Name: Ferrer, Joseph Bryan M.	Date Performed: 08/17/2023
Course/Section: CPE31S6	Date Submitted: 08/ /2023
Instructor: Engr. Jonathan V. Taylar	Semester and SY: 1st sem / 2023-2024

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

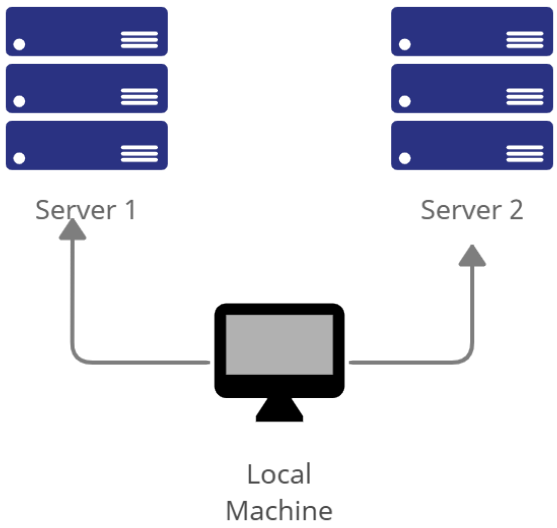
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

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

2. **Discussion:**

Network Topology:

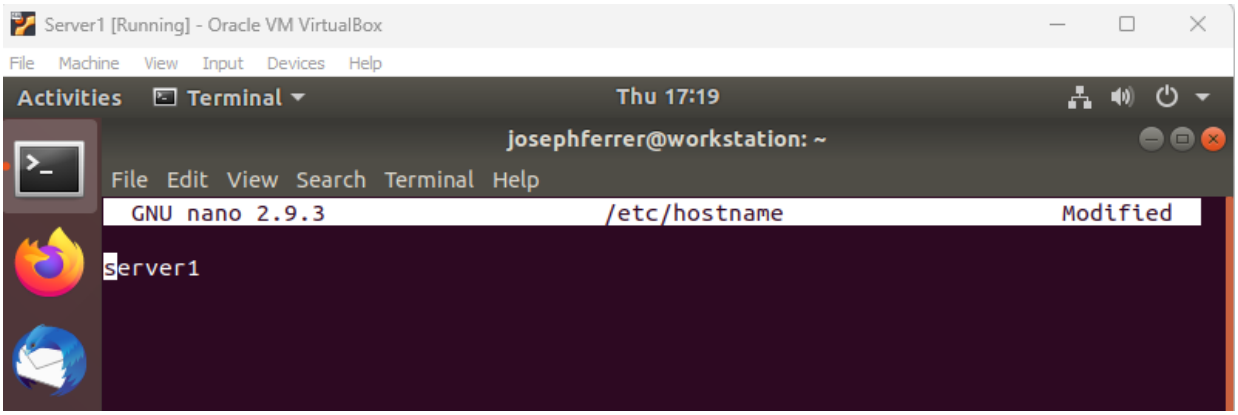
Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine*).



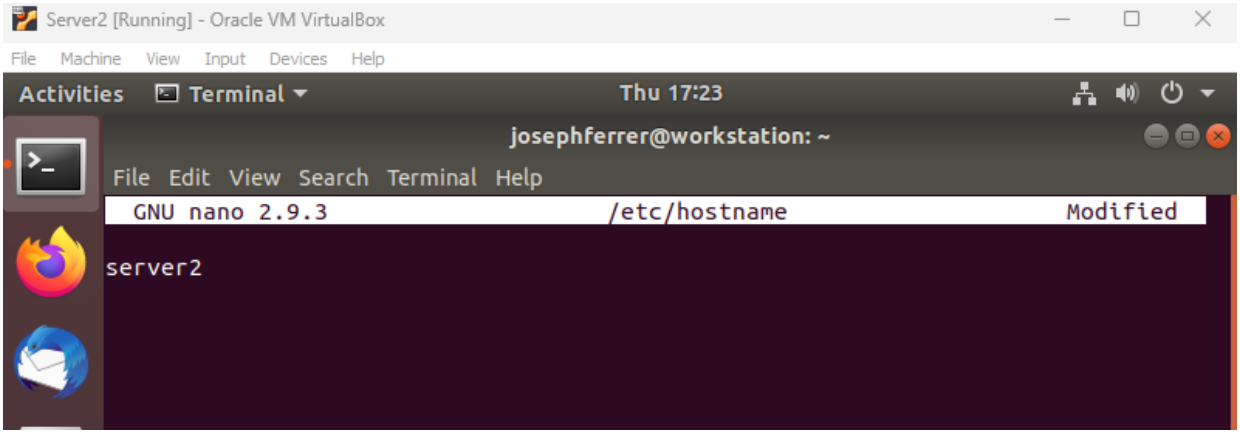
Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

