

M07-Unit 5 Restrict network access to PaaS resources with virtual network service endpoints

Task 1: Create a virtual network

1-3.Select + Create.

[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 * ⓘ

Create new

Instance details

Name *

Region *

West Europe

Review + create

< Previous

Next : IP Addresses >

[Download a template for automation](#)

4. Enter, or select, the following information:

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) myResourceGroup

Create new

Instance details

Name *

CoreServicesVNet

Region *

East US

Review + create

< Previous

Next : IP Addresses >

[Download a template for automation](#)

5. Select the IP Addresses tab and enter the following values (select default to change the subnet name):

HOME / VIRTUAL NETWORKS /

Create virtual network ...

IPv4 address space

10.0.0.0/16

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+

 Add subnet

🗑️

 Remove subnet

Subnet name	Subnet address range	NAT gateway
This virtual network doesn't have any subnets.		

✖

 This virtual network doesn't have any subnets.

ℹ️

 A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Review + create

< Previous

Next : Security >

[Download a template for automation](#)

Add subnet

Subnet name *
Public

Subnet address range * ⓘ
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

NAT GATEWAY

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. [Learn more](#)

NAT gateway
None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Add Cancel

6. Select the Security tab and enter the following values: ![Graphical user interface, text, application, email Description automatically generated](../media/ create-virtual-network-security.png)

Create virtual network ...

Basics

IP Addresses

Security

Tags

Review + create

BastionHost ⓘ

☒ Disable
☐ Enable

DDoS Protection Standard ⓘ

☒ Disable
☐ Enable

Firewall ⓘ

☒ Disable
☐ Enable

7. Click Review + Create. Once the resource is validated select Create

Microsoft.VirtualNetwork-20220928110352 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

We'd love your feedback →

✓ Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20220928... Start time: 9/28/2022, 11:09:36 AM
Subscription: Azure for Students Correlation ID: 15a0b030-96db-4d87-a17d-06660c07dddf
Resource group: myResourceGroup

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 >](#)

Task 2: Enable a service endpoint

1-2. Add a subnet to the virtual network. Under Settings, select Subnets, and then select + Subnet, as shown in the following picture:

Home > Microsoft.VirtualNetwork-20220928110352 | Overview > CoreServicesVNet

CoreServicesVNet | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

Name	IPv4	IPv6	Available
Public	10.0.0.0/24	-	251

Name *

Subnet address range * 10.0.1.0/24 10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space

NAT gateway None

Network security group None

Route table None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Save Cancel

3. Under Add subnet, select or enter the following information

CoreServicesVNet

Gateway subnet Refresh Manage users Delete

IPv4 ↑↓	IPv6 ↑↓	Available
10.0.0.0/24	-	251

Add subnet

None

Network security group

None

Route table

None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

Microsoft.Storage

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

Save Cancel

1. 4. Select **Save**.

CoreServicesVNet | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Search subnets

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
Public	10.0.0.0/24	-	251	-	-	-	...
Private	10.0.1.0/24	-	251	-	-	-	...

Task 3: Restrict network access for a subnet

1-2. In Network security groups, select + Create.

Create network security group ...

Basics

Tags

Review + create

Project details

Subscription *

Azure for Students

Resource group *

Create new

Instance details

Name *

Region *

West Europe

Review + create

< Previous

Next : Tags >

Download a template for automation

3. Enter or select, the following information:

Create network security group ...

Basics

Tags

Review + create

Project details

Subscription *

Azure for Students

Resource group *

myResourceGroup

Create new

Instance details

Name *

ContosoPrivateNSG

Region *

East US

Review + create

< Previous

Next : Tags >

Download a template for automation

4-5. After the ContosoPrivateNSG network security group is created, select Go to resource.

Microsoft.NetworkSecurityGroup-20220928111639 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.NetworkSecurityGroup-20220... Start time: 9/28/2022, 11:19:04 AM
Subscription: Azure for Students Correlation ID: bc7f35e1-504d-4e44-9965-f784b203bf
Resource group: myResourceGroup

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 >

6-7. Select + Add.

