Name: Echiverri Syd Ashley L	**Date Performed: 08/14/23**
Course/Section: CPE 232 - CPE31S4	**Date Submitted: 08/15/23**
Instructor: Jonathan Taylar	**Semester and SY: 2023-2024**

Activity 1: Configure Network using Virtual Machines

1. Objectives:

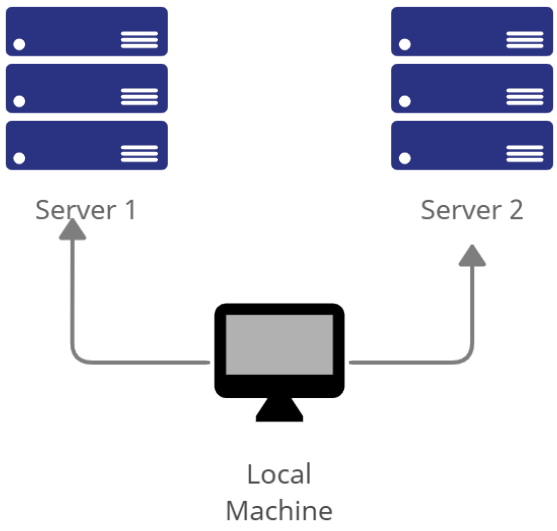
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

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

2. Discussion:

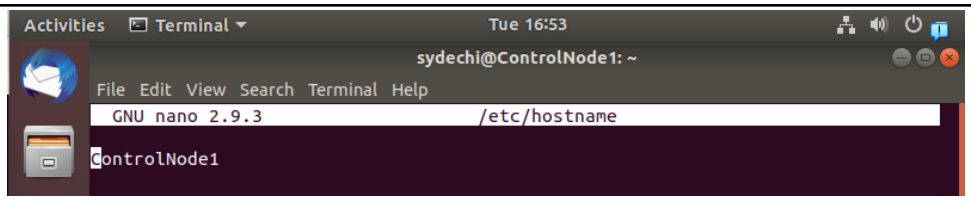
Network Topology:

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*).

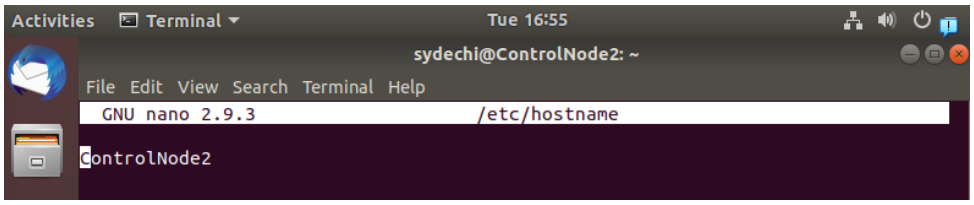


Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

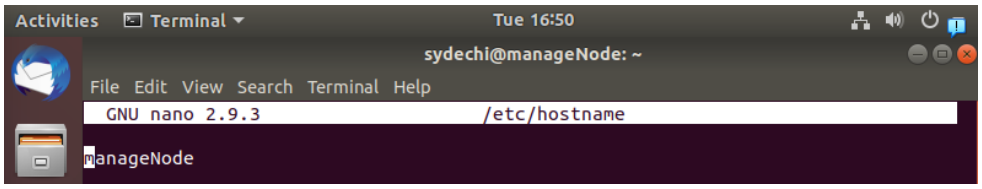
1. Change the hostname using the command *sudo nano /etc/hostname*
   1.1 Use server1 for Server 1



