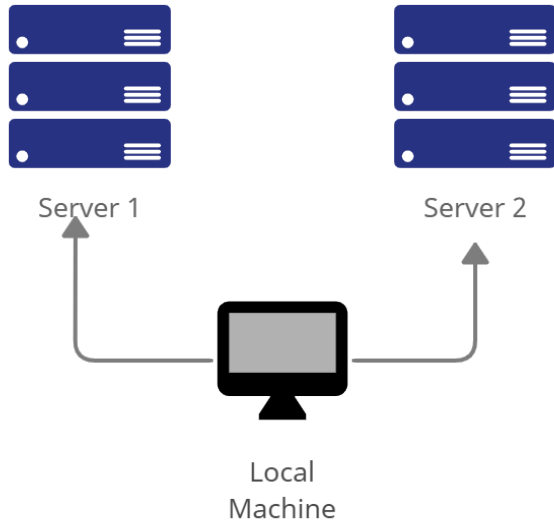


Name: Perez, Dean Lenard D.	Date Performed: 8/30/24
Course/Section: CPE 31S21	Date Submitted: 8/30/24
Instructor: Engr. Robin Valenzuela	Semester and SY: 1st 2024-225
Activity 1: Configure Network using Virtual Machines	
1. Objectives: 1.1. Create and configure Virtual Machines in Microsoft Azure or 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>).	
	
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>dldperez@server1:~\$ su root Password: root@server1:/home/dldperez# sudo nano /etc/hostname</pre>	

```
GNU nano 2.9.3 /etc/hostname
server1
```

```
dldperez@server1:~$
```

1.2 Use server2 for Server 2

```
dldperez@Perez:~$ su root
Password:
root@Perez:/home/dldperez# sudo nano /etc/hostname
```

```
GNU nano 2.9.3 /etc/hostname
server2
```

```
dldperez@server2:~$
```

1.3 Use workstation for the Local Machine

```
dldperez@hostname:~$ su root
Password:
root@hostname:/home/dldperez# sudo nano /etc/hostname
```

```
GNU nano 2.9.3 /etc/hostname
workstation
```

```
dldperez@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

```
root@server1:/home/dldperez# sudo nano /etc/hosts
```

```
GNU nano 2.9.3 /etc/hosts
1 127.0.0.1 localhost
127.0.0.1 Perez.myguest.virtualbox.org Perez
```

2.2 Type 127.0.0.1 server 2 for Server 2

```
root@server2: /home/dldperez
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts
1 127.0.0.1 localhost
127.0.0.1 Perez.myguest.virtualbox.org Perez

# 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
```

2.3 Type 127.0.0.1 workstation for the Local Machine

```
root@workstation: /home/dldperez
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/hosts
127.0.0.1 localhost
127.0.0.1 Perez.myguest.virtualbox.org Perez

# 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
```

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.

Local Machine

```
root@hostname:/home/dldperez# 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
217 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
Setting up libxpat1:amd64 (2.2.5-3ubuntu0.9) ...
Setting up libicu60:amd64 (60.2-3ubuntu3.2) ...
Setting up libjson-glib-1.0-common (1.4.2-3ubuntu0.18.04.1) ...
Setting up cups-server-common (2.2.7-1ubuntu2.10) ...
Setting up libllvm10:amd64 (1:10.0.0-4ubuntu1~18.04.2) ...
Setting up python3-apt (1.6.6) ...
Setting up libip4tc0:amd64 (1.6.1-2ubuntu2.1) ...
Setting up glib-networking-common (2.56.0-1ubuntu0.1) ...
Setting up nautilus-data (1:3.26.4-0~ubuntu18.04.6) ...
```

server1

```
root@server1:/home/dldperez# sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```

root@server1:/home/dldperez# 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 NEW packages will be installed:
  distro-info fwupd-signed gstreamer1.0-gtk3 libllvm10 libnetplan0 libxmb1
  linux-headers-5.4.0-150-generic linux-hwe-5.4-headers-5.4.0-150
  linux-image-5.4.0-150-generic linux-modules-5.4.0-150-generic
  linux-modules-extra-5.4.0-150-generic python3-click python3-colorama
  python3-dateutil ubuntu-advantage-desktop-daemon ubuntu-pro-client
  ubuntu-pro-client-l10n xdg-desktop-portal xdg-desktop-portal-gtk

```

server2

```

root@Perez:/home/dldperez# sudo apt update
Hit:1 http://ph.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
676 packages can be upgraded. Run 'apt list --upgradable' to see them.

```

```

root@Perez:/home/dldperez# 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 NEW packages will be installed:
  distro-info fwupd-signed gstreamer1.0-gtk3 libllvm10 libnetplan0 libxmb1
  linux-headers-5.4.0-150-generic linux-hwe-5.4-headers-5.4.0-150
  linux-image-5.4.0-150-generic linux-modules-5.4.0-150-generic
  linux-modules-extra-5.4.0-150-generic python3-click python3-colorama
  python3-dateutil ubuntu-advantage-desktop-daemon ubuntu-pro-client
  ubuntu-pro-client-l10n xdg-desktop-portal xdg-desktop-portal-gtk
The following packages will be upgraded:
  accountsservice amd64-microcode apparmor apport apport-gtk apt apt-utils
  aptdaemon aptdaemon-data aspell avahi-autoind avahi-daemon avahi-utils

```

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

Local Host