Home > Microsoft.NetworkSecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Outbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Filter by name

Port == all Protocol =

Priority	Name	Port	Protocol
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

Network security group security rules are evaluated by priority using the combination of priority and direction. Security rules can't have the same priority and direction as an existing rule. You can't delete a rule that is part of a rule set. [Learn more](#)

Source

Any

Source port ranges

*

Destination

Any

Service

Custom

Destination port ranges

8080

Protocol

Any

TCP

UDP

ICMP

Action

Add Cancel

8. Create a rule that allows outbound communication to the Azure Storage service. Enter, or select, the following information:

19 | Overview > ContosoPrivateNSG

Outbound security rules

Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of rule name, priority, and direction. Rules with the same priority and direction as an existing rule. You can't delete a rule that is associated with a network interface.

Name ↑↓	Port ↑↓	Protocol
AllowVnetOutBound	Any	Any
AllowInternetOutBound	Any	Any
DenyAllOutBound	Any	Any

Add outbound security rule ContosoPrivateNSG

Source ^①

Source service tag * ^①

Source port ranges * ^①

Destination ^①

Destination service tag ^①

Service ^①

Destination port ranges * ^①

Protocol

☒ Any

Add **Cancel**

SecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Outbound security rules

« + Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of rule name, priority, and direction. Rules with the same priority and direction as an existing rule. You can't delete a rule that is associated with a network interface. [Learn more](#)

Filter by name

Port == all Protocol ==

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

Add outbound security rule ContosoPrivateNSG

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority * ^①

Name *

Description

Add **Cancel**

9. Select Add:

Home > Microsoft.NetworkSecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Outbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Task 4: Add additional outbound rules

1. Select +Add under Outbound security rules. +2. Enter, or select, the following information:

Home > Microsoft.NetworkSecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Outbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Add outbound security rule

ContosoPrivateNSG

Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Action

☐ Allow

☒ Deny

Priority * ⓘ

110 ✓

Name *

Deny-Internet-All ✓

Description

Add Cancel

3. Select Add.

ContosoPrivateNSG | Outbound security rules

Network security group

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-Storage-All	Any	Any	VirtualNetwork	Storage	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Task 5: Allow access for RDP connections

1. On ContosoPrivateNSG | Outbound security rules, under Settings, select Inbound security rules.

Home > Microsoft.Network.SecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Inbound security rules

Network security group

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnose and solve problems

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all

Protocol == all

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule

ContosoPrivateNSG

Source

Any

Source port ranges *

*

Destination

Any

Service

Custom

Destination port ranges *

8080

Protocol

Any

TCP

UDP

ICMP

Action

Allow

Deny

Add

Cancel

2.-3. In Add inbound security rule, enter the following values::

Home > Microsoft.NetworkSecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Inbound security rules

Network security group

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostic settings

+ Add

Hide default rules

Refresh

Delete

Give feedback

Filter by name

Port == all

Protocol == all

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority.

Learn more

Priority	Name	Port	Protocol	Action
65000	AllowVnetInBound	Any	Any	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	Allow
65500	DenyAllInBound	Any	Any	Deny

Add inbound security rule

ContosoPrivateNSG

Protocol

Any

TCP

UDP

ICMP

Action

Allow

Deny

Priority

120

Name

Allow-RDP-AnyToAny

Description

Add

Cancel

4. And then select Add.

Home > Microsoft.NetworkSecurityGroup-20220928111639 | Overview > ContosoPrivateNSG

ContosoPrivateNSG | Inbound security rules

Network security group

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

+ Add

Hide default rules

Refresh

Delete

Give feedback

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority.

Learn more

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

5. -6. Select + Associate.

The screenshot shows the Azure portal interface for a Network Security Group (NSG) named 'ContosoPrivateNSG'. The left-hand navigation pane is open, showing various settings and monitoring options. The 'Subnets' option is selected. The main pane displays the 'Associate' button. A dialog box titled 'Associate subnet' is open, showing a search bar for subnets and a table with columns 'Name' and 'Address range'. The table currently shows 'No results.' The dialog also includes a 'Virtual network' dropdown menu and an 'OK' button.

7. Under Associate subnet, select Virtual network and then select CoreServicesVNet under Choose a virtual network.

This screenshot shows the same 'Associate subnet' dialog box as the previous one, but with the 'Virtual network' dropdown menu expanded. The 'CoreServicesVNet' option is selected. The 'Subnet' dropdown menu is also visible, showing a search bar and a list of subnets. The 'OK' button is at the bottom of the dialog.

