

**Fatma Omar Salim**

**Cloud Security Project**

**Cloud Provider: Azure**

**Network Security Groups and Application Security Groups**

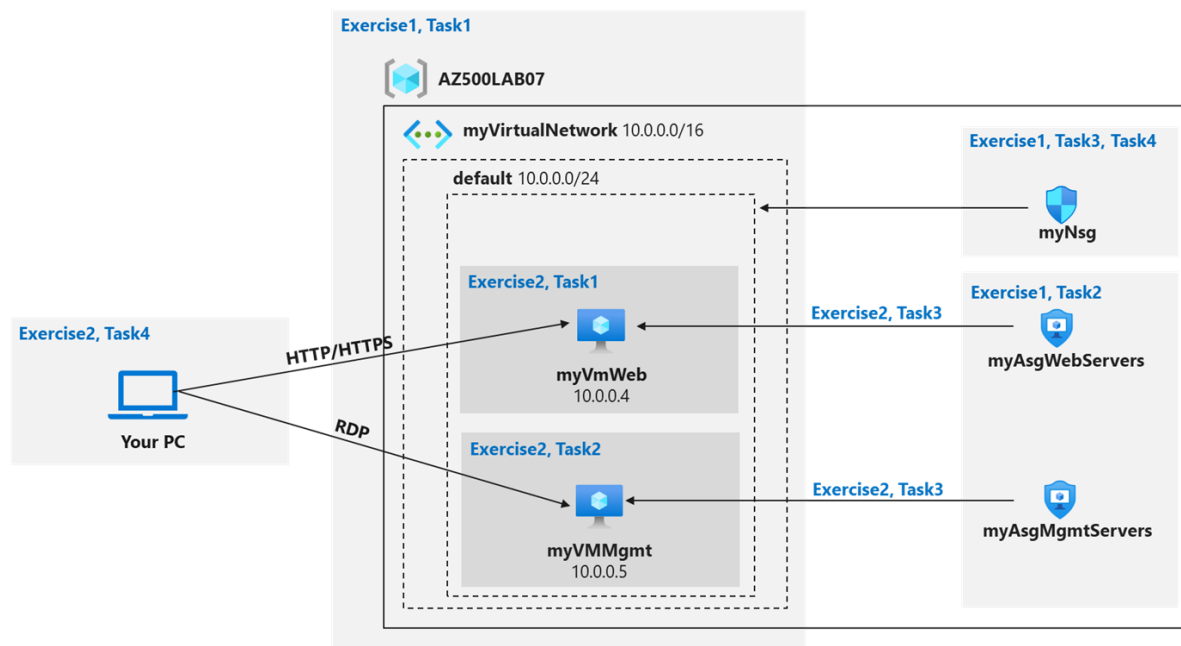
**Lab Scenario**

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:

The screenshot shows the 'Create virtual network' blade in the Azure Portal. The breadcrumb navigation at the top reads 'Home > Virtual networks >'. The main heading is 'Create virtual network' followed by three dots. Below this is a tabbed interface with 'Basics' selected, and other tabs for 'IP Addresses', 'Security', 'Tags', and 'Review + create'. A descriptive paragraph about Azure Virtual Network (VNet) is provided, followed by a link to 'Learn more about virtual network'. The form is divided into two sections: 'Project details' and 'Instance details'. In 'Project details', 'Subscription' is set to 'Azure for Students' and 'Resource group' is set to '(New) AZ500LAB07', with a 'Create new' link below. In 'Instance details', 'Name' is 'myVirtualNetwork' (marked with a green check) and 'Region' is 'East US'.

Home > Virtual networks >

## Create virtual network ...

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

### Project details

Subscription \* ⓘ Azure for Students

Resource group \* ⓘ (New) AZ500LAB07  
[Create new](#)

### Instance details

Name \* myVirtualNetwork ✓

Region \* East US

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**.

