Name: Bernice M. Peña	**Date Performed:** 08/22/2023
Course/Section: Managing Enterprise Servers/CPE31S5	**Date Submitted:** 08/23/2023
Instructor: Engr. Roman Richard	**Semester and SY:** 1st semester, 2023-2024

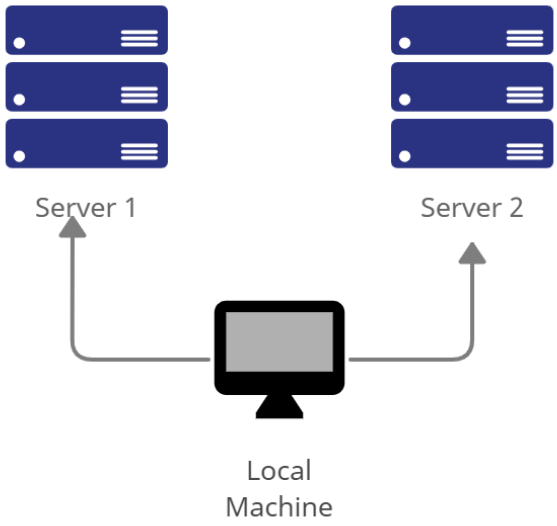
Activity 1: Configure Network using Virtual Machines

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:**

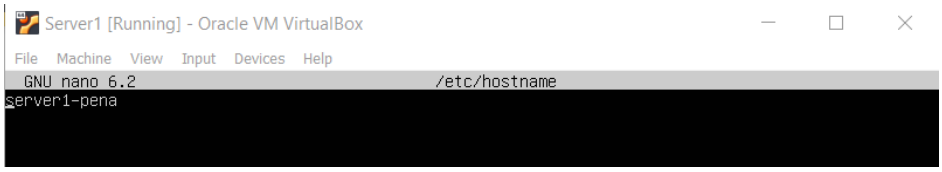
Network Topology:

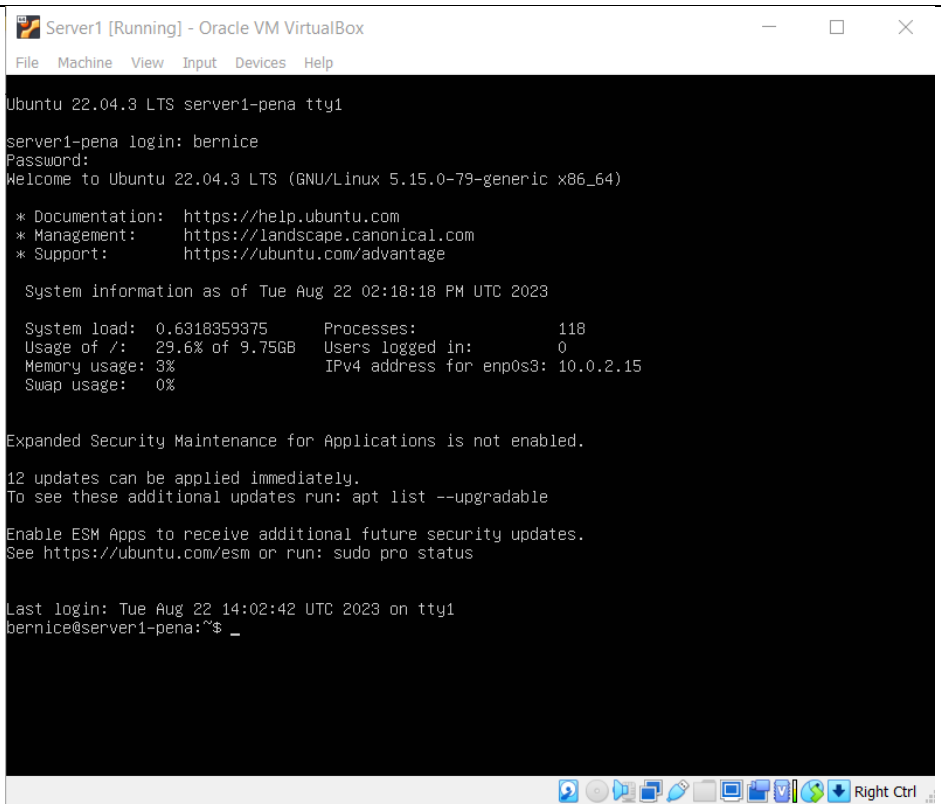
Assume that you have created the following network topology in Virtual Machines, *provide screenshots for each task*. (Note: *it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine*).



