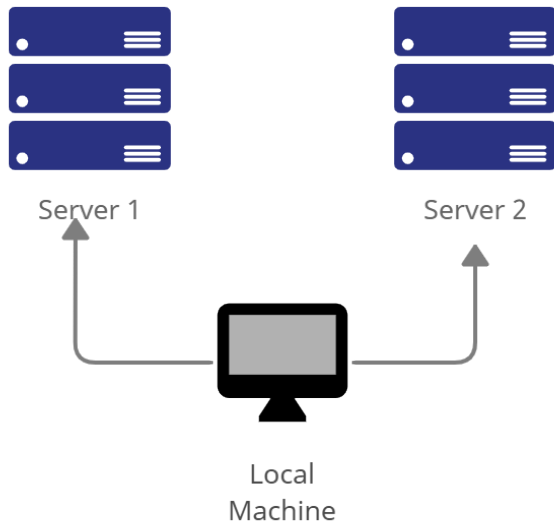
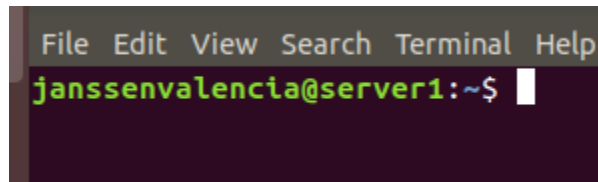


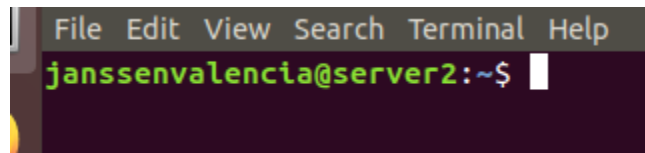
<b>Name: Valencia, Mark Janssen</b>	<b>Date Performed: August 17, 2023</b>
<b>Course/Section: CPE31s6</b>	<b>Date Submitted: August 17, 2023</b>
<b>Instructor: Dr. Jonathan Taylar</b>	<b>Semester and SY: 2023-2024</b>
<b>Activity 1: Configure Network using Virtual Machines</b>	
<b>1. Objectives:</b> 1.1. Create and configure Virtual Machines in Microsoft Azure or VirtualBox 1.2. Set-up a Virtual Network and Test Connectivity of VMs	
<b>2. Discussion:</b>  <b>Network Topology:</b> 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] --&gt; Server1[Server 1]     LocalMachine --&gt; Server2[Server 2]   </pre> <p>The diagram illustrates a network topology. At the bottom center is a computer icon labeled "Local Machine". Two lines extend upwards from the Local Machine, each ending in an arrow pointing to a stack of three server icons. The left stack is labeled "Server 1" and the right stack is labeled "Server 2". Each server icon is a blue rectangle with a white dot and three horizontal lines on the right side.</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.

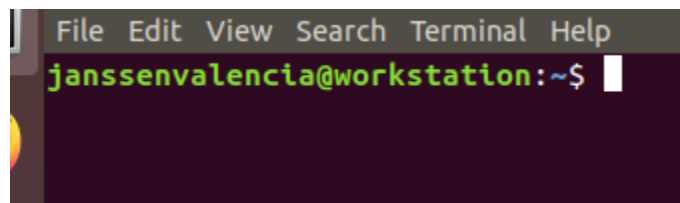
1. Change the hostname using the command *sudo nano /etc/hostname*
  - 1.1 Use server1 for Server 1
  - 1.2 Use server2 for Server 2
  - 1.3 Use workstation for the Local Machine
2. Edit the hosts using the command *sudo nano /etc/hosts*. Edit the second line.
  - 2.1 Type 127.0.0.1 server 1 for Server 1

A terminal window with a dark background and a light gray menu bar at the top containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt 'janssenvalencia@server1:~\$' is displayed in green text, followed by a white cursor.

- 2.2 Type 127.0.0.1 server 2 for Server 2

A terminal window with a dark background and a light gray menu bar at the top containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt 'janssenvalencia@server2:~\$' is displayed in green text, followed by a white cursor.

- 2.3 Type 127.0.0.1 workstation for the Local Machine

A terminal window with a dark background and a light gray menu bar at the top containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt 'janssenvalencia@workstation:~\$' is displayed in green text, followed by a white cursor.

**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.

```
File Edit View Search Terminal Help
janssenvalencia@server1:~$ sudo apt update
[sudo] password for janssenvalencia:
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.
janssenvalencia@server1:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

```
File Edit View Search Terminal Help
janssenvalencia@server2:~$ sudo apt update
[sudo] password for janssenvalencia:
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.
janssenvalencia@server2:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
```

```
janssenvalencia@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.
janssenvalencia@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:
```

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

```
Learn more about Ubuntu Pro for 18.04 at https://ubuntu.com/18-0
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
janssenvalencia@server1:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
```

```
Learn more about Ubuntu Pro for 18.04 at https://ubuntu.com/18-0
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
janssenvalencia@server2:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

```
File Edit View Search Terminal Help
janssenvalencia@workstation:~$ sudo apt install openssh-server
[sudo] password for janssenvalencia:
Reading package lists... Done
Building dependency tree
```