1.2 Use server2 for Server 2

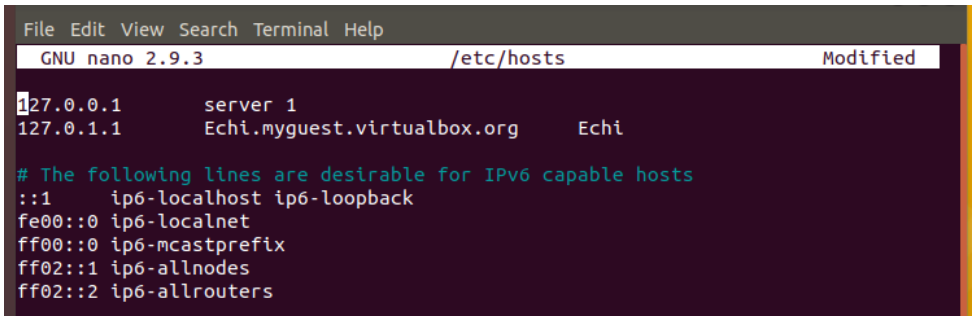


1.3 Use workstation for the Local Machine

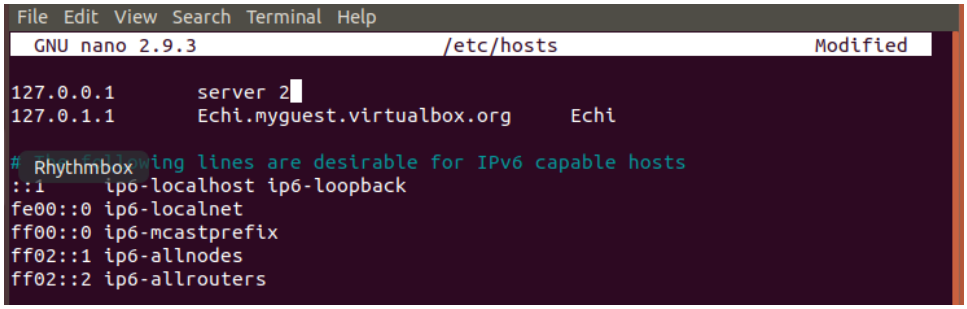


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

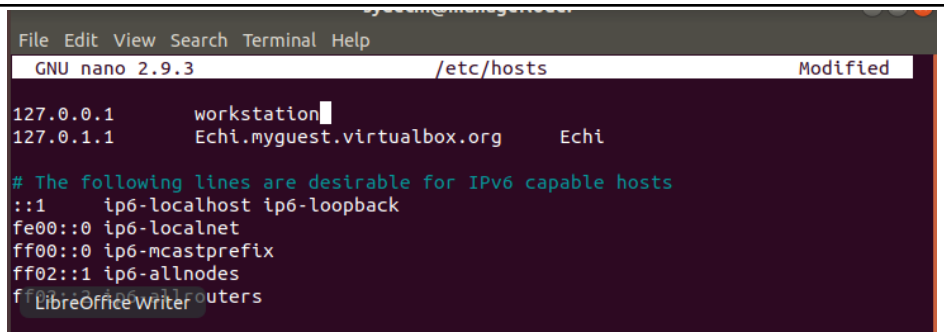
2.1 Type 127.0.0.1 server 1 for Server 1