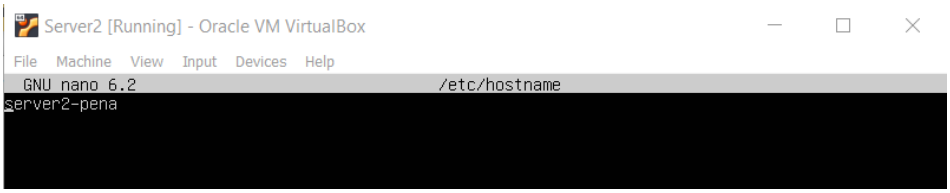
Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

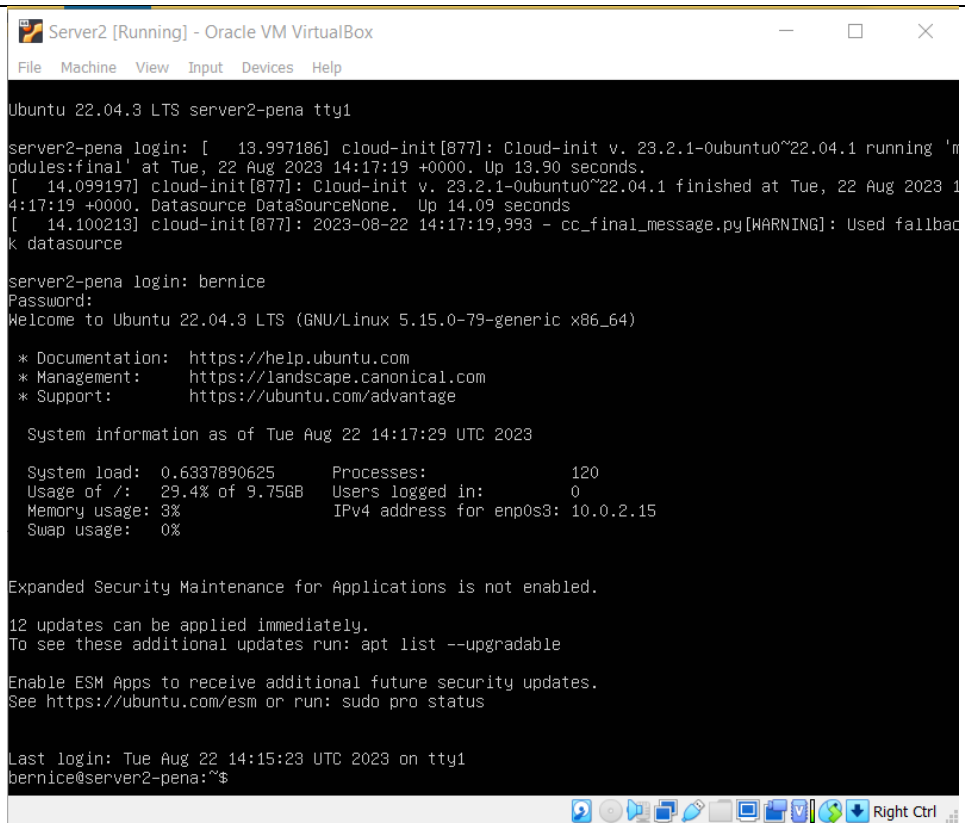
1. Change the hostname using the command *sudo nano /etc/hostname*
   1.1 Use server1 for Server 1