8. Under Choose subnet, select Private, and then select OK.

[Overview](#) > [ContosoPrivateNSG](#)

✦ ☆ ...

↑↓	Address range

Associate subnet

ContosoPrivateNSG

Virtual network ⓘ
CoreServicesVNet

Subnet ⓘ
Private

Task 6: Restrict network access to a resource

1-2. Select +Create.

[Home](#) > [Storage accounts](#)

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ * contostorageit

Region ⓘ * (US) East US

Performance ⓘ *
☒ Standard: Recommended for most scenarios (general-purpose v2 account)
☐ Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ * Locally-redundant storage (LRS)

[Review](#) < Previous Next: Advanced >

7. select Review + create, then click Create.

The screenshot shows the Azure portal interface for a deployment named 'contosostorageit_1664358834915'. The left sidebar contains a search bar and a navigation menu with 'Overview' (selected), 'Inputs', 'Outputs', and 'Template'. The main content area has a top bar with 'Delete', 'Cancel', 'Redeploy', 'Download', and 'Refresh' buttons. Below this, a message says 'We'd love your feedback!'. The central part of the page displays 'Your deployment is complete' with a green checkmark. It lists deployment details: 'Deployment name: contosostorageit_16643588349...', 'Subscription: Azure for Students', 'Resource group: myResourceGroup', 'Start time: 9/28/2022, 11:54:10 AM', and 'Correlation ID: b6b30ce5-f820-4a9e-a244-dd87936b2619'. There are expandable sections for 'Deployment details' and 'Next steps', with a 'Go to resource' button. On the right, there are three informational cards: 'Cost Management' (with a 'Set up cost alerts' link), 'Microsoft Defender for Cloud' (with a 'Go to Microsoft Defender for Cloud' link), and 'Free Microsoft tutorials' (with a 'Start learning today' link).

Task 7: Create a file share in the storage account

1-2. Select File shares, as shown in the following picture:

The screenshot shows the 'File shares' page in the Azure portal for the 'contosostorageit' storage account. The left sidebar has a search bar and a navigation menu with 'Data migration', 'Events', 'Storage browser', 'Data storage' (expanded), 'File shares' (selected), 'Queues', 'Tables', 'Security + networking' (expanded), 'Networking', 'Azure CDN', 'Access keys', 'Shared access signature', and 'Encryption'. The main content area has a top bar with '+ File share' and 'Refresh' buttons. Below this, the 'File share settings' section shows 'Active Directory: Not configured', 'Soft delete: 7 days', 'Maximum capacity: 5 TiB', and 'Security: Maximum compatibility'. There is a search bar for file shares and a 'Show deleted shares' toggle. A table with columns 'Name', 'Modified', 'Tier', and 'Quota' is shown, but it is empty with the message 'You don't have any file shares yet. Click '+ File share' to get started.'

3.-4. Enter marketing under Name, and then select Create.

The image shows two screenshots of the Azure portal interface for managing file shares in a storage account named 'contosostorageit'.

Top Screenshot: 'New file share' dialog

- Name:** marketing
- Tier:** Transaction optimized
- Performance:**
 - Maximum IO/s: 1000
 - Egress Rate: 60 MiB / s
 - Ingress Rate: 60 MiB / s
 - Maximum capacity: 5 TiB
 - Large file shares: Disabled
- Buttons:** Create, Cancel

