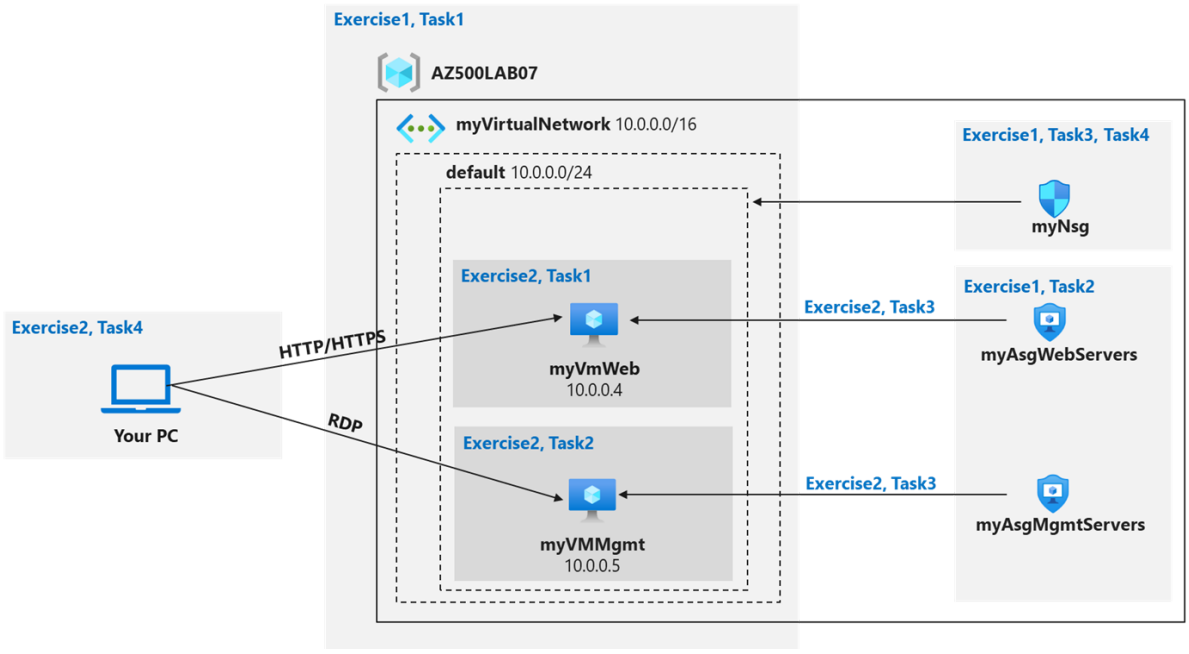
Fatma Omar Salim
Cloud Security Project
Cloud Provider: Azure
Network Security Groups and Application Security Groups
Lab Scenario

I have been asked to implement my organization's virtual networking infrastructure and test to ensure that it is working correctly. To add more context:

1. The organization has two groups of servers: Web Servers and Management Servers.
2. Each group should be in its own Application Security Group.
3. I should be able to RDP into the Management Servers, but not the Web Servers.
4. The Web Servers should display the IIS web page when accessed from the internet.
5. Network Security Group rules should be used to control network access.

Lab Objectives

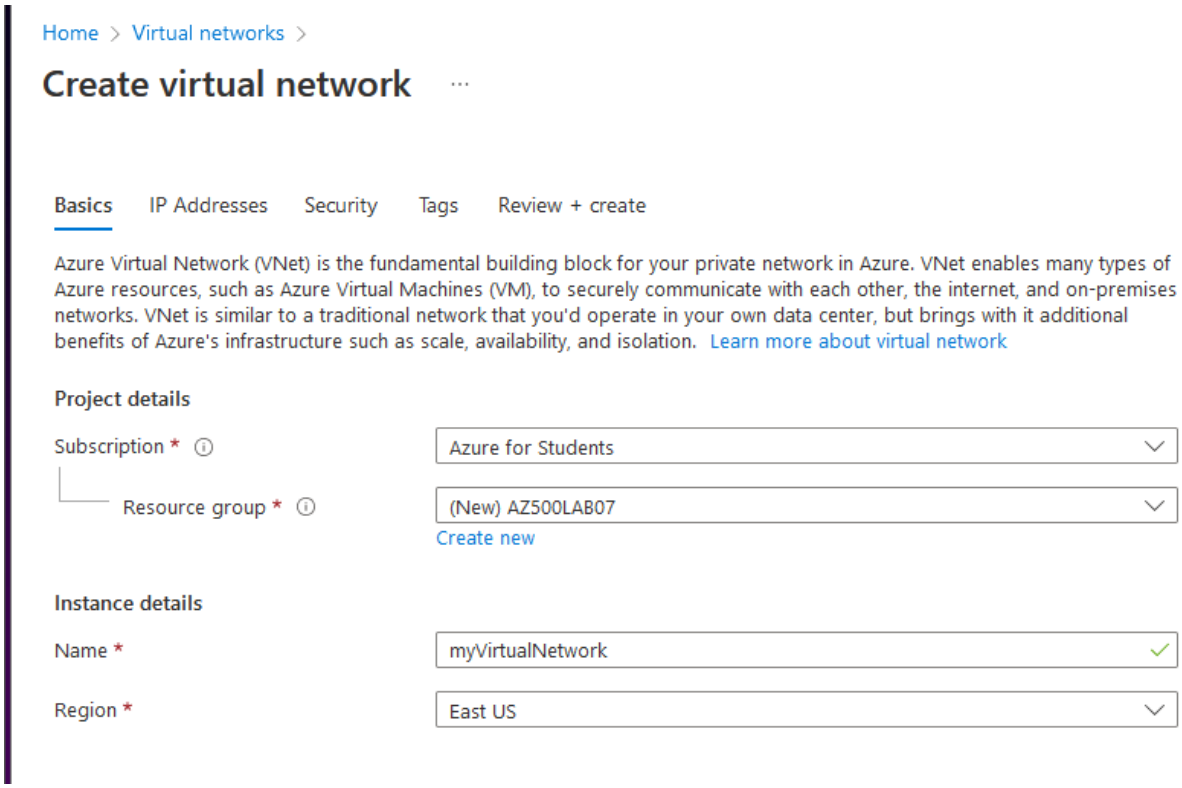
1. Exercise 1: Create the virtual networking infrastructure.
2. Exercise 2: Deploy virtual machines and test the network filters.



