LAB 1- Server and Application Provisioning

Date: Friday January 24, 2025

MOP Name: COMP595-Lab1

Author: Joelle Waugh

Instructor: Andrew Bell

Version: 1

1. Purpose/Description:

The purpose of this lab is to configure two VM on vSphere. First it is to install the Ubuntu server and to be able to connect the server to Windows 11 workstation via ssh connection. In addition, to having the ability to connect to the Apache2 server and to install Fail2ban. This document will outline the steps needed to follow to reach the desired outcome. It will include various screenshots and instructions, to be read carefully.

2. Prerequisite:

This section will list the necessary elements required before commencing the lab and for the lab to be completed.

- Equipment: A computer or laptop
- Virtual Machines: Pre-installed Windows VM and Ubuntu server VM, vSphere
- Instructions: Lab 1 Documentation
- Website Resources can be referred to for reference:
    - https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-ubuntu-20-04

- https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04
- https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_keymanagement
- https://answers.microsoft.com/en-us/windows/forum/all/how-to-create-a-local-account-in-windows-11/24c2e160-ac65-4748-a733-529e6507dfdf

3. Steps:

This section will outline the necessary steps taken to complete the full configuration. Please follow each step carefully.

1. **Installing Ubuntu server:**

   A VM should already be on vSphere; it will not be fully installed. If not, please contact your instructor.

   1.1 When prompted, select the language as English. Continue with the rest of the installation and press ***'Done'*** to move forward.

   1.2 When you get to the username and password section, enter your username as the Fleming College username with srv-1 at the end.

   Example: joewau-srv1

   1.3 There will be an option to upgrade the Ubuntu installer; do not upgrade the installer.

   1.4 When prompted, do not install the Pro version of Ubuntu; continue by selecting '***Done'***.

1.5 When you get to the OpenSSH part of the installation, ensure that you install OpenSSH by marking the selection. An ***'x'*** will appear to indicate that it has been marked.

1.6 Continue with the rest of the installation. Once completed, wait for the installation to finish.

1.7 Once the installation is complete, it will prompt you to restart your Ubuntu server VM.

2. Set up a local user

2.1 Open the Windows 11 Workstation. Use the password ***'password'*** to log in to the administration account.

2.2 To create the local account, click on Win + R Keys. A box will appear: Do not enter an email. Click next.

2.2 Enter the same username and password as on the Ubuntu Server.

2.3 To check that the user has been created, open Local Users and Groups from PowerShell using the command ***lusrmgr.***

3. Install OpenSSH

Here, you will install OpenSSH on the Windows 11 workstation first to obtain a key pair. Follow the steps below:

3.1 Open Windows PowerShell in Administrator mode.

3.2 Type in the command ***"Get-Service -Name | Set–Service -StartupType Automatic" and*** press enter.

3.3 Then type in the command ***"Start-Service sshd"*** and press Enter.

3.4 Then type “ssh-keygen -t ed25519” and press enter.

3.5 Once you see “Enter file in which to save the key:” do not type anything, just press enter.

3.6 Then, “Enter passphrase” will appear. Do not enter a passphrase; just press enter. It will ask you to do it again, so do the same as the latter step. The key fingerprint will appear.

3.7 Now you have received the public key and private key.

4. Sending the SSH Key from Windows to Ubuntu Server

4.1 First, you need to be in the /.ssh directory, which you can do by ***cd .ssh***.

4.2 Once you are in the .ssh directory, do ls to make sure you have all four files. Your private key, public key, known_hosts, and known_hosts.old should be there.

4.3 To make sure that your Windows workstation connects to your Ubuntu server. In Windows PowerShell, you need to enter ***ssh <yourservername-srv1>@<Ubuntuserveip>.*** It should automatically bring you to your Ubuntu server.

Example: ssh joewau-srv1@10.59.5.74

4.4 To send the public key over to the Ubuntu server in PowerShell, type in scp (WinScp) the file name of the public key and the <yourservername-srv1> @<Ubuntuserverip>.

Example: scp id_ed25519.pub joewau-srv1@10.59.5.74.

4.5 Go to the Ubuntu server, ***cd .ssh*** once in the directory, do ***ls,*** and you should see the public key id_ed25519.pub.