[Home](#) > [Virtual networks](#) >

## Create virtual network ...

✓ Validation passed

[Basics](#)   [IP Addresses](#)   [Security](#)   [Tags](#)   [Review + create](#)

### Basics

Subscription	Azure for Students
Resource group	(new) AZ500LAB07
Name	myVirtualNetwork
Region	East US

### IP addresses

Address space	10.0.0.0/16
Subnet	default (10.0.0.0/24)

### Tags

None

### Security

BastionHost	Disabled
DDoS protection plan	Basic
Firewall	Disabled

7. Virtual Network creation is now successful:

Home >

Microsoft.VirtualNetwork-20220926082354 | Overview ✨ ...

Deployment

Search << Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-202... Start time: 9/26/2022, 8:26:30 AM  
Subscription: [Azure for Students](#) Correlation ID: 50a10ae3-b693-4b93-8149-f340a1a2  
Resource group: [AZ500LAB07](#)

Deployment details

Next steps

[Go to resource](#)

Cost Management

Get notified to stay within your budget and prevent unexpected charges on your bill.  
[Set up cost alerts >](#)

Microsoft Defender for Cloud

Secure your apps and infrastructure  
[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials

[Start learning today >](#)

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.  
[Find an Azure expert >](#)

## 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:

[Home](#) > [Application security groups](#) >

## Create an application security group ...

**Basics** Tags Review + create

### Project details

Subscription *	Azure for Students	▼
Resource group *	AZ500LAB07	▼

[Create new](#)

### Instance details

Name *	myASGWebServers	✓
Region *	East US	▼

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

[Home](#) > [Application security groups](#) >

## Create an application security group ...

**Basics** Tags Review + create

### Project details

Subscription *	Azure for Students	▼
Resource group *	AZ500LAB07	▼

[Create new](#)

### Instance details

Name *	myAsgMgmtServers	✓
Region *	East US	▼

- 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:

[Home](#) > [Network security groups](#) >

## Create network security group ...

**Basics**   Tags   Review + create

### Project details

Subscription \*

Azure for Students



Resource group \*

AZ500LAB07

[Create new](#)

