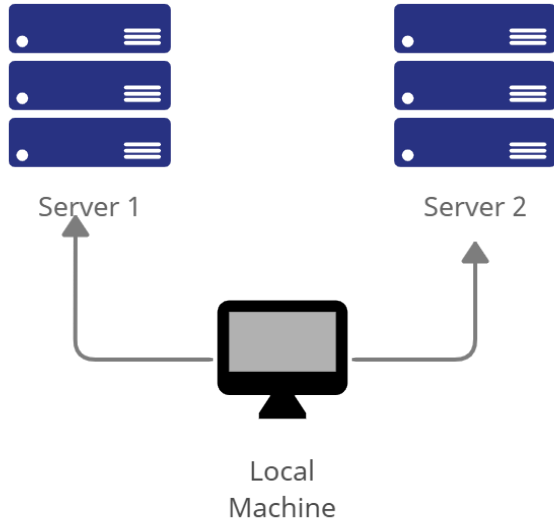


Name: Bacong, El Cid A.	Date Performed: 08/08/25
Course/Section: CPE 212 - CPE31S4	Date Submitted: 08/08/25
Instructor: Engr. Robin Valenzuela	Semester and SY: 1stSem SY 2025-2026
Activity 1: Configure Network using Virtual Machines	
1. Objectives: 1.1. Create and configure Virtual Machines in Microsoft 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: <i>it is assumed that you have the prior knowledge of cloning and creating snapshots in a virtual machine</i>).	
 <pre> graph TD LocalMachine[Local Machine] --> Server1[Server 1] LocalMachine --> Server2[Server 2] </pre> <p>The diagram illustrates a network topology where a central 'Local Machine' (represented by a monitor icon) is connected to two separate server stacks. 'Server 1' and 'Server 2' are each represented by three stacked server rack icons. Arrows point from the 'Local Machine' to both 'Server 1' and 'Server 2', indicating network connectivity.</p>	
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 <i>sudo nano /etc/hostname</i> 1.1 Use server1 for Server 1	
<pre> cidee@BacongCN:~\$ sudo nano /etc/hostname [sudo] password for cidee: </pre>	

server1

1.2 Use server2 for Server 2

```
cidee@BacongCN:~$ sudo nano /etc/hostname  
[sudo] password for cidee:
```

server2

1.3 Use workstation for the Local Machine

```
cidee@BacongCN:~$ sudo nano /etc/hostname  
[sudo] password for cidee:
```

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

```
GNU nano 2.9.3  
127.0.0.1 localhost  
127.0.0.1 server1
```

2.2 Type 127.0.0.1 server 2 for Server 2

```
GNU nano 2.9.3  
127.0.0.1 localhost  
127.0.0.1 server2
```

2.3 Type 127.0.0.1 workstation for the Local Machine

```
GNU nano 2.9.3 /  
127.0.0.1 localhost  
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.

```
cidee@workstation:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
cidee@workstation:~$ sudo apt upgrade
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.
The following security updates require Ubuntu Pro with 'esm-infra' enabled:
  libpam0g libsoup-gnome2.4-1 bluez libcroco3 libwebp6 libkrb5-3
  libgssapi-krb5-2 libpython3.6-minimal poppler-utils libnghttp2-14
  libisccfg160 libcups2 intel-microcode update-manager-core xserver-common
  vim-common gir1.2-soup-2.4 libapt-inst2.0 libldap-2.4-2 libpam-modules
  openssl libblockdev-swap2 bluez-cups libdw1 gir1.2-gdkpixbuf-2.0
  libgdk-pixbuf2.0-0 libc6-dbg libssh-4 imagemagick libwbclient0
  xserver-xorg-core-hwe-18.04 git-man libsystemd0 libraw16 apt libgd3
  libavahi-glib1 libgs9 snapd libpam-cap libsqlite3-0 update-manager
  liborc-0.4-0 libpython3.6-stdlib libcdb17 libelf1 python3-urllib3 binutils
```

```
cidee@server1:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
cidee@server1:~$ sudo apt upgrade
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.
The following security updates require Ubuntu Pro with 'esm-infra' enabled:
  libpam0g libsoup-gnome2.4-1 bluez libcroco3 libwebp6 libkrb5-3
  libgssapi-krb5-2 libpython3.6-minimal poppler-utils libnghttp2-14
  libisccfg160 libcups2 intel-microcode update-manager-core xserver-common
  vim-common gir1.2-soup-2.4 libapt-inst2.0 libldap-2.4-2 libpam-modules
  openssl libblockdev-swap2 bluez-cups libdw1 gir1.2-gdkpixbuf-2.0
  libgdk-pixbuf2.0-0 libc6-dbg libssh-4 imagemagick libwbclient0
  xserver-xorg-core-hwe-18.04 git-man libsystemd0 libraw16 apt libgd3
  libavahi-glib1 libgs9 snapd libpam-cap libsqlite3-0 update-manager
  liborc-0.4-0 libpython3.6-stdlib libcdb17 libelf1 python3-urllib3 binutils
```