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

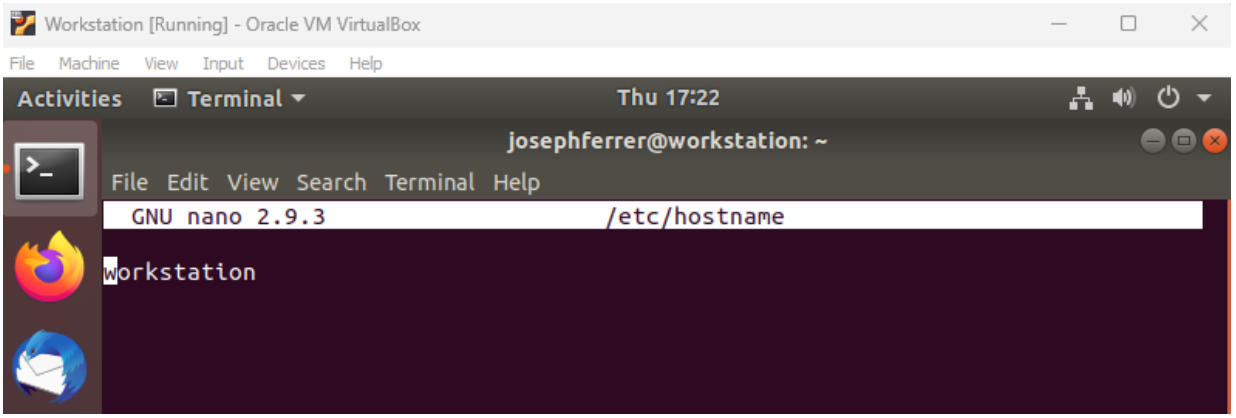
1.1 Use server1 for Server 1



1.2 Use server2 for Server 2

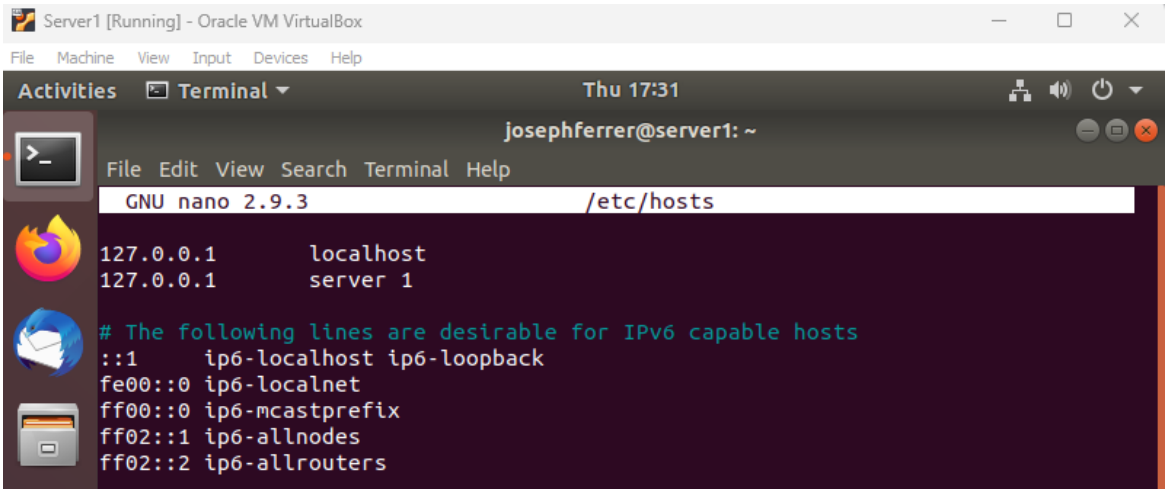