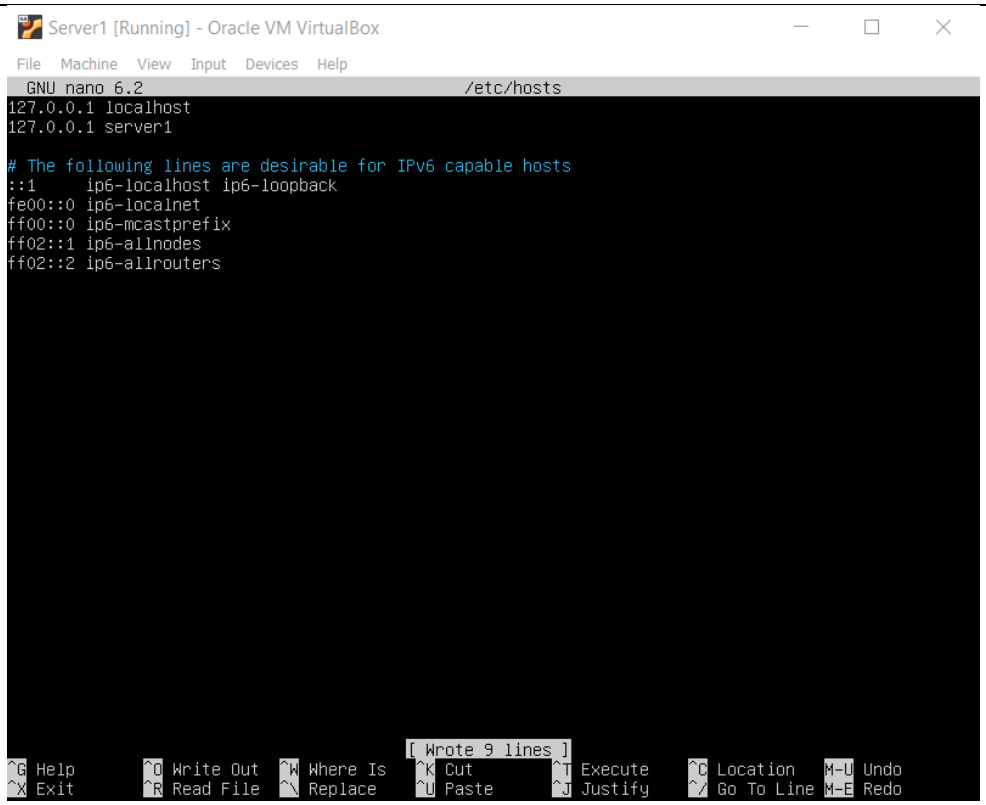
1.2 Use server2 for Server 2



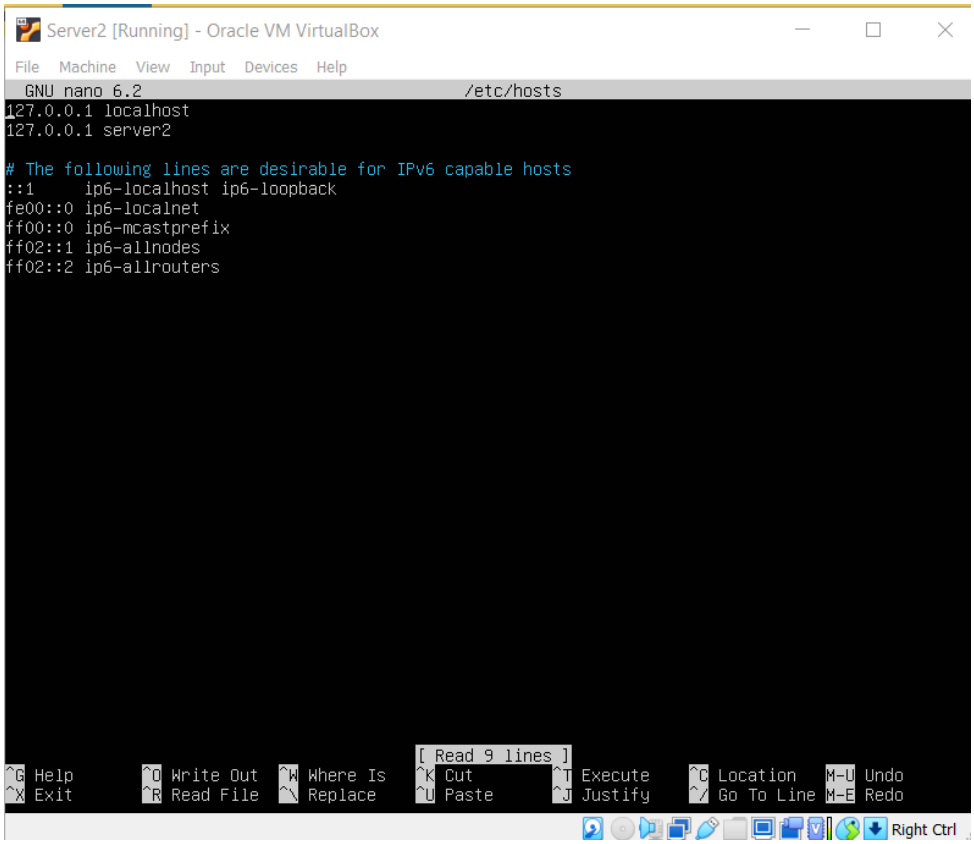


1.3 Use workstation for the Local Machine

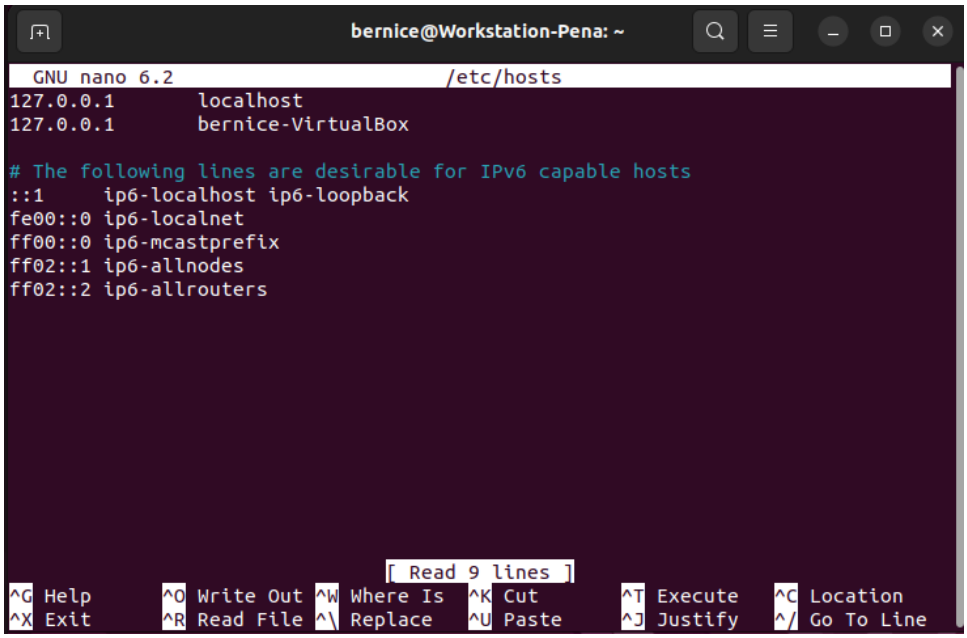
2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.
   2.1 Type 127.0.0.1 server 1 for Server 1



