Lab: Set up a secure server configuration, including basic firewall rules

In this lab, you will learn how to set up a secure server configuration on Microsoft Azure. You will create a virtual machine, apply a basic firewall configuration, and verify that your rules are working correctly.

Prerequisites

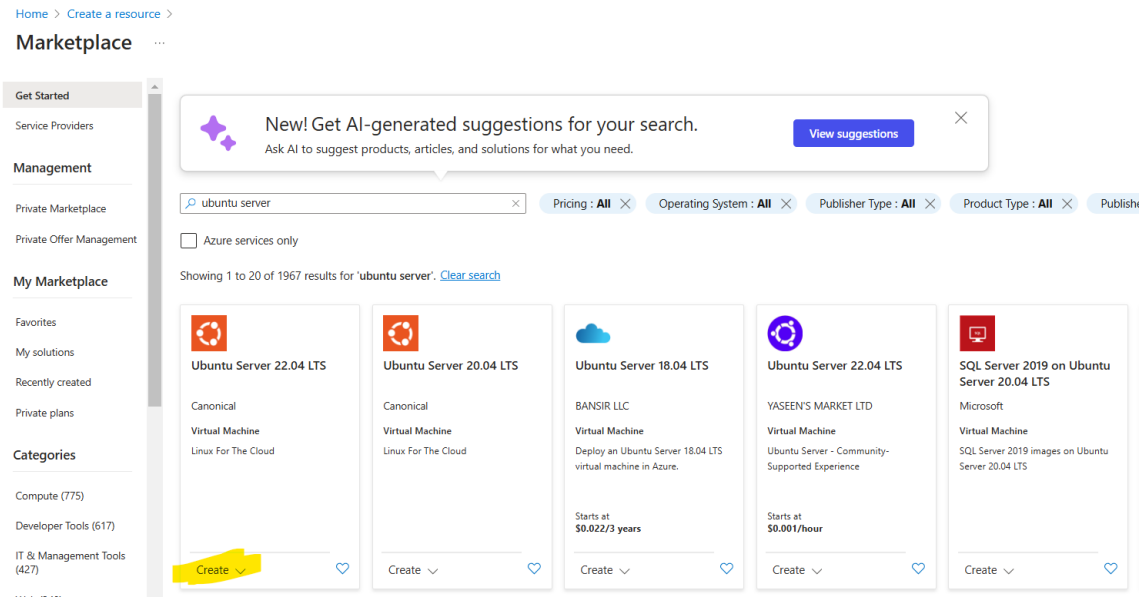
1. **Azure Portal Access**: You will use the Azure Portal to create and configure resources.
2. **Naming Convention**: All students share the same Azure environment, so each student must include their name as a prefix in resource names. Example: `YOUR_NAME-ubuntu-server`.
3. **Basic Networking Knowledge**: Familiarity with concepts like ports and firewall is recommended.

Lab Objectives

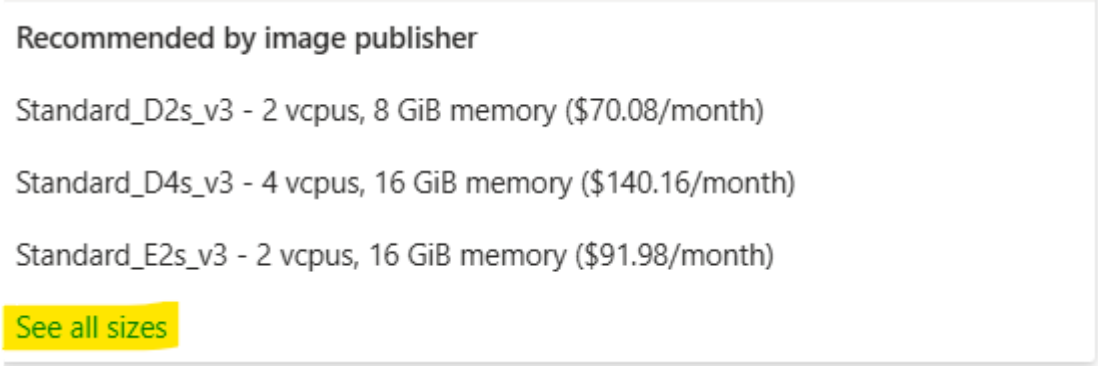
- Create an Azure Virtual Machine (VM)
- Configure the VM's network security group (NSG) for basic firewall rules
- Install and enable a firewall on the server
- Install and test Nginx
- Verify the firewall configuration and ensure secure access