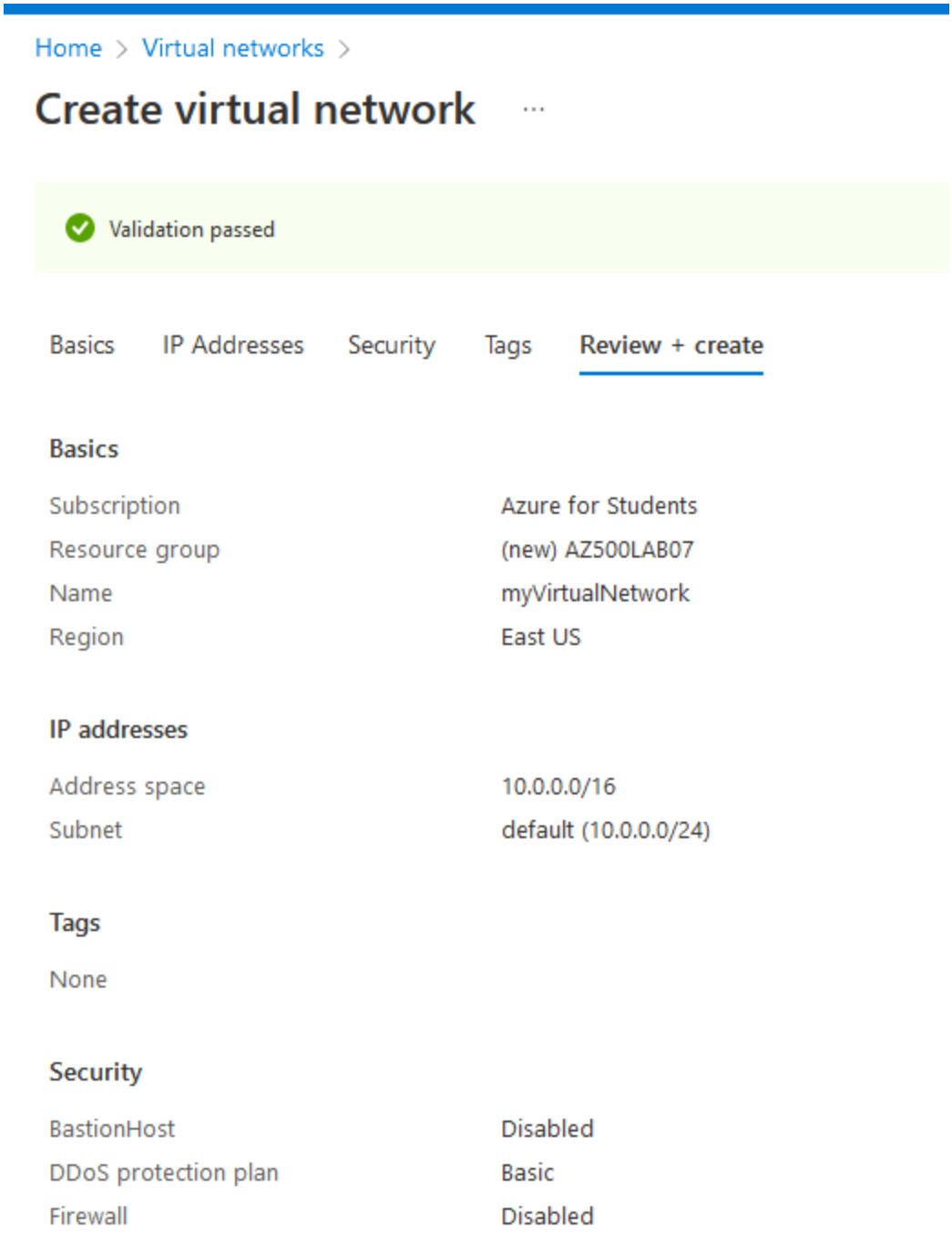
Exercise 1: Creating the virtual networking infrastructure

Task 1: Creating a virtual network with one subnet

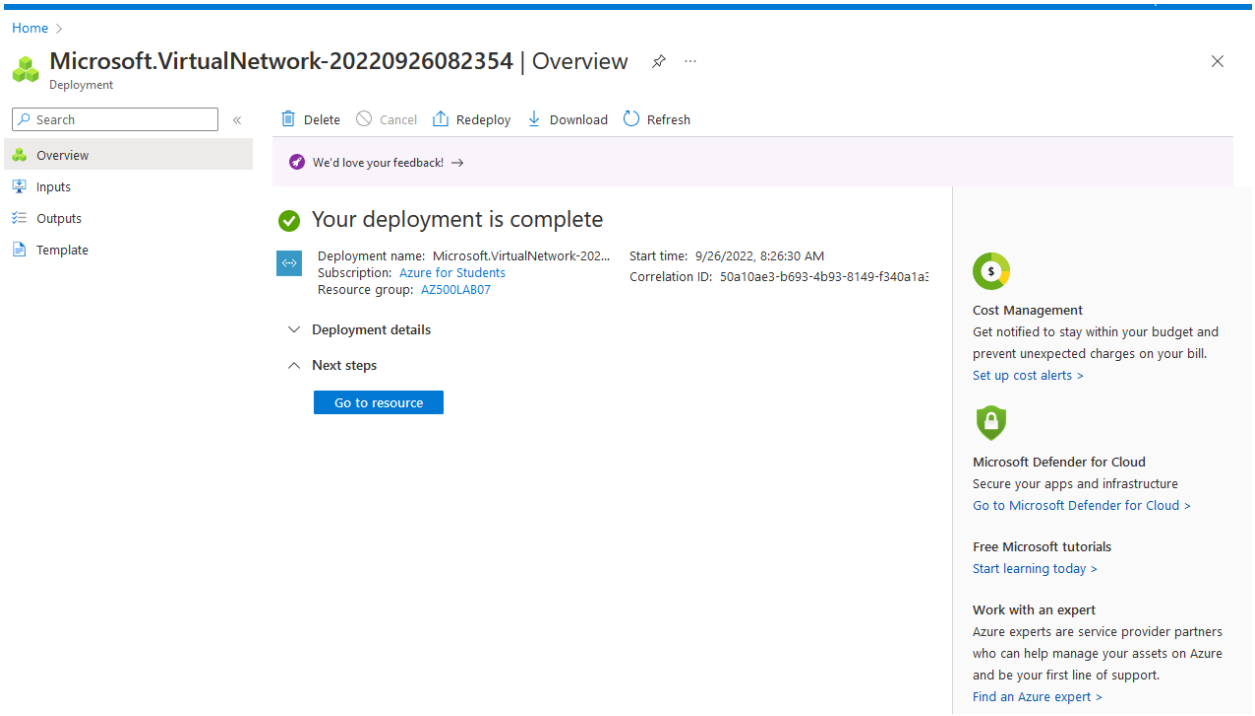
1. Sign in to the Azure Portal.
2. In the **Search** bar, type **Virtual Networks** and press **Enter**.
3. On the **Virtual Networks** blade, click **+ Create**.
4. Specify the following:



5. On the **IP addresses** tab of the **Create virtual network** blade, set the **IPv4 address space** to **10.0.0.0/16**, and, if needed, in the **Subnet name** column, click **default**, on the **Edit subnet** blade, specify the following settings and click **Save**.
6. Back on the **IP addresses** tab of the **Create virtual network** blade, click **Review + create**.