5. Turn off the password

5.1 In the Ubuntu Server type the command ***cd /etc/ssh*** to get into the ssh directory

5.2 Then press ***ls*** to see what is in the directory

5.3 From there, do the command ***cd sshd.config.d*** to get into the directory

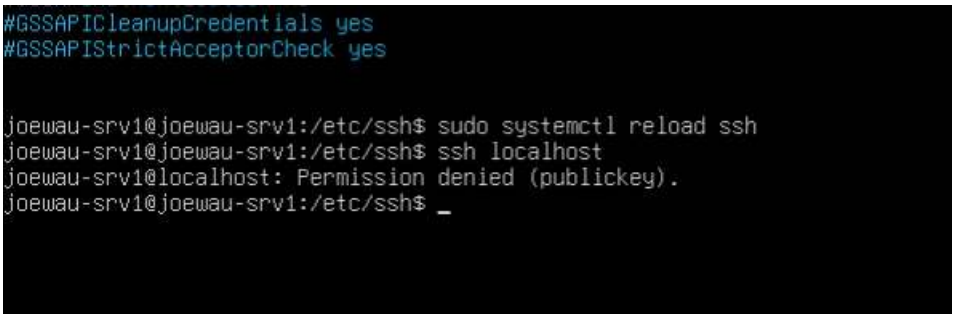
5.4 From there, do the command ***sudo cat 50-cloud-init.conf***. This should appear: #PasswordAuthentication yes

5.5 Leave the directory by typing ***cd ..***

5.6 Then enter the command ***sudo nano sshd_config file***

5.7 5.7 In the sshd_config file, scroll down to # Password Authentication. Yes. Uncomment the statement and change the yes to a no. Save the file by pressing Ctrl + O, and to exit, press Ctrl + X.

5.8 To check that it works, type the command sudo systemctl reload ssh, then ssh localhost. This should deny you access, as shown below.



6. Installing Fail2ban

6.1 To install Fail2ban on the Ubuntu Server, enter ***sudo apt update***

6.2 Once the server finishes updating, then enter ***sudo apt install fail2ban***

6.3 Then do ***systemctl status fail2ban.service***

6.4 To make sure that everything is working, do ***cd /etc/fail2ban***

6.5 Then do the command ***head -20 jail.conf,*** there should be an output.

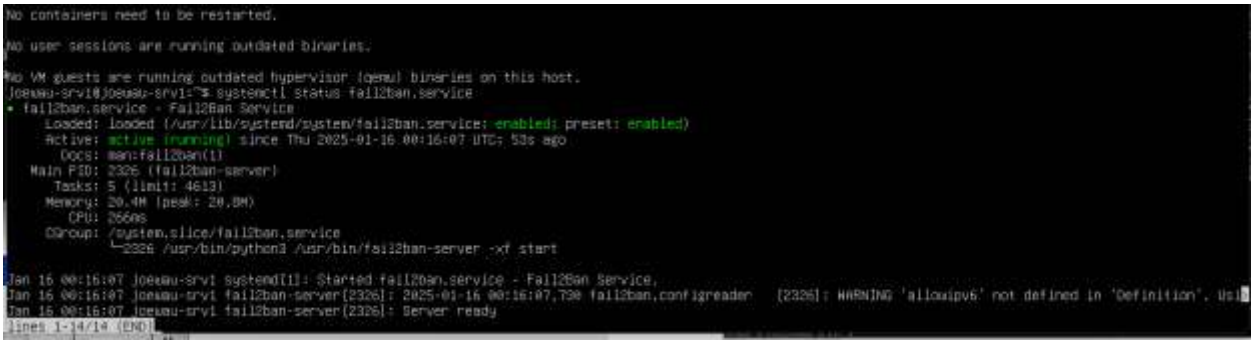
6.6 To see if Fail2ban is active, enter these commands below:

6.6.1 sudo systemctl enable fail2ban

6.6.2 sudo systemctl start fail2ban

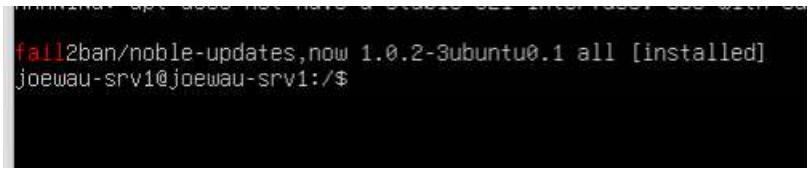
6.6.3 ***sudo systemctl status fail2ban***

6.7 After the status command, you should see an output as depicted below.



6.8 To verify that fail2ban is installed, use the command apt list—installed | grep fail.

The results should show up as below.