Bottom Screenshot: 'File shares' overview

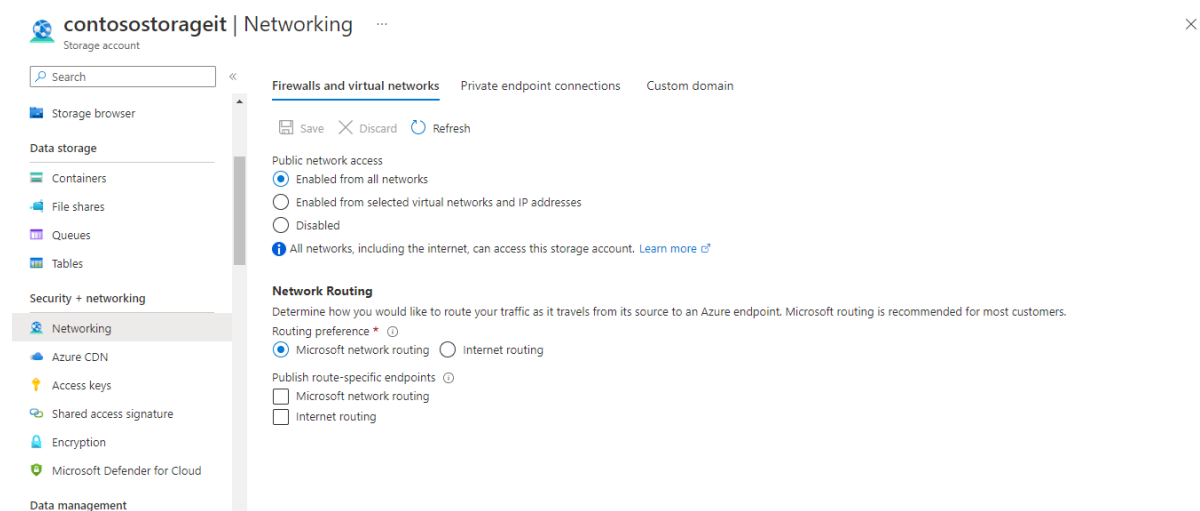
File share settings: Active Directory: Not configured, Soft delete: 7 days, Maximum capacity: 5 TiB, Security: Maximum compatibility

Search file shares by prefix (case-sensitive)

Name	Modified	Tier	Quota
marketing	9/28/2022, 11:58:54 AM	Transaction optimized	5 TiB

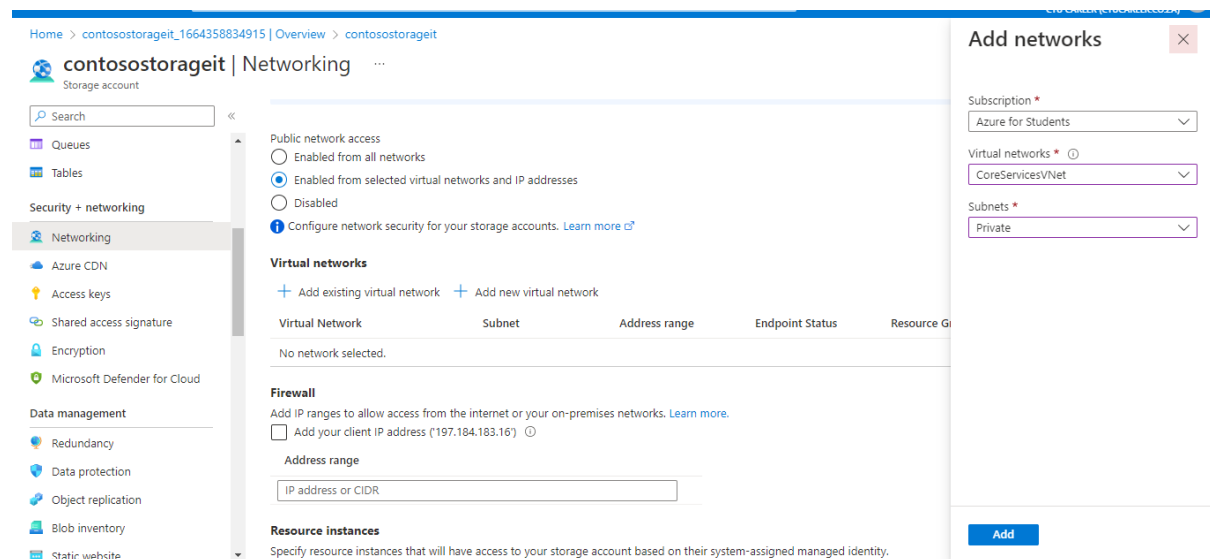
Task 8: Restrict network access to a subnet

1-2. Select Selected networks.



The screenshot shows the Azure portal interface for the 'contosostorageit' storage account. The left sidebar contains navigation links for 'Storage browser', 'Data storage' (Containers, File shares, Queues, Tables), 'Security + networking' (Networking, Azure CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), and 'Data management'. The main content area is titled 'Networking' and has three tabs: 'Firewalls and virtual networks' (selected), 'Private endpoint connections', and 'Custom domain'. Under 'Firewalls and virtual networks', there are buttons for 'Save', 'Discard', and 'Refresh'. The 'Public network access' section has three radio buttons: 'Enabled from all networks' (selected), 'Enabled from selected virtual networks and IP addresses', and 'Disabled'. Below this is a note: 'All networks, including the internet, can access this storage account. [Learn more](#)'. The 'Network Routing' section has a heading 'Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.' and a 'Routing preference' section with two radio buttons: 'Microsoft network routing' (selected) and 'Internet routing'. Below this is a 'Publish route-specific endpoints' section with two checkboxes: 'Microsoft network routing' and 'Internet routing'.