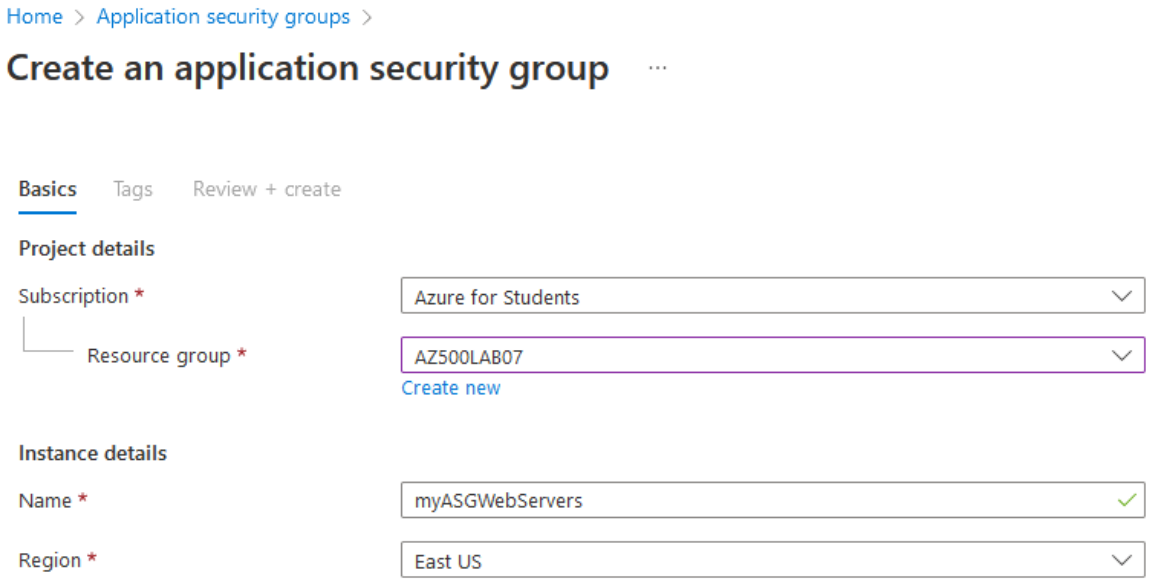


7. Virtual Network creation is now successful:

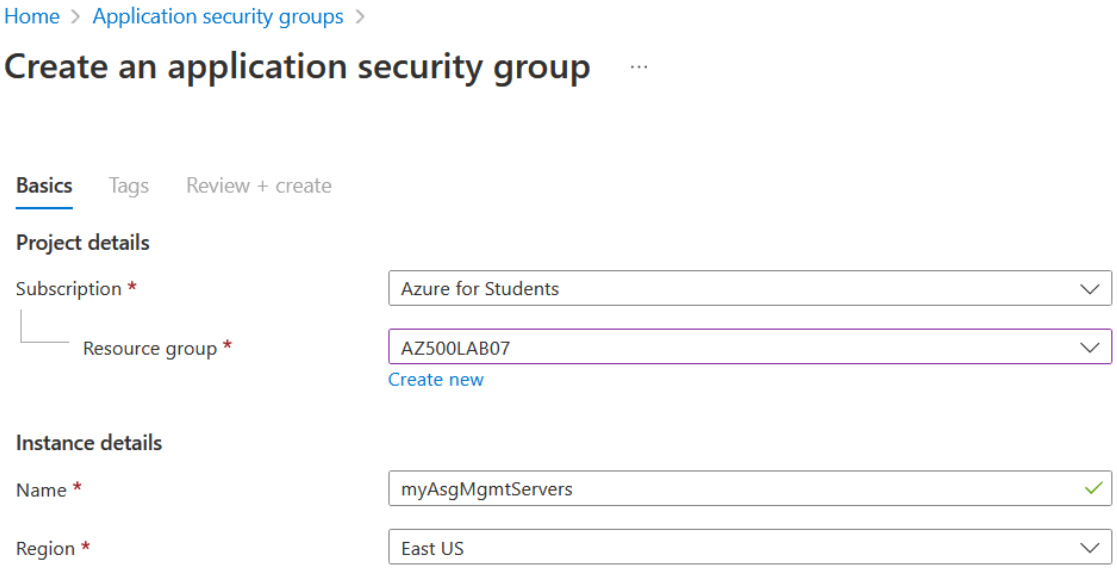


Task 2: Creating the application security group.

1. In the **Search bar**, type **Application Security Groups** and press **Enter**.
2. On the **Application security groups** blade, click **+ Create**.
3. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:



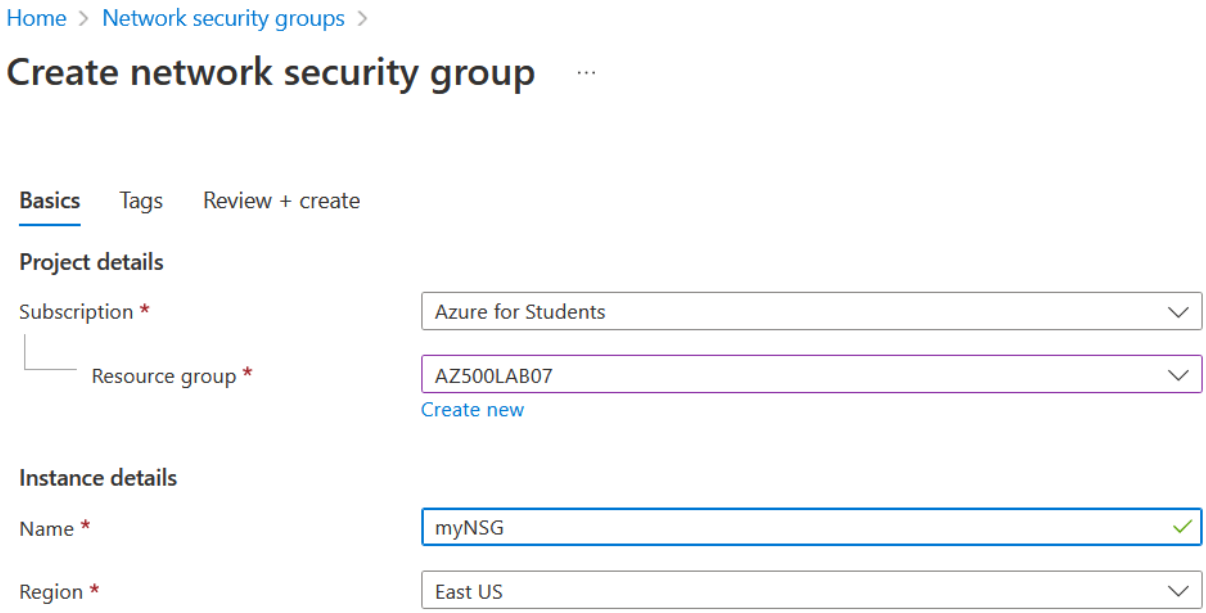
4. Click **Review + create** and then click **Create.**
5. Navigate back to the **Application security groups** blade and click **+ Create**.
6. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:



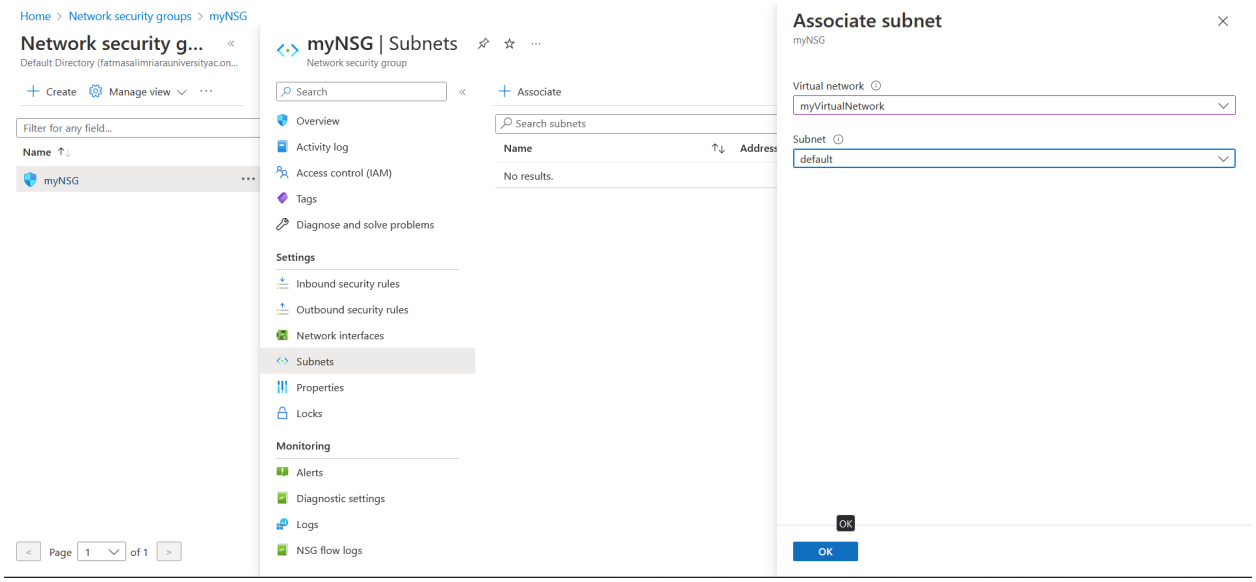
7. Click **Review + create** and then click **Create**.