1.3 Use workstation for the Local Machine

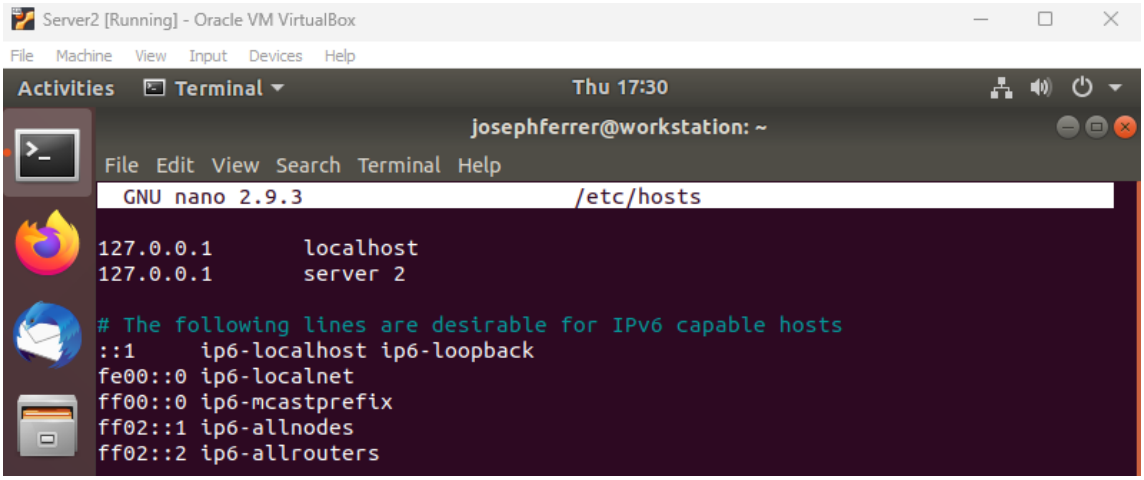


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

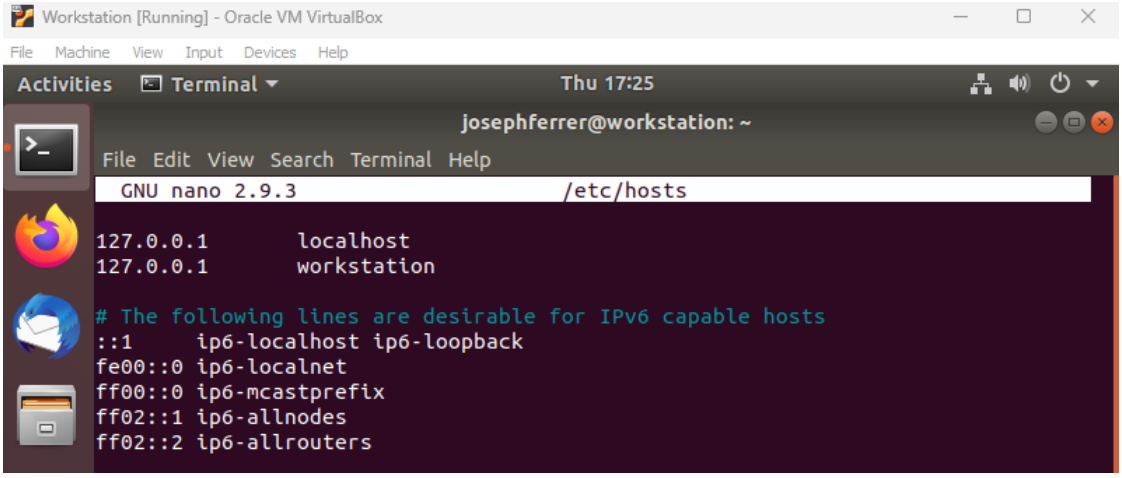
2.1 Type 127.0.0.1 server 1 for Server 1



