

Name: Catherine Joy D. Atian	Date Performed: Aug 8, 2025
Course/Section: CPE31S4	Date Submitted: Aug 8, 2025
Instructor: Engr. Robin Valenzuela	Semester and SY: 1st SEM, 2025-2026

### Activity 1: Configure Network using Virtual Machines

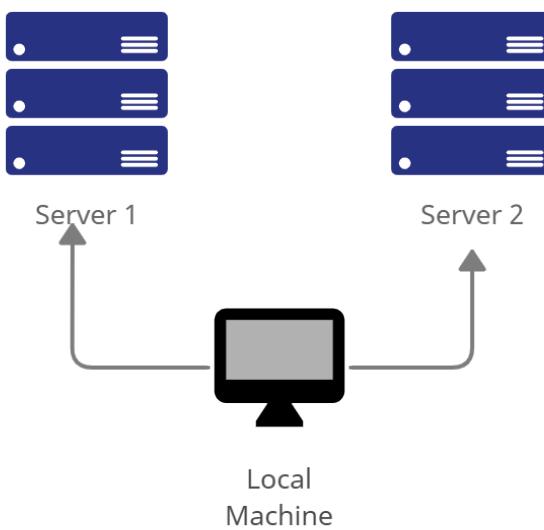
#### 1. Objectives:

- 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:

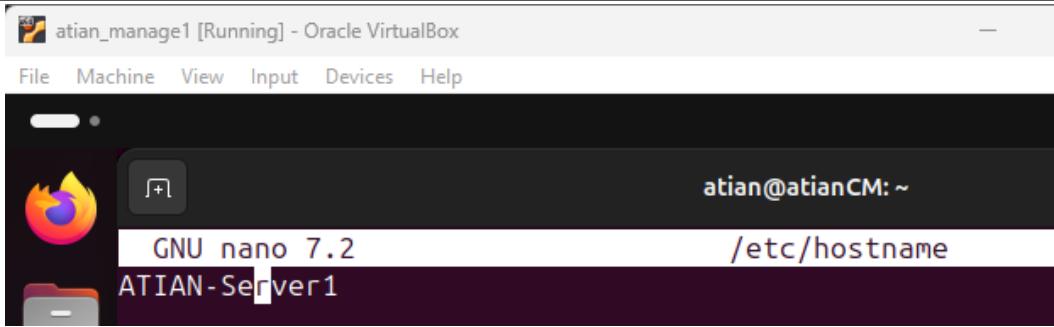
##### Network Topology:

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

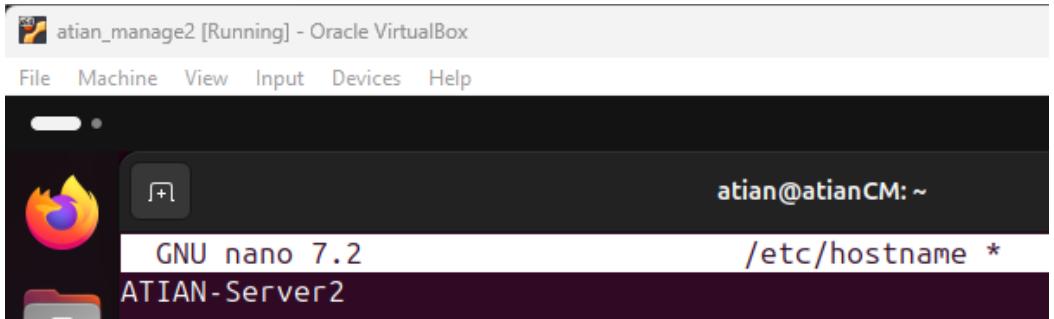


**Task 1:** Do the following on Server 1, Server 2, and Local Machine. In editing the file using nano command, press control + O to write out (save the file). Press enter when asked for the name of the file. Press control + X to end.

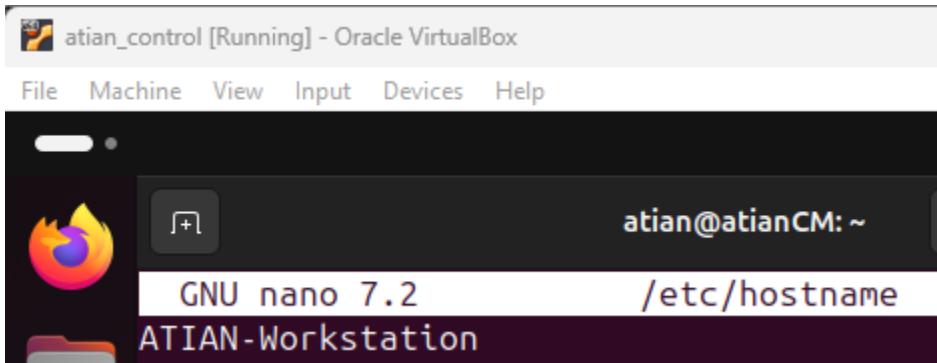
1. Change the hostname using the command ***sudo nano /etc/hostname***
  - 1.1 Use server1 for Server 1