### Instance details

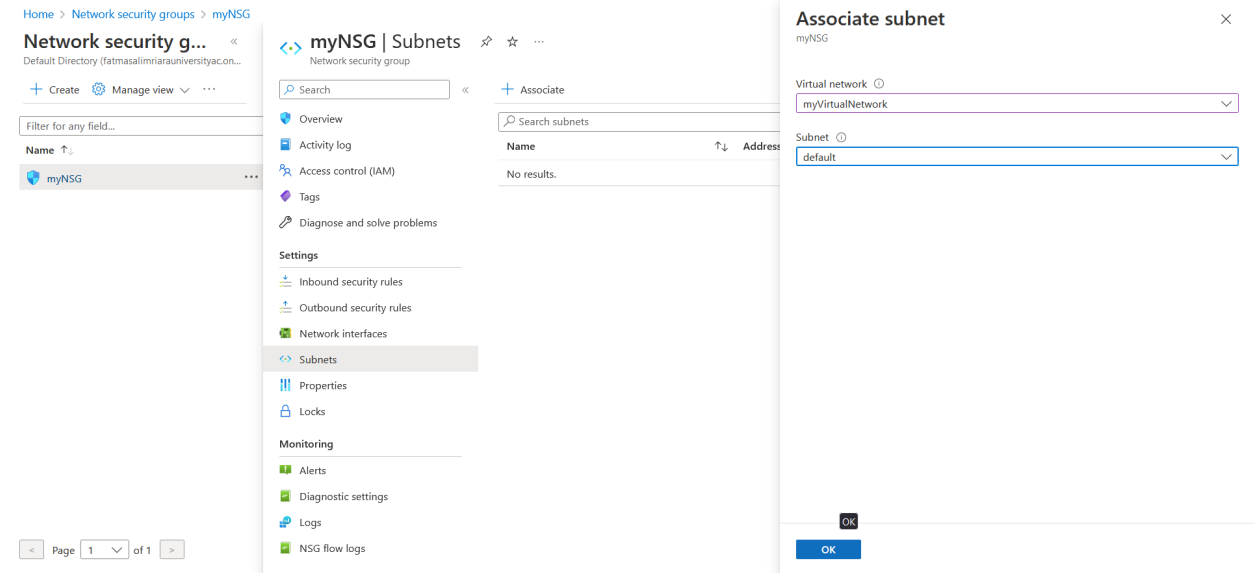
Name \*

myNSG

Region \*

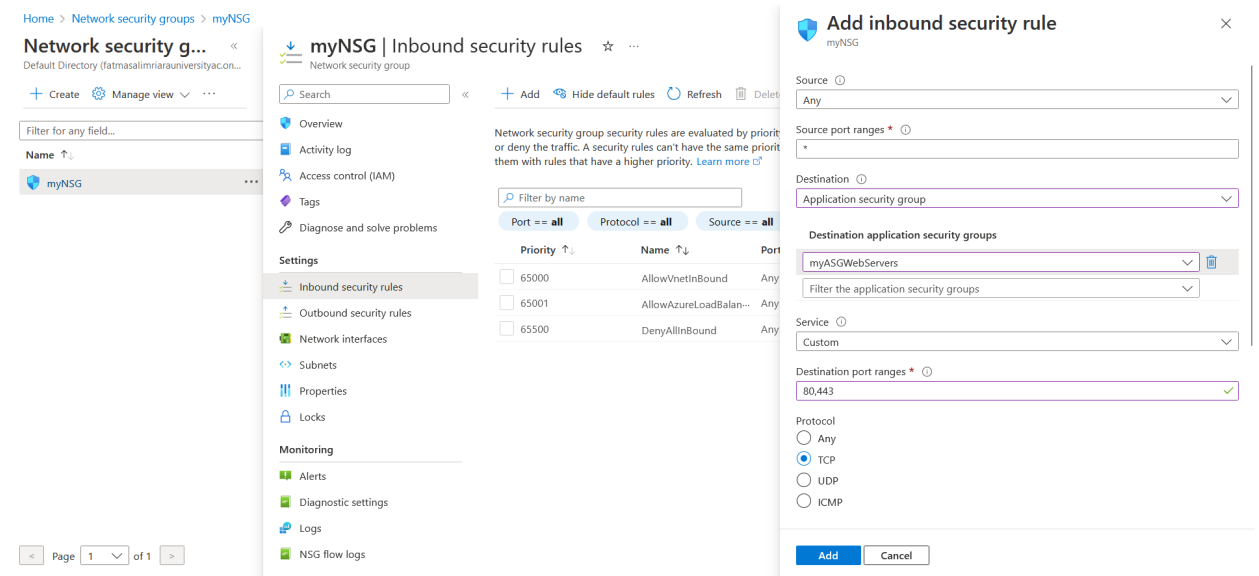
East US

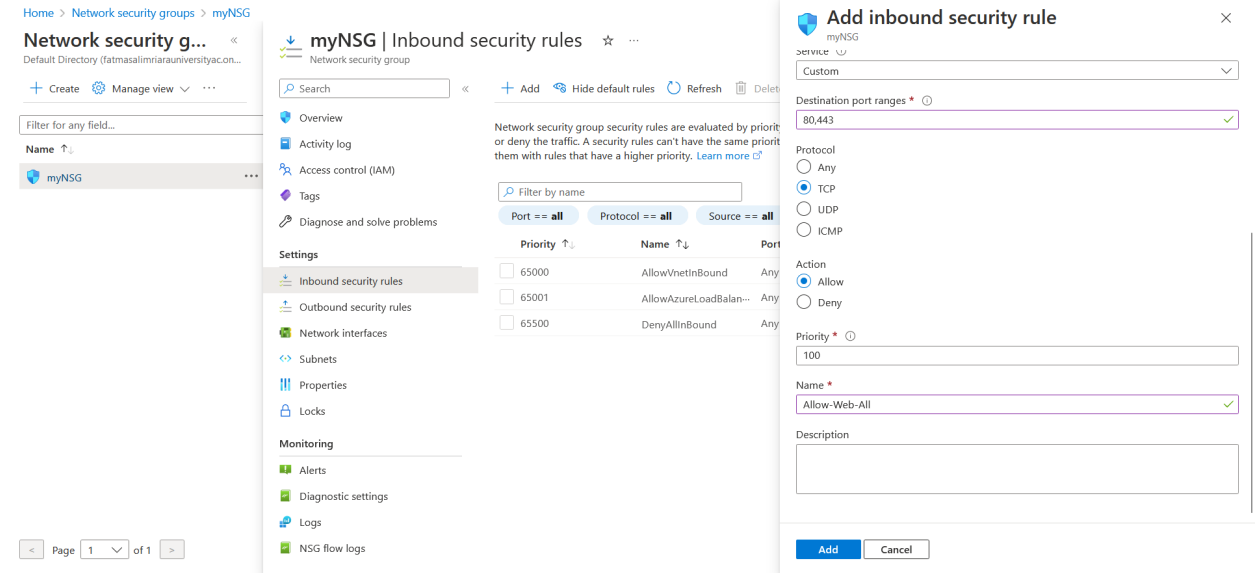
4. Click **Review + create** and then click **Create**.
5. In the Azure portal, navigate back to the **Network security groups** blade and click the **myNsg** entry.
6. On the **myNsg** blade, in the **Settings** section, click **Subnets** and then click **+ Associate**.
7. On the **Associate subnet**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