2.2 Type 127.0.0.1 server 2 for Server 2



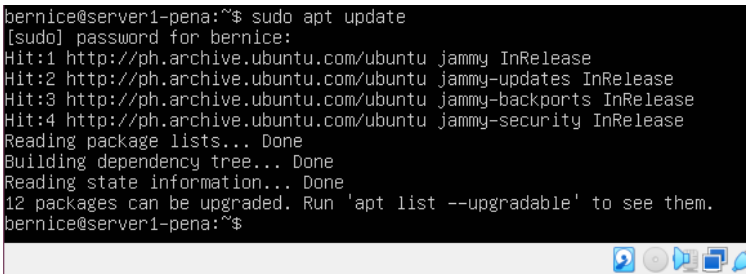
2.3 Type 127.0.0.1 workstation for the Local Machine

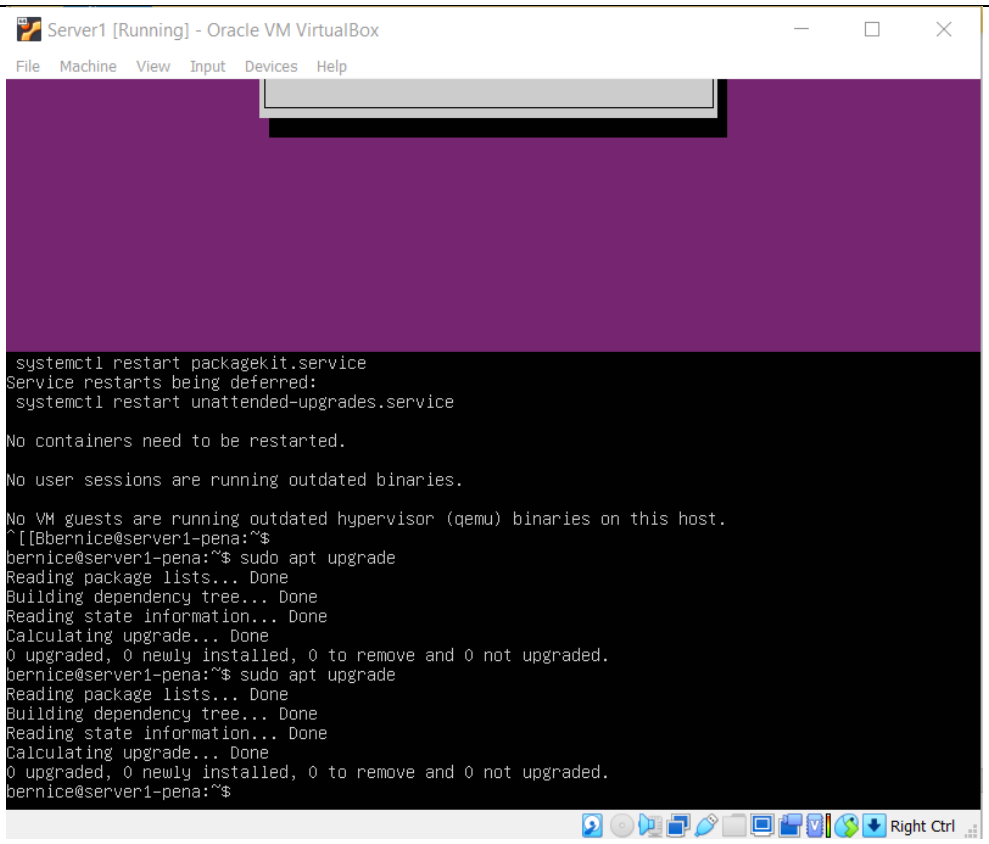


Task 2: Configure SSH on Server 1, Server 2, and Local Machine. Do the following:

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

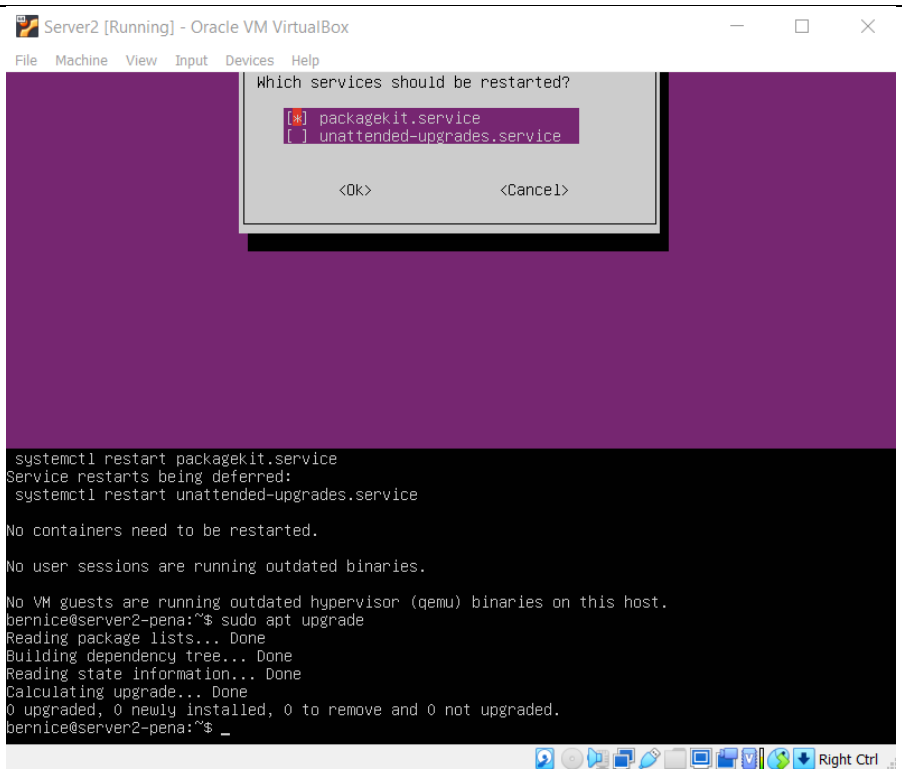
   Server 1:



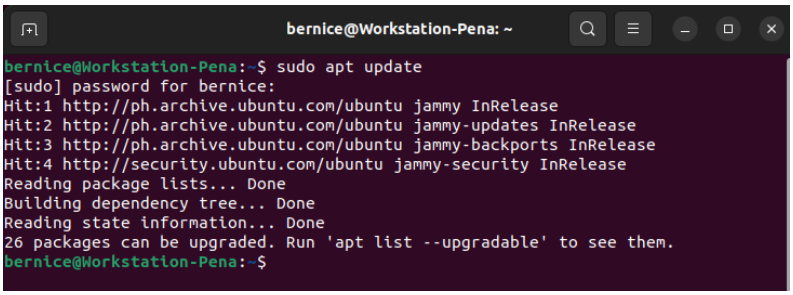


Server 2:

```
bernice@server2-pena:~$ sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
bernice@server2-pena:~$
```



Local Machine:



```
bernice@Workstation-Pena:~$ sudo apt upgrade
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:
  apt apt-utils ghostscript ghostscript-x gir1.2-javascriptcoregtk-4.0
  gir1.2-webkit2-4.0 initramfs-tools initramfs-tools-bin initramfs-tools-core
  intel-microcode libapt-pkg6.0 libgs9 libgs9-common
  libjavascriptcoregtk-4.0-18 libldap-2.5-0 libldap-common libsmbclient
  libtiff5 libwbclient0 libwebkit2gtk-4.0-37 samba-libs vim-common vim-tiny
  xxd
24 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
13 standard LTS security updates
Need to get 0 B/51.2 MB of archives.
After this operation, 364 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
(Reading database ... 162029 files and directories currently installed.)
Preparing to unpack .../libapt-pkg6.0_2.4.10_amd64.deb ...
Unpacking libapt-pkg6.0:amd64 (2.4.10) over (2.4.9) ...
Setting up libapt-pkg6.0:amd64 (2.4.10) ...
(Reading database ... 162029 files and directories currently installed.)
Preparing to unpack .../archives/apt_2.4.10_amd64.deb ...
Unpacking apt (2.4.10) over (2.4.9) ...
Setting up apt (2.4.10) ...
(Reading database ... 162029 files and directories currently installed.)
Preparing to unpack .../00-apt-utils_2.4.10_amd64.deb ...
Unpacking apt-utils (2.4.10) over (2.4.9) ...
Preparing to unpack .../01-libsmbclient_2%3a4.15.13+dfsg-0ubuntu1.3_amd64.deb ..
.
Unpacking libsmbclient:amd64 (2:4.15.13+dfsg-0ubuntu1.3) over (2:4.15.13+dfsg-0u
buntu1.2) ...
Preparing to unpack .../02-libldap-2.5-0_2.5.16+dfsg-0ubuntu0.22.04.1_amd64.deb
...
Unpacking libldap-2.5-0:amd64 (2.5.16+dfsg-0ubuntu0.22.04.1) over (2.5.15+dfsg-0
ubuntu0.22.04.1) ...
Preparing to unpack .../03-libwbclient0_2%3a4.15.13+dfsg-0ubuntu1.3_amd64.deb ..
```

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

Server 1:

```
bernice@server1-pena:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.3).
openssh-server set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
bernice@server1-pena:~$ _
```

Server 2:

```
bernice@server2-pena:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.3).
openssh-server set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
bernice@server2-pena:~$ _
```

Local Machine:

```
bernice@Workstation-Pena:~$ sudo apt install openssh-server
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]
Get:2 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.3 [434 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 6.3-2ubuntu0.1 [267 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10.1 kB]
Fetched 751 kB in 1s (797 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 162030 files and directories currently installed.)
```

