Lab2-Securing IaaS workloads

Objectives

To create an Azure VM and secure the web application configured on that VM by enabling the required ports.

Sections

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

Note:

1. All the steps are to be done within VS Code and Azure Portal on your VM Machine.
2. There will be breakout rooms assigned for both individual and group labs.
3. Group ID: Every 4-5 participants will belong in a group and each group will have a Group ID [1-4]
4. Participant ID: Every participant will also get a unique number as participant id. This id along with group id will be used to help name Azure resources.

> *Please remember and note your [Participant ID+Group ID]*

5. Once you are logged into your VM Machine. Login into Azure Portal
    a. Go to https://portal.azure.com
    b. Login with the supplied credentials (username and password).
        i. Each participant has a unique integer for their login [1-20] eg. vmuser[1-20]
        ii. For example, participant number 5 will have
            1. Username: vmuser5@acclod.ca
            2. Password: will be provided during the class.
    c. You will then see the landing Azure homepage. Dismiss any popups/message boxes

6. Although this is a group lab, every individual will complete the lab on their VM Machine. Individuals within a group are expected to discuss and help each other.

It’s important that you enter all the resource names as the same as mentioned and only access the one that you have created as there will be many within a single group.

Section 1: Create a Virtual Network and Subnet

Steps

1. Login into Azure Portal
2. Type **“Virtual networks”** on the search bar and select **“Virtual networks”** from the drop down. You will be redirected to **“Virtual networks”** page.
3. Click on **“+ Create”**
4. **Basics**
    a. **Subscription**: Select subscription.
    b. **Resource group**: Select resource group.
    c. **Virtual Network name:** Enter a unique name, **aimlsecvnet[participant id +group id]**.
    For example: aimlsecvnet216 (participant id as 21 and group id as 6)
    d. **Region:** Select your assigned Region.

Group1	Group2	Group3	Group4
East US 2	West US	West US2	Canada Central

    e. Leave all the other defaults and click on **“Next”**
5. **Security** Tab
    a. Accept all the defaults and click on **“IP addresses”**
6. **IP addresses** Tab
    a. Look at the address space. Click on **“+ Add a subnet”**
    b. Name: “**subnet[participantid+groupid**]” (Remember this subnet)
    c. Look at all the different options and don’t change the defaults
    d. Click on **“Add”**. You have created a new subnet.

    Knowledge Check: Can you create a subnet with starting address as 10.1.0.0. Discuss within the group.

    e. Accept all the 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. Once the deployment is completed, click on **“Go to resource”**

Section 2: 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 "**vmaiml[participant id +group id]"**
    c. **Region:** Select your assigned Region.

Group1	Group2	Group3	Group4
East US 2	West US	West US2	Canada Central

    d. Availability Options: Select **"No Infrastructure redundancy required"**
    e. Security Type: Choose **"Standard"**
    f. Image: Choose **"Ubuntu Server 24.04 LTS – x64 Gen2"** from the dropdown menu
    g. Image: Click on **"See all sizes"** and select **"B2s_v2"** or **"D2s_v2"**
    h. Authentication type: Select **"Password"**
        i. Username: **"azureuser"**
        ii. Password/Confirm Password: **"<enter any password>"**
    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. Virtual Network: Select the one you created above
    b. Subnet: Select the one you created above (not the "default" one)
    c. Public IP: New
    d. NIC network security group: **None**
    e. Delete public IP and NIC when VM is deleted: **Check that**
    f. Click on **"Next : Management"**
6. **Management Tab**
    a. Enable system assigned managed identity: **Check that**
    b. **Uncheck the Enable auto-shutdown**
    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. Notice the public IP.

Section 3: Provision a Network Security Group

Steps

1. Login into Azure Portal
2. Type **"NSG"** 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 network security name as "**nsg"+"group number"+"participant id"** e.g. if your participant id is 21 and group number is 4, name the resource as **"nsg215" .**
    c. **Region:** Select your assigned Region.

Group1	Group2	Group3	Group4
East US 2	West US	West US2	Canada Central

    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 **"the one you created"** from the drop down.
    c. Click "OK"

8. Try to SSH to the public IP of the VM and login.
   You can use Putty
   or
   on VS Code Terminal Window, type ssh azureuser@<public ip>

9. PAUSE: You should not be able to login successfully.
   Discuss within the Breakout room, why?

10. Within the newly created NSG, click on **Inbound security rules** under Settings
11. 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 a few moments to have it create the security rule.

12. Try to again SSH to the public IP of the VM and login. You should be able to login successfully.

Section 4: Configure Web server on Azure VM

Steps

1. SSH to the VM through Terminal or any 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 photoprism/photoprism

   docker run -d --name photoprism -p 2342:2342 -e PHOTOPRISM_UPLOAD_NSFW="true"
   -e PHOTOPRISM_AUTH_MODE="public"   -v /photoprism/storage  -v
   ~/Pictures:/photoprism/originals  photoprism/photoprism
   ```

   (This will run an image of Photoprism on the VM on port 2342)

3. Open a web browser and go to http://<public ip of vm>:2342. You should not be able to access the Photoprism homepage.

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

Section 5: Allow Access to VM Server

Steps

1. Type **"Network security groups"** on the search bar and select the one you have just created.
2. Within the newly created NSG, click on **Inbound security rules** under Settings
3. 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 **"Custom"**
    g. Destination port ranges: Enter **2342**
    h. Action: **"Allow"**
    i. Priority: **"110"**
    j. Name: **Take the default**
    k. Click on **"Add". Wait few moments**

4. Open a web browser and go to http://<public ip of vm>:2342. You should be able to see the Photoprism homepage.
5. Lastly, do Step 3 a couple of times and add both HTTP (port 80) and HTTPS (443).

End of Lab.