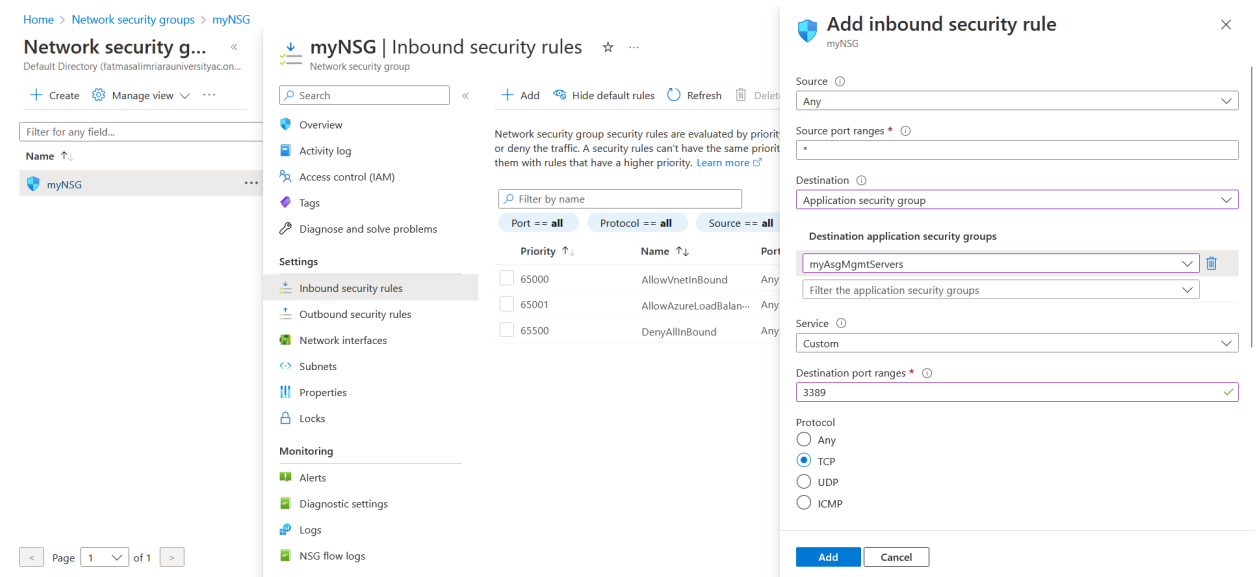
## Task 4: Creating inbound NSG security rules to all traffic to web servers and RDP to the servers.