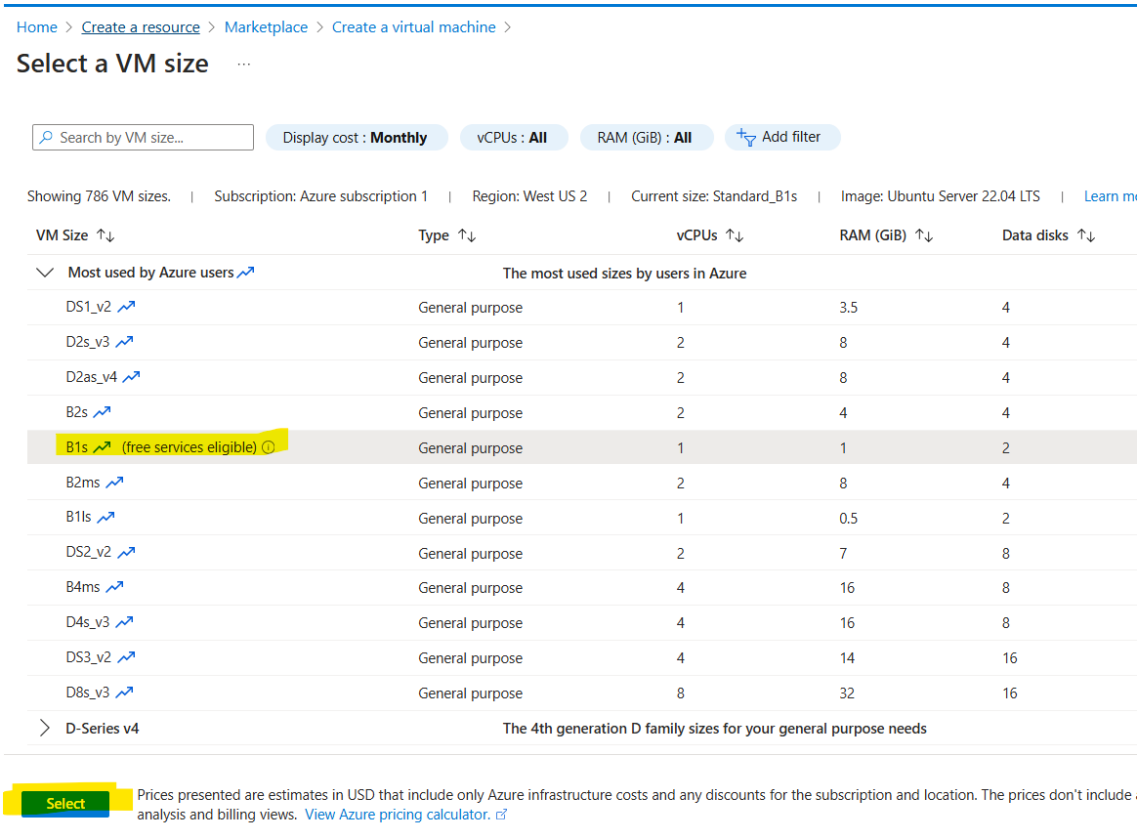
Section 1: Create a Virtual Machine

1. **Sign in to Azure Portal**
   - Open your web browser and go to the Azure Portal.
   - Enter your credentials to log in.
2. **Create a Resource**
   - On the Azure Portal homepage, click **Create a resource**.
   - In the **Search the Marketplace** field, type **Ubuntu Server** (or your preferred Linux distribution).
   - Select **Ubuntu Server** from the search results.
   - Click **Create**.



3. **Configure Basic Settings**
   - **Resource Group**: Select an existing resource group : `software-ecosystem-student-tmp` .
   - **Virtual Machine Name**: Use your name as the prefix. For example, `YOUR_NAME-ubuntu-vm` .
   - **Region**: `(US) WEST US 2` .
   - **Image**: Verify it's set to **Ubuntu Server**.
   - **Size**: Please make sure to select `B1s` .

