Name: Lance Gebrielle A. Santos	Date Performed: 01/16/2024
Course/Section: CPE232 - CPE31S1	Date Submitted: 01/23/2024
Instructor: Dr. Jonathan V. Taylar	Semester and SY: 2nd Semester 2023-2024

Activity 1: Configure Network using Virtual Machines

1. **Objectives:**

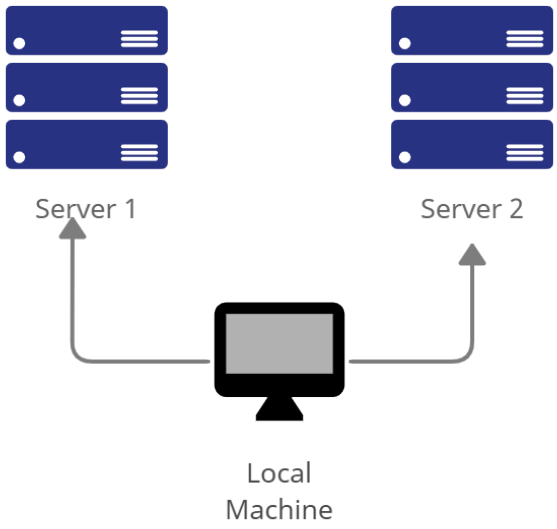
1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox

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*).

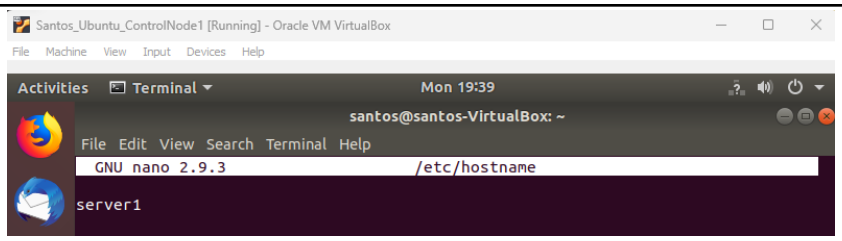


Task 1: Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

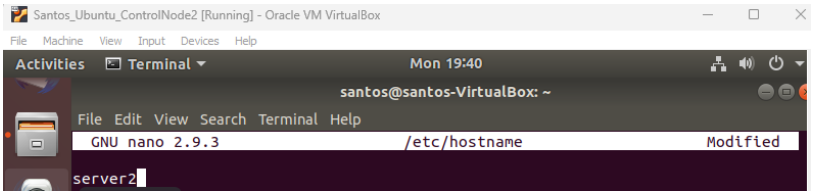
1. Change the hostname using the command *sudo nano /etc/hostname*