Task 3: Creating a network security group and associate the NSG to the subnet.
In this task, I will create a network security group.

1. In the **Search** bar, type **Network Security Group** and press **Enter**.
2. On the **Network security groups** blade, click **+ Create**.
3. On the **Basics** tab of the **Create network security group** blade, specify the following settings:

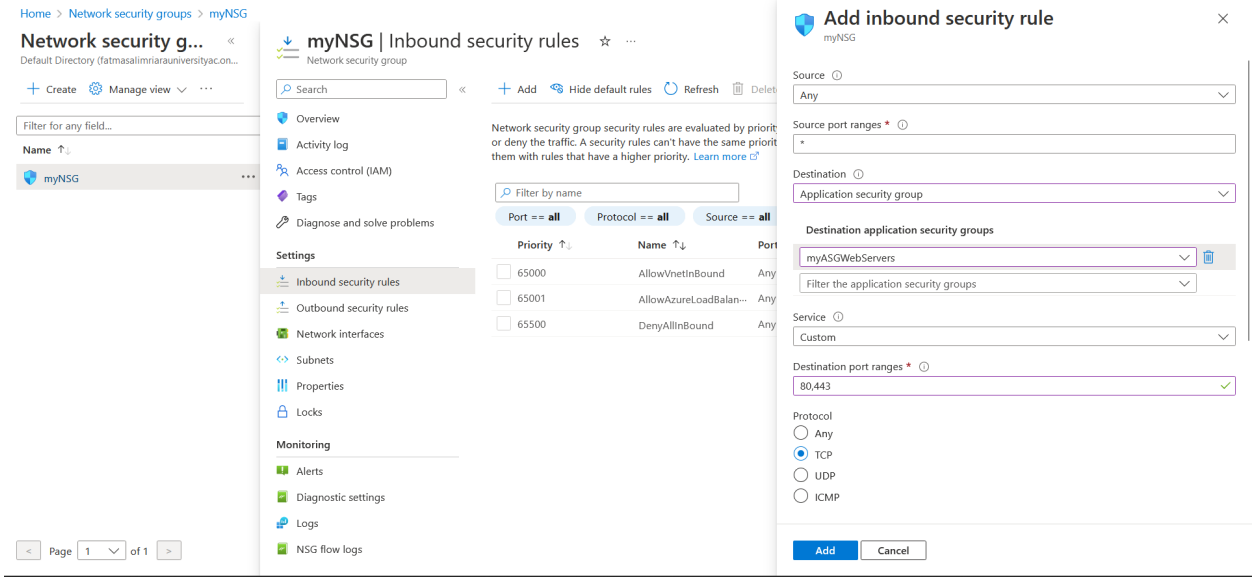


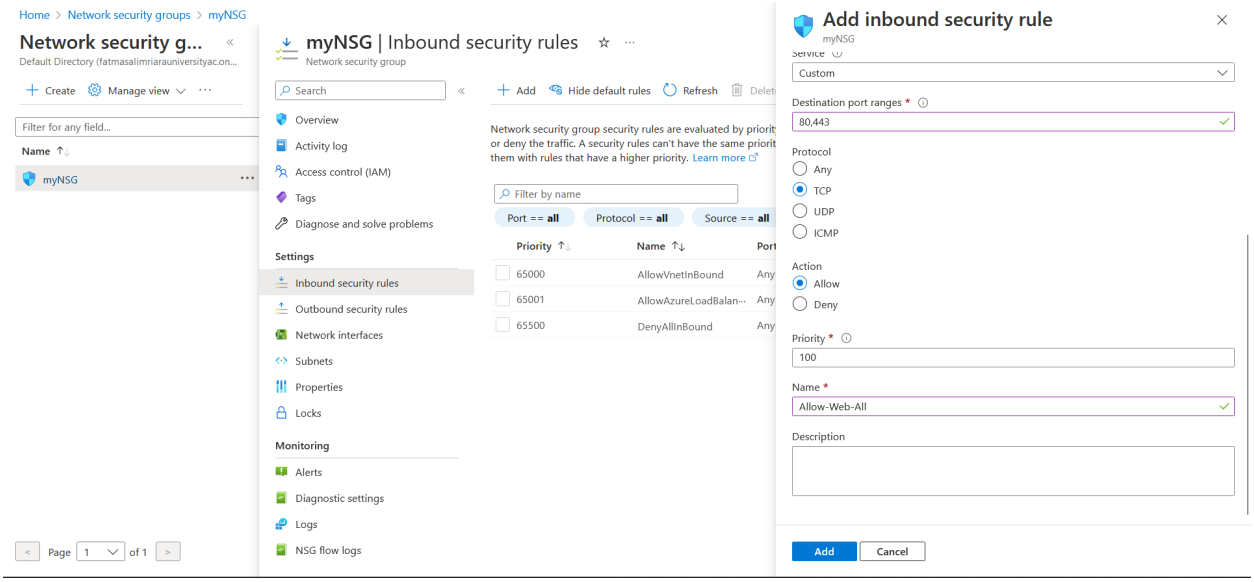
4. Click **Review + create** and then click **Create**.
5. In the Azure portal, navigate back to the **Network security groups** blade and click the **myNsg** entry.
6. On the **myNsg** blade, in the **Settings** section, click **Subnets** and then click **+ Associate**.
7. On the **Associate subnet** blade, specify the following settings and click **OK**:



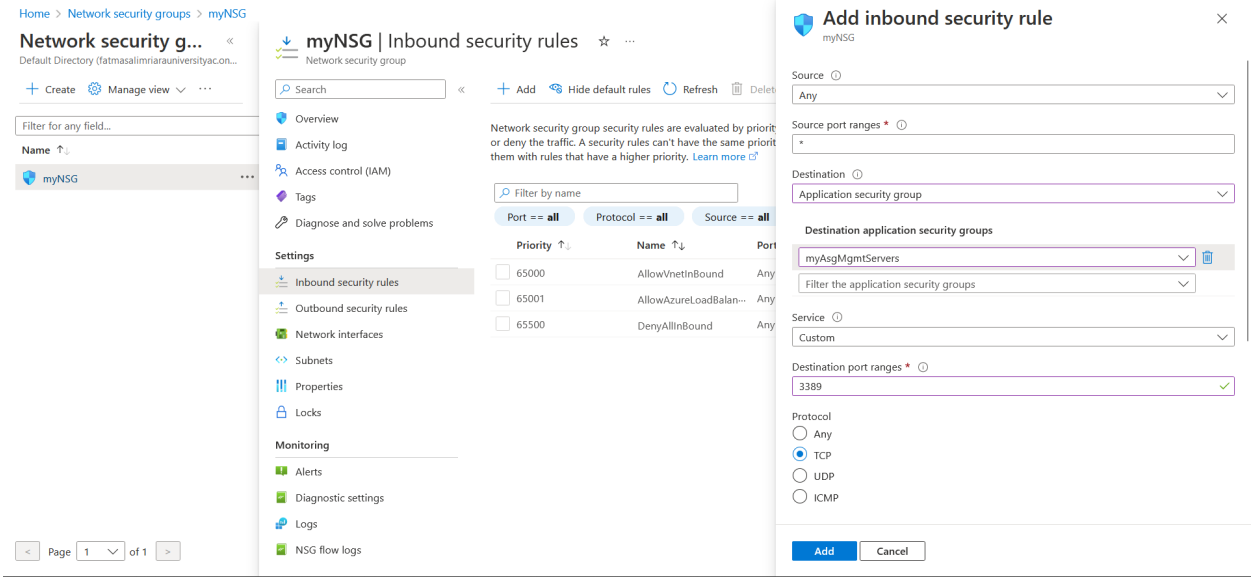
Task 4: Creating inbound NSG security rules to all traffic to web servers and RDP to the servers.