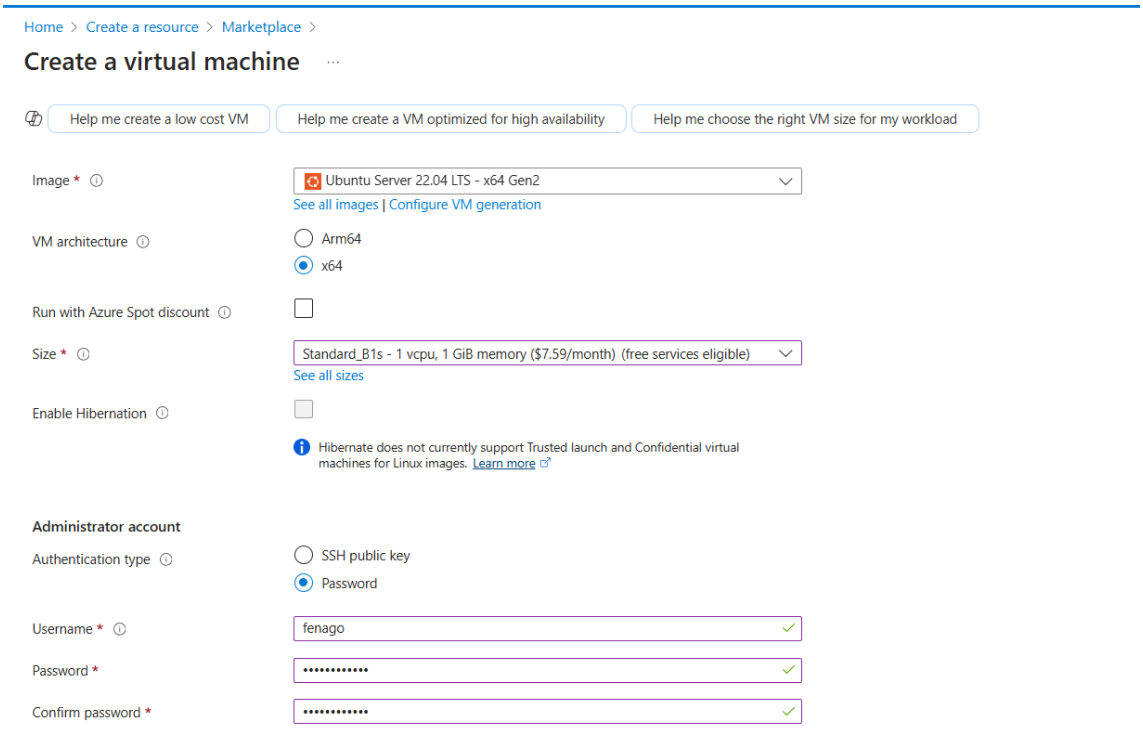




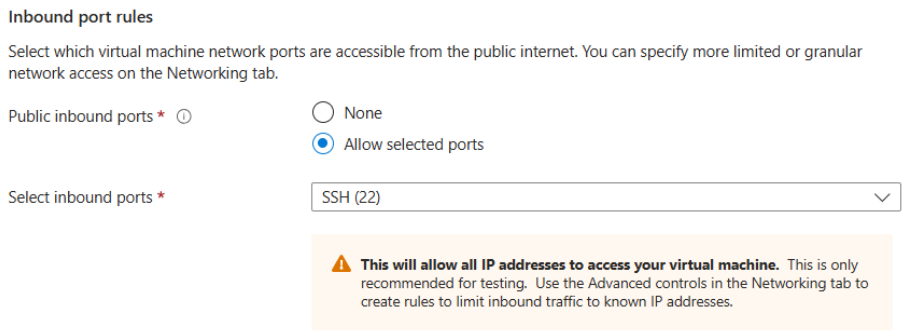
IMPORTANT: If `B1s` size is not available, then you can select `Standard_D2s_v3` or any other available size.

4. **Administrator Account**
   - **Authentication type**: Select & enter **Password**.
   - **Username**: `fenago`

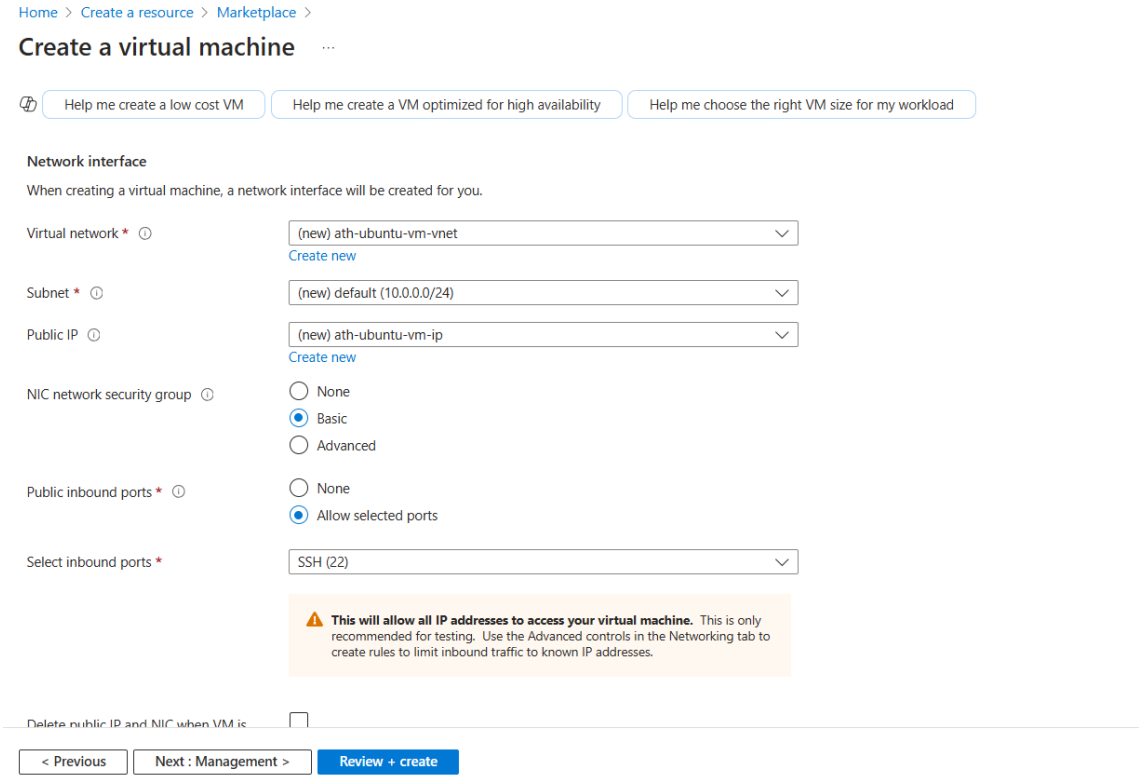
- **Password**: Make sure to remember the password you enter or use same password as Azure account.