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*

```
janssenvalencia@workstation:~$ sudo service ssh start
janssenvalencia@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 17:33:24 PST; 46s ago
   Main PID: 2089 (sshd)
     Tasks: 1 (limit: 4656)
    CGroup: /system.slice/ssh.service
            └─2089 /usr/sbin/sshd -D

Aug 17 17:33:24 workstation systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:33:24 workstation sshd[2089]: Server listening on 0.0.0.0 port 22.
Aug 17 17:33:24 workstation sshd[2089]: Server listening on :: port 22.
Aug 17 17:33:24 workstation systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
janssenvalencia@server1:~$ sudo service ssh start
janssenvalencia@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 17:27:04 PST; 8min ago
   Main PID: 2566 (sshd)
     Tasks: 1 (limit: 4656)
    CGroup: /system.slice/ssh.service
            └─2566 /usr/sbin/sshd -D

Aug 17 17:27:04 server1 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:27:04 server1 sshd[2566]: Server listening on 0.0.0.0 port 22.
Aug 17 17:27:04 server1 sshd[2566]: Server listening on :: port 22.
Aug 17 17:27:04 server1 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-12/12 (END)
```

```
janssenvalencia@server2:~$ sudo service ssh start
janssenvalencia@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 17:28:08 PST; 7min ago
   Main PID: 2564 (sshd)
     Tasks: 1 (limit: 4656)
    CGroup: /system.slice/ssh.service
            └─2564 /usr/sbin/sshd -D

Aug 17 17:28:08 server2 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 17 17:28:08 server2 sshd[2564]: Server listening on 0.0.0.0 port 22.
Aug 17 17:28:08 server2 sshd[2564]: Server listening on :: port 22.
Aug 17 17:28:08 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*

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

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

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

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

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

```
flags=4163<UP,BROADCAST
inet 192.168.56.102
inet6 fe80::1c28:9ce1:
```

1.2 Server 2 IP address: 192.168.56.103

```
flags=4163<UP,BROADCAST
inet 192.168.56.103
inet6 fe80::f1d6:49e8:
```

1.3 Workstation IP address: 192.168.56.101

```
flags=4163<UP,BROADCAST
inet 192.168.56.101
inet6 fe80::9614:1546:
```

2. Make sure that they can ping each other.

2.1 Connectivity test for Local Machine 1 to Server 1: **Successful**

```
janssenvalencia@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=1.20 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.450 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.471 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.468 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.434 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.441 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.565 ms
```

2.2 Connectivity test for Local Machine 1 to Server 2: **Successful**

```
janssenvalencia@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=1.22 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.472 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.479 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.463 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=64 time=0.520 ms
```

2.3 Connectivity test for Server 1 to Server 2: **Successful**

```
janssenvalencia@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 time=0.675 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.495 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.549 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.575 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`

```
janssenvalencia@workstation:~$ ssh janssenvalencia@192.168.56.102
```

1.2 Enter the password for server 1 when prompted

```
Warning: Permanently added '192.168.56.102'
janssenvalencia@192.168.56.102's password:
```

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

For example, `jvtaylor@server1`

```
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.

janssenvalencia@server1:~$
```

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

```
janssenvalencia@server1:~$ logout
Connection to 192.168.56.102 closed.
janssenvalencia@workstation:~$
```

3. Do the same for Server 2.

```
janssenvalencia@workstation:~$ ssh janssenvalencia@192.168.56.103
```

```
Warning: Permanently added '192.168.56.103' (192.168.56.103) to the list of
janssenvalencia@192.168.56.103'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.

janssenvalencia@server2:~$
```

```
janssenvalencia@server2:~$ logout
Connection to 192.168.56.103 closed.
janssenvalencia@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)

```
127.0.1.1    workstation
192.168.56.102  server1
192.168.56.103  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.

```
janssenvalencia@workstation:~$ ssh janssenvalencia@server1
janssenvalencia@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 18:07:43 2023 from 192.168.56.101
janssenvalencia@server1:~$
```

```
connection to server2 closed.
janssenvalencia@workstation:~$ ssh janssenvalencia@server2
janssenvalencia@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 18:09:33 2023 from 192.168.56.101
janssenvalencia@server2:~$
```

**Reflections:****1. How are we able to use the hostname instead of IP address in SSH commands?**

- **Yes**, I was able to use the host name when accessing both the server1 and server2 in the workstation, instead of using the servers individual ip addresses.

**2. How secured is SSH?**

- SSH, short for Secured Shell, is a network protocol that is used in connecting linux servers remotely. Secured shell is very secure since it uses encryption to secure the connection from the workstation to the server itself.

**Conclusion:**

- For The first Hands on activity for this semester on the course Managing Enterprise servers we were tasked to create and remotely access two virtual machines in a virtual box named server1 and server2 using and implementing SSH. This hands-on activity is indeed one of the most fundamental skills and knowledge that I will use in the future hands on activity and hopefully soon as a future systems administrator.

*"I Valencia, Mark Janssen Affirm that I will not give or receive any unauthorized help on this activity and that all work shall be my own"*