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

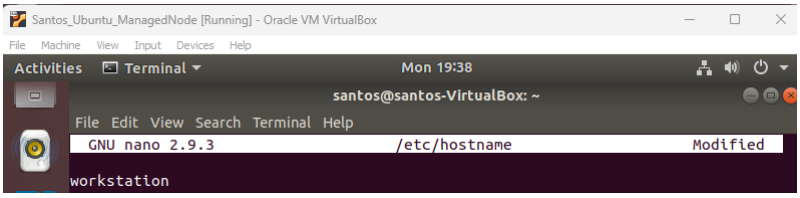
1.1 Use server1 for Server 1



1.2 Use server2 for Server 2

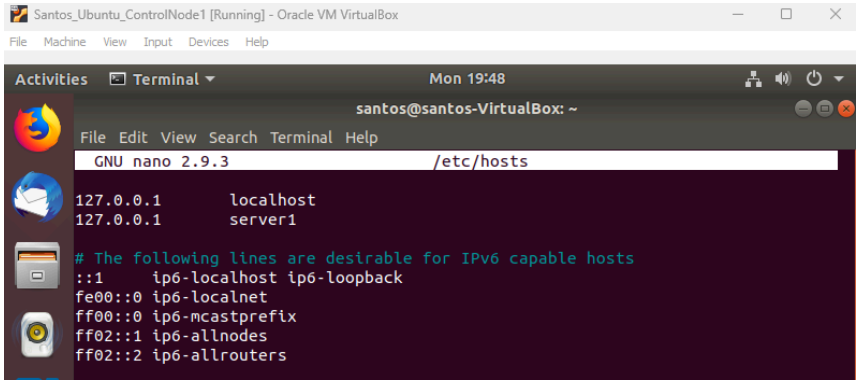


1.3 Use workstation for the Local Machine

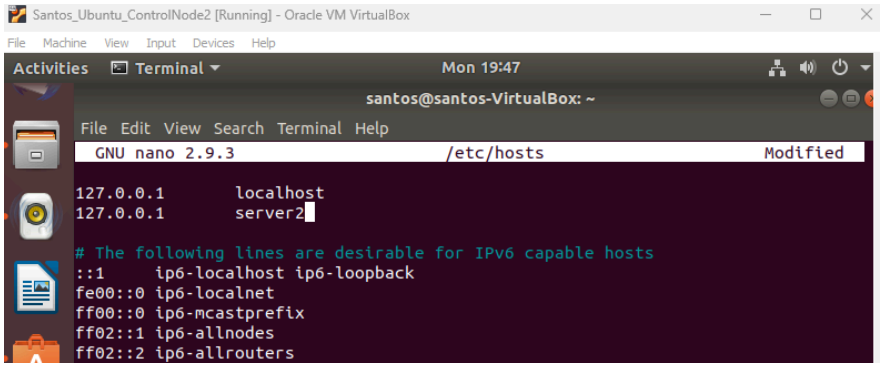


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

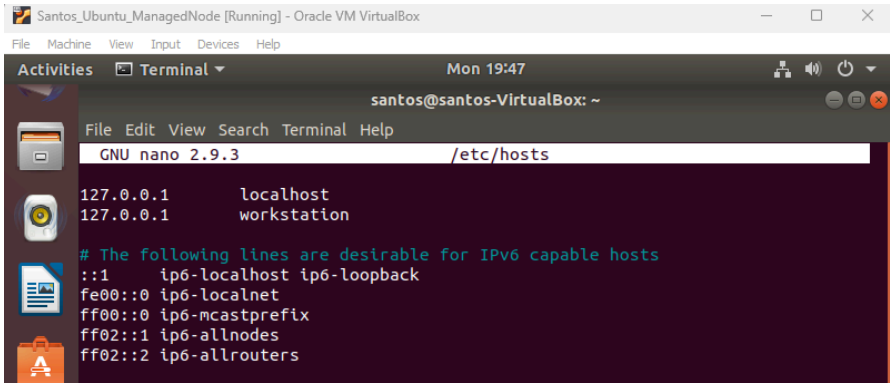
2.1 Type 127.0.0.1 server 1 for Server 1



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

```
santos@server1:~$ sudo apt update | sudo apt upgrade -y --fix-missing

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

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 libxmlb1
  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-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-autoipd avahi-daemon avahi-utils
  base-files bash bind9-host binutils binutils-common
  binutils-x86-64-linux-gnu bluez bluez-cups bluez-obexd bsdutils
  busybox-initramfs busybox-static bzip2 ca-certificates command-not-found
  command-not-found-data console-setup console-setup-linux cpio cpp cpp-7
```

   Server 2

```
santos@server2:~$ sudo apt update | sudo apt upgrade -y --fix-missing
[sudo] password for santos:
sudo: ignoring time stamp from the future
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 libxmlb1
  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-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-autoipd avahi-daemon avahi-utils
  base-files bash bind9-host binutils binutils-common
  binutils-x86-64-linux-gnu bluez bluez-cups bluez-obexd bsdutils
  busybox-initramfs busybox-static bzip2 ca-certificates command-not-found
  command-not-found-data console-setup console-setup-linux cpio cpp cpp-7
  cron cups cups-browsed cups-bsd cups-client cups-common cups-core-drivers
  cups-daemon cups-filters cups-filters-core-drivers cups-ipp-utils cups-ppdc
  cups-server-common dbus dbus-user-session dbus-x11 debconf debconf-i18n
  deja-dup dirmngr distro-info-data dmidecode dmsetup dnsmasq-base dnsutils
```