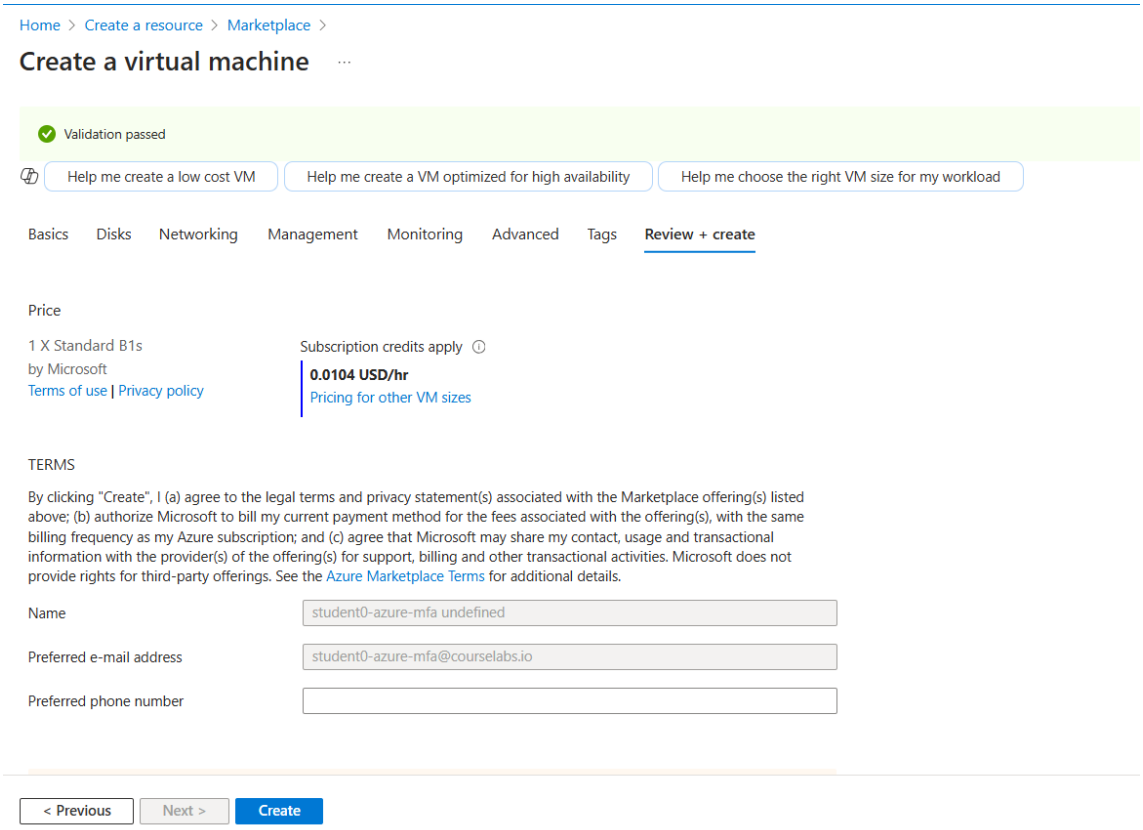
5. **Inbound Port Rules**
   - To keep this lab secure, do not allow all ports publicly. However, for the sake of this exercise, you may allow **SSH (port 22)** so you can connect.
   - Any other ports you need should be locked down until you configure your firewall properly.



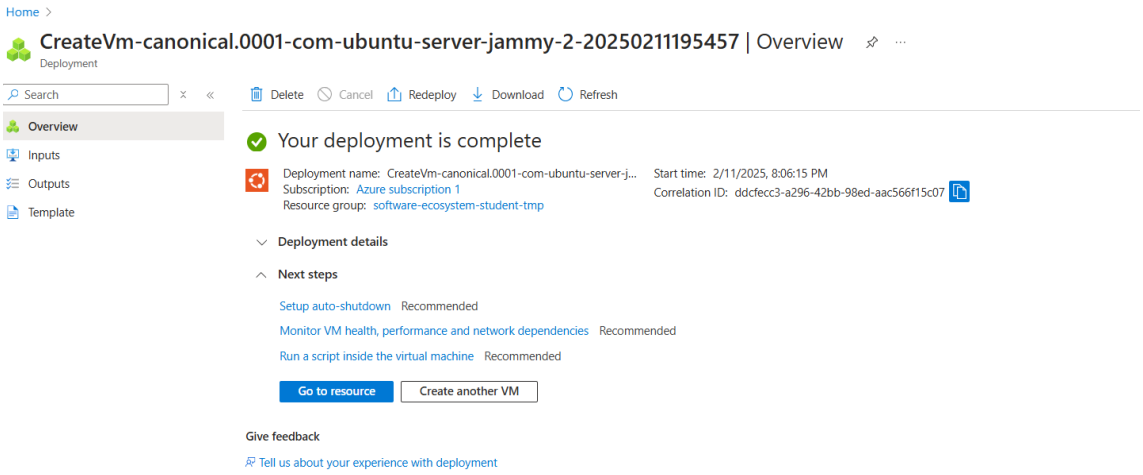
6. **Disks & Networking**
   - **Disks**: Use the OS disk type `Standard HDD`.
   - **Networking**: A default Virtual Network and Subnet should be created. Keep the default settings.
   - **Public IP**: Make sure a Public IP is assigned if you need to SSH from the internet.
   - **NIC Network Security Group**: Select **Basic** and allow **SSH**.