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

3.1 *sudo service ssh start*

Server 1:

```
bernice@server1-pena:~$ sudo service ssh start
bernice@server1-pena:~$ _
```

Server 2:

```
bernice@server2-pena:~$ sudo service ssh start
bernice@server2-pena:~$
```

Local Machine:

```
bernice@Workstation-Pena:~$ sudo service ssh start
bernice@Workstation-Pena:~$
```

3.2 *sudo systemctl status ssh*

Server 1:

```
bernice@server1-pena:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-08-22 14:17:41 UTC; 25min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 713 (sshd)
      Tasks: 1 (limit: 7389)
     Memory: 4.4M
        CPU: 32ms
     CGroup: /system.slice/ssh.service
             └─713 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 14:17:41 server1-pena systemd[1]: Starting OpenBSD Secure Shell server...
Aug 22 14:17:41 server1-pena sshd[713]: Server listening on 0.0.0.0 port 22.
Aug 22 14:17:41 server1-pena systemd[1]: Started OpenBSD Secure Shell server.
Aug 22 14:17:41 server1-pena sshd[713]: Server listening on :: port 22.
bernice@server1-pena:~$
```

Server 2:

```
bernice@server2-pena:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-08-22 14:17:14 UTC; 26min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 711 (sshd)
      Tasks: 1 (limit: 7389)
     Memory: 4.4M
        CPU: 55ms
     CGroup: /system.slice/ssh.service
             └─711 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 14:17:14 server2-pena systemd[1]: Starting OpenBSD Secure Shell server...
Aug 22 14:17:14 server2-pena sshd[711]: Server listening on 0.0.0.0 port 22.
Aug 22 14:17:14 server2-pena sshd[711]: Server listening on :: port 22.
Aug 22 14:17:14 server2-pena systemd[1]: Started OpenBSD Secure Shell server.
bernice@server2-pena:~$ _
```

Local Machine:

```
bernice@Workstation-Pena:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
     Active: active (running) since Tue 2023-08-22 22:30:10 PST; 15min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 9786 (sshd)
      Tasks: 1 (limit: 7423)
     Memory: 1.7M
        CPU: 25ms
     CGroup: /system.slice/ssh.service
             └─9786 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 22 22:30:10 Workstation-Pena systemd[1]: Starting OpenBSD Secure Shell serv>
Aug 22 22:30:10 Workstation-Pena sshd[9786]: Server listening on 0.0.0.0 port 2>
Aug 22 22:30:10 Workstation-Pena sshd[9786]: Server listening on :: port 22.
Aug 22 22:30:10 Workstation-Pena systemd[1]: Started OpenBSD Secure Shell serve>
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:

```
bernice@server1-pena:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
bernice@server1-pena:~$ _
```

Server 2:

```
bernice@server2-pena:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
bernice@server2-pena:~$ _
```

Local Machine:

```
bernice@Workstation-Pena:~$ sudo ufw allow ssh
[sudo] password for bernice:
Rules updated
Rules updated (v6)
bernice@Workstation-Pena:~$
```

4.2 *sudo ufw enable*

Server 1:

```
bernice@server1-pena:~$ sudo ufw enable
Firewall is active and enabled on system startup
bernice@server1-pena:~$ _
```

Server 2:

```
bernice@server2-pena:~$ sudo ufw enable
Firewall is active and enabled on system startup
bernice@server2-pena:~$ _
```

Local Machine:

```
bernice@Workstation-Pena:~$ sudo ufw enable
Firewall is active and enabled on system startup
bernice@Workstation-Pena:~$
```

4.3 *sudo ufw status*

Server 1:

```
bernice@server1-pena:~$ sudo ufw status
Status: active

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

bernice@server1-pena:~$
```

Server 2:

```
bernice@server2-pena:~$ sudo ufw status
Status: active

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

bernice@server2-pena:~$
```

Local Machine:

```
bernice@Workstation-Pena:~$ sudo ufw status
Status: active

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

bernice@Workstation-Pena:~$
```

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: 192.168.56.101

```
bernice@server1-pena:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe89:746a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:89:74:6a  txqueuelen 1000  (Ethernet)
        RX packets 5659  bytes 8346156 (8.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1536  bytes 102237 (102.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 236  bytes 20771 (20.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 236  bytes 20771 (20.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.2 Server 2 IP address: 192.168.56.102

```
bernice@server2-pena:~$ ifconfig
enp0s3: 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::a00:27ff:fe6d:33b1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:6d:33:b1  txqueuelen 1000  (Ethernet)
        RX packets 5656  bytes 8346304 (8.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1636  bytes 108445 (108.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 252  bytes 21821 (21.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 252  bytes 21821 (21.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

bernice@server2-pena:~$
```

1.3 Server 3 IP address: 192.168.56.103

```
bernice@Workstation-Pena:~$ ifconfig
enp0s3: 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::bcee:c5ce:cd29:d455  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cd:28:b3  txqueuelen 1000  (Ethernet)
        RX packets 1213  bytes 1402206 (1.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 787  bytes 65870 (65.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 259  bytes 24819 (24.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 259  bytes 24819 (24.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Make sure that they can ping each other.

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