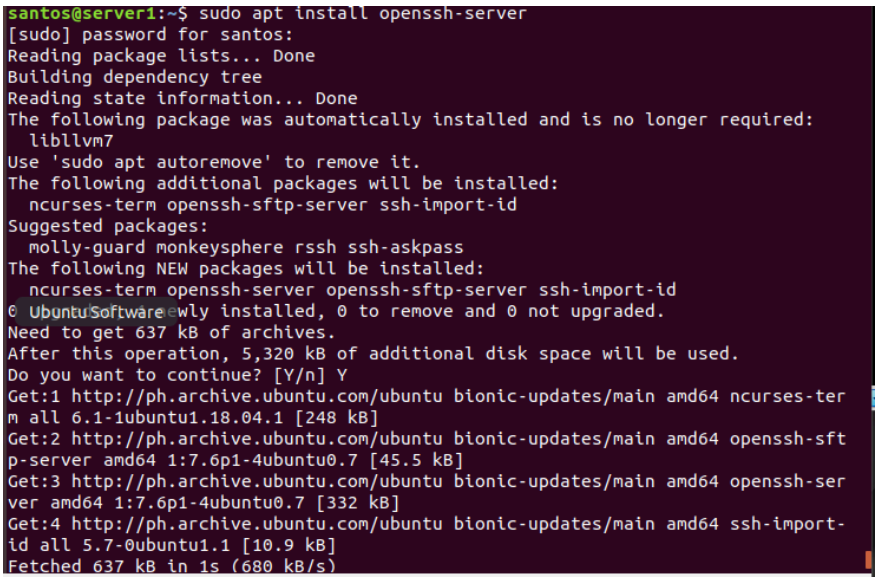
Local Machine

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

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

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 libxmlb1
  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-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-autoipd avahi-daemon avahi-utils
  base-files bash bind9-host binutils binutils-common
  binutils-x86-64-linux-gnu bluez bluez-cups bluez-obexd bsdutils
  busybox-initramfs busybox-static bzip2 ca-certificates command-not-found
  command-not-found-data console-setup console-setup-linux cpio cpp cpp-7
  cron cups cups-browsed cups-bsd cups-client cups-common cups-core-drivers
  cups-daemon cups-filters cups-filters-core-drivers cups-ipp-utils cups-ppdc
  cups-server-common dbus dbus-user-session dbus-x11 debconf debconf-i18n
```

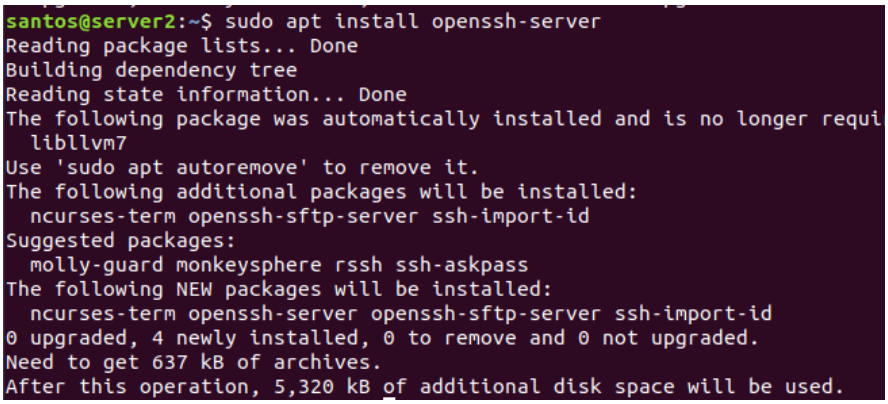
Right Ctrl

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

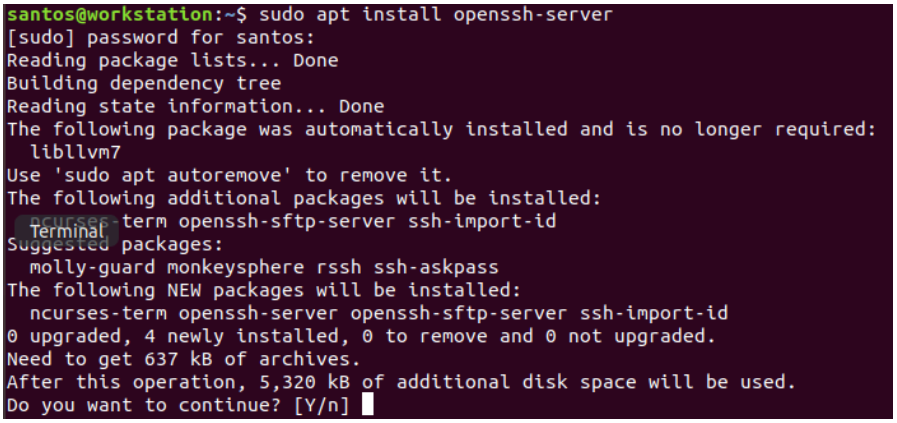
Server 1



Server 2



Local Machine



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

   3.1 *sudo service ssh start*

   Server 1

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

Server 2

