Name: Zamora, Denzel	Date Performed: 08 / 17 / 23
Course/Section: CPE 232 - CPE31S6	Date Submitted: 08 / 17 / 23
Instructor: Dr. Jonathan Taylar	Semester and SY: 1st Sem 2023 -2024

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

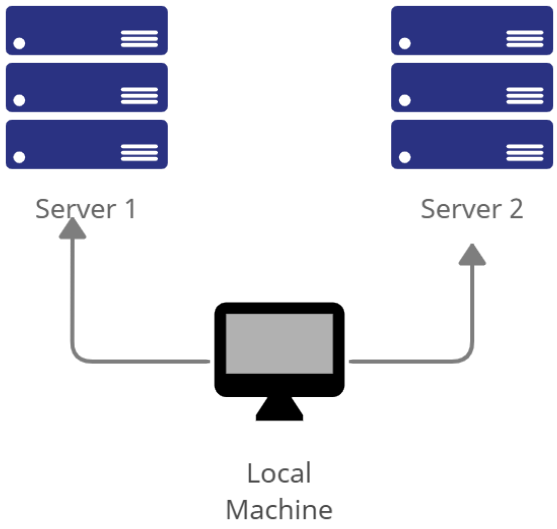
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

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

```
zamora@server1:~$
```

1.2 Use server2 for Server 2

```
zamora@server2:~$
```

1.3 Use workstation for the Local Machine

```
zamora@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
   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.

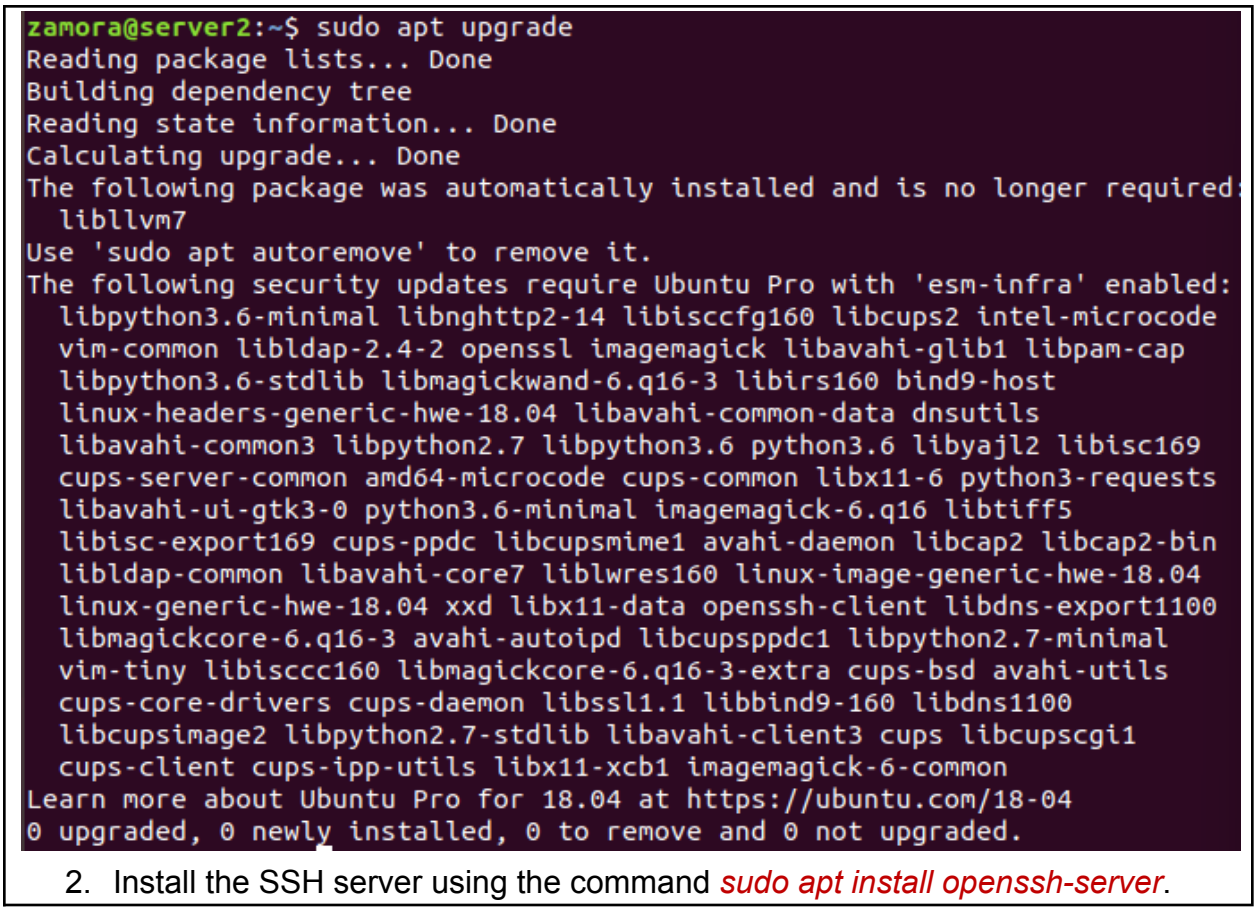
```
zamora@zamora-workstation:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```

```
zamora@zamora-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:
  libpython3.6-minimal libnghttp2-14 libisccfg160 libcups2 intel-microcode
  vim-common libldap-2.4-2 openssl imagemagick libavahi-glib1 libpam-cap
  libpython3.6-stdlib libmagickwand-6.q16-3 libirs160 bind9-host
  linux-headers-generic-hwe-18.04 libavahi-common-data dnsutils
  libavahi-common3 libpython2.7 libpython3.6 python3.6 libyajl2 libisc169
  cups-server-common amd64-microcode cups-common libx11-6 python3-requests
  libavahi-ui-gtk3-0 python3.6-minimal imagemagick-6.q16 libtiff5
  libisc-export169 cups-ppdc libcupsmime1 avahi-daemon libcap2 libcap2-bin
  libldap-common libavahi-core7 liblwres160 linux-image-generic-hwe-18.04
  linux-generic-hwe-18.04 xxd libx11-data openssh-client libdns-export1100
  libmagickcore-6.q16-3 avahi-autoipd libcupsppdc1 libpython2.7-minimal
  vim-tiny libisccc160 libmagickcore-6.q16-3-extra cups-bsd avahi-utils
  cups-core-drivers cups-daemon libssl1.1 libbind9-160 libdns1100
