

Name: Olivera, Angelo Carl S.	Date Performed: 08/14/2023
Course/Section: CPE232 CPE31S4	Date Submitted: 08/15/2023
Instructor: Jonathan V. Taylar	Semester and SY: 1st sem 2023-24

Activity 1: Configure Network using Virtual Machines

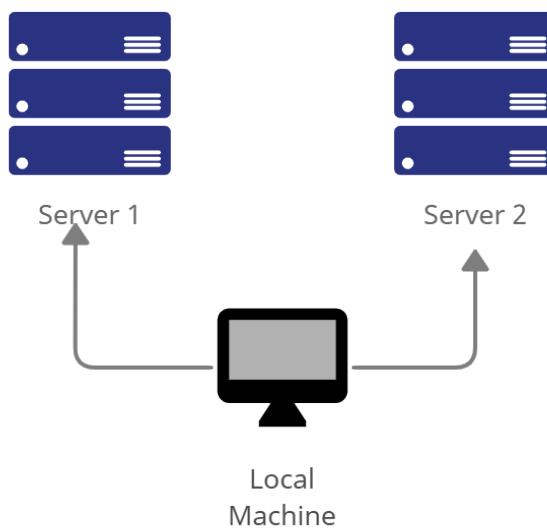
1. Objectives:

- 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:

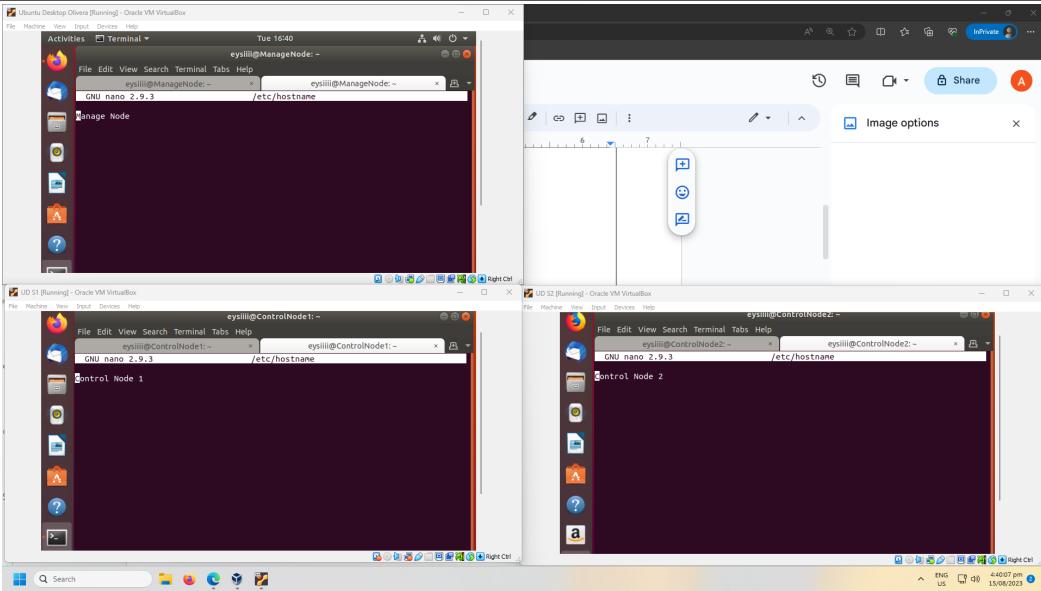
Network Topology:

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*).

