Name: Erebete, Jan Kenneth F	**Date Performed: 8/8/25**
Course/Section: CPE31S4	**Date Submitted: 8/8/25**
Instructor: Engr. Robin Valenzuela	**Semester and SY:1st sem - 2025-2026**

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

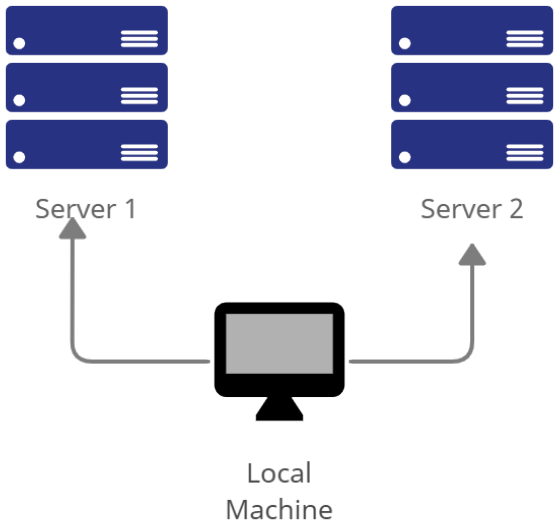
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

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

2. **Discussion:**

Network Topology:

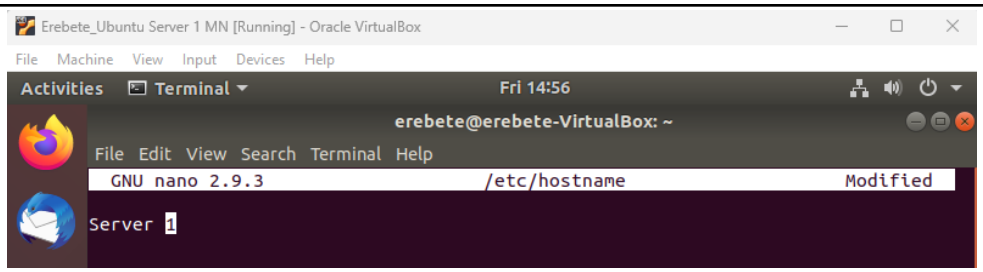
Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine*).



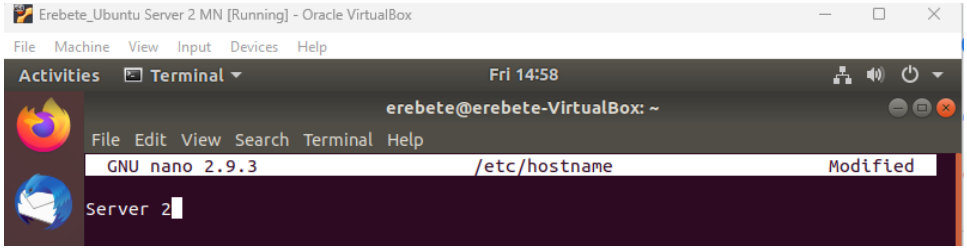
Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