  libcupsimage2 libpython2.7-stdlib libavahi-client3 cups libcupscgi1
  cups-client cups-ipp-utils libx11-xcb1 imagemagick-6-common
Learn more about Ubuntu Pro for 18.04 at https://ubuntu.com/18-04
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
zamora@server1:~$ sudo apt update
[sudo] password for zamora:
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```

```
zamora@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:
  libpython3.6-minimal libnghttp2-14 libisccfg160 libcups2 intel-microcode
  vim-common libldap-2.4-2 openssl imagemagick libavahi-glib1 libpam-cap
  libpython3.6-stdlib libmagickwand-6.q16-3 libirs160 bind9-host
  linux-headers-generic-hwe-18.04 libavahi-common-data dnsutils
  libavahi-common3 libpython2.7 libpython3.6 python3.6 libyajl2 libisc169
  cups-server-common amd64-microcode cups-common libx11-6 python3-requests
  libavahi-ui-gtk3-0 python3.6-minimal imagemagick-6.q16 libtiff5
  libisc-export169 cups-ppdc libcupsmime1 avahi-daemon libcap2 libcap2-bin
  libldap-common libavahi-core7 liblwres160 linux-image-generic-hwe-18.04
  linux-generic-hwe-18.04 xxd libx11-data openssh-client libdns-export1100
  libmagickcore-6.q16-3 avahi-autoipd libcupsppdc1 libpython2.7-minimal
  vim-tiny libisccc160 libmagickcore-6.q16-3-extra cups-bsd avahi-utils
  cups-core-drivers cups-daemon libssl1.1 libbind9-160 libdns1100
  libcupsimage2 libpython2.7-stdlib libavahi-client3 cups libcupscgi1
  cups-client cups-ipp-utils libx11-xcb1 imagemagick-6-common
Learn more about Ubuntu Pro for 18.04 at https://ubuntu.com/18-04
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
zamora@server2:~$ sudo apt update
[sudo] password for zamora:
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```