2.2 Type 127.0.0.1 server 2 for Server 2



2.3 Type 127.0.0.1 workstation for the Local Machine

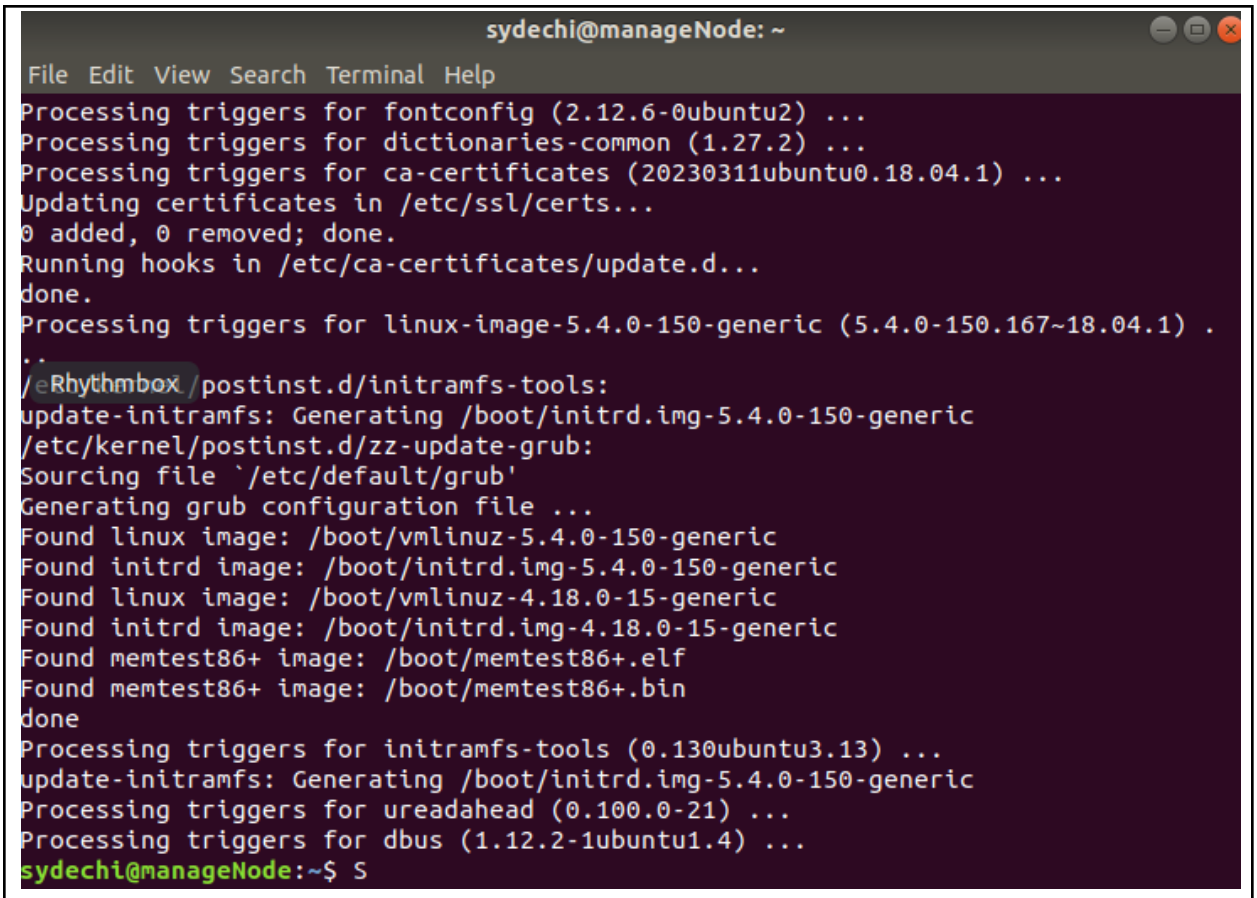


Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

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

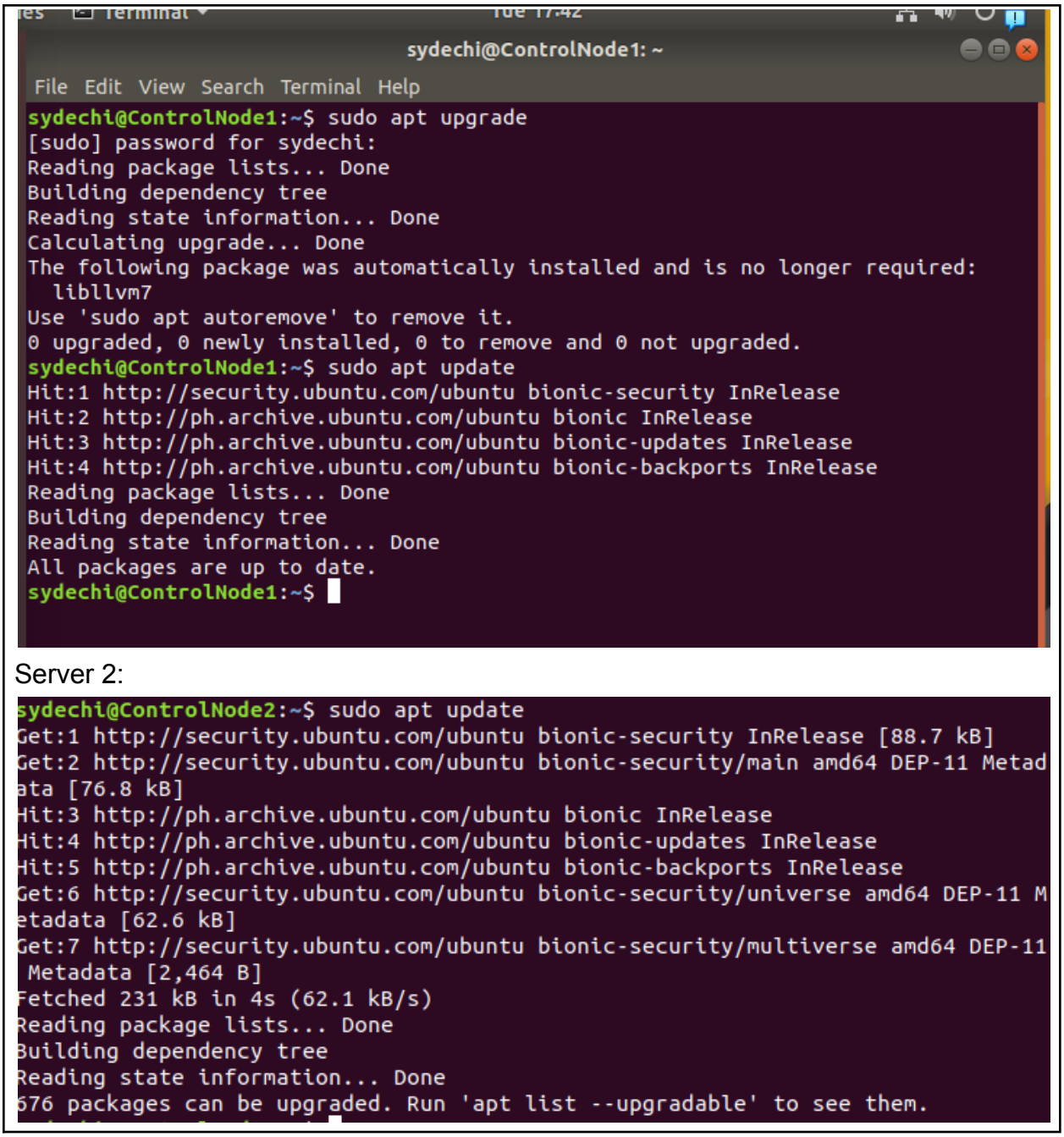
Local Machine:

```
sydechi@manageNode:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
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
Get:5 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metad
ata [76.8 kB]
Ubuntu Software
urity.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 M
etadata [62.6 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11
 Metadata [2,464 B]
Fetched 231 kB in 2s (113 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.
sydechi@manageNode:~$
```



Server 1:

```
sydechi@ControlNode1:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:5 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metad
ata [76.8 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 M
etadata [62.6 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11
 Metadata [2,464 B]
Fetched 231 kB in 2s (101 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.
sydechi@ControlNode1:~$
```

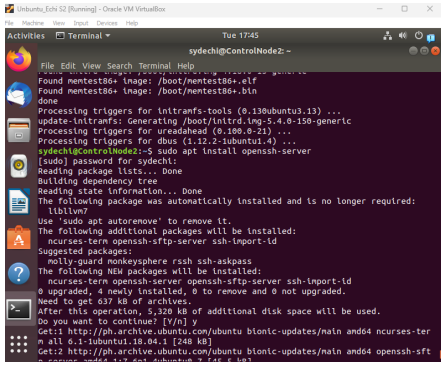

sydechi@ControlNode1: ~
File Edit View Search Terminal Help
sydechi@ControlNode1:~$ sudo apt upgrade
[sudo] password for sydechi:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
libllvm7
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sydechi@ControlNode1:~$ 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.
sydechi@ControlNode1:~$