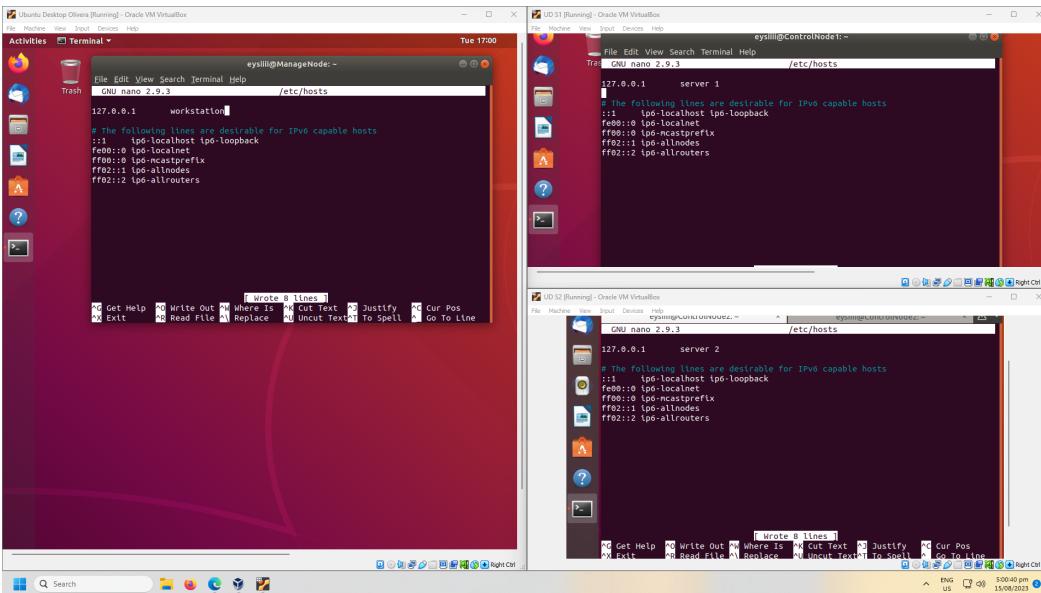


Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

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

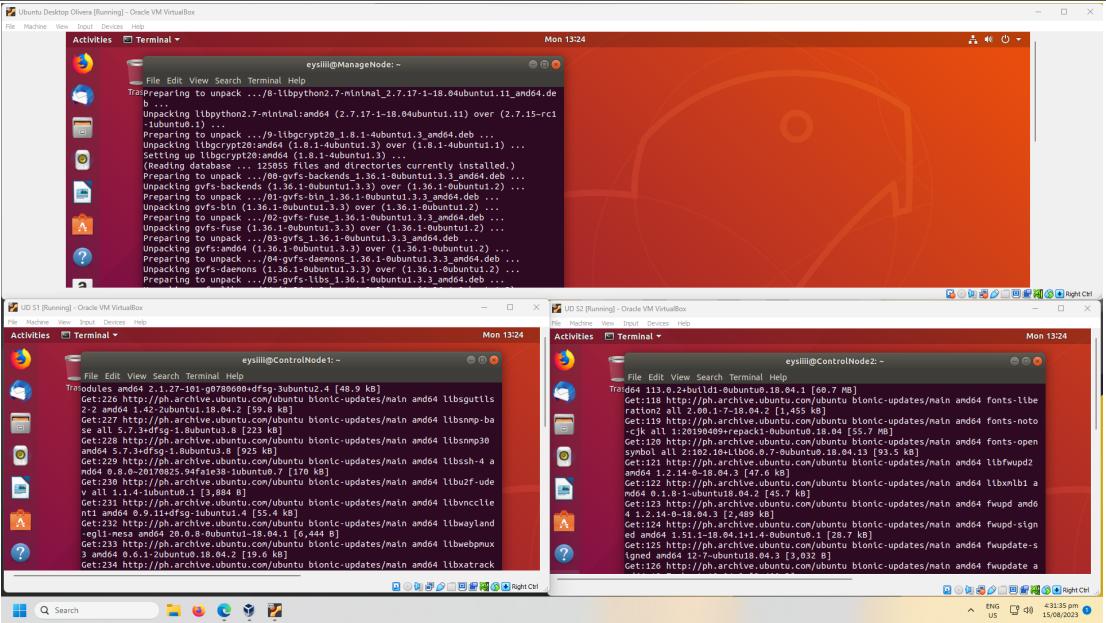


2. Edit the hosts using the command ***sudo nano /etc/hosts***. Edit the second line.
- 2.1 Type 127.0.0.1 server 1 for Server 1
- 2.2 Type 127.0.0.1 server 2 for Server 2
- 2.3 Type 127.0.0.1 workstation for the Local Machine