```

root@hostname:/home/dldperez# sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass

```

server1

```

root@server1:/home/dldperez# 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]

```

server2

```

root@Perez:/home/dldperez# 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

```

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*

Local Machine

```
root@workstation:/home/dldperez# sudo service ssh start
root@workstation:/home/dldperez# 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 2024-08-30 10:36:30 +08; 17min ago
   Process: 1074 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCE
   Process: 1069 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Process: 999 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 1022 (sshd)
    Tasks: 1 (limit: 2339)
   CGroup: /system.slice/ssh.service
           └─1022 /usr/sbin/sshd -D

Aug 30 10:36:29 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 30 10:36:30 workstation sshd[1022]: Server listening on 0.0.0.0 port 22.
Aug 30 10:36:30 workstation sshd[1022]: Server listening on :: port 22.
Aug 30 10:36:30 workstation systemd[1]: Started OpenBSD Secure Shell server.
Aug 30 10:36:31 workstation systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 30 10:36:31 workstation sshd[1022]: Received SIGHUP; restarting.
Aug 30 10:36:31 workstation sshd[1022]: Server listening on 0.0.0.0 port 22.
Aug 30 10:36:31 workstation sshd[1022]: Server listening on :: port 22.
lines 1-19/19 (END)
```

server1

```
dldperez@server1:~$ su root
Password:
root@server1:/home/dldperez# sudo service ssh start
sroot@server1:/home/dldperez# 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 2024-08-30 10:45:34 +08; 11min ago
   Process: 830 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCE
   Process: 826 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Process: 734 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 771 (sshd)
    Tasks: 1 (limit: 2318)
   CGroup: /system.slice/ssh.service
           └─771 /usr/sbin/sshd -D

Aug 30 10:45:33 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 30 10:45:34 server1 sshd[771]: Server listening on 0.0.0.0 port 22.
Aug 30 10:45:34 server1 sshd[771]: Server listening on :: port 22.
Aug 30 10:45:34 server1 systemd[1]: Started OpenBSD Secure Shell server.
Aug 30 10:45:35 server1 systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 30 10:45:35 server1 sshd[771]: Received SIGHUP; restarting.
Aug 30 10:45:35 server1 sshd[771]: Server listening on 0.0.0.0 port 22.
Aug 30 10:45:35 server1 sshd[771]: Server listening on :: port 22.
lines 1-19/19 (END)
```

server2

```

root@server2:/home/dldperez# sudo service ssh start
root@server2:/home/dldperez# 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 2024-08-30 10:23:39 +08; 32min ago
     Process: 864 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
     Process: 857 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Process: 767 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 791 (sshd)
      Tasks: 1 (limit: 2318)
     CGroup: /system.slice/ssh.service
             └─791 /usr/sbin/sshd -D

Aug 30 10:23:38 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 30 10:23:39 server2 sshd[791]: Server listening on 0.0.0.0 port 22.
Aug 30 10:23:39 server2 sshd[791]: Server listening on :: port 22.
Aug 30 10:23:39 server2 systemd[1]: Started OpenBSD Secure Shell server.
Aug 30 10:23:42 server2 systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 30 10:23:42 server2 sshd[791]: Received SIGHUP; restarting.
Aug 30 10:23:42 server2 sshd[791]: Server listening on 0.0.0.0 port 22.
Aug 30 10:23:42 server2 sshd[791]: Server listening on :: port 22.
lines 1-19/19 (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*

Local Machine

```

root@hostname:/home/dldperez# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@hostname:/home/dldperez# sudo ufw enable
Firewall is active and enabled on system startup
root@hostname:/home/dldperez# sudo ufw status
Status: active

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

root@hostname:/home/dldperez#

```

Server 1

```

root@server1:/home/dldperez# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@server1:/home/dldperez# sudo ufw enable
Firewall is active and enabled on system startup
root@server1:/home/dldperez# sudo ufw status
Status: active

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

root@server1:/home/dldperez#

```

Server 2

```

root@Perez:/home/dldperez# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@Perez:/home/dldperez# sudo ufw enable
Firewall is active and enabled on system startup
root@Perez:/home/dldperez# sudo ufw status
Status: active

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

root@Perez:/home/dldperez#

```

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 0 (workstation) IP address: 192.168.56.____

```

root@workstation:/home/dldperez# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.128 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::3bb1:90b4:5736:8880 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a0:cc:da txqueuelen 1000 (Ethernet)
    RX packets 277 bytes 56403 (56.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 100 bytes 11582 (11.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

1.2 Server 1 IP address: 192.168.56.____