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

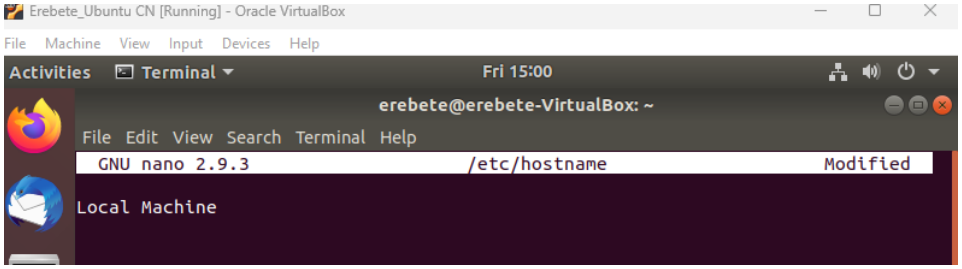
1.1 Use server1 for Server 1



1.2 Use server2 for Server 2

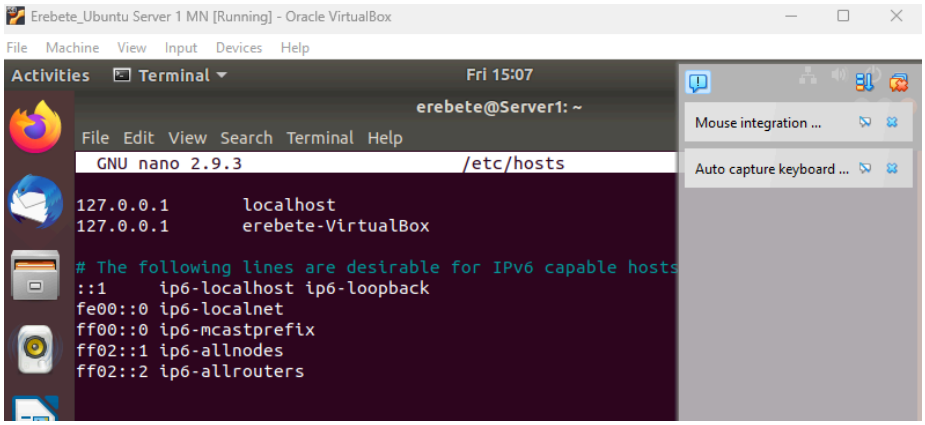


1.3 Use workstation for the Local Machine

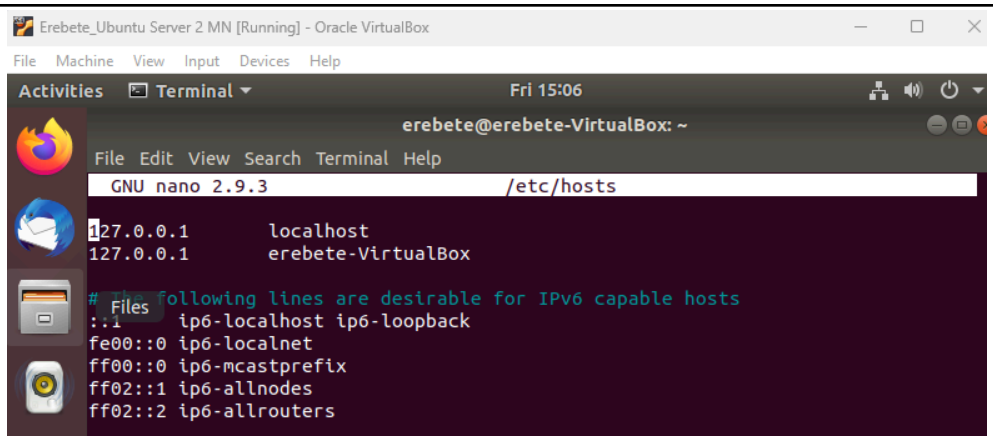


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

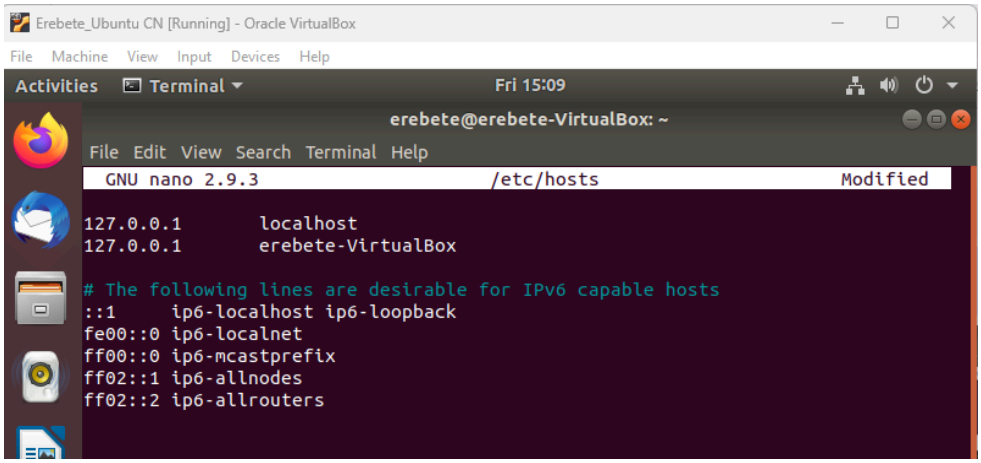
2.1 Type 127.0.0.1 server 1 for Server 1



2.2 Type 127.0.0.1 server 2 for Server 2



2.3 Type 127.0.0.1 workstation for the Local Machine



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.