```
bernice@Workstation-Pena:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.437 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.865 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.532 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.638 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=64 time=1.02 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=0.974 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.786 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.877 ms
^C
--- 192.168.56.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7094ms
rtt min/avg/max/mdev = 0.437/0.766/1.024/0.197 ms
bernice@Workstation-Pena:~$
```

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

```
bernice@Workstation-Pena:~$ 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=0.992 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.605 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.745 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.651 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.803 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=1.19 ms
^C
--- 192.168.56.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5070ms
rtt min/avg/max/mdev = 0.605/0.831/1.193/0.203 ms
bernice@Workstation-Pena:~$
```

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

```
bernice@server1-pena:~$ 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=0.681 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.15 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.20 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.787 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.785 ms
^C
--- 192.168.56.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 0.681/0.919/1.197/0.210 ms
bernice@server1-pena:~$
```

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*

```
bernice@server1-pena:~$ ssh bernice@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:Y0RZum5jtR0DqvLmnin0sw8VcTmyuh4Ftx/s1akd7s0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ED25519) to the list of known hosts.
bernice@192.168.56.101's password:
```

1.2 Enter the password for server 1 when prompted

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

```
bernice@192.168.56.101's password:

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 03:48:49 PM UTC 2023

  System load:  0.0849609375      Processes:               114
  Usage of /:   29.7% of 9.75GB   Users logged in:         1
  Memory usage: 4%                IPv4 address for enp0s3: 192.168.56.101
  Swap usage:   0%


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 22 15:48:49 2023 from 192.168.56.103
bernice@server1-pena:~$
```

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

```
bernice@server1-pena:~$
logout
Connection to 192.168.56.101 closed.
bernice@Workstation-Pena:~$
```

3. Do the same for Server 2.

```
bernice@Workstation-Pena:~$ ssh bernice@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:6O/vC30PQrEAk+tmsT5JpfjmNXaQZ3/HQo8drtMxYzI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ED25519) to the list of known hosts.
bernice@192.168.56.102's password:
```

```
bernice@Workstation-Pena:~$ ssh bernice@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:6O/vC30PQrEAk+tmsT5JpfjmNXaQZ3/HQo8drtMxYzI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ED25519) to the list of known hosts.
bernice@192.168.56.102's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 16:14:03 UTC 2023

  System load:  0.0               Processes:               113
  Usage of /:   29.5% of 9.75GB   Users logged in:         1
  Memory usage: 4%                IPv4 address for enp0s3: 192.168.56.102
  Swap usage:   0%