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

```
zamora@zamora-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://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 2s (313 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
```

```
zamora@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://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-ter
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-sft
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-ser
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-import-
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 8s (83.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ncurses-term.
(Reading database ... 162327 files and directories currently installed.)
```

```
zamora@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://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ncurses-t
m all 6.1-1ubuntu1.18.04.1 [248 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-s
p-server amd64 1:7.6p1-4ubuntu0.7 [45.5 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 openssh-s
ver amd64 1:7.6p1-4ubuntu0.7 [332 kB]
Get:4 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 ssh-impor
id all 5.7-0ubuntu1.1 [10.9 kB]
Fetched 637 kB in 31s (20.4 kB/s)
Preconfiguring packages ...
```

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*

```
zamora@zamora-workstation:~$ sudo service ssh start
zamora@zamora-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 Thu 2023-08-17 17:41:18 PST; 2min 52s ago
 Main PID: 2640 (sshd)
    Tasks: 1 (limit: 4656)
   CGroup: /system.slice/ssh.service
           └─2640 /usr/sbin/sshd -D

Aug 17 17:41:18 zamora-workstation systemd[1]: Starting OpenBSD Secure Shell se
Aug 17 17:41:18 zamora-workstation sshd[2640]: Server listening on 0.0.0.0 port
Aug 17 17:41:18 zamora-workstation sshd[2640]: Server listening on :: port 22.
Aug 17 17:41:18 zamora-workstation systemd[1]: Started OpenBSD Secure Shell ser
 ESCOD
```

```
zamora@server1:~$ sudo service ssh start
zamora@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 Thu 2023-08-17 17:41:33 PST; 6min ago
 Main PID: 2617 (sshd)
    Tasks: 1 (limit: 4656)
   CGroup: /system.slice/ssh.service
           └─2617 /usr/sbin/sshd -D

Aug 17 17:41:33 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:41:33 server1 sshd[2617]: Server listening on 0.0.0.0 port 22.
Aug 17 17:41:33 server1 sshd[2617]: Server listening on :: port 22.
Aug 17 17:41:33 server1 systemd[1]: Started OpenBSD Secure Shell server.
```

```
zamora@server2:~$ sudo service ssh start
zamora@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 Thu 2023-08-17 17:41:51 PST; 6min ago
 Main PID: 2624 (sshd)
    Tasks: 1 (limit: 4656)
   CGroup: /system.slice/ssh.service
           └─2624 /usr/sbin/sshd -D

Aug 17 17:41:51 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:41:51 server2 sshd[2624]: Server listening on 0.0.0.0 port 22.
Aug 17 17:41:51 server2 sshd[2624]: Server listening on :: port 22.
Aug 17 17:41:51 server2 systemd[1]: Started OpenBSD Secure Shell server.
```

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*

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

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

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

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

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

```
zamora@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::2f2a:bccd:72af:78b6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e2:ad:52  txqueuelen 1000  (Ethernet)
        RX packets 1400  bytes 1801770 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 906  bytes 76478 (76.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.105  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::704e:6029:1a62:5244  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bb:f0:4a  txqueuelen 1000  (Ethernet)
        RX packets 221  bytes 25639 (25.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 8979 (8.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.2 Server 2 IP address: 192.168.56.106