### 1.2 Use server2 for Server 2

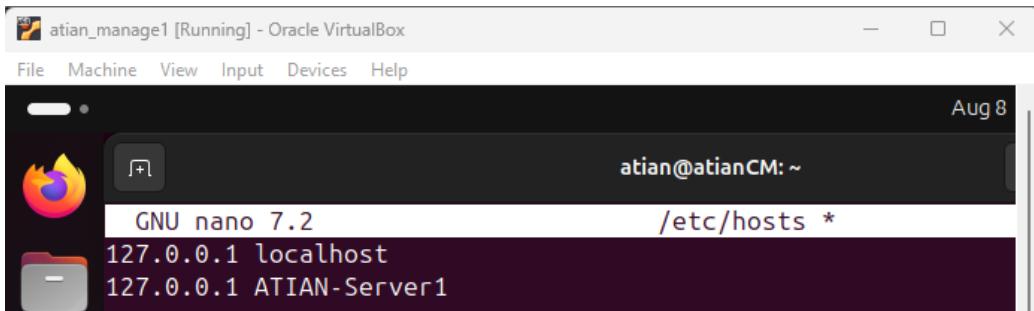


### 1.3 Use workstation for the Local Machine

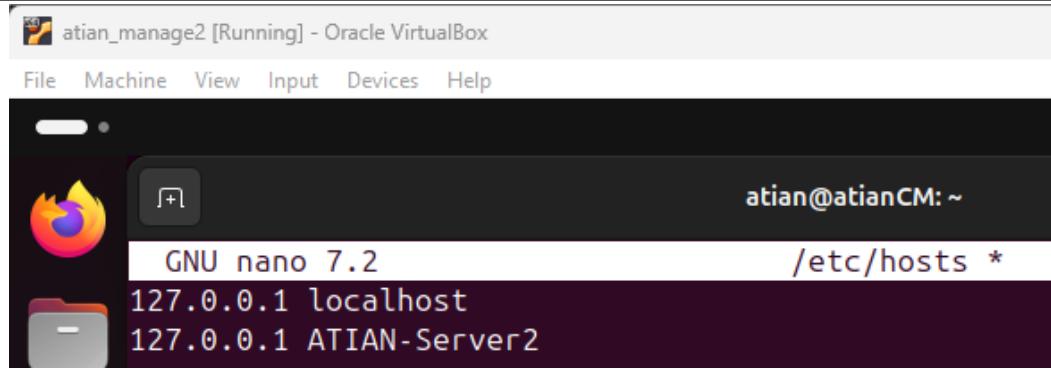


2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.

#### 2.1 Type 127.0.0.1 server 1 for Server 1

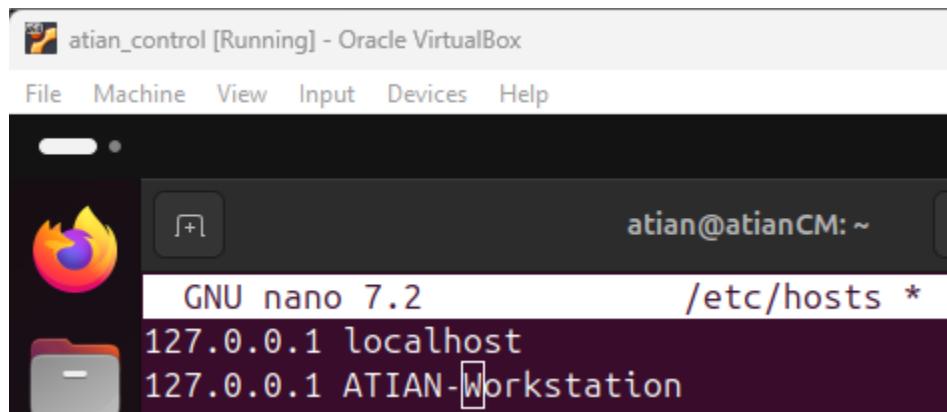


#### 2.2 Type 127.0.0.1 server 2 for Server 2



```
GNU nano 7.2          /etc/hosts *
127.0.0.1 localhost
127.0.0.1 ATIAN-Server2
```

2.3 Type 127.0.0.1 workstation for the Local Machine



```
GNU nano 7.2          /etc/hosts *
127.0.0.1 localhost
127.0.0.1 ATIAN-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.