   Update

   Local Machine

```
erebete@LocalMachine:~$ 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
All packages are up to date.
```

Server 1

```
erebete@Server1:~$ sudo apt update
[sudo] password for erebete:
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```

Server 2

```
erebete@Server2:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```

Upgrade

Local Machine

```
erebete@erebete-VirtualBox:~$ 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
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Server 1

```
erebete@Server1:~$ 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
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Server 2

```
erebete@erebete-VirtualBox:~$ 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
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

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

Local Machine

```
erebete@erebete-VirtualBox:~$ 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
Get:1 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 2s (339 kB/s)
Preconfiguring packages ...
```

Server 1

```
erebete@Server1:~$ 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
Get:1 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 1s (457 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
```

Server 2

```
erebete@erebete-VirtualBox:~$ 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
Get:1 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 1s (513 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
```

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*

Local Machine

```
erebete@erebete-VirtualBox:~$ sudo service ssh start
erebete@erebete-VirtualBox:~$ sudo systemclt status ssh
sudo: systemclt: command not found
erebete@erebete-VirtualBox:~$ 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 15:11:03 PST; 7min ago
 Main PID: 2039 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─2039 /usr/sbin/sshd -D

Aug 08 15:11:03 erebete-VirtualBox systemd[1]: Starting OpenBSD Secure Shell se
Aug 08 15:11:03 erebete-VirtualBox sshd[2039]: Server listening on 0.0.0.0 port
Aug 08 15:11:03 erebete-VirtualBox sshd[2039]: Server listening on :: port 22.
Aug 08 15:11:03 erebete-VirtualBox systemd[1]: Started OpenBSD Secure Shell ser
lines 1-12/12 (END)
```

Server 1

```
erebete@Server1:~$ sudo service ssh start
erebete@Server1:~$ sudo systemclt status ssh
sudo: systemclt: command not found
erebete@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 2025-08-08 15:13:08 PST; 7min ago
   Main PID: 2045 (sshd)
      Tasks: 1 (limit: 2318)
     CGroup: /system.slice/ssh.service
             └─2045 /usr/sbin/sshd -D

Aug 08 15:13:08 Server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 08 15:13:08 Server1 sshd[2045]: Server listening on 0.0.0.0 port 22.
Aug 08 15:13:08 Server1 sshd[2045]: Server listening on :: port 22.
Aug 08 15:13:08 Server1 systemd[1]: Started OpenBSD Secure Shell server.
```

Server 2

```
erebete@erebete-VirtualBox:~$ sudo service ssh start
erebete@erebete-VirtualBox:~$ sudo systemclt status ssj
sudo: systemclt: command not found
erebete@erebete-VirtualBox:~$ sudo systemclt status ssh
sudo: systemclt: command not found
erebete@erebete-VirtualBox:~$ 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 15:14:23 PST; 7min ago
   Main PID: 2040 (sshd)
      Tasks: 1 (limit: 2318)
     CGroup: /system.slice/ssh.service
             └─2040 /usr/sbin/sshd -D

Aug 08 15:14:23 erebete-VirtualBox systemd[1]: Starting OpenBSD Secure Shell se
Aug 08 15:14:23 erebete-VirtualBox sshd[2040]: Server listening on 0.0.0.0 port
Aug 08 15:14:23 erebete-VirtualBox sshd[2040]: Server listening on :: port 22.
Aug 08 15:14:23 erebete-VirtualBox systemd[1]: Started OpenBSD Secure Shell ser
```

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*

Local Machine

```
erebete@erebete-VirtualBox:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
erebete@erebete-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
erebete@erebete-VirtualBox:~$ sudo ufw status
Status: active