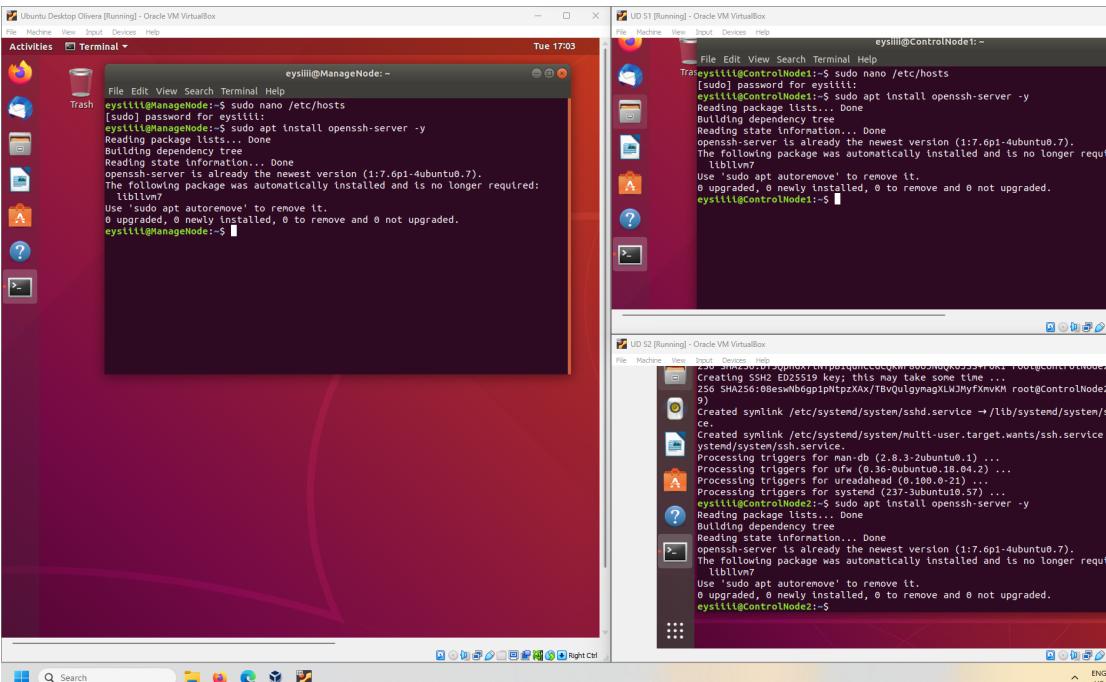


Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

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`.



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

3.1 *sudo service ssh start*

```

Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Tue 17:07
File Edit View Search Terminal Help
eystilli@ManageNode:~$ sudo apt install openssh-server -y
[sudo] password for eystilli
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
liblawnv*
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
eystilli@ManageNode:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2023-08-15 16:54:16 PST; 1min ago
     Main PID: 989 (sshd)
    Tasks: 1 (limit: 131072)
   CGroup: /system.slice/ssh.service
           └─989 /usr/sbin/sshd -D

Aug 15 16:54:16 ManageNode systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 15 16:54:16 ManageNode sshd[989]: Received SIGHUP; restarting.
Aug 15 16:54:16 ManageNode systemd[1]: Reloaded OpenBSD Secure Shell server.

UD 51 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
eystilli@ControlNode1:~$ sudo apt install openssh-server -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:7.6p1-4ubuntu0.7).
The following packages were automatically installed and are no longer required:
liblawnv*
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
eystilli@ControlNode1:~$ sudo service ssh start
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2023-08-15 17:02:12 PST; 1min ago
     Main PID: 824 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─824 /usr/sbin/sshd -D

Tasks: 1 (limit: 2318)
Group: 824 /usr/sbin/sshd -D