3.-4. Under Add networks, select the following values:



The screenshot shows the same Azure portal interface as before, but with the 'Add networks' dialog box open on the right side. The dialog has a title bar with a close button. It contains three dropdown menus: 'Subscription' (set to 'Azure for Students'), 'Virtual networks' (set to 'CoreServicesVNet'), and 'Subnets' (set to 'Private'). At the bottom of the dialog is a blue 'Add' button. The background page shows the 'Public network access' section with 'Enabled from selected virtual networks and IP addresses' selected, and the 'Virtual networks' section with a table showing 'No network selected'.

5.-6. Select Save.

Home > contosostorageit_1664358834915 | Overview > contosostorageit

contosostorageit | Networking

Search

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Redundancy

Data protection

Object replication

Blob inventory

Static website

Firewalls and virtual networks

Private endpoint connections

Custom domain

Save Discard Refresh

Public network access

Enabled from all networks

Enabled from selected virtual networks and IP addresses

Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

Add existing virtual network Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
CoreServicesVNet	1			myResourceGroup	Azure for Students

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

Add your client IP address (197.184.183.16)

Address range

IP address or CIDR

Successfully saved firewall and virtual network settings

Successfully saved firewall and virtual network settings for storage account 'contosostorageit'.

7. Under Security and Networking for the storage account, select Access keys. +8. Select Show Keys. Note the Key value, as you'll have to manually enter it in a later step when mapping the file share to a drive letter in a VM.

Home > contosostorageit_1004500034915 | Overview > contosostorageit

contosostorageit | Access keys

Search

Queues

Tables

Security + networking

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Redundancy

Data protection

Object replication

Blob inventory

Static website

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account. [Learn more about managing storage account access keys](#)

Storage account name

contosostorageit

key1 Rotate key

Last rotated: 28/09/2022 (0 days ago)

Key

w2Yus3CoFPckqHVPO03kNtLpGnGROe2t8EQCAaNVzhHYbScvX7g3eDjn97wpy...

Hide

Connection string

DefaultEndpointsProtocol=https;AccountName=contosostorageit;AccountKey=w...

Hide

key2 Rotate key

Last rotated: 28/09/2022 (0 days ago)

Key

DG2iVWct/sjyc7XV9n/YVWPj0Lj50jeY0DWVTEZrt6KZocVpNSohQ8iNMAkFD9lo...

Hide

Connection string

DefaultEndpointsProtocol=https;AccountName=contosostorageit;AccountKey=D...

Hide

Task 9: Create virtual machines

1-2. In the toolbar of the Cloud Shell pane, select the Upload/Download files icon, in the drop-down menu, select Upload and upload the following files VMs.json and VMs.parameters.json into the Cloud Shell home directory one by one from the source folder F:\Allfiles\Exercises\M07. +3. Deploy the following ARM templates to create the VMs needed for this exercise:

```
Type "help" to learn about Cloud Shell

MOTD: Read more about PowerShell in CloudShell: https://aka.ms/pscloudshell/docs

VERBOSE: Authenticating to Azure ...
VERBOSE: BuildingNew-AzResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile VMs.json -TemplateParameterFile VMs.parameters.json
PS /home/ilunga> New-AzResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile VMs.json -TemplateParameterFile VMs.param
DeploymentName      : VMs
ResourceGroupName   : myResourceGroup
ProvisioningState    : Succeeded
Timestamp           : 9/28/2022 10:48:36 AM
Mode                 : Incremental
TemplateLink         :
Parameters
  Name      Type      Value
  =====
  vmName1   String    "ContosoPublic"
  nicName1   String    "ContosoPublic-nic"
  vmName2   String    "ContosoPrivate"
  nicName2   String    "ContosoPrivate-nic"
  vmSize     String    "Standard_DS1_v2"
  adminUsername String    "TestUser"
  adminPassword SecureString null

Outputs
DeploymentDebugLogLevel :

PS /home/ilunga>
```

4. When the deployment is complete, go to the Azure portal home page, and then select Virtual Machines.

Virtual machines

CTU Career (ctucareer.co.za)

Create

Switch to classic

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Filter for any field...