```
zamora@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::3ea5:9de8:76df:3e2c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c8:a5:87  txqueuelen 1000  (Ethernet)
        RX packets 1404  bytes 1801488 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 920  bytes 77347 (77.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.106  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::7280:885f:da43:dc71  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2b:4a:d5  txqueuelen 1000  (Ethernet)
        RX packets 179  bytes 19483 (19.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 82  bytes 9657 (9.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.3 Server 3 IP address: 192.168.56.103

```
zamora@zamora-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::fbde:c31f:4937:3e85  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9f:68:80  txqueuelen 1000  (Ethernet)
        RX packets 1377  bytes 1772994 (1.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 762  bytes 67110 (67.1 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::853e:396f:3e2b:ef61  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:37:cb:97  txqueuelen 1000  (Ethernet)
        RX packets 207  bytes 24889 (24.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 82  bytes 9727 (9.7 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

```
zamora@zamora-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=0.898 ms
64 bytes from 192.168.56.105: icmp_seq=2 ttl=64 time=0.408 ms
64 bytes from 192.168.56.105: icmp_seq=3 ttl=64 time=0.423 ms
64 bytes from 192.168.56.105: icmp_seq=4 ttl=64 time=0.398 ms
```

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

```
zamora@zamora-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=0.765 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=0.487 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=1.18 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=0.403 ms
64 bytes from 192.168.56.106: icmp_seq=5 ttl=64 time=1.04 ms
```

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

```
zamora@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=0.775 ms
64 bytes from 192.168.56.106: icmp_seq=2 ttl=64 time=0.474 ms
64 bytes from 192.168.56.106: icmp_seq=3 ttl=64 time=0.441 ms
64 bytes from 192.168.56.106: icmp_seq=4 ttl=64 time=1.11 ms
64 bytes from 192.168.56.106: icmp_seq=5 ttl=64 time=0.511 ms
```

Task 4: Verify SSH connectivity on Server 1, Server 2, and Local Machine.

1. On the Local Machine, issue the following commands:

1.1 ssh username@ip_address_server1 for example, *ssh jvtaylar@192.168.56.120*

1.2 Enter the password for server 1 when prompted

```
zamora@zamora-workstation:~$ ssh zamora@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:AxciOFGZRzSgWQGhH/mjar1kRV8F8X6sz2zGWtYFBws.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.105' (ECDSA) to the list of known hosts.
zamora@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 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.
```

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

```
zamora@server1:~$
```

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

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

3. Do the same for Server 2.