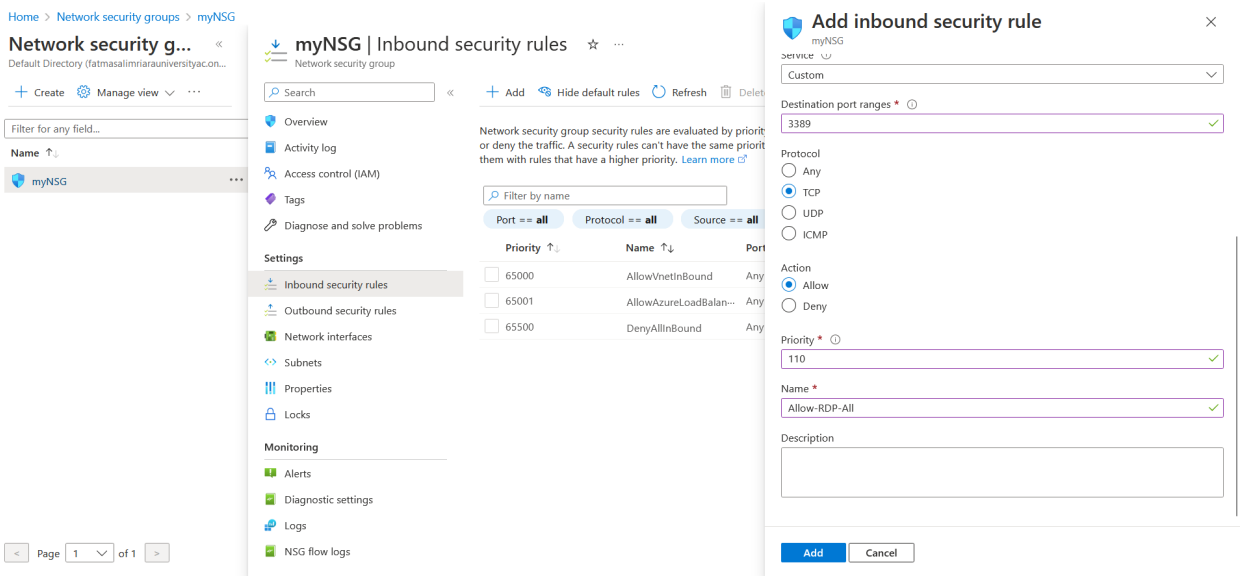
1. On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**.
2. Review the default inbound security rules and then click **+ Add**.
3. On the **Add inbound security rule** blade, specify the following settings to allow TCP ports 80 and 443 to the **myAsgWebServers** application security group (leave all other values with their default values):





4. On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.
5. On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**, and then click **+ Add**.
6. On the **Add inbound security rule** blade, specify the following settings to allow the RDP port (TCP 3389) to the **myAsgMgmtServers** application security group (leave all other values with their default values):





7. On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.

I have now deployed a virtual network, network security with inbound security rules, and two application security groups.

Exercise 2: Deploying virtual machines and testing network filters.

Task 1: Creating a virtual machine to use as a web server.

1. In the **Search** bar, type **Virtual Machines** and press **Enter**.
2. On the **Virtual machines** blade, click **+ Create** and, in the dropdown list, click **+ Azure virtual machine**.
3. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

Home > Virtual machines >

Create a virtual machine ...

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

Resource group * : AZ500LAB07

Create new

Instance details

Virtual machine name * : myVmWeb

Region * : (US) West US 3

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : Windows Server 2022 Datacenter: Azure Edition - Gen2

See all images | Configure VM generation

VM architecture :

- Arm64
- x64

Arm64 is not supported with the selected image.

Home > Virtual machines >

Create a virtual machine ...

Run with Azure Spot discount ☐

Size * Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US$137.24/month)

See all sizes

Administrator account

Username * Student

Password * ••••••••••••••

Confirm password * ••••••••••••••

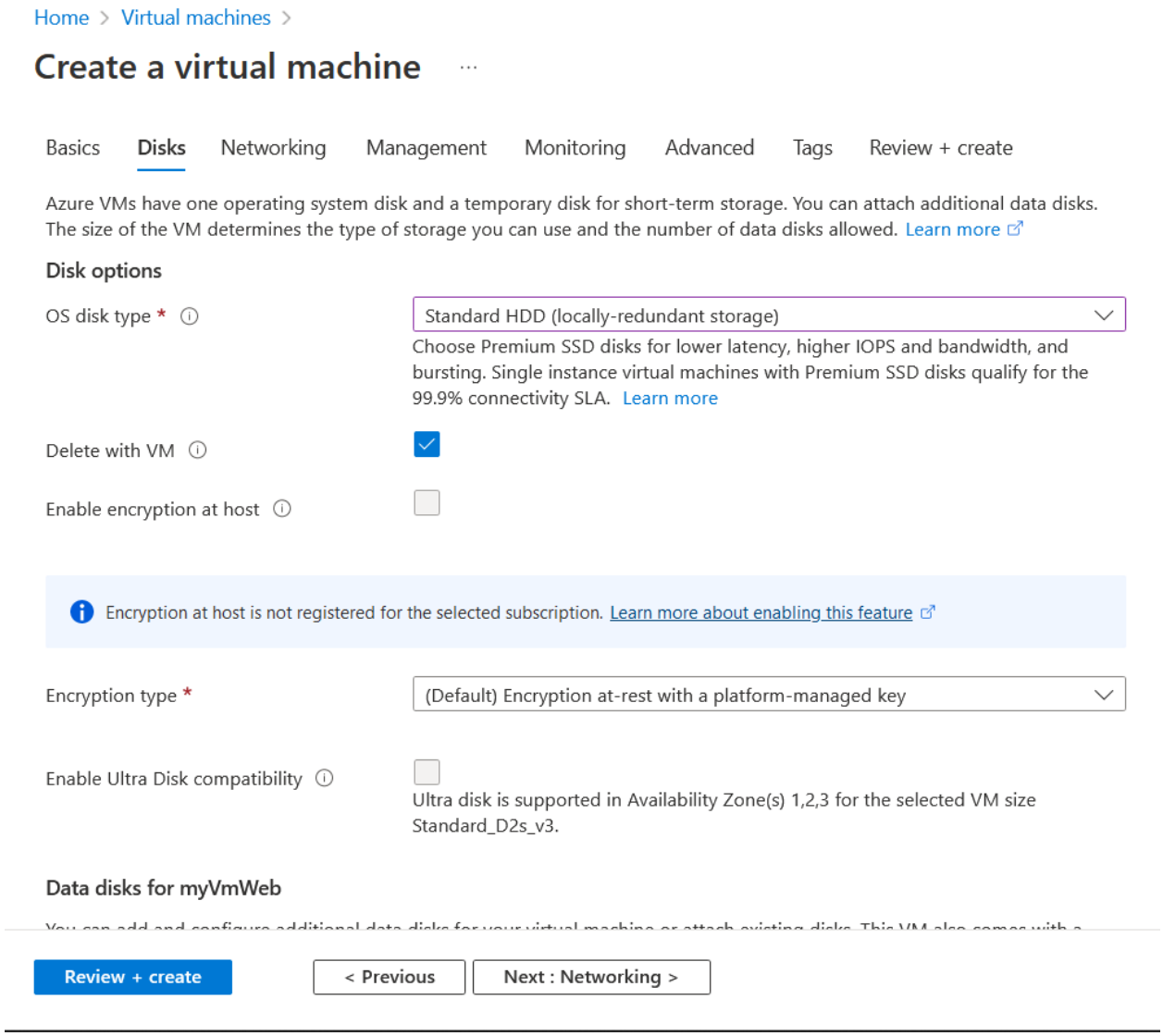
Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ◉ None ○ Allow selected ports