7. **Management, Advanced, and Tags**
    - Accept defaults
8. **Review + Create**
    - Review all settings on the **Review + create** tab.
    - If everything is correct, click **Create**.



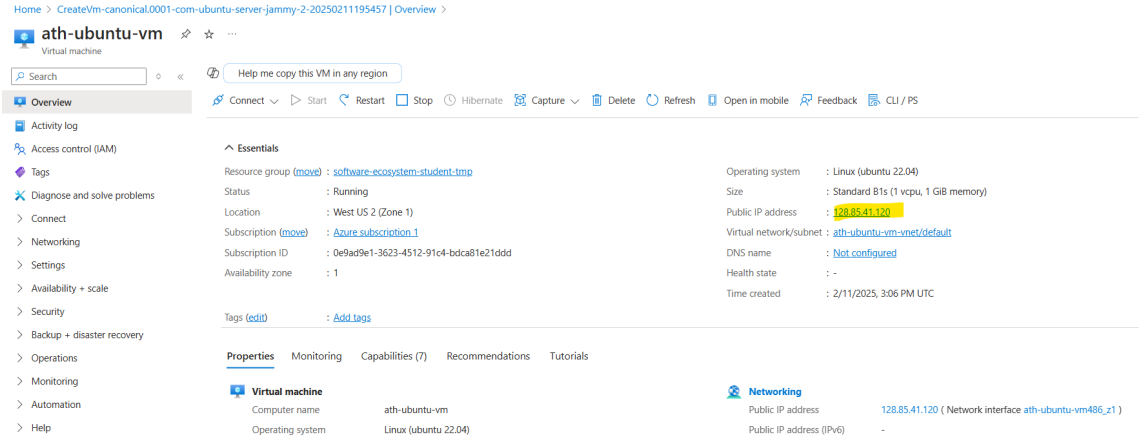
9. **Wait for Deployment**
    - The VM deployment can take a few minutes. Once done, proceed to the next section.



Section 2: Connect to the VM

1. **Locate Public IP**
    - In the Azure Portal, navigate to the new VM's **Overview** page.

- Copy the **Public IP address**.



2. **SSH into the VM** (assuming you allowed SSH in your inbound rules):

```
ssh fenago@<public-ip>
```

   - Replace `<public-ip>` with the one from the portal.

3. **Confirm Connection**

   - Once connected, you should see a terminal prompt like: `fenago@YOUR_NAME-ubuntu-vm:~$`

```
$ ssh fenago@128.85.41.120
The authenticity of host '128.85.41.120 (128.85.41.120)' can't be established.
ED25519 key fingerprint is SHA256:S7mysgK8Rw/rEZGGOPQPiaxFBENdoMMfS46mnGAcm+4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '128.85.41.120' (ED25519) to the list of known hosts.
fenago@128.85.41.120's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1020-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Tue Feb 11 15:10:17 UTC 2025

  System load:  0.09              Processes:             109
  Usage of /:   5.2% of 28.89GB   Users logged in:       0
  Memory usage: 29%               IPv4 address for eth0: 10.0.0.4
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

fenago@ath-ubuntu-vm:~$
```

Section 3: Familiarize Yourself with VM Settings

Before configuring firewalls, it's a good practice to check basic server health and settings:

1. **Check System Information**

   ```
   lsb_release -a
   uname -r
   ```

   - These commands confirm your Ubuntu version and kernel.

2. **Free Disk Space and Memory**

   ```
   df -h
   free -m
   ```

   - Ensure you have sufficient storage and RAM for any additional software.

Section 4: Install and Configure UFW on Ubuntu

Now that you're connected to the VM, you can install and configure the Uncomplicated Firewall (UFW), which is a simple yet effective way to manage firewall rules on Ubuntu.