7. Installing the Apache2 server

7.1 To install Apache2 server, you need to do ***sudo apt update***

7.2 Then ***sudo apt install apache2***

7.3 After executing this command, sudo ufw app list, there should be an output.

7.4 Out of the list, you will select sudo ufw allow 'Apache'; this will disable the firewall.

7.5 Then do ***sudo ufw status***. There should be an output of active status

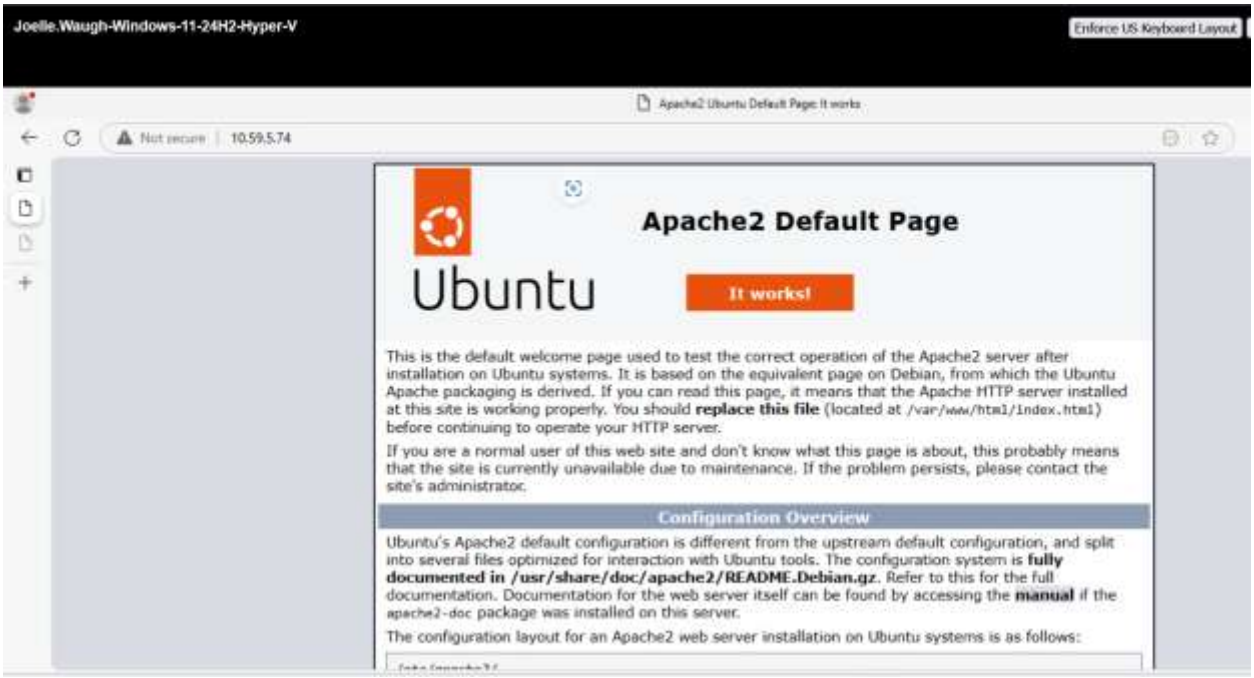
7.6 To make everything installed, type the command sudo systemctl status apache2. There should be an output stating that the server is up and active.

7.7 To check all the connections, type the command ***hostname -I,*** the IP address of the server should appear

7.8 To see if you can connect from the server to an external IP address, type this command curl -4 icanhazip.com. An IP address should appear.

7.9 On your Windows 11 workstation, open a web browser, type http:// <ubuntu server ip>, and the Apache2 Ubuntu Default page should appear as shown below.

Example: http://10.59.5.74



7.10 If you are not able to connect to Apache2, try the commands below:

7.10.1 sudo systemctl stop apache2

7.10.2 sudo systemctl start apache2

7.10.3 sudo systemctl restart apache2

7.10.4 ***sudo systemctl reload apache2***

4. Conclusion:

To conclude, the lab objectives should all have been met. The Ubuntu server and Windows 11 Workstation should be able to communicate and send files to each other. All the installations should be completed and shown as active in the Ubuntu server, such as Fail2Ban and the Apache2 server. Finally, you should be able to connect to the Apache2 server via the Windows 11 workstation web browser.