```

3.2 sudo systemctl status ssh

```

Ubuntu Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Tue 17:06
File Edit View Search Terminal Help
eystilli@ManageNode:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2023-08-15 16:54:16 PST; 1min ago
     Main PID: 989 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─989 /usr/sbin/sshd -D

Aug 15 16:54:16 ManageNode systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 15 16:54:16 ManageNode sshd[989]: Received SIGHUP; restarting.
Aug 15 16:54:16 ManageNode systemd[1]: Reloaded OpenBSD Secure Shell server.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on :: port 22.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on :: port 22.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:16 ManageNode sshd[989]: Reloaded OpenBSD Secure Shell server.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on :: port 22.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:16 ManageNode sshd[989]: Server listening on :: port 22.
(lines 1-18/18 (END))

UD 51 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
eystilli@ControlNode1:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2023-08-15 17:02:12 PST; 1min ago
     Main PID: 824 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─824 /usr/sbin/sshd -D

Aug 15 16:54:27 ControlNode1 systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 15 16:54:27 ControlNode1 sshd[824]: Received SIGHUP; restarting.
Aug 15 16:54:27 ControlNode1 systemd[1]: Reloaded OpenBSD Secure Shell server.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on :: port 22.
Aug 15 16:54:27 ControlNode1 systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 15 16:54:27 ControlNode1 sshd[824]: Received SIGHUP; restarting.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on :: port 22.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on :: port 22.
(lines 1-12/12 (END))

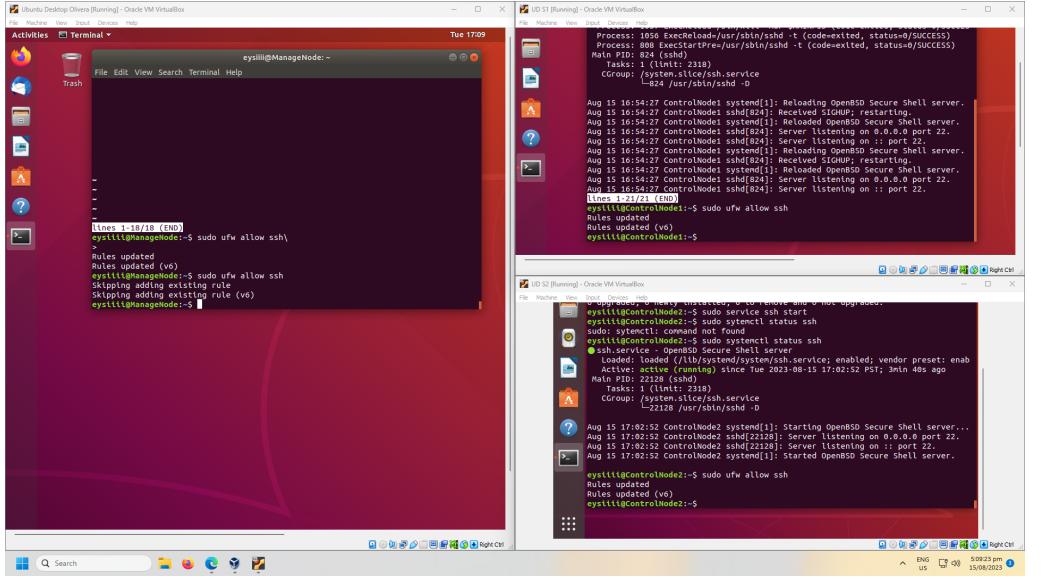
UD 52 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
eystilli@ControlNode2:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2023-08-15 17:02:52 PST; 3min 46s ago
     Main PID: 22128 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─22128 /usr/sbin/sshd -D

Aug 15 17:02:52 ControlNode2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 17:02:52 ControlNode2 sshd[22128]: Server listening on 0.0.0.0 port 22.
Aug 15 17:02:52 ControlNode2 sshd[22128]: Server listening on :: port 22.
Aug 15 17:02:52 ControlNode2 sshd[22128]: Started OpenBSD Secure shell server.
(lines 1-12/12 (END))

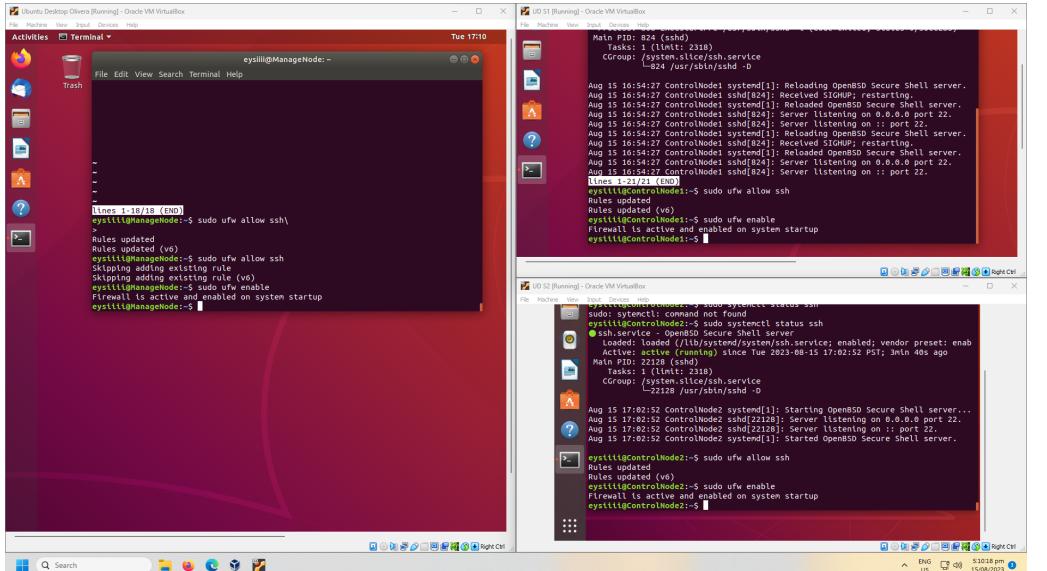
```