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

Server 1

```
erebete@Server1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
erebete@Server1:~$ sudo ufw enable
Firewall is active and enabled on system startup
erebete@Server1:~$ sudo ufw status
Status: active

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

Server 2

```
erebete@Server2:~$ sudo ufw allow ssh
[sudo] password for erebete:
Rules updated
Rules updated (v6)
erebete@Server2:~$ sudo ufw enable
Firewall is active and enabled on system startup
erebete@Server2:~$ 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._102__
   1.2 Server 2 IP address: 192.168.56._103__
   1.3 Server 3 IP address: 192.168.56._101__
2. Make sure that they can ping each other.
   2.1 Connectivity test for Local Machine 1 to Server 1: ☐ Successful ☐ Not Successful
   - Yes, successful

```
erebete@LocalMachine:~$ ping 192.168.56.102 -c 4
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.736 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.405 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.387 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.372 ms

--- 192.168.56.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.372/0.475/0.736/0.151 ms
```

   2.2 Connectivity test for Local Machine 1 to Server 2: ☐ Successful ☐ Not Successful
   - Yes,successful

```
erebete@LocalMachine:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.956 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.420 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.403 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.473 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.401 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=0.408 ms
^C
--- 192.168.56.103 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5088ms
rtt min/avg/max/mdev = 0.401/0.510/0.956/0.201 ms
```

   2.3 Connectivity test for Server 1 to Server 2: ☐ Successful ☐ Not Successful
   - Yes, successful

```
erebete@Server1:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.502 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.669 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.467 ms
^C
--- 192.168.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.467/0.735/1.304/0.338 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.*

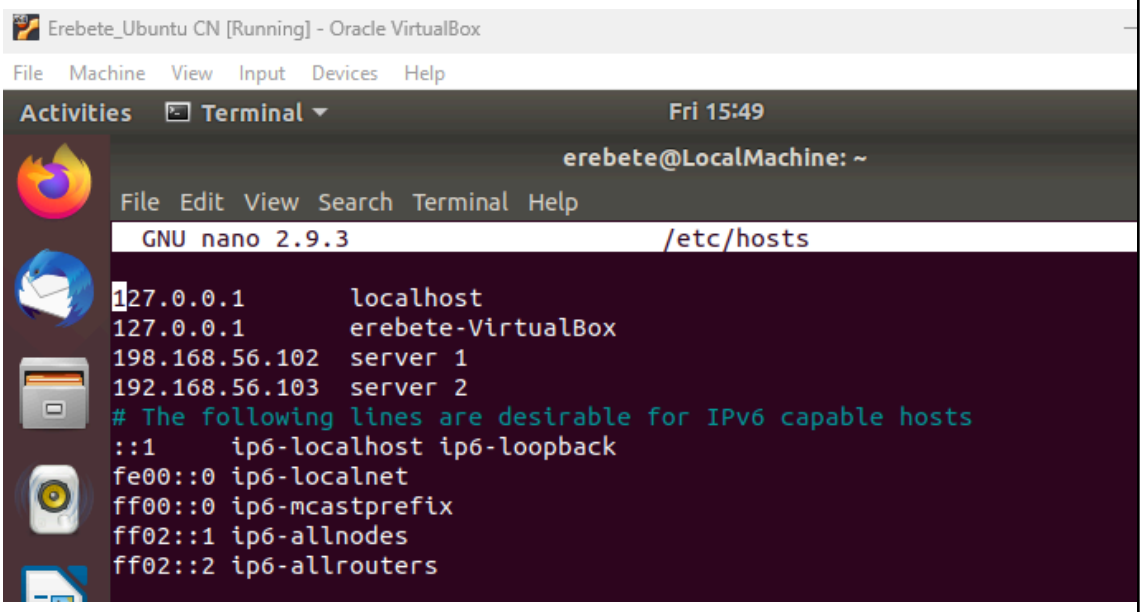
```
erebete@LocalMachine:~$ ssh erebete@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established
.
ECDSA key fingerprint is SHA256:NV1T0W8dTHziWtkUD6h6VDrPrAwFdy+nAKxphl+Izzk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
erebete@192.168.56.102'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.

erebete@Server1:~$ logout
Connection to 192.168.56.102 closed.
erebete@LocalMachine:~$ ssh erebete@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established
```

3. Do the same for Server 2.