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 22 14:17:29 2023
bernice@server2-pena:~$
```

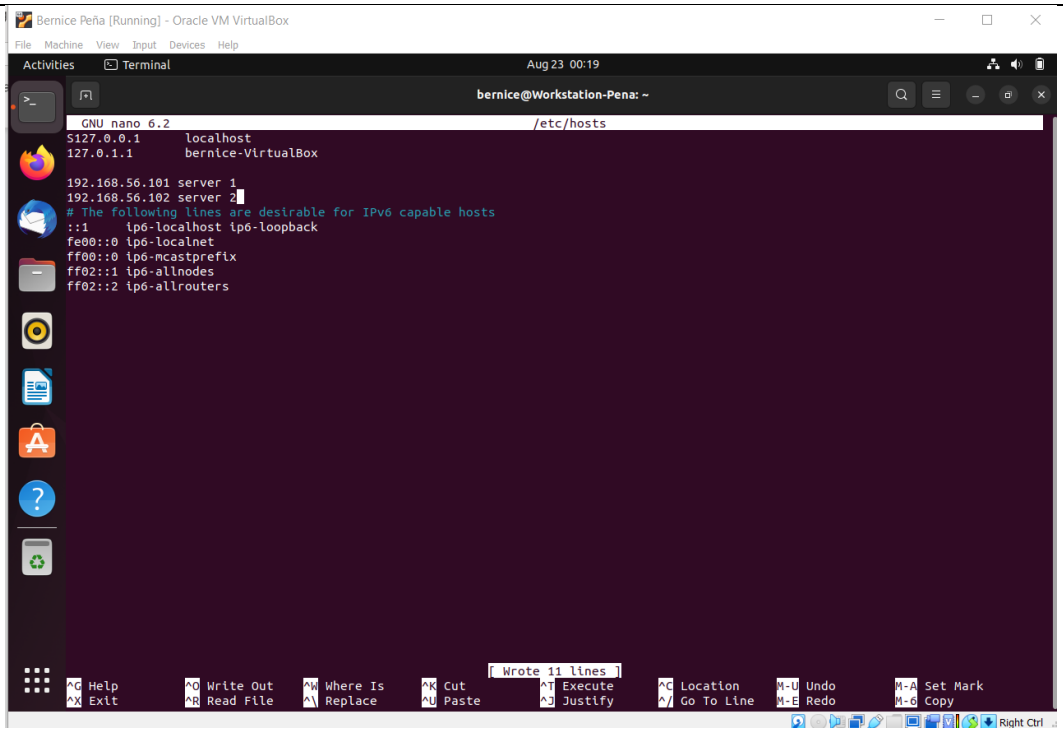
```
bernice@server2-pena:~$
logout
Connection to 192.168.56.102 closed.
bernice@Workstation-Pena:~$
```

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.

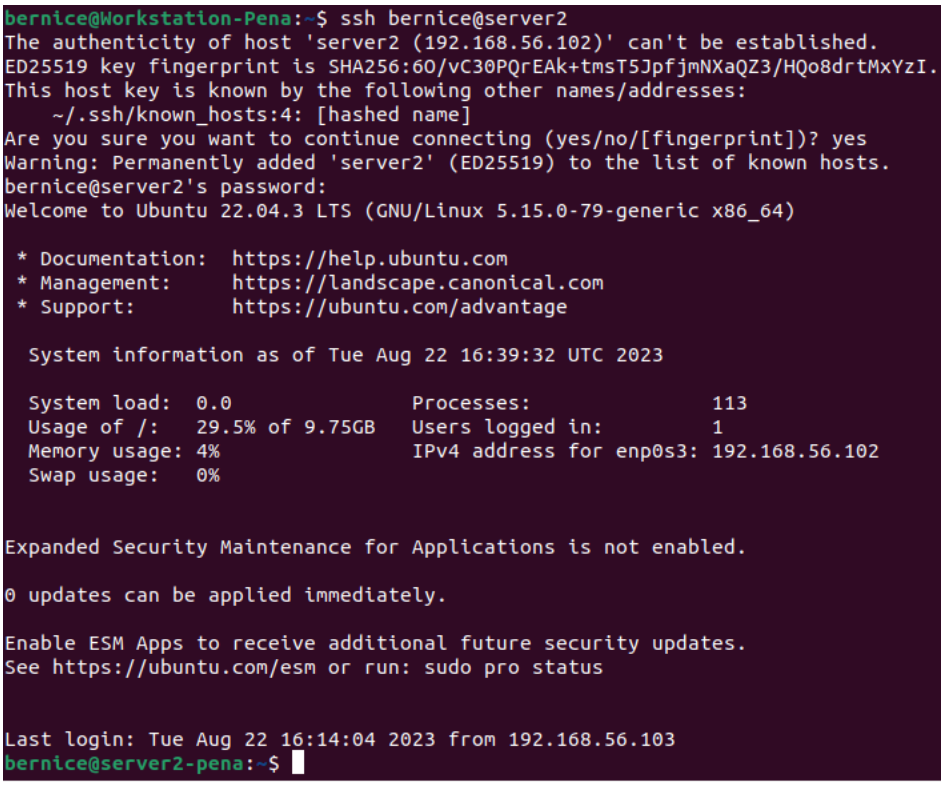


5. On the local machine, verify that you can do the SSH command but this time, use the hostname instead of typing the IP address of the servers. For example, try to do *ssh jvtaylar@server1*. Enter the password when prompted. Verify that you have entered Server 1. Do the same for Server 2.

Server 1:

```
bernice@Workstation-Pena:~$ ssh bernice@server1
The authenticity of host 'server1 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:Y0RZum5jtR0DqvLmnin0sw8VcTmyuh4Ftx/s1akd7s0.
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.
bernice@server1's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

  System information as of Tue Aug 22 04:37:31 PM UTC 2023

  System load:  0.080078125       Processes:               114
  Usage of /:   29.7% of 9.75GB   Users logged in:         1
  Memory usage: 4%                IPv4 address for enp0s3: 192.168.56.101
  Swap usage:   0%


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 22 16:10:50 2023 from 192.168.56.103
bernice@server1-pena:~$
```

Server 2:



Reflections:

Answer the following:

1. How ar0065 we able to use the hostname instead of IP address in SSH commands?
   The "DNS" domain name system enables the substitution of hostnames for IP addresses in SSH commands. DNS serves as a public directory that converts human-readable hostnames (like "server1") to their corresponding numeric IP addresses (like "192.168.56.101"). When we specify the hostname in the SSH command, our local machine will refer to its DNS resolver configuration. It first checks its local address book, usually the /etc/hosts file, to find the hostname to IP address mapping. If found, it will use that IP address to connect. Otherwise, it will contact DNS servers on the Internet for hostname resolution. It's basically like using a friend's name to find their phone number in your contacts or look it up in a general directory.
2. How secured is SSH?
   SSH or Secure Shell is renowned for its security features, it provides a highly secure means of remote communication and data transfer. SSH ensures security through encryption, protecting data from interception by encrypting it during transmission, it also offers strong authentication mechanisms, including public key authentication, which enhances security by eliminating the need for passwords. Aside from these,

SSH includes server verification, which guards against impersonation attempts. Access control mechanisms enable administrators to specify who can access a system and what they can do once connected, audit trails maintain comprehensive records of user activities for security monitoring and compliance. With this being said, SSH is considered one of the most secure protocols for remote access and data transfer, but its effectiveness depends on proper configuration and adherence to security best practices.