 IP_address server 1 (provide the ip address of server 1 followed by the hostname)

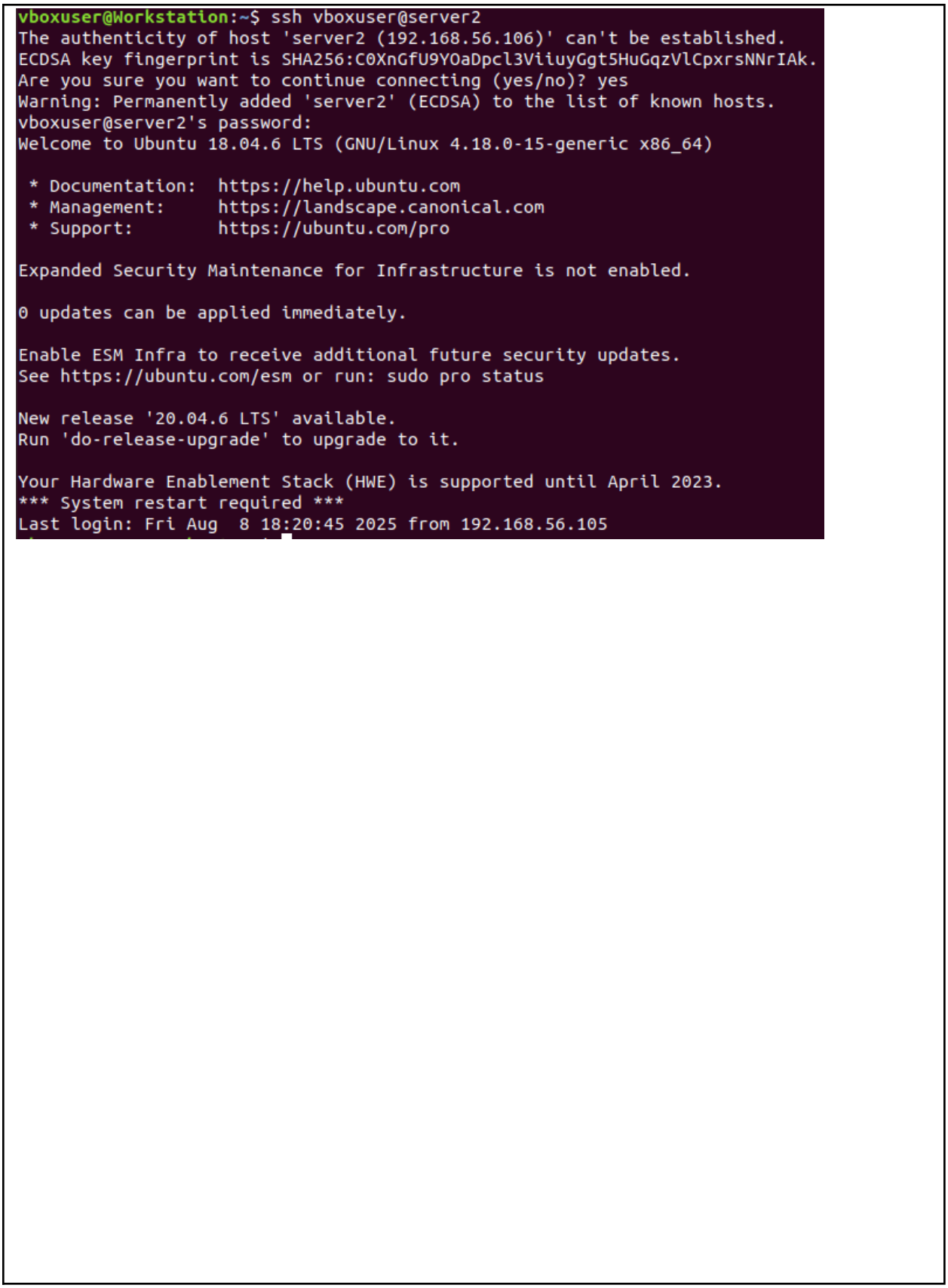
4.2 IP_address server 2 (provide the ip address of server 2 followed by the hostname)

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.




vboxuser@Workstation:~$ ssh vboxuser@server2
The authenticity of host 'server2 (192.168.56.106)' can't be established.
ECDSA key fingerprint is SHA256:C0XnGfU9YOaDpcl3ViiuyGgt5HuGqzVlCpxrsNNrIAk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
vboxuser@server2's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.18.0-15-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
New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Your Hardware Enablement Stack (HWE) is supported until April 2023.
*** System restart required ***
Last login: Fri Aug 8 18:20:45 2025 from 192.168.56.105

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
    - We are able to use the hostname instead of the IP address in SSH commands because of hostname resolution, which maps human-readable names to IP addresses. This can be configured locally using the /etc/hosts file, where specific IP addresses are manually assigned to hostnames. For example, adding a line like 192.168.56.107 server1 allows the system to recognize server1 as the IP address 192.168.56.108. This makes it easier to manage and remember machine names rather than numeric IPs. In larger networks, this is typically handled by a DNS (Domain Name System) server, which performs the same function automatically.
2. How secured is SSH?
    - SSH (Secure Shell) is considered very secure when properly configured, as it encrypts all data transmitted between the client and server, protecting it from interception and tampering. It supports multiple authentication methods, including passwords and public key authentication, with key-based login being more secure and commonly used in production environments. SSH also verifies the identity of the remote system, reducing the risk of man-in-the-middle attacks. Security can be further improved by disabling root login, restricting access via firewalls, changing the default port, and enforcing strong key or password policies.