```
atian@ATIAN-Workstation:~$ sudo apt update
[sudo] password for atian:
Hit:1 http://ph.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
atian@ATIAN-Workstation:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libgl1-amber-dri libglapi-mesa
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  libgl1-amber-dri
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

```
atian@ATIAN-Server1:~$ sudo apt update

[sudo] password for atian:
Sorry, try again.
[sudo] password for atian:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu noble InRelease

Hit:3 http://ph.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
27 packages can be upgraded. Run 'apt list --upgradable' to see them.
atian@ATIAN-Server1:~$ sudo apt upgrade

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
atian@ATIAN-Server2:~$ sudo apt update

[sudo] password for atian:
Sorry, try again.
[sudo] password for atian:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://ph.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://ph.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://ph.archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
27 packages can be upgraded. Run 'apt list --upgradable' to see them.
atian@ATIAN-Server2:~$ sudo apt upgrade

Reading package lists... Done
Building dependency tree... Done
```

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

```
atian@ATIAN-Workstation:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed
```

```
atian@ATIAN-Server1:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no
longer required:
  libgl1-amber-dri libglapi-mesa
```

```
atian@ATIAN-Server2:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and a
re no longer required:
  libgl1-amber-dri libglapi-mesa
```

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***

```
atian@ATIAN-Workstation:~$ sudo service ssh start
atian@ATIAN-Workstation:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh>
  Active: active (running) since Fri 2025-08->
    TriggeredBy: ● ssh.socket
      Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3938 ExecStartPre=/usr/sbin/sshd -t>
   Main PID: 3939 (sshd)
     Tasks: 1 (limit: 2266)
    Memory: 1.3M (peak: 1.6M)
       CPU: 18ms
      CGroup: /system.slice/ssh.service
```

```
atian@ATIAN-Server1:~$ sudo service ssh start
atian@ATIAN-Server1:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service)
    Active: active (running) since Fri 2025-08-03 10:23:45 UTC
      TriggeredBy: ● ssh.socket
          Docs: man:sshd(8)
                  man:sshd_config(5)
        Process: 9248 ExecStartPre=/usr/sbin/sshd -t (>
       Main PID: 9250 (sshd)
          Tasks: 1 (limit: 2266)
         Memory: 1.2M (peak: 1.7M)
            CPU: 15ms
           CGroup: /system.slice/ssh.service
                     └─9250 "sshd: /usr/sbin/sshd -D [list]"

atian@ATIAN-Server1:~$
```

```
atian@ATIAN-Server2:~$ sudo service ssh start
atian@ATIAN-Server2:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service)
    Active: active (running) since Fri 2025-08-08 10:23:45 UTC
      TriggeredBy: ● ssh.socket
          Docs: man:sshd(8)
                  man:sshd_config(5)
        Process: 9292 ExecStartPre=/usr/sbin/sshd -t (>
       Main PID: 9294 (sshd)
          Tasks: 1 (limit: 2266)
         Memory: 1.2M (peak: 1.5M)
            CPU: 14ms
           CGroup: /system.slice/ssh.service
                     └─9294 "sshd: /usr/sbin/sshd -D [list]"

atian@ATIAN-Server2:~$
```

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***

```
atian@ATIAN-Workstation:~$ sudo ufw allow ssh
[sudo] password for atian:
Rules updated
Rules updated (v6)
atian@ATIAN-Workstation:~$ sudo ufw enable
Firewall is active and enabled on system startup
atian@ATIAN-Workstation:~$ sudo ufw status
Status: active

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

```
atian@ATIAN-Server1:~$ sudo ufw allow ssh
[sudo] password for atian:
Rules updated
Rules updated (v6)
atian@ATIAN-Server1:~$ sudo ufw enable
Firewall is active and enabled on system startup
atian@ATIAN-Server1:~$ sudo ufw status
Status: active

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

```
atian@ATIAN-Server2:~$ sudo ufw allow ssh  
[sudo] password for atian:  
Rules updated  
Rules updated (v6)  
atian@ATIAN-Server2:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
atian@ATIAN-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. 102

```
atian@ATIAN-Server1: ~      atian@ATIAN-Server1: ~        
          TX errors 0  dropped 0  overruns 0  carrier  
          0  collisions 0  
  
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  
        mtu 1500  
          inet 192.168.56.102  netmask 255.255.255.0  
            broadcast 192.168.56.255  
              inet6 fe80::f27:d54d:2ebf:7f9  prefixlen 6  
4  scopeid 0x20<link>  
                ether 08:00:27:c3:39:c0  txqueuelen 1000  
(Ethernet)
```

1.2 Server 2 IP address: 192.168.56.103