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):

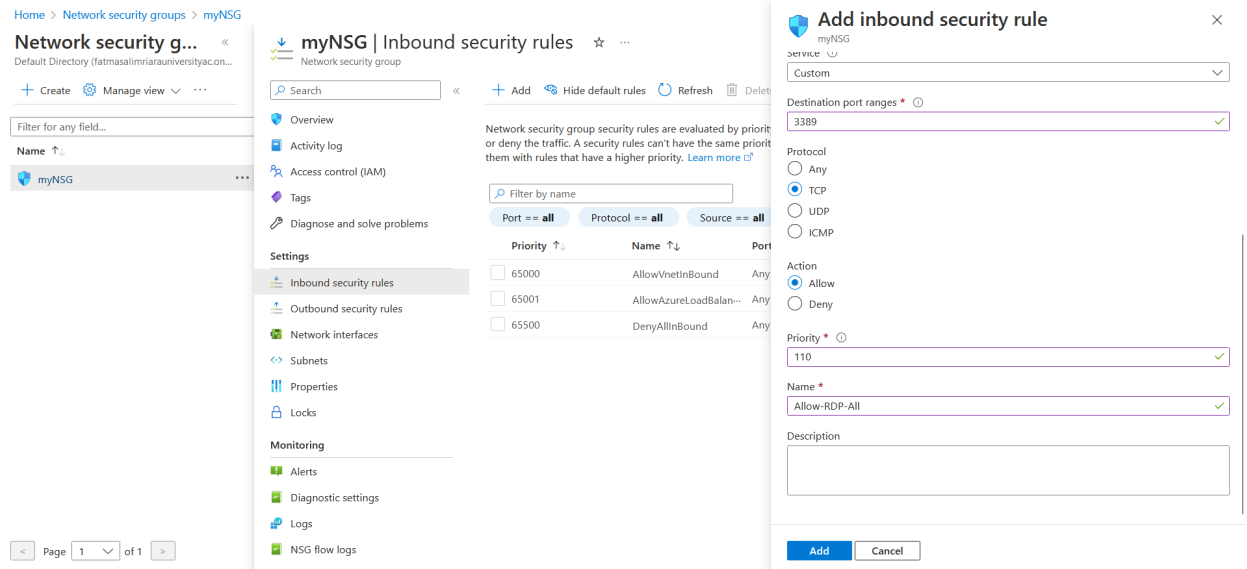




- On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.
- On the **myNSG** blade, in the **Settings** section, click **Inbound security rules**, and then click **+ Add**.
- On the **Add inbound security rule** blade, specify the following settings to allow the RDP 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):

## 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.

## 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.

## Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

### Disk options

OS disk type \* ⓘ

Standard HDD (locally-redundant storage) ▼

Choose Premium SSD disks for lower latency, higher IOPS and bandwidth, and bursting. Single instance virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA. [Learn more](#)

Delete with VM ⓘ



Enable encryption at host ⓘ



Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

Encryption type \*

(Default) Encryption at-rest with a platform-managed key ▼

Enable Ultra Disk compatibility ⓘ



Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard\_D2s\_v3.

### Data disks for myVmWeb

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a

[Review + create](#)

[< Previous](#)

[Next : Networking >](#)

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

- 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** >.

## Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

### Disk options

OS disk type \* ⓘ

Standard HDD (locally-redundant storage) ▼

Choose Premium SSD disks for lower latency, higher IOPS and bandwidth, and bursting. Single instance virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA. [Learn more](#)

Delete with VM ⓘ



Enable encryption at host ⓘ



**i** Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

Encryption type \*

(Default) Encryption at-rest with a platform-managed key ▼

Enable Ultra Disk compatibility ⓘ



Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard\_D2s\_v3.

### Data disks for myVmWeb

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a

[Review + create](#)

[< Previous](#)

[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:

[Home](#) > [Virtual machines](#) >

## Create a virtual machine ...

Basics   Disks   **Networking**   Management   Monitoring   Advanced   Tags   Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#) 

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ

(new) AZ500LAB07-vnet

[Create new](#)

Subnet \* ⓘ

(new) default (10.1.0.0/24)

Public IP ⓘ

(new) myVmWeb-ip

[Create new](#)

NIC network security group ⓘ

☒ None

☐ Basic

☐ Advanced



All ports on this virtual machine may be exposed to the public internet. This is a security risk. Use a network security group to limit public access to specific ports. You can also select a subnet that already has network security groups defined or remove the public IP address.