```
Terminal
ver2:~$ sudo service ssh start
santos@server2:~$
```

Local Machine

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

3.2 *sudo systemctl status ssh*

Server 1

```
santos@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 Mon 2024-01-22 20:19:05 PST; 5min ago
   Main PID: 19666 (sshd)
      Tasks: 1 (limit: 4915)
     CGroup: /system.slice/ssh.service
             └─19666 /usr/sbin/sshd -D

Jan 22 20:19:05 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Jan 22 20:19:05 server1 sshd[19666]: Server listening on 0.0.0.0 port 22.
Jan 22 20:19:05 server1 sshd[19666]: Server listening on :: port 22.
Jan 22 20:19:05 server1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

Server 2

```
santos@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 Tue 2024-01-23 16:40:27 PST; 41s ago
   Main PID: 2649 (sshd)
      Tasks: 1 (limit: 4915)
     CGroup: /system.slice/ssh.service
             └─2649 /usr/sbin/sshd -D

Jan 23 16:40:27 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Jan 23 16:40:27 server2 sshd[2649]: Server listening on 0.0.0.0 port 22.
Jan 23 16:40:27 server2 sshd[2649]: Server listening on :: port 22.
Jan 23 16:40:27 server2 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

Local Machine

```
santos@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 Mon 2024-01-22 20:23:07 PST; 2min 29s ago
   Main PID: 19360 (sshd)
      Tasks: 1 (limit: 4915)
     CGroup: /system.slice/ssh.service
             └─19360 /usr/sbin/sshd -D

Jan 22 20:23:07 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Jan 22 20:23:07 workstation sshd[19360]: Server listening on 0.0.0.0 port 22.
Jan 22 20:23:07 workstation sshd[19360]: Server listening on :: port 22.
Jan 22 20:23:07 workstation 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*

Server 1

```
santos@server1:~$ sudo ufw allow ssh
[sudo] password for santos:
Rules updated
Rules updated (v6)
```

Server 2

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

Local Machine

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

4.2 *sudo ufw enable*

Server 1

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

Server 2

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

Local Machine

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

4.3 *sudo ufw status*

Server 1

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

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

Server 2

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

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

Local Machine

```
santos@workstation:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Welcome to Ubuntu
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.**125**

   ```
   192.168.56.125
   ```

   1.2 Server 2 IP address: 192.168.56.**126**

   ```
   192.168.56.126
   ```

   1.3 Server 3 IP address: 192.168.56.**124**

   ```
   192.168.56.124
   ```

2. Make sure that they can ping each other.
   2.1 Connectivity test for Local Machine 1 to Server 1: ☐ Successful ☐ Not Successful

   ```
   santos@workstation:~$ ping 192.168.56.125
   PING 192.168.56.125 (192.168.56.125) 56(84) bytes of data.
   64 bytes from 192.168.56.125: icmp_seq=1 ttl=64 time=1.77 ms
   64 bytes from 192.168.56.125: icmp_seq=2 ttl=64 time=1.26 ms
   64 bytes from 192.168.56.125: icmp_seq=3 ttl=64 time=0.564 ms
   64 bytes from 192.168.56.125: icmp_seq=4 ttl=64 time=1.41 ms
   64 bytes from 192.168.56.125: icmp_seq=5 ttl=64 time=0.466 ms
   64 bytes from 192.168.56.125: icmp_seq=6 ttl=64 time=1.90 ms
   ```

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

   ```
   santos@workstation:~$ ping 192.168.56.126
   PING 192.168.56.126 (192.168.56.126) 56(84) bytes of data.
   64 bytes from 192.168.56.126: icmp_seq=1 ttl=64 time=0.968 ms
   64 bytes from 192.168.56.126: icmp_seq=2 ttl=64 time=0.538 ms
   64 bytes from 192.168.56.126: icmp_seq=3 ttl=64 time=0.474 ms
   64 bytes from 192.168.56.126: icmp_seq=4 ttl=64 time=0.527 ms
   ```

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

   ```
   santos@server1:~$ ping 192.168.56.126
   PING 192.168.56.126 (192.168.56.126) 56(84) bytes of data.
   64 bytes from 192.168.56.126: icmp_seq=1 ttl=64 time=1.82 ms
   64 bytes from 192.168.56.126: icmp_seq=2 ttl=64 time=0.821 ms
   64 bytes from 192.168.56.126: icmp_seq=3 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 jvtaylar@192.168.56.120*