```
atian@ATIAN-Server2: ~      atian@ATIAN-Server2: ~        
          RX errors 0  dropped 0  overruns 0  frame 0  
          TX packets 180894  bytes 10874166 (10.8 MB)  
          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::b93f:c5c5:9e7:ebcb  prefixlen 6  
4  scopeid 0x20<link>  
                ether 08:00:27:46:4f:e0  txqueuelen 1000  (|  
Ethernet)
```

1.3 Server 3 IP address: 192.168.56.101

```
atian@ATIAN-Workstation: ~
atian@ATIAN-Worksta... × atian@ATIAN-Worksta... ×
r 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST
> mtu 1500
      inet 192.168.56.101 netmask 255.255.255.
      0 broadcast 192.168.56.255
      inet6 fe80::b397:9ea9:a390:712a prefixle
n 64 scopeid 0x20<link>
      ether 08:00:27:8a:22:21 txqueuelen 1000
(Ethernet)
      RX packets 644 bytes 102086 (102.0 KB)
```

2. Make sure that they can ping each other.

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

```
atian@ATIAN-Workstation: ~
atian@ATIAN-Workstation: ~ × atian@ATIAN-Workstation: ~ ×
atian@ATIAN-Workstation:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.963 m
s
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.485 m
s
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.398 m
s
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.447 m
s
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.434 m
```

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

```
atian@ATIAN-Workstation:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.857 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.726 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.513 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.545 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=64 time=0.481 ms
^Z
[2]+ Stopped ping 192.168.56.103
```

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

```
atian@ATIAN-Server1:~$ 
atian@ATIAN-Server1:~$ 
TX errors 0 dropped 0 overruns 0 carrier
0 collisions 0

atian@ATIAN-Server1:~$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes
of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 ti
me=2.35 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 ti
me=0.500 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 ti
me=0.404 ms
^Z
[1]+ Stopped ping 192.168.56.103
atian@ATIAN-Server1:~$
```

**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`

```
atian@ATIAN-Workstation:~$ ssh atian@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:qXw81KRZA6RZtvtd1Ac26VCp9j
3jLJZPB1OyrXRw6ag.
```

```
atian@ATIAN-Workstation:~$ ssh atian@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ED25519 key fingerprint is SHA256:qXw81KRZA6RZtvtd1Ac26VCp9j
3jLJZPB1OyrXRw6ag.
This host key is known by the following other names/addresses
```

```
atian@ATIAN-Server1:~$ ssh atian@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:qXw81KRZA6RZtvtd1Ac26VCp9j
3jLJZPB1OyrXRw6ag.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[finger
```

- 1.2 Enter the password for server 1 when prompted

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

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

```
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Aug  8 07:44:04 2025 from 192.168.56.101
atian@ATIAN-Server1:~$
Logout
Connection to 192.168.56.102 closed.
```

3. Do the same for Server 2.

```
Last login: Fri Aug  8 07:44:33 2025 from 192.168.56.102
atian@ATIAN-Server2:~$
logout
Connection to 192.168.56.103 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)

```
atian@ATIAN-W... × atian@ATIAN-Se... × atian@ATIAN-W...
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.0.1 ATIAN-Workstation
192.168.56.102 Server1
192.168.56.103 Server2
192.168.56.101 Workstation
```

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.

```
atian@ATIAN-Workstation:~$ ssh atian@Server1
atian@server1's password:
Permission denied, please try again.
atian@server1's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-27-generic
86_64)
```

```
Last login: Fri Aug  8 07:56:39 2025 from 192.168.56.101
atian@ATIAN-Server1:~$
```

```
atian@ATIAN-Workstation:~$ ssh atian@Server2
The authenticity of host 'server2 (192.168.56.103)' can't
be established.
ED25519 key fingerprint is SHA256:qXw81KRZA6RZtvtd1Ac26VC
3jLJZPB1OyrXRw6ag.
This host key is known by the following other names/address:
```

```
Last login: Fri Aug  8 07:47:11 2025 from 192.168.56.103
atian@ATIAN-Server2:~$ 
logout
Connection to server2 closed.
```

#### 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 instead of the IP address in SSH commands because it is connected from the workstation to the two server with the help of the SSH and the IP address of each. Each is verified through login and pinging.
2. How secured is SSH?
  - SSH is secured because it uses password authentication and has encrypted data conserving the two connected computers. Whenever you are trying to connect with it you have to put your password and then log out after.