```
cidee@server2:~$ sudo apt update
[sudo] password for cidee:
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
cidee@server2:~$ sudo apt upgrade
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.
The following security updates require Ubuntu Pro with 'esm-infra' enabled:
  libpam0g libsoup-gnome2.4-1 bluez libcroco3 libwebp6 libkrb5-3
  libgssapi-krb5-2 libpython3.6-minimal poppler-utils libnghttp2-14
  libiscfg160 libcups2 intel-microcode update-manager-core xserver-common
  vim-common gir1.2-soup-2.4 libapt-inst2.0 libldap-2.4-2 libpam-modules
  openssl libblockdev-swap2 bluez-cups libdw1 gir1.2-gdkpixbuf-2.0
  libgdk-pixbuf2.0-0 libc6-dbg libssh-4 imagemagick libwbclient0
  xserver-xorg-core-hwe-18.04 git-man libsystemd0 libraw16 apt libgd3
  libavahi-glib1 libgs9 snapd libpam-cap libsqlite3-0 update-manager
  liborc-0.4-0 libpython3.6-stdlib libcdio17 libelf1 python3-urllib3 binutils
  libmagickwand-6.q16-3 librs160 bind9-host libarchive13
```

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

```
cidee@workstation:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh_askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 3s (242 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
(Reading database ... 163342 files and directories currently installed.)
```

```
cidee@server1:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 3s (235 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
```

```

cidee@server2:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 637 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 3s (237 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.

```

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*

```

cidee@workstation:~$ sudo service ssh start
cidee@workstation:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2025-08-08 14:26:28 +08; 2min 19s ago
     Main PID: 2536 (sshd)
        Tasks: 1 (limit: 2318)
       CGroup: /system.slice/ssh.service
               └─2536 /usr/sbin/sshd -D

Aug 08 14:26:28 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 08 14:26:28 workstation sshd[2536]: Server listening on 0.0.0.0 port 22.
Aug 08 14:26:28 workstation sshd[2536]: Server listening on :: port 22.
Aug 08 14:26:28 workstation systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)

```

```

cidee@server1:~$ sudo service ssh start
cidee@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 Fri 2025-08-08 14:27:09 +08; 2min 28s ago
   Main PID: 2412 (sshd)
     Tasks: 1 (limit: 2318)
    CGroup: /system.slice/ssh.service
            └─2412 /usr/sbin/sshd -D

Aug 08 14:27:09 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 08 14:27:09 server1 sshd[2412]: Server listening on 0.0.0.0 port 22.
Aug 08 14:27:09 server1 sshd[2412]: Server listening on :: port 22.
Aug 08 14:27:09 server1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)

```

```

cidee@server2:~$ sudo service ssh start
cidee@server2:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2025-08-08 14:26:55 +08; 2min 21s ago
   Main PID: 2393 (sshd)
     Tasks: 1 (limit: 2318)
    CGroup: /system.slice/ssh.service
            └─2393 /usr/sbin/sshd -D

Aug 08 14:26:55 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 08 14:26:55 server2 sshd[2393]: Server listening on 0.0.0.0 port 22.
Aug 08 14:26:55 server2 sshd[2393]: Server listening on :: port 22.
Aug 08 14:26:55 server2 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*

```

cidee@workstation:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
cidee@workstation:~$ sudo ufw enable
Firewall is active and enabled on system startup
cidee@workstation:~$ sudo ufw status
Status: active

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

```

```
cidee@server1:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
cidee@server1:~$ sudo ufw enable
Firewall is active and enabled on system startup
cidee@server1:~$ sudo ufw status
Status: active
```

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

```
cidee@server2:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
cidee@server2:~$ sudo ufw enable
Firewall is active and enabled on system startup
cidee@server2:~$ sudo ufw status
Status: active
```

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

Task 3: Verify network settings on Server 1, Server 2, and Local Machine. On each device, do the following:

1. Record the ip address of Server 1, Server 2, and Local Machine. Issue the command *ifconfig* and check network settings. Note that the ip addresses of all the machines are in this network 192.168.56.XX.

