Lab 1: Securing Web App in Azure VM

Objective

1. Create an Azure Virtual Machine.
2. Provision a Network Security Group
3. Configure Web server on Azure VM
4. Allow Access to Web Server.

Note:

1. All the steps are to be done within Azure Portal.
2. There will be breakout rooms assigned and each room will have a group number [1-5]
3. Login into Azure Portal
    a. Go to https://portal.azure.com
    b. Login with the supplied credentials (username and password).
        i. Each group has a unique integer for their login [1-5] eg. usergroup[1-5]
        ii. For example, group number 5 will have
            1. Username: usergroup5@makecloudwork.com
            2. Password: will be provided during the class.
    c. You will then see the landing Azure homepage. Dismiss any popups/message boxes

---

It's important that you enter all the resource names as the same as mentioned.

Section 1: Create an Azure VM

Steps

1. Type **"Virtual Machines"** on the search bar and select **"Virtual Machines"** from the drop down. You will be redirected to **"Virtual Machines"** page.
2. Click on **"+Create"** button and select **"Azure virtual machine"**
3. **Basics Tab**
    a. Select the resource group from the dropdown.
    b. Give name to Virtual Machine name as "**vmlinuxsb"+"group number"** add your group number as suffix e.g. if your group number is 4, name the machine as **"vmlinuxsb4"**
    c. Region: Choose **(US) East US**
    d. Availability Options: Select **"No Infrastructure redundancy required"**
    e. Security Type: Choose **"Standard"**
    f. Image: Choose **"Ubuntu Server 20.04 LTS – Gen2"** from the dropdown menu

g. Size: Click on **"See all sizes"** and select **"B2s"**.
h. Authentication type: Select **"Password"**
    i. Username: **"azureuser"**
    ii. Password/Confirm Password: **"Welcome@1234"**
i. Public inbound ports: Select **"Allow selected ports"**
    i. Select inbound ports: **"SSH (22)"**
j. Click on **"Next : Disks"**

4. **Disks Tab**
    a. Leave the defaults and click on **"Next: Networking".**
5. **Networking Tab**
    a. Choose the default Virtual Network and Subnet and public IP.
    b. NIC network security group: **None**
    c. Delete public IP and NIC when VM is deleted: Check that
    d. Click on **"Next : Management"**
6. **MaangementTab**
    a. Boot diagnostics: Disable
    b. System assigned managed identity: Check that
    c. Don't change the other defaults and click on **"Review + create"**
7. **Review+Create Tab**
    a. Let the validation run and pass.
    b. Click on **"Create"** and wait for the deployment to complete
    c. Click on **"Go to resource"**. This will take you to the overview page of the newly created Virtual Machine

Observations

1. SSH to the public IP of the VM and login. You should be able to login successfully.

Section 2: Provision a Network Security Group

Steps

1. Login into Azure Portal
2. Type **"Network security groups"** on the search bar and select **"Network security groups"** from the drop down. You will be redirected to **"Network security groups"** page.
3. Click on **"+Create"** button
4. **Basics Tab**
    a. Select the resource group from the dropdown.
    b. Give unique name to Key vault name as "**nsgsb"+"group number"** add your group number as suffix e.g. if your group number is 4, name the resource as **"nsgsb4" .**
    c. Region: Select **"East US"**
    d. Click on **"Review + create"**

5. **Review+Create Tab**
    a. Let the validation run and pass.
    b. Click on **"Create"** and wait for the deployment to complete
    c. Click on **"Go to resource"**. This will take you to the overview page of the newly created NSG
6. Click on **Subnets** under Settings
7. Click on **"+Associate"**
    a. Virtual network: Select from the drop down
    b. Subnet: Select "default" from the drop down.
    c. Click "OK"
8. Try to SSH to the public IP of the VM and login. You should not be able to login successfully.

    Discuss within the Breakout room, why?

9. Within the newly created NSG, click on **Inbound security rules** under Settings
10. Click on **"+Add"**
    a. Source: Select **"Service Tag"**
    b. Source Service tag: Select **"Internet"**
    c. Source port ranges: **"*"**
    d. Destination**:** Select **"Service Tag"**
    e. Destination Service tag: Select **"VirtualNetwork"**
    f. Service: Select **"SSH"**
    g. Action: **"Allow"**
    h. Priority: **"100"**
    i. Name: **"Port_ssh"**
    j. Click on **"Add". Wait few moments**
11. Try to SSH to the public IP of the VM and login. You should be able to login successfully.

Section 3: Configure Web server on Azure VM

Steps

1. SSH to the VM through Terminal or ssh client.
2. Once logged in, run the following commands (one by one)

    sudo apt update

    sudo apt upgrade

    sudo apt install docker.io

    sudo su

    docker pull nginx

    docker run --name nginx-container -d -p 80:80 nginx

3. Open a web browser and go to http://<public ip of vm>. You should not be able to access the nginx homepage.

   Discuss within the Breakout room, why? and what needs to be done.

Section 4: Allow Access to Web Server

Steps

1. Within the newly created NSG, click on **Inbound security rules** under Settings
2. Click on **"+Add"**
   a. Source: Select **"Service Tag"**
   b. Source Service tag: Select **"Internet"**
   c. Source port ranges: **"*"**
   d. Destination**:** Select **"Service Tag"**
   e. Destination Service tag: Select **"VirtualNetwork"**
   f. Service: Select **"HTTP"**
   g. Action: **"Allow"**
   h. Priority: **"110"**
   i. Name: **"Port_http"**
   j. Click on **"Add". Wait few moments**
3. Open a web browser and go to http://<public ip of vm>. You should be able to access the nginx homepage.

End of Lab.