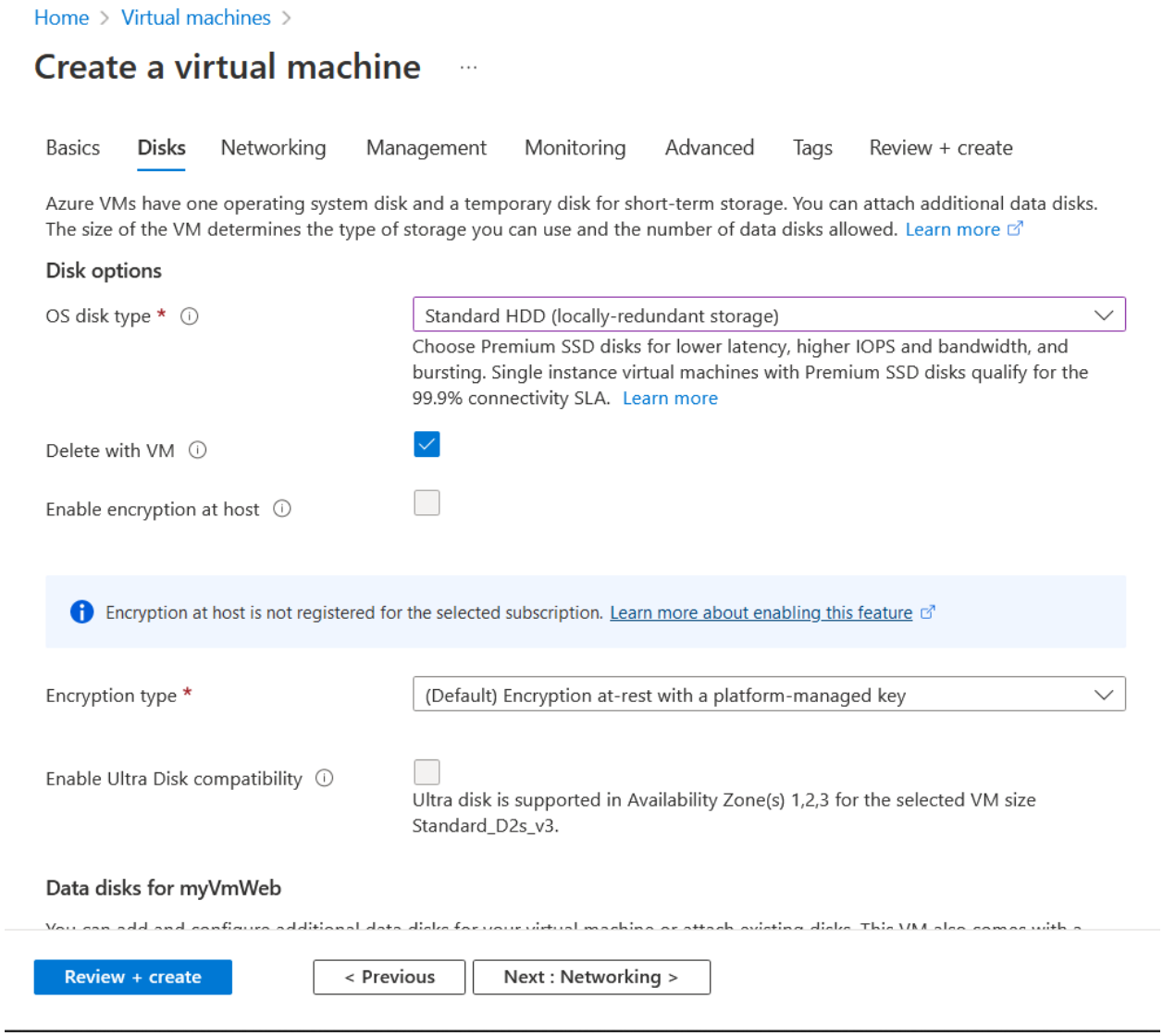
Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