```
zamora@zamora-workstation:~$ ssh zamora@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:sdAZPzqTMamCkaYV/4iKkEDNTumx/aOxwDPvNhldUkA.
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.
zamora@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 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.
zamora@server2:~$
```

4. Edit the hosts of the Local Machine by issuing the command *sudo nano /etc/hosts.* Below all texts type the following:

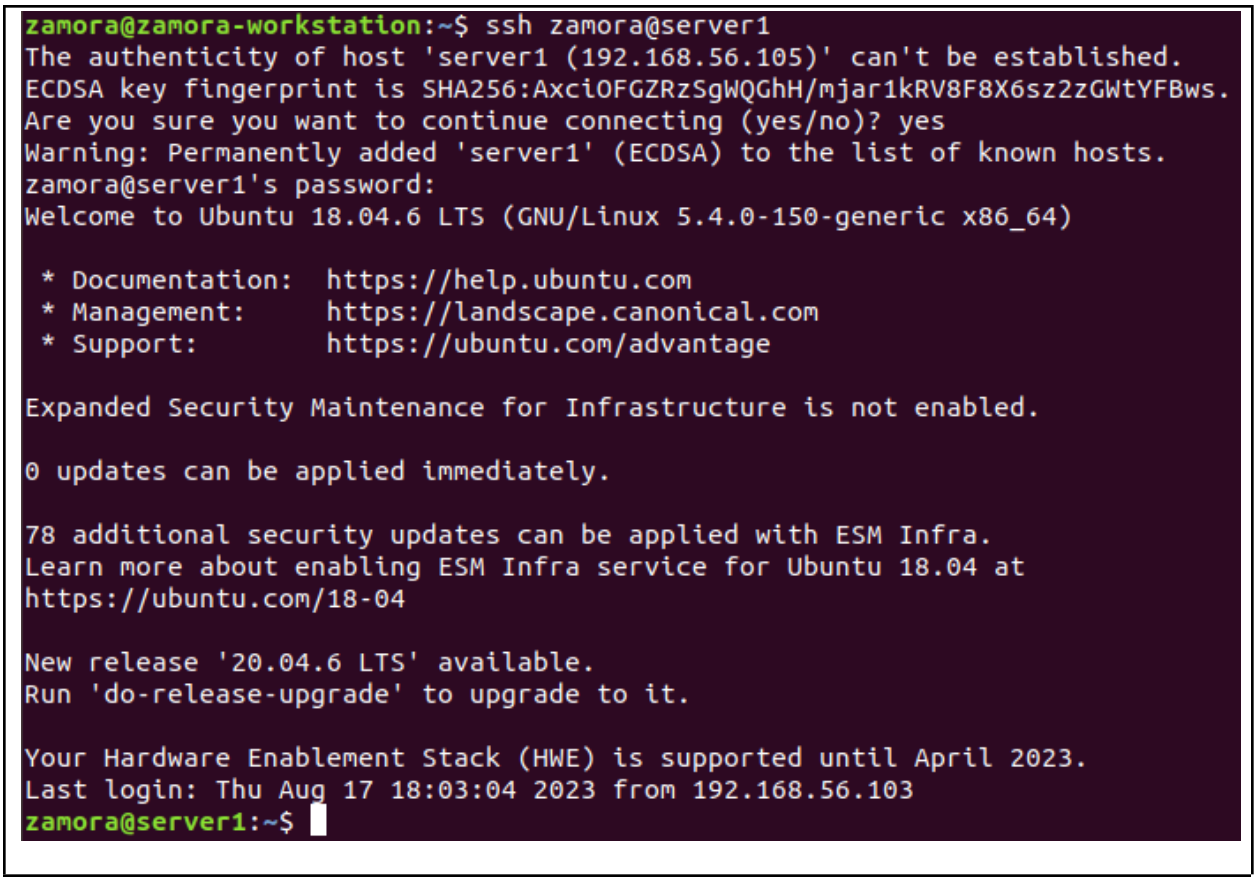
4.1 IP_address server 1 (provide the ip address of server 1 followed by the hostname)

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

4.3 Save the file and exit.

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

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.


zamora@zamora-workstation:~$ ssh zamora@server1
The authenticity of host 'server1 (192.168.56.105)' can't be established.
ECDSA key fingerprint is SHA256:AxciOFGZRzSgWQGhH/mjar1kRV8F8X6sz2zGWtYFBws.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1' (ECDSA) to the list of known hosts.
zamora@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/advantage
Expanded Security Maintenance for Infrastructure is not enabled.
0 updates can be applied immediately.
78 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: Thu Aug 17 18:03:04 2023 from 192.168.56.103
zamora@server1:~$

```
zamora@zamora-workstation:~$ ssh zamora@server2
The authenticity of host 'server2 (192.168.56.106)' can't be established.
ECDSA key fingerprint is SHA256:sdAZPzqTMamCkaYV/4iKkEDNTumx/aOxwDPvNhldUkA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
zamora@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/advantage

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

78 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: Thu Aug 17 18:04:39 2023 from 192.168.56.103
zamora@server2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
   - inside the sudo nano /etc/hosts, we encrypt the ip address of both server 1 & 2 and provide them their respective server names in order to indicate that ip address and server name are of one server.
2. How secure is SSH?
   - SSH provides a secure connection between servers using encryption.

Conclusion:

SSH provides a secure connection between servers using encryption. It allows remote access to servers making it easier and faster to access.