Subscription equals all

Type equals all

Resource group equals all

Location equals all

Add filter

No grouping

List view

<input type="checkbox"/>	Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public
<input type="checkbox"/>	ContosoPrivate	Virtual machine	Azure for Students	myResourceGroup	East US	Running	Windows	Standard_DS1_v2	20.169.
<input type="checkbox"/>	ContosoPublic	Virtual machine	Azure for Students	myResourceGroup	East US	Running	Windows	Standard_DS1_v2	20.124.

< Previous

Page 1 of 1

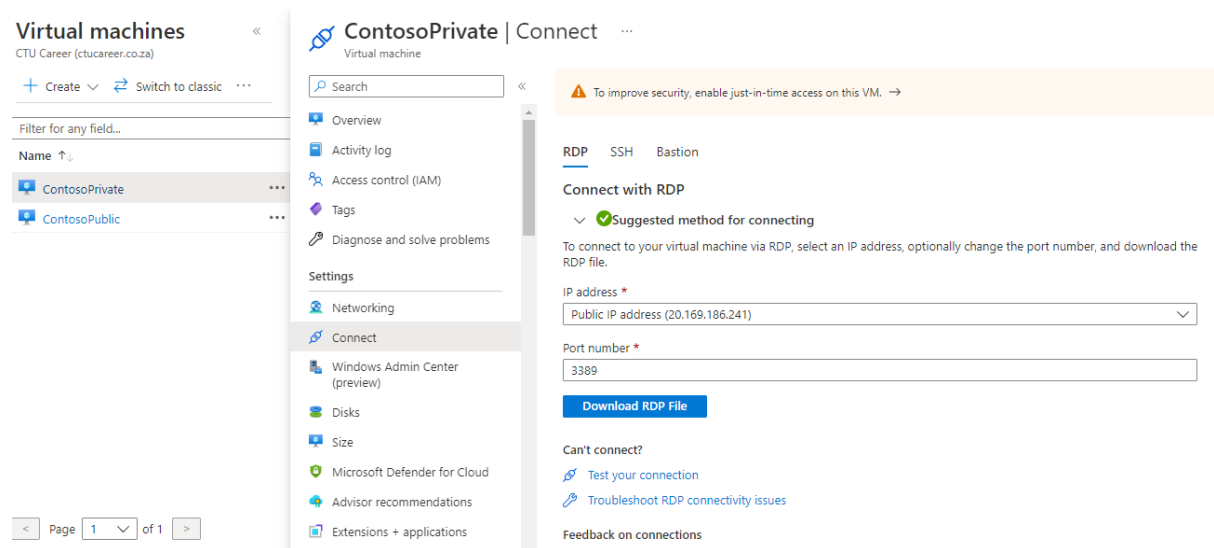
Next >

Showing 1 to 2 of 2 records.