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

```

Ubuntu Desktop Olivera [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Tue 17:10
Terminal
eysiliti@ManageNode:~-
[lines 1-18/10 (END)]
eysiliti@ManageNode:~$ sudo ufw allow ssh
> 
Rules updated
Rules updated (v6)
eysiliti@ManageNode:~$ sudo ufw allow ssh
Skipping adding existing rule (v6)
eysiliti@ManageNode:~$ sudo ufw enable
Firewall is active and enabled on system startup
eysiliti@ManageNode:~$ sudo ufw status
Status: active
To Action From
-- -- --
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

eysiliti@ManageNode:~$ 

UD S1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on :: port 22.
Aug 15 16:54:27 ControlNode1 sshd[824]: Received SIGTERM; stopping OpenBSD Secure Shell server.
Aug 15 16:54:27 ControlNode1 sshd[824]: Received SIGHUP; restarting.
Aug 15 16:54:27 ControlNode1 sshd[824]: Reloaded openbsd Secure Shell server.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on 0.0.0.0 port 22.
Aug 15 16:54:27 ControlNode1 sshd[824]: Server listening on :: port 22.
[lines 1-2/21 (END)]
eysiliti@ControlNode1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
eysiliti@ControlNode1:~$ sudo ufw enable
Firewall is active and enabled on system startup
eysiliti@ControlNode1:~$ sudo ufw status
Status: active
To Action From
-- -- --
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

eysiliti@ControlNode1:~$ 

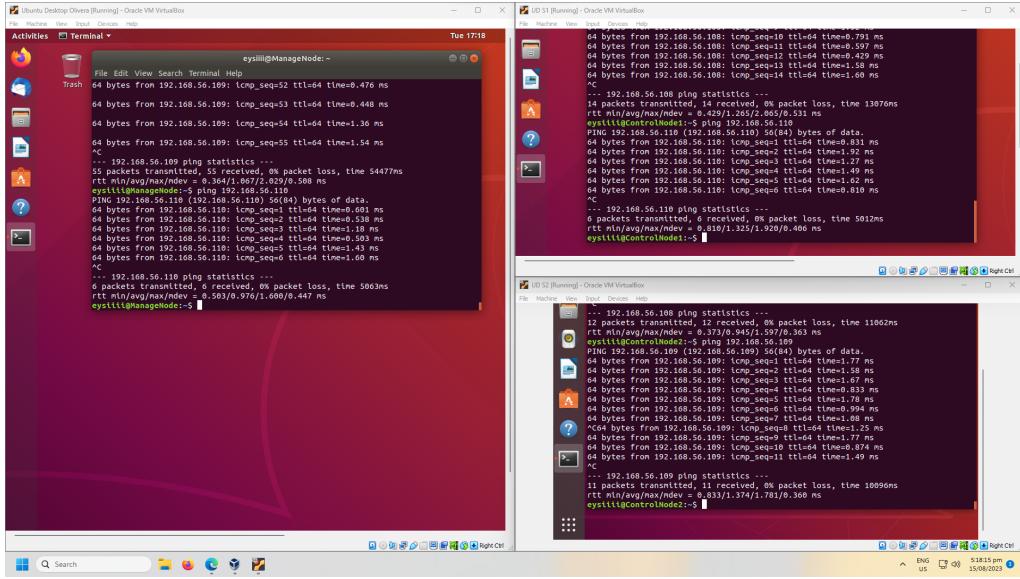
UD S2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Aug 15 17:02:52 ControlNode2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 17:02:52 ControlNode2 sshd[22128]: Server listening on 0.0.0.0 port 22.
Aug 15 17:02:52 ControlNode2 sshd[22128]: Server listening on :: port 22.
Aug 15 17:02:52 ControlNode2 sshd[22128]: Started OpenBSD Secure Shell server.
eysiliti@ControlNode2:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
eysiliti@ControlNode2:~$ sudo ufw enable
Firewall is active and enabled on system startup
eysiliti@ControlNode2:~$ sudo ufw status
Status: active
To Action From
-- -- --
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

eysiliti@ControlNode2:~$ 