**Review + create**

< Previous

Next : Management >

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):

# 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

 Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

☐

Size \* ⓘ

Standard D3s v3 - 2 vCPUs, 8 GiB memory (D3s unavailable)

▼

[Home](#) > [Virtual machines](#) >

## Create a virtual machine ...

Username * ⓘ	<input type="text" value="student"/> ✓
Password * ⓘ	<input type="password" value="••••••••"/> ✓
Confirm password * ⓘ	<input type="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 * ⓘ	<input checked="" type="radio"/> None <input type="radio"/> Allow selected ports
--------------------------	---

Select inbound ports	<input type="text" value="Select one or more ports"/> ▼
----------------------	---

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

### Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#) ↗

Would you like to use an existing Windows Server license? * ⓘ	<input type="checkbox"/>
---	--------------------------

[Review Azure hybrid benefit compliance](#) ↗

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**.



[Home](#) > [Virtual machines](#) >

## Create a virtual machine ...


Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#) 

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network <sup>*</sup> ⓘ	<div>(new) AZ500LAB07-vnet</div> <div><a href="#">Create new</a></div>
Subnet <sup>*</sup> ⓘ	<div>(new) default (10.1.0.0/24)</div> <div><a href="#">Create new</a></div>
Public IP ⓘ	<div>(new) myVMMgmt-ip</div> <div><a href="#">Create new</a></div>
NIC network security group ⓘ	<div><input checked="" type="radio"/> None</div> <div><input type="radio"/> Basic</div> <div><input type="radio"/> Advanced</div>

 All ports on this virtual machine may be exposed to the public internet. This is a security risk. Use a network security group to limit public access to specific ports. You can also select a subnet that already has network security groups defined or remove the public IP address.

Delete public IP and NIC when VM is deleted ⓘ ☐

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

[Home](#) > [Virtual machines](#) >

## Create a virtual machine ...

Basics   Disks   Networking   Management   Monitoring   Advanced   Tags   Review + create

Configure monitoring options for your VM.

### Diagnostics

Boot diagnostics ⓘ

- ☒ Enable with managed storage account (recommended)  
☐ Enable with custom storage account  
☐ Disable

Enable OS guest diagnostics ⓘ

☐

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.

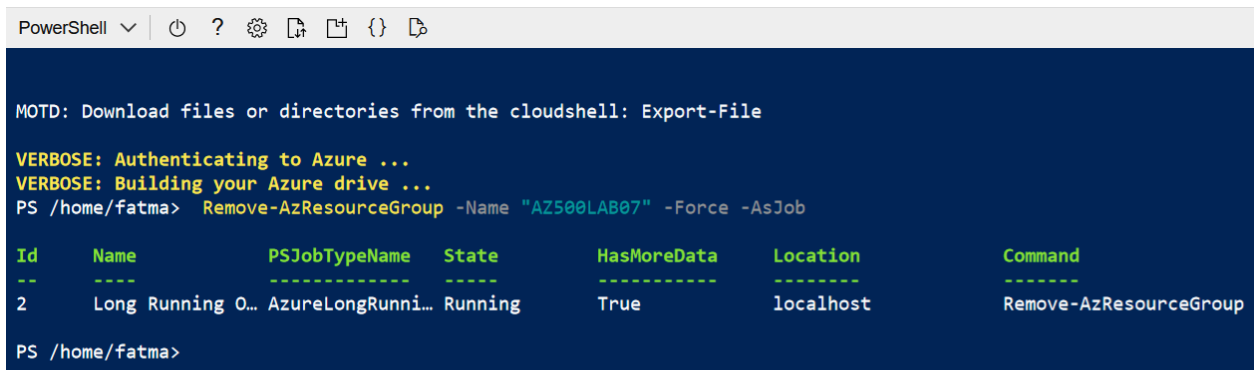
### Task 3: Associating each virtual machines network interface to its application security group.

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:



```
PowerShell v | [Power Icon] ? [Settings Icon] [Copy Icon] [Paste Icon] [Terminal Icon] [Help Icon]
```

MOTD: Download files or directories from the cloudshell: Export-File

VERBOSE: Authenticating to Azure ...  
VERBOSE: Building your Azure drive ...

PS /home/fatma> Remove-AzResourceGroup -Name "AZ500LAB07" -Force -AsJob

Id	Name	PSJobTypeName	State	HasMoreData	Location	Command
2	Long Running O...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup

PS /home/fatma>

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