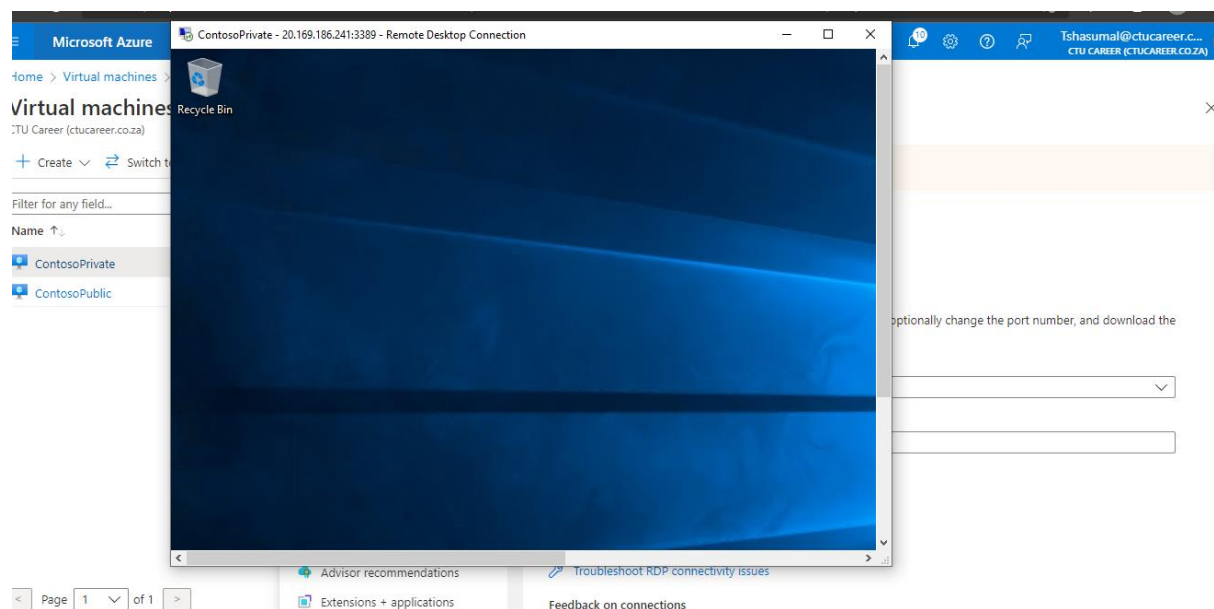
Give feedback

Task 10: Confirm access to storage account

1. Once the ContosoPrivate VM finishes creating, open the blade for the VM by selecting Go to resource. Select the Connect button, then select RDP.



- 3.-5. You may receive a certificate warning during the sign-in process. If you receive the warning, select Yes or Continue to proceed with the connection.



6.-7. Confirm that the VM has no outbound connectivity to the internet from a command prompt:

```

Name                Used (GB)    Free (GB) Provider      Root
-----
Z                    -           -           FileSystem    \\contosostoragean1.file.core.wi...

PS C:\Users\TestUser> ping bing.com

Pinging bing.com [204.79.197.200] with 32 bytes of data:
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119

Ping statistics for 204.79.197.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\TestUser> ping bing.com

Pinging bing.com [204.79.197.200] with 32 bytes of data:
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119

Ping statistics for 204.79.197.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\TestUser> $acctKey = ConvertTo-SecureString -String "V7T0g746fgblIszCImvqI4r92kwo2BMt2LfMTn1Pz9kcxl"
>>
>> $credential = New-Object System.Management.Automation.PSCredential -ArgumentList "contosostoragean1", $acctKey

```

Confirm access is denied to storage account

1-4. Confirm that the public VM does have outbound connectivity to the internet from a command prompt:

ping bing.com

```

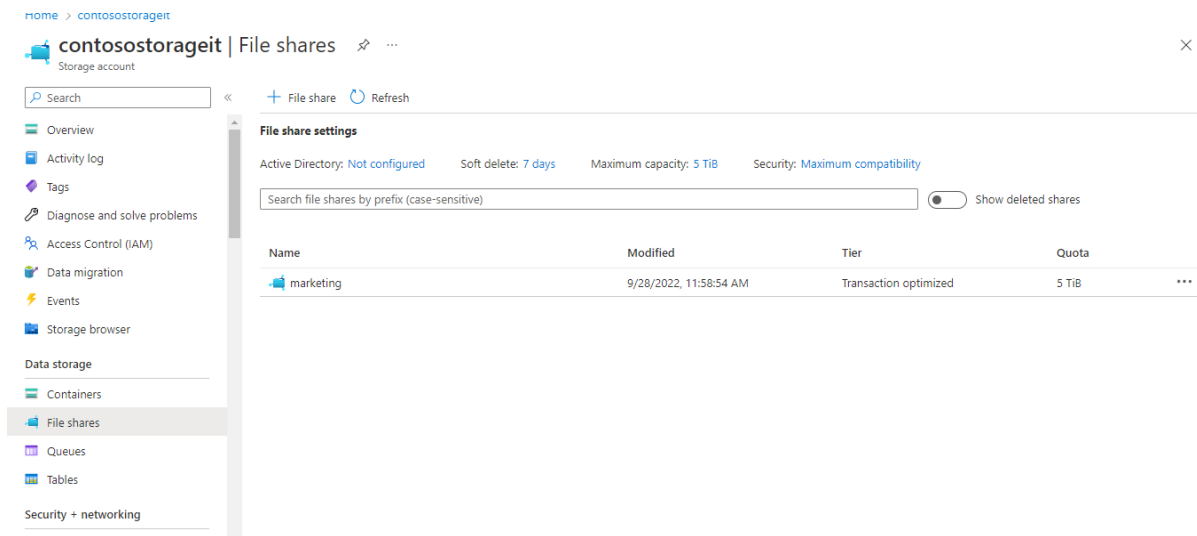
PS C:\Users\TestUser> ping bing.com

Pinging bing.com [204.79.197.200] with 32 bytes of data:
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119
Reply from 204.79.197.200: bytes=32 time=1ms TTL=119

Ping statistics for 204.79.197.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\TestUser>