1. **Update Package Lists**

```
sudo apt-get update
```

2. **Install UFW** (it may already be installed on some Ubuntu images):

```
sudo apt-get install -y ufw
```

3. **Check UFW Status** (by default, it may be inactive):

```
sudo ufw status
```

```
fenago@ath-ubuntu-vm:~$ sudo apt-get update
Hit:1 http://azure.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://azure.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2316 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [387 kB]
Get:13 http://azure.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2944 kB]
Get:14 http://azure.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [515 kB]
Get:15 http://azure.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1187 kB]
Get:16 http://azure.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [291 kB]
Get:17 http://azure.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [26.4 kB]
Get:18 http://azure.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [44.5 kB]
Get:19 http://azure.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [11.5 kB]
Get:20 http://azure.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [440 B]
Get:21 http://azure.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [67.7 kB]
Get:22 http://azure.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [11.1 kB]
Get:23 http://azure.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:24 http://azure.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:25 http://azure.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [30.0 kB]
Get:26 http://azure.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [16.6 kB]
Get:27 http://azure.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [672 B]
Get:28 http://azure.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:29 http://azure.archive.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2077 kB]
Get:30 http://azure.archive.ubuntu.com/ubuntu jammy-security/main Translation-en [325 kB]
Get:31 http://azure.archive.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2836 kB]
Get:32 http://azure.archive.ubuntu.com/ubuntu jammy-security/restricted Translation-en [498 kB]
Get:33 http://azure.archive.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [961 kB]
Get:34 http://azure.archive.ubuntu.com/ubuntu jammy-security/universe Translation-en [205 kB]
Get:35 http://azure.archive.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [19.5 kB]
Get:36 http://azure.archive.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [37.6 kB]
Get:37 http://azure.archive.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [8260 B]
Get:38 http://azure.archive.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [224 B]
Fetched 35.6 MB in 8s (4638 kB/s)
Reading package lists... Done
fenago@ath-ubuntu-vm:~$ sudo apt-get install -y ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.1-4ubuntu0.1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 41 not upgraded.
fenago@ath-ubuntu-vm:~$ sudo ufw status
Status: inactive
fenago@ath-ubuntu-vm:~$
```

4. **Set Default Policies** (it's a good security practice to deny all incoming and allow all outgoing traffic by default):

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

5. **Allow Necessary Inbound Connections**

- **SSH (port 22)**:

  ```
  sudo ufw allow 22
  ```

- **HTTP (port 80)**, To run a web server:

  ```
  sudo ufw allow 80
  ```

- **HTTPS (port 443)**, if you plan to run a secure web server:

  ```
  sudo ufw allow 443
  ```

6. **Enable UFW**:

   ```
   sudo ufw enable
   ```

   - When asked if you want to proceed, type `y` and press Enter.

7. **Verify UFW Status**:

   ```
   sudo ufw status verbose
   ```

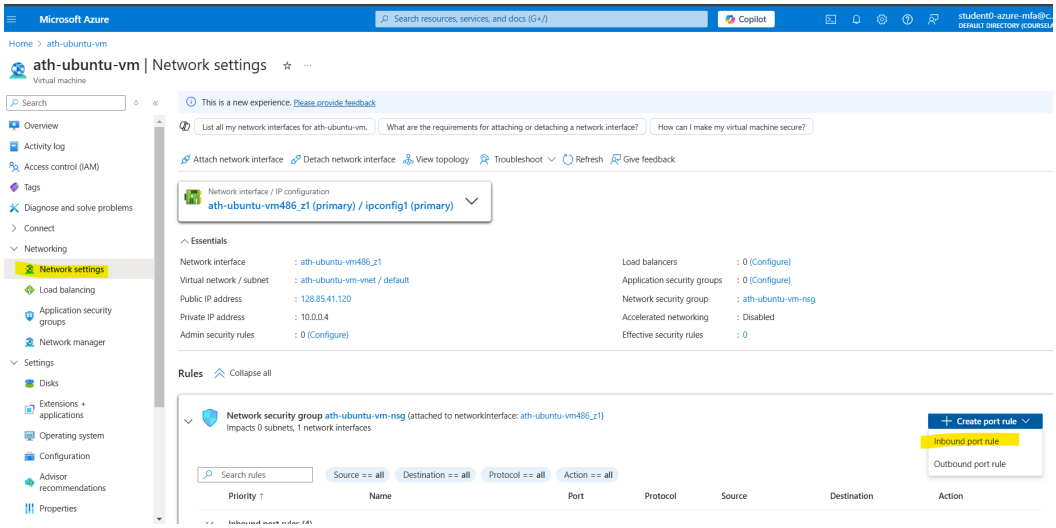
   - You should see rules for 22, 80, and 443 (if you allowed them).

```
fenago@ath-ubuntu-vm:~$
fenago@ath-ubuntu-vm:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
fenago@ath-ubuntu-vm:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
fenago@ath-ubuntu-vm:~$ sudo ufw allow 22
Rules updated
Rules updated (v6)
fenago@ath-ubuntu-vm:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
fenago@ath-ubuntu-vm:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
fenago@ath-ubuntu-vm:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
fenago@ath-ubuntu-vm:~$
fenago@ath-ubuntu-vm:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)

fenago@ath-ubuntu-vm:~$
```