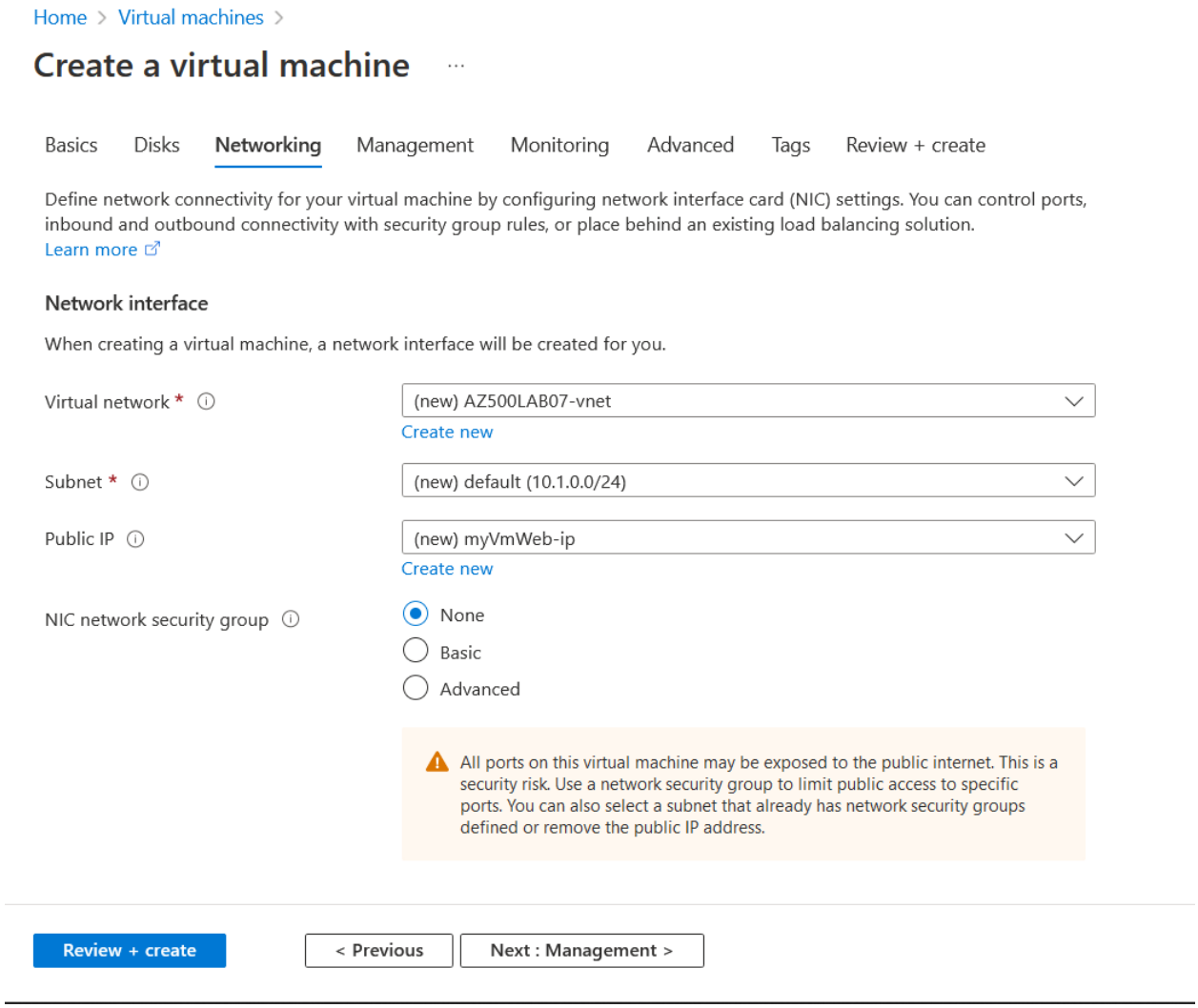


For public inbound ports, we will rely on the precreated NSG.

4. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.



5. On the **Networking** tab of the **Create a virtual machine** blade, select the previously created network **myVirtualNetwork**.
6. Under **NIC network security group** select **None**.
7. Click **Next: Management >**, then click **Next: Monitoring >**on the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:



8. Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create**.

Task 2: Creating a virtual machine to use as a management server.

1. In the Azure portal, navigate back to the **Virtual machines** blade, click **+ Create**, and, in the dropdown list, click **+ Azure virtual machine**.
2. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

Home > Virtual machines >

Create a virtual machine ...

your resources.

Subscription * ⓘ — Azure for Students

Resource group * ⓘ — AZ500LAB07

Create new

Instance details

Virtual machine name * ⓘ — myVMMgmt

Region * ⓘ — (US) West US 3

Availability options ⓘ — No infrastructure redundancy required

Security type ⓘ — Standard

Image * ⓘ — Windows Server 2022 Datacenter: Azure Edition - Gen2

See all images | Configure VM generation

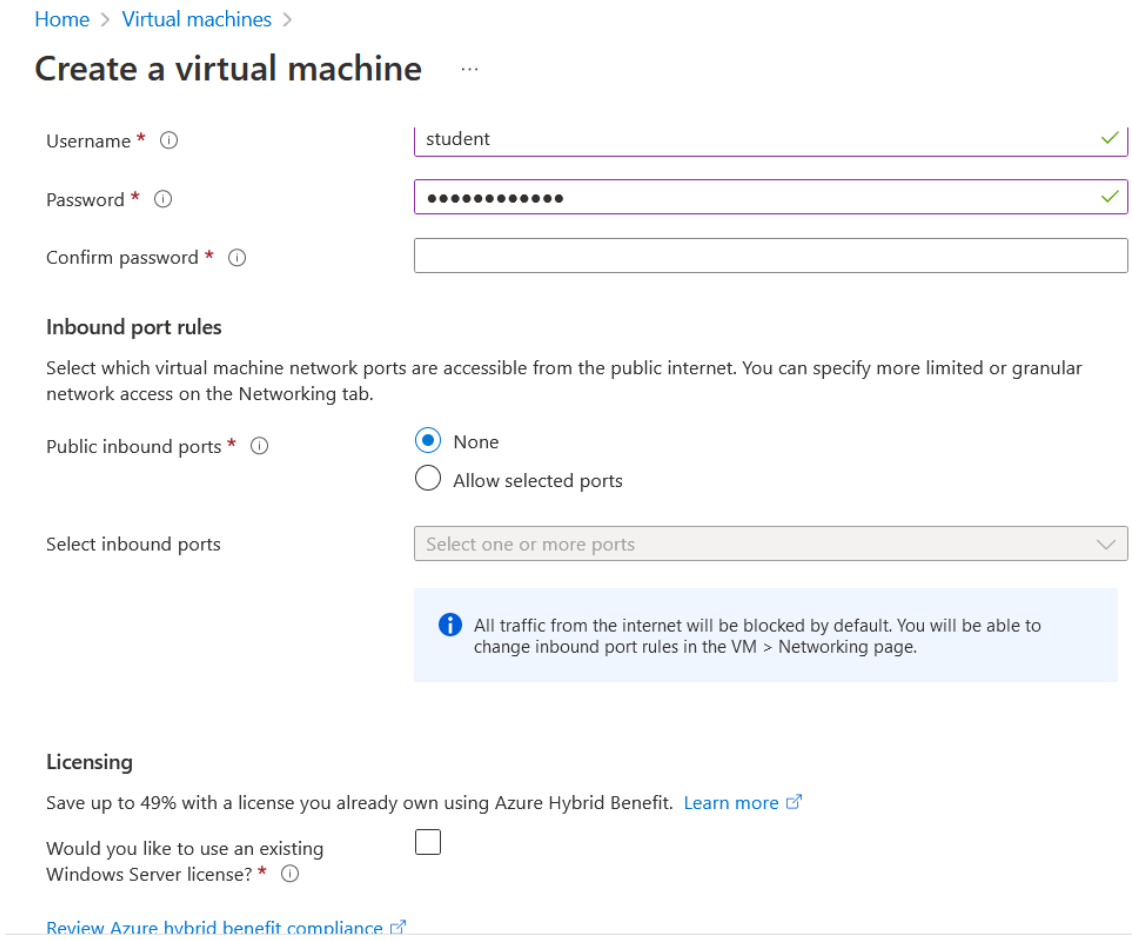
VM architecture ⓘ

- Arm64
- x64 (selected)