```
root@server1:/home/dldperez# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.129 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::1fa7:824:915f:52cd prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:62:59:ec txqueuelen 1000 (Ethernet)
    RX packets 144 bytes 32087 (32.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 86 bytes 9857 (9.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

1.3 Server 2 IP address: 192.168.56.____

```
root@server2:/home/dldperez# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.130 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::bf84:b32c:ff61:47f8 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:26:a4:f4 txqueuelen 1000 (Ethernet)
    RX packets 535 bytes 102070 (102.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 99 bytes 12450 (12.4 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 **SUCCESSFUL**

```
dldperez@workstation:~$ ping 192.168.56.128
PING 192.168.56.128 (192.168.56.128) 56(84) bytes of data.
64 bytes from 192.168.56.128: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 192.168.56.128: icmp_seq=2 ttl=64 time=0.016 ms
64 bytes from 192.168.56.128: icmp_seq=3 ttl=64 time=0.031 ms
64 bytes from 192.168.56.128: icmp_seq=4 ttl=64 time=0.027 ms
^C
--- 192.168.56.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.016/0.023/0.031/0.008 ms
dldperez@workstation:~$
```

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

```
dldperez@workstation:~$ ping 192.168.56.130
PING 192.168.56.130 (192.168.56.130) 56(84) bytes of data.
64 bytes from 192.168.56.130: icmp_seq=1 ttl=64 time=0.929 ms
64 bytes from 192.168.56.130: icmp_seq=2 ttl=64 time=0.402 ms
64 bytes from 192.168.56.130: icmp_seq=3 ttl=64 time=0.528 ms
64 bytes from 192.168.56.130: icmp_seq=4 ttl=64 time=0.505 ms
64 bytes from 192.168.56.130: icmp_seq=5 ttl=64 time=0.802 ms
^C
--- 192.168.56.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.402/0.633/0.929/0.199 ms
dldperez@workstation:~$
```


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

```
root@server1:/home/dldperez# ping 192.168.56.130
PING 192.168.56.130 (192.168.56.130) 56(84) bytes of data.
64 bytes from 192.168.56.130: icmp_seq=1 ttl=64 time=0.984 ms
64 bytes from 192.168.56.130: icmp_seq=2 ttl=64 time=0.761 ms
64 bytes from 192.168.56.130: icmp_seq=3 ttl=64 time=0.584 ms
64 bytes from 192.168.56.130: icmp_seq=4 ttl=64 time=0.478 ms
64 bytes from 192.168.56.130: icmp_seq=5 ttl=64 time=0.489 ms
^C
--- 192.168.56.130 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4036ms
rtt min/avg/max/mdev = 0.478/0.659/0.984/0.192 ms
root@server1:/home/dldperez#
```

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

```
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.
```

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

```
Your Hardware Enablement Stack (HWE) is supported until April 2023.
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

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

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

For example, `jvtaylor@server1`

```
dldperez@server1:~$
```

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

```

ECDSA key fingerprint is SHA256:88Bs8igwzKIPjtjz900a2R2Y57Lm/Ms6DgdbFxEyEjE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.129' (ECDSA) to the list of known hosts.
dldperez@192.168.56.129'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.

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

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

dldperez@server1:~$

```

3. Do the same for Server 2.

```

root@workstation:/home/dldperez# ssh dldperez@192.168.56.130
dldperez@192.168.56.130'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.

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 11:07:29 2024 from 192.168.56.128
dldperez@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)

```

GNU nano 2.9.3 /etc/hosts
127.0.0.1    localhost
127.0.0.1    Perez.myguest.virtualbox.org    Perez
192.168.56.129 server1
192.168.56.130 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.

```

dldperez@server2:~$ logout
Connection to 192.168.56.130 closed.
root@workstation:/home/dldperez# sudo nano /etc/hosts
root@workstation:/home/dldperez# ssh dldperez@server1
The authenticity of host 'server1 (192.168.56.129)' can't be established.
ECDSA key fingerprint is SHA256:88Bs8igwzKIPjtjz900a2R2Y57Lm/Ms6DgdbFxEyEjE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1' (ECDSA) to the list of known hosts.
dldperez@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.

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 11:10:15 2024 from 192.168.56.128

```

```
dldperez@server1:~$ logout
Connection to server1 closed.
root@workstation:/home/dldperez# ssh dldperez@server2
The authenticity of host 'server2 (192.168.56.130)' can't be established.
ECDSA key fingerprint is SHA256:i25QI8FAaHGICNJQA1LZpRDzTqSZXemj0zaUGIn80gU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
dldperez@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.

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Fri Aug 30 11:12:09 2024 from 192.168.56.128
dldperez@server2:~$
```

Reflections:

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
We are able to use the hostname because the hostnames are assigned their own server and this server has its own IP addresses.
2. How secure is SSH?

It is very secure to use when accessing another computer from a different computer over an unsecured network because it uses encryption and authentication. But it also has its disadvantages.