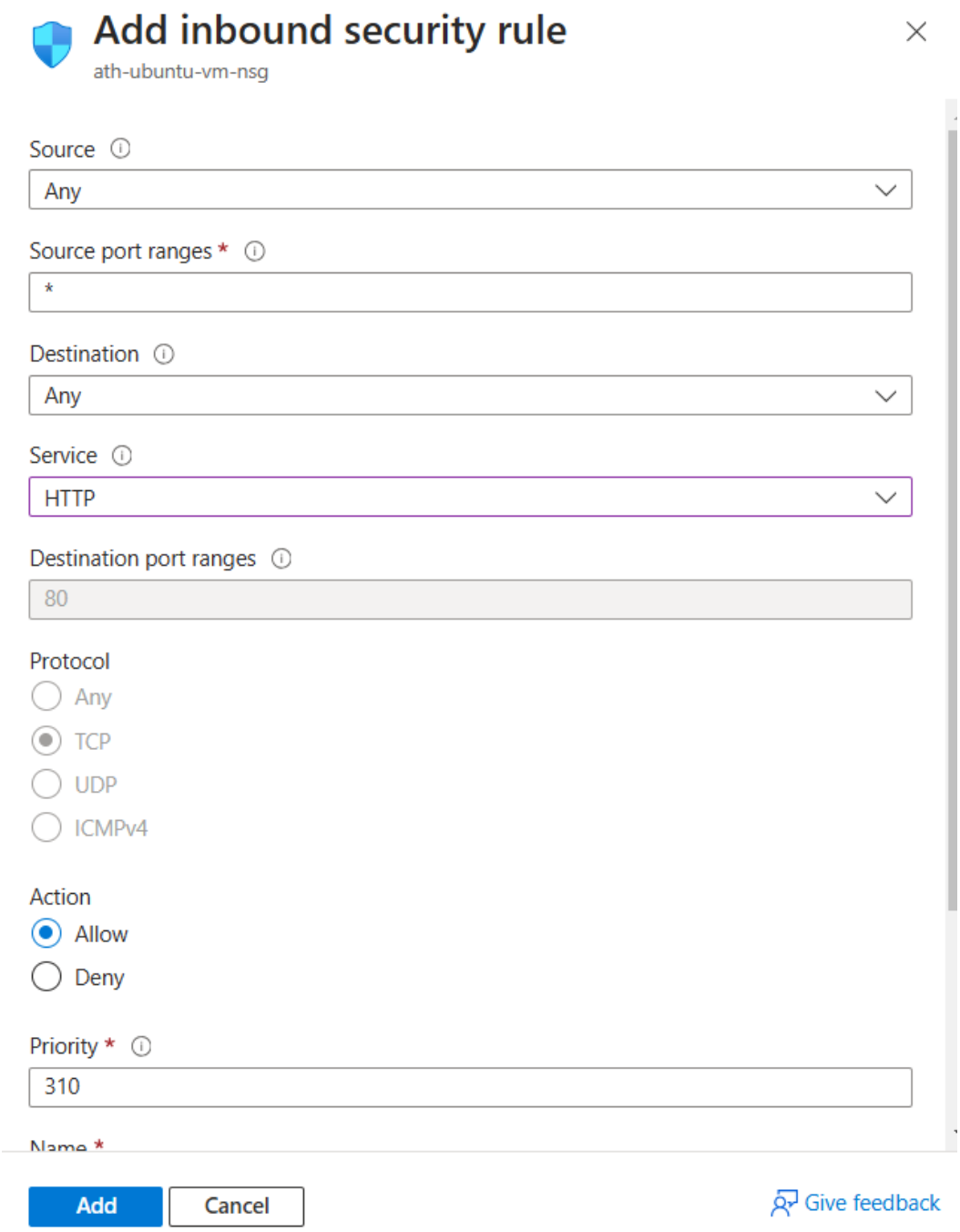
Section 5: Configure Azure Network Security Group (NSG) Rules

In addition to the VM's internal firewall (UFW), Azure enforces inbound and outbound rules through a Network Security Group (NSG). Let's ensure our Azure NSG rules align with what we configured on the VM.

1. **Locate the Network Interface**
   - In the Azure Portal, go to **Virtual machines** and select your VM (for example, `YOUR_NAME-ubuntu-vm`).
   - On the left-hand side, under **Networking**, click **Network Settings**.
2. **View an NSG**
   - You should see existing inbound port rules for your VM's NSG.



3. **Add or Adjust Inbound Security Rules**
   - Click **Add inbound port rule**.
   - **Source**: `Any` (or restrict to specific IP address ranges as needed for better security).
   - **Source port ranges**: `*`.
   - **Destination**: `Any`.
   - **Service**: `HTTP`.
   - **Protocol**: `TCP`.
   - **Action**: `Allow`.
   - **Name**: Provide a descriptive name (e.g., `Allow-80-http`).
   - Click **Add** or **Save** to apply the new rule.



4. **Confirm Any Additional Ports**
   - If you opened any other port on your VM, ensure you add corresponding rules in your NSG.
5. **Review Default NSG Rules**
   - Review all the Default NSG rules

Section 6: Install and Test Nginx

Nginx is a popular open-source web server. Let's install it and verify whether it's accessible based on our firewall settings.