1.1 Server 1 IP address: 192.168.56.105

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.105 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a1e7:7e68:21ee:e30e prefixlen 64 scopeid 0x20<link>
```

1.2 Server 2 IP address: 192.168.56.106

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.106 netmask 255.255.255.0 broadcast 192.168.56.255
```

1.3 Server 3 IP address: 192.168.56.104

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.104 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a1e7:7e68:21ee:e30e prefixlen 64 scopeid 0x20<link>
```

2. Make sure that they can ping each other.

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

```
cidee@workstation:~$ ping 192.168.56.105
PING 192.168.56.105 (192.168.56.105) 56(84) bytes of data.
64 bytes from 192.168.56.105: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 192.168.56.105: icmp_seq=2 ttl=64 time=0.419 ms
64 bytes from 192.168.56.105: icmp_seq=3 ttl=64 time=0.405 ms
64 bytes from 192.168.56.105: icmp_seq=4 ttl=64 time=0.408 ms
64 bytes from 192.168.56.105: icmp_seq=5 ttl=64 time=0.415 ms
64 bytes from 192.168.56.105: icmp_seq=6 ttl=64 time=0.410 ms
64 bytes from 192.168.56.105: icmp_seq=7 ttl=64 time=0.452 ms
64 bytes from 192.168.56.105: icmp_seq=8 ttl=64 time=0.421 ms
64 bytes from 192.168.56.105: icmp_seq=9 ttl=64 time=0.437 ms
64 bytes from 192.168.56.105: icmp_seq=10 ttl=64 time=0.441 ms
```

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

```
cidee@workstation:~$ ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=0.814 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=0.460 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=0.607 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=0.458 ms
64 bytes from 192.168.56.106: icmp_seq=5 ttl=64 time=0.430 ms
64 bytes from 192.168.56.106: icmp_seq=6 ttl=64 time=0.415 ms
64 bytes from 192.168.56.106: icmp_seq=7 ttl=64 time=0.417 ms
64 bytes from 192.168.56.106: icmp_seq=8 ttl=64 time=0.421 ms
```

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

```
cidee@server1:~$ ping 192.168.56.106
PING 192.168.56.106 (192.168.56.106) 56(84) bytes of data.
64 bytes from 192.168.56.106: icmp_seq=1 ttl=64 time=0.948 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=0.441 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=2.29 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=0.462 ms
64 bytes from 192.168.56.106: icmp_seq=5 ttl=64 time=0.441 ms
64 bytes from 192.168.56.106: icmp_seq=6 ttl=64 time=0.446 ms
64 bytes from 192.168.56.106: icmp_seq=7 ttl=64 time=0.434 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

```
cidee@workstation:~$ ssh cidee@192.168.56.105
The authenticity of host '192.168.56.105 (192.168.56.105)' can't be established
.
ECDSA key fingerprint is SHA256:yR0TFbLQhDye9zm9DQLEAHzVYS/k0/XeSVh6cehr1RY.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.56.105' (ECDSA) to the list of known hosts.
cidee@192.168.56.105'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/pro

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

228 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.
```

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

```
individual files in /usr/share/doc/*/copyright.

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

cidee@server1:~$
```

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

```
cidee@server1:~$ logout
Connection to 192.168.56.105 closed.
cidee@workstation:~$
```

3. Do the same for Server 2.

```
cidee@workstation:~$ ssh cidee@192.168.56.106
The authenticity of host '192.168.56.106 (192.168.56.106)' can't be established
.
ECDSA key fingerprint is SHA256:uGiX1mak2FzsFLBa/d8CBuNuTyUooo7f3Y4r2wEYYPM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.106' (ECDSA) to the list of known hosts.
cidee@192.168.56.106'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/pro

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

228 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.
```

```
cidee@server2:~$
```

```
cidee@server2:~$ logout
Connection to 192.168.56.106 closed.
cidee@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 2.9.3

/etc/hosts

```
127.0.0.1    localhost
127.0.0.1    workstation
# 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
192.168.56.105  server1
192.168.56.106  server2
```

4.3 Save the file and exit.

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

```
cidee@workstation:~$ ssh cidee@server1
The authenticity of host 'server1 (192.168.56.105)' can't be established.
ECDSA key fingerprint is SHA256:yR0TFbLQhDye9zm9DQLEAHzVYS/k0/XeSVh6cehr1RY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1' (ECDSA) to the list of known hosts.
cidee@server1's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

228 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: Fri Aug  8 14:43:09 2025 from 192.168.56.104
cidee@server1:~$
```

```
cidee@workstation:~$ ssh cidee@server2
The authenticity of host 'server2 (192.168.56.106)' can't be established.
ECDSA key fingerprint is SHA256:uGiX1mak2FzsFLBa/d8CBuNuTyUooo7f3Y4r2wEYYPM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
cidee@server2's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

228 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: Fri Aug  8 14:45:33 2025 from 192.168.56.104
cidee@server2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
We can use hostnames in SSH because our system resolves them to IP addresses using DNS or local methods like the hosts file. This makes connections easier to manage and remember, especially in networks where IPs might change.
2. How secured is SSH?
SSH is secure because it encrypts data and uses strong authentication methods. It protects against hackers and keeps connections safe, especially when set up with good practices like using keys and disabling root access.