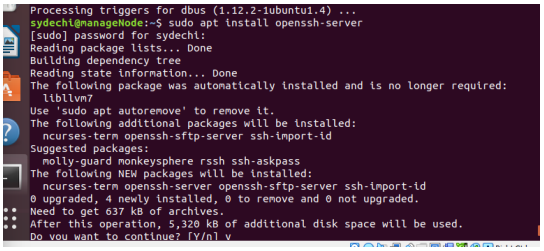
Server 2:

sydechi@ControlNode2:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:2 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metad
ata [76.8 kB]
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:5 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:6 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 M
etadata [62.6 kB]
Get:7 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11
Metadata [2,464 B]
Fetched 231 kB in 4s (62.1 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.

```
File  Edit  View  Search  Terminal  Help
Processing triggers for fontconfig (2.12.6-0ubuntu2) ...
Processing triggers for dictionaries-common (1.27.2) ...
Processing triggers for ca-certificates (20230311ubuntu0.18.04.1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for linux-image-5.4.0-150-generic (5.4.0-150.167~18.04.1) .
..
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-5.4.0-150-generic
/etc/kernel/postinst.d/zz-update-grub:
Sourcing file `/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.4.0-150-generic
Found initrd image: /boot/initrd.img-5.4.0-150-generic
Found linux image: /boot/vmlinuz-4.18.0-15-generic
Found initrd image: /boot/initrd.img-4.18.0-15-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
done
Processing triggers for initramfs-tools (0.130ubuntu3.13) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-150-generic
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for dbus (1.12.2-1ubuntu1.4) ...
sydechi@ControlNode2:~$
```

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





```
Processing triggers for dbus (1.12.2-1ubuntu1.4) ...
sydechi@manageNode:~$ sudo apt install openssh-server
[sudo] password for sydechi:
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
```

```
All packages are up to date.
sydechi@ControlNode1:~$ 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]
```

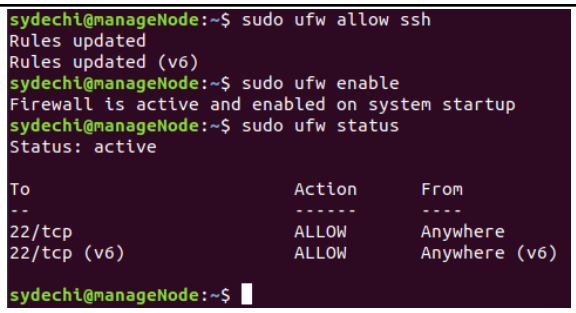
3. Verify if the SSH service has started by issuing the following commands:
   3.1 *sudo service ssh start*
   3.2 *sudo systemctl status ssh*

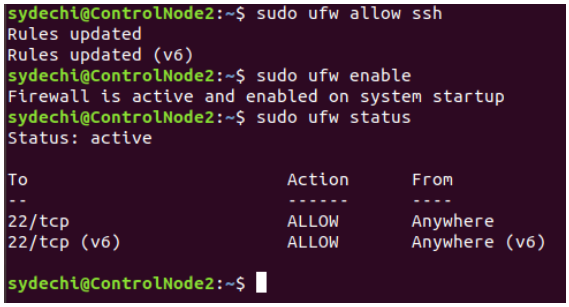
```
sydechi@manageNode:~$ sudo service ssh start
sydechi@manageNode:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
     Active: active (running) since Tue 2023-08-15 17:44:02 +08; 3min 27s ago
   Main PID: 22215 (sshd)
      Tasks: 1 (limit: 2318)
     CGroup: /system.slice/ssh.service
             └─22215 /usr/sbin/sshd -D

Aug 15 17:44:02 manageNode systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 17:44:02 manageNode sshd[22215]: Server listening on 0.0.0.0 port 22.
Aug 15 17:44:02 manageNode sshd[22215]: Server listening on :: port 22.
Aug 15 17:44:02 manageNode systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

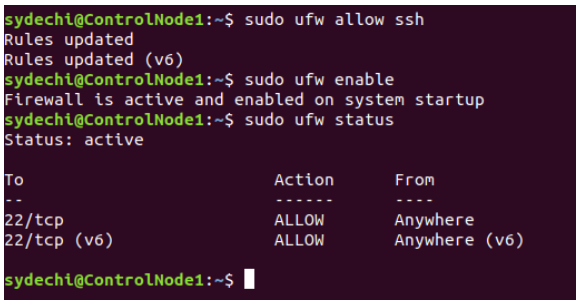
```
sydechi@ControlNode1:~$ sudo service ssh start
sydechi@ControlNode1:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
     Active: active (running) since Tue 2023-08-15 17:46:55 +08; 1min 24s ago
   Main PID: 2938 (sshd)
      Tasks: 1 (limit: 2318)
     CGroup: /system.slice/ssh.service
             └─2938 /usr/sbin/sshd -D