1. **Install Nginx**

   ```
   sudo apt-get install -y nginx
   ```

   - This will also install any dependencies needed for Nginx.

2. **Check Nginx Status**

   ```
   systemctl status nginx
   ```

   - Make sure it shows `active (running)`.

3. **Verify Port 80 is Open**

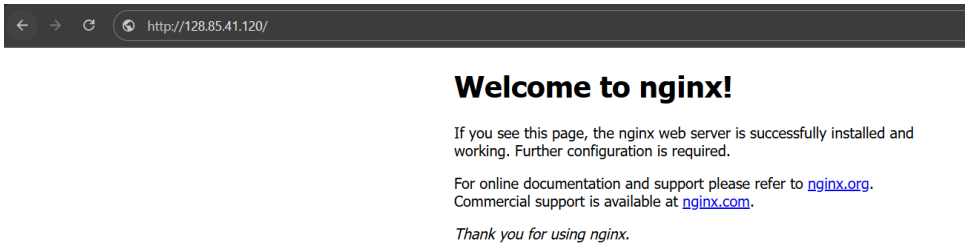
   - If you followed the previous steps, you should have allowed port 80 in both UFW and your NSG.
   - Confirm that port 80 is allowed in UFW:

     ```
     sudo ufw status
     ```

     You should see `80/tcp ALLOW`.
   - Confirm that port 80 is allowed in Azure NSG as well (under **Networking** for your VM in the Azure Portal).

4. **Test Access from a Browser**

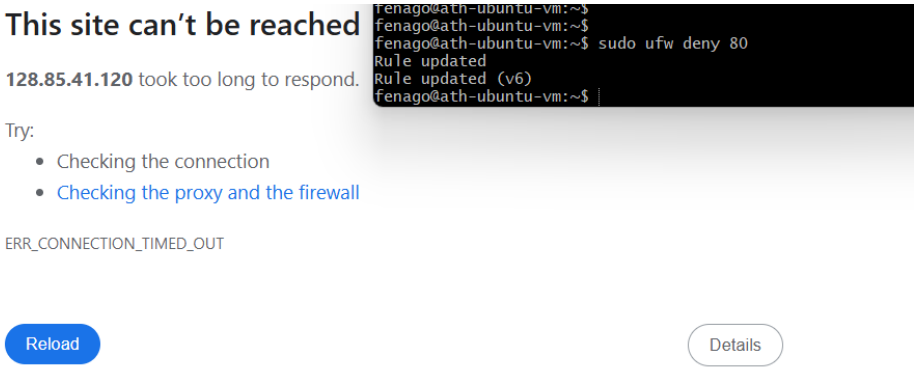
   - On your local machine, open a web browser and go to `http://<public-ip>`.
   - If everything is correctly set up, you should see the default Nginx welcome page.



5. **Test Blocking by Removing or Blocking Port 80**

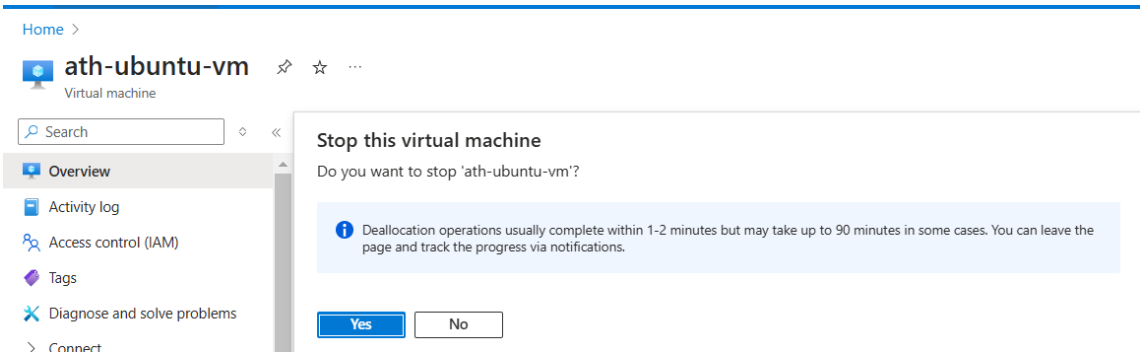
   - If you remove port 80 from UFW or your NSG, retry loading `http://<public-ip>` in the browser. It should fail to connect.

- This confirms your firewall rules are actively controlling access.



Section 7: Stop VM

Make sure to to **Stop** the VM from the Azure Portal.



Conclusion

By completing this lab, you have:

- Created a Linux-based virtual machine in Azure.
- Configured firewall settings using **UFW** on the server.
- Applied and verified Azure Network Security Group (NSG) rules.
- Installed and tested Nginx.
- Confirmed secure access by testing allowed ports and blocked ports.

With these steps, you have taken an essential step toward understanding and implementing a secure server configuration in the Azure cloud.