2.2 Type 127.0.0.1 server 2 for Server 2

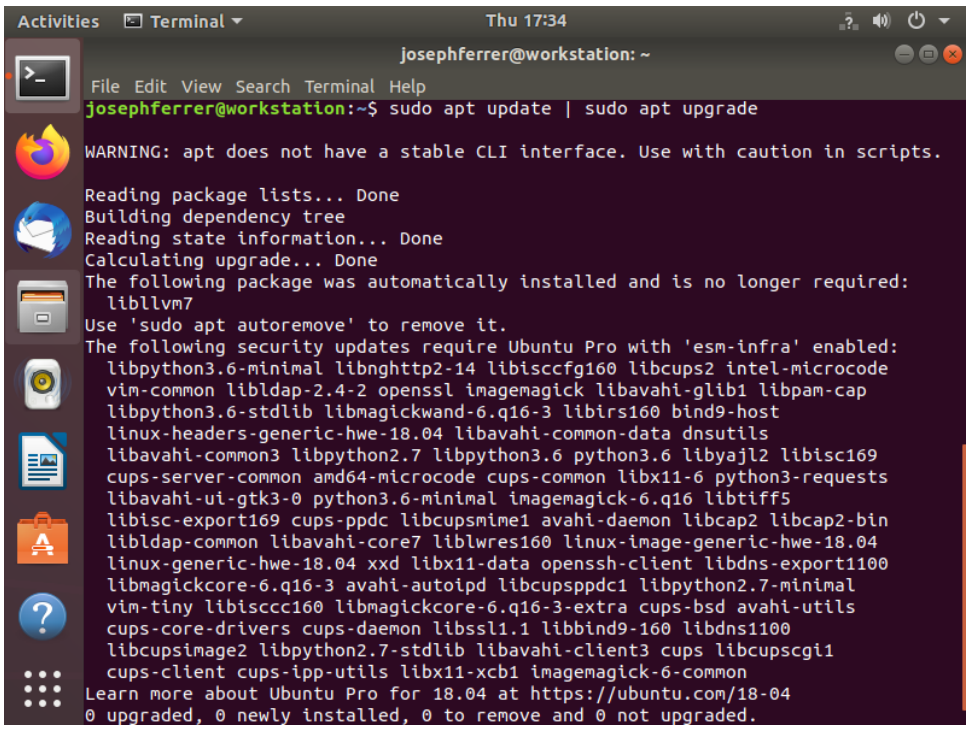


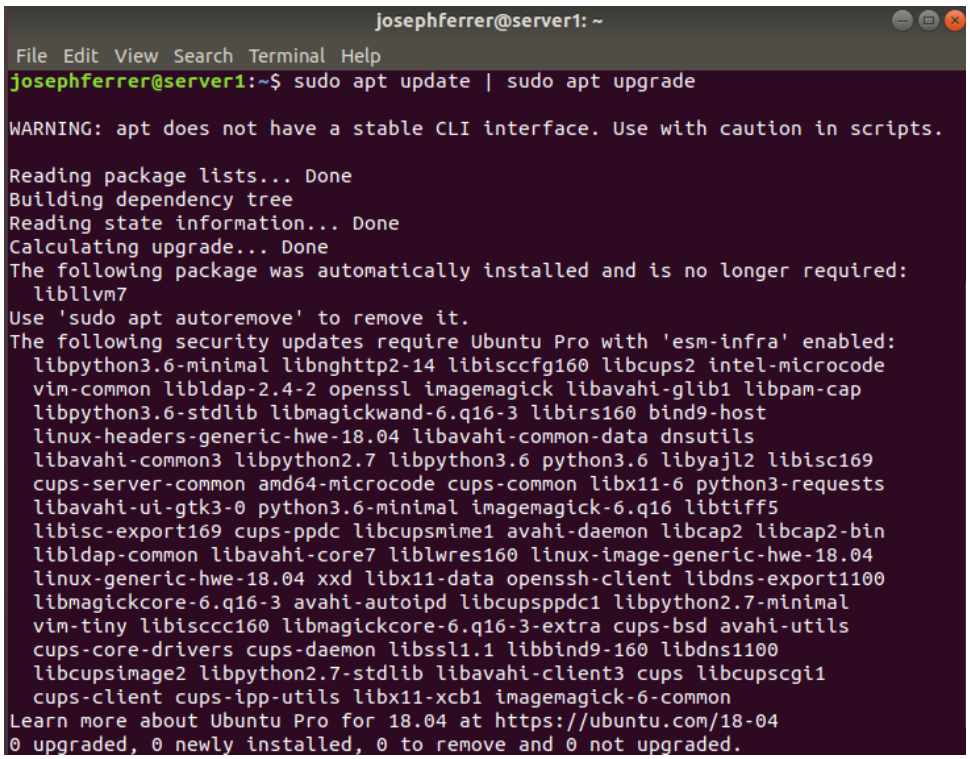
2.3 Type 127.0.0.1 workstation for the Local Machine

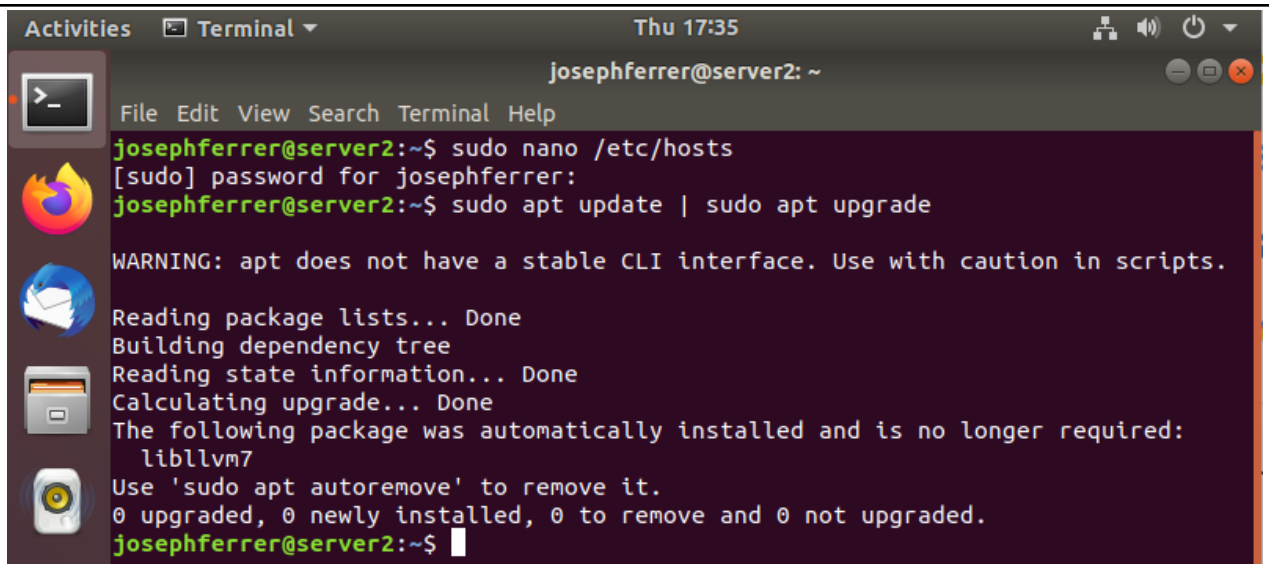


Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

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







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

```
josephferrer@workstation:~$ 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 (305 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
(Reading database ... 162327 files and directories currently installed.)
```

```
josephferrer@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 2s (296 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
(Reading database ... 162327 files and directories currently installed.)
```

```
josephferrer@server2:~$ 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 (300 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
(Reading database ... 162327 files and directories currently installed.)
```

3. Verify if the SSH service has started by issuing the following commands:

3.1 *sudo service ssh start*

```
josephferrer@workstation:~$ sudo service ssh start
```

```
josephferrer@server1:~$ sudo service ssh start
```

```
josephferrer@server2:~$ sudo service ssh start
```

3.2 *sudo systemctl status ssh*

```
josephferrer@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 Thu 2023-08-17 17:37:25 PST; 3min 10s ago
 Main PID: 3102 (sshd)
    Tasks: 1 (limit: 4884)
   CGroup: /system.slice/ssh.service
           └─3102 /usr/sbin/sshd -D

Aug 17 17:37:25 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:37:25 workstation sshd[3102]: Server listening on 0.0.0.0 port 22.
Aug 17 17:37:25 workstation sshd[3102]: Server listening on :: port 22.
Aug 17 17:37:25 workstation systemd[1]: Started OpenBSD Secure Shell server.
...skipping...
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Thu 2023-08-17 17:37:25 PST; 3min 10s ago
 Main PID: 3102 (sshd)
    Tasks: 1 (limit: 4884)
   CGroup: /system.slice/ssh.service
           └─3102 /usr/sbin/sshd -D

Aug 17 17:37:25 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:37:25 workstation sshd[3102]: Server listening on 0.0.0.0 port 22.
Aug 17 17:37:25 workstation sshd[3102]: Server listening on :: port 22.
Aug 17 17:37:25 workstation systemd[1]: Started OpenBSD Secure Shell server.
```

```
josephferrer@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 Thu 2023-08-17 17:38:51 PST; 3min 41s ago
 Main PID: 3104 (sshd)
    Tasks: 1 (limit: 4884)
   CGroup: /system.slice/ssh.service
           └─3104 /usr/sbin/sshd -D

Aug 17 17:38:51 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:38:51 server1 sshd[3104]: Server listening on 0.0.0.0 port 22.
Aug 17 17:38:51 server1 sshd[3104]: Server listening on :: port 22.
Aug 17 17:38:51 server1 systemd[1]: Started OpenBSD Secure Shell server.
```

```
josephferrer@server2:~$ 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 Thu 2023-08-17 17:38:28 PST; 4min 36s ago
 Main PID: 2594 (sshd)
    Tasks: 1 (limit: 4884)
   CGroup: /system.slice/ssh.service
           └─2594 /usr/sbin/sshd -D

Aug 17 17:38:28 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:38:28 server2 sshd[2594]: Server listening on 0.0.0.0 port 22.
Aug 17 17:38:28 server2 sshd[2594]: Server listening on :: port 22.
Aug 17 17:38:28 server2 systemd[1]: Started OpenBSD Secure Shell server.
```

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

4.1 *sudo ufw allow ssh*

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

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

```
josephferrer@server2:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
```

4.2 *sudo ufw enable*

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

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

```
josephferrer@server2:~$ sudo ufw enable
Firewall is active and enabled on system startup
```

4.3 *sudo ufw status*

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

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

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

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

```
josephferrer@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 Local Machine 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**

```
josephferrer@workstation:~$ ping 192.168.56.102
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=0.503 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.278 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.465 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.396 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.452 ms
^C
--- 192.168.56.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4095ms
rtt min/avg/max/mdev = 0.278/0.418/0.503/0.082 ms
```

   2.2 Connectivity test for Local Machine 1 to Server 2: **Successful**

```
josephferrer@workstation:~$ 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=1.08 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.447 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.522 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.430 ms
^C
--- 192.168.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.430/0.622/1.089/0.271 ms
```

   2.3 Connectivity test for Server 1 to Server 2: **Successful**

```
josephferrer@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=1.09 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.485 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.433 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.560 ms
^C
--- 192.168.56.103 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.426/0.599/1.094/0.253 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*

```
josephferrer@workstation:~$ ssh josephferrer@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:Ur6zbgmVSSDrrWvM8XbODB/0jJUd1o2bp6YO5aKOc40.
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.
```

1.2 Enter the password for server 1 when prompted

```
josephferrer@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

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
```

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

```
josephferrer@server1:~$
```

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

```
josephferrer@server1:~$ logout
Connection to 192.168.56.102 closed.
josephferrer@workstation:~$
```

3. Do the same for Server 2.

```
josephferrer@workstation:~$ ssh josephferrer@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:A61/LNrSq9WOfEZq2U19DIzXx4Sj73c3+HMOnIiHEyw.
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.
josephferrer@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

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.
```

```
josephferrer@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)

```
                                josephferrer@workstation: ~
 File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1       localhost
127.0.0.1       workstation
192.168.56.102  server1
```

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

```
                                josephferrer@workstation: ~
 File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                        /etc/hosts

127.0.0.1       localhost
127.0.0.1       workstation
192.168.56.102  server1
192.168.56.103  server2
```

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.

```
josephferrer@workstation:~$ ssh josephferrer@server1
josephferrer@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

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: Thu Aug 17 18:09:01 2023 from 192.168.56.101
josephferrer@server1:~$
```

```
josephferrer@workstation:~$ ssh josephferrer@server2
The authenticity of host 'server2 (192.168.56.103)' can't be established.
ECDSA key fingerprint is SHA256:A61/LNrSq9WOfEZq2U19DIzXx4Sj73c3+HMOnIiHEyw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
josephferrer@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

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: Thu Aug 17 18:03:50 2023 from 192.168.56.101
josephferrer@server2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   We specified the IP address associated with a name in the host shell script in the SSH commands. In order to add a hostname to the /etc/hosts file. we open the file in a text editor with root privileges, such as using the command sudo nano. Then, we add an entry for the server's hostname and IP address.

2. How secured is SSH?
   SSH is the most used method for securely managing distant servers and is a secure protocol. The SSH protocol has been shown to be very secure when used with common security measures. However, maintaining the security of SSH connections depends in large part on human factors. Attacks using brute force on SSH servers are a frequent occurrence. SSH keys let you establish connections that are more secure than those that need password authentication without a password. SSH traffic is entirely encrypted. Users' actions are private whether they are sharing a file, browsing the web, or executing a command.

Conclusion:

In this activity, I have been able to accomplish the objective which is to create or configure Virtual Machines in Microsoft Azure or VirtualBox and Set-up a Virtual Network and Test Connectivity of VMs. I have been able to accomplish this objective by following the syntaxes and instructions given by our professor. I encountered some errors in the terminal but I have been able to fix it by troubleshooting. With this activity, I have been able fulfill the given requirements such as connecting server 1 and server 2 from the workstation. I also used given syntaxes such as sudo nano in order to edit and add entries for the server's hostname and IP address.