Aug 15 17:46:55 ControlNode1 systemd[1]: Starting OpenBSD Secure Shell server..
Aug 15 17:46:55 ControlNode1 sshd[2938]: Server listening on 0.0.0.0 port 22.
Aug 15 17:46:55 ControlNode1 sshd[2938]: Server listening on :: port 22.
Aug 15 17:46:55 ControlNode1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
sydechi@ControlNode2:~$ sudo service ssh start
sydechi@ControlNode2:~$ 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 Tue 2023-08-15 17:44:38 +08; 4min 17s ago
   Main PID: 21768 (sshd)
      Tasks: 1 (limit: 2318)
     CGroup: /system.slice/ssh.service
             └─21768 /usr/sbin/sshd -D

Aug 15 17:44:38 ControlNode2 systemd[1]: Starting OpenBSD Secure Shell server..
Aug 15 17:44:38 ControlNode2 sshd[21768]: Server listening on 0.0.0.0 port 22.
Aug 15 17:44:38 ControlNode2 sshd[21768]: Server listening on :: port 22.
Aug 15 17:44:38 ControlNode2 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*
   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:

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: 192.168.56.6
   1.2 Server 2 IP address: 192.168.56.7
   1.3 Server 3 IP address: 192.168.56.5
2. Make sure that they can ping each other.
   2.1 Connectivity test for Local Machine 1 to Server 1: ☐ Successful ☐ Not Successful

```
sydechi@manageNode:~$ ping 192.168.56.6
PING 192.168.56.6 (192.168.56.6) 56(84) bytes of data.
64 bytes from 192.168.56.6: icmp_seq=1 ttl=64 time=0.802 ms
64 bytes from 192.168.56.6: icmp_seq=2 ttl=64 time=1.25 ms
64 bytes from 192.168.56.6: icmp_seq=3 ttl=64 time=0.427 ms
64 bytes from 192.168.56.6: icmp_seq=4 ttl=64 time=0.843 ms
64 bytes from 192.168.56.6: icmp_seq=5 ttl=64 time=1.22 ms
^C
--- 192.168.56.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4023ms
rtt min/avg/max/mdev = 0.427/0.910/1.253/0.308 ms
```

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

```
sydechi@manageNode:~$ ping 192.168.56.7
PING 192.168.56.7 (192.168.56.7) 56(84) bytes of data.
64 bytes from 192.168.56.7: icmp_seq=1 ttl=64 time=1.04 ms
64 bytes from 192.168.56.7: icmp_seq=2 ttl=64 time=104 ms
64 bytes from 192.168.56.7: icmp_seq=3 ttl=64 time=0.465 ms
64 bytes from 192.168.56.7: icmp_seq=4 ttl=64 time=0.419 ms
^C
--- 192.168.56.7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3025ms
rtt min/avg/max/mdev = 0.419/26.484/104.010/44.760 ms
```