```
erebete@LocalMachine:~$ ssh erebete@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established
.
ECDSA key fingerprint is SHA256:4qFGinPTu+/4WesG2lMGwJ+OcmyNqmN45MLomUHf2Uw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.103' (ECDSA) to the list of known hosts.
erebete@192.168.56.103'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.

erebete@Server2:~$ logout
Connection to 192.168.56.103 closed.
```

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)

```
192.168.56.102  server 1
```

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

```
192.168.56.103  server 2
```

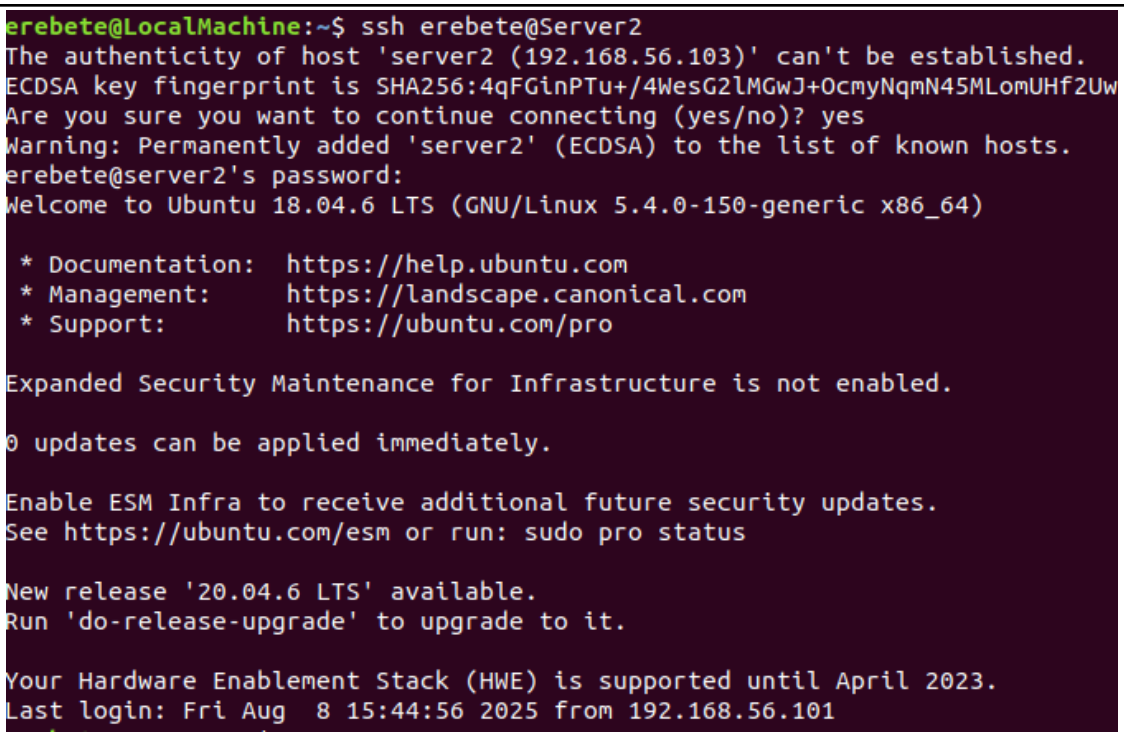
4.3 Save the file and exit.

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.

Server 1

```
erebete@LocalMachine:~$ ssh erebete@Server1
erebete@server1's password:
Permission denied, please try again.
erebete@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

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.
Last login: Fri Aug  8 15:44:04 2025 from 192.168.56.101
```

Server 2



Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   - We just simply use the sudo nano /etc/hosts command and just put the ip address of each server and also their names and also use the ssh username and the name of the server itself.
2. How secured is SSH?
   - It is secured because it requires a password for you to navigate and change. For example, we want to change to a different server and it is secured because each step that is needed depends on it.