```

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.
 - Local Machine IP address: 192.168.56.108
 - Server 1 IP address: 192.168.56.109
 - Server 2 IP address: 192.168.56.110
- Make sure that they can ping each other.
 - Connectivity test for Local Machine 1 to Server 1: Successful Not Successful
 - Connectivity test for Local Machine 1 to Server 2: Successful Not Successful
 - Connectivity test for Server 1 to Server 2: Successful Not Successful



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**
 - 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*

```
eysiili@ControlNode1: ~
File Edit View Search Terminal Help
eysiili@ManageNode:~$ ssh eyesiili@192.168.56.109
The authenticity of host '192.168.56.109 (192.168.56.109)' can't be established.
ECDSA key fingerprint is SHA256:R/WJQiuUh92WOMMGm7mRzzue8fCv0KgEy39koTiarji0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.109' (ECDSA) to the list of known hosts.
eysiili@192.168.56.109'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.

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.

eysiili@ControlNode1:~$
```

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

```
eysiili@ControlNode1:~$ logout
Connection to 192.168.56.109 closed.
eysiili@ManageNode:~$
```

- Do the same for Server 2.

```

eysiili@ManageNode: ~
File Edit View Search Terminal Tabs Help
eysiili@ControlNode2: ~ x eysiili@ManageNode: ~ x
eysiili@ManageNode:~$ ssh eysiili@192.168.56.110
eysiili@192.168.56.110'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.

76 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: Tue Aug 15 17:36:09 2023 from 192.168.56.108
eysiili@ControlNode2:~$ logout
Connection to 192.168.56.110 closed.
eysiili@ManageNode:~$
```

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)

```

eysiili@ManageNode: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts

127.0.0.1      workstation
192.168.56.109 ControlNode1
192.168.56.110 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
```

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

```
eysiili@ManageNode: ~
File Edit View Search Terminal Help
S GNU nano 2.9.3 /etc/hosts

127.0.0.1      workstation
192.168.56.109 ControlNode1
192.168.56.110 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
```

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.

```
eysiili@ManageNode:~$ ssh eysiili@ControlNode1
The authenticity of host 'controlnode1 (192.168.56.109)' can't be established.
ECDSA key fingerprint is SHA256:R/WJQiUh92WOMMGm7mRzzue8fCv0KgEy39koTIarji0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'controlnode1' (ECDSA) to the list of known hosts.
eysiili@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.

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: Tue Aug 15 17:31:21 2023 from 192.168.56.108
eysiili@ControlNode1:~$
```

```
eysiili@ManageNode:~$ ssh eysiiii@ControlNode2
The authenticity of host 'controlnode2 (192.168.56.110)' can't be established.
ECDSA key fingerprint is SHA256:DT3QpnGx7lNTpBIqunccGCQkWF86oJNdQk6J53+F0KI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'controlnode2' (ECDSA) to the list of known hosts.
eysiili@controlnode2'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.

76 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: Tue Aug 15 17:37:27 2023 from 192.168.56.108
eysiili@ControlNode2:~$ logout
Connection to controlnode2 closed.
eysiili@ManageNode:~$
```

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 by adding the Ip address and the Control Nodes in the sudo nano /etc/hostname
2. How secured is SSH?
SSH is secured that it encrypts the keys and have user authentication for other modifications.

Conclusion:

In summary, accomplishing the specified goals showcases a strong understanding of cloud-based computing and network configuration. By effectively establishing and fine-tuning Virtual Machines using either Microsoft Azure or VirtualBox, you have demonstrated your capability in deploying and overseeing virtualized settings. Moreover, the successful establishment of a Virtual Network and the subsequent verification of VM connectivity highlight your adeptness in building and managing intricate network infrastructures. These achievements collectively underscore your

expertise in virtualization, cloud solutions, and network management – crucial proficiencies in the ever-changing digital arena.