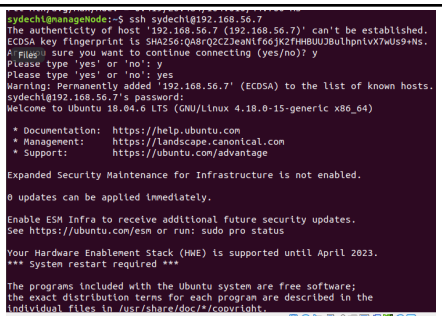
2.3 Connectivity test for Server 1 to Server 2: ☐ Successful ☐ Not Successful

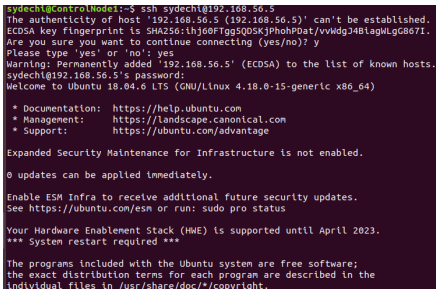
```
sydechi@ControlNode1:~$ ping 192.168.56.7
PING 192.168.56.7 (192.168.56.7) 56(84) bytes of data.
64 bytes from 192.168.56.7: icmp_seq=1 ttl=64 time=0.503 ms
64 bytes from 192.168.56.7: icmp_seq=2 ttl=64 time=0.432 ms
64 bytes from 192.168.56.7: icmp_seq=3 ttl=64 time=0.798 ms
64 bytes from 192.168.56.7: icmp_seq=4 ttl=64 time=1.03 ms
64 bytes from 192.168.56.7: icmp_seq=5 ttl=64 time=0.728 ms
^C64 bytes from 192.168.56.7: icmp_seq=6 ttl=64 time=1.12 ms
^C
--- 192.168.56.7 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5042ms
rtt min/avg/max/mdev = 0.432/0.770/1.128/0.253 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*





```
sydechi@ControlNode2:~$ ssh sydechi@192.168.56.5
The authenticity of host '192.168.56.5 (192.168.56.5)' can't be established.
ECDSA key fingerprint is SHA256:ihj60FTgg5QDSKjPhohPDat/vvWdgJ4BiagWLgG867I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.5' (ECDSA) to the list of known hosts.
sydechi@192.168.56.5'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/advantage

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: Tue Aug 15 18:00:44 2023 from 192.168.56.6
sydechi@manageNode:~$
```

1.2 Enter the password for server 1 when prompted

```
sydechi@192.168.56.7'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/advantage

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.
*** System restart required ***

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.
```

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

```
sydechi@ControlNode2:~$
```

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

```
sydechi@manageNode:~$ logout
Connection to 192.168.56.5 closed.
sydechi@ControlNode1:~$
```

3. Do the same for Server 2

```
sydechi@manageNode:~$ logout
Connection to 192.168.56.5 closed.
sydechi@ControlNode2:~$
```

.

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.

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                  /etc/hosts                       Modified

192.168.56.6            ControlNode1
192.168.56.7            ControlNode2

# 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
```

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.

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'controlnode1,192.168.56.6' (ECDSA) to the list of k
nown hosts.
sydechi@controlnode1'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.

77 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.

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

sydechi@ControlNode1:~$
```

```
sydechi@manageNode:~$ ssh sydechi@controlnode2
The authenticity of host 'controlnode2 (192.168.56.7)' can't be established.
ECDSA key fingerprint is SHA256:QA8rQ2CZJeaNif66jK2fHHBUUJBulhpnivX7wUs9+Ns.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'controlnode2' (ECDSA) to the list of known hosts.
sydechi@controlnode2'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/advantage

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: Tue Aug 15 17:59:17 2023 from 192.168.56.5
sydechi@ControlNode2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   For simplicity, you can just use the hostname command. Once you have your hostname, add. nearby. Since it's on your local network, it functions.

2. How secured is SSH?

   SSH traffic is entirely encrypted. Users' actions are private whether they are sharing a file, browsing the web, or executing a command. While a standard user ID and password can be used to access SSH, public key pairs are more frequently used to authenticate hosts to one another.

Conclusion: