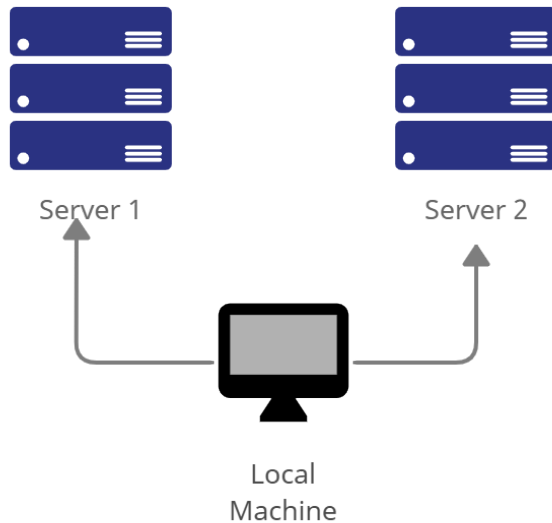



Name: Jasmin Raiza Tendencia	Date Performed: 08/14/2023
Course/Section: CPE31S4	Date Submitted: 08/15/2023
Instructor: Dr. Jonathan Taylar	Semester and SY: 1st 2023-2024
Activity 1: Configure Network using Virtual Machines	
1. Objectives: 1.1. Create and configure Virtual Machines in Microsoft Azure 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, <i>provide screenshots for each task.</i> (Note: it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine).	
 <pre> graph TD LocalMachine[Local Machine] --> Server1[Server 1] LocalMachine --> Server2[Server 2] </pre> <p>The diagram illustrates a network topology. At the bottom center is a computer icon labeled "Local Machine". Two lines extend from the "Local Machine" to two server racks. The server rack on the left is labeled "Server 1" and the server rack on the right is labeled "Server 2". Each server rack consists of three blue server units.</p>	
Installation of Virtual Machine:	



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: ✓

Folder:

ISO Image:

Edition:

Type:

Version:

☐ Skip Unattended Installation

ⓘ No ISO image is selected, the guest OS will need to be installed manually.


Help

Expert Mode

Back

Next

Cancel



Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB

Processors: 2

1 CPU 24 CPUs


☐ Enable EFI (special OSes only)

Help

Back

Next

Cancel



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

☒ Create a Virtual Hard Disk Now

Disk Size: 35.00 GB

☐ Pre-allocate Full Size

☐ Use an Existing Virtual Hard Disk File

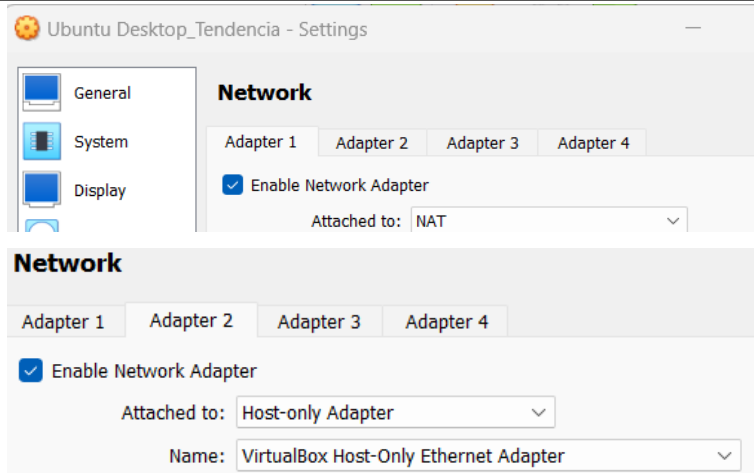
☐ Do Not Add a Virtual Hard Disk

Help

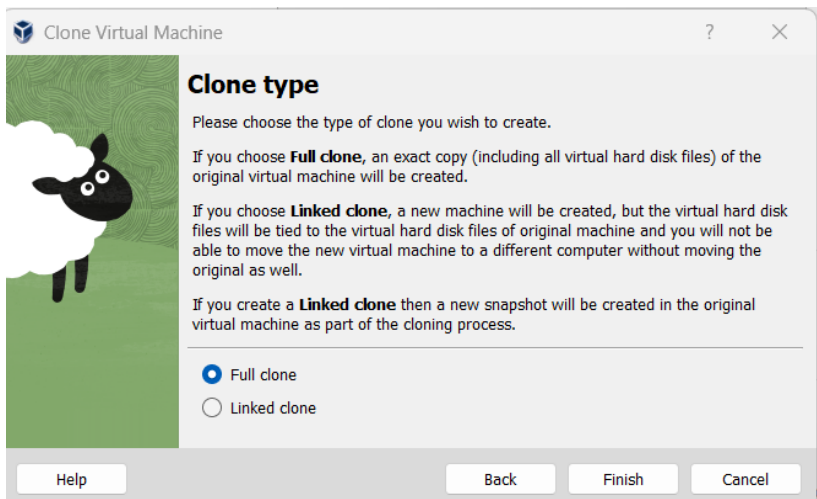
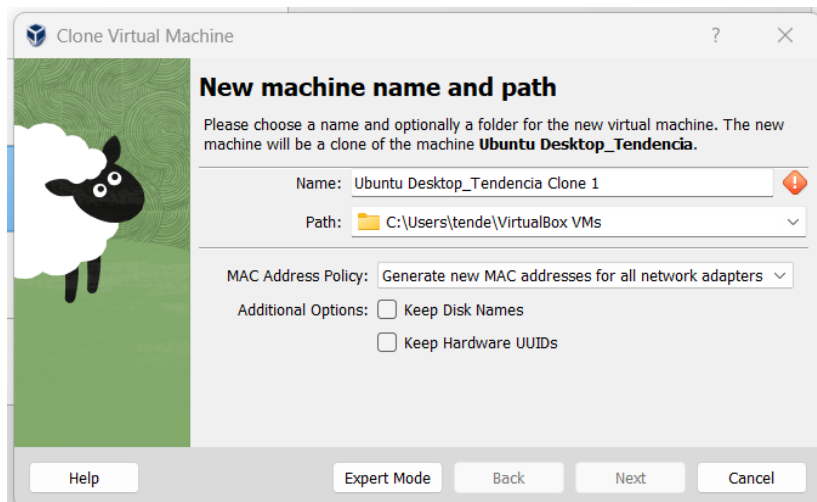
Back

Next

Cancel



Cloning:



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

```
tendencia@tendencia-VirtualBox:~$ sudo nano /etc/hostname
[sudo] password for tendencia:
```

```
GNU nano 6.2 /etc/hostname
tendencia-VirtualBox
```

```
GNU nano 6.2
server1
```

```
File Name to Write: /etc/hostname
^G Help          M-D DOS Format
^C Cancel        M-M Mac Format
```

```
[ Wrote 1 line ]
```

```
tendencia@tendencia-VirtualBox:~$ reboot
```

```
tendencia@server1:~$
```

- 1.2 Use server2 for Server 2

```
GNU nano 6.2
server2
```

```
tendencia@tendencia-VirtualBox:~$ reboot
```

```
tendencia@server2:~$
```

- 1.3 Use workstation for the Local Machine

```
GNU nano 6.2
workstation
```

```
tendencia@tendencia-VirtualBox:~$ reboot
```

```
tendencia@workstation:~$
```

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

```
tendencia@server1:~$ sudo nano /etc/hosts
[sudo] password for tendencia:
```

```
GNU nano 6.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    tendencia-VirtualBox

# 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

GNU nano 6.2
127.0.0.1    server1

Save modified buffer?
Y Yes
N No      ^C Cancel

File Name to Write: /etc/hosts
^G Help      M-D DOS Format
^C Cancel    M-M Mac Format

[ Wrote 8 lines ]
```

2.2 Type 127.0.0.1 server 2 for Server 2

```
tendencia@server2:~$ sudo nano /etc/hosts
[sudo] password for tendencia:
```

```
GNU nano 6.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    tendencia-VirtualBox

# 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

GNU nano 6.2
127.0.0.1    server2
```

2.3 Type 127.0.0.1 workstation for the Local Machine

```
tendencia@workstation:~$ sudo nano /etc/hosts
[sudo] password for tendencia:
```

```
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 tendencia-VirtualBox

# 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
```

```
GNU nano 6.2
127.0.0.1 workstation
```

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.

Server 1:

```
tendencia@server1:~$ sudo apt update | sudo apt upgrade -y

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
E: The repository 'http://security.ubuntu.com/ubuntu jammy-security InRelease' is no longer signed.
E: Failed to fetch http://security.ubuntu.com/ubuntu/dists/jammy-security/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
E: The repository 'http://ph.archive.ubuntu.com/ubuntu jammy InRelease' is no longer signed.
E: Failed to fetch http://ph.archive.ubuntu.com/ubuntu/dists/jammy/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
E: Failed to fetch http://ph.archive.ubuntu.com/ubuntu/dists/jammy-updates/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
```

Server 2:

```
tendencia@server2:~$ sudo apt update | sudo apt upgrade -y

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
E: The repository 'http://ph.archive.ubuntu.com/ubuntu jammy InRelease' is no longer signed.
E: Failed to fetch http://ph.archive.ubuntu.com/ubuntu/dists/jammy/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
E: The repository 'http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease' is no longer signed.
E: Failed to fetch http://ph.archive.ubuntu.com/ubuntu/dists/jammy-updates/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
E: Failed to fetch http://ph.archive.ubuntu.com/ubuntu/dists/jammy-backports/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
E: The repository 'http://ph.archive.ubuntu.com/ubuntu jammy-backports InRelease' is no longer signed.
E: Failed to fetch http://security.ubuntu.com/ubuntu/dists/jammy-security/InRelease
```

Local Machine:

```
tendencia@workstation:~$ sudo apt update | sudo apt upgrade -y
[sudo] password for tendencia:

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  gjs libgjs0g
The following packages will be upgraded:
  intel-microcode libldap-2.5-0 libldap-common
3 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
1 standard LTS security update
Need to get 0 B/6,315 kB of archives.
After this operation, 364 kB of additional disk space will be used.
E: The repository 'http://ph.archive.ubuntu.com/ubuntu jammy InRelease' is no longer signed.
E: Failed to fetch http://ph.archive.ubuntu.com/ubuntu/dists/jammy/InRelease Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
E: The repository 'http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease' is no longer signed.
```

2. Install the SSH server using the command *sudo apt install openssh-server*.
Server 1:

```
tendencia@server1:~$ sudo apt install openssh-server
[sudo] password for tendencia:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere 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 2 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-
server amd64 1:8.9p1-3ubuntu0.3 [38.8 kB]
Ign:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-
server amd64 1:8.9p1-3ubuntu0.3
Get:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-serve
r amd64 1:8.9p1-3ubuntu0.3 [434 kB]
Ign:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-serve
r amd64 1:8.9p1-3ubuntu0.3
```

Server 2:

```
tendencia@server2:~$ sudo apt install openssh-server
[sudo] password for tendencia:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere 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 2 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-
server amd64 1:8.9p1-3ubuntu0.3 [38.8 kB]
Ign:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-
server amd64 1:8.9p1-3ubuntu0.3
Get:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-serve
r amd64 1:8.9p1-3ubuntu0.3 [434 kB]
Ign:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-serve
r amd64 1:8.9p1-3ubuntu0.3
```

Local Machine:


```
tendencia@workstation:~$ sudo apt install openssh-server
[sudo] password for tendencia:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere 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 2 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-
server amd64 1:8.9p1-3ubuntu0.3 [38.8 kB]
Ign:1 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-
server amd64 1:8.9p1-3ubuntu0.3
Get:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-serve
r amd64 1:8.9p1-3ubuntu0.3 [434 kB]
Ign:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-serve
r amd64 1:8.9p1-3ubuntu0.3
Get:3 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term
```

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

3.1 *sudo service ssh start*

Server 1:

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

Server 2:

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

Local Machine:

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

3.2 *sudo systemctl status ssh*

Server 1:

```
tendencia@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 Tue 2023-08-15 15:49:27 PST; 1min 57s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 2618 (sshd)
      Tasks: 1 (limit: 2253)
     Memory: 1.7M
        CPU: 31ms
    CGroup: /system.slice/ssh.service
            └─2618 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 15 15:49:26 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 15:49:27 server1 sshd[2618]: Server listening on 0.0.0.0 port 22.
Aug 15 15:49:27 server1 sshd[2618]: Server listening on :: port 22.
Aug 15 15:49:27 server1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

Server 2:

```
tendencia@server2:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Tue 2023-08-15 15:49:20 PST; 3min 22s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 2512 (sshd)
      Tasks: 1 (limit: 2253)
     Memory: 1.7M
        CPU: 46ms
    CGroup: /system.slice/ssh.service
            └─2512 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 15 15:49:20 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 15:49:20 server2 sshd[2512]: Server listening on 0.0.0.0 port 22.
Aug 15 15:49:20 server2 sshd[2512]: Server listening on :: port 22.
Aug 15 15:49:20 server2 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

Local Machine:

```
tendencia@workstation:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Tue 2023-08-15 15:39:14 PST; 4min 50s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 2389 (sshd)
      Tasks: 1 (limit: 2253)
     Memory: 1.7M
        CPU: 35ms
    CGroup: /system.slice/ssh.service
            └─2389 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 15 15:39:14 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 15 15:39:14 workstation sshd[2389]: Server listening on 0.0.0.0 port 22.
Aug 15 15:39:14 workstation sshd[2389]: Server listening on :: port 22.
Aug 15 15:39:14 workstation systemd[1]: Started OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

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

4.1 *sudo ufw allow ssh*

Server 1:

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

Server 2:

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

Local Machine:

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

4.2 *sudo ufw enable*

Server 1:

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

Server 2:

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

Local Machine:

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

4.3 *sudo ufw status*

Server 1:

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

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

Server 2:

```
tendencia@server2:~$ sudo ufw status
Status: active

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

Local Machine:

```
tendencia@workstation:~$ 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

```
tendencia@server1:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::9c0b:ea2b:e2ce:929 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:83:31:11 txqueuelen 1000 (Ethernet)
    RX packets 947 bytes 1113669 (1.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 449 bytes 52403 (52.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::22b2:125c:201f:bd21 prefixlen 64 scopeid 0x20<link>
```

1.2 Server 2 IP address: 192.168.56.103

```
tendencia@server2:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::112f:f550:b812:128e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:92:95:97 txqueuelen 1000 (Ethernet)
    RX packets 947 bytes 1129506 (1.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 509 bytes 55815 (55.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::26fd:5341:31b7:2f52 prefixlen 64 scopeid 0x20<link>
```

1.3 Server 3 (Local) IP address: 192.168.56.101

```
tendencia@workstation:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::9851:ec68:fb8b:c6c7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e4:67:19 txqueuelen 1000 (Ethernet)
    RX packets 123 bytes 57229 (57.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 193 bytes 27241 (27.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
```

2. Make sure that they can ping each other.

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

```
tendencia@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=2.50 ms
 64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.67 ms
 64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.37 ms
 64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=1.64 ms
 64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=2.07 ms
 64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=1.53 ms
 64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=2.77 ms
^C
--- 192.168.56.102 ping statistics ---
 7 packets transmitted, 7 received, 0% packet loss, time 6136ms
 rtt min/avg/max/mdev = 1.369/1.935/2.766/0.488 ms
```

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

```
tendencia@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=34.3 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.20 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=1.99 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=1.46 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=1.84 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=1.75 ms
^C
--- 192.168.56.103 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6838ms
rtt min/avg/max/mdev = 1.197/6.313/34.279/11.419 ms
```

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

```
tendencia@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=5.10 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=2.12 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=6.87 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.983 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=1.79 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=1.78 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=64 time=1.04 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=64 time=1.85 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=64 time=1.57 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=64 time=2.76 ms
--- 192.168.56.103 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9045ms
rtt min/avg/max/mdev = 0.983/2.586/6.866/1.808 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 jvtaylor@192.168.56.120`

1.2 Enter the password for server 1 when prompted

```
tendencia@workstation:~$ ssh tendencia@192.168.56.102
tendencia@192.168.56.102's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue Aug 15 16:23:21 2023 from 192.168.56.101
tendencia@server1:~$
```

1.3 Verify that you are in server 1. The user should be in this format `user@server1`.

For example, `jvtaylor@server1`

```
tendencia@server1:~$
```

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

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

3. Do the same for Server 2.

```
tendencia@workstation:~$ ssh tendencia@192.168.56.103  
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.  
ED25519 key fingerprint is SHA256:Q8//pAoBFGLmUN7qrJX97dW5i7HphwKrkaxhldTeu8.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts  
.  
tendencia@192.168.56.103's password:  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
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.  
  
tendencia@server2:~$
```

```
tendencia@server2:~$  
logout  
Connection to 192.168.56.103 closed.  
tendencia@workstation:~$
```

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)


```

GNU nano 6.2 /etc/hosts *
127.0.0.1    workstation
192.168.56.102  server1
192.168.56.103  server2

# 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.

```

[ Wrote 10 lines ]

```

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.

Server 1:

```

tendencia@workstation:~$ ssh tendencia@server1
The authenticity of host 'server1 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:rNgHjyK9XmKgsGM0BERR0RoQTAGiWjprExyd7NMvRHc.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server1' (ED25519) to the list of known hosts.
tendencia@server1's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue Aug 15 18:28:55 2023 from 192.168.56.101
tendencia@server1:~$

```

Server 2:

```
tendencia@workstation:~$ ssh tendencia@server2
The authenticity of host 'server2 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:Q8//pAoBFGLmUN7qrJX97dW5i7HphwKrkaxhlhdTeu8.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server2' (ED25519) to the list of known hosts.
tendencia@server2's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue Aug 15 18:31:28 2023 from 192.168.56.101
tendencia@server2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?

The SSH client relies on the Domain Name System (DNS) to translate the hostname to an IP address which allows the usage of the hostname in SSH commands as if it were an IP address. We can use the `ssh tendencia@server1` instead of `ssh tendencia@192.168.56.102`.

Making sure that the hostname is resolvable through DNS, either by having an entry in local `/etc/hosts` file or by having the hostname properly configured in the network's DNS server. This way, the SSH client can perform the hostname-to-IP address resolution and establish the connection using the resolved IP address.

2. How secured is SSH?

SSH (Secure Shell) is considered to be a secure method for remote access and data communication where it offers several security features that contribute to its reputation:

- a. Encryption - it encrypts the data exchanged between the client and the server, which prevents eavesdropping and unauthorized access to the data being transmitted.
- b. Authentication: Passwords, public-key authentication, and multi-factor authentication (MFA). Public-key authentication is particularly secure because it involves a pair of keys: a private key stored securely on the client and a

corresponding public key stored on the server. This eliminates the need to transmit passwords over the network.

c. Data Integrity: Ensures that the data transferred between the client and server remains unchanged during transmission.

d. Host Key Verification: SSH uses host keys to verify the authenticity of the server. When connected to a server for the first time, the server's public key is presented to the SSH client, and if the key doesn't match what the client expects, it will send a signal. This helps prevent man-in-the-middle attacks.

e. Port Forwarding and Tunneling: SSH allows secure tunneling of various network services through the encrypted SSH connection. This feature enable to secure other services like web browsing or database access without exposing them directly to the network.

f. Configurable Access Control: Configuring SSH access to allow specific users, groups, or IP addresses, enhancing control over who can access the system.

While SSH is generally secure, there are potential vulnerabilities that can be exploited if not properly configured or maintained; including weak passwords, compromised private keys, outdated SSH versions, and misconfigurations. To maximize the security of SSH connections:

- Usage of strong, unique passwords or consider using public-key authentication.
- Regularly updated SSH software to benefit from security patches.
- Limit the users who have SSH access to your system.
- Harden the server's configuration by disabling unnecessary features.
- Monitor SSH logs.