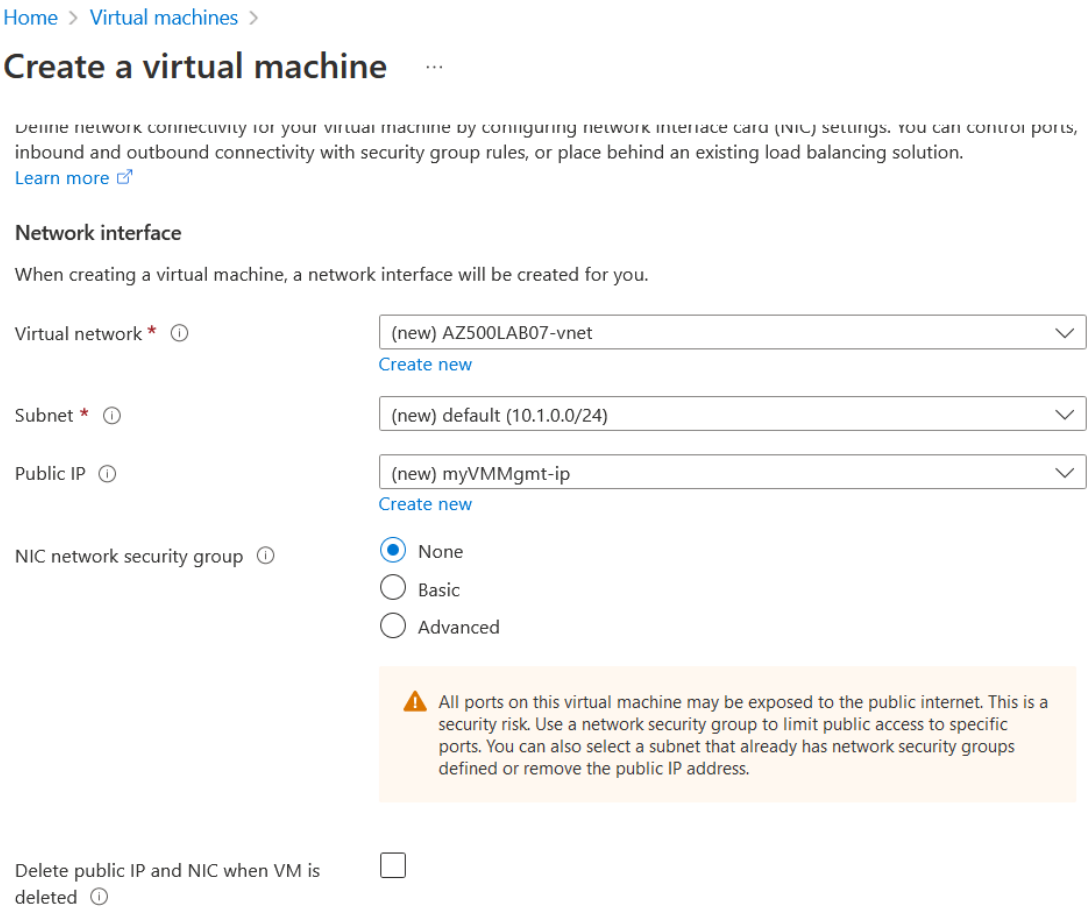
Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

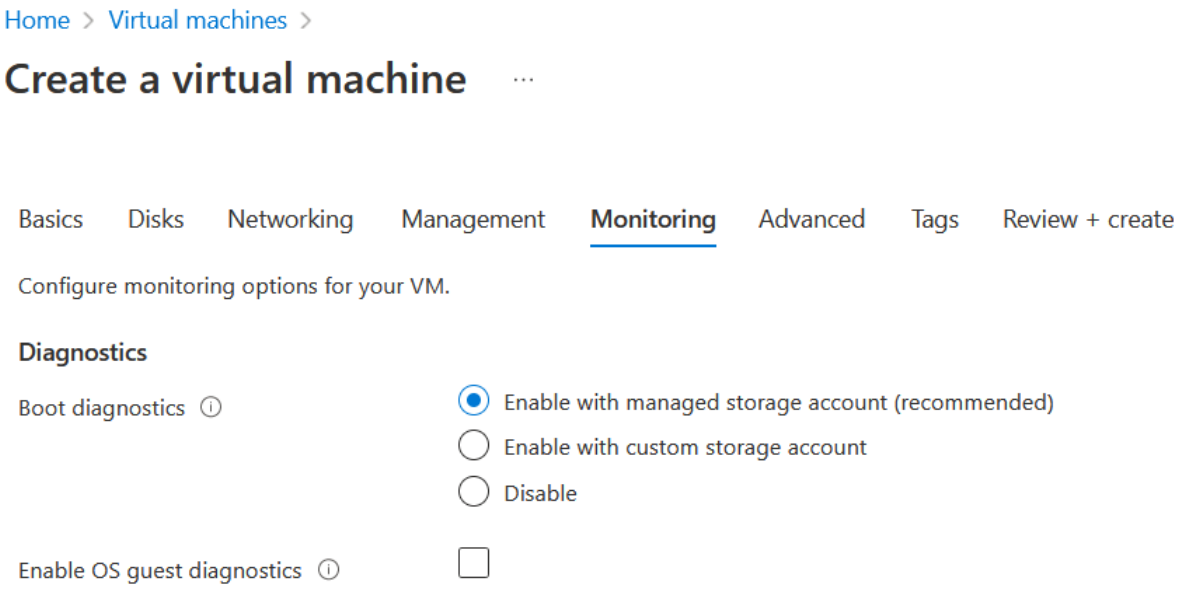
Size * ⓘ



3. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.
4. On the **Networking** tab of the **Create a virtual machine** blade, select the previously created network **myVirtualNetwork**.
5. Under **NIC network security group** select **None**.



6. Click **Next: Management >**, then click **Next: Monitoring >**on the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:



7. Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create**.

Wait for both virtual machines to be provisioned before continuing.

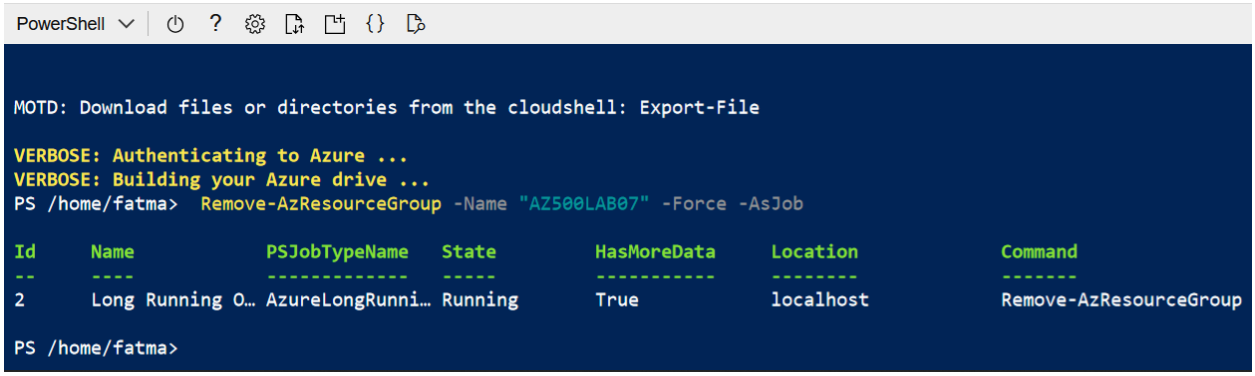
Task 3: Associating each virtual machines network interface to its application security group.

1. In the Azure portal, navigate back to the **Virtual machines** blade and verify that both virtual machines are listed with the **Running** status.
2. In the list of virtual machines, click the **myVMWeb** entry.
3. On the **myVMWeb** blade, in the **Settings** section, click **Networking** and then, on the **myVMWeb | Networking** blade, click the **Application security groups** tab.
4. Click **Configure the application security groups**, in the **Application security group** drop-down list, select **myAsgWebServers**, and then click **Save**.
5. Navigate back to the **Virtual machines** blade and in the list of virtual machines, click the **myVMMgmt** entry.
6. On the **myVMMgmt** blade, in the **Settings** section, click **Networking** and then, on the **myVMMgmt | Networking** blade, click the **Application security groups** tab.

7. Click **Configure the application security groups**, in the **Application security group** drop-down list, select **myAsgMgmtServers**, and then click **Save**.

Clean up resources

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **Create storage**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:



4. Close the **Cloud Shell** pane.