```

5.-7. Enter the name of the storage account you created in the Search resources, services, and docs box. When the name of your storage account appears in the search results, select it



Home > contosostorageit | File shares

Storage account

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Data storage

Containers

File shares

Queues

Tables

Security + networking

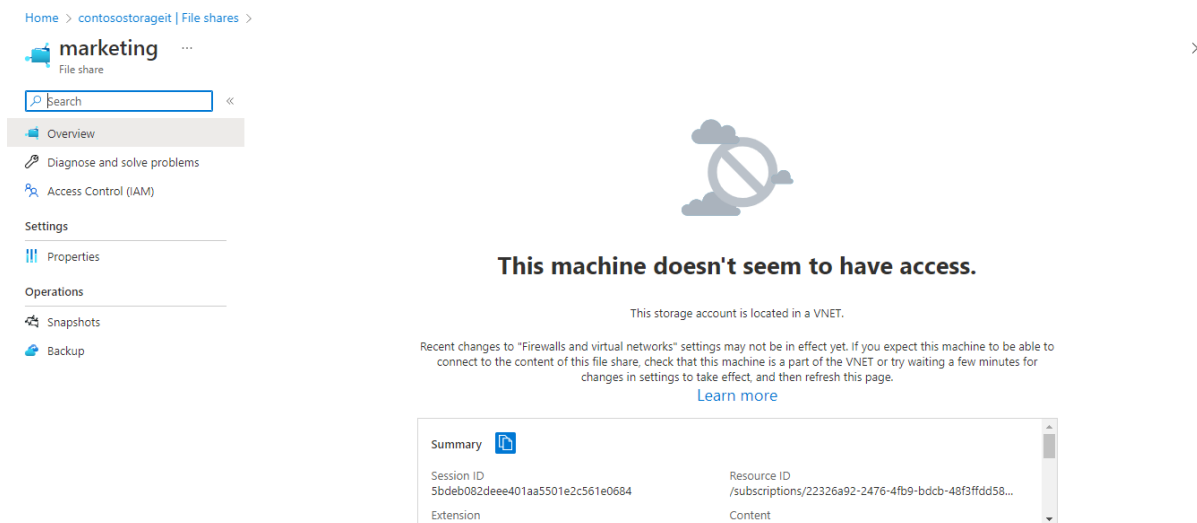
File share settings

Active Directory: Not configured Soft delete: 7 days Maximum capacity: 5 TiB Security: Maximum compatibility

Search file shares by prefix (case-sensitive) ☐ Show deleted shares

Name	Modified	Tier	Quota	
marketing	9/28/2022, 11:58:54 AM	Transaction optimized	5 TiB	...

8. Select File shares then select the marketing file share.+9. You receive the error shown in the following screenshot:



Home > contosostorageit | File shares > marketing

File share

Search

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

Properties

Operations

Snapshots

Backup

This machine doesn't seem to have access.

This storage account is located in a VNET.

Recent changes to "Firewalls and virtual networks" settings may not be in effect yet. If you expect this machine to be able to connect to the content of this file share, check that this machine is a part of the VNET or try waiting a few minutes for changes in settings to take effect, and then refresh this page.

[Learn more](#)

Summary

Session ID	Resource ID
5bdeb082deee401aa5501e2c561e0684	/subscriptions/22326a92-2476-4fb9-bdcb-48f3ffdd58...
Extension	Content

Task 11: Clean up resources

1.-2. Delete all resource groups you created throughout the labs of this module by running the following command:

```
PowerShell | ? | ? | ? | ? | {} | 
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

MOTD: Modules installed with 'Install-Module' are persisted across sessions

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/ilunga> Remove-AzResourceGroup -Name 'myResourceGroup' -Force -AsJob

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

PS /home/ilunga>
```