1.2 Enter the password for server 1 when promptedVerify that you are in server 1. The user should be in this format user@server1. For example, *jvtaylar@server1*

```
santos@workstation:~$ ssh santos@192.168.56.125
The authenticity of host '192.168.56.125 (192.168.56.125)' can't be established
.
ECDSA key fingerprint is SHA256:h6AgC48Gzp9cufmazizM/dnvhVWO7IvhZZ+ChOtFMgo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.125' (ECDSA) to the list of known hosts.
santos@192.168.56.125's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.18.0-15-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.
*** System restart required ***

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

santos@server1:~$
```

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

```
santos@server1:~$ logout
Connection to 192.168.56.125 closed.
santos@workstation:~$
```

3. Do the same for Server 2.

```
santos@workstation:~$ ssh santos@192.168.56.126
The authenticity of host '192.168.56.126 (192.168.56.126)' can't be established
.
ECDSA key fingerprint is SHA256:YgpaZbOD4z27d/LzTKO62fj/zCJLMTp2s/uGz13510I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.126' (ECDSA) to the list of known hosts.
santos@192.168.56.126'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.

145 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.

santos@server2:~$
```

```
santos@server2:~$ logout
Connection to 192.168.56.126 closed.
```

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.

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    /etc/hosts

127.0.0.1       localhost
127.0.0.1       workstation
192.168.56.125 server1
192.168.56.126 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.

```
santos@workstation:~$ ssh santos@server1
The authenticity of host 'server1 (192.168.56.125)' can't be established.
ECDSA key fingerprint is SHA256:h6AgC48Gzp9cufmazizM/dnvhVWO7IvhZZ+ChOtFMgo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1' (ECDSA) to the list of known hosts.
santos@server1's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.18.0-15-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

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.
*** System restart required ***
Last login: Tue Jan 23 16:59:13 2024 from 192.168.56.124
santos@server1:~$
```

```
santos@server1:~$ logout
Connection to server1 closed.
```

```
santos@workstation:~$ ssh santos@server2
The authenticity of host 'server2 (192.168.56.126)' can't be established.
ECDSA key fingerprint is SHA256:YgpaZbOD4z27d/LzTKO62fj/zCJLMTp2s/uGz13510I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server2' (ECDSA) to the list of known hosts.
santos@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.

145 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: Tue Jan 23 17:00:56 2024 from 192.168.56.124
santos@server2:~$
```

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

Reflections:

In this first activity, we first installed Ubuntu and cloned them, as well as making a host and client server in the virtual machines. I tend to have issues installing Ubuntu in Virtualbox, but eventually, it was installed. I also learned how to set-up a virtual network and test the connectivity of VMs.

Answer the following:

1. How are we able to use the hostname instead of IP address in SSH commands?
    - We were able to use the hostname instead of IP address in SSH commands by configuring it into the nano command where we have to set up the ip address of the hostname to simply into servers using the hostnames.

2. How secure is SSH?
    - It was designed to provide secure communication over a network, offering encryption and authentication mechanisms to protect against unauthorized access and data interception. It's important to ensure proper configuration and practices, such as using strong authentication methods and keeping software up to date, to maintain a high level of security.